Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 4316029, 8 pages
https://doi.org/10.1155/2017/4316029

WILEY | Hindawi

Research Article

Performance of p-Norm Detector in Cognitive Radio Networks with Cooperative Spectrum Sensing in Presence of Malicious Users

Nandita Lavanis[1] and Devendra Jalihal[2]

[1]*Department of ECE, SSN College of Engineering, Chennai, India*
[2]*EE Department, Indian Institute of Technology, Madras, India*

Correspondence should be addressed to Nandita Lavanis; nandital@hotmail.com

Received 26 July 2016; Revised 5 October 2016; Accepted 18 October 2016; Published 12 January 2017

Academic Editor: Gonzalo Vazquez-Vilar

A cognitive radio network (CRN) with a cooperative spectrum sensing scheme is considered. This CRN has a primary user and multiple secondary users, some of which are malicious secondary users (MSUs). Energy detection at each SU is performed using a p-norm detector with $p \geq 2$, where $p = 2$ corresponds to the standard energy detector. The MSUs are capable of perpetrating spectrum sensing data falsification (SSDF) attacks. At the fusion center (FC), an algorithm is used to suppress these MSUs which could be either an adaptive weighing algorithm or one of the following: Tietjen-Moore (TM) test or Peirce's criterion. This is followed by computation of a test statistic (TS) which is a random variable. In this paper, we assume TS to have either a Gamma or a Gaussian distribution and calculate the threshold accordingly. We provide closed-form expressions of probability of false alarm and probability of miss-detection under both assumptions. We show that Gaussian assumption of TS is more suited in presence of an SSDF attack when compared with the Gamma assumption. We also compare the detection performance for various values of p and show that $p = 3$ along with the Gaussian assumption is the best amongst all the cases considered.

1. Introduction

The increase in demand for high-data-rate communication over wireless channels has fueled research in many possible directions. Some of these include developing spectrally efficient modulation schemes, channel codes that approach capacity, and many such techniques. In this context, one of the prime areas of research is cognitive radio, which enables efficient use of wireless spectrum [1]. Wireless spectrum is a scare resource, and a study carried out in the United States revealed the inefficient utilization of this resource [2]. The scanning of spectrum brought into light the following observations: some bands of the spectrum were completely unoccupied and some other bands were used only sparingly, while some were heavily occupied. Spectrum holes are those frequencies in the spectrum, which have been allocated to a user, but are not in use at that point in time-frequency and geographic area [3]. For a superior utilization of the spectrum, it was proposed that users can be permitted to use spectrum holes. The user who is allocated the spectrum is the licensed user and also known as the primary user (PU), whereas the user, who uses the spectrum when PU is not using it, is known as a secondary user (SU). SU employs cognition at the receiver in order to detect the PU and adapts its parameters accordingly. Hence, SU acts as a cognitive radio (CR) which is aware of its environment.

The presence of a PU and several SUs forms a cognitive radio network (CRN). In a network of cognitive radios, it is obvious that the detection of PU can be made more reliable by providing cooperation amongst SUs. This is cooperative spectrum sensing (CSS) approach [4]. There are various types of cooperative sensing methods like centralized, distributed, and relay-assisted cooperative spectrum sensing. Centralized cooperative spectrum sensing consists of a fusion center (FC), which gathers information from all the SUs and makes a hypothesis on the presence or absence of PU.

The objectives of a cognitive radio are efficient use of spectrum along with highly reliable communication. To meet

these objectives, the CR must sense the spectrum to find opportunities. The CR can employ various signal processing techniques such as feature detection, energy detection (ED), and cyclostationary approach to detect the PU [5].

Though cooperative sensing performed by several users has the advantage of providing a more reliable decision about the PU, there is also the disadvantage of presence of malicious secondary users (MSUs). In the spectrum sensing process, an MSU can alter the cooperative decision by transmitting false signal leading to incorrect decision of presence of PU. Such attacks are known as spectrum sensing data falsification (SSDF) attacks [6], leading to Byzantine failure.

Various types of SSDF attacks are analyzed for a CR network (CRN) in the literature which include selfish SSDF, interference SSDF, and confusing SSDF [6]. The first type of attack is the selfish SSDF or "always yes" attack. In this attack, an MSU continuously transmits a signal indicating that PU is present and then uses the spectrum without letting other SUs to use it. In an interference SSDF or "always no" attack, an MSU continuously transmits a low energy signal indicating the absence of a PU. In this case, other SUs start using the spectrum and cause interference to the PU when the PU is on. Similarly, in case of a confusing SSDF attack, the MSU confuses other SUs by indicating the presence or absence of PU with certain probability.

Malicious user detection is addressed in [7] in which the authors use outlier-detection schemes. These schemes assign outlier factors to SUs using biweight and biweight scale method which are recursive methods to suppress the outliers. The performance is compared using plots of additional probability of false alarm versus additional probability of miss-detection. In [8], Grubb's methods I and II along with Dixon's test are analyzed, for "always yes" SSDF attack in order to remove MSUs. The authors have shown that Dixon's test performs better for removal a single MSU; however, it cannot remove more than one MSU. The analysis is performed by plotting the receiver operating characteristics (ROC). In [9], removal of multiple outliers is addressed using Tietjen-Moore (TM) test [10] and Shapiro-Wilk (SW) test. The TM test is an extension of Grubb's test for multiple outlier detection. In [11], the authors address removal of MSUs using a weighted adaptive algorithm in which weights are assigned to all the SUs and iteratively updated. It shown that this algorithm performs better than the one in [7].

An improved energy detector (IED) or a p-norm detector for cognitive radios is proposed in [12] and it is shown to perform better than the standard ED for various values of p. The test statistic (TS) is the summation of pth power of received values and the probability density function (pdf) of the TS is approximated as Gamma pdf. p-norm detector is used in CRN in the following papers: [13] analyzes the performance of diversity systems and provides closed-form expressions; in [14], performance of CSS is analyzed with p-norm detector and optimal number of SUs is found out; in [15], the authors have combined p-norm detector with another improved energy detector and analyzed the performance on generalized κ-ν fading channel.

In this paper, a CRN with interweave mode of operation is considered in the presence of some SUs and MSUs. In the interweave mode of operation, the SU opportunistically uses the spectrum by detecting spectrum holes. The IEEE 802.22 standard [16] proposes the use of cognitive radios for rural broadband wireless access, and the PHY layer is based on OFDM/OFDMA. Since OFDM splits the entire spectrum into narrow band channels, each of which can be considered additive white Gaussian noise channel (AWGN), this paper assumes AWGN channel model.

The scenario considered is as follows: a cognitive radio network is considered which has one PU, some SUs, and MSUs. The number of MSUs is assumed a small percentage of the total number of SUs. This CRN employs CSS. All the SUs and MSUs sense the channel and transmit their quantized energy values to the FC. These energy values are pth power of the received signal, where p is an arbitrary positive constant. At FC, one of the following algorithms is executed to suppress the MSUs: (1) TM test, (2) Peirce's criterion, and (3) adaptive weighing. After the removal of MSU data from the received energy values, the energy values are summed to form a global test statistic (TS). This global TS is compared with the threshold to make a decision on the PU. The following assumptions are made: (i) at FC, the energy values from SUs are combined to form a global TS which forms a random variable; (ii) the global TS is assumed to have either a Gamma or a Gaussian distribution and the threshold is calculated accordingly. The Gamma assumption of global TS follows [12].

In this paper, a unified performance analysis of MSU detection schemes is provided. Following is the summary: (i) closed expressions of probability of false alarm and probability of miss-detection are provided for MSU removal scheme which uses p-norm detector using assumption of Gamma pdf of TS. (ii) It is observed that, in an SSDF attack, the Gaussian assumption suits the system better than the Gamma assumption. This is so since the p-norm detector improves the performance of most of schemes while using the Gaussian assumption for TS, whereas use of Gamma assumption for TS does not improve performance of the p-norm detector. (iii) In the entire set of observations, it is seen that TM test performs equally well as the adaptive weighing algorithm, whereas Peirce's criterion performs worse than both of these for suppression of multiple malicious users.

The paper is organized as follows. Section 2 describes the system model of CRN. In Section 3, the algorithms for MSU suppression are described. Section 4 describes the observations and results and Section 5 provides the conclusions.

2. System Model

A CRN with a PU, N SUs, and an FC is considered. N SUs cooperate amongst each other. It is assumed that, out of N SUs, M users are malicious where $N \gg$ M. All SUs sense the presence of PU based on the received signal at SU and send their quantized estimates of signal energy to the FC through error-free control channels. The FC takes a decision on whether the primary is present or not based on these received signal values. The channels between PU and SU are assumed to be AWGN. The presence or absence of a PU is

a hypothesis testing problem. Hypothesis $\mathcal{H}_0$ corresponds to the absence of PU, whereas hypothesis or outcome $\mathcal{H}_1$ corresponds to the presence of PU.

2.1. Processing at SU. The corresponding signals at any SU are given as follows:

$$\begin{aligned} &\mathcal{H}_0\colon\ y_i(t) = n_i(t), \quad i = 1, \ldots, N; \\ &\mathcal{H}_1\colon\ y_i(t) = s_i(t) + n_i(t), \quad i = 1, \ldots, N. \end{aligned} \tag{1}$$

In (1), $y_i(t)$ is the received signal at each SU. $n_i(t)$ is additive white Gaussian noise (AWGN) with zero mean and variance σ_n^2. In the absence of the primary signal, only noise is received. $s_i(t)$ is the PU signal which is assumed to be Gaussian with zero mean and variance σ_s^2. Hence, the average signal-to-noise ratio is $\text{snr} = \sigma_s^2/\sigma_n^2$. At each of the SU after sampling the signal, L samples are used to estimate the PU signal. This forms the local TS using a p-norm detector. At ith SU, the local TS is formed in the following way:

$$W_i = \sum_{k=0}^{L-1} \left(\frac{|y_i(k)|}{\sigma_n} \right)^p. \tag{2}$$

In (2), p is an arbitrary positive constant [12]. It should be noted that $p = 2$ corresponds to the standard ED.

2.2. Processing at FC. At the FC, the quantized energy values from all SUs first filtered using an algorithm for MSU suppression and then are combined using either equal gain combining (EGC) or weighted combining to create a global TS. The global TS is described in the next section. In case of a standard ED, the statistics of W_i in (2) are computed in [17] as normal distribution. However, in the case of a p-norm detector, the pdf of W_i is approximate. In [12], this pdf is approximated by a Gamma distribution whose mean and variance are computed. When $L \gg 1$, CLT assumption can be invoked and the Gaussian distribution is used to approximate this pdf in [13].

In this paper, we assume W_i to be a Gamma random variable whose mean and variance are given by the following [12]:

$$\begin{aligned} &\mathcal{H}_0\colon\ \mu_0 = L\frac{2^{p/2}}{\sqrt{\pi}}\Gamma\left(\frac{p+1}{2}\right); \\ &\mathcal{H}_0\colon\ \sigma_0^2 = L\frac{2^p\Gamma\left(p+1/2\right)}{\sqrt{(\pi)}} - L\frac{2^p}{\pi}\Gamma^2\left(\frac{p+1}{2}\right), \end{aligned} \tag{3}$$

under $\mathcal{H}_0$ and

$$\begin{aligned} &\mathcal{H}_1\colon\ \mu_1 = L\frac{2^{p/2}}{\sqrt{\pi}}\Gamma\left(\frac{p+1}{2}\right)\left(\sqrt{1+\text{snr}}\right)^p; \\ &\mathcal{H}_1\colon\ \sigma_1^2 \\ &\quad = L\frac{(2+2\text{snr})^p}{\sqrt{(\pi)}}\left(\Gamma\left(p+\frac{1}{2}\right) - \frac{\Gamma^2\left((p+1)/2\right)}{\sqrt{\pi}}\right), \end{aligned} \tag{4}$$

under $\mathcal{H}_1$. In (3) and (4), snr is the average SNR.

2.3. Related Definitions. The local TS in (2) is compared with threshold λ in order to detect the presence of PU. The important metrics for any hypothesis testing problem are

$$P_f = \Pr\left(\mathcal{H}_1 \mid \mathcal{H}_0\right) = \Pr\left(W_i > \lambda \mid \mathcal{H}_0\right), \tag{5}$$

$$P_m = \Pr\left(\mathcal{H}_0 \mid \mathcal{H}_1\right) = \Pr\left(W_i < \lambda \mid \mathcal{H}_1\right), \tag{6}$$

$$P_d = \Pr\left(\mathcal{H}_1 \mid \mathcal{H}_1\right) = \Pr\left(W_i > \lambda \mid \mathcal{H}_1\right). \tag{7}$$

In (5), the probability of false alarm (P_f) is defined, whereas (6) defines probability of miss-detection (P_m). Probability of detection (P_d) is defined by (7).

3. Algorithms for MSU Suppression

At the FC, algorithms for MSU suppression fall into the category of nonadaptive and adaptive algorithms, some of which are described below.

3.1. Nonadaptive Algorithms. In this case, at FC, all of the SSDF attacks are considered as an outlier-detection problem, since the energy of the MSU is extremely higher/lower than that of the SU as assumed in [6–8]. Outlier detection is also a hypothesis testing problem where the null hypothesis is absence of any outlier and the alternative hypothesis is the presence of one or more outliers. Two algorithms are considered, namely, Peirce's criterion and the TM test which are described below.

3.1.1. Peirce's Criterion. Peirce's criterion [18] has been used to eliminate the outlier data and does not make any assumptions on significance level as in other tests. The decision is taken based on the number of MSUs and total number of users. To eliminate the outlier values for data set $W_1, W_2, \ldots, W_N$, the following operations are performed. Initially, the mean and standard deviation of the data set are calculated. R represents ratio maximum allowable deviation of a measured value from data mean value to the standard deviation. Hence, $R = |W_i - W_m|_{\max}/\sigma$, where W_m is mean of data. R is obtained from a table provided by Peirce [18] assuming a single doubtful observation (or assuming a single outlier initially, though there can be more). Following this, maximum allowable deviation $|W_i - W_m|_{\max} = \sigma R$ is calculated. For any suspicious data, $|W_i - W_m|$ is obtained. A measurement is eliminated if $|W_i - W_m| > |W_i - W_m|_{\max}$. The above steps are repeated assuming two outliers, assuming original mean, standard deviation, and number of measurements. The calculations are repeated by increasing the number of outliers, until no more data measurements need to be eliminated.

3.1.2. TM Test. TM test was proposed by Tietjen and Moore in [10] and it is an iterative implementation of Grubb's test. It consists of two Grubb-type statistics: one to address removal of upper and lower outliers and the other to address removal of bidirectional outliers. Consider data set $W_1, W_2, \ldots, W_N$ and order it according to increasing values. Assuming that the

number of outliers in the data set is estimated and denoted by q, the first statistic for calculating upper outliers is given by

$$L_{q,u} = \frac{\sum_{i=1}^{N-q} \left(W_i - \overline{W}_q\right)^2}{\sum_{i=1}^{N} \left(W_i - \overline{W}\right)^2}, \tag{8}$$

where $\overline{W}_q = \sum_{i=1}^{N-q} W_i/(N-q)$ and $\overline{W}$ is the mean of the full sample. Similarly, the TS for calculating lower outliers is

$$L_{q,l} = \frac{\sum_{i=q+1}^{N} \left(W_i - \overline{W^*}_q\right)^2}{\sum_{i=1}^{N} \left(W_i - \overline{W}\right)^2}, \tag{9}$$

where $\overline{W^*}_q = \sum_{i=q+1}^{N} W_i/(N-q)$. For a prefixed significance value, the critical value (CV) is obtained from the table in [10]. If $L_{q,u} < \text{CV}$, q data values are upper outliers and are eliminated from the data set. Similarly, if $L_{q,l} < \text{CV}$, q data values are lower outliers and are eliminated from the data set. Hence, a single test is needed to eliminate all outliers simultaneously without the need of repetition.

3.1.3. Global Test Statistic. The global TS at FC for the nonadaptive algorithms is formed by using EGC in the following manner:

$$\widetilde{Z} = \frac{1}{N}\sum_{i=1}^{N} W_i, \tag{10}$$

where W_i is defined in (2).

3.2. Adaptive Algorithms

3.2.1. Adaptive Weighing Algorithm Using Standard ED. A particular algorithm [11] is considered in which MSU suppression is addressed by assigning an adaptive weight to each of the SU. The algorithm is described here. The local TS used,

$$W_{i,wc} = \sum_{k=0}^{L-1} \left(\left|y_i(k)\right|\right)^2, \tag{11}$$

calculated at each SU, has a central Chi-square distribution under $\mathcal{H}_0$ and noncentral Chi-square pdf under $\mathcal{H}_1$. The mean and variance of this local TS are given in [17]. The weighted or global TS is given by

$$\widetilde{Z}_k = \frac{1}{N}\sum_{i=1}^{N} w_{k,i} W_{k,i,wc}. \tag{12}$$

In (12), k denotes iteration index and $w_{k,i}$ denotes the weight applied to each of the SU and $W_{k,i,wc}$ is given in (11). Hypothesis testing is performed by comparing $\widetilde{Z}_k$ with threshold $\lambda_{0,wc}$. Each weight is $w_{k,i} = \rho(C_{k,i})$, where ρ is monotonically decreasing function and assumed as a raised cosine function. Initial value of $C_{k,i}$ is set to 0 and it increases to unity for MSUs as the algorithm proceeds, indicating a loss of credibility. Accordingly, the weight is calculated using ρ function. At FC, $\widetilde{Z}_k$ is assumed to have a Gaussian pdf. The mean and variance of $\widetilde{Z}_k$ depend on the weighing factors. Closed-form expression for threshold and probability of false alarm and probability of miss-detection are provided in [11] which are given below:

$$\lambda_{0,wc} = \sigma_n^2\left(\sqrt{\frac{2L}{N}}Q^{-1}\left(P_{f,wc}\right) + L\right), \tag{13}$$

$$P_{f,wc}\left(\lambda_{0,wc}\right) = Q\left(\frac{\left(\lambda_{0,wc} - \mu_{0,wc}\right)W_p}{\sigma_{0,wc}}\right), \tag{14}$$

$$P_{m,wc}\left(\lambda_{0,wc}\right) = 1 - Q\left(\frac{\left(\lambda_{0,wc} - \mu_{1,wc}\right)W_p}{\sigma_{1,wc}}\right). \tag{15}$$

In (14), W_p is the factor arising out of weighted combining. $\mu_{0,wc}$ and $\sigma_{0,wc}$ are mean and variance of the Gaussian random variable (r.v.) $W_{k,i,wc}$. These are expressed as follows:

$$\begin{aligned} \mathcal{H}_0&\colon \mu_{0,wc} = L\sigma_n^2; \\ \mathcal{H}_0&\colon \sigma_{0,wc}^2 = 2L\sigma_n^4, \end{aligned} \tag{16}$$

under $\mathcal{H}_0$ and

$$\begin{aligned} \mathcal{H}_1&\colon \mu_{1,wc} = L\sigma_n^2\left(1 + \text{snr}\right); \\ \mathcal{H}_1&\colon \sigma_{1,wc}^2 = 2L\sigma_n^4\left(1 + 2\text{snr}\right), \end{aligned} \tag{17}$$

under $\mathcal{H}_1$ [11].

3.2.2. Adaptive Weighing Algorithm Using p-Norm Detector

(A) Gamma Assumption of the Global Test Statistic. p-norm detector in (2) is used along the adaptive weighing scheme in order to perform the suppression of MSUs. As described in the system model, the quantized data sent by each SU to FC is modeled as Gamma r.v. with mean and variance in (3) and (4). The effect of quantization is neglected for computing mean and variance. In case of the adaptive weighing scheme, this data is weighted using the combining scheme and the global TS is

$$\widetilde{Z}_k = \frac{1}{N}\sum_{i=1}^{N} w_{k,i} W_{k,i}. \tag{18}$$

It is shown, in [11], that weights $w_{k,i}$ converge to unity for all the honest SUs and converge to zero for MSUs. Hence, EGC assumption can be used. Apart from that, we also assume that all energy values are i.i.d Gamma r.v.s. The independence assumption is justified since the sources of energy are independent. Hence, using result of Moschopoulos [19], we conclude that $\widetilde{Z}_k$, for $N \gg M$, has a Gamma pdf whose mean and variance are given by

$$\begin{aligned} \mathcal{H}_0&\colon \mu_{p,0} = NL\frac{2^{p/2}}{\sqrt{\pi}}\Gamma\left(\frac{p+1}{2}\right); \\ \mathcal{H}_0&\colon \sigma_{p,0}^2 = NL\frac{2^p}{\sqrt{\pi}}\left(\Gamma\left(p + \frac{1}{2}\right) - \frac{1}{\sqrt{\pi}}\Gamma^2\left(\frac{p+1}{2}\right)\right), \end{aligned} \tag{19}$$

under $\mathscr{H}_0$ and

$$\mathscr{H}_1\colon \mu_{p,1} = NL\frac{2^{p/2}}{\sqrt{\pi}}\Gamma\left(\frac{p+1}{2}\right)\left(\sqrt{1+\text{snr}}\right)^p;$$

$$\mathscr{H}_1\colon \sigma^2_{p,1} = \frac{NL\,(2+2\text{snr})^p}{\sqrt{\pi}}\left(\Gamma\left(p+\frac{1}{2}\right)-\frac{1}{\sqrt{\pi}}\Gamma^2\left(\frac{p+1}{2}\right)\right), \tag{20}$$

under $\mathscr{H}_1$. In this case, assuming the threshold as λ_{01}, P_f in (5) is expressed as

$$P_f = \Pr\left(\widetilde{Z}_k > \lambda_{01} \mid H_0\right) = \Gamma\left(\frac{NL\Gamma^2\left((p+1)/2\right)}{\Gamma\left((2p+1)/2\right)\sqrt{\pi}-\Gamma^2\left((p+1)/2\right)}, \frac{\lambda_{01}L\sqrt{\pi}\Gamma\left((p+1)/2\right)}{2^{p/2}\left(\sqrt{\pi}\Gamma\left((2p+1)/2\right)-\Gamma^2\left((p+1)/2\right)\right)}\right). \tag{21}$$

In (21), $\Gamma(a, x)$ is the upper incomplete Gamma function [20]. The proof of (21) is provided in Appendix. The threshold from (21) is

$$\lambda_{01} = \frac{2^{p/2}\left(\sqrt{\pi}\Gamma\left((2p+1)/2\right)-\Gamma^2\left((p+1)/2\right)\right)}{L\sqrt{\pi}\Gamma\left((p+1)/2\right)}\cdot\Gamma^{-1}\left(P_f\right), \tag{22}$$

where P_f is a fixed value decided by the system requirement.

Similarly, the probability of miss-detection defined in (6) is given by

$$P_m = 1-\Pr\left(\widetilde{Z}_k > \lambda_{01} \mid H_1\right) = 1-\Gamma\left(\frac{NL\Gamma^2\left((p+1)/2\right)}{\Gamma\left((2p+1)/2\right)\sqrt{\pi}-\Gamma^2\left((p+1)/2\right)}, \frac{\lambda_{01}L\sqrt{\pi}\Gamma\left((p+1)/2\right)}{2^{p/2}\left(1+\text{snr}\right)^{p/2}\left(\sqrt{\pi}\Gamma\left((2p+1)/2\right)-\Gamma^2\left((p+1)/2\right)\right)}\right). \tag{23}$$

The proof of (23) is provided in Appendix.

(B) Gaussian Assumption of the Global Test Statistic. To derive the corresponding λ_0, P_f, and P_m under the Gaussian assumption of global TS, (3) and (4) are substituted in (13), (14), and (15), respectively. The corresponding expressions for threshold, probability of false alarm, probability of miss-detection are

$$\lambda_0 = \frac{1}{\sqrt{\pi}}\left(L\Gamma\left(\frac{1+p}{2}\right)+Q^{-1}\left(P_f\right)\sqrt{\frac{L\Gamma\left(p+1/2\right)}{N}}\right),$$
$$P_f = Q\left(\frac{\lambda_0 - NL\left(2^{p/2}/\sqrt{\pi}\right)\Gamma\left((p+1)/2\right)}{\sqrt{NL\left(2^p/\sqrt{\pi}\right)\left(\Gamma\left(p+1/2\right)-\left(1/\sqrt{\pi}\right)\Gamma^2\left((p+1)/2\right)\right)}}\right), \tag{24}$$
$$P_m = 1-Q\left(\frac{\left(\lambda_0 - NL\left(2^{p/2}/\sqrt{\pi}\right)\Gamma\left((p+1)/2\right)\left(\sqrt{1+\text{snr}}\right)^p\right)\sqrt{N}}{\sqrt{\left(NL\,(2+2\text{snr})^p/\sqrt{\pi}\right)\left(\Gamma\left(p+1/2\right)-\left(1/\sqrt{\pi}\right)\Gamma^2\left((p+1)/2\right)\right)}}\right).$$

4. Observations and Discussion

Monte Carlo simulations are performed for a CRN using CSS considering $N = 40$ SUs and $M = 3$ malicious users. A random input signal with BPSK modulation is considered and an "always yes" attack is assumed. The average SNR (snr) varies in the range −16 to −4 dB. The number of samples used for detection is fixed to $L = 40$. The probability of false alarm is fixed to $P_f = 0.01$ for some of the simulations. The data sent by SUs to FC is quantized to 8 bits. For various simulations, the value of p is considered in the range $2 \le p \le 6$, where $p = 2$ corresponds to the standard ED. Though [12] does not provide any maximum value p, in the simulations in [12], maximum of $p = 10$ is used. Further, the Monte Carlo simulations are compared with theoretical results which are derived in (21) and (23).

Figure 1 shows the plot of SNR versus P_m with a Gaussian assumption of global TS and using a standard ED as well as IED with a fixed $P_f = 0.01$. For any p, it is observed that the TM test and the adaptive weighing method of MSU suppression perform better and are almost close to the theoretical P_m in [11], whereas Peirce's criterion performs slightly worse than the adaptive weighing and TM test. Hence, with Gaussian pdf assumption, the p-norm detector performs better with respect to a standard ED.

Figure 2 shows the comparative performance of SNR versus P_m for a CRN with 3 MSUs with $p = 2, 3$ and fixed $P_f = 0.01$ using Gamma assumption for of global TS. Similar to the Gaussian assumption, in this case too, the TM test and adaptive method perform close to theoretical P_m derived in (23). For the adaptive weighing algorithm as well as statistical tests, the corresponding plots for $p = 2$ lie below that of $p = 3$ indicating that, in case of Gamma pdf assumption of global TS, standard ED performs better than p-norm detector. This can be attributed to the fact that the input energy values of the FC consists of certain outliers making the Gaussian

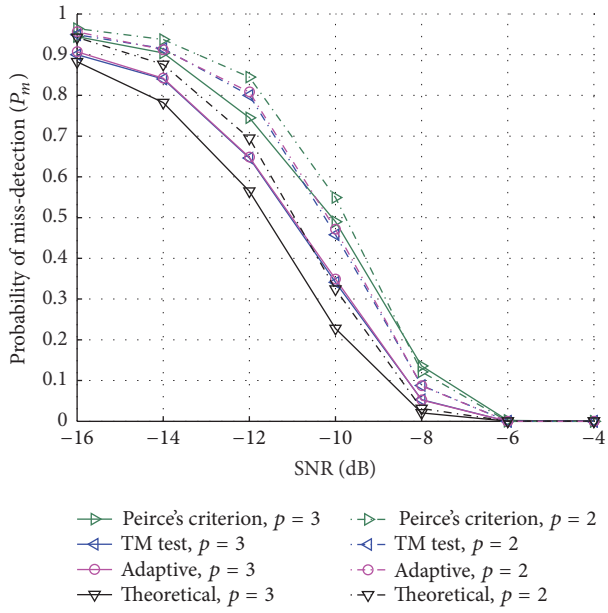

FIGURE 1: Probability of miss-detection (P_m) versus SNR for $M = 3$. $p = 2, 3$ with fixed probability of false alarm (P_f) = 0.01 and Gaussian assumption of pdf of global TS.

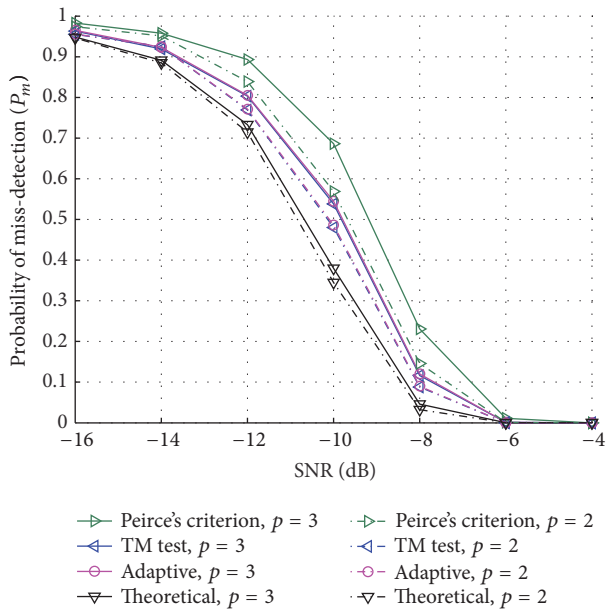

FIGURE 2: Probability of miss-detection (P_m) versus SNR for $M = 3$. $p = 2$ and 3 with fixed probability of false alarm (P_f) = 0.01 and Gamma assumption of pdf of global TS.

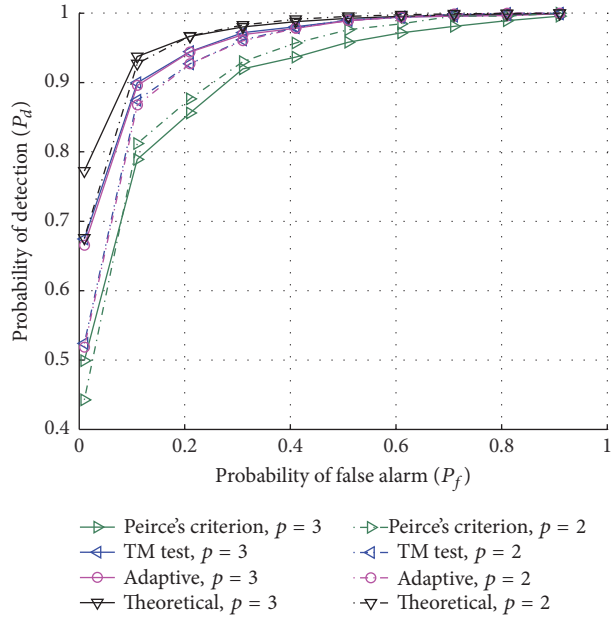

FIGURE 3: ROC at snr = −10 dB for $M = 3$, $p = 2$, and $p = 3$ with Gaussian pdf assumption of global TS.

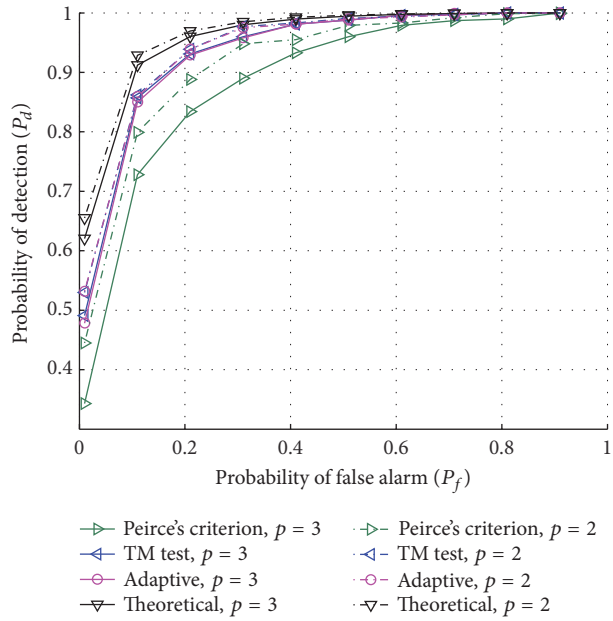

FIGURE 4: ROC at snr = −10 dB for $M = 3$, $p = 2$, and $p = 3$ with Gamma pdf assumption of global TS.

assumption of global TS more appropriate than the Gamma assumption.

An ROC is a plot of P_m versus P_d and indicates the performance of any detection scheme. An ROC curve of any good detection scheme should lie above $x = y$ line. Figure 3 plots the ROC of a standard and p-norm detector assuming $M = 3$ and an average SNR of snr = −10 dB under Gaussian pdf assumption of global TS. It is observed that, under the Gaussian assumption, p-norm detector performs better when compared with standard ED for most cases. The TM test and adaptive method perform well and are close to the theoretical curve. The standard ED performs better for Peirce's criterion with Gaussian assumption.

Figure 4 plots the ROC curve for the same parameters as before and with a Gamma pdf assumption of global TS. However, with the Gamma assumption, it is observed that

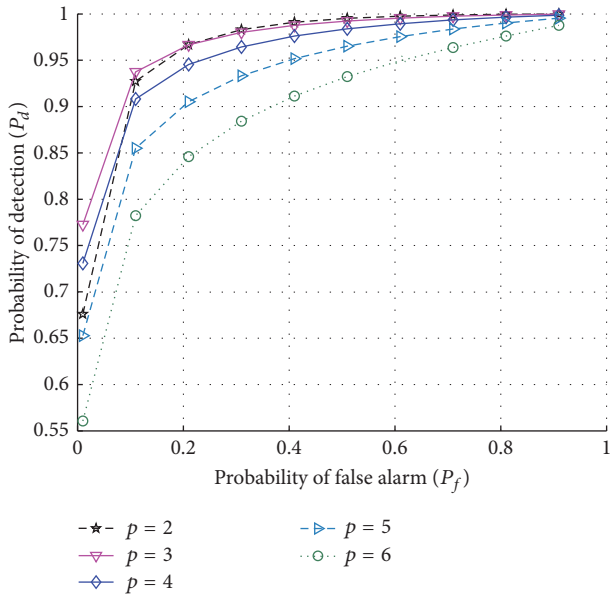

FIGURE 5: ROC for $M = 3$, $p = 2, 3, 4, 5$, and $p = 6$ using Gaussian assumption of global TS for theoretical case.

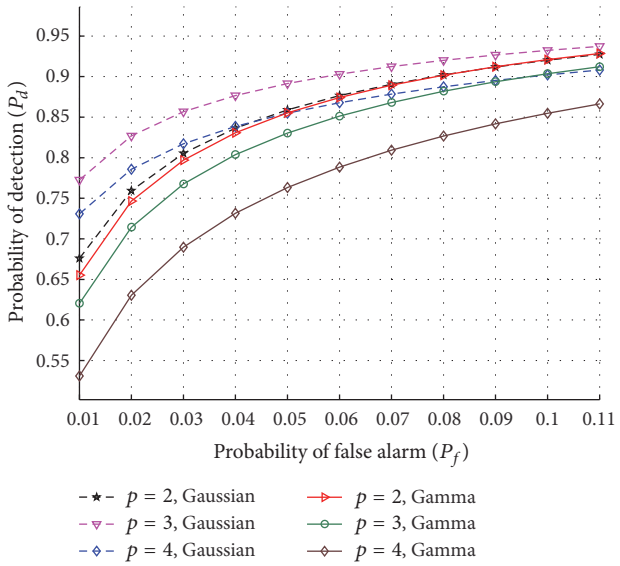

FIGURE 6: ROC for $M = 3$, $p = 2, 3$, and $p = 4$ for theoretical case and $P_f \leq 0.11$.

standard ED performs better than p-norm detector ($p = 3$) for all the algorithms except for the Peirce's criterion.

It is observed that when the Gaussian assumption is used for the global TS, the performance of the system improves as p increases from two to three, whereas, for $p > 3$, the performance of the system starts reducing. This is also observed from Figure 5 in which $p = 2$ to 6 are considered. It is seen that the maximum value of p for which P_d is maximized is $p = 3$. It should be noted that $p = 2$ corresponds to a standard ED.

Figure 6 plots the ROC curves for the Gamma and Gaussian pdf assumption of global TS using the theoretical formula for low values of probability of false alarm, that is, for $P_f \leq 0.11$ which are to be used in practice [21]. The IEEE 802.22 standards have given the sensing requirements on P_f and P_d which are $P_f \leq 0.1$ and $P_d \geq 0.9$ [21]. It is observed that p-norm detector gives a better probability of detection only when the Gaussian assumption of global TS is invoked for computation of threshold. If Gamma distribution is assumed in the threshold computation, then the standard energy detector performs better. Similarly, using Gaussian assumption of global TS, $p = 3$ gives the best performance for practical values of P_f.

5. Conclusion

In this paper, a CRN with CSS was considered which consisted of multiple malicious users capable of perpetrating SSDF attacks. In such a scenario, the problem of malicious user suppression was dealt with. Either of these algorithms, namely, Peirce's criterion or the TM test or an adaptive weighing algorithm, was used for the malicious user suppression which was preceded by either a standard or p-norm ED. Closed-form expressions of probability of false alarm and probability of miss-detection for the adaptive weighing algorithm with a p-norm detector were computed under the assumption of a Gamma or Gaussian distribution of the test statistic. Performance comparison of these algorithms indicated that the Gaussian assumption for distribution of test statistic suited this setup as compared to the Gamma assumption in presence of an SSDF attack. Assuming a Gaussian distribution of test statistic, the performance improved as p is increased from two to three but degraded for higher values of p. From the observations, we concluded that $p = 3$ with Gaussian assumption of the TS provided the best performance when various values of p were considered. In the entire set of observations, it was seen that TM test performs equally well as the adaptive weighing algorithm for suppression of multiple malicious users, whereas Peirce's criterion could not meet up with the performance.

Appendix

Proof for Probability of False Alarm

The pdf and cumulative distribution function (CDF) of a Gamma random variable X_i with the following parameters, shape k and scale θ, is given by [19]

$$f_{X_i}(x_i) = \frac{x_i^{k-1} e^{-x_i/\theta}}{\Gamma(k)\,\theta^k}, \tag{A.1}$$

$$F_{X_i}(x) = \frac{\gamma(k, x/\theta)}{\Gamma(k)}. \tag{A.2}$$

The mean and variance of X_i, respectively, are

$$E[X_i] = k\theta,$$
$$\mathrm{Var}(X_i) = k\theta^2. \tag{A.3}$$

The definition of probability of false alarm from (5) is considered. Since $\widetilde{Z}_k$ is a sum of N random variables which have Gamma distribution, the pdf of $\widetilde{Z}_k$ is also Gamma according to [19]. The mean and variance of $\widetilde{Z}_k$ from (19) are considered. Hence, under $\mathscr{H}_0$, the shape and scale parameters for $\widetilde{Z}_k$ are

$$k_0 = \frac{NL\Gamma^2\left(\left(p+1\right)/2\right)}{\left[\sqrt{\pi}\Gamma\left(\left(2p+1\right)/2\right) - \Gamma^2\left(\left(p+1\right)/2\right)\right]},$$
$$\theta_0 = \frac{2^{p/2}}{L\sqrt{\pi}}\left(\frac{\sqrt{\pi}\Gamma\left(\left(2p+1\right)/2\right) - \Gamma^2\left(\left(p+1\right)/2\right)}{\Gamma\left(\left(p+1\right)/2\right)}\right). \tag{A.4}$$

Using (A.4) in (A.2), we obtain the probability of false alarm in (21).

Similarly, the probability of miss-detection can be obtained by using the definition in (6). The corresponding mean and variance of $\widetilde{Z}_k$ under $\mathscr{H}_1$ are given by (20). Hence, under $\mathscr{H}_1$, the shape and scale parameters for $\widetilde{Z}_k$ are

$$k_1 = \frac{NL\Gamma^2\left(\left(p+1\right)/2\right)}{\left[\sqrt{\pi}\Gamma\left(\left(2p+1\right)/2\right) - \Gamma^2\left(\left(p+1\right)/2\right)\right]},$$
$$\theta_1 = \frac{\left(2+2\mathrm{snr}\right)^{p/2}}{L\sqrt{\pi}}\left(\frac{\sqrt{\pi}\Gamma\left(\left(2p+1\right)/2\right) - \Gamma^2\left(\left(p+1\right)/2\right)}{\Gamma\left(\left(p+1\right)/2\right)}\right). \tag{A.5}$$

Using (A.5) in (A.2), we obtain the probability of false alarm in (23).

Competing Interests

The authors declare that they have no competing interests.

References

[1] J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[2] M. McHenry and D. McCloskey, "New York city spectrum occupancy measurements september 2004," Shared Spectrum Company, 2004, http://www.sharedspectrum.com/.

[3] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.

[4] K. B. Letaief and W. Zhang, "Cooperative communications for cognitive radio networks," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 878–893, 2009.

[5] S. Haykin, D. J. Thomson, and J. H. Reed, "Spectrum sensing for cognitive radio," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 849–877, 2009.

[6] F. Richard 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 *Proceedings of the 2009 IEEE Military Communications Conference (MILCOM '09)*, pp. 1–7, Boston, Mass, USA, October 2009.

[7] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2488–2497, 2010.

[8] S. S. Kalamkar, A. Banerjee, and A. Roychowdhury, "Malicious user suppression for cooperative spectrum sensing in cognitive radio networks using Dixon's outlier detection method," in *Proceedings of the 18th National Conference on Communications (NCC '12)*, pp. 1–5, Kharagpur, India, February 2012.

[9] S. S. Kalamkar, P. K. Singh, and A. Banerjee, "Block outlier methods for malicious user detection in cooperative spectrum sensing," in *Proceedings of the 79th IEEE Vehicular Technology Conference (VTC '14)*, Seoul, South Korea, May 2014.

[10] G. L. Tietjen and R. H. Moore, "Some Grubbs-type statistics for the detection of several outliers," *Technometrics*, vol. 14, no. 3, pp. 583–597, 1972.

[11] T. Zhao and Y. Zhao, "A new cooperative detection technique with malicious user suppression," in *Proceedings of the IEEE International Conference on Communications (ICC '09)*, pp. 2754–2758, 2009.

[12] Y. Chen, "Improved energy detector for random signals in gaussian noise," *IEEE Transactions on Wireless Communications*, vol. 9, no. 2, pp. 558–563, 2010.

[13] V. R. Sharma Banjade, C. Tellambura, and H. Jiang, "Performance of p-norm detector in AWGN, fading, and diversity reception," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 7, pp. 3209–3222, 2014.

[14] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Cooperative spectrum sensing in multiple antenna based cognitive radio network using an improved energy detector," *IEEE Communications Letters*, vol. 16, no. 1, pp. 64–67, 2012.

[15] M. Jain, V. Kumar, R. Gangopadhyay, and S. Debnath, "Improved p-norm energy detector in Generalized κ-μ fading channel for spectrum sensing in cognitive radio," in *Proceedings of the 2nd International Conference on Communications, Signal Processing, and their Applications (ICCSPA '15)*, pp. 1–4, IEEE, Sharjah, The United Arab Emirates, 2015.

[16] C. R. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. J. Shellhammer, and W. Caldwell, "IEEE 802.22: the first cognitive radio wireless regional area network standard," *IEEE Communications Magazine*, vol. 47, no. 1, pp. 130–138, 2009.

[17] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE Journal on Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 28–40, 2008.

[18] S. M. Ross, "Peirce's criterion for the elimination of suspect experimental data," *Journal of Engineering Technology*, vol. 20, no. 2, pp. 38–41, 2003.

[19] P. G. Moschopoulos, "The distribution of the sum of independent gamma random variables," *Annals of the Institute of Statistical Mathematics*, vol. 37, no. 3, pp. 541–544, 1985.

[20] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*, vol. 55, Courier Corporation, North Chelmsford, Mass, USA, 1964.

[21] S. J. Shellhammer, "Spectrum sensing in IEEE 802.22," in *Proceedings of the IAPR Workshop on Cognitive Information Processing*, pp. 9–10, 2008.