Reliable Communication in Cognitive Radio Networks

by

Hossna Shirshekar

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF APPLIED SCIENCE

in

The Faculty of Graduate and Postdoctoral Studies

(Electrical and Computer Engineering)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

August 2013

©Hossna Shirshekar 2013
Abstract

The emergence of new wireless applications has driven increased demand for radio spectrum and therefore, the fixed spectrum assignment approach cannot efficiently utilize the radio spectrum. On the other side, several researches show that there are many parts of the licensed spectrum bands that are left unused most of the time. To address the problem of limited spectrum resources and underutilization of the radio spectrum resource, cognitive radio was used to make it possible for secondary users to opportunistically access the underutilized radio spectrum bands. However, in comparison with the general wireless network, cognitive radio technology gives invaders more possibilities to influence the wireless networks. This makes it more challenging to guarantee reliable communication in cognitive radio networks.

In this thesis, first we describe the cognitive radio, cognitive radio networks, and security threats in these networks. Then the concepts of spectrum sensing as well as cooperative spectrum sensing are presented.

There are two important kinds of security threats in the cognitive radio networks, which have attracted considerable attention in the literature. The first kind of threat which is called primary user mimicry invasion includes the cognitive radios or some outsiders that try to emulate the primary user’s signal characteristics in order to interrupt the spectrum sensing process. In the second kind of invasion, known as spectrum sensing data distortion invasion, the disruption of the spectrum sensing process is caused by those cognitive radios that send false data to the fusion center.
Primary user mimicry invasion and spectrum sensing data distortion invasion have been majorly focused on in the past researches. Considering the significance of these two kinds of security threats in the ways in which they have disturbing effects on the overall performance of the cognitive radio networks, I focus my research work on these two kinds of threats. Then I provide a survey of the state of the art detection and mitigation techniques against them. The shortcomings associated with some of these detection and mitigation techniques are also investigated, which can be used as starting points for future researches.
Preface

This thesis is original, unpublished, independent work by the author, Hossna Shirshekar.
# Table of Contents

Abstract........................................................................................................................................... ii
Preface ................................................................................................................................................ iv
Table of Contents .............................................................................................................................. v
List of Tables ....................................................................................................................................... vii
List of Figures ..................................................................................................................................... viii
List of Abbreviations ........................................................................................................................ ix
Acknowledgments ............................................................................................................................ xi
1  Introduction ...................................................................................................................................... 1
   1.1 Overview and Motivation ............................................................................................................ 1
   1.2 Thesis Organization .................................................................................................................... 4
2  Cognitive Radio Technology .......................................................................................................... 5
   2.1 Cognitive Radio .......................................................................................................................... 5
   2.2 Cognitive Radio Network .......................................................................................................... 8
      2.2.1 Spectrum Sensing in Cognitive Radio Networks ................................................................. 10
      2.2.2 Ensuring Trustworthy Communication in Cognitive Radio Networks ................................. 15
      2.2.3 Techniques for Analyzing Reliability of Cognitive Radio Networks ................................. 17
3  Classification of Disturbing Activities in Cognitive Radio Networks ...................................... 21
   3.1 Disturbing Cognitive Radio Networks by Emulating Primary Users ........................................ 22
   3.2 Disturbing Cognitive Radio Networks by Interrupting Spectrum Sensing Process ................. 23
   3.3 Other Kinds of Disturbing Activities in Cognitive Radio Networks ........................................ 24
      3.3.1 Objective Function Invasion ............................................................................................ 24
      3.3.2 Jamming Invasion ............................................................................................................. 25
      3.3.3 Hello Flood Invasion ...................................................................................................... 25
      3.3.4 Sybil Invasion ................................................................................................................. 25
      3.3.5 Lion Invasion .................................................................................................................. 25
4  Techniques for Mitigating Disturbing Activities in Cognitive Radio Network ........................... 26
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Mitigation of Primary User Mimicry Invasions</td>
<td>26</td>
</tr>
<tr>
<td>4.2 Mitigation of Spectrum Sensing Data Distortion Invasions</td>
<td>39</td>
</tr>
<tr>
<td>4.3 Mitigation of Different kinds of Invasions</td>
<td>53</td>
</tr>
<tr>
<td>5 Conclusion and Future Work</td>
<td>56</td>
</tr>
<tr>
<td>Bibliography</td>
<td>58</td>
</tr>
</tbody>
</table>
List of Tables

Table 4.1: Summary of discussed mitigation techniques against PUMIs .................................35

Table 4.2: Summary of discussed mitigation techniques against SSDDIs .................................49
List of Figures

Figure 2.1: Classification of SS methods in CRNs .................................................. 11

Figure 2.2: Classification of CSS based on the schemes CRs use for sharing the sensed data in CRN .................................................................................................................. 15

Figure 2.3: Taxonomy of methods for analyzing security in CRNs............................. 17

Figure 3.1: Classification of various security threats for each layer of OSI model......... 21
List of Abbreviations

ANN      Artificial Neural Network
AWGN     Additive White Gaussian Noise
CR       Cognitive Radio
CRN      Cognitive Radio Network
CSS      Cooperative Spectrum Sensing
DSA      Dynamic Spectrum Access
EWSPRT   Enhanced Weighted Sequential Probability Ratio Test
EWSZOT   Enhanced Weighted Sequential Zero One Test
FCC      Federal Communication Commission
FC       Fusion Center
FDOA     Frequency Difference Of Arrival
KNN      K-Nearest Neighbor
MDV      Markov Decision Process
MU       Malicious User
MAC layer Medium Access Control layer
NPCHT    Neyman Pearson Composite Hypothesis Test
OSI      Open System Interconnection
PDF      Probability Distribution Function
PF       Probability of False Alarm
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMD</td>
<td>Probability of Missed Detection</td>
</tr>
<tr>
<td>PN</td>
<td>Primary Network</td>
</tr>
<tr>
<td>PU</td>
<td>Primary User</td>
</tr>
<tr>
<td>PUMI</td>
<td>Primary User Mimicry Invasion</td>
</tr>
<tr>
<td>SDR</td>
<td>Software Defined Radio</td>
</tr>
<tr>
<td>SH</td>
<td>Spectrum Hole</td>
</tr>
<tr>
<td>SN</td>
<td>Secondary Network</td>
</tr>
<tr>
<td>SS</td>
<td>Spectrum Sensing</td>
</tr>
<tr>
<td>SSDDI</td>
<td>Spectrum Sensing Data Distortion Invasion</td>
</tr>
<tr>
<td>SVDD</td>
<td>Support Vector Data Description</td>
</tr>
<tr>
<td>SU</td>
<td>Secondary User</td>
</tr>
<tr>
<td>TDOA</td>
<td>Time Difference Of Arrival</td>
</tr>
<tr>
<td>3D-CTMC</td>
<td>Three Dimensional-Continuous Time Markov Chain</td>
</tr>
<tr>
<td>WSPRT</td>
<td>Weighted Sequential Probability Ratio Test</td>
</tr>
</tbody>
</table>
Acknowledgments

First and foremost, I would like to thank God, the Almighty, for having made everything possible by giving me strength and courage to do this work. I would like to express my gratitude to Dr. Vijay Bhargava, my supervisor, for his detailed and constructive comments, and for his important support throughout this work. He taught me how to do intellectual research, and helped me think creatively and independently.

I have furthermore to thank Dr. David Michelson and Dr. Alireza Nojeh, my examination committee members, for their invaluable comments.

Last but not least, sincere thanks to my family, relatives and friends who all gave me courage and support. Without them none of my academic goals would have been possible.
Chapter 1

1 Introduction

1.1 Overview and Motivation

The actual propelling factor for developing cognitive radio (CR) and related concepts is the consumer’s desire for wireless access to the Internet and having more bandwidth. In providing the wireless service requirements of different users, radio spectrum is considered as an irrefutable limiting factor. Radio spectrum is a scarce and precious resource for wireless communication systems. The problem arose from the way in which we manage the spectrum. Allocating spectrum statically for particular types of service leads to the spectrum scarcity and underutilization of the electromagnetic radio resources. Although, assigning some bands of frequency to unlicensed users can solve the problem of spectrum scarcity to some extent, it cannot be a long term solution as the frequency bands become highly occupied and interferences will limit deployment of further CRs [1].

In order to make the wireless network capable of being scaled with demand, the federal communication commission (FCC) has made the opportunistic access of underutilized licensed spectrum possible to unlicensed operations. This access is conditioned on the fact
that the unlicensed users don’t cause significant interference to the licensed users. This is what is called dynamic spectrum access (DSA) [2].

The realization of the DSA is possible through the application of CR technology. CR is an enabling technology for DSA that has the capability to sense and understand the environment and proactively change its mode of operation as needed. It uses software to measure unused portions of the wireless spectrum and adapts the radio’s operating characteristics to operate in these unused portions in a way to cause no or minimal interference to other devices [3].

In DSA networks, we can categorize the users as either the primary users (PUs) who can access the spectrum bands at any time, or the secondary users (SUs) who can only use the spectrum bands when they are not used by PUs. The SU must regularly monitor the bandwidth to see whether the PU has returned back or not. They have to leave the band immediately after the return of the PU. Finding the unused bands as well as leaving the band immediately upon the arrival of PU, both makes the spectrum sensing (SS) one of the most essential components of CR in DSA networks. Sensing the PU is difficult task due to the presence of variable path losses, fading and SU interference [4]. Therefore sensing is never completely reliable and will always produce some errors depending on the channel conditions between the primary transmitter and CR sensors. Depending upon the sensing system used, there is usually a trade-off between probability of missed detection (PMD) of PU signal and probability of false alarm (PF). The PMD is the probability of CR stating that
a PU is not present while the PU is actually using the spectrum and the PF is the probability of CR expressing that a PU is present when the spectrum is not being used by PU. The PMD will increase the interference to the PU caused by the CR system and the probability of false alarm will limit the throughput of the CR system.

Energy detection, matched filter, and cyclostationary detection are among several energy detection techniques that are used for detecting PU signal. Cooperative and distributed methods can also be considered as two major techniques for controlling the spectrum and making a decision about the presence of the PU’s signal.

Since the performance of a single user is limited due to the noise uncertainty, shadowing, and multipath effect, cooperative sensing has been suggested as an effective way to improve detection accuracy by taking advantage of the spatial and multi-user diversity [5].

Although application of cognitive radio networks (CRNs) can solve the problem of spectrum scarcity to a large extent, cognitive characteristics of them cause many more security threats apart from those found in wireless networks [6].

In addition to all kinds of security menaces present in the traditional wireless network, CRNs encounter some unique types of threats due to their cognitive properties. There are two important types of security menaces, which are linked to the SS. The first one is primary user mimicry invasion (PUMI), in which some malicious users (MUs) try to mimic the characteristics of the PU signals to prevent other users from utilizing specific bands of frequency. The second kind of invasion is called spectrum sensing data distortion invasion
(SSDDI), where malicious CRs send distorted sensed data to the FC in case of cooperative spectrum sensing.

In this thesis, we focus on these two types of invasion and provide analytical survey of the detection and mitigation techniques against these two types of invasions that are presented in the previous works in the field of security in CRNs. The shortcomings of these techniques have also been investigated.

1.2 Thesis Organization

The rest of the thesis is organized as follows. Chapter 2 studies the general concepts of cognitive radio, cognitive radio networks, and security issues in cognitive radio networks. Two main security threats for cognitive radio networks along with some other types of invasions are explained in Chapter 3. Consequently, we present state of the art counter measuring methods for mitigating these types of invasion in Chapter 4. Chapter 5 concludes the thesis.
Chapter 2

2 Cognitive Radio Technology

2.1 Cognitive Radio

To improve the management of the electromagnetic radio spectrum, whose usage is controlled by the government, the FCC published a report in this regard in November 2002 [7]. What seems very interesting in this report is the result that tells instead of focusing on the problem of spectrum scarcity, it is more essential to discover efficient ways of accessing the available bands. This is due to the fact that usually there are some frequency bands that are underutilized most of the time, some other bands are partly used, and the rest are overutilized. Therefore it seems logical to search for those bands of frequencies that are dedicated to the PUs but are underutilized at some geographical location or specific time. These underutilized bands are called spectrum holes (SHs). CR is a technology that is able to find these SH, make them available to SUs, and in this way can improve the spectrum exploitation [8].

The cognition is a combination of mental processes such as awareness, memory, learning, reasoning, problem solving, and decision making [8].
CR is a wireless communication system, which intelligently scans its surrounding and learns from outside environment. It then adopts itself to statistical changes in the incoming radio frequency (RF) by modifying its operating parameters, such as transmit power, carrier frequency, modulation technique, and operation bandwidth accordingly. The CR pursues two main aims by doing these actions. First, it attempts to efficiently utilize the electromagnetic radio spectrum resource in a way to maximize the utility function of the users in the network while causing least interference to PUs. Secondly, it tries to provide a reliable communication when and where demanded.

Another feature of CR that is very much related to its cognitive capability is its reconfigurability property. By reconfigurability we mean having the ability to change, modify, and update the operating parameters with any statistical variation in the input signal. Achieving this property is possible through the use of software defined radio (SDR), which is a communication system that enables the software implementation of hardware components, such as detectors, mixer, modulator and demodulator, on an embedded system or a personal computer [9].
The cognitive capability of the CR requires the following tasks [10]:

- Spectrum sensing: Detection of the spectrum holes based on the information of the available bands;
- Spectrum analysis: Evaluation of the characteristics of detected spectrum holes;
- Spectrum decision: Selection of the spectrum band based on the characteristics of the spectrum and requirements of the user.

Some of the reconfigurable parameters that enable CR to adapt to changing environment are as follows:

- Frequency of operation: Since cognitive radio is capable of varying its operating frequency, it can select the most appropriate frequency based on the information about the environment and start communication on that frequency.
- Modulation: CR can be reconfigured in a way that suits the requirements of user and satisfies channel statues.
- Transmit power: CR can be reconfigured in such a way that makes the diverse power requirements of different applications possible. This approach is made possible by employment of power control systems.
- Communication technology: CR can make various communication systems capable of working together.
2.2 Cognitive Radio Network

The term cognitive network was first introduced by Mitola in [11]. The CRN, which is also referring to the same notion, consists of several CRs that broaden the radio link specifications to the above layers’ tasks in open system interconnection (OSI) model. In order to be able to develop better communication protocols, it is necessary to delineate the CRN architecture. This architecture is composed of two bodies. The first one is the primary network (PN), which is a network infrastructure that has been dedicated specific spectrum bands. The cellular and TV broadcast networks are examples of this type of network. The PN consists of the following units [10]:

- **Primary user:** These users are given a license for operating in a specific band and this process of granting access admission is governed solely by primary central station. According to FCC [7] PUs don’t need to be modified or have any extra duties in order to stand along with the secondary user network and SUs should not cause any interference to the PUs’ operations.

- **Primary central station:** It is a fixed infrastructure, which also has given license for using specific spectrum band. Although this station doesn’t have capability of sharing spectrum with SUs, it should have legacy and SU protocols in order to give PN access to SUs.

The second part of the CRN architecture is the secondary network (SN). This network can only access the spectrum band in an opportunistic way and it is not given license for
operation in some specific band. The deployment of SN can be either as a fixed infrastructure network or in a form of ad hoc network. The SN consists of the following units [10]:

- Secondary users: No license is given to these users and therefore in order to become able to use the licensed spectrum bands, they have to take on some extra duties. The SUs can access secondary central station and other SUs through ad-hoc connection both on licensed and unlicensed spectrum bands. They can also access the primary central station on the license band.

- Secondary central station: It is a fixed infrastructure part of the network that possesses all capabilities of SUs. The communication between this station and SUs is provided by single hop connections. Then the SUs are connected to other networks through these one hop connections.

- Spectrum sharing manager: This central network has the responsibility of sharing electromagnetic spectrum among SNs. It can be attached to any SNs and make each SU network capable of working with other networks through controlling the spectrum information [12].
2.2.1 Spectrum Sensing in Cognitive Radio Networks

Detection of SHs is the main task of the SN. This task is done through SS process, which enables the CR to get adapted to the surrounding environment.

Detection of the primary signal based on the data obtained from nearby SUs is the most common technique of detecting SHs. As it is shown in Figure 2.1 the SS techniques can be broadly classified into:

- Non-cooperative detection
- Cooperative detection

It has to be mentioned that CRNs faces some limitations in the process of SS. These limitations include having no prior knowledge about the technologies that are using spectrum, bounded sensing time, and sensitivity to fading environment [13].

In the following sections, we describe the mostly used SS techniques in CRNs.
Non-Cooperative Detection

In the context of CRN there exist cases where no cooperation is allowed between SUs or only one terminal presents for sensing. Non-cooperative detection scheme uses the local observations of SUs to detect the weak signal from a primary transmitter [14]. Following expression defines the basic hypothesis model for non-cooperative detection [15]:

\[ x(t) = \begin{cases} 
  n(t), & H_0 \\
  hs(t) + n(t), & H_1
\end{cases} \]

Where \( x(t) \) is the received signal by SU, \( s(t) \) is the transmitted signal from PU, \( n(t) \) is the additive white Gaussian noise (AWGN) signal, and \( h \) is the channel amplitude gain. \( H_0 \) is a
null hypothesis that reports the absence of the PU signal in a specific band and $H_1$ is an alternative hypothesis that states the presence of some licensed user signal.

In principle, there are three non-cooperative SS schemes, i.e., energy detection [16], [17], matched filter detection [18], and cyclostationary feature detection [19].

**Energy Detection**

The most commonly used SS technique is the energy detection, which is based on the assumption that the energy of the signal to be detected is more than that of the noise signal. This scheme actually detects the primary signal based on the comparison of the received signal’s energy with a predefined threshold and without considering the characteristics of that signal [16], [20]. This inability to distinguish one signal type from other is considered as a drawback of this technique. Another problem associated with this technique is its susceptibility to noise power uncertainty [10].

**Matched Filter Detection**

Matched filter is the most favorable detection method in the stationary Gaussian noise environment conditioned on the fact that there exists some prior information about the PU signal, such as type and order of modulation, format of the packet, and pulse shape. The reason for being considered as the most desirable detection method is its ability to maximize the received signal-to-noise ratio [21] and capability of achieving high processing gain in short time [10].
Cyclostationary Feature Detection

The matched filter detection method needs prior knowledge about the PU signal, which is not always available to SUs. Therefore, it is required to search for a detection method which can work with limited knowledge of the transmitted signal. The cyclostationary feature detection is a technique that best suits this condition. This technique takes advantage of the periodicity property of signal, which is developed as a result of attaching sine wave carriers, repeating spreading, pulse trains, hopping sequences or cyclic prefixes to the modulated signals in order to differentiate the wide-sense stationary noise signal from the cyclostationary PU signal [19], [22], [23]. These modulated signals are considered cyclostationary due to the fact that their mean and autocorrelation show periodicity [10].

Robustness against noise power uncertainty is the property that enables the cyclostationary feature detection method to perform better than energy detection technique [24]. The main disadvantage of this method is its computational complexity and lengthy monitoring time.

Cooperative Detection

The performance of the SS process may be greatly deteriorated due to the multipath fading, shadowing, and hidden terminal issue. These problems can be dealt with by taking advantage of spatial diversity among distributed CRs. Instead of making decision based on the local observations, CRs can cooperate with each other and make a combined decision about the presence of PU signal at the sensed spectrum to improve the detection performance [13].
Based on the way that CRs share the sensed data in the CRN, the cooperative spectrum sensing (CSS) can be categorized into [13]:

- Centralized: In this type of CSS, the fusion center (FC) as a central entity controls the SS process. At the beginning, a frequency band of interest is selected by FC for sensing and all CRs are ordered to start local sensing process. After that all sensed data are sent to the FC through control channel. Then the FC decides on presence of the PUs’ signals based on the combined locally sensed data.

- Distributed: In this type of CSS, first each CR performs local sensing and shares this data with other user within its transmission range. Then each CR combines the received data from neighbors with its own data and decides on the presence of the PU based on its local rule. In case that the local rule is not satisfied, CRs again send their decision results to other CRs. This process is continued until the algorithm converges and a common cooperative decision is attained.

- Relay assisted: In the relay assisted CSS, the CRs having strong channels to the FC can be used as relays for forwarding other CRs’ sensing data.
2.2.2 Ensuring Trustworthy Communication in Cognitive Radio Networks

Any secure communication system, including CRN, needs to satisfy the following requirements [25]:

- Availability: This is the fundamental requirement of any kind of network, which is related to data availability. While availability refers to the availability of the airwave for transmission purposes in the context of wireless networks, it indicates the capability of primary or secondary users in accessing the spectrum in CRNs. To be specific, spectrum availability for PUs means having the ability to transmit in the licensed band without receiving harmful interference from SUs. On the other hand for
SUs, availability refers to the presence of bands of spectrum, in which the SUs can perform transmissions without causing harmful interference to the PUs.

- **Identification:** This basic security requirement associates a user with its identity.
- **Integrity:** The satisfaction of this requirement is necessary in order to make sure that the received data is exactly what has been sent by an authorized individual. This plays a more essential role in the wireless network which is more vulnerable to the attackers.
- **Confidentiality:** This security requirement guarantees that the transmitted data is transformed in such a way that is not apprehensible by an unauthorized user.
- **Authentication:** In order to confirm the communicating individual’s identity and authority, this security component is required.
- **Authorization:** There are different levels of authorization that are assigned according to network access control policy to the various individuals in the network.
- **Non-repudiation:** This component prevents both the sender and receiver from refusing a transmitted message.

In order to successfully deploy the CRNs and make best use of the advantages it brings, the application of the robust security mechanisms is necessary. Since the CR opportunistically accesses the electromagnetic spectrum and has to leave the spectrum band immediately after reappearance of the PU, new security threats are introduced to these CRNs in addition to those presented in traditional wireless networks [26]. Therefore, new detection and mitigation schemes have to be considered in these networks.
2.2.3 Techniques for Analyzing Reliability of Cognitive Radio Networks

In this section, we review game theory and data mining techniques as a tool for analyzing reliability in CRNs. Figure 2.3 shows the classification of these techniques.

Figure 2.3: Taxonomy of methods for analyzing security in CRNs
2.2.3.1 Game Theory

The planned interactions between multiple intelligent rational decision makers are studied using game theory. It provides the mathematical models for cooperation and conflict among these intelligent and rational decision makers [27].

The Theory of Games and Economic Behavior was the first book on game theory [28], which consists of the Von Neumann and Morgenstern’s criterion on the way of finding mutually consistent solutions for two persons zero-sum games. Cooperative game theory, which examines optimal tactics for groups of individual, then appeared during the late 1940s. In early 1950s, Nash equilibrium criterion was introduced by J. Nash, which characterizes mutually consistent players’ tactics. This criterion is considered more general than the Von Neumann and Morgenstern’s measure, since it can be applied to non-zero-sum games as well. Game theory has been known as an important tool in different disciplines such as computer science, engineering, biology, etc [29].

CRs utilize the dynamics of the sensed spectrum along with the adopted actions of other CRs to make smart decisions on spectrum usage and the operating parameters. On the other hand, there are some CRs who compete for spectrum resources without having any incentive to cooperate with other users. Therefore, it is advantageous to employ the game theory for examining the smart behaviors of the normal CRs and selfish interactions of the MUs [30].
2.2.3.2 Data Mining

As was mentioned before, SS, which consists of signal detection and modulation classification functions, is an important feature of the cognitive radio [31]. To facilitate the process of signal demodulation by CR, modulation classification function is used to identify the type of modulation scheme used by a given communication system.

There are different data mining techniques that can be used to classify the modulation schemes based on the features obtained from cyclostationary feature detection method. These techniques include artificial neural networks, support vector machine, k-nearest neighbor [32].

Artificial neural network (ANN) is a parallel distributed system made of neurons as its processing units. These units are interconnected by synaptic weights and the interaction between them gives intelligence to the network. The ANN as a mathematical model tries to find complex relationships in a set of data by getting inspired from biological neural network [33].

The principle of the structural minimization is implemented using a group of learning algorithms that is called support vector machine (SVM) [34]. The SVM classifier aims to find a hyperplane in a feature space in a way that the boundary between members of one class and another is at a maximum [35].
The k-nearest neighbor (KNN) is a member of lazy learning or instance based learning family [36] that classifies the objects based on the closest training data in the feature space. This method needs large computational effort since with each classification process a sweep in the training data is necessary [32].
In CRNs, any activity that attempts to have harmful effect on the performance of PUs or SUs, by causing interference to PUs or disturbing the opportunistic spectrum access of SUs, is considered as disturbing activity or invasion.

**Figure 3.1:** Classification of various security threats for each layer of OSI model

In this section first we discuss two important threats to CSS, namely primary user mimicry invasion (PUMI) and spectrum sensing data distortion invasion (SSDDI), which are the main focus of this thesis and then some other kinds of invasions associated with different layers of the open system interconnection (OSI) model of CRNs will be briefly explained.
3.1 Disturbing Cognitive Radio Networks by Emulating Primary Users

In order to make no or least interference to PUs, CRs have to leave a currently used spectrum bands once the PUs reappear and subsequently, the CRs have to look for different SHs for transmissions. This spectrum hand-off process usually causes deterioration in the performance of CRs. In adversarial wireless environment, enemy system may take advantage of this property of CR and modify the air interface to imitate a PU’s characteristics. In this manner, the enemy system can get peerless access to the specific spectrum band. In this work, the term PUMI is coined to refer to this kind of disturbing activity. In CRNs, there are two kinds of users that set up this type of invasion [37]:

- Egocentric users: these users urge other CRs to leave a specific spectrum band in order to take exclusive use of that band.
- Malicious users: these users prevent CRs from using unused SH.
3.2 Disturbing Cognitive Radio Networks by Interrupting Spectrum Sensing Process

There are some cases in which an invader sends false sensing data to the neighboring CRs or to the FC to bring them into making wrong decision about the presence of the PUs. This type of invasion, which is known as spectrum sensing data distortion invasion (SSDDI) or Byzantine invasion [25], targets both centralized and distributed CRNs. Although, in case of the centralized network the Byzantine invader can prevent CRs from using available spectrum bands or can cause interference to PUs by allowing usage of already occupied bands, FC usually can find some intelligent ways of detecting these invaders. On the other hand, in case of the distributed network it is more challenging to control the propagation of false data and SSDDI can cause more harm to this kind of network.

Generally, there are three kinds of Byzantine invaders in CRNs [6]:

- Egocentric users: These users try to take exclusive control of specific bands by falsely reporting the presence of PU on that particular band.

- Malicious users: these users make other CRs or the FC confused by sending false sensing data. They intend to mislead other CRs about the presence or absence of PUs in a way that causes free spectrum bands to be evacuated or results in harmful interference to PUs.
• Malfunctioning users: these users are neither egocentric nor malicious. Instead due to improper functioning of some software or hardware components, they report false information about the availability of the spectrum bands.

3.3 Other Kinds of Disturbing Activities in Cognitive Radio Networks

In this section we briefly explain some other important kinds of attacks on different layers of open systems interconnection (OSI) model [6].

3.3.1 Objective Function Invasion

CR has to adjust its operating parameters, such as carrier frequency, bandwidth, modulation type, and power, in order to fulfill specific requirements of the CRNs. The CR computes these parameters by solving some objective functions. In the process of finding the well-suited parameters, the invader can manipulate these parameters to achieve its ill purposes. This kind of invasion is known as objective function invasion and it usually happens at physical layer.
3.3.2 Jamming Invasion

A kind of denial of service invasion in which the invader deliberately sends signals to stop other CRs from using available services is jamming invasion. This type of invasion can be done in both physical and MAC (Media Access Control) layers.

3.3.3 Hello Flood Invasion

In CRNs, there exists some invader who tries to persuade other CRs that it is their neighbor by sending a broadcast message to all of them. This intruder is considered as hello flood invader.

3.3.4 Sybil Invasion

In Sybil invasion, a MU can form several forged IDs and in this way it makes the trust management or the reputation system used for detecting other invasions dysfunctional.

3.3.5 Lion Invasion

There is a kind of invasion that although it is carried out at the link layer but it intends to have negative impact on the transport layer. This disturbing action which is called lion invasion tries to force other CRs to do frequency handoff by emulating a PU transmission and therefore causes throughput degradation.
Chapter 4

4 Techniques for Mitigating Disturbing Activities in Cognitive Radio Networks

4.1 Mitigation of Primary User Mimicry Invasions

To the best of my knowledge, [38] is the first paper that began the discussion on the security issues of SS in CRNs. Based on the fact that the PU transmitters are placed at fixed locations, Chen et al have proposed a non-interactive location verification scheme in [38]. In this scheme, two location verification methods have been exploited. While the first one, namely the Distance Ratio Test method (DRT), utilizes the strength of the received signals at two different verifiers to examine the transmitter's location, the second technique, namely, Distance Difference Test (DDT), checks the phase difference between signals received by two verifiers to authenticate the transmitter.

According to FCC rules, opportunistic access to the radio spectrum should apply no variation to the primary system [7]. Therefore to verify the received signal and confirm that it belongs to the primary transmitter, Chen et al have suggested a FCC confirming scheme in [39], which uses estimated location of signal’s transmitter as well as its characteristics in order to authenticate the transmitter of the signal. This scheme takes advantage of a wireless
sensor network to senses the received signal from PU, and then applies local averaging smooth method to estimate the location of PU transmitter.

In [40] PUMIs are named as abnormal spectrum usage invasions that disturb the CRs from accessing the radio spectrum opportunistically. This paper is the first work that uses the combination of the data from physical and network layers to find the invader and determine its location. In particular, this work puts together the SS data provided from physical layer with the statistical multipath analysis from the network layer to get information about the utilization of spectrum and its abnormal usage.

Although there has been a considerable amount of work done on the defense against PUMIs, the first analytical model that finds the probability of PUMI based on energy detection was presented by Anand et al in [41]. They have used Fenton’s approximation and Markov inequality methods to find the probability of PUMIs and the lower limit on this probability, respectively. Next, Anand et al have continued their work in [42] and analyzed the detection of PUMIs using Wald’s sequential probability ratio test (WSPRT). First, they have used Fenton’s approximation to find the probability density function (PDF) of the received signal from the malicious users as well as primary transmitters, and then used these obtained PDFs to perform WSPRT.

Jin et al. have applied Neyman-Pearson composite hypothesis test (NPCHT) in addition to WSPRT at FC to detect PUMI in CRNs [43]. Using the NPCHT method, the CRs can minimize the probability of PUMI while keeping the PMD fixed. To put it simply, this
technique cannot minimize both of these probabilities at the same time. Therefore, WSPRT method is used to bring the advantage of providing simultaneous minimization of false alarm and misdetection probabilities. Taking more observations when making final decision, this method brings a better capability of lowering the PF compared to NPCHT technique.

Unlike the mechanisms discussed in [4],[5] that have used centralized SS, authors in [44] have applied distributed SS to detect PUMI. They first have modeled the power received by each CR using flexible log-normal sum approximation, which is presented by Wu et al in [45]. Then in order to detect the PUMI, they have proposed and applied an experiential based detection technique at each single CR. The data obtained from this local detection is then being broadcasted to nearby CRs so that they can compare it with their own detection information and make final decision based on this comparison. This collaborative decision making process has been used to better alleviate the PUMIs even in the presence of Byzantine invasions.

Authors in [46] have divided the mitigation mechanisms against PUMI into two classes. In the first one, the detection of PUMIs is based on the PU transmitter properties, while in the second class the channel properties are utilized in order to detect PUMIs.

As it was discussed in the earlier PUMI detection schemes, these methods are mostly based on the PU’s properties. To overcome the weaknesses of these detection techniques, for the cases of mobile CRNs or when PU and invader both send relatively same amount of
signal power, authors in [46] have utilized channel’s properties to distinguish the invader from PU. They believe it is difficult for the invader to mimic the properties of the channel and therefore they use the variance of the received signal power, which has undergone shadow fading, to authenticate the transmitter.

Yang et al. in [47] have discussed a situation when two invaders work together for doing the PUMI. To make the detection mechanism suggested in [46] ineffective, they control their transmission powers in such a way that emulation of channel properties would be possible for them. Next, the authors have stepped forward and suggested a detection technique, which is based on the cooperation of normal SUs.

In [48], Jin et al have first determined the received power at SU using flexible log-normal sum approximation. Then, in order to obtain the sensing result at each SU, they have proposed a local detection mechanism. The authors have derived the probability of fortunate PUMI at each SU to see the number of SUs affected by the invader. Using this data, the effect of the PUMI on the whole network has been studied. After that, Jin et al. have proposed a robust global spectrum decision method for centralized FC, to protect the network against PUMI. The effective of the proposed technique in alleviating the PUMI in the presence of Byzantine invasion has also been demonstrated.

When PUMI happens, the affected CRs should either use another spectrum band or leave the whole system if there is no free channel available for use. This may cause CRs’ incoming or ongoing calls to be rejected or dropped, respectively. Jin et al in [49] have studied the
effect of the PUMI on CRs’ call functioning in CRNs. In order to plan how the spectrum bands are used by honest, malicious, and primary users, they have suggested a three dimensional continuous time Markov chain (3D-CTMC). Using this plan, they have evaluated the possibility of call rejection or drop in the network that is influenced by PUMI. They have also shown the effectiveness of the suggested approaches, i.e. the techniques discussed in [44], [48], against PUMI in reducing the possibility of call rejection and drop in CRNs.

In a series of research works done by Li et al. [50-53], the defense strategies against PUMIs have been divided into two classes, namely proactive and passive approaches. In proactive approach, it is assumed that the invader is immobile and its transmission power is low compared to that of the PU. In this case the invader can be easily detected by computing its transmitted power. The defense techniques against PUMI that are proposed in [39] is example of this kind of approach. When these assumptions are no longer valid, passive approaches will be considered. In passive approach and when there are more than one channel in a CRN, CR has to smartly select a channel which is less frequently used by PUs, and at the same time it is less vulnerable to PUMIs [51]. On the other side, an invader also has to find the best strategy to block these good channels. Authors in [52] have investigated these two tactics using game and Markov decision process theories. In this work, on one hand, it is assumed that CR and invader have always some side information about the status of the channel and therefore the optimal plans of actions for them can be found using this
information. On the other hand, they have also considered that the invader has fixed and reasonable invading tactics. But in real systems, firstly, the channel statistics are usually unknown to both the invader and SU, and secondly the invader could be unreasonable and choose a random invading tactic.

Therefore in [53] Li et al. have continued their work in [52] and studied the cases, in which the CR defender and the invader both have no side information about the radio channel and the invader’s tactics are random. They have applied adversarial multi-armed bandit technique [54],[55], with each channel considered as a bandit arm, to fight against the PUMI in a condition of having no information about channel, invader’s tactic, and other CR defenders.

To overcome shortcomings associated with DRT and DDT, Huang et al. have taken advantages of both Time difference of arrival (TDOA) and frequency difference of arrival (FDOA) techniques in [56] to verify the location of the transmitter. TDOA and FDOA techniques are two positioning methods that are usually used for finding the location of a object without interacting with that.

Belief propagation technique uses local message exchanges to make an inference about some unknown issue [57]. Authors in [58] have taken advantage of this technique to estimate the location of the PUM invader. In this algorithm, each CR makes its belief about the location of the dubious transmitter based on repeated collaboration with the neighboring CRs. Ultimate decision about the invader will be made using the mean of all the CRs’ final
believes. Then the characteristics of the detected invader will be made available to all CRs in the network to prevent any future invasions. In this method, there is no need for hardware implementation of TDOA and FDOA techniques or for deploying wireless sensor network to identify the transmitter’s location and these are the advantage of the proposed scheme over the techniques that have been explained in [39], [20].

Yuan et al. have extended their work in [58] and considered more advanced system model as well as more complex complementary function for belief propagation algorithm in [59].

Liu et al [60] have suggested a FCC confirming method which takes advantage of both the received signal’s cryptographic signature as well as its radio channel characteristics to distinguish PUM invader from the PU transmitter. This PUMI detection method doesn’t directly interact with PU, but instead it deploys an assistant node near each PU and uses its cryptographic signature as well as its radio channel characteristics, to verify the PU transmitter. First it uses the received signal’s cryptographic signature to attest the assistant node, and then the proposed method exploits the channel characteristics of the assistant node, which very much resembles to those of PU, to verify the PU’s signal.

Authors in [61] have modeled a system, which uses cryptographic signature as well as radio channel characteristics, like the one explained in [60], for verification of the PU signal. The main difference between these two approaches comes from the assistant nodes’ locations, which are close to the SU network in the approach outlined in [61]. These assisted nodes perform two functions. First, they verify the PU signal and then disseminate
the information regarding the availability of the spectrum to the SUs. This system model allows us to have mobile CRNs as well as systems with less energy-consuming assisted nodes.

The first work that deals with the PUMI in CRNs with mobile PUs is presented by chen et al in [62]. First, they have classified the PUs in the TV bands into two groups. The first group consists of stationary PUs like TV towers and the second one includes mobile PUs such as wireless microphones. To verify the credibility of the mobile PUs, in this case microphones, they have proposed a detection technique that evaluates the correlation of the energy level of radio frequency signals to acoustic data received by each SU’s acoustic sensor.

The methodology developed in [62] have been expanded to the case of noisy environment in [63]. A noise alleviating technique, which takes advantage of cooperative sensing between SUs, has been added to the detection algorithm in [62] in order to detect PUMI in the noisy CRNs with mobile PUs.

Susceptibility to noise, having CRNs with only stationary users, and the demand for complex hardware and software systems are the limitations of the PUMI detection techniques that have been discussed in [39], [42], [60], [64]. Therefore, Pu et al have proposed a neural network based detection algorithm in [65], which can overcome these constraints to some extent. At the beginning, the energy detection technique is used to find the frequency being used by the user under investigation. Then, the receiver monitors and
files the signals from that particular user for a specific period of time. Subsequently, the artificial neural network will utilize cyclostationary features of signals in order to classify the users according to their modulation types and finally detect the MU.

Despite many advantages brought by [65] compared to [39], [42], [60],[64], this approach encounters shortcomings in two respects. First, the proposed approach doesn’t function properly in the case of having two signals with modulation schemes from same digital modulation class. Secondly, all signals’ modulation schemes should be known to the system before classifying the users. These problems have motivated Pu and Wyglinski to work further and propose a complementary approach that considers these issues [66]. They have applied video processing technique, similar to those used in [67], and [68] for action recognition, on the FFT sequences of the transmitted signals’ to identify the actions of the users in the CRN. Then, the NN have been employed to classify the users based on their actions.

Table 4.1 provides short review of the state of the art mitigation techniques against PUMIs. Following this table is a short analysis of these detection techniques.
<table>
<thead>
<tr>
<th>Citation no.</th>
<th>Does it interact with primary transmitter?</th>
<th>Awareness about the Location of the PU</th>
<th>Main Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>[38]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Invasion detection using transmitter verification scheme</td>
</tr>
<tr>
<td>[39]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Invasion Detection Using the location and characteristics of the signal</td>
</tr>
<tr>
<td>[40]</td>
<td>Non-interactive</td>
<td>unknown</td>
<td>Detection and localization of the invasion using data difference between physical and network layers</td>
</tr>
<tr>
<td>[41]</td>
<td>Non-interactive</td>
<td>known</td>
<td>First Analytical model that uses Markov inequality and Fenton’s approximation to find the probability of fortunate invasion and the lower limit on this probability in fading wireless environment</td>
</tr>
<tr>
<td>[42]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Using WSPRT to analytically study the detection of PUMI in CRN over fading channel</td>
</tr>
<tr>
<td>[43]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Using NPCHT and WSPRT to analytically study the detection of PUMI in CRN over fading channel and in the presence of multiple invaders</td>
</tr>
<tr>
<td>[44]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Distributed SS for the detection of PUMI</td>
</tr>
<tr>
<td>[46]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Introduction of an advanced PUMI and an advanced mitigation technique</td>
</tr>
<tr>
<td>[47]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Introduction of a potential cooperative invasion, in which two invaders mimic the channel parameter, and suggestion of its countermeasure method, which is based on cooperative decision of SUs</td>
</tr>
<tr>
<td>[48]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Suggestion of a robust local and global spectrum decision methods for mitigation of the PUMI</td>
</tr>
<tr>
<td>[49]</td>
<td>N/A</td>
<td>N/A</td>
<td>First analytical study about the effect of PUMI on SU’s call dropping and blocking</td>
</tr>
<tr>
<td>[52]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Investigation of the optimal channel selection tactic and invasion strategy using game theory and Markov decision while having side information about the radio channel and considering invader with fixed strategy</td>
</tr>
<tr>
<td>[53]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Defense against PUMI in dogfight using adversarial bandit problem when there is no side information about the radio channel and the invader’s tactics are random</td>
</tr>
<tr>
<td>Citation no.</td>
<td>Does it interact with primary transmitter?</td>
<td>Awareness about the Location of the PU</td>
<td>Main Contribution</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------</td>
<td>----------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>[56]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Application of TDOA and FDOA for mitigating the PUMI</td>
</tr>
<tr>
<td>[58]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Defense against PUMI using belief propagation method</td>
</tr>
<tr>
<td>[59]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Defense against PUMI using more advanced system model and belief propagation method than the model suggested in [58]</td>
</tr>
<tr>
<td>[60]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Detecting PUMI using received signal’s cryptographic signature as well as its radio channel characteristics with the help of assisted nodes deployed near PU</td>
</tr>
<tr>
<td>[61]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Detecting PUMI using received signal’s cryptographic signature as well as its radio channel characteristics with the help of assisted nodes deployed near SU network</td>
</tr>
<tr>
<td>[62]</td>
<td>Non-interactive</td>
<td>unknown</td>
<td>Detection of the PUMI in CRNs consisting of mobile PUs</td>
</tr>
<tr>
<td>[63]</td>
<td>Non-interactive</td>
<td>unknown</td>
<td>Detection of the PUMI in CRNs consisting of mobile PUs while considering noisy environment</td>
</tr>
<tr>
<td>[65]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Detection of PUMI using neural network based algorithm</td>
</tr>
<tr>
<td>[66]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Application of video processing technique to identify the actions of the CRN’s users and employing the NN to classify the users based on their actions</td>
</tr>
</tbody>
</table>

In [38] the performance of the DRT technique is highly affected by the radio propagation model, which by itself depends on many environmental factors. Therefore significant changes have to be applied to this technique in order to get accurate results. On the other hand, DDT method uses the fact that there is a relative phase difference between the signals received at two receivers locating at different distance from a single transmitter. Hence, it
requires tight synchronization among receivers, which brings additional implementation costs.

In the detection method proposed in [39], authors assumed the availability of the prior information about the location of the primary transmitter. This assumption is not always valid, especially in case of having mobile primary transmitters. The second issue regarding the suggested method is the deployment of separate sensor network for PUMI detection purpose. Although this sensor network can bring many advantages, such as saving the available recourses to CRN, it introduces additional implementation and maintenance expenses. This method also doesn’t consider cases where there are smart invaders capable of transmitting variable output power. Another problem with this method is the utilization of the received signal strength for authenticating primary signal, which can vary largely even within small geographical areas due to the transmitter and channel imperfections.

The method proposed in [40] is based on two assumptions. First, the SU and invader both consume same power for performing their processing activities. Secondly, the invader has smaller transmission range compared to primary transmitter. These assumptions are not true all the time, especially in case of having mobile user in the network.

In the work discussed in [42], using WSPRT as a hypothesis test method may cause infinite sampling and lengthy sensing times. The authors have also assumed that all the users in the network receives signal with the same PDF. This assumption is not true for the case of hostile environment.
In [43] the authors have compared the proposed detection method in [42], which is based on WSPRT, with the NPCHT based detection technique. The results show that the WSPRT performs better than NPCHT for the same threshold on the PMD. Considering enough distance between the SU and invader, in order to avoid SUs from receiving large power from MUs, and taking into account MUs with fixed transmission power are the limitations associated with the approach suggested in [43].

The drawback of the method proposed in [46] is the assumption of having knowledge of the location of the invader apriori, which doesn’t make sense in real applications.

The need to deploy expensive hardware to implement TDOA and FDOA, and considering many assumptions are the shortcomings of the approach discussed in [56].

The existence of the helper node near primary transmitter in [60] and close to SN in [61] introduces additional costs. The advantage of the approach outlined in [61] over the one explained in [60] is that in the former case low power helper nodes can be deployed.

In [62], [63] since the correlation between the RF signal and acoustic signal are used to detect invader, SUs have to be equipped with sound sensors.

Despite many advantages brought by cyclostationary based detection [65] for solving challenges regarding PUMI detection, there are some issues with this approach. First, it needs prior information about the modulation type of the signal. Secondly, it doesn’t give good result in case of having two users with modulation types from same modulation family.
4.2 Mitigation of Spectrum Sensing Data Distortion Invasions

To defeat Byzantine invasions in CRNs, Chen et al. have put their focus on the data fusion mechanism in [69]. They have first briefly explained some data fusion methods, namely, AND rule, OR rule, and Majority rule, Bayesian and Neyman-Pearson. These methods don’t consider the effect of sensing terminal background on decision making at FC and they also cannot control the PF and PMD. These two weaknesses have been considered as the main incentives for authors to propose a new credibility based fusion technique. This fusion technique, which presents a credibility based method into the sequential probability ratio test, is called weighted sequential probability ratio test (WSPRT). In this work, Chen et al have first assigned a credibility value to each sensing terminal based on its past reports. Then, this value has been taken into account for performing sequential probability ratio hypothesis test.

Authors in [70] have proposed two new schemes, enhanced weighted sequential probability ratio test (EWSPRT) and enhanced weighted sequential zero/one test (EWSZOT), which are powerful against SSDDI and achieve much less sampling numbers compared to WSPRT. The EWSPRT surpasses the WSPRT scheme by using the same test system as the one used in WSPRT method, but with having new weighting system. In case of EWSZOT scheme, both test and weight systems are modified relative to WSPRT in order to improve the overall performance.

Li and Han in [71] have proposed an algorithm which doesn’t require any antecedent information about the strategy of an invader. Instead, it utilizes a data mining inspired
technique, i.e. outlier detection, in order to discover the unconventional behavior of an invader and then block its data from being fused with other data at base station.

Authors in [72] have proposed a credibility-based defense technique against SSDDIs in cooperative CRNs. In this scheme, FC assigns a dubious level to each SU based on the degree of honesty it shows in reporting its sensed data. If the dubious level of some SU exceeds a predefined value, its reported data will be simply ignored when making final decision. In this approach, it is assumed that the decision making agent is aware of invasion strategies.

A smart invasion tactic is presented by Noon and Li in [73], which can withstand the defense technique discussed in [72]. In this invasion tactic, the invader can obtain knowledge about its dubious level and hence can switch between sincere and deceptive states. It keeps sending false data to FC as long as its dubious level doesn’t exceed a threshold value. Once the dubious level passes this value, the invader will quickly return back to the sincere state. This invasion tactic is analogous to the hit and escape scenario in the vehicle accidents. To mitigate this smart invasion strategy, Noon and Li have proposed a defense scheme in [73], which is inspired by the point mechanism of the department of motor vehicles in the US. In this scheme, demerit point is assigned to a SU whose dubious level surpasses the suspect threshold and these points are added up until it reaches rejection threshold. At this point, the SU whose accumulated points have passed the threshold value will be omitted from being involved in future decision making process.
In order to design CR systems, the aim is to improve unlicensed users’ spectrum access in a way that results in zero or no interference to primary users. Wang et al in [74] have looked at this goal as an optimization problem with quality of service requirements as limiting factors. They have then solved this nonlinear integer problem using numerical algorithms. The effects of system parameters, invasions and their countermeasures on the CR system performance have also been evaluated. Therefore this paper can be used as a reference when we study the security issues at the physical layer of cognitive radio networks.

To defense against SSDDIs, authors in [75], have proposed a method which calculate the dubious level of SUs based on the histories of their sensing reports. It then finds reliance and compatibility values of SUs to eliminate the decision of less reliable and compatible users in making final decision about the presence of the PU’s signal.

In [74], final decision at the FC is made using x-out-of-y rule. In this method, first y nodes are polled out of the total N nodes in the network. Then out of these data, the decision is made solely based on the sensing reports that come from x sensing nodes. However, for the large networks that are more reliable under SSDDI invasions, large computational complexity needed by exhaustive search makes optimal x-out-of-y rule infeasible. In order to overcome this computational complexity issue, authors in [76] have modified their work in [74] and proposed a suboptimal x-out-of-y method that takes advantage of the linear relation between the network size N and x, y parameters. In this way, the computational complexity has significantly been reduced.
To eliminate the destructive effect of MU in cooperative CRNs, Praveen et al in [77] have proposed detection schemes that find outlier users, which send data very different from the rest of the CRs’ sensing data. In these schemes, sensing data from different CRs are merged at FC using simple average combining scheme. In this paper, first an outlier detection technique is used to remove nodes that send data sorely different from other CRs’. Then a reliance factor is assigned to each user, which is used in average combining for making ultimate decision at FC. Praveen et al. have also shown that their proposed scheme works equally well, even when the sensed data are quantized before transmission.

In [78], Praveen et al. have continued their work in [77] by applying more powerful outlier detection methods. First, they have modified the way of calculating outlier factors. In the process of calculating the outlier factors, the received energy signals’ Biweight and Biweight scale are considered as powerful measures of distribution location and scale, respectively. They have proposed a detection method, in which at the end of each iteration the outlier factor of every user is compared with a predefined threshold and the users with outlier factors greater than the threshold will be considered as MUs. They have also suggested a method that can further improve the performance of the proposed detection scheme by having some side information about the PU’s activities. Considering a dynamic PU, which periodically switches between the transmission and idle states, any SU that doesn’t reflect this periodic behavior will be considered as a MU. Authors have also shown further improvement with the utilization of SU’s spatial information in the wide CRN.
In order to alleviate SSDDI invasions in cooperative CRNs, Chen et al have proposed a two-stage fusion scheme in [79]. In this scheme for making final decision, the FC implements a data combining mechanism, which takes advantage of node’s geographical information along with the data sent from that node. Although cooperative sensing can be done in two ways, i.e., centralized and distributed, this paper has chosen the first method because the centralized spectrum sending can provide more accurate result compared to distributed one. They have provided the detailed analysis of their work in [80].

In [81], Marano et al have analyzed the impact of Byzantine invasions on the distributed detection in the wireless sensor networks. In order to counter the Byzantine invasion in CRNs, authors in [82] have been inspired from the result obtained from the analysis done in [81]. First, they have analyzed the effect of the autonomous as well as cooperative Byzantine invasions on the performance of distributed detection in the CRNs. It has been shown that when the number of invaders exceeds some limit, FC becomes totally non-operational in detecting invaders. Then, they have proposed an efficient and fast method to mitigate the Byzantine invasions. This method counts the mismatches between local decisions and the global decision at the FC over a time window to remove the Byzantine invaders from the data fusion process. This work has also taken advantage of minimax theorem, which is a standard used in game theory for selecting a strategy that minimizes the maximum loss, to find the optimal approaches for the invader as well as the FC.
To confront the Byzantine invasions, authors of [83] have proposed a credibility-based scheme, in which the decisions from users with small credibility values will be ignored in making final decision. In this scheme, first the SS process is divided into small time intervals. Then, the local decision made by each CR is compared with the one made at FC for each time interval and based on this comparison the FC assigns a credibility value to each CR. The number of times there is inconsistency between the local and global decisions is used for assigning credibility value to each user.

Li and Han have proposed a detection scheme in [84], which is based on the data mining techniques for anomaly detection described in [85]. Unlike most of the works on detection of SSDDIs in cooperative CRNs which require prior knowledge of the invasion tactics, this detection scheme doesn’t require any information about the invader. It records the history of each SU’s sensing report. Based on these reports, it selects the users whose reports histories are very similar to or very different from the rest of the SUs’ reports and then considers them as MUs. The authors have analyzed the performance of their proposed detection technique in the presence of single invader. They have considered two scenarios. In the first scenario, the invader is assumed to be unaware of other SUs’ sensing reports. However, in the second scenario the invader waits for other SUs to send their sensed data and then according to those data it will form its report. It has been shown that while in the first case the invader can ultimately be detected, it can hide itself from being detected in the second case. In order to
show how well the proposed detection technique works for the case of multiple invaders, authors have performed some numerical simulations and presented the results.

In [86], the authors have suggested a reputation based algorithm, which doesn’t require any preceding information about the invaders’ tactics. In this algorithm, the FC collects the sensing data from all SUs and keeps history of these data for some specific time window. Then using this information and the reputation of each SU, they have employed a medoid based clustering technique to divide the CRN into different clusters of SUs. In each cluster, the local decision is made based on each member’s sensed data, where the influence of each SU’s data is weighted by its distance from the median of that cluster. After all, the final decision is made at the FC by applying majority voting on the clusters. In this recursive algorithm, the creation of new clusters and updating of SUs’ reputations are done on the basis of the final decision. This paper has evaluated the performance of the proposed algorithm in the presence of both independent and collaborative invasions.

To detect the MUs and mitigate their effect on the detection performance, Arshad in [87] has proposed an algorithm which is based on the maximum normal residual test. Maximum normal residual test is a well-known detection test for finding an outlier in a data that is normally distributed [88]. Author in [87] has proposed an improved version of this test, in which the detection of multiple outliers has been considered in the cooperative SS process.

Kalamkar et al have proposed a cooperative SS mechanism in [89], which can detect only one MU by applying a Dixon based [90] outlier detection technique. Then, they have
compared the performance of the proposed technique to that of maximum normed residual
test and boxplot based [91] outlier detection techniques and shown the superiority of the
Dixon based technique over those two methods. It has also been shown that this technique
have some shortcomings in case of having multiple MUs.

Most of the approaches for detecting MU in cooperative CRNs only consider three types of
MU, namely, MUs giving fallacious values greatly above or greatly below the threshold and
once in a while greatly above threshold. Unlike these approaches, authors in [92] have not
only considered these MUs but have also taken into account the effect of those that send
fallacious values marginally above, or below the threshold or send random incorrect values.
After detecting these MUs, they have proposed a comparison based method for alleviating
their detrimental effect on the SS process. In this method, the FC compares the local decision
of each node with the global decision and makes the final decision based on this comparison.

To alleviate SSDDIs, Farmani et al in [93] have proposed a mechanism which utilizes the
support vector data description (SVDD) during SS procedure. SVDD is a sort of one-class
classifier that is inspired by the support vector classifier and tries to make a spherical
perimeter around the target data [94]. These SVDD decision perimeters are known as support
vectors. In the proposed algorithm by Farmani et al, the sensed data are collected from all
SUs and then the MUs are found using SVDD algorithm. In this way, the MUs’ decisions
will be excluded from final decision making process.
Authors in [95] have proposed a dubious level based algorithm which doesn’t need any prior knowledge of invasion techniques. In this algorithm the sensing reports of SUs are saved for some specific period of time, i.e. observing time, and then they are compared with the reports of other SUs for that specific duration. It has to be mentioned that the observing period consist of fixed number of sensing periods. A dubious value is given to the SU, if the number of times its report differs from any other SUs exceeds a threshold. Once the observing duration is over, the total dubious value for each SU is calculated and it is called dubious level. After two consecutive observing time, the SU whose aggregated dubious level gets the highest value for both observing periods will be considered as MU.

In order to prevent unauthorized MUs from using spectrum bands, authors in [96] have proposed an abnormality detection technique that uses propagated signal’s path loss exponent to detect MU.

Min et al have proposed a scheme [97], in which a powerful SS mechanism is embedded inside the FC for removing deviant sensing reports without considering type of invasion. This algorithm uses the sensed data from SUs to estimate the transmit power of the primary transmitter and the path loss exponent, namely system states. It will then compare the estimated value of the transmitted power from primary transmitter with the actual received power from SUs to detect the invaders. The main incentive behind the proposed algorithm is that the received primary signal is controlled by the network topology as well as the rule of signal propagation at the PHY-layer, which cannot be simply changed by invaders. The
promising results obtained by the proposed algorithm have motivated the authors to further propose a primary detection method to improve the spectrum efficiency to a greater extent.

Duan et al have considered two types of cooperative invasion in CRNs [98]. In the first type of invasion, the invader only care about their short term achievements, while in the second type they are more concerned about their long term successes. Then, the authors have proposed two invasion prevention mechanisms, namely, direct and indirect punishment mechanisms to estrange invaders from setting up an invasion. Most of the previous works done for mitigating SSDDIs, e.g. [69], [71] and [99], detect MUs and disallow them from cooperating in decision making at FC. Unlike these works, the proposed invasion prevention algorithm can rule out an inroad without detecting MUs and separating them from normal users.

Since it is not always possible to avoid all kinds of invasions on SS, the authors in [100] have proposed a sensing mechanism whose objective is to reduce the effect of MUs on the final decision at FC. This mechanism utilizes the spatial correlation between neighboring SUs’ received signal and the physical layer signal features, which cannot be manipulated by invaders, to remove abnormal reports.

Table 4.2 provides short review of the state of the art mitigation techniques against SSDDIs. Following this table is a short analysis of these detection techniques.
Table 4.2: Summary of discussed mitigation techniques against SSDDIs

<table>
<thead>
<tr>
<th>Citation no.</th>
<th>Does it interact with primary transmitter?</th>
<th>Awareness about the Location of the PU</th>
<th>Main Contribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>[59]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Defeating SSDDI using a credibility based fusion technique called WSPRT</td>
</tr>
<tr>
<td>[70]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Mitigation of the SSDDI using EWSPRT and EWSZOT method</td>
</tr>
<tr>
<td>[71], [84]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Detection and mitigation of SSDDI with the Application of data mining technique called outlier detection</td>
</tr>
<tr>
<td>[72]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Credibility based defense method against SSDDI</td>
</tr>
<tr>
<td>[73]</td>
<td>Non-interactive</td>
<td>known</td>
<td>A SSDDI detection method inspired by point system of DMV for discovering smart invader</td>
</tr>
<tr>
<td>[74]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Reference paper for studying the security issues at the physical layer of CRNs</td>
</tr>
<tr>
<td>[75]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Detection and elimination of the MUs using their suspicious level</td>
</tr>
<tr>
<td>[77], [78]</td>
<td>Non-interactive and interactive</td>
<td>known</td>
<td>Mitigation of the SSDDI using outlier detection techniques</td>
</tr>
<tr>
<td>[79], [80]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Defeating SSDDI using two level information fusion technique</td>
</tr>
<tr>
<td>Citation no.</td>
<td>Does it interact with primary transmitter?</td>
<td>Awareness about the Location of the PU</td>
<td>Main Contribution</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------</td>
<td>--------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>[83]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Detecting and removing MUs by counting the number of inconsistency between CR’s decision and FC’s decision</td>
</tr>
<tr>
<td>[86]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Using a credibility based clustering method to mitigate SSDDIs without having prior knowledge about invader strategy</td>
</tr>
<tr>
<td>[87]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Detection and mitigation of SSDDI using maximum normal residue test based algorithm</td>
</tr>
<tr>
<td>[89]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Application of the Dixon based outlier detection method to find single MU</td>
</tr>
<tr>
<td>[93]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Detection of the MU using SVDD</td>
</tr>
<tr>
<td>[96]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Using propagated signal’s path loss exponent to detect MU</td>
</tr>
<tr>
<td>[98]</td>
<td>Non-interactive</td>
<td>known</td>
<td>Preventing SSDDI without detecting MUs</td>
</tr>
</tbody>
</table>

As was mentioned before, there are some the drawbacks, such as the need for large number of samples and infinite sensing time, associated with WSPRT techniques discussed in [69]. To improve these problems, authors in [70] have proposed EWSPRT algorithm. This algorithm uses a soft decision approach to differentiate SUs and therefore it can better represents the SU’s sensing data compared to WSPRT that uses hard decision. Unlike
WSPRT that uses random selection of SU for polling, the EWSPRT uses best of rest strategy to give priority to more reliable users in making final decision about the presence of the primary signal. In this way, EWSPRT can improve the sensing delay. On the other hand, EWSPRT avoids infinite sensing by stopping its operation once maximum number of samples has been used. The authors have also compared the performance of WSPRT and EWSZOT using simulations. The results show that EWSZOT outperforms WSPRT by using less number of samples and having lesser sensing time.

The advantage of the detection method outlined in [75] over [83] is that it brings back the reputation metric of temporarily misbehaved SU. This is due to the fact that a SU may temporarily have faced problems such as fading, multipath, or interferences and should not be permanently excluded from decision making process.

In contrast with the SSDDI detection method proposed in [75] that only takes into account the presence of single MU in the network, authors in [72] have considered a defense technique against multiple MUs. The problem with this technique is its requirement for having prior knowledge about the invasion strategy. To make this approach universal, authors in [84] have proposed a data mining based SSDDI detection method that does not need any prior information about the attacker. Yet the problem with the method described in [84] is that there is no clear reason for considering a SU with the sensing reports very close to other SUs in the network as an invader.
In the detection technique proposed in [73], the data from a SU whose accumulated point
passes a predefined threshold is omitted for making final decision about primary transmitter’s
activity. This approach actually excludes such SU without considering the effects of fading,
multipath or unintentional short term malfunctioning of SU.

In the work done in [77] although authors have studied the negative effect of sending
false data to FC, they haven’t consider the cases where MUs cooperative among themselves
to make the FC completely dysfunctional. Authors in [82] have taken care of such cases by
analyzing that situation and suggesting possible mitigating technique at FC.

The shortcoming of the unauthorized spectrum usage detection method suggested in [96]
is that it only determines potential invasion and do not suggest any mitigation method.
4.3 Mitigation of Different kinds of Invasions

In order to provide security in cognitive radio, it is essential to ensure the credibility of the CRs. In [101], a reliability-based technique for ensuring security in cognitive radio networks is proposed. In this method, when a CR user demands for spectrum usage, its various communication characteristics will be evaluated to estimate its reliability value. Once this reliability value is compared with some credibility threshold, the obtained result will be used to provide the demanded spectrum band to it.

In [102], authors have proposed multi-objective programming model to protect CRNs from OFIs. The proposed model prevents the invader from altering the CR’s parameters and from making it unable to intelligently adapting to the environment.

In [103], a proactive hopping approach has been suggested for defense against jamming invasion in CRNs. In this scheme, the invader randomly scans all the bands to find the SU and the invade-defense is modeled as MDP. Then for estimation of the CR’s parameters, a learning algorithm has been suggested.

In [104], Hernandez-Serrano et al. have proposed a scheme that makes the TCP protocol aware of the physical layer’s activities. The suggested scheme uses cross layer data sharing between physical/link and transport layers. Therefore, the TCP connection parameters remain unchanged by CR devices during frequency handoff and they will be adapted to new environment after the handoff.
In [105] Sybil invasion is considered, in which a single malicious SU tries to deceive other SUs in the network by showing up as multiple SUs with different identities. Douceur coined the term Sybil invasion, inspired by the story of a woman with dissociative identity disorder[106]. This type of attack was first brought forward for the peer to peer network [107]. Tan et al in [105] first modeled a Sybil invasion in which a malicious SU sends different identity data in multiple beacon frames in order to deceive other neighboring SUs and make them consider it as multi SUs. Then, authors have suggested a detection mechanism which is based on the statistics of the time interval between beacon frames. It actually differentiates MU from the normal user by comparing their beacon intervals statistics.

In [108], the creation of multiple Sybil identities by single MU has been used as a tool to launch both PUMIs and SSDDI concurrently. Then the authors have analytically derived the invading tactics which utilizes multiple Sybil identities such that they have maximum destructive effects on the CRNs. To find these invading strategies, two cases have been considered. While in the first case non-reputation based FC is taken into account, in the second case the decision making at the FC is based on the SU’s reputation values.

There are some CRs in the network that despite of having ordinary equipment in their system, show some irregular behavior in order to utilize the communication recourses exclusively. This type of invasion takes place at the MAC layer in CRNs. In order to make nodes do fair cooperation without ignoring the rights of other CRs, a very precise punishment
technique has been proposed in [109]. This method is applied in the common control as well as the data channel.
Chapter 5

5 Conclusion and Future Work

In the last decade, increasing demands for the wireless access to the Internet has caused overcrowding of some specific bands of the radio spectrum. However, there are several bands of frequency that are assigned to the licensed user and are underutilized most of the time. Cognitive radio (CR) is a promising technology that can overcome these challenges by providing opportunistic access to the underutilized spectrum.

Despite the many advantages brought by CRs to wireless networks, this technology faces new security threats and challenges in addition to those that are already present in the wireless networks.

In this work, first the general concepts of CR, cognitive radio networks, and security issues in cognitive radio networks were investigated. Then, two main security threats for cognitive radio networks, i.e., primary user mimicry and spectrum sensing data distortion invasions, along with some other types of invasion were discussed. Consequently, we provided a survey of the state of the art counter-measuring methods for detection and mitigation of these invasions. The shortcomings associated with the proposed techniques have also been investigated. Overcoming these limitations can be considered as future researches in the area of security in cognitive radio networks.
Future works may also include considering:

- Detection and mitigation techniques, which are based on other spectrum sensing methods like matched filter detection, and cyclostationary feature detection rather than only using energy detection as signal detection technique. Although this method is simple to implement, it doesn’t work well in dynamic environment due to noise uncertainty.

- Advanced techniques that do not assume a prior knowledge of primary transmitters’ locations. This is due to the reason that most of the works in the literature assume that primary transmitters’ locations are known a priori, which makes these approaches very naïve and unrealistic.

- Distributing the responsibilities of the fusion center among other users in the network to avoid the breakdown of the whole cognitive radio network in case the FC is invaded by adversaries.

- Adversaries with sophisticated invasion policies.
Bibliography


