Hindawi
International Journal of Antennas and Propagation
Volume 2018, Article ID 2346317, 11 pages
https://doi.org/10.1155/2018/2346317

Research Article

Defense against Malicious Users in Cooperative Spectrum Sensing Using Genetic Algorithm

Noor Gul[1,2] **Ijaz Mansoor Qureshi**,[3] **Atif Elahi**,[1] **and Imtiaz Rasool**[2]

[1]*Department of Electrical Engineering, Faculty of Engineering and Technology, International Islamic University, Islamabad 44000, Pakistan*
[2]*Department of Electronics, University of Peshawar, Peshawar 25000, Pakistan*
[3]*Department of Electrical Engineering, Air University, Islamabad 44000, Pakistan*

Correspondence should be addressed to Noor Gul; noor.phdee51@iiu.edu.pk

Received 4 August 2017; Accepted 18 October 2017; Published 24 January 2018

Academic Editor: Ana Alejos

In cognitive radio network (CRN), secondary users (SUs) try to sense and utilize the vacant spectrum of the legitimate primary user (PU) in an efficient manner. The process of cooperation among SUs makes the sensing more authentic with minimum disturbance to the PU in achieving maximum utilization of the vacant spectrum. One problem in cooperative spectrum sensing (CSS) is the occurrence of malicious users (MUs) sending false data to the fusion center (FC). In this paper, the FC takes a global decision based on the hard binary decisions received from all SUs. Genetic algorithm (GA) using one-to-many neighbor distance along with z-score as a fitness function is used for the identification of accurate sensing information in the presence of MUs. The proposed scheme is able to avoid the effect of MUs in CSS without identification of MUs. Four types of abnormal SUs, opposite malicious user (OMU), random opposite malicious user (ROMU), always yes malicious user (AYMU), and always no malicious user (ANMU), are discussed in this paper. Simulation results show that the proposed hard fusion scheme has surpassed the existing hard fusion scheme, equal gain combination (EGC), and maximum gain combination (MGC) schemes by employing GA.

1. Introduction

A spectrum demand is on its rise due to new applications and wireless devices. The federal communication commission (FCC) survey shows that most of the licensed radio frequency spectrum is underutilized, temporally and spatially. Cognitive radio network (CRN) is a way for secondary users (SUs) to exploit the spectrum holes of the primary user (PU) for better utilization [1]. In CRN, SUs utilize the spectral holes in the PU spectrum without causing any disturbances to the PUs and have to vacate the channel for the PU when it is transmitting [2, 3]. The PU status is determined by adopting various detection schemes such as the generalized likelihood ratio test detector, matched filter detector, feature detector, and energy detector. Energy detectors are computationally less complex in comparison with all other detectors, which measure the received signal energy and compare the result with a preselected constant to take decision of the PU spectrum. The low signal-to-noise ratio (SNR) environment of the fading channel and noise uncertainty drastically reduces the performance of energy detector and it is, therefore, difficult to get reliable spectrum decisions with them [4, 5].

The effects of fading, shadowing, and receiver uncertainty problems make the sensing information provided by a single SU unsatisfactory and unreliable [6, 7]. The strong fading or shadowing effects lead to some correlated observations to be under the threshold of the conventional energy detector, which degrades the detection probability. An innovative test is proposed in [8] for the case of correlated observations, in order to improve the detection performance. In centralized cooperative spectrum sensing (CSS), all SUs perform individual spectrum sensing and share this information with the FC. A global decision of the PU channel is made at FC by combining the data received from all cooperative SUs [9–12]. The aim of CSS is to increase the probability of PU detection, while keeping the probability of false alarm minimum [13]. A malicious user (MU) in CSS

misdirects other SUs about the availability of the PU spectrum and may stop them from using the vacant channel resulting in an increased false alarm in the system. Similarly, MUs provide an incorrect look about the spectrum availability, while it is already in use by the PU which reduces overall detection probability of the system. The detection of unfair user using a novel method is proposed in [14], in which the unfair user hides its radio signal under the noise floor in the presence of an active primary user or SU for a constant false alarm rates. An innovative technique for the detection of orthogonal frequency division multiplexing- (OFDM-) based PU signal is proposed under the constant false alarm rate (CFAR) in [15]. CSS is investigated as an efficient detection method in the presence of primary user emulation attack in [16]. Priority values are assigned to SUs based on reputation results of each SU in [17–20] to give less importance to the sensing results of SUs with a reputation below threshold. A reputation-based CSS method is proposed in [21] that improves the system performance by detecting and rejecting the Byzantine malicious users, in order to improve system performance and efficiency. Block outlier is used as a detection method for MUs in [22]. Statistical features utilized by MUs in attack where they perform malicious acts with certain probability are discussed in [23], and an abnormality-based approach, a powerful technique in the field of data mining for the detection of MUs, is proposed in [24, 25]. An energy harvest-based weighted CSS for jointly optimizing the number of cooperative SUs and sensing time is in [26].

There are some soft decision fusion (SDF) schemes, such as equal gain combination soft decision fusion (EGC-SDF) and maximum gain combination soft decision fusion (MGC-SDF) in which SUs forward all energy statistics to the FC [27]. MGC-SDF is the optimal choice; however, this scheme requires information between the SU and the PU, which is difficult to get in practice. The MGC-SDF is also sensitive to the attack of MUs sending false data to the FC [28–30]. The CSS protection scheme, discussed in [31], is used for the detection of the always yes and always no MUs, where outlier detection technique is used. Kullback-Leibler divergence-based CSS is proposed in [32] to protect the CSS from the spectrum sensing data falsification (SSDF) attack [33] of the always yes and always no MUs and work fine in case of a large number of MUs. In the hard decision fusion (HDF) as in [8, 34–36], SUs send a hard binary decision of the PU channel to the FC. These hard decisions are fused together by the FC in counting and voting rules in [37].

Genetic algorithm (GA) is a class of computational algorithms which is motivated by evolution, pioneered by John Holland in 1974 [38]. GA can be utilized to find optimized solutions to examine problems through the application of biologically inspired methods [38–40]. Holland referred to the chromosomes as strings of binary symbols encoding a candidate solution to the given problem. Wireless networks make use of the GA due to its well-known and remarkable generality and versatility and have been applied in a wide variety of settings in wireless communication networks [40]. The work in [41, 42] focuses on the optimization of probability of detection and false alarm in CRN to minimize probability of error of a particular SU in a centralized CRN with GA.

In this paper, we investigate GA-based CSS to defend against SSDF attack of MUs to reduce the probability of misdetection and false alarm, which results in an overall reduction in the probability of errors. The study in [39] is based on the combination of double-sided neighbor distance (DSND) algorithm-based GA, where MUs are first identified using DSND and then GA is used for the selection of the best spectrum sensing results at the end of the given number of iterations. The best selected results of the GA in [39] are followed by the majority voting hard decision (MV-HDF) to take a global decision of the PU spectrum. Unlike [39], this proposed method required no additional steps for the identification of MUs using the DSND algorithm. Cooperative SUs including both normal SUs (NSUs) and MUs report to the FC by their single-bit hard binary decisions. The FC utilizes the one-to-many hamming distances and z-score as a composite outlier score and fitness function of the GA. Out of the total outlier scores, the sensing information with the minimum total outlying value is selected as the best sensing reports on behalf of all cooperative SUs for a global decision at the FC. The MV-HDF scheme then decides globally about the actual status of the PU. In comparison with [39], this work optimizes the detection, false alarm, and error results when MUs take low and high SNR of the channel in comparison with NSUs. The proposed scheme is tested at different levels of SNR and increasing number of cooperative users with simple soft decision fusion (SDF) and hard decision fusion (HDF) schemes in [28–36]. Simulation results at different levels of cooperative SUs and various SNR levels confirmed that with the use of the one-to-many neighbor distance- and z-score-based GA, the system is able to produce more sophisticated detection results for the HDF schemes in the presence of MUs. The proposed GA-based MV-HDF (GAMV-HDF) is able to beat simple equal gain combination soft decision fusion (EGC-SDF), maximum gain combination soft decision fusion (MGC-SDF), and simple majority voting hard decision fusion (MV-HDF) schemes during PU channel recognition by keeping the error probability low with high detection and low false alarm results at different rates of cooperative SUs and SNR levels.

In this paper, the proposed method outcomes are verified and tested against the existence of an opposite malicious user (OMU), random opposite malicious user (ROMU), always yes malicious user (AYMU), and always no malicious user (ANMU) [32, 39]. An AYMU provides a high-energy signal to the FC irrespective of the actual PU spectrum status, thus increasing false alarm probability and reducing throughput for the SUs. The ANMU provides an all-time availability of the licensed user channel and, therefore, results in both the misdetection probability and increasing interference to the PU transmission. Similarly, the OMU always negates the actual condition of the PU. The OMU results in false alarm, misdetection probability, reduction of bandwidth, and increase in interference to the PU. The malicious nature of the ROMU is unpredictable and difficult to eliminate because they perform malicious acts probabilistically. The ROMU

operates as an OMU with probability p and appears as a NSU with probability $1 - p$.

The rest of the paper is organized as follows. Section 2 presents the system model. Section 3 addresses how GA is used to overcome the effects of MUs. Experimental results are presented in Section 4. Section 5 concludes the paper.

2. System Model

All SUs report to the FC about the channel condition of the PU if it is free or occupied. SUs, including both normal and malicious, decide locally to report a hard binary decision "1" for the PU channel occupancy and "0" for the vacant channel. Based on the received spectrum reports of all SUs, the FC identifies and creates a global decision about the availability of the PU channel.

SUs as in Figure 1 try to detect the PU channel with no information about the location, structure, and signal strength of the PU. Energy detection due to its simplicity follows the optimum spectrum sensing method in this scenario.

The spectrum sensing operation of each SU in a particular spectrum results in deciding hypotheses H_1 and H_0 as [18, 32, 39]

$$x_j(n) = \begin{cases} H_0, w_j(n) \\ H_1, h_j e(n) + w_j(n) \end{cases}, \quad (1)$$

where hypothesis H_1 represents occupancy of the channel by the PU and hypothesis H_0 is about the availability of the PU channel. $x_j(n)$ is the received signal by the jth user in the nth time slot. $e(n)$ is the transmitted signal of the PU in the nth time slot. This received signal is distorted by the channel gain h_j between the PU and jth SU, which is assumed to be constant during detection interval. The signal $e(n)$ at the nth observation slot is further corrupted by the zero mean additive white Gaussian noise (AWGN) $w_j(n)$. Without lossing generality, $e(n)$ and $w_j(n)$ are assumed to be independent of each other. In this paper, energy detection is applied at each SU. The observed signal energy of the PU channel by the jth SU user at the ith sensing interval is as follows:

$$Z_j(i) = \begin{cases} \sum_{n=n_i}^{n_i+M-1} |w_j(n)|^2, & H_0 \\ \sum_{n=n_i}^{n_i+M-1} |h_j e(n) + w_j(n)|^2, & H_1 \end{cases}, \quad (2)$$

where, $Z_j(i)$ is the sum of the squares of M Gaussian random variables in the ith sensing interval. According to the central limit theorem (CLT), if the number of samples is large enough, $Z_j(i)$ is asymptotically normally distributed under both H_0 and H_1 hypotheses [18, 32] as

$$Z_j(i) = \begin{cases} N(\mu_0 = M, \sigma_0^2 = 2M), & H_0 \\ N\left(\mu_1 = M\left(\beta_j + 1\right), \sigma_1^2 = 2M\left(\beta_j + 1\right)\right), & H_1 \end{cases}, \quad (3)$$

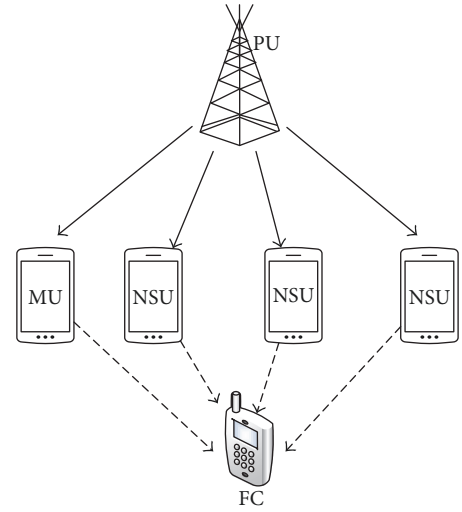

Figure 1: The conventional CSS mechanism.

where β_j is the SNR ratio between the PU and the jth SU. Similarly, (μ_0, σ_0^2) and (μ_1, σ_1^2) are the means and variances of the energy under H_0 and H_1 hypotheses.

3. Proposed GA-Based Methodologies

The proposed cooperative spectrum sensing model is shown in Figure 2. SUs sense the licensed channel and take a local decision to forward either H_1 or H_0 decision to the FC. The role of the FC is divided into two parts. First, it collects local spectral observations from all SUs and applies GA using one-to-many hamming distance along with z-score as a total outlier factor for determining the fitness of all sensing reports. The final sensing selection is made for the sensing report with minimal total outlier score results at the end of desired iterations. In the second part, it uses the MV-HDF scheme to declare the final status of the PU channel based on the selection results of the GA.

A Pseudocode 1 of the proposed method is shown below.

3.1. Local Spectrum Decisions. SUs take its local decision by comparing the observed energy of the PU channel with a threshold in order to send a hard decision "1" or "0" to the FC using the control channel between the SU and the FC as

$$y_j(i) = \begin{cases} 1, & Z_j(i) \geq \delta_j \\ 0, & \text{otherwise} \end{cases}, \quad (4)$$

where $Z_j(i)$ is the received energy in the ith sensing interval by the jth SU and δ_j is the threshold value for the jth SU. If the energy of the receiving signal by the jth SU is greater than the threshold, then it declares PU existence by forwarding a binary decision "1" to the FC; otherwise, decision "0" is forwarded to the FC to state the channel as free of the incumbent authorized user.

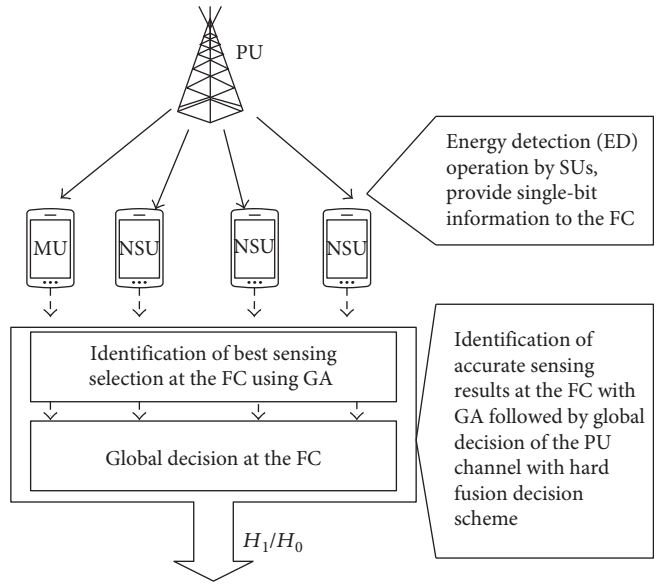

Figure 2: The proposed CSS mechanism.

```
for k = 1 to sensing limit
  for i = 1 to iterations
    for j = 1 to total SUs
      if Z_j(i) > threshold
 y_j(i) = 1 hard decision "1"
      else
 y_j(i) = 0 hard decision "0"
      end
    end
    for j = 1 to total SUs
      m_ij = {(Σ_{j=1}^{S} y_ij) − y_ij/S − 1}
      o_j^1(i) = |y_ij − m_ij|, i ∈ 1, .., N, j ∈ 1, ... , S
      o_j^2(i) = |(y_ij − μ(i))/σ(i)|, i ∈ 1, ... , N, j ∈ 1, ... , S
    end
   o_i^1 = Σ_{j=1}^{S} (o_j^1(i)), i ∈ 1, ... , N
   o_i^2 = Σ_{j=1}^{S} (o_j^2(i)), i ∈ 1, ... , N
     f(i) = (o_i^1 + o_i^2)
     Crossover the new population
     Randomly mutation of the least fit
 end iterations
 best sensing sample y_j(b) out of Y
 if Σ_{j=1}^{S} y_j(b) ≥ K
   global decision G_B(i) = H_1
 else
   global decision G_B(i) = H_0
 end
end sensing limit
```

Pseudocode 1

The detection probability $P_{d,j}$ of the jth SU based on the present hypothesis H_1 of the PU channel is as follows:

$$P_{d,j} = P\left\{y_j(i) = 1|H_1\right\} = P\left\{Z_j(i) \geq \delta_j|H_1\right\}. \quad (5)$$

Similarly, the false alarm probability due to the jth SU decision based on the absence hypothesis H_0 is as follows:

$$P_{f,j} = P\left\{y_j(i) = 1|H_0\right\} = P\left\{Z_j(i) \geq \delta_j|H_0\right\}. \quad (6)$$

Likewise, the probability of detection, false alarm, and misdetection over the AWGN channel can be expressed [34] as follows:

$$\begin{aligned} P_{d,j} &= Q_k\left(\sqrt{2\beta_j}, \sqrt{\delta_j}\right), \\ P_{f,j} &= \frac{\Gamma\left(M, \delta_j/2\right)}{\Gamma(M)}, \\ P_{m,j} &= 1 - P_{d,j}, \end{aligned} \quad (7)$$

where β_j is the SNR between the jth SU and the PU. $M = TW$ is the time bandwidth product representing total samples in each sensing period. $Q_K(.,.)$ is the generalized Marcum Q-function, and $\Gamma(.)$ and $\Gamma(.,.)$ are the complete and incomplete gamma functions, respectively [36].

After taking hard binary decisions made by S, as in (4) for N intervals, the FC collects the local spectrum sensing decision of individual SUs and generates a reporting matrix as below:

$$\mathbf{Y} = \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1S} \\ y_{21} & y_{22} & \cdots & y_{2S} \\ \vdots & \vdots & \ddots & \vdots \\ y_{N1} & y_{N2} & \cdots & y_{NS} \end{bmatrix}, \quad (8)$$

where $\mathbf{Y}$ is a population matrix of size $N \times S$ containing the hard binary decisions at the FC by S in the N sensing reports of the PU channel. The population is built for both the NSUs and MUs. Furthermore, GA is used as a tool for minimizing the spectrum sensing data falsification effects of MU and any imperfections by the NSU in the following section.

3.2. Best Sensing Report Selection Using Genetic Algorithm (GA). In receiving all the sensing information of SUs during each sensing interval as above, the FC further utilizes GA for determining the best sensing results out of the local decision reports provided by individual SUs for taking out a global decision.

The FC determines absolute differences of the sensing results of the jth SU with the average sensing energy provided by all other SUs based on the result in (8). The average of all SU decisions is calculated by neglecting the jth SU result in the ith sensing interval to find out the impact of not including this particular user in the collective sensing result. A similar procedure is followed for the reports of all S users in the N sensing interval as

$$\mathbf{A} = \begin{bmatrix} m_{11} & m_{12} & \dots & m_{1S} \\ m_{21} & m_{22} & \dots & m_{2S} \\ \vdots & \vdots & \ddots & \vdots \\ m_{N1} & m_{N2} & \dots & m_{NS} \end{bmatrix}, \tag{9}$$

where

$$m_{ij} = \left\{ \frac{\left(\sum_{j=1}^{S} y_{ij}\right) - y_{ij}}{S-1} \right\}. \tag{10}$$

In (10), S is the total number of SUs and N is the total number of sensing reports made by S reporting users. m_{ij} is the average value of energy reports of all other SUs in the it h sensing interval while keeping away the sensing results of the jth SU out of the average measurement. The PU spectrum reports of the MUs are different from the NSUs; therefore, taking MUs out in the m_{ij} during each sensing interval is generating dissimilar averaging results for the OMU, ROMU, AYMU, and ANMU compared with NSUs.

3.2.1. Outlying Using One-to-Many Sensing Distance. To figure out how much the individual sensing results of each SU "y" are behaving differently from the average sensing results "m" of all other users, outlying factors are determined for the sensing reports of SUs based on the one-to-many sensing distances $\mathbf{o}_j^1(i)$ for the jth user in the ith sensing interval as

$$\mathbf{o}_j^1(i) = \left| y_{ij} - m_{ij} \right|, \quad i \in 1, \dots, N, \quad j \in 1, \dots, S. \tag{11}$$

Based on the results in (11), the outlier scores $\mathbf{o}_j^1(i)$ of the NSUs and MUs are added to discover the total one-to-many hamming distance score under each sensing interval as

$$\mathbf{o}_i^1 = \sum_{j=1}^{s} \left(\mathbf{o}_j^1(i) \right), \quad j \in 1, \dots, S, \tag{12}$$

where, $\mathbf{o}_i^1$ is the total outlier score representing the absolute sum of the hamming distances of the one individual SU detection y_{ij} with the many average detection m_{ij} of all other SUs in the ith sensing interval.

The calculations in (12) are made for all the N intervals and results are collected as

$$\mathbf{o}^1 = \begin{bmatrix} \mathbf{o}_1^1 & \mathbf{o}_2^1 & \dots & \mathbf{o}_N^1 \end{bmatrix}^T. \tag{13}$$

where $\mathbf{o}^1$ is the outlier score result for all the N sensing intervals. This score is a measurement of how far the report of each SU is from the average sensing reports provided by all other SUs by seperating those sensing intervals during which MU and NSU imperfections were misguiding the FC's final decision about the PU channel.

3.2.2. Outlying Using z-Score. Similarly, the other outlier score measurement for each user report is made with the help of the z-score measurement in comparison with that for the sensing report received from each SU as

$$\mathbf{o}_j^2(i) = \left| \frac{\left(y_{ij} - \mu(i) \right)}{\sigma(i)} \right|, \quad i \in 1, \dots, N, \quad j \in 1, \dots, S, \tag{14}$$

where $u(i) = \sum_{j=1}^{S} (y_{ij}/S)$ is the mean value of the sensing reports of all S users in the ith sensing interval. $\sigma(i) = \sqrt{\sum_{j=1}^{S} (y_{ij} - \mu(i))^2 / S}$ is the standard deviation of the ith interval reports, and $\mathbf{o}_j^2(i)$ is the z-score outlying of the jth user report in the ith interval of the historical formation.

The result for $\mathbf{o}_j^2(i)$ in (14) shows how much local sensing observation of the jth user is detached away from the group observations provided by all other users using z-score.

Now, to guarantee the authenticity of each of the ith reports, the sum of the z-score results for all intervals is made as follows:

$$\mathbf{o}_i^2 = \sum_{j=1}^{S} \left(\mathbf{o}_j^2(i) \right), \quad i \in 1, \dots, N. \tag{15}$$

The total $\mathbf{o}^2$ score results for all N sensing reports are collected as follows:

$$\mathbf{o}^2 = \begin{bmatrix} \mathbf{o}_1^2 & \mathbf{o}_2^2 & \dots & \mathbf{o}_N^2 \end{bmatrix}^T. \tag{16}$$

As fitness function is the representation for the suitability of each sensing reports, the final selection of the fitness of each sensing reports from both the NSU and MU reports is determined. The best selection results having less abnormal behavior on behalf of the NSU and MU users are calculated.

To select the best sensing reports received from the normal users and MUs, *fitness function* is calculated based on the result in (12) and (15) as

$$\mathbf{f}(i) = \left(\mathbf{o}_i^1 + \mathbf{o}_i^2 \right). \tag{17}$$

The result of (17) is able to make clear separation between reports under the predominant impact of MU and NSU malfunctioning, from the one containing less effect of these abnormalities. The fit chromosomes in (17) are allowed to pass through heredity, while the

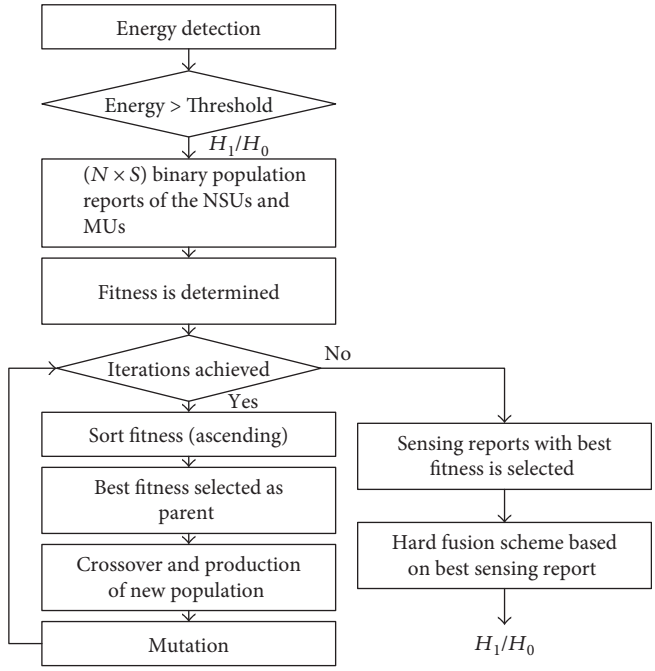

Figure 3: Proposed CSS flowchart.

unhealthy chromosomes with higher abnormalities decreased due to the natural phenomenon of the survival of the fittest.

The sensing results in **Y** with the minimum total outlier score in (17) are selected as the best chromosome and considered to be accurate sensing information on behalf of the NSU and MUs. Based on the fitness results as in (17), the top chromosomes are selected as the parent chromosomes and crossover operations are done among the rest to determine new offspring.

The crossover procedure is basically an effort to exploit the best behaviors of the current chromosomes and to mix them in a bid to increase their appropriateness. This operator randomly selects a locus and exchanges the subsequences before and after that locus between two parent chromosomes to build a pair of children. A crossover point is randomly selected here in this work.

The fittest chromosomes are more likely to be passed on to the next generation. The population is then sorted in ascending order of fitness values.

The process of mutation represents a random change in the bit values of the gene. The mutation operation is performed on the sensing information of the least fit chromosome. Genome bits of the least fit chromosome are inverted after random selection.

After a random mutation of genome bits and crossover operation, a new population matrix **Y** is obtained and the same procedure as in (11) to (16) is repeated for the determination of best fitness which results in new values of the fitness function as in (17). After achieving the iteration criteria, the sensing reports with the minimum total outlier in (17) are used to select the best sensing sample of the **Y** population in (8) for a global decision.

A flowchart representing the detailed operation of the proposed scheme from local binary decisions by the SUs followed by the data collection at the FC and GA operation for identifying and selecting the best sensing reports on behalf of NSUs and MUs is presented in Figure 3.

3.3. Counting Rule as Hard Decision Rule at the FC. After selecting of best sensing reports $y_j(b)$ in **Y** with a minimal outlier value in (17), FC applies one of the hard fusion combination schemes to take a global decision of the primary user status. The three most commonly used hard fusion schemes applied by the FC are the voting rule (majority decision here), OR rule, and AND rule.

The voting rule decides about the PU activity based on the voting of K SU decision out of the total cooperative users S. If K out of S decides that a signal is present, then the FC takes a global decision H_1. Here, S is the total number of cooperative SUs and K is the count of how many of the SUs have reported PU signal presence. The count $K = S/2$ is selected as a special case of the voting rule called the majority decision rule. Similarly, in the majority voting decision, if the PU detection reports are less than K, then, the FC takes the global decision as H_0

$$G_B(i) = \left\{ \begin{array}{ll} H_1: & \sum_{j=1}^{S} y_j(b) \geq K \\ H_0: & \text{otherwise} \end{array} \right\}. \tag{18}$$

While applying the AND rule by the FC, all the M SUs has to provide a unanimous decision of the PU detection; then, the FC declares the channel as occupied by the PU and generates a global decision H_1, representing the PU signal; otherwise, decision H_0 is made by the FC as

$$G_B(i) = \left\{ \begin{array}{ll} H_1: & \sum_{j=1}^{S} y_j(b) = S \\ H_0: & \text{otherwise} \end{array} \right\}. \quad (19)$$

In following the OR rule procedure by the FC during each sensing interval, if at least one of the SUs provides local detection information to the FC, then FC decides a global decision H_1; otherwise, decision is made in favour of H_0.

$$G_B(i) = \left\{ \begin{array}{ll} H_1: & \sum_{j=1}^{S} y_j(b) \geq 1 \\ H_0: & \text{otherwise} \end{array} \right\}. \quad (20)$$

The results of the cooperative detection and false alarm probability for the voting rule based on the local detection of all the S SUs are demarcated at the FC as

$$\begin{aligned} P_{\mathrm{d}} &= \Pr\{G_B(i) = 1 | H_1\} = \Pr\left\{ \sum_{j=1}^{S} y_j(b) \geq K | H_1 \right\}, \\ P_{\mathrm{f}} &= \Pr\{G_B(i) = 1 | H_0\} = \Pr\left\{ \sum_{j=1}^{S} y_j(b) \geq K | H_0 \right\}. \end{aligned} \quad (21)$$

Here, the FC declares a global decision as $G_B(i) = 1$ of the PU status if K out of S is reporting in favour of H_1. The majority voting decision is taken as a special case of the voting rule with $K = S/2$. Both the OR and AND rules are also special cases of the voting rule with $K = 1$ for the OR category and $K = S$ for the AND category of the hard fusion combination schemes.

Similarly, the results of the cooperative detection and false alarm probabilities for the OR and AND rules are as given below:

$$\begin{aligned} P_{\mathrm{d\_OR}} &= 1 - \prod_{j=1}^{S} \left(1 - P_{\mathrm{d},j}\right), \\ P_{\mathrm{f\_OR}} &= 1 - \prod_{j=1}^{S} \left(1 - P_{\mathrm{f},j}\right), \\ P_{\mathrm{d\_AND}} &= \prod_{j=1}^{S} \left(P_{\mathrm{d},j}\right), \\ P_{\mathrm{f\_AND}} &= \prod_{j=1}^{S} \left(P_{\mathrm{f},j}\right), \end{aligned} \quad (22)$$

where $P_{\mathrm{d\_OR}}$ and $P_{\mathrm{f\_OR}}$ are the cooperative spectrum detection and false alarm probabilities, respectively, while applying the OR rule, while $P_{\mathrm{d\_AND}}$ and $P_{\mathrm{f\_AND}}$ are the detection and false alarm results, respectively, when the AND hard fusion scheme is applied.

4. Simulation Results

For the simulation, cognitive radio network parameters are set with S including NSUs, MUs, and FC. Out of S, 4 users are selected as AYMU, ANMU, OMU, and ROMU natures of MUs. Performance of the proposed and other schemes is tested under various simulation conditions. At first, the total number of cooperating SUs is taken as 12 at different average SNR values (−9.5 dB, −13.5 dB, and −15.5 dB). In this study, MUs were observed under low and higher SNR values compared with NSUs. In the second part, the simulation is done for the proposed and all other schemes at different ratios of cooperative SUs with 8, 12, and 16. The sensing time is taken as 1 *ms* and the number of samples M in each sensing interval is 270. The total number of sensing iterations is taken as 1000. The sensing intervals during which ROMU performs a malicious act are selected randomly from 1 to 1000. The crossover points for the GA are randomly selected from 1 to S. The crossover operation in the chromosomes and the production of new offspring is observed for 10 cycles. MUs are equally distributed as OMU, ROMU, AYMU, and ANMU. The GA population consists of $N = 10$ chromosomes with S in each chromosome. The GA population represents the sensing information of S in the N trials.

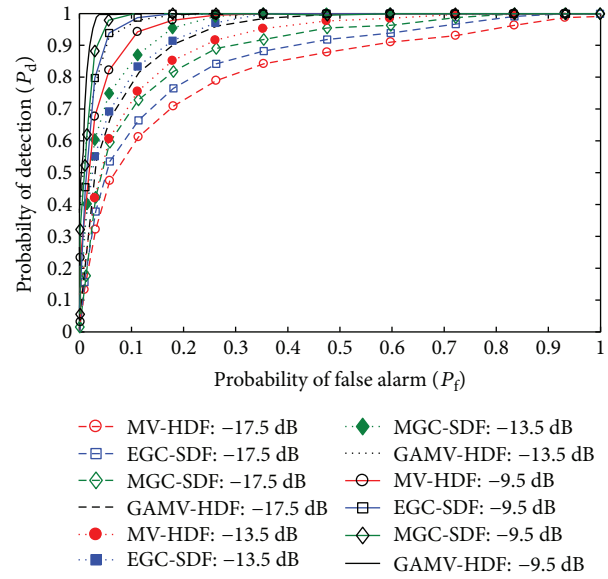

Figure 4: Probability of detection versus probability of false alarm (ROC) at different SNR values with MUs having low SNR compared with NSUs.

The simulation results collected in Figures 4–7 show the ROC curves for the GAMV-HDF, MV-HDF, EGC-SDF, and MGC-SDF schemes. The results in Figures 4 and 5 show that as the average SNR increases from −17.5 dB to −9.5 dB, the ROC curves of all fusion schemes are enhanced. In Figure 4, the total number of cooperating SUs is fixed as 12 and simulation is done for the proposed GAMV-HDF, MV-HDF, EGC-SDF, and MGC-SDF at different average SNR values. In this part of the simulation, MUs are observed with low SNR values compared with normal cooperating SUs. The results show that the proposed scheme has better ROC results at all average SNR values. This is followed by the MGC-SDF, EGC-SDF, and simple MV-HDF schemes. Unlike Figure 4, the outcomes in Figure 5 illustrate that the ROC results against different average SNR values for a total of 12 cooperative SUs with malicious behavior changed for the abnormal SUs. In this part, MUs are taking higher SNR

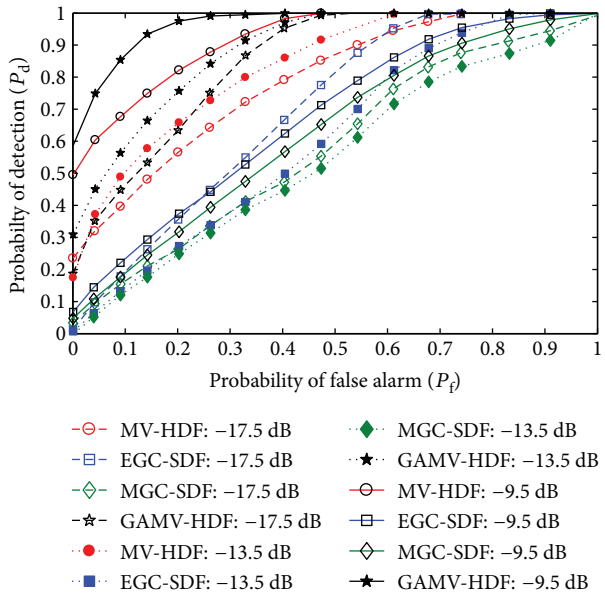

Figure 5: Probability of detection versus probability of false alarm at different SNR values with MUs having high SNR compared with NSUs.

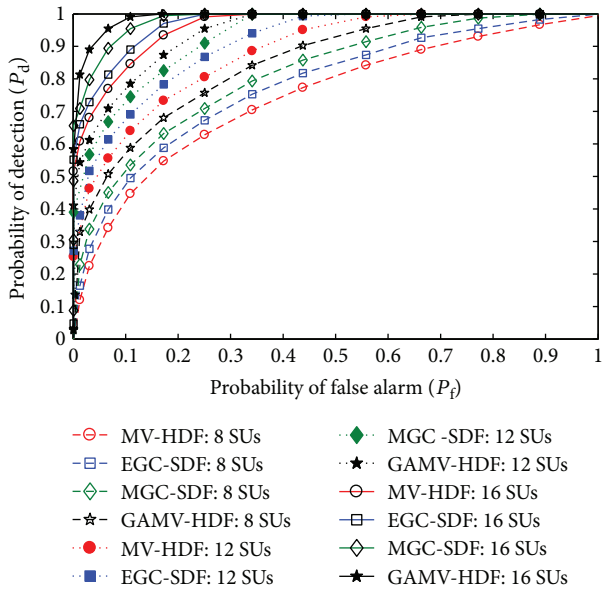

Figure 6: Probability of detection versus probability of false alarm at different ratios of cooperating SUs with MUs having low SNR compared with NSUs.

values compared to normal cooperating SUs. In Figure 5, when MUs are having higher SNR values compared with normal cooperating SUs, the results of the EGC-SDF and MGC-SDF are getting worse among all schemes. The proposed method has improved the performance at all values of SNR in Figure 5 compared with other combination schemes.

Similarly, Figures 6 and 7 show probability of detection versus probability of false alarm under −10.5 dB average SNR. In Figure 6, the system is tested against 8, 12, and 16

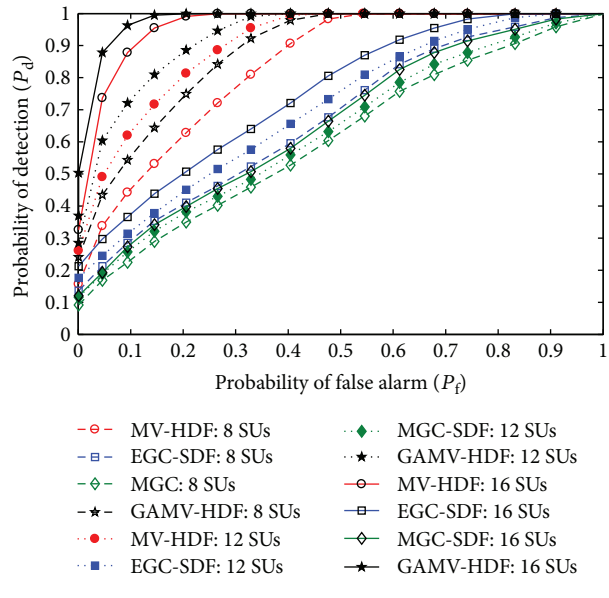

Figure 7: Probability of detection versus probability of false alarm (ROC) at different ratios of cooperating SUs with MUs having high SNR compared with NSUs.

cooperative SUs with low SNR by MUs compared with NSUs while in Figure 7, the system was observed when MUs participate with higher SNR against the NSUs. It is clear from the results in Figures 6 and 7 that the performance of cooperation has resulted in improved performance for all fusion schemes when the number of cooperative stations increases from 8 to 16.

In Figure 6, when MUs participate with low SNR, the MGC-SDF scheme has better performance compared with the EGC-SDF and simple MV-HDF schemes. The proposed GAMV-HDF method has surpassed all other schemes in Figure 6 in this low SNR situation of MUs. This is similar for the results in Figure 7 with higher SNR participation by MUs compared with NSUs. The ROC results of the MGC-SDF are poor under all 8, 12, and 16 total numbers of cooperating SU cases when MUs take higher SNR. The simple MV-HDF is able to produce the better ROC performance in comparison with the EGC-SDF and MGC-SDF schemes in Figure 7.

Results for the probability of detection of the PU are obtained against the varying SNR in Figures 8 and 9 at different ratios of cooperating SUs. In Figure 8, detection results are collected when MUs are observed with low SNR and in Figure 9 with higher SNR values for MUs compared with normal cooperative users. It is good to see improvement in the detection results for the proposed GAMV-HDF scheme with increasing SNR in both results. When MUs have low SNR values compared with the normal SUs as in Figure 8, the proposed method has better detection results at all values of SNRs in all cases of 8, 12, and 16 cooperating users. The proposed method detection results are followed by the MGC-SDF and EGC-SDF schemes, while the detection results obtained for the simple MV-HDF scheme is the lowest of all in Figure 8. In Figure 9, when MUs have higher SNR, the detection results of the proposed method are less

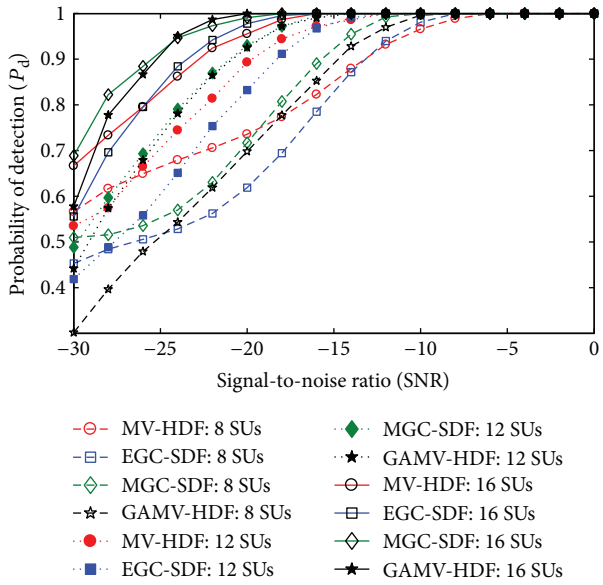

Figure 8: The probability of detection versus signal-to-noise ratio at different ratios of cooperative SUs with MUs having low SNR compared with NSUs.

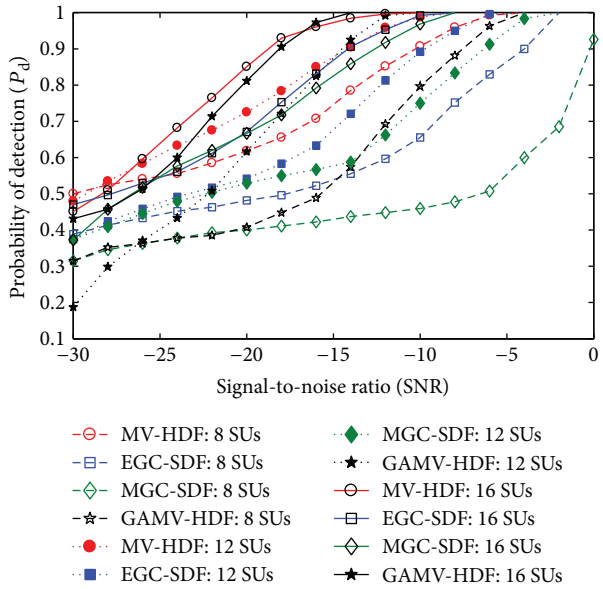

Figure 9: The probability of detection versus signal-to-noise ratio at different ratios of cooperative SUs with MUs having high SNR compared with SUs.

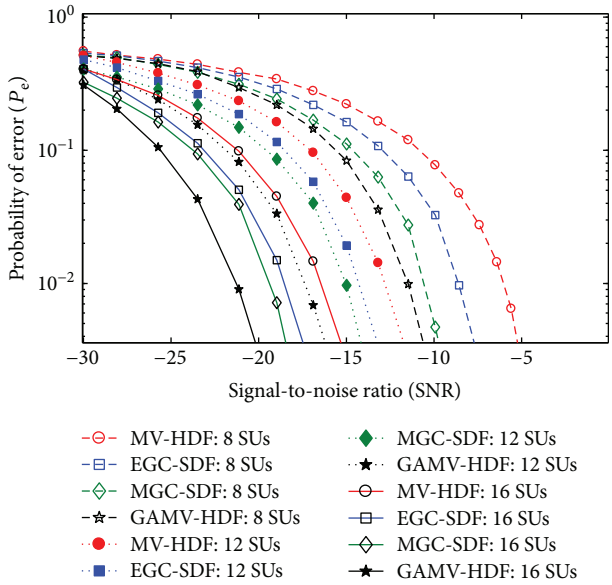

Figure 10: Probability of error versus signal-to-noise ratio at different ratios of cooperative SUs with MUs having low SNR compared with NSUs.

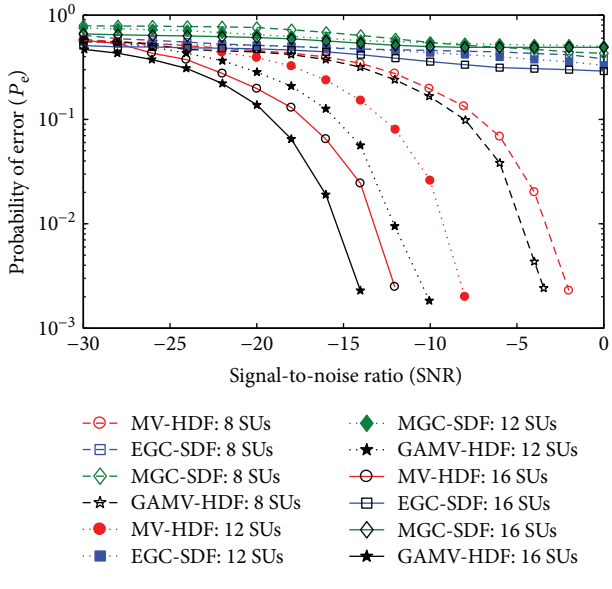

Figure 11: Probability of error versus signal-to-noise ratio at different ratios of cooperative SUs with MUs having high SNR compared with NSUs.

vulnerable. The simple MV-HDF is able to surpass both the EGC-SDF and MGC-SDF schemes at all values of SNRs and different ratios of cooperating SUs.

Finally, the probability of error results of the PU detection is shown in Figures 10 and 11 to compare the accuracy of the proposed scheme with all other schemes. The graphical result in Figures 10 and 11 shows the minimum error of the proposed GAMV-HDF scheme against the simple MV-HDF, EGC-SDF, and MGC-SDF schemes. In Figures 10 and 11, results are drawn with a total of 8, 12, and 16 users under low SNR observation for MUs as in Figure 10 and with higher SNR values for MUs in Figure 11.

The proposed scheme gives less detection error in terms of sensing the licensed user channel followed by the MGC-SDF scheme in Figure 10. Furthermore, the simple MV-HDF scheme has resulted in high probability of error in Figure 10. From the results in Figure 11, when MUs have higher SNR values as compared with NSUs, the error probability of the MGC-SDF and EGC-SDF increases compared with the simple MV-HDF and proposed GAMV-HDF

methods. The MGC-SDF performance degrades in this case because MGC-SDF is giving higher preference to the detection of SUs with higher SNR information. As MUs are considered with higher SNR, therefore, MGC-SDF decision about the PU channel is strongly misguided by the MUs. Similarly, EGC-SDF performance is also affected by the higher SNR of the MUs because it is equally considering the reported information of all SUs for a global decision.

It is clear from these simulations that the use of GA followed by the MV-HDF scheme makes the performance of CSS more authentic and valid in the presence of MUs at various numbers of cooperating SUs and SNR ratios.

The harmful risk of AYMU, ANMU, ROMU, and OMU user participation in CSS is reduced with the usage of the proposed scheme. From the graphical results of the proposed, simple MV-HDF, EGC-SDF, and MGC-SDF schemes, it is clear that the process of cooperation turns out to be more reliable and accurate by following the proposed methodology. The proposed scheme is able to make the sensing process reliable without actually identifying MUs.

5. Conclusion

Existence of malicious users in a CSS environment is reducing the advantages of using cooperation among SUs. Efficient and timely detection of MUs in a CSS environment is necessary to avoid the FC to conclude incorrect reference to the PU spectrum. This paper focuses on improving the performance of CSS using GA. The FC is taking sensing information from all cooperating SUs, including normal and malicious users, and combining them for a more precise and concrete decision about the licensed user spectrum using MV-HDF with GA. The decisions of the MV-HDF are shaped more authentically and reliably with GA by identifying optimum sensing results with selection and crossover in the presence of MUs. Simulations reflect the superiority and authenticity of the proposed scheme in producing a more accurate and reliable decision in CSS at the FC.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

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

[2] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: requirements, challenges and design trade-offs," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 32–39, 2008.

[3] L. Zhai, H. Wang, and C. Gao, "A spectrum access based on quality of service (QoS) in cognitive radio networks," *PLoS One*, vol. 11, no. 5, article e0155074, 2016.

[4] F. Benedetto, G. Giunta, E. Guzzon, and M. Renfors, "Detection of hidden users in cognitive radio networks," in *2013 IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 2296–2300, London, UK, September 2013.

[5] F. Benedetto, G. Giunta, and M. Renfors, "A spectrum sensing algorithm for constant modulus primary users signals," *IEEE Communications Letters*, vol. 20, no. 2, pp. 400–403, 2016.

[6] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *2004 Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, vol. 1, pp. 772–776, Pacific Grove, CA, USA, November 2004.

[7] R. Tandra and A. Sahai, "Fundamental limits on detection in low SNR under noise uncertainty," in *International Conference on Wireless Networks, Communications and Mobile Computing*, vol. 1, pp. 464–469, Maui, HI, USA, June 2005.

[8] F. Benedetto, G. Giunta, A. Tedeschi, and E. Guzzon, "Performance improvements of cooperative spectrum sensing in cognitive radio networks with correlated cognitive users," in *2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, pp. 1–5, Prague, Czech Republic, 2015.

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

[10] M. Monemian and M. Mahdavi, "Analysis of a new energy-based sensor selection method for cooperative spectrum sensing," *IEEE Sensors Journal*, vol. 14, no. 9, pp. 3021–3032, 2014.

[11] D. Lee, "Adaptive random access for cooperative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 2, pp. 831–840, 2015.

[12] Y. He, J. Xue, T. Ratnarajah, M. Sallaturai, and F. Khan, "On the performance of cooperative spectrum sensing in random cognitive radio networks," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–12, 2016.

[13] H. Guo, W. Jiang, and W. Luo, "Linear soft combination for cooperative spectrum sensing in cognitive radio networks," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1573–1576, 2017.

[14] F. Benedetto, G. Giunta, E. Guzzon, and M. Renfors, "Effective monitoring of freeloading user in the presence of active user in cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 5, pp. 2443–2450, 2014.

[15] E. Guzzon, S. Member, F. Benedetto, G. Giunta, and S. Member, "Performance improvements of OFDM signals spectrum sensing in cognitive radio," in *IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1–5, Quebec City, QC, Canada, September 2012.

[16] A. A. Sharifi, M. Sharifi, and N. I. Y. A. M. J. Musevi, "Collaborative spectrum sensing under primary user emulation attack in cognitive radio networks," *IETE Journal of Research*, vol. 62, no. 2, pp. 205–211, 2016.

[17] K. Zeng, P. Pawelczak, and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Communications Letters*, vol. 14, no. 3, pp. 226–228, 2010.

[18] H. Vu-Van and I. Koo, "A sequential cooperative spectrum sensing scheme based on cognitive user reputation," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 4, pp. 1147–1152, 2012.

[19] M. Nabil, W. El-Sayed, and M. Elnainay, "A cooperative spectrum sensing scheme based on task assignment algorithm for cognitive radio networks," in *International Wireless*

Communications and Mobile Computing Conference (IWCMC), pp. 151–156, Nicosia, Cyprus, August 2014.

[20] G. Zhang, Z. Chen, L. Tian, and D. Zhang, "Using trust to establish a secure routing model in cognitive radio network," *PLoS One*, vol. 10, no. 9, article e0139326, 2015.

[21] F. Benedetto, A. Tedeschi, G. Giunta, and P. Coronas, "Performance improvements of reputation-based cooperative spectrum sensing," in *IEEE 27th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–6, Valencia, Spain, September 2016.

[22] S. S. Kalamkar, P. K. Singh, and A. Banerjee, "Block outlier methods for malicious user detection in cooperative spectrum sensing," in *IEEE Vehicular Technology Conference*, Seoul, South Korea, May 2015.

[23] F. Penna, Y. Sun, L. Dolecek, and D. Cabric, "Detecting and counteracting statistical attacks in cooperative spectrum sensing," *IEEE Transactions on Signal Processing*, vol. 60, no. 4, pp. 1806–1822, 2012.

[24] H. Li and Z. Han, "Catch me if you can: an abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3554–3565, 2010.

[25] H. A. Shah and I. Koo, "Optimal quantization and efficient cooperative spectrum sensing in cognitive radio networks," in *2015 International Conference on Emerging Technologies (ICET)*, pp. 1–6, Peshawar, Pakistan, December 2015.

[26] X. Liu, J. Yan, and K. Chen, "Optimal energy harvest-based weighed cooperative spectrum sensing in cognitive radio," in *2016 International Workshop on Sustainability, Implementation and Resilience of Energy-Aware Networks, ICNC*, pp. 16–20, Kauai, USA, February 2016.

[27] D. Hamza, S. Aïssa, and G. Aniba, "Equal gain combining for cooperative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4334–4345, 2014.

[28] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *2006, Proceeding IEEE International Conference on Communications*, vol. 4no. c, pp. 1658–1663.

[29] S. P. Herath, N. Rajatheva, and C. Tellambura, "On the energy detection of unknown deterministic signal over Nakagami channels with selection combining," in *2009. CCECE '09. Canadian Conference on Electrical and Computer Engineering*, vol. 12120, pp. 745–749, St. John's, NL, Canada, May 2009.

[30] S. P. Herath and N. Rajatheva, "Analysis of equal gain combining in energy detection for cognitive radio over Nakagami channels," in *GLOBECOM - IEEE Global Telecommunications Conference*, pp. 1–5, New Orleans, LO, USA, 2008.

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

[32] H. Vu-Van and I. Koo, "A robust cooperative spectrum sensing based on Kullback-Leibler divergence," *IEICE Transactions on Communications*, vol. E95–B, no. 4, pp. 1286–1290, 2012.

[33] L. Wang, L. Zhang, and X. Chen, "A dynamic threshold strategy against SSDF attack for cooperative spectrum sensing in cognitive radio networks," in *2015 International Conference on Wireless Communications & Signal Processing (WCSP)*, pp. 1–5, Nanjing, China, October 2015.

[34] D. B. Teguig, B. Scheers, and V. L. Nir, "Data fusion schemes for cooperative spectrum sensing in cognitive radio networks-*Military Communications and Information Systems Conference, MCC*, vol. 1, pp. 104–110, Gdansk, Poland, October 2012.

[35] J. Unnikrishnan and V. V. Veeravalli, "Cooperative spectrum sensing and detection for cognitive radio," in *2007. GLOBECOM '07. IEEE Global Telecommunications Conference*, pp. 2972–2976, Washington, DC, USA, November 2007.

[36] T. Jiang and D. Qu, "On minimum sensing error with spectrum sensing using counting rule in cognitive radio networks," in *Proceedings of the 4th International ICST Conference on Wireless Internet*, Belgium, 2008.

[37] N. Marchang, R. Rajkumari, S. B. Brahmachary, and A. Taggu, "Dynamic decision rule for cooperative spectrum sensing in cognitive radio networks," in *2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pp. 1–5, Coimbatore, India, March 2015.

[38] A. Zainab and P. Sinha, "A survey of cognitive radio reconfigurable antenna design and proposed design using genetic algorithm," in *IEEE Students' Conference on Electrical, Electronics and Computer Science*, pp. 1–6, Bhopal, India, 2016.

[39] N. Gul, A. Naveed, A. Elahi, T. SaleemKhattak, and I. M. Qureshi, "A combination of double sided neighbor distance and genetic algorithm in cooperative spectrum sensing against malicious users," in *2017 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pp. 746–753, Islamabad, Pakistan, January 2017.

[40] U. Mehboob, J. Qadir, S. Ali, and A. Vasilakos, "Genetic algorithms in wireless networking: techniques, applications, and issues," *Soft Computing*, vol. 20, no. 6, pp. 2467–2501, 2016.

[41] S. Bhattacharjee, "Optimization of probability of false alarm and probability of detection in cognitive radio networks using GA," in *2015 IEEE 2nd International Conference on Recent Trends in Information Systems (ReTIS)*, Kolkata, India, July 2015.

[42] M. Akbari and M. Ghanbarisabagh, "A novel evolutionary-based cooperative spectrum sensing mechanism for cognitive radio networks," *Wireless Personal Communications*, vol. 79, no. 2, pp. 1017–1030, 2014.