Security in Cognitive Radio

A Project Report

Presented to
The Faculty of the Department of
General Engineering
San Jose State University

In Partial Fulfilment
Of the Requirements for the Degree
Master of Science in Engineering

By
Shrestha, Junu
Sunkara, Avinash
Thirunavukkarasu, Balaji

May 2010
APPROVED FOR THE DEPARTMENT OF GENERAL ENGINEERING

Prof. Morris Jones
Technical Advisor,
Part-Time Professor, Dept. of Electrical Engineering,
San Jose State University

Dr. Rakesh Rajbanshi
Industrial Sponsor,
Cisco Systems Inc.

Dr. Ali Zargar
Professor, Department of Aviation and technology,
San Jose State University
Abstract

SECURITY IN COGNITIVE RADIO

By

Shrestha, Junu

Sunkara, Avinash

Thirunavukkarasu, Balaji

A number of wireless applications have been growing over the last decade. Most of the frequency spectrum has already been licensed by government agencies, such as Federal Communications Commission (FCC). Therefore, there exists an apparent spectrum scarcity for new wireless applications and services. Cognitive radio can efficiently utilize the unused spectrum for secondary usage without interfering a primary licensed user. In cooperative environment, a primary licensed user can share spectrum occupancy information with a secondary user to enable dynamic spectrum access. However, a secondary user needs to verify accuracy of the spectrum occupancy information and it comes from the legitimate primary users. Without the verification, a malicious user can falsify the spectrum occupancy information. This can result interference to the primary users and minimize available spectrum for the secondary usage. In this project, we propose to develop an efficient technique to verify the source of the spectrum occupancy information to be from the legitimate primary user thereby maximizing the spectrum utilization efficiency and minimizing any interference to the primary licensed users.
ACKNOWLEDGEMENT

We would like to express our respect and appreciation to Professor. Morris Jones, Part-Time Professor, Dept of Electrical Engineering, San Jose State University for his support in achieving our goal.

We would like to thank Dr. Rakesh Rajbanshi, Cisco Systems Inc. for his continuous support, encouragement and direction.

We would like to thank Dr. Ali Zargar, Professor, Dept. of Aviation and Technology, San Jose State University for his suggestions and guidance throughout the ENGR 298 course in SPRING 2010 Semester.

We would like to thank to our family members who continuously gave us an encouragement and support.

Shrestha, Junu
Sunkara, Avinash
Thirunavukkarasu, Balaji
# Table of Contents

1. **Introduction**............................................................................................................................... 1

   1.1 Different Scenarios in Cognitive Radio....................................................................................6

   1.2 Types of Cognitive Radio.........................................................................................................7

2. **Hypothesis**.................................................................................................................................. 8

3. **Advantages of Cognitive Radio**.............................................................................................. 9

4. **Literature Survey**.................................................................................................................... 10

   4.1 Overview....................................................................................................................................10

   4.2 Challenges in Dynamic Spectrum Access Environment.........................................................12

   4.3 Misbehaving User Detection....................................................................................................15

   4.4 Countermeasures for DOS attacks..........................................................................................15

   4.5 Implementation of Trust Metrics .............................................................................................16

   4.6 Attack proof collaborative spectrum sensing............................................................................17

   4.7 Summary...................................................................................................................................18

5. **Problem Statement on Security** ............................................................................................ 19

6. **Economic Analysis and Project Justification** ........................................................................ 20

7. **Proposed Approach** ................................................................................................................ 22

   7.1 Introduction...............................................................................................................................22

   7.2 Proposed Algorithm: ................................................................................................................24

       7.2.1 Distance estimate based on location coordinates: .........................................................24

       7.2.2 Distance estimate based on received power level: .........................................................25

       7.2.3 Relative Trustworthiness..................................................................................................26

       7.2.4 Spectrum occupancy estimates: ......................................................................................28

   7.3 Simulation Setup: ....................................................................................................................30

   7.4 Simulation Results: ..................................................................................................................30

   7.5 Summary..................................................................................................................................37

8. **Economic Justification** ............................................................................................................ 40

   8.1 Problem Statement: ..................................................................................................................40

   8.2 Solution & Value Proportion: ....................................................................................................40

9. **Top institutes for research in cognitive radio in the United State of America**.................... 48
10. Project Schedule .................................................................................................................... 49
11. Team and Committee Members .......................................................................................... 51
    11.1 Project Team: .................................................................................................................. 51
    11.2 Project Committee: ........................................................................................................ 51
12. Conclusion ............................................................................................................................. 53
13. References .............................................................................................................................. 54
14. Appendix .............................................................................................................................. 57
List of Figures

Figure 1: United States frequency allocations.........................................................3
Figure 2a: Used and Unused Spaces from 9 kHz to 1 GHz........................................4
Figure 2b: Used and Unused Spaces from 924 MHz to 948 MHz.............................5
Figure 3: Basic cognition cycle.............................................................................11
Figure 4: Flowchart of the transmitter verification scheme.....................................15
Figure 5: Primary user detection algorithm.............................................................17
Figure 6: Layout for showing malicious user interference to the cognitive radio environment..23
Figure 7a: Man in the middle attack.....................................................................28
Figure 7b: Noise in between the received signal power and distance (SNR= 0 dB)......31
Figure 7c: Noise in between the received signal power and distance (SNR= 10 dB)......32
Figure 7d: Noise in between the received signal power and distance (SNR=20 dB).....33
Figure 7e: Noise in between the received signal power and distance (SNR= 30 dB)....34
Figure 7f: Trustworthiness of a primary and malicious user for various SNR values......35
Figure 7g: Trust Metrics for Penalty Factor 1.........................................................36
Figure 7h: Trust Metrics for Penalty Factor 2.........................................................37
Figure 7i: Trust Metrics for Penalty Factor 3..........................................................38
Figure 8a: Estimated Wireless Subscribers from June 1985-2009............................44
Figure 8b: Number of wireless users from June 2000-2016..................................45
Figure 8c: ROI graph............................................................................................47
Figure 9a: Project Phase 1 Gantt chart.................................................................49
Figure 9b: Project Phase 2 Gantt chart.................................................................50
List of Tables

Table 1: Summary of Trust Metrics for different Penalty Factor..............................................39
Table 2: Number of Users who use our algorithm and corresponding revenues......................45
Table 3a: Expenses estimate for our project in the year 2009............................................... 46
Table 3b: Estimate of our expenses for a period of 6 years....................................................46
Table 3c: Estimate of our ROI for a period of 6 years...........................................................47
1. Introduction

Government agencies, such as Federal Communications Commission (FCC), license radio frequency spectrum to wireless applications. Most of the frequency spectrum has already been licensed out (Atakali, 2008). Due to an increase in new wireless applications over decades, there is a scarcity of the radio frequency spectrum to allocate to these new applications. This spectrum scarcity problem is artificial because the licensed users do not utilize their allocated frequency bands efficiently (Rajbanshi, 2007). The allocation of the radio frequency spectrum band in United States is shown in the Fig. 1. A small portion of the spectrum is allocated for unlicensed users. For example, ISM bands around 900 MHz, 2.4GHz, and 5.8GHz are allocated for Industrial, Scientific, and Mechanical purposes which are always overcrowded and are prone to interference (Rajbanshi, 2007). For new users and new wireless technologies there exists scarcity of spectrum. Several regulatory bodies like Federal Communications Commission (FCC) in United States and Of Com in United Kingdom found that the allotted frequency bands are inefficiently utilized. Several studies conducted across the country demonstrated the poor utilization of the allotted frequency band spectrum (Wang, 2009, Atakali, 2008). So, all the white spaces present in the allocated frequency bands can be used by the secondary users. So, the spectrum occupancy information should share between the primary users and secondary users. Dr. Joseph Mitola had envisioned a cognitive radio during his Ph.D. studies (Mitolla III, J., 2000). A Cognitive radio is a fully reconfigurable device which can observe and change or adapt its communication parameters for enabling secondary usage of the spectrum and yield an efficient usage of the spectrum. However, it is important to make sure that the use of the spectrum by the secondary user does not cause any interference to the legitimate users i.e.
primary users as they hold exclusive rights of the spectrum.

The availability of the unused spectrum can be determined by the following techniques (Marcus, 2005):

- Passively sensing the spectrum
- Using location information of the radio to check the database for frequency spectrum usage
- Using separate transmitters to indicate the spectrum availability

In our project, we develop an efficient technique to verify that the source of the spectrum occupancy information is getting from the legitimate user not from the malicious user. We calculate the trustworthiness of the user based on distance estimates.

In this report, in chapter 2 we discuss the Hypothesis of our project. In chapter 3 we discuss the advantages of the use of Cognitive Radio. Chapter 4 deals with the Literature Survey. Chapter 5 deals with the Problem Statement on Security. In chapter 6, we discuss about our Economic Analysis and Project Justification. Chapter 7 gives an idea about our proposed approach and simulation results. In chapter 8, we give the details about our Project Economic Justification and lastly Chapter 10 gives an idea about our Project Schedule followed by the References and Appendix.
Figure 1: United States frequency allocations

Source: (FCC, 2008)
Fig. 2(a) indicates white spaces are unused spaces and rest are the used spaces. Unused spaces are those spaces where primary users are not using spectrum band at that time.

Figure 2a: Used and Unused Spaces (8/31/2005, Lawrence, KS)

Source: (Rajbanshi, 2007)
Whereas in Figure 2(b) also explains the used spaces and unused spaces. Used spaces are shown by the high power and unused spaces are shown with low power.

![Graph showing used and unused spaces between 924 MHz to 948 MHz](image)

**Figure 2b: Used and Unused Spaces between 924 MHz to 948 MHz (7/11/2008, Worcester, MA)**

Source: (Yuan, 2009)

The results of those studies show clearly how frequency spectrums are occupied sparsely. As the frequency band spectrums are utilized inefficiently, a dynamic spectrum access technique is being developed to use those unused spectrum bands by the primary users by some secondary users (Marcus, 2005). In order to utilize the spectrum efficiently, the concept of Cognitive Radio technology came into existence.

The primary goal of the Cognitive Radio is to provide highly reliable communication and highly efficient spectrum utilization. The method of sharing the spectrum by primary users and secondary users is known as spectrum sharing. The primary users may or may not cooperate with the secondary users for spectrum sharing.
1.1 Different Scenarios in Cognitive Radio

There are two different types of spectrum sharing scenarios. They are

- Cooperative scenario
- Non-cooperative scenario.

In cooperative scenario, a primary user provides secondary users with all information regarding the occupancy of the spectrum and about the unused spectrum so that the secondary users make use of that unused spectrum and keep away from the occupied spectrum. In the non-cooperative scenario, a secondary user needs to sense the spectrum for the unused spectrum and use that spectrum band without causing any interference to the primary user (Akyildiz, Lee, Vuran & Mohanty, 2006). In the cooperative scenario, a malicious user can masquerade as the primary user and provide false information to the secondary user regarding the occupancy of the spectrum, such as the spectrum is unoccupied and the secondary user can use though the primary user occupies the spectrum. With the information provided, the secondary user tries to occupy the spectrum and as a result, interference takes place between the primary user and secondary user. In some cases, the malicious user informs the secondary user as the spectrum is occupied even though the spectrum is free and as a result the spectrum is not utilized either by primary user or by secondary user. Because of these issues, a secondary user must make sure that the information regarding the occupancy of the spectrum is provided by a legitimate primary user. In this project, we propose a trust model to identify the legitimate users, the information is provided by a legitimate primary user there by maximizing the utilization of the spectrum and avoiding the interference between the primary users and secondary users (Chen, Park, & Reed, 2008).
1.2 Types of Cognitive Radio

Depending on the available network side information and the regulatory constraints [Andrea Goldsmith, 2009] there are three different classes of Cognitive radio paradigms. They are

1. Underlay
2. Overlay
3. Interweave

The Underlay cognitive radio paradigm is used when the interference between the cognitive users and non cognitive users is below a certain threshold. In Overlay cognitive radio paradigm communication is provided by sophisticated signal processing. The Interweave cognitive radio paradigms opportunistically exploit the white spaces without causing any interference to the other transmissions (Andrea Goldsmith, 2009). Generally, Interweave cognitive radio system is used.

There are four broad inputs in a Cognitive radio. They are

1. Understanding the working environment in which it operates
2. Understanding the users requirements for a better communication
3. Understanding all regulatory policies that applies to it
4. Understanding its own capabilities i.e. spectrum sensing, spectrum management, spectrum mobility and spectrum sharing. (Doyle, 2004)
2. Hypothesis

In order to enable secondary usage of the unused spectrum in a cooperative scenario, primary user can provide spectrum occupancy information to the secondary user. It needs to be verified that the spectrum occupancy information is only provided by the legitimate primary user and not from a malicious user masquerading to be a primary user. In this project, we developed an efficient technique to authenticate the legitimate primary user, so that the decision about the spectrum occupancy can be accurately made.
3. Advantages of Cognitive Radio

The main purpose of using a cognitive radio over a primitive radio is because of the following advantages:

1. Senses the radio frequency environment for the presence of white spaces
2. Manages the unused spectrum
3. Increases the efficiency of the spectrum utilization significantly
4. Improves the spectrum utilization by neglecting the over occupied spectrum channels and filling the unused spectrum channels (Andrew, 2004)
5. Improves the performance of the overall spectrum by increasing the data rate on good channels and moving away from the bad channels (Anil, 2006)
6. Use the unused spectrum for new business propositions, such as providing high speed internet in the rural areas and high data rate network applications like video conferencing can be made. (Mikkio, Timo, Rantalainen, 2009)

A cognitive radio makes use of the available spectrum efficiently, solves the spectrum scarcity issue and thus can save millions of dollars.
4. Literature Survey

We have performed an intensive literature survey; all of which concluded the same aspect that the licensed users are under utilizing the spectrum over a period of time at different locations. Dynamic Spectrum Access (DSA) technique is one way to sense unused spectrum and utilize it without any interference to the primary user.

4.1 Overview

Cognitive Radios (CR) has the capability to adapt to the communication parameters. As Akyildiz et. al explains about the re-configurability and the cognitive capability. The radio should sense the environment constantly, based on the result; it needs to change the parameters giving birth to a cognitive cycle (Haykin, 2005). Fig. 3 shows a basic cognitive cycle. Based on the environmental parameters, namely battery life, occupancy information, noise power, etc., the CR can change the transmission parameters like carrier frequency, power, modulation method and index, bandwidth, symbol rate, etc., for a proficient usage of the spectrum (Newman, 2007). According to Akyildiz et.al, the four basic functions of the cognitive radios for enabling DSA are as follows:

- Sensing of Spectrum: Cognitive radio need to sense unused spectrum for secondary usage without interfering primary user.
- Management of Spectrum: Cognitive radio need to find the best available spectrum for optimizing the communication requirements.
- Mobility of Spectrum: Cognitive radio need to seamlessly transition the spectrum used for communication, when needed to leave the currently used spectrum.
Sharing of Spectrum: Cognitive radio need to fairly share the available spectrum among the coexisting secondary users.

Figure 3: Basic cognition cycle

Source: (Haykin, 2005)

By enabling secondary utilization of the spectrum, cognitive radios can help in efficient usage of the spectrum.
4.2 Challenges in Dynamic Spectrum Access Environment

Cognitive Radios facilitate in the secondary usage of the licensed spectrum (when not in use). When in use by a primary user, the secondary user cannot use it. Therefore, accurate spectrum occupancy information needs to be maintained by a secondary user. This minimizes the interference. A malicious user can try to falsify the spectrum occupancy information, which may cause interference.

In dynamic spectrum access environment, the following security threats are prominent: (Clancy, Goergen, 2006)

1. Dynamic spectrum access attack:
   In this attack, a malicious user poses as a primary user and transmits signals very similar to the ones by a primary user. The secondary user would blindly believe that the spectrum is occupied by the primary user. In another circumstance, the malicious user falsifies as a primary user and informs the secondary user that the spectrum is in use. Thus, a malicious user can obtain illegitimate access to the spectrum. We call these malicious users as a “selfish” user.

2. Malicious behavior attack:
   A selfish or misbehaving user masquerades to be a primary user and broadcasts jamming signals that is very difficult, to be detected by the secondary user, such that the cognitive radio mistakenly learns that it can use the available spectrum when primary user is transmitting. In another circumstance, the misbehaving user fakes as a primary user and notifies the secondary user that the spectrum is actually available, when it is still in use by the primary user. Thus, giving rise to interference. We term this type of misbehaving user as a “malicious” user.
3. Denial of Service (DOS) attack: (Khan, Loo, Naeem, Khan, 2008)

There could be three types of DOS attacks. The first one being a low intensity attack, next being the high intensity attack and the last one being of the highest intensity. A low intensity attack is on a single node that makes it work inefficiently and thus making it inaccessible by the neighboring nodes in the same network. High intensity DOS attacks is for a group of nodes in an enclosed area, thus making it malfunction and deny services for the other areas in the same network. Highest intensity attack (Distributed Denial of Service) is for the entire network (say broadband) and makes the network inaccessible due to unlimited traffic being pumped from many malicious users, resulting in the network outage.

4. Actions of selfish and malicious users:

Selfish users make constant requests in the network that they need more allocation of channels, more than what is required. They might indicate that the channels allocated to them are corrupt and thus require more of them. Taking into consideration the poor interference scenario, these users could request for a high priority band. A selfish user can also increase their productivity by making the other users ditch the bands they were using by some intentional junk traffic. Whereas, a malicious user is a specialist in spoofing; he follows the packet patterns in the network and appears to be the genuine user. This results in the actual legitimate user being denied the spectrum usage. The Quality of Service (QoS) of the spectrum is tainted and causing the network to be instable.
These four attacks stated above causes the network to work inefficiently resulting in an unfair outcome. As a part of the conclusion, it is always wise not to decide upon the spectrum allocation and utilization using information from a misbehaving user.

### 4.3 Misbehaving User Detection

In cooperative scenario, the primary user shares the spectrum occupancy information with the legitimate secondary user to improve the reliability and better spectrum utilization. In this scenario, a misbehaving user (node) can masquerade to be a primary user and send fallacious spectrum occupancy information to the secondary users, thus disproving the dynamic spectrum theory. It is very important to detect the misbehaving user and disregard the information and requests sent by them.

Our research on identifying a misbehaving user led to pleasant surprises. Chen et.al proposes a transmitter verification technique using the signal characteristics and more importantly the location of the primary user. The below Fig. 4 shows a flowchart for verifying whether a transmitter is a malicious or misbehaving user, or a secondary user or a legitimate primary user (Chen, 2008). The authors propose this method to combine with the existing methods for detecting the spectrum occupancy information and to improve their trustworthiness.
This technique makes use of the location information to verify the transmitter. As the location information may also be known to a malicious user, he may masquerade the location information and pretend to be a primary user, thereby negating the goal of the dynamic spectrum access.

4.4 Countermeasures for DOS attacks

Cognitive radio characteristics could be of tremendous help at the layer one to avoid jamming and cluttering attacks. Since existing encryption algorithms, like AES, DES, WEP and WPA2 are prone to eavesdropping and resulting in DOS attacks, advanced encryption mechanism like 3DES, PGP could be implemented to avoid them. Location detection and IDS (Intrusion
Detection Systems) could be of immense help to prevent DOS attacks.

4.5 Implementation of Trust Metrics

In a cognitive radio environment, it would be a significant step to identify the neighbouring nodes and learn about the trust metrics associated with them, which will in turn help in building the trustworthiness of the neighbouring user (node). The information shared among the users in a network is very important for efficient and reliable spectrum sharing and usage.

Authors Atakli et.al proposed a weighted trust evaluation technique for detecting the misbehaving user in wireless sensor networks. A malicious user is defined as the user propagating erroneous information in the network. Sensor node (SN) is a radio, transmitting the sensed information to the collection agent, also defined as forwarding node (FN). In the proposed technique, the forwarding node calculates the aggregation result (E) based on the information from the sensor nodes ($U_n$) and their weights ($W_n$) (Akyildiz, 2006).

$$E = \sum_{n=1}^{N} W_n \times U_n$$

Where, $E$ = Aggregation result

$W_n$ = Weight of the sensor node ($0 \leq W_n \leq 1$)

$U_n$ = Information provided by the sensor node.

The weight of the SN is dependent on whether it reports correct or false information. If the SN in picture constantly provides inconsistent information (when compared to the expected outcome), it is classified to be providing a false information, resulting in the decrease of its weight. Vice versa, for a node providing the correct information, the weight increases according to the equation,
Where, $\theta$ is the WPR (weighted penalty ratio) for a SN providing consistent false information.

4.6 Attack proof collaborative spectrum sensing

Authors Wang et al. proposed an algorithm for calculating the level of suspicion, with respect to the users and use the result to identify a misbehaving user and alleviate its influence in spectrum occupancy information. Fig. 5 shows the technique proposed by the authors. In the algorithm, $\phi_n(t)$ represents the trust value and $\psi_n(t)$ represents the consistency value. If the trust value and consistency values are lower than dynamically chosen thresholds, $threshold_1$ and $threshold_2$, the result is not used for determining the spectrum occupancy.

![Figure 5: Primary user detection algorithm](Source: (Wang, Lee, Sun, Han, 2009))

Several other researchers have also focused on the study of trust metrics evaluation for determining the trustworthiness of the spectrum occupancy information provided by a specific user.
4.7 Summary

From our extensive literature survey, we conclude that the cognitive radio is definitely a promising solution to achieve dynamic spectrum access and alleviate the inefficient spectrum utilization. In dynamic spectrum access networks, mutual sharing of the spectrum occupancy information helps accomplish the goal to use the spectrum efficiently and minimize the interference to the primary users. However, it is also important to detect and conclude the information is from the trustworthy user and the information is not compromised, so that the spectrum sharing objective is accomplished. As Wireless Network Engineers we are implementing a market winning algorithm to make the communication and the spectrum access more secure.
5. Problem Statement on Security

We know that most of the frequency spectrum band has already been licensed and the licensed spectrum is not being utilized efficiently. Cognitive radio helps to efficiently utilize the spectrum band when the primary user is not using it. The main objective of the cognitive radio is to identify the unoccupied spectrum for the secondary usage without interfering the primary licensed holders. When primary user is using the spectrum band then secondary user can not use that band at that time. When a primary user starts using the spectrum band, secondary users have to stop using the spectrum band as soon as possible for avoiding any interference to the primary users. Primary users hold the exclusive rights to the licensed spectrum. This can be classified as a core business problem as the primary user has to acknowledge a few compromises and deal with it as well.

There are two scenarios in spectrum sharing: Cooperative and Non-Cooperative scenarios. In the cooperative scenario, the primary users and secondary user may share the spectrum occupancy information thereby maximizing the spectrum utilization and minimizing the interference. However, the source of spectrum occupancy information needs to be verified to be from the primary user. In this case, malicious user can claim as a primary user and might cause interference with the primary user. So, trustworthiness between the server and client needs to be ensured so that the secondary users make sure that they are communicating with the primary user not with the malicious user. (Rajbanshi, 2007)
6. Economic Analysis and Project Justification

In this project, we primarily focus on the security in cognitive radio which is one of the needs for new technologies requiring spectrum bands. As we are developing an efficient technique for determining the legitimacy of the spectrum occupancy information, we do not focus on the economic analysis. We are not going to make any device or software. Moreover, cognitive radios are not commercially available yet, so commercial cost of a cognitive radio is not available. We know that the entire spectrum band has already been assigned to the licensed users. Dynamic spectrum access enables the primary user to share their spectrum band with secondary user when primary users are not using at that time. So, cognitive radio helps to sense the spectrum band and find out which band is available and let the secondary users know that the band is available and use it if you want. As a finite amount of spectrum band is available and cannot be manufactured, spectrum band is priceless. So, we focus on justification of the project rather than on economic analysis. We justify our project with a need of security and trust on cognitive radio.

We had reviewed several research papers including journals and conference papers and came up with an idea with an efficient technique to verify the source of the spectrum occupancy information which should be coming from the legitimate primary user. Various techniques to evaluate the trust of a user in cognitive radio environment have been proposed in the literature. Chen et. al have proposed a technique called transmitter verification technique which is used for the location and characteristics of signal of primary user. Transmitter will verify who is primary user, secondary user, or malicious user. Authors combine their technique with existing technique to determine spectrum occupancy and develop the trustworthiness of the occupancy information. (Chen, 2008)

However, in this technique, users need to know the signal characteristics of primary and
secondary users. As the location information and signal characteristics are assumed to be known, the malicious user also knows the primary signal characteristics and he can pretend to be a primary user.

Atakali et. al have proposed a technique called weighted trust evaluation method. It was developed for wireless sensor network, where the sensing information is shared and trust value degrades if the sensor node provides false information. (Atakali, 2008)

However, in dynamic spectrum access environment, spectrum occupancy information needs to be highly acceptable. The impact of malicious users can be more rigorous than selfish users because interference to primary users can have serious legal consequences. This is because the primary user holds exclusive rights to the licensed spectrum.

Wang et.al have proposed a technique for evaluating trustworthiness of an user by calculating the suspicious level of users. (Wang, 2009)

However, the technique does not mention how to calculate the thresholds and does not utilize the location information of the primary users.

Even though several techniques have been proposed in the literature for evaluating trust of a user in cognitive radio environment, they suffer from several shortcomings. In this project, we propose to develop an efficient algorithm for evaluating trust of the users utilizing the location information.
7. Proposed Approach

In this project, we analyzed the importance of ensuring trustworthiness of the Spectrum Occupancy Information and propose an efficient technique to verify the source of the information is from the legitimate primary user.

7.1 Introduction

For our research, we make the following assumptions:

- Our first assumption is that the location of the primary users should be known by the secondary user as well. All users broadcast their location information to a cognitive radio user. A cognitive radio user calculates the distance between the secondary user and the primary user based on various parameters. If distance calculated with the different techniques match, then a cognitive radio user knows that it is talking with a legitimate trustworthy user; otherwise it is a malicious user.

- Our second assumption is that transmit power level of all the users are predefined and known to all users. We consider a ground reflection (two-ray) model for calculating the power level of a received signal over a distance, \(d\). The received power level is given by [Theodore S. Rappaport. (2002).]:

\[
\text{Received Power Level} = \frac{P_{transmit} \cdot G_{transmit} \cdot G_{receive} \cdot \lambda^2}{(4 \pi d)^2}
\]
\[ R_p = P_t G_t G_r \frac{h_t^2 h_r^2}{d^4 L} \] .............................. (1)

Where,

\( P_t \) = Transmit power level,

\( h_t \) = Height of a transmitter

\( h_r \) = Height of a receiver

\( G_t \) = Transmitter antenna gain

\( G_r \) = Receiver antenna gain

\( L \) = System loss factor

Figure 6: Layout for showing malicious user interference to the cognitive radio environment
In the cognitive radio environment, users can share spectrum occupancy information for correct evaluation of the unused spectrum as shown in Figure 6. A malicious user can claim to be a primary user and falsify the spectrum occupancy information, thereby minimizing the spectrum utilization efficiency. As the cognitive radios are limited resources, a robust and well established security techniques developed in Computer Networks may not be a suitable solution in cognitive radio environment. Based on the above assumptions, we propose an efficient technique for validating the source of the spectrum occupancy information.

7.2 Proposed Algorithm:

In our proposed technique, we calculate distance between a cognitive radio user and other users based on location coordinates as well as received power level. If the distance calculated with both of these techniques, then the user is a trustworthy user. In other case, it would be considered malicious user.

7.2.1 Distance estimate based on location coordinates:

Based on the location coordinates, distance between the users can be calculated. Consider \((x, y)\) is \(x\) and \(y\) coordinates of a cognitive radio and \((x_1, y_1)\) is \(x\) and \(y\) coordinates of an existing (primary) users. The distance between a cognitive radio and an existing user, \(d\), is given by the following equation:

\[
d = \sqrt{(x - x_1)^2 + (y - y_1)^2}
\]

Per our assumption, all users broadcast their location coordinates. With this information, distance between any users can be computed.
7.2.2 Distance estimate based on received power level:

Distance between users can also be calculated by measuring the received power level with a known transmit power level. The received power level, $P_r$, is given by the equation (1) for a given transmit power level $P_t$:

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

where,

$P_t$ = Transmit power level,

$h_t$ = Height of a transmitter

$h_r$ = Height of a receiver

$G_t$ = Transmitter antenna gain

$G_r$ = Receiver antenna gain

$L$ = System loss factor

Consider $h_t, h_r, G_t, G_r$, and $L$ are constant and equal to 1. Therefore, the received power level will depend on the transmit power level and distance:

$$P_r = \frac{P_t}{d^4}$$

Consider the transmit power level, $P_t$, is unity. Based on received power level, the distance between the users is given by:

$$d = \frac{1}{\sqrt[4]{P_r}}$$

Hence, distance between the users can be estimated based on the received power level, given the transmit power level is known.
7.2.3 Relative Trustworthiness

If the distance calculated using the coordinates matches the distance calculated with received power level, then the user can be considered trustworthy or vice versa. We define the relative trustworthiness of a user, \( \alpha \), as:

\[
\alpha = \min \left( \frac{d_1}{d_2}, \frac{d_2}{d_1} \right)
\]

Based on the noise level, the distance calculated with received power level may not be very accurate. However, statistically, the distance calculated with both of the methods should come close. We expect the trust values to be close to 1 for trustworthy users. Similarly, we expect the trust value to be low for untrustworthy users.

**Why is trust value for untrustworthy user not equal to zero?**

To calculate the trustworthiness, we need the distance \( d_1 \) and \( d_2 \). As \( d_1 \) and \( d_2 \) are never become the negative values and it’s never have non-zero values. Therefore, relative trust value never equal to zero.

For example:

Distance between the primary user and cognitive radio.
Where as,

\[ d_1 = \sqrt{(x - x_2)^2 + (y - y_2)^2} \]

\[ = \sqrt{(6 - 6)^2 + (1 - 7)^2} \]

\[ = \sqrt{0^2 + (-6)^2} \]

\[ = \sqrt{36} = 6 \]

Distance between the malicious user and cognitive radio.

Where as,

\[ d_2 = \sqrt{(x - x_2)^2 + (y - y_2)^2} \]

\[ = \sqrt{(6 - 3)^2 + (1 - 1)^2} \]

\[ = \sqrt{(-3)^2 + 0} \]

\[ = \sqrt{9} = 3 \]

The relative trustworthiness is given by:

\[ \sigma = \min \left( \frac{d_1}{d_2}, \frac{d_2}{d_2} \right) = 0.5 \]

If the malicious user masquerades as a primary user, then by verifying the distance \( d_1 \) and \( d_2 \) we can decide upon the legitimate primary user’s integrity.
7.2.4 Spectrum occupancy estimates:

In wireless communication environment, spectrum occupancy can be determined by measuring power level of a received signal. However, making the decision with single user information can be misleading and inaccurate.

![Figure 7a: Man in the middle attack](image)

The above figure indicates the man-in-the-middle-attack. When A and B are communicating with each other and C is unaware that A and B are communicating. So, there may be chances of interference when C wants to communicate with either A or B. Because of this reason we need to get the occupancy information from more than one user.

Based on the trust values of trustworthy and malicious users and their interpretation of the spectrum occupancy, we develop the following hypothesis:
For non-occupied spectrum:

\[ Y_c = \sum_{i=1}^{N} \alpha_{1i} W_{1i} \]

Whereas,

\[ \alpha_{1} = \text{Trust level of a trustworthy user} \]

\[ n = \text{penalty factor} \]

\[ W_1 = \begin{cases} 
-1, & \text{not occupied} \\
1, & \text{occupied} 
\end{cases} \]

For occupied spectrum:

\[ Y_c = \sum_{i=1}^{N} \alpha_{1i} W_{1i} \]

Whereas,

\[ \alpha_{1} = \text{Trust level of a trustworthy user} \]

\[ n = \text{penalty factor} \]

\[ W_1 = \begin{cases} 
1, & \text{not occupied} \\
-1, & \text{occupied} 
\end{cases} \]

For trustworthiness user, both the distance d1 and d2 should match whereas if malicious user, distance does not match.
7.3 Simulation Setup:

We will use linear programming and mathematical analysis to develop and justify the proposed solution. We will use MATLAB simulation for verifying the proposed technique and compare the results. We use MATLAB to verify our proposed algorithm. We assumed an area bounded by coordinate (-1,-1) to (1, 1). We have assumed a Gaussian noise only for various SNR levels. We consider 100 instances random coordinates for 50,000 samples. So, the distance can be calculated based on coordinates and received power levels.

7.4 Simulation Results:

Power decreases over distances. However, based on different SNR levels, the received power may be different as shown in figure below
Figure 7b: Noise in between the received signal power and distance (SNR= 0 dB).
Figure 7c: Noise in between the received signal power and distance (SNR= 10 dB).
Figure 7d: Noise in between the received signal power and distance (SNR= 20 dB).
Figure 7e: Noise in between the received signal power and distance (SNR= 30 dB).

From the above figures, Fig 7b to Fig 7e we can understand that the noise level decreases as the SNR value increases. For example, when SNR= 0, there is more noise, When SNR= 10, the noise level decreases and when SNR=30dB, it seems like there is no noise level. From this we can conclude that greater the value of SNR, lower is the noise.
The Fig 7f shows the trustworthiness of a user. If the SNR value increases then correspondingly the trustworthiness increases. If the trustworthiness reaches to 1, then we can conclude that we are communicating with the primary user and not with the malicious user. Even if the trustworthiness is approximately equal to 1, we can trust the primary user, because there may be some interfering noise that will reduce the trustworthiness. As SNR value increases, the trustworthiness also increases and reaches to 1 when SNR=5. Whereas, malicious users trustworthiness remains constant at 0.6, even though the SNR value increases.

Figure 7f: Trustworthiness of a Primary and Malicious user for various SNR values
The above figure indicates the trust metrics for the number of malicious users and the number of trustworthy users. If the penalty factor is equal to 1, the number of trustworthy users is equal to 20 and if the number of malicious users is equal to 40, a correct decision can be made. As the value of SNR increases, we may end up taking a wrong decision as the number of malicious users is more and the number of trustworthy users is less. Thus, we may end up listening to the malicious user.

**Figure 7g: Trust Metrics for Penalty Factor 1**
Figure 7h: Trust Metrics for Penalty Factor 2
Figure 7i: Trust Metrics for Penalty Factor 3
7.5 Summary

At a high SNR value (SNR=50), as the Penalty factor increases, the probability of making a correct decision increases as shown in the below table.

For SNR= 50,

<table>
<thead>
<tr>
<th>Penalty Factor</th>
<th>No: of Malicious User</th>
<th>No: of Trustworthy User</th>
<th>Decision</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>40</td>
<td>20</td>
<td>Wrong</td>
</tr>
<tr>
<td>2</td>
<td>50</td>
<td>17</td>
<td>Correct</td>
</tr>
<tr>
<td>3</td>
<td>50</td>
<td>10</td>
<td>Correct</td>
</tr>
</tbody>
</table>

Table 1: Summary of Trust Metrics for different Penalty Factors

In conclusion, we notice that the trustworthiness of primary user is always better than the malicious users. So, we can make correct decision based on occupancy of spectrum.
8. Economic Justification

In this section we discuss the problem statement, our solution and how different it is from the other proposed ones, market size, required capital, competitors, break even point, ROI.

8.1 Problem Statement:

In a Co-operative scenario, Cognitive radio environment the Primary user and the Secondary user share the spectrum occupancy information in order to maximize the utilization of the spectrum and minimize the interference between the users. So, we develop an efficient technique to determine the legitimacy of the spectrum occupancy and to avoid the use of the spectrum by malicious user.

8.2 Solution & Value Proportion:

Product Service: Most of the frequency spectrum has been already allocated to some users by government agencies like FCC. So there is a spectrum scarcity for the new wireless applications. But all the licensed users do not utilize the spectrum efficiently. There are a lot of unused spaces in the spectrum. The cognitive radio senses the unused spaces and provides the spectrum information to the secondary users so that, they utilize the spectrum without causing any interference to the primary user. But some malicious and selfish users provide false information to the secondary users and cause interference between the primary and secondary users. So, in order to thwart these malicious and selfish users we develop a technique to determine the legitimacy of the primary user and to verify the information provided by that user.

How our solution is different from others?

Chen et. al have proposed a technique called transmitter verification technique which is used for the location and characteristics of signal of primary user. Transmitter will verify who is
primary user, secondary user, or malicious user. Authors combine their technique with existing
technique to determine spectrum occupancy and develop the trustworthiness of the occupancy
information. (Chen, 2008)

However, in this technique, users need to know the signal characteristics of primary and
secondary users. As the location information and signal characteristics are assumed to be known,
the malicious user also knows the primary signal characteristics and he can pretend to be a
primary user.

Atakali et. al have proposed a technique called weighted trust evaluation method. It was
developed for wireless sensor network, where the sensing information is shared and trust value
degraded if the sensor node provides false information. (Atakali, 2008)

However, in dynamic spectrum access environment, spectrum occupancy information needs to
be highly acceptable. The impact of malicious users can be more rigorous than selfish users
because interference to primary users can have serious legal consequences. This is because the
primary user holds exclusive rights to the licensed spectrum.

Wang et.al have proposed a technique for evaluating trustworthiness of an user by calculating the
suspicious level of users. (Wang, 2009)

However, the technique does not mention how to calculate the thresholds and does not utilize the
location information of the primary users.

**Our Solution** - first assumption is that the location of the primary users should be known by the
secondary user as well. For this the secondary user calculates the distance between the secondary
user and the primary user. If that distance comes correct then the secondary user will know that
he is talking with the legitimate user not with the malicious user.
• Our second assumption is primary user can start and stop using the licensed frequency spectrum at any time because they own the exclusive rights to the spectrum.

• Our third assumption is primary users cooperate with secondary users and provide the spectrum occupancy information for enabling the secondary usage of the unused spectrum.

• The last assumption is that Cognitive radios have limited resources, such as CPU power, memory, and battery.

**Market Size:**

As the Cognitive radio is an emerging technology to provide a solution to the spectrum scarcity problem there are several groups in various universities who focus on research in this Cognitive Radio field.

**Competitors:**

At present, there is no hardware or prototype model for this Cognitive Radio. Our solution is a proposed solution. So there are no competitors for us as of now.

**Customer:**

As the number of wireless users has been increasing from year to year, the unlicensed users who want to use the frequency spectrum can be our customers.

**Cost:**

A large number of people can benefit from the cognitive radio. In a dynamic spectrum access environment, there are primary users, secondary users, service providers, and researchers investigating new technologies.
The main problem is that the entire frequencies band has already been licensed by
government agencies, such as Federal Communication Commission (FCC). Because of that
scarcity causes for the new wireless applications and services. So, Cognitive radio helps to
allocate the unused spectrum to the secondary user when it is not in used.

If a primary user is not using the frequency band then he can lease the frequency band to the
secondary user and charge money. This way he can get some monetary benefits when he is
not using frequency band. For example, if someone wants to use the video conferencing
facility, then he could lease the frequency band for 2-3 hours and primary user can charge for
that period of time and get benefits from the secondary user.

For the secondary user, if they can lease the line for 2-3 hours and they don’t have to
purchase whole frequency band. For the service provider, they provide cheaper price and
good data plans to the customer and attract more customers. So, that service provider will get
more benefits.

For a researcher, we have tried to develop our own algorithm based on the security features
in cognitive radio. If we develop this algorithm successfully, then we can charge royalty from
the primary users as well as to the secondary users for implementing our algorithm.

Evidently in our project we came up with an efficient technique to verify the source of the
spectrum occupancy information which should be coming from the legitimate primary user.

So, our algorithm is beneficial for secondary user because he wants to make sure that he is
communicating with the primary user and not with the malicious user. We will charge to the
secondary users whenever they are implementing our algorithm. It is beneficial for us as
well.
The above figure indicates that in the United States the number of wireless users has been increasing from the past 25 years. According to CTIA-The Wireless Association, there are around 276,610,560 users who use the wireless service provided by the service providers. In future, the numbers of users will definitely increase and may double each year. In our estimation, in 2015, there may be approximately 402 million wireless users as shows in the graph below.
Table 2: Number of users who use our algorithm and corresponding revenues

<table>
<thead>
<tr>
<th></th>
<th>Wireless Users</th>
<th>CR Users</th>
<th>Algorithm User</th>
<th>Revenue</th>
<th>Cumulative Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun-00</td>
<td>97</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-01</td>
<td>118</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-02</td>
<td>134</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-03</td>
<td>148</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-04</td>
<td>169</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-05</td>
<td>194</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-06</td>
<td>219</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-07</td>
<td>243</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-08</td>
<td>262</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jun-09</td>
<td>270</td>
<td>0.270</td>
<td>0.054</td>
<td>0.540</td>
<td>0.540</td>
</tr>
<tr>
<td>Jun-10</td>
<td>299</td>
<td>0.299</td>
<td>0.060</td>
<td>0.599</td>
<td>1.139</td>
</tr>
<tr>
<td>Jun-11</td>
<td>320</td>
<td>0.320</td>
<td>0.064</td>
<td>0.640</td>
<td>1.779</td>
</tr>
<tr>
<td>Jun-12</td>
<td>341</td>
<td>0.341</td>
<td>0.068</td>
<td>0.681</td>
<td>2.460</td>
</tr>
<tr>
<td>Jun-13</td>
<td>361</td>
<td>0.361</td>
<td>0.072</td>
<td>0.723</td>
<td>3.183</td>
</tr>
<tr>
<td>Jun-14</td>
<td>382</td>
<td>0.382</td>
<td>0.076</td>
<td>0.764</td>
<td>3.946</td>
</tr>
<tr>
<td>Jun-15</td>
<td>402</td>
<td>0.402</td>
<td>0.080</td>
<td>0.805</td>
<td>4.751</td>
</tr>
</tbody>
</table>

Figure 8b: Number of wireless users from June 2000-2016
For our project, the estimated cost is:

<table>
<thead>
<tr>
<th>Year 2009 Expenses</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineer</td>
<td>240,000</td>
</tr>
<tr>
<td>Rent</td>
<td>100,000</td>
</tr>
<tr>
<td>Training</td>
<td>60,000</td>
</tr>
<tr>
<td>Attorney</td>
<td>100,000</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>200,000</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>100,000</td>
</tr>
<tr>
<td>Total</td>
<td>800,000</td>
</tr>
</tbody>
</table>

Table 3a: Expenses for our project in the year 2009

<table>
<thead>
<tr>
<th>Year to year expense estimate</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun-09</td>
<td>800000 800000</td>
</tr>
<tr>
<td>Jun-10</td>
<td>640000 1440000</td>
</tr>
<tr>
<td>Jun-11</td>
<td>512000 1952000</td>
</tr>
<tr>
<td>Jun-12</td>
<td>409600 2361600</td>
</tr>
<tr>
<td>Jun-13</td>
<td>327680 2689280</td>
</tr>
<tr>
<td>Jun-14</td>
<td>262144 2951424</td>
</tr>
<tr>
<td>Jun-15</td>
<td>209715 3161139</td>
</tr>
</tbody>
</table>

Table 3b: Estimate of our expenses for a period of next 6 years

Price point:

For over a period of 25 years, there are 276,610,560 wireless users. Out of this number, if 0.1% users use the Cognitive radio, then there will be approximately 2,766,100 users. In 2015, the number of users will be approximately 0.402 million users. Assuming 20% implement our algorithm, there will be approximately 553200 users. In 2015, the number of users will be approximately 0.08 million users.

In 2009, if we charge $500/radio for each user and $10 royalty per radio for our algorithm, the total cost would be $553200×10= $0.552 million. In 2015, the total cost would be $0.805 million even if we did not increase our revenue for 5 years.
Personnel:
In order to complete our project we are working in a group of three who are Network Engineers.

Business & Revenue Model: We plan to sell our algorithm to those unlicensed users who want to use the frequency spectrum without causing any interference to the licensed users and we charge $500/ radio for each user and $10 royalty per radio for our algorithm

Exit strategy:
So, our Return on Investment is on June 2012.

ROI is calculated by the ratio of the difference of the value of final investment \( V_f \) and value of initial investment \( V_i \) to the value of initial investment \( V_i \) i.e.

\[
ROI = \frac{V_f - V_i}{V_i} \quad \text{(Wikipedia, 2010)}
\]

<table>
<thead>
<tr>
<th>Cumulative Expense</th>
<th>Cumulative Revenue</th>
<th>Cumulative ROI (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun-09</td>
<td>800000</td>
<td>540000</td>
</tr>
<tr>
<td>Jun-10</td>
<td>1440000</td>
<td>1138800</td>
</tr>
<tr>
<td>Jun-11</td>
<td>1952000</td>
<td>1778836</td>
</tr>
<tr>
<td>Jun-12</td>
<td>2464000</td>
<td>2460109</td>
</tr>
<tr>
<td>Jun-13</td>
<td>2976000</td>
<td>3182618</td>
</tr>
<tr>
<td>Jun-14</td>
<td>3488000</td>
<td>3946364</td>
</tr>
<tr>
<td>Jun-15</td>
<td>4000000</td>
<td>4751345</td>
</tr>
</tbody>
</table>

Table 3c: Estimate of our ROI for a period of next 6 years
Figure 8c: ROI Graph
9. Top institutes for research in cognitive radio in the United State of America

Cognitive radio is one of the emerging technologies for mitigating an apparent spectrum scarcity problem. Several groups in various research universities have focused extensive research in the field of cognitive radio.

1. Massachusetts Institute of Technology, Cambridge, CA
2. Stanford University, Stanford, CA
3. University of California, Berkeley, CA
4. University of California, Davis, CA
5. University of Kansas, Lawrence, KS
6. Virginia Polytechnic Institute and State University, Blacksburg, VA
7. University of Maryland, College Park, MD
8. University of Texas, Dallas, TX
9. Georgia Institute of Technology, Atlanta, GA
10. University of Central Florida, Orlando, FL
11. University of South Florida, Tampa, FL
12. Worcester Polytechnic Institute, Worcester, MA
10. Project Schedule

Below figure indicates the schedule for phase one of our project for the term August 09 to November 09

Figure 9a: Project Phase 1 Gantt chart
Below figure indicates the schedule for phase two of our project for the term January 10 to April 10.

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Duration</th>
<th>Start</th>
<th>Finish</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economic analysis</td>
<td>28 days</td>
<td>Thu 1/28/10</td>
<td>Fri 3/6/10</td>
</tr>
<tr>
<td>Mathematical Analysis</td>
<td>24 days</td>
<td>Wed 2/10/10</td>
<td>Fri 3/12/10</td>
</tr>
<tr>
<td>Matlab simulation</td>
<td>37 days</td>
<td>Fri 1/29/10</td>
<td>Sun 3/21/10</td>
</tr>
<tr>
<td>Project Progress Report</td>
<td>6 days</td>
<td>Fri 2/26/10</td>
<td>Fri 3/6/10</td>
</tr>
<tr>
<td>Error Detection</td>
<td>3 days</td>
<td>Fri 3/19/10</td>
<td>Tue 3/23/10</td>
</tr>
<tr>
<td>Error Correction</td>
<td>2 days</td>
<td>Tue 3/23/10</td>
<td>Wed 3/24/10</td>
</tr>
<tr>
<td>Final testing</td>
<td>8 days</td>
<td>Thu 3/25/10</td>
<td>Mon 4/5/10</td>
</tr>
<tr>
<td>Recheck for errors</td>
<td>3 days</td>
<td>Mon 4/5/10</td>
<td>Wed 4/7/10</td>
</tr>
<tr>
<td>Draft Report</td>
<td>35 days</td>
<td>Fri 2/19/10</td>
<td>Wed 4/7/10</td>
</tr>
<tr>
<td>Project Report-1</td>
<td>3 days</td>
<td>Wed 4/7/10</td>
<td>Fri 4/9/10</td>
</tr>
<tr>
<td>Review by the committee</td>
<td>6 days</td>
<td>Fri 4/9/10</td>
<td>Fri 4/16/10</td>
</tr>
<tr>
<td>Final Project Report-2</td>
<td>3 days</td>
<td>Mon 4/19/10</td>
<td>Wed 4/21/10</td>
</tr>
<tr>
<td>Final Project presentation</td>
<td>1 day</td>
<td>Fri 4/23/10</td>
<td>Fri 4/23/10</td>
</tr>
</tbody>
</table>

**Figure 9b: Project Phase 2 Gantt chart**
11. Team and Committee Members

Below is the introduction to our project team and the committee members.

11.1 Project Team:

Junu Shrestha
- Currently, she is pursuing her MSE degree concentrating in Networking at San Jose State University.
- She focused on dynamic spectrum access and trust evaluation of the cognitive radios.

Avinash Sunkara
- Currently, he is pursuing his MSE degree concentrating in Networking at San Jose State University.
- He focused on security threats in cognitive radios.

Balaji Thirunavukkarasu
- Currently, he is pursuing his MSE degree concentrating in Networking at San Jose State University.
- He worked on Literature Survey and project documentation.

11.2 Project Committee:

Dr. Rakesh Rajbanshi (Industry Sponsor)

Background: Currently he is working at Cisco Systems, Inc. He completed his Ph.D. degree in Electrical Engineering with honours in 2007 from University of Kansas. His Ph.D. research focused on OFDM-Based Cognitive Radio for DSA Networks.
Responsibilities: He reviewed the team work and guides the team by sharing his knowledge and expertise in wireless communication. He will review the technical content in the report and suggest necessary changes.

Prof. Morris Jones (Faculty Reader)

Background: Currently he is working as a part-time faculty in Electrical Engineering department at San Jose State University. His past experience includes many years in Intel Corp. and Chips and Technologies. He received his MSEE degree from Brigham Young University.

Responsibilities: He reviewed the report and make sure that the report meets the university standards for a Masters Project.
12. Conclusion

The Cognitive Radio provides an efficient solution to the spectrum scarcity problem by sensing the unused spectrum of the licensed users and providing that unused spectrum to the secondary users without causing any interference between primary user and the secondary user. Cognitive radio increases the efficiency of the spectrum significantly. But the secondary user must make sure that the information regarding the occupancy of the spectrum is provided by a legitimate primary user. Thus we can conclude that our algorithm is an efficient technique to authenticate the legitimate primary user. Also, from the economic analysis we can conclude that the break-even will occur after two years from the date of our product launch. The Return on Investment will be achieved in June 2012. The combined analysis specifies that our approach will be a great success.
13. References


Appendix

(i) Power Plot:

clear all;
close all;
clc

% Plot it for various SNR_dB

SNR_dB=30; % SNR in dB
SNR = 10.^(SNR_dB/10); % SNR in real value
distance=0:0.005:5;
N2=1
tx_signal_power=1; % original transmit power without noise

noise_power = tx_signal_power/SNR;

% for dd =0:10
rx_signal_power=[];
for ii=1:length(distance)
d=distance(ii);
    noise_signal=sqrt(noise_power) * randn(1,N2); % assume Gaussian Noise
    tx_signal = sqrt(tx_signal_power) * randsrc(1,N2); % transmitted signal
    rx_signal = tx_signal + noise_signal; % received signal

    rx_signal_power=[rx_signal_power (mean((rx_signal).^2))./(d.^4)]; % actual received signal power over actual distance d1
end

rx_signal_power_ideal = (mean((tx_signal).^2))./(distance.^4);

rx_signal_power_dB=10*log(rx_signal_power);
rx_signal_power_ideal_dB=10*log(rx_signal_power_ideal);
figure(1);
plot(distance,rx_signal_power_ideal_dB,'-',distance,rx_signal_power_dB)
legend('Ideal Received Signal Power','Actual Received Signal Power','Location','NorthEast');
grid on;
% title ('False Detection');
% title ('Trustworthiness of a Primary User');
xlabel ('Distance');
ylabel ('Received Signal Power (in dB)');
axis([min(distance) max(distance) -150 100]);
titletext=['SNR = ',num2str(SNR_dB),' dB'];
title(titletext);
(ii) Primary Trustworthiness:

clc;
clear all;
close all;

n1= 1; % number of primary users
n2= 10; % number of secondary users
N2=50000 % number of samples

% coordinate of cognitive radio
x=0.5;
y=0.5; % me

% gain of the wireless channel
% gain=1;
%
% x1 =1.5
% y1 =1.5

x1=rand(1,n1) % primary users x coordinate
y1=rand(1,n1) % primary users y coordinate
%
% distance of the cognitive radio from the primary user
d_coordinate=sqrt((x-x1).^2+(y-y1).^2)
%

SNR_db_all= -10:5:50; % SNR in decibel
trustworthiness = zeros(1,length(SNR_db_all));

for ii=1:length(SNR_db_all)
    SNR_db=SNR_db_all(ii); % SNR in dB
    SNR = 10.^(SNR_db/10); % SNR in real value
    tx_signal_power=1; % original transmit power without noise

    noise_power = tx_signal_power/SNR;

    noise_signal=sqrt(noise_power) * randn(1,N2); % assume Gaussian Noise

    tx_signal = sqrt(tx_signal_power); % transmitted signal
    rx_signal = tx_signal + noise_signal; % received signal

    rx_signal_power= ((rx_signal).^2)/(d_coordinate^4); % actual received signal power over actual distance d1

    d_power=(tx_signal_power./rx_signal_power).^(1/4); % calculated distance based on received signal power

    trust_iteration = min(d_coordinate./d_power, d_power./d_coordinate); % trustworthiness based on power
trustworthiness(ii)=mean(trust_iteration);
end

% trustworthiness
plot(SNR_dB_all,trustworthiness);
grid on;
title ('Trustworthiness of a Primary User');
xlabel ('SNR_{dB}');
ylabel ('Trustworthiness');
axis([min(SNR_dB_all) max(SNR_dB_all) 0.6 1]);
(iii) Malicious Trustworthiness:

clc;
clear all;
close all;

% n1= 1; % number of primary users
n2= 10; % number of secondary users
N2=50000 % number of samples

% % coordinate of cognitive radio
% x=0.5;
% y=0.5; % me
NN=100;

x_all = -1+2*rand(1,NN); % primary users x coordinate
y_all = -1+2*rand(1,NN); % primary users y coordinate
x1_all = -1+2*rand(1,NN); % primary users x coordinate
y1_all = -1+2*rand(1,NN); % primary users y coordinate
x2_all = -1+2*rand(1,NN); % malicious users x coordinate
y2_all = -1+2*rand(1,NN); % malicious users y coordinate

mean_error = sqrt((sum((x1_all-x2_all).^2 + (y1_all-y2_all).^2)))

SNR_dB_all= -10:5:50; % SNR in decibel
trustworthiness2=[];

for iteration = 1:NN
    iteration
    x = x_all(iteration);
    y = y_all(iteration);
    x1 = x1_all(iteration);
    y1 = y1_all(iteration);
    x2 = x2_all(iteration);
    y2 = y2_all(iteration);
    % distance of the cognitive radio from the primary user
    d_coordinate=sqrt((x-x1).^2+(y-y1).^2);
    % distance of the cognitive radio from the malicious user
    d_actual=sqrt((x-x2).^2+(y-y2).^2);
    trustworthiness = zeros(1,length(SNR_dB_all));
    for ii=1:length(SNR_dB_all)
        SNR_dB=SNR_dB_all(ii); % SNR in dB
        SNR = 10.^(SNR_dB/10); % SNR in real value
        tx_signal_power=1; % original transmit power without noise
        noise_power = tx_signal_power/SNR;
    end
end
noise_signal = sqrt(noise_power) * randn(1,N2);  % assume Gaussian noise

tx_signal = sqrt(tx_signal_power) * randsrc(1,N2);  % transmitted signal

rx_signal = tx_signal + noise_signal;  % received signal

rx_signal_power = ((rx_signal).^2)/d_actual^4;  % actual received signal power over actual distance d1

d_power = (tx_signal_power / rx_signal_power)^((1/4));  % calculated distance based on received signal power

trust_iteration = min(d_coordinate./d_power, d_power./d_coordinate);  % trustworthiness based on power

trustworthiness(ii) = mean(trustIteration);
end

trustworthiness2 = [trustworthiness2; trustworthiness];
end

plot(SNR_dB_all, mean(trustworthiness2, 1));
grid on;
title ('Trustworthiness of a Malicious User');
% title ('Trustworthiness of a Primary User');
xlabel ('SNR_{dB}');
ylabel ('Trustworthiness');
axis([min(SNR_dB_all) max(SNR_dB_all) 0.5 1]);
(iv) Correct Detection:

clc;
clear all;
close all;

% Plot it for Different Penalty Factors

SNR_dB_all= -10:5:50; % SNR in decibel
Trustworthy = [0.6248, 0.6881, 0.7237, 0.7902, 0.8783, 0.9315, 0.9611, 0.9779, 0.9875, 0.9929, 0.9960, 0.9978, 0.9987];

Untrustworthy = [0.5092, 0.5387, 0.5525, 0.5736, 0.5980, 0.6054, 0.6075, 0.6081, 0.6082, 0.6082, 0.6082, 0.6082, 0.6082];

occupied = 1;
not_occupied = -1;

N=100;
N2=2000;
n=4 % Penalty Factor

Trust_users = 1:N;
Malicious_users = 1:N2;
detection =[];
detection2=[];

% tipping_point2=[];
for jj=1:13
    tipping_point=[];
    for ii=1:N
        detection = (Trustworthy(jj).^n)*Trust_users(ii) * occupied +
        (Untrustworthy(jj).^n).*Malicious_users * not_occupied;
        false_decision = find([detection<0]);
        tipping_point = [tipping_point false_decision(1)];
    end
    detection2=[detection2; detection];
end
% tipping_point2
% tipping_point2=[tipping_point2; tipping_point];

figure(1);

% line_type=['-' ':' '-.' '--' 'b' 'g' 'r' 'c' 'm' 'y' 'd' '.b' '.g'];
% for jj=1:13
%     plot(Trust_users,tipping_point2(jj,:),line_type(jj));
%     legend('SNR_{dB}=')
%     hold on;
% end
plot(Trust_users,tipping_point2(1,:), 'r', Trust_users,tipping_point2(2,:), 'b',
    Trust_users,tipping_point2(3,:), 'k', Trust_users,tipping_point2(4,:), '-.r',
    Trust_users,tipping_point2(5,:), '-.b', Trust_users,tipping_point2(6,:), '-.
SNR_{dB}=-10,'SNR_{dB}=-5', 'SNR_{dB}=0', 'SNR_{dB}=5', 'SNR_{dB}=10', 'SNR_{dB}=15', 'SNR_{dB}=20', 'SNR_{dB}=25', 'SNR_{dB}=30', 'SNR_{dB}=35', 'SNR_{dB}=40', 'SNR_{dB}=45', 'SNR_{dB}=50', 'Location','NorthEastOutside');

SNR_{dB} \text{ all}= -10:5:50; % SNR in decibel
Trustworthy = [0.6248, 0.6881, 0.7237, 0.7902, 0.8783, 0.9315, 0.9611, 0.9779, 0.9875, 0.9929, 0.9960, 0.9978, 0.9987];

Untrustworthy = [0.5092, 0.5387, 0.5525, 0.5736, 0.5980, 0.6054, 0.6075, 0.6081, 0.6082, 0.6082, 0.6082, 0.6082, 0.6082];

figure(2)

plot(SNR_{dB} \text{ all}, Trustworthy, '-ok', SNR_{dB} \text{ all}, Untrustworthy, '*-b');
legend('Primary User', 'Malicious User');
grid on;
title('Trustworthiness of a User');
xlabel('SNR_{dB}');
ylabel('Trustworthiness');
axis([\text{min}(SNR_{dB} \text{ all}) \text{ max}(SNR_{dB} \text{ all}) 0.5 1]);