Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 3153915, 14 pages
https://doi.org/10.1155/2018/3153915

Research Article

One-to-Many Relationship Based Kullback Leibler Divergence against Malicious Users in Cooperative Spectrum Sensing

Noor Gul,[1,2] **Ijaz Mansoor Qureshi**,[3] **Sadiq Akbar**,[2] **Muhammad Kamran**,[2] **and Imtiaz Rasool**[2]

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

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

Received 21 April 2018; Revised 2 August 2018; Accepted 11 August 2018; Published 2 September 2018

Academic Editor: Sungchang Lee

The centralized cooperative spectrum sensing (CSS) allows unlicensed users to share their local sensing observations with the fusion center (FC) for sensing the licensed user spectrum. Although collaboration leads to better sensing, malicious user (MU) participation in CSS results in performance degradation. The proposed technique is based on Kullback Leibler Divergence (KLD) algorithm for mitigating the MUs attack in CSS. The secondary users (SUs) inform FC about the primary user (PU) spectrum availability by sending received energy statistics. Unlike the previous KLD algorithm where the individual SU sensing information is utilized for measuring the KLD, in this work MUs are identified and separated based on the individual SU decision and the average sensing statistics received from all other users. The proposed KLD assigns lower weights to the sensing information of MUs, while the normal SUs information receives higher weights. The proposed method has been tested in the presence of always yes, always no, opposite, and random opposite MUs. Simulations confirm that the proposed KLD scheme has surpassed the existing soft combination schemes in estimating the PU activity.

1. Introduction

The rapid evolution in wireless communication demands new wireless services in both the used and unused parts of the radio spectrum [1]. The Federal Communications Commission (FCC) exclusively assigns spectrum bands to various services [2, 3]. Cognitive radio (CR) is a smart technique that gains knowledge from the environment and adjusts its parameters accordingly [4]. The incumbent primary users (PUs) are free to transmit any time with no restrictions, while the secondary users (SUs) can get the benefit of the spectrum only when the licensee declares it free [5].

In cognitive radio network (CRN), sensing the incumbent user spectrum is vital. An offensive detection on the PU channel due to false alarm reduces the SUs opportunity to utilize the free spectrum. Similarly, any misdetection in the PU transmission will produce interference in the transmission of legitimate and opportunistic users. In case of the frequent usage of the spectrum by the PUs, the termination probability of SUs is not easy to ensure. The proposed scheme in [6] uses channel reservation to improve the quality of service (QoS) for SUs. To confirm the status of the PU a number of detection schemes, such as energy detector (ED), feature detector (FD), and matched filter detector (MFD), are used in [3, 7]. The use of multiple antennas for spectrum sensing is considered in [8], when noise and signal of the PU are considered as independent complex zero-mean Gaussian random variables. Detection results of the orthogonal frequency division multiplexing (OFDM) signals in the frequency selective fading channels are considered in [9, 10]. Optimal interference subcarriers are obtained based on Genetic Algorithm (GA) to suppress intercarrier interference of the unlicensed user to the licensee [11]. In [12], side-lobes reduction using generalized side-lobe canceller combined with GA and differential evolution is proposed. The GA and interior point method design schemes enhance

the performance of hybrid computing technique based on active noise control for random, complex random, and sinusoidal input noise variations in the primary secondary paths [13]. An improved energy detector scheme is suggested in [14] to maximize the throughput of a CRN network with minimum interference to the PUs.

Individual SU faces a number of restrictions to sense the PU spectrum accurately. The sensing performance of a solitary device is degraded due to fading, shadowing, energy constraints, and hidden station dilemmas of the primary signal. It is therefore most probable that a single user might fail to spot detection of the licensee transmitter [5]. The cooperative user devices placed more than a few wavelengths apart experience an independent fading effect. The doubt to efficiently detect the licensed spectrum possession is mitigated by enabling different users to share their local sensing results and make a cooperative decision [15–19]. The particle swarm optimization is able to find their foods by sharing their search information in contrast with GA using crossover and kids reproduction [20]. Cooperative spectrum sensing (CSS) using energy harvest-based weighed method in [21] reduces the energy wastage of the SUs with better sensing results. The use of cyclostationary signatures in [22] is used to subdue large number of challenges related to cooperative network in the rising applications of the CR. The proposed method in [23] enhances throughput of the CRN in the presence of mobile SUs to access the PU spectrum. The MUs presence in a CSS environment reduces the effectiveness of the cooperation. Therefore, precise recognition and exclusion of the false sensing information are extremely vital [24]. Significant investigations are carried out to make the collaborative schemes resistant to any MU attack. The aim of any MU in CSS is to provide false sensing data to the FC [25].

The assistance of trusted nodes in a reputation based CSS network is discussed in [26], where Nyman-Pearson and likelihood ratio test is utilized for spectrum sensing improvements. The primary emulation category of MUs discussed in [27] tries to impersonate activities of the legitimate PU transmitter. A robust technique with prime focus on always yes group of MUs is implemented in [28]. An extended sequential cooperative scheme that reduces the number of sensing reports is investigated in [29]. In the soft fusion combination schemes proposed in [30–32] sensing energies from different SUs are combined to take accurate decision about the PU spectrum holes. Similarly, in the hard fusion schemes SUs provide a hard binary decision to the FC to predict the licensed user activity in the spectrum [33–35]. The optimal quantization scheme in [36, 37] is able to produce improved detection with a control on the probability of false alarm. Bioinspired heuristics based on GA find the design parameters of nonlinear Hammerstein controlled autoregressive systems with distinct values of the noise variance [38]. The study in [39–45] focuses on evolutionary computation for optimizing the detection and false alarm probabilities to minimize the sensing error for a particular SU.

In this paper, Kullback Leibler Divergence (KLD) has been employed to protect the CSS against the spectrum falsification attack (SFA) of always no (AN), always yes (AY), random opposite (RO), and the always opposite (AO) categories of MUs by assigning weights to the sensing reports of SUs before global combination at the FC. In our previous study [46], SUs perform their local sensing, report soft energies to the FC, and also store this information in its local database. FC determines the KL divergence score against each user and also acknowledges this same information to the user. A normally declared user tries to send mean of the previous energy reports to the FC based on its current observation. The work in [46, 47] uses the KLD to determine the probability distribution function (PDF) dissimilarity of a particular SU under the presence and absence hypothesis of the licensed user channel. The PDF uses the energy statistics of an individual user under both hypotheses for declaring it normal or malicious. In this work, FC takes sensing data from all SUs and determines KLD score based on the energy statistics of individual user with the average statistics received from all other users. The final decision is made at FC by assigning weights to the local energy information of each individual SU based on the measured KLD score of each SU. Lower weights are assigned to the sensing data of MUs based on the KLD results, while the regular user sensing information receives higher weights. The lower weights keep the FC final decision less prone to the attack of MUs. By following the proposed method, the performance of CSS is kept at its maximum in the presence of MUs without identifying any malicious activity.

The proposed method results are tested in the company of AO, RO, AY, and AN categories of MUs in a cooperative environment. The outcome shows that these MUs in CSS increase the false alarm and misdetection, resulting in an increased interference to the primary transmission and reduced throughput of the network. Simulations confirmed that the proposed one-to-many relation based KLD method leads to more accurate and sophisticated detection than the traditional soft combination schemes in [46, 47].

The rest of the paper is organized as follows: In Section 2, the system model is presented. Section 3 explains the proposed scheme, where proposed method is used to overwhelm the MUs effects in the global decision of the FC. Experimental outcomes are presented in Section 4. Section 5 concludes the paper.

2. System Model

In the CSS as in Figure 1, all SUs report their local sensing information of the PU channel to the FC. The FC collects sensing notifications of all individual SUs and generates a global decision to show the actual status of the PU spectrum.

The spectrum sensing decisions H_1 and H_0 made by each SU in a particular spectrum are as follows:

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

where H_0 is the hypothesis about the availability and H_1 is the hypothesis for the occupancy of the PU spectrum by the licensed user. $y_j(l)$ is the received signal by the j^{th} user at the l^{th} time slot. $n_j(l)$ is the Additive White Gaussian Noise at the j^{th} user receiver. h_j is the amplitude of the channel gain and $s(l)$ denotes the PU transmit signal.

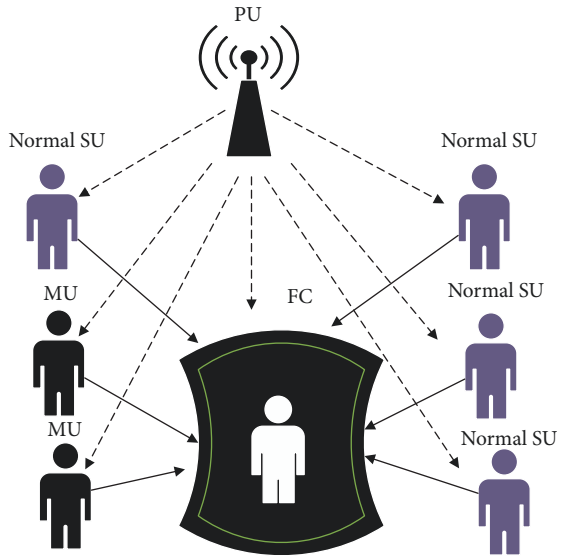

Figure 1: The conventional CSS mechanism.

Accordingly, as a consequence of H_1 and H_0 hypothesis, the observed signal energy at the j^{th} receiver can be represented as

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

In (2), each of the i^{th} sensing intervals is divided into K total number of samples. When the number of samples is considered large enough, the soft energy report of these SUs is similar to that of a Gaussian random variable in the H_0 and H_1 hypothesis as in [29, 30].

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

Here η_j is the signal-to-noise ratio between the primary transmitter and the j^{th} user. Moreover, (μ_0, σ_0^2) and (μ_1, σ_1^2) are the energy distributions means and variances when H_0 and H_1 hypotheses are true.

The KLD between the two normally distributed functions $a(x)$ and $b(x)$ is calculated as follows [46]:

$$K(a \parallel b) = \int a(x) \log\left(\frac{a(x)}{b(x)}\right) dx \quad (4)$$

Similarly, the KLD representation for functions $a(x)$ and $b(x)$ with the means and variances (μ_a, σ_a^2) and (μ_b, σ_b^2) is as follows:

$$K(a \parallel b) = K\left(\mu_a, \mu_b, \sigma_a^2, \sigma_b^2\right) = \frac{1}{2}\left(\log\left(\frac{\sigma_b^2}{\sigma_a^2}\right) - 1 + \left(\frac{\sigma_a^2}{\sigma_b^2}\right) + \frac{\left(\mu_a - \mu_b\right)^2}{\sigma_b^2}\right) \quad (5)$$

The MUs in Figure 2 are producing dissimilar energy distribution in the H_1 and H_0 hypothesis as compared with normal SUs. The KLD score against these MUs is dissimilar to the normal SUs and is easily separable from the normal user category.

The probability distribution functions of the energy statistics reported by the normal SU, AY, AN, AO, and RO users are given in Figure 2. The energy distributions provided by all four categories of MUs are different from the normal user distributions. Therefore, any cooperative user having energy distribution dissimilar to the normal user in Figure 2(a) is treated as malicious one. The AO user distribution in Figure 2(b) always negates the distribution of the normal user. The AY user in Figure 2(c) is producing similar high energy distributions under both hypotheses. Similarly, the AN user with always free state information of the licensee channel has its low energy distributions in Figure 2(d). The RO user behaves as AO with probability P and as a normal user with probability (1-P) in Figure 2(e).

3. The Proposed One-to-Many Relations Based KLD

The proposed work considers total cooperative users larger in number compared with MUs. All the cooperative users inform FC about their local spectrum observations of the primary channel. FC collects and takes its global decision based on the received energy statistics of the reporting users. Before making any global decision, FC assigns weights to the local sensing of SU reports with the proposed KLD method. The resultant weights illustrate reliability of the local spectrum sensing information of the individual cooperating users prior to making any final decision at the FC.

A pseudocode showing the proposed KLD algorithm for the local detection determining KLD score using one-to-many relationship based energy statistics and taking global decision based on the received energy and measured weights is given below:

(1) For $i = 1$ to limit

(2) For $j = 1$ to SU

(3) Local detection $E_j(i)$ by the j^{th} user

(4) New values of mean and variance $(\mu_{ja}(i), \sigma_{jb}^2(i))$ based on $E_j(i)$

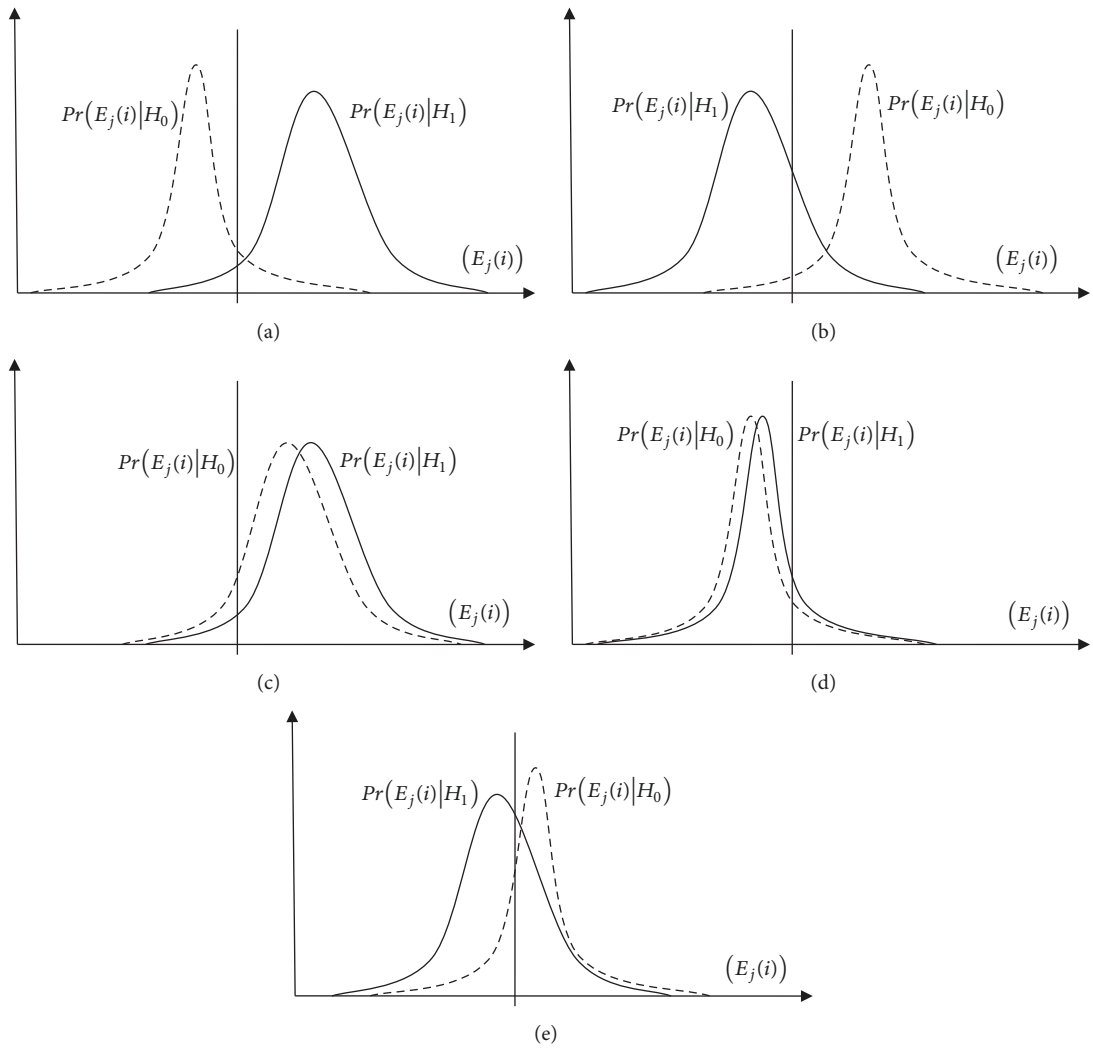

Figure 2: The probability density function of the users based on the reported statistics: (a) normal, (b) AO malicious, (c) AY malicious, (d) AN malicious, and (e) RO malicious.

(5) Average means and variance values while taking out the j^{th} user energy statistics.

$$\mu_{ja'}(i) = \left(\frac{\left(\sum_{j=1}^{M} \mu_{ja}(i)\right) - \mu_{ja}(i)}{(M-1)} \right), \quad i \in 1, \ldots N$$
$$\sigma^2_{jb'}(i) = \left(\frac{\left(\sum_{j=1}^{M} \sigma^2_{jb}(i)\right) - \sigma^2_{jb}(i)}{(M-1)} \right), \quad i \in 1, \ldots, N \tag{6}$$

(6) One-to-many relationship based KLD

$$K_j(i) = KL\left(\mu_{ja'}(i), \mu_{ja}(i), \sigma^2_{jb'}, \sigma^2_{jb}\right) \tag{7}$$

(7) Weights for the j^{th} user in the i^{th} interval

$$\boldsymbol{c}_j(i) = \left(\frac{1}{K_j(i)} \right)$$
$$\boldsymbol{w}_j(i) = \left(\frac{\boldsymbol{c}_j(i)}{\sum_{j=1}^{M} \boldsymbol{c}_j(i)} \right), \quad i \in 1, \ldots, N \tag{8}$$

(8) End SUs

(9) If $\sum_{j=1}^{M} \boldsymbol{w}_j(i) * E_j(i) \geq \varepsilon$

(10) Global decision, $G_B(i) = H_1$

(11) Else

(12) Global decision, $G_B(i) = H_0$

(13) End

(14) End limit

3.1. Data Collection and Adjustments by the FC. FC receives the individual soft energy information $E_j(i)$ in the i^{th} interval from all the j^{th} cooperating SUs as

$$\boldsymbol{e} = \left[E_1(i)\ \ E_2(i)\ \ E_3(i)\ \ \ldots\ \ E_M(i)\right], \quad i \in 1, \ldots, N \tag{9}$$

where $\boldsymbol{e}$ is a row vector containing the soft spectrum sensing data of all M users during the i^{th} interval. The soft energy report $E_j(i)$ has mean and variance (μ_1, σ_1^2) under hypothesis H_1 and (μ_0, σ_0^2) under the H_0 hypothesis.

FC further determines new values of the mean and variance for all users in the i^{th} sensing interval based on the received energy observations in (9) as

$$\boldsymbol{a}(i) = \left[\mu_{1a}(i)\ \ \mu_{2a}(i)\ \ \mu_{3a}(i)\ \ \ldots\ \ \mu_{Ma}(i)\right], \quad i \in 1, \ldots, N \tag{10}$$

$$\text{where } \mu_{ja}(i) = \begin{Bmatrix} z_1\mu_{j1} + z_2E_j(i), & H_1 \\ z_1\mu_{j0} + z_2E_j(i), & H_0 \end{Bmatrix} \tag{11}$$

Here $\mu_{ja}(i)$ is the new value of the mean for the j^{th} SU in the i^{th} sensing interval, which is updated according to the received energy $E_j(i)$ and (z_1, z_2) preselected constants.

Similarly, new variance values are determined and collected based on the received energy $E_j(i)$ as

$$b(i) = \left[\sigma_{1b}^2\ \ \sigma_{2b}^2\ \ \sigma_{3b}^2\ \ \ldots\ \ \sigma_{Mb}^2\right], \quad i \in 1, \ldots, N \tag{12}$$

$$\text{where } \sigma_{jb}^2(i) = \begin{Bmatrix} z_1\sigma_{j1}^2 + z_1\left[E_j(i) - \mu_{j1}\right]^2, & H_1 \\ z_1\sigma_{j0}^2 + z_1\left[E_j(i) - \mu_{j0}\right]^2, & H_0 \end{Bmatrix} \tag{13}$$

In the new mean and variance measurements in (11) and (13), the constant $z_1 = (k-1)/(k)$ and the constant $z_2 = (1/k)$, where the constant k is the effective level of the mean and variance by the received energy $E_j(i)$.

3.2. One-to-Many Relationship Based KLD Measurement. After the collection of mean and variance information on behalf of all M users in the i^{th} sensing intervals, FC measures a difference in the mean and variance of the j^{th} user energy statistics with all other users. The average mean values are measured on behalf of all M SUs based on the new mean values of (10) as

$$\mu_{ja'}(i) = \left(\frac{\left(\sum_{j=1}^{M}\mu_{ja}(i)\right) - \mu_{ja}(i)}{(M-1)}\right) \tag{14}$$

The one-to-many difference results of the mean for all M SUs are collected as

$$\boldsymbol{a}'(i) = \left[\mu_{1a'}(i)\ \ \mu_{2a'}\ \ \ldots\ \ \mu_{Ma'}(i)\right], \quad i \in 1, \ldots, N \tag{15}$$

Similarly, the average variance values are measured on behalf of all M SUs based on the new variance values of (12) as follows:

$$\sigma_{jb'}^2(i) = \left(\frac{\left(\sum_{j=1}^{M}\sigma_{jb}^2(i)\right) - \sigma_{jb}^2(i)}{(M-1)}\right) \tag{16}$$

$$\boldsymbol{b}'(i) = \left[\sigma_{1b'}^2(i)\ \ \sigma_{2b'}^2(i)\ \ \sigma_{3b'}^2(i)\ \ \ldots\ \ \sigma_{Mb'}^2(i)\right], \quad i \in 1, \ldots, N \tag{17}$$

Here $\mu_{ja'}(i)$ is the average mean and $\sigma_{ja'}^2(i)$ is the average variance value of the energy samples provided by all other users while ignoring the mean and variance results of the j^{th} user. These mean and variance values are obtained by excluding the j^{th} user. The result in (15) and (17) determines the impact of not including each cooperative user during the average mean and variance observation measurement. As all MUs including AY, AN, AO, and RO have dissimilar results of the mean and variance in comparison with normal SUs, therefore the average results attained against these users are different from the normal SUs in (15) and (17).

The KLD value for the j^{th} SU is determined between the individual sensing results in (10), (12), and the information provided by all other SU information as in (15) and (17) as

$$K_j(i) = KL\left(\mu_{ja'}(i), \mu_{ja'}(i), \sigma_{jb'}^2(i), \sigma_{jb}^2(i)\right) \tag{18}$$

where $K_j(i)$ denotes the KLD result in the presence and absence hypothesis of the j^{th} SU in the i^{th} interval. These KLD scores against each SU sensing are modified as

$$c_j(i) = \left(\frac{1}{K_j(i)}\right), \quad i \in 1, \ldots, N,\ j \in 1, \ldots, M \tag{19}$$

The result in (19) is normalized for assigning weights to each SU decision as

$$w_j(i) = \left(\frac{c_j(i)}{\sum_{j=1}^{M}c_j(i)}\right), \quad i \in 1, \ldots, N,\ j \in 1, \ldots, M \tag{20}$$

In (20) the users with abnormal behavior acquire lower weights in comparison with normal users.

Table 1 shows the weight measurement for the normal and malicious users against various signals-to-noise ratios. These weights are obtained for the case when one of the four categories of MUs participates in CSS. In Table 1 as the value of signal-to-noise ratio increases the weight assigned to these MUs decreases while the normal user's weights increase.

Similarly, Table 2 shows the weights for the case when all four categories of MUs participate in CSS. In Table 2, the weight result assigned to each MU is shown along with the average weights received by all the normal cooperative SUs. In this case, the different weights received by these MUs approach zero with increasing signal-to-noise ratio while the normal SUs weights increase with increasing signal-to-noise ratio.

Table 1: KLD weights assigned by the FC under one category of MU participation.

SNR (dB)	Weights				
	AY only	AN only	AO only	RO only	Normal User
-20	0.006757	0.006553	0.016615	0.008775	0.080399
-19	0.006750	0.006551	0.008679	0.006123	0.080798
-18	0.006745	0.006547	0.008341	0.005763	0.081049
-17	0.006740	0.006544	0.008341	0.005757	0.081110
-16	0.006737	0.006539	0.006206	0.005616	0.081198
-15	0.006731	0.006537	0.006186	0.005537	0.081231
-14	0.006722	0.006532	0.006164	0.005393	0.081266
-13	0.006717	0.006530	0.005722	0.005295	0.081306
-12	0.006715	0.006526	0.005722	0.005290	0.081324
-11	0.006711	0.006525	0.005629	0.004688	0.081428
-10	0.006709	0.006521	0.005629	0.004318	0.081441
-9	0.006706	0.006518	0.005190	0.003863	0.081545
-8	0.006704	0.006516	0.004947	0.003836	0.081636
-7	0.006701	0.006510	0.003674	0.003773	0.081739
-6	0.006692	0.006505	0.001509	0.003198	0.081777
-5	0.006687	0.006502	0.001507	0.001335	0.082069

Table 2: KLD weights assigned by the FC when all categories of MUs participate.

SNR (dB)	Weights				
	1 AY	1 AN	1 AO	1 RO	Normal User
-20	0.000682	0.000359	0.001661	0.065425	0.077865
-19	0.000523	0.000331	0.001155	0.012339	0.082344
-18	0.000466	0.000319	0.001085	0.006149	0.082800
-17	0.000379	0.000277	0.001037	0.005841	0.082875
-16	0.000287	0.000212	0.000825	0.005060	0.082967
-15	0.000229	0.000169	0.000817	0.004495	0.082984
-14	0.000175	0.000159	0.000766	0.004449	0.083008
-13	0.000160	0.000139	0.000645	0.004355	0.083035
-12	0.000137	0.000113	0.000637	0.003774	0.083047
-11	0.000112	0.000080	0.000477	0.002980	0.083048
-10	0.000096	0.000079	0.000469	0.002719	0.083058
-9	0.000095	0.000070	0.000285	0.002563	0.083061
-8	0.000094	0.000069	0.000242	0.002524	0.083136
-7	0.000082	0.000066	0.000222	0.002486	0.083254
-6	0.000055	0.000039	0.000137	0.001171	0.083307
-5	0.000010	0.000008	0.000057	0.000266	0.083694

3.3. Global Decision at FC. On the basis of weighted results measured to guarantee the authenticity of each SU sensing information in (20), the global statement $G_B(i)$ is declared by the FC as

$$G_B(i) = \left\{ \begin{array}{l} H_1, \ \sum_{j=1}^{M} \boldsymbol{w}_j(i) * E_j(i) \geq \varepsilon \\ H_0, \ otherwise \end{array} \right\}, \quad i \in 1, \ldots, N \tag{21}$$

where $\boldsymbol{w}_j$ is the weight assigned to the j^{th} user energy in the data fusion at the FC and ε the threshold value for the detection of the PU. The lesser weight results are charged by the FC against the sensing information of a user with malicious behavior, while the normal user sensing report is assigned with a higher weight value. All MUs including AY, AN, AO, and RO are easily identified by the proposed scheme with their KLD behavior. The normal SUs have a higher KLD result because they have less inconsistency with the average of all other users sensing information. The MUs receive minimum weight because the information provided by MUs deviates more from the average sensing information provided by all other SUs. It is therefore noticeable that these MUs get lower weights as compared with normal SUs.

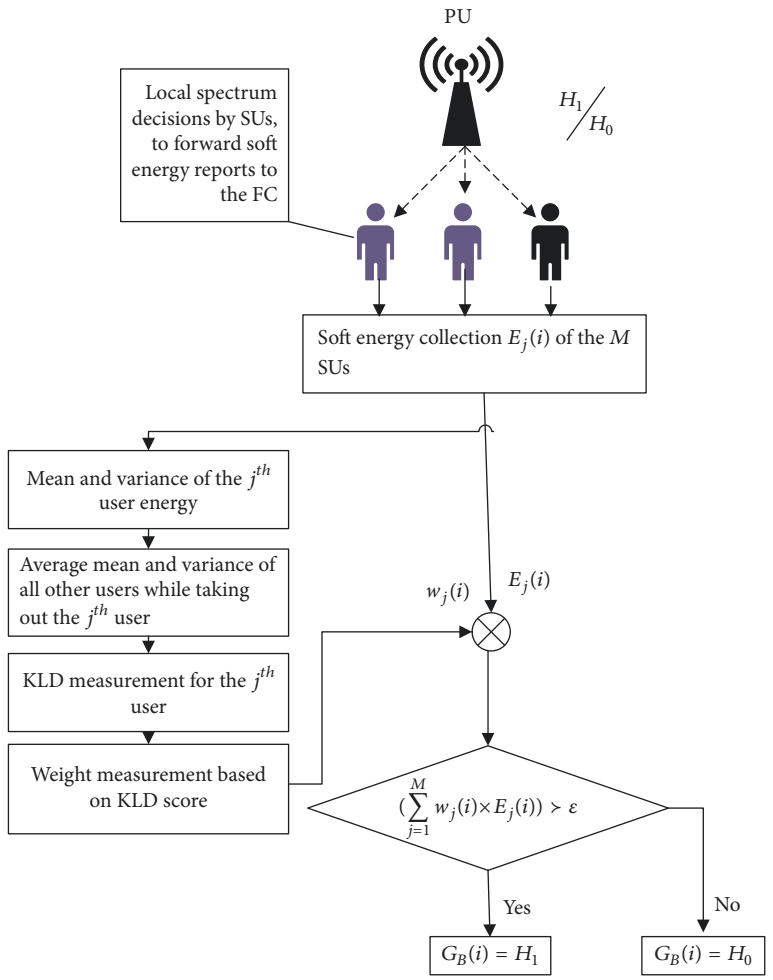

Figure 3: Flowchart of the proposed CSS mechanism.

3.4. Updating Statistics Based on the Global Decision. Due to the nonavailability of the exact information about the PU, optimal values of the means (μ_{j1}, μ_{j0}) and variances $(\sigma_{j0}^2, \sigma_{j1}^2)$ for measuring KLD are not possible. It is therefore good to consider the global decision $G_B(i)$ results as an estimate of the primary signal, in order to calculate and update these values. The updated mean and variance will be used by the FC in the KLD calculation in the next sensing interval.

$$E_{j1} = \left\{E_j(i) \mid H_1\right\} \approx \left\{E_j(i) \mid G_B(i) = H_1\right\} \quad (22)$$

$$E_{j0} = \left\{E_j(i) \mid H_0\right\} \approx \left\{E_j(i) \mid G_B(i) = H_0\right\} \quad (23)$$

After the establishment of universal decision at the FC, resultant decision $G_B(i) = 1$ will update mean μ_{j1} and variance σ_{j1}^2 values under the H_1 hypothesis as follows:

$$\begin{aligned} \mu_{j1} &= B_1 \mu_{j1} + B_2 Z_j(i) \\ \sigma_{j1}^2 &= B_1 \sigma_{j1}^2 + \frac{B_1}{B_2}\left[Z_j(i) - \mu_{j1}\right]^2 \end{aligned} \quad (24)$$

Similarly, the decision $G_B(i) = 0$ will update mean μ_{j0} and variance σ_{j0}^2 under the H_0 hypothesis for all cooperative users as

$$\begin{aligned} \mu_{j0} &= B_1 \mu_{j0} + B_2 E_j(i) \\ \sigma_{j0}^2 &= B_1 \sigma_{j0}^2 + \frac{B_1}{B_2}\left[E_j(i) - \mu_{j0}\right]^2 \end{aligned} \quad (25)$$

In (25) $B_1 = z/(z-1)$ and $B_2 = 1/z$, where z indicate the window size of the sensing history for the estimated mean and variance.

The proposed scheme flowchart diagram in Figure 3 illustrates the stepwise procedure of the local detection, KL divergence measurement based on the weight assignments at the FC, and global decision establishment by the FC.

4. Numerical Results and Discussion

In order to get simulation results for the CRN, parameters settings are made with 10, 16, 20, and 30 total cooperative users. Out of the total cooperative SUs, four users are intentionally selected as AY, AO, RO, and AO nature of MUs. The average signal-to-noise ratios for the simulation

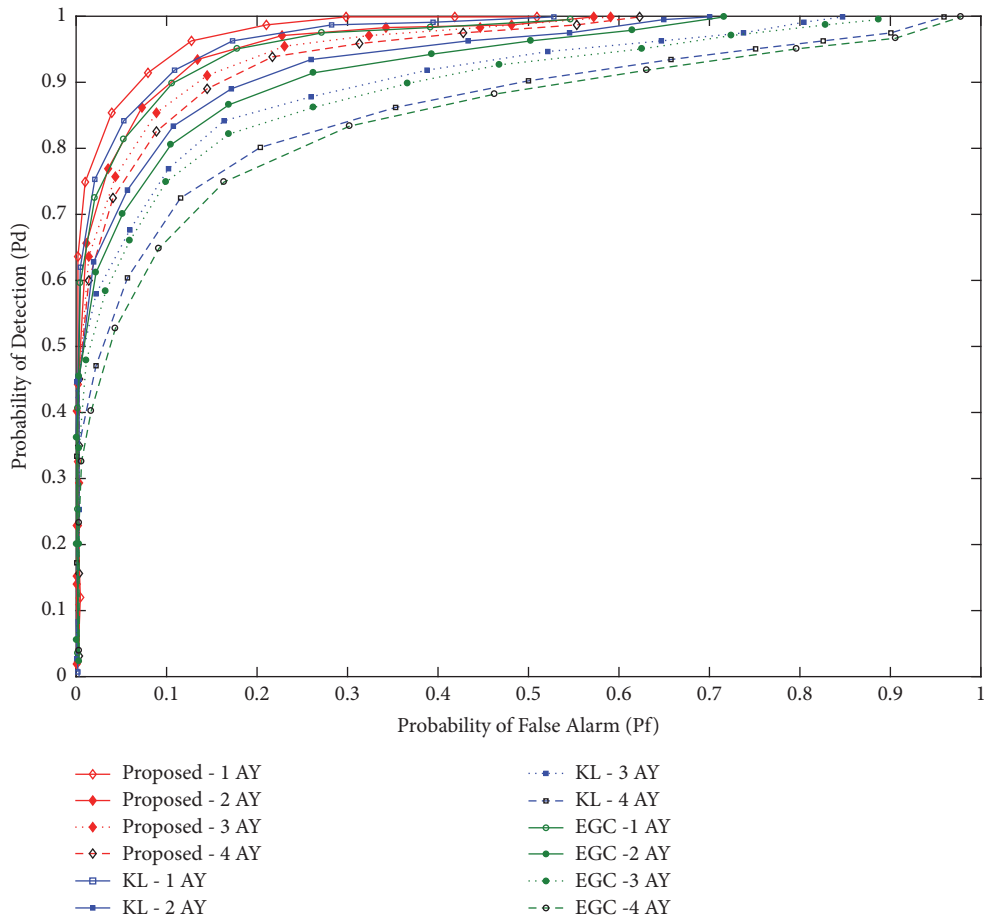

Figure 4: Detection vs. false alarm results with AY malicious users.

are selected as -20 dB to -5 dB for all SUs. The sensing time for each SU is selected as 1 ms containing 270 samples in each sensing interval. Total sensing intervals for the cooperative users are selected as 200. The RO users perform malicious acts probabilistically in the intervals 1 to N. The window size (z) for updating mean and variance is selected as 270. In the study, all 4 categories of MUs, i.e., AY, AN, AO, and RO, are spread evenly.

The proposed KLD performance is compared with traditional KL and equal gain combination (EGC) schemes in 6 different cases as follows.

Case 1. In this case ROC results are drawn between the proposed method and traditional KL and EGC scheme under various signal-to-noise ratio values of -20 dB to -5 dB as displayed in Figure 4. MUs are selected as AY only in the first part of the comparison in Figure 4. Results are obtained for all combinations by taking the total AY users number as 1, 2, 3, and 4 subsequently. The results show that the proposed KLD scheme is more secure against the increasing number of AY users 1 to 4 and has better detection probability results in comparison with all other schemes. In Figure 4 when there is only 1 AY user active in CSS the ROC results of all fusion schemes are less affected, but when the total number of AY users is increased to 3 and 4 the proposed KL results dominate the traditional KL and EGC schemes by producing a high detection with fewer false alarms. The EGC scheme is more affected by the increasing number of AY users because EGC is giving equal weight to the detection performance of normal and AY users. The proposed KL is able to assign less weight to the AY users in comparison with normal SUs as it is clear from the average weight value measured against each AY users in Table 1. The less weight assigned to the AY users reduces the false data effect of the AY users participation in CSS. The harmful effect of the AY users contribution in CSS is further reduced with increasing average SNR by lowering the weight assignment to them in the global decision.

Case 2. In this part of the simulation, all parameters are kept similar to Case 1 with changing only the nature of MUs from AY to AN user. Comparison is made between proposed KL, traditional KL, and EGC scheme by testing the system against increasing AY users number from 1 to 4 as in Figure 5.

Since the proposed KL is treating AY and AN users similarly in determining the KLD, therefore using proposed KLD the weight that AN user receives is almost equal to the AY user weights in Case 1. The ROC performance of the proposed and all other schemes against the AN scenario is very similar to Case 1, due to the similar behavior of the AN user to that of the AY user. As in Case 1, when the numbers

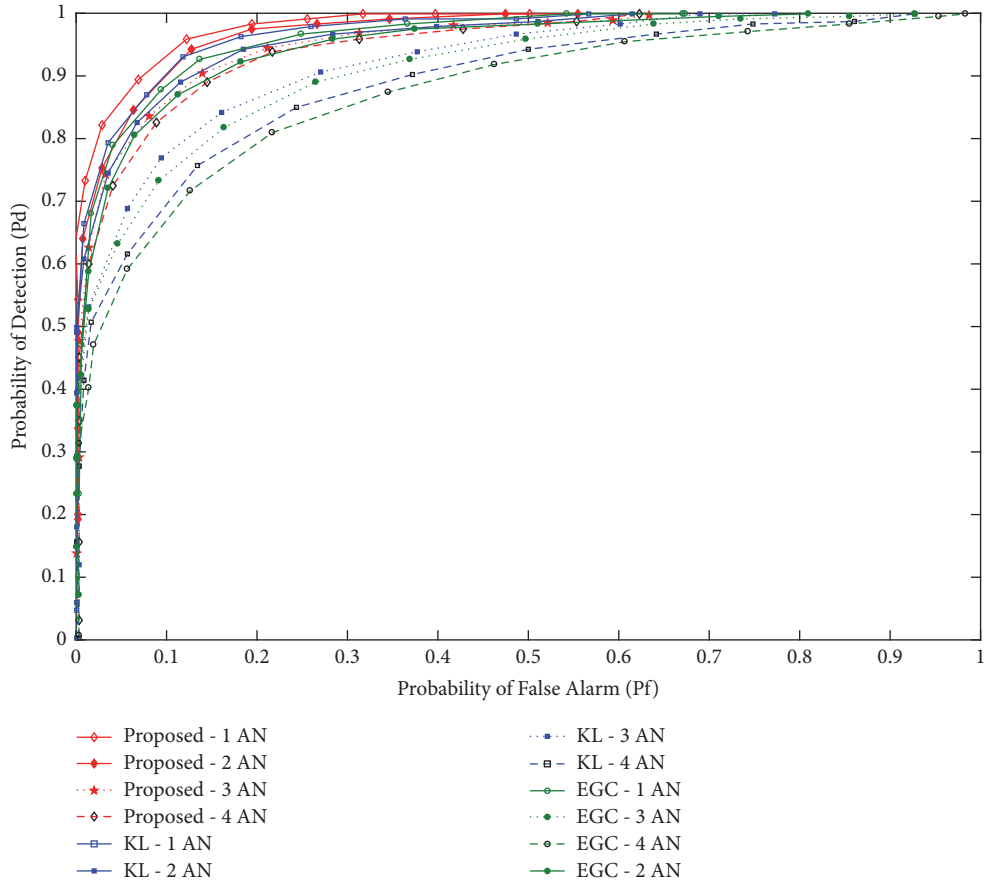

Figure 5: Detection vs. false alarm results with AN malicious users.

of AN users are increased from 1 to 4, the proposed KL is less affected by this increment in Figure 5. All AN users receive lower weight due to their KLD score results while the normal SUs receive higher weights in comparison with AN users which results in better performance of the proposed KL scheme. The traditional KL and EGC schemes performance in detecting the licensed PU channel reduces more quickly in comparison with the proposed KL method as the total AY increases from 1 to 4. The gap in the ROC curves of the traditional fusion schemes becomes wider for a total of 4 AN users from the one when only 1 AN user takes part as shown in Figure 5.

Case 3. In the third scenario detection and false alarm results are obtained for the increasing number of AO users from 1 to 4 in Figure 6 with the same parameters in Cases 1 and 2. Since the AO users have their mean and variance results opposite to the average mean and variance values provided by all other users, therefore, the proposed KL method is able to generate lower reliability report in terms of weight for the AO user in comparison with normal cooperative users. The results show that as the number of AO users increases to 4 few drops are observed in the ROC curve of the proposed scheme as compared with the traditional KL and EGC scheme. In comparison with Cases 1 and 2, the traditional soft combination schemes like KL and EGC performance degrade even more. The existence of AO users results in less correct detection and high false alarm rate of the PU spectrum for the EGC and KL scheme. Proposed method results in Figure 6 are followed by the KL while EGC has shown its worst performance among all fusions.

Case 4. The ROC results for the scenario in which only RO user participates in CSS are depicted in Figure 7. The RO user hides its malicious identity by acting probabilistically as AO at randomly selected sensing intervals in the N total intervals and is difficult to catch with the provided statistics.

The traditional KL and EGC schemes are not able to handle the RO user information intelligently and their ROC results degrade severely with the increased number of RO participations in Figure 7.

The proposed KL scheme is able to identify the RO users when they perform malicious acts probabilistically and generate better detection and false alarm results in Figure 7 compared with the traditional KL and EGC schemes. Results show that the proposed KLD is less affected by the increasing number of RO users, unlike the traditional EGC and KLD schemes. All the RO nature users in the proposed CSS receive lesser weights in comparison with weights obtained by the normal SUs because their malicious behavior is easily caught by the proposed KL scheme.

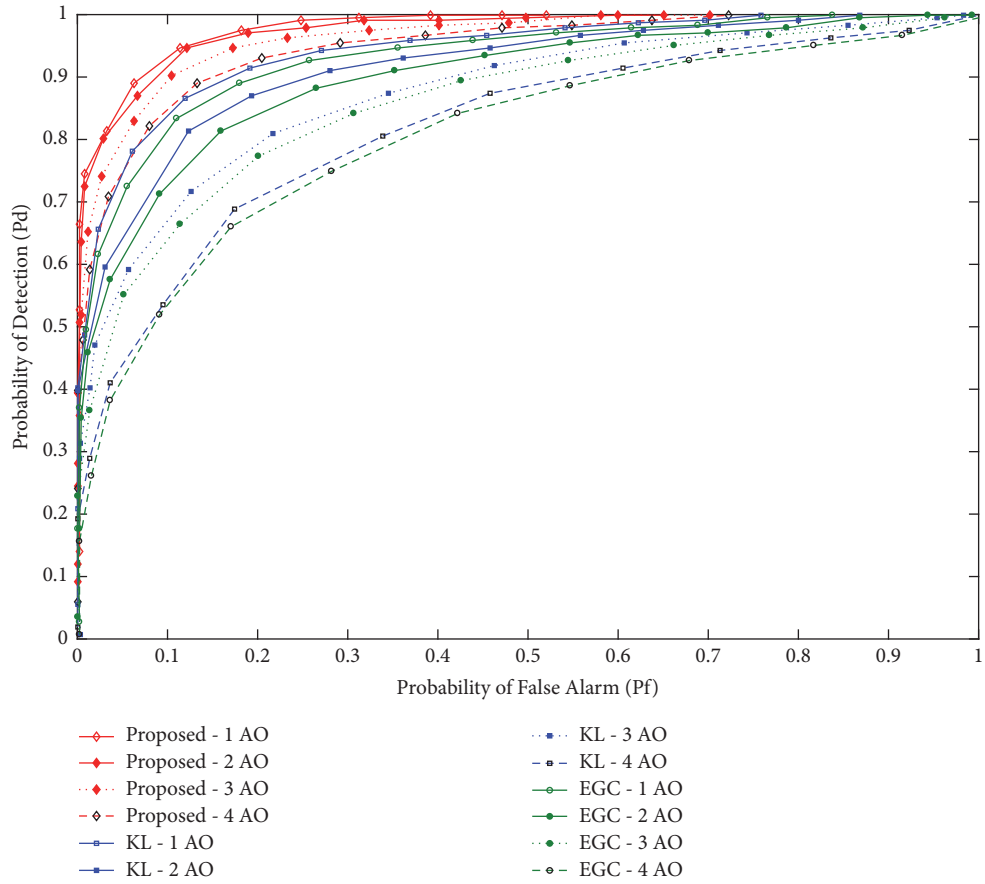

Figure 6: Detection vs. false alarm results with AO malicious users.

Case 5. In this part of the simulation as in Figure 8 MUs are equally selected in numbers as AY, AN, AO, and RO categories. The simulation is performed against an average signal-to-noise ratio of -12.5 dB.

The detection and false alarm probability results are obtained for the proposed, traditional KL, and EGC schemes for a total of 10, 20, and 30 cooperative SUs in Figure 8 under average signal-to-noise ratio of -12.5 dB and total 4 MUs. Figure 8 shows that the one-to-many relation based KLD scheme has better ROC performance than all other schemes with different levels of the cooperative users. It is noticeable that the detection performance is enhanced for all combination schemes with the increasing number of total cooperative and fixed MUs. The proposed method ROC results are more precise and superior to the traditional schemes, i.e., KLD and EGC schemes, at all levels of the total sensing users.

Case 6. In this case, the AY, AO, AN, and RO users number is kept the same. The total number of participating SUs in CSS is kept fixed as 16 and different ROC results are plotted for the one-to-many relations based KLD and other soft combination schemes at different levels of the averages signal-to-noise ratios.

The simulation results in Figure 9 show that under fixed malicious and total cooperative users the ROC performance rises with increasing signal-to-noise ratio values for all combination schemes. Similarly, in Figure 9 as the signal-to-noise ratio value increases from -15.5 dB to -9.5 dB, all schemes are able to generate a high detection rate with minimum false alarm. The proposed scheme ROC results are more accurate and precise than the traditional combination schemes at both SNR levels. The proposed method ROC improvement with increasing signal-to-noise ratio is due to more clear distinction in the energy distribution of the absence and presence hypothesis information provided by the normal and MUs. As the SNR increases in Figure 9, the proposed method detection results rise more quickly against other methods. These results also show that the CSS performance improves more with the increasing signal-to-noise ratio information in Case 6 as compared with the increasing total number of users in Case 5.

All the above experimental results clarify the fact that by following the proposed one-to-many relations based KLD method an improvement is obvious in the sensing performance at the FC. This improvement in performance is achieved by raising the detection probability and lowering the false alarm results leading to a reduction in the error probability of the system. The proposed fusion combination scheme shows optimum and accurate results in the presence of MUs. The use of the proposed method for calculating

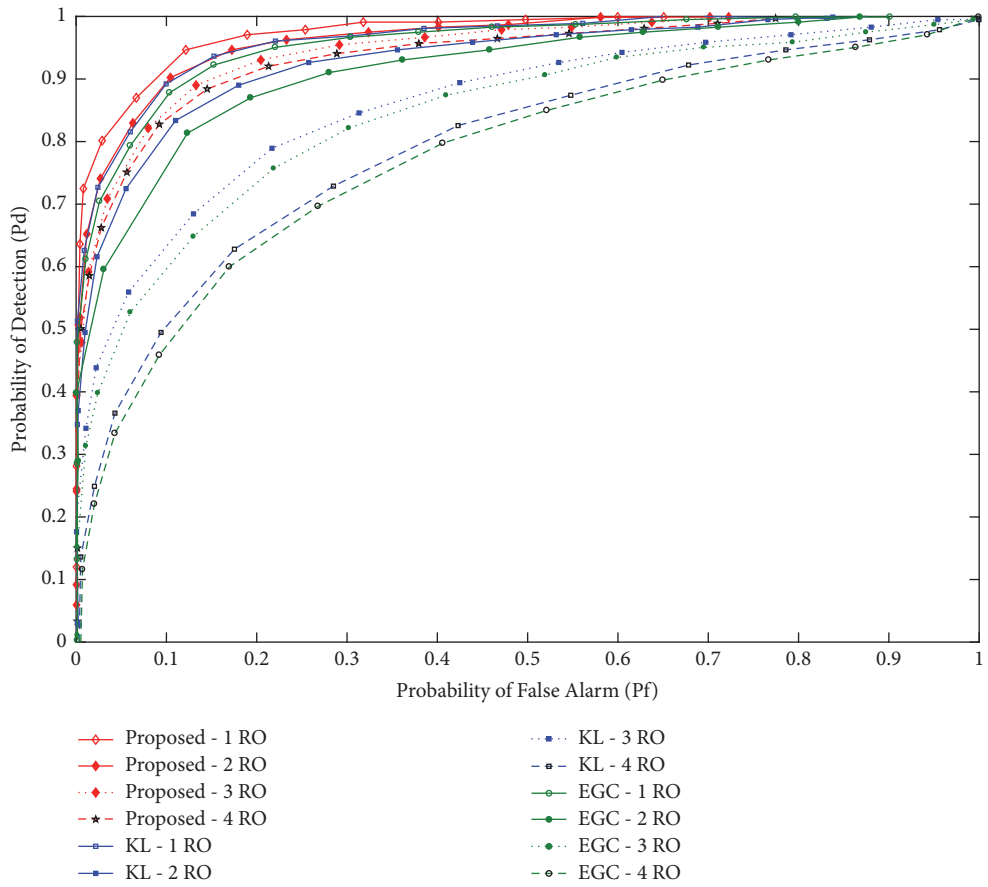

Figure 7: Detection vs. false alarm results with RO users.

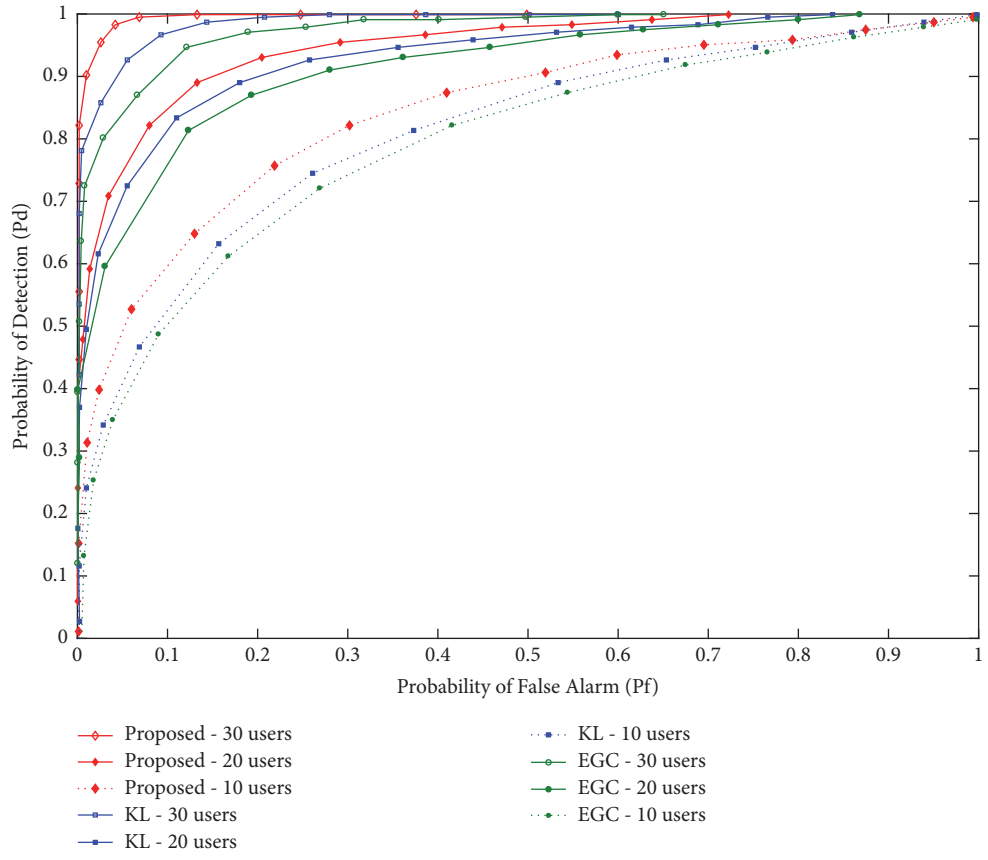

Figure 8: Detection vs. false alarm results with all MUs and different number of total reporting users.

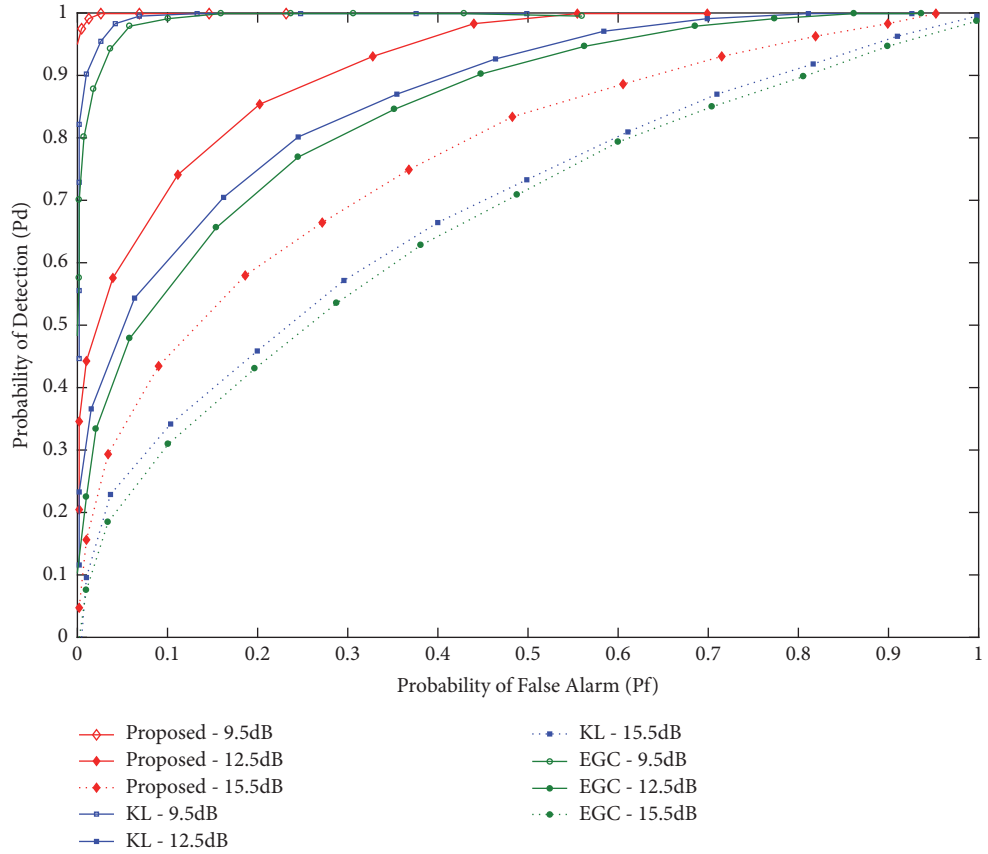

Figure 9: Detection vs. false alarm results with all MUs and different levels of signal-to-noise ratios.

weights following soft combination scheme makes the proposed CSS results more valid in the presence of malicious user. The simulation results show that the risk of AY, AN, RO, and AO users with CSS significantly reduces by adopting the proposed scheme. It is clear from the graphical result that the process of cooperation turns out to be more precise by using the suggested methodology. The one-to-many relation based KLD is able to generate better sensing results, by assigning lower weights to the MUs information, and is able to eliminate the effect of MUs in the resultant CSS.

5. Conclusion

In this paper, the efficiency degradation due to the presence of abnormal users in CSS is minimized using one-to-many relationship based KLD method for the PU detection. Functionality of the proposed scheme is verified in the presence of AY, AN, AO, and RO type MUs. FC first receives the individual sensing information of all SUs and then applies the proposed method for measuring weights against each SU. MUs with abnormal behavior as compared with normal SUs are given lower weights by the proposed scheme, while the normal SUs receive higher weights. FC further employs these weights in combining the sensing information of all SUs in predicting a global decision. The results show that the user with abnormal behavior has less impact on the global decision as compared to a normal SU decision. Simulation result reflects the superiority and authenticity of the proposed scheme in producing more precise and reliable decisions as compared with EGC and traditional KL fusion schemes.

Data Availability

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

Disclosure

The authors received no specific funding for this work.

Conflicts of Interest

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

References

[1] 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.

[2] R. Chen, J.-M. Park, Y. T. Hou, and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 50–55, 2008.

[3] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Proceedings of the IEEE International Conference on Communications*, pp. 1658–1663, Istanbul, Turkey, July 2006.

[4] S. Kaur, "Intelligence in wireless networks with cognitive radio networks!," *IETE Technical Review*, vol. 30, no. 1, pp. 6–11, 2013.

[5] 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.

[6] L. Zhai, H. Wang, and C. Gao, "A spectrum access based on quality of service in cognitive radio networks," *PLOS ONE*, vol. 11, no. 5, pp. 2005–2009, 2016.

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

[8] A. Taherpour, M. Nasiri-Kenari, and S. Gazor, "Multiple antenna spectrum sensing in cognitive radios," *IEEE Transactions on Wireless Communications*, vol. 9, no. 2, pp. 814–823, 2010.

[9] C.-H. Hwang, G.-L. Lai, and S.-C. Chen, "Spectrum sensing in wideband OFDM based cognitive radio," *IEEE Transactions on Signal Processing*, vol. 58, no. 2, pp. 709–719, 2015.

[10] A. Ali and W. Hamouda, "Spectrum monitoring using energy ratio algorithm for OFDM-based cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 4, pp. 2257–2268, 2015.

[11] 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.

[12] 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, 2017.

[13] M. A. Raja, M. S. Aslam, N. I. Chaudhary, and W. U. Khan, "Bio-inspired heuristics hybrid with interior-point method for active noise control systems without identification of secondary path," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 2, pp. 246–259, 2018.

[14] Y. Eghbali, H. Hassani, A. Koohian, and M. Ahmadian-Attari, "Improved energy detector for wideband spectrum sensing in cognitive radio networks," *Radioengineering*, vol. 23, no. 1, pp. 430–434, 2014.

[15] H. Guo, W. Jiang, and W. Luo, "Linear Soft Combination for Cooperative Spectrum Sensing in Cognitive Radio Networks," *IEEE Communications Letters*, vol. 21, no. 7, pp. 1573–1576, 2017.

[16] J. Wang, S. Feng, Q. Wu, X. Zheng, Y. Xu, and G. Ding, "A robust cooperative spectrum sensing scheme based on Dempster-Shafer theory and trustworthiness degree calculation in cognitive radio networks," *EURASIP Journal on Advances in Signal Processing*, vol. 2014, no. 1, 2014.

[17] J. Tong, M. Jin, Q. Guo, and Y. Li, "Cooperative Spectrum Sensing: A Blind and Soft Fusion Detector," *IEEE Transactions on Wireless Communications*, vol. 17, no. 4, pp. 2726–2737, 2018.

[18] M. Zheng, W. Liang, H. Yu, and M. Song, "SMCSS: A Quick and Reliable Cooperative Spectrum Sensing Scheme for Cognitive Industrial Wireless Networks," *IEEE Access*, vol. 4, pp. 9308–9319, 2016.

[19] J. Wang, I. Chen, J. J. Tsai, and D. Wang, "Trust-based mechanism design for cooperative spectrum sensing in cognitive radio networks," *Computer Communications*, vol. 116, pp. 90–100, 2018.

[20] F. Zaman, "Joint Angle-Amplitude Estimation for Multiple Signals with L-Structured Arrays Using Bioinspired Computing," *Wireless Communications and Mobile Computing*, vol. 2017, Article ID 9428196, 12 pages, 2017.

[21] X. Liu, J. Yan, and K. Chen, "Optimal energy harvest-based weighed cooperative spectrum sensing in cognitive radio," in *Proceedings of the 2016 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1–5, Kauai, HI, USA, Feburary 2016.

[22] P. D. Sutton, K. E. Nolan, and L. E. Doyle, "Cyclostationary signatures in practical cognitive radio applications," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 13–24, 2008.

[23] S. A. Hosseini, B. Abolhassani, and S. M. S. Sadough, "A new protocol for cooperative spectrum sharing in mobile cognitive radio networks," *Radioengineering*, vol. 24, no. 3, pp. 757–764, 2015.

[24] L. Zhang, G. Ding, Q. Wu, and F. Song, "Defending against byzantine attack in cooperative spectrum sensing: defense reference and performance analysis," *IEEE Access*, vol. 4, pp. 4011–4024, 2016.

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

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

[27] R. Yu, Y. Zhang, Y. Liu, S. Gjessing, and M. Guizani, "Securing cognitive radio networks against primary user emulation attacks," *IEEE Network*, vol. 29, no. 4, pp. 68–74, 2015.

[28] 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.

[29] V. Heip 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.

[30] H. Guo, N. Reisi, W. Jiang, and W. Luo, "Soft combination for cooperative spectrum sensing in fading channels," *IEEE Access*, vol. 5, pp. 975–986, 2017.

[31] M. Emami, H. Zarrabi, M. R. Jabbarpour, M. Sadat Taheri, and J. J. Jung, "A soft cooperative spectrum sensing in the presence of most destructive smart PUEA using energy detector," *Concurrency and Computation: Practice and Experience*, vol. 30, no. 15, p. e4524, 2018.

[32] Y. L. Lee, W. K. Saad, A. A. 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.

[33] D. Teguig, B. Scheers, and V. Le Nir, "Data fusion schemes for cooperative spectrum sensing in cognitive radio networks," in *Proceedings of the 2012 Military Communications and Information Systems Conference, MCC 2012*, pp. 104–110, Poland, October 2012.

[34] J. So and W. Sung, "Group-Based Multibit Cooperative Spectrum Sensing for Cognitive Radio Networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10193–10198, 2016.

[35] S. Nallagonda, Y. R. Kumar, and P. Shilpa, "Analysis of hard-decision and soft-data fusion schemes for cooperative spectrum sensing in rayleigh fading channel," in *Proceedings of the*

7th IEEE International Advanced Computing Conference, IACC 2017, pp. 220–225, India, January 2017.

[36] W. Ejaz, G. Hattab, T. Attia, M. Ibnkahla, F. Abdelkefi, and M. Siala, "Joint Quantization and Confidence-Based Generalized Combining Scheme for Cooperative Spectrum Sensing," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1909–1920, 2018.

[37] H. Wu, F. Yao, Y. Chen, Y. Liu, and T. Liang, "Multibit-Quantization-Based Collaborative Spectrum Sensing Scheme for Cognitive Sensor Networks," *IEEE Access*, vol. 5, pp. 25207–25216, 2017.

[38] M. A. Raja, A. A. Shah, A. Mehmood, N. I. Chaudhary, and M. S. Aslam, "Bio-inspired computational heuristics for parameter estimation of nonlinear Hammerstein controlled autoregressive system," *Neural Computing and Applications*, vol. 29, no. 12, pp. 1455–1474, 2018.

[39] S. Bhattacharjee, P. Das, S. Mandal, and B. Sardar, "Optimization of probability of false alarm and probability of detection in cognitive radio networks using GA," in *Proceedings of the 2015 IEEE 2nd International Conference on Recent Trends in Information Systems (ReTIS)*, pp. 53–57, Kolkata, India, July 2015.

[40] 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, 2018.

[41] N. Gul, A. Naveed, A. Elahi, T. Saleemkhattak, and I. M. Qureshi, "A combination of double sided neighbor distance and Genetic Algorithm in cooperative spectrum sensing against malicious users," in *Proceedings of the 14th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2017*, pp. 746–753, Pakistan, January 2017.

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

[43] 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.

[44] A. A. EL-Saleh and K. Hussain, "Cognitive radio engine model utilizing soft fusion based genetic algorithm for cooperative spectrum optimization," *International Journal of Computer Networks and Communications*, vol. 2, no. 3, pp. 169–173, 2013.

[45] 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, Engineering & Information Technology*, pp. 223–228, Sousse, Tunisia, 2014.

[46] N. Gul, I. M. Qureshi, A. Omar, A. Elahi, S. Khan, and B. Podobnik, "History based forward and feedback mechanism in cooperative spectrum sensing including malicious users in cognitive radio network," *PLoS ONE*, vol. 12, no. 8, p. e0183387, 2017.

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