Malicious User Detection in a Cognitive Radio Cooperative Sensing System

Malicious User Detection in a Cognitive Radio Cooperative Sensing System

Praveen Kaligineedi, *Student Member, IEEE,* Majid Khabbazian, *Member, IEEE,* and Vijay K. Bhargava, *Fellow, IEEE*

***Abstract*—Reliable detection of primary users (PUs) is an important task for cognitive radio (CR) systems. Cooperation among a few spectrum sensors has been shown to offer significant gain in the performance of the CR spectrum-sensing system by countering the shadow-fading effects. We consider a parallel fusion network in which the sensors send their sensing information to an access point which makes the final decision regarding presence or absence of the PU signal. It has been shown in the literature that the presence of malicious users sending false sensing data can severely degrade the performance of such a cooperative sensing system. In this paper, we investigate schemes to identify the malicious users based on outlier detection techniques for a cooperative sensing system employing energy detection at the sensors. We take into consideration constraints imposed by the CR scenario such as the lack of information about the primary signal propagation environment and the small size of the sensing data samples. Considering partial information of the PU activity, we propose a novel method to identify the malicious users. We further propose malicious user detection schemes that take into consideration the spatial information of the CR sensors. The performance of the proposed schemes are studied using simulations.**

***Index Terms*—Cognitive radio, cooperative sensing, malicious user detection, outlier detection.**

I. Introduction

In A recent study conducted by the Federal Communications Commission (FCC), it was found that most of the allocated radio frequency spectrum is not efficiently utilized by the licensed (primary) users [1]. In order to improve spectral utilization, it has been suggested that opportunistic access of the spectrum be given to unlicensed secondary users [2]. Cognitive Radio (CR) is an emerging technology that would allow an unlicensed (cognitive) radio user to sense and make efficient use of any available radio spectrum at a given time.

Identifying the presence of primary users (PUs) with high reliability is crucial for a CR system. This process is difficult due to the presence of a wide range of PUs using different modulation schemes, transmission powers and data rates, and due to interference from other secondary users, variable propagation losses and thermal noise. The burden on signal processing techniques to detect the PU can be reduced to a large extent by using cooperative diversity between CR spectrum sensors. Cooperation among a few sensing devices sufficiently distant from one another (in order to ensure independent propagation loss) can help reduce the individual sensitivity requirements by countering the shadowing effects [3], [4], [5].

In this paper, we consider a parallel fusion sensing architecture in which the spectrum sensors send their sensing data to an access point. The access point makes a final decision regarding the presence or absence of a primary signal based on the data obtained from the sensors. It was shown in [3] that the presence of a few malicious users sending false sensing data can severely affect the performance of such a cooperative sensing system. Techniques to detect the malicious users in CR cooperative sensing systems have recently been proposed in the literature [6], [7].

In our previous work [7], a malicious-user detection scheme was proposed based on an outlier-detection technique [8] considering energy detection at the sensors and assuming constant path loss between the PU transmitter and the CR sensors. Using the average combination scheme as the data fusion rule at the access point, it was shown in [7] that employing outlier detection technique improves the performance of the system affected by the malicious users. An outlier is an observation which is far away from rest of the data [8]. Outlier detection techniques are extensively used to identify fraudulent data in the field of data mining. Their applications include video surveillance, intrusion detection and identifying fraudulent transactions.

In this paper, we further investigate malicious user detection schemes that are based on robust outlier-detection techniques. We focus on those malicious users that reduce the throughput of the CR system by giving false high energy values when the PU signal is not present. 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 PU network and the small size of the sensing data samples among which the malicious user data points need

Manuscript received March 17, 2009; revised October 22, 2009 and March 17, 2010; accepted May 23, 2010. The associate editor coordinating the review of this paper and approving it for publication was S. Wei.

This research was supported, in part, by the Natural Sciences and Engineering Research Council of Canada (NSERC) under their Strategic Project Grant Program.

P. Kaligineedi and V. K. Bhargava are with the Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC, V6T 1Z4 Canada (e-mail: {praveenk, vijayb}@ece.ubc.ca).

M. Khabbazian is with MIT Computer Science and Artificial Intelligence Laboratory, Cambridge, MA, USA 02139 (e-mail: majidk@mit.edu).

Digital Object Identifier 10.1109/TWC.2010.061510.090395

to be identified (It was shown in [3] 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 paper are not influenced by uncertainty in the noise measurement and do not require any feedback from the PU 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 PU 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 paper is organized as follows. In Section II, we define the cooperative sensing system model and discuss the effect of malicious users on the system. In Section III, we discuss techniques to assign robust and efficient outlier factors to the cognitive users based on their sensing data. In Section IV, we propose techniques which use these outlier factors to detect the malicious users present in the system. In Section V, we propose malicious user detection technique which takes into consideration the users' spatial information. Section VI 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 VII. Finally, conclusions are drawn in Section VIII.

II. 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. We assume that the CR sensors can cancel the interference caused due to other CR transmissions in the network. 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 $e_n[k]$ represent the output of energy detector at n^{th} sensor during the k^{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 [9]

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

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.

A. Impact of Malicious Users

The presence of malicious users can significantly affect the performance of a CR cooperative sensing system [3]. 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 PU 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 PU system.

III. 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 paper, 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 PU system.

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

$$o_n[k] = \frac{e_n^{dB}[k] - \mu[k]}{\sigma[k]} \quad (2)$$

where $e_n^{dB}[k]$ represents the energy detector outputs in decibels (dB), $\mu[k]$ and $\sigma[k]$ are, respectively, the sample mean and the sample standard deviation of the energy values $e_n^{dB}[k]$ of all users at a given iteration k. The sample mean is an estimate of the location of a distribution, and the standard deviation is an estimate of the scale. This method of outlier assignment was used in [7] 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). 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 $e_n[k]$ 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 [11]. 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 distribution 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). First, the mean and the standard deviation are not robust estimates and can be easily manipulated by the data of the malicious users. 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.

A. Alternatives to Mean

As discussed earlier in this section, the sample mean is highly vulnerable to outliers. A robust alternative to the sample mean to estimate the location of a distribution in (2) is the median ($\tilde{\mu}$). The median has a 50% breakdown point (the minimum proportion of contaminated points in a sample that can make the estimate unbounded) 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.

A more efficient and robust estimate of the location is the bi-weight estimate ($\hat{\mu}[k]$) [10], which is calculated iteratively as follows:

$$\hat{\mu}[k] = \frac{\sum w_n[k] e_n^{dB}[k]}{\sum w_n[k]} \tag{3}$$

where

$$w_n[k] = \begin{cases} \left(1 - \left(\frac{e_n^{dB}[k] - \hat{\mu}[k]}{c_1 S}\right)^2\right)^2 & : \quad \left(\frac{e_n^{dB}[k] - \hat{\mu}[k]}{c_1 S}\right)^2 < 1 \\ 0 & : \quad \text{Otherwise} \end{cases} \tag{4}$$

and

$$S = \underset{n}{\text{median}}\{|e_n^{dB}[k] - \hat{\mu}[k]|\} \tag{5}$$

The bi-weight estimate calculates a weighted mean with lower weightage being given to the observations away from the estimate. Initially, all data points are assigned equal weights $w_n[k]$ and then the bi-weight estimate is calculated recursively. S measures the median absolute deviation from the location estimate $\hat{\mu}[k]$. 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. Generally, a tuning constant of $c_1 = 6$ is used [12]. It has been shown in the literature that the bi-weight estimate ($\hat{\mu}[k]$) has higher efficiency than the median, is very robust and has a high breakdown point [10]. The bi-weight estimate 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 [10]. Hence, the bi-weight estimate considers the influence of data points that are not necessarily outliers and at the same time restricting the influence of the outliers beyond certain value. Thus, it is efficient as well as robust.

B. Alternatives to Standard Deviation

One possible alternative to standard deviation for the scale estimate (2) is the median absolute deviation (MAD). Median absolute deviation measures the median of the absolute distances of the data points from the sample median. MAD ($\tilde{\sigma}$) of the e_n^{dB} is given by

$$\tilde{\sigma}[k] = \underset{n}{\text{median}}\{|e_n^{dB}[k] - \tilde{\mu}[k]|\} \tag{6}$$

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 [12].

A more efficient and robust measure of scale is the bi-weight scale (BWS) given by [10]

$$\hat{\sigma}[k] = \sqrt{\frac{N \sum_{u_n^2 < 1} (e_n^{dB}[k] - \mu^*[k])^2 (1 - u_n^2)^4}{s(-1+s)}} \tag{7}$$

where

$$s = \sum_{u_n^2 < 1} (1 - u_n^2)(1 - 5u_n^2) \tag{8}$$

and

$$u_n = \frac{e_n^{dB}[k] - \mu^*[k]}{c_2 \underset{n}{\text{median}}\{|e_n^{dB}[k] - \mu^*[k]|\}} \tag{9}$$

$\mu^*[k]$ is a robust estimate of location such as the median ($\tilde{\mu}[k]$) or the bi-weight estimate ($\hat{\mu}[k]$). c_2 is the tuning constant. c_2 can be used to determine the impact of the extreme data points on the BWS estimate. In [12], it was shown that BWS ($\hat{\sigma}$) is very efficient for a wide range of symmetric distributions compared to other robust estimates of scale. It can be shown that 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 [10]. Generally, a tuning constant of $c_2 = 9$ is found to be more efficient for a wide range of distributions [12].

IV. Malicious User Detection

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

A. 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), 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 PU might have a high outlier factor especially if the distribution of the PU signal-to-noise ratio (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 PU 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 PU does not change its state over a period of time, it is not possible to determine without *a priori* knowledge of PU signal statistics, the channel conditions between PU transmitter and CR sensors or the background noise level, whether the high outlier factor is due good channel between the PU and the CR sensor or due to false data.

B. Method II

If the PU system is dynamic, with the PU 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 PU has started transmission during the particular sensing iteration. Similarly, when the energy values of sensors show significant decrease might indicate that PU has stopped transmission. The change in the energy values of the CR users, as the state of the PU 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 PU 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 III, to identify the iterations during which there was a change in the PU 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 $\hat{\mu}_a[k]$ and adjusted bi-weight scale $\hat{\sigma}_a[k]$ 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 $\hat{\mu}_a[k]$ from iteration k and the adjusted bi-weight estimate from the iteration $k-1$ is obtained as follows

$$\Delta\hat{\mu}_a[k] = \hat{\mu}_a[k] - \hat{\mu}_a[k-1] \tag{10}$$

If the adjusted bi-weight increases from the $k-1^{th}$ iteration to the k^{th} iteration (i.e. if $\Delta\hat{\mu}_a[k]$ is positive), it could be due to the appearance of PU signal in between iterations k and $k-1$. It is also possible that the PU 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 PU and their sensors. Similarly, if the $\Delta\hat{\mu}_a[k]$ is negative, it could be due to disappearance of PU signal, malicious users or due to variations in channel fading and noise components. However, magnitude of $\Delta\hat{\mu}_a[k]$, in general, is expected to be higher if the PU stops transmission.

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

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

$$P_n[k] = \sum_{k' \in S_+[k]} \left(o_n^+[k'-1] + o_n^-[k']\right) + \sum_{k' \in S_-[k]} \left(o_n^-[k'-1] + o_n^+[k']\right) \quad (11)$$

where

$$o_n^-[k'] = \begin{cases} -\frac{e_n^{dB}[k'] - \hat{\mu}_a[k']}{\hat{\sigma}_a[k']} & ; e_n^{dB}[k'] < \hat{\mu}_a[k'] \\ 0 & ; \text{Otherwise} \end{cases} \quad (12)$$

$$o_n^+[k'] = \begin{cases} \frac{e_n^{dB}[k'] - \hat{\mu}_a[k']}{\hat{\sigma}_a[k']} & ; e_n^{dB}[k'] > \hat{\mu}_a[k'] \\ 0 & ; \text{Otherwise} \end{cases} \quad (13)$$

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

Suppose a user consistently produces high energy values irrespective of the presence or absence of the PU. If in between iterations $k-1$ and k the PU reappears, then $\Delta\hat{\mu}_a[k]$ will be positive. As a result, the users producing high energy value during iteration $k-1$ will receive a penalty factor based on their adjusted outlier factors from iteration $k-1$. Also, the CR sensors with low primary SNR will be assigned a penalty factor based on their adjusted outlier factors from iteration k. 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 PU SNR will also be assigned a high penalty factor when the PU disappears in between iterations $k-1$ and k. 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 PU. In such scenario, adjusted bi-weight might decrease due to fluctuations in fading and noise components even though the PU was present during both iterations $k-1$ and k. The choice of K_m and K would depend upon the number of times a PU 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 PU SNR as long as there are few CR users with good channels between PU and their sensors.

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

$$\bar{o}_n[k] = \frac{P_n[k] - \hat{\mu}_P[k]}{\hat{\sigma}_P[k]} \quad (14)$$

where $\hat{\mu}_P[k]$ and $\hat{\sigma}_P[k]$ are bi-weight location and scale estimates of $P_n[k]$. 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.

1) 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 PU changes. Even though the malicious user could be identified using Method II, since it would be not be sure whether the PU 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

$$\Delta\hat{\mu}_a^{\delta}[k] = \hat{\mu}_a[k] - \hat{\mu}_a[k-\delta] \quad (15)$$

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

$$P_n^{\delta}[k] = \sum_{k' \in S_+^{\delta}[k]} \left(o_n^+[k'-\delta] + o_n^-[k']\right) + \sum_{k' \in S_-^{\delta}[k]} \left(o_n^-[k'-\delta] + o_n^+[k']\right) \quad (16)$$

Final penalty factors are assigned as follows

$$P_n[k] = \sum_{\delta \in D_\delta} P_n^{\delta}[k] \quad (17)$$

where D_δ is the set of δ values considered. The outlier factors $\bar{o}_n[k]$ are calculated as in (14). 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.

V. 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 [13], [14]. 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 information of the 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, compared to sensors spread over a larger area. Spatial outlier factors $o_n^s[k]$ are computed as follows

$$o_n^s[k] = \frac{e_n^{dB}[k] - \hat{\mu}^s[k]}{\hat{\sigma}^s[k]} \quad (18)$$

where $\hat{\mu}^s[k]$ and $\hat{\sigma}^s[k]$ 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 $o_n^s[k]$ calculated as in (18) and $o_n[k]$ calculated as in (2), a final outlier factor $o_n^f[k]$ is assigned as follows:

$$o_n^f[k] = \begin{cases} \min\{|o_n^s[k]|, |o_n[k]|\} & ; o_n[k] \geq 0 \\ -\min\{|o_n^s[k]|, |o_n[k]|\} & ; o_n[k] < 0 \end{cases} \quad (19)$$

The minimum of $o_n^s[k]$ and $o_n[k]$ is taken instead of just assigning $o_n^s[k]$ 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 IV-A, using the values $o_n^f[k]$ instead of $o_n[k]$. Alternatively, Method II discussed in Section IV-B can be used. The algorithm remains the same except that $o_n^-[k]$ in (12) and $o_n^+[k]$ in (13) are assigned:

$$o_n^-[k'] = \begin{cases} \min\{|\bar{o}_n^s[k']|, |\bar{o}_n[k']|\} & ; \bar{o}_n[k'] < 0 \\ 0 & ; \text{Otherwise} \end{cases} \quad (20)$$

$$o_n^+[k'] = \begin{cases} \min\{|\bar{o}_n^s[k']|, |\bar{o}_n[k']|\} & ; \bar{o}_n[k'] \geq 0 \\ 0 & ; \text{Otherwise} \end{cases} \quad (21)$$

where

$$\bar{o}_n^s[k'] = \frac{e_n^{dB}[k'] - \hat{\mu}_a^s[k']}{\hat{\sigma}_a^s[k']} \quad (22)$$

$$\bar{o}_n[k'] = \frac{e_n^{dB}[k'] - \hat{\mu}_a[k']}{\hat{\sigma}_a[k']} \quad (23)$$

where $\hat{\mu}_a^s[k']$ and $\hat{\sigma}_a^s[k']$ 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.

VI. 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 due to its simplicity. The equal gain combining method is as follows:

$$\frac{1}{N}\sum_{n=1}^{N} e_n[k] \underset{H_0}{\overset{H_1}{\gtrless}} e_T \quad (24)$$

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:

$$\bar{P}_f = Pr(\hat{d}_m = 1/\hat{d}_0 = d = 0) \quad (25)$$

$$\bar{P}_m = Pr(\hat{d}_m = 0/\hat{d}_0 = d = 1) \quad (26)$$

where d is the PU 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 PU 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 PU 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 $\hat{d}_0 = 1$. Thus, for a system affected by the malicious users and implementing the malicious user detection scheme, the probability of false alarm $\hat{P}_f$ and misdetection $\hat{P}_m$ are given by

$$\hat{P}_f = P_f + (1 - P_f)\bar{P}_f \quad (27)$$

$$\hat{P}_m = P_m + (1 - P_m)\bar{P}_m \quad (28)$$

where P_f and P_m represent the probability of false alarm and misdetection, respectively, for the system unaffected by the malicious users. In malicious user detection Methods I and II described in Section IV, 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.

VII. Simulation Results

We consider a cooperative sensing system with $N = 20$ users. An urban micro-cell propagation model is considered for the primary signal. 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. 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 (7) and (9). The threshold e_T in (24) is chosen so that the probability of false alarm at the fusion center is 0.01. We assume that the probability of a PU 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 $8e_T$.

We assign the spatial locations of the sensors using a two-dimensional model. In Fig 1., 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 $150m$. The (X, Y) coordinates of the PU transmitter are $(0, 0)$ and ignoring fading effects,

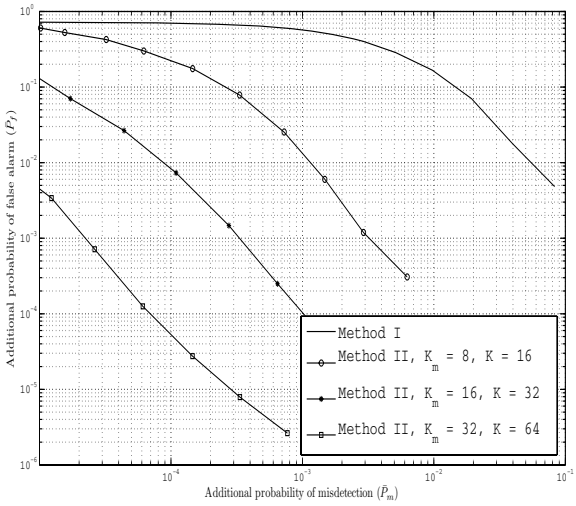
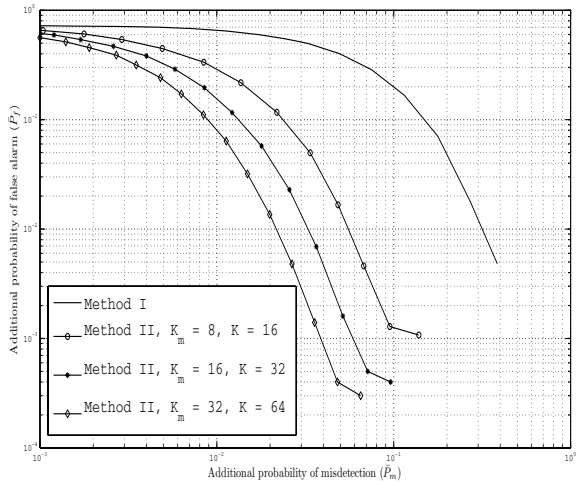


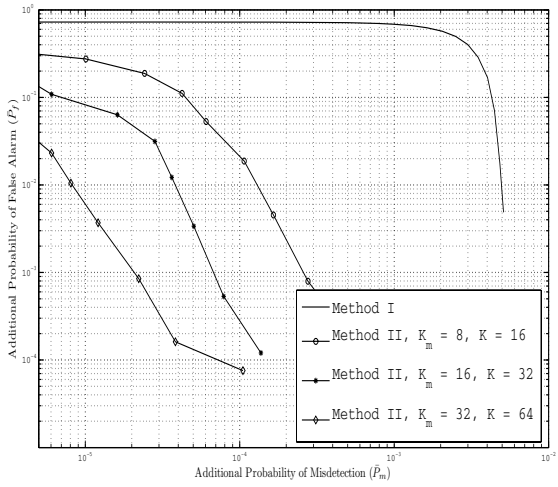
Fig. 1. Performance of malicious user detection schemes for CR network spread over a small area in the presence of $M = 1$ malicious user and $M_{max} = 2$.

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, 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 PU SNR at $(100m, 100m)$ is -5dB and 3dB in case of Fig. 2a and Fig. 2b, respectively. All other parameters are similar to those used in Fig 1. 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. 1. 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. 2a that compared to the system considered in Fig. 1, 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 PU as malicious. Moreover, the impact of eliminating such users on the sensing system would be higher. We also notice that at higher SNR values,



(a) PU SNR at (100m, 100m) ignoring fading effects = -5dB



(b) PU SNR at (100m, 100m) ignoring fading effects = 3dB

Fig. 2. Performance of malicious node detection schemes for CR network spread over a large area in the presence of $M = 1$ malicious user.

as in Fig. 2b, Method II offers significant improvement in the performance.

In Fig. 3, we consider the performance of Method II for the system considered in Fig 2a. We vary the value of K keeping K_m constant at 16. We see that the performance of 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 PU. However, an increase in K also leads to latency in malicious user detection scheme.

In Fig. 4, we consider the performance of Method II at different values of K_m keeping K constant at 32, for the system considered in Fig. 2a. We observe that the best performance is obtained when K_m is $0.5K$. This is due the nature of the PU considered in these simulations. Since, the probability of PU being in state $d = 1$ (PU signal present) or state $d = 0$ (PU signal absent) is assumed to be 0.5 and

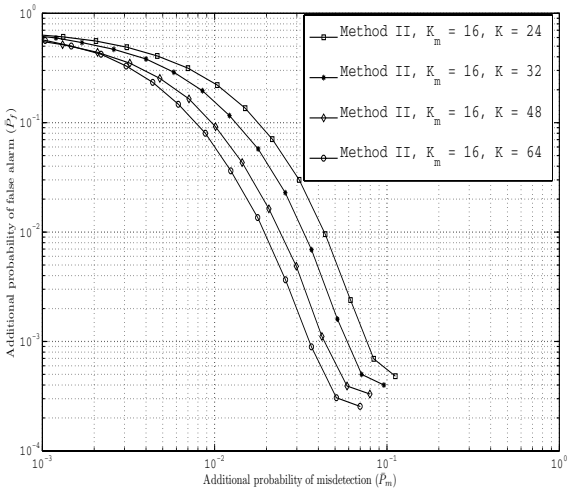


Fig. 3. Performance of Method II at different values of K for $M = 1$, $M_{max} = 2$ and $K_m = 16$.

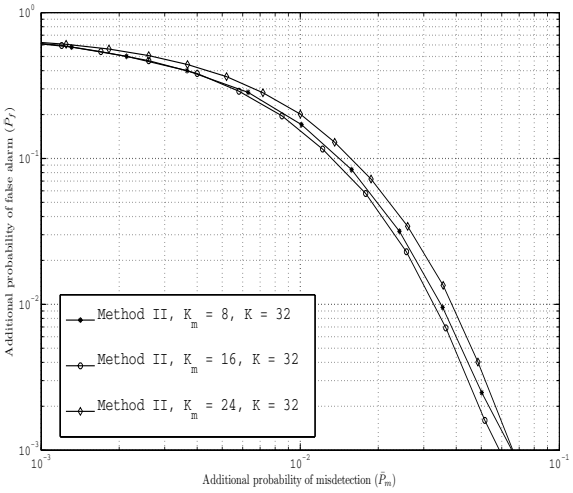
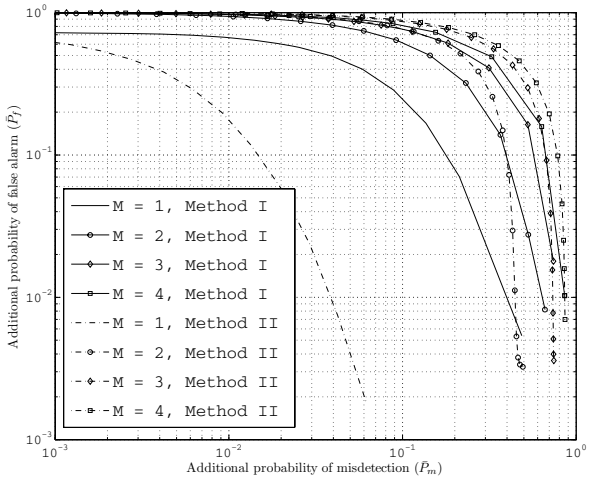


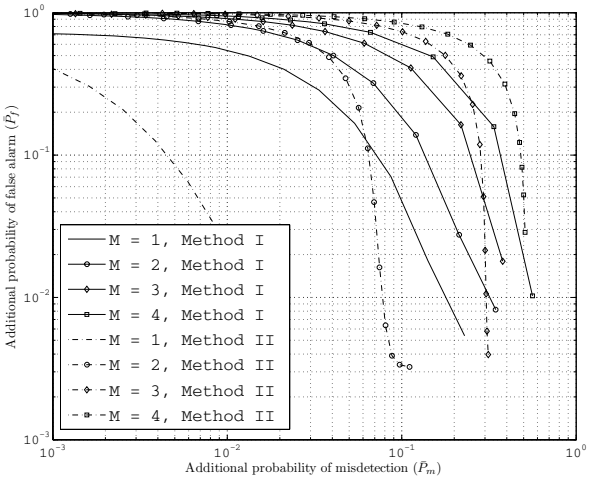
Fig. 4. Performance of Method II at different values of K_m for $M = 1$, $M_{max} = 2$ and $K = 32$

independent from one iteration to another, the most likely number of PU 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 PU 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 PU have been considered in assigning penalty factor, again leading to a poorer performance. Thus, more precise knowledge of the PU activity (expected number of state transitions in a given time interval) can be used to appropriately choose K_m and K.

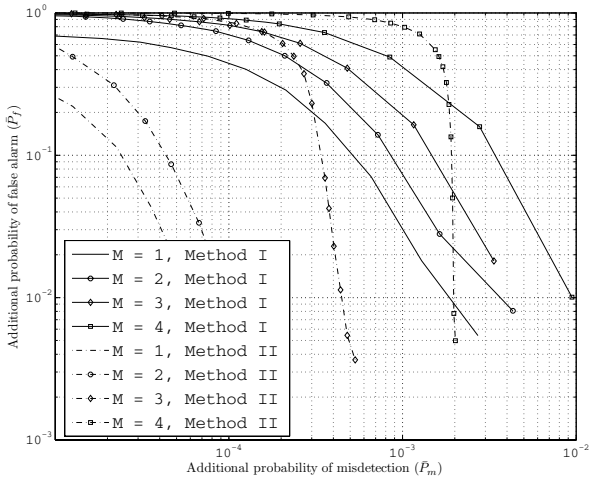
In Fig. 5, we consider the performance of Methods I and II at different values of M for $M_{max} = 20$. The system considered is similar to the system analyzed in Fig. 2a. The PU SNR (ignoring fading effects) at $(100m, 100m)$ is assumed to be -5dB, 0dB and 8dB in Fig. 5a, Fig. 5b and Fig.



(a) PU SNR at (100m, 100m) ignoring fading effects = -5dB



(b) PU SNR at (100m, 100m) ignoring fading effects = 0dB



(c) PU SNR at (100m, 100m) ignoring fading effects = 8dB

Fig. 5. Performance of malicious user detection schemes at different values of M for $M_{max} = 20$

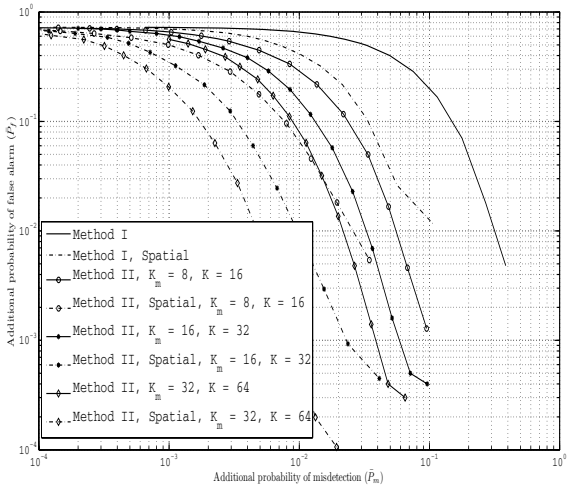
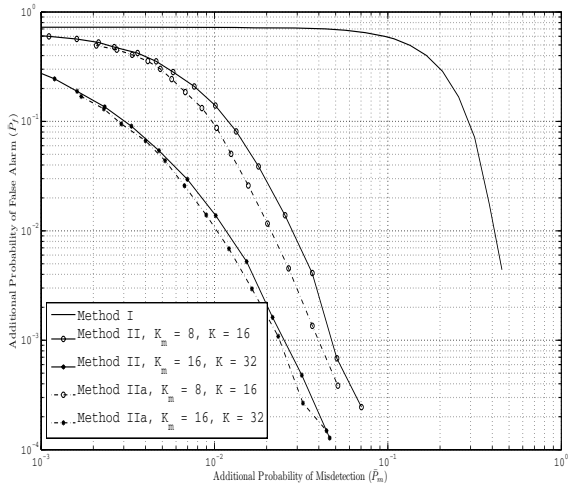
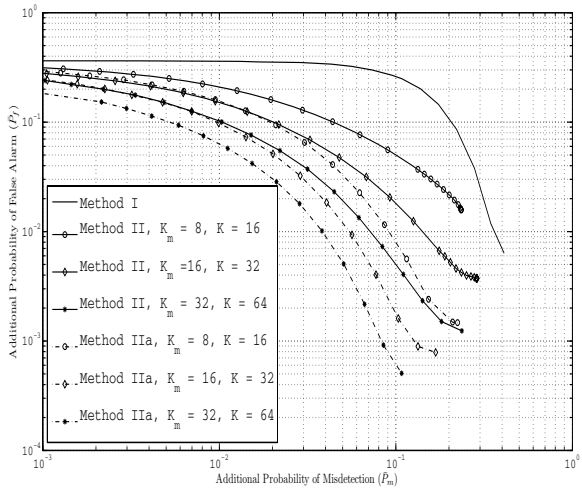


Fig. 6. Performance of malicious user detection schemes using spatial information of the CR network for $M = 1$ malicious user and $M_{max} = 2$.



(a) 'Always Yes' malicious user



(b) Smart malicious user

Fig. 7. Performance of malicious node detection schemes for CR network spread over a large area in the presence of $M = 1$ malicious user.

5c, 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 PU. 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 PU SNR (Fig. 5a). This is because at low PU SNR values there are not enough non-malicious users with good channels from the PU. 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 PU, leading to severe performance degradation in case of Method II. However, as seen from Fig. 5c, 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 PU SNR values.

In Fig. 6, we consider the performance of malicious user detection techniques using spatial information for the system considered in Fig 2a 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 PU 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 PU 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 choice of A would depend on the propagation environment of PU signal.

In Fig. 7, we analyze the performance of Method IIa when $D_\delta = \{1, 2, 3, 4\}$ for the system considered in Fig. 2a. In Fig. 7a, we consider 'Always Yes' malicious user and in Fig. 7b, we consider a smart malicious user that avoids sending false sensing values during the iterations when there is change in the PU state. Same K_m^δ value is used for each δ and is denoted by K_m in Fig. 7a and Fig. 7b. We see 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.

VIII. Conclusion

In this paper, we have proposed malicious user detection schemes based on outlier-detection techniques for a CR cooperative sensing system. A parallel fusion sensing network was considered in which all sensors send their 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 various robust methods to assign outlier factors to the users during each sensing iteration. Malicious user detection schemes using these outliers factors are then proposed to identify malicious users and reduce their impact on the performance of the sensing system. We focused on identifying the malicious users which decrease the CR throughput by sending false high energy values when the PU is absent. Several important constraints imposed by the CR scenario have been taken into consideration. The proposed malicious user detection schemes do not require feedback from the PU network or knowledge of the additive noise variance and the location of the primary transmitter. Assuming partial knowledge of the PU activity, we proposed a novel method to improve the performance of the malicious user detection scheme. 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 PU and various sensors, we proposed improved malicious user detection schemes in which spatial 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. In the future, we will consider malicious-user detection techniques for CR cooperative sensing systems when the data sent to the access point by the sensors is quantized.

REFERENCES

[1] Spectrum Policy Task Force report, technical report 02-135, Federal Communications Commission, Nov. 2002.

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

[3] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among CRs," in *Proc. IEEE International Conf. Commun. (ICC'06)*, vol. 4, pp. 1658-1663, June 2006.

[4] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proc. IEEE Conf. Dynamic Spectrum Access Netw. (DYSPAN'05)*, pp. 131-136, Nov. 2005.

[5] G. Ganesan and Y. Li, "Cooperative spectrum sensing in CR networks," in *Proc. IEEE Conf. Dynamic Spectrum Access Netw. (DYSPAN'05)*, pp. 137-143, Nov. 2005.

[6] R. Chen, J.-M. Park, and J. Reed, "Defense against PU emulation attacks in CR networks," *IEEE J. Sel. Areas Commun.*, vol. 26, pp. 2537, Jan. 2008.

[7] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *IEEE International Conf. Commun. (ICC'08)*, pp. 3406-3410, May 2008.

[8] D. Hawkins, *Identification of Outliers*. London: Chapman and Hall, 1980.

[9] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, pp. 523-531, Apr. 1967.

[10] F. Mostseller and J. W. Tukey, *Data Analysis and Regression: A Second Course in Statistics*. Reading, MA: Addison-Wesley.

[11] G. E. P. Box and D. R. Cox, "An analysis of transformations," *J. Stat. Soc.*, B28, pp. 211-252, 1964.

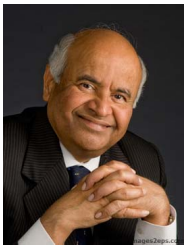
[12] D. A. Lax, "Robust estimators of scale: finite-sample performance in long-tailed symmetric distributions," *J. American Statistical Association*, vol. 80, no. 391, pp. 736-741, Sep. 1985.

[13] M. Hubert and E. Vandervieren, "An adjusted boxplot for skewed distributions," *Comput. Stat. Data Anal.*, vol. 52, pp. 5186-5201, 2008.

[14] G. Brys, M. Hubert, and A. Struyf, "A comparison of some new measures of skewness," *Developments Robust Statistics (ICORS 2001)*, pp. 98-113.

Praveen Kaligineedi received his Bachelor of Technology (B.Tech.) degree in Electrical Engineering from the Indian Institute of Technology (IIT), Kanpur, India, in May 2004 and M.A.Sc degree from University of British Columbia (UBC), Canada in November 2006. He is now pursuing a Ph.D. degree in Electrical and Computer Engineering at UBC, Canada. His current research interests are in the areas of cooperative communications and cognitive radio.

Majid Khabbazian received his B.Sc. degree in computer engineering from Sharif University of Technology, Tehran, Iran, in 2002, and his Ph.D. degree in electrical and computer engineering from the University of British Columbia, Vancouver, British Columbia, Canada, in 2008. He is currently a postdoctoral fellow at MIT Computer Science and Artificial Intelligence Lab. His research interest include wireless networks, network security and distributed algorithms.



Vijay K. Bhargava (S'70, M'74, SM'82, F'92) received the B.Sc., M.Sc., and Ph.D. degrees from QueenŠs University, Kingston, ON, Canada in 1970, 1972 and 1974 respectively. Currently, he is a Professor in the Department of Electrical and Computer Engineering at the University of British Columbia, Vancouver, Canada. Previously he was with the University of Victoria (1984-2003) and with Concordia University in Montreal (1976-1984). He is a co-author of the book *Digital Communications by Satellite* (New York: Wiley, 1981), co-editor of *Reed-Solomon Codes and Their Applications* (New York: IEEE, 1994) and co-editor of *Communications, Information and Network Security* (Boston: Kluwer, 2003). His research interests are in wireless communications.

Dr. Bhargava is a Fellow of the Engineering Institute of Canada (EIC), the IEEE, the Canadian Academy of Engineering and the Royal Society of Canada. He is a recipient of the IEEE Centennial Medal (1984), IEEE CanadaŠs McNaughton Gold Medal (1995), the IEEE Haraden Pratt Award (1999), the IEEE Third Millennium Medal (2000), IEEE Graduate Teaching Award (2002), and the Eadie Medal of the Royal Society of Canada (2004).

Dr. Bhargava is very active in the IEEE and has served on the Board of Governors of the IEEE Information Theory Society and the IEEE Communications Society. He served as Editor-in-Chief for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS during 2007, 2008 and 2009. In 2010, he was appointed for a two year term as the IEEE Communications Society Director of Journals. He is a Past President of the IEEE Information theory Society.