Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8846948, 11 pages
https://doi.org/10.1155/2020/8846948

*Research Article*

# Support Vector Machine-Based Classification of Malicious Users in Cognitive Radio Networks

**Muhammad Sajjad Khan,[1,2] Liaqat Khan,[1] Noor Gul,[1] Muhammad Amir,[1] Junsu Kim,[2] and Su Min Kim[2]**

[1]*Department of Electrical Engineering, Faculty of Engineering and Technology, International Islamic University, Islamabad 44000, Pakistan*
[2]*Department of Electronics Engineering, Korea Polytechnic University, 237 Sangidaehak-ro, Siheung-si, Gyeonggi-do 15073, Republic of Korea*

Correspondence should be addressed to Su Min Kim; suminkim@kpu.ac.kr

Received 30 April 2020; Revised 23 June 2020; Accepted 7 July 2020; Published 18 July 2020

Academic Editor: Farman Ullah



Cognitive radio is an intelligent radio network that has advancement over the traditional radio. The difference between the traditional and cognitive radio is that all the unused frequency spectrum is utilized to the best of available resources in the cognitive setup unlike the traditional radio. The main role of cognitive radio is spectrum sensing, in which the secondary users (SUs) opportunistically access the spectrum while avoiding interference to the primary user (PU) channel. Various aspect of the spectrum sensing problem are studied from cognitive radio perspective. Cooperative spectrum sensing in cognitive radio has a promising performance compared to the individual sensing. However, the existence of the malicious users (MUs) highly degrades the performance of the cognitive radio network (CRN) by sending falsified results to the fusion center (FC). In this paper, we proposed a machine learning algorithm called support vector machine (SVM) to classify normal SUs and MUs in the network. SVM is used for both classification and regression, but mostly it is used for classification problems. SVM clearly classify both normal and MUs by drawing hyper plane on the base of maximal margin. The results of the legitimate SUs are combined at the FC by utilizing Dempster-Shafer (DS) evidence theory. The effectiveness of the proposed scheme is demonstrated through simulation by comparing with the other existing schemes.

Cognitive radio is an intelligent radio network that has advancement over traditional radio. The difference between the traditional radio and the cognitive radio is that all the unused frequency spectrum can be utilized to the best of available resources in the cognitive radio unlike the traditional radio. The core technology of cognitive radio is spectrum sensing, in which secondary users (SUs) opportunistically access the spectrum while avoiding interference to primary user (PU) channels. Various aspects of the spectrum sensing have been studied from the perspective of cognitive radio. Cooperative spectrum sensing (CSS) technique provides a promising performance, compared with individual sensing techniques. However, the existence of malicious users (MUs) highly degrades the performance of cognitive radio network (CRN) by sending falsified results to a fusion center (FC). In this paper, we propose a machine learning algorithm based on support vector machine (SVM) to classify legitimate SUs and MUs in the CRN. The proposed SVM-based algorithm is used for both classification and regression. It clearly classifies legitimate SUs and MUs by drawing a hyperplane on the base of maximal margin. After successful classification, the sensing results from the legitimate SUs are combined at the FC by utilizing Dempster-Shafer (DS) evidence theory. The effectiveness of the proposed SVM-based classification algorithm is demonstrated through simulations, compared with existing schemes.

## 1. Introduction

With burgeoning wireless technologies, the demand of spectrum is increasing consistently, which yields scarcity in spectrum resource. Previous assumptions on crisis of spectrum availability result in misconception. By the federal communication commission (FCC), it has been resolved that underutilization of licensed spectrum bands in either temporal or spatial is a principal reason of the spectrum scarcity [1]. To efficiently utilize the spectrum resource, cognitive radio (CR) with adaptive intelligence is fascinating researchers and developers to break through a spectrum congestion bottleneck [2]. CR is an intelligent wireless communication technology with efficient spectrum utilization, trying to learn environments and adjust its parameters properly [2]. Licensed primary users (PUs) can transmit at any time with no restrictions, while secondary users (SUs) in CR networks (CRNs) obtain the benefit of spectrum access when the PUs do not use the corresponding spectrum [3].

Spectrum sensing is one of the important parts of CRN. Such far, various sensing techniques such as cyclo-stationary-based sensing, waveform-based sensing, and energy detection-based sensing were proposed and utilized for spectrum sensing [4]. Among these techniques, the energy detection is the most efficient technique when no prior information of the PU is available. Individual sensing at each SU is often inaccurate due to multipath fading, shadowing, and hidden terminal problems in wireless environments [5]. These are able to cause incorrect detections in PU activity, which result in false alarm and thus reduce the SUs' opportunities to access the spectrum. Similarly, any misdetection of the occupied PU channel in CRN can produce interference to the licensed PUs. To overcome these issues, cooperative spectrum sensing (CSS) was proposed. It significantly improves the accuracy of detection of PU activity and helps to increase the performance of secondary communication systems [6–8]. The CSS is able to be implemented in either distributed or centralized manner. In distributed spectrum sensing, each SU individually senses the spectrum and decides whether the spectrum is available or not. In centralized spectrum sensing, a number of SUs form a network and send their local sensing results (either 0 or 1) to the fusion center (FC) in order to decide the existence of PUs. The final decision regarding the existence of PUs is made based on the information received from all the SUs by using AND, OR, and majority rules [9].

However, CSS is also vulnerable to security threats. Security for CRN is an important part to ensure secure operations of underlying network infrastructure [10]. Various attacks, which highly degrade the performance of network, have been studied in the literature. Two most common attacks in CRN are primary user emulation attack (PUEA) and spectrum sensing data falsification (SSDF) attacks [11, 12]. In PUEA, some outliers try to mimic data transmission of the PU to disturb sensing operations of SUs. The presence of PUEA makes the FC decide that the spectrum band under consideration is unavailable, and SUs hold their processes for opportunistic spectrum access. In SSDF attacks, false information is sent to the FC that leads an incorrect global decision on the PU channel activity. In [13], six types of SSDF attacks are elaborated. In always yes MU (AYMU) attack, the SU always sends "1" to the FC whatever a local result is determined. Hence, this attack denies the SU to access the spectrum. On the contrary, in always no MU (ANMU) attack, the SU always sends "0" to the FC. Thus, it causes interference to the PU channel. In always opposite MU (AOMU) attack, the MU sends the inverse of the local sensing result. It is the most dangerous attack. In random yes MU (RYMU) attack, the MU randomly sends "1" to the FC, regardless of the local sensing results. In random no MU (RNMU) attack, the MU randomly sends "0" to the FC, regardless of the local sensing results. In random opposite MU (ROMU), the MU randomly sends the inverse of the local sensing result to the FC. To mitigate the effect of these attacks, several different schemes were proposed [14–16].

Some heuristic approaches in CSS can lead to an optimal global decision. Among them, a genetic algorithm (GA), a class of computational algorithm motivated by evolution, is a good candidate to find the optimal solution by applying bioinspired approaches to given problems [17, 18]. On the other hand, a machine learning (ML) technique is another good candidate by learning surrounding environments. The heuristic nature of ML technique encourages employing in CRN as well. Moreover, these techniques can provide sufficiently good performance in spectrum sensing classification [19].

As representative ML-based classification and regression algorithms, there are $k$-nearest neighbor, decision tree, naive Bayes, logistic regression, support vector machine (SVM), $k$-means clustering neural networks, and so on [20, 21]. In general, the SVM-based classifier outperforms the other techniques in practical problems due to kernel function trick [22–24]. In the SVM-based classifier, the problems that are not properly classifiable in a feature space are transformed to a high-dimensional space where classification is possible using a linear hyperplane.

In this paper, we employ an SVM-based classifier in order to classify the spectrum sensing results into legitimate SU and MU categories. In addition, an energy detection technique is utilized for sensing environments. Once the sensing is performed, the proposed SVM-based algorithm is employed on the data set and, it finds the maximal margin between the legitimate SUs and MUs. After the classification of legitimate SUs and MUs at the FC, the FC employs the DS evidence theory to measure the performance of the proposed SVM-based algorithm. The proposed scheme is verified in terms of false sensing probability when there exists either AYMUs, ANMUs, or random MUs (RMUs) in CSS environments. The AYMU sends higher energy statistics of the channel than actual status, and thus, it increases false alarm probability. The ANMU forwards lower energy statistics than actual status. Therefore, it results in misdetection and induces interference to the PUs. The RMUs randomly behaves in between both classes with probability 1-$p$. The effectiveness of the proposed scheme is evaluated through simulations in comparison with other existing schemes.

The rest of this paper is organized as follows. In Section 2, the system model considered through this paper is presented. In Section 3, the proposed SVM-based algorithm to classify

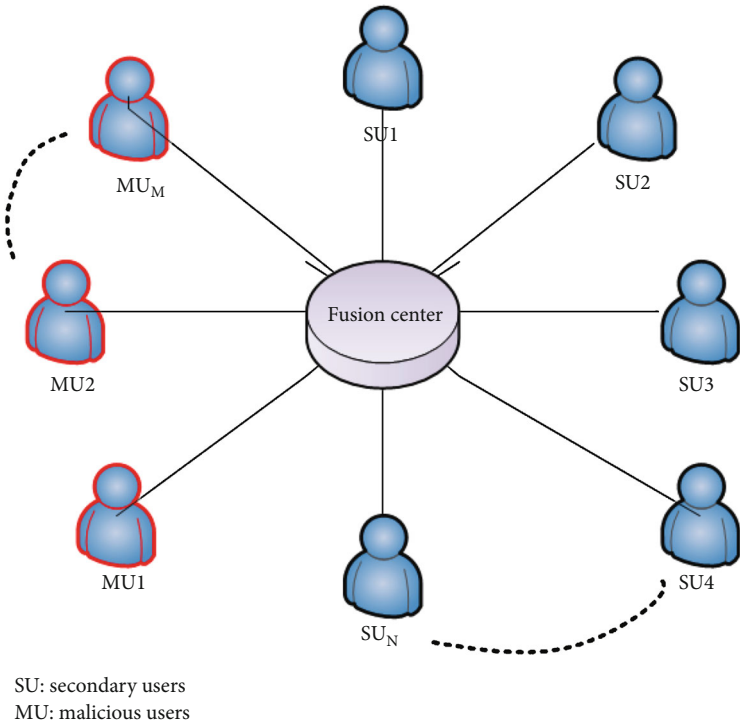


Figure 1: CSS system model.

legitimate SUs and MUs in CRN is presented. Numerical results are shown through simulations in Section 4. Finally, the paper is concluded in Section 5.

## 2. System Model

In this paper, we consider a CRN with $N$ SUs and $M$ MUs, where $M < N$ as shown in Figure 1. Initially, all the SUs including MUs perform spectrum sensing to determine the status of the PU in the network.

As in Figure 1, the SUs cooperate to sense the activity of the PU channel and inform the FC on their sensing information. The received information from the AYMU gives a higher energy signal which implies busy status of the PU channel. Similarly, the ANMU provides a low energy signal to the FC. The FC makes a global decision on the existence of the PUs in the network.

Each SU performs local sensing and sends its local result, either $H_0$ or $H_1$ for the absence or presence of PUs, respectively. The binary hypotheses test at the $j^{\text{th}}$ SU is expressed as follows:

$$x_j(t) = \begin{cases} H_0 & n_j(t), \\ H_1 & h_j s(t) + n_j(t), \end{cases} \tag{1}$$

where $H_0$ corresponds to the absence of the PU, $H_1$ corresponds to the presence of the PU, $x_j(t)$ is the received signal at the $j^{\text{th}}$ SU, $n_j(t)$ is the additive white Gaussian noise (AWGN), $h_j$ is the channel gain between the PU and the $j^{\text{th}}$ SU, and $s(t)$ is the signal transmitted by the PU.

Energy detection technique is very popular in CSS due to its ease of implementation and no requirement of prior information for the PU signal [25]. In this paper, we consider the energy detection for sensing the PU signals in the network.

The received signal test statistics of the PU channel by the $j^{\text{th}}$ SU is given by

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

where $K$ is the number of samples in the $i^{\text{th}}$ sensing interval. According to the central limit theorem (CLT), the number of samples needs to be large enough so that the energy reported by each SU becomes similar to a Gaussian random variable under both $H_0$ and $H_1$ as in [25]:

$$\begin{cases} N\left(\mu_0 = K, \sigma_0^2 = 2K\right), H_0, \\ N\left(\mu_1 = K\left(\gamma_j + 1\right), \sigma_1^2 = 2K\left(\gamma_j + 1\right)\right), H_1, \end{cases} \tag{3}$$

where $\gamma_j$ is the signal to noise ratio (SNR) between the PU and the $j^{\text{th}}$ SU. Similarly, $(\mu_0, \sigma_0^2)$ and $(\mu_1, \sigma_1^2)$ are the mean and variance values of the reported signals under $H_0$ and $H_1$ hypotheses, respectively.

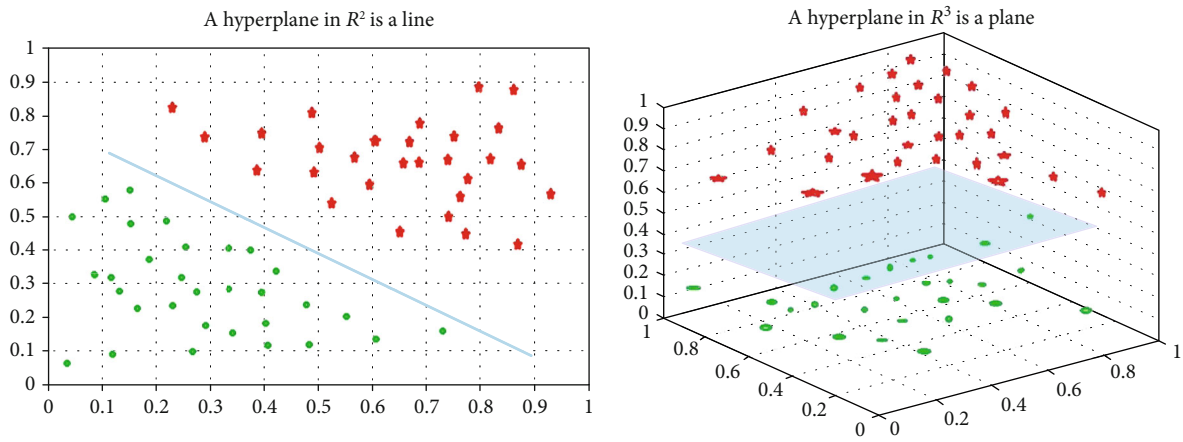


FIGURE 2: A hyperplane in $R^n$ is an $n$-1 dimensional space [29].

## 3. Proposed Support Vector Machine-Based MU Classification Algorithm

ML provides a computational machine with the ability to learn without being explicitly programmed. ML methods are very effective when the data set is large, diverse, and fast changing. These algorithms give deep and predictive analysis of data, and they are classified into two big groups: supervised learning (classification and regression) and unsupervised learning (clustering techniques) [26, 27]. Our objective is to classify legitimate SUs and MUs among all the SUs available in the environment. SVM is a highly competitive learning method which is popular in many fields based on statistical learning theory [28].

In this paper, we proposed an SVM-based classification algorithm in CRN to classify legitimate SUs and MUs. The SVM can be used both for classification and regression problems. However, it is mostly used for classification [26]. It works on the basis of a hyperplane, which divides the different classes of data well. A hyperplane is a classifier that may be a dot, a line, or a plane depending upon the data scattered. The dimension of the hyperplane is less than the dimension of the data, i.e., if data is three dimensional, the hyperplane has to be a plane of two dimensions, and if the data is two dimensional, the hyperplane can be a line as shown in Figure 2.

The hyperplane is a point for one dimensional data. The concept of maximal margin decides the optimal hyperplane, whereas the margin is the distance between two support vectors. The support vectors are the data points nearest to the hyperplane, and these points are called critical points. If these points are moved, the position of hyperplane can be altered. Whenever test data is added, its position is decided as one of the classes.

As an application of SVM classification in CRN, we consider an environment in which $N$ legitimate SUs and $M$ MUs exist.

The notation of the data set is expressed as

$$D = \left\{ \left( \mathbf{x}_j, \mathbf{y}_j \right) \mid \mathbf{x}_j \in \mathbb{R}^n, \mathbf{y}_j \in \{-1, 1\} \right\}_{j=1}^{n}, \tag{4}$$

where $\mathbf{x}_j$ is the energy vector of $N$ SUs, $\mathbf{y}_j$ is the class vector, and class "1" and "-1" represent legitimate SUs and MUs, respectively.

Once the sensing is done, the sensing results are fed into the SVM. The main objective of the proposed SVM-based scheme is to precisely classify legitimate SUs and MUs. First of all, we trace the support vectors and then draw two support hyperplanes. The optimal forms that define support hyperplanes to classify the legitimate SUs and MUs are given by

$$w.x + b = \delta, \tag{5}$$

$$w.x + b = -\delta, \tag{6}$$

where $w$ is the weight vector obtained in training phase, $b$ is a threshold value, and $\delta$ is an arbitrary constant. In the training phase, the distance between these two hyperplanes is called margin, and there are no data points in the margin. The margin can be clearly visualized by the following formula:

$$Y_i(w.x_i + b) \leq \delta. \tag{7}$$

The overlap region formed by (7) is the margin. At last step, we classify the given data by the hyperplane. The linearly nonseparable patterns are mapped onto a higher dimensional space such that the classification is possible using a linear hyperplane.

The overall flow chart of the proposed SVM-based scheme is shown in Figure 3.

The proposed SVM-based MU classification algorithm are shown in Algorithm 1. The algorithm consists of three phases of data generation, sensing, and classification.

Once the classification is done through the proposed SVM-based algorithm, the FC utilizes the DS evidence theory to combine the evidence values of $H_0$ and $H_1$ to make a global decision for the existence of the PU in the network.

In the DS evidence theory, the frame of discernment can be defined as $F_r = \{H_1, H_0, \Omega\}$ where $\Omega$ is the ignorance hypothesis, which describes whether hypotheses are true or

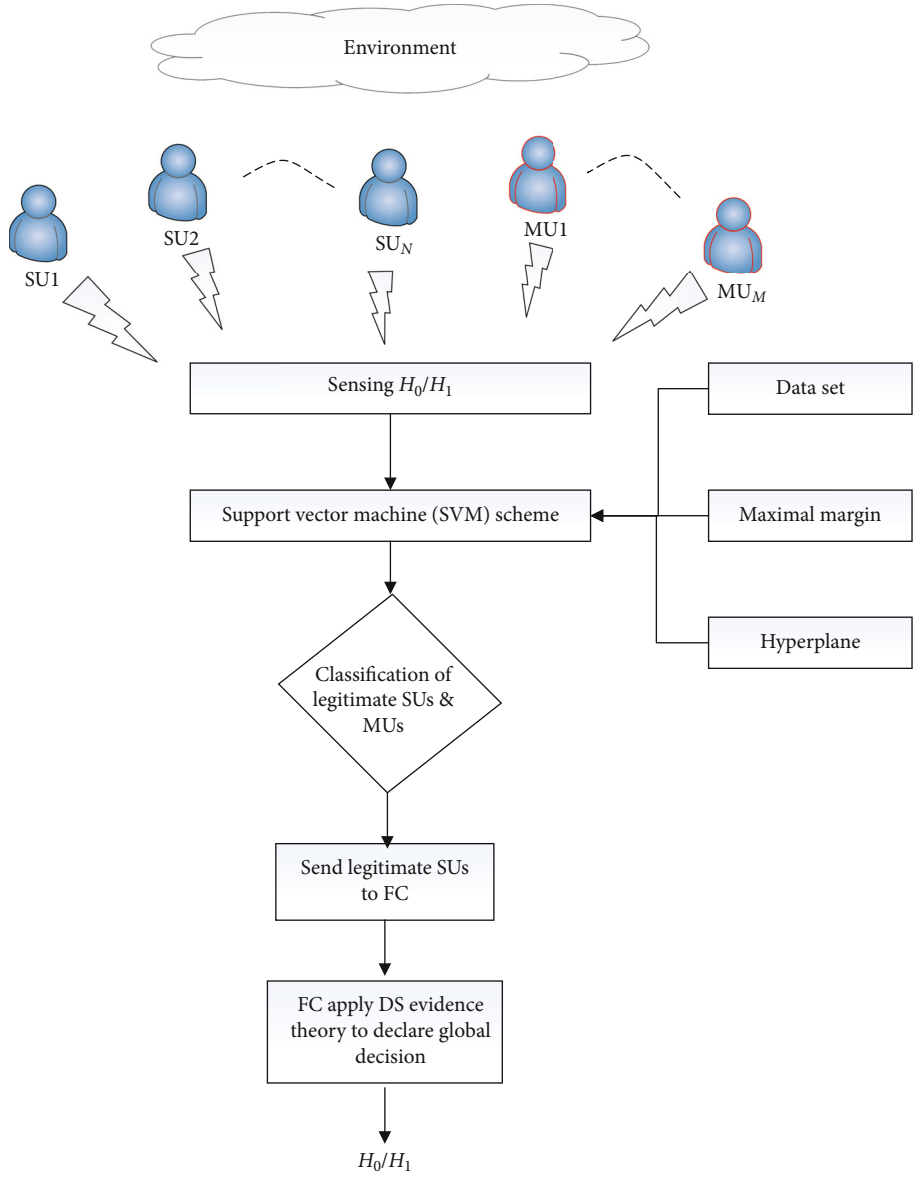


Figure 3: Proposed flowchart.

not. After each SU measures the basic probability assignment (BPA), $m(H_0)$ and $m(H_1)$, under hypotheses $H_0$ and $H_1$, respectively. The BPA measures are defined in the form of cumulative distribution function as follows [30]:

$$m_j(H_0) = \int_{E_j}^{+\infty} \frac{1}{\sqrt{2\pi}\sigma_{0j}} \exp\left(-\frac{\left(\mathbf{X}_j - \mu_{0j}\right)^2}{2\sigma^2{}_{0j}}\right) dx, \quad (8)$$

$$m_j(H_1) = \int_{-\infty}^{E_j} \frac{1}{\sqrt{2\pi}\sigma_{1j}} \exp\left(-\frac{\left(\mathbf{X}_j - \mu_{1j}\right)^2}{2\sigma^2{}_{1j}}\right) dx, \quad (9)$$

where $m_j(H_1)$, $m_j(H_0)$, and $m_j(\Omega)$ are the BPA hypotheses of $j^{\text{th}}$ SU, respectively. These values are sent to the FC by SUs, and the FC makes a global decision on the existence of the PU by using these measures.

According to the DS evidence theory, the BPA can be combined based on the following equations [30]:

$$m_j(H_0) = \sum_{Fr_1 \cap Fr_2 \cdots Fr_n = H_0} \prod_{j=1}^{n} m_j(\mathrm{Fr}_j)/(1-k), \quad (10)$$

$$m_j(H_1) = \sum_{Fr_1 \cap Fr_2 \cdots Fr_n = H_1} \prod_{j=1}^{n} m_j(\mathrm{Fr}_j)/(1-k), \quad (11)$$

where $k = \sum_{Fr_1 \cap Fr_2 \cdots Fr_n = \varnothing} \prod_{j=1}^{n} m_j(\mathrm{Fr}_j)$, and $\mathrm{Fr}_j$ is an element of the set $\{H_1, H_0, \Omega\}$.

*A. Generation of Data*
Initialization of parameters such as number of iteration, number of Sus.
Generate random MUs with Gaussian distribution.
Generate normal SUs.
Generate the indices on which MUs attack.
Generate indices for position of normal SUs.
*B. Sensing the data*
*For* $n = 1$ to *Sensing Interval*
*For* $i = 1$ to $N$
Energy reported by the $j^{th}$ SUs.
*End*
*For* $i = 1$ to $M$
Energy reported by the MUs.
*End*
End sensing interval
*C. Support Vector Machine Algorithm*
*1. Data Processing*
i. Combining the data
ii. Input the data
iii. Train the data
iv. Find the number of examples and attributes used in the data.
v. Extract the attribute matrix X and the label vect Y.
*2. Support Vector*
i. Finding the support vectors (Corner points)
ii. Draw the upper and lower hyperplanes.
iii. Finding the maximal margin by the upper and lower hyperplane.
*3. Classification*
i. Linear
Finding weights
$Y_1 = -(w_1.x_1 + b)/w_2$
ii. Drawing the hyperplane to classify the data.
*D. Plotting*
i. Normal data plotting.
ii. Malicious data plotting.
iii. Plotting of hyperplane.

Algorithm 1. Proposed SVM-based MU classfication algorithm.

Table 1: Simulation parameters.

| Parameters | Values |
|---|---|
| Number of SUs | 10 |
| Probability of PU | 0.5 |
| Number of MUs | 4 |
| Number of iterations | 100 |

Finally, a simple decision strategy is chosen at the FC to declare the global decision as

$$f_d = \begin{cases} H_1; & \dfrac{m(H_1)}{m(H_0)} > \lambda, \\ H_0; & \dfrac{m(H_1)}{m(H_0)} \leq \lambda. \end{cases} \quad (12)$$

## 4. Numerical Results and Evaluation

To evaluate the effectiveness of the proposed SVM-based scheme, we conduct extensive simulations by using MATLAB tool. In our simulation, we consider a CRN with $M = 10$ SUs. Among the total number of SUs, six SUs are selected as legitimate SUs, and four are randomly selected as MUs. According to IEEE 802.22 standards, it is assumed that the used bandwidth is 6 MHz, and the PU activity is 0.5. The detailed simulation parameters are listed in Table 1.

We perform the simulation in two parts. In the first part, we simulate the proposed SVM-based scheme when no MUs exist in the network, AYMUs exist in the network, ANMUs exist in the network, and RMUs exist in the network. In the second part, we compare the performance of the proposed SVM-based scheme with those of the other existing schemes.

First of all, we show the results when only legitimate SUs exist in the network, ANMUs exist in the network, AYMUs exist in the network, and when RMUs exist in the network. In Figures 4–7, the random generation of legitimate SUs and MUs is shown, and the classification of legitimate SUs and MUs is clearly presented by employing the proposed SVM-based scheme. The AYMU is the one which always feeds the local sensing result as the PU absence. The ANMU is the one which always feeds it as the PU presence. The RMU is the most difficult attack to classify, since in this attack, the

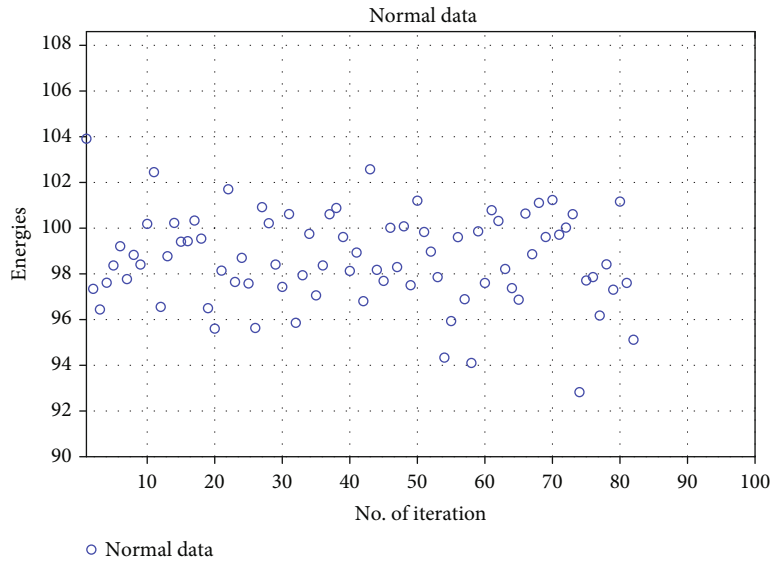


Figure 4: Normal data generation.

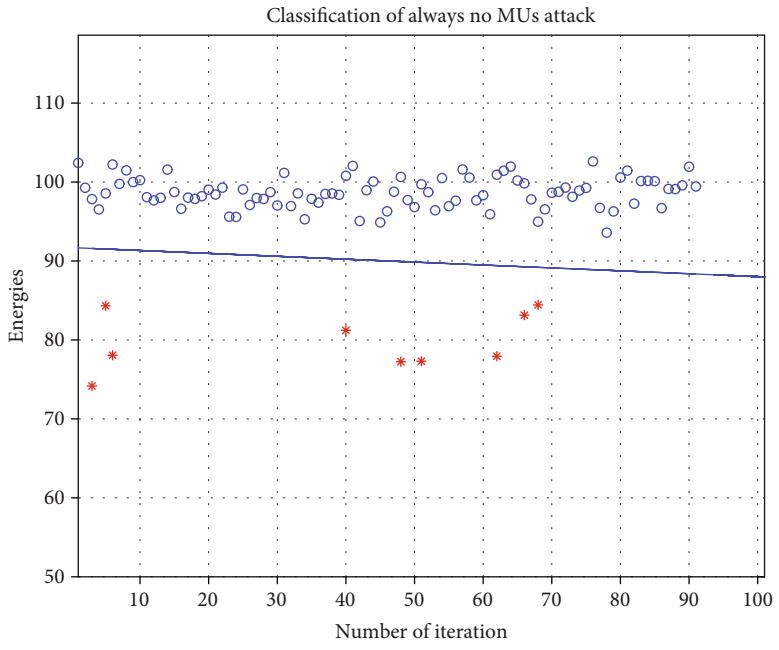


Figure 5: Classification of legitimate SUs and MUs, when ANMUs exist.

MUs sometime behave like AYMU and sometime like ANMU with probability 1-$p$.

Figure 4 shows the normal data generation by legitimate SUs. The range of sensing energies at the legitimate SUs lies on the range of 90-108. From Figure 4, it can be observed that the legitimate SUs send different energies with different probabilities and different number of iterations. None of the number of iterations is out of the range of the defined energy range (i.e., 90-108). Thus, for all the number of iterations, the data of the legitimate SUs are represented.

Figure 5 shows the classification result of the legitimate SUs and ANMUs by employing the proposed SVM-based scheme. The SVM works on the concept of hyperplane. A hyperplane is an $n$-dimensional line used to classify different classes of the data by maximum margin. In Figure 5, the legitimate SUs are denoted by blue circles, while MUs are denoted by red circles. The result shows that when the ANMU attack where MUs always produce lower energies than actual status exist in the network, it is well-classified by the proposed SVM-based algorithm.

Figure 6 shows the classification of legitimate SUs and MU, when AYMUs exist in the networks. The AYMU always sends higher energies than actual status to the FC, which results in the existence of the PU in the network. The AYMU degrades the system performance in terms of the opportunity of channel access by the SUs. It is shown that the proposed

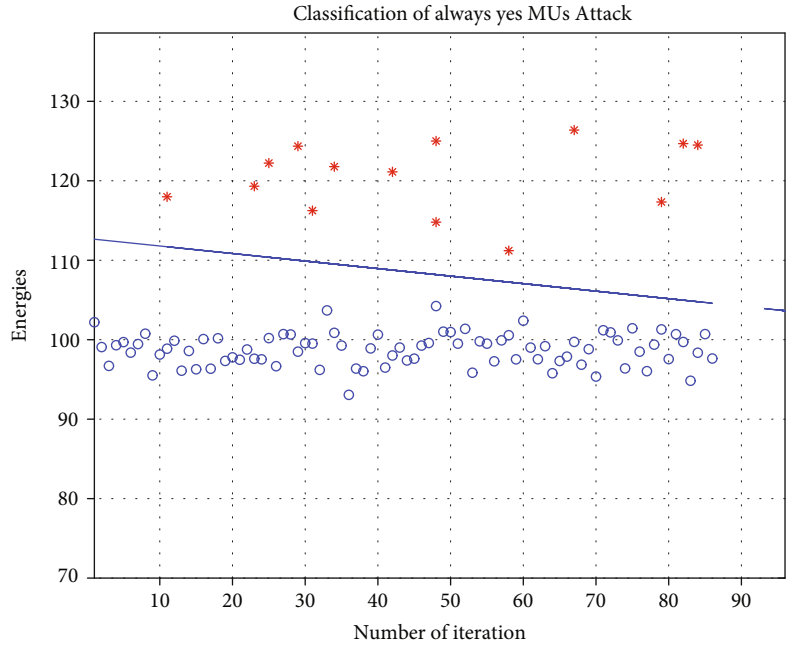


Figure 6: Classification of legitimate SUs and MUs, when AYMUs exist.

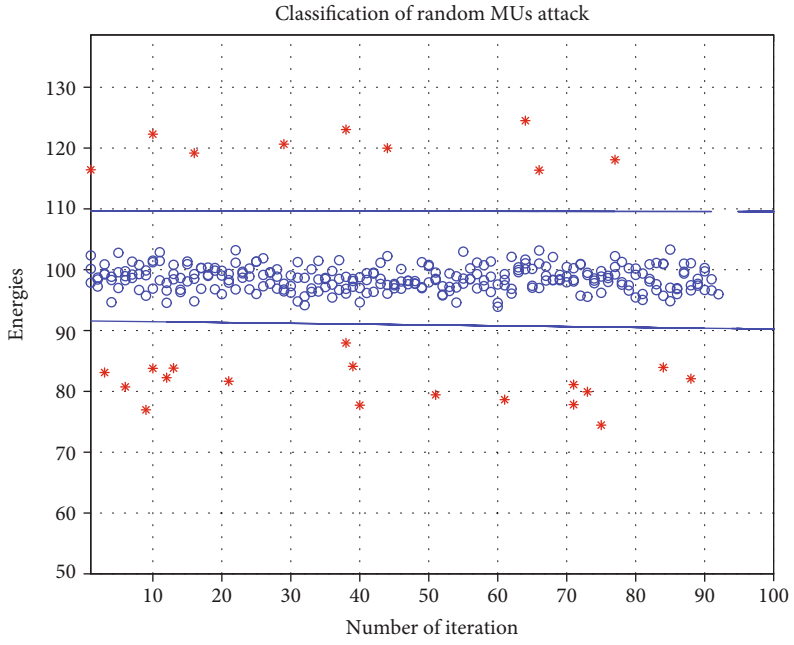


Figure 7: Classification of legitimate SUs and MUs, when RMUs exist.

SVM-based algorithm efficiently classifies the legitimate SUs from the MUs in the network.

Figure 7 shows the classification of legitimate SUs and MUs, when RMUs, who sometimes behave like AYMUs and sometimes like ANMUs, exist in the networks. The legitimate SUs are in the range of 90-108 energy level. The AYMUs have energy level higher than 108, and the ANMUs have the energy level less than 90. The RMUs are the most difficult attack to classify, since the SUs behave randomly with probability 1-$p$. Through the proposed SVM scheme, the legitimate SUs and the RMUs can be efficiently classified.

In this part of the simulation, we compare the performance of the proposed SVM-based scheme with the other existing schemes. Through Figures 8–10, we show the performance of the proposed SVM-based scheme when ANMUs, AYMUs, and RMUs attackers are in the network, compared to the existing schemes.

Figure 8 shows the region of convergence (ROC) curve of the proposed SVM-based scheme in comparison with other

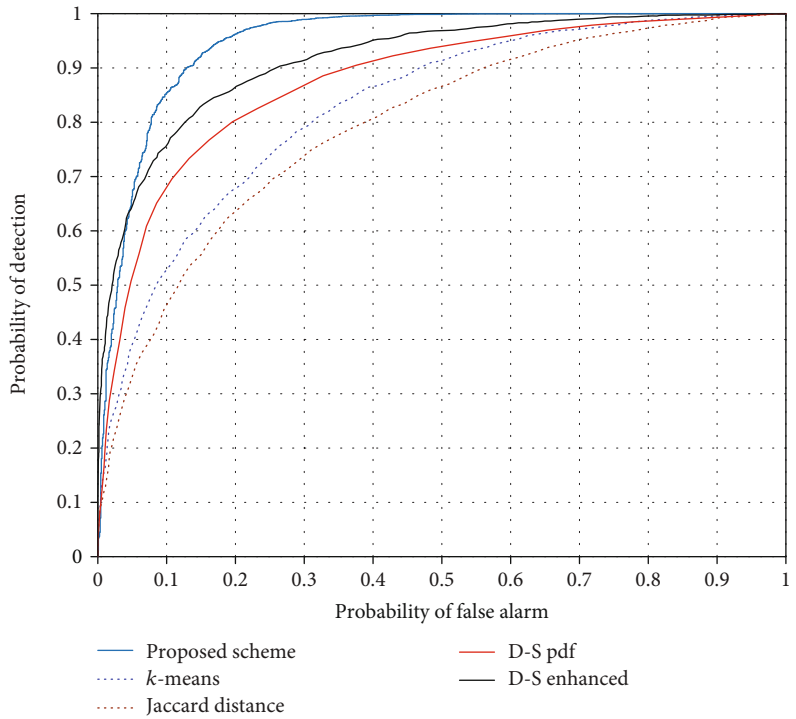


Figure 8: ROC curve of proposed scheme with other schemes, when ANMUs exist.

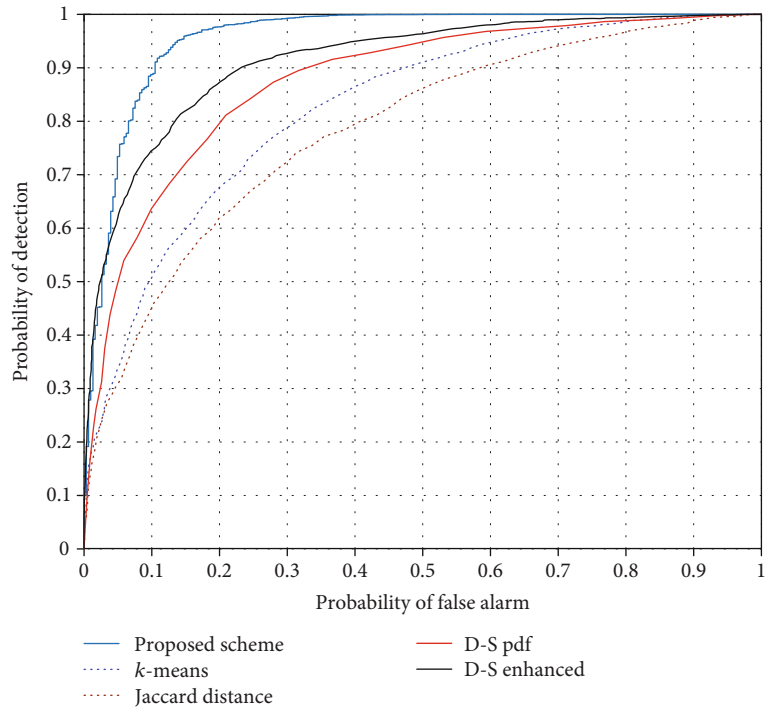


Figure 9: ROC curve of proposed scheme with other schemes, when AYMUs exist.

existing schemes, when ANMUs exist in the network. It is shown through simulation results that the proposed SVM-based scheme efficiently classifies the legitimate SUs and ANMUs. Once the legitimate SUs and ANMUs classified, the ROC of the proposed SVM-based scheme is plotted in comparison with those of the existing schemes. It is observed that the proposed SVM-based scheme outperforms the other existing schemes.

Figure 9 shows the ROC curve of the proposed SVM-based scheme in comparison with other existing schemes,

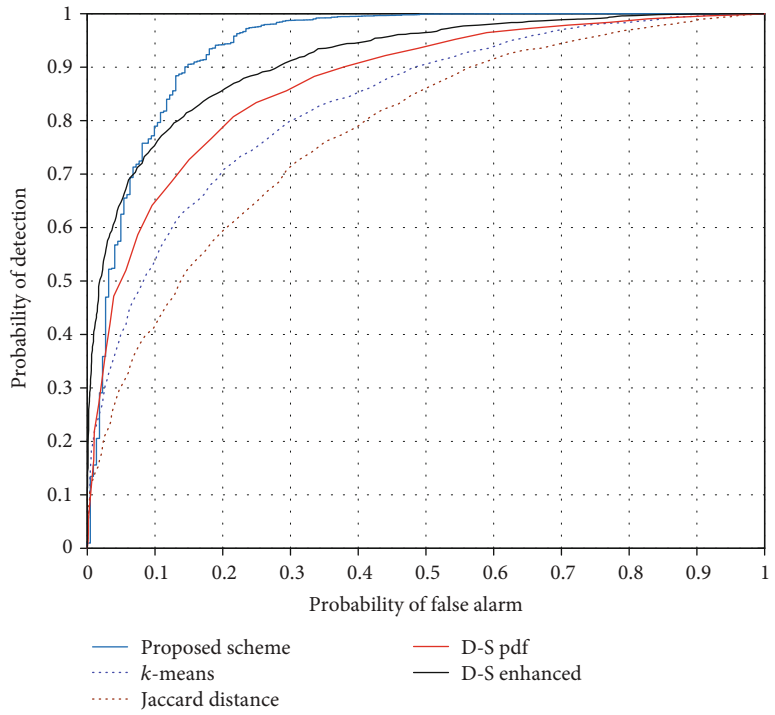


Figure 10: ROC curve of proposed scheme with other schemes, when RMUs exist.

when AYMU exist in the network. It is shown through simulation that the proposed SVM-based scheme efficiently classifies the legitimate SUs and AYMUs. The ROC curve shows that the proposed SVM-based scheme has better performance than the other existing schemes.

Figure 10 shows the ROC curve of the proposed SVM scheme in comparison with other schemes, when RMUs exist in the network. It is shown that proposed SVM-based scheme efficiently classifies the legitimate SUs and RMUs. The ROC shows that the proposed SVM-based scheme also outperforms the other existing schemes even when RMUs exist.

It is clear that based on the SVM-based classification, the proposed SVM-based scheme can optimize to classify legitimate SUs from MUs efficiently. The risk of considering the MUs in CSS is significantly removed with the proposed SVM-based scheme. Consequently, the proposed SVM-based scheme is able to identify and classify the MUs and provide the reliable sensing results in CSS-based CRNs.

## 5. Conclusions

Recently, machine learning has attracted attentions in spectrum sensing. The main reason of the attraction is that it is a heuristic approach without requiring the prior information about surrounding environments. Cooperative spectrum sensing (CSS) improves the performance of cognitive radio networks (CRNs). However, the performance of CSS severely degrades by attacks from malicious users (MUs). In this paper, we proposed a support vector machine- (SVM-) based algorithm to classify legitimate secondary users (SUs) and MUs. Once the legitimate SUs and MUs are classified through the proposed SVM-based algorithm, a fusion center (FC) combines the diversified sensing reports received from the legitimate SUs based on the DS evidence theory in order to make a global decision on the existence of primary users (PUs) in the network. The numerical results verified the superiority and the authenticity of the proposed SVM-based classification of the legitimate SUs and MUs.

## Data Availability

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

## Conflicts of Interest

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

## Acknowledgments

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

## References

[1] FCC, *Notice of proposed rule-making and order*, Washington, D.C., 2003ET Docket No. 03-222.

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

[3] L. Zhai, H. Wang, and C. Gao, "A Spectrum Access Based on Quality of Service (QoS) in Cognitive Radio Networks," *PLoS One*, vol. 11, no. 5, p. e0155074, 2016.

[4] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[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] M. S. Khan, M. Jibran, I. Koo, S. M. Kim, and J. Kim, "A Double Adaptive Approach to Tackle Malicious Users in Cognitive Radio Networks," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 2350694, 9 pages, 2019.

[7] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radio," in *2006 IEEE International Conference on Communications*, Istanbul, Turkey, 2006.

[8] Y. He, J. Xue, T. Ratnarajah, M. Sellathurai, and F. Khan, "On the Performance of Cooperative Spectrum Sensing in Random Cognitive Radio Networks," *IEEE Systems Journal*, vol. 12, no. 1, pp. 881–892, 2018.

[9] S. Chilakala and M. S. S. Ram, "Optimization of cooperative secondary users in cognitive radio networks," *Engineering Science and Technology, an International Journal*, vol. 21, no. 5, pp. 815–821, 2018.

[10] M. Jenani, "Network security, a challenge," *International Journal of Advanced Networking and Applications*, vol. 8, no. 5, pp. 120–123, 2017.

[11] J. Marinho, J. Granjal, and E. Monteiro, "A survey on security attacks and countermeasures with primary user detection in cognitive radio networks," *EURASIP Journal on Information Security*, vol. 2015, no. 1, 2015.

[12] H. Wu, X. Sun, C. Guo, and S. Ren, "Malicious user detection for wide-band cognitive radio network," in *2016 Asia-Pacific Microwave Conference (APMC)*, New Delhi, India, 2016.

[13] A. Taggu, C. Chunka, and N. Marchang, "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 - WCI '15*, Kochi India, 2015.

[14] B. Sarala, S. R. Devi, M. Suganthy, and S. J. Ida, "A novel authentication mechanism for cognitive radio networks," *International Journal of Recent Technology and Engineering*, vol. 8, no. 4, pp. 713–718, 2019.

[15] R. Wan, L. Ding, N. Xiong, and X. Zhou, "Mitigation strategy against spectrum sensing data falsification attack in cognitive radio sensor networks," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019.

[16] F. Farmani, M. A. Jannatabad, and R. Berangi, "Detection of SSDF Attack Using SVDD Algorithm in Cognitive Radio Networks," in *2011 Third International Conference on Computational Intelligence, Communication Systems and Networks*, Bali, Indonesia, 2011.

[17] 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.

[18] M. S. Khan, N. Gul, J. Kim, I. M. Qureshi, and S. M. Kim, "A Genetic Algorithm-Based Soft Decision Fusion Scheme in Cognitive IoT Networks with Malicious Users," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 2509081, 10 pages, 2020.

[19] F. Azmat, Y. Chen, and N. Stocks, "Analysis of Spectrum Occupancy Using Machine Learning Algorithms," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, pp. 6853–6860, 2016.

[20] P. Harrington, *Machine Learning in Action*, Manning Publications, 2012.

[21] K. Patan, "Artificial neural networks for modelling and fault diagnosis of technical process," *Lecture Notes in Control and Information Sciences*, vol. 377, 2008.

[22] F. Wang, Z. Zhen, B. Wang, and Z. Mi, "Comparative study on KNN and SVM based weather classification Models for day ahead short term solar PV power forecasting," *Applied Science*, vol. 8, no. 1, p. 28, 2018.

[23] K. Elangovan, Y. Krishnasamy Tamilselvam, R. Mohan, M. Iwase, N. Takuma, and K. Wood, "Fault Diagnosis of a Reconfigurable Crawling–Rolling Robot Based on Support Vector Machines," *Applied Science*, vol. 7, no. 10, p. 1025, 2017.

[24] S. U. Jan, Y.-D. Lee, J. Shin, and I. Koo, "Sensor Fault Classification Based on Support Vector Machine and Statistical Time-Domain Features," *IEEE Access*, vol. 5, pp. 8682–8690, 2017.

[25] M. S. Khan and I. Koo, "The Effect of Multiple Energy Detector on Evidence Theory Based Cooperative Spectrum Sensing Scheme for Cognitive Radio Networks," *Journal of Information Processing Systems*, vol. 12, no. 2, pp. 295–309, 2015.

[26] Y. Molina-Tenorio, A. Prieto-Guerrero, R. Aguilar-Gonzalez, and S. Ruiz-Boqué, "Machine Learning Techniques Applied to Multiband Spectrum Sensing in Cognitive Radios," *Sensors*, vol. 19, no. 21, p. 4715, 2019.

[27] V. Sharma and V. Bohara, "Exploiting machine learning algorithms for cognitive radio," in *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, New Delhi, India, 2014.

[28] D. Zhang and X. Zhai, "SVM-based spectrum in cognitive radio," in *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, Wuhan, China, 2011.

[29] N. S. Chauhan, *A Friendly Introduction to Support Vector Machine (SVM)*, Towards Data Science, 2019.

[30] M. S. Khan and I. Koo, "Mitigation of Adverse Effects of Malicious Users on Cooperative Spectrum Sensing by Using Hausdorff Distance in Cognitive Radio Networks," *Journal of information and communication convergence engineering*, vol. 13, no. 2, pp. 74–80, 2015.