Cooperative Spectrum Sensing for Cognitive Radio Networks

by

Praveen Kaligineedi

B. Tech, Indian Institute of Technology Kanpur, 2004

M. A. Sc, The University of British Columbia, 2006

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

Doctor of Philosophy

in

THE FACULTY OF GRADUATE STUDIES

(Electrical and Computer Engineering)

The University Of British Columbia
(Vancouver)

November 2010

Abstract

Radio spectrum is a very scarce and important resource for wireless communication systems. However, a recent study conducted by Federal Communications Commission (FCC) found that most of the currently allocated radio spectrum is not efficiently utilized by the licensed primary users. Granting opportunistic access of the spectrum to unlicensed secondary users has been suggested as a possible way to improve the utilization of the radio spectrum. Cognitive Radio (CR) is an emerging technology that would allow an unlicensed (cognitive) radio to sense and efficiently use any available spectrum at a given time. Reliable detection of the primary users is an important task for CR systems. Cooperation among a few sensors can offer significant gains in the performance of the CR spectrum sensing system by countering shadow-fading effects.

In this thesis, we consider a parallel fusion based cooperative sensing network, in which the sensors send their sensing information to an access point, which makes the final decision regarding presence or absence of the primary signal. We assume that energy detection is used at each sensor. Presence of few malicious users sending false sensing data can severely degrade the performance of such a cooperative sensing system. In this thesis, we investigate schemes to identify malicious users based on outlier detection techniques. We take into consideration constraints imposed by the CR scenario, such as limited informa-

tion about the primary signal propagation environment and small sensing data sample size. Considering partial knowledge of the primary user activity, we propose a novel method to identify malicious users. We further propose malicious user detection schemes that take into consideration the spatial location of the sensors.

We then investigate efficient sensor allocation and quantization techniques for a CR network operating in multiple primary bands. We explore different methods to assign CR sensors to various primary bands. We then study efficient single-bit quantization schemes at the sensors. We show that the optimal quantization scheme is, in general, non-convex and propose a suboptimal solution based on a convex restriction of the original problem. We compare the performance of the proposed schemes using simulations.

Preface

I am the primary researcher and author for all the research contributions made in this thesis. I identified the research problems, performed literature review, and conducted research to address those problems. Mathematical formulation and analysis of the problems and development of novel schemes were carried out by me. I wrote the programs for analyzing the mathematical models and simulating performance of proposed schemes. I also prepared the associated manuscripts ([34–37]) for publication. Dr. Majid Khabbazian is a co-author for contributions in Chapter 2. I consulted him during identification and formulation of the research problem. He also provided some technical feedbacks and editorial corrections for the associated manuscripts ([36, 37]). My supervisor Prof. Vijay Bhargava is a co-author for the contributions made in Chapters 2 and 3. I consulted him during the identification and formulation of the research problems. He also provided editorial feedbacks during my preparation of the associated manuscripts.

Table of Contents

List of Tables

List of Figures

Acknowledgments

First and foremost, I would like to thank my supervisor, Professor Vijay K. Bhargava, for his guidance, encouragement and support. I would like to thank Dr. Majid Khabbazian for contributing valuable insights to my thesis work. I am very grateful to Professor Robert Schober, Professor Lutz Lampe, Professor Dave Michelson and Professor Vikram Krishnamurthy for serving on my committee. I would like to thank the instructors of my graduate courses for helping me obtain a good understanding of the basic concepts. Finally, I would like to thank all members of our lab for their support and for providing a stimulating and fun environment in which to learn and grow.

Chapter 1

Introduction

Recent explosive growth in the wireless communication market and proliferation of multimedia capable mobile devices has led to increase in demand for radio spectrum. However, most of the radio spectrum has already been licensed to various entities across different geographical areas giving them exclusive transmission rights in the allocated spectral bands. This was done to avoid interference between two systems operating in the same spectral band in close vicinity to each other. However, a recent study conducted by the Federal Communications Commission (FCC) found that most of the currently allocated radio spectrum is not efficiently utilized by the licensed (primary) users [19]. It has been suggested that the utilization of the radio frequency spectrum could be improved by giving opportunistic access of the spectrum to unlicensed secondary users. Cognitive radio (CR) is an emerging technology which would allow an unlicensed (cognitive) radio to automatically sense and make efficient use of any available radio spectrum at a given time [44]. CR design is, therefore, an innovative radio design philosophy which involves smartly sensing the swaths of spectrum and then determining the transmission characteristics of secondary

users based on the primary users behavior. Specifically, CR is likely to be built on software defined radio (SDR) [44], which would allow it to adjust its transmitter characteristics dynamically, based on the interaction with the environment in which it operates. Due to the immense potential of improving the spectral utilization by using CR, adaptive access system design for CR networks has emerged as one of the most important research areas in the field of wireless communications. The IEEE 802.22 standard based on CR technology for wireless regional access networks (WRAN) is presently under development, to bring broadband access to hard-to-reach rural areas with low population density [60].

Identifying the presence of licensed primary users is a very important task for a CR system [13, 63]. Fast and accurate spectrum sensing is necessary to improve the opportunistic spectrum access gains of the CR system and to decrease the interference caused to the primary user system. If the CR sensing system falsely determines that there is a primary user present, even though there is no primary user operating in the band, it would lead to a missed opportunity for transmission, which would decrease the CR throughput. On the other hand, if the the CR system misdetects the primary signal then it will lead to interference to the primary user which could be unacceptable to the primary user system. Nevertheless, the spectrum sensing process is a very difficult task, due to presence of wide range of primary users using different modulation schemes, transmission powers and data rates, secondary user interference, variable propagation losses and thermal noise.

Several signal processing techniques have been proposed in the literature to identify primary users [13]. The simplest of the proposed detectors is the energy detector that measures energy in a particular spectrum band and concludes presence of a primary user if the energy detected in the band is higher than a certain threshold [67]. The energy detector has low complexity and requires no knowledge of the primary user signal characteristics.

Performance of energy detection for the CR networks has been studied in [63]. Energy detection requires high sensing time to accurately detect a primary signal compared to other detectors. Moreover, it was shown in [62] that the energy detector fails to detect the primary signal at very low signal-to-noise ratio (SNR), due to presence of noise-uncertainty (uncertainty in estimating the background noise power). The SNR below which detection is impossible is called the SNR wall [62].

Another spectrum sensing technique is cyclostationary feature detection. A signal is said to be n^{th}-order cyclostationary if it exhibits periodicity in its n^{th}-order moments [24]. Most of the signals encountered in wireless communications are 2^{nd} order cyclostationary whereas the noise is stationary. As a result, the cyclostationarity of the primary signals can be used to detect their presence. The 2^{nd} order cyclostationarity of a signal is not reflected in the power spectral density (PSD). However, it is reflected in the spectral correlation density (SCD) function, which is obtained by the Fourier transform of the cyclic autocorrelation function [24]. The signal detectors based on cyclostationarity give better performance than the energy detectors for same number of signal samples and have lower SNR wall compared to energy detector. However, they are highly complex compared to energy detector and require knowledge of primary signal characteristics which might not always be available. Further, eigenvalue based detection was proposed for CR sensors equipped with multiple receiver antennas [77]. Eigenvalue based detectors utilizes the fact that background noise is uncorrelated across the receive antennas whereas the primary signal is correlated. The eigenvalue detector has a higher complexity compared to the energy detector.

One of the major issues with spectrum sensing using a single sensor is the impact of shadow fading due to presence of an obstacle between the primary transmitter and the CR

sensor [43]. For example, The CR sensing device may not detect the primary signal when the channel between the primary transmitter and the sensing device is under a deep fade. As a result, the CR system might transmit a signal in the corresponding primary user band, causing interference to the nearby primary receiver. This is called the hidden terminal problem and can have significant effect on the sensing performance of the CR system.

The burden on signal processing techniques can be reduced to a large extent by using cooperative diversity between CR spectrum sensors. Cooperative sensing among few sensing devices sufficiently distant from one another (in order to ensure independent propagation loss) can improve the detection efficiency of the sensing system and essentially help overcome the hidden terminal problem by countering the shadowing effects [43]. Alternatively, cooperative sensing can be seen as a means to reduce the sensing time for the same level of detection [21, 22]. Cooperative sensing would also reduce the impact of noise uncertainty on sensing system by lowering the SNR wall [43].

Recently, several cooperative spectrum sensing architectures for CR networks have been proposed in the literature [21–23, 43, 56, 63, 66]. In [56], it has been proposed that either, spectrum sensing devices can be collocated with the cognitive users or, a separate network of sensors could be used for spectrum sensing. The latter scheme could be used to save bandwidth of the cognitive users, as they do not need to allocate some of their transmission time period for sensing. This could especially be useful in the areas where CR density is expected to be high as the cost of having separate network of sensors can be compensated by the total throughput gain achieved. Several fusion architectures can be considered to combine the sensing data from various sensing devices. The most commonly proposed architecture is a parallel fusion network, in which all the sensing devices send their sensing information directly to an access point, which makes a final decision regard-

ing the presence or absence of the primary signal based on their sensing data using a data fusion rule [43, 66]. The parallel fusion rule is more robust to sensor failures and requires less processing at the sensors.

Another possible sensing architecture is the serial fusion architecture [70], in which each sensing devices sends its sensing data to another sensing device which based on the received sensing data and its own sensing data, makes a decision and sends its decision to the next sensing device. This process is continued until the last sensing device, which is generally the access point, makes a decision regarding the presence or absence of the signal. Yet another sensing mechanism is the decentralized sensing architecture, which does not have any access point [21, 22]. In this architecture, each individual user with a sensing device makes a decision regarding the presence or absence of signals based on its own data and data obtained from other sensing devices according to some predetermined rule.

1.1 Scope, Motivation and Objectives

In this thesis, we consider a parallel fusion cooperative sensing network. Each CR sensor uses energy detection to sense the primary user. Several cooperative sensing techniques for CR networks have been recently considered in the literature based on parallel fusion architecture [25, 43, 66]. There are several issues that need to be addressed in order to obtain maximum possible sensing gain from cooperation. In this thesis, we identify two major challenges involved in parallel fusion cooperative sensing schemes. The first challenge is to tackle malicious users, which send false sensing data to the access point. Another important challenge is to design fast and efficient methods to combine the sensing information available from various sensing devices.

Security is one of the most crucial aspects of CR cooperative sensing system [12, 78]. CR cooperative sensing system is vulnerable to two different kinds of security threats [12]. One is an outsider attack in which a malicious transmitter tries to manipulate the sensor readings by transmitting signals emulating the primary user signal characteristics. Techniques to identify these kind of attacks have been studied in [1, 16, 17]. In [16], the authenticity of the signal is tested by estimating the location of the origin of the signal. If the origin of the signal is not at the same location as that of the primary user transmitter, then the signal is considered malicious. In [17], signal classification algorithms were proposed to distinguish primary and malicious signals. In [1], a primary user emulator is identified using certain distinctive behavior in primary transmitter.

The other kind of security threat is the insider attack, where a user belonging to the CR sensor network sends false sensing information to the access point. It was shown in [43] that the presence of a few malicious users sending false sensing data can severely affect the performance of a parallel fusion cooperative spectrum sensing system. A CR user might be malicious for selfish reasons or due to sensor malfunctioning. In the former case, a CR might detect that the primary signal is absent. However, it might force the access point to erroneously decide that a primary signal is present by sending false sensing data. The malicious user can then selfishly transmit its own signal on the free channel. If the sensor is malfunctioning, it might generate random energy values. In this thesis, one of our goals is to identify such malicious users and weed them out of the system.

CR systems are proposed to simultaneously operate over multiple primary bands and dynamically use the available channels for transmission [30]. Multi-band sensing has been suggested in [42] to take advantage of sparse nature of the available spectrum. Sensing multiple bands simultaneously can help improve the opportunistic spectral gain by making

dynamic and efficient use of the free spectrum. Good spectral utilization requires quick sensing of large swath of spectrum with high accuracy. However, the sensing resources are usually limited in terms of sensing time and bandwidth. Moreover, due to bandwidth limitations in the control channels, the sensors might have to quantize their sensing data in order to reliably communicate it to the access point. Efficient ways to allocate sensors to various primary bands and quantize the sensing information need to be investigated to achieve maximum possible opportunistic spectral gain for such a system. In this thesis, we explore methods to assign narrow-band sensors to various primary user bands. We then investigate efficient techniques to determine the quantization thresholds at each sensor in each primary band.

The objectives of this thesis are as follows:

- Identify possible methods used by the malicious users to degrade the CR cooperative sensing system performance. Propose techniques to reliably detect the presence of the malicious users and nullify their effect on the performance of the sensing system.

- In a CR system operating in multiple bands, identify methods to assign CR sensors to various primary user bands and determine the energy detection thresholds at each sensor, taking into consideration the rates available in each primary band along with cost of interference with the respective primary users.

1.2 Literature Survey

In this section, we give an overview of the works related to the detection of insider attacks in CR cooperative sensing networks as well as the quantization and data fusion schemes for CR sensing systems.

1.2.1 Detection of Insider Attacks

Techniques to detect the insider attacks in CR cooperative sensing systems have recently received attention in the literature [15, 73–75, 77]. In [15], a technique to identify malicious users based on weighted sequential probability test was proposed in a system in which single-bit quantization is used at the sensors. Weights were assigned based on the reputation gained from the previous sensing iterations. If a user's decision is in agreement with the final decision at the access point then its weightage is increased and if not, its weightage is decreased. However, in [15], accurate knowledge of the primary signal distribution at the CR sensors is assumed which is not always available to the CR network. Also, the performance of the malicious user detection depends on the influence of the malicious users on final decision. If the malicious users can influence the final global decision, then the entire scheme would fail. In [76], a reputation-based CR spectrum sensing was proposed in which some of the users can be completely trusted. Through the assistance of these trusted nodes in the network, the malicious users are detected.

In [74], a scheme to identify the malicious nodes is proposed based on the CR sensors' past reports. The knowledge of the distance between primary user and CR sensors is assumed and then suspicious level of each node is calculated using Bayesian criterion based on the data measurements from all sensors. However, this requires knowledge of primary user signal distribution at the CR sensors based on distance between the primary user and CR sensors, which might be difficult to estimate. In [73], a robust cooperative sensing scheme was developed which takes into account the the possible presence of malicious user data while determining a fusion rule at the access point. They assume independent and identical primary signal fading at the sensors which is not true in practical scenarios due to presence of variable shadow fading and path losses. In [75], a malicious user detection

technique was proposed for ad hoc CR networks based on consensus algorithms.

In this thesis, we investigate schemes to identify the malicious users based on outlier detection techniques. An outlier is an observation which is far away from rest of the data [29]. Outlier detection techniques have been well studied in the field of database research to identify extreme data points [2, 4, 9, 29, 39]. Their applications include video surveillance, intrusion detection and identifying fraudulent transactions. Some of the outlier detection techniques have been recently applied to the sensor networks to identify suspicious sensor readings [8, 48, 58, 59]. Nevertheless, using the outlier detection techniques for CR cooperative sensing network has a very different set of challenges when compared to most of the sensor networks. For example, the CR sensor network is not aware whether a primary user signal is present or not. Further, it has limited knowledge of the underlying distribution of the data points when the primary signal is present. Thus, model based outlier detection schemes ([4, 29]) which assume a particular underlying data distribution cannot be applied. Further, even in the case when the underlying data distribution is not known, most of the sensor networks have large database of sensor readings from which the outliers can be efficiently detected using non-parametric methods [9, 39]. However, in CR networks, the number of collaborating sensors is generally low ($\sim 10-20$) [43] and these non-parametric outlier detection techniques cannot be directly applied to CR cooperative sensing systems. In this thesis, we take into consideration some of these constraints imposed by the CR scenario to devise novel malicious user detection techniques.

1.2.2 Sensor Allocation and Quantization

As a part of this thesis, we also investigate sensing schemes for CR system operating in multiple bands. In [52], a multi-band CR system operating with wide-band spectrum sen-

sors was considered, in which each sensor measures the signal energy in all primary bands. The energy detector output from each sensor is sent to the access point assuming perfect reporting channels. The access point then calculates a weighted sum of energy detector outputs from the sensors in each band, which is compared to a threshold in order to determine whether a primary signal is present or not. The set of equations to find the optimal weights were then presented and the optimization problem was shown to be non-convex. Sub-optimal weighing factors for each sensor data and energy detection threshold at the access point in each primary band were derived. In [54], the optimal weights were obtained by solving non-convex optimization problem using genetic algorithm.

However, in [52], the results are obtained for un-quantized data. However, in systems with control channel bandwidth limitations, quantization is necessary to transmit the sensing result reliably to the access point. Moreover, the wide-band sensing considered in [52] might require a very high sampling rate to precisely determine the band in which the primary user is present. Quantization scheme based on controlling the false discovery rate (FDR) was proposed for sensor networks in [53]. This technique was extended for multi-band sensing in [3]. However, the CR sensing system in [3] still requires multi-band energy detection at each sensor which would need large sensing time.

In this thesis, we consider a multi-band CR system in which sensors that can sense one primary band at a time. For such a system, it has been shown that a tradeoff can be achieved between the sensing time and the amount of collaborative gain obtained using cooperative sensing by dividing the sensors into clusters with each cluster of sensors operating in an assigned primary band [28, 61].

Efficient techniques to allocate sensors to various primary bands need to be investigated. The sensor allocation belong to a category of combinatorial optimization problems called

assignment problems. The original assignment problem [46] involved optimally assigning the "tasks" representing the jobs to be done to the "agents" representing the machines or the people that can do those jobs. There is a cost attached with assigning an agent to a task and the aim is to minimize the sum total cost. Several variations of the assignment problem with different cost functions and constraints have been studied [49]. In our thesis, the detection of signal in primary user bands represent the tasks and the CR sensors represent the agents. We propose various assignment algorithms to allocate CR sensors to primary users based on different cost functions.

Once the sensors are assigned to the primary users, techniques to quantize the sensing data are explored. Distributed detection and data fusion for the parallel fusion network is a well studied topic in the field of sensor networks [5, 64, 69, 70]. In general, the complexity of designing the optimum distributed detection (quantization) scheme increases exponentially with number of sensors and number of quantization levels. Even in case of independent and identical distribution of received primary signal energy at various sensing devices, the optimum quantization thresholds for each sensing device will not be same at all the sensors. Thus, the problem is highly complex to solve. Several low-complexity quantization schemes have been proposed in the literature [38, 41]. However, the design complexity of these quantizers is still very high. The design complexity can be reduced to a large extent by assuming that all sensors use identical quantization thresholds as it decreases the dimension of the optimization problem. However, this would degrade the performance of the cooperative sensing system. Nevertheless, it has been shown in [65], that for identical sensing data distribution, distributed detection performance based on sensing devices using identical quantization thresholds asymptotically approaches the optimum distributed detection performance as the number of sensors goes to infinity, in case of binary hypoth-

esis testing. Further, in [47], it was shown that using equal thresholds at the sensors and a *k*-out-of-*N* fusion rule at the access point is also asymptotically optimal in case of different variable fading losses among sensors. In a *k*-out-of-*N* fusion rule, the access point declares that the primary user is present only when *k* or more out of *N* sensors send bit '1' to the access point. It has been shown in the literature that 'OR' fusion rule (1-out-of-*N* fusion rule) is robust and gives performance close to that of the optimal *k*-out-of*N* fusion rule for many CR cooperative sensing system models [25].

Quantization and data fusion schemes for CR sensing systems operating in a single primary band has been considered in [14, 18, 57, 68]. In [14], locally optimal multi-bit quantization schemes were analyzed. Suboptimal schemes were then proposed based on iterative estimation of likelihood ratios. In [18], spatio-temporal quantization is considered where both spatial and temporal distributions of the primary signal distribution are utilized to design dynamic quantization levels. In [57], low complexity quantization schemes based on maximizing the deflection coefficient were proposed. In [68], control channel transmission errors were taken into consideration while determining the quantization thresholds.

In this thesis, we explore the multi-band CR sensing systems in which equal energy thresholds are used in all the sensors allocated to a particular primary band and a *k*-out-of-*N* fusion rule is used at the access point. We propose efficient schemes to determine sensor quantization thresholds in each primary band taking into account the throughput rates available in various bands and corresponding interference limitations.

1.3 Outline of the Thesis

The rest of this thesis is organized as follows:

- In Chapter 2, we propose malicious user detection schemes based on outlier detec-

tion techniques for CR cooperative sensing network. We take into consideration constraints imposed by the CR scenario, such as limited knowledge of the primary signal propagation environment and small size of the sensing data samples. Considering partial information of the primary user activity, we propose a novel method to identify the malicious users. We further propose malicious user detection schemes that take into consideration the spatial location of the CR sensors. The performance of the proposed schemes are studied using simulations.

- In Chapter 3, we consider a CR system operating in multiple primary bands. We explore methods to allocate the sensors to various primary user bands using assignment algorithms. We then investigate efficient techniques to determine the quantization thresholds at each sensor. We initially consider the case when the 'OR' fusion rule is used at the access point in each primary band. We then investigate quantization schemes for the case when the *k*-out-of-*N* fusion rule is used at the access point in each primary band. We compare the performance of the proposed schemes using simulations.

- Conclusions and possible directions for future research are discussed in Chapter 4.

Chapter 2

Malicious User Detection

2.1 Background

In this chapter, malicious-user detection schemes for CR cooperative sensing system are proposed based on the outlier-detection techniques [29]. Identifying malicious users in CR cooperative sensing system is very difficult since the malicious user detection schemes do not know whether a primary signal is present or not. Thus, they are unaware of the underlying distribution of the energy detector outputs. We also take into consideration further constraints imposed by the CR scenario such as the lack of complete information about the primary signal propagation environment, the absence of feedback from primary user network and the small size of the sensing data samples among which the malicious user data points need to be identified (It was shown in [43] that most of the gain through cooperation is achieved by using $\sim 10-20$ users). We only consider those malicious user detection schemes that are based on the non-parametric outlier detection techniques and hence, do not require the prior knowledge of the underlying data distribution parameters. Thus, the malicious user schemes detection proposed in this chapter are not influenced by uncertainty

in the noise measurement and do not require any feedback from the primary user system or knowledge of the location of the primary transmitter. Low number of spectrum sensors also make the detection of the malicious sensors among them very challenging. Robust as well as efficient outlier detection techniques are necessary to ensure reliable detection of the malicious users based on small size of sensor data samples. We later assume partial knowledge of the primary user activity and propose improved malicious user detection schemes based on this information. We also propose methods which consider the spatial location information of the CR users to further improve the performance of malicious user detection schemes, especially, for the CR systems spread over a wide area.

The rest of this chapter is organized as follows. In Section 2.2, we define the cooperative sensing system model and discuss the effect of malicious users on the system. In Section 2.3, we discuss techniques to assign robust and efficient outlier factors to the cognitive users based on their sensing data. In Section 2.4, we propose techniques which use these outlier factors to detect the malicious users present in the system. In Section 2.5, we propose malicious user detection technique which takes into consideration the users' spatial information. Section 2.6 describes the method used to compare the performances of various malicious user detection schemes for the case when equal gain combining is used as the fusion rule at the access point. Simulation results are presented in Section 2.7. Conclusions are finally drawn in Section 2.8.

2.2 System Model

We consider a group of N CRs with collocated spectrum sensors in the presence of a primary transmitter. All of the sensors use energy detectors. The sensors send their sensing data to an access point through control channels, which are assumed to be perfect. Based

on the data obtained from the sensors, the access point makes a decision regarding the presence or absence of the primary signal using a data fusion and detection scheme.

Let $e_n[l]$ represent the output of energy detector at n^{th} sensor during the l^{th} sensing iteration. Let hypotheses H_1 and H_0 denotes the presence and absence of a primary signal, respectively. The output of the n^{th} user's energy detector in the baseband is given by [67]

$$e_n[l] = \begin{cases} \int_{T_k}^{T_k+T-1} |h_n(t)s(t)+z_n(t)|^2 dt & ;H_1 \\ \int_{T_k}^{T_k+T-1} |z_n(t)|^2 dt & ;H_0 \end{cases} \tag{2.1}$$

where T denotes the length of the sensing interval, $s(t)$ is the primary transmitted signal and $h_n(t)$ represents the channel between the primary transmitter and the n^{th} spectrum sensor. $z_n(t)$ is the additive white Gaussian noise (AWGN) at the n^{th} sensor. In this chapter, we assume a generic wide area propagation model for the primary signal [55]. However, we assume no knowledge of the distributions of the channel gains between the primary transmitter and CR sensors.

2.2.1 Impact of Malicious Users

The presence of malicious users can significantly affect the performance of a CR cooperative sensing system [43]. A user might be malicious for selfish reasons or due to sensor malfunctioning. In the former case, a CR might detect that the primary signal is absent. However, it might force the access point to erroneously decide that a primary signal is present by sending false sensing data. The malicious user can then selfishly transmit its own signal on the free channel. If the sensor is malfunctioning, it might generate random energy values.

There are, generally, two ways in which malicious users can affect the cooperative

sensing system. They may send high energy values when there is no primary signal present, thus increasing the probability of a false alarm and decreasing the available bandwidth for the CR system. Malicious users may also send low energy values when the signal is present, thus decreasing the probability of detection of the primary signal and causing increased interference to the primary user system. Since most of the data fusion schemes at the access point take into consideration that some of the sensors will have weak channels from the primary transmitter, the impact of malicious users sending low energy values when a primary signal is present will, in general, be low on the performance of the cooperative sensing system. However, when the malicious users send high energy values when no primary signal is present, the impact on the performance of the cooperative sensing system will be much more severe. Thus, malicious user detection schemes should be efficient in identifying malicious users that falsely send high energy values to the access point. At the same time, the scheme chosen to identify these malicious users should not misdetect a non-malicious user as a malicious user. When the primary signal is present, it is especially important that the data of non-malicious users that receive good signal strength from the primary transmitter should not be rejected, as this would severely decrease the probability of detection of the cooperative sensing system leading to severe interference to the primary user system.

2.3 Assigning Outlier Factors

Each user is assigned a set of outlier factors based on the energy detector outputs. The outlier factor gives a measure of the outlyingness of a data point. These outlier factors are then used to identify and nullify the effect of malicious users. In this chapter, we assume that the outlier factor assignment schemes are unaware of the additive noise variance and

location of the primary transmitter and receives no feedback from the primary user system.

A simple way to assign outlier factors $o_n[l]$ based on the energy values obtained during the l^{th} sensing iteration is as follows:

$$o_n[l] = \frac{e_n^{dB}[l] - \mu[l]}{\sigma[l]} \tag{2.2}$$

where $e_n^{dB}[l]$ represents the energy detector outputs in decibels (dB), $\mu[l]$ and $\sigma[l]$ are, respectively, the sample mean and the sample standard deviation of the energy values $e_n^{dB}[l]$ of all users at a given iteration l. The sample mean is an estimate of the location of a distribution, and the standard deviation is an estimate of the scale. We proposed this method of outlier factor assignment in [37] to detect the malicious users in CR networks.

The energy-detector outputs are considered in dB because it is desirable that the underlying data distribution be close to symmetric when assigning outlier factors as in (2.2). If the underlying distribution is highly skewed (un-symmetric), then the valid data points lying on the heavy-tailed side of the skewed distribution will be assigned very high outlier factors. Distribution of $e_n[l]$ can have a high positive skew, especially in the presence of a primary signal. One way to reduce the positive skew in the data is to use logarithmic transformation (i.e., consider energy-detector outputs in dB). A more computationally complex and widely used technique to reduce skewness in any distribution is the Box-Cox transformation [6]. However, Box-Cox transformations are not robust against outliers. Moreover, most of the channel shadow-fading models in wireless communications follow a log-normal distribution. Therefore, if the sensors are distributed over a small area in which the path-loss component can be assumed to be same for all the sensors, taking the logarithm would make the distribution of energy detector outputs close to normal distri-

bution with low skew. Also, in the case where no primary signal is present, the logarithm operation does not induce significant negative skewness in the energy distribution.

However, there are several issues with assigning outlier factors as in (2.2). First, the mean and the standard deviation are not robust estimates and can be easily manipulated by the data of the malicious users, especially, in the case of un-quantized data fusion at the access point. Even a few malicious users can severely degrade the performance of the system without being detected when outlier detection schemes use non-robust location and scale estimates such as the mean and standard deviation. Therefore, robust alternatives to the sample mean and the sample standard deviation need to be studied. Secondly, these robust estimates of location and scale must also be efficient. The efficiency of a statistic determines the degree to which the statistic is stable from sample to sample. An estimate having low efficiency can have a huge deviation from the underlying distribution, especially for a low number of sample data points. Thirdly, the logarithm transformation does not completely remove the skew in the data under hypothesis H_1. The data might still have a high positive skew if the secondary user network size is large with variable path loss between the primary transmitter and the sensors. Techniques to tackle skewness in the energy distribution need to be explored.

2.3.1 Alternatives to the Mean

As discussed in Section 2.3.1, the sample mean is highly vulnerable to outliers. A robust alternative to the sample mean to estimate the location of a distribution in (2.2) is the median ($\tilde{\mu}$). One way to measure the robustness of an estimate is by its breakdown point. The breakdown point is the minimum proportion of contaminated points (outliers) in a sample that can make the estimate unbounded. Note that the outliers can still have an

impact on the estimate when their percentage is lower than the breakdown point. However, their effect would be limited and they cannot randomly change the estimate. The median has a 50% breakdown point compared to $\frac{100}{N}$% for the mean, where N is the sample size.

Even though the median has a very high breakdown point, its efficiency is low. The efficiency of a statistic is the degree to which the statistic is stable from sample to sample. Efficiency is defined as the ratio of the inverse of the Fisher information to the variance of the statistic [45]. An estimate having low efficiency can have a huge deviation from the underlying distribution, especially for a low number of sample data points. Therefore, high efficiency is very desirable in small sample sizes.

A more efficient and robust estimate of the location is the bi-weight estimate ($\hat{\mu}$) [45], which is calculated iteratively as follows:

$$\hat{\mu} = \frac{\sum w_n e_n^{dB}}{\sum w_n} \tag{2.3}$$

where

$$w_n = \begin{cases} \left(1 - \left(\frac{e_n^{dB} - \hat{\mu}}{c_1 S}\right)^2\right)^2 & : \quad \left(\frac{e_n^{dB} - \hat{\mu}}{c_1 S}\right)^2 < 1 \\ 0 & : \quad \text{Otherwise} \end{cases} \tag{2.4}$$

and

$$S = \text{median}\{|e_n^{dB} - \hat{\mu}|\} \tag{2.5}$$

The bi-weight estimate calculates a weighted mean with lower weightage being given to the observations away from the estimate. S is a measure of the spread of the underlying distribution. It measures the median absolute deviation from the location estimate $\hat{\mu}$. The parameter c_1 is called the tuning constant. Observations at a distance of more than c_1 times S from the estimate are assigned zero weight. Thus, c_1 can be used to determine the impact

of extreme data points on the calculation of the bi-weight estimate $\hat{\mu}$. It has been shown in the literature that the bi-weight estimate ($\hat{\mu}$) has higher efficiency than the median, is very robust and has a high breakdown point [45].

The performance efficiency of the bi-weight estimate can be understood better in terms of its empirical influence curve [45]. An empirical influence curve measures the influence of a new data point on an estimate calculated for a given sample of data as the new data point takes all possible values. In Fig. 2.1, we obtain influence curve for the mean, median and bi-weight estimate for a sample of 19 data points with values $(-0.9, -0.8, ..., 0.8, 0.9)$. The value of the 20^{th} data point is changed gradually from large negative values to large positive values and its influence is measured on the mean, median and bi-weight estimate.

As seen from Fig. 2.1, the sample mean can change from negative infinity to positive infinity along with the new data measurement; thus, it can be easily influenced by a malicious user. On the other hand, the median is not affected by a measurement outside a narrow range. The bi-weight estimate, however, only ignores data points that are substantially far away from rest of the data. It is much more sensitive to data that is at a moderate distance from the location estimate. Thus, the bi-weight estimate still considers the influence of data points that are not necessarily outliers. At same time, it restricts the outliers from having an influence beyond certain value. Thus, it is efficient as well as robust. The values of data points that are ignored can be adjusted using the tuning constant c_1. Generally, for a bi-weight estimate a tuning constant of $c_1 = 6$ is used [40].

2.3.2 Alternatives to Standard Deviation

One possible alternative to standard deviation for the scale estimate in (2.2) is the median absolute deviation (MAD). Median absolute deviation measures the median of the absolute

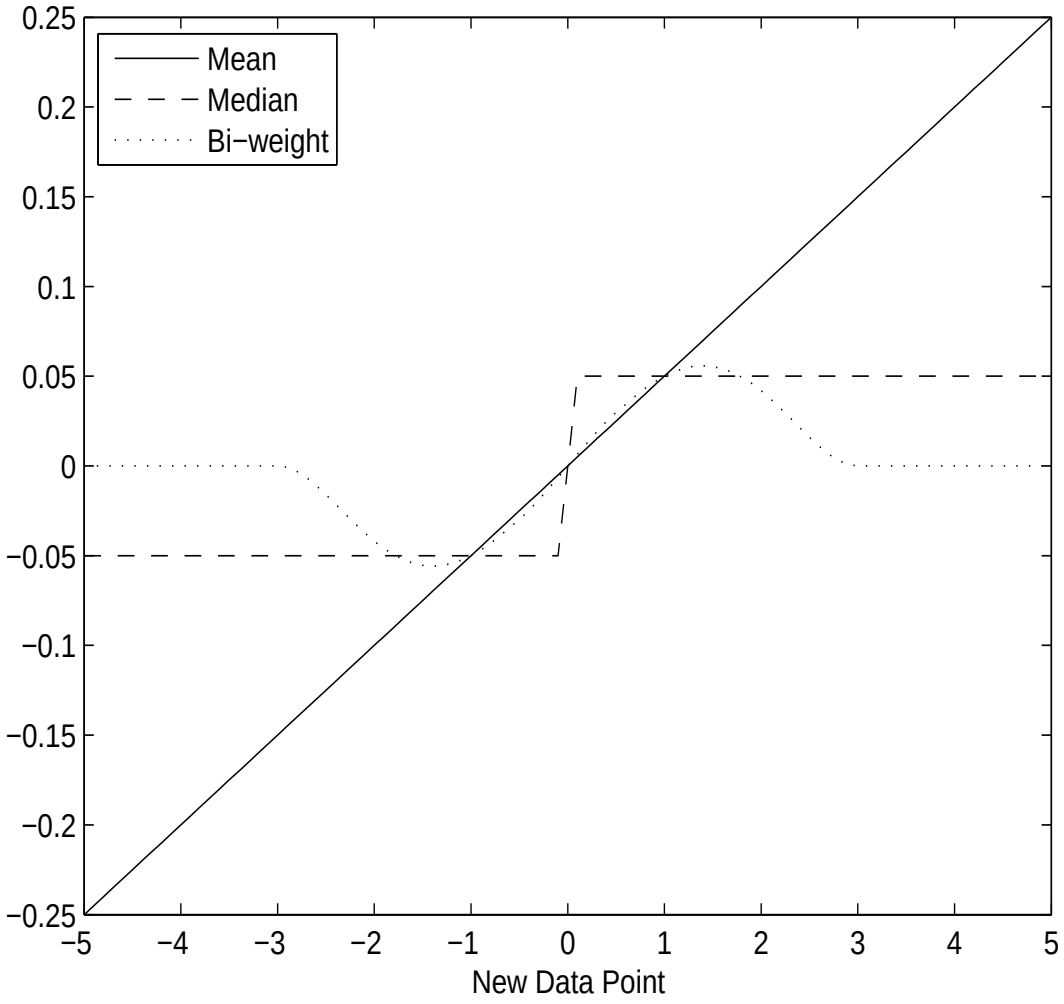

Figure 2.1: Empirical influence curves for mean, median and bi-weight location estimate.

distances of the data points from the sample median. MAD (σ_1) of the e_n^{dB} is given by

$$\sigma_1 = \text{median}|e_n^{dB} - \tilde{\mu}| \tag{2.6}$$

MAD has a breakdown point of 50%, and is used as a robust alternative to standard deviation in many applications. However, MAD is not an efficient estimate of the scale. It has an efficiency of only 36.74% for Gaussian distributions [40].

A more efficient and robust measure of scale is the bi-weight scale (BWS) given by [45]

$$\sigma_2 = \sqrt{\left(\frac{N \sum_{u_n^2<1} (e_n^{dB} - \mu^*)^2 (1-u_n^2)^4}{\left[\sum_{u_n^2<1} (1-u_n^2)(1-5u_n^2)\right]\left[-1+\sum_{u_n^2<1} (1-u_n^2)(1-5u_n^2)\right]} \right)} \tag{2.7}$$

where

$$u_n = \frac{e_n^{dB} - \mu^*}{c_2 \text{median}|e_n^{dB} - \mu^*|} \tag{2.8}$$

μ^* is a robust estimate of location such as the median ($\tilde{\mu}$) or the bi-weight estimate ($\hat{\mu}$). c_2 is the tuning constant. c_2 can be used to determine the impact of the extreme data points on the BWS estimate. Note that all of the summations in (2.7) are only over the values of n for which $u_n^2 < 1$. In [40], it was shown that BWS (σ_2) is very efficient for a wide range of symmetric distributions compared to other robust estimates of scale, particularly for the tuning constant $c_2 = 9$.

In Fig. 2.2, the empirical influence curves of the standard deviation, MAD and BWS for the same data sample $(-0.9, -0.8, ..., 0.8, 0.9)$ used in Section 2.3.2 are shown. As can be seen from the figure, the standard deviation is easily influenced by the new data point

whereas the MAD is not influenced by the new data point beyond a narrow range. The BWS is sensitive to the data points that are at a moderate distance from the location estimate and only ignores the extreme data points, like the bi-weight location estimate. Note that while calculating the bi-weight scale, a tuning constant of $c_2 = 9$ was found to be more efficient for a wide range of distributions, compared to a tuning constant of $c_1 = 6$ for the bi-weight location estimate. This is because the extreme observations contribute more substantial information about scale than about the location. Therefore, robust scale estimators should ignore fewer of the extreme observations to attain efficiency [40]. The optimal value of $c_2 = 9$ in calculating the BWS estimate was obtained through Monte Carlo simulations in [40].

BWS was used by Alan Gross [26] to define robust confidence intervals for bi-weight estimate as follows

$$\hat{\mu} \pm t_\nu \frac{\sigma_2}{\sqrt{N}} \tag{2.9}$$

where $\nu = 0.7(N-1)$ and t_ν is the Student-t distribution with ν degrees of freedom. Similarly, using a bi-weight location estimate and a variant of the BWS, Horn [32] proposed a technique for robust estimation of a $(1-\alpha)100\%$ prediction interval for the next observation X_{n+1} based on the observed random sample $x_1, x_2, ..., x_n$ drawn from a symmetric distribution. Based on these results, the percentage of sample values lying in the interval $[\hat{\mu} - \beta\sigma_2, \hat{\mu} - \beta\sigma_2]$ can be expected to be close to each other for a wide range of symmetric distributions. This means that the probability of o_n being greater than β using bi-weight estimates for location and scale would be similar for most of the symmetric distributions. This sort of consistency is essential in assigning outlier factors, since the outlier factors should give a consistent measure of the outlyingness of a data point, irrespective of the underlying distribution of $\{e_n^{dB}\}_{n=1}^N$ (which is generally short-tailed in the case of hypothesis

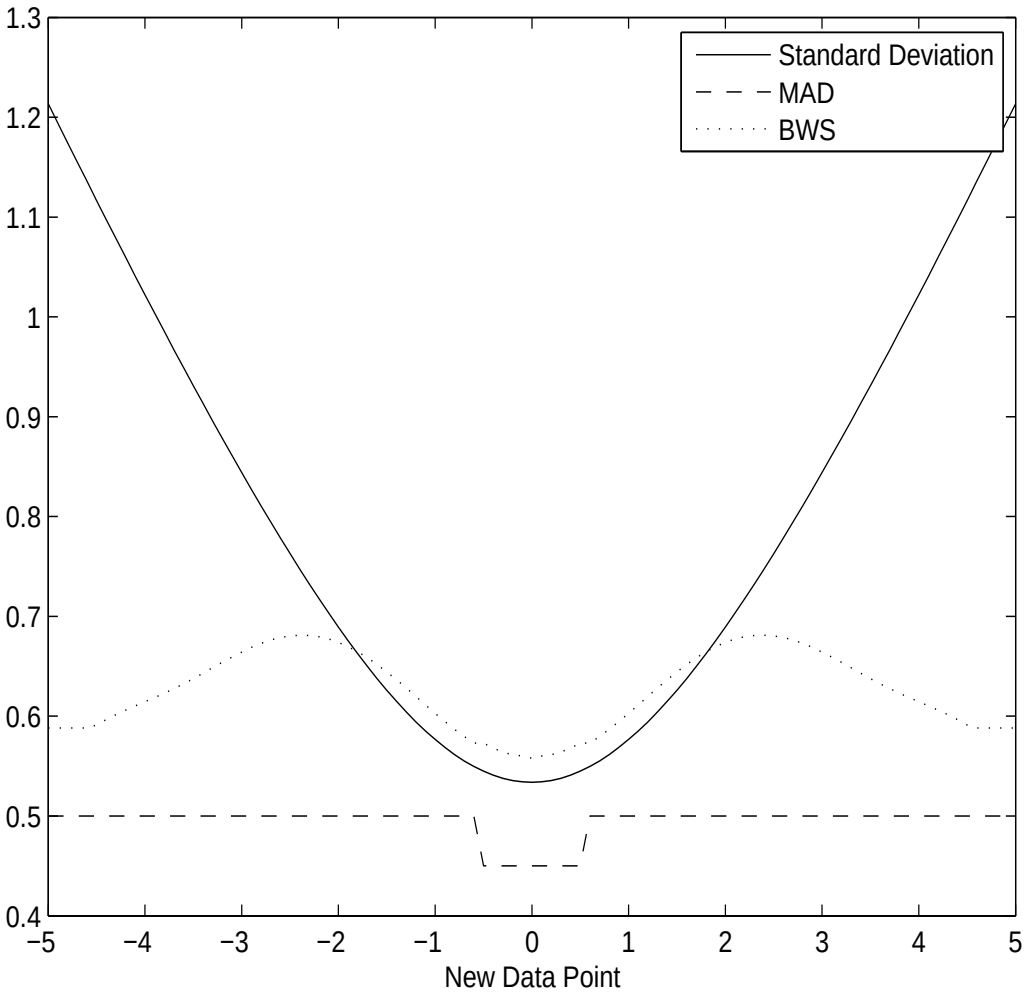

Figure 2.2: Empirical influence curves for standard deviation, median absolute deviation (MAD) and bi-weight scale (BWS).

H_0 and long-tailed in the case of hypothesis H_1).

2.3.3 Tackling Skew in the Data

The outlier detection techniques described in Sections 2.3.2 and 2.3.3 are effective for symmetric data distributions. However, significant positive skewness could be present in the energy distribution under hypothesis H_1 even after logarithm operation, particularly when the secondary user network spatial size is large, with few users having low path loss and the others having very high path loss. This would lead to assignment of high outlier values for the users having high channel gain when the primary signal is present, leading to severe degradation in probability of detection of the sensing system. However, as mentioned in Section 2.3.1, other transformations to remove skewness, such as the Box-Cox method, are not very robust against outliers.

Another way to tackle skew in the data distribution is to estimate the amount of skewness present in the data and then use it to modify the outlier factor. Skew in data is, generally, measured by its skew factor, given by

$$\gamma_1 = \frac{\frac{1}{N}\sum(e_n^{dB} - \mu)^3}{\sigma^3} \tag{2.10}$$

However, this measure is not robust and is easily influenced by the malicious user's data. Several robust estimates of skew factor have been studied in the literature [10]. Recently, a robust skew estimate called Med-Couple (*MC*) [11] was proposed. *MC* is given by

$$MC = \underset{e_i^{dB} < \tilde{\mu} < e_j^{dB}}{\text{med}} \frac{(e_j^{dB} - \tilde{\mu}) - (\tilde{\mu} - e_i^{dB})}{e_j^{dB} - e_i^{dB}} \tag{2.11}$$

MC has a breakdown point of 25% and has been shown to offer a good tradeoff between

robustness and efficiency compared to other robust estimates of skewness [10]. An exponential function of *MC* has been used in [33] to adjust the upper and lower limits of the Tukey box-plots used to detect the outliers. However, reliable estimation of *MC* would require a large number of data points. For small sample sizes, even a few malicious users can have a substantial effect on the *MC* estimate. Moreover, skew estimates exhibit significant variation from sample to sample for a low number of data points. Therefore, this measure cannot be used effectively to compensate for the skew, particularly for a low number of sensors.

2.4 Malicious User Detection

In this section, malicious user detection techniques are proposed that employ robust and efficient outlier factor assignment techniques discussed in Section 2.3. The maximum number of malicious users that the cooperative sensing system is expected to tolerate is denoted by M_{max}.

2.4.1 Method I

One method to identify the malicious users in the system is to compare the magnitudes of the outlier factors, computed using bi-weight as the location estimate and BWS as the scale estimate in Eq. (2.2), with a threshold θ_1 during each iteration. The users whose outliers values have the magnitude above the threshold are considered malicious. If the number of such users is more than M_{max}, then only the M_{max} users with the largest outlier factor magnitudes are considered malicious. The users identified as malicious are not used for the decision making process during the particular iteration. However, deciding whether a user is malicious or not just based on its present outlier factor can potentially degrade the

performance of the system. For example, in order to reliably detect the malicious users falsely producing high energy values a low detection threshold θ_1 is needed. However, if the primary signal is present, a non-malicious cognitive user with very good channel between its receiver and the primary user might have a high outlier factor especially if the distribution of the primary user SNR at the CR users is skewed. Thus, lower threshold value θ_1 would increase the chances of misdetection of such a user as malicious, which might severely decrease the probability of detection of the primary user signal by the cooperative sensing system. On the other hand, if a high outlier detection threshold is used, then the malicious users can potentially report higher energy values without being identified as the bad users. This could drastically increase the probability of false alarm of the system affected by the 'Always Yes' malicious users. If the primary user does not change its state over a period of time, it is not possible to determine without *a priori* knowledge of primary user signal statistics, the channel conditions between primary user transmitter and CR sensors or the background noise level, whether the high outlier factor is due good channel between the primary user and the CR sensor or due to false data.

2.4.2 Method II

If the primary user system is dynamic, with the primary user signal appearing and disappearing after every few sensing iterations, the malicious user detection schemes can be further improved. Significant increase in the energy values of the CR users from one sensing iteration to another would, in general, imply that the primary user has started transmission during the particular sensing iteration. Similarly, when the energy values of sensors show significant decrease, it might be an indication that primary user has stopped transmission. The change in the energy values of the CR users, as the state of the primary user changes

over a period of time, can be used to detect those malicious users which do not exhibit similar behavior as rest of the users. However, it is important to precisely identify the iteration during which the change in the energy values is due to change in the state of primary user rather than due to malicious users or fluctuations in noise and fading components. In this subsection, we propose a technique, based on robust statistics discussed in Section 2.3, to identify the iterations during which there was a change in the primary user state and using it to detect the malicious users.

During each iteration, the energy values of users having very high outlier factor magnitudes that are above a certain threshold θ_2 are ignored and the adjusted bi-weight estimate $\hat{\mu}_a[l]$ and adjusted bi-weight scale $\hat{\sigma}_a[l]$ are estimated using remaining energy values. θ_2 is generally used to eliminate only extreme outliers. If the number of outlier factors with magnitudes above θ_2 is more than M_{max}, only M_{max} energy values are ignored before evaluating the adjusted bi-weight location and scale estimates. The difference between the adjusted bi-weight estimate $\hat{\mu}_a[l]$ from iteration l and the adjusted bi-weight estimate from the iteration $l-1$ is obtained as follows

$$\Delta\hat{\mu}_a[l] = \hat{\mu}_a[l] - \hat{\mu}_a[l-1] \tag{2.12}$$

If the adjusted bi-weight increases from the $l-1^{th}$ iteration to the l^{th} iteration (i.e. if $\Delta\hat{\mu}_a[l]$ is positive), it could be due to the appearance of primary user signal in between iterations l and $l-1$. It is also possible that the primary user has remained in the same state (i.e. it hasn't started transmission) and the increase in the bi-weight estimate is due to fluctuations in the channel fading and noise components or due to the presence of malicious users. However, a malicious user data has only limited impact on the adjusted bi-weight estimate,

especially since the data of users with very large outlier factor magnitudes is eliminated. The impact of variations in noise and fading components will not be significant compared to increase due to appearance of a primary signal as long as there are few non-malicious users with good channels between primary user and their sensors. Similarly, if the $\Delta\hat{\mu}_a[l]$ is negative, it could be due to disappearance of primary user signal, malicious users or due to variations in channel fading and noise components. However, magnitude of $\Delta\hat{\mu}_a[l]$, in general, is expected to be higher if the primary user stops transmission.

At each sensing iteration, $\Delta\hat{\mu}_a[l]$ from previous K iterations are taken into consideration. Among these K iterations, we identify the set of $K_m/2$ iterations $S_+[l]$ such that $\Delta\hat{\mu}_a[l']$, for $l' \in S_+[l]$, are positive with $K_m/2$ largest magnitudes, and the set of $K_m/2$ iterations $S_-[l]$ such that $\Delta\hat{\mu}_a[l']$, for $l' \in S_-[l]$, are negative with $K_m/2$ largest magnitudes. Thus, $S_+[l]$ represents the set of iterations during which there is a high chance that the primary user has started transmission and $S_-[l]$ represents the set of iterations during which the primary user might have stopped transmission.

The penalty factors $P_n[l]$ are now assigned to each user as follows:

$$\begin{aligned} P_n[l] &= \sum_{l' \in S_+[l]} \left(o_n^+[l'-1] + o_n^-[l']\right) \\ &\quad + \sum_{l' \in S_-[l]} \left(o_n^-[l'-1] + o_n^+[l']\right) \end{aligned} \tag{2.13}$$

where

$$o_n^-[l'] = \begin{cases} -\frac{e_n^{dB}[l'] - \hat{\mu}_a[l']}{\hat{\sigma}_a[l']} & ; e_n^{dB}[l'] < \hat{\mu}_a[l'] \\ 0 & ; \text{Otherwise} \end{cases} \tag{2.14}$$

$$o_n^+[l'] = \begin{cases} \frac{e_n^{dB}[l'] - \hat{\mu}_a[l']}{\hat{\sigma}_a[l']} & ; e_n^{dB}[l'] > \hat{\mu}_a[l'] \\ 0 & ; \text{Otherwise} \end{cases} \tag{2.15}$$

Therefore, for all values of $l' \in S_+[l]$, during which the primary user has most likely started transmission, magnitudes of only negative adjusted outlier factors $o_n^-[l']$ for iteration l' and positive adjusted outlier factors $o_n^+[l'-1]$ for iteration $l'-1$ are added to the penalty factor, and for values $l' \in S_-[l]$, the magnitudes of only positive adjusted outlier factors $o_n^+[l']$ for iteration l' and negative adjusted outlier factors $o_n^-[l'-1]$ for iteration $l'-1$ are added to the penalty factor.

Suppose a user consistently produces high energy values irrespective of the presence or absence of the primary user. If in between iterations $l-1$ and l the primary user reappears, then $\Delta\hat{\mu}_a[l]$ will be positive. As a result, the users producing high energy value during iteration $l-1$ will receive a penalty factor based on their adjusted outlier factors from iteration $l-1$. Also, the CR sensors with low primary SNR will be assigned a penalty factor based on their adjusted outlier factors from iteration l. However, these sensors will not have significant impact on the final decision at the access point. In a similar way, malicious users and CR users with low primary user SNR will also be assigned a high penalty factor when the primary user disappears in between iterations $l-1$ and l. Sometimes, the sensors with high primary user SNR could be assigned penalty factors. This would usually happen when some of K_m iterations chosen from previous K iterations do not correspond to a change in state of the primary user. In such scenario, adjusted bi-weight might decrease due to fluctuations in fading and noise components even though the primary user was present during both iterations $l-1$ and l. The choice of K_m and K would depend upon the number of times a primary user is expected to change its state during a given time period. For a good choice of K_m and K, the proposed method would avoid assignment of high penalty factors to non-malicious CR users having high primary user SNR as long as there are few CR users with good channels between primary user and their sensors.

Based on these penalty factors another set of the outlier factors $\bar{o_n}[l]$ are defined as follows:

$$\bar{o_n}[l] = \frac{P_n[l] - \hat{\mu}_P[l]}{\hat{\sigma}_P[l]} \tag{2.16}$$

where $\hat{\mu}_P[l]$ and $\hat{\sigma}_P[l]$ are bi-weight location and scale estimates of $P_n[l]$. A positive threshold θ_3 is applied to determine the malicious users. All the users with positive outlier factors above this threshold (or users with the M_{max} largest outlier factors if the number of users with outlier factors above θ_3 is more than M_{max}) are considered malicious.

Method IIa

If a malicious user is aware that Method II is being used at the access point, it can avoid sending false values whenever the state of primary user changes. Even though the malicious user could be identified using Method II, since it would be not be sure whether the primary user would change its state during the next iteration, it could still escape getting assigned a high penalty factor. In this section, we propose a method to identify such smart malicious users. We define

$$\Delta\hat{\mu}_a^{\delta}[l] = \hat{\mu}_a[l] - \hat{\mu}_a[l-\delta] \tag{2.17}$$

K_m^{δ}, $S_+^{\delta}[l]$ and $S_-^{\delta}[l]$ are defined based on $\Delta\hat{\mu}_a^{\delta}[l]$ in a similar way as K_m, $S_+[l]$ and $S_-[l]$ were defined based on $\Delta\hat{\mu}_a[l]$. The penalty factors $P_n^{\delta}[l]$ are assigned as follows:

$$\begin{aligned} P_n^{\delta}[l] \;=\; & \sum_{l' \in S_+^{\delta}[l]} \left(o_n^+[l'-\delta] + o_n^-[l']\right) \\ & + \sum_{l' \in S_-^{\delta}[l]} \left(o_n^-[l'-\delta] + o_n^+[l']\right) \end{aligned} \tag{2.18}$$

Final penalty factors are assigned as follows

$$P_n[l] = \sum_{\delta \in D_\delta} P_n^{\delta}[l] \tag{2.19}$$

where D_δ is the set of δ values considered. The outlier factors $\bar{o_n}[l]$ are calculated as in (2.16). Values of $\delta > 1$ could be used to identify the smart malicious users mentioned earlier. Moreover, δ values can also be chosen randomly by the access point. Both Methods II and IIa, cannot accurately identify malicious users which send false sensing values once every few iterations keeping their overall penalty factors low. However, the impact of such malicious users would be less on the throughput of the cooperative sensing system.

2.5 Malicious User Detection Using Spatial Information

As mentioned in earlier sections, significant skewness could be present in the energy distribution under hypothesis H_1 even after logarithm operation, particularly when the CR network spatial size is large. Another way to tackle skew is to estimate the skewness present in the data by calculating the skew factor and then use it to modify the outlier factors [10, 33]. However, for small sample sizes, robust skew estimates exhibit significant variation from sample to sample and the false data points can have a substantial effect on the estimate. Therefore, these measures cannot be used effectively to compensate for the skew, particularly for a low number of sensors.

If the spatial location of the CR users is available at the access point, then the outlier factor can be assigned to each user based on the energy-detector outputs of its closest spatial neighbors. In wireless communication systems, the distribution of the energy-detector outputs is generally expected to be less skewed for sensors spread over a small area, com-

pared to sensors spread over a larger area. Spatial outlier factors $o_n^s[l]$ are computed as follows

$$o_n^s[l] = \frac{e_n^{dB}[l] - \hat{\mu}^s[l]}{\hat{\sigma}^s[l]} \tag{2.20}$$

where $\hat{\mu}^s[l]$ and $\hat{\sigma}^s[l]$ are the bi-weight estimate and bi-weight scale of the energy values of the A closest neighbors of a user n (including the user n). Based on $o_n^s[l]$ calculated as in (2.20) and $o_n[l]$ calculated as in (2.2), a final outlier factor $o_n^f[l]$ is assigned as follows:

$$o_n^f[l] = \begin{cases} \min\{|o_n^s[l]|, |o_n[l]|\} & ; o_n[l] \geq 0 \\ -\min\{|o_n^s[l]|, |o_n[l]|\} & ; o_n[l] < 0 \end{cases} \tag{2.21}$$

The minimum of $o_n^s[l]$ and $o_n[l]$ is taken instead of just assigning $o_n^s[l]$ as the outlier factor of each user to prevent assignment of high outlier factors to certain non-malicious users. For example, a non-malicious user might have a high channel gain from the primary transmitter compared to rest of the sensors in its spatial neighborhood, thus, getting a high spatial outlier factor o_n^s under Hypothesis H_1. However, when compared to other sensors in the entire system the channel gain of this particular user is not too high to raise any suspicion. Taking just o_n^s will lead to erroneous assignment of high outlier factor to such non-malicious user.

Malicious users can now be identified by Method I discussed in Section 2.4.1, using the values $o_n^f[l]$ instead of $o_n[l]$. Alternatively, Method II discussed in Section 2.4.2 can be used. The algorithm remains the same except that $o_n^-[l]$ in (2.14) and $o_n^+[l]$ in (2.15) are

assigned:

$$o_n^-[l'] = \begin{cases} \min\{|\bar{o}_n^s[l']|, |\bar{o}_n[l']|\} & ; \bar{o}_n[l'] < 0 \\ 0 & ; \text{Otherwise} \end{cases} \tag{2.22}$$

$$o_n^+[l'] = \begin{cases} \min\{|\bar{o}_n^s[l']|, |\bar{o}_n[l']|\} & ; \bar{o}_n[l'] \geq 0 \\ 0 & ; \text{Otherwise} \end{cases} \tag{2.23}$$

where

$$\bar{o}_n^s[l'] = \frac{e_n^{dB}[l'] - \hat{\mu}_a^s[l']}{\hat{\sigma}_a^s[l']} \tag{2.24}$$

$$\bar{o}_n[l'] = \frac{e_n^{dB}[l'] - \hat{\mu}_a[l']}{\hat{\sigma}_a[l']} \tag{2.25}$$

where $\hat{\mu}_a^s[l']$ and $\hat{\sigma}_a^s[l']$ are the new spatial neighborhood bi-weight location and scale estimate obtained after eliminating users with outlier factors having magnitudes above the threshold θ_2.

2.6 Performance Analysis

In this section, a method to compare the performances of the proposed malicious user detection schemes is considered. The equal gain combination scheme is considered at the access point [71]. The equal gain combining method is as follows:

$$\frac{1}{N}\sum_{n=1}^{N} e_n[l] \underset{H_0}{\overset{H_1}{\gtrless}} e_T \tag{2.26}$$

where e_T is the detection threshold used at the access point.

The performances of the malicious user detection schemes are analyzed by defining

measures additional probability of false alarm $\bar{P_f}$ and additional probability of misdetection $\bar{P_m}$ as follows:

$$\bar{P_f} = Pr(\hat{d_m} = 1/\hat{d_0} = d = 0) \tag{2.27}$$

$$\bar{P_m} = Pr(\hat{d_m} = 0/\hat{d_0} = d = 1) \tag{2.28}$$

where d is the primary user state ($d = 1$ and $d = 0$ denote the presence and absence of the primary signal, respectively), $\hat{d_0}$ is the decision made by the ideal malicious user detection scheme that correctly identifies and ignores the data of the malicious users. $\hat{d_m}$ is the decision made by a system, affected by the malicious users, implementing the proposed malicious user detection scheme. Thus, when the primary user is not present, $\bar{P_f}$ represents the probability that the malicious user identification scheme fails to detect the malicious users or misdetects non-malicious user as malicious resulting in a wrong decision $\hat{d_m} = 1$, when in fact the ideal malicious user detection scheme would have made the correct decision $\hat{d_0} = 0$. Similarly, when the primary user is present, $\bar{P_m}$ represents the probability that malicious user detection scheme fails to detect the malicious user or misdetects a good user as a malicious user resulting in making a wrong decision $\hat{d_m} = 0$ when for the same set of energy values an ideal malicious user detection scheme would have made the correct decision $\hat{d_0} = 1$.

In malicious user detection Methods I and II described in Section 2.4, the values of $\bar{P_f}$ and $\bar{P_m}$ depend on the outlier detection thresholds θ_1 and θ_3, respectively. The trade-off between $\bar{P_f}$ and $\bar{P_m}$, as the values of thresholds θ_1 and θ_3 are varied, is studied to analyze the performance of the malicious user detection schemes.

2.7 Simulation Results

We consider a cooperative sensing system with $N = 20$ users. A generic wide area propagation model is considered for the primary signal [55]. The path loss constant is 5. The standard deviation of log-normal shadowing is 5 dB. The correlation between shadowing components of two sensors is assumed to be exponentially decreasing with the distance between the sensors, with a correlation of 0.3 at a distance of 10m [27]. Independent and identically distributed small-scale Rayleigh fading is assumed at each sensor. The sensing period at each sensor is given by $T = 5/B$, where B is the channel bandwidth. The CR sensors are assumed to be stationary with fixed path loss and shadowing components. Outlier factors are calculated using bi-weight location and scale estimates. BWS is calculated using the median as the location estimate μ^* in (2.7) and (2.8). The threshold e_T in (2.26) is chosen so that the probability of false alarm at the fusion center is 0.01. We assume that the probability of a primary user being present during a sensing iteration is 0.5 and this probability is independent from one iteration to another. We consider 'Always Yes' malicious users that generate values that are randomly distributed between the values $4e_T$ and $8e_T$. M represents the number of malicious users present in the system.

We assign the spatial locations of the sensors using a two-dimensional model. The (X,Y) coordinates of the primary user transmitter are $(0,0)$. In Fig. 2.3, we assume that the sensors are distributed in an area of $50m \times 50m$ as 5×4 uniform rectangular grid. The X and Y coordinates of the sensors lie between the values $100m$ and $150m$. Ignoring fading effects, the SNR at $(100m, 100m)$ is -5dB. The number of malicious users is $M = 1$ and the maximum number of malicious users tolerated is $M_{max} = 2$. The location of the malicious user is chosen as $(100m, 100m)$. Performances of the Methods I and II are compared. In case of Method II, the threshold θ_2 which is used to eliminate extreme outliers before

calculating adjusted bi-weight location and scale estimates is chosen to be 4. We see that Method II significantly outperforms Method I. Moreover, the performance improves as value of K increases for given K_m/K ratio. It should also be noted that the $\bar{P_f}$ cannot be reduced below a certain value for each malicious user detection scheme, since at low values of outlier detection thresholds, some of the good users are misidentified as bad users. The case when no malicious node detection scheme is used corresponds to the left end of the performance curve of Method I (at low $\bar{P_m}$), i.e., for very high detection threshold (θ_1) at which the malicious user is not detected. As we can see, the malicious user significantly increases the probability of false alarm of the system.

In Fig. 2.4 and Fig. 2.5, we assume that the sensors are distributed in an area of $225m \times 225m$ as 5×4 uniform rectangular grid. The X and Y coordinates are distributed between the values $25m$ and $250m$. Ignoring fading, the primary user SNR at $(100m, 100m)$ is -5dB and 3dB in case of Fig. 2.4 and Fig. 2.5, respectively. All other parameters are similar to those used in Fig. 2.3. The skew in the received energy distribution in dB under hypothesis H_1 is generally expected to be higher compared to the system considered in Fig. 2.3. We consider the performance of Method I and II for $M = 1$ and $M_{max} = 2$. The location of the malicious user is chosen to be $(25m, 25m)$. We see from Fig. 2.4 that compared to the system considered in Fig. 2.3, to achieve similar decrease in the value of $\bar{P_f}$ would result in higher $\bar{P_m}$. This is due to higher probability of misdetection of CR users with strong channels from primary user as malicious. Moreover, the impact of eliminating such users on the sensing system would be higher. We also notice that at higher SNR values, as in Fig. 2.5, Method II offers significant improvement in the performance.

In Fig. 2.6, we consider the performance of Method II for the system considered in Fig. 2.4. We vary the value of K keeping K_m constant at 16. We see that the performance of

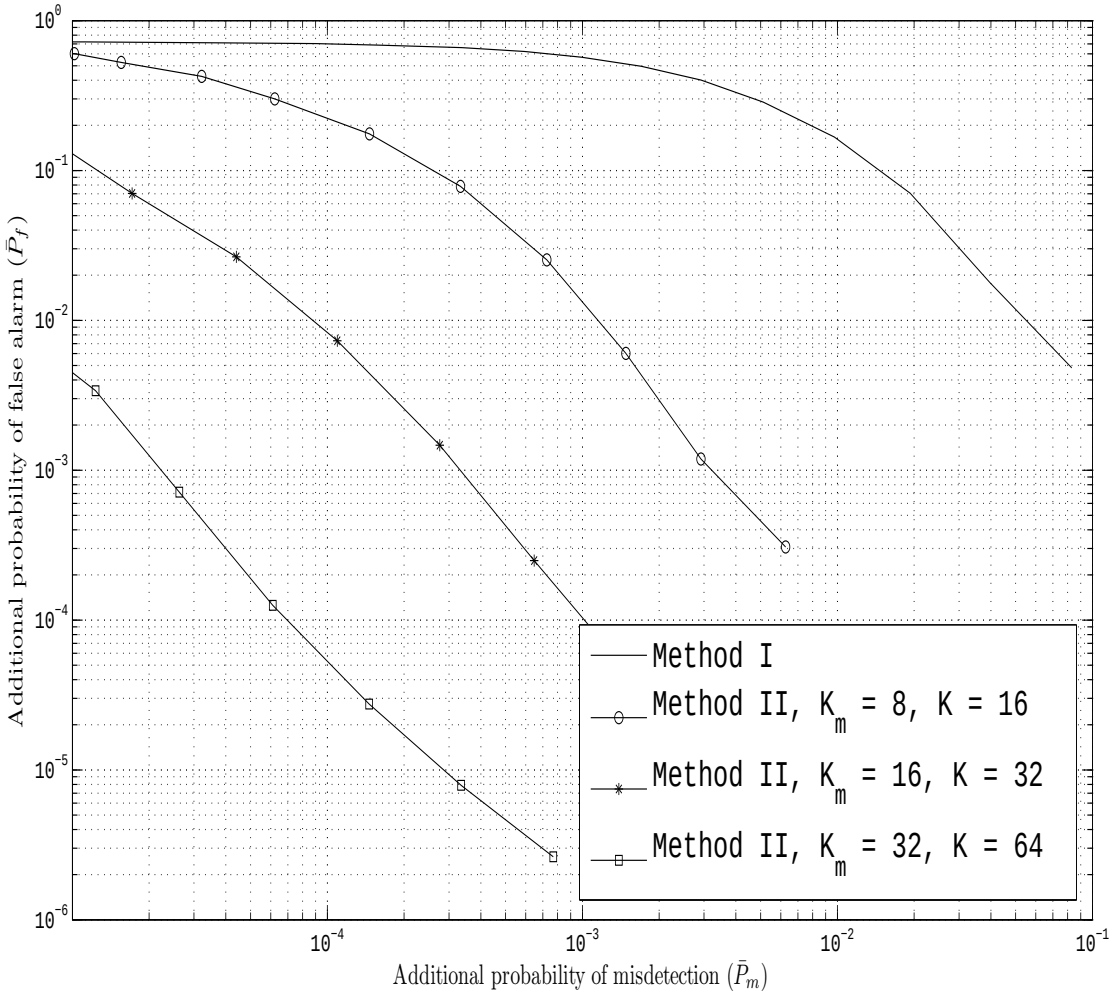

Figure 2.3: Performance of malicious user detection schemes for CR network spread over a small area in the presence of $M = 1$ malicious user and $M_{max} = 2$.

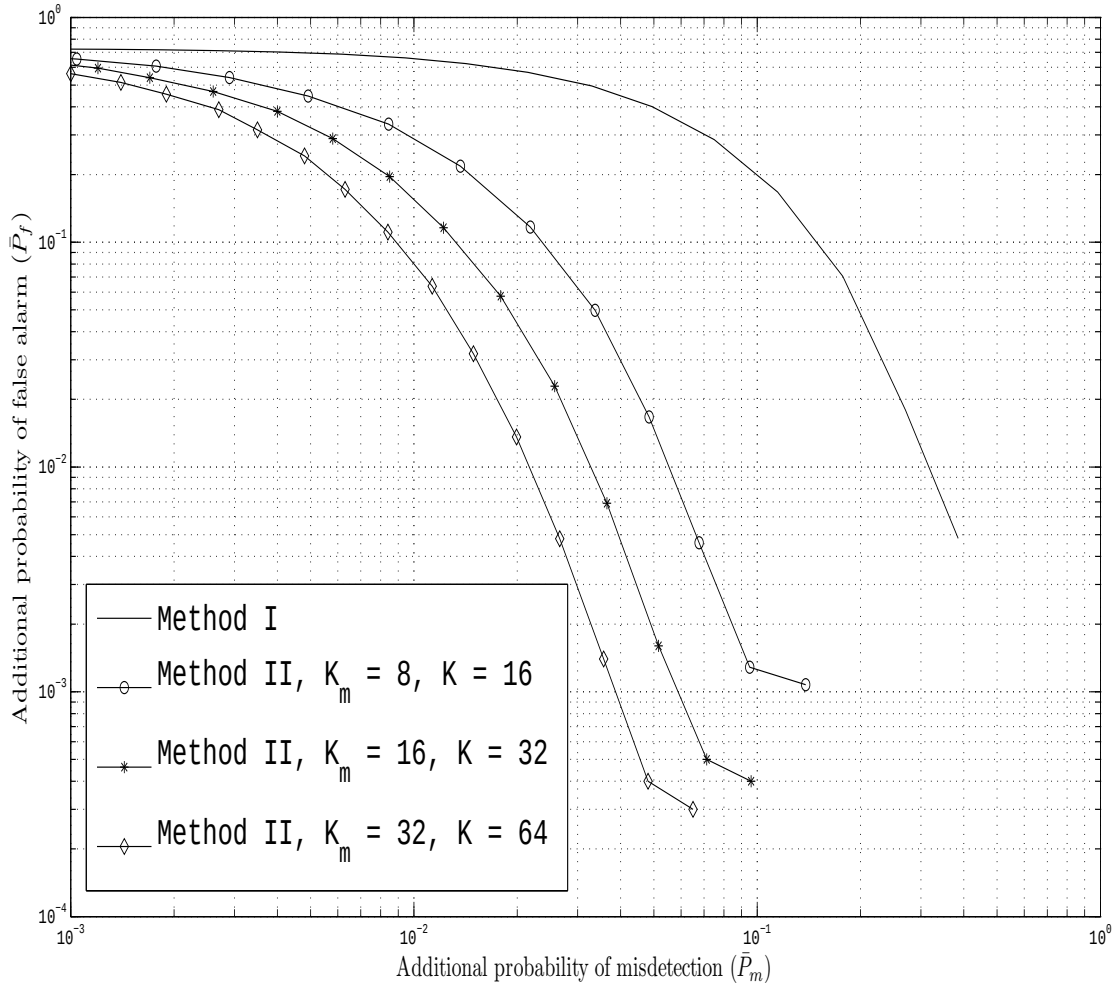

Figure 2.4: Performance of malicious node detection schemes for CR network spread over a large area in the presence of $M = 1$ malicious user with primary user SNR at (100m, 100m) ignoring fading effects = -5dB.

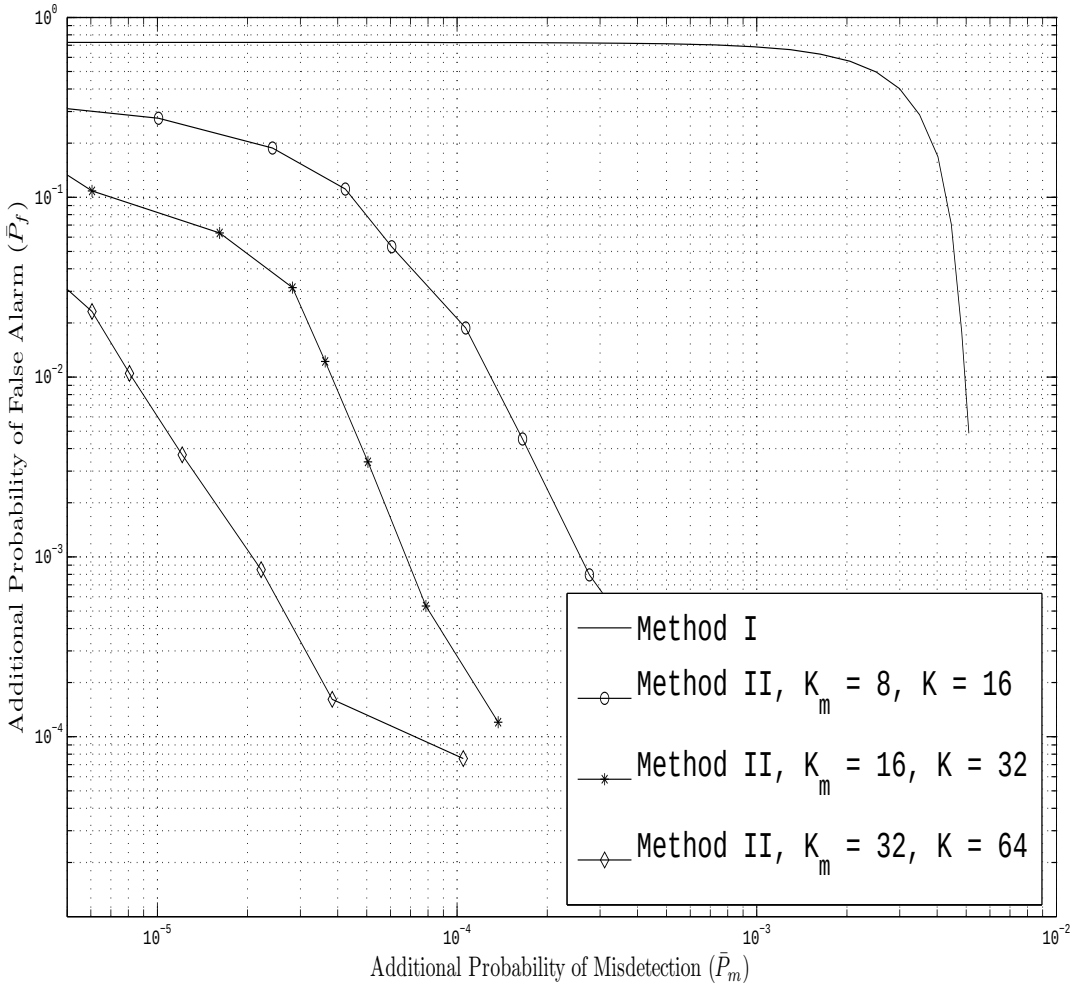

Figure 2.5: Performance of malicious node detection schemes for CR network spread over a large area in the presence of $M = 1$ malicious user with primary user SNR at (100m, 100m) ignoring fading effects = 3dB.

the malicious user detection scheme increases with increasing value of K. This is because for larger values of K, the K_m iterations during which the change in the bi-weight location estimate has been largest, more precisely corresponds to the change in the state of the primary user. However, an increase in K also leads to latency in malicious user detection scheme.

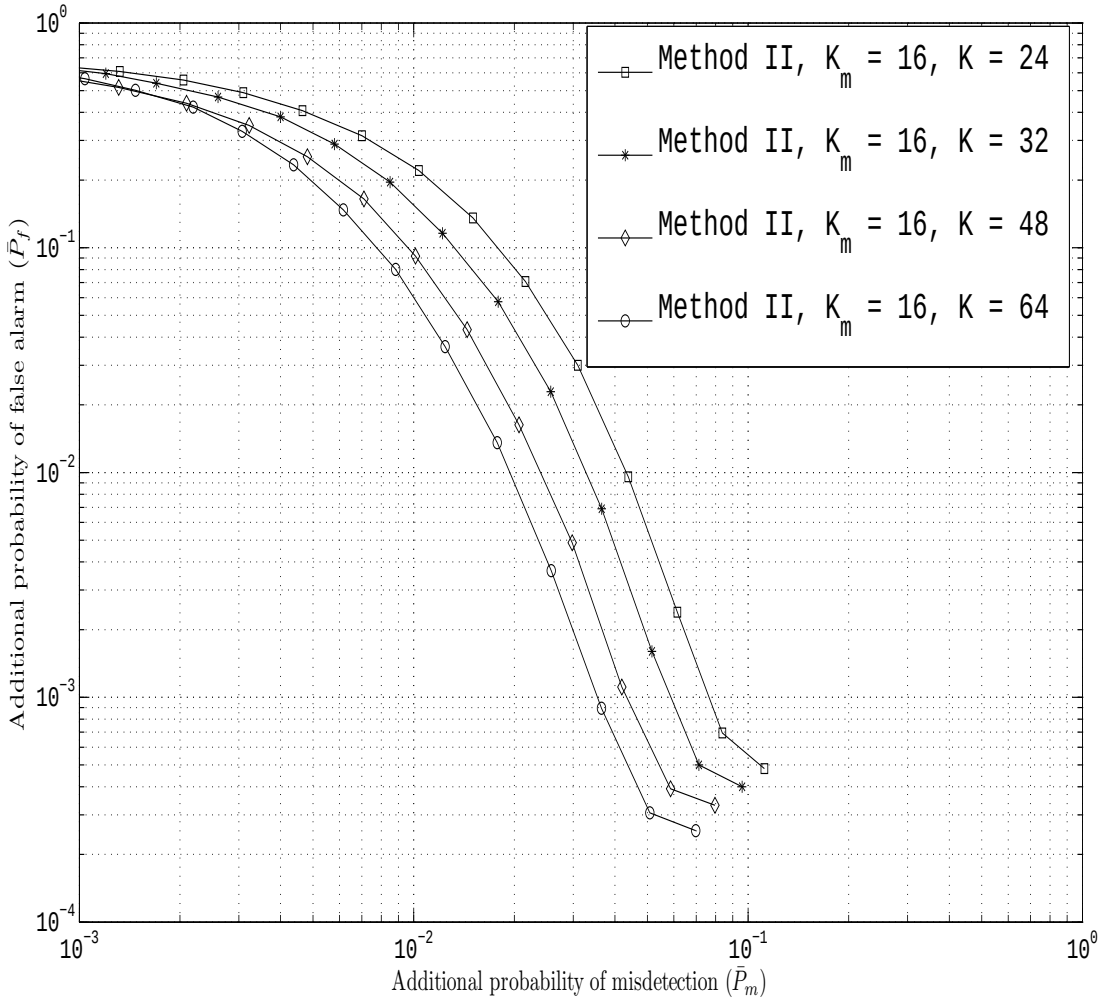

Figure 2.6: Performance of Method II at different values of K for $M = 1$, $M_{max} = 2$ and $K_m = 16$.

In Fig. 2.7, we consider the performance of Method II at different values of K_m keeping K constant at 32, for the system considered in Fig. 2.4. We observe that the best performance is obtained when K_m is $0.5K$. This is due the nature of the primary user considered in these simulations. Since, the probability of primary user being in state $d = 1$ (primary user signal present) or state $d = 0$ (primary user signal absent) is assumed to be 0.5 and independent from one iteration to another, the most likely number of primary user state transitions during the K iterations would be $0.5K$. Therefore, if $K_m < 0.5K$, there is a high probability that the some of the iterations during which there was a change in the primary user state have not been considered in assigning penalty factor, leading to poorer performance. If $K_m > 0.5K$, there is a high chance that some of iterations during which there was no change of state of the primary user have been considered in assigning penalty factor, again leading to a poorer performance. Thus, more precise knowledge of the primary user activity (expected number of state transitions in a given time interval) can be used to appropriately choose K_m and K.

In Fig. 2.8, Fig. 2.9 and Fig. 2.10, we consider the performance of Methods I and II at different values of M for $M_{max} = 20$. The system considered is similar to the system analyzed in Fig. 2.4. The primary user SNR (ignoring fading effects) at $(100m, 100m)$ is assumed to be -5dB, 0dB and 8dB in Fig. 2.8, Fig. 2.9 and Fig. 2.10, respectively. We assume that all malicious users collude together and produce equal high energy values. We consider the worst possible case in which all the malicious users in the system are the ones spatially closest to the primary user. In case of Method II, we choose K_m = 16 and $K = 32$. We see that the performance of Method II degrades more compared to that of Method I as M increases. This is especially true at low values of primary user SNR (Fig. 2.8). This is because at low primary user SNR values there are not enough non-malicious users with

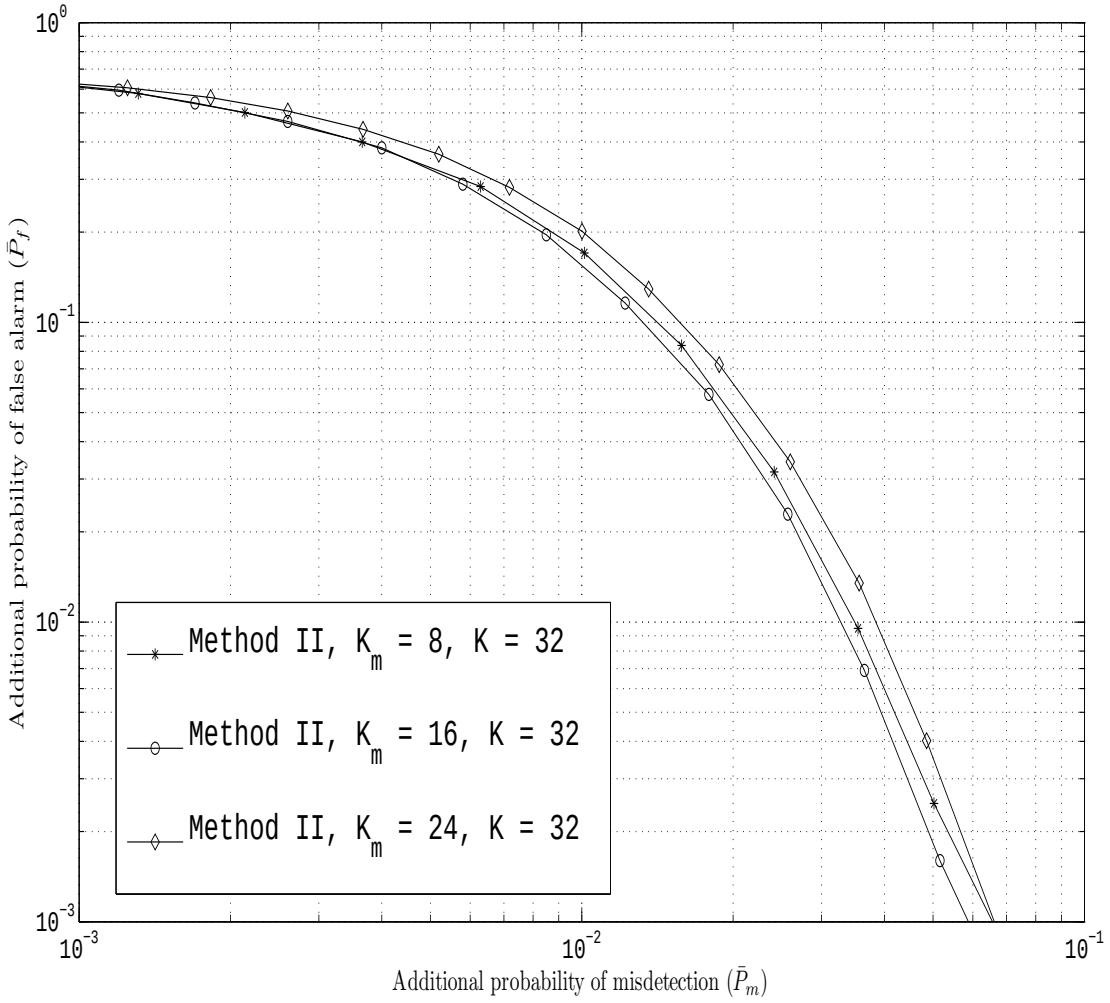

Figure 2.7: Performance of Method II at different values of K_m for $M = 1$, $M_{max} = 2$ and $K = 32$

good channels from the primary user. Therefore, it is not necessarily true that the largest increase or decrease in the adjusted bi-weight estimates is due to change in the state of the primary user, leading to severe performance degradation in case of Method II. However, as seen from Fig. 2.10, at high values of SNR, Method II still outperforms Method I even for high values of M. Both Method I and II would offer a trade-off between the probability of false alarm and probability of misdetection for a system affected by malicious users as long as their percentage is less than 50. However, the trade-off might not be practical for high values of M and low primary user SNR values.

In Fig. 2.11, we consider the performance of malicious user detection techniques using spatial information for the system considered in Fig. 2.4 with $M = 1$ and $M_{max} = 2$. The size of spatial neighborhood considered is $A = 8$. We see that the performances of both Methods I and II improve substantially when spatial outlier factors are taken into consideration. This is due to assignment of lower magnitude outlier factors to non-malicious users with good channels from the primary user which decreases the probability of such users of having a outlier magnitude or penalty factor higher than the malicious users or CR users with low SNR from the primary user. Even though, in this method, the chances of sensors with low primary user SNR getting high outlier or penalty factor are higher, the effect of these sensors will be low on the performance of the cooperative sensing system. The optimal choice of A would depend on the propagation environment of primary user signal.

In Fig. 2.12 and Fig. 2.13, we analyze the performance of Method IIa when $D_\delta = \{1,2,3,4\}$ for the system considered in Fig. 2.4. In Fig. 2.12, we consider 'Always Yes' malicious user and in Fig. 2.13, we consider a smart malicious user that avoids sending false sensing values during the iterations when there is change in the primary user state. Same K_m^δ value is used for each δ and is denoted by K_m in Fig. 2.12 and Fig. 2.13. We see

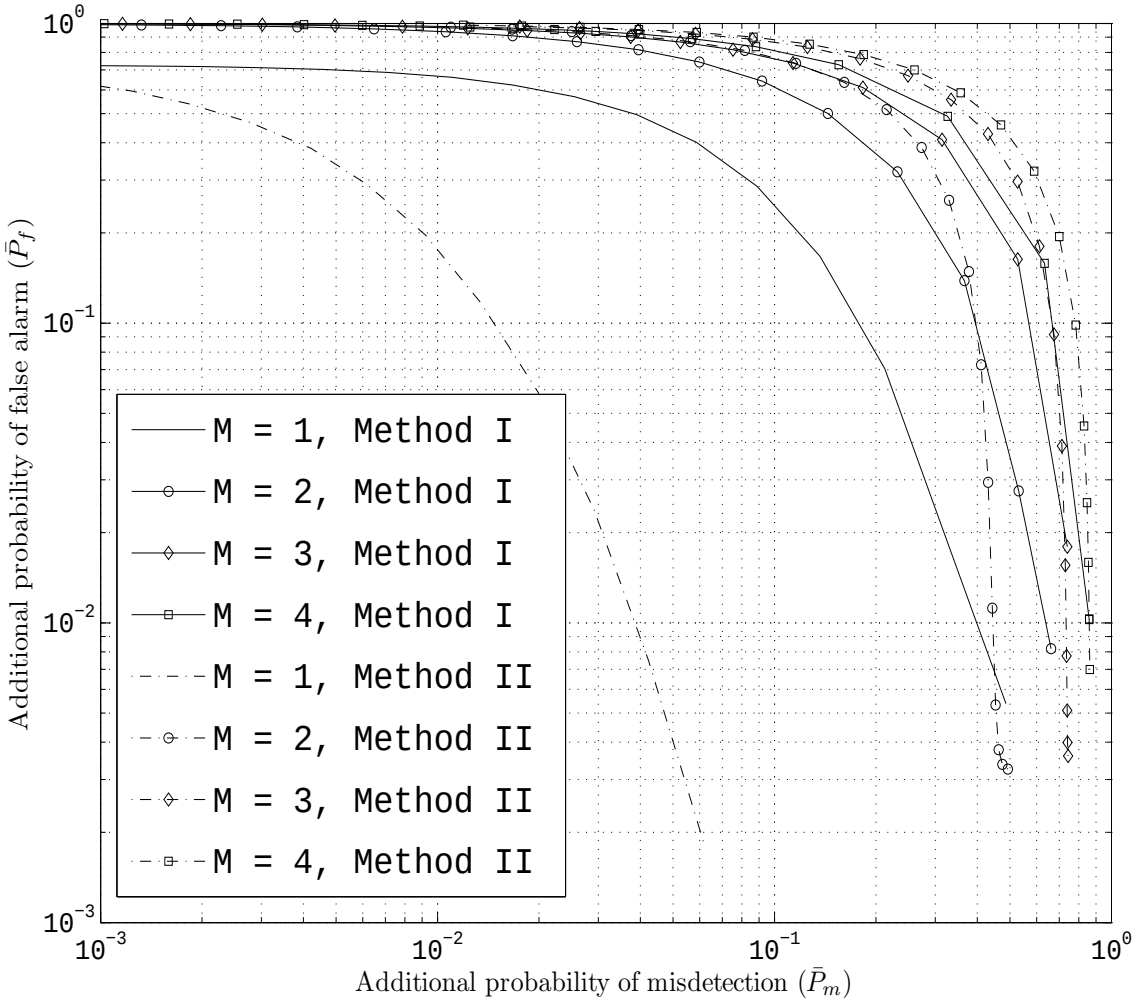

Figure 2.8: Performance of malicious user detection schemes at different values of M for $M_{max} = 20$ with primary user SNR at (100m, 100m) ignoring fading effects = -5dB.

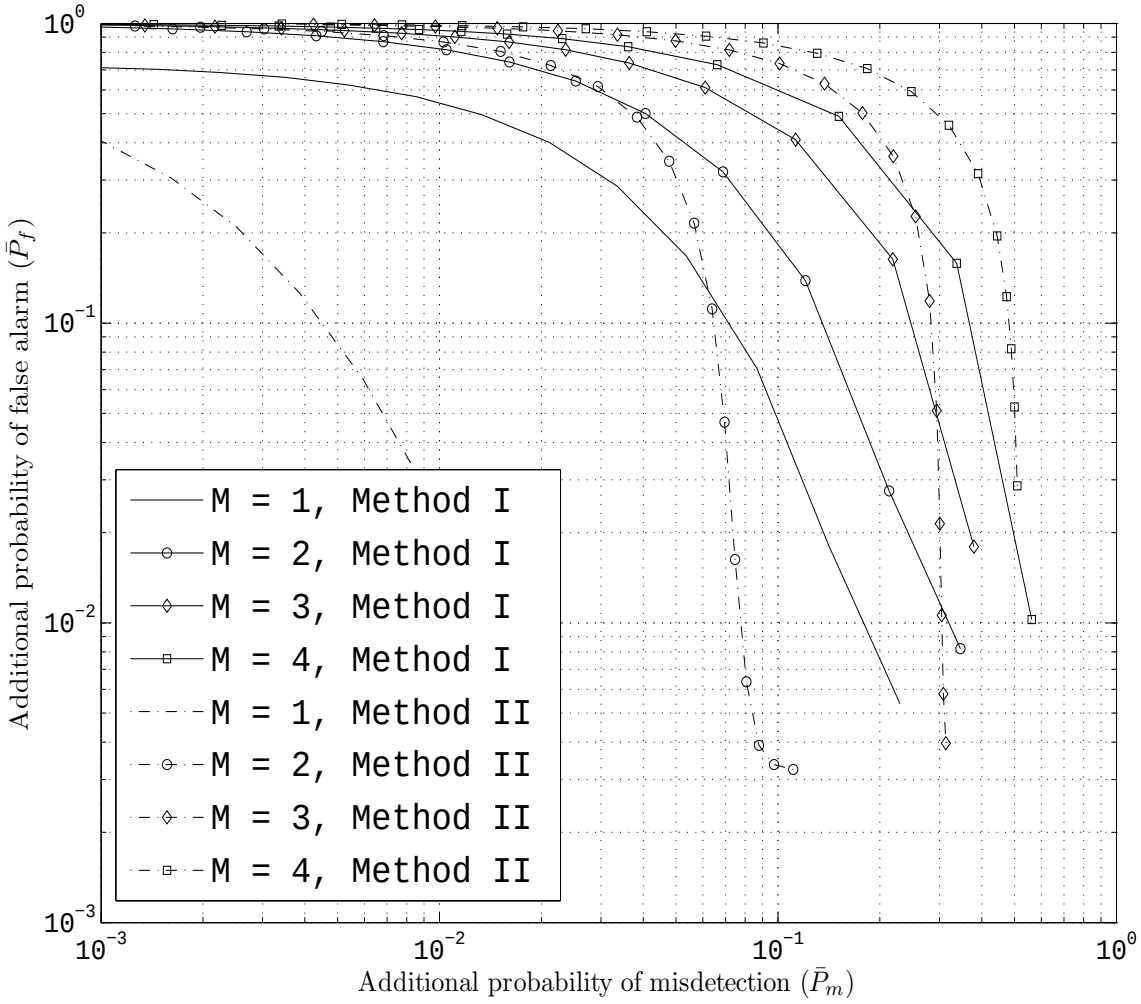

Figure 2.9: Performance of malicious user detection schemes at different values of M for $M_{max} = 20$ with primary user SNR at (100m, 100m) ignoring fading effects = 0dB.

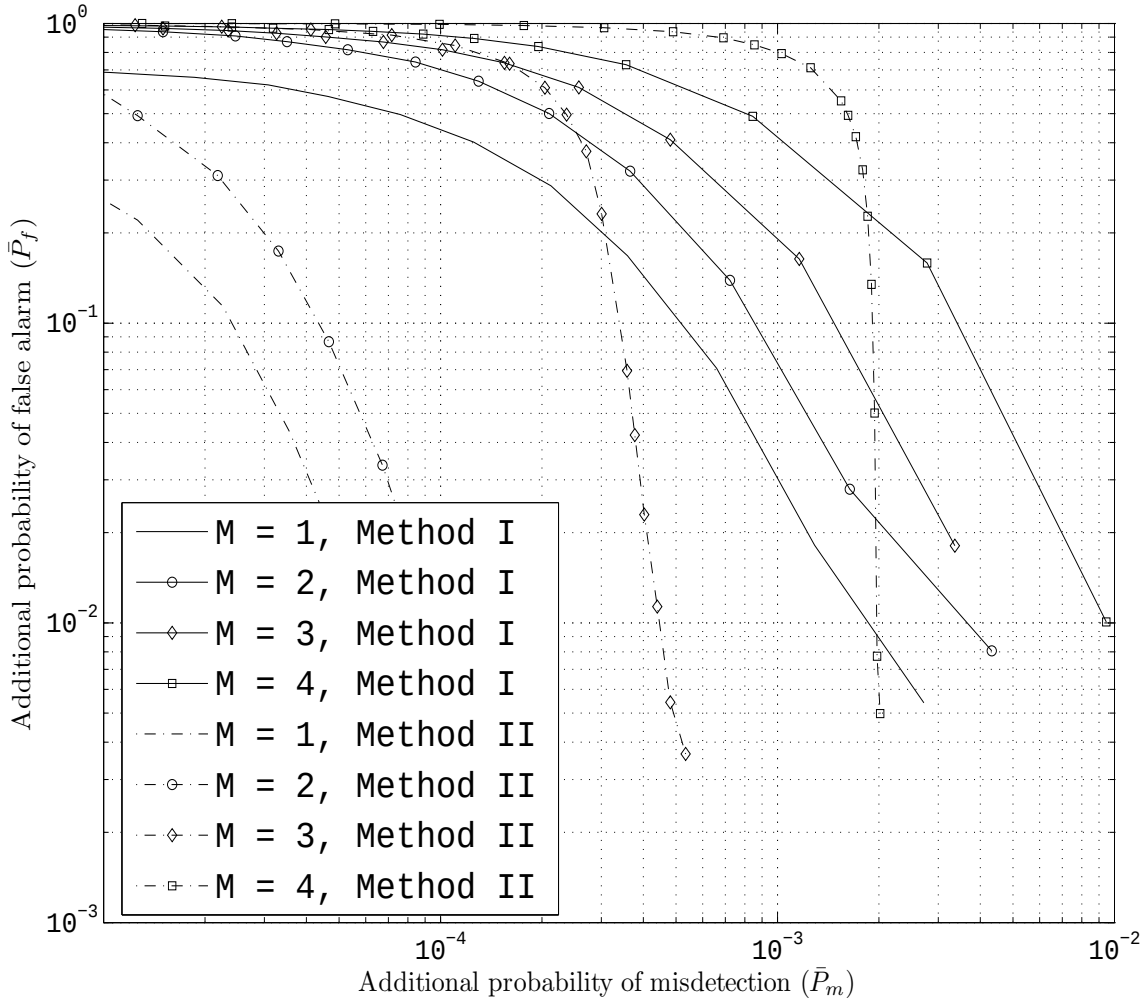

Figure 2.10: Performance of malicious user detection schemes at different values of M for $M_{max} = 20$ with primary user SNR at (100m, 100m) ignoring fading effects = 8dB.

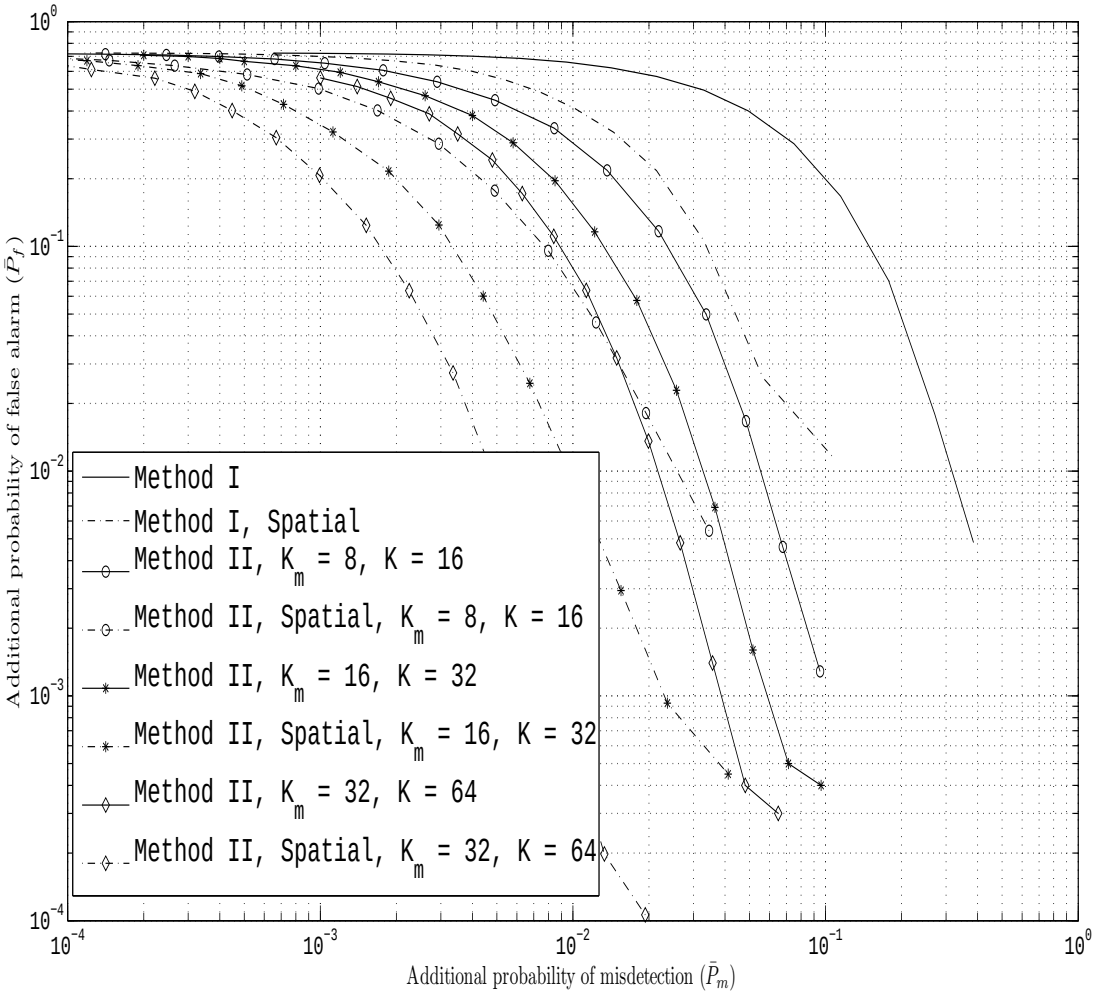

Figure 2.11: Performance of malicious user detection schemes using spatial information of the CR network for $M = 1$ malicious user and $M_{max} = 2$.

that Method IIa performs close to Method II in case of 'Always Yes' malicious user. At the same time, Method IIa significantly outperforms Method II in case of smart malicious user. This is because the smart malicious user escapes getting a penalty during most iterations in case of Method II. However, for $\delta > 1$, it still receives the penalty and thus is identified using Method IIa.

2.8 Conclusions

In this chapter, we studied CR cooperative sensing system based on a parallel fusion sensing architecture in which all sensors send their quantized or un-quantized energy detector outputs to an access point which then applies a data fusion and detection scheme to determine the presence of a primary signal. We investigated schemes to identify malicious CR sensors sending false sensing information to the access point which can lead to severe degradation in performance of the CR sensing system. We explored techniques based on outlier detection to identify such malicious users. Several important constraints imposed by the CR scenario such as small data sample size and limited knowledge of primary signal propagation environment were taken into consideration. We investigated various robust statistics that could be used to assign outlier factors to the CR users during each sensing iteration. Malicious user detection schemes based on these outliers factors were then proposed to identify users sending false sensing information and reduce their impact on the performance of the sensing system. The proposed malicious user detection schemes do not require feedback from the primary user network or knowledge of the additive noise variance and the location of the primary transmitter. We especially focused on identifying the malicious users which decrease the CR throughput by sending false high energy values when the primary user is absent. Assuming partial knowledge of the primary user activity,

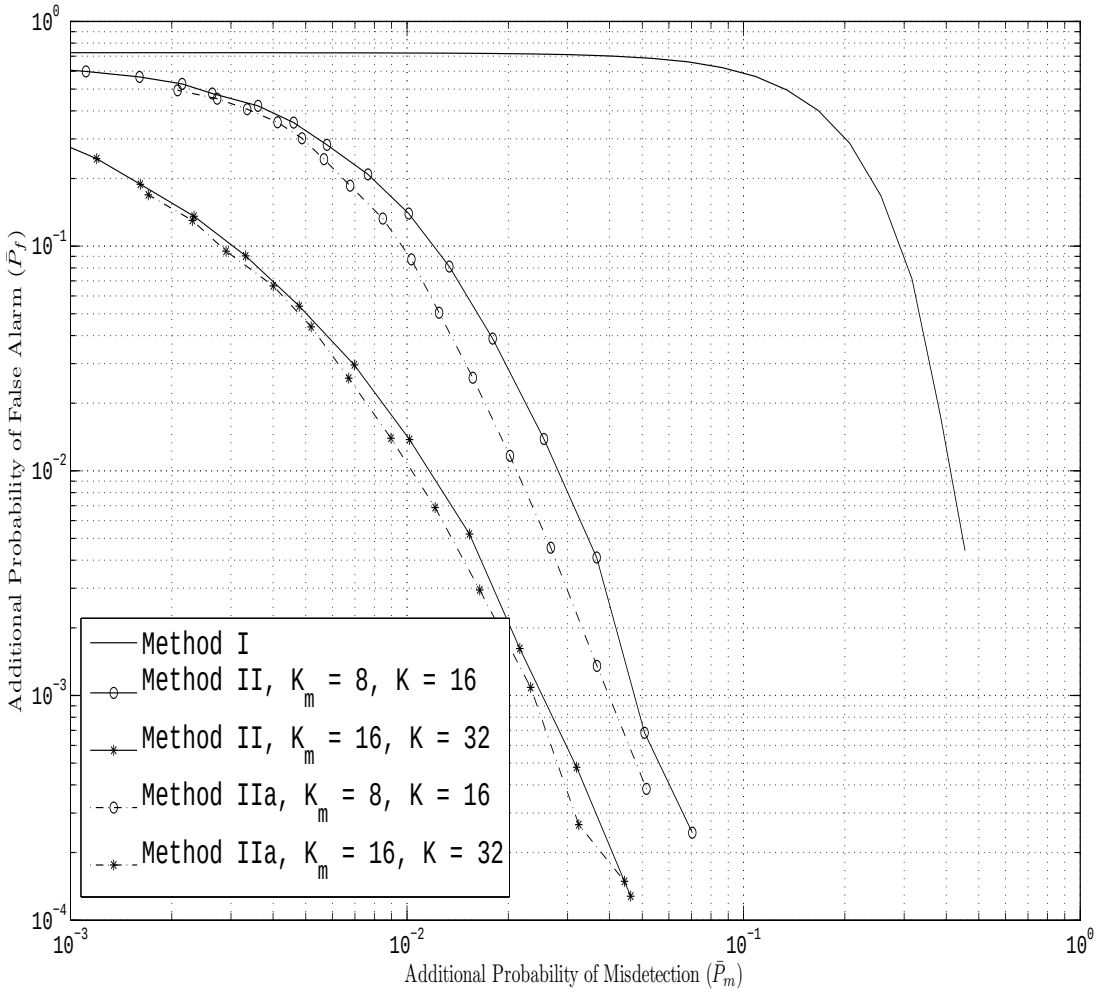

Figure 2.12: Performance of malicious node detection schemes for CR network spread over a large area in the presence of a single 'Always Yes' malicious user

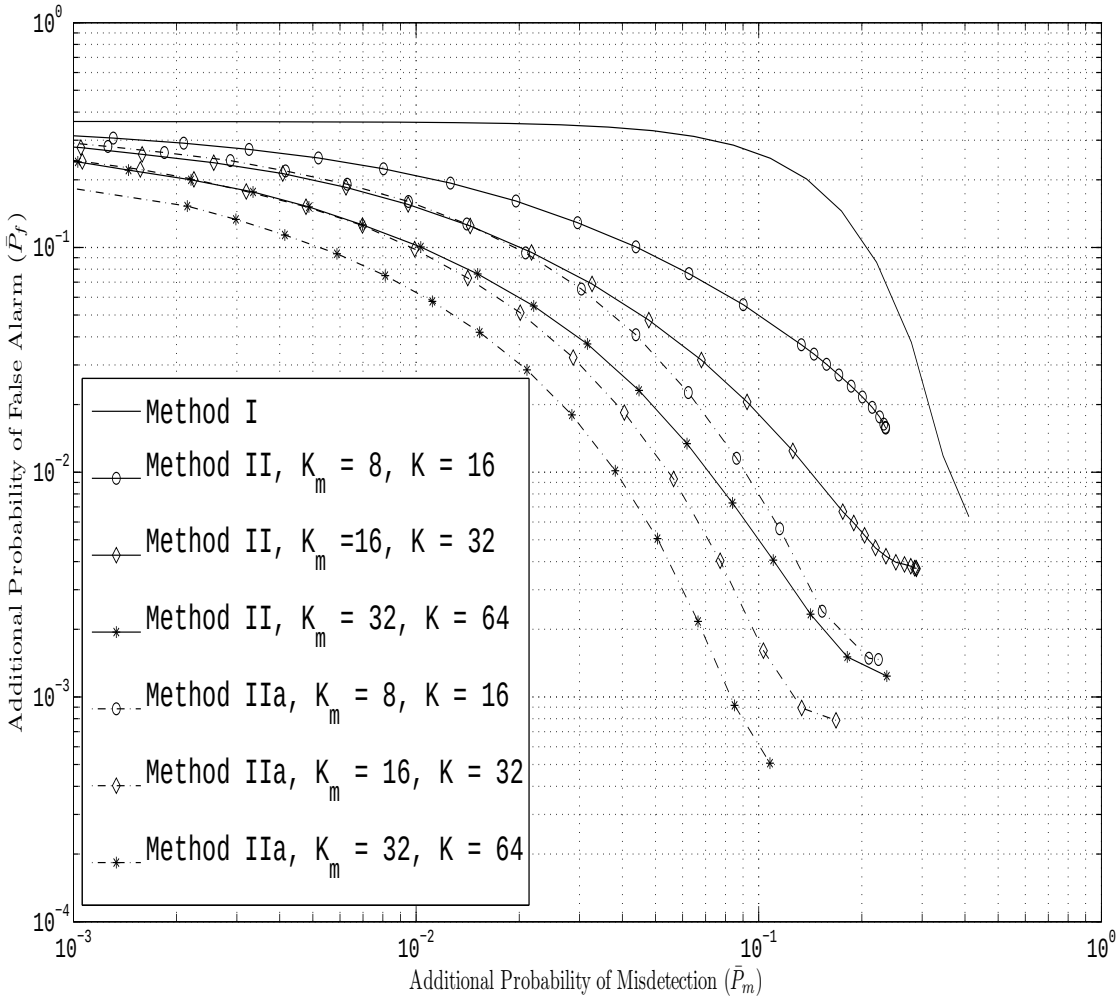

Figure 2.13: Performance of malicious node detection schemes for CR network spread over a large area in the presence of a single smart malicious user

we proposed a novel method to improve the performance of the malicious user detection schemes. For the case of a CR cooperative sensing system spread over a wide area with significant difference in path loss components of the channels between the primary user and various CR sensors, we proposed improved malicious user detection schemes in which spatial location information of the sensors is taken into consideration. We analyzed the performance of the proposed schemes through simulations for a cooperative sensing system using equal gain combining as the data fusion scheme at the access point.

Chapter 3

Sensor Allocation and Quantization Schemes

3.1 Background

In this chapter, we consider a CR system operating in multiple primary bands. We assume that the CR sensors are equipped with narrow-band detectors that can only scan one primary band at a time. For such a system, we present the optimal joint sensor allocation and single-bit quantization problem when 'OR' fusion rule is used in each primary band at the access point. Since the original problem is a highly complex mixed integer optimization problem, we propose to solve it sub-optimally by separating it into two subproblems. We first propose schemes to allocate sensors to various primary bands based on assignment algorithms [46, 49]. We then study optimal single-bit quantization scheme at the sensors assuming equal quantization thresholds at all the sensors assigned to the same primary band. We show that the optimal quantization scheme is, in general, non-convex and propose a suboptimal solution based on convex restriction of the optimal problem. We further

study quantization schemes when a general *k*-out-of-*N* fusion rule is used in each primary band at the access point. In this chapter, we assume that the CR network has information about certain primary transmitter characteristics such as the timing of the primary user pilot signals which it can use to evaluate the channel gains between the primary transmitters and CR sensors.

The rest of this chapter is organized as follows. In Section 3.2, we define the system model and define the optimization problem when the 'OR' fusion rule is implemented at the access point in each primary band. In Section 3.3, we propose schemes to assign sensors to various primary user bands. In Section 3.4, we propose efficient techniques to determine energy detection thresholds at each sensor. In Section 3.5, we extend the results for the case when general *k*-out-of-*N* fusion rule is implemented at the access point. Simulation results are presented in Section 3.6. Conclusions are finally drawn in Section 3.7.

3.2 System Model and Problem Formulation

We consider a group of L CR sensors operating in P primary user bands. Energy detector is implemented at each sensor. The energy detector measures the signal energy level in the assigned primary band and sends bit '1' to the access point via a reporting channel if the energy level is above a certain energy threshold and bit '0' if the energy level is below the energy threshold. We assume that channel coding is used in the reporting channels and the effect of errors due to reporting channels is negligible on the performance of the CR sensing system. In this section, we assume that 'OR' fusion rule is used at the access point in each primary band.

We assume that all primary bands are assigned equal number of sensors. Thus, assuming L is a multiple of P, each primary band is assigned $N = L/P$ sensors. The optimiza-

tion criteria used for assigning sensors and quantization thresholds can vary from system to system. In this chapter, we consider two optimization criteria: 1) Maximize the sum throughput rate of the CR system and 2) Maximize the minimum throughput rate available to the CR system among various primary bands.

The optimal sensor assignment and detection thresholds that maximize the sum throughput rate, for a 'OR' fusion rule, can be obtained by solving following optimization problem

$$\max_{\lambda_{ij},x_{ij}} \sum_{i=1}^{P} r_i(1-P_{f_i}) = \sum_{i=1}^{P} r_i \prod_{j=1}^{PN}(1-P_{f_{ij}}(\lambda_{ij}))^{x_{ij}} \tag{3.1}$$

$$\text{s.t.} \quad \sum_{i=1}^{P} c_i(1-P_{d_i}) = \sum_{i=1}^{P} c_i \prod_{j=1}^{PN}(1-P_{d_{ij}}(\lambda_{ij}))^{x_{ij}} < C \tag{3.2}$$

$$\prod_{j=1}^{PN}(1-P_{d_{ij}}(\lambda_{ij}))^{x_{ij}} < \bar{P}_{m_i} \quad \forall i = 1 \text{ to } P \tag{3.3}$$

$$1-\prod_{j=1}^{PN}(1-P_{f_{ij}}(\lambda_{ij}))^{x_{ij}} < \bar{P}_{f_i} \quad \forall i = 1 \text{ to } P \tag{3.4}$$

$$\sum_{j=1}^{PN} x_{ij} = N \tag{3.5}$$

$$\sum_{i=1}^{P} x_{ij} = 1 \tag{3.6}$$

$$x_{ij} \in \{0,1\} \tag{3.7}$$

where λ_{ij} is energy detection threshold at the sensor j in the primary band i. $x_{ij}=1$ indicates that the sensor j has been assigned to primary band i and $x_{ij}=0$ indicates otherwise. $P_{d_{ij}}$ and $P_{f_{ij}}$ denote probability of detection of the primary signal and probability of false alarm, respectively, for sensor j in primary band i. P_{d_i} and P_{f_i} represent the probability of detection of the primary signal and probability of false alarm, respectively, in primary band i. r_i represents the data throughput rate available to a CR user in band i when the

primary user is absent. c_i represents the cost to be paid to a primary user system if the CR system fails to detect the primary user signal in band i, as a result, causing interference to the primary user. $\bar{P}_{m_i}$ represents the maximum probability of mis-detection that can be tolerated by primary user system in band i. $\bar{P}_{f_i}$ represents the maximum probability of false alarm that can be tolerated in band i, in order to ensure a minimum opportunistic spectral utilization of the band.

As in [52], we assume that each primary band has a strict limit over the amount of interference that it can tolerate which is represented by Eq. (3.3). Even within these interference limits, we assume that each primary system further imposes a cost on the CR system proportional to the interference caused due to misdetection of the primary signal. Parameter C in Eq. (3.2) denotes the maximum total sum cost of misdetection over all the primary bands which the CR system is willing to pay. At the same time, it is also necessary to provide certain quality of service to CR users operating in each primary band. Therefore, constraints are imposed on the probability of false alarm in each primary band as in Eq. (3.4). Eq. (3.5) denotes that N sensors are assigned to each primary band. Eq. (3.6) specifies that a sensor can be assigned to only one primary band.

Alternatively, it might be of interest in certain systems to guarantee a max-min fairness to the CR users. In this case, the aim of the sensor system is to maximize the minimum throughput rate available to the CR system among various bands. The max-min optimization problem is given by

$$\max_{\lambda_{ij},x_{ij}} \min_{i} \prod_{j=1}^{PN} (1 - P_{f_{ij}}(\lambda_{ij}))^{x_{ij}} \tag{3.8}$$

given the constraints (3.2)-(3.7).

Let v denote the number of signal samples taken by the energy detector at each sensor in each band. Let $|h_{ij}|$ represent the effective channel gain between the primary transmitter in

band i to the sensor j assuming that the transmitter transmits signal at unit power. The CR sensors can estimate $|h_{ij}|$ by taking energy samples during the periods when the primary transmitters are known to be transmitting (for example when they are transmitting pilot signals) [52]. We assume additive white Gaussian noise (AWGN) with variance σ^2 in each channel. For such a system, the probability of detection and false alarm at each sensor are given by [43]

$$P_{d_{ij}}(\lambda_{ij}) = Pr\left(\chi_v^2\left(v\frac{|h_{ij}|^2}{\sigma^2}\right) > \lambda_{ij}\right) \tag{3.9}$$

$$P_{f_{ij}}(\lambda_{ij}) = Pr(\chi_v^2 > \lambda_{ij}) \tag{3.10}$$

where $\chi_v^2\left(v\frac{|h_{ij}|^2}{\sigma^2}\right)$ represents non-central chi-square distribution with v degrees of freedom and non-centrality parameter $v\frac{|h_{ij}|^2}{\sigma^2}$ and χ_v^2 represents central chi-square distribution with v degrees of freedom.

Using the central limit theorem for large v, both central and non-central chi-square distribution can be approximated with Gaussian distributions. This yields following approximations for probability of detection and false alarm at the sensors [52]

$$P_{d_{ij}}(\lambda_{ij}) \approx Q\left(\frac{\lambda_{ij} - 2v(\sigma^2 + |h_{ij}|^2)}{\sqrt{4v(\sigma^2 + 2|h_{ij}|^2)\sigma^2}}\right) \tag{3.11}$$

$$P_{f_{ij}}(\lambda_{ij}) \approx Q\left(\frac{\lambda_{ij} - 2v\sigma^2}{\sqrt{4v\sigma^4}}\right) \tag{3.12}$$

where $Q(\cdot)$ represents the Gaussian Q-function.

For the probability of detection $P_{d_{ij}}(\lambda_{ij})$ and false alarm $P_{f_{ij}}(\lambda_{ij})$ given in (3.11) and (3.12), respectively, (3.1) and (3.8) are mixed integer optimization problems and are highly complex to solve. In order to reduce the complexity, we separate the problem into two

subproblems. We first propose schemes to assign the sensors to different primary user bands. Once the sensors are assigned to various primary bands, we investigate efficient quantization schemes.

3.3 Sensor Assignment

In this section, we study two possible techniques that could be used to assign the sensors based on the channel gains between various primary transmitters and the CR sensors, the costs c_i of causing interference to the primary users and throughput rates r_i available in the primary bands.

3.3.1 Maximum Weighted Sum Channel Gain Assignment

One method to assign sensors is to maximize the cost weighted sum of channel gains between each primary user and sensors assigned to the primary user. The sensor allocation problem in this case is as follows

$$\max_{x_{ij}} \sum_{i=1}^{P} \sum_{j=1}^{PN} \frac{r_i}{c_i} |h_{ij}|^2 x_{ij} \tag{3.13}$$

$$\sum_{i=1}^{P} x_{ij} = 1 \tag{3.14}$$

$$\sum_{j=1}^{PN} x_{ij} = N \tag{3.15}$$

$$x_{ij} \in \{0,1\} \tag{3.16}$$

The sensor allocation problem in (3.13)-(3.16) is well studied in the literature and can be optimally solved using Munkres algorithm [46], which has a complexity of $O((PN)^3)$.

3.3.2 Max-Min Channel Gain Assignment

The maximum weighted sum channel gain assignment scheme can however lead to assignment of all good sensors to one user and assignment of sensors with weak channels to another. Thus, it might not offer a good trade-off between the probability of detection and probability of false alarm in some of the primary bands. Especially, in case of max-min optimization criterion as in (3.8), assigning sensors such that the minimum weighted sum of the channel gains assigned to various primary users is maximized could offer better performance. Such a max-min assignment problem can be formulated as follows

$$\max_{x_{ij}} \min_{i} \sum_{j=1}^{PN} \frac{r_i}{c_i} |h_{ij}|^2 x_{ij} \tag{3.17}$$

given the constraints (3.14)-(3.16). The optimization problem in (3.17) is max-min variant of the bottleneck assignment problem under categorization (which is a min-max assignment problem) and is strictly NP-hard [51]. Therefore, we propose a suboptimal greedy algorithm to solve (3.17). The proposed algorithm is a modification of the greedy algorithm discussed in [51], in which the min-max version of the problem in (3.17) was studied. The greedy algorithm is described in Table 3.1. As seen from Table 3.1, the greedy algorithm assigns the sensors in serial order. During each iteration, the band with lowest cost weighted sum of channel gains is selected and assigned the best sensor available to it. In case of a tie (i.e. if two or more primary bands have the same minimum weighted sum of channel gains at a particular iteration), the primary band with maximum available sensor channel gain among rest of the unallocated sensors is chosen and corresponding sensor is assigned to it. The greedy algorithm is suboptimal but has a much lower complexity of $O(P^2 N \log(PN))$ [51], compared to the optimal max-min assignment algorithm based on

exhaustive search. During each iteration, the greedy algorithm attempts to maximize the minimum weighted sum channel gain values assigned to each primary band. This should intuitively lead to a solution close to the optimal solution.

Table 3.1: Greedy algorithm

Step 0 (Initialization):		
l	=	0
$\hat{x}_{ij}$	=	0 $\quad \forall i = 1$ to P and $j = 1$ to N
Step 1 (Assignment):		
l	=	$l + 1$
$\hat{i}$	=	$\arg\min_{i \in R_l^p} \sum_j \frac{r_i}{c_i} \lvert h_{ij} \rvert^2 \hat{x}_{ij}$ where $R_l^p = \{i : \sum_j \hat{x}_{ij} < N\}$
$\hat{j}$	=	$\arg\max_{j \in R_l^n} \lvert h_{\hat{i}j} \rvert^2$ where $R_l^n = \{j : \sum_i \hat{x}_{ij} = 0\}$
$\hat{x}_{\hat{i}\hat{j}}$	=	1 ($\hat{x}_{ij} = 1$ implies that the sensor j has been assigned to primary band i)
Step 2 (Finish): Stop if l	=	PN else go to Step 1

3.4 Quantization Thresholds

Once the sensors are assigned to each primary band, we optimize the quantization thresholds at each sensor. In general, the optimal thresholds are not equal even in case of a single primary user with equal channel gains $|h_{ij}|$ at all sensors [65]. However, it has been shown in the literature that equal thresholds are asymptotically optimal by Neyman-Pearson or Bayesian criteria [47, 65, 69] as the number of sensors goes to infinity.

Therefore, in order to reduce the complexity of the algorithm, we assume that all the sensors assigned to a single primary band use equal energy detection thresholds (i.e., $\lambda_{ij} = \lambda_i, \forall j$). Let S^i represent the set of sensors assigned to primary band i. Assuming 'OR'

fusion rule, the optimal thresholds can be determined by solving the following problem

$$\max_{\lambda_i} \sum_{i=1}^{P} r_i \left(1 - Q\left(\frac{\lambda_i - 2\nu\sigma^2}{\sqrt{4\nu\sigma^4}}\right)\right)^N \tag{3.18}$$

$$s.t. \sum_{i=1}^{P} c_i \prod_{j \in S^i} \left(1 - Q\left(\frac{\lambda_i - 2\nu(\sigma^2 + |h_{ij}|^2)}{\sqrt{4\nu(\sigma^2 + 2|h_{ij}|^2)\sigma^2}}\right)\right) < C \tag{3.19}$$

$$\prod_{j \in S^i} \left(1 - Q\left(\frac{\lambda_i - 2\nu(\sigma^2 + |h_{ij}|^2)}{\sqrt{4\nu(\sigma^2 + 2|h_{ij}|^2)\sigma^2}}\right)\right) < \bar{P}_{m_i} \quad \forall i \tag{3.20}$$

$$1 - \left(1 - Q\left(\frac{\lambda_i - 2\nu\sigma^2}{\sqrt{4\nu\sigma^4}}\right)\right)^N < \bar{P}_{f_i} \quad \forall i \tag{3.21}$$

In rest of this chapter, we use following notation for convenience

$$\alpha_i = \frac{\lambda_i - 2\nu\sigma^2}{\sqrt{4\nu\sigma^4}} \tag{3.22}$$

$$\beta_{ij} = \frac{\lambda_i - 2\nu(\sigma^2 + |h_{ij}|^2)}{\sqrt{4\nu(\sigma^2 + 2|h_{ij}|^2)\sigma^2}} \tag{3.23}$$

(3.21) is a linear constraint. We show in Appendix A that the objective function in (3.18) is concave for values of α_i satisfying (from Eq. (A.6))

$$\frac{\sum_{j \in S^i} \alpha_i}{N} \geq \bar{x}^{(1,N)} \tag{3.24}$$

where $\bar{x}^{(1,N)}$ values are shown in Table 3.2. We also show in Appendix A that condition (3.24) holds for all values of α_i for which the probability of false alarm in the primary band i, P_{f_i}, is less than or equal to $P_{f_{max}}^{(1,N)}$ (from Eq. (A.8)). Therefore, for $\bar{P}_{f_i} \leq P_{f_{max}}^{(1,N)}$, the objective function in (3.18) is concave over the set of λ_i values satisfying the constraint (3.21). The values of $P_{f_{max}}^{(1,N)}$ are shown in Table 3.3. As seen from Table 3.3, the values of $P_{f_{max}}^{(1,N)}$ lie above 0.5 for all values of N and thus, the constraint in (3.24) is very reasonable

for practical CR systems.

Table 3.2: Values of $\vec{x}^{(k,N)}$ at different values of k and N

N	k									
	1 'OR' rule	2	3	4	5	6	7	8	9	10
1	0									
2	0.51	-0.51								
3	0.77	0	-0.77							
4	0.94	0.28	-0.28	-0.94						
5	1.06	0.47	0	-0.47	-1.06					
6	1.16	0.61	0.19	-0.19	-0.61	-1.16				
7	1.24	0.72	0.34	0	-0.34	-0.72	-1.24			
8	1.31	0.81	0.45	0.15	-0.15	-0.45	-0.81	-1.31		
9	1.37	0.89	0.55	0.26	0	-0.26	-0.55	-0.89	-1.37	
10	1.42	0.95	0.63	0.36	0.12	-0.12	-0.36	-0.63	-0.95	-1.42

However, constraint (3.19) is not guaranteed to be convex in general. The necessary conditions to guarantee convexity are very complex to derive and need not necessarily hold true for all values of λ_i satisfying (3.19) and (3.20). Thus, this problem in general is non-convex and cannot be solved to obtain unique optimal solution [7].

In this chapter, we propose a suboptimal solution to the optimization problem in (3.18)-(3.21) by solving a convex restriction to the original optimization problem. We show in Appendix B that $Q(x)$ is a log-concave function. Therefore, $1-Q(x) = Q(-x)$ is also

Table 3.3: Values of $P_{f_{max}}^{(k,N)}$ at different values of k and N

N	k									
	1 'OR' rule	2	3	4	5	6	7	8	9	10
1	0.5									
2	0.5189	0.4811								
3	0.5292	0.5	0.4708							
4	0.5360	0.5087	0.4913	0.4640						
5	0.5410	0.5142	0.5	0.4858	0.4590					
6	0.5449	0.5181	0.5052	0.4948	0.4819	0.4551				
7	0.5481	0.5212	0.5088	0.5	0.4912	0.4788	0.4519			
8	0.5508	0.5238	0.5116	0.5036	0.4964	0.4884	0.4762	0.4492		
9	0.5530	0.5259	0.5139	0.5062	0.5	0.4938	0.4861	0.4741	0.4470	
10	0.5550	0.5277	0.5158	0.5083	0.5026	0.4974	0.4917	0.4842	0.4723	0.4450

log-concave. Thus, we have

$$\begin{aligned} \frac{1}{N}\sum_{j\in S^i}\log\left(1-Q(\beta_{ij})\right) &\leq \log\left(1-Q\left(\frac{\sum_{j\in S^i}\beta_{ij}}{N}\right)\right) \\ \Longrightarrow \prod_{j\in S^i}\left(1-Q\left(\beta_{ij}\right)\right) &\leq \left(1-Q\left(\frac{\sum_{j\in S^i}\beta_{ij}}{N}\right)\right)^N \end{aligned} \tag{3.25}$$

with equality holding when the channel gains of the sensors assigned to primary band i are all equal. We show in Appendix A (see Eq. (A.7)) that $1-\left(1-Q\left(\frac{\sum_{j\in S^i}\beta_{ij}}{N}\right)\right)^N$ is concave and thus, $\left(1-Q\left(\frac{\sum_{j\in S^i}\beta_{ij}}{N}\right)\right)^N$ is convex for

$$\frac{\sum_{j\in S^i}\beta_{ij}}{N} < \bar{x}^{(1,N)} \tag{3.26}$$

For β_{ij} satisfying (3.26), $1-\left(1-Q\left(\frac{\Sigma_{j\in S^i}\beta_{ij}}{N}\right)\right)^N$ is greater than $P_{f_{max}}^{(1,N)}$ (from (A.9)) and hence, $\left(1-Q\left(\frac{\Sigma_{j\in S^i}\beta_{ij}}{N}\right)\right)^N$ is less than $1-P_{f_{max}}^{(1,N)}$.

As seen from Table 3.3, the values of $1-P_{f_{max}}^{(1,N)}$ are above 0.44 for values of $N \leq 10$ (In [43], it was shown that most of the gain through cooperation is achieved by using $\sim 10-20$ sensors). Thus, for practical CR systems, it would be reasonable to assume that $\bar{P}_{m_i}$ is less than $1-P_{f_{max}}^{(1,N)}$. Therefore, all the values of β_{ij}, for which $\left(1-Q\left(\frac{\Sigma_{j\in S^i}\beta_{ij}}{N}\right)\right)^N < \bar{P}_{m_i}$, satisfy the constraint (3.26) and hence, $\left(1-Q\left(\frac{\Sigma_{j\in S^i}\beta_{ij}}{N}\right)\right)^N$ would be convex at those values of β_{ij}.

Since α_i and β_{ij} are linear functions of λ_i, constraints (3.24) and (3.26) are satisfied for following linear constraint on λ_i

$$\sqrt{4\nu\sigma^4}\bar{x}^{(1,N)} + 2\nu\sigma^2 < \lambda_i < \frac{\bar{x}^{(1,N)} + \sum_{j\in S^i}\frac{2\nu(\sigma^2+|h_{ij}|^2)}{\sqrt{4\nu(\sigma^2+2|h_{ij}|^2)\sigma^2}}}{\sum_{j\in S^i}\frac{1}{\sqrt{4\nu(\sigma^2+2|h_{ij}|^2)\sigma^2}}} \tag{3.27}$$

Thus, we obtain the following restricted convex optimization problem

$$\max_{\lambda_i}\sum_{i=1}^{P} r_i\left(1-Q(\alpha_i)\right)^N \tag{3.28}$$

$$s.t.\sum_{i=1}^{P} c_i\left(1-Q\left(\frac{\Sigma_{j\in S^i}\beta_{ij}}{N}\right)\right)^N < C \tag{3.29}$$

$$\left(1-Q\left(\frac{\Sigma_{j\in S^i}\beta_{ij}}{N}\right)\right)^N < \bar{P}_{m_i} \quad \forall i = 1 \text{ to } P \tag{3.30}$$

$$1-\left(1-Q(\alpha_i)\right)^N < \bar{P}_{f_i} \quad \forall i = 1 \text{ to } P \tag{3.31}$$

(3.28) is a convex restriction of the problem (3.18) since the constraints (3.29) and (3.30)

are more restrictive on the values λ_i compared to (3.19) and (3.20), respectively. Nevertheless, (3.28)-(3.31) is a convex optimization problem as long as $\bar{P}_{f_i} \leq P_{f_{max}}^{(1,N)}$ and $\bar{P}_{m_i} \leq 1 - P_{f_{max}}^{(1,N)}$, since the corresponding solution set would always satisfy the linear constraint (3.27), for which the objective function in (3.28) is concave, constraint (3.29) is convex and, constraints (3.30) and (3.31) are linear. As discussed earlier, these restrictions on $\bar{P}_{f_i}$ and $\bar{P}_{m_i}$ are very reasonable in practical systems. The solution of the suboptimal problem (3.28)-(3.31) forms a lower bound on the solution of the original optimization problem in (3.18)-(3.21) [7]. The suboptimal solution is equal to the optimal solution if in each primary band, all the sensors have equal channel gains from the primary transmitter. The complexity of the suboptimal solution will, in general, be lower than the optimum solution.

The suboptimal solution can be further simplified by solving (3.28)-(3.31) assuming that all the sensors assigned to various primary bands are allocated equal thresholds (i.e. $\lambda_1 = \lambda_2 = ... = \lambda_P = \lambda$). This would reduce the complexity further since the number of optimization variables is reduced from P to 1.

3.4.1 Max-Min Optimization

If the aim of the threshold allocation algorithm is to maximize the minimum throughput rate available among various primary bands, the optimization problem after sensor assignment is as follows

$$\max_{\lambda_i} \min_{i} r_i (1 - Q(\alpha_i))^N \tag{3.32}$$

given constraints (3.19), (3.20) and (3.21).

The max-min optimization in (3.32) can be reformulated by introducing a new variable

γ as follows [50]

$$\min_{\gamma>0,\ \lambda_i} \quad -\gamma \tag{3.33}$$

$$s.t.\ \gamma - r_i(1-Q(\alpha_i))^N \ < \ 0 \quad \forall i = 1 \text{ to } P \tag{3.34}$$

given the constraints (3.19), (3.20) and (3.21). Using the convex restriction techniques proposed earlier in this section, a suboptimal solution can be obtained by solving a convex restriction of the original problem in (3.32), as long as the constraint (3.27) is valid.

3.5 General k-out-of-N Fusion Rule

In this section, we extend the results obtained in the previous section to the case when a general k-out-of-N fusion rule is used by the access point in each primary band. The threshold optimization problem after sensor assignment for k-out-of-N fusion rule is given by

$$\max_{\lambda_i} \sum_{i=1}^{P} r_i \left(1 - \sum_{r=k}^{N} \binom{N}{r} Q(\alpha_i)^r (1-Q(\alpha_i))^{N-r}\right) \tag{3.35}$$

$$s.t. \sum_{i=1}^{P} c_i \left(1 - \sum_{r=k}^{N} \sum_{s\in S_r^i} \prod_{\substack{j\in s \\ j'\in S^i - s}} Q\left(\beta_{ij}\right)\left(1-Q\left(\beta_{ij'}\right)\right)\right) \ < \ C \tag{3.36}$$

$$1 - \sum_{r=k}^{N} \sum_{s\in S_r^i} \prod_{\substack{j\in s \\ j'\in S^i - s}} Q\left(\beta_{ij}\right)\left(1-Q\left(\beta_{ij'}\right)\right) \ < \ \bar{P}_{m_i} \ \forall i \tag{3.37}$$

$$\sum_{r=k}^{N} \binom{N}{r} Q(\alpha_i)^r (1-Q(\alpha_i))^{N-r} \ < \ \bar{P}_{f_i} \ \forall i \tag{3.38}$$

where S_r^i represents the set of all combinations of size r among the users assigned to primary band i. $S^i - s$ represents the set of users in S^i but not in s.

In Appendix A, we show that the objective function in (3.35) is concave and (3.38) is a convex constraint as long as

$$\frac{\sum_{j\in S^i}\alpha_i}{N} \geq \bar{x}^{(k,N)} \tag{3.39}$$

Values of $\bar{x}^{(k,N)}$ are given in Table 3.2. In Appendix A, we show that for the values of α_i satisfying (3.39), the probability of false alarm P_{f_i} in each band is less than $P_{f_{max}}^{(k,N)}$ whose values are given in Table 3.3. As seen from Table 3.3, the values of $P_{f_{max}}^{(k,N)}$ are greater than 0.44 for values of N less than or equal to 10. Therefore, the constraint in (3.39) must be reasonable for most of the CR systems.

The log-concavity of the Q-function used in case of 'OR' fusion rule to obtain a convex restricted problem cannot be used for $k > 1$. We instead take the performance of the system when all sensors assigned to a primary band have a channel gain equal to worst among them. Thus, the suboptimal solution is obtained by solving following problem

$$\max_{\lambda_i} \sum_{i=1}^{P} r_i \left(1 - \sum_{r=1}^{k} \binom{N}{r} Q(\alpha_i)^r (1-Q(\alpha_i))^{N-r}\right) \tag{3.40}$$

$$s.t. \sum_{i=1}^{P} c_i \left(1 - \sum_{r=k}^{N} \binom{N}{r} Q(\beta_i^w)^r (1-Q(\beta_i^w))^{N-r}\right) < C \tag{3.41}$$

$$1 - \sum_{r=k}^{N} \binom{N}{r} Q(\beta_i^w)^r (1-Q(\beta_i^w))^{N-r} < \bar{P}_{m_i} \quad \forall i \tag{3.42}$$

$$\sum_{r=k}^{N} \binom{N}{r} Q(\alpha_i)^r (1-Q(\alpha_i))^{N-r} < \bar{P}_{f_i} \quad \forall i \tag{3.43}$$

where

$$\beta_i^w = \frac{\lambda_i - 2\nu(\sigma^2 + \min_{j\in S^i}|h_{ij}|^2)}{\sqrt{4\nu(\sigma^2 + 2\min_{j\in S^i}|h_{ij}|^2)\sigma^2}} \tag{3.44}$$

(3.40)-(3.43) is a convex optimization problem as long as β_i^w satisfies the following constraint

$$\beta_i^w < \bar{x}^{(k,N)} \tag{3.45}$$

We show in Appendix A that constraint (3.45) is satisfied as long as the system in which the channel gains of the all the sensors allocated to a primary user band i are equal to the worst among them, has a probability of misdetection less than $1 - P_{f_{max}}^{(k,N)}$. As can be seen from Table 3.3, the values of $1 - P_{f_{max}}^{(k,N)}$ lie between 0.44 and 0.56 for values of N less than or equal to 10.

3.6 Simulation Results

In Fig. 3.1, we consider a system with L = 20 CR sensors operating in P = 4 primary bands. Each primary band is assigned N = 5 CR sensors to detect the presence of a primary user in that band. We assume that the channels from the primary transmitters to the sensors undergo independent and identical log-normal shadowing and small scale Rayleigh fading. The mean signal to noise ratio (SNR) due to path loss at the sensors is assumed to be -3dB in each primary band. The variance of log-normal shadowing between each primary user and sensor is 4dB. The throughput rates r_i available in the primary bands are randomly distributed between 1 Mbps and 2 Mbps. $\mathbf{c} = [c_1, c_2, c_3, c_4] = [0.1, 0.2, 0.3, 0.4]$ is used as the cost vector. The maximum allowed probability of miss detection $\bar{P}_{m_i}$ and false alarm $\bar{P}_{f_i}$ are chosen as 0.1 and 0.4, respectively, in all primary bands. The access point uses 'OR' (1-out-of-5) fusion rule in each primary band. We study the performance of various sensor allocation and quantization schemes to solve the sum throughput rate optimization problem in (3.1). Sensors are assigned using the algorithm described in Section 3.3. A close to optimal solution to the original non-convex optimization problem in (3.18)-(3.21)

is obtained by using convex optimization algorithms starting from different initial points. In the figure, we refer to this solution as optimal eventhough its not possible to determine the optimal point since the problem is non-convex. We also present the suboptimal solutions obtained by solving convex restriction problem in (3.28)-(3.31). In the figure, we refer to it as the suboptimal solution. We further present the performance of the suboptimal solution, obtained by solving convex restricted optimization problem (3.28)-(3.31), assuming equal thresholds at all the sensors operating in all primary bands.

From Fig 3.1., we see that the performance of the max-min sensor assignment scheme is, in general, better than the maximum weighted sum channel gain assignment scheme. This is because the maximum weighted sum channel gain scheme might lead to assignment of sensors with low channel gains to certain primary bands thus reducing the tradeoff available between probability of detection and probability of false alarm in those primary bands. We also notice that the suboptimal solution obtained by solving the restricted convex problem is close to the optimal solution, especially, at higher cost threshold C. We observe that using different thresholds for each band leads to much better performance compared to using equal thresholds in all the primary bands. We also compare the performance in the case when no quantization is used.

In Fig. 3.2, we consider the same system as considered in Fig 3.1. However, the optimization criterion is to maximize the minimum throughput rate available among various primary bands as described in (3.8). We see from Fig. 3.2 that max-min sensor assignment scheme significantly outperforms the maximum weighted sum channel gain assignment. We notice that the restricted convex optimization problem performs close to the original optimization problem at higher values of threshold C. We further observe that using different thresholds for different primary bands leads to better performance.

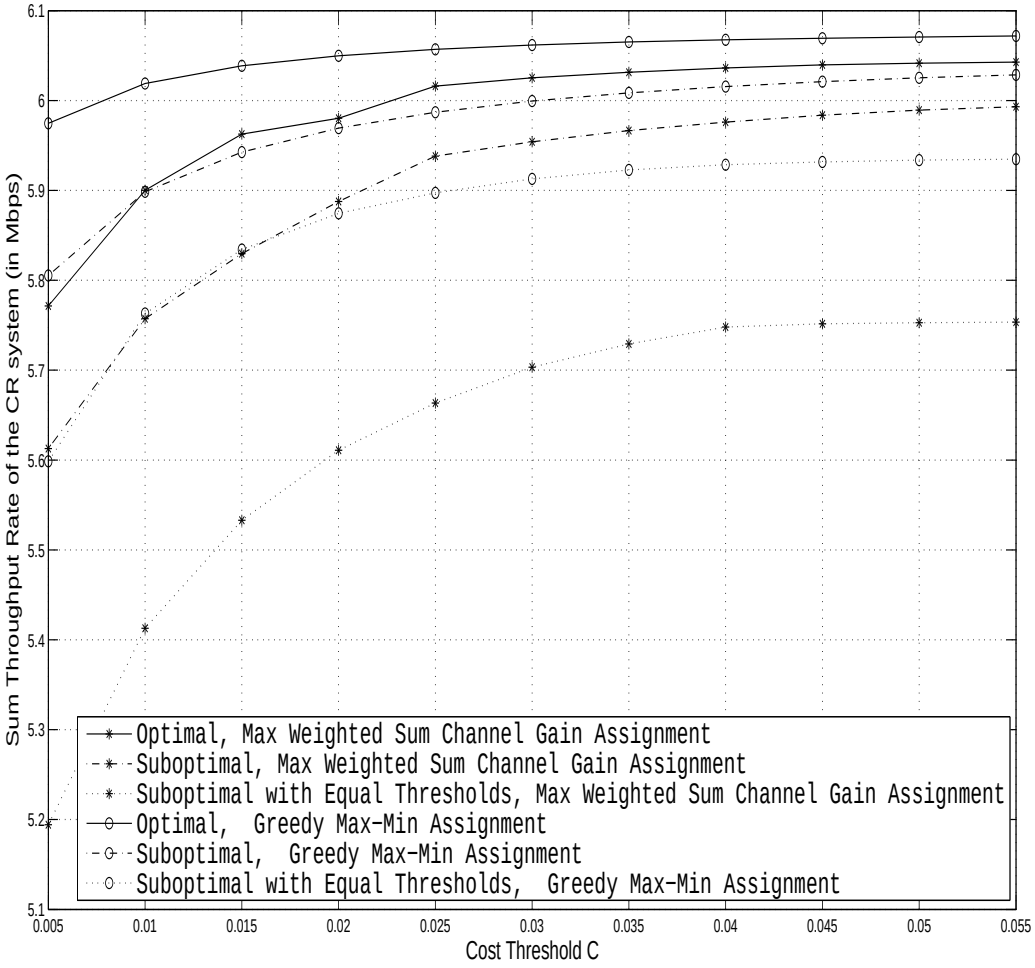

Figure 3.1: Sum throughput rate of the CR system using 'OR' fusion rule for different sensor allocation and quantization schemes

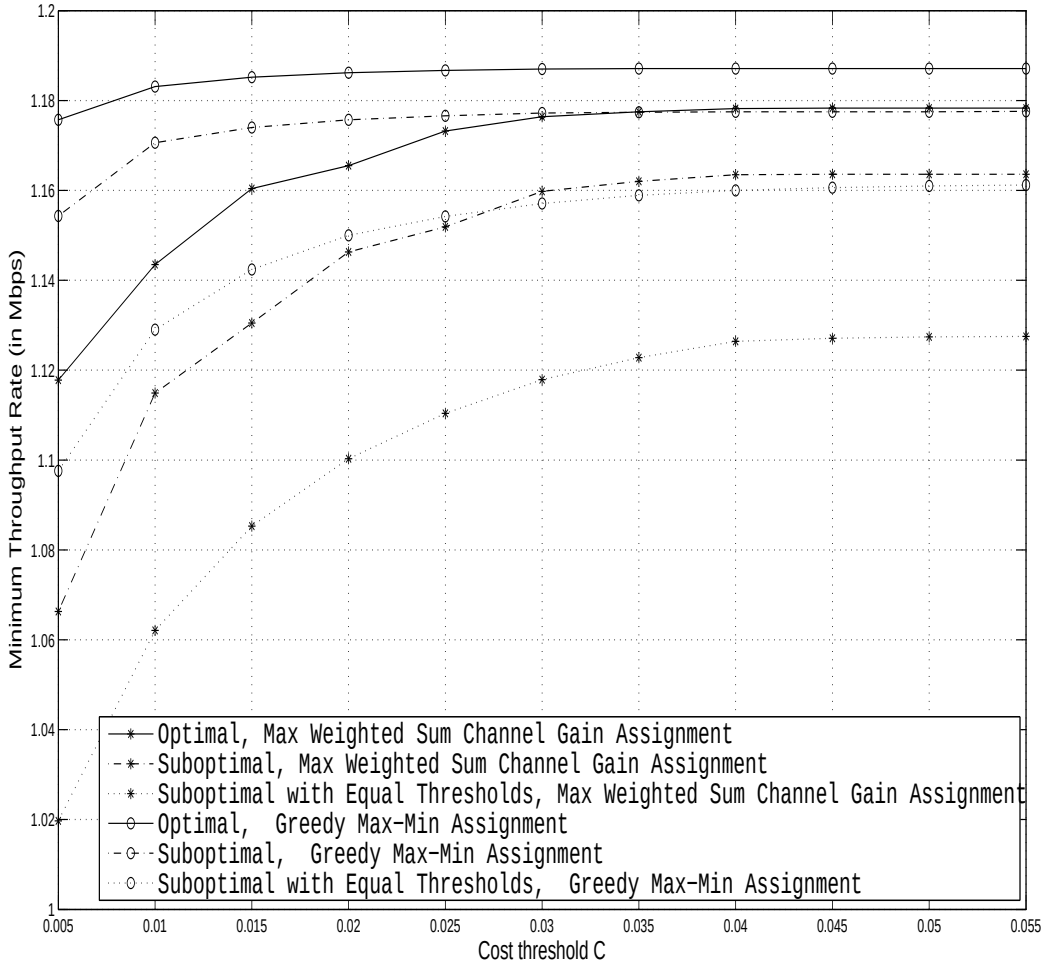

Figure 3.2: Min throughput rate among various bands using 'OR' fusion rule for different sensor allocation and quantization schemes

In Fig. 3.3 and Fig. 3.4, we consider the system considered as in Fig 3.1. However, '2'-out-of-'5' and '3'-out-of-'5' fusion rules are used at the access point in Fig 3.3 and Fig. 3.4, respectively. We see that greedy max-min sensor assignment still outperforms the weighted sum channel gain assignment. We see slightly larger gap in the performance of the optimal and suboptimal schemes. This is because convex restriction in case of '2'-out-of-'5' and '3'-out-of-'5' fusion rule is less close to the original problem (since the channel gains of all sensors assigned to a primary band are replaced with that of worst sensor among them) compared to convex restriction obtained in case of the 'OR' fusion rule.

In Fig. 3.5, we compare the performance of the greedy assignment algorithm to the exhaustive search algorithm which optimally solves (3.17) for a system with $P = 2$ and $N = 4$ for max-min optimization criteria in Fig. 3.5 and sum throughput optimization criteria in Fig. 3.6. 'OR' fusion rule is used in each primary band. The throughput rates r_i in each band are randomly distributed between 1 Mbps and 2 Mbps. $\mathbf{c} = [c_1, c_2] = [0.4, 0.6]$ is used as the cost vector. The maximum allowed probability of miss detection $\bar{P}_{m_i}$ and false alarm $\bar{P}_{f_i}$ are chosen as 0.1 and 0.4, respectively, in all primary bands. We see that the performance degradation due to greedy algorithm, in case of max-min optimization criteria shown in Fig. 3.5, is marginal even though the complexity of the greedy algorithm is substantially lower than the optimal exhaustive search algorithm. Similarly, in case of sum throughput optimization criteria considered in Fig. 3.6, the performances of greedy algorithm and optimal max-min assignment algorithm are very close to each other.

3.7 Conclusions

In this chapter, we investigated cooperative sensing schemes to identify multiple primary signals operating in different spectrum bands. We considered narrow-band CR sensors that

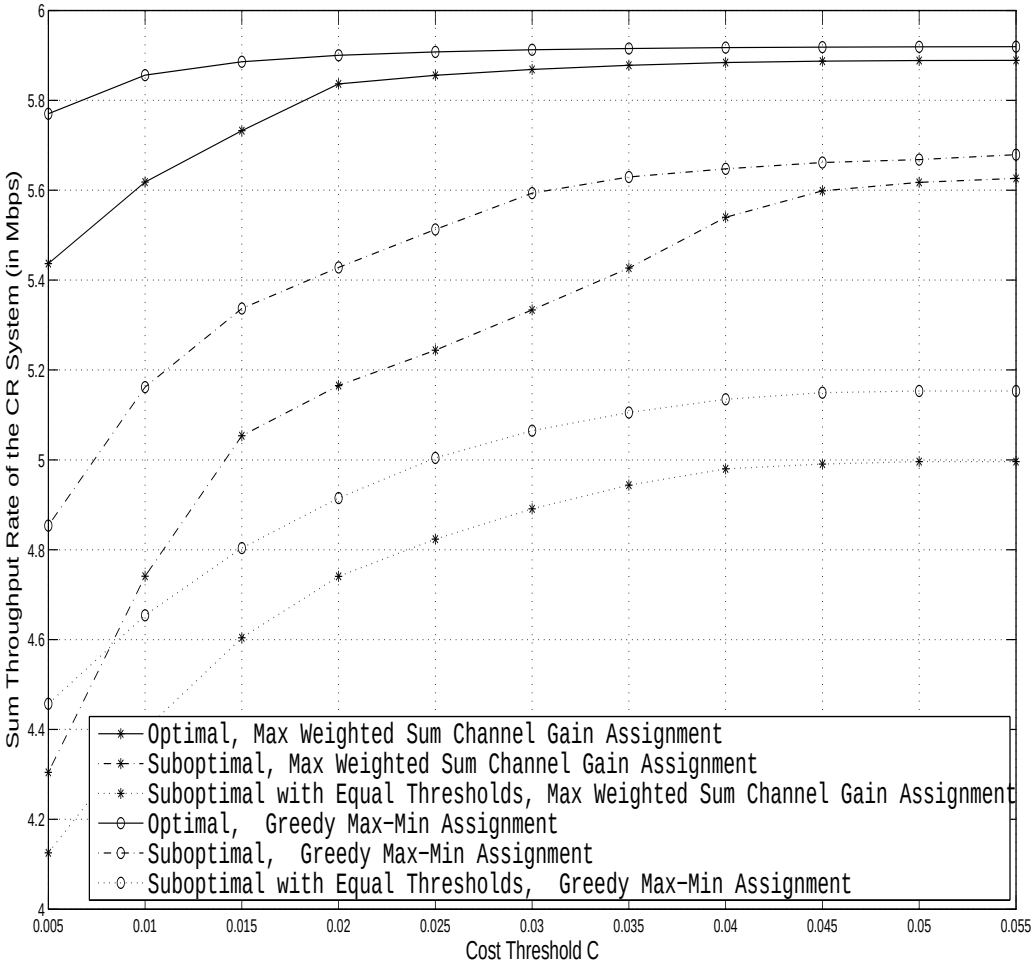

Figure 3.3: Sum throughput rate of the CR system for different sensor allocation and quantization schemes when '2'-out-of-'5' fusion rule is used at the access point in each primary band

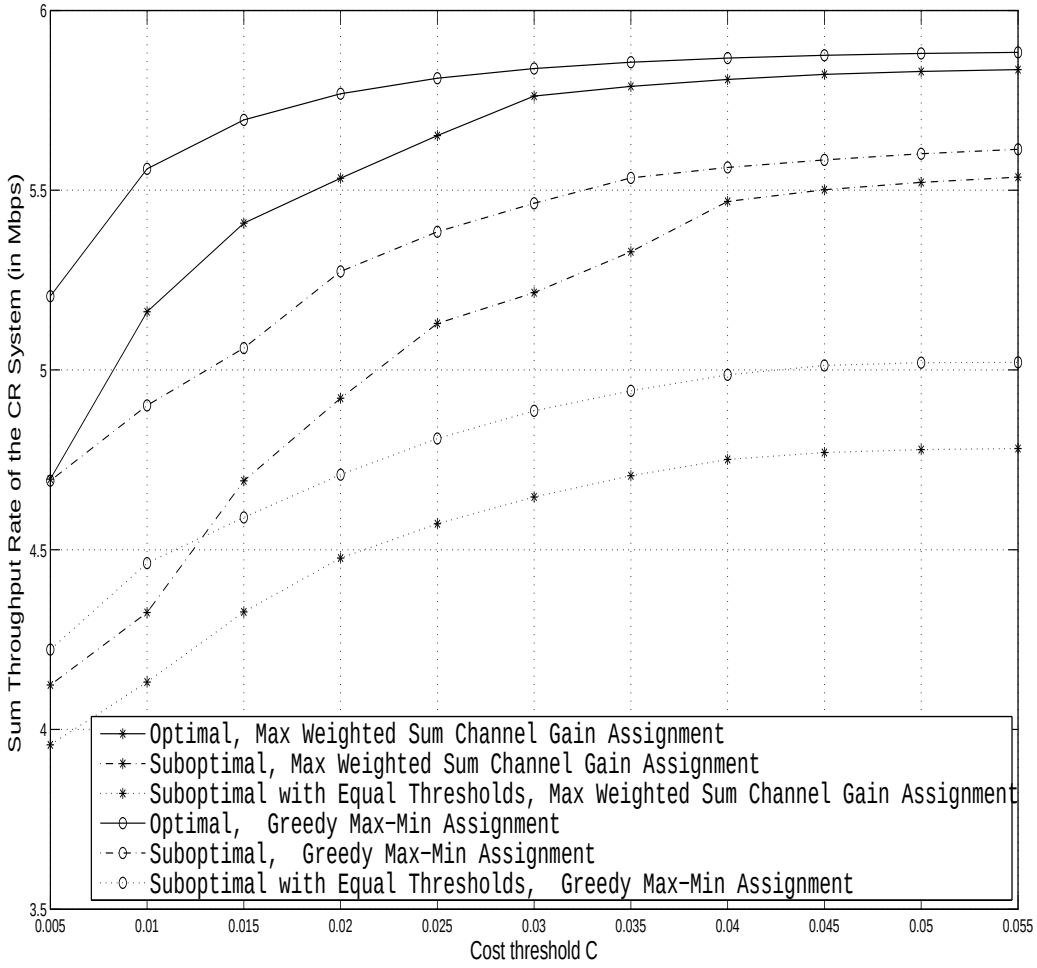

Figure 3.4: Sum throughput rate of the CR system for different sensor allocation and quantization schemes when '3'-out-of-'5' fusion rule is used at the access point in each primary band

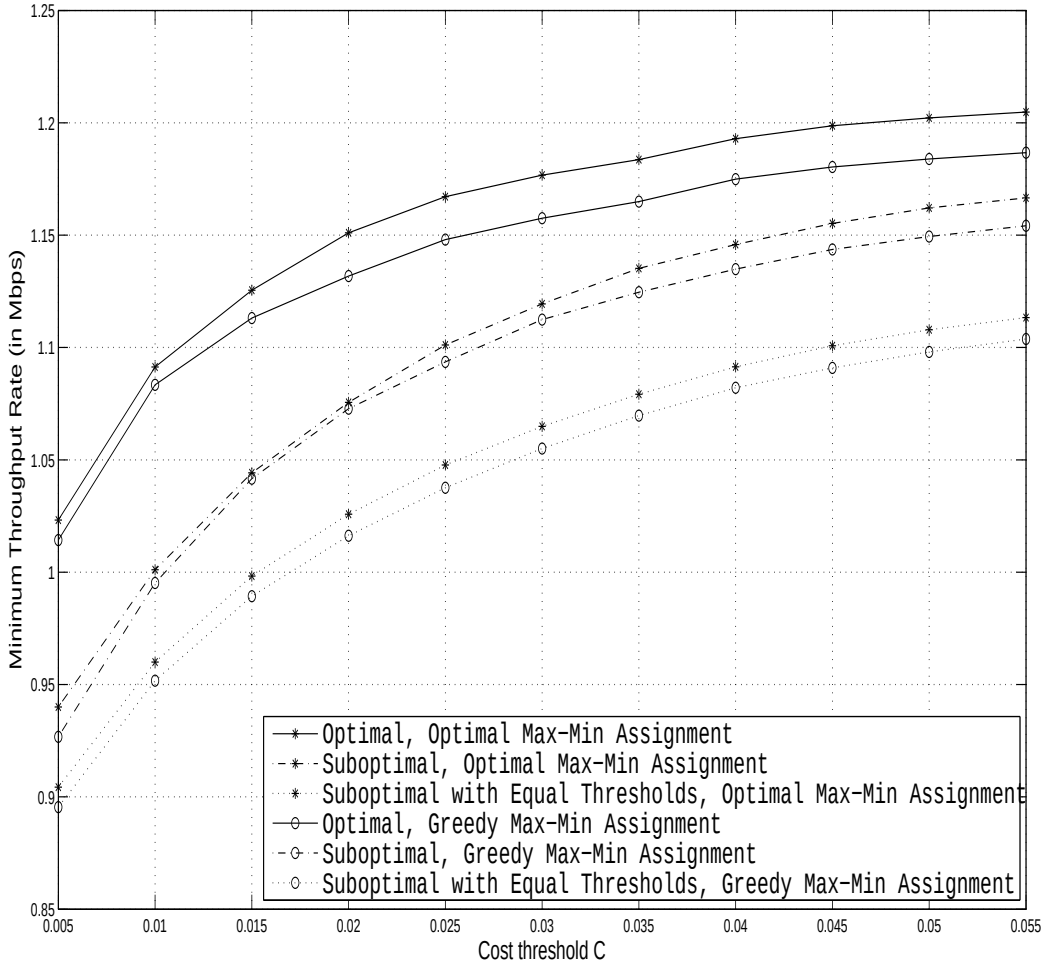

Figure 3.5: Comparison of the optimal and greedy max-min assignment algorithms for 'OR' fusion rule when maximizing the minimum throughput rate among various primary bands

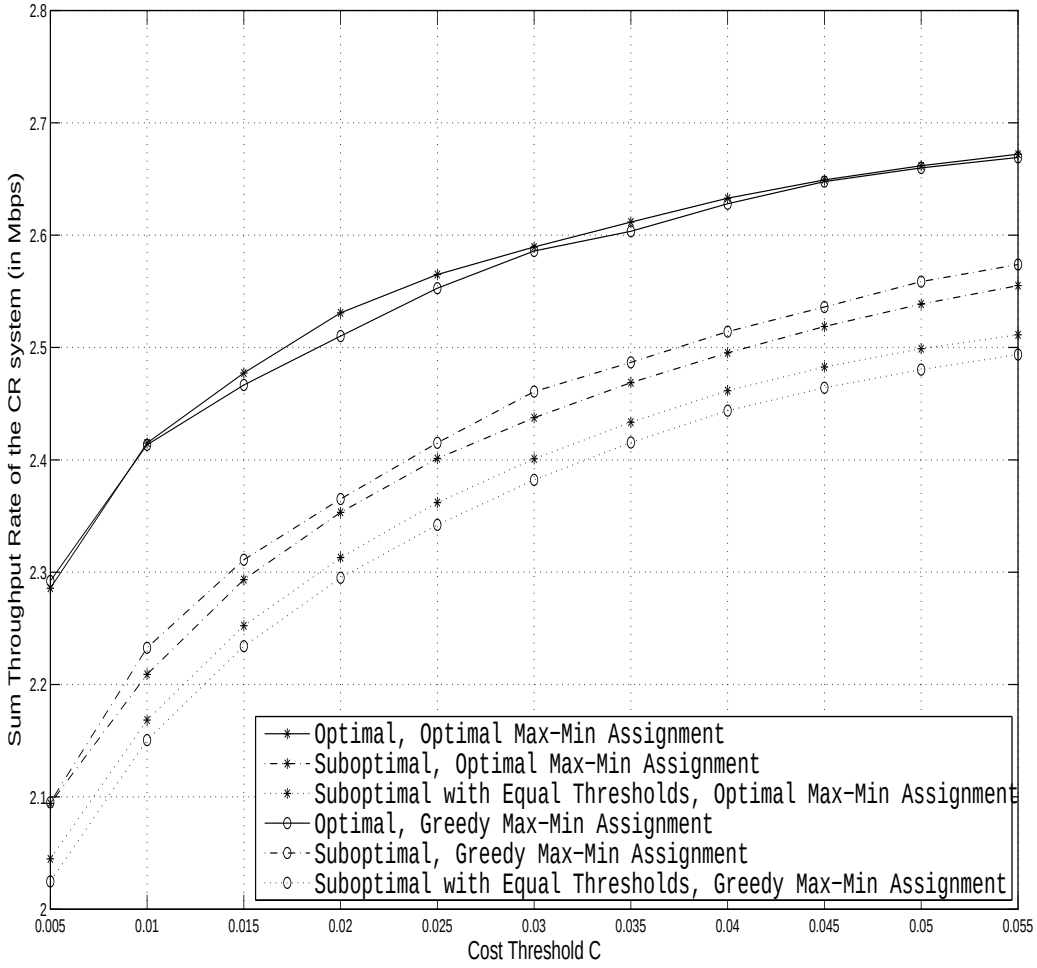

Figure 3.6: Comparison of the optimal and greedy max-min assignment algorithms for 'OR' fusion rule when maximizing the sum throughput rate of the CR system

can sense a single primary band during each sensing iteration. Further, the sensors quantize their sensing information using a single bit before sending it to access point due to bandwidth limitations of the reporting channels. We assumed that a certain data throughput rate is available to the CR system in each band when the primary user is absent. Further, it was assumed that each primary user has certain strict limitations on the interference that CR system could cause due to misdetection of the primary signal. Moreover, even within these interference limits, each primary system imposes a cost on the CR system proportional to the interference caused. For such a system, we studied efficient sensor allocation and quantization schemes. We considered sum throughput rate optimization in which sum of the opportunistic throughput rates available to the CR users is maximized taking into account the cost, interference and QoS constraints. We also investigated the max-min rate optimization in which the minimum rate available among various primary bands is maximized. We initially considered the case when 'OR' fusion rule is used at the access point in each primary band. The original problem, that jointly optimizes the sensor allocation and quantization thresholds, is a mixed integer optimization problem and is highly complex to solve. Therefore, we found suboptimal solutions by solving the original problem in two steps: Allocation of CR sensors to various primary bands based on the channel gains between the CR sensors and primary transmitters followed by determination of the quantization thresholds at the CR sensors. We considered various schemes that could be used to allocate CR sensors. A low complexity greedy algorithm to efficiently assign CR sensors to various primary bands was proposed. After sensor allocation, we studied the optimal scheme to determine the quantization thresholds at the CR sensors, assuming equal quantization thresholds at all the sensors assigned to the same primary band. We showed that the optimal quantization, in general, involves solving a non-convex optimization problem.

Therefore, we proposed a suboptimal convex restriction to the optimal problem using the log-concavity of the Q-function. We further studied quantization schemes when a general *k*-out-of-*N* fusion rule is used at the access point in each primary band.

Chapter 4

Conclusions and Future Research Directions

4.1 Conclusions

In this thesis, we studied CR cooperative sensing system based on a parallel fusion architecture and using energy detection at the sensors. In the first part of this thesis, we investigated schemes to identify CR sensors reporting false high energy values even when the primary signal is not present, which leads to decrease in the throughput rate of the CR system. We presented malicious user detection schemes that use outlier detection techniques based on robust statistics. The proposed malicious user detection schemes do not require knowledge of the primary transmitter location or knowledge of the additive noise variance. Assuming partial knowledge of the primary user activity, we proposed a novel method to improve the performance of the malicious user detection schemes. We also proposed improved malicious user detection schemes assuming knowledge of the spatial location information of the CR sensors. The performance of the proposed schemes were analyzed via simulations

for a cooperative sensing system using equal gain combining as the data fusion scheme at the access point.

We further considered CR systems operating in multiple primary bands. We investigated distributed detection and data fusion schemes to identify multiple primary signals operating in different spectrum bands. Considering narrow-band CR sensors that can sense a single primary band during each sensing iteration and single-bit quantization at the CR sensors, we studied efficient sensor allocation and quantization schemes. We considered sum throughput rate optimization in which sum of the opportunistic throughput rates available to the CR system in all the primary bands is maximized. Also the max-min rate optimization was investigated in which the minimum rate available among various primary bands is maximized. Considering 'OR' fusion rule at the access point in each primary band, we presented the optimization problem that jointly optimizes the sensor allocation and quantization thresholds. Joint sensor allocation and quantization is a mixed integer optimization problem and is NP-hard to solve. Therefore, we solved the problem in two steps. First, CR sensors were allocated to various primary bands based on the channel gains between the CR sensors and primary transmitters. Then, the quantization thresholds were determined at the CR sensors. We considered various methods that could be used to allocate CR sensors. A low complexity greedy sensor allocation algorithm was proposed. After sensor allocation, assuming equal quantization threshold in all the sensors assigned to the same primary band, we studied the optimal scheme to determine the quantization thresholds at the CR sensors. We showed that the optimal quantization scheme, in general, involves solving a non-convex optimization problem and proposed a suboptimal convex restriction to the optimal problem. We further studied quantization schemes when a general k-out-of-N fusion rule is used at the access point in each primary band.

4.2 Future Research Directions

In this section, we propose the possible research directions that can follow from this thesis.

4.2.1 Malicious User Detection

Malicious User Detection Techniques based on Further Information

In the scenarios where CR networks have more information regarding the primary user system such as the location of the primary user, primary user spectral usage behavior, the distribution of channel gains between the primary transmitter and the CR sensors etc., malicious user detection techniques that utilize this knowledge need to be investigated. Model based outlier detection techniques [4, 29] could be applied in such cases.

Single Bit Quantization

Even though the malicious user detection schemes discussed in Chapter 2 can be applied when the sensors quantize their data before sending it to the access point, they might not be efficient, especially when single-bit quantization is used at the sensors. Therefore, it would be interesting to investigate efficient schemes based on the outlier detection techniques to detect malicious users in a CR cooperative sensing systems using data quantization.

Game Theoretic Analysis

Game theory [20] has been applied for analyzing security threats in CR networks in the literature [72]. Game theoretic approach could be used to investigate various methods in which a group of malicious users can avoid detection by the malicious user detection schemes presented in Chapter 2. This can be helpful in further improving the performance of the malicious user detection schemes by devising algorithms to identify such malicious

users.

4.2.2 Sensor Allocation and Quantization Schemes

Channel Estimation Errors and Reporting Channel Errors

In Chapter 3, for sensor allocation and determination of the quantization thresholds at the sensors, we assumed perfect knowledge of the channel gains between the primary transmitters and the CR users. However, there might be errors in the estimation of these channel gains. The effects of channel estimation errors on the performance of the sensor allocation and quantization schemes need to be analyzed. Further, the errors due to reporting channels between the CR sensors and the access point were assumed to be negligible in Chapter 3. In some CR systems, with deep fading between the sensors and the access point, this might not be the case. For such systems, the errors due to the reporting channels must be taken into consideration while allocating sensors and determining the quantization thresholds.

Non-Gaussian Noise

In this thesis, we assumed that the additive noise is white and Gaussian distributed. However, this assumption may not be true in general for CR systems due to presence of other secondary user interferences [62]. The sensor allocation schemes and quantization schemes obtained in this thesis could be extended for the case of colored non-Gaussian noise.

Bibliography

[1] O. Afolabi, K. Kim, and A. Ahmad. On secure spectrum sensing in cognitive radio networks using emitters electromagnetic signature. In *Proceedings of 18th Internatonal Conference on Computer Communications and Networks (ICCCN)*, pages 1–5, 2009. → pages 6

[2] C. Aggarwal and S. Yu. An effective and efficient algorithm for high-dimensional outlier detection. In *The International Journal on Very Large Data Bases*, volume 14, pages 211–221, 2005. → pages 9

[3] G. Atia, E. Ermis, and V. Saligrama. Robust energy efficient cooperative spectrum sensing in cognitive radios. In *IEEE/SP 14th Workshop on Statistical Signal Processing (SSP) 2007*, pages 502–507, 2007. → pages 10

[4] V. Barnett and T. Lewis. *Outliers in Statistical Data*. John Wiley & Sons., 3rd edition, 1994. → pages 9, 82

[5] R. S. Blum, S. A. Kassam, and H. V. Poor. Distributed detection with multiple sensors: Part ii-advanced topics. In *Proceedings of IEEE*, volume 85, pages 64–79, Jan 1997. → pages 11

[6] G. E. P. Box and D. R. Cox. An analysis of transformations. In *Journal of Royal Statistical Society*, volume B28, pages 211–252, 1964. → pages 18

[7] S. Boyd and L. Vanderberghe. *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2003. → pages 63, 66

[8] J. Branch, B. Szymanski, C. Giannella, R. Wolff, and H. Kargupta. In-network outlier detection in wireless sensor networks. In *26th IEEE International Conference on Distributed Computing Systems (ICDCS) 2006*, pages 51–51, 2006. → pages 9

[9] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander. Lof: identifying density-based local outliers. In *ACM SIGMOD*, volume 29, pages 93–104, 2000. → pages 9

[10] G. Brys, M. Hubert, and A. Struyf. A comparison of some new measures of skewness. In *Developments in Robust statistics, ICORS 2001*, pages 98–113, 2001. → pages 26, 27, 33

[11] G. Brys, M. Hubert, and A. Struyf. A robust measure of skewness. In *Journal of Computational and Graphical Statistics*, volume 13, pages 996–1017, 2004. → pages 26

[12] J. L. Burbank. Security in cognitive radio networks: The required evolution in approaches to wireless network security. In *Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, pages 1–7, 2008. → pages 6

[13] D. Cabric, S. M. Mishra, and R. W. Brodersen. Implementation issues in spectrum sensing for cognitive radio. In *Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004*, volume 1, pages 772–776, Nov 2004. → pages 2

[14] L. Chen, J. Wang, and S. Li. Cooperative spectrum sensing with multi-bits local sensing decisions in cognitive radio context. In *IEEE Wireless Communications and Networking Conference (WCNC) 2008*, pages 570–575, 2008. → pages 12

[15] R. Chen, J.-M. Park, and K. Bian. Robust distributed spectrum sensing in cognitive radio networks. In *The 27th IEEE Conference on Computer Communications (INFOCOM)*, pages 1876–1884, 2008. → pages 8

[16] R. Chen, J.-M. Park, and J. Reed. Defense against pu emulation attacks in cr networks. In *IEEE Journal on Selected Areas in Communications*, volume 26, pages 25–37, Jan 2008. → pages 6

[17] T. Clancy and N. Goergen. Security in cognitive radio networks: Threats and mitigation. In *Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, pages 1–8, 2008. → pages 6

[18] T. Do and B. L. Mark. Joint spatial-temporal spectrum sensing for cognitive radio networks. In *43rd Annual Conference on Information Sciences and Systems, 2009. CISS 2009.*, pages 124–129, 2009. → pages 12

[19] FCC. Spectrum policy task force report. In *Technical Report 02-135*, Nov 2002. → pages 1

[20] D. Fudenberg and J. Tirole. *Game Theory*. MIT Press, 1st edition, 1991. → pages 82

[21] G. Ganesan and Y. Li. Cooperative spectrum sensing in cognitive radio: Part i: two user networks. In *IEEE Transactions on Wireless Communications*, volume 6, pages 2204–2213, June 2007. → pages 4, 5

[22] G. Ganesan and Y. Li. Cooperative spectrum sensing in cognitive radio: Part ii: multiuser networks. In *IEEE Transactions on Wireless Communications*, volume 6, pages 2214–2222, June 2007. → pages 4, 5

[23] G. Ganesan and Y. Li. Cooperative spectrum sensing in cr networks. In *IEEE Conference on Dynamic Spectrum Access Networks (DYSPAN'05)*, pages 137–143, Nov 2005. → pages 4

[24] W. A. Gardner. *Cyclostationarity in Communications and Signal Processing*. New Jersey, NY, USA: IEEE Press, 1993. → pages 3

[25] A. Ghasemi and E. S. Sousa. Opportunistic spectrum access in fading channels through collaborative sensing. In *Journal of Communications (JCM)*, volume 2, pages 71–82, March 2007. → pages 5, 12

[26] A. M. Gross. Confidence interval robustness with long-tailed symmetric distributions. In *Journal of the American Statistical Association*, volume 71, pages 409–416, June 1976. → pages 24

[27] M. Gudmundson. Correlation model for shadow fading in mobile radio systems. In *Electronic Letters*, volume 27, pages 2145–2146, 1991. → pages 37

[28] C. Guo, T. Peng, S. Xu, H. Wang, and W. Wang. Cooperative spectrum sensing with cluster-based architecture in cognitive radio networks. In *Proceedings of IEEE Vehicular Technology Conference (VTC), Spring 2009*, pages 1–5, April 2009. → pages 10

[29] D. Hawkins. *Identification of outliers*. Chapman and Hall, London, 1980. → pages 9, 14, 82

[30] S. Haykin. Cognitive radio: Brain-empowered wireless communications. In *IEEE Journal on Selected Areas in Communications*, volume 23, pages 201–220, 2005. → pages 6

[31] C. W. Helstrom. Gradient algorithm for quantization levels in distributed detection systems. In *IEEE Transactions on Aerospace and Electronic Systems*, volume 31, pages 390–398, Jan 1995. → pages 94

[32] P. S. Horn. A biweight prediction interval for random samples. In *Journal of the American Statistical Association*, volume 83, pages 249–256, 1988. → pages 24

[33] M. Hubert and E. Vandervieren. An adjusted boxplot for skewed distributions. In *Computational Statistics and Data Analysis*, volume 52, pages 5186–5201, 2008. → pages 27, 33

[34] P. Kaligineedi and V. K. Bhargava. Sensor allocation and quantization schemes for multi-band cognitive radio cooperative sensing system. In *IEEE Transactions on Wireless Communications (Accepted)*. → pages iv

[35] P. Kaligineedi and V. K. Bhargava. Distributed detection of primary signals in fading channels for cognitive radio networks. In *Proceedings of IEEE Global Communications Conference (Globecom) 2008*, pages 1–5, 2008. → pages

[36] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava. Malicious user detection for cognitive radio systems. In *IEEE Transactions on Wireless Communications*, volume 9, pages 2488–2497, August 2010. → pages iv

[37] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava. Secure cooperative sensing techniques for cognitive radio systems. In *IEEE International Conference on Communications (ICC) 2008*, pages 3406–3410, May 2008. → pages iv, 18

[38] D. Kazakos. New error bounds and optimum quantization for multisensor distributed signal detection. In *IEEE Transactions on Communications*, volume 40, pages 1144–1151, July 1992. → pages 11

[39] E. M. Knorr and R. T. Ng. Algorithms for mining distance-based outliers in large datasets. In *Proc. the 24th International Conference on Very Large Databases (VLDB)*, pages 392–403, 1998. → pages 9

[40] D. A. Lax. Robust estimators of scale: Finite-sample performance in long-tailed symmetric distributions. In *Journal of the American Statistical Association*, volume 80, pages 736–741, Sept. 1985. → pages 21, 23, 24

[41] M. Longo, T. D. Lookabaugh, and R. M. Gray. Quantization for decentralized hypothesis testing under communication constraints. In *IEEE Transactions on Information Theory*, volume 36, pages 241–255, March 1990. → pages 11

[42] S. M. Mishra, R. Tandra, and A. Sahai. The case for multiband sensing. In *Proceedings of the Allerton Conference on Communications, Control and Computing*, 2007. → pages 6

[43] S. M. Mishra, A. Sahai, and R. W. Brodersen. Cooperative sensing among crs. In *IEEE International Conference on Communications (ICC) 2006*, pages 1658–1663, June 2006. → pages 4, 5, 6, 9, 14, 16, 58, 65

[44] J. Mitola. *Software Radio Architecture*. John Wiley & Sons, 2000. → pages 1, 2

[45] F. Mostseller and J. W. Tukey. *Data Analysis and Regression: A second course in Statistics*. Reading, MA: Addison-Wesley, 1978. → pages 20, 21, 23

[46] J. Munkres. Algorithms for the assignment and transportation problems. In *Journal of the Society for Industrial and Applied Mathematics*, volume 5, pages 32–38, March 1957. → pages 11, 54, 59

[47] R. Niu, P. K. Varshney, and Q. Cheng. Distributed detection in a large wireless sensor network. In *International Journal on Information Fusion*, volume 7, pages 380–394, 2006. → pages 12, 61

[48] T. Palpanas, D. Papadopoulos, V. Kalogeraki, and D. Gunopulos. Distributed deviation detection in sensor networks. In *ACM SIGMOD*, volume 32, pages 77–82, 2003. → pages 9

[49] D. W. Pentico. Assignment problems: A golden anniversary survey. In *European Journal of Operational Research*, volume 176, pages 774–793, 2008. → pages 11, 54

[50] K. T. Phan, L. B. Le, S. A. Vorobyov, and T. Le-Ngoc. Centralized and distributed power allocation in multi-user wireless relay networks. In *Proceedings of IEEE International Conference on Communications (ICC) 2009*, pages 1–5, 2009. → pages 67

[51] A. P. Punnen and Y. P. Aneja. Categorized assignment scheduling: a tabu search approach. In *Journal on Operational Research Society*, volume 44, pages 673–679, 1993. → pages 60

[52] Z. Quan, S. Cui, A. H. Sayed, and H. V. Poor. Optimal multiband joint detection for spectrum sensing in cognitive radio networks. In *IEEE Transactions on Signal Processing*, volume 57, pages 1128–1140, 2009. → pages 9, 10, 57, 58

[53] P. Ray and P. K. Varshney. Distributed detection in wireless sensor networks using dynamic sensor thresholds. In *International Journal of Distributed Sensor Networks*, volume 4, pages 5–12, 2010. → pages 10

[54] M. Sanna and M. Murroni. Optimization of non-convex multiband cooperative sensing with genetic algorithms. In *IEEE Journal of Selected Topics in Signal Processing*, 2010. → pages 10

[55] S. Saunders and A. Aragon-Zavala. *Antennas and Propagation for Wireless Communication Systems*. John Wiley & Sons., 2nd edition, 2007. → pages 16, 37

[56] N. S. Shankar, C. Cordeiro, and K. Challapali. Spectrum agile radios: utilization and sensing architectures. In *IEEE Conference on Dynamic Spectrum Access Networks (DYSPAN'05)*, pages 160–169, Nov 2005. → pages 4

[57] B. Shen, T. Cui, K. Kwak, C. Zhao, and Z. Zhou. An optimal soft fusion scheme for cooperative spectrum sensing in cognitive radio network. In *IEEE Wireless Communications and Networking Conference (WCNC), 2009*, pages 1–5, 2009. → pages 12

[58] B. Sheng, Q. Li, W. Mao, and W. Jin. Outlier detection in sensor networks. In *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*, pages 219–228, 2007. → pages 9

[59] A. Silberstein, K. Munagala, and J. Yang. Energy-efficient monitoring of extreme values in sensor networks. In *Proceedings of the 2006 ACM SIGMOD international conference on Management of data*, pages 169–180, 2006. → pages 9

[60] C. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. Shellhammer, and W. Caldwell. Ieee 802.22: The first cognitive radio wireless regional area network standard. In *IEEE Communications Magazine*, volume 47, pages 130–138, Jan. 2009. → pages 2

[61] C. Sun, W. Zhang, and K. B. Lataief. Cluster-based cooperative spectrum sensing in cognitive radio systems. In *Proceedings of IEEE International conference on Communications (ICC) 2007*, pages 2511–2515, June 2007. → pages 10

[62] R. Tandra and A. Sahai. Snr walls for signal detection. In *IEEE Journal on Selected Topics in Signal Processing*, volume 2, pages 4–17, Feb 2008. → pages 3, 83

[63] R. Tandra, A. Sahai, and S. M. Mishra. What is a spectrum hole and what does it take to recognize one? In *Proceedings of the IEEE*, volume 97, pages 822–848, 2009. → pages 2, 3, 4

[64] S. Thomopoulos, R. Viswanathan, and D. Bougoulias. Optimal distributed decision fusion. In *IEEE Transactions on Aerospace and Electronic Systems*, volume 25, pages 761–765, Sep. 1989. → pages 11

[65] J. N. Tsitsiklis. Decentralized detection by a large number of sensors. In *Mathematics of Control, Signals and Systems*, volume 1, pages 167–182, 1988. → pages 11, 61

[66] J. Unnikrishnan and V. Veeravalli. Cooperative sensing for primary detection in cognitive radios. In *IEEE Journal on Selected Topics in Signal Processing*, volume 2, pages 18–27, Feb 2008. → pages 4, 5

[67] H. Urkowitz. Energy detection of unknown deterministic signals. In *Proceedings of IEEE*, volume 55, pages 523–531, April 1967. → pages 2, 16

[68] O. van den Biggelaar, J.-M. Dricot, P. De Doncker, and F. Horlin. Quantization and transmission of the energy measures for cooperative spectrum sensing. In *IEEE 71st Vehicular Technology Conference (VTC 2010-Spring)*, pages 1–5, 2010. → pages 12

[69] P. K. Varshney. *Distributed Detection and Data fusion*. New York: Springer-Verlag, 1996. → pages 11, 61

[70] V. V. Veeravalli. Sequential decision fusion: theory and applications. In *Journal of the Franklin Institute*, volume 336, pages 301–322, 1999. → pages 5, 11

[71] F. E. Visser, G. M. Janssen, and P. Paweczak. Multinode spectrum sensing based on energy detection for dynamic spectrum access. In *IEEE Vehicular Technology Conference*, pages 1394–1398, May 2008. → pages 35

[72] B. Wang, Y. Wu, Z. Ji, K. J. R. Liu, and T. C. Clancy. Game theoretical mechanism design methods: suppressing cheating in cognitive radio networks. In *IEEE Signal Processing Magazine*, volume 25, pages 74–84, 2008. → pages 82

[73] H. Wang, L. Lightfoot, and T. Li. On phy-layer security of cognitive radio: Collaborative sensing under malicious attacks. In *44th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6, 2010. → pages 8

[74] W. Wang, H. Ki, Y. Sun, and Z. Han. Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks. In *EURASIP Journal on Advances in Signal Processing*, pages 1–15, 2010. → pages 8

[75] F. R. Yu, H. Tang, M. Huang, Z. Li, and P. C. Mason. Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios. In *IEEE Military Communications Conference (MILCOM)*, pages 1–7, 2009. → pages 8

[76] K. Zeng, P. Paweczak, and D. Cabric. Reputation-based cooperative spectrum sensing with trusted nodes assistance. In *IEEE Communications Letters*, volume 14, pages 226–228, March 2010. → pages 8

[77] Y. Zeng and Y.-C. Liang. Maximum-minimum eigenvalue detection for cognitive radio. In *Proceedings of the IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC)*, pages 1–15, Sept. 2007. → pages 3, 8

[78] Y. Zhang, G. Xu, and X. Geng. Security threats in cognitive radio networks. In *10th IEEE International Conference on High Performance Computing and Communications (HPCC)*, pages 1036–1041, Sept. 2008. → pages 6

Appendix A

Convexity Conditions for the Objective Functions (3.18) and (3.35)

Consider the function $P_f^{(k,N)}(x) = \sum_{r=k}^{N} \binom{N}{r} Q(x)^r (1-Q(x))^{N-r}$. $P_f^{(k,N)}(\alpha_i)$ represents the probability of false alarm P_{f_i} when a k-out-of-N fusion rule is used at the access point in primary band i. Note that, for the 'OR' fusion rule, $P_f^{(k,N)}(x) = P_f^{(1,N)}(x) = \sum_{r=1}^{N} \binom{N}{r} Q(x)^r (1-Q(x))^{N-r} = 1-(1-Q(x))^N$. The derivative of $P_f^{(k,N)}(x)$ is given by

$$\frac{d}{dx} P_f^{(k,N)}(x) = N \binom{N-1}{k-1} Q(x)^{k-1} (1-Q(x))^{N-k} \frac{d}{dx} Q(x) \tag{A.1}$$

The double derivative of $P_f^{(k,N)}(x)$ (using the fact that $\frac{d}{dx}Q(x) = -\frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$ and $\frac{d^2}{dx^2}Q(x) =$

$\frac{x}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}$) is given by

$$\frac{d^2}{dx^2}P_f^{(k,N)}(x) = N\binom{N-1}{k-1}Q(x)^{k-1}(1-Q(x))^{N-k-1}\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}} \left[x(1-Q(x)) - (N-1)\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}} + (k-1)\frac{\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}}{Q(x)} \right] \quad \text{(A.2)}$$

Notice that the terms outside the square brackets on RHS of (A.2) are all positive. We denote the term within the square brackets as

$$g(x) = x(1-Q(x)) - (N-1)\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}} + (k-1)\frac{\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}}{Q(x)} \quad \text{(A.3)}$$

We consider two different cases, Case I: $k \leq \frac{N+1}{2}$ and Case II: $k > \frac{N+1}{2}$, as follows

Case I: $k \leq \frac{N+1}{2}$

For $x < 0$,

$$\begin{aligned} g(x) &= x(1-Q(x)) - (N-1)\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}} + (k-1)\frac{\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}}{Q(x)} \\ &\leq x(1-Q(x)) - ((N-1)-2(k-1))\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}} \quad (\text{since } Q(x) > 0.5 \text{ for } x < 0) \\ &< 0 \qquad (\text{since } x < 0 \text{ and } (N-1)-2(k-1) \geq 0) \end{aligned} \quad \text{(A.4)}$$

Thus, $g(x) < 0$ for $x < 0$. Now consider the derivative of the $g(x)$ for $x \geq 0$,

$$\begin{aligned}
\frac{dg}{dx} &= 1 - Q(x) + x\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}} + x(N-1)\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}} + \\
&\quad (k-1)\frac{1}{Q(x)^2}\left(-Q(x)x\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}} + \left(\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}\right)^2\right) \\
&= 1 - Q(x) + Nx\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}} + (k-1)\frac{\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}}{Q(x)^2}\left(-Q(x)x + \frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}\right)
\end{aligned} \tag{A.5}$$

Using the fact that $Q(x) \leq \frac{1}{x\sqrt{2\pi}}e^{-\frac{x^2}{2}}$ for $x > 0$, it can be easily seen from (A.5) that $\frac{dg}{dx} > 0$ is for $x > 0$.

Thus, $g(x)$ is monotonically increasing for $x > 0$. Now $g(0) \leq 0$ for $k \leq N + 1/2$ and $\lim_{x\to\infty} g(x) = \infty$. Therefore, there exists a point $\bar{x}^{(k,N)} \geq 0$ such that

$$\frac{d^2}{dx^2}P_f^{(k,N)}(x) \geq 0 \quad : \quad x \geq \bar{x}^{(k,N)} \tag{A.6}$$

$$\frac{d^2}{dx^2}P_f^{(k,N)}(x) < 0 \quad : \quad x < \bar{x}^{(k,N)} \tag{A.7}$$

$\bar{x}^{(k,N)}$ can be found by evaluating the root of $g(x)$ using a false position algorithm [31].

Since $P_f^{(k,N)}(x)$ is a decreasing function of x, it follows that there exists a $P_{f_{max}}^{(k,N)}$ corresponding to $\bar{x}^{(k,N)}$ such that

$$P_f^{(k,N)}(x) \text{ is convex} \quad : \quad P_f^{(k,N)}(x) \leq P_{f_{max}}^{(k,N)} \tag{A.8}$$

$$P_f^{(k,N)}(x) \text{ is concave} \quad : \quad P_f^{(k,N)}(x) > P_{f_{max}}^{(k,N)} \tag{A.9}$$

Case II: $k > \frac{N+1}{2}$

It can be shown that (using the fact that $\binom{N}{r}Q(x)^r(1-Q(x))^{N-r}$ are terms of a binomial probability function $B(N,Q(x))$ and $Q(-x) = 1-Q(x)$)

$$P_f^{(k,N)}(x) = 1 - P_f^{(N-k+1,N)}(-x) \tag{A.10}$$

Since, $N-k+1 \leq \frac{N+1}{2}$, from Case I it follows hat $P_f^{(N-k+1,N)}(-x)$ is concave for $-x \leq \bar{x}^{(N-k+1,N)}$ and thus $P_f^{(k,N)}(x))$ is convex for $x \geq -\bar{x}^{(N-k+1,N)}$.

Thus, for $k > \frac{N+1}{2}$,

$$\bar{x}^{(k,N)} = -\bar{x}^{(N-k+1,N)} \tag{A.11}$$

$$P_{f_{max}}^{(k,N)} = 1 - P_{f_{max}}^{(N-k+1,N)} \tag{A.12}$$

Table 3.2 shows the values of $\bar{x}^{(k,N)}$ for which $P_f(k,N)(x)$ is convex for $x > \bar{x}^{(k,N)}$ and concave for $x < \bar{x}^{(k,N)}$ for various values of k and N. Table 3.3 shows the maximum probability of false alarm $P_{f_{max}}^{(k,N)}$ below which the P_{f_i} is convex, for a k-out-of-N fusion rule, at different values of k and N. From Table 3.3, it can be see that the values of $P_{f_{max}}^{(k,N)}$ are greater than 0.44 for all values of N less than 10.

Appendix B

Log-Concavity of Q-function

The double derivative of log of Q-function is given by

$$\frac{d^2}{dx^2}\log Q(x) = \frac{Q(x)\frac{d^2}{dx^2}Q(x) - \left(\frac{d}{dx}Q(x)\right)^2}{Q(x)^2} \tag{B.1}$$

$$= \frac{Q(x)x\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}} - \left(-\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}\right)^2}{Q(x)^2} \tag{B.2}$$

$$= \frac{\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}}{Q(x)^2}\left[xQ(x) - \frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}\right] \tag{B.3}$$

Its easy see that terms outside the square brackets on RHS of (B.3) are positive. Now, the term inside the square brackets, $xQ(x) - \frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}$, is less than or equal to zero for $x \leq 0$, since both $xQ(x)$ and $-\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}$ are less than or equal to zero. For $x > 0$, it is well known that $Q(x) < \frac{1}{x\sqrt{2\pi}}e^{-\frac{x^2}{2}}$. Therefore, $xQ(x) - \frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}$ is less than zero for $x > 0$. Hence, from (B.3), it follows that double derivative of $\log Q(x)$ is negative for all x and thus, $\log Q(x)$ is a concave function. Therefore, $Q(x)$ is a log-concave function.