Wireless Personal Communications (2023) 130:1993–2012
https://doi.org/10.1007/s11277-023-10368-6

# Extreme Learning Machine Based Identification of Malicious Users for Secure Cooperative Spectrum Sensing in Cognitive Radio Networks

Manish Kumar Giri[1] · Saikat Majumder[1]

Accepted: 6 March 2023 / Published online: 21 March 2023

**Abstract**
Cognitive radio (CR) technology has evolved over the traditional radio to successfully utilize the unused frequency spectrum. In CR the secondary users (SUs) perform cooperative spectrum sensing to access the available frequency band. The opportunistic nature of sensing prevents any interference with primary users (PUs) in the network. However, the presence of security threats like malicious users (MUs) strongly influences the performance. In CR network, MUs act like normal SUs and transmit false information to the fusion center and degrades the performance. To overcome this issue, we proposed an extreme learning machine (ELM) based approach to classify the legitimate SUs with the MUs. In this work, ELM is used as a classifier to separate the legitimate SUs and MUs. Extensive simulation results are presented to highlight the effectiveness of the proposed approach. The proposed approach highlights significant improvement in terms of training time and provides better trade-off compare to the other competitive techniques in the literature.

**Keywords** Cooperative spectrum sensing · Malicious users · ELM · Classification · Cognitive radio · Detection · Security

## 1 Introduction

The continual advances in wireless technologies have caused a rapid increase in the use of advanced wireless devices. This has produced significant interest for more spectrum resources over recent years, that causes spectrum scarcity. The underutilization of the spectrum band is the primary reason behind the spectrum scarcity as mentioned by the FCC report [1]. Cognitive radio (CR) has emerged as a reliable solution for spectrum scarcity problem, and gained popularity among researchers worldwide [2]. CR is one of the most prolific technology that provide effective spectrum utilization, in which parameters can be

✉ Manish Kumar Giri
mkgiri.phd2018.etc@nitrr.ac.in

Saikat Majumder
smajumder.etc@nitrr.ac.in

[1] Department of Electronics and Communication, National Institute of Technology, Raipur, Raipur, CG 492010, India

systematically adjusted according to the environment. The users that have license to use the spectrum are called primary users (PUs). They can transmit their information without any restriction. Whereas, secondary users (SUs) are unlicensed users, and can access the spectrum when channel is available or not used by the PUs [3]. One of the most important concept relates to the CR is spectrum sensing (SS). A number of different SS techniques have been proposed and utilized such as energy detection, eigenvalue based detection, waveform based detection, and cyclostationary detection [4]. Out of these methods energy detection (ED) is the widely utilized approach due to its simplicity and non-dependability on the prior information about the PU. Each SUs performs local sensing, however the sensing results gets severely affected by the fading, shadowing, and hidden node problems [5]. This further causes reduction in detection rate and increases the false alarm in the process. The inability to detect the PU successfully reduces the chances of opportunistic spectrum access by the SUs. Moreover, there will be chances of interference in the network if misdetetcion happens.

These issues are well covered in the literature, and researchers proposed cooperative spectrum sensing (CSS) to prevent it. The PU activity detection is significantly improved by the application of CSS and performance of secondary network also highlights an improvement [6–8]. CSS techniques have been adopted for both distributed and centralized type CR scenario. In distributed type of SS approach, each SU perform individual sensing and decides about the spectrum availability. On other hand, in centralized type of SS approach, local sensing is performed by each SU, and transmits their results to the fusion center (FC) to identify the PU presence or channel availability. The final decision about the channel availability is made at the FC, and it depends on collective results of all SUs. Several fusion algorithms like hard decision or soft decision fusion algorithms are applied to make a final decision [9]. However, CSS approach has high susceptibility to the security threats. It is important that the CR system is secure and amenable to underlay infrastructure [10]. Numerous security attacks that affect the network performance are highlighted in the literature. The most primary attacks are primary user emulation attack (PUEA) and spectrum sensing data falsification attack (SSDF) [11, 12].

In PUEA, a direct interference from the outliers can be recognized, these outliers tries to act like PU and disturbs the sensing process of the SUs. In this way the FC makes a decision that the channel is busy and the SUs hold their spectrum access process. Whereas in the SSDF attack, false sensing information is transmitted to the FC. This causes an inaccuracy in final global decision about the PU channel availability. Some studies have mentioned about the different possible combination of SSDF attack [13]. First one is always yes malicious user (AYMU) attack; in which SU always transmits ‘1’ (channel unavailable) to the FC irrespective of the determined local result. This attack will cause a halt in opportunistic spectrum access by denying access to the SUs. In contrast, in always no malicious user (ANMU) attack SUs always transmits ‘0’ (channel available) to the FC. Hence, this attack will causes interference to the PU channel. The other attack is always opposite malicious user (AOMU) attack, in which always opposite of local result is transmit to FC. AOMU is a critical attack, and it can increase false alarm in the sensing process. In the random yes malicious user (RYMU) attack, malicious users (MUs) transmit ‘1’ (channel unavailable) randomly to FC irrespective to local result. Whereas, in random no malicious user (RNMU) attack, MUs transmit ‘0’ (channel available) randomly to the FC irrespective to the local sensing result. Lastly the random opposite malicious user (ROMU) attack, in which MUs randomly transmits opposite of the local sensing results to the FC. Several new strategies are proposed by researchers to reduce the impact of these attacks [14–16]. In the next section we highlighted some current state of the art related to the concerned area.

## 2 Related Works

Several techniques have been proposed by the researchers to mitigate the interference between PUs and SUs and to detect the MUs successfully. Authors in [17] proposed a simple outlier detection approach to successfully detect the MUs presence in CR network. The authors considered a low harm type selfish or greedy attack scenario. In [18] a hidden Markov model (HMM) based approach was proposed to identify the MUs presence in CR network. Dempster-Shafer theory-based approach was utilized in [19] to identify the MUs presence. Authors in [15, 20] proposed multiple approach to prevent the effect of data falsification attack in CR network scenario. Authors in [21] developed a metaheuristic-based scenario to identify the presence of MUs in the network. Authors adopted genetic algorithm and calculated the z-score to achieve accurate sensing results. In [22], authors proposed a technique for outlier detection considering fading and noisy environment in a wireless regional area networks (WRANs) scenario. A different approach for compressive SS was proposed by authors in [12] by reconstructing the original signal to identify the presence of MUs. Authors in [23] developed a unique approach covering experimental analysis based on non-Kruskal-Wallis and Conover-Inman theory to detect the presence of MUs in the network.

Beside these approaches emergence of machine learning (ML) has also influenced the concerned research domain. ML impact can be successfully seen by the work performed by the researchers in this area. Different ML based techniques are available in the literature that successfully exploited both the supervised and unsupervised learning techniques for identification of MUs in the network. In most cases the support vector machine (SVM) algorithm provides better results compare to the other approaches as mentioned in [24–26]. The applicability of different kernel function available in SVM makes them liable to adopt for classification task. Authors in [27] developed a ML based technique for CSS, in which final global decision was made by the FC adopting a weighted fusion rule. However, Identification of MUs was not considered in the developed work. Authors in [28] adopted the reinforcement learning approach to propose a transmission scheduling technique in CR-IoT scenarios. The authors highlighted the transmission of packets via multiple channels to improve the system throughput. However, MUs detection was not performed in the concerned work. Recently authors in [29, 30], proposed unsupervised learning based approach for CSS in CR networks. However, the MUs detection was not analysed. A novel technique based on fuzzy SVM algorithm was proposed by authors in [31] considering the noise uncertainty problem. However, MUs impact was not studied in the work. Authors in [32] developed a scenario for multiclass hypothesis testing for CR network using the SVM algorithm. However, authors did not analyse the MUs detection in their work. A CSS scheme based on ML algorithms was proposed by authors in [33], where different grouping techniques were used to minimize the overhead. However, the MUs detection was not analysed in the work.

Authors in [34] adopted reinforcement learning and proposed an efficient transmission mode selection technique for CSS. Authors highlighted an improvement in throughput, energy efficiency and reduced the PU interference. However, the study related to MUs detection was not performed. A detailed survey was provided by authors in [35], in which authors highlighted the ML application in several CR related areas such as modulation classification and power allocation. However, the study related to MUs detection was not mentioned. Authors in [36] utilized different supervised and unsupervised ML algorithms for CSS in CR network scenario. However, study of MUs detection for security related aspect was not provided. In [37], the authors developed a technique utilizing the SVM algorithm to classify the PUEA present in the network. An outlier detection approach was proposed by authors in [38], using spatial correlation between the SUs. Recently authors in [39] developed a ML based approach adopting the pattern described link signature (PDLS) method to identify the legitimate users and the MUs in the network. In [40] authors proposed an ML based approach for successful distribution of spectrum in CR scenario. Authors in [41], studied the PUEA and jamming attacks in a CR network. They proposed a ML based algorithm to detect the spectrum hole and attacks present in the network. In [42], authors proposed a MUs classification approach utilizing the SVM algorithm for a dataset. However, training and testing time-based study was not performed in the work. In recent development authors in [43] proposed a SVM based algorithm to detect the MUs presence in the network. Authors developed different dataset for the performance measurement, however the training and testing time-based study was not analysed. Relevant works by the researchers in the concerned area are highlighted in Table 1.

### 2.1 Scope and Contribution of Work

The literature mentioned above focused on mitigation of SSDF and PUEA attacks in CR network. Most of the work applied ML techniques to achieve successful MUs detection. However the timing analysis is not provided in most of the work [43–45, 48]. Generally, in ML techniques time required to train and test a dataset plays an important role. Hence it becomes of great importance to perform a study based on timing analysis to achieve a better trade-off between performance and complexity. Authors have adopted supervised learning and ensemble approaches to achieve better performance. However the increased complexity of the system makes them less liable to adopt.

To overcome the shortcomings of previous studies outlined above, we propose an ELM based approach to identify the presence of MUs in the network. This is a simple method, and effective enough to facilitate classification problem with less training time. Main contributions of this work are highlighted below:

1. To the best of our knowledge, timing based analysis for ELM approach is introduced in this work for the first time in the field of malicious user detection. The classification obtained in the context of proposed algorithms are based on supervised algorithm and differ in shape depending on the type of attack induced. Moreover, depending on the type of attack; ROC performance may be varied. Hence, we propose ELM based MU detection algorithm and compare the performance of different methods utilised in the study.
2. The performance of our method is almost identical with that of SVM method and provide best training time results. The proposed approach performs better in terms of detection rate and AUC values with respect to other methods.
3. This method provides an improvement over other methods by providing a better trade-off.
4. Extensive simulations are performed to compare proposed ELM based MU detection algorithm with some of the well known schemes in literature [36, 42, 44]. For fair evaluation, comparison is also done with existing schemes in which unsupervised and supervised both types of ML algorithms are considered [36]. Results show that proposed ELM based scheme significantly outperform similar ML based schemes and recent well known techniques in literature.

**Table 1** Comparison between previous works and the proposed work

| Existing works | Contributions | Limitations |
|---|---|---|
| [44] | A framework was proposed to mitigate the SSDF attacks and binary output shortcoming of SVM fusion is improved by including probabilistic output | A complex algorithm since multiple ML algorithm are merged together with SVM. The training dataset size must be fixed to maintain the SVM performance |
| [45] | Propose an ensemble ELM algorithm for CSS under SSDF attack | An hierarchical algorithm mixed with ELM, making it computationally complex. The training and testing time analysis is not provided |
| [46] | Double reputation strategy is adopted for mitigation of SSDF attackers | In uncertain SUs condition the reputation strategy performance can be improved further |
| [47] | A sliding window trust model using Bayesian inference was proposed to defend against SSDF attackers | The work have not considered the stochastic nature of the CR channel and manual selection of threshold value is adopted |
| [48] | Propose a reliable SS framework using the neural network-based PUEA detector. Real time experiment was performed on RTL-SDR and USRP platform | The performance measurment was peromef for limited metrics, training and testing time analysis was not provided |
| [49] | Hidden Markov Model (HMM) is utilized to obtain relation between PU states and sensed values of SU. Afterwards, ML based algorithm was developed to identify MUs | The dataset is generated from HMM model that creates a correlation dependency and lead to deterministic model |
| This work | Methodology: Extreme learning machine based algorithm to classify the malicious users successfully and reduce the impact of security threats in global decision | Improvement over competitive techniques: Overcomes the issues of appropriate kernel function selection and a large training and testing time of dataset in SVM [44, 45, 48] |

Remaining part of the article is organized as follows. Section 3 describes the system model and briefly explains about the generation of energy vector. In Sect. 4, proposed ELM-based MU detection framework is presented. For clarity of understanding, this section describes the implementation of proposed algorithm with ELM. In Sect. 5, the performance analysis and simulation results are provided. Section 5 also presents the challenges found in this work and some future scope of the article. Finally, the article is concluded in Section 6.

## 3 Cooperative Spectrum Sensing System Model

### 3.1 System Model

A cooperative spectrum sensing scenario is illustrated in Fig. 1. It has $M$ secondary user (SU) nodes which also act as spectrum sensing units and $N$ malicious user (MU) nodes. It is assumed that the number of SUs are greater than the MUs ($M > N$). The system model consists of only one licensed PU which has the first priority over other users for using the channel. SUs periodically monitor the spectrum and communicate the sensed information to the fusion center (FC) through a dedicated reporting channel. Then, FC makes a global decision on the availability of the spectrum and informs all the SUs whether the licensed spectrum can be accessed. In case of AYMU attack, a higher energy value is received

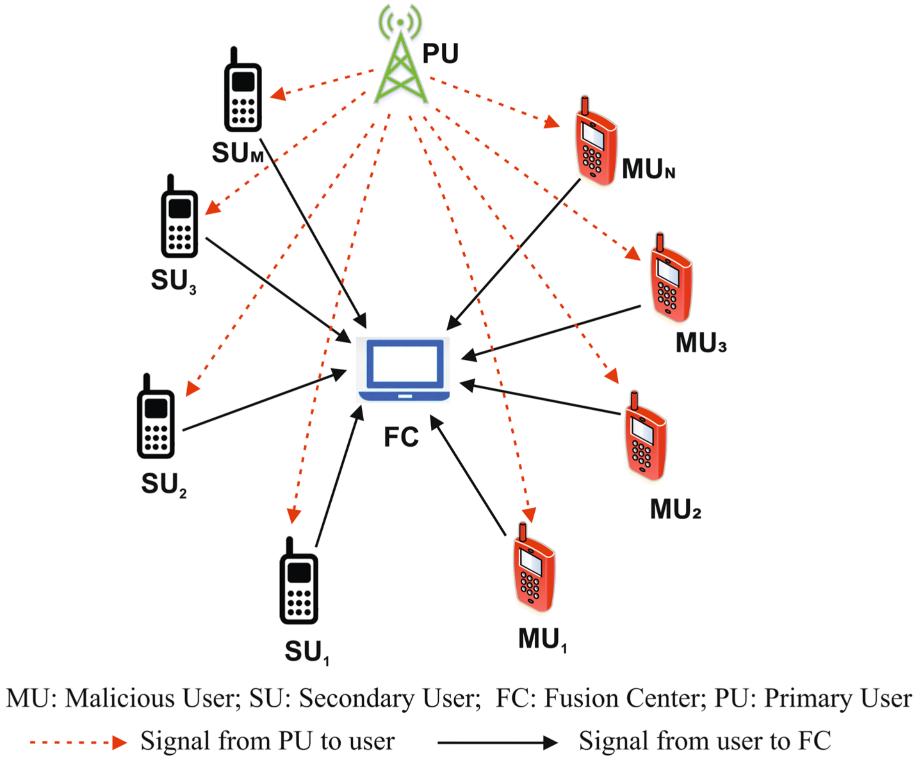

PU
SUM
MUN
SU3
MU3
FC
SU2
MU2
SU1
MU1
MU: Malicious User; SU: Secondary User; FC: Fusion Center; PU: Primary User
Signal from PU to user
Signal from user to FC

**Fig. 1** Typical cooperative spectrum sensing system model involving multiple SUs and MUs

which signifies the PU channel is busy. Whereas, in ANMU attack a low energy value is received to the FC. All users including the normal SUs and MUs transmits their local results to the FC over fading environment. Then, the FC make a robust global decision by separating the normal SUs and MUs based on the proposed ELM algorithm. The final decision was made based on the sensing results of the normal SUs only.

The local sensing task is performed by each SUs and send their locally generated results, either $\mathcal{H}_0$ or $\mathcal{H}_1$. Here $\mathcal{H}_0$ or $\mathcal{H}_1$ denotes the absence or presence of PUs, respectively. The signal received by the $i$th SU can be formulated as binary hypothesis,

$$\mathcal{H}_0 \,:\, z_i(k) = w_i(k), \tag{1}$$

$$\mathcal{H}_1 \,:\, z_i(k) = h_i p(k) + w_i(k) \tag{2}$$

where $k = 1, 2, \ldots, K$, $K$ is the number of sampling points, $i = 1, 2, \ldots, M$, $M$ represents the number of SUs. Some of the assumptions of the model are stated as follows:

1. $z_i(k)$ is the signal received at $i$th SU for $k$th sample, $p(k)$ is the signal from the PU, and $h_i$ is the channel gain between PU and $i$th SU.
2. Noise $w_i(n)$ at the $i$th SU is modelled as additive white Gaussian noise with zero mean and variance $\sigma^2 = 1$.

Energy detection (ED) is a widely used conventional technique for the SS. This method is simple to implement without having any prior knowledge about the PU signal. The sensing outcome $z_i(k)$ represents the received power for $i$th SU in the time domain for a band. The energy at the output of the SU is represented as

$$\xi_i = \frac{1}{K} \sum_{k=1}^{K} |z_i(k)|^2 \tag{3}$$

In case of large number of samples the expression 3 can be represented in form of a Gaussian distribution for both hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ with mean value $\alpha_{\mathcal{H}_0}, \alpha_{\mathcal{H}_1}$ and variance $\sigma^2_{\mathcal{H}_0}, \sigma^2_{\mathcal{H}_1}$ respectively, as:

$$\xi_i = \begin{cases} \alpha_{\mathcal{H}_0} = 2\tau_s B, & \sigma^2_{\mathcal{H}_0} = 4\tau_s B \\ \alpha_{\mathcal{H}_1} = 2\tau_s B(1 + \Upsilon_i), & \sigma^2_{\mathcal{H}_1} = 4\tau_s B(1 + 2\Upsilon_i) \end{cases} \tag{4}$$

where $\Upsilon_i$ represents the SNR of the $i$th SU, $\tau_s$ denotes the sensing duration, and $B$ represents the spectrum bandwidth.

## 4 Proposed Malicious User Detection Algorithm

This section illustrates the procedure of our proposed algorithm. ELM is adopted for detecting the presence of malicious users. In the proposed approach a neural network was trained and ELM is used as an classifier. The conventional energy detector approach is utilized to generate an energy vector. Each SUs including the MUs perform spectrum sensing based on energy detector, and an energy vector was formed. Afterwards this energy vector is converted into training and testing dataset. In Fig. 2 the proposed approach based on the ELM is presented. Basically, ELM utilizes a feed-forward (FF) type neural network in

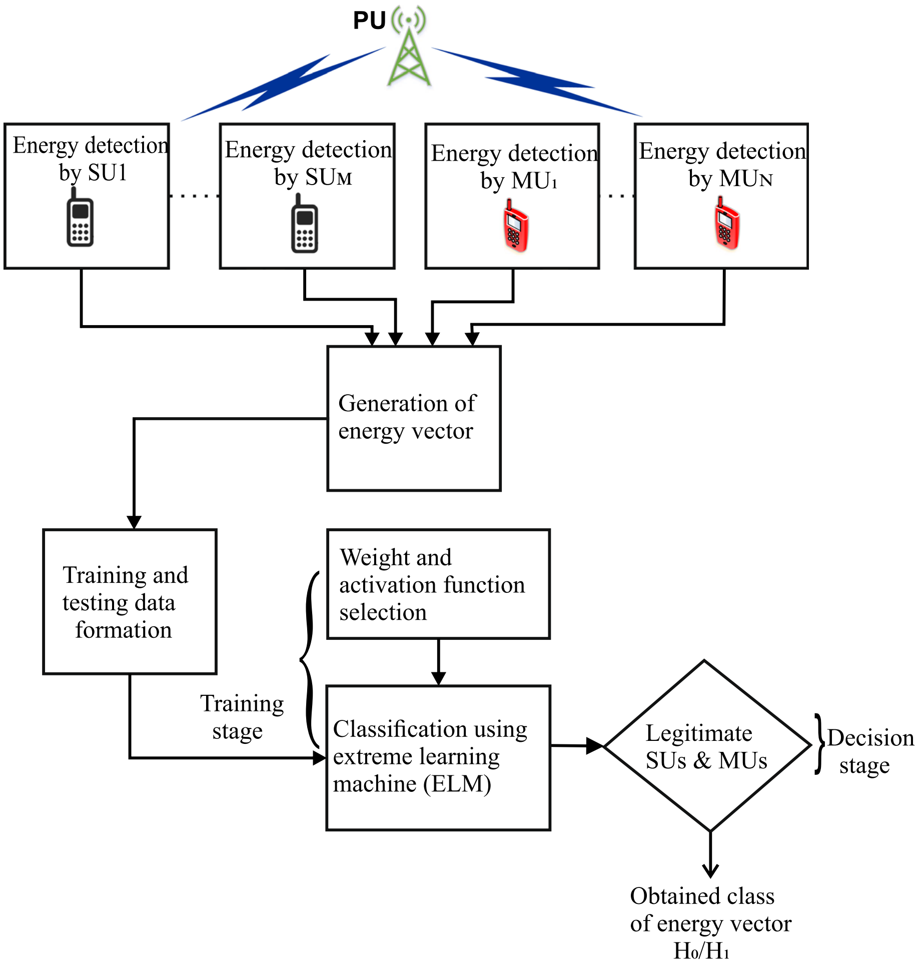

PU
Energy detection by SU1
Energy detection by SUM
Energy detection by MU1
Energy detection by MUN
Generation of energy vector
Training and testing data formation
Weight and activation function selection
Training stage
Classification using extreme learning machine (ELM)
Legitimate SUs & MUs
Decision stage
Obtained class of energy vector H0/H1

**Fig. 2** Proposed training and spectrum sensing framework based on ELM

which gradient based learning is adopted. The iterative procedure is adopted for parameter tuning [50]. However, applying the learning approach efficiently is a time-consuming task. To prevent this random selection of ELM's output weights are taken into account [51]. In ELM, independent learning is achieved by changing hidden node parameters [52]. In a way it can be said that ELM accuracy depends on different factors. The primary variables that significantly affects the ELM performance are learning parameter, output weights, and norm parameter minimization [53].

For $U$ different energy samples $(r_j, q_j)$, and $V$ hidden neurons, output equation can be given as:

$$\mathcal{O}_j = \sum_{i=1}^{V} \Phi_i \varrho\left(\Omega_i r_j + \beta_i\right) \quad \text{for } j = 1.. \dots, U \tag{5}$$

where $r_j = [r_{j1}, r_{j2}, ..., r_{jn}]^T \in \mathcal{R}^n$ and $q_j = [q_{j1}, q_{j2}, ..., q_{jn}]^T \in \mathcal{R}^m$ denote distinct (unique) energy vectors, $\varrho(.)$ is for activation function, and $\boldsymbol{\Phi}$ denotes output weight. $\Omega$ and $\beta$ denote the input weight and bias. The error found in the iteration is $\mathcal{E} = \sum_{j=1}^{U} \mathcal{O}_j - q_j$. This can be expressed as:

$$\sum_{j=1}^{U} \left( \sum_{i=1}^{V} \boldsymbol{\Phi}_i \varrho\big(\Omega_i r_j + \beta_i\big) \right) - q_j \tag{6}$$

It is generally accepted that the random selection of parameter values can vary insignificantly [53]. Hence, the choice of ideal approximation is seems to be a sensible one. Therefore, the error most likely reduces to zero, i.e.

$$\sum_{j=1}^{U} \left( \sum_{i=1}^{V} \boldsymbol{\Phi}_i \varrho\big(\Omega_i r_j + \beta_i\big) \right) - q_j = 0 \tag{7}$$

$$\sum_{i=1}^{V} \boldsymbol{\Phi}_i \varrho\big(\Omega_i r_j + \beta_i\big) = q_j \tag{8}$$

The above Eq. 8 can be expressed as $G\boldsymbol{\Phi} = J^+$ where,

$$G = \begin{bmatrix} \varrho\big(\Omega_1 r_1 + \beta_1\big) & \dots & \varrho\big(\Omega_V r_1 + \beta_V\big) \\ \vdots & \ddots & \vdots \\ \varrho\big(\Omega_1 r_U + \beta_1\big) & \dots & \varrho\big(\Omega_V r_U + \beta_V\big) \end{bmatrix} \tag{9}$$

$$\boldsymbol{\Phi} = \begin{bmatrix} \boldsymbol{\Phi}_1 \\ \vdots \\ \boldsymbol{\Phi}_V \end{bmatrix} \text{and } J^+ = \begin{bmatrix} q_1 \\ \vdots \\ q_U \end{bmatrix} \tag{10}$$

Given, the sample size is equal to the number of hidden neurons ($U = V$), $G$ will transform into a square matrix. Moreover, if the matrix $G$ is non singular, then $G$ will be invertible. This may lead to elimination of error in network. If $V << U$, then $G$ is not invertible. Therefore, ideal solution in this case is unattainable. Optimum solution could certainly be achieved by reducing the approximation error to a level [51]. This is expressed as the following formula

$$\hat{G}\hat{\boldsymbol{\Phi}} - J^+ \approx G\boldsymbol{\Phi} - J^+ \tag{11}$$

$\hat{G}$ and $\hat{\boldsymbol{\Phi}}$ can be denoted as

$$\hat{G} = \begin{bmatrix} \hat{\varrho}\big(\hat{\Omega}_1 r_1 + \hat{\beta}_1\big) & \dots & \hat{\varrho}\big(\hat{\Omega}_V r_1 + \hat{\beta}_V\big) \\ \vdots & \ddots & \vdots \\ \hat{\varrho}\big(\hat{\Omega}_1 r_U + \hat{\beta}_1\big) & \dots & \hat{\varrho}\big(\hat{\Omega}_V r_U + \hat{\beta}_V\big) \end{bmatrix} \tag{12}$$

$$\hat{\boldsymbol{\Phi}} = \begin{bmatrix} \hat{\boldsymbol{\Phi}}_1 \\ \vdots \\ \hat{\boldsymbol{\Phi}}_V \end{bmatrix} \tag{13}$$

The errors have been strongly reduced when accounting for proper activation function $\hat{\varrho}(.)$ and $\hat{\Omega}, \hat{\beta}, \hat{\boldsymbol{\Phi}}$ values. In present work, $\hat{\varrho}(.)$ is treated as a continuous sigmoid function. The ELM technique presented is capable of producing less training error and time consumption [53, 54]. Convincing results from randomized selection of $\hat{\Omega}$, $\hat{\beta}$, and $\hat{\boldsymbol{\Phi}}$ values can be achieved. The $\hat{\boldsymbol{\Phi}}$ values were calculated using MP pseudo-inverse method as mentioned in [52]. The detailed expressions of $\hat{\boldsymbol{\Phi}}$ can be given as

$$\hat{\boldsymbol{\Phi}} = \hat{G}^{+} \cdot J^{+} = (\hat{G}' \cdot \hat{G})^{-1} \cdot \hat{G}'.J^{+} \tag{14}$$

ELM method is much quicker than conventional gradient based methods. To achieve minimum training error and least norm weight, it is also necessary to include proper selection of weight initialization and activation functions. The details of the proposed ELM based algorithm are described in Algorithm 1.

**Algorithm 1:** Proposed ELM-based MU classification algorithm.

```
Input: Initialize necessary variables: number of iteration, $M$, $N$, $\varrho$, $U$, $V$, $\Omega$, $\beta$ etc.
Output: Classification result from the ELM model
Data: training dataset (energy vector)
Create ($N$) number of Gaussian distributed MUs.
Create ($M$) number of legitimate SUs.
Allocate indices for MUs attackk.
Allocate indices for legitimate SUs.
A. Perform sensing
for $n = 1$ to sensing duration do
    for $i = 1$ to $N$ do
        Calculate energy for SUs.
    end
    for $i = 1$ to $M$ do
        Calculate energy for MUs.
    end
end
B. Perform classification using ELM technique
 1. Data Processing
 2. Combining the data
 3. Convert the data into training and testing set
 4. Input the data
 5. Randomly assign the weight and hidden layer bias
 6. Collect the matrix $\hat{G}$ by using Eq. 12
 7. Get the $\hat{\Phi}$ value from Eq. 14
 8. Store updated weight and bias values
 9. Apply stored results to test the target dataset
10. Collect classified results
```

## 5 Simulation Results

Here we present tests that evaluate the performance of the proposed technique compared with some current state of the art algorithms. Similar to [42, 43, 54], a setup was developed to aid in the development and testing of the proposed method. To perform simulation we consider a total of 10 CR users with 4 randomly chosen MUs, and 6 normal SUs. PU signal is modelled as a Gaussian random variable. The channel between PU and SU is assumed to be Rayleigh flat fading. The total number of samples was 100, and 20000 iterations were performed for each user to create an energy vector. The used bandwidth is 6 MHz based on the IEEE 802.22 standard. The probability of PU being in active and idle state is $P\left(\mathcal{H}_1\right)$ and $P\left(\mathcal{H}_0\right)$, respectively. For all the simulations, parameters are set as follows: $\sigma^2 = 1$, $\alpha = 4$, $P\left(\mathcal{H}_0\right) = 0.5$ and $P\left(\mathcal{H}_1\right) = 0.5$. The proposed ELM based scheme is having a single hidden layer with 5 hidden nodes.

First we checked the performance of the ELM in terms of accuracy with varying values of number of neurons. The number of neuron value is varied between 0 to 50. It is evident from Fig. 3 that the testing accuracy achieved is better compare to the training accuracy. This highlights that the classification achieved from the ELM is accurate. Next to adopt an activation function (AF), we check the ROC performance of the ELM based algorithm for different AFs. From Fig. 4 we can see that the BentIde is providing best results followed by the Sigmoid. Throughout this article we adopted Sigmoid AF and Relu weight initialization scheme (WIS) for performance evaluation.

The simulation results are presented in two sections. First, we present the results for the proposed scheme based on the different cases of attacks in the network namely, a) MUs absent, b) AYMUs present, c) ANMUs present, and d) RMUs present. Secondly, the performance of the proposed ELM-based approach is compared with other schemes in the literature. The significance of the proposed technique is highlighted using the receiver operating characteristics (ROC) curve. The energy values obtained from the spectrum sensing for normal users is utilized for plotting the ROC. It is worth mentioning here that the energy value achieved is higher in case of AYMU, that signifies the PU absence. The lower energy value for the ANMU signifies the PU presence. Whereas, in the RMU energy level lies in the mid region signifying the behaviours of AYMU and ANMU alternatively with probability $1 - P\left(\mathcal{H}_0\right)$.

We evaluated the performance of proposed ELM based scheme in case of AYMU, ANMU and RMU attacks present in the network. The results are presented in the figures 5–7. We compared the performance of the proposed scheme with other techniques like SVM [42], K-means [36], Naive Bayesian (NB), Gaussian mixture model (GMM) and

**Fig. 3** Accuracy performance of the proposed schemes, signifying correct classification. Comparison is made with varying number of neurons

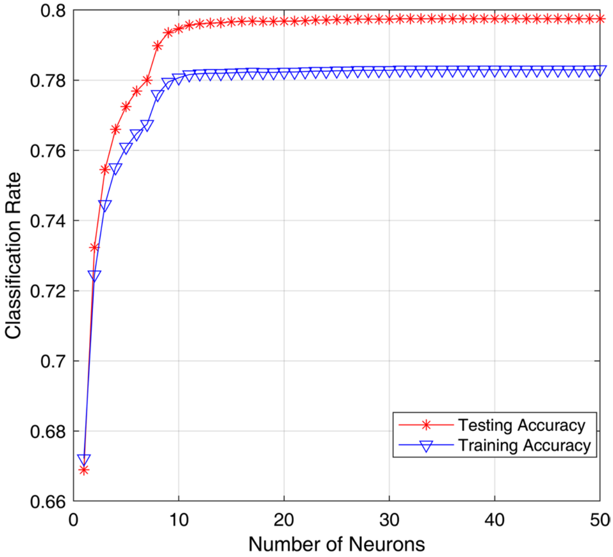


**Fig. 4** Variation of probability of detection $P_d$ for different activation function

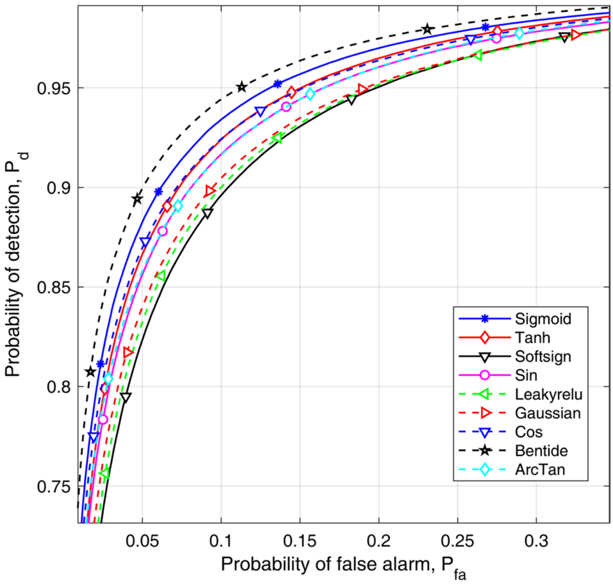
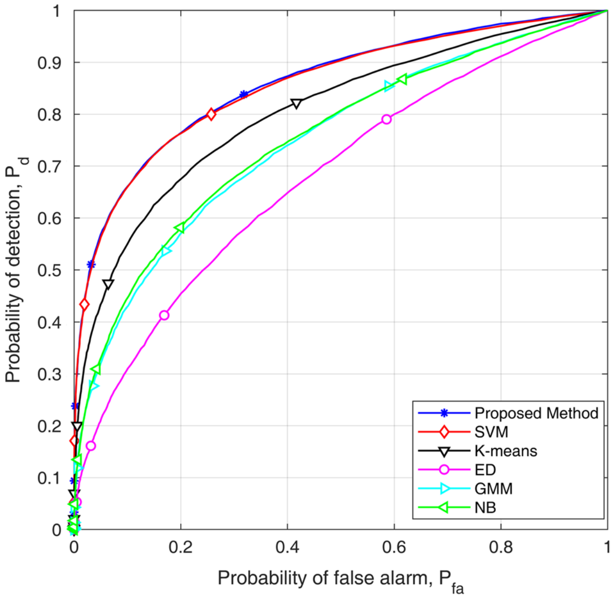


**Fig. 5** Comparison of ROC performance for different techniques (AYMU attack)



the traditional energy detection (ED) [55]. In Fig. 5 the ROC curve of the proposed ELM-based approach for AYMU attack is presented and compared with the existing schemes in literature. From the figure it is clear that the proposed approach obtains similar results like the SVM [42] based approach. Whereas, compare to the K-means [36], GMM, NB, and ED [55], it performs superiorly. This highlights that the proposed approach effectively classifies the normal SUs and the AYMUs. It is worth to mention here that both the SVM and proposed ELM based approach are supervised learning approaches and the actual status of the channel will known to the FC via a labelled data. Hence the identical performance is justified.

Fig. 6 presents the ROC curve for different techniques in case of ANMU attack in the network. We compare the performance of the proposed approach with other schemes in the literature. From the figure it is clear that the proposed approach obtains similar results like the SVM based approach [42]. Whereas, compare to the K-means [36], GMM, NB and ED [55] it performs superiorly. This highlights that the proposed approach effectively classifies the normal SUs and the ANMUs. One interesting observation is that the ROC performance for all the approaches including the proposed one is decreased. This is due to the fact that the energy level received in case of ANMU is less compare to the AYMU.

Figure 7 present the ROC curve for different techniques in case of RMUs in the network. We compared the performance of proposed techniques with other schemes. From figure we can see that the proposed ELM based approach achieves identical performance like SVM [42], and outperforms all the other K-means [36], GMM, NB, and ED approaches [55]. This represents that the classification achieved in the proposed approach is accurate and legitimate users are successfully separated from the MUs. Moreover, the risk involved in RMUs consideration is significantly reduced. It is worth noting that the performance of all the approaches reduced compared to the AYMU and ANMU cases. This is due to fact that some random MUs present in the network will send low values of sensing information. Whereas, some random MUs will send higher values of sensing information irrespective of the locally determined results.

The bar plot in Fig. 8 presents the comparison of training time spent for different techniques for varying number of samples. We selected 100 and 500 number of samples for the

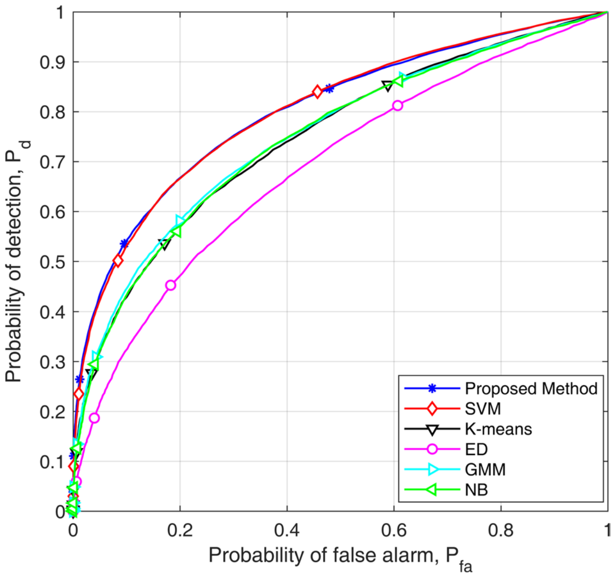


**Fig. 6** Comparison of ROC performance for different techniques (ANMU attack)

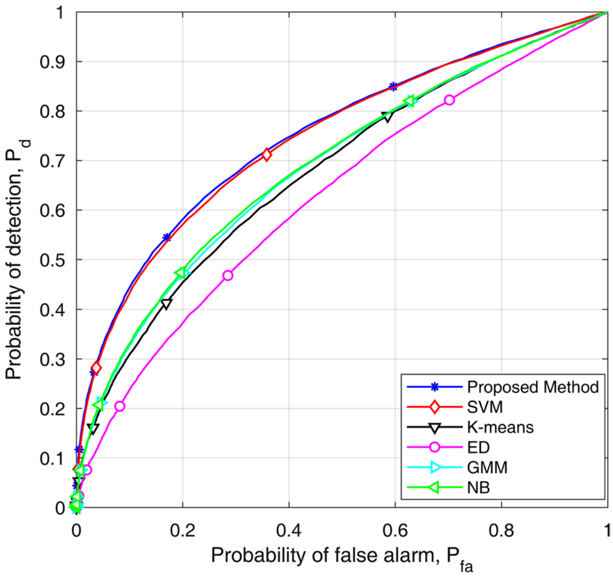


**Fig. 7** Comparison of ROC performance for different techniques (RMU attack)

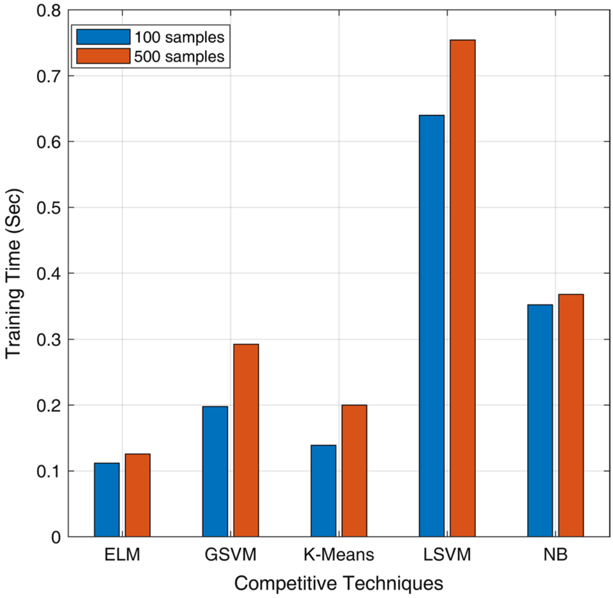


**Fig. 8** Comparison of training time for different techniques as varying number of samples $K = 100, 500$

comparison. The result demonstrates that the training time increases for increasing number of samples value. It was found that among the competitive techniques only ELM (proposed method) and NB presents approximately a constant training time for increased value of samples. Whereas, the SVM technique [42] takes greater time to train the data samples.

The results highlight the improved performance of the proposed algorithm to training a dataset quickly compare to the other competitive techniques.

The results presented above were for Sigmoid function and ReLu Scheme. However, different AFs are available in the literature and there is a possibility of achieving different performance for different set of parameter selection. For achieving a concrete outcome, timing analysis for different set of parameters must be taken into account. Hence we presented a detailed timing analysis for different combination of AF and WIS. The detailed results are provided in Table 2. It is evident from Table 2, that area under curve (AUC) results are efficient for Xavier and ReLu scheme. Moreover, Sigmoid and Tanh functions are providing better performance. However, in case of no AF, performance of each WIS is similar. This represents the worth of selecting a proper AF for performance measurement.

### 5.1 Discussion

The proposed technique falls under the supervised ML domain, however the simple structure in terms of complexity and improved training time is an added advantage. The technique can be successfully applied to real world scenarios. The present work concerned with providing a improved trade-off between MUs identification and training time, and the objective is achieved. However the present work can be extended for real-time applications to build for a future scope. Another possibility is to apply optimization algorithm to achieve the best possible weight and optimal parameters for ELM technique. This will further improve the performance of the algorithm.

## 6 Conclusion

In this study, we presented a simple technique based on ELM algorithm to alleviate the malicious users attack in a cooperative spectrum sensing scenario. In conventional ML based spectrum sensing techniques, the classification results are seems to be satisfactory, however the increased computational time is an issue to consider. Proposed ELM based technique achieves similar results like other ML techniques with significant improvement in the computational time. It is clear from the presented results, that the proposed approach is better in terms of training time performance. Most importantly, proposed approach provides better trade-off than the other competitive schemes. However, the proposed approach is having some shortcomings such as a high number of hidden nodes are required in ELM to achieve better result. This signifies the adopted model is memorizing the data in place of prediction to provide the results. The authors will further analysed this shortcoming in the future work to improve the performance.

**Table 2** Timing analysis of the proposed approach for different activation function

| Activation Function | WIS | Testing time (s) | Testing accuracy(%) | AUC (%) |
|---|---|---|---|---|
| None | ortho | 0.012 | 92.17 | 85.02 |
| | rand(0, 1) | 0.021 | 92.50 | 85.06 |
| | rand(− 1, 1) | 0.015 | 92.70 | 85.04 |
| | xavier | 0.019 | 92.45 | 85.11 |
| | Relu | 0.020 | 92.8 | 85.09 |
| Relu | ortho | 0.014 | 90.11 | 84.55 |
| | rand(0, 1) | 0.016 | 91.43 | 84.72 |
| | rand(− 1, 1) | 0.028 | 89.56 | 83.93 |
| | xavier | 0.025 | 90.50 | 84.24 |
| | Relu | 0.018 | 92.00 | 85.73 |
| Sigmoid | ortho | 0.014 | 92.4 | 85.91 |
| | rand(0, 1) | 0.023 | 93.1 | 85.12 |
| | rand(− 1, 1) | 0.031 | 93.13 | 85.72 |
| | xavier | 0.042 | 92.9 | 85.90 |
| | Relu | 0.013 | 92.5 | 85.84 |
| Tanh | ortho | 0.031 | 91.20 | 84.82 |
| | rand(0, 1) | 0.029 | 91.87 | 85.46 |
| | rand(− 1, 1) | 0.034 | 91.95 | 85.10 |
| | xavier | 0.028 | 92.35 | 85.84 |
| | Relu | 0.025 | 91.17 | 85.12 |
| Softsign | ortho | 0.019 | 91.71 | 84.12 |
| | rand(0, 1) | 0.025 | 91.5 | 84.26 |
| | rand(− 1, 1) | 0.011 | 91.47 | 84.34 |
| | xavier | 0.020 | 91.63 | 84.51 |
| | Relu | 0.018 | 91.8 | 84.64 |
| Sin | ortho | 0.032 | 90.81 | 83.21 |
| | rand(0, 1) | 0.038 | 90.52 | 83.43 |
| | rand(− 1, 1) | 0.047 | 90.74 | 83.62 |
| | xavier | 0.041 | 90.36 | 83.15 |
| | Relu | 0.029 | 91.1 | 83.46 |
| Cos | ortho | 0.031 | 90.18 | 83.32 |
| | rand(0, 1) | 0.035 | 90.25 | 83.42 |
| | rand(− 1, 1) | 0.042 | 90.47 | 83.28 |
| | xavier | 0.037 | 90.63 | 83.52 |
| | Relu | 0.024 | 90.93 | 83.76 |
| LeakyRelu | ortho | 0.041 | 88.18 | 83.23 |
| | rand(0, 1) | 0.045 | 89.52 | 83.49 |
| | rand(− 1, 1) | 0.052 | 89.74 | 83.58 |
| | xavier | 0.047 | 88.63 | 83.24 |
| | Relu | 0.044 | 89.93 | 83.67 |

**Table 2** (continued)

| Activation Function | WIS | Testing time (s) | Testing accuracy(%) | AUC (%) |
|---|---|---|---|---|
| BentIde | ortho | 0.038 | 92.18 | 84.91 |
| | rand(0, 1) | 0.042 | 93.06 | 85.67 |
| | rand(− 1, 1) | 0.048 | 92.13 | 84.95 |
| | xavier | 0.043 | 92.65 | 85.23 |
| | Relu | 0.039 | 93.31 | 85.84 |
| ArcTan | ortho | 0.030 | 89.29 | 83.72 |
| | rand(0, 1) | 0.034 | 89.56 | 83.96 |
| | rand(− 1, 1) | 0.041 | 88.71 | 82.81 |
| | xavier | 0.033 | 89.38 | 83.54 |
| | Relu | 0.029 | 89.39 | 83.76 |
| Gaussian | ortho | 0.034 | 88.39 | 82.92 |
| | rand(0, 1) | 0.037 | 88.66 | 83.36 |
| | rand(− 1, 1) | 0.048 | 88.31 | 82.11 |
| | xavier | 0.039 | 89.28 | 83.64 |
| | Relu | 0.032 | 89.14 | 83.46 |

**Author Contributions** All authors contributed to the study conception and design. The manuscript was read and approved by all the authors.

**Funding** Not applicable.

**Data Availability** Not applicable.

**Code Availability** Not applicable.

## Declarations

**Conflict of interest** The authors declare that they have no conflict of interest.

## References

1. Federal Communications Commission. (2003). Notice of proposed rule making and order. ET Docket No. 03-222
2. Haykin, S. (2005). Cognitive radio: Brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications, 23*(2), 201–220.
3. Zhai, L., Wang, H., & Gao, C. (2016). A spectrum access based on quality of service (QoS) in cognitive radio networks. *PloS one, 11*(5), e0155074.
4. Yucek, T., & Arslan, H. (2009). A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Communications Surveys & Tutorials, 11*(1), 116–130.
5. Axell, E., Leus, G., Larsson, E. G., & Poor, H. V. (2012). Spectrum sensing for cognitive radio: State-of-the-art and recent advances. *IEEE Signal Processing Magazine, 29*(3), 101–116.
6. Khan, M. S., Jibran, M., Koo, I., Kim, S. M., & Kim, J. (2019). A double adaptive approach to tackle malicious users in cognitive radio networks. *Wireless Communications and Mobile Computing, 2019*, 2350694.

7. Mishra, S. M., Sahai, A., & Brodersen, R. W. (2006). Cooperative sensing among cognitive radios. In *2006 IEEE international conference on communications* (vol. 4, pp. 1658–1663). IEEE.
8. He, Y., Xue, J., Ratnarajah, T., Sellathurai, M., & Khan, F. (2016). On the performance of cooperative spectrum sensing in random cognitive radio networks. *IEEE Systems Journal, 12*(1), 881–892.
9. Chilakala, S., & Ram, M. S. S. (2018). Optimization of cooperative secondary users in cognitive radio networks. *Engineering Science and Technology, An International Journal, 21*(5), 815–821.
10. Jenani, M. (2017). Network security, a challenge. *International Journal of Advanced Networking and Applications, 8*(5), 120–123.
11. Marinho, J., Granjal, J., & Monteiro, E. (2015). A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. *EURASIP Journal on Information Security, 1*, 1–14.
12. Wu, H., Sun, X., Guo, C., & Ren, S. (2016). Malicious user detection for wide-band cognitive radio networks. In *2016 Asia-Pacific microwave conference (APMC)* (pp. 1–4). IEEE.
13. Taggu, A., Chunka, C., & Marchang, N. (2015). Codes: A collaborative detection strategy for ssdf attacks in cognitive radio networks. In *Proceedings of the third international symposium on women in computing and informatics* (pp. 118–123).
14. Sarala, B., Devi, S. R., Suganthy, M., & Ida, S. J. (2019). A novel authentication mechanism for cognitive radio networks. *International Journal of Recent Technology and Engineering, 8*(4), 713–718.
15. Wan, R., Ding, L., Xiong, N., & Zhou, X. (2019). Mitigation strategy against spectrum-sensing data falsification attack in cognitive radio sensor networks. *International Journal of Distributed Sensor Networks, 15*(9), 1550147719870645.
16. Farmani, F., Abbasi-Jannatabad, M., & Berangi, R. (2011). Detection of SSDF attack using SVDD algorithm in cognitive radio networks. In *2011 third international conference on computational intelligence, communication systems and networks* (pp. 201–204). IEEE.
17. Kaligineedi, P., Khabbazian, M., & Bhargava, V. K. (2010). Malicious user detection in a cognitive radio cooperative sensing system. *IEEE Transactions on Wireless Communications, 9*(8), 2488–2497.
18. He, X., Dai, H., & Ning, P. (2013). Hmm-based malicious user detection for robust collaborative spectrum sensing. *IEEE Journal on Selected Areas in Communications, 31*(11), 2196–2208.
19. Li, J., Liu, J., & Long, K. (2010). Reliable cooperative spectrum sensing algorithm based on Dempster–Shafer theory. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010* (pp. 1–5). IEEE.
20. Sharifi, A. A., & Mofarreh-Bonab, M. (2018). Spectrum sensing data falsification attack in cognitive radio networks: An analytical model for evaluation and mitigation of performance degradation. *AUT Journal of Electrical Engineering, 50*(1), 43–50.
21. Gul, N., Qureshi, I. M., Elahi, A., & Rasool, I. (2018). Defense against malicious users in cooperative spectrum sensing using genetic algorithm. *International Journal of Antennas and Propagation, 2018*, 2346317.
22. Dave, M. B., & Nakrani, M. B. (2014). Malicious user detection in spectrum sensing for wran using different outliers detection techniques. arXiv preprint arXiv:1405.2685
23. Adelantado, F., & Verikoukis, C. (2013). Detection of malicious users in cognitive radio ad hoc networks: A non-parametric statistical approach. *Ad Hoc Networks, 11*(8), 2367–2380.
24. Elangovan, K., Krishnasamy Tamilselvam, Y., Mohan, R. E., Iwase, M., Nemoto, T., & Wood, K. (2017). Fault diagnosis of a reconfigurable crawling-rolling robot based on support vector machines. *Applied Sciences, 7*(10), 1025.
25. Jan, S. U., Lee, Y. D., Shin, J., & Koo, I. (2017). Sensor fault classification based on support vector machine and statistical time-domain features. *IEEE Access, 5*, 8682–8690.
26. Wang, F., Zhen, Z., Wang, B., & Mi, Z. (2017). Comparative study on KNN and SVM based weather classification models for day ahead short term solar PV power forecasting. *Applied Sciences, 8*(1), 28.
27. Shah, H. A., & Koo, I. (2018). Reliable machine learning based spectrum sensing in cognitive radio networks. In *Wireless Communications and Mobile Computing 2018*.
28. Zhu, J., Song, Y., Jiang, D., & Song, H. (2017). A new deep-q-learning-based transmission scheduling mechanism for the cognitive internet of things. *IEEE Internet of Things Journal, 5*(4), 2375–2385.
29. Giri, M. K., & Majumder, S. (2021). Eigenvalue-based cooperative spectrum sensing using kernel fuzzy c-means clustering. *Digital Signal Processing, 111*, 102996.
30. Giri, M. K., & Majumder, S. (2022). On eigenvalue-based cooperative spectrum sensing using feature extraction and maximum entropy fuzzy clustering. *Journal of Ambient Intelligence and Humanized Computing*, 1–15.
31. Huang, Y. D., Liang, Y. C., & Yang, G. (2016). A fuzzy support vector machine algorithm for cooperative spectrum sensing with noise uncertainty. In *2016 IEEE Global Communications Conference (GLOBECOM)* (pp. 1–6). IEEE.

32. Jan, S. U., Vu, V. H., & Koo, I. (2018). Throughput maximization using an SVM for multi-class hypothesis-based spectrum sensing in cognitive radio. *Applied Sciences, 8*(3), 421.
33. Li, Z., Wu, W., Liu, X., & Qi, P. (2018). Improved cooperative spectrum sensing model based on machine learning for cognitive radio networks. *IET Communications, 12*(19), 2485–2492.
34. Rahman, M., Lee, Y. D., Koo, I., et al. (2016). An efficient transmission mode selection based on reinforcement learning for cooperative cognitive radio networks. *Human-centric Computing and Information Sciences, 6*(1), 1–14.
35. Alshawaqfeh, M., Wang, X., Ekti, A. R., Shakir, M. Z., Qaraqe, K., & Serpedin, E. (2015). A survey of machine learning algorithms and their applications in cognitive radio. In *International conference on cognitive radio oriented wireless networks* (pp. 790–801). Springer.
36. Thilina, K. M., Choi, K. W., Saquib, N., & Hossain, E. (2013). Machine learning techniques for cooperative spectrum sensing in cognitive radio networks. *IEEE Journal on Selected Areas in Communications, 31*(11), 2209–2221. https://doi.org/10.1109/JSAC.2013.131120
37. Cadena Muñoz, E., Pedraza Martínez, L. F., & Ortiz Triviño, J. E. (2020). Detection of malicious primary user emulation based on a support vector machine for a mobile cognitive radio network using software-defined radio. *Electronics, 9*(8), 1282.
38. Chen, C., Song, M., Xin, C., & Alam, M. (2012). A robust malicious user detection scheme in cooperative spectrum sensing. In *2012 IEEE global communications conference (GLOBECOM)* (pp. 4856–4861). IEEE.
39. Albehadili, A., Ali, A., Jahan, F., Javaid, A. Y., Oluochy, J., & Devabhaktuniz, V. (2019). Machine learning-based primary user emulation attack detection in cognitive radio networks using pattern described link-signature (PDLS). In *2019 wireless telecommunications symposium (WTS)* (pp. 1–7). IEEE.
40. Lu, J., Li, L., Chen, G., Shen, D., Pham, K., & Blasch, E. (2017). Machine learning based intelligent cognitive network using fog computing. *Sensors and Systems for Space Applications X, SPIE, 10196*, 149–157.
41. Furqan, H. M., Aygül, M. A., & Nazzal, M. (2020). Primary user emulation and jamming attack detection in cognitive radio via sparse coding. *EURASIP Journal on Wireless Communications and Networking, 1*, 1–19.
42. Khan, M. S., Khan, L., Gul, N., Amir, M., Kim, J., & Kim, S. M. (2020). Support vector machine-based classification of malicious users in cognitive radio networks. *Wireless Communications and Mobile Computing, 2020*, 8846948.
43. Hossain, M. S., & Miah, M. S. (2021). Machine learning-based malicious user detection for reliable cooperative radio spectrum sensing in cognitive radio-internet of things. *Machine Learning with Applications, 5*, 100052.
44. Zhang, Y., Wu, Q., & Shikh-Bahaei, M. R. (2020). On ensemble learning-based secure fusion strategy for robust cooperative sensing in full-duplex cognitive radio networks. *IEEE Transactions on Communications, 68*(10), 6086–6100.
45. Kumar, G. P., & Reddy, D. K. (2022). Hierarchical cat and mouse based ensemble extreme learning machine for spectrum sensing data falsification attack detection in cognitive radio network. *Microprocessors and Microsystems, 90*, 104523.
46. Xu, Z., Sun, Z., & Guo, L. (2021). Throughput maximization of collaborative spectrum sensing under SSDF attacks. *IEEE Transactions on Vehicular Technology, 70*(8), 8378–8383.
47. Fu, Y., & He, Z. (2019). Bayesian-inference-based sliding window trust model against probabilistic SSDF attack in cognitive radio networks. *IEEE Systems Journal, 14*(2), 1764–1775.
48. Ponnusamy, V., Kottursamy, K., Karthick, T., Mukeshkrishnan, M., Malathi, D., & Ahanger, T. A. (2020). Primary user emulation attack mitigation using neural network. *Computers & Electrical Engineering, 88*, 106849.
49. Taggu, A., & Marchang, N. (2021). Detecting byzantine attacks in cognitive radio networks: a two-layered approach using hidden Markov model and machine learning. *Pervasive and Mobile Computing, 77*, 101461.
50. Huang, G. B., Zhu, Q. Y., & Siew, C. K. (2006). Extreme learning machine: Theory and applications. *Neurocomputing, 70*(1–3), 489–501.
51. Hansen, L. K., & Salamon, P. (1990). Neural network ensembles. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 12*(10), 993–1001.
52. Huang, G. B., Wang, D. H., & Lan, Y. (2011). Extreme learning machines: A survey. *International Journal of Machine Learning and Cybernetics, 2*(2), 107–122.
53. Huang, G. B., Zhu, Q. Y., & Siew, C. K. (2004). Extreme learning machine: A new learning scheme of feedforward neural networks. In *2004 IEEE international joint conference on neural networks (IEEE Cat. No. 04CH37541)* (Vol. 2, pp. 985-990). IEEE.

54. Giri, M. K., & Majumder, S. (2020). Extreme learning machine based cooperative spectrum sensing in cognitive radio networks. In *2020 7th international conference on signal processing and integrated networks (SPIN)* (pp. 636–641). IEEE. https://doi.org/10.1109/SPIN48934.2020.9071418

55. Giri, M. K., & Majumder, S. (2022). Cooperative spectrum sensing using extreme learning machines for cognitive radio networks. *IETE Technical Review, 39*, 698–712.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Manish Kumar Giri** Manish Kumar Giri received his B.E. and M.E. degrees from SSCET Bhilai, and Government Engineering College Ujjain, India, respectively. Currently, he is pursuing his Ph.D. degree in Electronics and Communication Engineering from the National Institute of Technology Raipur, India. His research interests are cognitive radio focused on spectrum sensing using machine learning techniques.

**Saikat Majumder** Saikat Majumder is an Assistant Professor in the Department of Electronics and Communication Engineering of the National Institute of Technology, Raipur, India. He completed his Bachelor of Technology degree from North Eastern Regional Institute of Science and Technology, Nirjuli, India in 2004. He obtained his M.Tech from National Institute of Technology, Calicut, India in 2006 and Ph.D. in Electronics and Communication Engineering from National Institute of Technology, Raipur, India in 2017. His current research interests include cognitive radio, wireless communication, machine learning and statistical signal processing.