

Article

Differential Evolution Based Machine Learning Scheme for Secure Cooperative Spectrum Sensing System

Noor Gul ^{1,2}, Su Min Kim ² , Saeed Ahmed ³ , Muhammad Sajjad Khan ⁴  and Junsu Kim ^{2,*}¹ Department of Electronics, University of Peshawar, Peshawar 25120, Pakistan; noor@uop.edu.pk² Department of Electronics Engineering, Korea Polytechnic University, Siheung-si 15073, Korea; suminkim@kpu.ac.kr³ Department of Electrical Engineering, Mirpur University of Science and Technology, New Mirpur City 10250, Pakistan; saeed.ahmed@must.edu.pk⁴ Department of Electrical Engineering, International Islamic University, Islamabad 44000, Pakistan; sajjad.khan@iiu.edu.pk

* Correspondence: junsukim@kpu.ac.kr; Tel.: +82-31-8041-0497

Abstract: The secondary users (SUs) in cognitive radio networks (CRNs) can obtain reliable spectrum sensing information of the primary user (PU) channel using cooperative spectrum sensing (CSS). Multiple SUs share their sensing observations in the CSS system to tackle fading and shadowing conditions. The presence of malicious users (MUs) may pose threats to the performance of CSS due to the reporting of falsified sensing data to the fusion center (FC). Different categories of MUs, such as always yes, always no, always opposite, and random opposite, are widely investigated by researchers. To this end, this paper proposes a hybrid boosted tree algorithm (HBTA)-based solution that combines the differential evolution (DE) and boosted tree algorithm (BTA) to mitigate the effects of MUs in the CSS systems, leading to reliable sensing results. An optimized threshold and coefficient vector, determined against the SUs employing DE, is utilized to train the BTA. The BTA is a robust ensembling machine learning (ML) technique gaining attention in spectrum sensing operations. To show the effectiveness of the proposed scheme, extensive simulations are performed at different levels of signal-to-noise-ratios (SNRs) and with different sensing samples, iteration levels, and population sizes. The simulation results show that more reliable spectrum decisions can be achieved compared to the individual utilization of DE and BTA schemes. Furthermore, the obtained results show the minimum sensing error to be exhibited by the proposed HBTA employing a DE-based solution to train the BTA. Additionally, the proposed scheme is compared with several other CSS schemes such as simple DE, simple BTA, maximum gain combination (MGC), particle swarm optimization (PSO), genetic algorithm (GA), and K-nearest neighbor (KNN) algorithm-based soft decision fusion (SDF) schemes to validate its effectiveness.

Keywords: cognitive radio; machine learning; genetic algorithm; cooperative communication; particle swarm optimization; boosted trees algorithm; multipath channels



Citation: Gul, N.; Kim, S.M.; Ahmed, S.; Khan, M.S.; Kim, J. Differential Evolution Based Machine Learning Scheme for Secure Cooperative Spectrum Sensing System. *Electronics* **2021**, *10*, 1687. <https://doi.org/10.3390/electronics10141687>

Academic Editor: Paul Mitchell

Received: 6 June 2021

Accepted: 13 July 2021

Published: 14 July 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The exponential growth in wireless communication devices and the demands of high data rates require the development of new techniques to meet user and spectrum requirements. As the static spectrum allocation policy is unable to accommodate new applications and services, dynamic spectrum allocation (DSA) is the best alternative for static spectrum allocation [1,2]. The cognitive radio network (CRN) has emerged as a vital solution to the problem of an underutilized radio spectrum [3]. Of the different goals in the CRN, spectrum sensing, in which the secondary users (SUs) sense the activity of primary users (PUs) before accessing the channel dynamically, has attracted special attention [4,5]. Similarly, the SU vacates the channel when the PU becomes active again.

The reliability of the sensing results of SUs may reduce due to fading, shadowing, and hidden terminal problems between the PU and the SUs. Cooperative spectrum sensing (CSS) is one way to obtain reliable sensing decisions [6]. In CSS, SUs at different geographical positions sense the given PU channel and report their local observations to the fusion center (FC) for a final decision. The CSS system has two broad categories: distributed and centralized. The SUs in the distributed CSS system perform spectrum-sensing jobs and share their decisions without considering any central coordinator [7,8].

The sensing reliability of CSS may be seriously degraded by the participation of malicious users (MUs). The MUs may report the deliberately falsified sensing information to the FC, aiming to mislead the FCs in making their final decision. Security issues in the CSS system are a significantly important topic, and several research works have been studied to enhance the system's security [9–13]. Byzantine users, jammers, and primary user emulation attackers (PUEAs) are the major security concerns for researchers. In a Byzantine attack, the MUs report false sensing data to the FC to deteriorate the network performance and to access spectral resources for their own purposes [14]. The jammers target the frequency band of the operating radio with the injection of malicious signals that interfere with the desired receiver signal. During a PUEA, the MU transmits while pretending to be a PU to mislead the SUs about the actual PU's activity [15].

In [16], the FC is protected against the Byzantine users using a novel corruption strategy behavior, where the message-passing algorithm helps the FC to distinguish normal and attacking users. A contract-theory-based approach is proposed in [17] as an incentive design mechanism, where the honest SUs are rewarded to boost future cooperation. Similarly, in [18], contestants of the Byzantine attackers are filtered with the computation of a noisy gradient at the tuning parameter server. The work in [19] formulates a composite binary hypothesis test against the transmission of faulty devices and various categories of selfish and malicious injected data. The detection process of both the MU and mobile CRN is improved using location reliability and malicious intension (LRMI) in [20]. A recursive updating algorithm is proposed in [21] that helps in the selection of the SUs with a higher sensing reputation and reduces the impact of the MUs. The scheme presented in [22] allows honest SUs to recommend decisions to the FC about a PU as final along with their local sensing reports to guarantee the reliability of CSS. A low-density parity-check code-based CSS scheme that protects the relayed sensing information to the FC against variations in the wireless channel is investigated in [23]. The cryptographic scheme in [24] uses a privacy-preserving protocol to preserve the location of an SU while maintaining sensing reliability. Similarly, the scheme in [25] follows additional architectural and cryptographic techniques to maintain the user's location privacy during spectrum sensing. In another work in [26], the effects of the false sensing data are reduced using sensing credit measurement. The data fusion scheme in [27] helps to counter the effects of spectrum sensing data falsification (SSDF) and PUEA in cognitive radio wireless sensor networks. A novel attack proof scheme using an adaptive linear combination technique is analyzed in [28] for the identification of MUs.

The work presented in [29–32] focused on the use of distance measurement, the sliding window trust model, and random selection, while assuming attacking patterns to strengthen the collusive attackers of the FC.

As with other disciplines, machine learning (ML) techniques are also being employed in the CRN field. The work in [33] suggested deep cooperative sensing-based CRN, where the spectrum sensing problem is resolved using the k -nearest neighbor (KNN) approach. Similarly, malicious activities in vehicular-based machine-to-machine communication are detected using an ML-based trust scheme in [34]. The use of ML and statistical analysis-based approaches presented in [35] helped against the detection of malicious software in caters and mobile devices. The reinforcement-learning scheme proposed in [36] helps to improve the sensing decisions of individual sensing users. Ensembling methods are gaining acceptance among researchers to solve detection and prediction problems in various fields, such as in depression detection, electrocardiograph artifacts, abnormal

echo propagation in weather radar, islanding detection in smart grids, and so on [37–42]. The boosted tree algorithm (BTA) leads to improved prediction performance by forming a strong classifier. To establish a combined ensemble model for prediction, the training dataset trains and boosts several weak classifiers. Thus, the weak classifier is updated while easing the re-training requirement. Since data are expected to have various characteristics of the classification instances, the diversity in weak classifier outputs offers the advantage of more desirable predictions. On the other hand, individual learners may result in biased prediction; thus, an ensembling strategy to integrate and optimize individual poor results is a superior alternative [37].

The work in [43] employs a differential evolution (DE)-based scheme that supports the CSS system to find the PUs' statistics in the presence of various categories of MUs. This enables the FC to determine a suitable coefficient vector against the users' sensing reports, further leading to better sensing results. In contrast, in [44], the simple BTA is investigated to find optimum sensing results. The BTA is trained based on the soft energy reports of the users in the first phase while the algorithm searches for the suitable PU channel availability after the collection of enough reports in the second phase.

Extending the previous work to the enhanced security and improved authentication of CSS results, the proposed scheme combines the key features of the DE and BTA, thus developing a new scheme that is termed as hybrid BTA (HBTA) in this work. The main contributions of the paper are summarized as follows:

- A hybrid scheme that integrates the essential features of the DE, such as an optimum threshold with a coefficient vector, and the BTA algorithm is proposed. The adaptive threshold with minimum sensing error obtained in the DE phase of the proposed HBTA results in an optimum coefficient vector that assists the FC in dealing with all the SUs according to their sensing notifications;
- One of the significant contributions of the proposed HBTA scheme is that it is trained based on the solutions obtained through DE and not directly from the SUs, contrary to [44], where direct sensing reports by SUs are employed to train the simple BTA. The proposed HBTA fuses the soft energy statistics received from the SUs with the weighted coefficient vector obtained in the DE phase to further train the BTA section of the proposed HBTA. Thus, the reliance of the FCs on the received MU statistics is lessened because of the penalty in the form of least weights during the training phase.

Earlier, in [43,44], the authors showed that the error probability decreases with an increasing signal-to-noise-ratio (SNR) and increasing numbers of sensing samples. However, in this paper, we further extend the earlier investigation by combining the effects of BTA with DE. We evaluate the error probabilities against varying SNRs at two distinct levels for (1) sensing samples, (2) algorithm iterations, and (3) population sizes. Furthermore, the SNR range is widened for an additional analysis of the error probability's dependency upon (1) the heuristic algorithm iterations exhibited in Section 4 as Case 1 and (2) the heuristic algorithm population size, shown as Case 2.

The rest of the paper is organized as follows: the system model is discussed in Section 2. The proposed model for determining optimal sensing results using HBTA is presented in Section 3. Section 4 illustrates the simulation outcomes. Finally, concluding remarks and future research directions are included in Section 5. Table 1 consists of the abbreviations employed in the paper.

Table 1. Common abbreviations.

Abbreviation	Meaning	Abbreviations	Meaning
DSA	Dynamic spectrum allocation	DE	Differential evolution
CRN	Cognitive radio network	PSO	Particle swarm optimization
SU	Secondary user	GA	Genetic algorithm
PU	Primary user	MGC	Maximum gain combination
MU	Malicious user	EGC	Equal gain combination
MUC	Malicious user center	SDF	Soft decision fusion
CSS	Cooperative spectrum sensing	RNN	Recurrent neural network
FC	Fusion center	AY	Always yes
PUEA	Primary user emulation attacker	AN	Always no
LRMI	Location reliability and malicious intention	AO	Always opposite
SSDF	Spectrum sensing data falsification	RO	Random opposite
KNN	K-nearest neighbor	AYC	Always yes collusion
BTA	Boosted tree algorithm	ANC	Always no collusion
HBTA	Hybrid boosted tree algorithm	AOC	Always opposite collusion
ML	Machine learning	ROC	Random opposite collusion
SNR	Signal-to-noise ratio	AWGN	Additive white gaussian noise

2. System Model

A model of the conventional centralized CSS system is shown in Figure 1. Here, the individual SUs sense the PUs' activity and report their sensing statistics to the FC. The MUs report their observations to both the main FC and malicious user center (MUC). The MUC collusion centers in the Figure 1 combine local attacks of the individual MUs that result in more serious threats at the FC by overcoming weaknesses in the individual attackers. In this model, the MUC reports an average of the analogous MUs sensing observations to the main FC. The MUC center of the always opposite (AO) users—i.e., the always opposite collusion (AOC) center—receives sensing reports from all AO users, while the random opposite collusion (ROC) center obtains sensing data from the random opposite (RO) categories of MUs. Similarly, the MUC of an always yes (AY) user is the always yes collusion (AYC) center and the MUC anticipated for the always no (AN) users is the always no collusion (ANC) center. The participation of the AO and AOC center is implemented to reduce the network data rate and increased interference for the PU, as both the AO and AOC oppose actual PU activity in the sensing channel. As the AY reports high-energy statistics irrespective of the actual PU status, both the AY and AYC center result in increased false alarms in the system, thus decreasing network throughput. The AN user tries to sense the PU channel and inform both the main FC and ANC regarding the availability of the PU channel for access. This leads to increased interference with legitimate PU transmission. The RO and ROC centers behave similarly to the AO and AOC, which report opposite energy statistics with probability (P) and report normal sensing data with probability ($1 - P$). The contribution of this category of MU results in unacceptable interference and a reduced data rate for the SUs.

In the given centralized CSS, the users report their soft energy statistics to the FC to make a global decision, where soft decision fusion (SDF) is employed as a combination scheme. The challenge is to investigate the performance of the CSS in the presence of AO, AOC, AY, AYC, AN, ANC, RO, and ROC categories of MUs.

The (H_0/H_1) hypothesis of the sensing channel availability presented by the j^{th} SU in the l^{th} sensing slot is [9]

$$\begin{cases} H_0 : x_j(l) = v_j(l) \\ H_1 : x_j(l) = g_j c(l) + v_j(l) \end{cases}, j \in \{1, 2, \dots, M\}, l \in \{1, 2, \dots, K\}, \quad (1)$$

where $x_j(l)$ is the j^{th} user observation of the PU transmitted signal $c(l)$ with mean 0 and variance σ_c^2 . Here, l shows the sensing slot, M the total number of SUs, and $K = 2BT_s$ is the total number of samples in a bandwidth B and sensing period T_s . $v_j(l)$ is the additive

white gaussian noise (AWGN) of the channel between the PU and j^{th} user that has mean zero and variance σ_v^2 . Similarly, g_j is the PU and j^{th} user channel gain. The H_0 hypothesis in (1) states the availability of the PU channel for SU access, while the H_1 hypothesis is presented to show the transmission of the PU over the given sensing channel. Therefore, the SUs are allowed to gain access to the PU channel under the H_0 hypothesis only.

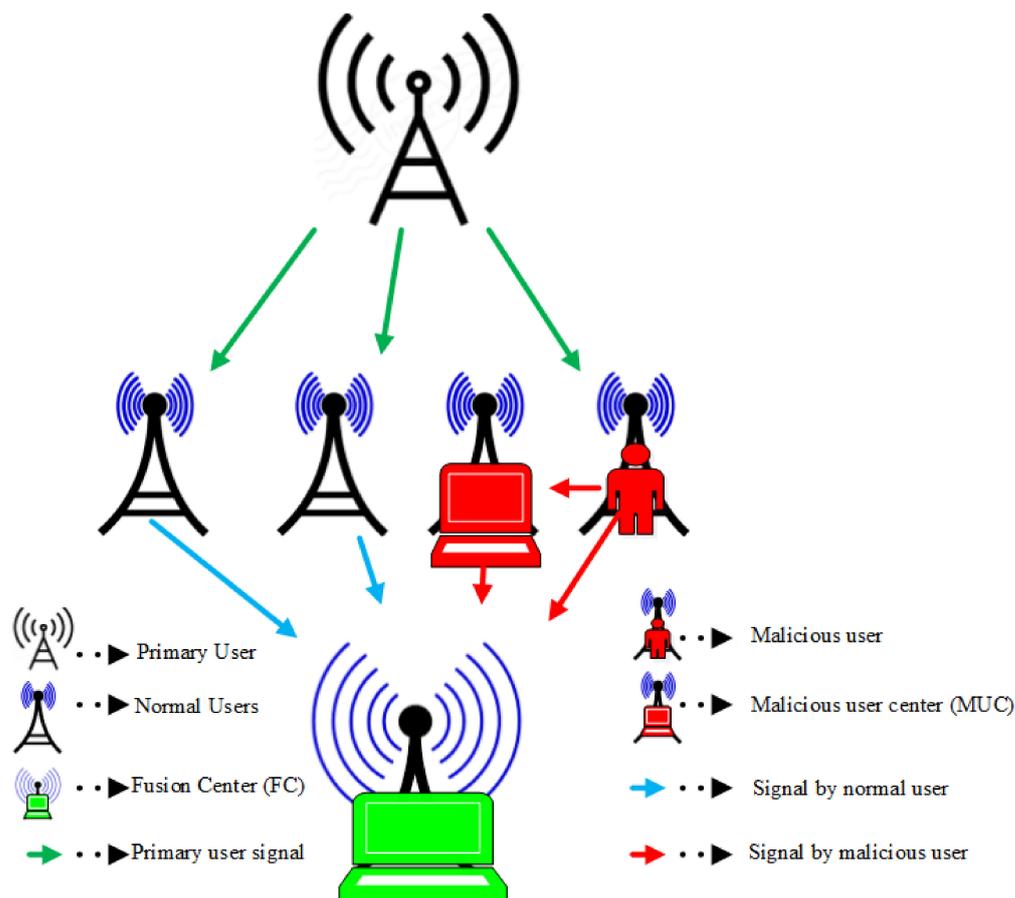


Figure 1. Conventional centralized cooperative spectrum sensing (CSS).

The K sensing observations in (1) are combined to form the energy for the threshold detector as [9,11,45,46].

$$X_j(i) = \begin{cases} \sum_{l=l_i}^{l_i+K-1} |v_j(l)|^2, & H_0 \\ \sum_{l=l_i}^{l_i+K-1} |g_j c(l) + v_j(l)|^2, & H_1 \end{cases} \quad (2)$$

As the soft energy observation X_j under both hypotheses for a sufficient number of sensing samples $K > 10$ [45] closely resembles a Gaussian distribution according to the central limit theorem, (2) is rewritten as follows [9,11,45,46]:

$$X_j \sim \begin{cases} N(\mu_0 = K, \sigma_0^2 = 2K), & H_0 \\ N(\mu_1 = K(g_j + 1), \sigma_1^2 = 2K(g_j + 1)), & H_1 \end{cases} \quad (3)$$

where g_j is the j^{th} user and PU channel gain, while the mean and variance results under both the H_0 and H_1 hypotheses are (μ_0, σ_0^2) and (μ_1, σ_1^2) . The energy reported from the j^{th} user Z_j to the FC is

$$Z_j = \sum_{l=1}^K |U_j(l)|^2 \tag{4}$$

where $U_j(l) = \sqrt{P_{R,j}}h_jX_j(l) + N_j(l)$ is the signal delivered to the FC using the channel between j^{th} user and FC in the l^{th} sensing slot. Here, $P_{R,j}$ is the j^{th} SU transmission power with h_j channel gain between FC and SU, whereas, the AWGN distribution has zero mean and variance σ_j^2 , i.e., $N_j(l) \sim N(0, \sigma_j^2)$. Similar to the channel between the PU and SU, the SU to the FC channel noise is also assumed to be AWGN with mean zero and variance δ_j^2 .

A global decision of the PU status is generated by combining sensing reports of the M SUs with the weighting coefficient vector as

$$Z(i) = \sum_{j=1}^M (w_j Z_j(i)) \tag{5}$$

where w_j is the weighting coefficient vector that shows the authenticity of the j^{th} user sensing data, which is determined using DE. As an individual user reports statistics, $Z_j(i)$ is normally distributed, and thus the resultant $Z(i)$ is assumed to be normally distributed in nature, as in [32].

Thus,

$$E(Z(i)|H_0) = \sum_{j=1}^M w_j K \sigma_{0,j}^2 \tag{6}$$

$$E(Z(i)|H_1) = \sum_{j=1}^M w_j K \sigma_{1,j}^2 \tag{7}$$

$$Var(Z(i)|H_0) = \sum_{j=1}^M 2w_j^2 K (\sigma_{0,j}^2 + \delta_j^2)^2 = \vec{w}^T \Phi_{H_0} \vec{w} \tag{8}$$

$$Var(Z(i)|H_1) = \sum_{j=1}^M 2w_j^2 K (\sigma_{1,j}^2 + \sigma_{0,j}^2)^2 = \vec{w}^T \Phi_{H_1} \vec{w} \tag{9}$$

In (6) and (7), $\sigma_{0,j}^2$ and $\sigma_{1,j}^2$ are $U_j(l)$ variances under H_0/H_1 of the j^{th} user, where $\sigma_{0,j}^2 = P_{R,j}|h_j|\sigma_{v_j}^2 + \delta_j^2$ and $\sigma_{1,j}^2 = P_{R,j}|g_j|^2|h_j|^2\sigma_c^2 + \sigma_{0,j}^2$.

The goal is then to find an optimal coefficient vector that can help in determining the appropriate threshold β with minimum sensing error. These optimal weighting coefficients help us to train the BTA scheme in the description of the proposed model.

The H_0/H_1 hypotheses result in the following covariance matrices:

$$\Phi_{H_0} = diag(2K\sigma_{0,j}^4) \tag{10}$$

$$\Phi_{H_1} = diag(2K(P_{R,j}|g_j|^2|h_j|^2\sigma_c^2 + \sigma_{0,j}^2)^2) \tag{11}$$

where $\sigma_{0,j}^2$ and $\sigma_{1,j}^2$ represent square diagonal matrices in (10) and (11).

The detection and false alarm probabilities show the occupancy of the licensee channel by the PU and the idle status when it is falsely identified to be in use by the licensee as

$$P_f = P(Z(i) > \beta | H_0) = Q\left(\frac{\beta - E(Z(i)|H_0)}{\sqrt{\text{var}(Z(i)|H_0)}}\right) = Q\left(\frac{\beta - \vec{w}^T \vec{\mu}_0}{\sqrt{\vec{w}^T \Phi_{H_0} \vec{w}}}\right) \quad (12)$$

$$P_d = P(Z(i) > \beta | H_1) = Q\left(\frac{\beta - E(Z(i)|H_1)}{\sqrt{\text{var}(Z(i)|H_1)}}\right) = Q\left(\frac{\beta - \vec{w}^T \vec{\mu}_1}{\sqrt{\vec{w}^T \Phi_{H_1} \vec{w}}}\right) \quad (13)$$

where β is the optimal threshold, represented as

$$\beta = \left(\frac{\sqrt{w^T \Phi_{H_1} w \mu_0^T \vec{w}} + \sqrt{\vec{w}^T \Phi_{H_1} w \mu_1^T w}}{\sqrt{w^T \Phi_{H_0} w} + \sqrt{w^T \Phi_{H_1} w}} \right) \quad (14)$$

Assuming the false alarm probability to be $P_f = 1 - P_d$ and $P_f = P_m$, where P_m is the misdetection probability, the total error probability P_e is determined as follows:

$$P_e = P_f + P_m = Q\left(\frac{\beta - \vec{w}^T \vec{\mu}_0}{\sqrt{\vec{w}^T \Phi_{H_0} \vec{w}}}\right) + Q\left(\frac{\vec{w}^T \vec{\mu}_1 - \beta}{\sqrt{\vec{w}^T \Phi_{H_1} \vec{w}}}\right) \quad (15)$$

The error probability in (15) depends on the selection of \vec{w} . The optimal threshold β using (14) is substituted in (12), (13), and (15), which produces the minimum false alarm, high detection, and low error probability results.

Using the proposed scheme, we see in the following section that $0 < w_j(i) < 1$ and $\sqrt{\sum_{j=1}^M w_j^2(i)} = 1$, in order to reduce the selection procedure of the search space for the DE.

3. Proposed Hybrid Boosted Tree Algorithm

In the proposed model, we use the DE scheme to select weighting coefficients against the SUs by assigning high weights to normal users and minimum significance to the sensing of MUs. The optimal weighting coefficients identified in the first part are further utilized to train the BTA scheme.

Unlike the training procedure in [44], where the reporting users' soft energy information is used to train the BTA, this work collects both soft energy reports of the users along with optimal coefficient vectors from the DE, allowing the BTA to rely strongly on the sensing decisions of the normal SUs. An abstract block diagram of the proposed method is shown in Figure 2.

3.1. Differential Evolution-Based Solution

DE is a population-based search algorithm following crossover, mutation, and selection methods as in [8,43]. The major difference between DE and other optimization algorithms, while searching for the best fitness, is that DE selection depends on mutation. In addition, DE uses a non-uniform crossover, where child vector parameters of one parent are taken into consideration strongly in comparison with other parents. The DE has the ability to identify the global minimum irrespective of some initial parameters and exhibits quick convergence to the problem solution with fewer control parameters.

The self-adaptability in DE introduced via the mutation and selection procedure is its major advantage. Storm and Price were the first to suggest DE as a population-based stochastic search algorithm for the optimization of continuous functions in [47].

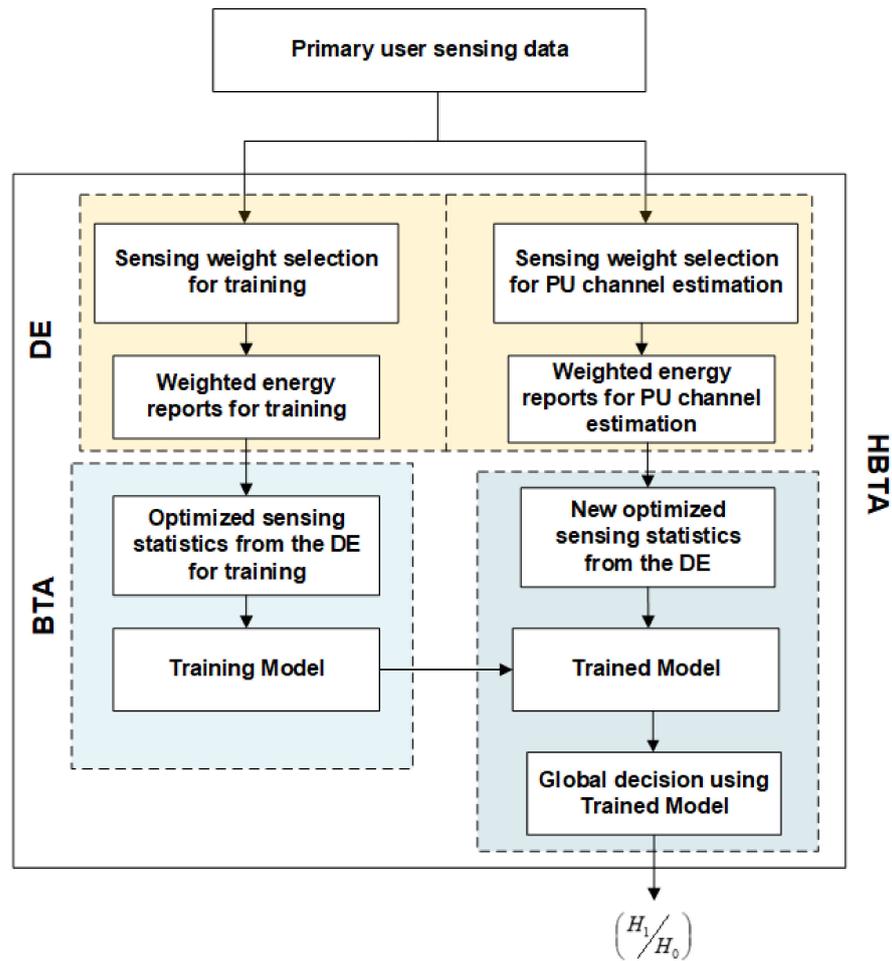


Figure 2. Abstract functional block diagram of the hybrid boosted tree algorithm (HBTA).

In this part of the proposed scheme, DE is employed to determine the optimal coefficient vector against the users’ reporting statistics. The selected coefficient vector in the final stage of the DE assigns a high weight to the sensing of a normal user to make their reports more authentic. Similarly, different categories of MUs are charged with minimum weights that enable the FC to rely on the reports of normal sensing users. The steps involved in DE finding an optimal threshold and coefficient vectors are as follows.

Step 1: Initialization

In this work, a total of N candidate solutions (individuals) for DE have been considered. The algorithm starts with a population initialization that has N candidate solutions and M dimensions equal to the total number of SUs; i.e., $\vec{w}_x = [w_1 w_2 \dots w_M]^T, x \in 1, \dots, N$:

$$w_x = L + (H - L) \times rand(N, M) \tag{16}$$

where L and H are the lower and upper limits of the x coefficient vector. The fitness value of each coefficient vector is determined in terms of the error probabilities $P_e(\vec{w}_x(1)), P_e(\vec{w}_x(2)), \dots, P_e(\vec{w}_x(N))$. Therefore, the vector with the minimum error probability out of all N vectors is selected along with corresponding threshold β value as an optimal threshold.

Step 2: Random Numbers Selection

In the second step, dissimilar random numbers n_1, n_2, n_3 are produced such that none of them is equal to any other.

Step 3: Mutation

In this step, the initial population, w_x , and dissimilar random numbers n_1, n_2, n_3 from step 2 are used to generate a new population as

$$w_y = w_x(n_1) + F \times (w_x(n_2) - w_x(n_3)) \quad (17)$$

where w_y is the mutant or mutation vector. The difference employed in the result of (17) forms the given algorithm DE. The selection of the constant number, F , is dependent on the problem, which is placed to keep the value of genes in the range of L and H .

Step 4: Crossover

A crossover operation is performed in this step using w_x and the mutant vector, w_y , to select genes among w_x and w_y as

$$w_z = \begin{cases} w_y & \text{if } a_j \leq CR \text{ or } j = jrand \\ w_x & \text{otherwise} \end{cases} \quad (18)$$

where a_j is a uniformly distributed random number between 0 and 1, while j is the element number of the candidate solution and $jrand$ is an integer randomly selected from 1 to M . Similarly, the value of CR in (18) is $0 \leq CR \leq 1$.

Step 5: Particles Fitness

The suitability of the w_z coefficient vectors is determined in this step using the error probabilities $P_e(\vec{w}_z(1))$, $P_e(\vec{w}_z(2))$, ..., $P_e(\vec{w}_z(N))$. Therefore, the coefficient vector with the minimum error probability is identified as the new global best vector and its associated threshold, β , is selected as the new global best threshold.

Step 6: Population and Global Best Vector Up-Gradation

The fitness values of w_z is compared with the initial population, w_x , to search for any up-gradation as

$$w_x = \begin{cases} w_z & \text{Fitness}(w_z) > \text{Fitness}(w_x) \\ w_x & \text{otherwise} \end{cases} \quad (19)$$

Similarly, the fitness of the new global best in w_z is compared with that of w_x to upgrade the global best and optimum threshold results accordingly.

Step 7: Stopping Criteria

In this step, a check is made to start recycling DE in step 2 or to end the DE process by inspecting the fitness function; i.e., whether the minimum error probability results have been achieved or the required number of iterations has been reached. The algorithm finally returns the global best coefficient vector and optimum threshold results.

3.2. Boosted Tree Algorithm

The working principle used by the BTA to solve the given problem is categorized into three major steps.

In the first step, N sensing observations consisting of user energy statistics along with coefficient vectors from the DE are collected at the FC and stored as feature vectors for the proposed BTA scheme. In step 2, the BTA is trained with the AdaBoost ensembling method. A more suitable and accurate decision is made using the BTA by accumulating and strengthening weak classifiers in this step. The detection and false alarm probabilities in step 3 are determined by considering the results in step 2 to make a global decision.

Step 1: Data Matrix Formulation

A history-reporting matrix is formed at the FC, consisting of a combination of individual users' soft energy statistics and weighting coefficient vectors, as shown below.

$$S = [s_{ij}] = \begin{bmatrix} s_{11} & s_{12} & \dots & s_{1M} \\ s_{21} & s_{22} & \dots & s_{2M} \\ s_{31} & s_{32} & \dots & s_{3M} \\ \vdots & \vdots & \ddots & \vdots \\ s_{N1} & s_{N2} & \dots & s_{NM} \end{bmatrix}, i \in \{1, 2, \dots, N\}, j \in \{1, 2, \dots, M\}, \quad (20)$$

where $s_{ij} = Z_j(i) \times w_j(i)$ is the j^{th} user's sensing statistics in combination with the j^{th} component of the coefficient vector. The M users sensing data including both normal and malicious participants are accumulated in N sensing periods with K sensing samples. The spectrum sensing falsification effects of MUs are minimized by the proposed technique in the following steps. The ML algorithms can find natural patterns in the data, which helps in decision making and produces improved prediction results.

Step 2: BTA Training Phase

The BTA scheme proposed in this paper uses adaptive boosting (AdaBoost) as an ensemble method, where weak classifiers are ensemble to make a strong classifier. The training set consists of $T = \{(s_{ij}, y_i)\}_{i=1}^N$, $s_{ij} \in \mathbb{R}^N$, $y_i \in \{-1, 1\}$, where $y_i = 1$ represents the class label presence of PU activity, whereas $y_i = -1$ denotes the availability of the PU channel for SU access. The training set T is constructed as an $N \times (M + 1)$ with dimensional space $T \in \mathbb{R}^{N \times (M+1)}$ and is written as

$$T = \left[\begin{array}{cccc|c} s_{11} & s_{12} & \dots & s_{1M} & y_1 \\ s_{21} & s_{22} & \dots & s_{2M} & y_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ s_{N1} & s_{N2} & \dots & s_{NM} & y_N \end{array} \right], \quad (21)$$

$$\text{where } s^1 = \begin{bmatrix} s_{11} \\ s_{12} \\ \vdots \\ s_{1M} \end{bmatrix}^T, s^2 = \begin{bmatrix} s_{21} \\ s_{22} \\ \vdots \\ s_{2M} \end{bmatrix}^T, s^3 = \begin{bmatrix} s_{31} \\ s_{32} \\ \vdots \\ s_{3M} \end{bmatrix}^T \text{ and } s^N = \begin{bmatrix} s_{N1} \\ s_{N2} \\ \vdots \\ s_{NM} \end{bmatrix}^T \text{ are the } N$$

feature vectors used to train the BTA scheme consisting of weighted soft energy reports of the M SUs. The training set, T , consists of two sub matrices, S and Y , where sub matrix $S \in \mathbb{R}^{N \times M}$ is the matrix of the weighted soft energy statistics of the users' data, while $Y \in \mathbb{R}^{N \times 1}$ are the N label (targets) values of the actual PU activity.

In this work, a total of k classifiers at the FC participate in making sensing decisions in case s^i is used as the i^{th} feature vector. The different classifiers used here try to predict a class label for the feature vector s^i , where the final output is determined using a linear combination of the label estimation predicted by different classifiers. In the linear combination, each individual term is the product of the classifiers' predicted value and the weight assigned to the classifier-predicted values. AdaBoost is a boosted classifier such that each k^{th} classifier is assigned decision weights, while taking into consideration the already known predicted ($k - 1$) classifiers as

$$e_{k-1}(s^i) = \sum_{p=1}^{k-1} \alpha_p h_p(s^i), p \in \{1, 2, \dots, k-1\}, i \in \{1, \dots, N\}, \quad (22)$$

where $h_p(s^i)$ is the prediction of the p^{th} classifier and α_p is the weight assigned to the predicted value of the p^{th} classifier.

The prediction performance of the k^{th} classifier is combined with $h_k(s^i)$ as the predicted value of the classifier and α_k as the optimum weight of the classifier to establish a better boosted classifier. To determine α_k , the process is as follows:

$$e_k(s^i) = \sum_{p=1}^{k-1} \alpha_p h_p(s^i) + \alpha_k h_k(s^i) \tag{23}$$

Similarly, (23) is written using the value from (22) as

$$e_k(s^i) = e_{k-1}(s^i) + \alpha_k h_k(s^i) \tag{24}$$

where $e_k(s^i)$ is the compound predicted value aggregated through the prediction results of the k classifiers. The aim is to form a closed form formula for α_k that assigns α_k a value such that the total prediction error is minimized. As the total prediction error in AdaBoost is equal to the sum of the negative natural exponent of $y^i e_k(s^i)$ for all training examples [48] as

$$E = \sum_{i=1}^n e^{-y^i [e_{k-1}(s^i) + \alpha_k h_k(s^i)]}, \tag{25}$$

the representation of the total prediction error, E , now takes the form below:

$$E = \sum_{i=1}^n w_k^i e^{-y^i \alpha_k h_k(s^i)} \tag{26}$$

where $w_k^i = e^{-y^i e_{k-1}(s^i)}$ is the corresponding weight in the case of a classifier number of $k > 1$. The total prediction error, E , in (26) is split into cases with correct prediction as ($y^i h_k(s^i) = 1$) and the case that leads to an incorrect prediction ($y^i h_k(s^i) = -1$) as

$$\begin{aligned} E &= \sum_{y^i=h(s^i)} w_c e^{-y^i \alpha_k h_k(s^i)} + \sum_{y^i \neq h(s^i)} w_e e^{-y^i \alpha_k h_k(s^i)}, \\ &= \sum_{y^i=h(s^i)} w_c e^{-\alpha_k} + \sum_{y^i \neq h(s^i)} w_e e^{\alpha_k}, \\ &= e^{-\alpha_k} \sum_{y^i=h_k(s^i)} w_c + e^{\alpha_k} \sum_{y^i \neq h_k(s^i)} w_e, \\ &= W_c e^{-\alpha_k} + W_e e^{\alpha_k}, \end{aligned} \tag{27}$$

where $W_c = \sum_{y^i=h_k(s^i)} w_c$ and $W_e = \sum_{y^i \neq h_k(s^i)} w_e$. The object is to minimize the loss function, E , for the chosen weak classifier, h_k , selected earlier. Thus, the total error of prediction, E , is differentiated with the classifier weight, α_k , where the minimization condition is set to zero as

$$\frac{\partial E(\alpha_k)}{\partial \alpha_k} = 0 \tag{28}$$

As in (27), the minimization of the total error with reference to α_k is the same as if we minimize $(W_c e^{-\alpha_k} + W_e e^{\alpha_k})$ with respect to α_k :

$$\frac{\partial E(\alpha_k)}{\partial \alpha_k} = -W_c e^{-\alpha_k} + W_e e^{\alpha_k} \tag{29}$$

The solution of (29) in terms of α_k is as follows:

$$\alpha_k = \frac{1}{2} \ln \left(\frac{W_c}{W_e} \right) \tag{30}$$

As $W_c = W - W_e$, with W the total sum of the weights, therefore, is

$$\alpha_k = \frac{1}{2} \ln \left(\frac{W - W_e}{W_e} \right) \quad (31)$$

Finally, the expression for weight α_k in its final form is

$$\alpha_k = \frac{1}{2} \ln \left(\frac{1 - e_m}{e_m} \right) \quad (32)$$

where $e_m = \frac{W_e}{W}$ is the weighted error rate of the weak classifier h_k .

Step 3: Global Decision Using Proposed Scheme

There are a several combination schemes that should be employed at the FC while making a global decision. These include equal gain combination (EGC) and maximum gain combination (MGC). The EGC scheme assigns equal weights to the sensing reports of all SUs as

$$G_{EGC}(i) = \begin{cases} H_1 : & \frac{1}{M} \sum_{j=1}^M s_j(i) \geq \gamma \\ H_0 : & otherwise \end{cases} \quad (33)$$

The MGC scheme at the FC observes sensing reports from different branches and assign a high weight to users with high SNR reports, while the low SNR reports receive minimum weights. Thus, strong signal branches receive amplification and branches with weak signals are further weakened as

$$G_{MGC}(i) = \begin{cases} H_1 : & \sum_{j=1}^M (e_j \times s_j(i)) \geq \gamma \\ H_0 : & otherwise \end{cases} \quad (34)$$

where $e_j = \frac{g(j)}{\sum_{j=1}^M g(j)}$.

The system is trained based on users' reported sensing data received from all SUs and the optimum coefficient vector identified using DE. The HBTA considers the following sensing observations and coefficient vectors of the DE to make the final PU channel predictions as

$$G_{BTA}(i) = \begin{cases} H_1 : & \text{HBTA}(s^i) = 1 \\ H_0 : & otherwise \end{cases}, \quad (35)$$

where HBTA refers to the trained hybrid BTA algorithm that takes a new input feature vector, s^i , to estimate the occupancy of the PU channel. G_{BTA} is a global decision of the hybridized HBTA scheme. The channel is considered occupied if $\text{HBTA}(s^i) = 1$ results in 1; otherwise, the channel is considered vacant. Detection and false alarm probabilities at the FC based on (35) are calculated as

$$\begin{aligned} P_{d-HBTA} &= \Pr\{G_{HBTA}(i) = 1 | H_1\} = \Pr\{\text{HBTA}(s^i) = 1 | H_1\}, \\ P_{f-HBTA} &= \Pr\{G_{HBTA}(i) = 1 | H_0\} = \Pr\{\text{HBTA}(s^i) = 1 | H_0\}. \end{aligned} \quad (36)$$

An flowchart diagram of the proposed HBTA scheme is shown in Figure 3.

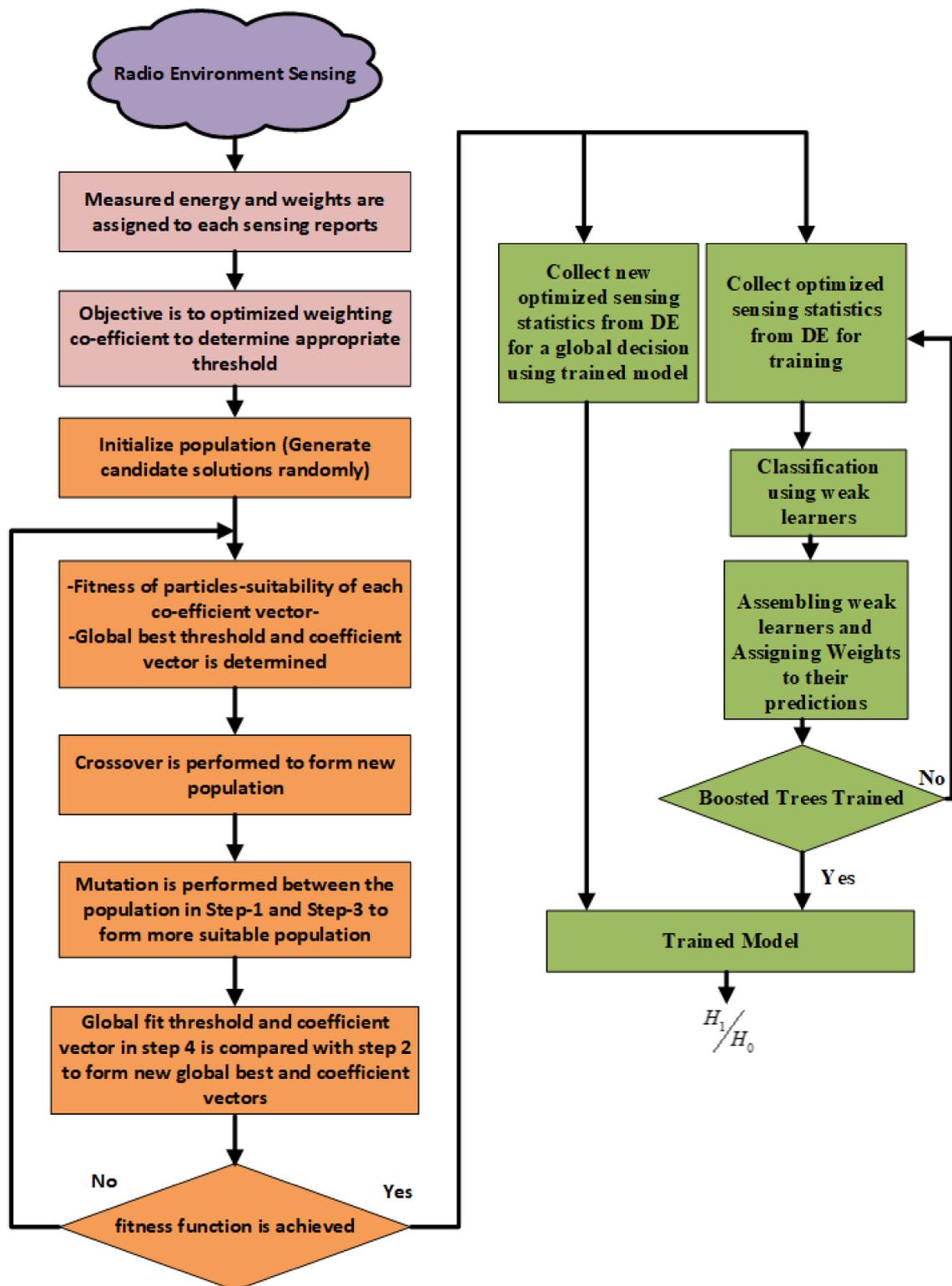


Figure 3. Flowchart diagram of the proposed HBTA scheme.

4. Simulation Results

In the simulations, the total number of SUs was kept at 14 to observe the changes in error probability concerning SNRs, sensing samples, the population size of the algorithm, and the number of iterations. The SNRs varied in the range of -20 dB to $+20$ dB, while the iterations of the algorithm changed from 50 to 110. Similarly, the population size varied in the range of 20 to 80, while the sensing samples changed from 270 to 335. The SUs were

placed in different SNRs to sense the PU channel independently. The genetic algorithm (GA) and particle swarm optimization (PSO) showed the total number of N chromosomes with M total gene bits. The maximum number of sensing iterations of the GA and PSO was kept at 50. Similarly, the GA crossover rate was randomly selected in the range of 1 to M . The performance of the proposed HBTA-based SDF algorithm was compared with the PSO, GA, DE, BTA and KNN-based SDF combination schemes.

The simulation environment was divided into six different cases. Case 1 showed the probability of error results against varying algorithm iterations. Case 2 showed the probability of error results with the contribution of varying population sizes. Similarly, Case 3 showed the error probability results with increasing sensing samples. Case 4 explored the total probability of error results versus varying SNRs at two different iteration levels. The results of the error probability at varying SNRs and with two different population sizes were explored in Case 5. Finally, Case 6 showed the error probabilities with two different sensing samples and a fixed population size, iteration number, and total number of users.

Case 1:

In this part of the simulation, the error probability was determined against an increasing number of algorithm iterations. The SNRs, algorithm population, sensing samples, and the total number of SUs were kept constant, as shown in Figures 4–6. In Figure 4, the error probability results are compared for the GA, DE, PSO, BTA, KNN, and HBTA schemes against varying iteration levels at average SNRs of -9.5 dB and -0.5 dB. The result in Figure 4 shows that the proposed HBTA scheme exhibited better sensing performance with minimum sensing error compared with the other schemes at different iteration levels in the presence of the AY category of MUs. The results in Figure 5 were collected in the presence of an AN-ANC user in CSS. These results show improved sensing performance with the proposed HBTA scheme, followed by the PSO, DE, KNN, and simple BTA schemes. The simple GA scheme showed the worst sensing performance, with high sensing error in the presence of the AN-ANC category of MUs. Similarly, the effects of an AO-AOC user in terms of misleading the FC's decision about the PU channel is investigated in Figure 6. The results in Figure 6 show the error probability against varying algorithm iterations at two different average SNRs of -0.5 dB and -9.5 dB with a fixed population size and total number of users. It is clear from the graphical illustrations in Figure 6 that the proposed HBTA scheme showed better performance for all algorithm iterations followed by the simple BTA scheme and KNN in terms of sensing. The GA and MGC-SDF schemes showed poor sensing performance with high sensing error.

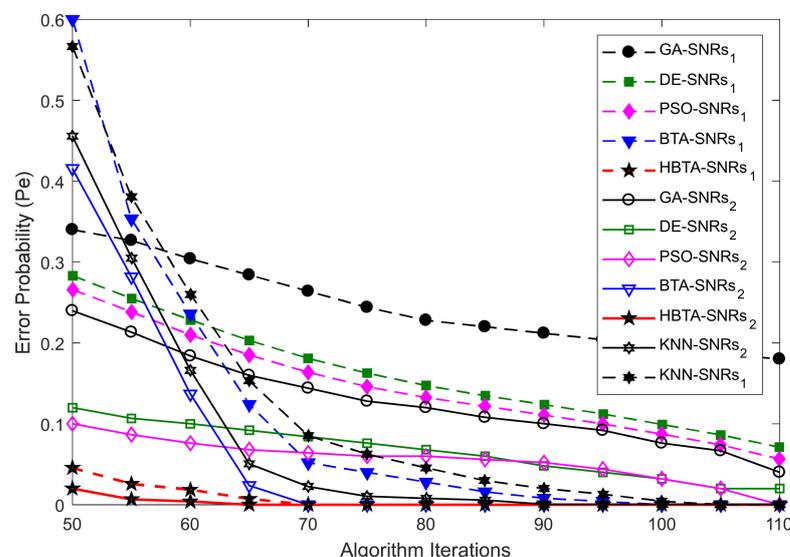


Figure 4. Error probability vs. iterations in the presence of AY-AYC users with SNRs₁ (-9.5 dB) and SNRs₂ (-0.5 dB).

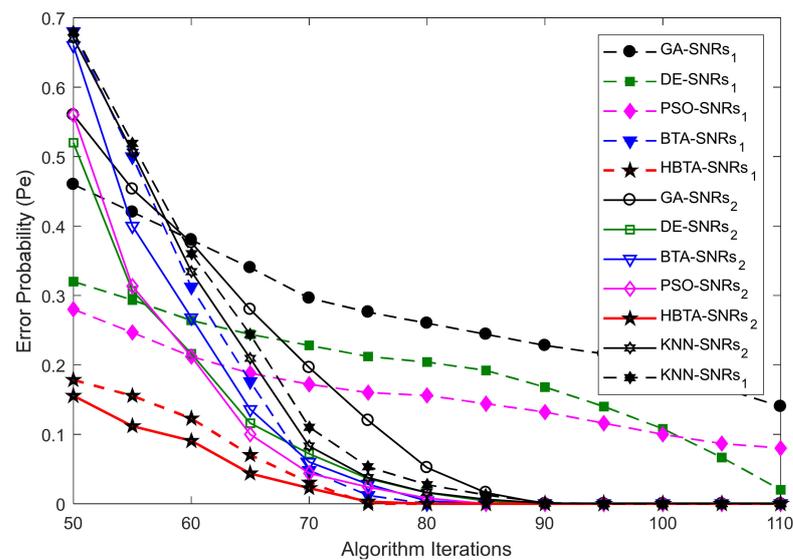


Figure 5. Error probability vs. iterations in the presence of AN-ANC users with SNRs₁ (−9.5 dB) and SNRs₂ (−0.5 dB).

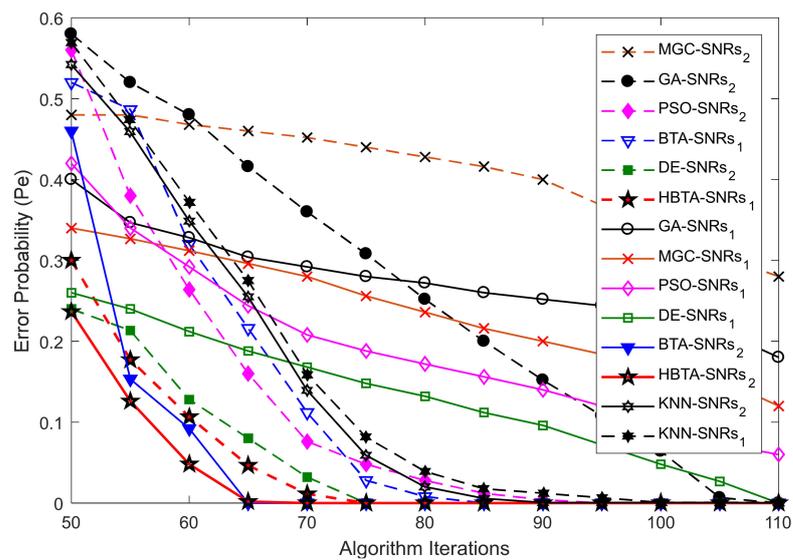


Figure 6. Error probability vs. iterations in the presence of AO-AOC users with SNRs₁ (−9.5 dB) and SNRs₂ (−0.5 dB).

Case 2:

Case 2 showed the error probability results against varying population sizes of the optimization algorithms at two different SNR levels of −9.5 dB and −0.5 dB. Here, the total number of sensing iterations was kept at 50, with 270 sensing samples and a total number of 14 SUs. The error probability results collected against the FC’s decision with the contributions of AY-AYC, AN-ANC, and AO-AOC categories of MUs are shown in Figures 7–9. The result in Figure 7 when the AY-AYC category of MUs participated in CSS shows better sensing performance for the proposed HBTA scheme with SNRs of both −9.5 dB and −0.5 dB. Similarly, the simple BTA and KNN schemes, as shown in the figure, were able to dominate PSO, DE, and GA schemes with minimum sensing, while the GA-based combination scheme was able to produce high sensing error at both SNR values. The results with the contribution of the AN-ANC category of MUs in CSS are illustrated in Figure 8. The results in Figure 8 show improved sensing results for the proposed HBTA scheme, followed by the results of the simple BTA and KNN schemes. The GA scheme in Figure 8

showed the worst sensing performance of all schemes. Finally, in Case 2, the performance of CSS was investigated with the participation of the AO-AOC category of MUs, which always negates the actual PU channel statistics. In Figure 9, the proposed HBTA scheme can be seen to show high sensing reliability with minimum sensing error as compared with all other schemes.

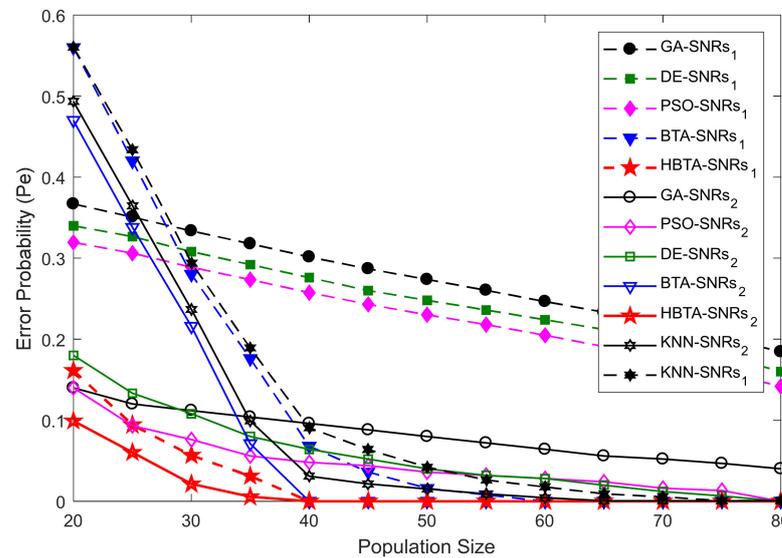


Figure 7. Error probability vs. population size in the presence of AY-AYC users with SNRs₁ (−9.5 dB) and SNRs₂ (−0.5 dB).

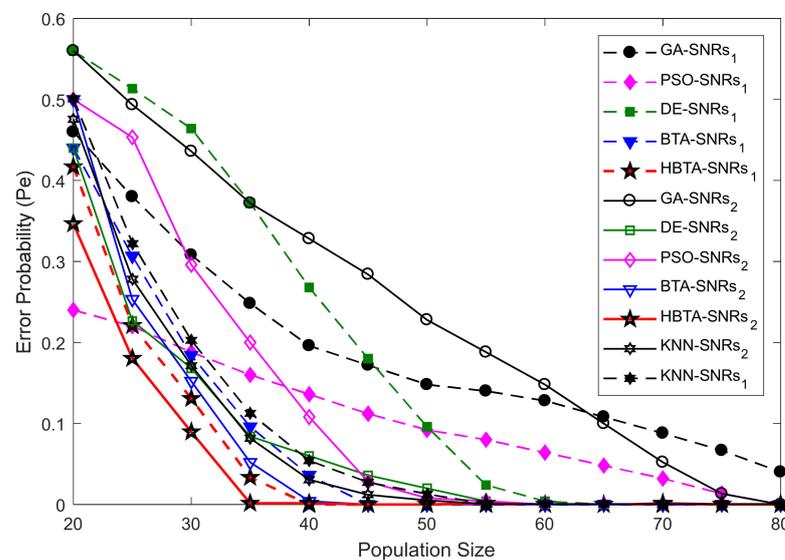


Figure 8. Error probability vs. population size in the presence of AN-ANC users with SNRs₁ (−9.5 dB) and SNRs₂ (−0.5 dB).

Case 3:

Case 3 explored the error probability results with varying sensing samples of the SUs at two different SNR values of −9.5 dB and −0.5 dB, as shown in Figures 10–12. The total number of sensing iterations was kept at 50, the population size was 30, and the total number of SUs was 14. The AY-AYC, AN-ANC, and AO-AOC MUs were differently investigated in the simulation results. The result in Figure 10 shows that the proposed HBTA dominated all other schemes with all sensing sample values and both SNR levels. The proposed HBTA scheme’s results were followed by the simple BTA and KNN schemes, which had initially high sensing error results, but as the sensing sample increased, they could outperform the

PSO, DE, GA, and MGC schemes. The result in Figure 11 shows the error probability results when the AN-ANC category of MUs participated in reporting their location decisions to the FC. Similarly, the DE combination scheme in this part could dominate the simple BTA, KNN, PSO, and GA combination schemes. The GA combination schemes in this part showed a high sensing error, leading to minimum sensing performance. Figure 12 shows the error probability results against increasing sensing samples at two different SNR values of -9.5 dB and -0.5 dB. The graphical results in the figure were collected with the presence of the AO-AOC category of MUs in CSS, with improved sensing performance shown by the proposed HBTA scheme in comparison with all other schemes, while the GA combination scheme can be seen to have exhibited the worst sensing reliability in Figure 12. Thus, it is concluded from the various graphical results in Case 2 that the proposed HBTA scheme has the best sensing reliability in producing improved sensing results as compared with the KNN, simple BTA, GA, PSO, and DE optimization schemes.

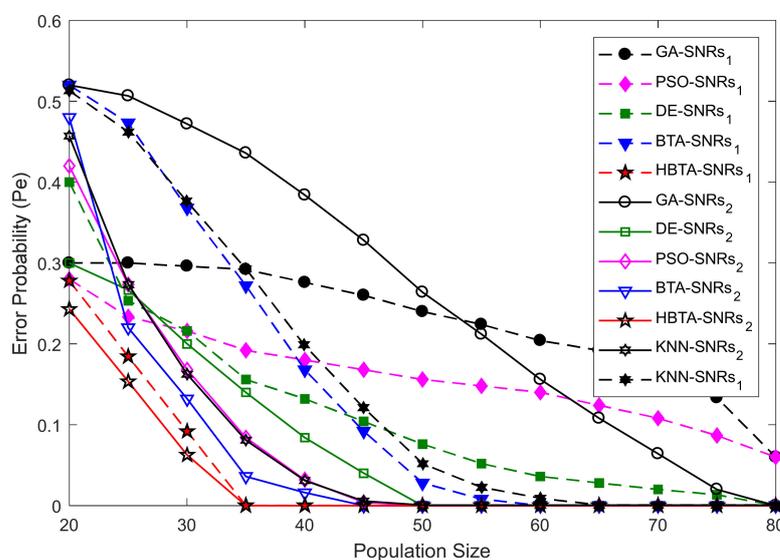


Figure 9. Error probability vs. population size in the presence of AO-AOC users with SNRs₁ (-9.5 dB) and SNRs₂ (-0.5 dB).

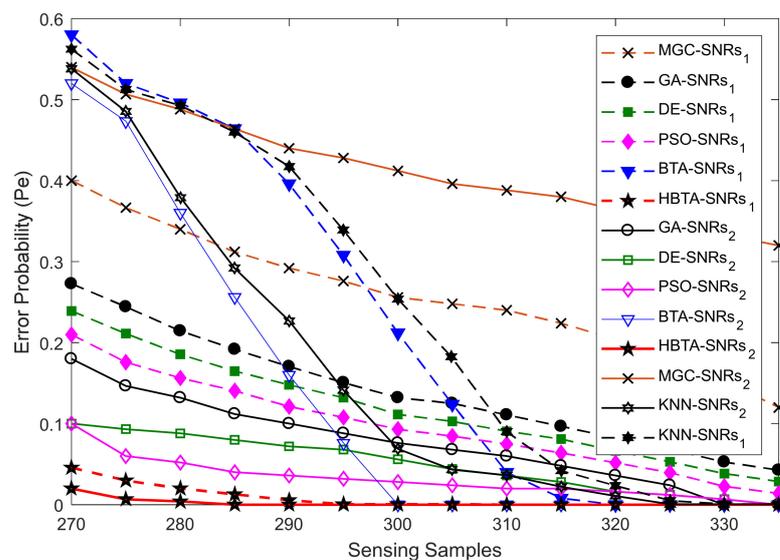


Figure 10. Error probability vs. sensing samples in the presence of AY-AYC users with SNRs₁ (-9.5 dB) and SNRs₂ (-0.5 dB).

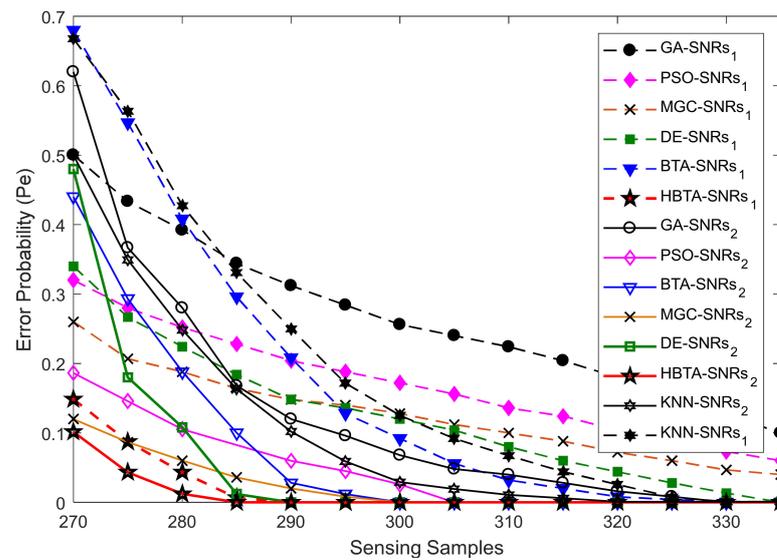


Figure 11. Error probability vs. sensing samples in the presence of AN-ANC users with SNRs₁ (−9.5 dB) and SNRs₂ (−0.5 dB).

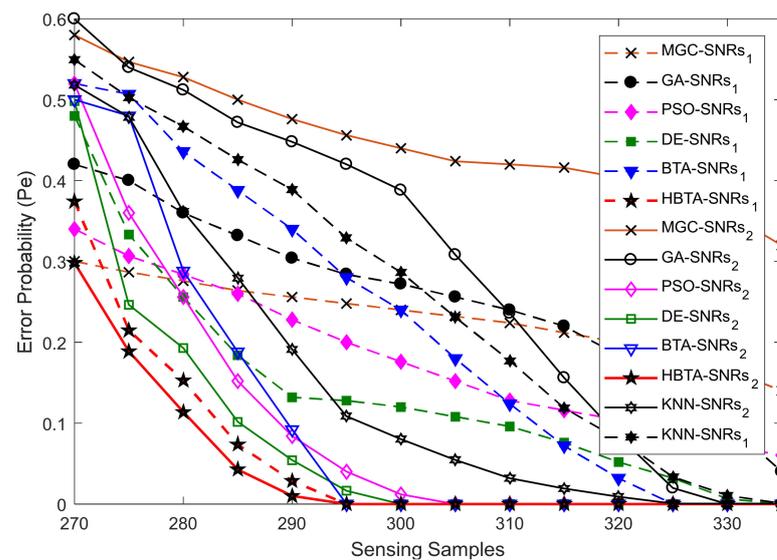


Figure 12. Error probability vs. sensing samples in the presence of AO-AOC users with SNRs₁ (−9.5 dB) and SNRs₂ (−0.5 dB).

Case 4:

In this portion of the simulation results, error probabilities were collected with increasing SNR values at two different numbers of algorithm iterations: 60 and 85. Here, the SU sensing samples were fixed at 270 with an algorithm population size of 20 and total number of SUs of 14.

Figure 13 shows the error probability results of the proposed approach and all other schemes with the contribution of AY-AYC MUs. The results in Figure 13 show improved sensing results for the proposed HBTA scheme at both algorithm iteration levels. It is visible from the graphical illustrations that the DE-based combination scheme resulted in the best sensing decision with minimum sensing error in comparison with PSO, GA, KNN, and the simple BTA and MGC schemes, with the highest error probability results obtained for the MGC scheme. The results in Figure 14 show that AN-ANC user effects were strongly overwhelmed by the proposed scheme while making a global decision; therefore, the proposed HBTA scheme resulted in the minimum error probability results in

comparison with all other schemes. In this part of the simulation, the simple BTA scheme was able to surpass the KNN, MGC, DE, PSO, and GA combination schemes when the SNRs were increased beyond certain limits, as shown in the figure. The GA scheme was able to reduce the error probability to a minimum by a sufficient increase in the SNR values. The proposed HBTA scheme was capable of keeping error probability at minimum with the contribution of AO-AOC users in Figure 15, in a similar manner to the AN-ANC users who participated in the CSS system.

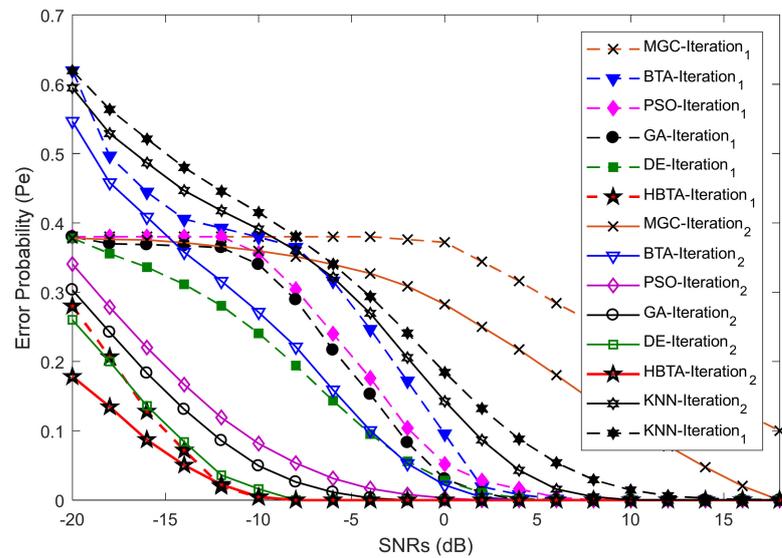


Figure 13. Error probability vs. SNRs in the presence of AY-AYC users with sensing iterations₁ (60) and iterations₂ (85).

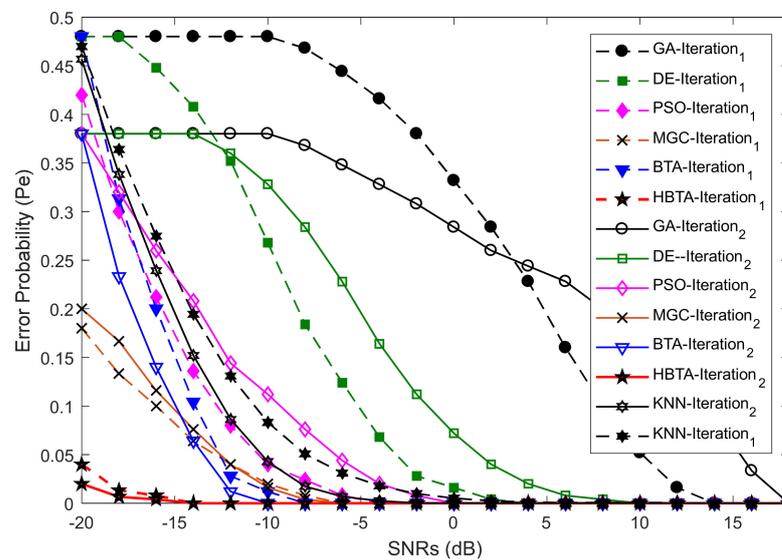


Figure 14. Error probability vs. SNRs in the presence of AN-ANC users with sensing iterations₁ (60) and iterations₂ (85).

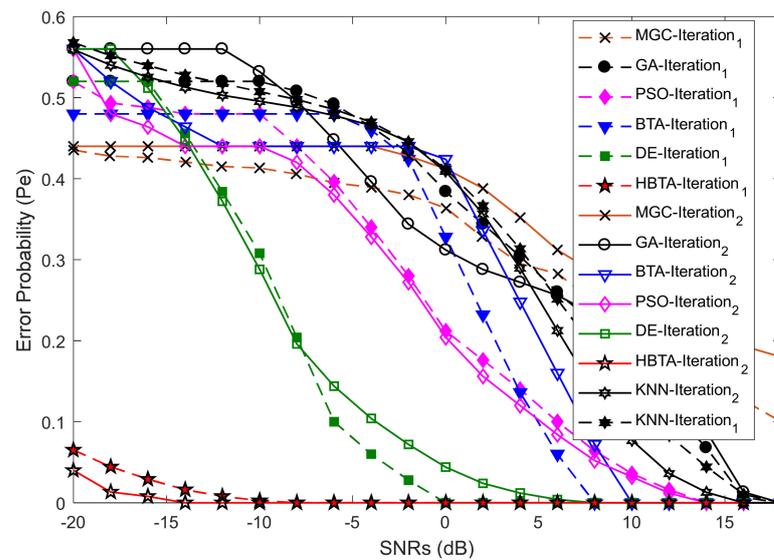


Figure 15. Error probability vs. SNRs in the presence of AO-AOC users with sensing iterations₁ (60) and iterations₂ (85).

Case 5:

Case 5 explored the error probability results against increasing SNR values with two different algorithm population sizes: 30 and 55. The total number of sensing samples for the SUs was selected as 270, with 50 algorithm iterations, as shown in Figures 16–18. These results were investigated in the presence of AY-AYC, AN-ANC, and AO-AOC categories of MUs. In the first part of Case 4, the participation of AY was investigated in CSS to obtain the error probability results at different levels of SNRs. Figure 16 shows that satisfactory sensing results were achieved by the proposed HBTA, DE, and GA schemes. The simple MGC and PSO algorithm results were the worst of all investigated schemes. The results achieved with the contribution of AN-ANC users that always negate the actual states of the PU channel and result in constant channel availability are shown in Figure 17. The result shows the dominant performance of the proposed HBTA scheme. The third part of Case 5 explored the results obtained from the proposed and existing schemes with the AO-AOC category of MUs that negate the actual PU status by reporting high-energy states when a PU is absent and reporting low energy states when the PU is available in the given spectrum. The results in Figure 18 clarify the superiority of the proposed scheme to obtain a low sensing error at low levels of SNRs. It is also clear from the figure that simple BTA and KNN schemes performed better than the proposed scheme. The DE algorithm showed better sensing results in comparison with the PSO, GA, and MGC combination schemes. It is also visible from this part of the simulation results that the global decisions made using MGC and GA schemes exhibited minimum reliability with a high sensing error at both population levels.

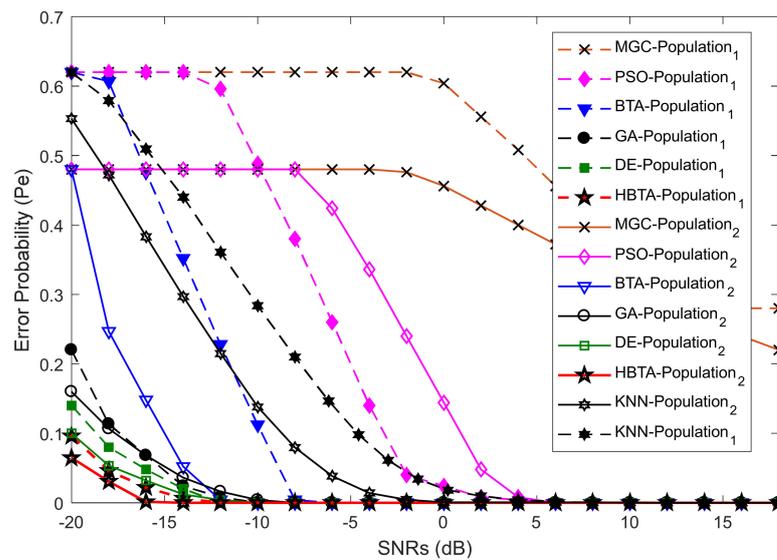


Figure 16. Error probability vs. SNRs in the presence of AY-AYC users with population₁ (30) and population₂ (55).

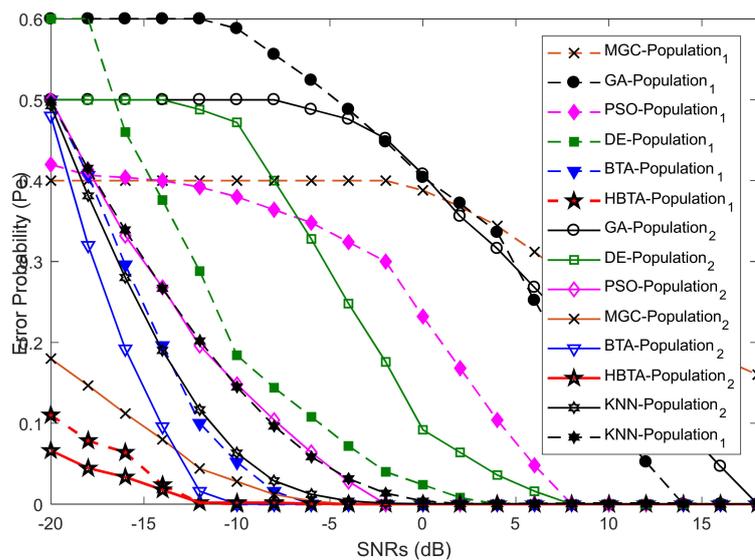


Figure 17. Error probability vs. SNRs in the presence of AN-ANC users with population₁ (30) and population₂ (55).

Case 6:

Finally, the error probability results were collected at varying SNRs, and two different levels of sensing samples were employed by the SUs: 280 and 305. To obtain the results, error probabilities were determined with the participation of AY-AYC, AN-ANC, and AO-AOC categories of Mus, as shown in Figures 19–21. The error probability results in Figure 19 when AY-AYC participated in the CSS show improved sensing performance with low sensing error results for the proposed HBTA scheme. The result of the proposed HBTA scheme was followed by the DE and GA schemes, which showed improved sensing performance in comparison with the simple BTA, KNN, PSO and MGC schemes. The MGC scheme employed at the FC to make a global decision about the PU channel showed the highest sensing error of all schemes at different levels of SNRs. In the second part of Case 6, when AN-ANC users were allowed to participate in CSS, is shown in Figure 20. The figure shows that better sensing results with minimum sensing error were achieved by the proposed scheme in comparison with all other schemes. The MGC scheme results

were reliable, producing minimum sensing error, as compared with the DE, PSO, and GA combination schemes. These results were followed by the simple BTA and KNN schemes, while the GA optimization scheme results were the worst of all schemes. In the third part of Case 6, the proposed HBTA scheme was compared with all other schemes with the participation of the AO-AOC category of MU. The proposed HBTA scheme in this part greatly outperformed all other schemes by producing minimum sensing error results. It is also clear from the results in Figure 21 that the simple BTA and KNN schemes in this part of the simulation showed improved sensing results as compared with GA, DE, PSO, and MGC combination schemes. Similarly, the MGC combination scheme was observed to have the worst sensing performance with the participation of the AO-AOC category of MUs.

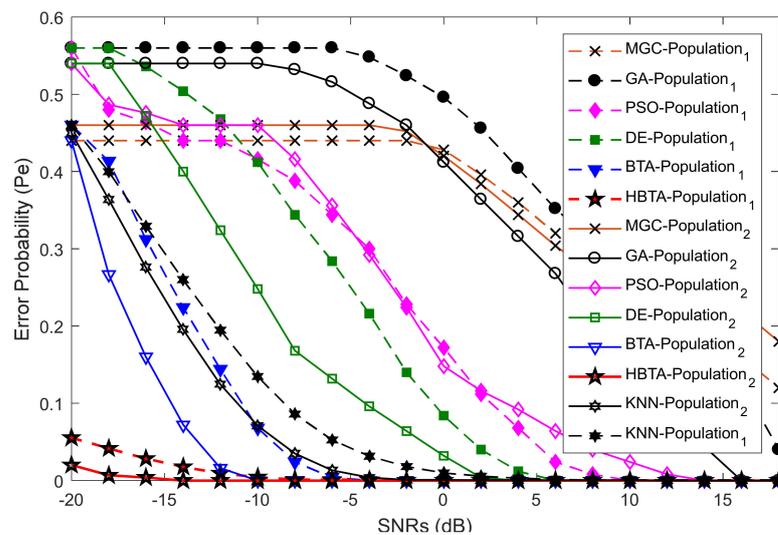


Figure 18. Error probability vs. SNRs in the presence of AO-AOC users with population₁ (30) and population₂ (55).

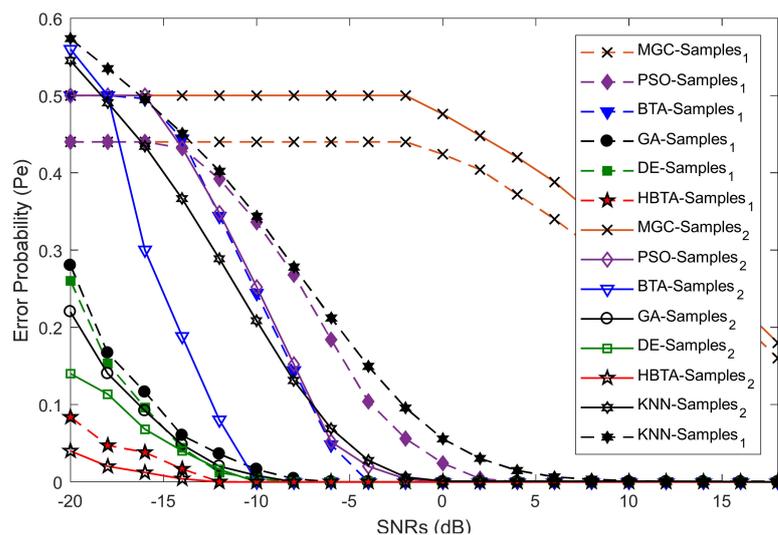


Figure 19. Error probability vs. SNRs in the presence of AY-AYC users with sensing samples₁ (280) and samples₂ (305).

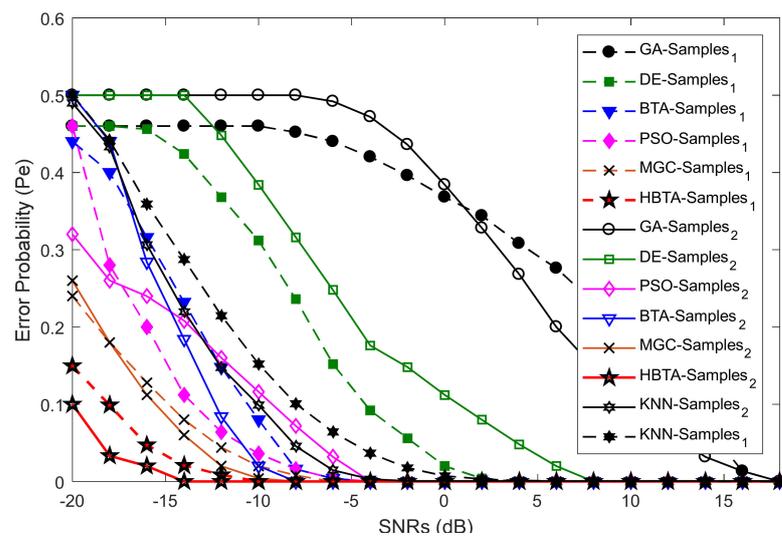


Figure 20. Error probability vs. SNRs in the presence of AN-ANC users with sensing samples₁ (280) and samples₂ (305).

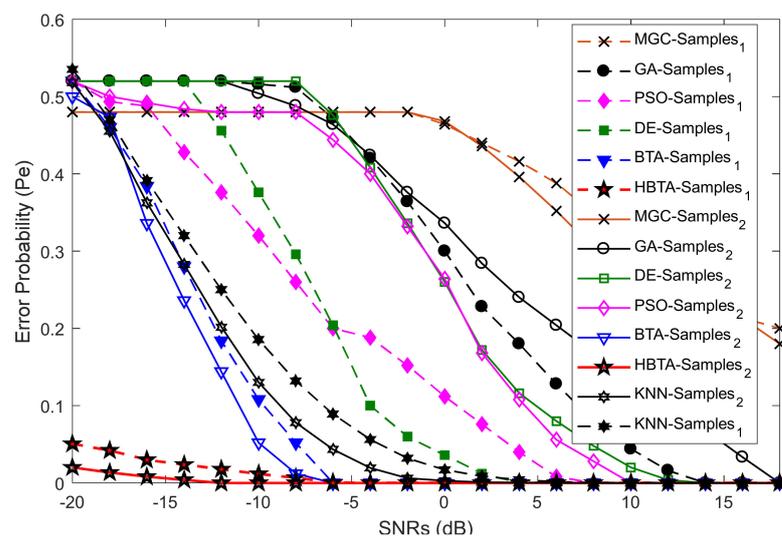


Figure 21. Error probability vs. SNRs in the presence of AO-AOC users with sensing samples₁ (280) and samples₂ (305).

5. Conclusions and Future Work

The sensing reliability of SUs leads to challenges in the Rayleigh fading environment. The proposed hybrid scheme in this paper combines the DE optimization scheme with the ML-based BTA algorithm with the aim of augmenting the sensing performance of CSS. The simulation results were obtained considering a variety of MU categories in CSS. To evaluate the effectiveness of the proposed scheme, sensing error was evaluated for multiple cases based on variations in SNRs, algorithm iterations, algorithm population, and sensing samples in the presence of AY-AYC, AN-ANC, and AO-AOC. The results validate the superiority of the proposed HBTA scheme in comparison with several other existing schemes.

To extend this work in the future, we intend to compare the proposed HBTA scheme with deep learning algorithms, such as the recurrent neural network (RNN). Furthermore, we plan to reduce sensing costs by reducing the sensing time and energy consumption while utilizing ML and deep learning techniques.

Author Contributions: Conceptualization, N.G.; data curation, N.G.; formal analysis, S.M.K., S.A., M.S.K. and J.K.; investigation, N.G.; methodology, N.G.; project administration, S.M.K. and J.K.; resources, S.M.K. and J.K.; software, N.G.; supervision, S.M.K. and J.K.; validation, N.G.; visualization, N.G.; writing—original draft, N.G., S.A. and M.S.K.; writing—review and editing, N.G., S.M.K. and J.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded and supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2016R1C1B1014069) and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MIST) (No. 2021R1A2C1013150).

Data Availability Statement: The data used to support the findings of this study are included within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Haykin, S. Cognitive Radio: Brain-Empowered Wireless Communications. *IEEE J. Sel. Areas Commun.* **2005**, *23*, 201–220. [[CrossRef](#)]
- Ghasemi, E.; Sousa, S. Spectrum Sensing in Cognitive Radio Networks: Requirements, Challenges and Design Trade-Offs. *Commun. Mag. IEEE* **2008**, *46*, 32–39. [[CrossRef](#)]
- Giupponi, L.; Galindo-Serrano, A.; Blasco, P.; Dohler, M. Cognitive Networks: An Emerging Paradigm for Dynamic Spectrum Management [Dynamic Spectrum Management]. *IEEE Wirel. Commun.* **2010**, *17*, 47–54. [[CrossRef](#)]
- Awin, F.; Abdel-Raheem, E.; Tepe, K. Blind Spectrum Sensing Approaches for Interweaved Cognitive Radio System: A Tutorial and Short Course. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 238–259. [[CrossRef](#)]
- Awin, F.A.; Alginahi, Y.M.; Abdel-Raheem, E.; Tepe, K. Technical Issues on Cognitive Radio-Based Internet of Things Systems: A Survey. *IEEE Access* **2019**, *7*, 97887–97908. [[CrossRef](#)]
- Teguig, D.; Scheers, B.; le Nir, V. Data Fusion Schemes for Cooperative Spectrum Sensing in Cognitive Radio Networks. In Proceedings of the IEEE Military Communications and Information Systems Conference (MCC), Gdansk, Poland, 8–9 October 2012.
- Gul, N.; Khan, M.S.; Kim, J.; Kim, S.M. Robust Spectrum Sensing via Double-Sided Neighbor Distance Based on Genetic Algorithm in Cognitive Radio Networks. *Mob. Inf. Syst.* **2020**, *2020*, 8876824. [[CrossRef](#)]
- Gul, N.; Khan, M.S.; Kim, S.M.; St-Hilaire, M.; Ullah, I.; Kim, J. Particle Swarm Optimization in the Presence of Malicious Users in Cognitive IoT Networks with Data. *Sci. Program.* **2020**, *2020*, 8844083. [[CrossRef](#)]
- Gul, N.; Qureshi, I.M.; Akbar, S.; Kamran, M.; Rasool, I. One-to-Many Relationship Based Kullback Leibler Divergence against Malicious Users in Cooperative Spectrum Sensing. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 3153915. [[CrossRef](#)]
- Sharifi, A.A.; Niya, J.M. Securing Collaborative Spectrum Sensing against Malicious Attackers in Cognitive Radio Networks. *Wirel. Pers. Commun.* **2016**, *90*, 75–91. [[CrossRef](#)]
- Gul, N.; Qureshi, I.M.; Omar, A.; Elahi, A.; Khan, M.S. History Based Forward and Feedback Mechanism in Cooperative Spectrum Sensing Including Malicious Users in Cognitive Radio Network. *PLoS ONE* **2017**, *12*, e0183387. [[CrossRef](#)]
- Mehboob, U.; Qadir, J.; Ali, S.; Vasilakos, A. Genetic Algorithms in Wireless Networking: Techniques, Applications, and Issues. *Soft Comput.* **2016**, *20*, 2467–2501. [[CrossRef](#)]
- Khan, M.S.; Gul, N.; Kim, J.; Qureshi, I.M.; Kim, S.M. A Genetic Algorithm-Based Soft Decision Fusion Scheme in Cognitive IoT Networks with Malicious Users. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 2509081. [[CrossRef](#)]
- Zhang, L.; Ding, G.; Wu, Q.; Zou, Y.; Han, Z.; Wang, J. Byzantine Attack and Defense in Cognitive Radio Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1342–1363. [[CrossRef](#)]
- Sharifi, A.A.; Sharifi, M.; Musevi Niya, M.J. Collaborative Spectrum Sensing under Primary User Emulation Attack in Cognitive Radio Networks. *IETE J. Res.* **2016**, *62*, 205–211. [[CrossRef](#)]
- Abrardo, A.; Barni, M.; Kallas, K.; Tondi, B. Decision Fusion with Unbalanced Priors under Synchronized Byzantine Attacks: A Message-Passing Approach. In Proceedings of the 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Honolulu, HI, USA, 12–15 November 2018; pp. 1160–1167.
- Gupta, N.; Dhurandher, S.K.; Sehgal, A. A Contract Theory Approach-Based Scheme to Encourage Secondary Users for Cooperative Sensing in Cognitive Radio Networks. *IEEE Syst. J.* **2019**, *14*, 2400–2410. [[CrossRef](#)]
- Cao, X.; Lai, L. Distributed Gradient Descent Algorithm Robust to an Arbitrary Number of Byzantine Attackers. *IEEE Trans. Signal. Process.* **2019**, *67*, 5850–5864. [[CrossRef](#)]
- Zhang, L.; Ding, G. Detecting Abnormal Power Emission for Orderly Spectrum Usage B. Generalized Likelihood Ratio Detector with Unknown. *IEEE Trans. Veh. Technol.* **2019**, *68*, 1989–1992. [[CrossRef](#)]
- Jana, S.; Zeng, K.; Mohapatra, P. Trusted Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks. In *2012 Proceedings IEEE INFOCOM, Orlando, FL, USA, 25–30 March 2012*; IEEE: Piscataway, NJ, USA, 2012; pp. 2621–2625. [[CrossRef](#)]
- Lee, S.; Zhang, Y.; Yoon, S.; Song, I. Order Statistics and Recursive Updating with Aging Factor for Cooperative Cognitive Radio Networks under SSDF Attacks. *ICT Express* **2020**, *6*, 3–6. [[CrossRef](#)]

22. Sun, Z.; Xu, Z.; Hammad, M.Z.; Ning, X.; Wang, Q.; Guo, L. Defending against Massive SSDF Attacks from a Novel Perspective of Honest Secondary Users. *IEEE Commun. Lett.* **2019**, *23*, 1696–1699. [[CrossRef](#)]
23. Iqbal, Z.; Nooshabadi, S.; Jadi, K.; Ghasemi, A. Sensor Cooperation and Decision Fusion to Improve Detection in Cognitive Radio Spectrum Sensing. In Proceedings of the 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON 2018), New York, NY, USA, 8–10 November 2018; pp. 276–281. [[CrossRef](#)]
24. Grissa, M.; Yavuz, A.A. Preserving the Location Privacy of Secondary Users in Cooperative Spectrum Sensing. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 418–431. [[CrossRef](#)]
25. Grissa, M.; Yavuz, A.; Hamdaoui, B. An Efficient Technique for Protecting Location Privacy of Cooperative Spectrum Sensing Users. In Proceedings of the 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPs), San Francisco, CA, USA, 10–14 April 2016; pp. 915–920.
26. Du, H.; Fu, S.; Chu, H. Credibility-Based Defense SSDF Attacks Scheme for the Expulsion of Malicious Users in Cognitive Radio. *Int. J. Hybrid Inf. Technol.* **2015**, *8*, 269–280. [[CrossRef](#)]
27. Sharifi, A.A. An Effective and Optimal Fusion Rule in the Presence of Probabilistic Spectrum Sensing Data Falsification Attack. *J. Commun. Eng.* **2019**, *8*, 78–92.
28. Chen, H.; Zhou, M.; Xie, L.; Li, J. Cooperative Spectrum Sensing with M-Ary Quantized Data in Cognitive Radio Networks under SSDF Attacks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 5244–5257. [[CrossRef](#)]
29. Feng, J.; Zhang, M.; Xiao, Y.; Yue, H. Securing Cooperative Spectrum Sensing against Collusive SSDF Attack Using XOR Distance Analysis in Cognitive Radio Networks. *Sensors* **2018**, *18*, 370. [[CrossRef](#)]
30. Fu, Y.; He, Z. Bayesian-Inference-Based Sliding Window Trust Model against Probabilistic SSDF Attack. *IEEE Syst. J.* **2019**, *14*, 1764–1775.
31. Zhao, F.; Li, S.; Feng, J. Securing Cooperative Spectrum Sensing against DC-SSDF Attack Using Trust Fluctuation Clustering Analysis in Cognitive Radio Networks. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 3174304. [[CrossRef](#)]
32. Wan, R.; Ding, L.; Xiong, N.; Zhou, X. Mitigation Strategy against Spectrum- Sensing Data Falsification Attack in Cognitive Radio Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1–12. [[CrossRef](#)]
33. Lee, W.; Kim, M.; Cho, D. Deep Cooperative Sensing: Cooperative Spectrum Sensing Based on Convolutional Neural Networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 3005–3009. [[CrossRef](#)]
34. Ezziama, E.; Ahmed, S.; Ahmed, S.; Awin, F.; Tepe, A.K. Detection of Adversary Nodes in Machine-To-Machine Communication Using Machine Learning-Based Trust Model. In Proceedings of the IEEE International Symposium on Signal. Processing and Information Technology, Ajman, United Arab Emirates, 10–12 December 2019.
35. Sucasas, V.; Mantas, G.; Althunibat, S.; Ortega, J.F.M. Editorial: Security and Privacy Protection for Mobile Applications and Platforms. *Mob. Netw. Appl.* **2020**, *25*, 151–152. [[CrossRef](#)]
36. Oksanen, J.; Lundén, J.; Koivunen, V. Reinforcement Learning Based Sensing Policy Optimization for Energy Efficient Cognitive Radio Networks. *Neurocomputing* **2011**, *80*, 102–110. [[CrossRef](#)]
37. Liu, H.; Zhu, X.; Fujii, T. Ensemble Deep Learning Based Cooperative Spectrum Sensing with Semi-soft Stacking Fusion Center. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–6.
38. Opitz, D.; Maclin, R. Popular Ensemble Methods: An Empirical Study. *J. Artif. Intell. Res.* **1999**, *11*, 169–198. [[CrossRef](#)]
39. Zhou, Z.H. *Introduction in Ensemble Methods: Foundations and Algorithms*; CRC Press: Boca Raton, FL, USA, 2012; Chapter 1; pp. 1–20.
40. Moeyersons, J.; Varon, C.; Testelmans, D.; Buyse, B.; van Hufel, S. ECG Artefact Detection Using Ensemble Decision Trees. In Proceedings of the Computing in Cardiology, Rennes, France, 24–27 September 2017; pp. 1–4.
41. Lee, H.; Kim, S. Decision Tree Ensemble Classifiers for Anomalous Propagation Echo Detection. In Proceedings of the 8th Joint International Conference on Soft Computing and Intelligent Systems and 17th International Symposium on Advanced Intelligent Systems, SCIS-ISIS'16, Sapporo, Japan, 25–28 August 2016; pp. 391–396.
42. Madani, S.S.; Abbaspour, A.; Beiraghi, M.; Dehkordi, P.Z.; Ranjbar, A.M. Islanding Detection for PV and DFIG Using Decision Tree and Adaboost Algorithm. In Proceedings of the 3rd IEEE PES Innovative Smart Grid Technologies Europe, ISGT Europe'12, Berlin, Germany, 14–17 October 2012; pp. 1–8.
43. Gul, N.; Qureshi, I.M.; Khan, M.S.; Elahi, A.; Akbar, S. Differential Evolution Based Reliable Cooperative Spectrum Sensing in the Presence of Malicious Users. *Wirel. Pers. Commun.* **2020**, *114*, 123–147. [[CrossRef](#)]
44. Gul, N.; Khan, M.S.; Kim, S.M.; Kim, J.; Elahi, A.; Khalil, Z. Boosted Trees Algorithm as Reliable Spectrum Sensing Scheme in the Presence of Malicious Users. *Electronics* **2020**, *9*, 1038. [[CrossRef](#)]
45. Wang, H.; Xu, Y.; Su, X.; Wang, J. Cooperative Spectrum Sensing with Wavelet Denoising in Cognitive Radio. In Proceedings of the 2010 IEEE 71st Vehicular Technology Conference, Taipei, Taiwan, 16–19 May 2010; Volume 2, pp. 2–6.
46. Ma, J.; Zhao, G.; Li, Y. Soft Combination and Detection for Cooperative Spectrum Sensing in Cognitive Radio Networks. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 4502–4507. [[CrossRef](#)]
47. Storn, R.; Price, K.V. *Differential Evolution: A Simple and Efficient Adaptive Scheme for Global Optimization Over Continuous Spaces*; Technical Report; International Computer Science Institute: Berkeley, CA, USA, March 1995.
48. Ahmad, H.B. Ensemble Classifier Based Spectrum Sensing in Cognitive Radio Networks. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 9250562. [[CrossRef](#)]