Primary User Emulation Attacks in Cognitive Radio - An Experimental Demonstration and Analysis

A Thesis Presented for

The Master of Science

Degree

The University of Tennessee, Knoxville

Benjamin James Ealey

August 2011

© by Benjamin James Ealey, 2011
All Rights Reserved.

I would like to dedicate this paper to my family as without their constant encouragement and support, even when they stopped understanding what I was learning about, I would never have made it as far as I have today. Thanks guys!

Acknowledgments

I would like to thank Dr. Husheng Li for guiding my immersion into the world of cognitive radio and helping me through my final two years as a student.

I would also like to thank Rukun Mao for his constant support and for helping me with even the silliest of questions.

Last but not least, I would like to thank Dr. Paul Crilly for originally peaking my interests in communications and helping me decide where to direct my education after undergrad.

"Do not spoil what you have by desiring what you have not; remember that what you now have was once among the things you only hoped for." Epicurus

Abstract

Cognitive radio networks rely on the ability to avoid primary users, owners of the frequency, and prevent collisions for effective communication to take place. Additional malicious secondary users, jammers, may use a primary user emulation attacks to take advantage of the secondary user's ability to avoid primary users and cause excessive and unexpected disruptions to communications. Two jamming / anti-jamming methods are investigated on Ettus Labs USRP 2 radios. First, pseudo-random channel hopping schemes are implemented for jammers to seek-and-disrupt secondary users while secondary users apply similar schemes to avoid all primary user signatures. In the second method the jammer uses adversarial bandit algorithms to avoid channels already heavily disrupted from primary user communications and concentrate efforts on channels heavily populated by secondary user communications. In addition the secondary users apply similar methods to avoid channels heavily occupied by jammers and primary users. The performance of these users is compared with and without the algorithm through channel delay, impact of algorithm on probability density functions, and user collision rate. Conclusions on made on the effectiveness of each technique.

Contents

List of Tables ix

List of Figures x

1 Introduction 1

1.1 The Issues . . . 1

1.2 Some History . . . 1

1.3 Cognitive Radio Networks . . . 3

1.4 The Network . . . 5

1.4.1 Header Structure . . . 7

2 Passive Primary Emulation Attack Avoidance - An Unassertive Game of Cat and Mouse 9

2.1 Introduction . . . 9

2.2 Theory . . . 10

2.2.1 Channel Model . . . 10

2.2.2 Secondary User Model . . . 10

2.2.3 Attacker Model . . . 11

2.2.4 Zero-Sum Game Formulation . . . 11

2.3 Network Design and Implementation . . . 12

2.3.1 Hopping Schemes . . . 16

2.3.2 Secondary User Synchronization . . . 18

2.3.3 Physical Placement 18
2.4 Data and Analysis 20
2.5 Conclusions 22
2.6 Future Works 23

3 Blind Learning with Partial Information - An Intelligent Game of Cat and Mouse **25**
3.1 Introduction 25
3.2 Theory 27
3.3 Network Design and Implementation 30
3.3.1 General Network 30
3.3.2 Primary User Model 31
3.3.3 Secondary User Model 32
3.3.4 Attacker Model 33
3.3.5 Learning Resistivity 35
3.4 Data and Analysis 36
3.4.1 Primary User Testing 36
3.4.2 Secondary User Analysis 38
3.4.3 Jammer Analysis 43
3.5 Conclusions 48
3.6 Future Works 49

4 General Conclusions **51**

Bibliography **53**

Vita **56**

List of Tables

1.1 Experimental Characteristics for the Ettus Labs USRP 2 6

2.1 Experimental Results 20

List of Figures

1.1 Ettus Labs USRP 2 Without Cover 2
1.2 Ettus Labs USRP 2 Used in Investigation 5
1.3 Header Structure Used In The Investigation 7

2.1 USRP 2 Cognitive Radio Network - Final Lab Setup 11
2.2 Probability of User Occupancy per Channel 13
2.3 State Diagram for the Primary User 13
2.4 State Diagram for the Secondary User 15
2.5 State Diagram for the PUE Jammer 16
2.6 Probability Distributions of PU Hopping Schemes 17
2.7 Probability Distributions of SU and PUE Jammer Hopping Schemes . 18
2.8 Images of Radio Placement 19
2.9 Placement of Radios 19
2.10 Collisions at Various Hopping Schemes Used 21
2.11 Throughput Data for Uniform vs. Ordered Hopping Schemes 23

3.1 Reward Weight for Secondary Users Over Time 26
3.2 Reward Weight for Jammer Over Time 27
3.3 Initial Probability Density Functions 31
3.4 State Diagram for Primary User 32
3.5 Transmitter State Diagram 33
3.6 Jammer State Diagram 34

3.7 Primary User Probability Density Functions 37
3.8 Non-learning Jammer with Various Primary User PDFs 38
3.9 Learning Jammer with Various Primary User PDFs 39
3.10 Non-learning Transmitter with Various Primary User PDFs 40
3.11 Learning Transmitter with Various Primary User PDFs 41
3.12 Learning Secondary User - Collisions Per Interval 42
3.13 Learning Secondary User - Piecewise Rate of Collisions 43
3.14 PDF After Test for Intelligent Secondary User 44
3.15 Learning Jammer - Collisions Per Interval 45
3.16 Learning Jammer - Piecewise Rate of Collisions 46
3.17 PDF After Test for Intelligent Jammer 47
3.18 Idle Channel Statistics - Intelligent Secondary User at 100x Resistivity 48
3.19 Idle Channel Statistics - Intelligent Secondary User at 2x Resistivity . 49

Nomenclature

$1, ..., N$	Range of Operating Channels
I	Idle Channel
n	Channel Number
O	Occupied Channel - Primary User Signature
P_I^n	Initial Channel Probabilities of Channel n Being Idle
P_O^n	Initial Channel Probabilities of Channel n Being Occupied
R	Reward of User's Actions
W_r	Weight of Reward at a Specific Time
DBPSK	Differential Binary Phase-Shift Keying
PDF	Probability Density Function
PU	Primary User / Licensed User
PUE	Primary User Emulation Attack
Rv	Resistivity Value
SU	Secondary User / Unlicensed User

Chapter 1

Introduction

1.1 The Issues

The rapidly expanding trend of wireless devices has created a fear of exhausting the number of frequencies available in the usable spectrum which is causing more advanced networking, shorter bandwidth, and lower powered devices to be used. It is not uncommon for consumers to have upward of 10 or more wireless devices in a single household. This has caused a demand for more efficient usage of different frequency bands.

1.2 Some History

Software defined radios are radio communications systems where many of the parts, previously physical, are implemented using software which is run on a separate computer. The development of software defined radios has been very important for research as it allows users to define their own modulation, control amplification, change filters, and model other physical traits without the need for building physical circuits.

Joseph Mitola III and Gerald Q. Maguire, Jr. proposed using software radio as a platform for implementing cognitive radio in August of 1999, Mitola and Maguire



Figure 1.1: Ettus Labs USRP 2 Without Cover

(1999). The idea they proposed as cognitive radio is a radio system where various stimuli and cues are given to the device which allows it to act in specific ways and fully understand its surroundings. Mitola and Magurie proposed that a system using cognitive radio could identify where it is and what it is doing by its surroundings. Examples of this include identifying that it is indoors because of the RF and LAN activity around it or perhaps the inability to connect with exterior towers. It could also use recent activity such as the purchase of a train ticket to identify that a train ride may be in its future.

In November 2008, the FCC ruled to permit previously unlicensed users to operate on licensed bands, given they avoid the users licensed to use that band, Commission (2008). The previous rules stated that only users licensed to use a specific spectrum were allowed to operate on this frequency. This caused cellular network bands to operate under a very heavy load where other bands such as amateur radio, military, and paging frequencies were not fully utilized. Cognitive radio proved to be a good way to take advantage of the FCC's ruling. Mitola and Maguire wanted to apply

the cognitive ability of a radio to allow it to make many varied decisions without any help from the user. Simon Haykin proposed a system where cognitive radios were used to avoid licensed users when operating in bands unlicensed to the current user. Haykin includes three cognitive tasks which are performed by the radio. This includes an analysis of the whole radio-scene, the state of the current channel as well as future modeling of the channel, and finally spectrum management and controlling the power of transmission. This has been coined spectrum sensing cognitive radio as opposed to the original proposal from Mitola and Maguire of full cognitive radio or Mitola radio where environmental aspects outside of spectrum analysis are taken into consideration by the radio. Full cognitive radio networks require sensors and other detection devices in addition to anything required for general operation.

1.3 Cognitive Radio Networks

Spectrum sensing cognitive radios consist of a variety of users which behave in different ways depending on the environment. The overall goal is for users who are not licensed on their current channel to avoid all licensed users and prevent any interference to them. The licensed users are called Primary Users (PU) because they have primary rights to the channel. Their location is typically known to other users and their transmission characteristics are identifiable but not always the same between primary users due to different applications. These users include but aren't limited to military radios on the military band and emergency help request transmissions on the emergency bands. According to the new FCC rules, the primary users are expected to never receive any interference from unlicensed users.

Unlicensed users fall into the category of Secondary Users (SU) since their transmissions are secondary in priority regarding the completion of the transmission. These users may operate on any frequency range which they are permitted by the FCC's new rules. They are expected to scatter and halt transmission immediately upon a PU's appearance as a PU must not experience any interference. These users

could be almost anything. A SU can use various tactics to avoid primary users but all of them require an immediate halt to transmissions. If the primary user's behavior makes any further transmissions on that channel impossible, SUs can either change frequencies and transmit on other channels to avoid the primary user or they can re-route the transmission to another SU node in the network outside of the PU's range. A mixture of both of these may be applied depending on the characteristics of the network. In this investigation node hopping will not be used so the effectiveness will depend on channel hopping.

Where there are benevolent transmissions there are always others trying to disrupt them and make it difficult continued communication. These users are jammers or malicious secondary users. They may use an assortment of jamming techniques. In Brown and Sethi (2007) the threat of denial of service attacks through the use of false primary user signals, false users, and traditional jamming is investigated. Others such as Sampath et al. (2007) investigate using cognitive radio's ability to switch channels rapidly to jam legacy wireless networks as well as other cognitive radio networks. In Peng et al. (2009) identification and avoidance of primary user emulation attacks is investigated. Peng et al. (2011) investigates the impact of a balanced approach consisting of traditional jamming and a primary user emulation attack. A stochastic zero-sum (Markovian) game model regarding primary user emulation attacks is performed in Zhu et al. (2010). Li and Han (2010b) and Chen et al. (2008) also investigate cognitive radio primary user emulation attacks. This will be the focus of this investigation. A primary user emulation attack occurs when a malicious secondary user, a jammer, imitates a primary user to cause other secondary users to flee from the channel. This type of attack can be used to cause interruptions to secondary user networks or for selfish use of spectrum. However the jammer executes its malicious intent, mitigation of these obstacles are the only way to ensure proper transmissions.

1.4 The Network

The network used in this investigation will consist of four total users. There is one primary user, two secondary users, and one jammer. Ettus Labs USRP II radios were used due to their availability and ease of operation. The network was designed to maximize the ability to switch hopping patterns and allow the use of random channel hopping patterns. This network will form the testbed for each of the tests performed in this investigation.



Figure 1.2: Ettus Labs USRP 2 Used in Investigation

The network was designed using the RFX2400 daughter board which operates on a frequency range of 2.4 to 2.47 gigahertz. The computers were all Dell Optiplex 580s with 2.8 gigahertz processors, has 2 gigabytes of RAM, and runs Ubuntu Lucid Lynx (10.04) as the operating system. The same computers were used throughout the entire investigation.

The communication parameters were set to a bit rate of 100kps using a modulation of differential binary phase-shift keying (DBPSK). These were the original defaults on the radio. The gain and amplitude were left at a default value of "midpoint" and 0.25 respectfully. It is assumed that all of the radios are within transmission range of each other so the gain and amplitude were left high to ensure this happened. Each test comprised of a series of transmissions with an average delay of 2.35 to 2.63ms

Table 1.1: Experimental Characteristics for the Ettus Labs USRP 2

Radio	
Radio Platform	*Ettus Labs USRP 2*
Daughter-Board	*RFX2400*
Channel Frequency	*2.4 - 2.47 Ghz*
Computer Comm.	*Ethernet - CAT 5*
Computer	
Computer	*Dell Optiplex 580*
Processor	*AMD X2 240 - 2.8 Ghz*
RAM	*2 Gigabytes*
Operating System	*Ubuntu Lucid Lynx - 10.04*
Communications / USRP Settings	
Bit Rate	*100kps*
Modulation	*DBPSK*
Gain	*Midpoint*
Amplitude	*0.25*
Average Delay	*2.35-2.63 ms*
Packets Per Test	*1999*

from transmission to response. The various transmission lengths were optimized to give good averages while showing data trends in a timely manner.

Though the daughter board allowed transmissions past 2.47 Ghz the frequency range for this investigation was conducted between 2.4 and 2.47 Ghz. Frequencies above 2.47 Ghz causes erroneous data and performed differently. Due to a hardware constraint each user could only listen or transmit on each channel but not both simultaneously.

The hopping schemes were pseudo-random for secondary users and random for jammers and primary users which provided an environment where the pseudo-random string would not cause issues since the other two users were random. Psuedo-random strings had to be used to maintain synchronization between users. The jammer and primary users also ran continuously across all testing so even similar seeds would not impact results.

1.4.1 Header Structure

The header structure for each packet is very important in this investigation as it allows each user to operate properly during the test. Not all sections of the headers are directly used by the radios. Some of the data transmitted is solely used by the primary investigator for debugging and for ensuring quality data is collected.

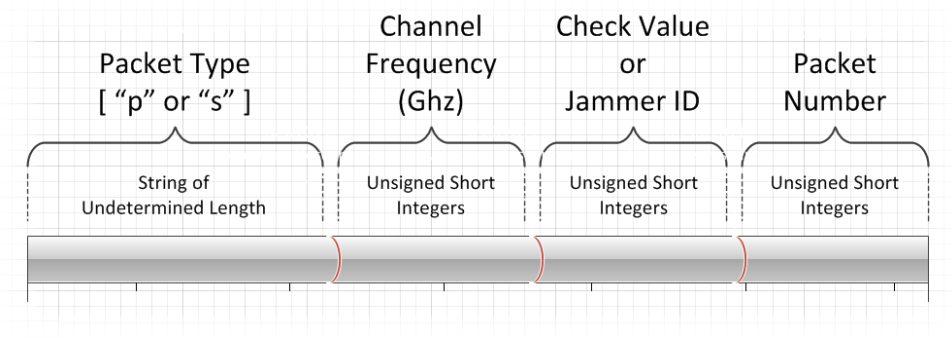


Figure 1.3: Header Structure Used In The Investigation

The structure consisted of a string of undetermined length and four unsigned short integers with a packed length of two bytes each.

The first provided the users with the type of packet being sent. Two user types were defined in the code, ”p” for a primary user and ”s” for a secondary user. A packet labeled ”p” caused each user to behave as instructed in the presence of a primary user and ”s” for secondary users.

The next part of the header was the normalized channel frequency. This was the current channel the user was on. Due to overlapping frequencies and the small area for testing the users were instructed to only accept packets from users on the same channel. The normalized value was used since 2,400,000,000 Hertz was too large to fit into the short integer type. The number 240 would be sent instead and then converted to the proper value once received.

The following slot held different values depending on the user. Secondary users stored data regarding the current pdf to ensure that proper communications were performed between the two secondary users. The jammer used this slot to differentiate

itself from the primary user solely for the principal investigator's benefit. This was used during the testing phases and was ignored during data collection.

The final slot contains a packet number. Every user transmitted the count of the current packet to prevent a user detecting a packet twice. This also helped identify each transmission for data analysis and allowed the secondary users to maintain synchronization.

Chapter 2

Passive Primary Emulation Attack Avoidance - An Unassertive Game of Cat and Mouse

2.1 Introduction

Cognitive radios must be well adapted to detect the presence of licensed users and avoid them at all cost. As mentioned in Chapter I, there exist many proposed techniques for avoiding primary users but in Zhu et al. (2010) it is proposed that primary and secondary users exist within a zero-sum game where both secondary users and primary users reach a beneficial stalemate. This occurs when following two random schemes where it is equally probable for each user to appear on a specific channel. In this chapter this passive game of cat and mouse is investigated and an analysis is made. Previous work on this subject has been mainly computational analysis, Chen et al. (2008), so the experimental results should lead to some beneficial conclusions. It is predicted that there will be an observed point where both users may ignore the tactics of the other as changing tactics will not benefit the user.

2.2 Theory

This section contains the theory behind the physical system model designed. The system was designed around a model proposed in Zhu et al. (2010) and Li and Han (2010b). It is proposed that the jammer and secondary user will satisfy the requirements of a zero-sum game.

2.2.1 Channel Model

We assume that there are totally N channels. Each channel can be simulated using a two-state Markov Chain where the states are idle (I) and occupied (O). In the occupied state the primary user or jammer is operating on the channel and the secondary user is unable to transmit. In the idle state the channel is free of primary users and jammers and the secondary user is free to transmit. The transition probability can be determined from the probability matrix :

$$Q_n = \begin{pmatrix} 1 - P_{IO}^n & P_{OI}^n \\ P_{IO}^n & 1 - P_{IO}^n \end{pmatrix}$$

where P_{IO}^n (P_{OI}^n) means the transition probability from idle to occupied (occupied to idle). p_{nI} and p_{n0} are the initial probabilities of channel n being idle.

The actual channels are assumed to possess the same characteristics to simplify calculations. This allows the results to reflect purely on the occupation of the channels and not the performance statistics of each channel, though it cannot be completely controlled in a real life scenario.

2.2.2 Secondary User Model

At the beginning of each time slot secondary users sense to see if the channel is occupied. If it is occupied by a primary user or jammer, it switches to the next unused channel. This exploitation of open channels allows users to take advantage of

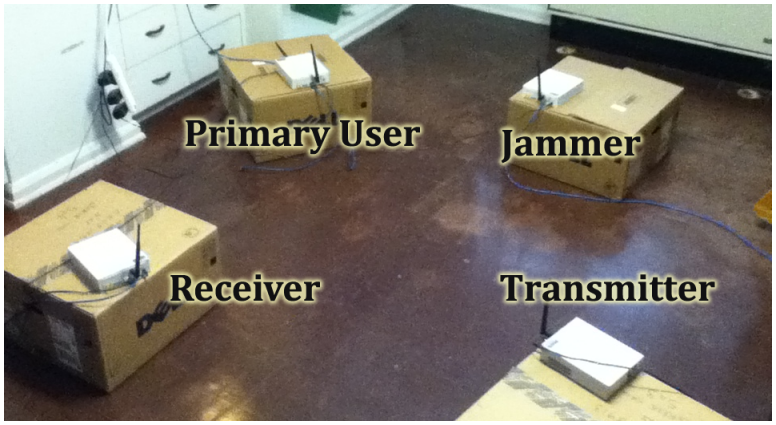


Figure 2.1: USRP 2 Cognitive Radio Network - Final Lab Setup

all unused channels. This pattern is used before every transmission at the start of the time slot. Mathematically, it is assumed that all secondary users have perfect sensing. For simplicity, we assume that the secondary user can access only one channel at a time.

2.2.3 Attacker Model

In this case, cognitive radio attackers use an attack called Primary User Emulation where attackers copy the traits of a primary user to cause faulty busy states on available channels. For simplicity, we assume that the PUE attack can jam only one channel at a time.

2.2.4 Zero-Sum Game Formulation

We model the game between the PUE attacker and the secondary user as a zero-sum game. The elements of the game are given below:

- Strategy: The strategies of the attacker and the secondary user are the channels to jam/access, respectively. We assume that mixed strategies are used, i.e., the players choose channels in a random manner. We denote by $\{u_i\}_{i=1,\ldots,N}$ and $\{v_i\}_{i=1,\ldots,N}$ the probabilities of accessing and jamming, respectively.

- Reward: The reward of the defender, R_2, equals to p_{iI} when it senses channel i and the PUE attacker is jamming another channel; otherwise, the reward is 0. Due to the assumption of zero-sum game, the reward of the attacker R_1 is equal to $-R_2$.

The following proposition shows the mixed strategy at the Nash equilibrium, whose proof is omitted.

Proposition 1. *Define K as*

$$K = \max\left\{k \middle| \frac{\frac{k-1}{p_{N-k+1,I}}}{\sum_{j=N-k+1}^{N} \frac{1}{p_{jI}}} < 1\right\}. \tag{2.1}$$

Then, there is a unique Nash equilibrium point in the game, which is given by

$$u_i = \begin{cases} \frac{\frac{1}{p_{iI}}}{\sum_{j=N-K+1}^{N} \frac{1}{p_{jI}}}, & i = N-K+1, ..., N, \\ 0, & i = 1, ..., N-K \end{cases}, \tag{2.2}$$

and

$$v_i = \begin{cases} 1 - \frac{\frac{K-1}{p_{iI}}}{\sum_{j=N-K+1}^{N} \frac{1}{p_{jI}}}, & i = N-K+1, ..., N \\ 0, & i = 1, ..., N-K \end{cases}. \tag{2.3}$$

2.3 Network Design and Implementation

The investigation consists of four primary components. There is a primary user, a secondary user transmitter, a secondary user receiver, and a PUE jammer. The users operate on a different sets of hopping schemes. Each of these can be seen in Figure 2.2 and further explanation is discussed in 2.3.1. Each is designed to comply with the requirements of the network and to properly simulate a realistic user.

The primary user is the basis of the network. All other users work around the presence of this user. It operates on a known frequency range and its transmissions

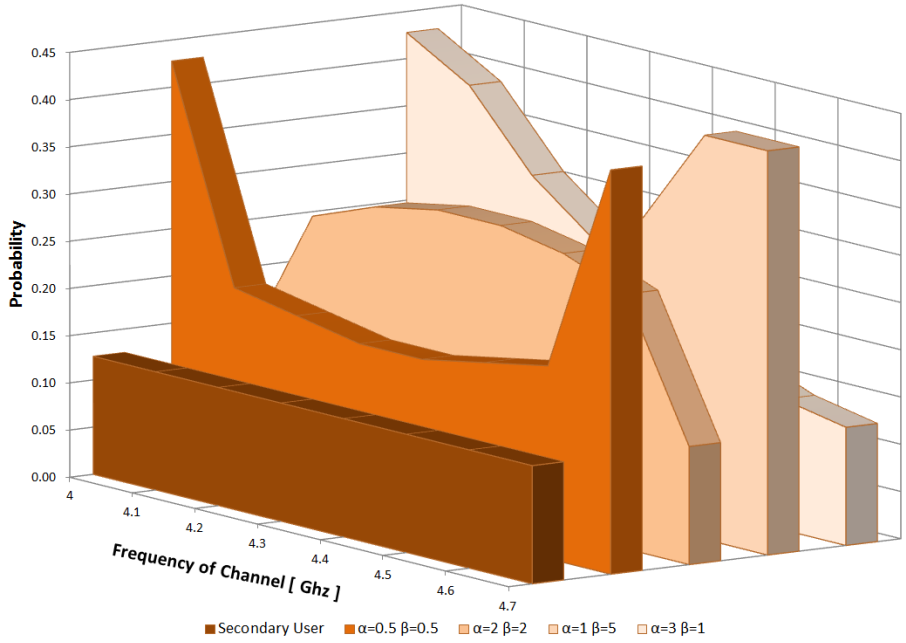


Figure 2.2: Probability of User Occupancy per Channel

are assumed to be received by all users in the network. It is simulated using a series of beta distributions as they can properly model a user who primarily operates on specific frequencies. This user transmits each packet then waits for a random period of time, t. This simulates the uncertainty of when a primary user is going to emerge. This user is only able to transmit on one channel at a time.

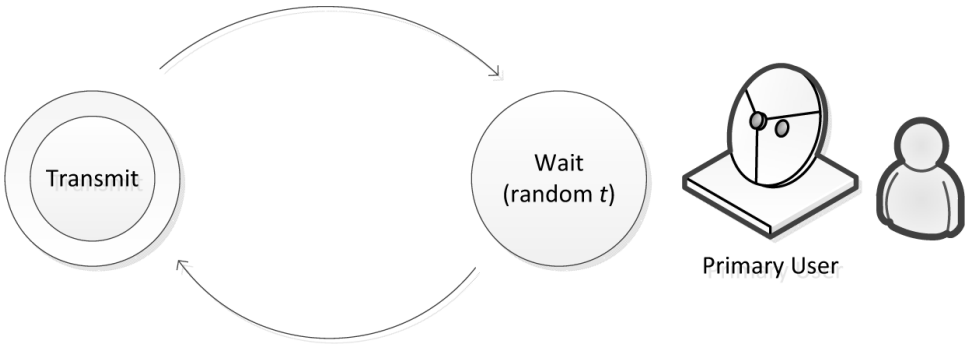


Figure 2.3: State Diagram for the Primary User

Though the primary user operates using the same specifications as shown in Table 1.1, not all transmissions are always detectable because of interference and users

operating in the wrong state for detecting transmissions. To fix this an assumption was made that all transmissions were detectable. This was enforced by allowing all users to transmit three times in quick succession so other users can fully detect its presence. The packet number was used as a way to prevent users from improperly reading duplicate transmissions as new. The topic of this paper was not to create an ideal detection technique so this assumption was fitting. Each user detects what type of user the packet originated from using the full contents of the header. If a bad packet is received because of a current transmission or environmental interference, detection will not occur and the two secondary users can become unsynchronized. This would invalidate the rest of the data.

The secondary user receiver and transmitter both work on the exact same pseudo-random channel hopping scheme. The two hopping schemes include an ordered (1,2,3...n) scheme and a uniformly distributed scheme. More about the hopping scheme will be discussed in the Section 2.3.1.

This user must be very attentive and always detect when a primary user transmission signature appears. When a primary user or jammer appears both secondary users hop to the next channel in the synchronized hopping scheme. Both users transmit and receive but the transmitter is known as the user who initiates the transmission. In addition, the receiver will wait for the transmitter as the receiver transmits only when a packet from the transmitter arrives and rarely misses a primary user or jammer.

The secondary users follow a pattern of transmit, receive, transmit acknowledgment, and repeat. The transmitter initiates this process and will time out and rule a packet as lost if the acknowledgment is not received in time. In this scenario, if either user does not properly detect a primary user or jammer then the users will become disconnected and may not regain contact. There were two attempts to correct this if it arises. The first is that each primary user and jammer transmit a trio of packets in quick succession to help both secondary users detect them. The receiver is also programmed to wait for the transmitter if not detected to minimize the distance

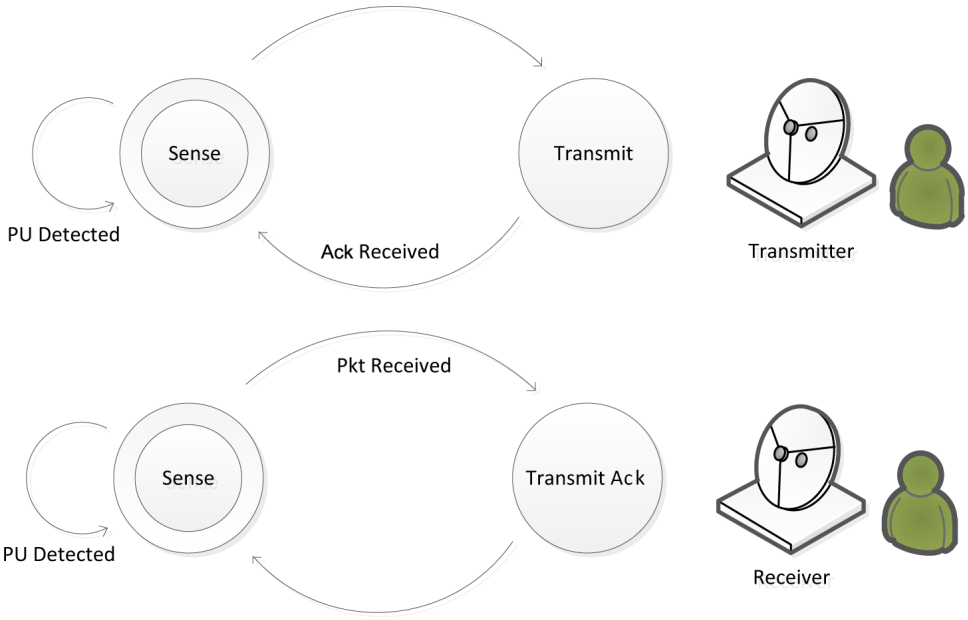


Figure 2.4: State Diagram for the Secondary User

between them. The transmitter tends to miss packets more often since it is initiating the transmission process and users are unable to receive while transmitting.

The jammer is the third user in the network and it transmits on the two hopping schemes with the same distribution, ordered (1,2,3...n) and uniformly distributed, as the secondary users but not the exact same sequence. This user's primary focus is to disrupt the secondary user's transmissions by making contact with it as many times as possible. Each time the jammer does this it forces the secondary users to change channels as they cannot differentiate it from a primary user. This increases the chances that packets will be corrupted or disrupted entirely.

Since the jammer is alone and is a selfish user, it follows the design of the primary user very closely. The only difference is that the jammer will halt transmissions at the sign of the primary user so as not to be detected by it. This action does not change the actions of a secondary user operating on this channel since differentiation is impossible. The secondary users will change channel whether it is a PU or a jammer. The jammer also hops at a consistently spaced interval of just under a

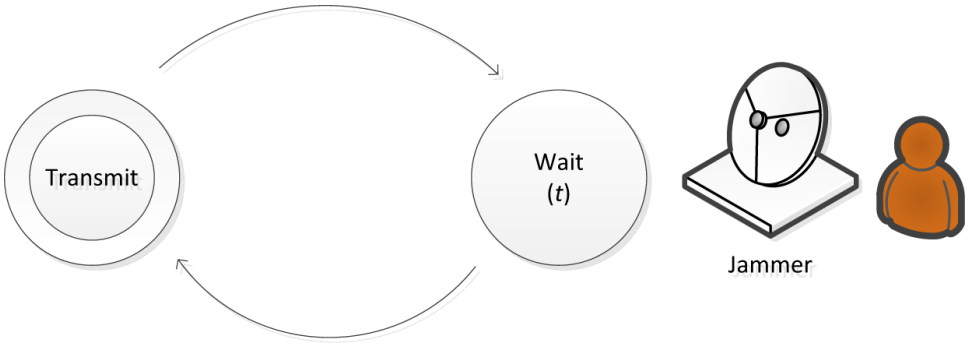


Figure 2.5: State Diagram for the PUE Jammer

second as opposed to the randomly determined rate used by a primary user. The jammer is expected to maximize disruptions so rapid transmissions are used.

2.3.1 Hopping Schemes

In this investigation we determine the effectiveness of the jamming/anti-jamming technique by the number of collisions that occur during each test. The number of collisions demonstrate the effectiveness of each method.

The primary user performs hops governed by a set of beta distributions to model the nature of a primary user. A primary user typically has a known set of frequencies it transmits over. The strength of the transmission may also be estimated since transmissions locations are typically established stations. This was modeled with four beta distribution curves which can be seen in Figure 2.6. Distributions were chosen so a concentration on either size of the spectrum were utilized as well as a concentration in the middle of the spectrum and the two extremes. These distributions were used so that the primary user was able to appear at any channel in the spectrum but was much less probable on certain channels.

The secondary user and jammer use the same distributions and the probability of a user landing on each channel is equal to any other channel in the spectrum. Two schemes were selected as both provide a uniform distribution under the applied conditions. Also, secondary users will use their full potential bandwidth to take

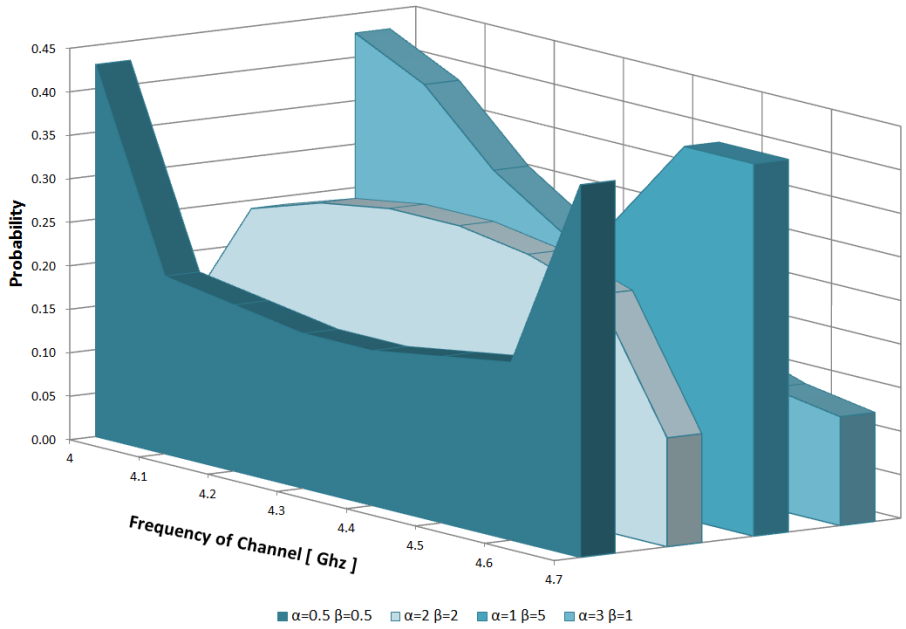


Figure 2.6: Probability Distributions of PU Hopping Schemes

advantage of their frequency hopping cognitive radio ability. The jammer will do the same in order to maximize productiveness. Similarly to a game of hide and seek, if one player is allowed to leave the boundaries then no one will be able to find them without also leaving the boundaries.

The first is an uniformly distributed hopping scheme. This PDF satisfies the requirement that all channels must be equally probable. The pseudo-random string differs between jammer and secondary users but the probability for either user to appear at a specific channel within the spectrum under test is equally probable. The second scheme used was an ordered hopping scheme which consists of each channel in order from least to greatest. This was chosen since, though it isn't random, it will give an equally distributed appearance across all channels within the spectrum since all users are unaware of the state of the other users. The ordered behavior of the user will appear to possess a uniform distribution because the previous state will remain unknown. The two distributions can be seen in Figure 2.7.

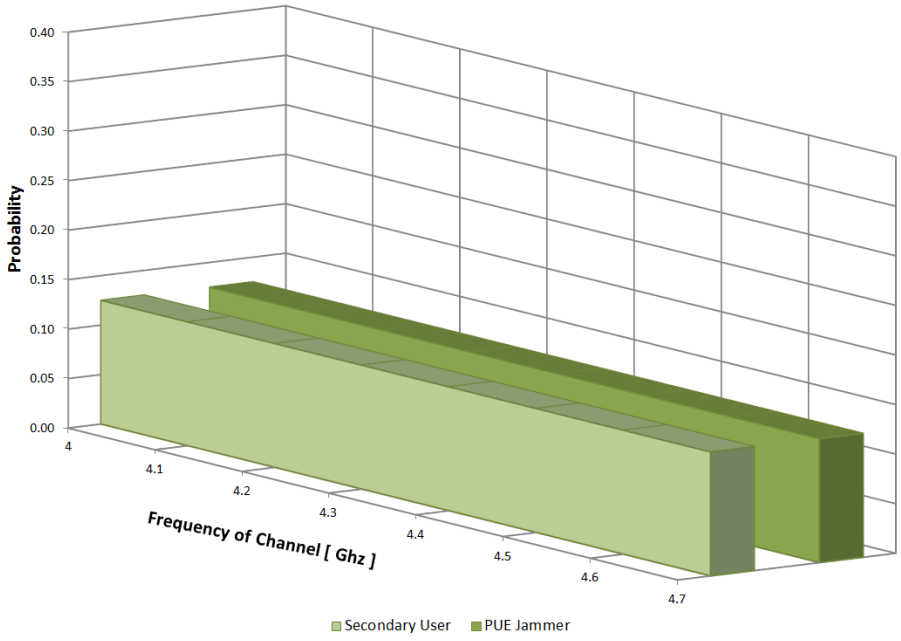


Figure 2.7: Probability Distributions of SU and PUE Jammer Hopping Schemes

2.3.2 Secondary User Synchronization

The development of cognitive radio networks presents a long standing issue in communications known as synchronization. Since the two secondary users, transmitter and receiver, had to operate simultaneously and act as one without confirming actions with each other, they had to maintain a list of the next group of channels to hop. This was implemented by hard coding pseudo-random sequences into each user and ensuring that both users detected primary users. Also, users were programmed to know when the other had fallen behind and to wait for them to catch up. Though this could cause extended downtime it prevented users from getting so separated the test became a total loss.

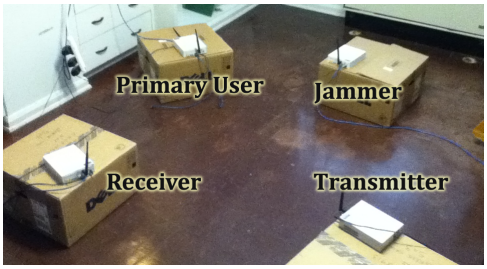
2.3.3 Physical Placement

During some of the preliminary testing it became apparent that the physical layout of the radios were important. Phenomena such as multi-path was impacting the radios

as they were positioned close to concrete walls and put in compact spaces. Severe network degradation was observed at these locations. The original positioning can be seen in Figure 2.8 and Figure 2.9.



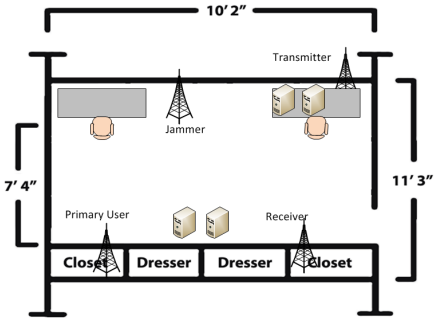
(a) Example Location of Erroneous Placement of Radios



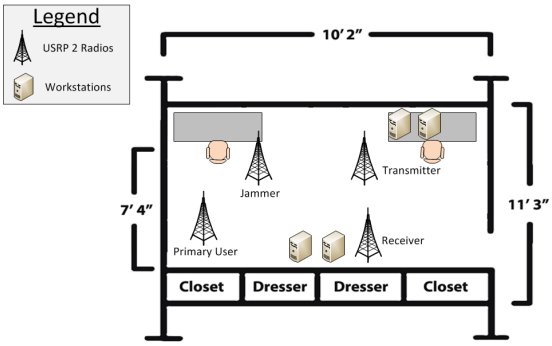
(b) Final Placement of Radios on Stands

Figure 2.8: Images of Radio Placement

The final layout pulled the radios away from the wall and lifted them off of the ground with electromagnetically permeable objects. Cardboard stands were used so that all radios were equidistant from the floor to prevent reflection off of the stand surface. They were positioned so that they were separated equally to minimize environmental influences, i.e. transmission power impacting transmissions. The original and final layout can be seen in Figure 2.9



(a) Original Erroneous Placement of Radios in Room



(b) Final Placement of Radios in Room

Figure 2.9: Placement of Radios

2.4 Data and Analysis

The investigation's primary objective is to make a comparison of the effectiveness of the proposed user behaviors on a cognitive radio network. Ideally, the jammer will maximize collisions with the secondary user while the secondary user strives for the opposite. A comparison is made of the number of collisions during each set of tests.

Table 2.1: Experimental Results

Users			**Avg. Statistics** [1]	
Beta Dist.	**Jammer Distribution**	**Secondary User Distribution**	**Percent Correct**$_2$	**Num. of Collisions**$_2$
α=0.5, β=0.5	Ordered	Ordered	*86.84*	*68.67*
		Uniform	*84.64*	*21.67*
	Uniform	Ordered	*89.38*	*12.33*
		Uniform	*85.50*	*20.67*
α=1, β=5	Ordered	Ordered	*89.24*	*69.33*
		Uniform	*92.72*	*20.67*
	Uniform	Ordered	*95.32*	*18.00*
		Uniform	*97.13*	*17.00*
α=3, β=1	Ordered	Ordered	*95.92*	*70.33*
		Uniform	*91.92*	*25.67*
	Uniform	Ordered	*95.32*	*13.67*
		Uniform	*92.58*	*20.33*
α=2, β=2	Ordered	Ordered	*88.71*	*71.00*
		Uniform	*91.38*	*24.33*
	Uniform	Ordered	*95.52*	*20.33*
		Uniform	*95.66*	*12.33*

[1] Values shown are an average of three trials with five hundred transmissions each.
[1] All collision and accuracy data was measured from the transmitter.

It was expected that a zero-sum case would exist and the data found in Table 2.1 agrees with this. It shows that it is more beneficial for a jammer using an ordered set. Every case where the jammer used an ordered set the number of collisions were higher than when a uniform distribution was used. A similar observation can be made for the secondary user. It is observed that every time a uniform distribution was used the secondary user benefited. It does need to be noted that every time a collision occurs, it is not primarily a jammer's action which caused it. The primary user and jammer

both trigger the same response to secondary users so technically the probability of a channel being occupied is the combined probability of the primary user and jammer.

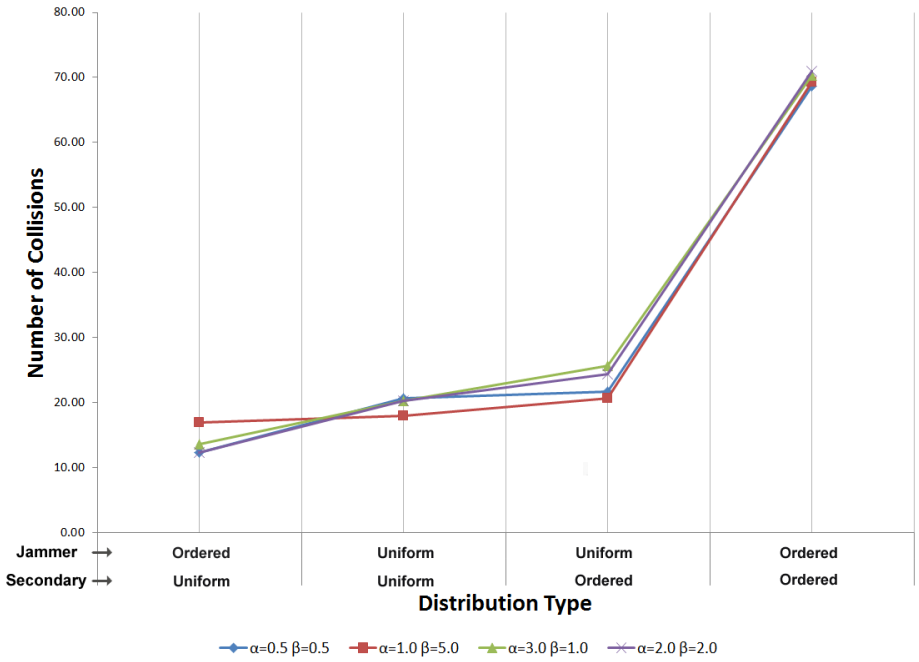


Figure 2.10: Collisions at Various Hopping Schemes Used

When the data is displayed graphically this becomes quite obvious. In figure 2.10 it is very easy to see the trend. Each PU setting shows similar results. When both users apply ordered distributions the jammer heavily benefits. The throughput values in Figure 2.11 agree with this. Though the throughput data does not depend purely on collisions but also on environmental influences it does show a general decrease. All throughput values were very high due to concise packet design and the simplicity of the network. The throughput data will not be collected in the second half of this investigation.

When a threat of jamming is present the best way for a user to avoid interference is avoid the jammer entirely. If the jammer cannot find the transmission then there is no way it can inflict any of the malicious tools it may possess. The greater the number of collisions with a user the greater the chance the jammer can maliciously influence the network. Thus the jammer wants to maximize the number of times it comes into

contact with the secondary users in the network. The data shows that these two users have mutually exclusive optimal choices which is theoretically predicted in Section 2.2.

The throughput of the system is fairly high in all cases and is hard to analyze due to the small change between them. The high throughput values may have resulted from the short length of the packets used in the test. In a real-life application much longer packets may be used and would be more prone to interruption. Shorter packets were sent to help the detection process as it was of primary importance in this investigation.

As previously discussed in Section 2.3, when secondary users become uncoupled and end up on different channels massive packet loss could occur and eventually would invalidate the data. This occurs because they may never couple again. This was one obstacle that had to be overcome in order to properly collect data. The safeguards put into place, as discussed in Section 2.3, prevented infinite decoupling from occurring. If decoupling occurs then the radios would catch up within a few packet transmissions. This may be partially the reason for the throughput data not always agreeing with the collision data.

It is interesting that there is a difference between the number of collisions for each hopping scheme since both are uniformly distributed. This must be since the ordered set is not a true uniform distribution since the next state depends on the current state. This would show that the random hopping was less efficient at finding users. If the ordered set produced more collisions, then the average time between each collision was greater with the uniform distribution than the ordered, sweeping set.

2.5 Conclusions

It was demonstrated in this investigation that there is indeed a zero sum game in regards to passive jamming and anti-jamming. This passive but intelligently designed hopping scheme shows that a baseline could be formed from these results to assist

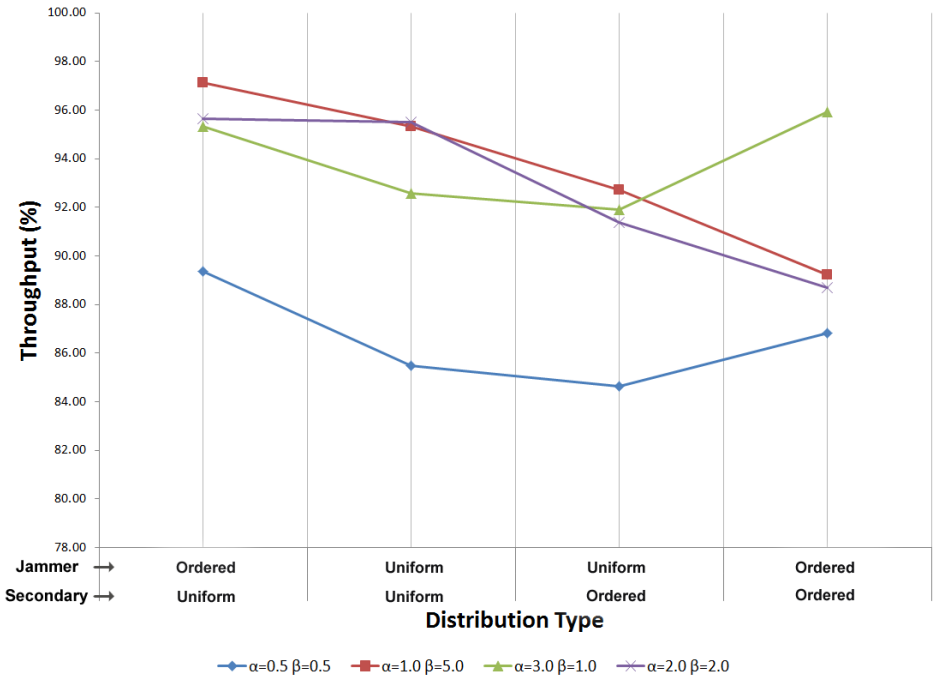


Figure 2.11: Throughput Data for Uniform vs. Ordered Hopping Schemes

intelligent systems. Higher level mechanisms require processing power as well as time for users to make decisions and execute them.

Though either user may know the hopping pattern of the opponent, the emergence of a zero-sum game allows users to pick one technique to achieve the best results. In this investigation the best choice for the secondary user was to randomly hop from channel to channel following a uniform distribution. The jammer performed best with a ordered set (1,2,3...n). The key to the zero-sum game is that the benefits of either action is mutually exclusive of the choices of the other. This provides a good baseline for passive avoidance.

2.6 Future Works

This investigation has quite a few assumptions. One such assumption was that the network was a single stage case. When more users are presented new discoveries could be made. It becomes more difficult when multiple users, possibly outside of the range

of a primary user, must remain on the same channel without being able to transmit to each other to say which channel they will reside.

In addition, secondary users avoided primary user transmissions by hopping to a different channel. In a multistage case the possibility of maintaining the same channel but transmitting around the primary user's reach is a possibility. This would add an additional level of complexity to the network since users would have to decide between re-routing or avoiding the users.

Chapter 3

Blind Learning with Partial Information - An Intelligent Game of Cat and Mouse

3.1 Introduction

Passive avoidance techniques may be beneficial in circumstances where all users are operating with limited computing power but most applications apply more intelligent algorithms. In radios that includes deciding how much power to transmit with, which channels are more likely to suit the user's needs, and determining if threats exist on each channel. In the jamming or anti-jamming case a user would most likely want to find a way to seek or avoid other users to satisfy it's purpose.

Intelligent selection of channels is very useful for jamming and anti-jamming as it allows users to pursue or avoid others by rewarding channels properly then evaluating the rewards every time a choice must be made. In addition, the target may not always be operating on the same bandwidth as the intelligent user. If both users are not operating on the same bandwidth then power would be wasted for a jammer

operating outside of the bandwidth used by the target. A secondary user could easily avoid a malicious user by moving to a channel where a jammer does not operate.

Work has been done in intelligent learning for cognitive radio networks. In Rieser et al. (2004) genetic algorithms are discussed. Mhnen et al. (2006) investigates a proposed cognitive radio resource manager which allows optimization of the communication stacks. Hedge algorithm based mirror descent schemes are discussed in Baes and Buergisser (2010). An early application of machine learning is discussed in Clancy et al. (2007). A balance of reasoning and learning is applied to provide beneficial results. In Li and Han (2010a), a multi-armed bandit was applied and forms a "dogfight in spectrum". The second part of this paper, Li and Han (2011), proposes a hedge algorithm based learning that follows three schemes, uniformly random, selectively random, and a maximum interception attack. Each of these is a different intensity of learning with uniform being no learning and maximum interception being purely learning. In this investigation this algorithm will be modified and is experimentally tested.

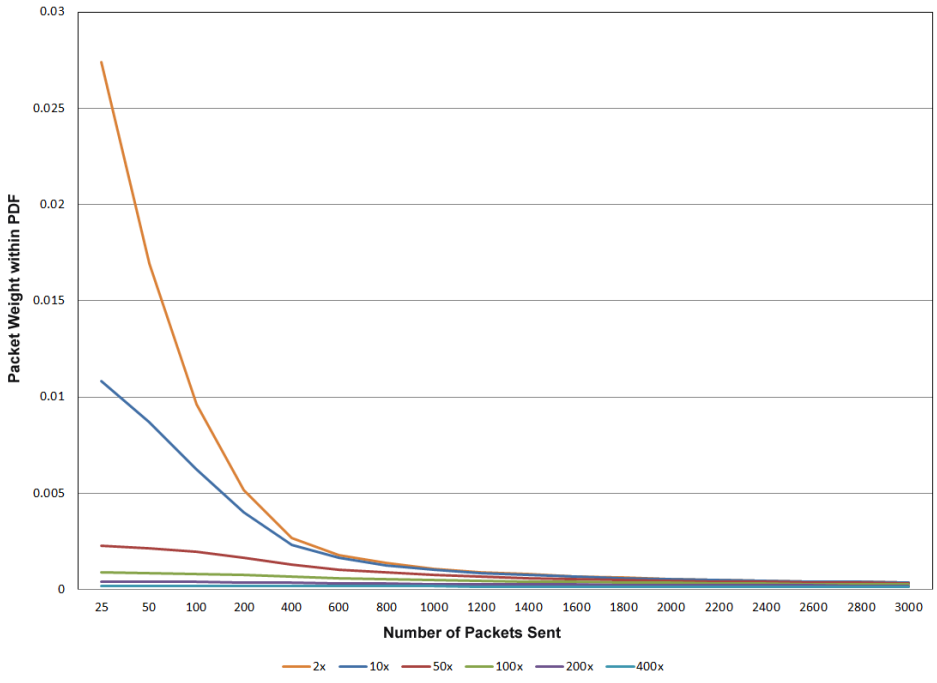


Figure 3.1: Reward Weight for Secondary Users Over Time

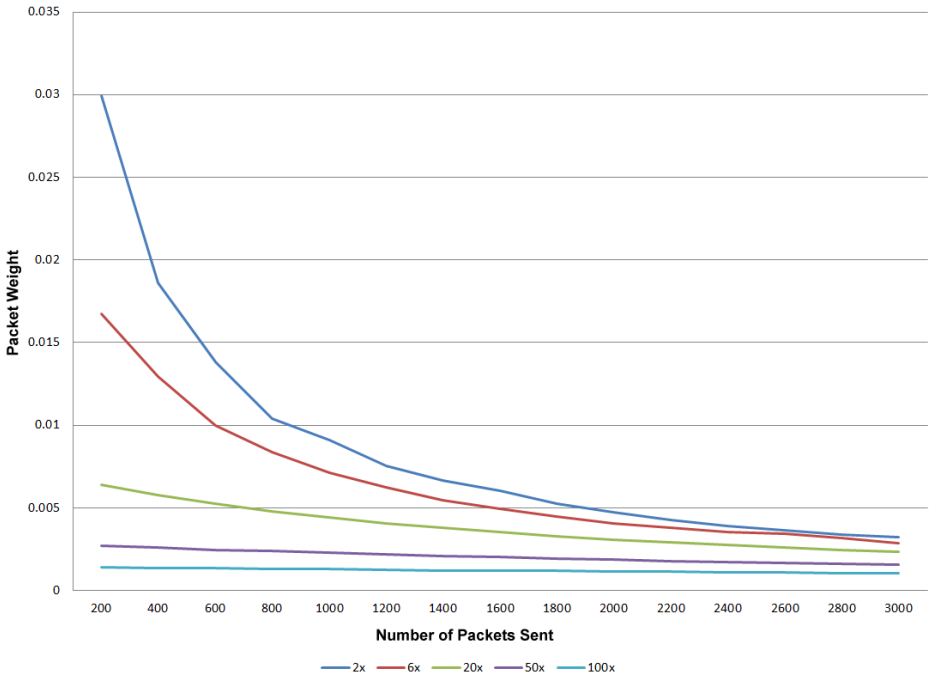


Figure 3.2: Reward Weight for Jammer Over Time

In this part of this paper a Hedge Algorithm is applied to the channel selection algorithm from Chapter 1. The initial impacts of this algorithm are tested with the understanding that long term execution will result in a steady-state sort of outcome where further learning will become more difficult, though not impossible, as the user becomes set in its ways. This effect can be seen in Figure 3.2 and Figure 3.1.

3.2 Theory

In Hedge based learning, expert feedback is given to a user every time an action is about to be performed. If the action is performed correctly it receives a positive reward and all the incorrect suggestions receive a negative reward. A simple explanation would be asking a number of students when the next pop quiz will be in a course. Every student gives their expert advice. The students who correctly guess the date earn trust while the others lose trust on their expertise regarding when pop quizzes occur. Each time this is performed students will receive or lose a reward value,

trust in this case, and will help define the which students are better at predicting the next quiz.

This basic concept is to be applied to cognitive radio. Every time a secondary user or jammer experiences a favorable reaction on a channel the user will reward this channel. Since the users can only detect what occurs on one channel at a time, they cannot give or remove rewards from other channels so no negative rewards can be given. This difference causes the algorithm applied in this investigation to differ from the Hedge Algorithm.

Every time a reward is given all future rewards have their value reduced. The impact of this is expected to allow future learning to perform smaller changes. This rough versus fine balance allows users on a cognitive radio network to adapt their own PDF to the target's PDF.

The general procedure for the learning algorithm is as follows:

Algorithm 1 Procedure of Learning Algorithm Applied by Users

```
1: Initialize all strings for selected probability.
2: Apply resistivity factor by appending probability string N times.
3: for each time slot t do do
4:    RandomlyChooseChannel
5:    if Secondary User then
6:       while channel is idle do
7:          Communicate
8:          ReceiveReward
9:       end while
10:   end if
11:   if PUE Jammer then
12:      while channel is occupied by secondary user do
13:         Communicate
14:         ReceiveReward
15:      end while
16:   end if
17: end for
```

As seen above, rewards are only given to jammers if a collision between a jammer and secondary user occurs. They are give to a secondary user if a transmission is

completed on a channel without primary user interruption. Each of these choices promotes the core purpose of the user. This mimics a Hedge Algorithm as each channel serves a provider of expert advice, the probability assigned to the channel. Channels that provide better rewards, collisions or a lack of, have their probability increased which decreases the probability of the other channels since they lie within the same PDF.

The rewards must also be attenuated so an operator can adjust the speed at which the algorithm learns and how quickly it moves from coarse to fine adjustments. This value has been coined the resistivity value as an increasing resistivity value increases the original PDF's resistance to the learning algorithm. Higher resistivity values will allow less learning than lower values.

Each reward is defined as $r(t) = 1$ where the sum of all rewards is $\sum_{\tau=0}^{\infty} r(\tau) = \infty$. The probability of a reward given is outlined by $P_{rj} = P(S \cap J)$ and $P_{rs} = P(S \cap J')$. $P_{rs} > P_{rj}$ is true while $n \geq 2$. If $n = 2$ then $P_{rs} = P_{rj}$ and if $n = 1$ $P_{rs} = 0$.

As discussed above, the weight of the reward changes based on the time elapsed. This weight is modeled by the following equation:

$$W_r(t) = \frac{1}{RvN + \sum_{\tau=0}^{t} r(t)}$$

where Rv is the resistivity value and N is the number of channels. Consequently the probability of a user appearing on a channel is given by the following equation:

$$P_n(t) = \frac{Rv + \sum_{\tau=0}^{t} r_n(\tau)}{RvN + \sum_{\tau=0}^{t} r(\tau)}$$

.

3.3 Network Design and Implementation

The channel model is very similar to the one used in Chapter I but with some major differences. The test bed previously developed was modified to satisfy the requirements of this test so the underlaying assumptions still exist.

3.3.1 General Network

It is assumed that there are N channels where each channel is modeled by a two-state Markov Chain. On each channel two states exist, idle (I) and occupied (O). A occupied state exists when a primary user or a PUE jammer is currently operating on that channel and the secondary user is not allowed to transmit. In an idle state the secondary user is allowed to transmit as no primary user or PUE jammer is currently transmitting on the channel. The transition probability can once again be determined from the probability matrix :

$$Q_n = \begin{pmatrix} 1 - P_{IO}^n & P_{OI}^n \\ P_{IO}^n & 1 - P_{IO}^n \end{pmatrix}$$

where P_{IO}^n (P_{OI}^n) means the transition probability from idle to occupied (occupied to idle). p_{nI} and p_{n0} are the initial probabilities of channel n being idle.

Each channel is assumed to operate with the same physical characteristics to simplify calculations, though it is understood that this cannot be controlled in a physical application so actions were taken to get as close as possible.

As before the radios are not able to transmit and receive simultaneously so each user was programmed to transmit multiple times in quick succession to allow near perfect detection of each user. Though this is not always so in physical applications, the design of a perfect transmitter and receiver was outside the scope of this investigation so alternative methods were implemented.

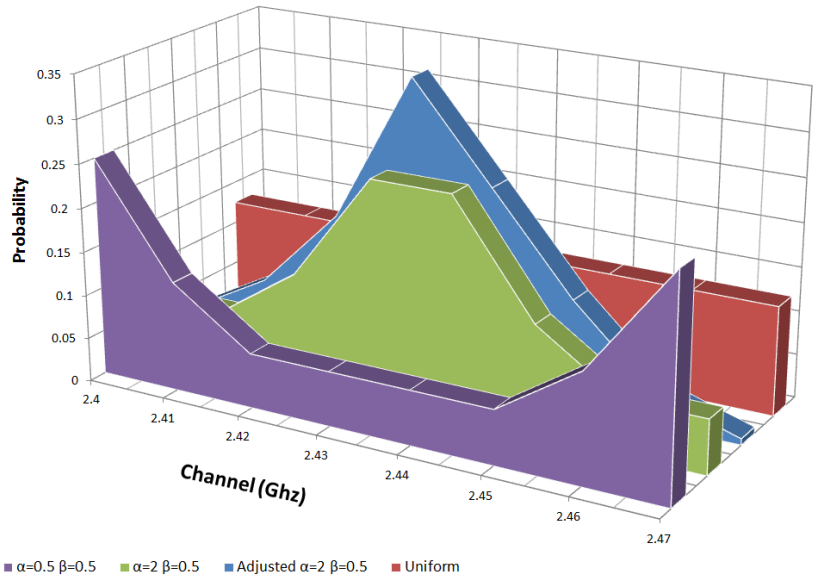


Figure 3.3: Initial Probability Density Functions

Each data set was instructed to run for 3000 secondary user transmissions to ensure that a proper curve developed so through conclusions could be made. Since different levels of learning resistivity were used it was necessary to run tests for extended periods of time to let each settle. The length of the test also allows the final results to represent the impact learning can make as time increases.

3.3.2 Primary User Model

The primary user operates exactly as it did in Chapter I. The primary user infinitely loops through two states, transmit and change channel. In the transmit state, the primary user wait a random amount of time (t) for the constraint $0 < t < 5$ seconds and then transmits. It listens to channel activity however it does not react to activity on the channel as primary users have full rights to channels and are allowed to interrupt other transmissions. Once the primary user reaches the change channel state it picks a random channel fitting the selected probability density function (PDF).

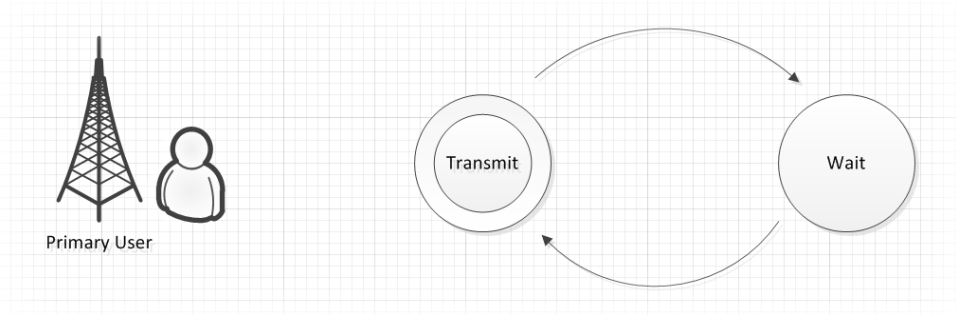


Figure 3.4: State Diagram for Primary User

The primary user operates on two PDFs in this chapter as opposed to the four in Chapter I. It uses two beta distributions which are roughly opposite of each other to show that the investigation into using Hedge Algorithm based learning is not heavily influenced by the behavior of the primary user. These distribution functions can be seen in Figure 3.3.

3.3.3 Secondary User Model

The secondary user must avoid the primary user and PUE jammer so it has a strong detection mechanism to keep it away from these users. It starts off in a sensing state where it determines if the channel is idle. If it is occupied it switches channels to the next channel as determined by its operating probability density function. Following the sensing state it will transmit packets and determine if the packets were transmitted successfully. If the packets are successfully transmitted, then a reward is applied. If some error occurs then the user returns to the sensing state.

The learning algorithm works by rewarding each successful transmission so that the user learns which channels hold a higher rate of success. It does not discriminate between n continuous transmissions and n single case transmissions as time on the channel does increase throughput by reducing recovery time. The overall ratio of successful time on a channel versus total time demonstrates the health of the channel. A learning resistivity value is applied to the algorithm to differentiate exploitation

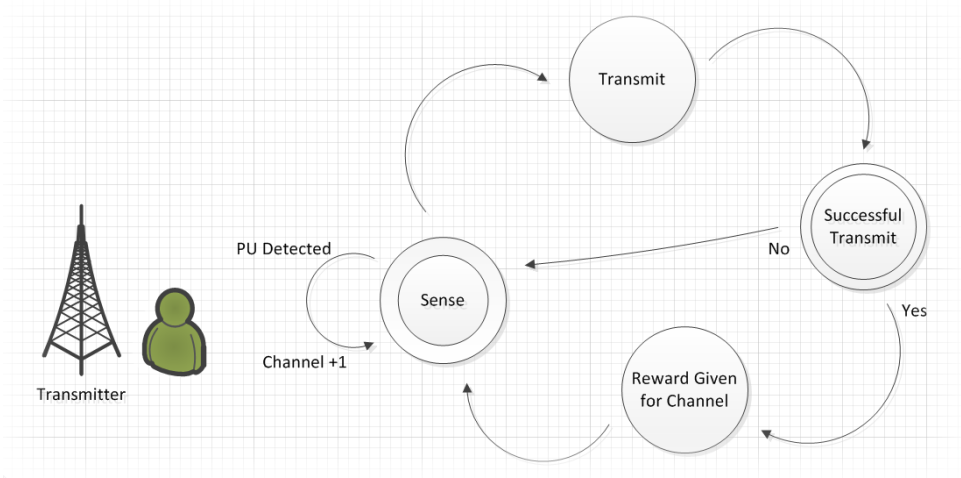


Figure 3.5: Transmitter State Diagram

of channels to random hopping. This will be discussed with more detain in Section 3.3.5.

The secondary user operates on a few different PDFs depending on what it is doing. During tests where it is performing the learning algorithm, it is initialized with a uniform distribution which evolves as the algorithm progresses. If the user is being followed by a learning jammer and it is not learning it follows a enhanced beta distribution as shown in Figure 3.3.

3.3.4 Attacker Model

The attacker operates as primary user emulator where it mimics the transmission signature of a primary user to take advantage of a secondary user's ability to avoid primary users. The secondary user is not allowed to transmit when a transmission with the signature of a primary user appears. The jammer takes advantage of this and launches a primary user emulation attack since the secondary user cannot determine if it is experiencing a true primary user or a malicious user.

The attacker operates on four states similarly to secondary users. It starts out on a sensing state to detect primary users to prevent two primary user signatures to appear on one channel. Transmissions during a primary user's transmission can

cause the jammer to be detected. Operating without detection is ideal for a jammer. A secondary user will react to either a PU or a jammer so two transmissions is unnecessary. If a primary user exists the jammer changes channels, following its assigned PDF shown in Figure 3.3, and starts the sensing process over. If the channel appears free of primary users the jammer will commence transmissions for a set period of time. If it detects a secondary user on the channel during this time it will place an award in that channel's coffers to increase the probability that it will return to this channel. If no user is detected it will still transmit. It will then return to the sensing state on a new channel but no reward will be given. A full cycle of all of the user's states takes about one second. A rapid rate was chosen since prolonged contact with a secondary user is not beneficial. If the jammer is detected then it may continue on to the next channel because the secondary user acts purely on the appearance of a primary user signature so prolonged channel activity is unnecessary.

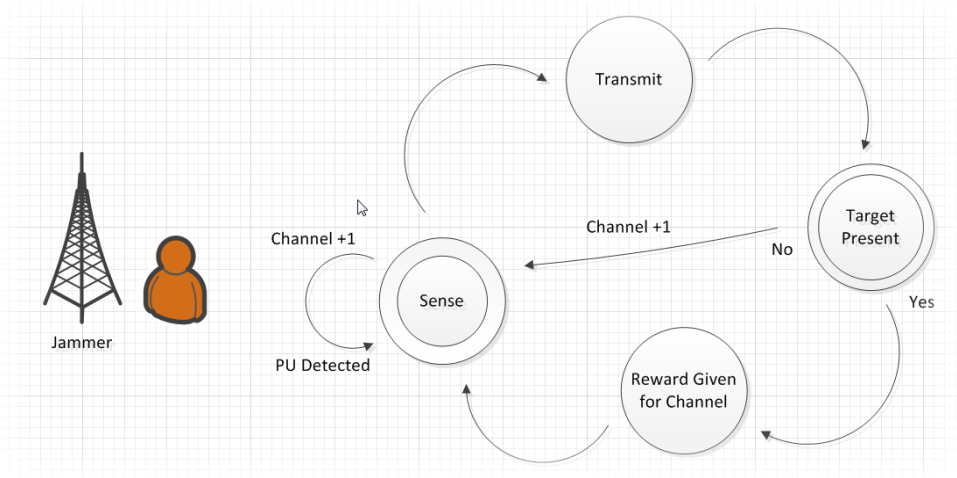


Figure 3.6: Jammer State Diagram

The jammer operates on two different probability density functions. If it is learning it starts with a uniform distribution as it offers a clean slate for changes to take place. If it is not learning and the secondary user is, it operates on an enhanced beta distribution which is shown in Figure 3.3. This function was modified to give more extreme peaks to increase the impact of the learning algorithm. If a shallower curve

is used it may be too close to a uniform distribution and may cause the change to be hard to differentiate.

The learning algorithm works for the jammer by rewarding each successful detection of a secondary user by increasing the probability that the jammer will return to this channel. A learning resistivity value is applied to the algorithm to determine how quickly the jammer will adjust its own PDF to mimic that of its target. This will be discussed further in Section 3.3.5.

3.3.5 Learning Resistivity

Since the jammer and secondary user applied the same base learning algorithm it was necessary to create a scaling factor to determine the resistivity of the algorithm. These values control the ability of each user to be balanced between exploitation and exploration. The secondary user applies a reward every time a packet is successfully transmitted but the jammer only applies rewards when a collision occurs. The secondary user rewards can quite quickly exceed the total rewards given by a jammer in a test. It was also of interest to test the impact of different resistivity values to the performance of both users apart from purely a calibration factor.

Each value increased the stubbornness of the initialized PDF by some factor. A resistivity factor of 2x would cause the initialized PDF to out weigh the learned value by 2:1 on each channel and 14:1 across all seven channels. Each user had a different set of resistivity values depending on the behavior of the user. All values given for resistivity settings are given for initial values. As the test runs the learning ratio changes as shown in 3.1 and 3.2.

The secondary user has to use higher resistivity values because of the high number of rewards given over a test. It uses 10x, 50x, 100x, 200x, and 400x. Tests conducted below 10x caused the user to heavily exploit initial channels and caused skewed results as it was rare for the user to leave the first few channels it experienced. The ratio of 70:1, 10:1 on each channel, gave the first decent results so it was used. The values

spanned up to 400x because 400x produced results which approach values given by no learning.

Since the jammer gives fewer rewards it can use a lower resistivity value. It uses 2x, 6x, 20x, 50x, and 100x. As mentioned in the secondary user case, a spread of resistivity values from just above exploitation to close to no learning were chosen. The range of 14:1 to 350:1, 2:1 and 50:1 on each channel respectively, were used.

Each of these resistivity values allow the algorithm to run for longer before reward's values significantly reduce their total weight. This algorithm was intended to serve as a point of reference for future investigations into methods for mid run PDF changes and for algorithms to dynamically change parameters to increase performance.

3.4 Data and Analysis

A series of tests were performed using the learning algorithm on the cognitive radio test bed to show the performance and limitations of a Hedge based learning algorithm. The first series is to prove that the actions of the primary user impacts the results but does not alter the general trend of the algorithm. After this test is performed, the learning algorithm is applied to the secondary user and jammer independently to show its performance over a period of 3000 transmissions.

3.4.1 Primary User Testing

In order to come to a general understanding that the primary user's performance does impact the final results of the test but does not impact the general trend of the learning algorithm, a series of tests were performed using two Beta distributions. These can be seen in Figure 3.7. The primary user was tested with both of these distributions against the fastest acting of each of the resistivity settings and no learning for both the jammer and secondary user. The jammer will use the 2x settings and the secondary

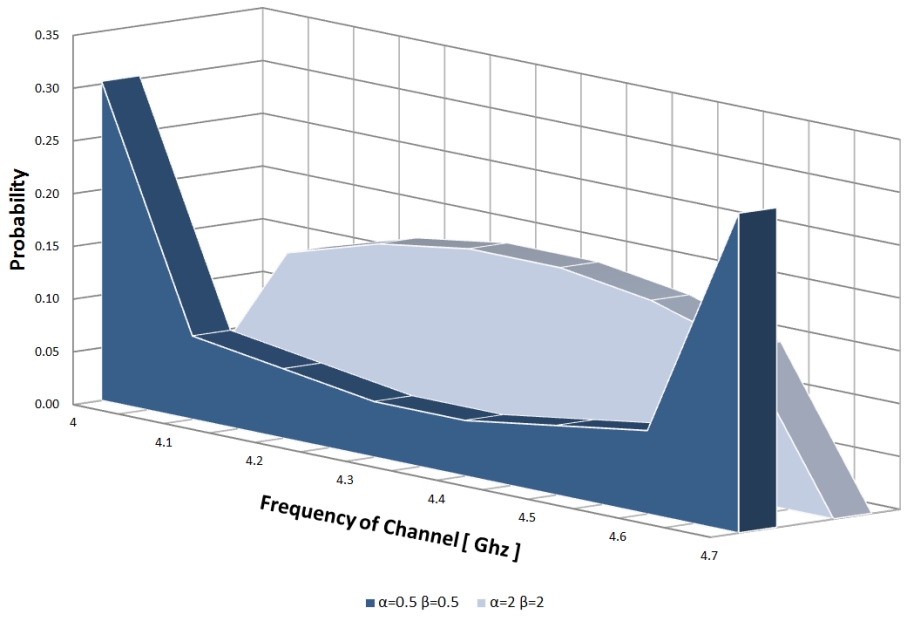


Figure 3.7: Primary User Probability Density Functions

user will use the 10x setting. This test operates on the same parameters as other tests in this section but with varying primary user PDFs.

The first set shows the primary user with the jammer learning turned off. In Figure 3.8 and Figure 3.9 it can be seen that the general outcome is quite similar. There is some deviation but this was formed by various outliers in the data as well as a smaller number of tests being averaged. A constant difference of collisions is expected but the general trend should remain the same throughout the tests. Since each PU PDF is so different from each other, it is expected that one will cause more collisions than the other. One distribution causes more collisions at the central channels but the other will help later in the test when the jammer visits the outlying channels less often since will visit central channels regularly.

Figure 3.10 and Figure 3.11 show the results from the secondary users. Similar slopes across the different PU PDFs are observed in these figures. The values were

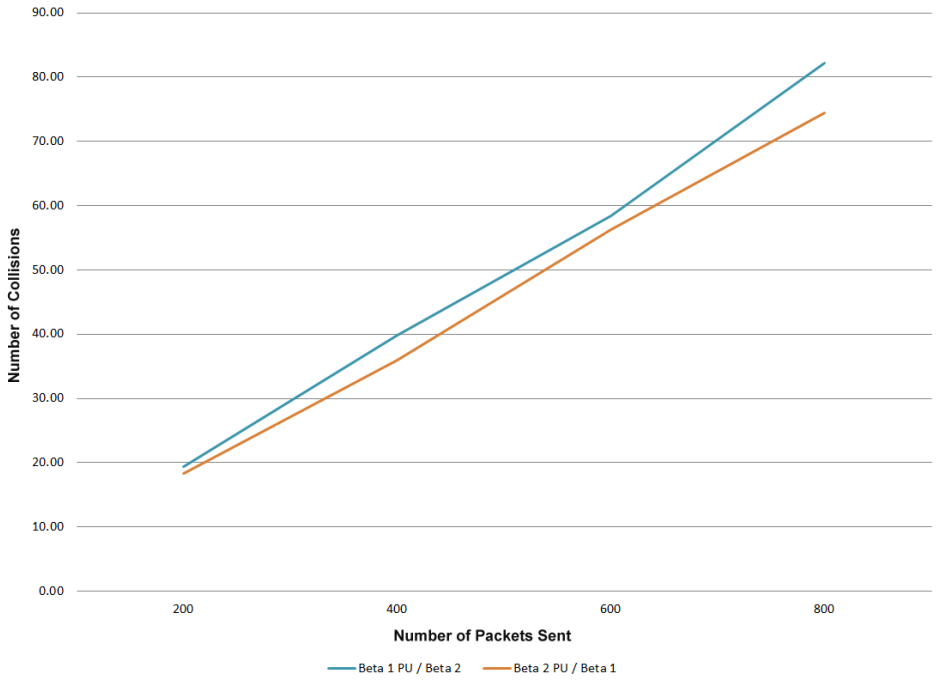


Figure 3.8: Non-learning Jammer with Various Primary User PDFs

consistent from test to test in Figure 3.8. Consistent values are not necessary and are unexpected since the primary user distributions are so different from each other.

The results from this section of the data show that the original hypothesis was true and that the primary user influences the data but does not impact the general performance trend caused by the algorithm. This successfully determines that the primary user can be removed as a heavy influence on the trends displayed in the coming sections.

3.4.2 Secondary User Analysis

The next phase of testing involves examining the impact of the learning algorithm at different points along a transmission 3000 packets in length. The data is expected to show how the algorithm changes the performance of the user with different resistivity values.

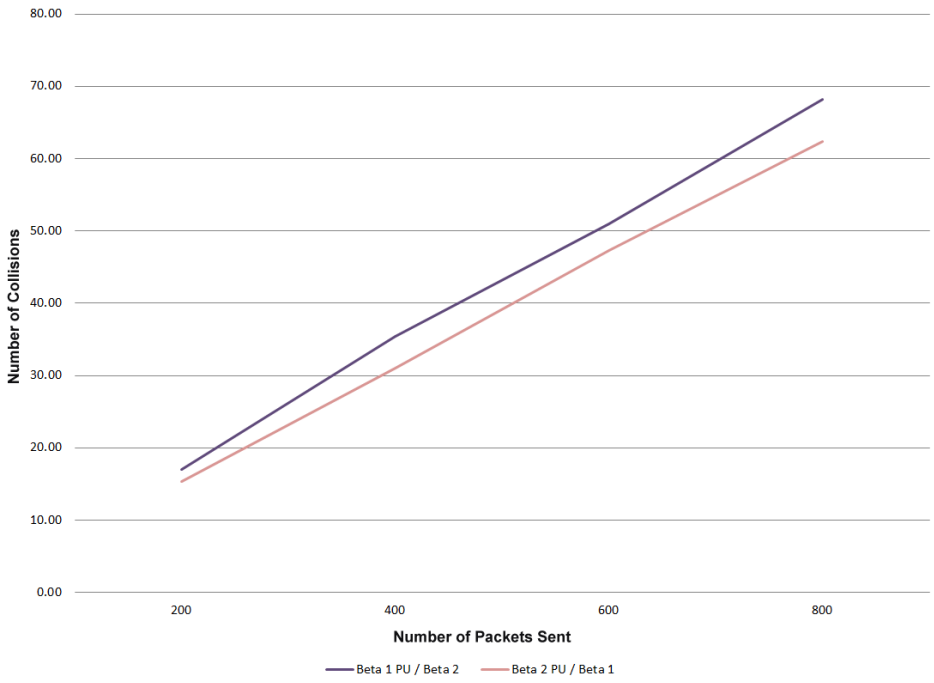


Figure 3.9: Learning Jammer with Various Primary User PDFs

While one user learns the other user does not so the performance of each user could be assessed separately. The algorithm is expected to improve results by lowering the number of collisions that occur.

The data shown in Figure 3.12 shows that the secondary user did indeed benefit from the algorithm. The top trend line represents the trend of no learning while the bottom line represents 10x resistivity to learning which is the producer of the least number of collisions. This shows that at the lowest value the user did indeed avoid collisions as desired. The different resistivity settings all lie between those two settings. It is strange that the 50x, 100x, and 200x resistivity settings fell so closely together since they differed by such a large factor. The 400x value did lie closer to the none value as expected.

In order to show the effectiveness of the learning algorithm the most extreme case was investigated further and the slopes were calculated. As seen in the figure, learning caused collisions over time to decrease by -3.895 collisions per 200 transmissions at

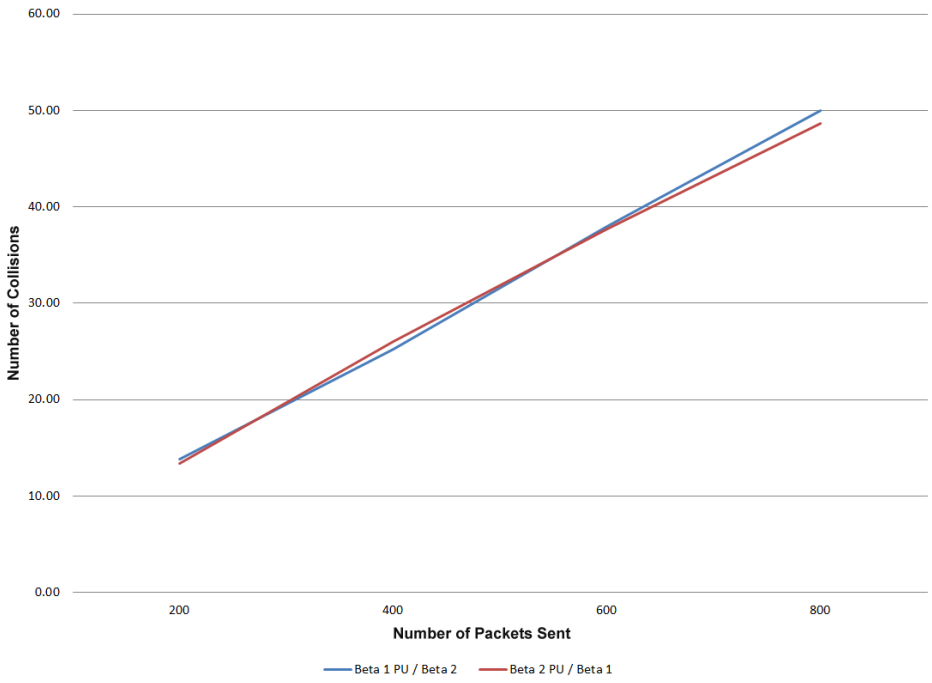


Figure 3.10: Non-learning Transmitter with Various Primary User PDFs

the 10x setting. This may not seem like much but over a long transmission this could make a large difference since each collision can cause significant packet loss if the jammer is effective in its disruption technique.

A closer look at the piecewise slope reveals that the difference isn't consistent but does have a general downward trend for all resistivity settings other than none, which remains fairly constant. It is also shown that as the resistivity values increase that the performance benefit decreases. In general the slope increases from 10x up to 400x in each set of 200 collisions. This shows that the resistivity values are properly adjusting the potency of the algorithm. Compared to the piecewise results for the jammer the secondary user results appear more orderly because of the larger number of rewards given over the same period of time.

Another key to knowing if the user is properly learning lies in the active adjustments to the PDF at each setting. As shown in Figure 3.14 each setting produced a different final PDF, each getting closer to the target PDF. The users

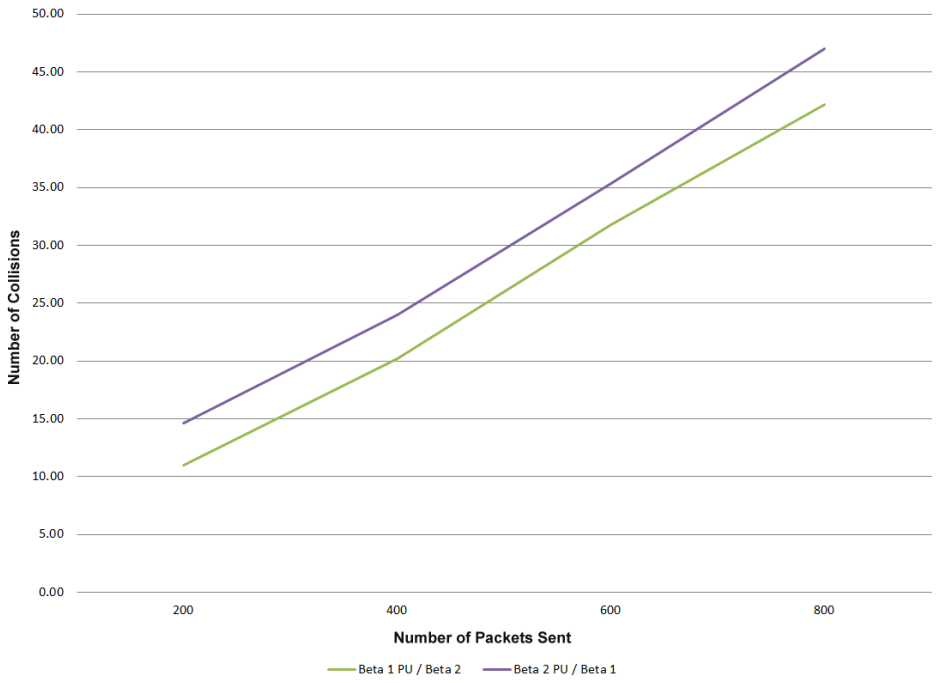


Figure 3.11: Learning Transmitter with Various Primary User PDFs

could only learn up to the PDF of the target since once a close match is achieved it would just spend the rest of the transmission fortifying what it had already learned by adding weight to channels then readjusting to this misapplied reward. A easy version to visualize would be trying to target a uniform distribution when starting with a uniform distribution. Every reward given would cause the user to behave differently than the target so the rest of the transmission would be spent adjusting to this change and trying to reach uniform once again.

The final PDFs also show why resistivity settings below 10x could not be applied. As the values are increased the PDF's curve becomes smoother and symmetric. At very low values, below 10x, the algorithm performed by purely exploiting and would learn on very few channels. This can be seen where the secondary user's final PDF is very uneven at lower resistivity values and the large probabilities that develop on a select few channels. The 5x value is partially exploiting but not enough to produce poor results. Lower setting values actually hurt their own performance

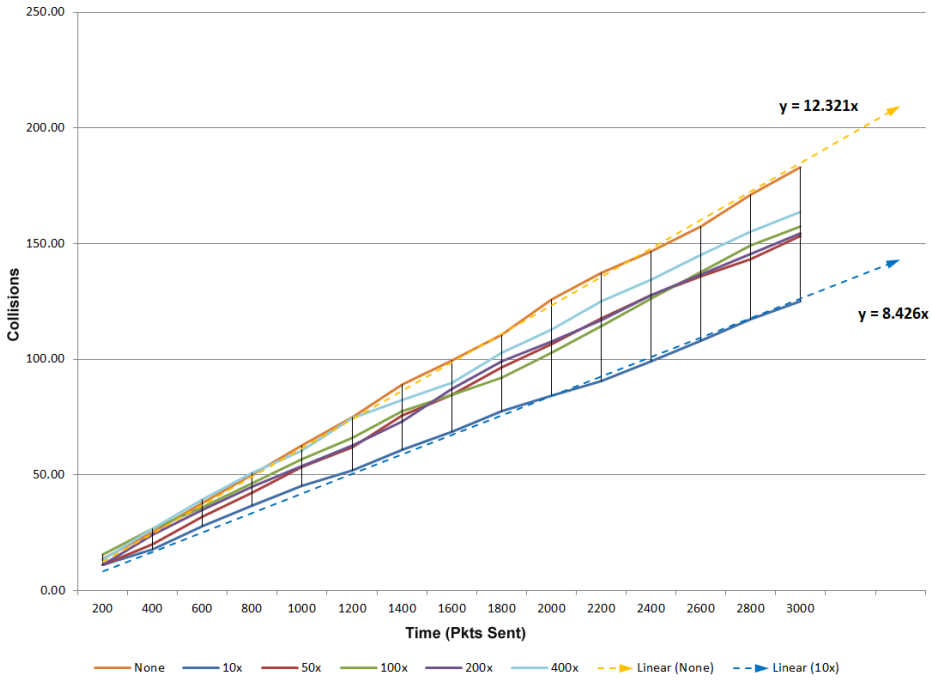


Figure 3.12: Learning Secondary User - Collisions Per Interval

because they would not change their frequency and would just stay on their current channel regardless of jammer behavior. This is beneficial if it occurs at less probable channels but if it fell within the center channels it would greatly increase collisions.

When the learning was turned off, the user operated on a uniform PDF throughout the test. As the resistivity was lowered it is shown that the curve diverges from this uniform PDF. It should be noted that the border channels, 2.4 Ghz and 2.47 Ghz, greatly increase in probability as the user applies heavier learning. This exposes an aspect to this algorithm that tends to benefit secondary users over jammers. This will be discussed further in the jammer section of results.

The data shows that a Hedge based learning algorithm is beneficial for use with a secondary user as it allows for a simple detection approach with longer transmissions as well as fewer collisions. Fewer collisions allows the user to spend less time recovering from channel hops and from resynchronization with other secondary users. Longer transmissions without interruption enable the secondary users to efficiently

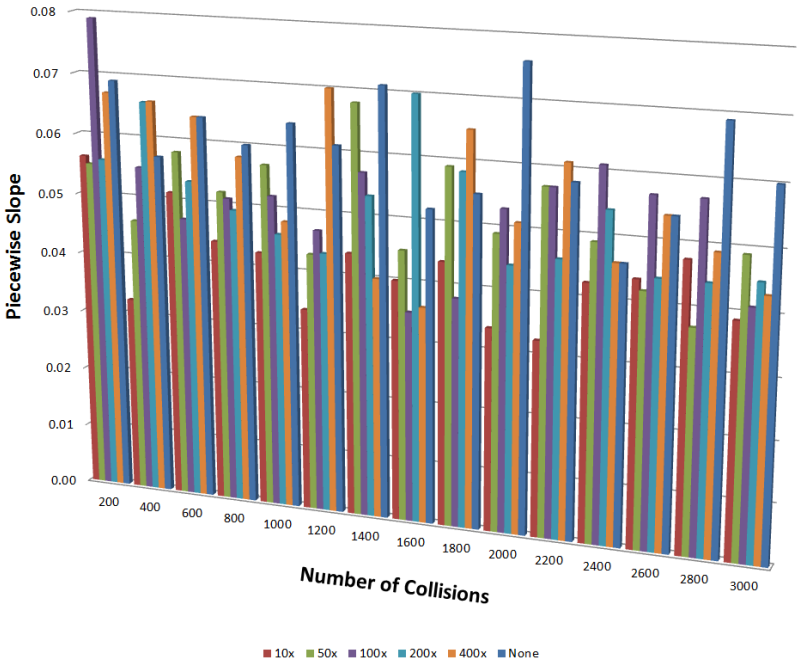


Figure 3.13: Learning Secondary User - Piecewise Rate of Collisions

communicate. Every time a collision occurs transmissions may be damaged and must be restarted. Though short transmissions are still beneficial in this application, longer transmissions may be preferred.

3.4.3 Jammer Analysis

The jammer was also set to learn and produced similar results but with smaller differences. This was to be expected since a secondary user could apply many more rewards over a period of time than the jammer since rewards were given after every successful transmission versus at every collision.

The data from the jammer fully spans the difference between none and optimal. The best setting was found to be 2x, a ratio of 1:14 or 1:2 on each channel. The 6x setting lies very close to the 2x setting but it was slightly worse in performance. The 20x and 50x values are very close to the same throughout the whole test and the 100x lies very close to having no learning whatsoever. The 2x setting produces 2.779

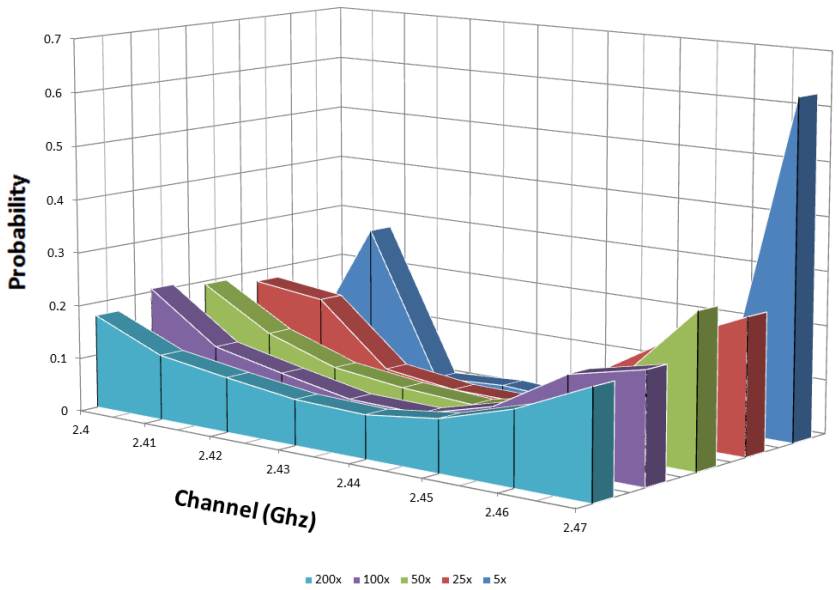


Figure 3.14: PDF After Test for Intelligent Secondary User

more collisions per 200 packets sent. Though this isn't a large difference it gives the jammer an edge and over prolonged transmissions could make a large difference if the disruption techniques were well applied.

The piecewise slope data for the jammer was not as revealing as the secondary user because of the reduced number of reward opportunities. The general trend almost appears even but an increasing trend can be seen across some of the different resistivity values. This can be expected since a smaller amount of data was evaluated due to the nature of the jammer and extended periods of uninterrupted transmissions from a secondary user can cause skewed data when it is viewed on a small scale.

It is shown that lower resistivity values allow the algorithm to shape the user's PDF to the target's own PDF. This resulted in higher collision rates. Initially it was puzzling why the algorithm only provided linear improvements to the performance of the users but after further investigation it was found that though it did increase,

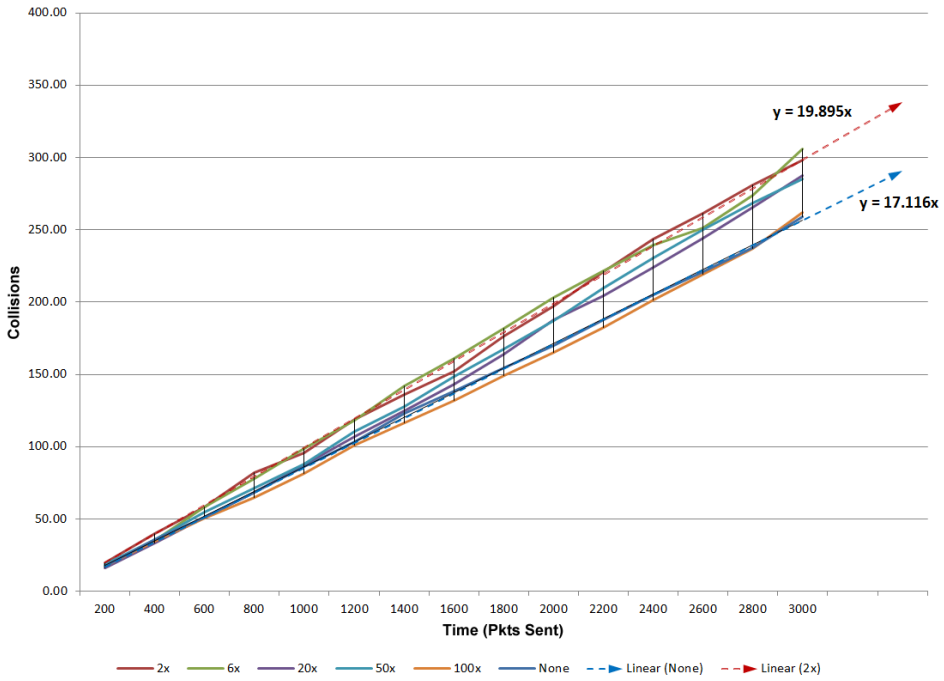


Figure 3.15: Learning Jammer - Collisions Per Interval

decrease for secondary users, the number of collisions it also caused certain frequencies to be neglected.

The success of a secondary user depends on the number of packets it can get through without interruption. Since the secondary user developed in this investigation was simple in nature and transmitted very concise packets the jammer will be investigated.

In Figure 3.18 a resistivity value of 100x was applied to the jammer which provided a fairly even average value across all channels. At this resistivity value the algorithm was not applying the learning very heavily so results will mimic no learning. The maximum and minimum values are almost random at this setting.

After heavy learning was applied it is apparent that the users do what may seem obvious, appear more often at more probable channels. This can be seen as the delay value starts to appear as the inverse of the PDF. In Figure 3.19 the minimum, maximum, and average delay values mimic exactly this. Since the shortest time spent

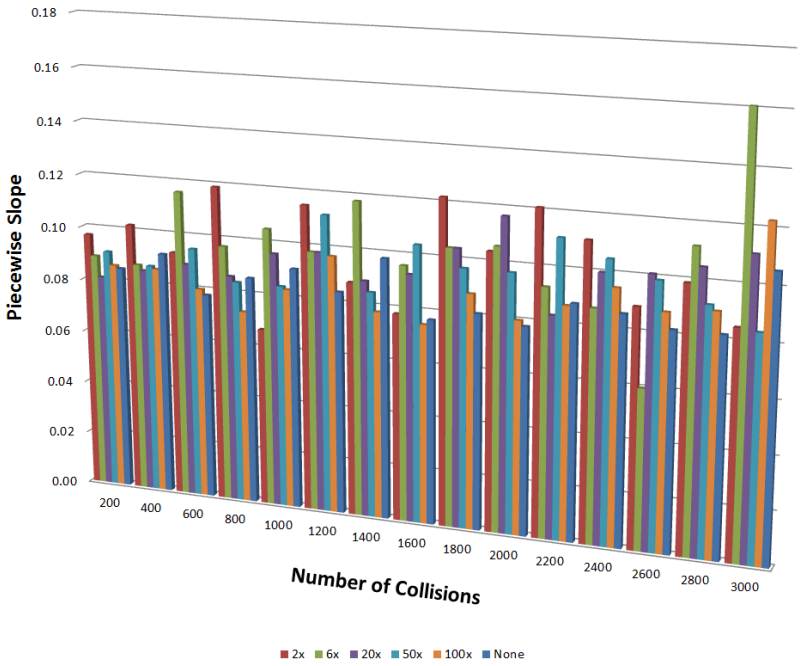


Figure 3.16: Learning Jammer - Piecewise Rate of Collisions

on a channel would occur when an immediate collision after a move occurred the minimum values all appear very similar. The average and maximum values however demonstrate the inverse PDF quite well. The amount of time spent on the exterior channels allows for longer uninterrupted transmissions. The max on 2.47 Ghz nears a whole minute. This is a long time when the jammer is transmitting and hopping channels close to once a second.

The increased time for continuous transmissions allows the secondary user to escape for increased amounts of time without being seen. This causes some suspicious data to appear in the initial tests. Collision data would remain constant for a entire slot of 200 packets since the user was essentially hiding in these exterior channels. Though the jammer was adjusting its PDF to the secondary user, it started to neglect the channels rarely used and gave the secondary user a sanctum for transmitting. Though increased collisions may appear beneficial, continuous and frequent collisions are more beneficial to a jammer as each of these collisions may cause the secondary

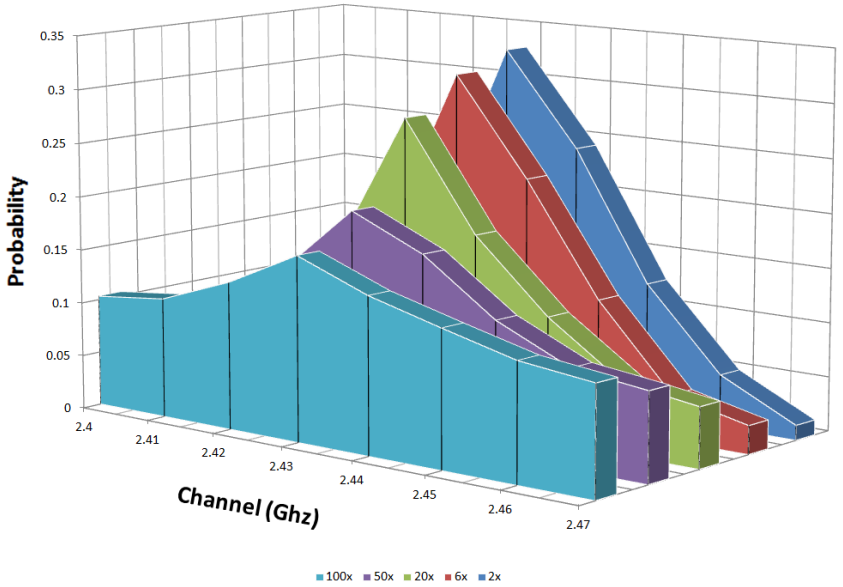


Figure 3.17: PDF After Test for Intelligent Jammer

users a period of downtime depending on the design of the network. Rapid and closely spaced interruptions followed by long uninterrupted transmissions can prove overall beneficial to secondary users. A secondary user could detect the presence of a jammer or primary user before it has time to recalibrate. Ideally interruptions would occur as soon as users regain control of the channel to cause maximum interruptions. This shows that this algorithm may be applicable for a jammer using higher resistivity settings but nevertheless it will reach the same steady state PDF at some point in time. If the target user operates on a similar PDF it will cause the same issue.

The jammer did benefit from using the Hedge based learning algorithm but at a cost, frequency of collisions. Since learning allows the jammer to target higher traffic channels it causes more frequent collisions but possibly so frequent as not to allow users to recover. If users hop prior to recovery it may not cause as much harm as if users were caught right after time was spent recovering from a channel hop. In addition the frequent appearance of the jammer in higher traffic channels opens less

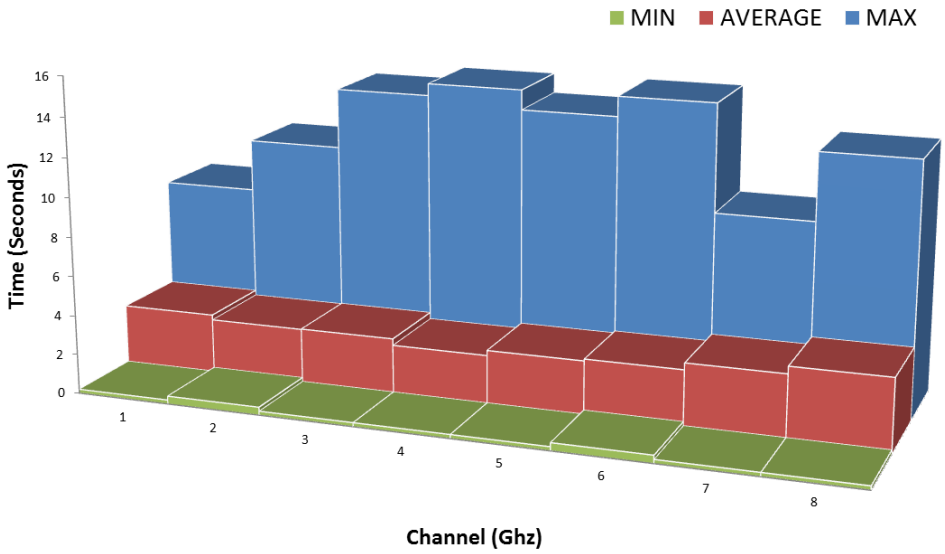


Figure 3.18: Idle Channel Statistics - Intelligent Secondary User at 100x Resistivity

frequented channels for secondary user exploitation. It was shown that the opening of these holes can allow transmissions of a minute or more without interruption.

3.5 Conclusions

Hedge based learning does alter collisions in a cognitive radio network but it is linearly dependent on the resistivity to learning algorithm contrary to exponential as initially expected. This is caused by the shaping of the PDF so channels less likely to be chosen by the other user become less probable for that user to choose. This causes extended periods without collisions causing the learning benefits to be dulled. This makes this learning algorithm beneficial for a jammer if target probability density functions tend to be shallow or higher resistivity settings are used.

Since this learning algorithm allows users to define the behavior of another user across multiple channels, it proves beneficial to a secondary user attempting to avoid a PUE jammer. It allows for avoidance without discrimination between jammer and primary user. The design helps the user find channels where longer transmission may occur and avoid channels where heavy primary user / jammer behavior exists.

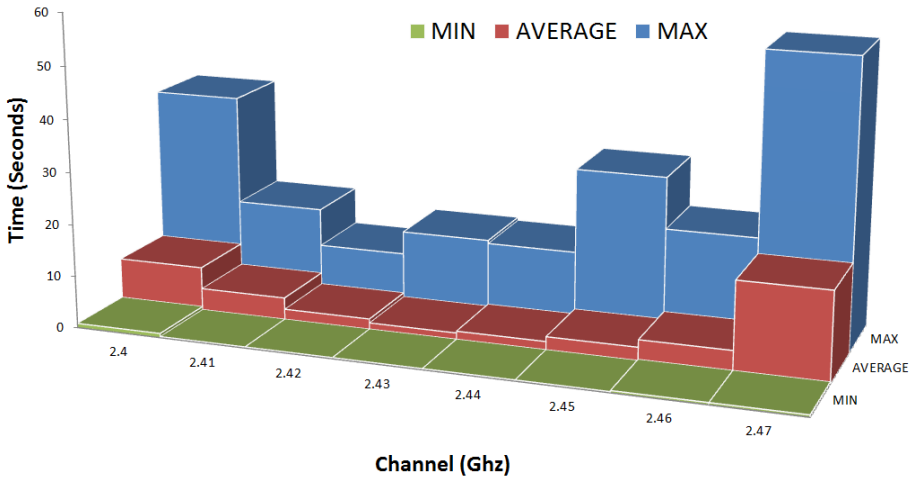


Figure 3.19: Idle Channel Statistics - Intelligent Secondary User at 2x Resistivity

This chapter of the investigation demonstrates the effectiveness of Hedge based learning algorithms in the application of cognitive radio for PUE jammers and secondary users alike.

3.6 Future Works

This investigation revealed some important traits with Hedge based learning in a cognitive radio network but further investigation is always beneficial.

A comparison was made with each user independently but no comparison was made with both users learning simultaneously. This could possess some interesting results. An application where two users are applying machine learning is a more realistic application unless users are applying simple cognitive radio networks.

Data was collected for 3000 packet transmissions but almost all resistivity values reach steady state at the end of the test. Further investigation could be made into a forgetting factor or a point of reset for the learning algorithm that would allow for targeting new users in a network. Major constraints in this investigation included the vast number of testing possibilities. A through examination would need to be

conducted where various restarting points were tested with numerous distributions. This could prove to be cumbersome but informative.

Chapter 4

General Conclusions

The investigation into cognitive radio primary user emulation attacks produced some interesting findings. In cognitive radio networks it is imperative for secondary users to avoid primary users and jammers to the best of their ability and to keep interruptions down as the only way for malicious users to influence transmissions is for them to end up on the same channel. Since a primary user emulation attack prevents secondary users from differentiating primary users and jammers, the only way to avoid one is to avoid both. A secondary user may not even understand that they are under attack if a jammer behaves appropriately.

Chapter I revealed that a jammer performing a sweeping motion over all channels within the spectrum strongly benefits a jammer. This sweeping motion ensures a regular and systematic check of all channels. Since continued and timely interruptions are key to keeping secondary user transmissions short and causing the most recovery time, the ordered (1,2,3...n) approach works well. In a theoretical environment, an ordered approach and a uniform distribution should provide similar results but since a second factor is added with the probability of the other user. The existence of two PDFs decreases the probability of both users being on the same channel at the same time. The secondary user benefits in this case since it has a (n-1)/n chances to avoid the jammer while the jammer only has a 1/n chance to find it.

Chapter II revealed that Hedge algorithm reward based learning does improve the rate at which collisions occur but with a side effect, longer allowed transmission times for secondary users on less probable channels. This may be beneficial for jammers depending on the design of the network they are operating on but if continuous and periodic interruptions are the goal then the learning algorithm must be applied lightly with a higher resistivity factor.

The investigation shows that a secondary user is naturally better off in either case. As long as it picks one channel the jammer does not occupy, it wins for that time slot. The uniform distribution worked best for the secondary user in Chapter I because of this. Once on a channel, the user transmits until interrupted so a sweeping pattern shouldn't impact the user greatly. The data showed a slight benefit to using uniform distributions but with much less of a difference than for the jammer.

If a jammer is operating on a set spectrum at a specific PDF it is very beneficial to secondary users to be able to identify those channels and avoid them. The learning algorithm applied in Chapter II greatly helped the secondary user since it identified the least occupied channels and causes the radio to frequently hop to these channels. This causes longer periods of uninterrupted transmissions and overall less collisions with jammer and primary user alike. Though this algorithm does reach steady state it would be beneficial for a secondary user to use it in an environment free of jammer activity. It would allow the secondary user to quickly identify the behavior of a primary user in the area and avoid it without ruling out channels occasionally occupied.

Overall the investigation was a success. A through assessment of a primary user emulation attack was evaluated from both the perspective of a jammer and a secondary user. Suggestions were made for both user types and the presented data will be helpful for further investigations.

Bibliography

Bibliography

Baes, M. and Buergisser, M. (2010). Hedge algorithm and subgradient methods. 26

Brown, T. X. and Sethi, A. (2007). Potential cognitive radio denial-of-service vulnerailities and protection countermeasures: A multi-dimensional analysis and assessment. In *Cognitive Radio Oriented Wireless Networks and Communications, 2007. CrownCom 2007. 2nd International Conference on*, pages 456 –464. 4

Chen, R., Park, J.-M., and Reed, J. (2008). Defense against primary user emulation attacks in cognitive radio networks. *Selected Areas in Communications, IEEE Journal on*, 26(1):25 –37. 4, 9

Clancy, C., Hecker, J., Stuntebeck, E., and O'Shea, T. (2007). Applications of machine learning to cognitive radio networks. *Wireless Communications, IEEE*, 14(4):47 –52. 26

Commission, F. C. (2008). November 4, 2008, commission meeting. *Daily Digest*, 27(217):5. 2

Li, H. and Han, Z. (2010a). Blind dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems with unknown channel statistics. In *Communications (ICC), 2010 IEEE International Conference on*, pages 1 –6. 26

Li, H. and Han, Z. (2010b). Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part i: Known channel statistics. *Wireless Communications, IEEE Transactions on*, 9(11):3566 –3577. 4, 10

Li, H. and Han, Z. (2011). Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems; part ii: Unknown channel statistics. *Wireless Communications, IEEE Transactions on*, 10(1):274 –283. 26

Mhnen, P., Petrova, M., Riihijrvi, J., and Wellens, M. (2006). Cognitive wireless networks: your network just became a teenager. In *in IEEE INFOCOM*. IEEE. 26

Mitola, J., I. and Maguire, G.Q., J. (1999). Cognitive radio: making software radios more personal. *Personal Communications, IEEE*, 6(4):13 –18. 1

Peng, Q., Cosman, P., and Milstein, L. (2009). Tradeoff between spoofing and jamming a cognitive radio. In *Signals, Systems and Computers, 2009 Conference Record of the Forty-Third Asilomar Conference on*, pages 25 –29. 4

Peng, Q., Cosman, P., and Milstein, L. (2011). Spoofing or jamming: Performance analysis of a tactical cognitive radio adversary. *Selected Areas in Communications, IEEE Journal on*, 29(4):903 –911. 4

Rieser, C., Rondeau, T., Bostian, C., and Gallagher, T. (2004). Cognitive radio testbed: further details and testing of a distributed genetic algorithm based cognitive engine for programmable radios. In *Military Communications Conference, 2004. MILCOM 2004. IEEE*, volume 3, pages 1437 – 1443 Vol. 3. 26

Sampath, A., Dai, H., Zheng, H., and Zhao, B. (2007). Multi-channel jamming attacks using cognitive radios. In *Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on*, pages 352 –357. 4

Zhu, Q., Li, H., Han, Z., and Basar, T. (2010). A stochastic game model for jamming in multi-channel cognitive radio systems. In *Communications (ICC), 2010 IEEE International Conference on*, pages 1 –6. 4, 9, 10

Vita

Benjamin Ealey was born in Montreal, Quebec Canada to the parents of Richard and Connie Ealey. He attended Idlewild Elementary in Memphis, Tennessee until his family moved to Nashville, Tennessee where he attended John Trotwood Moore Middle School followed by Hillsboro High School. After graduating in the top ten percent of his class with academic honors in 2005, he continued on to The University of Tennessee for his bachelors in Electrical Engineering with multiple scholarships. During his time at the University of Tennessee he became involved with Theta Tau Professional Engineering Fraternity where he served as brotherhood chairman in 2008-2009 as well as president in 2010-2011. After finding his senior level communications electives engaging he decided to continue his education. In 2009 he returned to the University of Tennessee with an assistantship to complete his masters in Electrical Engineering with a concentration in Communications Theory under the guidance of Dr. Husheng Li. Two year later, he graduated with his masters and is eager to enter the workforce.