ACTA IMEKO
ISSN: 2221-870X
March 2022, Volume 11, Number 1, 1 - 7

Mitigation of spectrum sensing data falsification attack using multilayer perception in cognitive radio networks

Mahesh Kumar Nanjundaswamy[1], Ane Ashok Babu[2], Sathish Shet[3], Nithya Selvaraj[4], Jamal Kovelakuntla[5]

[1] *Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka-560078, India*
[2] *Department of Electronics and Communication Engineering, PVP SIDDHARTHA INSTITUTE OF TECHNOLOGY, Vijayawada, Andhra Pradesh-520007, India*
[3] *Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bengaluru, Karnataka- 560060, India*
[4] *Department of Electronics and Communication Engineering, K. Ramakrishnan College of technology, Tiruchirappalli-621112, Tamilnadu, India*
[5] *Department of Electronics and Communication Engineering, Gokaraju Rangaraju Institute of Engineering and Technology (GRIET), Hyderabad, Telangana-500090, India*

ABSTRACT
Cognitive radio network (CRN) is used to solve spectrum scarcity and low spectrum utilization problems in wireless communication systems. Spectrum sensing is a vital process in CRNs, which needs continuous measurement of energy. It enables the sensors to sense the primary signal. Cooperative Spectrum Sensing (CSS) has recommended to sense spectrum accurately and to enhance detection performance. However, Spectrum Sensing Data Falsification (SSDF) attack being launched by malicious users can lead to wrong global decision on the availability of spectrum. It is an extremely challenging task to alleviate impact of SSDF attack. Over the years, numerous strategies have been proposed to mitigate SSDF attack ranging from statistical to machine learning models. Energy measurement through statistical models is based on some predefined criteria. On the other hand, machine learning models have low sensing performance. Therefore, it is necessary to develop an efficient method to mitigate the negative impact of SSDF attack. This paper intends to propose a Multilayer Perceptron (MLP) classifier to identify falsified data in CSS to prevent SSDF attack. The statistical features of the received signals are measured and taken as feature vectors to be trained by MLP. In this manner, measurement of these statistical features using MLP becomes a key task in cognitive radio networks. Trained network is employed to differentiate malicious users signal from honest users' signal. The network is trained with the Levenberg-Marquart algorithm and then employed for eliminating the effect of attacks due to the SSDF process. Once the simulated results are observed, it can be revealed that the proposed model could efficiently reduce the impact of malicious users in CRN.

Section: RESEARCH PAPER

Keywords: Cognitive radio network; cooperative spectrum sensing; energy statistic; machine learning model; spectrum sensing data falsification

Citation: Mahesh Kumar Nanjundaswamy, Ane Ashok Babu, Sathish Shet, Nithya Selvaraj, Jamal Kovelakuntla, Mitigation of spectrum sensing data falsification attack using multilayer perception in cognitive radio networks, Acta IMEKO, vol. 11, no. 1, article 21, March 2022, identifier: IMEKO-ACTA-11 (2022)-01-21

Section Editor: Md Zia Ur Rahman, Koneru Lakshmaiah Education Foundation, Guntur, India

Received November 20, 2021; **In final form** March 1, 2022; **Published** March 2022

Corresponding author: Mahesh Kumar Nanjundaswamy, e-mail: mkumar.n19@gmail.com

1. INTRODUCTION

Over the past years, the world has witnessed a tremendous growth in the field of wireless communication technologies due to the popularity of telemedicine, smart home, smartphones, autonomous vehicles, mobile televisions and smart cities. The increasing demand for wireless communications has brought the problem of spectrum scarcity. Energy detection and measurement is a key task in spectrum sensing in cognitive radio networks. As a result, development of hybrid machine learning or signal processing algorithms becomes an intense research area for both measurement technology as well as in cognitive radio communications. The Federal Communications Commission

(FCC) [1], [2] reported that most of the allocated spectrum is rarely used by the Primary Users (PUs) (FCC, 2002; FCC, 2003). In order to solve the conflicts between spectrum utilization and spectrum shortage, it has been recommended that opportunistic access to the licensed spectrum should be given to Secondary Users (SUs). Cognitive Radio Network (CRN) has been developed to solve the aforementioned issues by enabling dynamic spectrum access. It is a new paradigm that offers the potential to utilize the licensed spectrum in an opportunistic manner [3] (Wan et al. 2019). CRN allows SUs to sense and access free spectrum bands without interfering PUs. CRN allows SUs to use valid spectrum, the spectrum scarcity problem will be solved successfully. SUs needs to monitor continuously [4], [5] to sense the PU status. Therefore, spectrum sensing becomes an important process for CRN. Spectrum sensing is the process of identifying status of PU. An accurate detection of spectrum can enhance the performance of CRN significantly [6]-[8] (Ali et al., 2017). However, due to obstacles, shadowing and multipath fading, wrong detections could take place, thus resulting in an in-efficient usage considering the licensed spectrum. To deal such an issue, Cooperative Spectrum Sensing (CSS) has been considered as a satisfactory candidate for spectrum sensing [9] (Sharifi et al., 2016). CSS combines all CUs sensing signal and makes final decision. It prevents the effect of noise, pathloss, shadowing and fading that may occur in wireless communication. However, CSS is vulnerable to many security threats. Among many attacks, Spectrum Sensing Data Falsification (SSDF) can severely affect the detection performance of CRN. In SSDF attack, Malicious Users (Mus) sent falsified report to the Fusion Center (FC) about the spectrum band. SSDF attack mislead global decision by sending falsified report about the spectrum availability, hence degrading the CRN performance. Therefore, it is essential to develop an efficient method to eliminate the impact of SSDF attacks. The core contributions of this research work are as follows:

The main aim or the focus of this research article will relate to the designing of an efficient model by using artificial neural network to suppress the negative impact of MUs in CRN and to enhance the detection performance through measuring various statistical parameters. In this scheme, a set of features are extracted from the received signals and then generated a large representative dataset. Multilayer Perceptron (MLP) [10], [11] is designed with one of input layer, two layers which are hidden and one output layer. Next, the obtained feature vectors could be grouped into two sets, viz., training and testing. The data's with respect to the training sets could be used for developing and training the MLP. Testing data set is employed to validate the efficacy of the proposed model. Performance of the proposed model is evaluated by measuring some commonly used metrices. Spectrum sensing refers to the process of detecting the activity of PUs in a licensed spectrum band. It plays a vital role in CRNs and CSS [12]-[14] has been suggested to make accurate decision about spectrum availability by utilizing spatial diversity via observations of multiusers. But CSS has some limitations. SSDF can severely affect the detection performance of the CRNs in which false sensing report sent by MUs during the CSS. To eliminate SSDF attack, several methods have been reported in the literature. Each method has their own characteristics. None of the method provide consistent result. Thus, the main aim or the focus of this research article will relate to the designing of an efficient model by using artificial neural network to suppress the negative impact of MUs in CRN and to enhance the detection performance.

The rest of the article is outlined as mentioned in the following sentences. The 2nd section presents an exhaustive review of former methods. The section 3 describes the development of the system model which is proposed here. Section 4 provides experimental outcomes. The paper ends with the conclusive remarks presented in the 5th section.

2. RELATED WORK

Several research literatures have proved that CSS is a good candidate to detect the activity of PU in CRN. However, CSS is affected by many attacks such as the primary user emulsion attack and SSDF. Amidst, SSDF is the dangerous attack in CRN, SSDF attack can reduce the detection performance by sending falsified report to FC. Over the past years, several methods have proposed to resist SSDF attack. Wan et al., (2019) [15], [16] presented a method to mitigate the influence of the attacks using the SSDF concepts involving the concepts of the combinations of the linear weights. Adaptive reputation method is also presented to differentiate MUs from SUs. Feng et al. (2018) [17] used the Exclusive-OR (XOR) distance analysis to eliminate the influence of SSDF in CRN. In this approach, XOR distance with hypothesis detecting the information is employed to calculate the equivalency between the two super-users. Based on the XOR distance, MUs is separated from SUs. Soft decision-based scheme to resist SSDF is developed by Ahmadfard et al. (2017) proposed method achieved better result than existing methods.

In the article in Ahmed et al. (2014), the authors presented a method to combat the effect of MUs in CRNs using the Bayseiens strategies. The authors used statistical features of received samples to sense the inexistence and existence of PU. Li et al. (2014) investigated the potential of the Fuzzy C-Means algorithm in spectrum sensing. The proposed algorithm is capable of detecting PU signal accurately, which in turn enhance the detection performance. Robust algorithm [18] to defence SSDF proposed by Althunibat et al. (2014). In this approach, specific weights are assigned to sensing nodes. Results showed that the algorithm is capable of detecting MUs. According to the mean and standard deviation of the received samples, Mapunya and Velempini (2018) developed a SSDF mitigation method in CRN. Results proved that the proposed scheme could reduce the probability of false alarm rate. Sharif et al. (2018) presented a defence strategy against SSDF attack. Mean value of received samples are computed. Two parameters α and β are obtained and then used in the likelihood ratio test method to enhance the detection performance.

Li and Peng (2016) used unsupervised machine learning model to differentiate honest SUs from MUs. The proposed model utilizes past sensing report as a feature vector to categorize users. Nie et al. (2017) proposed a defence scheme which is based on Bayesian learning model. Each user has specific weight that reflects its trustworthiness. Farmani et al. (2011) suggested the 'support a vector data description' method to detect the activity of PU. The proposed differentiate honest SUs from MUs based on the energy statistic signal. However, this method failed to decrease the probability of false alarm rate. Cheng et al. (2017) developed a self-organizing map to classify nodes into honest and malicious nodes. The proposed method uses Average Suspicion Degree to discriminate MUs from honest users. Amar Taggu et al. (2021) [19] proposed a two-layer model framework to classify SSDF attackers The first layer, the Computational layer, employs the Hidden Markov Model (HMM) to establish a probabilistic relationship between the PU's states and the sensing reports of the SUs. This generates the set of data needed for the next layer. The second layer, the Decision layer, employs several ML algorithms to categorise SUs as Byzantine attackers or normal SUs.

3. PROPOSED SYSTEM MODEL

The fundamental focus of this research work is developing and rendering a scheme for mitigating SSDF attack in CRN by using the models developed using the concepts of machine learning's. One of the hidden properties in the process of machine learning's is the concept of learning how to develop the relation between the two variables, i.e., the input and the output via training process which makes the scheme more robust. The developed model is simulated, and its performance compared with the earlier methods to prove its superiority.

The Figure 1 depicts the structure of cognitive radio network with one PU and 5 SUs. SUs uses the communication channel whenever the PU signal is absent. The SU's will perform the process of the Least Square Set (LSS) in order to detect the absence or the presence of the PU's and finally reporting the processes to the FC. Next, the FC will make a final verdict with respect to the spectrum availability which is relying on the received information's by the respective users. In this context, because of the presence of the MU's, secondary user/s will send some falsified reports to the FC. Let M MUs are presented in SUs. MUs can send either always yes or always no to FC. Always yes represents high energy (1) which increases the probability of the fake alarms (FALSE) as they are going to give an active status information of the primary user/s when it will be inactive in nature. Similarly, always no corresponds to low energy (0) which decreases the probability of detection because they send the primary user's absentia information's, even due to the presence of the PU's in the system. Both high and low signal of MUs degrade the performance of CRN. To deal such an issue, MLP is developed.

Spectrum sensing mainly used for detecting the presence or the inexistence of the PU's, which is shown in Figure 1, each SU receives noisy informative signal once the primary user becomes inactive in nature and finally, energy of the parameters used in the process could be calculated at time of the t^th^ instant using the p^{th} SU, which could be expressed by (1) as

$$S_p(t) = \frac{1}{N_1}\sum_{n=0}^{N_1-1}\left|\eta_p(t,n)\right|^2 . \qquad (1)$$

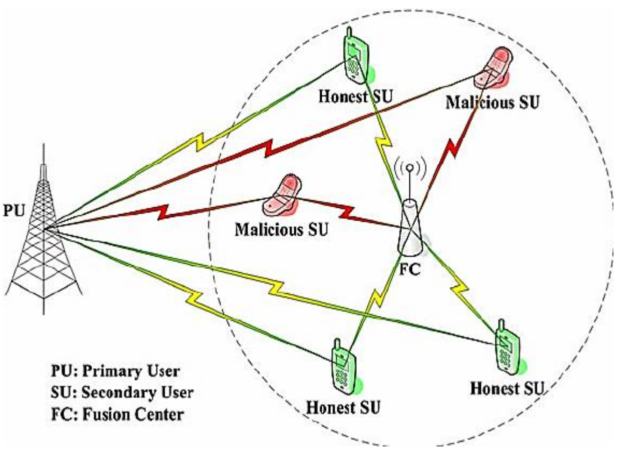

Figure 1. Cognitive radio network model.

In (1), the parameter $S_p(t)$ denotes the received noise by the p^{th} SU at t. N_1 represents the number of samples considered. When the PU is active, Equation (1) can be written in the form of Eqn. (2) as

$$S_p(t) = \frac{1}{N_1}\sum_{n=0}^{N_1-1}\left|H_p(t,n).S(t,n) + \eta_p(t,n)\right|^2 \qquad (2)$$

where, $H_p(t,n)$ denotes the channel gain between PU and p^{th} SU, $S(t,n)$ denotes the PU signal and $\eta_p(t,n)$denotes the additive Gaussian noise with 0 mean and variance. Several spectrum sensing methods are reported in the literature such as detecting the energy parameters, the method of matched filtering process and the features using the cyclo-stationary concepts. Amidst, energy detecting method is a good candidate for local spectrum sensing because the LSS will not need any earlier datas or information's about the primary user signal and the computational overhead is low. Utilizing energy detection method, the received signal can be expressed into binary hypothesis testing, H0 and H1, given in (3) as

$$r_p(t) = \begin{cases} \eta_p(t) & H_0 \\ H_p(t)\cdot S(t) + \eta_p(t) & H_1 \end{cases} . \qquad (3)$$

Here, the parameter$r_p(t)$ represents the signal which is being sensed., represents the presence and the absence of the primary user signals. After the local spectrum is being sended, the decision of each SU is represented as binary value, 0 and 1, on the inexistence and existence of PU signal with the mathematical model given by

$$SV_p(t) = \begin{cases} 0 & H_0 \\ 1 & H_1 \end{cases} , \qquad (4)$$

where SV_p is the sensing value of the p^{th} SU. 0 and 1 shows the inactive and active of PU signal respectively. Every secondary user will report the end verdict to the central unit. Then, the FC is going to make a final verdict regarding the spectrum which is relying on all of the data's which are obtained by the SUs. Because of the presence of few of the fake or falsified user/s, the secondary user/s may or may not send the modified information to FC, which is finally going to affect the overall performance of the communication system's spectrum. SSDF attacks such as always yes and always no are considered. Under such attacks, MUs can report contaminated data to the FC. MUs will change the local sensing report and falsify the test outcome. For an instance, MUs sends H0 while its local decision is H1 represents the existence of PU signal. Let the q^th^ SSDF attacker reports low energy when its local decision is H1 with probability H0 and reports high energy value to FC system, when the decision at the local level is depicted by the parameter H0 with using the probabilistic feature using the $P_{1,q}$ parameter with the mathematical model given by eqn. (5) and (6) as

$$P_{d,q} = (1 - P_{0,q})P_{d,q} + (1 - P_{d,q})P_{1,q} \qquad (5)$$

$$P_{f,q} = (1 - P_{0,q})P_{f,q} + (1 - P_{f,q})P_{1,q} . \qquad (6)$$

To mitigate the SSDF attacks, features such as energy statistic, autocorrelation, squared mean, standard deviation and maximum-minimum eigen value and are computed and fed as inputs to the MLP. Energy statistic of the signal can be represented using (7) as

$$E = \sum_{k=0}^{N_1-1} |r(k)|^2 \,. \tag{7}$$

Autocorrelation is a mathematical function which could be used for encoding the level of the association between two parameters which are procured from the similar source, i.e., the same source (correlating between itself). Autocorrelation measures the similarity of a signal with a delayed version of itself. Honest SUs sends the actual report to the FC that may vary depending on the existence and inexistence of PU signal. But, MUs report either low or high energy repeatedly. Autocorrelation value does not oscillate much. Therefore, autocorrelation value of signal is considered as one of the feature vectors. Autocorrelation value of the signal is given using (8) as

$$A(i) = \frac{1}{N_1} \sum_{k=0}^{N_1-1} r(k).r(k-i) \,. \tag{8}$$

Squared mean of the received signal can be computed using (9) as

$$\mu = \frac{1}{N_1} \sum_{k=0}^{N_1-1} |r(k)|^2 \,. \tag{9}$$

Features are labelled as 0 for H0 and 1 for H1. MLP is a feed forward, supervised Artificial Neural Network (ANN). The neural net has got 3 important layers, viz., an input layer, a no. of layers which are hidden and finally one output layer. The input layer of the ANN is used for getting the input signal as external stimuli. The no. of parameters in the input later will decide the no. of feature vectors. Each middle layer (hidden) in between the input and output consists of one or more units or hidden neurons. Number of hidden layer and its units are determined by experimentation. Output represents the final decision, and this output layer has one neuron representing binary classification, shown in Figure 2.

The MLP output at the output layer can be calculated using (10)

$$y_k = f\left|\sum_{j,k=1}^{N} w'_{j,k}\left(\left(g\sum_{i,j=1}^{N} x_i w_{i,j} + b\right)\right)\right| , \tag{10}$$

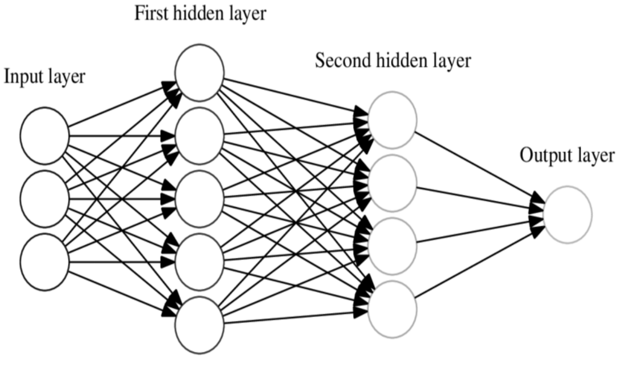

Figure 2. Multilayer perceptron with two hidden layers.

where x_i the i^th input vector, b is the bias and w_i denotes weight between the input and hidden zones (layer/s), the weight between the hidden and the output layer is denoted by w_j, finally the parameters g and f could be called as the function of activation, which are present at the hidden and output layer respectively. After labelling, feature vectors are categorized into two sets of data, i.e., the training ones and the testing ones, which are called as the training and testing information. The data which is used for training is employed to ensure the modelled ANN system recognizes data and test data used to check the ability of the model to predict new cases based on its training. Algorithm 3.1 explains the training procedure of MLP. Performance of the trained network is validated with the test data.

3.1. Algorithm: MLP training algorithm

- Create MLP network
- Initialize the weight and bias randomly
- Computer the feature vector $X = [x_1, x_2, x_3, \ldots, x_n]$
- Label the target vector $T = [0, 1]$, $0 = H_0$, $1 = H_1$
- For each training pair (X, T)
- Present input to the input layer.

Calculate the net output using (11)

$$h = \sum_{i,j=1}^{N} \left(x_i w_{i,j} + b\right) . \tag{11}$$

- Apply activation function to compute net input using (12)

$$h = g(h) \,. \tag{12}$$

- Calculate the net output at the output layer using (13)

$$y_k = \sum_{j,k=1}^{N} w'_{j,k=1} h \tag{13}$$

- Apply activation function to compute net outcome using (14)

$$y_k = f[y_k] \,. \tag{14}$$

- Calculate the error using (15)

$$Error = T - y \,. \tag{15}$$

- Back propagate the error and update weight and bias using (16) and (17)

$$w_{\text{new}} = w_{\text{old}} + \Delta w_{i,j} b_{\text{new}} = b_{\text{old}} + \Delta b_{i,j} \quad \text{(hidden layer)} \tag{16}$$

$$w_{\text{new}} = w_{\text{old}} + \Delta w_{j,k} b_{\text{new}} = b_{\text{old}} + \Delta b_{j,k} \quad \text{(output layer)} \tag{17}$$

- Test for stopping condition
- End.

4. SIMULATION RESULTS

Here, in the Section-IV, experimental outcomes are portrayed in order to prove the effectiveness of the mathematical model and the simulation is performed using MATLAB 2018a platform.

CRN is designed with one FC; one PU and 30 secondary users and pf will be set to 0.1 for all SUs. The percentage of MUs is ranged from 10 % to 60 %. The PU signal is a Quadrature Phase Shift Keying signal and outcomes are revealed using the simulations done using the Monte-Carlo methods with a step size of around 10000 runs. The signal to the noise ratio will be changed from a value of -20 dB up to zero decibels. with respect to this work, MLP is employed for mitigating negative impact of MUs in CRN. An input value to the MLP is composed of feature vectors obtained from the received signal. MLP is designed with 5 neurons representing 5 feature vectors, 2 layers which are hidden using 10 hidden neurons in every ANN layer and consisting of only 1 neuron in the output layer of the neural net and having only one neuron which corresponds to the output value 0 or 1 representing H_0 & H_1 hypothesis.

Tan sigmoid and linear activation function is used at the second and the third layer of the neural net (hidden/output). In this stage, the least means square (LMS) algorithm could be used to train the neural net by setting the epoch value up to 500 points. Efficacy of the developed model is ascertained or justified next. This is done with the help of probability detection and also using the help of probability of the False Alarm Rate parameter. The Figure 3 depicts the plot between the Signal-to-Noise Ratio (SNR) and the Probability of Detection (Pd) at the Probability of False Alarm *Pf* = 0.1. From the results of simulation, we can infer that considering Figure 3, the model which has been proposed by us give as an outstanding performance when compared to other methods taken for comparison. For an instance, *SNR* = - 12.5 dB, Pd performance of the proposed model is increased by 47.4 %, 46 % and 10 % as compared to Energy detection (ED), Generalized Likelihood Ratio Test (GLRT) and Hadamard Ratio (HR) sensing methods respectively.

The Figure 4 exhibits the probability of false alarm for always yes attack versus SNR considering a group of malicious secondary users (percentagewise). From the Figure 4, it is noticed that the proposed model can sense a yes attacking process correctly up to 50 % falsified secondary user/s in the presence for SNR varying from -10 dB to 0 dB. It proves that machine learning model can efficiently sense the SSDF attack launched by malicious SUs in CRN. Probability of false alarm for always no attack as a function of SNR for varying percentage of malicious SUs is graphically plotted in Figure 5. From the results, one can see apparently seeing the Figure 5 that model which is proposed by us is able to detect always no attack preciously up to 50 % malicious SUs presence for SNR varying from -10 dB to 0 dB. It further confirms that the proposed machine learning model can

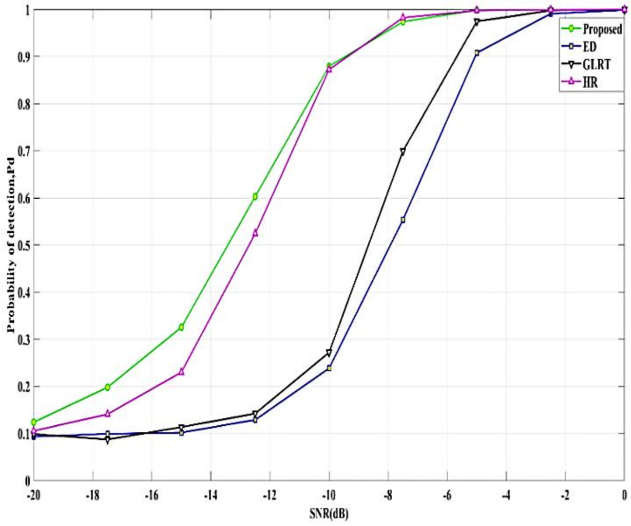

Figure 3. Probability of detection versus *SNR* at *Pf* = 0.1.

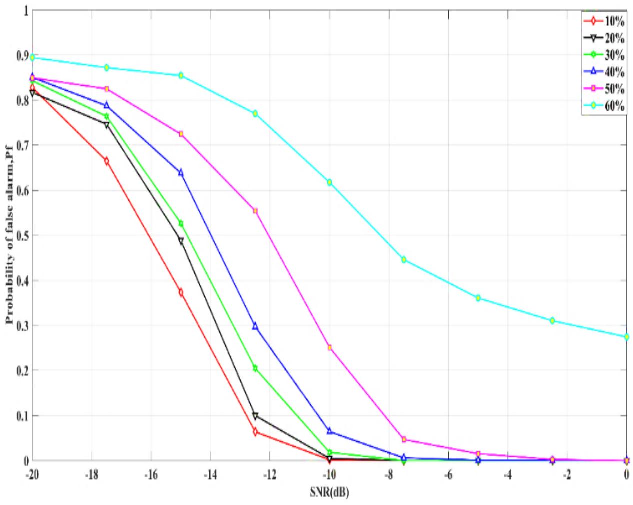

Figure 4. Probability of False Alarm versus *SNR* for varying falsified secondary users percentagewise (always a YES attacking phenomenon).

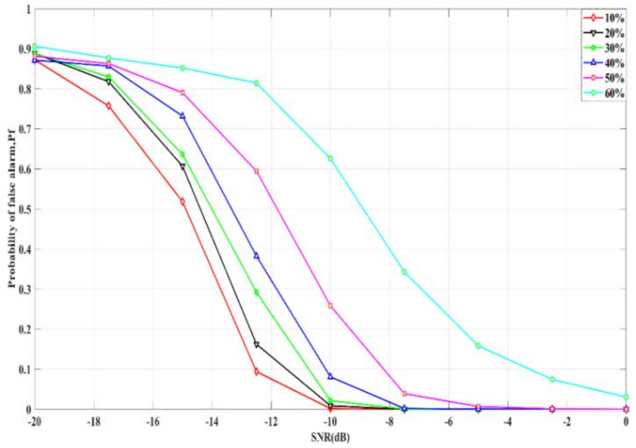

Figure 5. Probability of False Alarm versus *SNR* for varying percentage of falsified secondary user/s (always NO attacking phenomenon's).

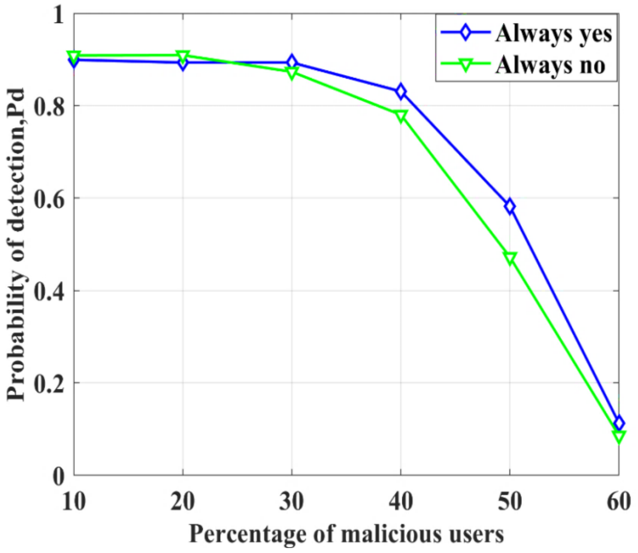

Figure 6. Probability of detection versus percentage of malicious users.

Table 1. Probability of Detection versus SNR.

Approaches vs. SNR	Proposed Technique	ED	GLRT	HR
SNR = - 20 dB	0.14	0.1	0.1	0.1
SNR = - 15 dB	0.32	0.1	0.12	0.23
SNR= - 12.5 dB	0.62	0.14	0.16	0.52
SNR = - 10 dB	0.88	0.25	0.28	0.87
SNR = - 4 dB	0.99	0.93	0.96	0.99
SNR = - 2 dB	0.99	0.98	0.99	0.99

efficiently detect the SSDF attack launched by malicious SUs in CRN.

In order to experimentally validate the performance characteristics of the model which is being proposed in this research article, a curve can be plotted between probability of detection and malicious users varying from 10 % to 60 % at SNR is -10 dB, as shown in the Figure 6, from where it can be revealed that the scheme which has been proposed by us yields more Pd value. From the empirical findings, it can be justified and enunciated that the ML dependent strategy could efficiently suppress the impact of MUs in the CRNs.

The efficacy of the proposed model can be observed using the concepts of probability detection and probability of false alarm rate. The proposed model provides outstanding performance when compared to other methods taken for comparison with respect to different values of SNR as shown in Table 1.

5. CONCLUSION

Performance of CRN is severely affected by malicious SUs. MUs may launch SSDF attack to mislead the global decision. This paper has presented a machine learning model using an MLP classifier to identify falsified data in CSS to prevent SSDF attack in CRN. Set of features are extracted from the received samples and labelled based on the inexistence and existence of Primary User. The obtained features used as input to the MLP model. The network is trained with the Levenberg-Marquart algorithm and then employed for eliminating the effect of attacks due to the SSDF process. Once the simulated results are observed, it can be revealed that the proposed model could efficiently reduce the impact of malicious users in CRN. However, it needs more time for training. In future work, meta heuristic algorithm will be explored to optimize the parameters of network and to further enhance detection performance.

ACKNOWLEDGEMENT

The authors acknowledge with thanks Dayananda Sagar College of Engineering, Bengaluru, JSS Academy of Technical Education, Bengaluru for all the support and encouragement given to me to take up this research work and publication.

REFERENCES

[1] A. Ahmadfard, Ali Jamshidi, Alireza Keshavarz-Haddad, Probabilistic spectrum sensing data falsification attack in cognitive radio networks, Signal Processing, 137, 2017, 1-9, ISSN 0165-1684.
DOI: 10.1016/j.sigpro.2017.01.033

[2] M. E. Ahmed, J. B. Song, Z. Han, Mitigating malicious attacks using Bayesian nonparametric clustering in collaborative cognitive radio networks, 2014 IEEE Global Communications Conference, Austin, TX, 999-1004.
DOI: 10.1109/GLOCOM.2014.7036939

[3] A. Ali, W. Hamouda, Advances on Spectrum Sensing for Cognitive Radio Networks: Theory and Applications, IEEE Communications Surveys & Tutorials, 19(2), 2017, 1277-1304.
DOI: 10.1109/COMST.2016.2631080

[4] S. Althunibat, M. Di Renzo, F. Granelli, Robust Algorithm against Spectrum Sensing Data Falsification Attack in Cognitive Radio Networks, IEEE 79th Vehicular Technology Conference (VTC Spring), Seoul, 2014, 1-5,
DOI: 10.1109/VTCSpring.2014.7023078

[5] Z. Cheng, T. Song; J. Zhang; J. Hu; Y. Hu; L. Shen; X. Li; J. Wu, Self-organizing map-based scheme against probabilistic SSDF attack in cognitive radio networks, 9th Int. Conf. on Wireless Comm. and Signal Processing (WCSP), Nanjing, 2017, 1-6.
DOI: 10.1109/WCSP.2017.8170994

[6] F. Farmani, M. Abbasi-Jannatabad, R. Berangi, Detection of SSDF Attack Using SVDD Algorithm in Cognitive Radio Networks, Third International Conference on Computational Intelligence, Communication Systems and Networks, Bali, 2011, 201-204.
DOI: 10.1109/CICSyN.2011.51

[7] Federal Communications Commission: ET Docket No 03-222, Notice of proposed rulemaking and order.

[8] Federal Communications Commission, Spectrum Policy Task Force. Rep. ET Docket no. 02-135. 2002. Online [Accessed 16 March 2022]
https://transition.fcc.gov/sptf/files/SEWGFinalReport_1.pdf

[9] J. Feng, M. Zhang, Y. Xiao, H. Yue, Securing Cooperative Spectrum Sensing Against Collusive SSDF Attack using XOR Distance Analysis in Cognitive Radio Networks, Sensors (Basel). 18(2), 2018, 370.
DOI: 10.3390/s18020370

[10] L. Li, C. Chigan, Fuzzy C-Means clustering based secure fusion strategy in collaborative spectrum sensing. In 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, 2014, 1355-1360.
DOI: 10.1109/ICC.2014.6883510

[11] S. Mapunya, M. Velempini, Design of Byzantine Attack Mitigation Scheme in Cognitive Radio Ad-hoc Networks, International Conf. on Intelligent and Innovative Comp. Apps. (ICONIC), PlaineMagnien, 2018, 1-4.
DOI: 10.1109/ICONIC.2018.8601087

[12] G. Nie, G. Ding, L. Zhang, Q. Wu, Byzantine Défense in Collaborative Spectrum Sensing via Bayesian Learning. IEEE Access 5, 2017, 20089-20098.
DOI: 10.1109/ACCESS.2017.2756992

[13] A. Sharifi, M. Mofarreh-Bonab, 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), 2018, 43-50.
DOI: 10.22060/eej.2017.12528.5094

[14] A. A. Sharifi, M. J. Musevi Niya, DefenseAgainst SSDF Attack in Cognitive Radio Networks: Attack-Aware Collaborative Spectrum Sensing Approach, IEEE Communications Letters, 20(1), 2016, 93-96,
DOI: 10.1109/LCOMM.2015.2499286

[15] Runze Wan, Naixue Xiong, Lixin Ding, Xing Zhou, Mitigation strategy against spectrum-sensing data falsification attack in cognitive radio sensor networks, International Journal of Distributed Sensor Networks, 15, 2019, 1550-1477.
DOI: 10.1177/1550147719870645

[16] Yang Li, Q. Peng, Achieving secure spectrum sensing in presence of malicious attacks utilizing unsupervised machine learning, MILCOM 2016 - IEEE Military Commn. Conf., Baltimore, MD, USA, 2016 174-179.
DOI: 10.1109/MILCOM.2016.7795321

[17] Imran Ahmed, Eulalia Balestrieri, Francesco Lamonaca, IoMT-based biomedical measurement systems for healthcare

monitoring: a review, Acta IMEKO, vol. 10, no.2, pp. 1-11, 2021. DOI: 10.21014/acta_imeko.v10i2.1080

[18] Armando Coccia, Federica Amitrano, Leandro Donisi, Giuseppe Cesarelli, Gaetano Pagano, Mario Cesarelli, Giovanni D'Addio, Design and validation of an e-textile-based wearable system for remote health monitoring, Acta IMEKO, vol.10, no.2, pp. 1-10, 2021.
DOI: 10.21014/acta_imeko.v10i2.912

[19] Amar Taggu, Ningrinla Marchang, Detecting Byzantine attacks in Cognitive Radio Networks: A two-layered approach using Hidden Markov Model and machine learning, Pervasive and Mobile Computing, V 77, 2021, ISSN1574-1192,
DOI: 10.1016/j.pmcj.2021.101461