



Research Article

Particle Swarm Optimization in the Presence of Malicious Users in Cognitive IoT Networks with Data

Noor Gul,¹ Muhammad Sajjad Khan ^{1,2} Su Min Kim,² Marc St-Hilaire,³ Ihsan Ullah,⁴ and Junsu Kim ²

¹Department of Electrical Engineering, Faculty of Engineering and Technology, International Islamic University, Islamabad 44000, Pakistan

²Department of Electronics Engineering, Korea Polytechnic University, 237 Sangidaehak-ro, Siheung-si, Gyeonggi-do 15073, Republic of Korea

³School of Information Technology and Department of Systems and Computer Engineering Carleton University, Ottawa, ON, Canada

⁴Department of Computer Science Engineering, Korea University of Technology, Cheonan, Republic of Korea

Correspondence should be addressed to Junsu Kim; junsukim@kpu.ac.kr

Received 28 September 2020; Revised 28 October 2020; Accepted 30 October 2020; Published 11 November 2020

Academic Editor: Habib Ullah Khan

Copyright © 2020 Noor Gul et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the increasing applications in the domains of ubiquitous and context-aware computing, Internet of Things (IoT) is gaining importance. The study to efficiently exploit and manage a spectrum resources for industrial IoT (IIoT) applications is currently in the interest of research community. As increasing number of IIoT devices is heading towards the future-connected society with the cost of high system complexity, to meet the growing demands of wireless communication in future, cognitive IoT (CIoT) technology is considered as a choice. Reliable detection of the vacant spectrum holes is a vital task in the CIoT network with data. However, the performance of spectrum sensing severely degraded with the existence of malicious users (MUs) which falsifies the sensing results by reporting false data to the fusion center (FC). In this paper, we focus on the use of particle swarm optimization (PSO) to safeguard the cooperative spectrum sensing (CSS) from the negative effects caused by the MUs. The effectiveness of the proposed scheme is verified numerically in various scenarios with different types of MUs through analysis and simulations.

1. Introduction

Wireless communication networks have gained tremendous progress in the last decade to meet the growth in application devices from 1G to 4G Long-Term Evolution (LTE) advanced wireless networks [1]. These generations have played their roles in order to achieve improved data rate, high reliability, minimum latency and more things on the way. Wireless communication is facing the challenge of how to connect wireless devices with each other at anytime and anywhere. In the evolution process, 5G is expected to offer significant contributions towards spectrum management, public safety consideration, energy utilization efficiency, improved data rate, and low latency [2–4]. Since the 5G wireless communication technology is on the

horizon in combination with IoT consideration as its center stage, IoT devices will perform a central role in the formation of a 5G network paradigm [5].

The term IoT introduced and mentioned by Ashton for the first time is a technological revolution that brings heterogeneous networks under the common umbrella of IoT [6]. This technological revolution represents the future of connectivity and reachability. Unlike the traditional networks of embedded systems, IoT is capable of interconnecting heterogeneous devices, having diverse functionalities, produced by different manufacturers [7]. IoT has changed the landscape of numerous industries tremendously ever since it has been introduced [8]. It is a promising subject of the social, technical, and economic implications that will hold a strong and meaningful impact

on our daily life in the near future. IoT is going to help in the improvised logistic learning, automation, e-health-care units, and intelligent transportation systems [8, 9]. The functionality of IoT is extended using mobile computing in the healthcare environment to bring massive healthcare in the form of mobile healthcare in [10]. Similarly, the fog-based IoT healthcare framework proposed to minimize energy consumption of the fog sensing nodes along with network delay in [11]. The major focus is this paradigm from a technological perspective is to enhance computation, communication, and connectivity procedures. However, connectivity and radio spectrum management are more crucial and challenging responsibilities in front of the research community. In the near future, over 50 billion wireless devices have to be interconnected that may demand for a large number of spectrum resources [12]. In [13], the authors argued on the importance and employment of cognitive capabilities in IoT with the objective that without implication of the cognitive capability, it is similar to an awkward stegosaurus with all brawn and no brains. A dozen of wireless communication technologies are already in use such as WiFi, Bluetooth, LTE, earlier 3G standards, ZigBee, Near Field Communication (NFC), and different satellite services. Therefore, the rapid growth in wireless communications demands for the new wireless services in both the used and unused part of the radio spectrum [14]. Spectrum sharing in 5.4 GHz band has already been legalized by the federal communication commission (FCC), where devices sense the existence of military radars before accessing the channel [15]. Cognitive radio (CR) is an intelligent wireless communication technology with efficient radio spectrum utilization abilities trying to learn and adjust its internal states according to environment [16]. The primary users (PUs) are able to transmit any time with no restrictions while the secondary users (SUs) gain the benefit of the spectrum access only when it is declared to be free [17].

In CR networks (CRNs), an incorrect detection of the PU results in false alarm and reduces the SUs' opportunities to access the spectrum. Similarly, any misdetection of the occupied PU channel produces interference to the PU by the secondary access. Masking of the optimal interference subcarrier is obtained based on genetic algorithm (GA) to suppress intercarrier interference caused by the SUs to the PU channel [18]. In [19], a side-lobe reduction scheme using a generalized side-lobe canceller combined with GA and differential evolution is proposed to minimize the impact of the interference.

Spectrum sensing with single SU is facing a number of limitations such as the limitations with the energy constraints, shadowing, fading, and hidden terminal problems [20]. On the other hand, in the cooperative spectrum sensing (CSS), the sensing problems faced by the single user is mitigated by allowing the cooperation among the multiple SUs to share their sensing results to make a global decision on the existence of PU [21]. In the CSS, the SUs forward their local decisions to the fusion center (FC) to make a global decision to infer the absence or presence of the PU [21].

However, the existence of malicious users (MUs) in the CSS severely reduces effectiveness of cooperation. Therefore,

proper detection and exclusion of the MUs' information are extremely critical [22]. Significant investigations have been carried out to make the CSS robust to the attack of MUs. The MU transfers erroneous sensing reports to the FC, in order to create confusion about the spectrum conditions. Such attacks are referred to as spectrum sensing data falsification (SSDF) attack [23]. A systematic review is conducted in [24] to analyze the security problem of IoT devices and to counter various security challenges using mobile computing.

Boosted trees algorithm (BTA) is proposed in [25] that uses the AdaBoost ensemble method to make results of the cooperative decision at the FC reliability in the presence of abnormal sensing data. The work in [26] suggested the use of differential evolution (DE) to identify the weighting coefficient vector against user sensing reports. This strengthens the reports of normal sensing users with high weights compared to the abnormal sensing users. An enhanced CSS scheme is determined at the FC using flower pollination algorithm (FPA) in [27]. Similarly, performance comparison is made at the FC between different hard combination schemes in the presence of abnormal reports of the lazy MU in [28]. The work in [29] reduces the effect of the false sensing reports before making the final decision at the FC using modified double-sided neighbor distance algorithm with a GA optimization scheme. A machine learning scheme such as support vector machine (SVM) in [30] effectively classified the normal sensing users and different categories of MUs to help FC decision. In [31], malicious sensing nodes with false sensing reports are quantified in the simulation environment of the Poisson point process. As the MUs do not share honest sensing reports with the FC, a contract theory approach with incentive design scheme is proposed in [32] to reward honest SUs and to strengthen their cooperation. The normal SUs discussed in [33] follow the FC recommendation as a final decision of the PU channel and use their local sensing decisions to guarantee the CSS reliability. A Bayesian-inference scheme is proposed in [34] to identify and countereffects of the individual and collaborative SSDF attackers using a sliding window trust model.

A robust scheme which deals with always yes malicious users (AYMUs) is implemented in [35]. An extended sequential cooperation scheme with reduced sensing reports and improved sensing performance is investigated in [36]. The soft fusion schemes such as maximum gain combining (MGC) and equal gain combining (EGC) combine the energy statistics reported from the SUs to make a decision [37–39]. All cooperating SUs in the hard decision scheme forward the binary values denoting the local decisions to the FC to make a global decision [40–42]. The works in [43, 44] utilize GA for optimizing the detection and false alarm probabilities to minimize the error probability. A novel evolution-based CSS mechanism is discussed in [45] to select and optimize the weight coefficients of the SUs' sensing result. The binary GA- (BGA-) based soft fusion scheme proposed in [46] is used to improve the detection performance and bandwidth utilization. Particle swarm optimization (PSO) is utilized as a tool for the optimization of the threshold point to enhance the spectral efficiency and detect the potential spectrum [47, 48]. An energy-efficient PSO

which provides high protection to the legitimate user is proposed in [49]. In our previous study in [50], FC determines the Kullback–Leibler (KL) divergence score based on the users' soft energy sensing reports. The KL divergence score is acknowledged to the users and stored in the FC local database to improve future decision. Similarly, in the proposed method in [51, 52], a double-sided neighbor distance (DSND) and outlier detection schemes followed by the majority voting decision in GA is used to reduce global decision error probability of the centralized CSS.

In this paper, the PSO algorithm has been employed to search for the spectrum information representing the actual status of the PU's activity on behalf of all cooperative SUs. The spectrum selection of the PSO results in overcoming the effect of MUs in the CSS. In the proposed scheme, the SUs forward their sensing results to the FC at certain sensing intervals. The FC utilizes the PSO algorithm to determine the most suitable energy statistics among the information received from the SUs including the MUs. Please note that the MUs pretend to be normal SUs. The one-to-many Hamming distances and z -score is used as a composite outlier score and fitness function of the PSO algorithm. Out of the PSO population, the sensing report with minimum outlying is selected as the PU channel status on behalf of all SUs for a global decision. The global decision of the PU channel is made with EGC, MGC, and majority voting hard fusion schemes based on the selections of the PSO algorithm. The PSO algorithm selection contains less harmful effects from any MUs; thus, the FC's decision becomes more reliable which improves the overall CSS performance.

The proposed scheme is verified in the false sensing of always no MU (ANMUs), AYMU, opposite MU (OMU), and random opposite MU (ROMU) in a cooperative environment. The AYMU sends an always high-energy statistics of the channel irrespective of the actual status; thus, it increases false alarm probability and reduces throughput of the SUs. The ANMU category of the MU forwards always low-energy statistics that result in misdetection and induce interference to the PU. The OMU, which is the most harmful type of the MU, forwards the opposite values of energy statistics against its actual sensing result. Finally, the ROMU acts like the OMU with probability P and like normal SU with probability $1 - P$.

The rest of the paper is organized as follows. In Section 2, the system model considered through this paper is presented. Section 3 describes the details that how the PSO algorithm is utilized to reduce the effects of abnormal SUs by identifying accurate sensing results before using EGC, MGC, and majority voting decision at the FC. Numerical evaluations and analysis are presented in Section 4. Finally, Section 5 concludes the paper.

2. System Model

As the probability of experiencing deep fading at all SUs is extremely low, the shared sensing results of the users to cooperatively decide the PU activity can reduce the sensing problems which may occur with single SU's sensing.

The objective is to minimize the error probability $P_e = P_f + P_m$, where P_f and P_m denote the false alarm and misdetection probabilities. Therefore, in order to reduce P_e , the detrimental effects of the misdetection $P_m = 1 - P_d$ and false alarm P_f probabilities must be minimized.

As in Figure 1, the SUs cooperate to sense the activity of the PU channel and inform the FC about their sensing information. The received information from the AYMU is an always high-energy signal representing busy status of the channel. Similarly, the ANMU provides with a low-energy signal to the FC. The OMU negates the actually sensed status of the PU and the ROMU acts like an OMU or a normal SU probabilistically. Hence, the ROMU's nature is more difficult to predict. Based on the received reports from the SUs, the FC makes global decision of the channel availability.

The binary hypothesis test at the l^{th} time slot with the j^{th} SU received signal is as follows [35]:

$$y_j(l) = \begin{cases} H_0, & n_j(l), \\ H_1, & h_j s(l) + n_j(l), \end{cases} \quad (1)$$

where the hypotheses H_0 denotes the idle status of the PU channel and H_1 represents the channel occupation by the PU, $y_j(l)$ is the received signal by the j^{th} SU in the l^{th} time slot, $n_j(l)$ is the additive white Gaussian noise (AWGN) at j^{th} SU, h_j is the channel gain between the PU channel and the j^{th} SU, and $s(l)$ is the signal transmitted by the PU in the l^{th} time slot, respectively.

The received signal energy of the PU channel by the j^{th} SU at the i^{th} sensing interval is

$$E_j(i) = \begin{cases} \sum_{l=i}^{i+K-1} |n_j(l)|^2, & H_0, \\ \sum_{l=i}^{i+K-1} |h_j s(l) + n_j(l)|^2, & H_1, \end{cases} \quad (2)$$

where K is the number of samples in the i^{th} sensing interval. According to the central limit theorem, the number of samples needs to be large enough so that the energy reported by each SU becomes similar to a Gaussian random variable under both H_0 and H_1 as [35, 53].

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

In (3), η_j is the signal to noise ratio (SNR) between the PU and j^{th} SU. Similarly, (μ_0, σ_0^2) and (μ_1, σ_1^2) are the mean and variance values of the energies reported under the H_0 and H_1 hypotheses.

3. Proposed Particle Swarm Optimization Process at FC

PSO is derived from the bird flocking or fish swarming introduced by Eberhart and Kennedy in 1992 [54]. In PSO, individual intelligence, as well as collective intelligence, plays an important role in finding an enhanced solution. In GA, it

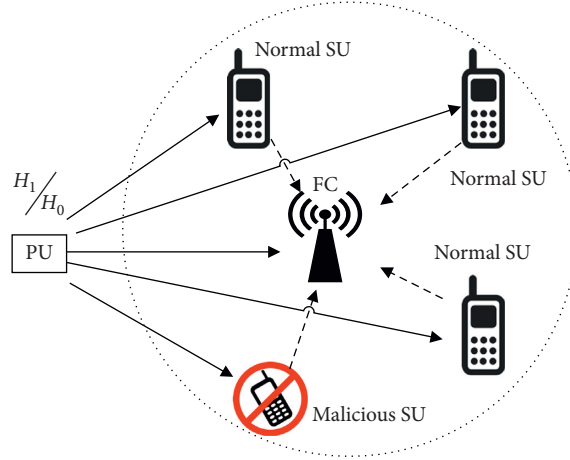


FIGURE 1: System model: CSS in CRN.

is likely that every novel group is flourishing better than the previous generations. Similarly, in the PSO, the same group is likely to become better and better. The individuals establish their intelligence and improve it with the passage of time. The whole group is expected to improve its group intelligence. Particles in the PSO algorithm utilize its own and neighbor knowledge to update their position and velocity. The PSO particle exchanges information about their best position among each other during a number of iterations.

The proposed model of the CSS using the PSO is shown in Figure 2. In this model, the SUs sense the PU channel and forward their energy statistics to the FC for a number of observations to form the PSO population. Then, the FC applies the PSO technique in identifying sensing reports which are closer to the actual status of the PU channel. The FC measures the fitness score under all sensing iterations and declares the minimum outlying particle as the actual channel information for a final decision. Fusion schemes are

applied by the FC, based on the selected global best particle of the population to generate a more accurate and reliable final decision of the PU channel.

In the PSO algorithm, a particle represents a row of the population matrix and each particle element (soft energy report) has a certain position and velocity. Initially, we assume that the positions and velocities of the particles are set to zero. The overall process of the PSO algorithm to determine the sensing reports, on the basis of which global decision is taken by the FC, is by proceeding the following steps:

Step 1: local spectrum decisions

The FC receives the soft energy reports from the SUs to form a history reporting matrix consisting soft energy statistical observations in the N_0 sensing intervals representing all SUs such as

$$E = [E_{ij}] = \begin{bmatrix} E_{11} & E_{12} & \dots & E_{1M} \\ E_{21} & E_{22} & \dots & E_{2M} \\ E_{31} & E_{32} & \dots & E_{3M} \\ \vdots & \vdots & \ddots & \vdots \\ E_{N_0,1} & E_{N_0,2} & \dots & E_{N_0,M} \end{bmatrix}, \quad i \in 1, 2, \dots, N_0, j \in 1, 2, \dots, M, \quad (4)$$

where E_{ij} denotes the energy information of the j^{th} SU in the i^{th} sensing interval. Spectrum sensing information is gathered at the FC database for the M SUs including the MUs in the N_0 intervals as in (3). The SSDF effect caused by the MUs can be minimized by utilizing the following steps.

Step 2: finding the fitness of the particles

After the collection of energy information as in (4), the FC modifies the particle positions to observe the differences in each individual sensing report with the reports provided by the other SUs. A new population is

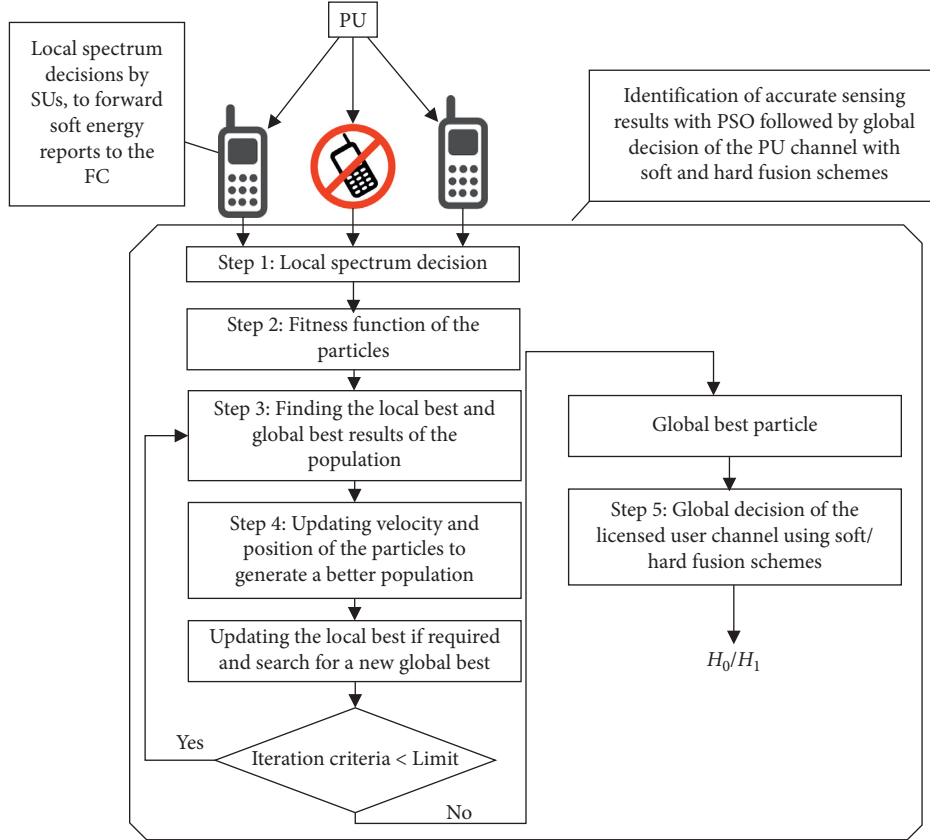


FIGURE 2: Proposed cooperative spectrum sensing scheme using PSO.

formed for all SUs based on the information already collected in (4) as

$$E' = [E'_{ij}] = \begin{bmatrix} E'_{11} & E'_{12} & \dots & E'_{1M} \\ E'_{21} & E'_{22} & \dots & E'_{2M} \\ E'_{31} & E'_{32} & \dots & E'_{3M} \\ \vdots & \vdots & \ddots & \vdots \\ E'_{N_0 1} & E'_{N_0 2} & \dots & E'_{N_0 M} \end{bmatrix}, \quad i \in 1, 2, \dots, N_0, \quad j \in 1, 2, \dots, M, \quad (5)$$

where $E'_{ij} = |(\sum_{j=1}^M E_{ij} - E_{ij}) / (M - 1)|$, which denotes the average of individual soft energy reports provided by all other SUs while taking out the report of the j^{th} user in this averaging.

Step 2.1: outlying using one-to-many sensing distances
Outlying factors are determined for the sensing reports from the SUs based on the one-to-many sensing distances $\mathbf{d}_j(i)$ for the j^{th} SU in the i^{th} sensing particle as

$$\mathbf{d}_j(i) = |E_{ij} - E'_{ij}|, \quad i \in 1, \dots, N_0, \quad j \in 1, \dots, M. \quad (6)$$

Based on the results in (6), the outlier score $\mathbf{d}_j(i)$ of the normal SUs and MUs is added to discover the total one-

to-many Hamming distance score under each sensing interval:

$$\mathbf{d}_i = \sum_{j=1}^M (\mathbf{d}_j(i)), \quad i \in 1, \dots, N_0, \quad j \in 1, \dots, M, \quad (7)$$

where \mathbf{d}_i is the total outlier score representing absolute sum of the Hamming distances of the individual reports E_{ij} with the average reports E'_{ij} of all other SUs in the i^{th} sensing interval.

The measurement in (7) is made for the N_0 intervals, and the results are collected as

$$\mathbf{d} = [\mathbf{d}_1 \ \mathbf{d}_2 \ \mathbf{d}_3 \ \cdots \ \mathbf{d}_{N_0}]^T, \quad (8)$$

where \mathbf{d} is the outlier score results of the N_0 sensing intervals. This score is a measurement of how far the report of each SU is away from the average sensing reports provided by all other SUs by separating those sensing intervals during which the MUs and the imperfection of the normal SU were misguiding the FC final decision about the PU channel.

Step 2.2: outlying using z-score

Similarly, the other outlier score measurement is made with the z-score measurement in comparison with the sensing reports received from each SU as

$$\mathbf{o}_j(i) = \left| \frac{(E_{ij} - \mu(i))}{\sigma(i)} \right|, \quad i \in 1, \dots, N_0, j \in 1, \dots, M, \quad (9)$$

where $\mu(i) = (\sum_{j=1}^M E_{ij})/M$ is the mean and $\sigma(i)$ is the standard deviation of the i^{th} particle in the PSO population. $\mathbf{o}_j(i)$ is the z-score outlying of the j^{th} report in the i^{th} interval of the history log. The result of $\mathbf{o}_j(i)$ in (9) shows how much the local sensing observation of the j^{th} user is detached away from the group observations provided by all other SUs.

Now, for guaranteeing the authenticity of each of the i^{th} reports, the sum of z-score measurements for all particles is made as

$$\mathbf{o}_i = \sum_{j=1}^M (\mathbf{o}_j(i)), \quad i \in 1, \dots, N_0, j \in 1, \dots, M. \quad (10)$$

The total z-score of the N_0 particles of PSO population is collected as

$$\mathbf{o} = [\mathbf{o}_1 \ \mathbf{o}_2 \ \mathbf{o}_3 \ \cdots \ \mathbf{o}_{N_0}]^T. \quad (11)$$

As the 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 normal SUs and MUs is determined, and the best selection of the sensing results having less abnormal behavior is calculated.

The criteria for selection of the particles according to their fitness values are declared according to (6) and (9) as

$$\mathbf{f}(i) = \mathbf{d}_i + \mathbf{o}_i. \quad (12)$$

The result in (12) declares the minimum score for sensing reports with fewer abnormalities in comparison

to those that are badly affected due to the abnormal behavior of the MUs.

Step 3: updating population

The global best position \mathbf{g} is the particle that results in minimum outlying score among all particles in \mathbf{E} according to (12). Each particle may improve its own if its new version is better compared to the previous one. Local best particles of the population are selected as $P = E$.

The positions and velocities are initially set to zero. The particle velocities are updated with the individual and collective intelligences as

$$V_{(i+1)j} = V_{ij} + C_1 \times R_1 \times (P_{ij} - E_{ij}) + C_2 \times R_2 \times (\mathbf{g}_j - E_{ij}), \quad (13)$$

where C_1 and C_2 are the learning acceleration coefficients that describe the particles' individual and social contributions. Similarly, R_1 and R_2 are the uniformly distributed random numbers in the range 0 to 1 to present stochastic contribution to the algorithm.

Next to the measurements of particles' velocities with the local and global intelligence, these velocities are rounded to the two extremes as

$$V_{(i+1)j} = \begin{cases} \max(V), & V_{ij} > \max(V), \\ \min(V), & V_{ij} < \min(V). \end{cases} \quad (14)$$

The j^{th} particle's position representing soft energy information at the $(i+1)^{\text{th}}$ iteration is updated with the measured velocities as

$$E_{(i+1)j} = E_{ij} + V_{(i+1)j}, \quad (15)$$

where $E_{(i+1)j}$ are the reports of the modified population, E_{ij} is the initial report of the j^{th} SU in the i^{th} interval, and $V_{(i+1)j}$ are the velocities as in (14).

Step 4: updating local best and global best

Fitness measurements of the new population in (15) are determined by following the same procedure as in (12).

The novel particle fitness is compared with the earlier population fitness to search for any improvements in the local and global best positions in comparison with the earlier energy reports. Similarly, the local best positions of the population are updated as

$$P_i = \begin{cases} E_i, & f(E_i) < f(P_i), \\ P_i, & \text{otherwise,} \end{cases} \quad i \in 1, \dots, N_0. \quad (16)$$

In (16), the results of the local best particles are updated by comparing the fitness of the new population (15) to that of the local best particles P fitness. The local best particles are updated and take values of the new particles if their outlying results in (12) are higher compared to the newly created population.

Similarly, a search is made to identify new global best particle in the entire population by cross analysis of the fittest. Fitness of the updated local best particles in (16) is placed for comparison to search for any improvement in the selection of the global best particle as

$$\mathbf{g} = \begin{cases} P_i, & f(P_i) < f(\mathbf{g}), \\ \mathbf{g}, & \text{otherwise,} \\ \forall i \in 1, \dots, N_0. \end{cases} \quad (17)$$

In (17), outlying score of each particle of the local best population is compared with the global best particle determined earlier. If any particle of the local best population has a fitness function found to be optimum in comparison with the global best particle with the minimum outlying score in (12), then the global best particle is replaced.

Here, the new global best particle is selected as \mathbf{g} representing the particle with the best fitness function having minimum outlying results in the current and previous PSO population.

The PSO production of the new population and search for the global best results continues until the stopping criterion is met. At the end of the desired number of iterations, the final global best particle containing reliable and trusted soft energy reports against M cooperating SUs is elected for a final decision by the FC.

Step 5: global decision combination schemes

Based on the final selection of the global best particle \mathbf{g} as the soft energy reports on behalf of all M cooperative SUs, FC utilizes soft and hard combination schemes in Section 2 for declaring a unanimous decision about the PU channel. The EGC, MGC, and majority voting hard fusion combination schemes are used as decision criteria in this section.

The EGC is combining the individual statistical information of all SUs by giving equal weight to each individual SU decision and summed coherently. The combination is compared with the threshold by the EGC as

$$\text{EGC} = \begin{cases} H_1, & \frac{(\sum_{j=1}^M \mathbf{g}_j)}{M} \geq \gamma, \\ H_0, & \text{otherwise.} \end{cases} \quad (18)$$

The cooperative detection and false alarm probabilities P_{d_EGC} and P_{f_EGC} made by the EGC scheme based on the global decision made about the PU spectrum are

$$P_{d_EGC} = \Pr \left\{ \frac{(\sum_{j=1}^M \mathbf{g}_j)}{M} \geq \gamma | H_1 \right\}, \quad (19)$$

$$P_{f_EGC} = \Pr \left\{ \frac{(\sum_{j=1}^M \mathbf{g}_j)}{M} \geq \gamma | H_0 \right\}.$$

In the MGC scheme, each receiving signal branch is multiplied with a weighed function proportional to the branch gain. The branches with a strong signal in the MGC are amplified more, while the weak signal components receive attenuations with the weights. The idea to boost the strong signal component and attenuate weak signal component in the MGC diversity is exactly the same as that of filtering and signal weighting in the matched filter receiver. Similarly, the MGC scheme at the FC is giving higher weights to the decision of the SUs with higher SNR values and low weights to the decisions of the SUs with low SNR values as

$$\text{MGC} = \begin{cases} H_1, & \sum_{j=1}^M (w_j \times \mathbf{g}_j) \geq \gamma, \\ H_0, & \text{otherwise,} \end{cases} \quad (20)$$

where $w_j = \eta(j) / \sum_{j=1}^M \eta(j)$. The cooperative detection and false alarm probabilities of the MGC scheme are measured based on the received soft energy statistics as

$$P_{d_MGC} = \left\{ \left(\sum_{j=1}^M (w_j \times \mathbf{g}_j) \geq \gamma \right) | H_1 \right\}, \quad (21)$$

$$P_{f_MGC} = \left\{ \left(\sum_{j=1}^M (w_j \times \mathbf{g}_j) \geq \gamma \right) | H_0 \right\}.$$

In the majority voting schemes, the FC counts the total number of the SUs with their energy value greater than the threshold as

$$\text{MV} = \begin{cases} H_1, & \sum_{j=1}^M (\mathbf{g}_j \geq \gamma_j) \geq k, \\ H_0, & \text{otherwise.} \end{cases} \quad (22)$$

The three commonly used hard combination schemes are the majority voting, OR, and AND fusion combination schemes. In the count hard decision, a global decision on the PU existence is made if k out of total M cooperative users provide PU detection information with their energies larger than a threshold. The FC concludes a final decision H_1 if k users' reports validate the PU existence. Similarly, the total number of cooperative users with PU detection information less than k lead the FC to conclude in favor of H_0 to declare an idle condition of the PU channel. The counting score k is taken as 1 for the OR fusion rule and M for the AND rule. In the proposed work, the majority voting scheme is selected with $k = M/2$. In case of majority voting, if half cooperative

SUs energies are passing the threshold, a global decision is made as H_1 ; otherwise, the decision is made in favor of H_0 .

The detection and false alarm probabilities measurement of the majority voting hard decision schemes based on the best selection of the PSO at the FC are as follows:

$$P_{d_MV} = \Pr \left\{ \sum_{j=1}^M \mathbf{g}_j \geq \frac{M}{2} | H_1 \right\},$$

$$P_{f_MV} = \Pr \left\{ \sum_{j=1}^M \mathbf{g}_j \geq \frac{M}{2} | H_0 \right\},$$
(23)

where P_{d_MV} and P_{f_MV} are cooperative detection and false alarm probabilities of the majority voting schemes when PSO is used as a detection mechanism at the FC.

4. Numerical Evaluation

For simulation purposes, parameter adjustment is made for the CRN with $M = 11$ SUs. Among the total SUs, 7 SUs are selected as normal and 4 SUs are randomly selected as AYMUs, ANMUs, OMUs, and ROMUs. The sensing time is kept as 1 ms which contains $K = 270$ sensing samples. The total number of sensing iterations N is selected as 100. The sensing interval in which the ROMU performs a malicious act is adjusted randomly from 1 to N . The system performance is verified in the presence of equal distributions of OMU, ROMU, AYMU, and ANMU users. The sensing reports of the SUs formed the PSO population of size $N_0 \times M$ with N_0 particles representing the sensing information of the M cooperating SUs.

In this part of the simulation, the MUs are first selected as AYMU, and then, its nature is changed to ANMU. In Figure 3, results are drawn to compare the performances of EGC, MGC, and majority voting schemes. From the simulation results in Figure 3, it is obvious to show an improvement in the detection results of the PSO-based EGC, MGC, and majority voting schemes against the conventional combination schemes. The cooperative scheme performance under the considerations of AYMU and ANMU is more optimized for the PSO based soft and hard combinations. It is shown that the detection response in both the cases when only AYMU and the one with only ANMU users' considerations are identical. The equal consideration of AYMU and ANMU cases are similarly treated in the CSS with almost identical probability of detection P_d for a given false alarm P_f . Figure 3 also shows better receiver operating characteristics (ROC) results for the PSO based-MGC scheme which is followed by the EGC scheme. The majority voting hard fusion combination illustrates minimum detection results compared with the other two schemes. It is also obvious that the PSO-based soft and hard fusion combination schemes are able to outperform the simple MGC, EGC, and hard fusion combinations for any given false alarm.

In the second part, authenticity of the system is verified by comparing results of the proposed PSO-based soft and hard combinations with conventional schemes. In this case,

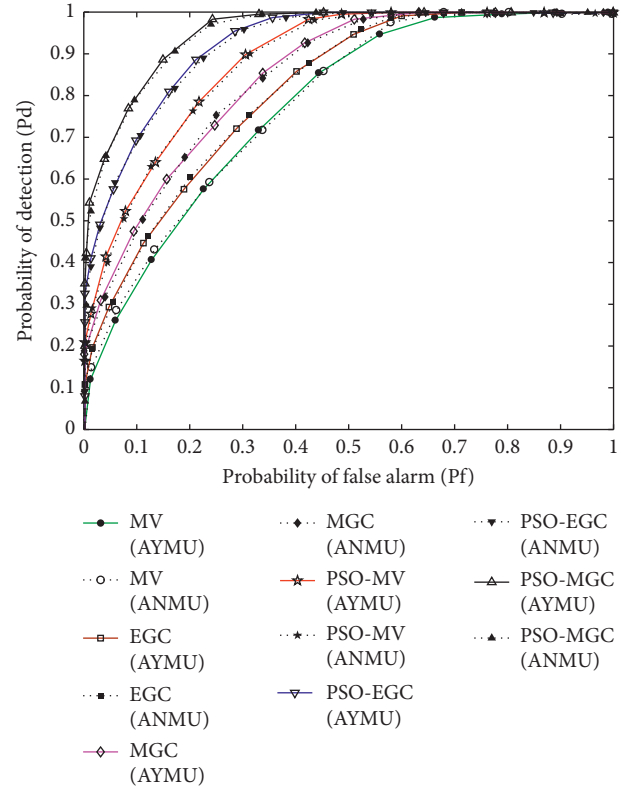


FIGURE 3: ROC curve, when AYMU and ANMU exist in the network.

the MUs are first selected as OMU, and then, their nature changes to ROMU. The result illustrates that the MGC scheme shows better detection compared with the EGC and majority voting counterparts. The ROC collection of the three schemes under the proposed and the conventional schemes show the reliabilities of the PSO-based combination techniques. In Figure 4, the ROMUs affect the sensing environment more hazardously than the OMU. The proposed scheme is superseding the traditional fusion schemes in both the OMU and ROMU cases.

In the third part of the simulation, the performances of the conventional and the proposed PSO-based fusion combination schemes are tested, when the MUs are distributed equally as AYMU, ANMU, OMU, and ROMU in Figure 5.

The minimum ROC results in Figure 5 show the performance of the conventional fusion schemes under the consideration of all 4 MUs, while the upper three ROC curves show the PSO fusion combination scheme performance under the same parameter settings. This shows an improvement in the detection performance of the PSO-based fusion combination schemes compared with the conventional combination schemes. It is noticeable that the MGC fusion combination scheme provides more sophisticated detection performance compared to the other schemes.

The proposed PSO-based fusion combination scheme is further verified by illustrating the error probability P_e according to the SNR varying from -35 dB to 0 dB in

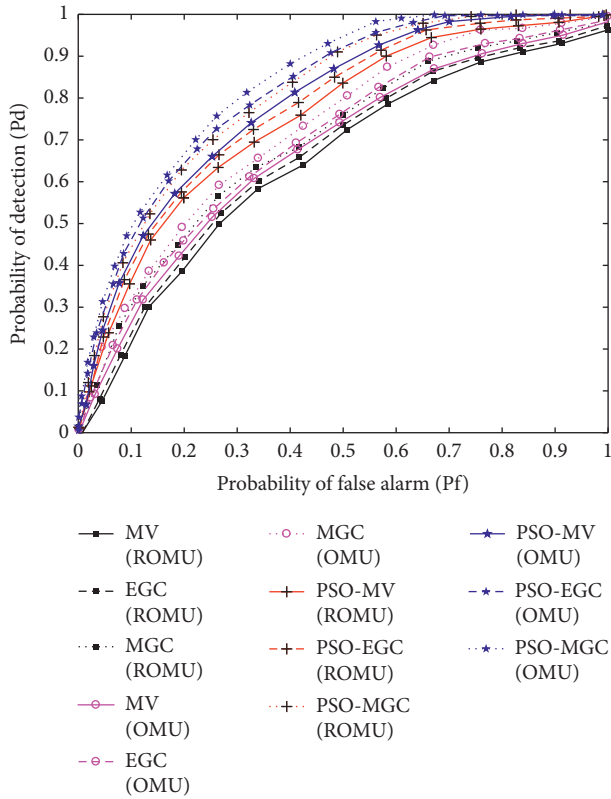


FIGURE 4: ROC curve, when OMU and ROMU exist in the network.

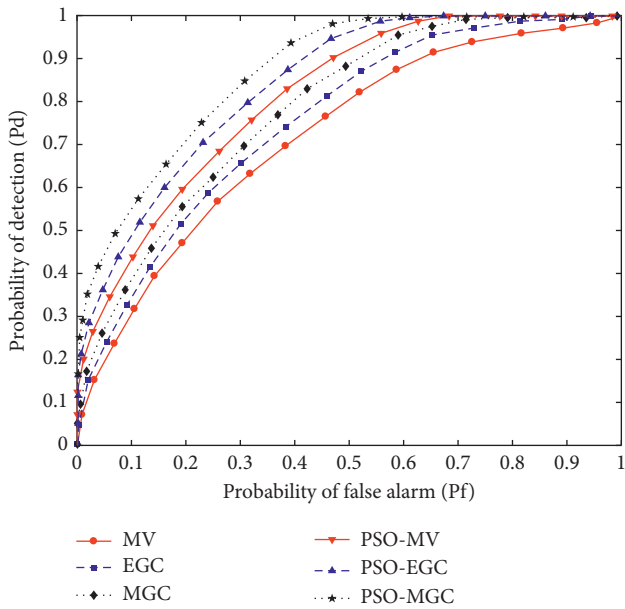


FIGURE 5: ROC curve, when AYMU, ANMU, OMU, and ROMU are equally distributed.

Figure 6. The error in sensing the PU channel by the proposed scheme is the minimum of all and with increasing

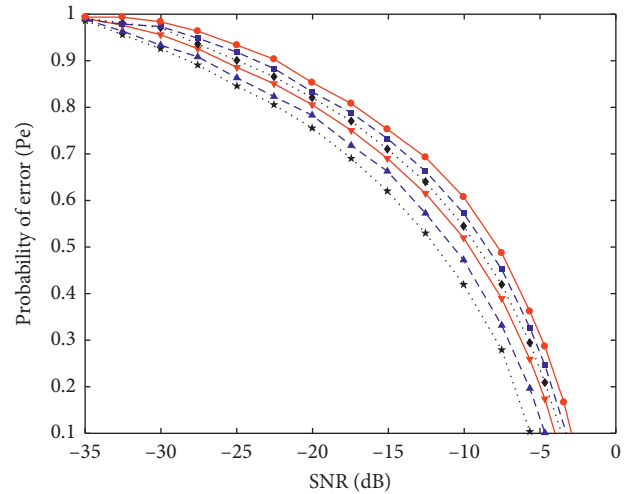


FIGURE 6: Probability of error vs. SNR.

SNR the proposed scheme error reduces more quickly as compared with the other traditional schemes.

It is clear that, by following the PSO-based algorithm, the proposed fusion combination schemes are more optimized and accurate in the presence of the MUs. The selections of the PSO following by the soft and hard fusion combinations make the CSS authentic and suitable against the MUs. The risk of considering the MUs in the CSS is significantly reduced with the proposed scheme. The results show that the SUs cooperation is more effective using the proposed scheme. The proposed scheme is able to eliminate the considerations of MUs in making global decision at the FC and produce reliable sensing results.

5. Conclusions

The impact of the MUs on the CSS reduces the effectiveness of cooperation in CIoT. Therefore, it is necessary to detect the MUs in order to avoid any confusion about the actual status of the PU channel. This paper focuses on improving the performance of the CSS by using the PSO algorithm. Based on the energy statistics reported by the SUs, the PSO is able to reduce the effect of the MUs in authenticating the global decision of the PU's existence. The FC combines the diversified sensing reports of the users using the proposed EGC, MGC, and majority voting decisions to acquire the global decision of the PU activity. The proposed PSO algorithm is able to overcome the effects of OMU, ROMU, AYMU, and ANMU categories of the MUs in the soft and hard combinations. Simulations verify the superiority and the authenticity of the proposed scheme in producing more accurate and reliable decisions for the soft and hard combination schemes at the FC.

Data Availability

The data used to support the finding of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2020-2018-0-01426) supervised by the IITP (Institute for Information and Communication Technology Planning, and Evaluation) and in part by the National Research Foundation (NRF) funded by the Korea government (MSIT) (No. 2019R1F1A1059125).

References

- [1] A. Agarwal, G. Mishra, and K. Agarwal, "The 5th generation mobile networks-key concepts, networks, architecture and challenges," *American Journal of Electrical & Electronics Engineering*, vol. 3, no. 2, pp. 22–28, 2015.
- [2] T. Q. Duong and N. S. Vo, "Wireless communication and network for 5G and beyond," *Mobile Networks and Applications*, vol. 24, no. 2, pp. 443–446, 2019.
- [3] B.-S. P. Lin, F. J. Lin, and L. P. Tung, "The role of 5G mobile broadband in the development of iot, big data, cloud and SDN," *Communication and Network*, vol. 8, no. 1, pp. 9–21, 2016.
- [4] R. Chavez-Santiago, M. Szydeko, A. Kliks et al., "5G: the convergence of wireless communication," *Wireless Personal Communications*, vol. 83, no. 3, pp. 1617–1642, 2015.
- [5] W. Ejaz, A. Anpalagan, M. A. Imran et al., "Internet of things (IoT) in 5G wireless communications," *IEEE Access*, vol. 4, pp. 10310–10314, 2016.
- [6] K. Ashton, "Internet of things," in *The Real World, Things Matter More than Ideas* Springer, Berlin, Germany, 2009.
- [7] F. A. Awin, Y. M. Alginahi, E. Abdel-Raheem, and K. Tepe, "Technical issues on cognitive radio-based internet of things systems: a survey," *IEEE Access*, vol. 7, pp. 97887–97908, 2019.
- [8] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *Proceedings of the IEEE International Conference on Frontiers of Information Technology*, Islamabad, Pakistan, December 2012.
- [9] A. A. Khan, M. H. Rehmani, and A. Rachedi, "When cognitive radio meets the internet of things," in *Proceedings of the IEEE International Wireless Communication & Computing Conference (IWCMC)*, Paphos, Cyprus, September 2016.
- [10] S. Nazir, Y. Ali, N. Ullah, and I. García-Magariño, "Internet of things for healthcare using effects of mobile computing: a systematic literature review," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 5931315, 15 pages, 2019.
- [11] C. Feng, M. Adnan, A. Ahmad, A. Ullah, H. U. Khan, and H. U. Khan, "Towards energy-efficient framework for iot big data healthcare solutions," *Scientific Programming*, vol. 2020, Article ID 7063681, 9 pages, 2020.
- [12] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Survey & Tutorial*, vol. 17, no. 4, pp. 2347–2376, 2015.
- [13] Q. Wu, G. Ding, Y. Xu et al., "Cognitive internet of things: a new paradigm beyond connection," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 129–143, 2014.
- [14] 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.
- [15] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radio," in *Proceedings of the IEEE International Conference on Communications*, Istanbul, Turkey, 2006.
- [16] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.
- [17] 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, pp. 2005–2009, 2016.
- [18] L. Miao, Z. Sun, and Z. Jie, "The parallel algorithm based on genetic algorithm for improving the performance of cognitive radio," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 5986482, 6 pages, 2018.
- [19] A. Elahi, I. M. Qureshi, F. Zaman, N. Gul, and T. Saleem, "Suppression of mutual interference in noncontiguous orthogonal frequency division multiplexing based cognitive radio systems," *Wireless Communications and Mobile Computing*, vol. 2017, Article ID 1860134, 9 pages, 2017.
- [20] E. Axell, G. Leus, E. G. Larsson, and H. V. Poor, "Spectrum sensing for cognitive radio: state-of-the-art and recent advances," *IEEE Signal Processing Magazine*, vol. 29, no. 3, pp. 101–116, 2012.
- [21] 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. 12, pp. 1–12, 2016.
- [22] M. S. Khan and I. Koo, "Mitigation of adverse effect of malicious users by hausdorff distance in cognitive radio networks," *Journal of Information and Communication Convergence Engineering*, vol. 13, no. 2, pp. 74–80, 2015.
- [23] 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, 2010.
- [24] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of iot devices by using mobile computing: a systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.
- [25] N. Gul, M. S. Khan, S. M. Kim, J. Kim, A. Elahi, and Z. Khalil, "Boosted trees algorithm as reliable spectrum sensing scheme in the presence of malicious users," *Electronics*, vol. 9, no. 6, pp. 1038–1123, 2020.
- [26] N. Gul, I. M. Qureshi, M. S. Khan, A. Elahi, and S. Akbar, "Differential evolution based reliable cooperative spectrum sensing in the presence of malicious users," *Wireless Personal Communications*, vol. 114, no. 1, pp. 123–147, 2020.
- [27] H. Asfandyar, N. Gul, I. Rasool, and A. Elahi, "Enhanced cooperative spectrum sensing in cognitive radio network using flower pollination algorithm," in *Proceedings of the 1st International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, pp. 24–25, Swat, Pakistan, July 2019.

- [28] A. Ahmed, N. Gul, I. Rasool, and A. Elahi, "Performance comparison of hard decision schemes in the presence of malicious users," in *Proceedings of the 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, pp. 24-25, Swat, Pakistan, July 2019.
- [29] N. Gul, M. S. Khan, J. Kim, and S. M. Kim, "Robust spectrum sensing via double-sided neighbor distance based on genetic algorithm in cognitive radio networks," *Mobile Information Systems*, vol. 2020, Article ID 8876824, 10 pages, 2020.
- [30] M. S. Khan, L. Khan, N. Gul, M. Amir, J. Kim, and S. M. Kim, "Support vector machine-based classification of malicious users in cognitive radio networks," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8846948, 2020.
- [31] M. Fathy, A. Tammam, and A. Saafan, "Influence of relaying malicious node within cooperative sensing in cognitive radio network," *Wireless Networks*, vol. 25, no. 5, pp. 2449-2458, 2019.
- [32] N. Gupta, S. K. Dhurandher, and A. Sehgal, "A contract theory approach-based scheme to encourage secondary users for cooperative sensing in cognitive radio networks," *IEEE Systems Journal*, vol. 14, pp. 1-11, 2019.
- [33] Z. Sun, Z. Xu, M. Z. Hammad, X. Ning, Q. Wang, and L. Guo, "Defending against massive SSDF attacks from a novel perspective of honest secondary users," *IEEE Communications Letters*, vol. 23, no. 10, pp. 1696-1699, Oct, 2019.
- [34] Y. Fu and Z. He, "Bayesian-inference-based sliding window trust model against probabilistic SSDF attack," *IEEE Systems Journal*, vol. 14, pp. 1-12, 2019.
- [35] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2488-2497, 2010.
- [36] V. V. Hiep 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.
- [37] J. Ma, G. Zhao, and Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 11, pp. 4502-4507, 2008.
- [38] Y. L. Lee, W. K. Saad, A. Abd El-Saleh, and M. Ismail, "Improved detection performance of cognitive radio networks in AWGN and rayleigh fading environments," *Journal of Applied Research and Technology*, vol. 11, no. 3, pp. 437-446, 2013.
- [39] 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.
- [40] D. B. Teguig, B. Scheers, and V. Le Nir, "Data fusion schemes for cooperative spectrum sensing in cognitive radio networks," in *Proceedings of the Military Communications And Information Systems Conference*, MCC, Gdansk, Poland, 2012.
- [41] N. Marchang, R. Rajkumari, S. B. Brahmachary, and A. Taggu, "Dynamic decision rule for cooperative spectrum," in *Proceedings of the International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, India, 2015.
- [42] J. Unnikrishnan and V. V. Veeravalli, "Cooperative spectrum sensing and detection for cognitive radio," in *Proceedings of the IEEE Global Telecommunications Conference (Globecom)*, Washington, DC, USA, November 2007.
- [43] S. Bhattacharjee, "Optimization of probability of false alarm and probability of detection in cognitive radio networks using GA," in *Proceedings of the 2nd IEEE International Conference on Recent Trends in Information Systems*, Kolkata, India, 2015.
- [44] M. S. Khan, N. Gul, J. Kim, I. M. Qureshi, and S. M. Kim, "A genetic algorithm-based soft decision fusion scheme in cognitive iot networks with malicious users," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 2509081, 20 pages, 2020.
- [45] 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.
- [46] A. A. EL-Saleh and K. Hussain, "Cognitive radio engine model utilizing soft fusion based genetic algorithm for cooperative spectrum optimization," *Proceedings of the International Journal of Computer Networks & Communications (IJCNC)*, vol. 2, no. 3, pp. 169-173, 2013.
- [47] A. Rauniyar and S. Y. Shin, "Improved detection performance of energy detector by optimization of threshold using BPSO algorithm for cognitive radio networks," in *Proceedings of the 2nd International Conference on Industrial Application Engineering*, Vancouver, Canada, 2015.
- [48] M. Taha and D. Alnadi, "Threshold adaptation in spectrum sensing for cognitive radio using particle swarm optimization," in *Proceedings of the International Conference on Control*, Suwon-si, South Korea, October 2014.
- [49] R. A. Rashid, A. H. F. Bin Abdul Hamid, N. Fisal et al., "Efficient in-band spectrum sensing using swarm intelligence for cognitive radio network," *Canadian Journal of Electrical and Computer Engineering*, vol. 38, no. 2, pp. 106-115, 2015.
- [50] N. Gul, I. M. Qureshi, A. Omar, A. Elahi, and M. S. Khan, "History based forward and feedback mechanism in cooperative spectrum sensing including malicious users in cognitive radio network," *PLoS One*, vol. 12, no. 8, 2017.
- [51] N. Gul and A. Naveed, "A combination of double-sided neighbor distance and genetic algorithm in cooperative spectrum sensing against malicious users," in *Proceedings of the 14th International Bhurban Conference On Applied Sciences & Technology (IBCAST)*, Islamabad, Pakistan, 2017.
- [52] N. Gul, I. M. Qureshi, A. Elahi, and I. Rasool, "Defense against malicious users in cooperative spectrum sensing using genetic algorithm," *International Journal of Antennas and Propagation*, vol. 2018, Article ID 2346317, 11 pages, 2018.
- [53] M. Jun and Li. Ye, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, 2007.
- [54] A. M. Vargas and A. G. Andrade, "Comparing particle swarm optimization variants for a cognitive radio network," *Elsevier Applied Soft Computing*, vol. 13, no. 2, pp. 1222-1234, 2013.