INVESTIGATION OF PRIMARY USER EMULATION ATTACK IN COGNITIVE RADIO NETWORKS

by

Chao Chen

A Proposal

Submitted to the Faculty of the Stevens Institute of Technology
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chao Chen, Candidate	Date

ADVISORY COMMITTEE

Yu-Dong Yao, Chairman	Date
Yingying Chen	Date
Koduvayur Subbalakshmi	Date
Jose Emmanuel Ramirez-Marquez	Date

STEVENS INSTITUTE OF TECHNOLOGY
Castle Point on Hudson
Hoboken, NJ 07030
2010

INVESTIGATION OF PRIMARY USER EMULATION ATTACK IN COGNITIVE RADIO NETWORKS

ABSTRACT

Cognitive radio technology (CR), as a key enabling functionality for the next generation (xG) mobile communication, can remarkably improve the performance of a wireless communication system by being aware of the changes of its surrounding and dynamically modifying its operating parameters to adapt such changes. Recently, the security issues of cognitive radio (CR) networks have drawn more and more research attentions. As the one of attacks against CR system, primary user emulation attack (PUEA) compromises the spectrum sensing of cognitive radio, where a malicious user forestalls vacant channels by impersonating the primary user to prevent other secondary users from accessing the idle frequency bands. In this thesis, we first introduce the background, motivation and advances of cognitive radio technology and summarize the security issues in the cognitive radio networks. After presenting the concept of spectrum sensing as well as its implementation approaches and current challenges, we propose a new cooperative spectrum sensing scheme, considering the existence of PUEA in CR networks. In the proposed scheme, the sensing information of different secondary users is combined at a fusion center and the combining weights are optimized with the objective of maximizing the detection probability of idle channels under the constraint of a required false alarm probability. We also investigate the impact of the channel estimation errors and multiple PUE attackers on the detection probability. Numerical and simulation results illustrate the advantages of the proposed scheme over the conventional maximal ratio combining (MRC) scheme in the cooperative spectrum sensing with the existence of PUEA.

Author: Chao Chen
Advisor: Yu-Dong Yao
Date: November, 2010
Department: Electrical and Computer Engineering
Degree: Doctor of Philosophy

Acknowledgments

Contents

List of Tables vii

List of Figures viii

1 Introduction **1**

1.1 Background and Motivation 1

1.2 Cognitive Radio Technology 2

1.2.1 What is Cognitive Radio? 2

1.2.2 Why Cognitive Radio? 3

1.2.3 Advances in Cognitive Radio Technology 5

1.3 Security Issues in Cognitive Radios 7

1.4 Thesis Organization 8

2 Spectrum Sensing in Cognitive Radios and Primary User Emulation Attack **10**

2.1 The Concept of Spectrum Opportunity 10

2.2 Spectrum Sensing in Cognitive Radio 11

2.2.1 Spectrum Sensing Methods 12

2.2.2 Challenges in Spectrum Sensing 17

2.3 Primary User Emulation Attack in Spectrum Sensing 20

2.3.1 Primary User Emulation Attack 20

2.3.2 Detection Schemes of PUEA 21

2.3.3 Defense Schemes against PUEA 21

3 Cooperative Spectrum Sensing in the Presence of PUEA **23**

3.1 Introduction 23

3.2 System Model 24
3.3 Optimal Combining Scheme for Cooperative Spectrum Sensing in the Presence of PUEA 26
3.4 Simulation Results 30
3.5 Conclusion 32

4 Cooperative Spectrum Sensing in the Presence of PUEA with Channel Estimation Error 33

5 Cooperative Spectrum Sensing with Multiple PUE Attackers 35

6 Conclusion and Future Work 36

6.1 Cooperative Spectrum Sensing in the presence of PUEA when Considering Channel Estimation Error 36
6.2 Cooperative Spectrum Sensing in the presence of PUEA when Considering Multiple PUE Attackers 36

Bibliography 37

List of Tables

List of Figures

1.1 The cognitive cycle [4] 2

1.2 Frequency allocation chart in United States [6] 4

1.3 The concept of spectrum hole [5] 5

2.1 Multiple dimensional spectrum opportunity [8] 11

2.2 Non-cooperative sensing problem 15

2.3 Interference temperature spectrum sensing [5] 17

3.1 System model of cooperative spectrum sensing with PUEA in cognitive radio network 24

3.2 Detection probability versus false alarm probability for the proposed optimal combining, conventional MRC and non-cooperative sensing schemes, SNR = 0 dB, $N = 4$ 30

3.3 Detection probability versus average SNR γ_p, $P_f = 10^{-1}$ and $\rho = 0.1, 1, 10$, $N = 4$ 32

4.1 Detection performance of proposed optimal combining and conventional MRC scheme, $\sigma^2_{e_m}$ = -15 dB, -10 dB, -5 dB and $\sigma^2_{e_p}$ = -15 dB, SNR = 0 dB, $N = 4$ 34

4.2 Detection performance of proposed optimal combining and conventional MRC scheme, $\sigma^2_{e_p}$ = -15 dB, -10 dB, -5 dB and $\sigma^2_{e_m}$ = -15 dB, SNR = 0 dB, $N = 4$ 34

Chapter 1

Introduction

1.1 Background and Motivation

Cognitive radio (CR) technology, proposed by Mitola, allows unlicensed (secondary) users to access the licensed (primary) frequency bands without interfering with the licensed users in order to realize more effective and reliable communication [1]. Spectrum sensing, as a fundamental functionality of cognitive radio, enables the secondary users to monitor the frequency spectrum and detect vacant channels to use. Among the various sensing schemes for CR networks, cooperative spectrum sensing method stands out due to its high detection performance of spectrum holes. Meanwhile, the security issues of cognitive radio have received more and more attentions recently since the intrinsic properties of CR networks would pose new challenges to wireless communications. Primary user emulation attack (PUEA), proposed by Chen and Park, identifies one potential vulnerability of spectrum sensing in CR networks where an attacker occupies the unused channels by emitting a signal with similar form as the primary user so as to deter the access of the vacant channels from other secondary users [2]. To date, several detection approaches of PUEA have been presented, however, the detection performance of white spaces in the presence of PUEA is not yet well understood. In this dissertation, we will investigate the detection performance of vacant channels in CR network in the presence of PUEA, attempting to mitigate the impact of PUEA on the detection performance of white spaces in CR networks. We will

give a brief overview of cognitive radio technology before introducing our own work.

1.2 Cognitive Radio Technology

In this section, we will present the background of emergence of cognitive radio technology. We will also briefly introduce the definition, classification, functions and advances of cognitive radio technology.

1.2.1 What is Cognitive Radio?

Cognitive radio is a technology for wireless communications in which a network or a user flexibly changes its transmitting or receiving parameters to achieve more efficient communication performance without interfering with primary or secondary users [3]. Under the assumption of cognitive radio, wireless system should be sufficiently smart to recognize the variation of the environment and dynamically adjust its operational parameters to accommodate the alternations. Figure 1.1 illustrates the basic cognitive cycle in cognitive radio [4]. Simply put, the cognitive radio technique generally includes four main functions

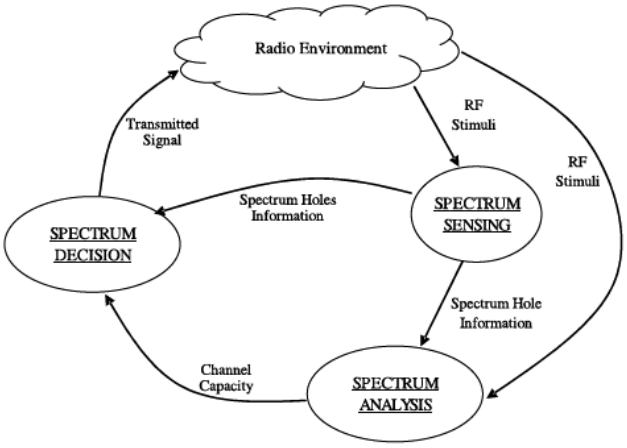


Figure 1.1: The cognitive cycle [4]

as follows [5].

- Spectrum Sensing

Spectrum sensing detects and shares the available spectrum without detrimental interference with other users. It is critical for cognitive radio network to find spectrum holes. And the most efficient and effective way to detect spectrum holes is to detect primary users.

- Spectrum Management

  Spectrum management captures the best available spectrum to meet the needs of the communication requirement among users. Cognitive radio users should select the best spectrum band to satisfy the quality of service (QoS) requirements over all available bands, which necessitates the spectrum management functions such as spectrum analysis and spectrum decision for cognitive radio users.

- Spectrum Sharing

  Spectrum sharing provides the fair spectrum scheduling mechanism. It exhibits some similarities of the classical media access control MAC problems in current wireless systems. Spectrum sharing can be classified as centralized and distributed; non-cooperative and cooperative; overlay and underlay in terms of different criteria as architecture, allocation behavior and access technique respectively.

- Spectrum Mobility

  Spectrum mobility is defined as a process that a secondary user vacates or switches to other channels than the one it is using when current channel conditions become worse or a primary user appears. Cognitive radio networks utilize the spectrum in a dynamic manner by allowing the radio terminals to operate in the best available frequency band, maintaining seamless communication requirements during the transition to better spectrum.

1.2.2 Why Cognitive Radio?

The radio frequency spectrum, as a natural resource, is an important medium bridging transmitters and receivers in wireless communications. The frequency spectrum is regulated and licensed by the governments or some government-aided organizations such as

Federal Communications Commission (FCC) in United States. Under the regulation of the governments or such organizations, frequency bands are statically assigned to different means or purposes of wireless communications. For example, the broadcasting FM radio stations goes from 87.5 to 108.0 MHz and low band TV VHF (Ch.2-6) ranges from 59 - 88 MHz [6]. Users that are allowed to use a specific band are called licensed (primary) users and others are called unlicensed (secondary or CR) users. During the past decades, a common belief that the radio frequency spectrum is a scarce resource has been pervasively accepted due to the ever-increasing growth of the wireless communication technology and the high demand of the capacity and date rates for wireless multimedia services. Figure 1.2

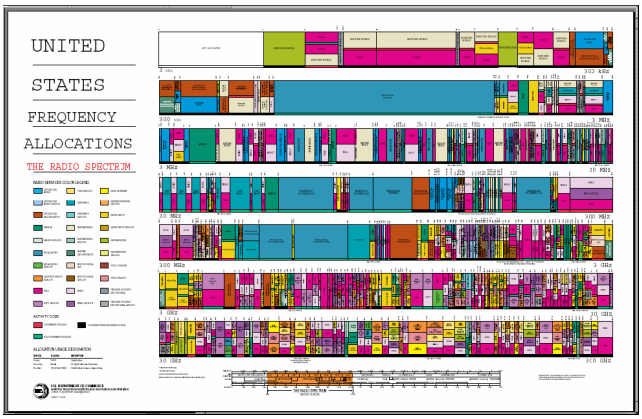


Figure 1.2: Frequency allocation chart in United States [6]

shows the radio spectrum frequency allocations in United States (as of 2003). It is indicated from the chart that there is no available bands left for the wireless systems or devices to use in the future. Nonetheless, the in-depth research work on the situation of the frequency spectrum use provides another perspective to the issue that spectrum access is actually a more significant problem than spectrum scarcity. On one hand, some frequency bands are heavily used indeed; on the other hand, the some bands are idle or only partially occupied most of the time. In other words, the precious spectrum assigned for exclusive usage are not utilized efficiently and there are some available licensed frequency bands at the certain time or location, which are also termed as spectrum holes, spectrum opportunity or white spaces (see Figure 1.3), can be exploited by other unlicensed users [5]. This situation gives birth to a new paradigm, namely cognitive radio, which detects and use these spectrum

holes to promote the efficient use of the spectrum.

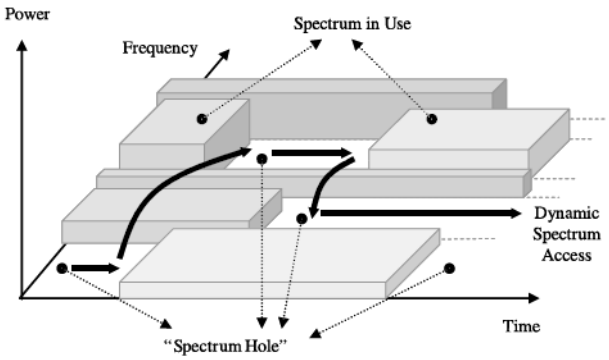


Figure 1.3: The concept of spectrum hole [5]

1.2.3 Advances in Cognitive Radio Technology

Cognitive radio is first officially proposed by Joseph Mitola III at The Royal Institute of Technology where he is pursuing for his Ph.D degree in 1998 [3]. Before generating this creative idea, he already comes up with another important concept, software-defined radio (SDR), which is a radio communication system realizes the components (e.g., filter, amplifiers, modulators/demodulators, etc.) in software on a computer or embedded devices instead of doing that on hardware directly. Cognitive radio can be viewed as a integrated agent architecture for SDR to evolve: a fully reconfigurable wireless black-box which can control its communication parameters automatically with respect to the demands of network and users.

Mitola defines and develops the architecture of cognitive radio, aiming to build a bridge between the wireless technology and computational intelligence [1][3]. He also studies the user cases of cognitive radio and derived several features required for the proposed architecture. Mathematical analysis is performed to imply that the radio software turns not to be Turing-computable but is constrained to a bounded-recursive subset of the total functions instead. The most significant contribution of his work lies in developing cognitive radio architecture from a rapid-prototype, where agent-based control, natural language processing and machine learning technique are integrated into software-defined radio platforms.

Haykin addresses threefold tasks in cognitive radios: 1)radio-scene analysis; 2) channel-state estimation and predictive modeling; 3) transmit-power control and dynamic management [4]. He also discusses several challenging issues of cognitive radio, including interference temperature detection, radio-scene analysis based on space-time processing, channel estimation and predictive modeling for channel capacity computation of a cognitive radio link, cooperation and competition in multiuser cognitive radio environment, stochastic games, iterative water-filling algorithm for distributed transmit-power control and dynamic spectrum management. At the end of the paper, Haykin envisions that the potential key issue for the evolution of cognitive radio technology would be trust by cognitive radio users or by other users who might be interfered with.

Akyildiz et.al publish an overview of cognitive radio technology, revealing the relationship between cognitive radio technology and next Generation (xG) network [5]. In the paper, authors present the motivation, classification and main functions of cognitive radio as well as the physical and network architecture of CR network. Authors also list the challenges of cognitive radio at the lower and upper layers with the interaction of cross-layer design and indicate that the challenges of CR is not only engaged in further developing cognitive radio technique, but also is related to designing the appropriate communication protocols to better adapt the spectrum-aware communication at the upper layers (e.g., network and transport layer).

Zhao and sadler survey dynamic spectrum access (as an important application of cognitive radio) in [7] where they look to analyze the cognitive radio technology from three angles: signal processing, networking and regulatory policy. In the paper, authors study how to identify, detect and track the spectrum opportunity, how to make decision for the access and how to share the opportunity among secondary users. They also explore the interaction between signal processing, networking and regulatory policy such that decision makers can devise more robust policies to accommodate future extensions of cognitive radio networks.

As the development of cognitive radio technology, a number of research efforts have been done on the various directions of cognitive radio. Yucek and Arslan summarize the

different spectrum sensing methods of cognitive radios [8]. Cabric et.al attempt to implement the cognitive radio on the hardware platform [9]. Liang et.al research the trade-off between the sensing and throughput performance of cognitive radio networks [10]. Devroye et.al investigate the achievable rates and channel capacity of cognitive radio network [11]. Etkin et.al study the spectrum sharing scheme for unlicensed bands [12]. Akyildiz et.al outline the spectrum management in CR networks [13].

1.3 Security Issues in Cognitive Radios

To date, the security issues have a plethora of research literature in the context of wireless networks. Nevertheless, the intrinsic properties of cognitive radio paradigm produce new threats and challenges to wireless communications. The potential security vulnerabilities and mitigation countermeasures are surveyed in [14] [15] [16].

In [14], Brown et. al exemplify intentional and unintentional attacks in cognitive radio networks and claim that the direct jamming can be significantly reduced by carefully designing the cognitive architecture. Authors also try to predict the potential denial of service vulnerabilities of cognitive radio including spectrum occupancy failures, policy failures, location failures, sensor failures, transmitter/receiver failures, operating system disconnect, compromised cooperative CR and common control channel attacks. A multi-dimensional analysis is conducted in the paper to determine how vulnerable victim CRs are to a potential Denial-of-Service attack in terms of three different dimensions: network architecture, spectrum access method and spectrum awareness model.

In [15], Burbank analyzes the several features of cognitive radio in the consideration of IEEE 802.22 which is the popular MAC layer protocol for CR networks. He also gives insights into what those features mean to the users and attackers and what effects/results the attack may bring about. The possible measurements of enhancing security posture, as given in [15], are to protect and secure the goals, methods and algorithms in the decision-making process of CR or to understand the attacking strategies.

In [16], Jakimoski and Subbalaskshmi take infrastructure and ad-hoc based cognitive radio system as the case study and demonstrate that under denial-of-service attack, CR

users can be spoofed either to vacate the channels they are using or to access the channels that are actually busy. Four designing goals are presented in [16] which are accurate and secure primary user detection, resilience to non-jamming DoS attacks on the secondary networks, efficient and fair spectrum sharing, and efficient implementations.

Other detailed work pertain to security of cognitive radio are: Leon et.al formulate a cross-layer attack forcing spectrum handoff and the influence it exerts on the TCP protocol [17]; Bian et.al describe how the attacker undermines IEEE 802.22 which is a compatible standard with cognitive radio technology and provides a cryptographic method to enhance the protection of the security sublayer in the protocol [18]; Clancy et.al specify the objective function attacks which disrupts the artificial intelligence (AI) learning algorithms of cognitive radios [19]; Kaligineedi et.al concentrate on the detection of the malicious users sending out erroneous messages deliberately in CR networks to compromise the detection performance of primary users [20]; Liu et.al devise an anomaly detection framework to detect unauthorized signal by three approaches as linearity check-give-location, one-class support vector machine and calibrating power [21]; Chen et.al study Byzantine failure problem in the context of data fusion, which may be caused either by malfunctioning sensing terminals or spectrum sensing data falsification (SSDF) attacks. To detect such attack, authors propose a weighted sequential probability ratio test (WSPRT), introducing a reputation-based mechanism to the sequential probability ratio test (SPRT) [22]. Safdar et.al present a framework to ensure the security of common control channel in cooperative communication cognitive radio networks by enabling secure key exchange between the nodes to guarantee confidentiality and integrity of the transactions [23]. Apart from the above work, one typical vulnerability of cognitive radio, called primary user emulation attack (PUEA) is identified in [2], which has been mentioned in many other literatures by the different forms of expression.

1.4 Thesis Organization

In this thesis, we will focus on an important security issue of spectrum sensing of cognitive radio technology — primary user emulation attack (PUEA). Chapter 2 will summarize the

current methods used in spectrum sensing as well as the detection and mitigation schemes against PUEA. Chapter 3 will study the cooperative spectrum sensing in the presence of PUEA in cognitive radio network. We will provide the performance of detection probability when the PUEA is present and discuss several relevant problems. Chapter 4 will show the detection performance of detection probability when the channel estimation error is considered. Chapter 5 will investigate the cooperative sensing when there are multiple PUE attackers threatening the spectrum band at the same time. Chapter 6 will draw the conclusions of the thesis and propose the possible research direction in the future.

Chapter 2

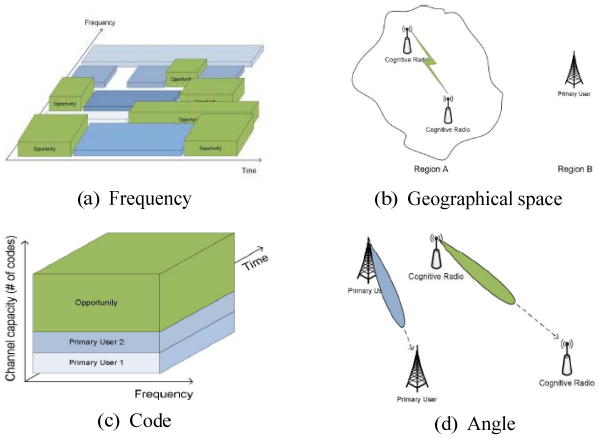
Spectrum Sensing in Cognitive Radios and Primary User Emulation Attack

As a crucial step of cognitive radio, spectrum sensing is to obtain awareness about the spectrum usage and existence of primary users in a geographical area. This awareness can be obtained by using geographical location and database, beacons or local spectrum sensing at cognitive radios. In this chapter, we will explain the concept of spectrum opportunity and also describe the different spectrum sensing methods to detect it. We will also introduce the focus of the thesis, primary user emulation attack, including its attacking principle, detection and defense approaches.

2.1 The Concept of Spectrum Opportunity

The conventional definition of the spectrum opportunity, which is often defined as “a band of frequencies that are not being used by primary user of that band at a particular time in a particular geographic area” [4], generally exploits three dimensions of the spectrum space only: frequency, time and space. In fact, there are other dimensions that can be exploited. For instance, the code dimension of the spectrum space could be an alternative. The conventional spectrum sensing algorithms cannot deal with signals using spread spectrum, time or frequency hopping codes, however, as the recent developments in multi-antenna

technologies (e.g. beamforming) [24], multiple users can be multiplexed into the same channel at the same time in the same geographical area. Therefore, code of spectral space can be created as an additional dimension of spectrum opportunity. Various dimensions of the space and corresponding measurement/sensing requirements are given in Figure 2.1. It notes that each dimension should have its own parameters sensed for a complete spectrum awareness [8].



(a) Frequency (b) Geographical space

(c) Code (d) Angle

Figure 2.1: Multiple dimensional spectrum opportunity [8]

2.2 Spectrum Sensing in Cognitive Radio

Spectrum sensing is an important element of cognitive radio. The most efficient way to detect spectrum holes is to detect the primary users that are receiving data within the communication range of a secondary user. In reality, however, it is difficult for a secondary user to have accurate channel information between a primary receiver and a transmitter due to the inherent property of cognitive radio. Thus, the most recent work engages in primary transmitter detection based on local observations of secondary users. The current spectrum sensing methods can be classified as three categories: Non-cooperative spectrum sensing, cooperative spectrum sensing and interference temperature spectrum sensing [5]. We will elaborate these methods in details in the following sections.

2.2.1 Spectrum Sensing Methods

A. Non-cooperative Spectrum Sensing

Non-cooperative spectrum sensing, also known as transmitter detection, is a sensing mechanism where a CR user distinguishes used and unused spectrum bands. That is, a secondary user should be able to decide whether a signal from a primary transmitter is present or not within a certain time and spectrum band. This method is based on the detection of the relatively weak signal from a primary emitter through the local observations of individual secondary users [25]. Basic hypothesis model for non-cooperative spectrum sensing can be defined as follows,

$$x(t) = \begin{cases} n(t), & \mathcal{H}_0 \\ hs(t) + n(t), & \mathcal{H}_1 \end{cases} \tag{2.1}$$

where $x(t)$ is the signal received by CR user, $s(t)$ is the transmitted signal from primary user, $n(t)$ is the additive white Gaussian noise and h is the amplitude gain of the channel. $\mathcal{H}_0$ and $\mathcal{H}_1$ are a null and a non-null hypothesis respectively, indicating the presence or absence of the primary user's signal. Typically, there are three main schemes for Non-cooperative spectrum sensing which are matched filter detection, energy detection and cyclostationary feature detection.

- Matched filter detection

  Matched filter detection [26] is a typical coherent detection in which certain features of primary user are known by the secondary users. The features includes the pilots, preambles or synchronization messages. The matched filter detector can extract the information of the primary signal such as the modulation type and order, the pulse shape, and the packet format from these features to optimize the detection probability. The main merit of the matched filter structure is that it takes less time to achieve high processing gain due to coherency. Nevertheless, it requires priori knowledge of the primary user signal and its performance would be severely deteriorated if such knowledge is not accurate.

- Energy detection

If the priori knowledge mentioned above is not available for secondary users, then the optimal scheme for spectrum sensing is energy detection which requires no information of primary user [27]. In order to measure the energy of the received signal, the output signal of bandpass filter with bandwidth W is squared and integrated over the observation interval T. TW is the time-bandwidth product and can be denoted as the sample number M in the detection process. Finally, the decision statistic Y is compared with a threshold λ, to decide the presence or absence of the primary user. According to [28], Y should follow chi-square distribution,

$$Y \sim \begin{cases} \chi^2_{2M}, & \mathcal{H}_0 \\ \chi^2_{2M}(2\gamma), & \mathcal{H}_1 \end{cases} \tag{2.2}$$

where χ^2_{2M} and $\chi^2_{2M}(2\gamma)$ denote central and non-central chi-square distribution, each with $2M$ degrees of freedom. γ is the signal-to-noise ratio (SNR). In the spectrum sensing of cognitive radio networks, false alarm probability P_f and detection probability P_d over a detection interval are defined as,

$$P_f = P_r(Y \geq \lambda | \mathcal{H}_0) \tag{2.3}$$

$$P_d = P_r(Y \geq \lambda | \mathcal{H}_1) \tag{2.4}$$

where λ is a detection threshold. When h is a constant, i.e., channel has no fading, the probabilities of false alarm and detection are given by,

$$P_f = \frac{\Gamma(M, \lambda/2)}{\Gamma(M)} \tag{2.5}$$

$$P_d = Q_m(\sqrt{2\gamma}, \sqrt{2\lambda}) \tag{2.6}$$

where $\Gamma(\cdot)$ and $\Gamma(\cdot,\cdot)$ are Gamma function and upper incomplete Gamma function respectively and $Q_m(\cdot,\cdot)$ is the generalized Marcum Q function [29]. If channel fading is taken into account, that is, h is a random variable following such distribution as Rayleigh, Rician or Nakagami, the average detection probability is obtained by

averaging the instantaneous detection probability over the fading channel,

$$\bar{P}_d = \int_x Q_m(\sqrt{2\gamma}, \sqrt{2\lambda}) f_\gamma(x) dx \tag{2.7}$$

where $f_\gamma(x)$ is the probability density function (pdf) of SNR based on the fading channel.

- Cyclostationary feature detection

  An alternative detection method is cyclostationary feature detection. The built-in periodicity of modulated signals coupled with sine wave carriers, pulse trains, repeating spreading, hopping sequences or cyclic prefixes makes it possible to detect the primary signal by analyzing a spectral correlation function of the transmitted signal [30]. Cyclostationary feature detector can perform better than the energy detector in discriminating against noise due to its robustness to the uncertainty in noise power. However, it requires more computational complexity and significantly long observation time. More enhanced detection scheme combining cyclic spectral analysis with pattern recognition (based on neural network) is proposed in [31] to obtain more efficient and reliable detection performance. Distinct features of the received signal are extracted using cyclic spectral analysis and represented by both spectral coherent function and spectral correlation density function, which is converted to the rules for the neural network to classify signals into different modulation types.

B. Cooperative Spectrum Sensing

Since it is usually impossible for secondary users to detect the location of primary receiver, the interference cannot be avoided. Moreover, an CR transmitter may not be able to detect the primary transmitter due to the channel fading or shadowing. These two issues are shown in Figure 2.2. Consequently, the sensing information from other users is required for more accurate detection and cooperative spectrum sensing arises. Compared to the non-cooperative sensing which is based on the local observation from each CR user independently, cooperative sensing method collects and incorporates sensing information

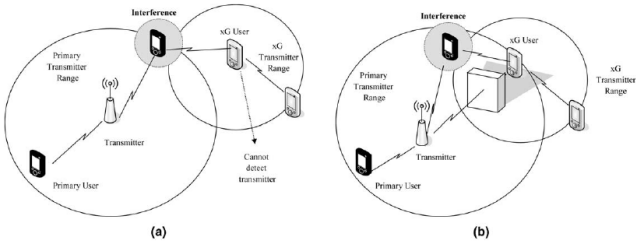


Figure 2.2: Non-cooperative sensing problem

from multiple CR users in order to improve the performance of spectrum sensing. Some important work in cooperative spectrum sensing are provided as follows.

Ghasemi and Sousa first propose the idea of cooperative spectrum sensing in 2005 [32]. In the paper, the spectrum sensing is carried out at each CR user individually through energy detection and the sensing result of each sensor, which is a binary number($\mathcal{H}_1$ or $\mathcal{H}_0$), is delivered to a fusion center where the final decision of the spectrum sensing is made. The rules used by fusion center for combining the results from multiple CR users are AND-rule or OR-rule that fusion center decides $\mathcal{H}_1$ if all secondary users decides $\mathcal{H}_1$ or if any of them claims $\mathcal{H}_1$. The average detection performance over the different fading channel environment is also given in the paper by using the method in [28].

Ganesan and Li [33] formulate another cooperative spectrum sensing model in cognitive radio network which is similar as cooperative diversity [34]. In the paper, authors propose and analyze non-cooperative (NC) and totally cooperative (TC) sensing schemes which employs different degrees of freedom respectively. In the former scheme, each user detects the primary user independently and the user who first detects the primary signal informs the result to other secondary users; in the latter scheme, all the users follow the amplify-and-forward (AF) cooperation protocol to sense the spectrum. Through the cooperation between secondary users, the overall detection time is reduced and better detection performance is achieved due to the spatial diversity in multiuser networks. Authors also study the impact of power constraint on cooperation schemes as well as some important properties of such networks. Furthermore, authors extend the proposed cooperation scheme to multi-carrier networks with utmost two users per carrier and derive expressions for agility gain [35].

Ma and Li propose a soft combination and detection method for cooperative spectrum

sensing based on the energy detection [36]. Instead of making binary decision at each CR user locally, the sensing information which is the sum of the energy samples of the received signal at the CR users, is converged to a fusion center with some weighted coefficients derived to optimize the detection probability. The result of derivation indicates that the optimal weights are identical to maximal ratio combination (MRC) method if the channel gains are available to secondary users. Authors also perform the simulations to show better performance of MRC and equal gain combination (EGC) over conventional hard combination scheme given in [32]. In addition, they also derive the equivalent SNR wall reduction achieved by cooperation under independent Nakagami channels and show that cooperation among secondary users can distinctly improve the robustness of energy detection to noise uncertainty over fading channels.

Quan et.al propose an optimal linear cooperation framework for cooperative spectrum sensing, aiming to minimize the interference to the primary user and at the same time, to meet the requirement of opportunistic spectrum utilization [37]. Within the framework, spectrum sensing is implemented based on the linear combination of local statistics of individual CR user. Authors formulate the sensing problem as a nonlinear optimization problem and develop efficient algorithms to solve for the optimal solutions. To further reduce the complexity and obtain more general solutions, authors propose a heuristic approach to optimize a modified deflection coefficient, which specifies the probability distribution function of the global test statistics at the fusion center.

C. Interference Temperature Spectrum Sensing

Recently, a new model of measuring interference, referred to as interference temperature shown in Figure 2.3 has been introduced by the FCC in the sense that the cognitive radio network is operated in an underlay manner [38]. In the model, the radio signal is designed to operate in a range at which the received power approaches the level of the noise floor. As additional interfering signals arise, the noise floor increases at various points within the service area, as indicated by the peaks above the original noise floor. The interference temperature model manages interference at the receiver rather than transmitter through the

interference temperature limit represented by the amount of new interference that the receiver could tolerate. In other words, the interference temperature model accounts for the cumulative RF energy from multiple transmissions and sets a maximum cap on their aggregate level. As long as CR users do not exceed this limit by their transmissions, they can use this spectrum band. There are some existing research work for the interference temperature

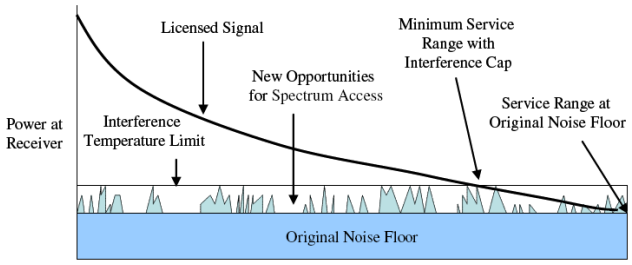


Figure 2.3: Interference temperature spectrum sensing [5]

detection method. Wild and Ramchandran exploit the local oscillator leakage power emitted by the RF front end of TV receivers to detect the presence of primary receivers [39]. The disadvantage of this approach is that it has short detection range and long detection time to achieve accuracy. It is proposed in the paper that low-cost sensors be deployed close to primary receivers for spectrum opportunity detection. In [40], the interference is defined as the expected fraction of primary users with service disrupted by the CR users who considers such factors as the type of unlicensed signal modulation, ability to detect active licensed channels, antennas, power control, and activity levels of the primary and secondary users.

2.2.2 Challenges in Spectrum Sensing

A. Hardware Requirements

Spectrum sensing for cognitive radio applications requires high sampling rate, high resolution analog to digital converters (ADCs) with large dynamic range and high speed signal processors. Sensing can be performed via two different architectures: single-radio and dual-radio. dual-radio exhibits better performance than Single-radio with higher cost. There are already available hardware and software platforms for the cognitive radio such as

GNU radio [41], universal software radio peripheral (USRP) [42] and shared spectrum's X radio [43]. However, few efforts on the exact implementation of these platforms have been done and many potential functions need to be developed in the platforms.

B. Hidden Primary User Problem

The hidden primary user problem is similar to the hidden node problem in carrier sense multiple accessing (CSMA). It can be caused by various factors like severe multipath fading or shadowing observed by secondary users. Figure 2.2(b) already shows an illustration of a hidden node problem in cognitive radio network. Secondary user is probably not able to detect the presence of a primary transmitter in its communication range due to the reasons given above and thus results in the interference to the primary network. The solution to this issue is cooperative spectrum sensing technique.

C. Detection of Primary Users in Spread Spectrum

It is difficult to detect primary signals using spread spectrum technique as primary user's power is actually spread over a very wide frequency bands, regardless of the actual bandwidth the signal occupies [9]. This problem can be partially resolved provided that the hopping pattern is known and perfect synchronization to the signal can be obtained. However, it is nontrivial to do the perfect estimation in the code dimension.

D. Detection Capability

One of the main requirements of CR networks is to detect primary users in a very short time. An appropriate and efficient mechanism would be OFDM-based CR networks [44] where the overall detection time is much reduced since as long as a primary user is detected over a single carrier, sensing in other carriers is not necessary. Nonetheless, the use of multi-carrier necessitates the requirement of a large number of carriers, which would produce a very high complexity. Hence, novel spectrum sensing algorithms should be designed to minimize the number of samples given a predefined detection probability.

E. Decision Fusion in Cooperative Sensing

In the cooperative sensing, how to share and combine the soft or hard sensing statistics is a challenging task. It has been shown that soft combination scheme outperforms hard combining method in [36]. On the other hand, hard combination method is found to perform as good as soft one when the number of cooperative secondary users is fairly high in [45]. The optimum fusion rule for combining sensing information is the Chair-Varshney rule which is based on log-likelihood ratio test [46] and has been verified by the combination of information from different secondary users by Dempster-Shafer's theory [8]. The challenges exist in the issue that at least how many secondary users are required for the detection probability optimization under a prefixed false alarm probability. At the mean time, the channel condition and the distance to a primary user of secondary users should also be considered.

F. Security Issues

To date, security issues of cognitive radio networks has become a hotspot of research endeavors. Some work has engaged in this area which predicts the potential vulnerabilities on the structure, function and policy of CR network that could be employed by the malicious or selfish users [14] [15]. Particularly, a selfish or malicious secondary user may preempt a idle frequency band by imitating the primary user and thus prevents other secondary users from accessing that band. Such a malicious behavior or attack has been investigated in [2] and is termed as primary user emulation attack (PUEA). The defense measurements involve as either locating the real position of attacker and primary user or increasing the trust level of the legitimated users in the network through public key encryption algorithm [47]. However, it is difficult to differentiate the locations of both attacker and actual primary user if they are very closed geographically. And for the encryption scheme, secondary users should be capable of strictly synchronizing and demodulating primary signals, which is a rigorous requirement for the CR users.

2.3 Primary User Emulation Attack in Spectrum Sensing

We have mentioned primary user emulation attack in the previous section. In this section, we will introduce this concept in details, including the definition, detection and defense measures of PUEA.

2.3.1 Primary User Emulation Attack

Primary user emulation attack (PUEA) is first identified by Chen and Park in 2006 [2]. This idea is also described in [14] and [15]. In PUEA, an attacker occupies the unused channels by emitting a signal with similar form as the primary user's signal so as to deter the access of the vacant channels from other secondary users. The cognitive radios have highly reconfigurable air interface which makes it possible for an attacker to modify the air interface to mimic a primary user signal's features and thereby leading legitimate secondary users to erroneously identify the attacker as a primary user. The investigation shows that a PUE attacker can severely compromise the spectrum sensing performance and significantly reduce the channel availability to legitimate secondary users [22].

PUEA can compromise a cognitive radio system using either of spectrum sensing methods given in Chapter 2. To attack the energy detection scheme, PUE attacker may masquerade the primary user by transmitting signal with the similar energy as primary user; to defeat cyclostationary detectors, an attacker can make its transmissions indistinguishable from primary user signals by transmitting signals that have the same cyclic spectral characteristics as primary user signals.

The fundamentals of PUEA is that the adversary is not focus on jamming primary users, but on forestalling idle spectrum bands that could have been used by other secondary users. Depending on the motivation behind the attack, a PUE attack can be classified as either a selfish PUE attack or a malicious PUE attack. A selfish PUE attacker aims to prevent other secondary users from competing for that band by sending signals with similar characteristics of primary user signals whereas a malicious user launching an attack in the same manner, is more interested in obstructing the whole dynamic spectrum access process rather than monopolizing the utilization of the frequency spectrum resource.

2.3.2 Detection Schemes of PUEA

Until now, some research work have been directed to the detection of PUEA in cognitive radio networks. In [2], Chen and Park propose a detection framework, called transmitter verification procedure, which employs a location verification scheme to distinguish primary signals from secondary signals pretending to be primary signals. The detection scheme integrated into the spectrum sensing is implemented by distance ratio test (DRT) and distance difference test (DDT). Simulation results illustrate that several factors, such as the location of the attacker's transmitter relative to the LVs can impact the performance of both DRT and DDT. Later on, Chen et.al propose another transmitter verification scheme, called LocDef (localization based defense) [48], which estimates its location and observes its signal characteristics to verify the source of a given signal. To estimate the location of the transmitter, a non-interactive localization approach is adopted which collects a sufficient number of received signal strength (RSS) measurements from a set of sensors widely deployed within a network and selects the location with the highest RSS value to be the location of a primary user. Anand et.al establish an analytical model based on Fentons approximation an Markov inequality and derive a lower bound on the probability of a successful PUEA on a secondary user by a group of collaborative PUE attackers [49]. The paper also discusses several factors which would affect the possibility of a PUEA. It shows that, as the distance increases between the primary and secondary users, the probability of a successful PUEA turns out to be higher as well. Furthermore, based on that model, Jin et.al present another analytical model as well as a practical mechanism to detect PUEA by using Fenton's approximation and Wald's probability ratio test (WSPRT) [50]. Their detection scheme does not need any location information and thus the dedicated sensor network is not a must.

2.3.3 Defense Schemes against PUEA

Apart from detection of PUEA, other researchers and scholars also make the contributions to the defense scheme against PUEA. Chen et.al [51] characterize an advanced primary user emulation attack as well as an advanced countermeasure against such an attack and show that both the attacker and the defender are intelligent to gain the information of the

environment through estimation and learning and thus design better strategies to adapt if any change of the environment happens. They also demonstrate that the it is easy for some advanced attack strategy to defeat the defense scheme which only focuses on the energy of the signal and on the contrary, the defense strategy can effectively counteract the advanced attack by making use of the invariant of communication channels. Li and Han study the PUEA in the multichannel cognitive radio network and propose a passive anti-jamming defense scheme, based on the assumption that there are multiple channels and one defending secondary user in the cognitive radio network [52]. In the passive approach, a secondary user randomly chooses a channel to sense and transmit at each time so as to avoid the PUE attack statistically. They also coin *dogfight* to describe such competition between the attacker and defender. Moreover, considering the limitations of channel statistic availability and random strategy selection in [52], Li and Han extend their work to the case of multiple defenders and unknown channel statistics [53], which is called *blind dogfight*. To counter arbitrary strategies of the attacker and the unknown channel statistics, the defender considers each channel as a bandit arm and uses the technique of adversarial multi-armed bandit as its strategy.

So far, some work have been performed on either detection or defense against PUEA, however, the detection performance of spectrum sensing with the existence of PUEA is not completely studied. In the following chapters, we will study the performance of cooperative spectrum sensing in the presence of one or multiple PUE attackers. We will also analyze the impact of channel estimation error on the performance of detection probability in the cooperative spectrum sensing.

Chapter 3

Cooperative Spectrum Sensing in the Presence of PUEA

3.1 Introduction

Although a variety of research efforts have been directed on the detection of PUEA, the cooperative spectrum sensing with the existence of PUEA is less investigated. In this chapter, we establish a model of cooperative spectrum sensing in the presence of PUEA and propose a scheme to maximize the detection probability of primary user. As the PUEA is launched in a CR network using cooperative sensing technique, each secondary user receives the signals from the attacker and the primary user and sends its sensing information to a fusion center. The received signal (or the sensing information) is then optimally combined with some appropriate weights to maximize the detection probability with a constraint of false alarm probability. The optimal weights are related to the channel state information (CSI) between the attacker and secondary users and between the primary user and secondary users, which are estimated by using existing channel estimation algorithms. The main contribution of this paper is to maximize the detection probability of the primary user by deriving the optimal combining weights, considering the existence of the PUEA in a CR network. Note that we assume the PUE attacker has been detected and this paper thus centers on the detection of the primary user rather than the detection of PUEA as in [22]

and [48].

3.2 System Model

In this chapter, we consider cooperative spectrum sensing in a CR network where N secondary users detect the presence of one primary transmitter, as shown in Figure 3.1. Taking PUEA into the consideration, the signal received by the ith secondary user at the kth time instant is,

$$y_i(k) = \alpha\sqrt{P_p}h_{pi}(k)x_p(k) + \beta\sqrt{P_m}h_{mi}(k)x_m(k) + n_i(k), \quad i = 1, 2, ..., N \tag{3.1}$$

where $x_p(k)$ and $x_m(k)$ are the signal transmitted by primary user and attacker, with the power P_p and P_m respectively. $h_{pi}(k)$ and $h_{mi}(k)$ denote the instantaneous channel response between primary user and ith secondary user and between attacker and ith secondary user, respectively. $n_i(k)$ is the additive white Gaussian noise at the ith secondary user with zero mean and variance σ_n^2. α and β are two binary indicators where $\alpha = 1$ or $\beta = 1$ indicates the presence of primary user or attacker and $\alpha = 0$ or $\beta = 0$ implies their absence. If no PUE attacker is detected, the indicator of the attacker $\beta = 0$ and the conventional MRC method can be used in the cooperative spectrum sensing [36]. Otherwise, $\beta = 1$, which indicates that the PUE attacker is present and therefore the combining scheme of MRC has to be redesigned to optimize the performance of the spectrum sensing.

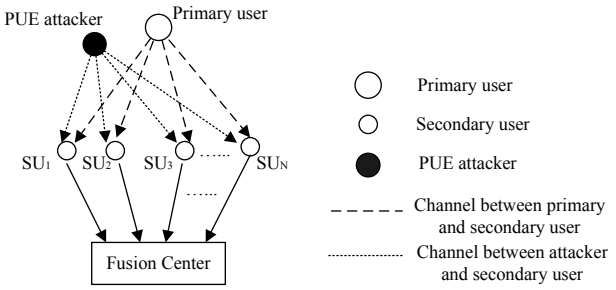


Figure 3.1: System model of cooperative spectrum sensing with PUEA in cognitive radio network

In a cooperative manner, the signals received by secondary users are weighted by some coefficients $w_i, i = 1, 2, ..., N$ and converged to a fusion center where a final decision is made, depending on the absence or presence of the primary user. It is assumed that the channels from secondary users to the fusion center are perfect, e.g., dedicated control channel [36]. The combined signal in the fusion center at the kth time instant is,

$$\begin{aligned} y(k) &= \sum_{i=1}^{N} w_i y_i(k) \\ &= \sum_{i=1}^{N} w_i \Big(\alpha \sqrt{P_p} h_{pi}(k) x_p(k) + \beta \sqrt{P_m} h_{mi}(k) x_m(k) + n_i(k) \Big) \\ &= \underbrace{\alpha \sqrt{P_p} \sum_{i=1}^{N} w_i h_{pi}(k) x_p(k)}_{\textbf{primary signal component}} + \underbrace{\beta \sqrt{P_m} \sum_{i=1}^{N} w_i h_{mi}(k) x_m(k)}_{\textbf{malicious signal component}} + \underbrace{\sum_{i=1}^{N} w_i n_i(k)}_{\textbf{noise component}} \end{aligned} \tag{3.2}$$

When the PUE attacker is absent ($\beta = 0$), the detection of the primary user is formulated as a hypothesis test problem between $\mathcal{H}_0$ and $\mathcal{H}_1$, i.e., to detect the primary signal is absent or present [32]. When there is a PUEA, i.e., $\beta = 1$, the detection problem is reformulated as,

$$y(k) = \begin{cases} \sqrt{P_m} \sum_{i=1}^{N} w_i h_{mi}(k) x_m(k) + \sum_{i=1}^{N} w_i n_i(k), & \mathcal{H}_0(\alpha = 0) \\ \sqrt{P_p} \sum_{i=1}^{N} w_i h_{pi}(k) x_p(k) + \sqrt{P_m} \sum_{i=1}^{N} w_i h_{mi}(k) x_m(k) + \sum_{i=1}^{N} w_i n_i(k), & \mathcal{H}_1(\alpha = 1) \end{cases} \tag{3.3}$$

To classify between $\mathcal{H}_0$ and $\mathcal{H}_1$, several methods can be applied in cooperative sensing, such as matched filter detection, energy detection and interference temperature detection [5]. In this paper, we adopt the energy detection method [9] in which M samples of the energy of $y(k)$ are summed during one detection interval,

$$Y = \sum_{k=1}^{M} |y(k)|^2 \tag{3.4}$$

The fusion center then calculates the decision statistic Y for each detection interval to make

a global decision.

The objective of cooperative spectrum sensing, as we will discuss in Section III, is to find optimal weights $w_i, i = 1, 2, ..., N$ to maximize the detection probability of the primary user under the constraint of a false alarm probability. This paper differs from the previous work, such as [36] and [37], in considering the existence of the PUE attacker in the cognitive radio network.

3.3 Optimal Combining Scheme for Cooperative Spectrum Sensing in the Presence of PUEA

In this section, we will derive the optimal weights to optimize the detection performance in cooperative sensing with the presence of PUEA. We will also demonstrate the expression of the instantaneous and average detection probability over the fading channel.

In the spectrum sensing of cognitive radio networks, false alarm probability P_f and detection probability P_d over a detection interval are defined as [28],

$$P_f = P_r(Y \geq T|\mathcal{H}_0) \tag{3.5}$$

$$P_d = P_r(Y \geq T|\mathcal{H}_1) \tag{3.6}$$

where T is a detection threshold. The following derivation obtains the optimal weights $\mathbf{w_{opt}}$ so that the detection probability P_d is maximized under the constraint of a false alarm probability P_f. Therefore, the detection problem is described as,

$$\mathbf{w_{opt}} = arg \max_{\mathbf{w}} \{P_d|P_f = \zeta\} \tag{3.7}$$

where ζ denotes a predefined false alarm probability and $\mathbf{w}$ is a vector of weights for the combination at the fusion center, which is given by,

$$\mathbf{w} = [w_1, w_2, ..., w_N] \tag{3.8}$$

and $\mathbf{w_{opt}}$ is a vector of optimal weights,

$$\mathbf{w_{opt}} = [w_{1_{opt}}, w_{2_{opt}}, ..., w_{N_{opt}}] \tag{3.9}$$

As in [36], primary user's signal x_p is assumed to be independently and identically distributed (i.i.d) complex Gaussian random variable with zero mean and unit variance. Due to the similarity between malicious and primary signal in PUEA, the attacker's signal x_m can also follow the complex Gaussian distribution. We assume that the existence of PUEA has been detected by some detection approach [21] [50], such that $\alpha = 1$ for the entire spectrum sensing process. In addition, all the channels are considered to be subject to block fading, that is, $h_{pi}(k)$ and $h_{mi}(k)$ are constant within one detection interval and k can thereby be omitted. For given h_{pi} and h_{mi}, the combined signal $y(k)$ is also a complex Gaussian distributed random variable,

$$y(k) \sim \begin{cases} \mathcal{CN}(0, \sigma_0^2), & \mathcal{H}_0 \\ \mathcal{CN}(0, \sigma_1^2), & \mathcal{H}_1 \end{cases} \tag{3.10}$$

where σ_0^2 and σ_1^2 are the variance of $y(k)$ for $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively,

$$\sigma_0^2 = P_m \left| \sum_{i=1}^{N} w_i h_{mi} \right|^2 + \sum_{i=1}^{N} |w_i|^2 \sigma_n^2 \tag{3.11}$$

$$\sigma_1^2 = P_m \left| \sum_{i=1}^{N} w_i h_{mi} \right|^2 + P_p \left| \sum_{i=1}^{N} w_i h_{pi} \right|^2 + \sum_{i=1}^{N} |w_i|^2 \sigma_n^2 \tag{3.12}$$

As such, the decision statistic Y is compliant with the central Chi-square (χ^2) distribution with $2M$ degrees of freedom and parameters σ_0^2 and σ_1^2 for $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively [28],

$$Y = \sum_{i=1}^{M} |y(k)|^2 = \begin{cases} Y_0 \sim \chi^2_{2M}(\sigma_0^2), & \mathcal{H}_0 \\ Y_1 \sim \chi^2_{2M}(\sigma_1^2), & \mathcal{H}_1 \end{cases} \tag{3.13}$$

Hence, the false alarm probability P_f and the detection probability P_d are expressed as,

$$P_f = \frac{\Gamma(M, \frac{T}{\sigma_0^2})}{\Gamma(M)} \tag{3.14}$$

$$P_d = \frac{\Gamma(M, \frac{T}{\sigma_1^2})}{\Gamma(M)} \tag{3.15}$$

where $\Gamma(\cdot)$ and $\Gamma(\cdot, \cdot)$ are Gamma function and upper incomplete Gamma function respectively [29].

Given $P_f = \zeta$, $\zeta \in [0, 1]$, the decision threshold T is represented as,

$$T = \Gamma^{-1}(M, \zeta\Gamma(M))\sigma_0^2 \tag{3.16}$$

where $\Gamma^{-1}(\cdot, \cdot)$ is the inverse incomplete Gamma function [29]. By inserting (3.16) into (3.15), P_d can be rewritten as,

$$P_d = \frac{\Gamma\big(M, \Gamma^{-1}(M, \zeta\Gamma(M))\frac{\sigma_0^2}{\sigma_1^2}\big)}{\Gamma(M)} \tag{3.17}$$

Due to the monotonicity of Gamma function, for given M and ζ, the optimization problem in (3.17) is equivalent to minimize σ_0^2/σ_1^2.

Let $\mathbf{h_m} = [h_{m1}(k), h_{m2}(k), ..., h_{mN}(k)]^T$, $\mathbf{h_p} = [h_{p1}(k), h_{p2}(k), ..., h_{pN}(k)]^T$, σ_0^2 and σ_1^2 can be denoted by two quadratic forms,

$$\sigma_0^2 = P_m \mathbf{w}\mathbf{H_m}\mathbf{w}^H + \sigma_n^2 \mathbf{w}\mathbf{w}^H \tag{3.18}$$

$$\sigma_1^2 = P_m \mathbf{w}\mathbf{H_m}\mathbf{w}^H + P_p \mathbf{w}\mathbf{H_p}\mathbf{w}^H + \sigma_n^2 \mathbf{w}\mathbf{w}^H \tag{3.19}$$

where H is the Hermitian transpose and $\mathbf{H_m} = \mathbf{h_m}\mathbf{h_m}^H$, $\mathbf{H_p} = \mathbf{h_p}\mathbf{h_p}^H$. Then,

$$\begin{aligned}\frac{\sigma_0^2}{\sigma_1^2} &= \frac{P_m \mathbf{w}\mathbf{H_m}\mathbf{w}^H + \sigma_n^2 \mathbf{w}\mathbf{w}^H}{P_m \mathbf{w}\mathbf{H_m}\mathbf{w}^H + P_p \mathbf{w}\mathbf{H_p}\mathbf{w}^H + \sigma_n^2 \mathbf{w}\mathbf{w}^H} \\ &= \frac{1}{1 + \dfrac{\mathbf{w}\boldsymbol{\Theta}\mathbf{w}^H}{\mathbf{w}\boldsymbol{\Phi}\mathbf{w}^H}}\end{aligned} \tag{3.20}$$

where $\boldsymbol{\Theta} = P_p\mathbf{H_p}$, $\boldsymbol{\Phi} = P_m\mathbf{H_m} + \sigma_n^2\mathbf{I}$ and $\mathbf{I}$ is the identity matrix. Note that $\boldsymbol{\Theta}$ and $\boldsymbol{\Phi}$ are both symmetric and $\boldsymbol{\Theta}$ is positive definite and of rank 1, according to [54], the optimal weight vector $\mathbf{w_{opt}}$ is,

$$\mathbf{w_{opt}} = \sqrt{P_p}(\boldsymbol{\Phi}^{-1}\mathbf{h_p})^H \tag{3.21}$$

and the minimal σ_0^2/σ_1^2 is,

$$(\frac{\sigma_0^2}{\sigma_1^2})_{min} = \frac{1}{1 + P_p\mathbf{h_p}^H\boldsymbol{\Phi}^{-1}\mathbf{h_p}} \tag{3.22}$$

which can also be given by the largest eigenvalue λ_{max} of $\boldsymbol{\Theta}\boldsymbol{\Phi}^{-1}$ [54]. Using (3.17) and (3.22), the maximal detection probability $P_d(\mathbf{w_{opt}})$ is,

$$P_d(\mathbf{w_{opt}}) = \frac{\Gamma\big(M, \Gamma^{-1}(M, \zeta\Gamma(M))\frac{1}{1+\lambda_{max}}\big)}{\Gamma(M)} \tag{3.23}$$

Specially, if $P_m = 0$, i.e., the signal strength of the attacker is negligible, $\mathbf{w_{opt}}$ is simplified to $\sqrt{P_p}\sigma_n^2\mathbf{h_p}^H$ which is identical to the conventional MRC method.

The rationale behind the proposed optimal combining scheme is that the optimal weights form a "virtual" antenna array which steers "null point" of its radiation pattern towards the malicious user in order that the malicious signal component can be eliminated from the received signal.

We have derived the optimal weights over one detection interval during which the channel response is considered to be constant. The average detection probability $\bar{P}_d(\mathbf{w})$ can be

obtained by averaging $P_d(\mathbf{w})$ over fading channels [32],

$$\bar{P}_d = \iint P_d(\mathbf{w_{opt}}) f(\mathbf{h_p}) f(\mathbf{h_m}) d\mathbf{h_p} d\mathbf{h_m} \tag{3.24}$$

where $f(\mathbf{h_p})$ and $f(\mathbf{h_m})$ denote the probability density functions (PDF) of the signal-to-noise ratio (SNR) over the fading channel which may follow Rayleigh, Rician or Nakagami distribution.

3.4 Simulation Results

In this section, we will implement the simulations of the cooperative sensing scheme with the existence of PUEA. The channels are assumed to be identically and independently distributed block Rayleigh fading. The number of secondary users is $N = 4$ and the number of samples during a detection interval is $M = 3$.

Figure 3.2 displays the detection probability versus false alarm probability for our optimal combining scheme, the conventional MRC and non-cooperative sensing scheme when considering the presence of PUEA in the CR network. In the simulation, all channel information are assumed to be known to the secondary users. The average SNR is set as 0 dB and the emitting power of the primary user and the attacker is $P_p = P_m = 1$.

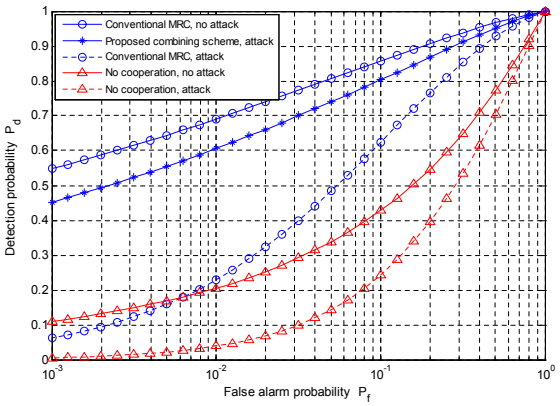


Figure 3.2: Detection probability versus false alarm probability for the proposed optimal combining, conventional MRC and non-cooperative sensing schemes, SNR = 0 dB, $N = 4$

Since we assume that the channel information can be obtained by secondary users

through the estimation algorithm, the optimal weight in conventional MRC is modified as h_{pi}^* rather than $|h_{pi}|^2$ as in [36]. From Figure 3.2, we find that the detection probability of conventional MRC and non-cooperative schemes are both severely compromised by PUEA. In our optimal combining scheme, as the PUEA has been detected, the optimal weights are set as in (3.21) and a significant improvement of detection performance is observed, compared to the conventional MRC and non-cooperation schemes. Essentially, the proposed optimal combining scheme considers the channel information between the attacker and secondary users, $\mathbf{h_m}$, as a result, the malicious signal is mitigated from received signal and thus the better detection performance is obtained.

Figure 3.3 illustrates the performance of the detection probability versus the signal-to-noise ratio of the cooperative sensing when PUEA is present. In the simulation, the false alarm probability is set as $P_f = 10^{-1}$ and SNR between primary and secondary users is defined as γ_p which is assumed to be same for each secondary user. Here, we define

$$\rho = \frac{P_m}{P_p} \tag{3.25}$$

which normalizes attacker's power in terms of primary user's power. A large ρ indicates a strong attacker. In Figure 3.3, the detection performance of the proposed combination scheme is compared with the conventional MRC scheme where the ρ is given as 0.1, 1 and 10, respectively.

It is seen from Figure 3.3 that the detection probability is improved with increasing average SNR. It also notes that the proposed combining scheme always has performance gain over the conventional MRC as the SNR increases from -15 dB to 15 dB. And as ρ increases from 0.1 to 10, the detection probabilities of both schemes are decreased and the conventional MRC exhibits more remarkable performance degradation. It is also viewed that the detection probability of conventional MRC is approximately constant over different SNR when $\rho = 10$. This is because the strength of malicious signal is dominant over the noise power such that the detection performance is poor even when the average SNR is very high.

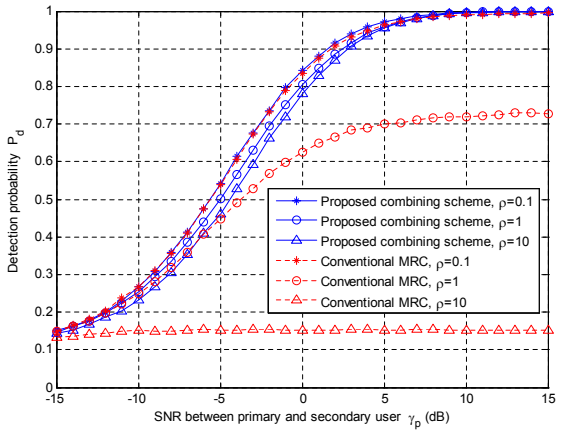


Figure 3.3: Detection probability versus average SNR γ_p, $P_f = 10^{-1}$ and $\rho = 0.1, 1, 10$, $N = 4$

3.5 Conclusion

In this chapter, we have studied the cooperative spectrum sensing in CR network in the presence of primary user emulation attack. PUEA is an attack where the malicious user pretends to be the primary user to preempt idle channels by transmitting a similar signal as the primary user. To maximize the detection probability of primary user with the presence of PUEA, we use the channel information between primary user and secondary users and between attacker and secondary users to derive the optimal weights for a combining scheme so that the detection probability of the spectrum hole is optimized under the constraint of a required false alarm probability. In essence, the proposed scheme takes advantage of a set of cooperative sensors to eliminate the malicious signal. Simulation results show the detection performance improvement of the proposed optimal combining scheme over the conventional MRC method.

Chapter 4

Cooperative Spectrum Sensing in the Presence of PUEA with Channel Estimation Error

From the above derivations, we find that the optimization of the combining weights requires the information of $\mathbf{h_p}$ and $\mathbf{h_m}$, which are the channel state information between the primary user and secondary users and between the attacker and secondary users. Due to the lack of interaction between primary and secondary users in cognitive radio networks, it is difficult for secondary users to have the perfect channel state information. However, such information can be achieved when some knowledge of the primary user is known to secondary users such as pilots, preambles or synchronization messages, which are embedded in the transmitted primary signal [37]. Moreover, since the PUE attacker completely imitates the primary user, the signal of a malicious user should also have the similar characteristics and is thus able to be estimated by secondary users as well. Alternatively, the CSI can also be obtained by a blind estimation method in case that the priori knowledge is unavailable for the secondary users [55]. Compared with the conventional energy detection, the proposed scheme needs the channel information as in [55] and [56]. The error of estimated CSI is not be negligible.

Figure 4.1 and 4.2 compare the detection performance of the proposed combination

with the conventional MRC scheme when the number of secondary users $N = 4$. Similar as the two secondary users case, the one of $\sigma^2_{e_p}$ and $\sigma^2_{e_m}$ is set as -15 dB, -10 dB and -5 dB and the other is fixed to be -15dB. It is seen that the proposed optimal combining scheme exhibits better performance than the conventional MRC for the various estimation error. Notice that the conventional MRC scheme does not require the CSI between attacker and secondary user, its performance is not affected by the change of $\sigma^2_{e_m}$ (see Figure 4.1).

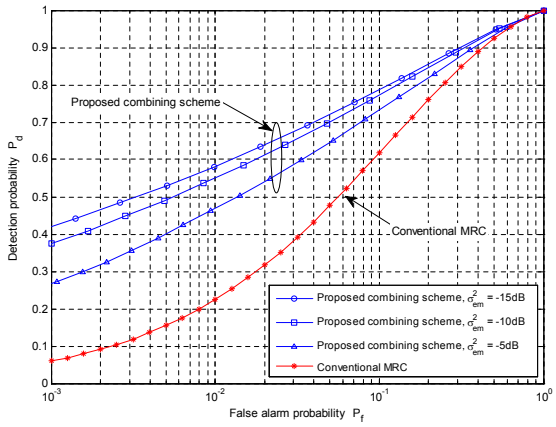


Figure 4.1: Detection performance of proposed optimal combining and conventional MRC scheme, $\sigma^2_{e_m}$ = -15 dB, -10 dB, -5 dB and $\sigma^2_{e_p}$ = -15 dB, SNR = 0 dB, $N = 4$

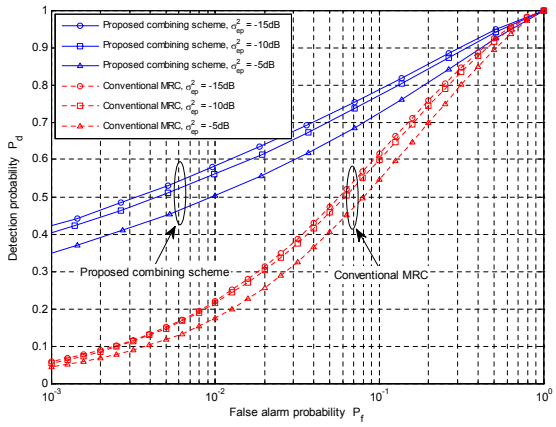


Figure 4.2: Detection performance of proposed optimal combining and conventional MRC scheme, $\sigma^2_{e_p}$ = -15 dB, -10 dB, -5 dB and $\sigma^2_{e_m}$ = -15 dB, SNR = 0 dB, $N = 4$

Chapter 5

Cooperative Spectrum Sensing with Multiple PUE Attackers

Chapter 6

Conclusion and Future Work

I have finished the cooperative spectrum sensing in the presence of primary user emulation attack in the cognitive radio network when secondary users have perfect knowledge of the channel state information. We have derived the optimal combining weights and performed simulations to verify the advantages of the combining scheme we have proposed. For the next step, I will continue to finish the following work that has not been done yet.

6.1 Cooperative Spectrum Sensing in the presence of PUEA when Considering Channel Estimation Error

I will extend the current work to the case when there exists different channel estimation error and investigate the corresponding impacts on the detection performance.

6.2 Cooperative Spectrum Sensing in the presence of PUEA when Considering Multiple PUE Attackers

I will also investigate the case when multiple PUE attackers are considered in the cooperative spectrum sensing and analyze the corresponding detection performance.

Bibliography

[1] J. Mitola and G. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Communication Magazine*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[2] R. Chen, J. Park, and J. Reed, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, Sep. 2006, pp. 110–119.

[3] J. Mitola, "Cognitive radio: an integrated agent architecture for software defined radio," Ph.D. dissertation, Royal Institute of Technology, Sweden, May. 2000.

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

[5] I. F. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Elsevier Computer Networks*, vol. 50, pp. 2127–2159, 2006.

[6] FCC, "Frequency spectrum allocation chart in united stated," Oct. 2003. [Online]. Available: http://www.ntia.doc.gov/osmhome/allochrt.pdf

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

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

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

[10] Y. Liang, Y. Zeng, E. Peh, and A. Hoang, “Sensing-throughput tradeoff for cognitive radio networks,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326–1337, Apr. 2008.

[11] N. Devroye, P. Mitran, and V. Tarokh, “Achievable rates in cognitive radio channels,” *IEEE Transactions on Information Theory*, vol. 52, no. 5, pp. 1813–1827, May. 2006.

[12] R. Etkin, A. Parekh, and D. Tse, “Spectrum sharing for unlicensed bands,” *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 517–528, Apr. 2007.

[13] I. F. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, “A survey on spectrum management in cognitive radio networks,” *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40–48, Apr. 2008.

[14] T. Brown and A. Sethi, “Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment,” in *IEEE International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, Aug. 2007, pp. 456–464.

[15] J. Burbank, “Security in cognitive radio networks: the required evolution in approaches to wireless network security,” in *IEEE International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, May. 2008, pp. 1–7.

[16] G. Jakimoski and K. Subbalakshmi, “Denial-of-service attacks on dynamic spectrum access networks,” in *IEEE International Conference on Communications (ICC)*, May. 2008, pp. 524–528.

[17] O. Leon, J. Hernandez-Serrano, and M. Soriano, “A new cross-layer attack to tcp in cognitive radio networks,” in *IEEE International Workshop on Cross Layer Design*, Jun. 2009, pp. 1–5.

[18] K. Bian and J. Park, "Security vulnerabilities in ieee 802.2," in *International Wireless Internet Conference*, 2008, pp. 1–9.

[19] T. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *IEEE International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, May. 2008, pp. 1–8.

[20] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *IEEE International Conference on Communications (ICC)*, May. 2008, pp. 3406–3410.

[21] S. Liu, Y. Chen, W. Trappe, and L. Greenstein, "Aldo: An anomaly detection framework for dynamic spectrum access networks," in *IEEE Conference on Computer Communications (INFOCOM)*, Apr. 2009, pp. 675–683.

[22] R. Chen, J. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *IEEE Conference on Computer Communications (INFOCOM)*, Apr. 2008, pp. 1876–1884.

[23] G. Safdar and M. O'Neill, "Common control channel security framework for cognitive radio networks," in *IEEE Vehicular Technology Conference*, Apr. 2009, pp. 1–5.

[24] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge University Press, 2005, pp. 290–331.

[25] Q. Zhao, L. Tong, A. Swami, and Y. Chen, "Decentralized cognitive mac for opportunistic spectrum access in ad hoc networks: A pomdp framework," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 589–600, Apr. 2007.

[26] A. Sahai, N. Hoven, and R. Tandra, "Some fundamental limits in cognitive radio," in *Allerton Conference on Communication, Control and Computing*, Oct. 2004, pp. 1–5.

[27] D. Cabric, A. Tkachenko, and R. Brodersen, "Experimental study of spectrum sensing based on energy detection and network cooperation," in *ACM 1st International Workshop on Technology and Policy for Accessing Spectrum (TAPAS)*, Aug. 2006.

[28] F. Digham, M. Alouini, and M. Simon, "On the energy detection of unknown signals over fading channels," in *IEEE International Conference on Communications (ICC)*, May. 2003, pp. 3575–3579.

[29] I. Gradshteyn and I. Ryzhik, *Table of integrals, series, and products*, 5th ed. Academic Press, 2005.

[30] R. Tandra and A. Sahai, "SNR walls for feature detectors," in *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, Apr. 2007, pp. 559–570.

[31] A. Fehske, J. Gaeddert, and J. Reed, "A new approach to signal classification using spectral correlation and neural networks," in *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, Nov. 2005, pp. 144–150.

[32] A. Ghasemi and E. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, Nov. 2005, pp. 131–136.

[33] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio, part I: Two user networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 6, pp. 2204–2213, Jun. 2007.

[34] J. Laneman, D. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[35] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio, part II: Multiuser networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 6, pp. 2214–2222, Jun. 2007.

[36] J. Ma, G. Zhao, and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 11, pp. 4502–4507, Nov. 2008.

[37] Z. Quan, S. Cui, and A. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 28–40, Feb. 2008.

[38] Y. Xing, C. Mathur, M. Haleem, R. Chandramouli, and K. Subbalakshmi, "Dynamic spectrum access with QoS and interference temperature constraints," *IEEE Transactions on Mobile Computing*, vol. 6, no. 4, pp. 423–433, Apr. 2007.

[39] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," in *IEEE Symposium on New Frontiers Dynamic Spectrum Access Networks*, Nov. 2005, pp. 124–130.

[40] T. Brown, "An analysis of unlicensed device operation in licensed broadcast service bands," in *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, Nov. 2005, pp. 11–29.

[41] E. Blossom, "GNU radio: tools for exploring the radio frequency spectrum," *Linux journal*, vol. 2004, no. 122, Jun. 2004.

[42] M. Ettus, "Universal software radio peripheral." [Online]. Available: www.ettus.com

[43] M. McHenry, E. Livsics, T. Nguyen, and N. Majumdar, "XG dynamic spectrum sharing field test results," in *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Apr. 2007, pp. 676–684.

[44] T. Weiss and F. Jondral, "Spectrum pooling: an innovative strategy for the enhancement of spectrum efficiency," *IEEE Communication Magazine*, vol. 42, no. 3, Mar. 2004.

[45] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," in *IEEE International Conference on Communications (ICC)*, May. 2006, pp. 1658–1663.

[46] Z. Chair and P. K. Varshney, "Optimal data fusion in multiple sensor detection systems," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 22, no. 1, pp. 98–101, Jan. 1986.

[47] C. Mathur and K. Subbalakshmi, "Digital signatures for centralized dsa networks," in *IEEE Workshop on Cognitive Radio Networks*, Jan. 2007, pp. 1037–1041.

[48] R. Chen, J. Park, and J. 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, Jan. 2008.

[49] S. Anand, Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *IEEE International Dynamic Spectrum Access Networks (DySPAN)*, Oct. 2008, pp. 1–6.

[50] Z. Jin, S. Anand, and K. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *IEEE International Conference on Communications (ICC)*, Jun. 2009, pp. 1–5.

[51] Z. Chen, T. Cooklevand, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *IEEE International Performance Computing and Communications Conference*, Dec. 2009, pp. 208–215.

[52] H. Li and H. Zhu, "Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems," in *IEEE Global Telecommunications Conference (GLOBECOM)*, Dec. 2009, pp. 1–6.

[53] ——, "Blind dogfight in spectrum: combating primary user emulation attacks in cognitive radio systems with unknown channel statistics," in *IEEE International Conference on Communications (ICC)*, May. 2010, pp. 1–6.

[54] D. Tracy and P. Dwyer, "Multivariate maxima and minima with matrix derivatives," *The Journal of the American Statistical Association*, vol. 64, no. 328, pp. 1576–1594, Dec. 1969.

[55] A. Taherpour, M. Nasiri-Kenari, and S. Gazor, “Multiple antenna spectrum sensing in cognitive radios,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 2, pp. 814–823, Feb. 2010.

[56] S. Atapattu, C. Tellambura, and H. Jiang, “Analysis of area under the ROC curve of energy detection,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 3, pp. 1216–1225, Mar. 2010.