EFFICIENT SYSTEM PROPERTIES FOR 5G NETWORKS

BY

HAMZA IQBAL

01-244182-005

SUPERVISED BY

DR. JUNAID IMTIAZ

Session-2018-2020

A Report Submitted to the Department of Electrical Engineering

Bahria University, Islamabad

in partial fulfilment of the requirement for the degree of MS(EE)

CERTIFICATE

We accept the work contained in this report as a confirmation to the required standard for the partial fulfillment of the degree of MS(EE).

_____	_____
Head of Department	Supervisor
_____	
Internal Examiner	External Examiner

DEDICATION

I would like to dedicate this thesis to my parents, siblings, friends, supervisor, and teachers for their love, endless support, and strong motivation which helped me in achieving my goals.

DECLARATION OF AUTHORSHIP

I hereby declare that the content of this thesis is my own work and that it is the result of work done during the period of registration. To the best of my knowledge, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or another institute of higher learning, except where due acknowledgment has been made in the text.

_____

(Student Signature)

ACKNOWLEDGMENTS

Firstly, I want to thank Allah Almighty, without his grace I could not have achieved anything. I like to especially thank Dr. Junaid Imtiaz, my supervisor, and teacher, for his advice, supervision, great support and guidance throughout the completion of this work. I would also thank my Electrical Engineering Department for their support and guidance.

This memorable period cannot be finalized without the inspiration and support of my family and friends. I also thank my friends who contributed to my research in every manner.

Thank you all.

(Hamza Iqbal)

ABSTRACT

Cognitive radio technologies tackle spectrum scarcity issues in the bandwidth when the number of users in the network begin to rise. Secondary users that access to the spectrum have to sense beforehand to detect any free spectrum offered and upon opportunity of vacant spectrums, gain access. During sensing, the network is prone to security attacks that are commonly caused by malicious users which severely affect the throughput of the network. In conventional spectrum access scheme, a fixed threshold is set that determines the transmitter energy of incoming signal. In this thesis, the throughput is analyzed and enhanced during the overlay mode of secondary user transmission, in the incidence of primary user emulation attackers, all the while optimizing the threshold of sensing that reduces the total error probability, that outperforms that of a conventional scheme that uses a fixed threshold.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

PUEA	Primary User Emulation Attack
SSDF	Spectrum Sensing Data Falsification
QoI	Quality-of-Information
QoS	Quality-of-Service
BER	Bit Error Rate
SNR	Signal-to-Noise Ratio
FCC	Federal Communication Commission
RF	Radio Frequency
OFDM	Orthogonal Frequency Division Multiplexing
PU	Primary User
SU	Secondary User
CU	Cognitive User
FC	Fusion Center
PUE	Primary User Emulation
AWGN	Additive White Gaussian Noise
PSK	Phase Shift Keying
QPSK	Quadrature Phase Shift Keying
BS	Base Station

DRT	Distance Ratio Test
DDT	Distance Difference Test
CR	Cognitive Radio
RSS	Received Signal Strength
TV	Television
CR-MANET	Cognitive Radio Mobile Ad-Hoc Network
iid	independent and identically distributed

Chapter 1

Introduction

CHAPTER 1. INTRODUCTION

1.1. Thesis Background/Overview

Cognitive wireless networks [1], [2] are an emerging field of next-generation telecommunications that provide adaptive modulation to wireless communication networks to detect and occupy available spectrum bands on the network, depending on the opportunity, and to provide opportunity reservations (mainly occupied by cognitive users). Some users of cognitive wireless networks attack networks internally by occupying spectrum bands, reducing spectrum efficiency and throughput, or by falsifying transmitting data during spectrum detection, corrupting the data [3]. These are malicious users who damage network security.

Cognitive spectrum detection in cognitive wireless networks generally improves the accuracy of spectrum detection to improve spectrum utilization. During these detection intervals 1) a *primary user emulation attack* (PUEA) [4], [5] or 2) a *spectrum sensing data falsification* (SSDF) [6], [7] attack headed by a malicious user on the system will occur. Therefore, a malicious attack will take advantage of network security, spectrum and corrupt throughput.

Cognitive wireless network throughput depends on two factors: detectability (which is determined by probability of detection) and the likelihood of PU being inactive momentarily before detection (determined by probability of false alarms) [8], [9]. Through a thorough understanding of the two malicious attacks, each attack affects its own way of handling. However, it computes both similar results: the probability of increased error, reduced throughput and wasted spectrum

1.2. Cognitive Radio Networks

The main idea and purpose behind cognitive radio is to use software resources that are designed to adapt to all existing wireless networks and to promote cognition by software radio

and provide maximum quality-of-information (QoI). The main focus is to provide spectrum sharing while alleviating the problem of lack of spectrum in telecommunication networks. This is handled by providing an opportunistic approach in the used and unused spectrum bandwidth that interferes minimally with licensed users.

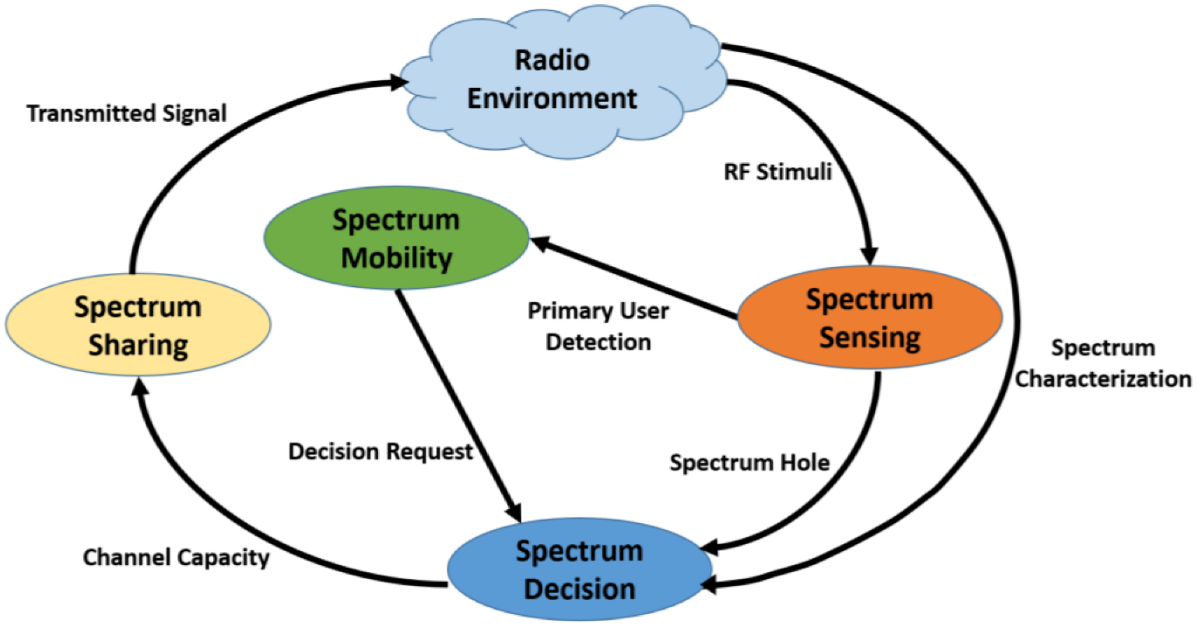

Figure 1.1. The cognitive radio cognition cycle [33]

Cognitive radio technology does the following: 1) When operating in a licensed band, identify vacant spectrum bands and search for authenticated users. 2) Selecting of best channel provided. 3) Coordinating access to channels with other users and 4) Securing channels if authorized users are detected.

In short:

- Spectrum sensing
- Spectrum management
- Spectrum sharing
- Spectrum mobility

This technology is a key enabler for wireless networks to utilize spectrum dynamically. Properties essential to the network are: *cognitive capability* and *reconfigurability* [2], [10]

1.2.1. Cognitive Capability

This allows cognitive radio functions to work together with real time environment to determine the proper communication factors and adjust to the environment accordingly. It is described in Fig 1.1, which shows the four main processes of cognitive cycle

Once the spectrum band is known, communication takes place. However, because the wireless environment faces constant variations over time and space, cognitive radios stores the information that can occur due to primary user appearances, or user mobility.

1.2.2. Reconfigurability

The ability to adjust operating parameters for immediate transmission without hardware changes. Some of the integrated reconfigurable parameters are:

Operating frequency: Cognitive radio determines the optimal operating frequency based on radio environment information

Modulation: Adaptive modulation according to user requirements and channel conditions. For delay-sensitive applications, the data rate is holds priority over the error rate, so a spectrally efficient modulation scheme is chosen. Conversely, in loss-sensitive applications, the focus is on the error rate at which low BER modulation is provided.

Transmission power: Power control allows dynamic transmission power setting within power limits.

Communication technology: Provides interoperability between different communication systems.

1.2.3. Spectrum Sensing

An imperative part of cognitive radio is the detection of "spectrum holes," [11] which are empty spectral bands. Cognitive radios are planned to recognize the surrounding environment and adapt accordingly. The three detection techniques are as follows:

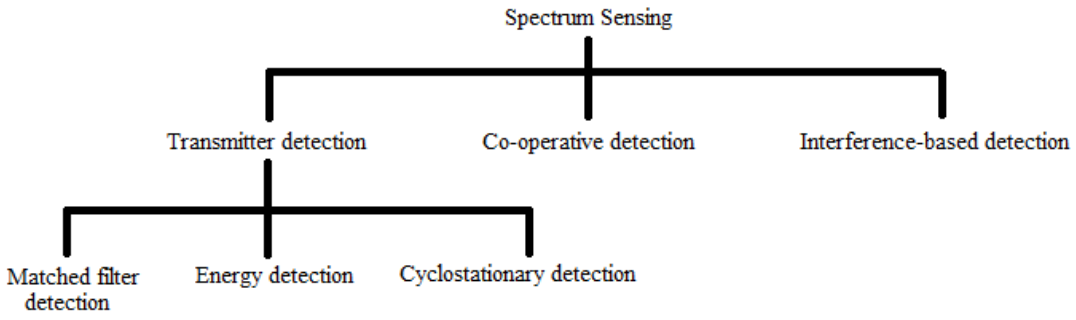

Figure 1.2. Spectrum sensing techniques [3]

1.2.3.1. Transmitter detection

The transmitter detection method is centered on detecting weak signals from the primary transmitters through observing of the mobile user. Three methods are used for transmitter detection: *matched filter detection*, *energy detection*, and *cyclo-stationary detection*.

Matched filter detection [12] is used when primary user signal information is known to the user, so the best detector to maximize the received signal-to-noise ratio (SNR) is the matched filter. It achieves high gain at the receiver for its coherent nature, but you need existing knowledge of the PU's signal, e.g. modulation type and packet information.

Energy detection [12], [20] uses detection that measures received signal energy, where the output is matched to a threshold to check if an authorized user is existent. Energy detection is used when there is insufficient or no information of the signal.

$$E_s = \int_{-\infty}^{\infty} |x(t)|^2 \, dx \tag{1.1}$$

$$E_s = \sum_{n=-\infty}^{\infty} |x(n)|^2 \quad (1.2)$$

where x(t) is the receiving continuous-time signal, and x(n) is the receiving discrete-time signal.

Cyclo-stationary detection [13-15], [21] is an alternate method in which it applies the concept of modulated signals being combined with sine wave carriers. These signals are henceforth categorized as cyclo-stationary as both their mean and autocorrelation display periodicity. It is effective and superior than the previous detection scheme, such that it is better at separating between the noise from the (modulated) signal energy.

1.2.3.2. Co-operative detection

Previous sensing schemes assume that the position of the primary receiver is indefinite, and thus cognitive radio measures weak state transmitter signals based on observing the mobile users. Cooperative detection refers to a spectrum detection method in which information gathered from multiple users is combined to detect the main user. Cooperative detection [16], [21-24] can be central or scattered. In the central case, the user's base station acts as an information-discovery collector, whereas in the distributed case it needs to be exchanged with other users.

Co-operative detection is more accurate among unlicensed users as it minimizes single-user uncertainty. It is also efficient in dense urban areas with additional mitigation of multipath and shadow effects [17].

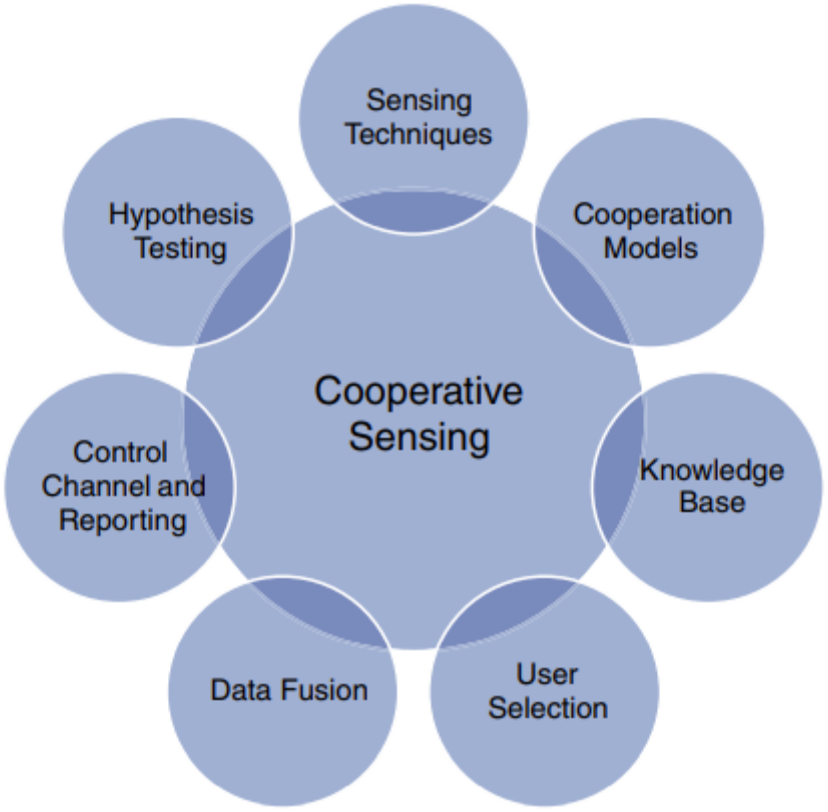

Figure 1.3. Elements of cooperative sensing

1.2.3.3. Interference-based detection

Interference is controlled from the transmitter via the power radiated from the receiver, out-of-band radiation and the position of the transmitter. Therefore, a new technique was introduced called *Interference Temperature* [18] by the FCC.

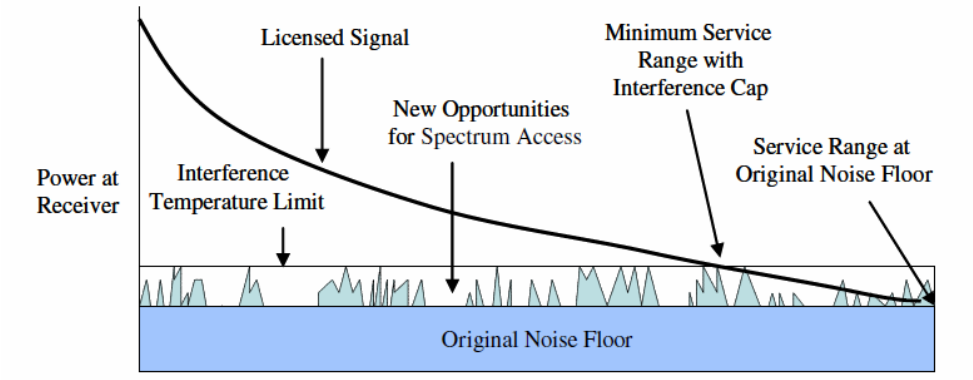

Figure 1.4. Interference temperature model [2]

Fig. 1.4. illustrates the signal behavior in the range where the received power is close to the noise floor. The noise floor increases when additional interfering signals are detected. Therefore, the interference temperature sets the maximum cap, taking into account the accumulated RF energy from multiple transmissions. The spectral band is empty unless the user exceeds the interference limit

1.2.3.4. Challenges

Interference temperature measurement: Users generally know the transmit power level and the exact location, but can cause significant interference at adjacent receivers due to the transfer.

Multi-user networks: There are many wireless networks that consist of multiple users and a default user. Therefore, a multi-user network is less likely to detect a basic user and provides an estimate of real interference.

Detection capability: Finding a default user on a modern wireless network is a quick process. OFDM-based wireless networks [19] take advantage of multiple carrier detection, which reduces detection time. However, this shows an increase in design complexity as it uses a higher number of carriers.

1.2.4. Spectrum Management

Unused spectrum bands in wireless networks are used over a wide frequency range, including bands that are licensed and unlicensed. New management capabilities are needed to provide the highest QoS requirements. These functions are categorized into *spectrum analysis* and *spectrum decision*

1.2.4.1. Spectrum analysis

Spectrum analysis [2] provide an appropriate spectral band to characterize another spectral band that has been misused for its user's requirements. Dynamic behavior of cognitive radio

networks requires not only time-varying wireless network environment but also PU activity and spectrum bandwidth information along with necessary parameters:

Interference: The spectrum band in use determines the interference characteristics of the spectrum band in a congested area.

Path loss: Keeping the user transfer the same reduces the range at higher frequencies.

Wireless link errors: Change in error rate according to modulation method and interference level

Link layer delay: Different types of link layer protocols are required to accommodate the different parameters discussed. As a result, delay in transmission of packets occurs

Holding time: Indicates the estimated time a user can occupy a licensed band before being suspended. Frequent handoffs can reduce hold time, so previous handoff statistics pattern is preferred

1.2.4.2. Spectrum decision

After all frequency bands have been categorized, an appropriate band is finalized for current transmission with QoS requirements in consideration. Based on the user requirements, data rate, acceptable error rate, and bandwidth of transmission can be determined.

1.2.4.3. Challenges

Decision model: The signal to noise ratio is insufficient to distinguish the spectral band. Besides SNR, many constraints affect quality.

Multiple spectrum band decision: Multi-spectrum transfer has less quality degradation than existing transports in a single spectrum band. Also, lower power consumption can be used in the spectrum band during transmission.

Co-operation with reconfiguration: Cognitive wireless technology allows reconstruction of transmission parameters for optimal operation. Therefore, there is a need for a cooperative framework that takes into account both spectrum determination and reconstruction.

1.2.5. Spectrum Sharing

There exist five steps [2] in spectrum sharing:

Spectrum sensing: If an unlicensed user does not use a particular part, the user can only assign a part of the spectrum. Similarly, when a node transmits, it first needs to know the spectrum usage.

Spectrum allocation: Depending on availability, nodes can allocate channels. More dependent on internal spectrum allocation policy.

Spectrum access: Since multiple nodes try spectrum access, coordinated access is needed to avoid collisions with overlapping users in the spectrum.

Transmitter-receiver handshake: Once part of the spectrum has been known, the receiver should also display the selected spectrum.

Spectrum mobility: Nodes are considered visitors of their assigned spectrum, so licensed users must continue to communicate in other empty parts of the spectrum

1.2.6. Spectrum Mobility

Wireless networks aim to use spectrum dynamically so that terminals operate at the highest available spectrum. Spectrum mobility is the method when the user changes its operating frequency.

Spectrum mobility occurs when channel settings deteriorate or when major users come in. Therefore, a new type of handoff, called a *spectrum handoff* [2], occurs. Every time a user changes its operating frequency, the network protocol that manages the node also changes.

Mobility management therefore provides a smooth transition as quickly as possible and minimizes performance degradation.

1.2.6.1. Challenges

At times several frequency bands are available, therefore algorithms are effectively required to decide which spectrum is best for availability, based on the channel characteristics. Once it is selected, the design of a new mobility and connection managing is required to reduce delay and loss.

If the current operating frequency is being used during communication, then the running application must be transmitted in other available frequency bands. Algorithmic support is needed again so that the application does not suffer from poor performance.

1.3. Primary User Emulation Attack

Two types of malicious attacks exist: *data falsification* and *security attacks* [3]. Data falsification compromises detection probability by sending falsified sensing data to fusion centers (FC). Security attacks compromise and disrupt cooperative sensing by adversary attacks.

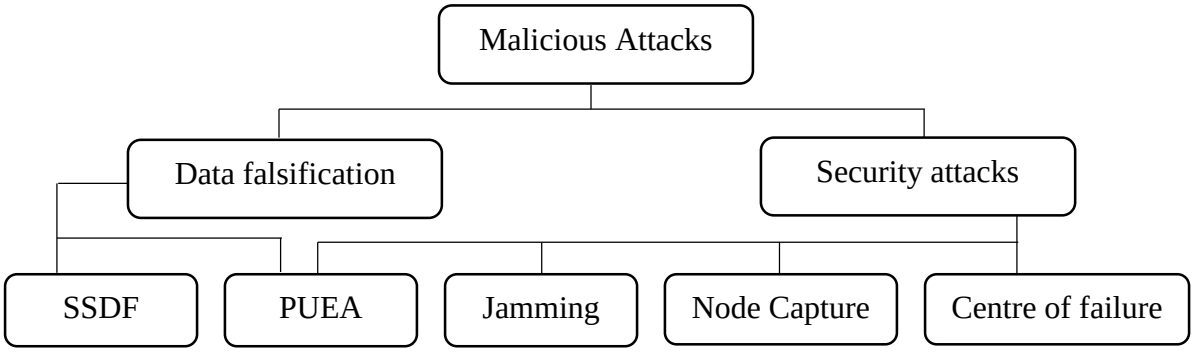

Figure 1.5. Classification of malicious attacks [3]

Primary user emulation attack (PUEA) emulate behavior of the primary user, by sending transmit signals almost in similarity to primary users. When spectrum sensing occurs, cognitive

users mistake these malicious users acting as PUs and thus vacate spectrum and thus attackers wrongfully access the spectrum and its privileges. Attackers variate their wireless transmitting frequency to imitate primary signals, and these attacks happen in the physical layer. Reducing the effects of these PUEAs, hard decision fusion rules occur at FCs to make a global decision.

PUEAs can be broken into two attack models [5]: *Selfish PUEA* and *Malicious PUEA.* Selfish PUEA is when the attacker maximizes its spectrum resources, thus preventing competing secondary users to occupy the vacant spectrum band. Mostly carried by selfish secondary users that use the vacant spectrum for their own intent. Malicious PUEA sole purpose is to hinder the spectrum sensing of legitimate secondary users. Unlike selfish PUEA, malicious does not necessarily need to attack vacant spectrum bands.

For the detection of a primary user emulation attacker, two types of tests are performed: DRT (Distance Ratio Test) and DDT (Distance Difference Test).

DRT depends on the location of the RSS (receiver signal strength) [29], [30] based on a robust correspondence between the distance of the radio link:

$$RSS = P_t G_t G_r \frac{h_t^2 h_r^2}{d^4 L} \tag{1.3}$$

where P_t is the power of the transmitter, G_t and G_r are the antenna gain of the transmitter and receiver, h_t and h_r are the height of the antenna of the transmitter and receiver, d is the propagating distance, and L is other loss.

$$DRT = \rho = \frac{\sqrt{(x_1 - u_1)^2 + (y_1 - v_1)^2}}{\sqrt{(x_2 - u_1)^2 + (y_2 - v_1)^2}} \tag{1.4}$$

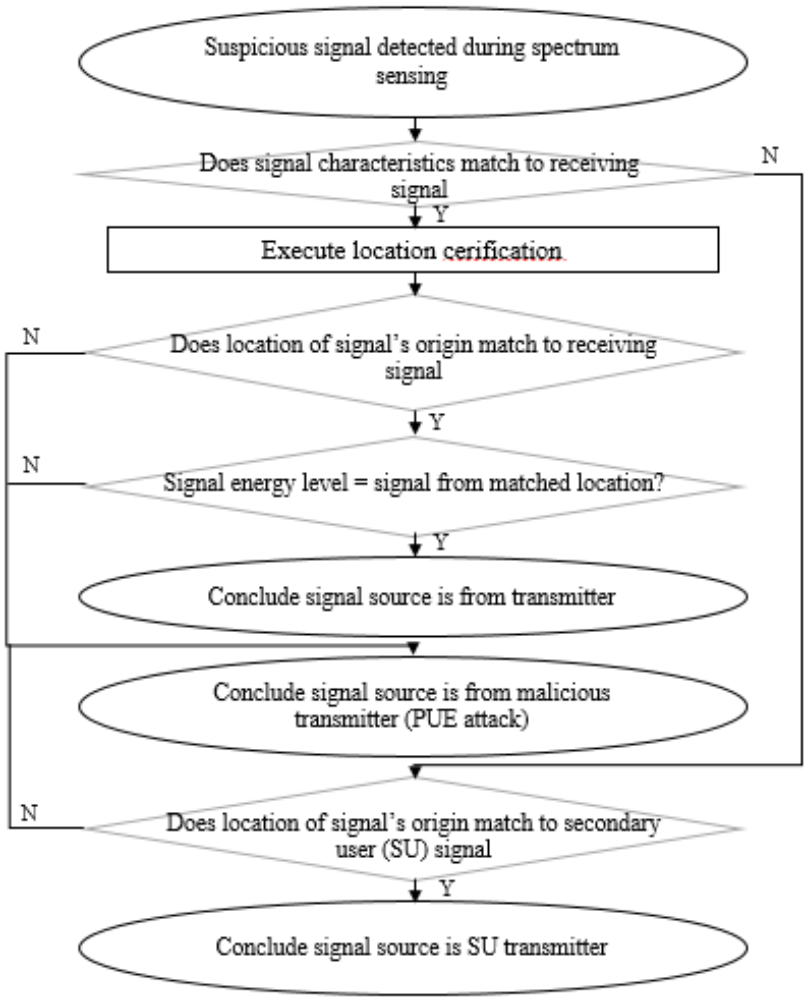

Figure 1.6. Flowchart showing transmitter verification procedure

Since DRT is for a large-scale propagation model (two-ray reflection model), therefore small-scale propagation fluctuations caused by RSS cannot be accurately considered. Also, in DRT, all other minor environmental variables are ignored.

The DDT can check the difference between the primary user and the pair LV and measure the phase change of the signal at both LVs.

$$DDT = \ s = \sqrt{(x_1 - u_1)^2 + (y_1 - v_1)^2} - \sqrt{(x_2 - u_1)^2 + (y_2 - v_1)^2} \qquad (1.5)$$

If both equations 1.4 and 1.5 fail, then the network identifies the presence of a primary user emulation attacker

1.4. Spectrum Sensing Data Falsification Attack

Data falsification occurs when malicious users send falsified data to FC for their own benefits. These severely affect cooperative gain.

Spectrum sensing data falsification attack mostly occur in the link layer and the malicious attackers intentionally send falsified data to FCs which result in an incorrect final decision. There exist three attack models [6] to SSDF attacks. Malicious attackers in the first model reports existence of a high primary user energy and hence concluded by all secondary users that the spectrum is occupied. The intention is to gain select access to the target spectrum. This attack is known as the *Selfish SSDF*. In the second model, in this case, malicious users send data of a primary user having low energy, therefore duping secondary users into sensing a vacant spectrum and therefore occupying it. This causes interference with legitimate primary users that want to occupy the "supposedly" vacant spectrum. Thus this attack is aptly named the *Interference SSDF*. In the third model, secondary users, likely to be malicious, send data either true or false, confusing the FC and thus waits till a consensus is approached for the final decision. This is known as the *Confusing SSDF*.

1.5. Problem Description

Cognitive and software defined radios has now become a popular topic of research in the wireless communication field, as it handles the challenges faced by previous wireless communications, especially spectrum sharing and spectrum allocation. But despite this improvement this new field of research faces many challenges, such as improving throughput, reducing probability of error, and increasing the speed of spectrum sharing and spectrum allocation. Recently, malicious users have posed new threat to cognitive radio networks, in such that attacks now occur within the radio network, which severely factors the degradation of performance in cognitive radio networks, such as throughput, spectrum utilization and efficiency, and bit-error rate.

1.6. Thesis Objectives

In this thesis, we will design and implement a cognitive radio network for a single secondary user transmitter and receiver, all while in the presence of primary user emulation attack, using energy detection sensing scheme. The secondary user is operating in overlay mode i.e. SU transmitter power is maximum. Optimizing the threshold at which spectrum sensing and detection occurs which will provide us with a throughput versus probability of error curve and observe how throughput varies with the increase in error probability. We will observe how an optimized threshold also beats the conventional scheme that is constructed on a fixed threshold. An increase in throughout is expected which will be compared to conventional sensing scheme and related literature.

1.7. Thesis Organization

The thesis is structured as follows: Chapter 2 focuses on related works dealing with error reduction in non-cooperative spectrum sensing PUE attacks and a study on throughput of cognitive radio networks, throughput performance under the presence of primary user emulation attack using a hybrid spectrum access scheme, and throughput performance by optimal threshold selection approach in the presence of primary user emulation attack. Chapter 3 will discuss the system model for our analytical view on throughput and error probability. Chapter 4 discusses the simulation results for the effects of throughput and enhancing throughput and simulated result discussion. Chapter 5 will focus on future work and conclusion

Chapter 2

Literature Review

CHAPTER 2. LITERATURE REVIEW

In this chapter, a literature review on the analysis of the two sensing techniques discussed in Chapter 1, Section 1.2.3 is done, and decide which of the two is more feasible. We will also see which type of attack is more prevalent, and how a relation exists between spectrum sensing and throughput and discuss a tradeoff between the two.

2.1 Sensing-Throughput Tradeoff

Using an energy detector system, a relationship is established between the detection probability and the false probability [9] that focuses on complex PSK and CSCG noise. For target probability of detection $\bar{P}_d$, the probability of false alarm is:

$$P_f = Q\left(\sqrt{2\gamma + 1}Q^{-1}(\bar{P}_d) + \sqrt{\tau f_s}\gamma\right) \tag{1.6}$$

where γ is the received signal-to-noise ratio of the primary user, and τ is the detection time of the transmission slot duration. Detection threshold ε:

$$Q^{-1}(\bar{P}_f) = \left(\frac{\epsilon}{\sigma_u^2} - 1\right)\sqrt{\tau f_s} \tag{1.7}$$

where σ_u^2 is variance of noise.

Similarly, for a target probability of false alarm $\bar{P}_f$, P_d is:

$$P_d = Q\left(\sqrt{2\gamma + 1}(Q^{-1}(\bar{P}_f) - \sqrt{\tau f_s}\right) \tag{1.8}$$

And the detection threshold ϵ is determined as:

$$\left(\frac{\epsilon}{\sigma_u^2} - \gamma - 1\right)\sqrt{\frac{\tau f_s}{2\gamma + 1}} = Q^{-1}(\bar{P}_d) \tag{1.9}$$

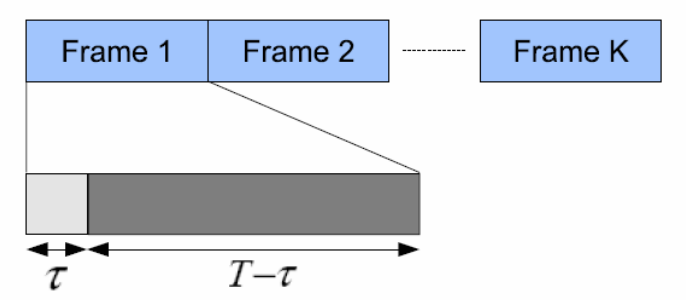

Figure 2.1. Frame design of cognitive network with intermittent spectrum sensing

C_0 is denoted as the throughput when primary users are absent, and C_1 is throughput when primary user is present, then

$$C_0 = \log_2(1 + SNR_S) \tag{2.0}$$

$$C_1 = \log_2\left(1 + \frac{SNR_S}{1 + SNR_P}\right) \tag{2.1}$$

where SNR_S is signal-to-noise ratio of secondary user and SNR_P is the interference signal-to-ratio when a primary user is present.

There are two scenarios present now:

Scenario 1: Primary user is missing and no false alarm created; throughput comes out as $\frac{T-\tau}{T} C_0$.

Scenario 2: Primary user is existent but not sensed; throughput comes out as $\frac{T-\tau}{T} C_1$

Thus it is defined:

$$R_0(\epsilon, \tau) = \frac{T-\tau}{T} C_0 \left(1 - P_f(\epsilon, \tau)\right) P(H_0) \tag{2.2}$$

and

$$R_1(\epsilon, \tau) = \frac{T-\tau}{T} C_1 \left(1 - P_d(\epsilon, \tau)\right) P(H_1) \tag{2.3}$$

Then the average achievable throughput for the secondary link comes out as

$$R(\tau) = R_0(\epsilon, \tau) + R_1(\epsilon, \tau) \tag{2.4}$$

The purpose of the sensing-throughput trade-off is to identify the optimal sensing time τ of each frame so that the achievable throughput is maximized while the primary user is sufficiently protected, so the optimization comes out as follows.:

$$\max_{\tau} \; R(\tau) = R_0(\epsilon, \tau) + R_1(\epsilon, \tau) \tag{2.5}$$

$$s.t. \qquad P_d(\epsilon, \tau) \geq \bar{P}_d$$

The target probability of detection $\bar{P}_d$ is set as 0.9 and SNR of -20db. The activity probability $P(H_1)$ is assumed to be less than 0.3. Since $C_0 > C_1$, the term on the right hand side of (2.5) is diminished, therefore:

$$\max_{\tau} \; \tilde{R}(\tau) = R_0(\epsilon, \tau) \tag{2.6}$$

$$s.t. \quad P_d(\epsilon, \tau) \geq \bar{P}_d$$

For energy detector scheme and by $P_d = \bar{P}_d$, the equation (2.6) becomes:

$$\tilde{R}(\tau) = C_0 P(H_0) \left(1 - \frac{\tau}{T}\right) \left(1 - Q\left(\alpha + \sqrt{\tau f_s}\gamma\right)\right) \tag{2.7}$$

where

$$\alpha = \sqrt{2\gamma + 1} Q^{-1}(\bar{P}_d) \tag{2.8}$$

Fig. 2.2 shows the curve achieved from equation (2.7) and equation (2.8) respectively. Both quantities show a maximum throughout at around 2.55ms.

2.2 Throughput Performance Under PUEA with Spectrum Prediction

In [31], a hybrid spectrum access system, where the CU shifts among overlay or underlay modes depending on spectrum sensing decision, is used to enhance the performance of throughput. It uses an imperfect spectrum prediction model that investigates the impact of PUE attacks through which an analytical expression is derived for the CU's throughput.

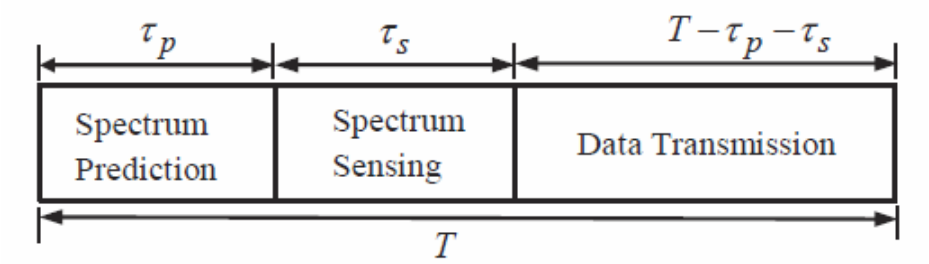

Figure 2.2 Frame structure of CU for spectrum access

First, the CU performs spectrum prediction for the number of channels present. The likelihood is a binary hypotheses test where the channels likelihood is idle or busy, during which the PU can be present or absent. These are indicated by two hypotheses H_0 and H_1:

The idle prediction is given as:

$$p_0 = P(H_0)(1-p_e) + P(H_1)p_e \tag{2.9}$$

And busy prediction is as:

$$p_1 = P(H_0)p_e + P(H_1)(1-p_e) \tag{3.0}$$

After spectrum prediction, CU performs sensing on idle channels only. The presence of PUE signals under the two hypotheses H_0 and H_1 are $\alpha = P(A^{on}/H_0)$ and $\beta = P(A^{on}/H_1)$ respectively (where α and β are two conditional properties). The absence of PUE signals under the two hypotheses H_0 and H_1 are $P(A^{off}/H_0) = 1 - P(A^{on}/H_0) = 1 - \alpha$ and $P(A^{off}/H_1) = 1 - P(A^{on}/H_1) = 1 - \beta$ respectively

The received signal at CU is:

$$y(i) = \begin{cases} w(i) & H_{s_0}: noise\ only \\ h_{p_1 s_1} s_1(i) + w(i) & H_{s_1}: PU + noise \\ h_{As_1} s_2(i) + w(i) & H_{s_2}: PUE + noise \\ h_{p_1 s_1} s_1(i) + h_{As_1} s_2(i) + w(i) & H_{s_3}: PU + PUE + noise \end{cases} \quad (3.1)$$

where y(i) is the received signal, w(i) is the additive noise that an iid arbitrary process with zero mean and variance σ_u^2 , $s_1(i)$ is the PU signal which is an iid arbitrary process with zero mean and variance $\sigma_{s_1}^2$, and $s_2(i)$ is the PU signal that is an iid arbitrary process with zero mean and variance $\sigma_{s_2}^2$. PUE transmitter and PU transmitter channels are denoted as h_{As_1} and $h_{p_1 s_1}$ respectively.

The probabilities of false alarms and probabilities of detections are presented below

$$P_{f_1}(\tau_s) = P\left(D^{on} \middle| H_{s_0}\right) = Q\left\{\frac{(\lambda - \mu_0)}{\sigma_0}\right\} \quad (3.2)$$

$$P_{d_1}(\tau_s) = P\left(D^{on} \middle| H_{s_1}\right) = Q\left\{\frac{(\lambda - \mu_1)}{\sigma_1}\right\} \quad (3.3)$$

$$P_{f_2}(\tau_s) = P\left(D^{on} \middle| H_{s_2}\right) = Q\left\{\frac{(\lambda - \mu_2)}{\sigma_2}\right\} \quad (3.4)$$

$$P_{d_2}(\tau_s) = P\left(D^{on} \middle| H_{s_3}\right) = Q\left\{\frac{(\lambda - \mu_3)}{\sigma_3}\right\} \quad (3.5)$$

where τ_s is the spectrum sensing frame.

Now, $\mu_0 = \sigma_u^2$, $\sigma_0^2 = \frac{1}{M}\sigma_u^4$, $\mu_1 = \sigma_u^2(\gamma_1 \left|h_{p_1 s_1}\right|^2 + 1)$, $\sigma_1^2 = \frac{1}{M}\sigma_u^4(\gamma_1 \left|h_{p_1 s_1}\right|^2 + 1)^2$, $\mu_2 = \sigma_u^2(\gamma_2 \left|h_{As_1}\right|^2 + 1)$, $\sigma_2^2 = \frac{1}{M}\sigma_u^4(\gamma_2 \left|h_{As_1}\right|^2 + 1)^2$, and $\mu_3 = \sigma_u^2(\gamma_1 \left|h_{p_1 s_1}\right|^2 + \gamma_2 \left|h_{As_1}\right|^2 + 1)$, $\sigma_3^2 = \frac{1}{M}\sigma_u^4(\gamma_1 \left|h_{p_1 s_1}\right|^2 + \gamma_2 \left|h_{As_1}\right|^2 + 1)^2$. Here $\gamma_1 = \sigma_{s_1}^2/\sigma_u^2$ and $\gamma_2 = \sigma_{s_2}^2/\sigma_u^2$ are the signal-to-noise ratio due to PU and PUE signals at SU.

Now the SU transmits data in a hybrid spectrum access scheme, i.e. in overlay or underlay modes depending on the PU being absent or present. In overlay approach, SU communicates at maximum power, and in underlay approach, SU communicates with a measured power with

a supportable interference limit forced by the PU. The following table discusses the various cases the SU operates in overlay or underlay modes:

Table 1 Hybrid spectrum access scheme for SU

Case	True channel state	Prediction results	Sensing decision	PUE	Transmission scheme
1.	Idle	Idle	Idle	OFF	Overlay
2.	Idle	Idle	Idle	ON	Overlay
3.	Idle	Idle	Busy	OFF	Underlay
4.	Idle	Idle	Busy	ON	Underlay
5.	Idle	Busy	Idle	OFF	Overlay
6.	Idle	Busy	Idle	ON	Overlay
7.	Idle	Busy	Busy	OFF	Underlay
8.	Idle	Busy	Busy	ON	Underlay

The mean capacity of SU can be expressed as:

$$C_j = B \int_0^{\infty} \log_2(1+x) f_{\gamma_j}(x)\, dx \tag{3.6}$$

Now the SU's throughputs are expressed as:

$$R_1 = \left(\frac{T-\tau_p-\tau_s}{T}\right) C_1(1-P_1)P(H_0)(1-\beta) \tag{3.7}$$

$$R_2 = \left(\frac{T-\tau_p-\tau_s}{T}\right) C_2(1-P_2)P(H_0)\beta \tag{3.8}$$

$$R_3 = \left(\frac{T-\tau_p-\tau_s}{T}\right) C_3P_3P(H_0)(1-\beta) \tag{3.9}$$

$$R_4 = \left(\frac{T-\tau_p-\tau_s}{T}\right) C_4P_4P(H_0)(1-\beta) \tag{4.0}$$

$$R_5 = \left(\frac{T-\tau_p-\tau_s}{T}\right) C_5(1-P_5)P(H_0)(1-\beta) \tag{4.1}$$

$$R_6 = \left(\frac{T-\tau_p-\tau_s}{T}\right) C_6(1-P_6)P(H_0)\beta \tag{4.2}$$

$$R_7 = \left(\frac{T-\tau_p-\tau_s}{T}\right) C_7P_7P(H_0)(1-\beta) \tag{4.3}$$

$$R_8 = \left(\frac{T - \tau_p - \tau_s}{T}\right) C_8 P_8 P(H_0)(1 - \beta) \tag{4.4}$$

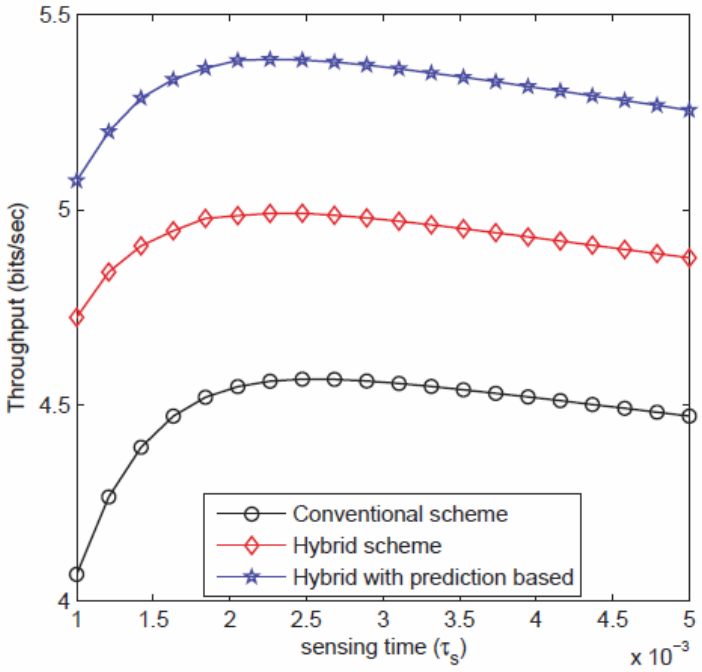

Figure 2.3 Throughput versus sensing time

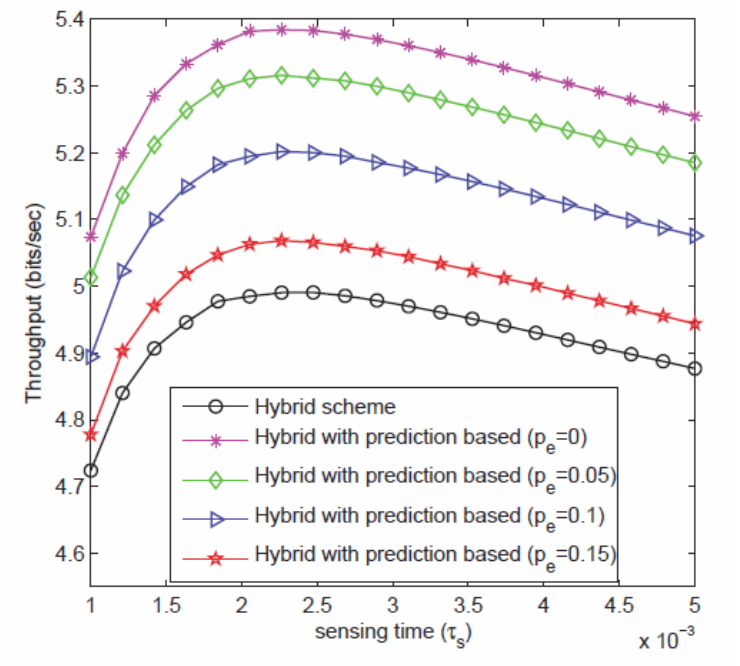

Figure 2.4 Throughput versus sensing time with imperfect spectrum prediction

Fig. 2.4. analyzes the throughput of the secondary user with conventional, hybrid access with and without spectrum likelihood. In the hybrid scheme, SU transmits data in underlay mode since PU is absent, and by spectrum prediction SU senses idler channels, thus it operates in overlay mode, and the reason why throughput increases significantly

Fig. 2.5. discusses the increase in throughput of SU by imperfect spectrum prediction, it is also observed that as prediction errors occur, the throughput decreases. This reduces selecting idle PU channels, which reduces data transmission

2.3 Throughput Performance Under PUEA By Optimal Threshold

In [32], two threshold models are discussed: the first being the conventional optimal threshold and the second being the proposed optimal threshold. There exist two hypotheses of the PU being absent or present denoted by H_0 and H_1 respectively, and $P(H_0)$ and $P(H_1)$ being their respective probabilities

So now the conventional threshold is derived to be:

$$\lambda = \frac{(\mu_0\sigma_1^2 - \mu_1\sigma_0^2) + \sqrt{L}}{(\sigma_1^2 - \sigma_0^2)} \tag{4.5}$$

where $L = (\mu_0\sigma_1^2 - \mu_1\sigma_0^2)^2 + (\sigma_1^2 - \sigma_0^2) * \left(\mu_1^2\sigma_0^2 - \mu_0^2\sigma_1^2 + 2\mu_0^2\sigma_1^2 \ln\left(\frac{\sigma_{1P(H_0)}}{\sigma_0 P(H_1)}\right)\right)$

The proposed optimal threshold was calculated by numerical methods, from which the throughput of CRN was evaluated with PUE attackers. The values of the optimal threshold were plugged in the false alarm probability and detection probability expressions stated below:

$$P_f(\tau) = (1-\beta)P_{f_1}(\tau) + \beta P_{f_2}(\tau) \tag{4.6}$$

$$P_d(\tau) = (1-\alpha)P_{d_1}(\tau) + \alpha P_{d_2}(\tau) \tag{4.7}$$

$$P_e(\tau) = P_f(\tau)\mathrm{P}(H_0) + (1\text{-}P_d(\tau))\mathrm{P}(H_1) \tag{4.8}$$

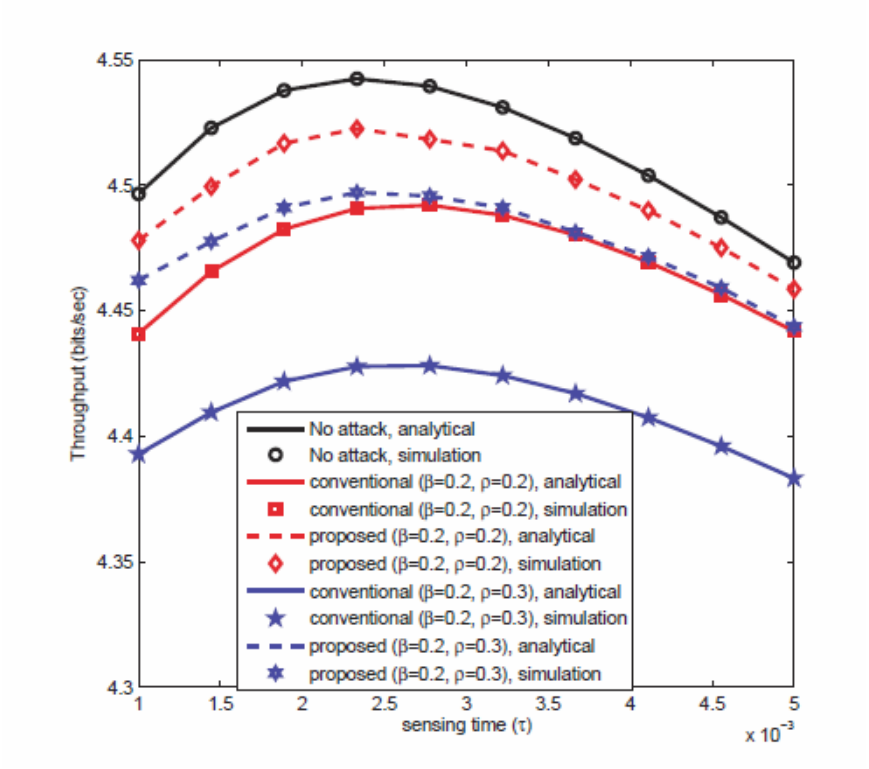

Figure 2.5. Throughput for different β

Fig. 2.6. shows the throughput of the SU with varying attacker strength ρ = 0.2, 0.3 and presence of attacker probability β = 0.2. Upon observation, throughput decreases as the attacker strength increases, which concludes the existence of PU under the hypothesis H_0 with a higher likelihood which degrades the throughput.

Chapter 3

Methodology

CHAPTER 3. METHODOLOGY

Using an energy detection scheme, we can implement a model for a distinct SU spectrum sensing to understand how throughput is determined, and a PUEA affects the throughput of a system

3.1 System Design

The reason energy detection is used in our design is due to its simplicity and how malicious attack analysis is easier to understand. By running Monte-Carlo simulation, energy detection scheme can be implemented to conclude the probability of detection versus probability of false alarm.

The modulation scheme used is a QPSK signal with a bandwidth of 6 MHz with a sampling frequency at the Nyquist rate, and noise is zero-mean CSCG variable.

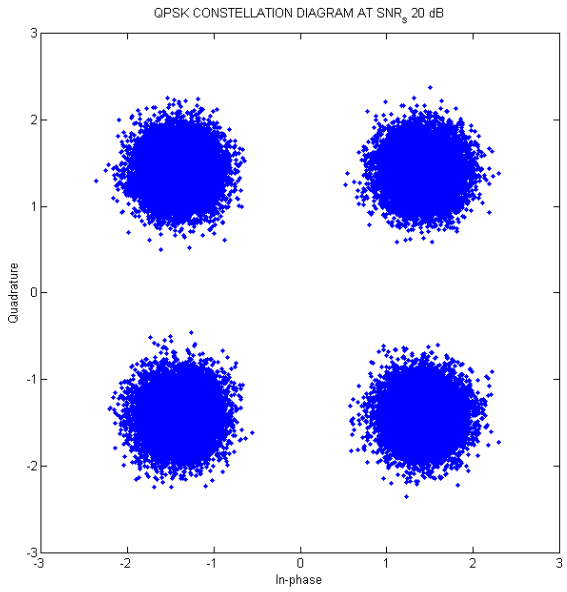

Figure 3.1. QPSK constellation diagram with SNR_s at 20 dB

An analytical is designed where there exist a single PUE attacker and a pair of primary user transmitter and receiver, and a pair of secondary user transmitter and receiver, under Rayleigh

fading channel, and all links are iid complex Gaussian variables. Four channels are present in Fig. 3.1., each having separate channel gains respectively: $g_{pt\text{-}sr} = |h_{pt\text{-}sr}|^2$, $g_{pt\text{-}st} = |h_{pt\text{-}st}|^2$, $g_{st\text{-}sr} = |h_{st\text{-}sr}|^2$, $g_{st\text{-}pr} = |h_{st\text{-}pr}|^2$ and $g_{st\text{-}sr} = |h_{st\text{-}sr}|^2$.

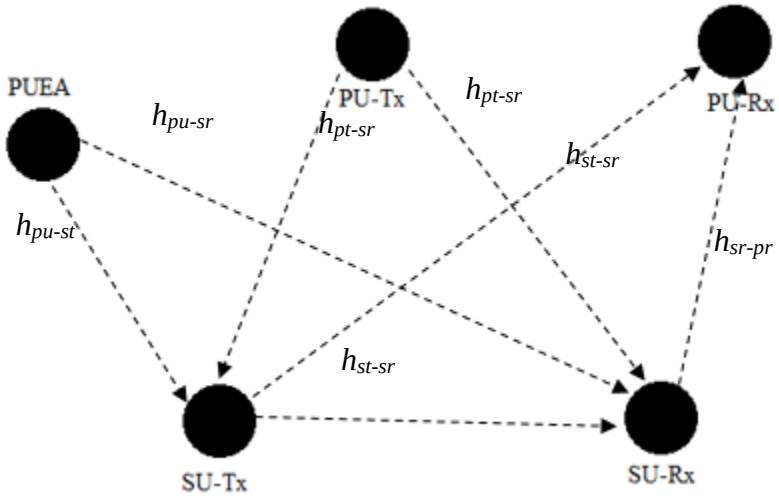

Figure 3.2. One secondary user system model

The receiving signal at the secondary user during sensing channel follows the given expression:

$$y(n) = \begin{cases} w(n) & H_1: only\ noise \\ h_{pt-sr}.s(n) + w(n) & H_2: PU + noise \\ h_{pu-sr}.s(n) + w(n) & H_3: PUEA + noise \end{cases} \quad (5.0)$$

The test statistics with which energy detection for SU occurs is given below

$$T = \frac{1}{K}\sum_{n=1}^{K}|y(n)|^2 \quad (5.1)$$

where the number of samples $K = \sqrt{\tau f_s}$

The threshold is determined by the Neyman-Pearson hypothesis test, which is given as:

$$\lambda = \sigma_T Q^{-1}(P_f) + \mu_T \quad (5.2)$$

Throughput for a cognitive radio utilizes Shannon's capacity theorem used for C_0 and C_1 in (2.0) and (2.1) respectively, while ensuring that the primary user is secure from malicious

attacks. With SNR_p = -15 dB at the primary transmitter and SNR_s = 20 dB at the secondary receiver, the scalar values of capacity are determined as C_0 is 6.658, and C_1 is 6.614. Thus the achievable throughput is determined from R(τ) from (2.4). The parameters are presented in the table below:

Table 2 Parameters for achievable throughput under the presence of PUEA

Parameter	Defined values
SNR at PU-Tx	-15 dB
SNR at SU-Rx	20 dB
Time frame (T)	100 ms
Sensing time	5 ms
Bandwidth	6 MHz
Modulation	QPSK
Attacker strength (ρ_a)	0.3
Attacker probability (β)	0.2
Probability of absence of attacker H_0 ($P(H_0)$)	0.8
Probability of presence of attacker H_1 ($P(H_1)$)	0.2

The overall probability of false alarm w.r.t. the sensing period is determined for hypothesis H_1 from (5.0):

$$\begin{aligned} P_f(\tau) &= P(D^{on}|H_0) \\ &= P\left(D^{on}\middle|H_{0,}A^{off}\right)P(A^{off}\middle|H_0) \\ &\quad + P\left(D^{on}\middle|H_{0,}A^{on}\right)P(A^{on}|H_0) \\ &= (1-\beta)P_{f_1}(\tau) + \beta P_{f_2}(\tau) \end{aligned} \tag{5.3}$$

where β is the probability of presence of PUE signal $P(A^{on}|H_0)$ and $P(A^{off}\middle|H_0) = 1-\beta$, and:

$$\begin{aligned} P_d(\tau) &= P(D^{on}|H_1) \\ &= P\left(D^{on}\middle|H_{1,}A^{off}\right)P(A^{off}\middle|H_1) \\ &\quad + P\left(D^{on}\middle|H_{1,}A^{on}\right)P(A^{on}|H_1) \end{aligned} \tag{5.4}$$

$$= (1-\alpha)P_{d_1}(\tau) + \alpha P_{d_2}(\tau)$$

where α is the probability of presence of PUE signal $P(A^{on}|H_1)$ and $P(A^{off}\big|H_1) = 1-\alpha$.

By defining an optimal threshold, we can determine the highest achievable throughput. The optimal threshold is achieved from the mean capacity C_j of the SU from (3.6). Therefore:

$$C_1 = -\frac{B}{\log_e 2}\exp(N_0/p_s)E_i(-N_0/p_s) \tag{5.5}$$

$$C_2 = \frac{Bp_s}{(p_a-p_s)\log_e 2}\exp(N_0/p_s)E_i(-N_0/p_s) - \frac{Bp_s}{(p_a-p_s)\log_e 2}\exp(N_0/p_a)E_i(-N_0/p_a) \tag{5.6}$$

Now, conventional threshold is determined in the absence of any attackers, therefore α and β are equal to 0, which gives $P_d(\tau) = P_{d_1}(\tau)$ from (5.4) and $P_f(\tau) = P_{f_1}(\tau)$ from (5.3). Since for optimal threshold in the presence of attackers, the achievable throughput now is:

$$R_1 = \left(\frac{T-\tau}{T}\right) C_1 \left(1 - P_{f_1}(\tau)\right) P(H_0)(1-\beta)$$

$$R_2 = \left(\frac{T-\tau}{T}\right) C_2 \left(1 - P_{f_2}(\tau)\right) P(H_0)(\beta)$$

and the overall achievable throughput is determined as:

$$R = R_1 + R_2$$

Chapter 4

Evaluation

CHAPTER 4. EVALUATION

Simulations were carried out in Matlab and the parameters for performance evaluation of the proposed system. Unless stated otherwise, the parameters are: target probability of detection will be set at 0.9, and both are measured under the influence of a PUEA

4.1 Simulation Results

The curve in figure 4.1 shows the throughput vs probability of error. As it is observed, for a conventional threshold, the throughput that appears at the probability of false alarm set at 0.1 and minimum probability of error is 5.12. However, for optimal threshold the throughput increases significantly for the same parameters set. The PUE attacker sends large amounts of PU signal, as the probability of the attacker increases. This in turn degrades the throughput whereas the power of the attacker strength is kept the same i.e. at 0.3

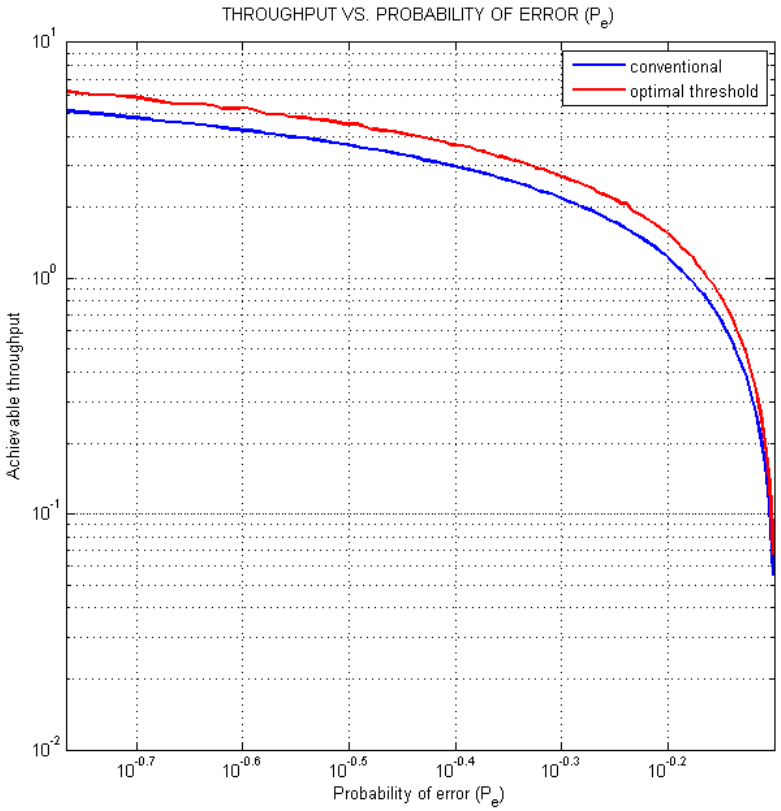

Figure 4.1. Achievable throughput versus probability of error at SNR 20 dB at SU

4.2 Result Discussion

Table 3 Result analysis with related work

Related Work	Attacker probability (β)	Attacker strength (ρ)	Throughput (bits/sec)	Sensing time (τ_s) (ms)	Increase/ Decrease
[9]	-	-	5.12	2.55	-
[31]	0.2	0.5	5.40	2.26	5.46% increase
Optimal Threshold	0.2	0.3	5.80	2.55	7.41% increase

In [9], a sensing-throughput tradeoff is implemented where the optimum throughput is achieved at a sensing interval of 2.55 ms. In this case however, there were no PUE attackers and therefore the throughput measured was in the absence of such attackers, hence the lack of any attacker probability and attacker strength.

In [31], the hybrid scheme applied utilizes sensing that operates in underlay and overlay schemes when attacker probability is at 0.2 and attacker strength is 0.5. The operation of data transmission is in the overlay mode while in the presence of PUE attackers. As the attacker strength increases during the absence of PU, SU detects attacker as PU signal therefore detection occurs and henceforth throughput decreases conventionally. With the hybrid scheme that incorporates spectrum prediction, the throughput goes through an increase of 5.46%

For optimal threshold, for the same attacker probability and reduced attacker strength of 0.3, the throughput for the given network increases. Since increasing attacker strength increases the likelihood of PU being absent and the strength of attacker is higher, throughput decreases. Therefore, a middle ground is achieved where the sensing time is at 2.55 ms and the attacker strength is at 0.3, which in turn maximizes the throughput.

Chapter 5

Conclusion and Future Work

CHAPTER 5. CONCLUSION AND FUTURE WORK

To conclude this research, the relation between the throughput and the probability of error was established and showed how the results proved it. It also illustrated how the influence of PUEA affected spectrum sensing and throughput of the network. A multi-user network can be established to further reduce the probability of error and in turn increase throughput. The main focus to use energy detection was due to its simplicity and popularity, therefore PUs were under constant threat of PUEA attack. A cooperative sensing model or other non-cooperative models that provide better robustness to the network can yield better results.

REFERENCES

[1] J. Mitola and G. Q. Maguire, Jr, "Cognitive radios: making software radios more personal," IEEE Personal Communications, vol. 6, no. 4, pp. 13-18, Aug. 1999

[2] I. F. Akyilidz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless network: a survey," Computer Network Journals (Elsevier), vol. 50, no. 13, pp. 2127-2159, Sept. 2006

[3] I. F. Akyilidz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: a survey," Physical Communicaton (Elsevier), vol. 4, no. 1, pp. 40-62, March 2010

[4] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks", in 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, 14-17 Oct. 2008, pp. 1-6

[5] R. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, Sept. 2006, pp. 110-119

[6] F. R. Yu, H. Tang, M. Huang, Z. Li, and P. C. Mason, "Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios," in MILCOM 2009 – 2009 IEEE Military Communications Conference, 18-21 Oct. 2009, pp. 1-7

[7] R. Chen, J. M. Park, Y. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," IEEE Communications Magazine, vol. 46, no. 4, pp/ 50-55, Apr. 2008

[8] J. Hillenbrand, T. A. Weiss, and F. K. Jondral, "Calculation of detection and false alarm probabilities in spectrum pooling systems," IEEE Communications Letters, vol. 9, no.4, pp. 349-351, Apr. 2005

[9] Y. C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," IEEE Transactions on Wireless Communications, vol. 7, no. 4, pp. 1326-1337, Apr, 2008

[10] R. W. Thomas, D. H. Friend, L. A. DaSilva, and A. B. MacKenzie, "Cognitive networks," in Proceedings of IEEE DySPAN 2005, Nov. 2005, pp. 352-360

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

[12] A. Sahai, N. Hoven, and R. Tandra, “Some fundamental limits on cognitive radio,” in Allerton Conference on Communication, 2004, pp. 1-11

[13] D. Cabric, S. M. Mishra, and R. W. Brodersen, “Implementation issues in spectrum sensing for cognitive radios” in Proceedings of 38th Asilomar Conference on Signals, Systems and Computers 2004, Nov. 2004, pp. 772-776

[14] A. Fehske, J. D. Gaeddert, and J. H. Reed, “A new approach to signal classification using spectral correlation and neural networks,” in Proceedings of IEEE DySPAN 2005, Nov. 2005, pp. 144-150

[15] H. Tang, “Some physical layer issues of wide-band cognitive radio system,” in Proceedings of IEEE DySPAN 2005, Nov. 2005, pp. 151-159

[16] J. Zhu, Y. Zou, and B. Zheng, “Cooperative detection for primary user in cognitive radio networks,” EURASIP Journal on Wireless Communications and Networking 2009, Feb. 2010, pp. 1-12

[17] A. Ghasemi and E. S. Sousa, “Collaborative spectrum sensing for opportunistic access in fading environments,” in Proceedings of IEEE DySPAN 2005, Nov. 2005, pp. 131-136

[18] FCC, “ET Docket No. 03-237 Notice of inquiry and notice of proposed rulemaking,” Nov. 2003, ET Docket No. 03-237

[19] G. Ganesan and Y. G. Li, “Agility improvement through cooperative diversity in cognitive radio networks,” in Proceedings of GLOBECOM, Nov. 2005, pp. 2505-2509

[20] H. Urkowitz, “Energy detection of unknown deterministic signals,” Proceedings of IEEE, vol. 55, no. 4, pp. 523-531, Apr. 1967

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

[22] J. Lunden, V. Koivunen, A. Huttunen, and H. V. Poor, “Collaborative cyclostationary spectrum sensing for cognitive radio systems,” IEEE Transactions on Signal Processing, vol. 57, no. 11, pp. 4182-4195, Nov. 2009

[23] A. Wald, “Sequential Analysis”, John Wiley and Sons, New York, NY, 1947

[24] B. F. Lo, I. F. Akyilidz, and A. M. Al-Dhelaan, “Efficient recovery control channel design in cognitive radio ad hoc networks,” IEEE Transaction on Vehicular Technology, vol. 59, no. 9, pp. 4513-4526, Nov. 2010

[25] Y. Selen, H. Tullberg, and J. Kronander, “Sensor selection for cooperative spectrum sensing,” in 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, 14-17 Oct. 2008, pp. 1-11

[26] A. C. Malady and C. R. C. M. da Silva, “Clustering methods for distributed spectrum sensing in cognitive radio systems,” in MILCOM 2008 – IEEE Military Communications Conference, 16-19 Nov. 2008, pp. 1-5

[27] K. Yadav, S. D. Roy, and S. Kundu, “Total error reduction in presence of malicious user in a cognitive radio network,” in 2nd International Conference on Electronics, Materials Engineering and Nano-Technology (IEMENTech 2018), 2018, pp. 1-4

[28] A. A. Sharifi, M. Sharifi, and M. J. M. Niya, “Secure cooperative spectrum sensing under primary user emulation attack in cognitive radio networks: Attack-aware threshold selection approach,” AEU, International Journal on Electronics and Communications, 2016, vol. 70, no. 1, pp. 95-104, Jan. 2016

[29] T. Locher, R. Wattenhofer, and A. Zollinger, “Received-Signal-Strength-Based logical positioning resilient to signal fluctuation,” in 1st ACIS International Workshop on Self-Assembling Wireless Sensor Networks (SAWN), May 2005

[30] T. S. Rappaport, *Wireless communications: principles and practice*, Prentice Hall, 1996

[31] K. Yadav, S. D. Roy, and S. Kundu, “Enhanced throughput performance under primary user emulation attack in cognitive radio networks with spectrum prediction,” International Journal of Communication Systems, 2017, doi: 10.1002/dac.3371.

[32] K. Yadav, S. D. Roy, and S. Kundu, “Enhanced throughput performance under primary user emulation attack in cognitive radio networks by optimal threshold approach,” International Journal of Communication Systems, 201

[33] K. Shuaib, E. Barka, N. Al-Hussein, M. Abdel-Hafez, and M. Alahmad, “Cognitive radio for smart grid with security considerations”, MDPI Computers 2016, vol. 5 no. 7, Jan 2016, doi: 10.3390/computers5020007