Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 4-B, pp. 1369–1383
DOI : 10.47974/JIOS-1885

Optimizing spectrum sensing performance and prediction of trustworthy users by implementing machine learning algorithms in cognitive radio network

Umakanta Samantsinghar *
Department of Electronics & Telecommunication
Buxi Jagabandhu Bidyadhar Autonomous College
Bhubaneswar 751014
Odisha
India

Srinivas Sethi †
Ramesh Chandra Sahoo §
Department of Computer Scienece & Engineering
Indira Gandhi Institute of Technology
Talcher
Odisha
India

Dhruba Charan Panda ‡
Department of Electronics Science
Berhampur University
Berhampur 760007
Odisha
India

Abstract

With the quick advancement of wireless communication technologies and the rising demand for spectrum resources, integrating learning and reasoning capabilities into cognitive

* *ORCID-ID:* 0000-0003-0535-8143
† *ORCID-ID:* 0000-0002-5130-2768
§ *ORCID-ID:* 0000-0001-5623-8446
‡ *ORCID-ID:* 0000-0003-1414-3400

* *E-mail:* umakantss@rediffmail.com
† *E-mail:* srinivas_sethi@igitsarang.ac.in
§ *E-mail:* ramesh0986@gmail.com
‡ *E-mail:* dcpanda@gmail.com

radio networks (CRN) has become essential. This study explores the spectrum sensing capabilities of Secondary Users (SUs) within a CRN. Various supervised machine learning (ML) techniques, including Bayes Network, Naive Bayes, and Decision Tree, are employed to assess the performance of the Secondary Users in spectrum sensing. These algorithms are used in order to predict the trustworthiness of Secondary Users by considering sensing reputation values altogether. It is a topic of discussion, to identify the most effective ML algorithm that can guarantee the maximum level of system accuracy & efficiency. In this study, the open-source data mining tool WEKA is used to create a wide range of classification models for the evaluation of performance and correct prediction of trustworthy users. The best possible model accuracy is attained with the aid of Receiver Operating Characteristics (ROC) curves and cost-benefit analysis of three different classifiers. The evaluation of SUs' trustworthiness and spectrum sensing repute in CRN concludes that the Decision Tree classifier provides best performance which enables the system for correct classification among malevolent users, suspicious users, and honest users.

Subject Classification (2020): *68T05, 94A12, 68M10.*

Keywords: *Machine learning algorithms, Trustworthiness, Accuracy, Sensing reputation, ROC curves.*

1. Introduction

As wireless communication technology progresses, the need for spectral resources by countless wireless applications and services has increased tremendously. Due to the limited availability of frequency spectrum, a new methodology had to be found in order to address the dual issues of Primary Users' (PUs) un-utilized licensed spectrum and the demand for more spectrum. The concept of Cognitive Radio Network (CRN) was first investigated by Joseph Mitola, which increases optimum use of radio spectrum and reduces the issue of spectrum scarcity. By using quick resource allocation techniques and sophisticated spectrum sensing principles, the CRN helps to resolve the radio spectrum issue problem with Scarcity [1]. The CRN may be able to self-configure transmission and reception characteristics in response to environmental changes and the detection of available unutilized spectrum. To achieve this goal, it may be possible to increase the effectiveness of unused channels by correctly recognizing, assigning, and sensing them without interfering with the PU. There are essentially two types of spectrum sensing: cooperative and non-cooperative. The final report in cooperative spectrum sensing is prepared by combining all the individual user's report. Therefore, each SU is permitted to detect and evaluate the white spaces (unused space) in a CRN. A node located at central position is known as Fusion Centre (FC),

which collects the sensed data and starts decision-making process based on their historical sensing records.

The cooperative spectrum sensing approach eliminates false alarms, resolves multipath fading problems, and gives greater accuracy and dependable spectrum sensing reputation than non-cooperative spectrum sensing. When cooperative spectrum sensing is employed, spectrum sensing occurs on a regular basis. Each node must take part in the decision-making of other nodes in order to increase accuracy. In this process a trust factor of each node has major impact for the measurement of Sensing Reputation (SR) in CRN. It is usually advised to FC not to receive any report originating from untrusted nodes. Therefore, a Trust and Reputation Management (TRM) model has been introduced, which ensures accurate and authenticate data about the entry of new secondary user (SU) into the network. The TRM model continuously measures the previous and present characteristics of each & every node and modifies trust values accordingly. Thus, this model is very much helpful for the evaluation of trustworthy users in the network.

This study presents an innovative TRM model for cooperative spectrum sensing, leveraging Machine Learning (ML) algorithms to attain precise trust value predictions for individual SUs. Various classification models are employed within ML techniques to ensure a high level of accuracy in spectrum sensing performance.

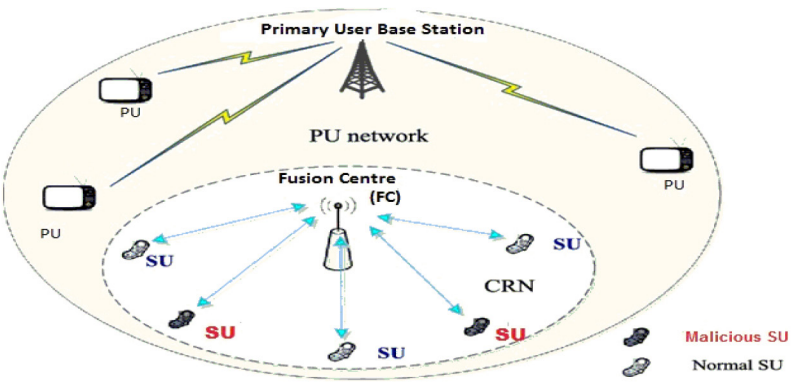

Figure 1

Architecture of Centralized Cognitive Radio Network

The study commences with an exploration of related work in Section II, followed by the system model in Section III. Section IV describes the proposed model, while Section V presents simulation results and observations. Section VI explains the Conclusion and future scope.

2. Related Works

When a new user enters into the existing SUs network registry, the Cognitive Base Station (CBS) initiates the trust management procedure. Each new entrant is given an initial sensing reputation value. The SU detects the unused channels and communicate their spectrum sensing report to the central node / Fusion Centre explained by author Meghanathan [2]. Notably, the Base Station consistently monitors the actions of each SU to update their reputation values based on sensing activities. The Central Base Station (CBS) then allocates available channels to SUs on a temporary basis in accordance with the Fusion Centre's decision [3].Top of Form Kavyashree and Nandini [5], discussed various models of the trust management scheme, including the reward system, in details. Based on the outcomes of trust assessment, Secondary Users (SUs) become eligible for either rewards or penalties. Rewards may involve granting preferences or prioritizing trustworthy SUs in decision-making processes. Conversely, penalties may include reducing the sensing reputation of suspicious or malicious users, leading to higher chances of exclusion from the Cognitive Radio Network (CRN) and lower access to unused network channels. Kar, Sethi, and Sahoo [4], proposed that Multi-Factor based Trust Management method offers a solution to minimize the Spectrum Sensing Data Falsification attack. This mechanism aids in assessing the trustworthiness of each Secondary User (SU) during cooperative spectrum sensing, demonstrating strong efficacy in decentralized Cognitive Radio Networks. Magdalene and Thulasimani [6], focused on fuzzy clustering approach which serves as the foundation for the free mitigation. Compared to previous approaches, fuzzy clustering means (FCM) are suggested as a way to reduce malicious user behaviour. Compared to the previous ways, the suggested methodology significantly increases the packet delivery ratio. Additionally, Khalunezhad, Moghim, and Ghahfarokhi, [7], introduced a novel trust management scheme specifically designed to counteract the Spectrum Sensing Data Falsification attack in a multi-hop collaborative spectrum sensing networks. The study by Sethi and Sahoo [8], emphasized the risk of interference with the Primary User (PU) spectrum in Cognitive Radio Networks (CRN) caused by deceitful

Secondary Users (SUs) trying to manipulate the spectrum access protocol. These dishonest actions have the potential to severely disrupt the regular functioning of the network. To tackle these challenges, the implementation of a Trust & Reputation Management system is regarded as essential to alleviate these risks in a connected context. With reference to Boutaba et al. [10], the author presented an innovative method employing the Least Mean Square (LMS) algorithm for collaborative spectrum sensing in CRNs. This algorithm promptly adjusts various weight factors, while the Fusion Center analyzes spectrum sensing reports from all Secondary Users (SUs). To enhance the accuracy in spectrum sensing process while minimizing computational time at the fusion center, Sadat and Abedi [9], introduced a Machine Learning approach using neural network technique. Khana et al.[11], introduced a block chain-based security system and spectrum sensing in CRN for enhancing system performance. The fake users in the CRN are identified using the block chain based approach and an adaptive threshold spectrum energy detection algorithm. Janu, Singh, and Kumar [12], suggested the CR technology and machine learning empower automatic learning and adaptation to the environment, offering the potential to dynamically access the spectrum and efficiently utilize spectrum resources. Author discussed [13], that using a trust mechanism to power CSS is insufficient. The feedback data from initiator SUs is typically left unchecked, which is a vulnerability for the trust system. In reference with Hossain and Miah [14], the author argued the significance of Machine Learning (ML) methodologies for network operation and management within future Cognitive Radio Networks (CRNs). However, the author overlooked the specific area where heightened accuracy could be attained. This led the implementation of Machine Learning (ML) techniques within this paper to enhance the precision of sensing reputation and prediction of trustworthiness of users at the Fusion Centre within CRNs.

3. System Model

A detailed explanation is provided for a proposed model that employs Machine Learning (ML) techniques to accurately classify cognitive users based on their trustworthiness and individual sensing reputation [15].

3.1 *Machine Learning Approach*

This paper applies machine learning techniques to improve system performance and accuracy while detecting underutilized spectrums owned by Primary Users (PUs). To achieve this, two distinct datasets—a training set and a validation set—are employed within the framework of machine learning techniques.

i) The training dataset is utilized to educate algorithm or machine, enabling it to grasp and apply concepts effectively to generate results in accordance with varying environmental conditions.

ii) The validation dataset serves as a test dataset utilized to both train and validate an Artificial Intelligence (AI) system's decision-making process. It employs AI concepts to optimize and select the most effective model for solving a specified task. A supervised Artificial Intelligence undergoes training using training data. The validation dataset is then employed to assess the model's overall efficiency, considering all parameters in conjunction during the training process.

In Figure 2, each row is interpreted as the predicted output, while each column represents the actual output. True Positive (TP) denotes the accurate prediction of positive instances. Conversely, True Negative (TN) signifies accurately predicted negative values. Additionally, False Positive (FP) and False Negative (FN) refers to incorrect predictions of positive and negative instances, respectively. Hence, the depiction of accuracy is encapsulated in the confusion matrix [12], as outlined below.

		Positive (P)	**Negative (N)**
Predicted Value	P	True Positive (TP)	False Positive(FP)
	N	False Negative(FN)	True Negative(TN)

Figure 2

Confusion Matrix Table

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \tag{1}$$

Consequently, a True Positive Rate (TPR) quantifies the ratio of accurately predicted values to the total number of positive values. TPR, also known as recall or sensitivity. The expression for TPR is

$$TPR = \frac{TP}{TP+FN} \tag{2}$$

Conversely, the false positive rate (FPR), also termed as 1-specificity, and represents the ratio of incorrect predicted values to the total number of negative values, derived from confusion matrix table. i,e

$$FPR = \frac{FP}{FP+TN} \tag{3}$$

In machine learning, the precision rate is a measure of how often actual positive examples provide outputs that are precisely predicted.

$$Precision = \frac{TP}{TP+FP} \tag{4}$$

The F-measure enables an analysis of the trade-off between Recall and Precision by offering their average harmonics, ideally aiming for a value of 1.

$$F-measure = 2.\frac{Precision*Recall}{Precision+Recall} \tag{5}$$

$$Sensitivity\,[18] = Recall = \frac{TP}{TP+FN} \tag{6}$$

$$Specificity = \frac{TN}{FP+TN} \tag{7}$$

3.1.2 ROC Curve

A Receiver Operating Characteristics (ROC) chart is a Visualization technique, Organization and selection of classifiers based on their performances. ROC charts are two-dimensional charts, where the "X" axis indicates the FPR (1-specificity) and "Y" axis indicates the TPR (sensitivity).

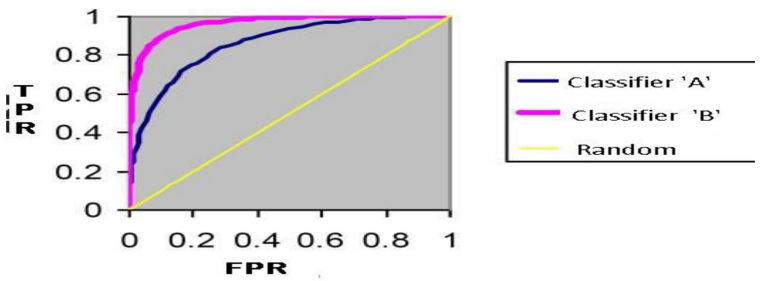

Figure 3

Sample ROC Curve

This graph shows the relative trade-offs between true positives rate and false positives rate [17]. Figure 3[17] shows a sample ROC curve representing two different classifiers (A & B).

Figure 3 shows two different ROC curves for classifier A & B, which are plotted between TPR (sensitivity) and FPR (1-specificity) for all possible threshold Values. That mean, each point on ROC curve indicates different threshold values and finally connected to form a curve. It begins in the lower left corner (0,0) and finishes at the upper right corner (1,1). As per the ROC principle, if that curve approaches more towards the upper left corner (0,1), then it treated as the best result as compared to others.

3.2 *Trust Computation*

It has been seen from the literature survey [4] that, the different methods have been proposed for the calculation of trust value of SUs. The network can be protected from the different kinds of attacks related to the trust values of SUs, they are referred as honest user, suspicious user and Malicious Users as reflected in Table-1.

Table 1

Trust Values

TYPE	TRUST LEVEL	USERS CATEGORY
A	0.9- 1	Honest
B	0.51- 0.89	Suspicious
C	0 - 0..5	Malicious

Finally, the Sensing Reputation (SR) of individual SU is evaluated [4] as per the expression mentioned bellow.

$$SR[u_n] = w1 * TF[u_n] + w2 * AF[u_n] + w3 * IF[u_n] + w4 * CF[u_n] \quad (8)$$

Where $w1$, $w2$, $w3$& $w4$ are the weight factors. *TF, AF*, *IF*& *CF* are considered as Trust Factor, Active Factor, Incentive Factor & Consistency Factor respectively.

Calculation of Sensing Reputation hinges on assessing the trustworthiness of SU. The trust level could be measured as follows:

$$TLS = \frac{Positive}{Positive + Negative} \quad (9)$$

4. Proposed Scheme

This section describes a suggested system which employs Machine Learning (ML) algorithms to enhance the accuracy for determining trustworthiness and evaluating the SUs reputation through spectrum sensing. This implementation facilitates the classification of SUs into distinct categories: malicious, suspicious and honest. This mathematical model outlined in paper [4], underwent simulation using MATLAB software, generating text-based data. Subsequently, validation took place utilizing the WEKA simulation tool [16], employing various ML algorithms known as Classification models/classifiers.

In this scenario, a Cognitive Radio Network (CRN) is composed of 5 Primary Users & 60 Secondary Users (SUs). Among the 60 SUs, 30 exhibit honest behavior while the remaining 30 shows malicious & suspicious behavior. The malicious users' behaviors are categorized into five distinct types, namely 'always yes,' 'always no,' 'opposite reporting,' 'hit and run,' and 'random reporting' [4], each category housing six malicious users. To compute Sensing Reputation, specific weight factors are assigned: w1 = 0.4, w2 = 0.2, w3 = 0.2, w4 = 0.2, correlated respectively with History-Based Trust, Active Trust, Incentive Trust, and Consistency Trust.

5. Simulation Result & Discussion

In this section, the presentation of simulated results and discussions are made across various dimensions. The findings underscore a noteworthy difference among the classifiers. Both the Decision Tree and Bayes Network classifiers achieved a perfect 100% accuracy in correctly classifying instances, indicating substantial precision. However, the Naïve Bayes classifier exhibited a slightly lower accuracy of 92% in correct classifications. Conversely, while the Decision Tree and Bayes Network showed a flawless 0% in incorrectly classified instances, but the Naïve Bayes classifier had a 7% error rate. This indicates a marked improvement in accuracy, specifically in assessing trustworthiness within this domain.

Table-2 contains the accurate validated data from three different classification models, which measures the accuracy of system performance basing on different parameters like TP Rate, FP rate Precision, Recall, F-measure, ROC and PRC. It is observed that in case of Decision Tree and Bayes Network ,the avg. weight value of all the mentioned parameters is '1' and the FP Rate is '0'. Similarly, in case of Naïve Bayes classifier the avg. weight for all the parameters is lying between 0.9 and 1, whereas, the FP

rate is 0.016. This means, the correctly predicted output is more and incorrectly predicted outputs is less.

Table 2
Accurate Data from Different Classifiers

TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	Class
NAÏVE BAYES						
0.936	0.079	0.688	0.936	0.793	0.993	Suspicious
0.765	0.014	0.956	0.765	0.85	0.995	Malicious
1	0	1	1	1	1	Honest
0.923	0.016	0.939	0.923	0.925	0.998	Avg. Weight
DECISION TREE						
1	0	1	1	1	1	Suspicious
1	0	1	1	1	1	Malicious
1	0	1	1	1	1	Honest
1	0	1	1	1	1	Avg. Weight
BAYES NETWORK						
1	0	1	1	1	1	Suspicious
1	0	1	1	1	1	Malicious
1	0	1	1	1	1	Honest
1	0	1	1	1	1	Avg. Weight
AVERAGE WEIGHT						
0.923	0.016	0.939	0.923	0.925	0.998	Naïve Bayes
1	0	1	1	1	1	Decision Tree
1	0	1	1	1	1	Bayes Network

5.1 *Results of Area under ROC Curve*

After simulation, the performance accuracy of the listed binary classification models is measured here through Receiver Operating Characteristic (ROC) curves and Area under Curve (AUC). From Fig 4, it has been seen from the ROC graph is at point (0,0) the TPR and FPR values are 0 but the threshold value is nearer to 1. When the curve flows towards upper left corner (1,0), basically it lies on the Y-axis where the TPR value increases but FPR value still remains 0 and threshold value also decreases. After that the curve flows towards upper right corner (1,1) where the TPR value remains 1 but FPR value increases gradually. It has been also

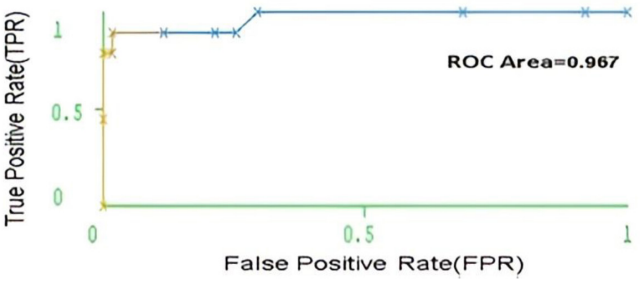

Figure 4

(ROC Curve of Bayes Network (Suspicious class)

observed from the ROC curve that, the Bayes Network model provides ROC area value 0.967 (nearly equal to 97%), which is very close to 1.

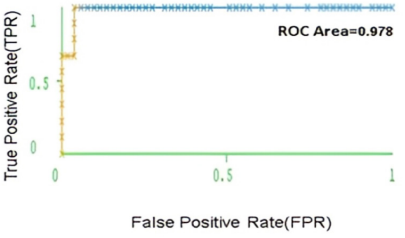

Figure 5

(ROC Curve of Bayes Net. (Malicious)

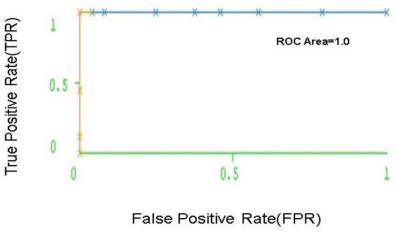

Figure 6

ROC Curve of Bayes Net. (Honest)

Fig 5 has been depicted that; the Bayes network Low class model achieved the ROC area (AUC) is 0.978 (98%), TPR is approaching to 100% and FPR is approaching to 0%. It has been observed from Fig 6 that, the Bayes network high class model achieved the ROC Area (AUC) is 1.0 (100%), True positive rate is equal to 100% and False positive rate is equal to 0%.

From Fig 7, It has been seen that the Naïve Bayes average class model has achieved the ROC Area (AUC) up to 0.9869 (98%), TPR value is nearly equal to 93% whereas, FPR value is nearly equal to 7%. From Fig 8, It has been seen that the Naïve Bayes low class model has achieved the ROC Area (AUC) is 0.9733 (97%), TPR & FPR values are nearly equal to 76% & 1.5% respectively. From Fig 9, It has been seen that the Naïve Bayes High class model has achieved the area under ROC (AUC) is 1.0 (100%), True

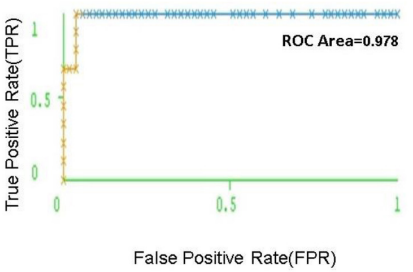

Figure 7

ROC Curve of Naïve Bayes (Suspicious)

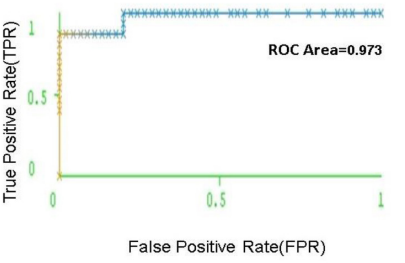

Figure 8

ROC Curve of Naïve Bayes (Malicious)

positive rate is nearly equal to 100% and False positive rate is nearly equal to 0%. Larger area has been covered by the ROC curve, so that the model has capability to provide best performance with higher accuracy. From Fig 10, It has been observed that, the Decision Tree average class model has achieved the ROC Area (AUC) is 0.9978 (99%), True positive rate is nearly equal to 100% and False positive rate is nearly equal to 0%. This model has come out with better performance with accuracy as compared to previous two average class models.

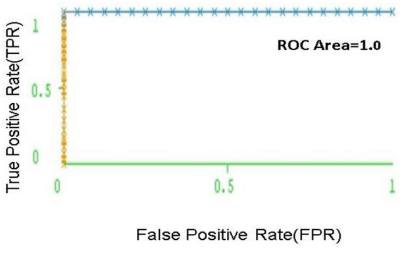

Figure 9

ROC Curve of Naïve Bayes (Honest)

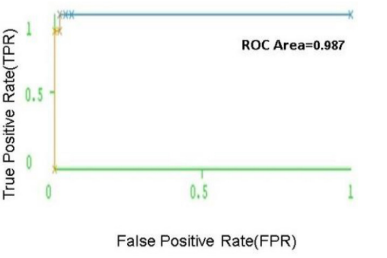

Figure 10

ROC Curve of Decision Tree(Suspicious)

From Fig 11, It has been seen that the Decision Tree low class model has achieved the ROC Area (AUC) is 0.9985 (~=100%), TPR value is nearly equal to 100% and FPR value is nearly equal to 0%. This model gave the better performance as compared to Naïve Bayes Low class model. From Fig 12 It has been observed that, the ROC curve has started from bottom left corner (0,0) and continued on the Y-axis till the upper left corner (1,0)

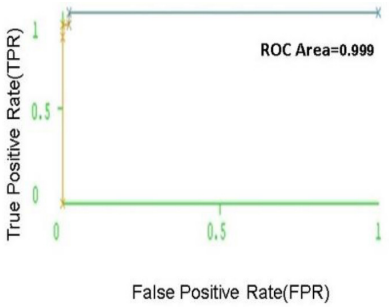

Figure 11

ROC Curve of Decision Tree (Malicious)

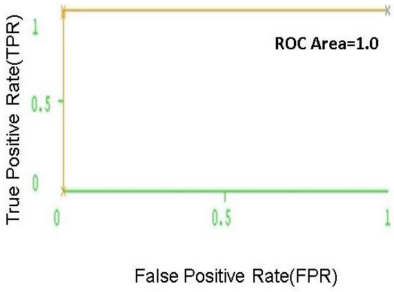

Figure 12

ROC Curve of Decision Tree(Honest)

where the TPR value is 1 and FPR value is 0. It means the Decision tree model has the highest True positive predicted outcomes and absolute zero false predictions with larger coverage area, which leads the higher accuracy.

6. Conclusion

A Trust-Reputation Management (TRM) scheme employing Machine Learning Algorithms significantly enhances the precision and efficiency of Models for optimizing sensing reputation and trustworthiness of each SU. Here MATLAB simulation generated extensive data, validated via the WEKA simulation Tool. Three distinct ML classifiers were introduced to analyse Model performance accuracy using ROC curves, Area under ROC, and cost-benefit factors. This approach aimed to mitigate interference caused by malicious and suspicious users in the spectrum sensing process of SUs. Ultimately, the Decision Tree (Random Forest) classifier exhibited superior performance compared to the other two classifiers. Its accuracy in identifying malicious and suspicious users significantly bolstered the trustworthiness of SUs, thereby enhancing CRN performance and efficiency.

References

[1] Joseph Mitola and Gerald Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18 (Aug. 1999).

[2] Natarajan Meghanathan, "A Survey on the Communication Protocols and Security in Cognitive Radio Networks," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 5, no. 1 (Apr. 2022), doi: 10.17762/ijcnis.v5i1.249.

[3] Ian F. Akyildiz, Brandon F. Lo, and Ravikumar Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, vol. 4, no. 1, pp. 40–62 (Mar. 2011).

[4] Swati Kar, Sudipta Sethi, and Rajkumar K. Sahoo, "A multi-factor trust management scheme for secure spectrum sensing in cognitive radio networks," *Wireless Personal Communications*, vol. 97, no. 2, pp. 2523–2540 (Jun. 2017), doi: 10.1007/s11277-017-4621-5.

[5] S. Kavyashree and B. M. Nandini, "Survey on trust management mechanism in CRN," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 5 (May 2017).

[6] A. Hyils Sharon Magdalene and L. Thulasimani, "Fuzzy clustering means (FCM) for mitigating spectrum sensing data falsification (SSDF) attack in cognitive radio networks," in *Proc. IEEE*, pp. 1–4 (Dec. 2017).

[7] Amir Khalunezhad, Narges Moghim, and Behrouz Shahgholi Ghahfarokhi, "Trust-based multi-hop cooperative spectrum sensing in cognitive radio networks," *Journal of Information Security and Applications*, vol. 42, pp. 29–35 (Aug. 2018).

[8] Swati Kar, Sudipta Sethi, and Rajkumar K. Sahoo, "A trust-based technique for secure spectrum access in cognitive radio networks," in *Progress in Computing, Analytics and Networking*, Springer, pp. 9–18 (2018).

[9] Zahra Sadat and Omid Abedi, "Detection of malicious node in centralized cognitive radio networks based on MLP neural network," in *Lecture Notes in Electrical Engineering*, pp. 865–877 (Jul. 2018).

[10] Raouf Boutaba, Mohammad A. Salahuddin, Noura Limam, Satyajayant Misra, Narayankumar Shahriar, Faiza Estrada-Solano, and Oscar M. Caicedo, "A comprehensive survey on machine learning for networking: Evolution, applications and research opportunities," *Journal of Internet Services and Applications*, vol. 9, no. 1 (Jun. 2018).

[11] Amit Khanna, Priyanka Rani, Tariq H. Sheikh, Deepak Gupta, Vishal Kansal, and Joel J. P. C. Rodrigues, "Blockchain-based security en-

hancement and spectrum sensing in cognitive radio network," *Wireless Personal Communications*, vol. 127, no. 3, pp. 1899–1921 (Jul. 2021).

[12] Dinesh Janu, Kamal Singh, and Sandeep Kumar, "Machine learning for cooperative spectrum sensing and sharing: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 1 (Sep. 2021).

[13] Jing Feng, Shuping Li, Shaoqing Lv, Honggang Wang, and Ai-Chun Fu, "Securing cooperative spectrum sensing against collusive false feedback attack in cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8276–8287 (May 2018).

[14] Md. Shahadat Hossain and Md. Shahin Miah, "Machine learning-based malicious user detection for reliable cooperative radio spectrum sensing in cognitive radio–Internet of Things," *Machine Learning with Applications*, vol. 5, p. 100052 (Sep. 2021).

[15] Yahia Arjoune and Naima Kaabouch, "A comprehensive survey on spectrum sensing in cognitive radio networks: Recent advances, new challenges, and future research directions," *Sensors*, vol. 19, no. 1, p. 126 (Jan. 2019), doi: 10.3390/s19010126.

[16] Anil Kumar, Pradeep Thakur, Sanjay Pandit, and Gurvinder Singh, "Threshold selection and cooperation in fading environment of cognitive radio network: Consequences on spectrum sensing and throughput," *AEU – International Journal of Electronics and Communications*, vol. 117, p. 153101 (Apr. 2020).

[17] Matej Majnik and Zoran Bosnić, "ROC analysis of classifiers in machine learning: A survey," *Intelligent Data Analysis*, vol. 17, no. 3, pp. 531–558 (May 2013).

Received October, 2024