



## 저작자표시 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.
- 이차적 저작물을 작성할 수 있습니다.
- 이 저작물을 영리 목적으로 이용할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#) 

August 2014

Master's Degree Thesis

# **Malicious Users Detection and Nullifying their Effects on Cooperative Spectrum Sensing in Cognitive Radio Networks**

Graduate School of Chosun University

Department of Information and Communication

Engineering

Prakash Prasain

# **Malicious Users Detection and Nullifying their Effects on Cooperative Spectrum Sensing in Cognitive Radio Networks**

August 25, 2014

Graduate School of Chosun University  
Department of Information and Communication  
Engineering  
Prakash Prasain

# **Malicious Users Detection and Nullifying their Effects on Cooperative Spectrum Sensing in Cognitive Radio Networks**

Advisor: Prof. Dong-You Choi

This thesis is submitted to Graduate School of  
Chosun University in partial fulfillment of the  
requirements for a Master's degree in Engineering

April, 2014

Graduate School of Chosun University  
Department of Information and Communication  
Engineering

Prakash Prasain

This is to certify that the master's thesis of

Prakash Prasain

has been approved by examining committee for the thesis  
requirement for the Master's degree in engineering.

Committee Chairperson



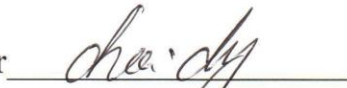
Prof. Seung-Jo Han

Committee Member



Prof. Goo-Rak Kwon

Committee Member



Prof. Dong-You Choi

May, 2014

**Graduate School of Chosun University**

# Table of Contents

<b>Table of Contents .....</b>	<b>i</b>
<b>List of Figures.....</b>	<b>iii</b>
<b>Acronyms .....</b>	<b>iv</b>
<b>Abstract (English) .....</b>	<b>v</b>
<b>Abstract (Korean) .....</b>	<b>vii</b>
<b>I. Introduction.....</b>	<b>1</b>
A. Research objective .....	2
B. Thesis layout .....	3
<b>II. Background .....</b>	<b>4</b>
A. Cognitive Radio (CR) technology .....	4
B. Spectrum sensing .....	6
1. Matched filter detection .....	7
2. Cyclostationary feature detection.....	8
3. Energy detection .....	8
C. Cooperative spectrum sensing (CSS).....	10
1. Data fusion .....	12
2. Security – Data falsification.....	13
<b>III. Methodology .....</b>	<b>15</b>
A. System model.....	15
B. Detecting malicious users and nullifying their effects.....	18
1. Grubb’s test.....	19

2. Boxplot method.....	20
3. Dixon's test .....	20
C. Proposed cooperative spectrum sensing based on reputation and weight ..	21
<b>IV. Performance Evaluation.....</b>	<b>25</b>
<b>V. Conclusion .....</b>	<b>31</b>
<b>References.....</b>	<b>32</b>

## List of Figures

Figure 2.1: Spectrum hole concept .....	5
Figure 2.2: Classification of cooperative sensing: a) centralized, b) distributed, and c) relay-assisted.....	10
Figure 3.1: Cooperative spectrum sensing structure in CRN .....	15
Figure 4.1: Energy detection spectrum sensing in AWGN channel with SNR = 5, 7, 9 dB .....	25
Figure 4.2: Energy detection spectrum sensing in non-cooperative and cooperative (20 SUs cases at SNR = 5 dB) .....	26
Figure 4.3: Probability of detection versus threshold when no malicious users, adding 10% of Always No malicious users and applying Grubb's test, Boxplot method and Dixon's test .....	27
Figure 4.4: Probability of false alarm versus threshold when no malicious users, adding 10% of Always Yes malicious users and applying Grubb's test, Boxplot method and Dixon's test .....	29
Figure 4.5: Performance of the scheme for nullifying effects of malicious users for a system containing 10% of Always No malicious users .....	30
Figure 4.6: Performance of the scheme for nullifying effects of malicious users for a system containing 10% of Always Yes malicious users .....	30



## Acronyms

CRN	: Cognitive Radio Networks
PU	: Primary User
SU	: Secondary User
FCC	: Federal Communications Commission
CSS	: Cooperative Spectrum Sensing
SSDF	: Sensing Data Falsification
FC	: Fusion Center
WRAN	: Wireless Regional Area Network
AWGN	: Additive White Gaussian Noise
ROC	: Receiver Operating Characteristic
SNR	: Signal-to-Noise Ratio

# ABSTRACT

## Malicious Users Detection and Nullifying their Effects on Cooperative Spectrum Sensing in Cognitive Radio Networks

Prakash Prasain

Advisor: Prof. Dong-You Choi, Ph.D.

Department of Information and

Communication Engineering,

Graduate School of Chosun University

Spectrum sensing in cognitive radio (CR) has a great role in order to utilize idle spectrum opportunistically, since it is responsible for making available dynamic spectrum access efficiently. In this research area, collaboration among multiple cognitive radio users has been proposed for the betterment of detection reliability. Even though cooperation among them improves the spectrum sensing performance, some falsely reporting malicious users may degrade the performance rigorously.

In this thesis, the detection and nullifying the harmful effects of such malicious users is studied by applying some well known outlier detection methods, i.e., Grubb's test, Boxplot method and Dixon's test in cooperative spectrum sensing. Initially, their performance is compared from receiver operating characteristic curves (ROC) and found that Boxplot method performs better among them. However, the limitation of Dixon's test is also discussed. Secondly, a new algorithm based on reputation and weight is developed to identify malicious users and cancel out their negative impact in final decision making. Simulation results demonstrate that the proposed scheme effectively identifies the malicious users and

suppress their harmful effects at the fusion center to decide whether the spectrum is idle for the improvement in the reliability of cooperative spectrum sensing in cognitive radio networks.

## 요 약

# 인지무선 네트워크에서 협력 스펙트럼 센싱에 대한 악성 사용자 감지 및 영향 제거

Prakash Prasain

지도교수: 최동유

조선대학교 대학원 정보통신공학과

인지무선(CR)의 스펙트럼 센싱은 유효한 동적 스펙트럼 접속을 효율적으로 만들 수 있기 때문에 적절한 유휴 스펙트럼을 활용하는데 큰 역할을 한다. 본 논문에서는 분야는 탐지 신뢰성을 향상시키기 위해 다중 인지무선 사용자 간의 협력을 제안하였다. 사용자 간의 협력이 스펙트럼 센싱의 성능을 향상시킨다고 해도 잘못된 보고를 하는 일부 악의적인 목적의 사용자가 그 성능을 매우 나쁘게 할 수 있다.

또한, 본 논문에서는 협력 스펙트럼 센싱에서 잘 알려진 탐지 방법, 즉, Grubb's test, Boxplot method, Dixon's test 를 적용해서 그런 악의적인 사용자의 탐지와 그들의 해로운 영향을 제거하기 위한 연구를 수행하였다. 첫 번째로, 그들의 성능을 ROC (Receiver Operating Characteristic)를 통해 비교한 결과 Boxplot method 가 가장 성능이 우수함을 확인하였고, Dixon's test 의 한계도 확인하였다. 두 번째로, 악의적인 사용자를 확인하기 위해 reputation 과 weight 에 기반한 새로운 알고리즘을

제안하였고, 최종 결정과정에서 그들의 부정적인 영향을 무효화하였다. 시뮬레이션 결과를 분석함으로써 제안한 알고리즘이 인지무선 네트워크에서 협력 스펙트럼 센싱의 유효성을 개선하기 위하여 스펙트럼 사용 유무를 결정하기 위한 퓨전센터(fusion center)의 악성 사용자를 식별하고 그들의 유효성을 억압할 수 있음을 확인하였다.

## I. Introduction

Currently, the frequency spectrum is statically allocated to licensed users, i.e., **primary users** (PUs) only, in a traditional wireless communication system. Since licensed users may not always occupy the allocated radio spectrum, this static spectrum allocation result in spectrum underutilization. This was confirmed in a report published in 2002 from the FCC (Federal Communications Commission) where it was shown that even in a crowded area; more than half of the radio spectrum is not occupied at any given time [1]. Thus, new spectrum allocation policies were introduced to allow unlicensed users, i.e., **secondary users** (SUs) to access radio spectrum when it is not occupied by PUs. However, when PU comes back into operation, the SU should vacate the spectrum instantly to avoid interference with the primary one. These new spectrum allocation policies are expected to improve spectrum utilization while satisfying the increasing spectrum demand for emerging wireless applications.

SUs are equipped with cognitive radio capability that can be split into *cognitive capability* and *re-configurability*. Cognitive capability refers to the ability to sense opportunities in the spectrum where channels are not utilized by PUs. These opportunities are called *spectrum holes*. Re-configurability means the capability to reconfigure its communication parameters and utilize the spectrum hole. However, SUs should access channels such that there is not any interference with PUs. Therefore, whenever the PU tries to access channel back, the SU should immediately refrain from its transmission. Hence, they need to employ efficient spectrum sensing techniques that ensure the quality of service for PUs and exploit all dynamic spectrum sharing chances. That is to say, in order to facilitate dynamic

spectrum access in licensed bands, effective spectrum sensing algorithm needs to be developed whereby high reliability along with effective utilization is achieved.

## **A. Research Objective**

If SUs have lack of knowledge about the characteristics of PU signal, energy detection is the optimal choice among many spectrum sensing techniques because of the least complexity [2] and generally adopted by most of the recent research work. Since sensing performance of a single unlicensed or SU may degrade due to the presence of various channel effects such as fading, shadowing and due to the hidden terminal problem experienced by SU, cooperative spectrum sensing (CSS) has been proposed to increase the detection reliability [3, 4]. It involves many SUs and they can share their sensing information for making a combined decision more accurate than individual decisions. They send their local sensing results to fusion center (FC) through a control channel. Then, the FC combines the received local sensing information and determines the presence of PU.

A number of collaborative spectrum sensing techniques have been proposed in this literature. However, collaboration between multiple SUs also raises a number of security issues. It has been shown in [5] that the cooperative gain can be severely affected by malfunctioning or malicious CR users in cooperative sensing. One of them is spectrum sensing data falsification (SSDF) attack, where malicious users transmit false information instead of real detection results and thereby affecting the global decision at FC. In general, malicious users continuously transmit extreme values indicating “Always Yes” or “Always No” decision. An “Always Yes” user gives a value above the threshold which means it declares that a PU is present all the time. Similarly, an “Always No” user gives a value below the threshold which means PU is absent all the time. Hence, the current CSS algorithm has to be

modified so that it can identify the malicious or malfunctioning SUs and suppress their effects in final decision making.

The main objective of this study is to optimize the CSS by identifying the malicious SUs and nullifying their negative effect on CSS. In this thesis, the performances of different outlier detection techniques based on Grubb's test, Boxplot method and Dixon's test [6] are compared initially. Their performances of those techniques have been evaluated through simulation, illustrated the limitations and finally proposed a new scheme based on reputation and weight to detect the presence of malicious users and nullify the falsely reported sensing data from them.

**Simulation:** A simulation code was written in Matlab R2013a to compare the performance of different outlier detection techniques and newly proposed scheme.

## **B. Thesis Layout**

Firstly, the CSS based on energy detection technique is studied. In chapter II, background and the spectrum sensing techniques in CR are discussed focusing mainly on the data falsification problem in CSS. In chapter III, the system model for cooperative spectrum sensing based on energy detection spectrum sensing is discussed including various outlier techniques based on Grubb's test, Boxplot method and Dixon's test. Finally, a new scheme based on reputation and weight is proposed and discussed about how it detects and alleviates sensing observations of malicious users. The performance of each outlier detection method and newly proposed scheme are analyzed through simulation results in Chapter IV. Finally, some conclusions of this study are drawn in chapter V.



## **II. Background**

### **A. Cognitive Radio (CR) Technology**

In the recent years, the rapid growth in wireless communication has led us to problems with spectrum utilization. The demand of the usable frequency spectrum is increasing. Lack of additional spectrum will become a serious limitation in the next few years. The solution how to deal with this problem is to share available bandwidths between licensed users. But in practice this solution leads to significant underutilization, resulting in spectrum wastage. For example, studies by the Federal Communications Commission (FCC) show that the spectrum utilization in the 0–6 GHz band varies from 15% to 85% [1]. Cognitive radio was born as the solution for such a contradiction. The concept was first proposed by Joseph Mitola III at a seminar at the Royal Institute of Technology in Stockholm in 1998 and published in an article by Mitola and Gerald Q. Maguire, Jr. in 1999 [7]. Cognitive radio is basically a software defined radio with a cognitive engine brain. Full cognitive radio or so called Mitola radio is observing and adjusting every possible parameter of a transceiver in order to maximize its performance. Those parameters include operating frequency, power, waveform, protocol and networking.

In the past few years, significant progress has been made in this field. Showing support for the cognitive radio idea, the FCC allowed for usage of the unused television spectrum by unlicensed users wherever the spectrum is free. IEEE has also supported the cognitive radio paradigm by developing the IEEE 802.22 standard for wireless regional area network (WRAN) which works on unused TV channels [8]. This research area is still at an immature stage because various research challenges have to be addressed and solved.

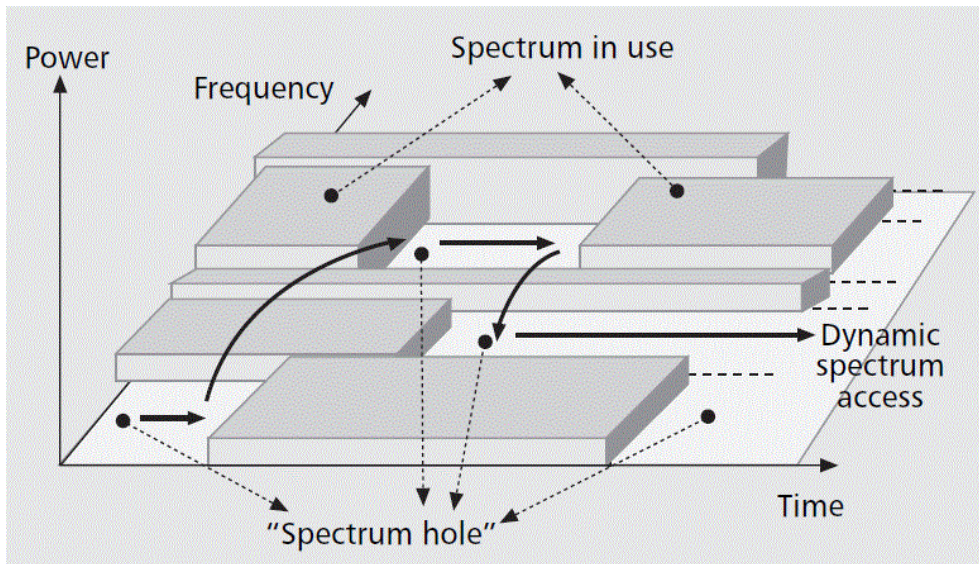


Fig. 2.1 spectrum hole concept

The key enabling technologies of CR networks are the cognitive radio techniques that provide the capability to share the spectrum in an opportunistic manner. Formally a CR is defined as a radio that can change its transmitter parameters based on interaction with its environment. As shown in Fig. 2.1, CR enables the usage of temporarily unused spectrum referred to as spectrum hole or white space. For this, each CR user in the CR networks must [9]:

- Determine which portions of the spectrum are available
- Select the best available channel
- Coordinate access to this channel with other users
- Vacate the channel when a licensed user is detected

These capabilities can be realized through spectrum management functions that address four main challenges: spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility [10].

- *Spectrum sensing*: A CR user can allocate only an unused portion of the spectrum. Therefore, a CR user should monitor the available spectrum bands, capture their information, and then detect spectrum holes.
- *Spectrum decision*: Based on the spectrum availability, CR users can allocate a channel. This allocation doesn't only depend on spectrum availability, but is also determined based on internal (and possibly external) policies.
- *Spectrum sharing*: Because there may be multiple CR users trying to access the spectrum, CR network access should be coordinated to prevent multiple users colliding in overlapping portions of the spectrum.
- *Spectrum mobility*: CR users are regarded as visitors to the spectrum. Hence, if the specific portion of the spectrum in use is required by a primary user, the communication must be continued in another vacant portion of the spectrum.

## **B. Spectrum Sensing**

Spectrum sensing in CR involves deciding whether the primary signal is present or not from the observed signal. In order to maintain the PUs' right to interference-free operation, the SUs need to regularly sense the allocated band and reliably detect the presence of the PUs' signals. Spectrum sensing plays a crucial role in the cognitive radio technology to prevent damaging interference to the primary users and to reliably and quickly spot the spectrum hole and utilize the opportunity.

Sensing for primary user detection can be formulated as a binary hypothesis problem as follows [11]:

$$y(t) = \begin{cases} n(t), & H0 \\ h(t).s(t) + n(t), & H1 \end{cases} \quad (1)$$

where  $y(t)$  denotes the received signal at the CR user,  $s(t)$  is the transmitted PU signal,  $h(t)$  is the channel gain of the sensing channel,  $n(t)$  is the zero-mean additive white Gaussian noise (AWGN),  $H0$  and  $H1$  denote the hypothesis of the absence and the presence of the PU signal in the frequency band of interest, respectively. For the evaluation of the detection performance, the probabilities of detection  $P_d$  and false alarm  $P_f$  are defined as

$$P_d = P\{decision = H1|H1\} = P\{Y > \lambda|H1\} \quad (2)$$

$$P_f = P\{decision = H1|H0\} = P\{Y > \lambda|H0\} \quad (3)$$

where  $Y$  is the decision statistic and  $\lambda$  is the decision threshold. The value of  $\lambda$  is set depending on the requirements of detection performance. Based on these definitions, the probability of a miss or miss detection is defined as  $P_m = 1 - P_d = P\{decision = H0|H1\}$ . The plot that demonstrates  $P_d$  versus  $P_f$  is called the receiver operating characteristic (ROC) curve, which is the metric for the performance evaluation of sensing techniques.

Various spectrum sensing methods have already been studied extensively in the literature. Mainly, there are three common solutions to detect the presence of the primary signal: matched filter detection, cyclostationary feature detection and energy detection.

## 1. Matched filter detection

Matched filtering-based methods are optimal for stationary Gaussian noise scenarios as they maximize the received signal-to-noise ratio (SNR) [12]. For this

optimal performance, they require perfect knowledge of the channel responses from the primary user to the secondary user and the structure and waveforms of the primary signal (including modulation type, frame format and pulse shape) as well as accurate synchronization at the secondary user. In cognitive radios, however, such knowledge is not readily available to secondary users and implementation cost and complexity of this detector is high especially as the number of primary bands increases. Therefore, this method is not practical and applicable to cognitive radio technology.

## **2. Cyclostationary feature detection**

Another detection method that can be applied for spectrum sensing is the cyclostationary feature detector. Cyclostationary feature detectors can distinguish between modulated signals and noise [13]. This detector exploits the fact that the primary modulated signals are cyclostationary with spectral correlation due to the built-in redundancy of signal periodicity (e.g., sine wave carriers, pulse trains, and cyclic prefixes), while the noise is a wide-sense stationary signal with no correlation. This task can be performed by analyzing a spectral correlation function. Therefore, cyclostationary feature detectors are robust to the uncertainty in noise power [14]. This is at the price of excessive computational complexity and long observation times. Moreover, it requires the knowledge of the cyclic frequencies of the primary users, which may not be available to the secondary users.

## **3. Energy detection**

Energy detection is the simplest spectrum sensing technology. An energy detector treats the primary signal simply as a random process and decides its presence or

absence based on the energy of the received waveform. This simple scheme accumulates the energy of the received signal during the sensing interval and declares the band to be occupied if the energy surpasses a certain threshold [15]. This threshold is set on the basis of desired probability of false alarm. Since an energy detector does not need a priori knowledge of the primary signal, it makes energy detection, robust to the parameters of the primary signal, which is beneficial for cognitive radio. Another advantage of energy detection is in its low complexity – no complicated signal processing is needed. Some of the challenges with energy detector based sensing include selection of the threshold for detecting primary users, inability of differentiating interference from, primary users and noise, and poor performance under low SNR values [12].

Let us assume that the received signal has the following simple form

$$y(n) = s(n) + w(n) \quad (4)$$

Where  $s(n)$  is the signal to be detected,  $w(n)$  is the additive white Gaussian noise (AWGN) sample, and  $n$  is the sample index. Note that  $s(n) = 0$  when there is no transmission by primary user. The detection metric for the energy detector can be written as

$$Y = \left(\frac{1}{N}\right) \sum_{n=0}^N |y(n)|^2 \quad (5)$$

where  $N$  is the size of the observation vector. The decision on the occupancy of a band can be obtained by comparing the decision metric  $Y$  against a fixed threshold  $\lambda$  as shown in equation (2) and (3).  $P_f$  should be kept as small as possible in order to prevent underutilization of transmission opportunities. The decision threshold  $\lambda$  can be selected for finding an optimum balance between  $P_d$  and  $P_f$ . However, this

requires knowledge of noise and detected signal's powers. In practice, the threshold is chosen to obtain a certain false alarm rate [12].

## C. Cooperative Spectrum Sensing

In practice, many factors such as multipath fading, shadowing, and the receiver uncertainty problem may significantly compromise the detection performance in spectrum sensing. The main idea of cooperative sensing is to enhance the sensing performance by exploiting the spatial diversity in the observations of spatially located CR users. By cooperation, CR users can share their sensing information for making a combined decision more accurate than the individual decisions [11].

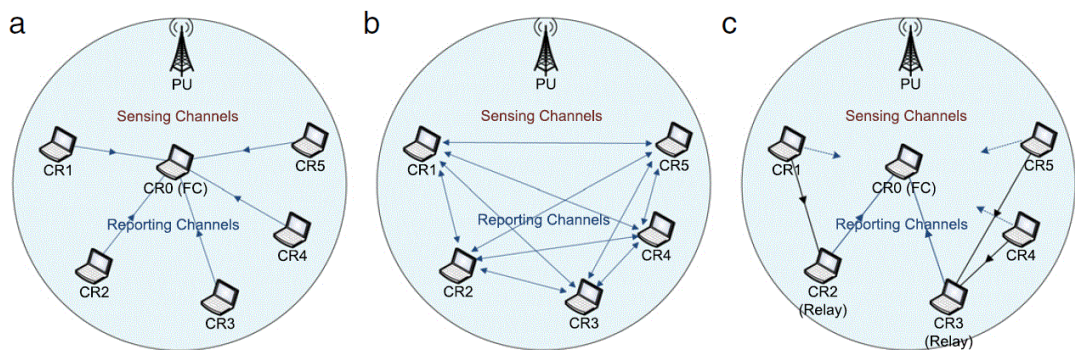


Fig. 2.2 Classification of cooperative sensing: a) centralized, b) distributed, and c) relay-assisted

To assist the analysis of cooperative spectrum sensing, it is classified into three categories based on how cooperating CR users share the sensing data in the network: centralized [16, 17], distributed [18], and relay-assisted [19, 20]. These three types of cooperative sensing are illustrated in Fig. 2.2. In this study, the centralized network among them is considered.



In centralized cooperative sensing, a central identity called fusion center (FC) controls the three step process of cooperative sensing. First, the FC selects a channel or a frequency band of interest for sensing and instructs all cooperating CR users to individually perform local sensing. Second, all cooperating CR users report their sensing results via the control channel. Then the FC combines the received local sensing information, determines the presence of PUs, and diffuses the decision back to cooperating CR users.

As shown in Fig. 2.2 (a), CR0 is the FC and CR1–CR5 are cooperating CR users performing local sensing and reporting the results back to CR0. For local sensing, all CR users tune to the selected licensed channel or frequency band where a physical point-to-point link between the PU transmitter and each cooperating CR user for observing the primary signal is called a sensing channel. For data reporting, all CR users tune to a control channel where a physical point-to-point link between each cooperating CR user and the FC for sending the sensing results is called a reporting channel.

Unlike centralized cooperative sensing, distributed cooperative sensing does not rely on a FC for making the cooperative decision. In this case, CR users communicate among themselves and converge to a unified decision on the presence or absence of PUs by iterations. Fig. 2.2 (b) illustrates the cooperation in the distributed manner. After local sensing, the cognitive radios from CR1 to CR5 share the local sensing results with other users within their transmission range. Based on a distributed algorithm, each CR user sends its own sensing data to other users, combines its data with the received sensing data, and decides whether or not the PU is present by using a local criterion. If the criterion is not satisfied, CR users send their combined results to other users again and repeat this process until the algorithm is converged and a decision is reached. In this manner, this distributed scheme may take several iterations to reach the unanimous cooperative decision.



In addition to centralized and distributed cooperative sensing, the third scheme is relay-assisted cooperative sensing. Since both sensing channel and report channel are not perfect, a CR user, observing a weak sensing channel and a strong report channel and a CR user with a strong sensing channel and a weak report channel, for example, can complement and cooperate with each other to improve the performance of cooperative sensing. In Fig. 2.2 (c), CR1, CR4, and CR5, who observe strong PU signals, may suffer from a weak report channel. CR2 and CR3, who have a strong report channel, can serve as relays to assist in forwarding the sensing results from CR1, CR4, and CR5 to the FC. In this case, the report channels from CR2 and CR3 to the FC can also be called relay channels.

## 1. Data fusion

In cooperative spectrum sensing, data fusion is a process of combining local sensing data for hypothesis testing. In general, the sensing results reported to the FC or shared with neighboring users can be combined in three different ways.

*Soft Combining*: CR users can transmit the entire local sensing samples or the complete local test statistics for soft decision.

*Quantized Soft Combining*: CR users can quantize the local sensing results and send only the quantized data for soft combining to alleviate control channel communication overhead.

*Hard Combining*: CR users make a local decision and transmit the one bit decision for hard combining. When binary local decisions are reported to FC, it is convenient to apply linear fusion rules to obtain the cooperative decision. The commonly used fusion rules are *AND*, *OR*, and majority rules. Let  $u_i$  be the local decision of CR user  $i$  and  $u$  be the cooperative decision made by the FC,  $u_i, u \in \{0, 1\}$ , and a '1' and a '0' indicate a PU's presence ( $H1$ ) and absence ( $H0$ ),

respectively. The *AND* rule refers to the FC determines  $u = 1$  if  $u_i = 1$ . Similarly, the *OR* rule refers to  $u = 1$  if  $u_i = 1$ , for any  $i$ . The majority rule requires at least a half of the CR users to report “1”. These simple fusion rules can be generalized to the *k-out-of-N* rule. Under this rule, the FC declares  $H_1$  ( $H_0$ ) if  $k$  out of  $N$  CR users report “1”. The probability of false alarm ( $Q_f$ ) and detection ( $Q_d$ ) for cooperative sensing under this rule for data fusion are given by [21]

$$Q_f = Prob\{H_1 | H_0\} = \sum_{l=k}^N \binom{N}{l} P_f^l (1 - P_f)^{N-l} \quad (6)$$

$$Q_d = Prob\{H_1 | H_1\} = \sum_{l=k}^N \binom{N}{l} P_d^l (1 - P_d)^{N-l} \quad (7)$$

It can be observed in (6) and (7) that when the value of  $k$  is taken as 1 and  $N$ , the  $k$  out of  $N$  rule becomes the *OR* and *AND* rules, respectively. The *OR* rule works best when the number of cooperating CR users is large. Similarly, the *AND* rule works well when the number of cooperating users is small. The majority rule can be obtained from the  $k$  out of  $N$  rule under the condition when  $k \geq N/2$ . Thus, it is important to determine the optimal value of  $k$  for which the detection errors are minimized. It has been shown that the optimal value of  $k$  depends on the detection threshold. For a small fixed threshold, the optimal rule is the *AND* rule, i.e.,  $k = N$ . Similarly, for a fixed very large threshold, the *OR* rule ( $k = 1$ ) is said to be optimal [20].

## 2. Security - Data falsification

The cooperation among CR users raises new concerns for the reliability and security in cooperating sensing. When multiple CR users cooperate in sensing, a few CR users who report unreliable or falsified sensing data can easily influence the cooperative decision. The report obtained from malfunctioning CR users could affect the decision from real value. Moreover, CR users, called malicious users can intentionally manipulate the sensing data and report the falsified data for their own

benefits. It has been shown in [5] that the cooperative gain can be severely affected by malfunctioning or malicious CR users in cooperative sensing. This is what it is called *data falsification*.

To address data falsification problem, existing cooperative sensing mechanisms should be modified to distinguish the malicious users so that they can be excluded from the cooperation to ensure the reliability of the sensing decisions.

In [22], the weighted SPRT with a reputation-based mechanism is proposed as the robust cooperative sensing scheme to address the data falsification problem. As a first step, the reputation ratings for cooperating CR users are calculated depending upon their sensing accuracy. Whenever the local sensing result matches the final decision, the reputation is increased. Otherwise, it is decreased. The reputation values are converted to the weights to be used in the modified likelihood ratio of an SPRT for data fusion. In this manner, the impact of the unreliable CR users can be reduced by putting weights in the genuine sensing data over the falsified ones.

In [23], the trust factor that measures the CR user's reliability is then evaluated as the weights in calculating the mean value of receiving sensing data. In that way, cooperative sensing can be more reliable by building trust toward CR users that report a sensing value close to the mean of all collected results at the FC.

### III. Methodology

In this chapter, some known outlier detection techniques based on Grubb's test, Dixon's test and Boxplot method are discussed initially. Later, a new scheme is proposed to identify malicious users and nullify their effects in decision making so that they cannot influence cooperative spectrum sensing badly.

#### A. System Model

A CR network composed of  $N$  secondary users and a common receiver (FC) is considered, as shown in Fig. 3.1 [21]. It is assumed that each CR performs spectrum sensing independently and then the local sensing data are sent to the common receiver which can fuse all available information to infer the absence or presence of the PU.

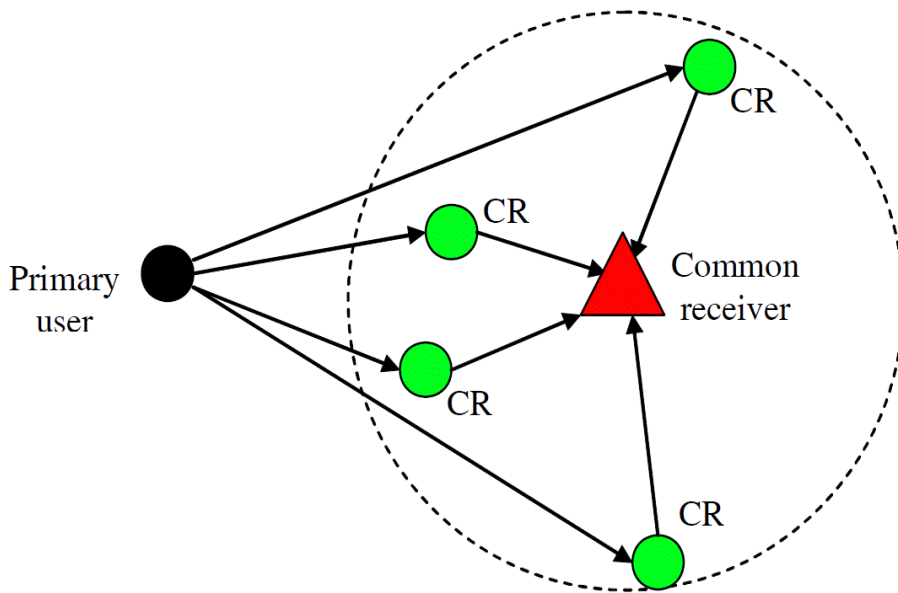


Fig. 3.1 Cooperative spectrum sensing structure in CRN

The essence of spectrum sensing for PU detection is a binary hypothesis-testing problem:

$H0$ : primary user is absent;

$H1$ : primary user is present.

Here, only the spectrum sensing at CR  $i$  is considered. The sensing method is to decide between the following two hypotheses,

$$y_i(n) = \begin{cases} u_i(n), & H0 \\ h_i(n).s(n) + u_i(n), & H1 \end{cases} \quad (8)$$

where  $y_i(n)$  is the received signal at the  $i^{\text{th}}$  CR,  $s(n)$  is the signal from PU, each sample is assumed to be an independent identically distributed (i.i.d.) random process with zero mean and variance  $E[|s(n)|^2] = \sigma_s^2$ . Similarly,  $u_i(n)$  is the additive white Gaussian noise (AWGN) with zero mean and variance  $E[|u_i(n)|^2] = \sigma_u^2$ , and  $h_i(n)$  denotes the channel gain of the sensing channel between PU and the  $i^{\text{th}}$  CR. It has the same variance  $E[|h_i(n)|^2] = \sigma_h^2$ . The area of coverage of the cognitive radio system is assumed to be small enough so that the variations in path loss can be neglected. The average received SNR at each SU is given as  $\gamma = \sigma_s^2 \sigma_h^2 / \sigma_n^2$ .

All of the SUs use energy detectors and the energy detector output  $Y_i$  at the  $i^{\text{th}}$  SU is given by

$$Y_i = \left(\frac{1}{M}\right) \sum_{n=1}^M |y_i(n)|^2 \text{ for } i=1, 2, \dots, N. \quad (9)$$

where  $M$  is the number of signal samples that are collected at each SU during the sensing period, which is the product of the sensing time  $\tau$  and the sampling frequency  $f_s$ .  $\lambda_i$  is denoted as the local detection threshold of the energy detector at the  $i^{\text{th}}$  SU. It can be derived in terms of the desired probability of false alarm ( $P_f$ )

which aims to minimize the probability of miss detection [11]. Then, the local decision  $d_i$  made by  $i^{th}$  SU is given by comparing with the threshold  $\lambda_i$ .

$$d_i = \begin{cases} H0, & \text{if } Y_i < \lambda_i \\ H1, & \text{if } Y_i \geq \lambda_i \end{cases} \quad (10)$$

A perfect channel conditions is assumed for the control channels between SUs and FC.

For the  $i^{th}$  CR with the energy detector, the average probability of false alarm, the average probability of detection, and the average probability of missed detection over AWGN channels are given, respectively, by [21]

$$P_{f,i} = \frac{\Gamma(u, \frac{\lambda_i}{2})}{\Gamma(u)} \quad (11)$$

$$P_{d,i} = Q_u(\sqrt{2\gamma_i}, \sqrt{\lambda_i}) \quad (12)$$

and

$$P_{m,i} = 1 - P_{d,i} \quad (13)$$

In the above equations,  $u$  is the time bandwidth product of the energy detector,  $\Gamma(a, x)$  is the incomplete gamma function given by  $\Gamma(a, x) = \int_x^\infty t^{a-1} e^{-t} dt$ ,  $\Gamma(a)$  is the gamma function, and  $Q_u(a, b)$  is the generalized Marcum Q-function given by  $Q_u(a, x) = \frac{1}{a^{u-1}} \int_x^\infty t^u e^{-\frac{t^2+a^2}{2}} I_{u-1}(at) dt$ , with  $I_{u-1}(\cdot)$  being the modified Bessel function of the first kind and order  $(u - 1)$ .

The assumptions are similar as in [21]. The distance between any two SUs is small in comparison with the distance from any SU to PU and the received PU signal at each SU experiences almost identical path loss. Moreover, all SU use the same

threshold  $\lambda$ , so that  $\lambda_1 = \lambda_2 = \dots \lambda_N = \lambda$ . It means that  $P_{f,i}$  is independent of  $i$  and can be denoted it as  $P_f$ . In case of AWGN channel, the  $P_{d,i}$  is independent of  $i$ , it is denoted as  $P_d$ . So, the probability of false alarm and probability of detection are given by (6) and (7). So, probability of miss detection  $P_m = 1 - P_d$ .

In the next section, the three methods for detecting outliers in a statistical data are discussed and later, compared their performance through simulation. For this, it has been considered that every SU sends their received energy values instead of sending local decision ('1' for the presence of PU and '0' for the absence of PU) through an error free control channel to the FC. Then, FC runs algorithms for detecting malicious users. For this, average combination scheme is followed due to its simplicity. In this scheme, the mean the received energies in dB by all SUs is calculated and FC compares it with a fixed threshold. Then the decision  $D$  made by FC is given by

$$D = \begin{cases} H0, & \text{if } Y < \lambda_{FC} \\ H1, & \text{if } Y \geq \lambda_{FC} \end{cases} \quad (14)$$

Where  $\lambda_{FC}$  is threshold at FC and  $Y$  is the mean of received energies which is given by  $Y = \left(\frac{1}{N}\right) \sum_{i=1}^N Y_i$ .

## **B. Detecting malicious users and nullifying their effects**

It has been shown that performance of cooperative sensing can significantly be affected by the presence of malicious SU. A SU might be malicious due to device malfunctioning or due to selfish reasons. As in [23], two different kind of malicious users are considered. One is 'Always Yes' user and another is 'Always No' user. An 'Always Yes' node gives a value above the threshold which means it declares that a PU is present all the time. Similarly, an 'Always No' node gives a

value below the threshold which means PU is absent all the time. An ‘Always Yes’ user increase the probability of false alarm  $P_f$  and an ‘Always No’ user decreases the probability of detection  $P_d$ . Also, there might be other malicious user that provides extreme false value once in a while and produce the correct values at rest of the time. The malicious user detection scheme proposed here can identify any malicious user whose energy value differs in distribution from the underlying distribution of the energy values of the reasonable users.

## 1. Grubb’s test

Grubb’s test is one of the most commonly used for the detection of a single outlier in univariate data [6]. This test for outliers compares the deviation of the suspect value of the sample mean with the standard deviation of the sample. The suspect value is the value that is furthest away from the mean. In order to use Grubb’s test for an outlier, the statistic  $G$  is calculated:

$$G = \frac{\left| \text{Suspect value} - \bar{x} \right|}{s} \quad (15)$$

where  $\bar{x}$  and  $s$  are mean and standard deviation respectively. They are calculated with the suspect value included. If the calculated value of  $G$  exceeds the critical value, the suspect value is taken as an outlier and it is rejected. A table of critical values at specified significance level for different sample size has been provided in [6].

Grubb’s test is used to detect the single outlier. To detect more than one outlier, this test is applied iteratively so that it can test one value at a time until and unless the sample data set of received energies is free from the extreme values produced by malicious SUs.



## 2. Boxplot method

In this method, different energy values obtained from different SUs are arranged in ascending order from smallest to largest  $Y_1 \leq Y_2 \leq \dots Y_N$ . Then, lower and upper bounds are calculated as follows:

$$Q_{lower} = Q_1 - 1.5Q_{intqtr} \quad (16)$$

$$Q_{upper} = Q_3 - 1.5Q_{intqtr} \quad (17)$$

where  $Q_{lower}$  and  $Q_{upper}$  are lower and upper threshold respectively.  $Q_1$  is first quartile,  $Q_3$  is third quartile and  $Q_{intqtr}$  is interquartile range. The values of obtaining energies below  $Q_{lower}$  and above  $Q_{upper}$  are considered as outliers.

## 3. Dixon's test

It is based on the ratios of differences between the observations and the calculation of the ratio depends on the number of observations. As in the previous two techniques, it avoids the calculation of mean and standard deviation [24]. This test is also for detecting a single outlier. In this method, outlier factors for each SU are calculated based on their local sensing results to detect the presence of malicious users. The received energy values are arranged in ascending order  $Y_1 \leq Y_2 \leq \dots Y_N$  and outlier factor  $factor_i$  for  $i^{th}$  SU is calculated as [24]:

For  $3 \leq N \leq 7$ ,

$$factor_i = \begin{cases} \frac{Y_2 - Y_1}{Y_N - Y_1}, & \text{if smallest value is suspected} \\ \frac{Y_N - Y_{N-1}}{Y_N - Y_1}, & \text{if largest value is suspected} \end{cases} \quad (18)$$

For  $8 \leq N \leq 10$ ,

$$factor_i = \begin{cases} \frac{Y_2 - Y_1}{Y_{N-1} - Y_1}, & \text{if smallest value is suspected} \\ \frac{Y_N - Y_{N-1}}{Y_N - Y_2}, & \text{if largest value is suspected} \end{cases} \quad (19)$$

For  $11 \leq N \leq 13$ ,

$$factor_i = \begin{cases} \frac{Y_3 - Y_1}{Y_{N-1} - Y_1}, & \text{if smallest value is suspected} \\ \frac{Y_N - Y_{N-2}}{Y_N - Y_2}, & \text{if largest value is suspected} \end{cases} \quad (20)$$

For  $14 \leq N \leq 25$ ,

$$factor_i = \begin{cases} \frac{Y_3 - Y_1}{Y_{N-2} - Y_1}, & \text{if smallest value is suspected} \\ \frac{Y_N - Y_{N-2}}{Y_N - Y_3}, & \text{if largest value is suspected} \end{cases} \quad (21)$$

where  $N$  is the number of statistical data i.e., number of SUs in our case. The calculated outlier factor  $factor_i$  is compared with a critical value  $Q$ , which depends on the  $N$  and the significance level. The table of the critical values for different values of  $N$  for three significance levels can be found in [24]. If the outlier factor is less than the critical value  $Q$ , this energy value is assumed to be normal, otherwise if it exceeds the critical value  $Q$ , it is assumed to be high energy reported by corresponding SU. The Outlier factor for the smallest suspect value and largest value are calculated individually.

### C. Proposed cooperative spectrum sensing based on reputation and weight

The main purpose our proposed scheme is to identify the malicious SUs and nullify the falsely reported data from them. In the previous section, the three outlier detection methods were discussed to detect and avoid the falsified sensing data in making global decision in CSS. Two methods out of three are designed for

detecting only one outlier at a time. Thus, those methods do not perform better and the performance is degraded if more than one outlier exists.

Thus, a new scheme based on the reputation and the weight of each SU is proposed. In this scheme, every SU is assigned with a reputation value based on the reliability of their sensing data. Then, the weight of each SU is calculated from their reputation and finally their weights are utilized to make global decision. In this way, this scheme is performed in three phases: *pre-filtering of the sensing data*, *reputation assignment* and *data combining*.

*Pre-filtering of the sensing data:* Let  $Y_i(k)$  for  $i=1, 2, \dots, N$  represents the output of energy detectors of each SU at time instant  $k$ . Initially, it is essential to filter those sensing data which are extremely far from the rest of the data. For this, one of the common outlier detection methods, i.e., a Boxplot method is applied to identify the extreme outliers which has already been discussed in the previous section.  $Q_{lower}(k)$  and  $Q_{upper}(k)$  are calculated according to equations (16) and (17). If a particular value does not lie in the interval  $[Q_{lower}(k), Q_{upper}(k)]$ , then this is considered as an outlier and is not included further for making global decision. Let  $F_k$  represents the set of the SUs whose energy values lie in the range  $[Q_{lower}, Q_{upper}]$  and the number of SUs in the set is  $P$ .

*Reputation assignment:* After the pre-filtering of the sensing data, each SU is assigned a reputation value in accordance with their reliability of sensing data. Here, the decision made by individual SU is referred as local decision and the decision made by fusion center (FC) as global decision. For each SU, if the local decision is matched with the global decision, the reputation value is increased, otherwise it will be decreased. Initially, an equal reputation value of 1 is assigned for each SU. Thus, the reputation value for the  $i^{th}$  SU at time  $k$  is updated as [22]:

$$r_i(k) = r_i(k-1) + (-1)^{d_i(k)+d(k)} \quad (22)$$

where  $d(k)$  is the global decision value which will be given in the next data combining phase and  $d_i(k)$  is the local decision which is given by:

$$d_i(k) = \begin{cases} 0, & \text{if } Y_i < \lambda \\ 1, & \text{if } Y_i \geq \lambda \end{cases} \quad (23)$$

Where  $\lambda$  denotes the threshold for SU. As already mentioned, all SUs that lie on the set  $F_k$  and use the same threshold  $\lambda$ , so that  $\lambda_1 = \lambda_2 = \dots = \lambda_p = \lambda$ .

*Data combining*: In this phase, all the cooperating SUs that fall on the set  $F_k$  are included in CSS based on their corresponding reputation value. For this, a weighted CSS is used to make global decision. Then, global decision made by FC is given by,

$$d(k) = \begin{cases} 1, & \text{if } \sum_{F_k} w_i(k) Y_i(k) \geq \lambda_{FC} \\ 0, & \text{otherwise} \end{cases} \quad (24)$$

where  $F_k$  represents the set of energy values after pre-filtering,  $\lambda_{FC}$  is the threshold used by FC. In this thesis, the Neyman-Pearson formulation is considered and the threshold  $\lambda_{FC}$  is determined so that the probability of false alarm is fixed at a certain value  $P_f$ . Similarly,  $w_i(k)$  is the reputation weight, which is the function of reputation value such that  $w_i(k) = f(r_i(k-1))$ . Here, the weighted function used in [22] is followed which is given below:

$$w_i(k) = \frac{w'_i(k)}{\sum_i w'_i(k)} \quad (25)$$

where,

$$w'_i(k) = \frac{r_i(k-1)}{\max(r_i(k-1))} \quad (26)$$

Based on the above discussion, the proposed scheme can be described using the following algorithm:

- a. Initialize reputation  $r_i = 1$  for all SUs.
- b. For each spectrum sensing attempt {
- c. Obtain spectrum sensing report  $Y_i$  from all SUs
- d. Apply pre-filtering for the extreme outliers
- e. Calculate local decision  $d_i$  for all remaining P SUs after pre-filtering.
- f. Calculate weight  $w_i$  for each P SUs.
- g. Combine weight  $w_i$  with  $Y_i$  and compare it with threshold  $\lambda_{FC}$  at FC.
- h. If  $w_i \times Y_i \geq \lambda_{FC}$ , accept  $H1$ , i.e. global decision  $d = 1$ . Otherwise, accept  $H0$ , i.e., global decision  $d = 0$ .
- i. Update reputation value as  $r_i \leftarrow r_i + (-1)^{d_i+d}$ .
- j. }

## IV. Performance Evaluation

In this chapter, the performance of malicious user detection techniques discussed in the previous chapter is presented by comparing their respective receiver operating characteristics (ROC) curves obtained through simulation. Later, the performance of newly proposed algorithm based on reputation and weight for nullifying the effects of malicious users on CSS is analyzed.

Initially, the energy detector in both non-cooperative and cooperative cases is studied which is an important starting point for this work. In simulation, Additive White Gaussian Noise (AWGN) channel is assumed and the primary user signal is assumed to be BPSK modulated. First, the ROC curve for probability of detection versus probability of false alarm is generated through Monte Carlo simulations at different SNR.

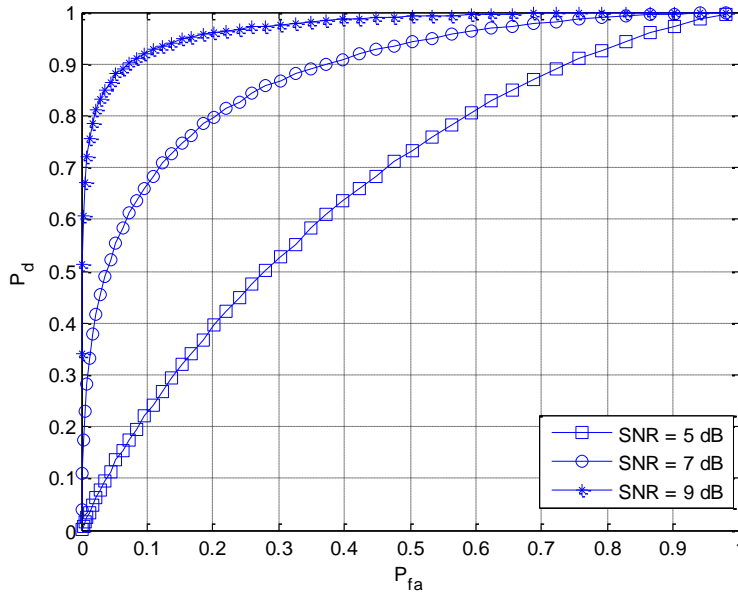


Fig. 4.1 Energy detection spectrum sensing in AWGN channel with SNR = 5, 7, 9 dB

Fig. 4.1 is the basic plot of energy detection spectrum sensing at different SNR i.e., 5 dB, 7 dB and 9 dB under the above assumptions. Probability of false alarm in horizontal axis and probability of detection in vertical axis. Both of those probabilities run from 0 to 1. It shows the relationship between the probability of detection and probability of false alarm. Probability of false alarm is function of threshold. At point the extreme point (1,1), threshold is very very small. It always decides that  $H1$  is true in both the cases of presence and absence of primary user signal actually. Similarly the threshold is very very high at the point (0,0) where it always decides that  $H0$ . It also shows that it performs better as SNR increases.

Similarly, Fig. 4.2 shows the ROC curve for both non-cooperative and cooperative cases using energy detection. For cooperative sensing,  $N = 20$  SUs are taken. Similarly, the SNR is taken 5 dB and followed the  $k$ -out-of- $N$  rule [21] for making a cooperative decision given by the equations (6) and (7).

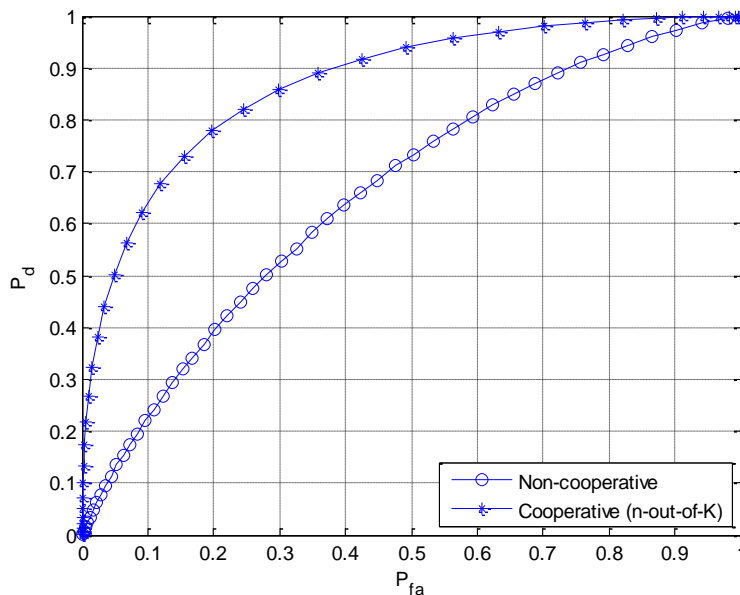


Fig. 4.2 Energy detection spectrum sensing in non-cooperative and cooperative (20 SUs) cases at SNR = 5 dB.

Second, our center of attraction is to evaluate the cooperative cases with malicious users. For the SU providing “Always No” decision, it is assumed that it reports energy 5 dB lower than the normal SU. Similarly, “Always Yes” user reports energy 5 dB higher than the normal SU. The significance level is taken 0.05. For simplicity, the average of all the received energy values is calculated at FC and a decision is made according to equation (14).

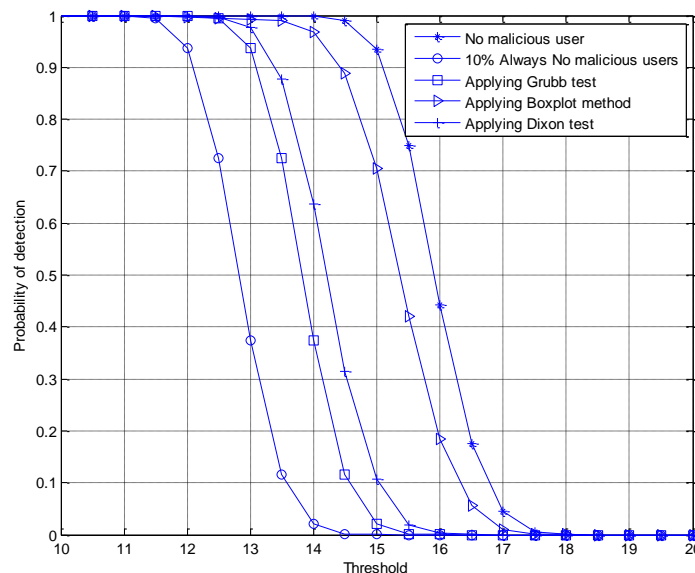


Fig. 4.3 Probability of detection versus threshold when no malicious users, adding 10% of Always No malicious users and applying Grubb’s test, Boxplot method and Dixon test

In Fig. 4.3, a cooperative spectrum sensing scenario is considered in which 10% of SUs are ‘Always No’ malicious users. The ROC curve of CSS is provided, which shows the degradation in performance when ‘Always No’ malicious users are added. It can be seen that ‘Always No’ type malicious users have decreased the probability of detection, i.e. increased the probability of miss detection. It also shows the performance of cooperative spectrum sensing after nullifying the



malicious effects by applying Grubb's test, Boxplot method and Dixon's test. Initially, one 'Always No' malicious user is assumed in which case, all the three tests show almost same performance, i.e., they successfully removed the effect of one malicious user. Later, when two 'Always No' users are introduced, some differences in their performances is found. It can be seen that probability of detection after applying Boxplot method is closest among the three tests to that of without any malicious user. As already mentioned that Grubb's test has been applied iteratively to detect the multiple malicious users since this test is supposed to detect only one malicious user at a time. On the other hand, Dixon test's performance is better than the Grubb's test and worse than Boxplot method in case of multiple malicious users introduced. The Dixon's test cannot be easily implemented for detecting multiple malicious users. If the first three users observed almost same energy, the numerator of equation (21) for the case of lowest suspected, becomes so small and the outlier factor will be so smaller than the critical value. This results in not detecting the malicious users present. This is because of method can detect multiple malicious users. This will degrade the performance of cooperative spectrum sensing.

Similarly, another ROC curve is plotted as shown in Fig. 4.4. It shows the performance of cooperative spectrum sensing after adding 10% of 'Always Yes' malicious users. 'Always Yes' type malicious users degrade the performance by increasing the probability of false alarm of the system. Similar to the previous case of adding 'Always No' malicious users, all the three outlier detection methods did not succeed to nullify the effects of malicious users completely. However, out of these three outlier detection methods, the Boxplot method performs better than that of the Grubb's test and Dixon's test and it succeeded to bring the probability of detection and probability of false alarm of the system closer to that of the cooperative spectrum sensing system without any malicious user.

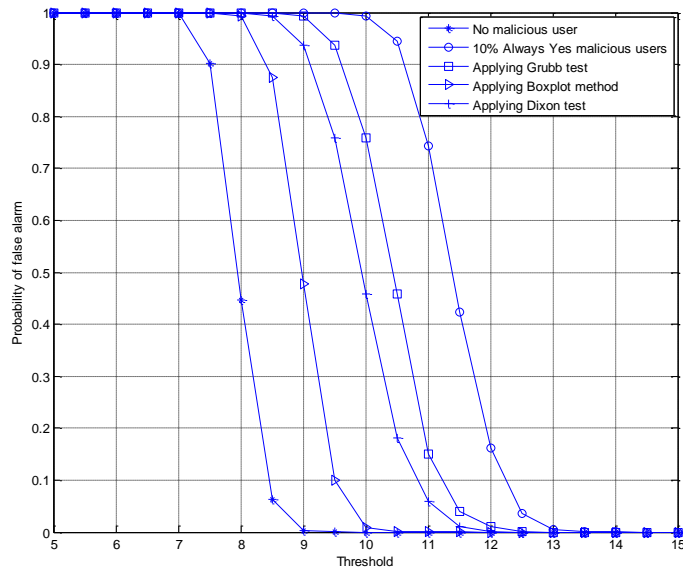


Fig. 4.4 Probability of false alarm versus threshold when no malicious users, adding 10% of Always Yes malicious users and applying Grubb's test, Boxplot method and Dixon test

Now, the probability of detection and false alarm versus threshold is presented for the case without applying any malicious user detection scheme and applying the proposed scheme for nullifying the effect of malicious users. Fig. 4.5 and 4.6 show the performance of our newly proposed scheme when applied in the system in which 10% of 'Always No' and 10% of 'Always Yes' malicious users are present respectively. From Fig. 4.5, it can be seen that newly proposed scheme for nullifying the effect of malicious users has been able to bring the probability of detection of the system very close to that of cooperative spectrum sensing with no malicious users. Similarly, when new scheme is applied in the system where 10% 'Always Yes' malicious is present, it brings the probability of false alarm very close to that of with no malicious users.

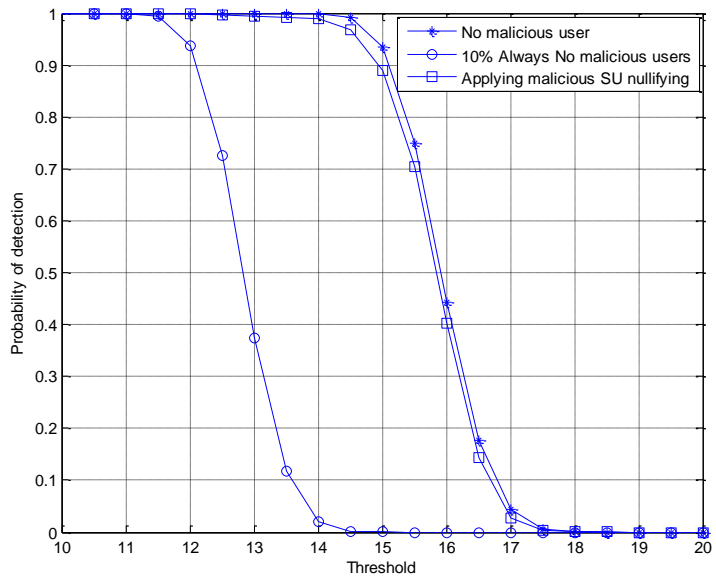


Fig. 4.5 Performance of the scheme for nullifying effects of malicious users for a system containing 10% of Always No malicious users

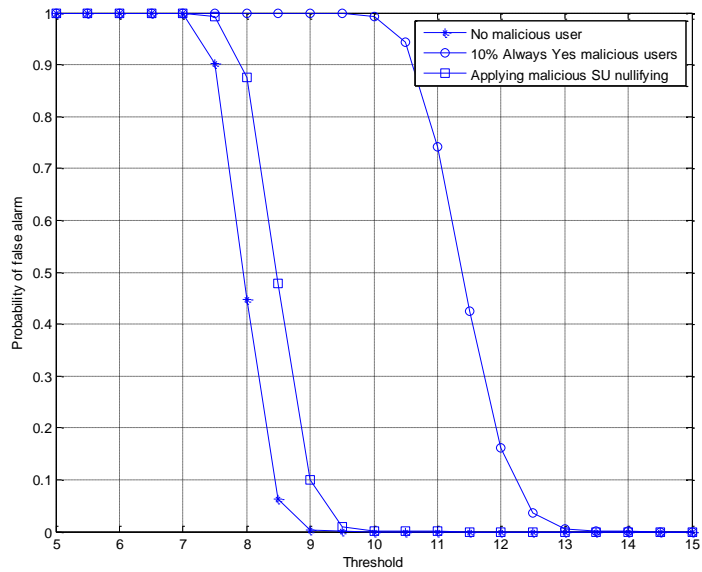


Fig. 4.6 Performance of the scheme for nullifying effects of malicious users for a system containing 10% of Always Yes malicious users

## V. Conclusion

In this thesis, the energy detection technique for spectrum sensing in CR is studied initially. Later it is applied in cooperative spectrum sensing and concentrated on the detection and nullifying the effects of falsely reported sensing data by malicious users in final decision making. For this, the techniques that detect the outliers in a statistical data are studied and compared their performance applying in cooperative spectrum sensing. Even though, the first two technique, i.e., Grubb's and Dixon's are supposed to detect one malicious user at a time, it is iterated to remove all possible malicious users. Through Monte Carlo simulations, their performances are analyzed and observed that Boxplot method performs better than the other two. However, none of them were able to nullify the negative effect of falsely reported sensing data completely. Further, the limitation of Dixon's test is also notified while it is applied to detect multiple malicious users.

Secondly, the performance of the newly proposed scheme was analyzed. The scheme is based on reputation and weight. The purpose of the scheme was to nullify the harmful effects of malicious users by introducing both 'Always No' and 'Always Yes' type malicious users separately in the system. Even though it also could not completely suppress the effects of such malicious users, it performs better than the above mentioned outlier detection techniques. It was able to bring the probability of detection and false alarm of the system very close to that of a system without any malicious users.

## References

- [1] FCC, Spectrum Policy Task Force report ET Docket 02-155, Nov. 2002.
- [2] A. Sahai, N. Hoven, and R. Tandra, "Some fundamental limits on cognitive radio," Allerton Conference on Communication, Control, and Computing, pp. 131–136, Oct. 2004.
- [3] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of tv transmissions in support of dynamic spectrum sharing," in First IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 338–345, Nov. 2005.
- [4] A. Ghasemi and E. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," First IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 131–136, Nov. 2005.
- [5] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," in IEEE International Conference on Communications, ICC, pp. 1658–1663, Jun. 2006.
- [6] Vic Barnett and Toby Lewis, "Outliers in Statistical Data," John Wiley and Sons, 3rd Edition, 1994.
- [7] J. Mitolla and G. Q. MaGuire, Jr. "Cognitive Radio: Making Software Radios More Personal," IEEE Pers. Commun, vol. 6, pp. 13–18, Aug. 1999.
- [8] C. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. Shellhammer, and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area networks (WRANs) standards," *IEEE Communications Magazine*, vol. 47, no. 1, pp. 130–138, Jan. 2009.

- [9] Akyildiz, I. F., Lee, W. Y., Vuran, M. C., and Mohanty, S, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, no. 13, pp. 2127-2159, 2006.
- [10] Akyildiz, I. F., Lee, W. Y., Vuran, M. C., and Mohanty, S, "A survey on spectrum management in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40-48, 2008.
- [11] Akyildiz, Ian F., Brandon F. Lo, and Ravikumar Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey." *Physical Communication*, vol. 4, no. 1, pp. 40-62, 2011.
- [12] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.
- [13] Y. Zeng, Y.-C. Liang, A. T. Hoang, and R. Zhang, "A review on spectrum sensing for cognitive radio: challenges and solutions," *EURASIP Journal on Advances in Signal Processing*, pp. 1–16, 2010.
- [14] S. Enserink and D. Cochran, "A cyclostationary feature detector," in *Proc. 28th Asilomar Conference on Signals, Systems, and Computers*, pp. 806–810, 1994.
- [15] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, no. 4, pp. 523–531, 1967.
- [16] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of tv transmissions in support of dynamic spectrum sharing," *IEEE DySPAN*, pp. 338–345, 2005.
- [17] J. Unnikrishnan and V.V. Veeravalli, "Cooperative sensing for primary detection in cognitive radio," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, 18–27, 2008.
- [18] Z. Li, F. Yu, and M. Huang, "A cooperative spectrum sensing consensus scheme in cognitive radios," *IEEE Infocom*, pp. 2546–2550, 2009.

- [19] G. Ganesan and Y.G. Li, "Cooperative spectrum sensing in cognitive radio—part I: two user networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 6, pp. 2204–2213, 2007.
- [20] G. Ganesan and Y.G. Li, "Cooperative spectrum sensing in cognitive radio—part II: multiuser networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 6, pp. 2204–2213, 2007.
- [21] W. Zhang, R. Mallik, and K. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5761–5766, 2009.
- [22] Chen, Ruiliang, Jung-Min Park, and Kaigui Bian, "Robust distributed spectrum sensing in cognitive radio networks," *IEEE Conference on Computer Communications*, 2008.
- [23] Kaligineedi, Praveen, Majid Khabbazzian, and Vijay K. Bhargava. "Secure cooperative sensing techniques for cognitive radio systems," *IEEE International Conference*, 2008.
- [24] Grubbs and Frank E. "Procedures for detecting outlying observations in samples," *Technometrics* vol. 11, no. 1, pp. 1-21, 1969.

## Acknowledgement

I would like to express my deepest gratitude to my advisor, Prof. Dong-You Choi, for his support, patience, and encouragement throughout my graduate studies. His technical and editorial advice was essential to the completion of this dissertation and has taught me innumerable lessons and insights on the workings of academic research in general.

I would like to express my special gratefulness to the National IT industry Promotion Agency (NIPA), Republic of Korea for awarding me NIPA scholarship for financial support to study and to research in Korea. I am immensely indebted to Chosun University for waiving tuition fee and providing academic support to study Masters in Information and Communications Engineering.

My thanks also go to the members of my supervising committee members Prof Seung-Jo Han and Prof. Goo-Rak Kwon for their valuable advice and comments throughout my research.

My sincere appreciation is to my fellow lab mates for the stimulating discussions, support and their useful suggestions throughout the course of my research.

I deeply thank my parents, Mr. Punya Prasad Prasain and Mrs. Manmaya Prasain for their unconditional trust, timely encouragement, distant care and endless patience. Last, but not least, I would like to thank my wife Mrs. Pratikshya Sharma for her understanding and love during the past years. Her support and encouragement was in the end what made this study possible.