EURASIP Journal on Wireless Communications and Networking

REVIEW Open Access

A survey on cognitive radio network attack mitigation using machine learning and blockchain

I. Evelyn Ezhilarasi[1†], J. Christopher Clement[1*†] and Joseph M. Arul[2†]

†I. Evelyn Ezhilarasi, J. Christopher Clement and Joseph M. Arul are contributed equally to this work.

*Correspondence: christopher.clement@vit.ac.in

[1] Department of Communication Engineering, School of Electronics Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India
[2] School of Computing and Information Sciences, Caritas Institute of Higher Education, Tseung Kwan O, New Territories, Hong Kong, China

Abstract

Cognitive radio network is a promising technology to enhance the spectrum utilization and to resolve the spectrum scarcity issues. But the malicious users play havoc with the network during spectrum sensing and demean the network performance. It is mandatory to identify such malicious attacks and address it. There have been many traditional methods to mitigate the cognitive radio network attacks. In this paper, we have surveyed advanced attack mitigation techniques like machine learning, deep learning and blockchain. Thus, by detecting and addressing the malicious activities, the throughput and overall network performance can be improved.

Keywords: Primary user emulation attack, Spectrum sensing data falsification attack, Jamming attack, Machine learning, Deep learning, Blockchain

1 Introduction

The opportunistic nature (as shown in Fig. 1) of using available spectrum has led to the invasion of various types of malicious attacks in cognitive radio network. Complete understanding of the attacker's intention and its repercussion is required to create a flawless secure cognitive framework. In [1], security parameters of 15 malicious threats of cognitive radio network have been reviewed. In [2], various types of cognitive radio network (CRN) attacks have been surveyed and the respective countermeasures of such attacks are tabulated in the study. Most of the researches [3] have surveyed on primary user emulation attack (PUEA) and spectrum sensing data falsification (SSDF) attack. In [4], the authors have studied several attacks in cognitive IoT.

In [5–8], the authors have given their related countermeasures along with the attacks. A survey on defending PUEA and SSDF attacks has been carried out in [9] and the defence mechanisms have been categorized into active (detecting the attacks immediately) and passive (detecting the attacks over a span of time). Various attacks that target the physical layer of the cognitive radio network have been analysed and its defence mechanisms have been analysed and compared in [10, 11]. One of the physical layer attacks is primary user emulation attack.

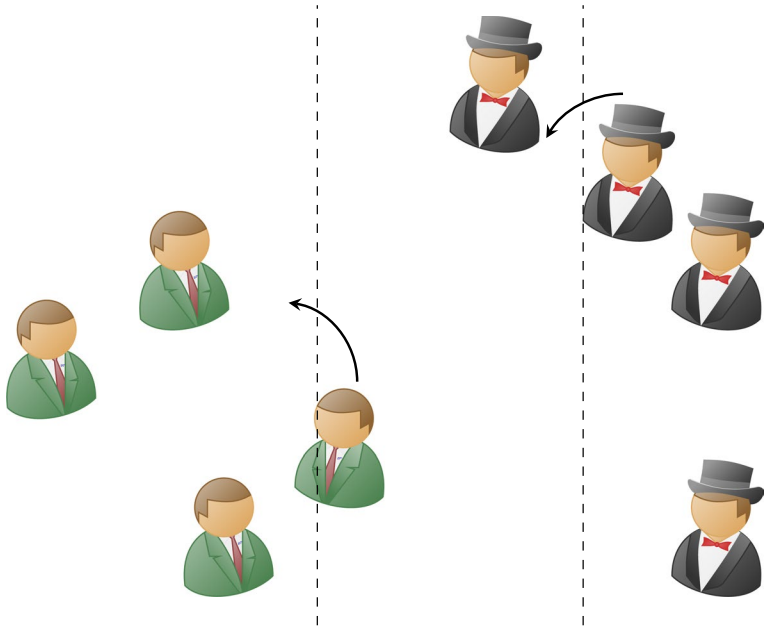

Fig. 1 SU leaves the channel, when the PU arrives. Figure portrays the opportunistic nature of cognitive radio network

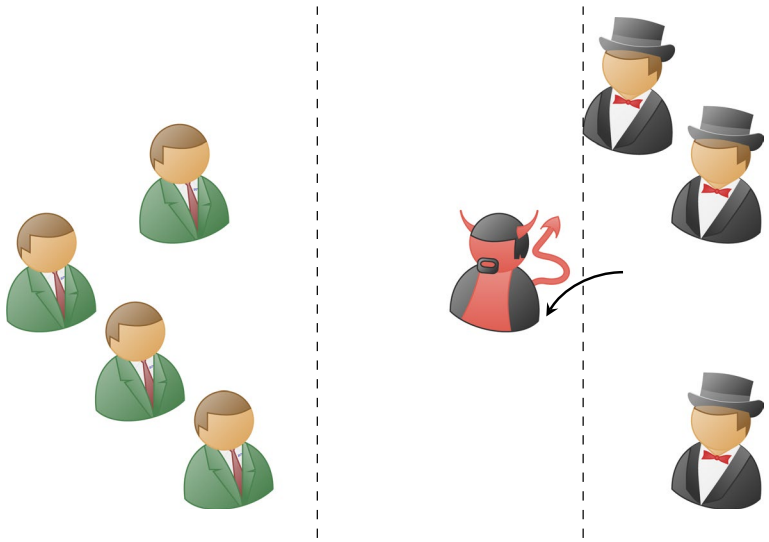

Fig. 2 Primary user emulation attack (PUEA). PUEA—malicious users acts like a primary user to hinder network performance

Primary user emulation attack (PUEA) is the counterfeit of the primary user signal to make the cognitive users believe that the spectrum is not vacant, so that the secondary users will not occupy the channel as shown in Fig. 2. The authors of [12] have shown the survey on PUEA countermeasures to combat the severe threat in spectrum sensing.

Spectrum sensing data falsification (SSDF) attack or Byzantine attack is the attack made by the malicious users by sending modified sensing results to the fusion centre,

to disrupt the proper decision produced by the fusion centre as shown in Fig. 3, thereby degrading the spectrum utilization and overall network performance.

In [13], mechanism of secure handoff is introduced to counter-attack cognitive user emulation attack (CUEA). In [14], the authors have reviewed various jamming attacks and their classification based on their functionality, and anti-jamming strategies using deep learning, reinforcement learning, game-theoretic learning, etc. The jamming attack is the attack where the malicious users select the nodes which are controlled by the malicious users.

These malicious attacks were mitigated using several conventional methods in the past. In [15], spectrum sensing methods and its recent advancement using the techniques of machine learning in the field of spectrum sensing and security against various attacks in the cognitive radio network are analysed. In this paper, the detection of malevolent nodes by machine learning techniques, deep learning techniques and blockchain technology is surveyed. In [16], the author has proposed machine learning-based defence methods to detect and prevent the attacks in the data link layer and network layer of cognitive radio networks. [17–19] present the application of blockchain in the management of spectrum sharing.

This paper is organized as follows:

Section 2 presents malicious user detection using machine learning algorithms. Section 3 presents malicious user detection using deep learning algorithms. Section 4 presents malicious user detection using blockchain.

2 Malicious user detection using machine learning algorithms

2.1 Support vector machine (SVM)

In [20], the authors have proposed a support vector machine (SVM) classifier, which classifies the malicious users and the authorized cognitive users. After segregating the users, the fusion centre collects all the local sensing reports from the authorized cognitive users using Dempster–Shafer evidence theory to make a global decision of the primary user activity. The attack which is considered in [20] is spectrum sensing data falsification (SSDF) attack. The region of convergence (ROC) curve in terms of

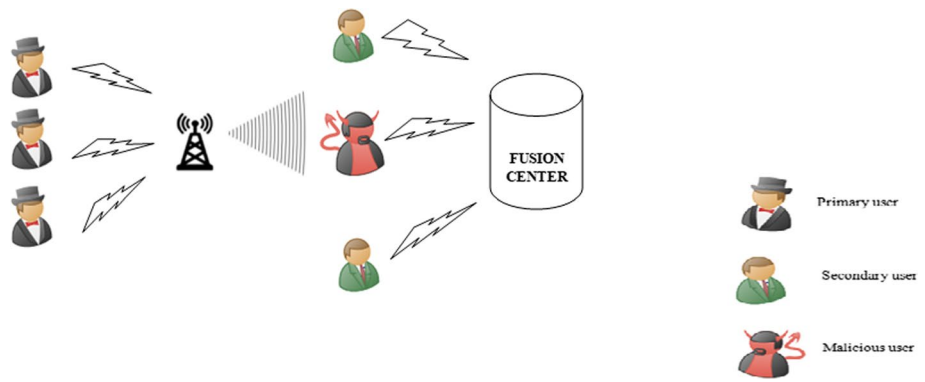

Fig. 3 Spectrum sensing data falsification (SSDF) attack. SSDF attack—malicious users sends modified sensing results to the fusion centre to disrupt proper decision produced by the fusion centre

false alarm and probability of detection, shows that the SVM classifier performs better than other classifiers.

Ernesto, Luis and Jorge [21] have employed SVM classifier to classify the malicious users, who try to mimic the primary user (primary user emulation attack) and the authorized primary users in mobile cognitive radio network. The model has been implemented on software-defined radio testbed with modulations like GMSK (Gaussian minimum shift keying) and orthogonal frequency division multiplexing (OFDM). Improved detection probability has been observed in low SNR compared to other traditional methods without threshold calculations.

Backoff manipulation attack (BMA), affecting the MAC layer, has been detected in cognitive radio network using SVM classifier with radial basis function (RBF) kernel in [22]. SVM classifier is trained using throughput and average transmission delay to distinguish the malicious nodes from the trust ones.

In [23], SVM classifier is used to identify the received signals modulation type based on its fractal dimension and to detect the primary user emulation attack (PUEA). When the SNR is > 10 dB, the PUE detection is 100% and when the SNR is -20 dB, the PUE detection probabilities are > 97%. Thus, the PUE attack is efficiently detected.

In [24], the authors have used the SVM classifier to detect and classify the malicious users in cognitive radio-based Internet of Things (CRIoT). The classification allows the fusion centre to make robust decisions only when the normal CRIoT users report it. With different datasets, classification achieves excellent accuracy with different kernels.

In [25], attacks have been detected using SVM classifier. This intrusion detection system creates an alert information, which is then sent to a probabilistic neural network for attack free opportunistic spectrum access. Throughput, system utility rate and packet delivery ratio have been enhanced, and there has been a drastic improvement in spectrum utilization as well.

2.2 K-nearest neighbour (KNN)

Mohammad and Kumaraswamy [26] have compared KNN and artificial neural network (ANN) in the detection of primary user emulation attack in cognitive radio network. They have used elliptical curve cryptography as data encryption for the security of the network. KNN achieves 98% detection accuracy as compared to ANN. Improved network performance in terms of throughput and security has been achieved using KNN classifier.

2.3 Analysis

The analysis of the performance in terms of classification capacity of both KNN and SVM classifier is shown in Fig. 4. Figure 4 shows that SVM outperforms KNN, as the classifier is not only linear, but it includes curvatures. Green line represents KNN classification, and black line denotes SVM classification. It is obvious from the given datasets, which overlap as shown in the figure, that it is impossible for a linear classifier to accurately distinguish them. But a linear classifier, like KNN fails in this case.

2.4 Ensemble

Ensemble learning is a useful method to obtain more accurate detection compared with the detection of individual classifiers. For the detection of spectrum sensing data falsification (SSDF) attack in cooperative spectrum sensing of cognitive radio networks, four machine learning techniques like SVM, neural network, ensemble and naive Bayes have been chosen in [27]. Training and testing has been conducted on (i) same dataset and (ii) different datasets. Under the same dataset, neural networks and ensemble learning perform better than the others. Under different datasets, ensemble learning outperforms the other methods. In [28], the authors have used boosted tree algorithm (BTA) with AdaBoost as an ensemble model, to mitigate SSDF attack in cooperative spectrum sensing environment. Results are compared with genetic algorithm soft decision fusion, particle swarm optimization soft decision fusion, count hard decision fusion models and maximum gain combination soft decision fusion schemes and found that BTA has achieved minimum error probability, reduced false alarm and high probability of detection. The authors of [29] have proposed an ensemble model with temporal convolutional recurrent neural network, reputation-based weighted majority vote algorithm, support vector machine (SVM) and logistic regression (LR) in a full-duplex cognitive radio network to resist the interference and malicious attackers. High accuracy, low time cost, low spectrum waste and collision probabilities are observed compared to single-model-based fusion methods and conventional majority vote rule-based fusion strategy. In [30], ensemble-based jamming behaviour detection and identification technique has been used to detect the jamming attack. The ensemble model is proposed with Bayesian classifier, K-nearest neighbour (KNN) classifier and random forest classifier. Results show efficiency in detection, accuracy and precision–recall rates with approximately '1.'

2.5 Decision tree

Machine learning (ML) models such as logistic regression, k-nearest neighbours, decision tree, Gaussian naive Bayes, support vector machine and linear discriminant analysis have been used for pattern recognition and the performance was evaluated with respect to recall, F-score, precision and accuracy. These ML models are trained and tested with the features extracted using a new technique called pattern-described link signature (PDLS) proposed in [31] to differentiate the authorized users and the malicious users to prevent from the PUEA (primary user emulation attack). The decision tree classifier showed better results, when trained with huge data.

In [32], a high accuracy degree is measured in calculating the trustworthiness and reputation of sensing in secondary users using machine learning techniques. Weka software has been used for data mining tasks. Accurate number of malicious users, suspicious users and honest users are identified. It is observed that Bayes network and decision tree perform better than naive Bayes in providing precise accuracy.

2.6 Logistic regression

In [33], the authors are concerned about malicious user detection in the energy harvested cognitive radio Internet of Things network. They have used energy detection methods for spectrum sensing and then classified the cognitive users and the malicious

users using three machine learning algorithms. Once the grouping has been done in the fusion centre, Dempster–Shafer (DS) theory is employed to make the global decision. Sensing gain, accuracy, network lifetime and sum rate are evaluated among SVM, K-nearest neighbour (KNN) and logistic regression. Logistic regression outperforms the other models.

In [34], PUEA has been detected and defended using logistic regression with MLE (maximum likelihood estimation) and gradient ascent. When compared with support vector machine and artificial neural network, the detection probability and false alarm probability are observed to be 99.5% and 0.6%.

In [35], different classifiers such as neural network, SVM, naive Bayes and logistic regression are compared based on the performance metrics for identifying malicious users. Logistic regression was proved to achieve 100% accuracy with the multifactor trust-based dataset. The trust dataset depends on the spectrum sensing results of every secondary user.

2.7 K-means clustering

To detect multiple attacks, viz. SSDF attack and jamming attack in cognitive radio network, improved k-means clustering algorithm is used in [37]. Promising results can be seen in secrecy rate, delay, signal-to-interference and noise ratio (SINR), probability of false alarm and packet delivery ratio.

Amar and Ningrinla [38] have proposed k-means++ clustering algorithm and RK-AES (improved version of advanced encryption scheme) encryption method to mitigate and detect the intelligent attackers that are responsible for smart primary user emulation attack (SPUEA). These attackers do not attack all the time but randomly, whenever the primary user is absent. Effective mitigation is done even when the attack is on the fly.

2.8 Binary clustering

The dynamic-collusive SSDF (DC-SSDF) attackers maintain high trust by dynamically submitting true sensing data and then fake sensing data in a collaborative way to increase the strength of their attack. Zhao, Li, Feng [39] have proposed a binary clustering algorithm-based (TFCA) trust fluctuation clustering analysis to combat the DC-SSDF attack in cooperative spectrum sensing. It improves the trust value calculation accuracy and reduces the DC-SSDF attack strength successfully.

2.9 Performance analysis: a comparison

2.9.1 Predicted value analysis

The performance analysis of the methods based on the algorithms decision tree, logistic regression, binary clustering and K-means is shown in Fig. 5. In Fig. 5, the actual value collected from confusion matrix is shown as a reference. When honest users are considered, the predicted values of decision tree, logistic regression, K-means and binary classifiers are matching with the actual value of the confusion matrix, whereas in case of malicious users, the predicted values of decision tree and logistic regression are conforming with the actual one, while K-means and binary classifiers perform inferior.

2.9.2 Receiver operating characteristic

In Fig. 6, the receiver operating characteristic curves of decision tree, K-means, logistic regression and binary clustering is shown. It is known that the shifting of curve towards upward left indicates an ideal performance. From this fact, it is known that decision tree outperforms all other algorithm and this is in conformance with previous discussion.

2.10 Fuzzy logic

Authorized eligible secondary users are selected based on three factors, like channel quality, SNR and trust factor to improve the performance of the network, using fuzzy logic-based data fusion scheme [40] . Malicious secondary users are identified and rejected in the decision making. The process is less time-consuming rather complex and best suited for real-time applications.

In [41], Neyman–Pearson criterion and machine learning-based adaptive neuro-fuzzy inference system have been proposed, which proves better overall network efficiency of 92% compared with artificial neural network (ANN), when subjected to four kinds of attacks, namely PUEA, SSDF, software-defined network attack and sinkhole attack.

In [42], a group of PUE attackers are investigated in cooperative spectrum sensing using fuzzy conditional entropy maximization. Results have shown that the scheme offers 17.54% and 39.39% higher probability of primary user detection in the presence of PUEA. Weighted fuzzy C means clustering is applied for detecting the (Denial of Service) DOS and replay attacks, while kernel cumulative sum model is applied for detecting the primary user emulation attack (PUEA) in [43], so as to improve the sensing of secondary users. Convergence improved bat optimization reduces the energy consumption, as it makes the power allocation process easier for secondary users. Fuzzy filter convolutional neural network is used for the optimal spectrum access. Results show the reduced rate of detection error of the attack and increased packet delivery ratio.

In [44], a fuzzy c-means-based semi-supervised algorithm is used to detect the SSDF attack. The secondary users can be divided into interactive and non-interactive users. The detection performance is illustrated in different conditions and the performance shows superiority among other algorithms.

2.11 Bayesian approach

In [45], the authors have proposed a new localization approach to detect the primary user emulation attack by combining the trilateration and RSSI (received signal strength indication) with Bayesian decision to involve the conditional risk while introducing the cost of decision. The position of the malicious users are estimated using trilateration-based RSSI, and the legitimacy of the primary user is evaluated using Bayesian decision approach.

Yuanhua and Zhiming [46] have proposed a trust model based on Bayesian interference-based sliding window and weighted trust calculation scheme during spectrum

sensing to locate and resist the SSDF attackers. Sigmoid log function is used to generate the trust value for every secondary user. Computational load of the model can be reduced by periodical evaluation. High detection accuracy is obtained for low attacking probabilities.

In [47], the authors have proposed a model to learn dynamic Bayesian network for orthogonal frequency division multiplexing (OFDM) modulated signals in CRIoT network. It detects the single/multiple affected OFDM subcarrier symbols attacked by jammers with high power or low power. Results show better performance compared with conventional methods.

In [48], jammer attack has been mitigated in multiple OFDM subcarriers using two single dynamic Bayesian network (DBN) and bank-parallel dynamic Bayesian network (DBN). Different M-QAM modulates the subcarriers, and optimum self-organizing map's (SOM) size is chosen for every QAM modulation based on detection probability of multiple attacks. Under multiple attacks, both the DBN exhibits almost similar performance.

In [45], received signal strength indication (RSSI) and trilateration techniques are combined along with the Bayesian decision theory to mitigate the primary user emulation attack. Results show that the PUEA detection zone is influenced by the decision making of security, balancing and productivity.

2.12 Random forest algorithm

In [51], the authors have proposed ProML algorithm (protection using machine learning), a random forest algorithm-based strategy to mitigate the random attacks on cognitive radio network channels. Jamming attack is the focussed attack to detect. The method is proved to be a promising solution for a larger network of more than 100 channels when compared with the traditional swapping methods.

2.13 Nearest centroid classifier

In [52], every secondary user evaluates its sensing report to existing sensing classes through the Levenshtein distance function. Depending on the quantitative variables, the prediction function of every sensing class is measured by the nearest centroid classifier. The sensing reports are classified based on the presence of the primary user. At the fusion centre, the predictive classes are integrated for the robust detection against PUEA and SSDF. It outperforms the conventional methods in terms of the metrics like sensing delay by 47%, throughput by 45% and prediction error by 46%.

2.14 Reinforcement learning

In [53], consensus fusion network and conventional collaborative sensing algorithms have been combined to increase the fusion network's convergence speed and to reduce the sensing time for detecting the malicious users, in order to improve the performance of spectrum sensing.

Monireh [54], in her dissertation, formulated online learning primary user emulation attack with two attacking strategies, AORO (Attack-OR-Observe) and ABOA (Attack-But-Observe-Another), where the attacker can dynamically choose a channel for attacking in each time slot, depending on its attacking experience.

In [55], reinforcement learning in clustering is used as an approach to achieve better network scalability. The effects of reinforcement learning (RL) parameters like discount factor and learning rate are analysed in a volatile cognitive radio, where some unauthorized users involve in launching attacks. To tackle such attacks, the cluster heads leverage on reinforcement learning model. From the results, it is understood that when the attack probability ranges from 0.3 to 0.7, the reinforcement model with learning rate '1' achieves high network scalability.

In [56], the thesis uses the multiarmed bandit problem and ProML machine learning design to analyse and mitigate the jamming attack in the cognitive radio network.

In [57], Markov decision process-based preventive approach is applied to detect the off-sensing DoS (denial of service) attack in cognitive radio network. Q-learning is used to learn the optimal policy. It improves the network throughput and performs better than the naive approach.

2.15 Extreme machine learning

In [58], PUEA detection and prevention are realized using extreme machine learning algorithm and time–distance with signal strength evaluation, which improve the energy efficiency, sensing ability, network performance and spectrum utilization and reduces the system delay in cognitive radio network.

Table 1 shows the reference study of possible types of attacks in CRN and their countermeasures using respective machine learning algorithms.

Table 2 depicts the performance comparison of machine learning models SVM, KNN, logistic regression, k-means and decision tree by analysing the parameters training time complexity, prediction time complexity, detection accuracy, false positive rate, precision and receiving operating characteristic.

3 Malicious user detection using deep learning algorithms

3.1 Neural network

In [63], the authors have proposed a neural network model to mitigate PUEA. The model has been designed using an input layer, 15 neurons with four hidden layers and an output layer. PUEA is formulated as a two-class classification problem to classify the signal into primary user and primary user emulation attack. The real-time signal classification is done with 97% accuracy, 2.5db gain with 100% detection probability.

In [64], secure hash algorithm and soft computing method (neural network) are integrated to detect the primary user emulation attack. The received signal strength and direction of arrival are used to localize the primary and secondary users.

In [65], cognitive user emulation attack is addressed for both centralized cognitive radio network and decentralized cognitive radio network. The attacker tries to block the authorized cognitive users from accessing the unused channels by imitating them during the spectrum handoff delay. The impact of cognitive user emulation attack (CUEA) in terms of delay, throughput and miss rate detection has been compared between ANN and traditional methods. ANN outperforms the traditional methods.

In [66], a multilayer neural network classifier with 2 hidden layers of 20 neurons each is proposed to detect the falsified reports in the cooperative spectrum sensing of CRN. The classification has used SNR ratio, distance between primary and secondary

Table 1 Machine learning reference work study

References	Type of attack	ML algorithm used
[20]	SSDF	SVM
[21]	PUEA	SVM
[22]	Backoff manipulation attack (BMA)	SVM
[23]	PUEA	SVM
[24]	SSDF	SVM
[25]	Malicious activity	SVM
[26]	PUEA	KNN
[27]	SSDF	Ensemble
[28]	SSDF	Ensemble
[29]	PUEA and SSDF	Ensemble
[30]	Jamming attack	Ensemble
[31]	PUEA	Decision tree
[32]	SSDF	Decision tree and Bayes network
[33]	Malicious users	LR, SVM, KNN
[34]	PUEA	Logistic regression with maximum likelihood estimation and gradient ascent
[35]	SSDF	Neural network
[36]	SSDF	K-medoids and mean shift clustering
[37]	SSDF and jamming attack	Improved K-means
[38]	PUEA	K-means ++ clustering
[39]	SSDF	Binary clustering
[40]	SSDF	Fuzzy logic
[41]	PUEA, SSDF, software-defined network attack, sinkhole attack	Neyman–Pearson criterion and adaptive neuro-fuzzy inference system
[42]	PUEA	Fuzzy conditional entropy maximization
[43]	PUEA, replay attack and DOS attack	Weighted fuzzy C means clustering cum kernel cumulative sum model
[44]	SSDF	fuzzy c-means-based semi-supervised algorithm
[45]	PUEA	Bayesian decision approach
[46]	SSDF	Bayesian interference-based sliding window and weighted trust calculation scheme
[47]	Jamming attack	Dynamic Bayesian network
[48]	Jamming attack	Two single dynamic Bayesian network (DBN) and bank-parallel dynamic Bayesian network (DBN)
[45]	PUEA	Bayesian decision theory
[49]	Learning-Evaluation-Beating attacks	adversarial machine learning
[50]	SSDF	Eclat algorithm
[51]	Jamming attack	ProML algorithm, a random forest algorithm-based strategy
[52]	PUEA and SSDF	Nearest centroid classifier
[53]	Malicious users	Reinforcement learning
[54]	PUEA	Reinforcement learning
[55]	Malicious users	Reinforcement learning
[56]	Jamming attack and other attacks	Reinforcement learning
[57]	Off-sensing attack	Reinforcement learning
[58]	PUEA	Extreme machine learning
[59]	Malicious user	particle swarm optimization and relevant vector machine (RVM) classifiers
[60]	SSDF	Improved apriori machine learning algorithm
[61]	PUEA	Linear regression algorithm
[62]	PUEA	Minimum covariance determinant

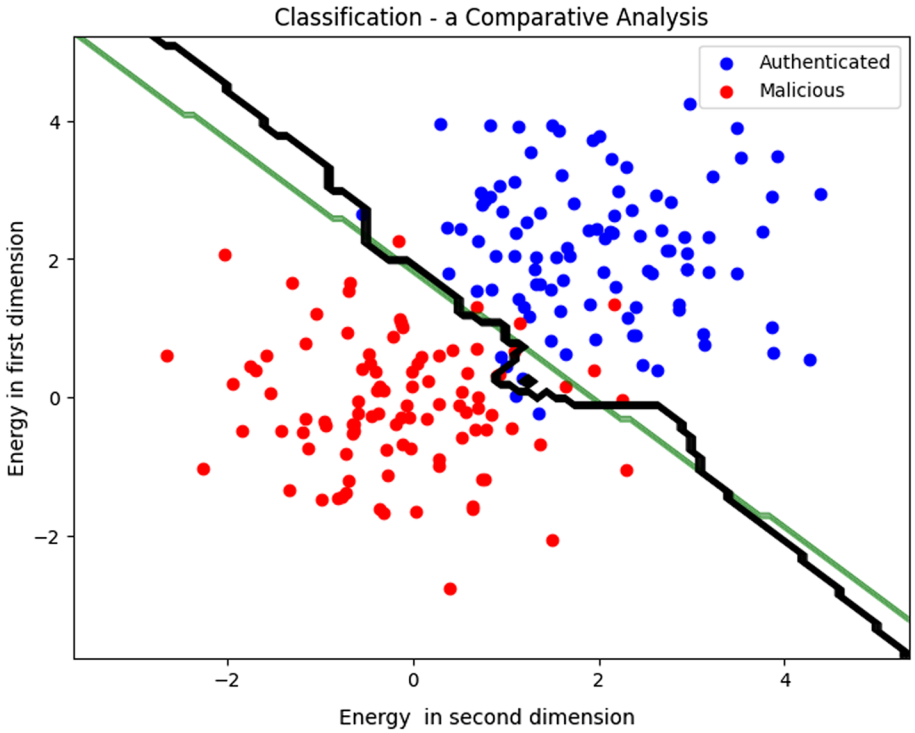

Fig. 4 Overall performance of classification—a comparative analysis. The analysis of the performance in terms of classification capacity of both KNN and SVM classifier is shown in the figure, where SVM outperforms KNN

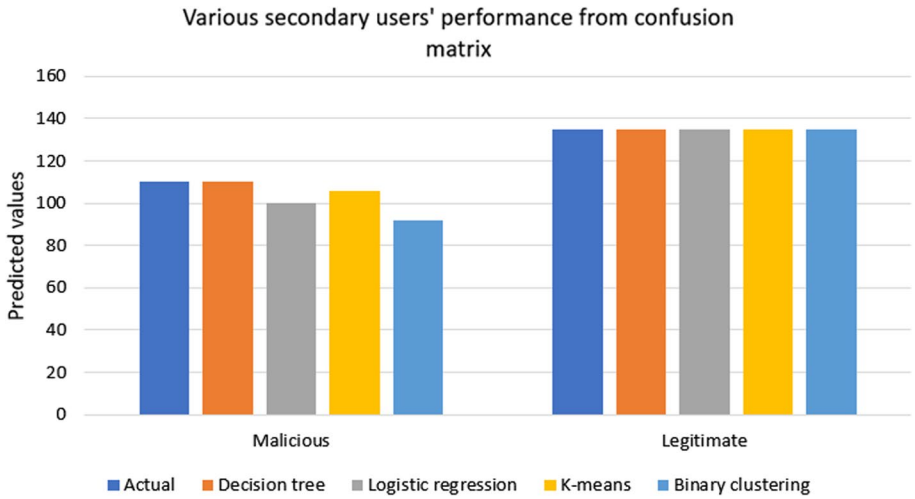

Fig. 5 Overall performance—a comparison. The performance analysis of the methods based on the algorithms decision tree, logistic regression, binary clustering and K-means is shown in figure

users and energy statistics of the received samples as the features. When compared with linear SVM, logistic regression and radial basis function (RBF) kernel SVM, accuracy of 98.5% is achieved with probability of detection as high as 90.4% and a probability of false alarm as low as 8%.

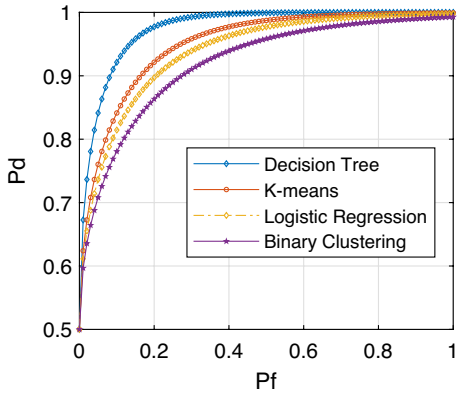

Fig. 6 Receiver operating characteristic curve. Receiver operating characteristic curves of decision tree, K-means, logistic regression and binary clustering are shown

Table 2 Performance comparison of ML models (n → number of training instances, k → number of clusters, I → number of iterations, d → number of features)

Parameters	SVM	KNN	Logistic regression	K-means	Decision tree
Training time complexity	O(n3)	O(1)	O(k*n*d)	O(k*n*d*I*t)	O(n*d*log(n))
Prediction time complexity	O(m*n)	O(n*d)	O(d)	O(k*d)	O(log(n))
Detection accuracy	Moderate to high	Require careful tuning and feature selection for good results	Limited in complex scenarios	Depends on K and the features quality	Vary
False positive rate	High when imbalanced data	Good at majority class and high for the minority class	Occur if the data are not well separated	Occur when the behaviour of normal user is classified as anomalous	Low when high risk of overfitting and high on unseen data
Precision	Low when imbalanced data	Low if noisy data	Low if data has overlapping patterns	Assessed based on the accuracy of identifying true positives	High when accurately separate classes and low if they overfit training data
Receiver operating characteristic	Deviate from ideal shape when imbalanced data	Do not produce traditional ROC	Achieves good when classes are well separated	Not directly applicable	Achieves good when classes are well separated

In [67], a multilayer perceptron-based neural network is used to defend the SSDF attack. The weights of the secondary users have been updated regularly and based on these trusted weights, the sensing results have been grouped in the fusion centre.

In [68], artificial neural network (ANN) is used as a classifier to detect the malicious users. Cyclostationary features have been extracted for every detected signal and are given to a neural network as training and testing data. The performance has been compared with energy detector-based classifier and naive Bayes-based classifier. Classification rate has been obtained as '1' approximately even at low transmission power.

3.2 Convolutional neural network (CNN)

To improve the primary user emulation attack (PUEA) detection accuracy, even when the attack signature changes inconsistently, the authors of [69] have used dual classification strategy (classification at the edge and core cognitive radio nodes) using deep learning convolution network (DLCN). The detection accuracy is compared with rule-based technique and feed-forward neural network. DLCN performs better than the compared ones.

The authors of [70] have proposed a one-dimensional convolutional neural network (1D-CNN) for detecting primary user emulation attack and jamming attack in cognitive radio network. 1D-CNN performs better than machine learning techniques in terms of receiver operating characteristics (ROC) and area under ROC.

In [71], PUE, SSDF and eavesdropper attacks are mitigated using signal strength-based location estimation (SSLE) scheme, convolutional neural network (CNN), hybrid advance encryption with Diffie–Hellman encryption (HAES-DHE) algorithm, respectively. Promising results have been obtained in detection probability, estimation of attack strength estimation, miss detection probability, honest nodes estimation and throughput.

3.3 Recurrent neural network (recurrent neural network (RNN))

The authors of [72] have proposed RNN model for detecting the cognitive user within primary user boundary and malicious user detection by ordering (MUDR) for differentiating the authorized and unauthorized users to avoid the illicit use of free white spectrum. It has been observed that the overall performance has increased by fast and precise detection.

The authors of [73] have proposed vertical federated learning-based cooperative sensing (VFL-CS) scheme using local RNN model to prevent the privacy threat at each secondary users, where local sensing results are available. It performs better than conventional soft-fusion-based cooperative sensing (SF-CS) scheme in terms of high area under curve.

3.4 Generative adversarial network (generative adversarial network (GAN))

In [75], spectrum anomaly is detected for cognitive mmWave radio network using deep learning generative models, such as auxiliary classifier generative adversarial network (AC-GAN), variational autoencoder (VAE) and conditional generative adversarial network (C-GAN). Real mmWave dataset has been used for evaluation. AC-GAN performs better than C-GAN and VAE with respect to accuracy and probability of detection.

In [76, 77], two models based on GAN have been designed- dumb GAN model without prior information of primary user and smart GAN model with prior information of the primary user to segregate the primary users and emulated primary users. Both the models detect the selfish and malicious primary user emulation attacker with more than 98% accuracy. Smart GAN model achieves better accuracy and faster saturation than the dumb model. In [77], also the pattern of long-term ON and OFF times of the primary user activities are learned using the ConvLSTM model, which gives 99.9% accuracy.

In [78], the authors have analysed two real-time applications, viz. high-dimensional data application and low-dimensional data application, using conditional generative

adversarial network (C-GAN) and dynamic Bayesian network (DBN), respectively, to detect the abnormal signals present in the cognitive radio network, thus developing a self-aware radio network.

In [79], the features are extracted from the Stockwell transform representation of the wideband spectrum and organized in a generalized state vector. Then the generative models are employed and learned to detect the malicious activity. Conditional GAN, auxiliary classifier GAN and deep VAE have been taken as generative models and compared.

3.5 Adaptive learning

In [81], the authors have used adaptive learning for detecting primary user emulation attack (PUEA) by analysing transmitter received power. The learning process adopts cyclostationary and distance feature-based analyses for differentiating authorized users from the malicious user and thus improved the throughput of the secondary user and detection probability by 16.31% and 9.67% and minimized the time of signal classification and misdetection by 48.53% and 18.3%, respectively.

3.6 Deep reinforcement learning

In [83], jamming activity mitigation and energy monitoring are done using multiobjective ant colony optimization model along with double Q-learning deep reinforcement model. The results are compared with genetic algorithm and artificial bee colony algorithm in terms of lifetime, throughput and malicious node mitigation [85].

In [84], the authors have designed double deep Q-network to confront the jamming attack in cognitive radio network. To maximize the successful transmission rate of users, deep reinforcement learning is used to learn the policy. Transformer encoder is used to implement the Q-network to analyse the spectrum data action values.

Table 3 shows the reference study of possible types of attacks in CRN and their countermeasures using respective machine learning algorithms.

3.7 Performance analysis of deep learning methods

The comparison of training loss curve of all deep learning models is shown in Fig. 7. Figure 7 shows that GAN outperforms other deep learning models that it converges with minimum loss within a few epochs, whereas other models take little longer epochs for the minimum loss convergence.

4 Malicious user detection using blockchain

Blockchain is a technology which works on peer-to-peer network, which we can also call it as distributed systems as shown in Fig. 8. But there are some major concerns in peer-to-peer network like security and trust. But blockchain, by using the concept of hashing and cryptography, overcomes such constraints.

The authors of [86] have used digital signature-based blockchain model during spectrum sensing to secure the cognitive radio network from the malicious users. Blockchain-based model is less complex than the existing models. Malicious users are distinguished 100% efficiently from the authorized ones and are blocked for further participation in spectrum sensing. The authors of [86] have considered attack

Table 3 Deep learning reference work study

References	Type of attack	DL algorithm used
[63]	PUEA	Neural network model
[64]	PUEA	Secure hash algorithm and soft computing method (neural network)
[65]	CUEA	ANN
[66]	SSDF	Neural network classifier
[67]	SSDF	Multilayer perceptron-based neural network
[68]	Malicious user	ANN
[69]	PUEA	Convolutional neural network
[70]	PUEA and jamming attack	One-dimensional convolutional neural network
[71]	PUEA, SSDF and eavesdropper attacks	Convolutional neural network (CNN), hybrid advance encryption with Diffie–Hellman encryption (HAES-DHE) algorithm
[72]	Malicious user	RNN
[73]	Malicious user	RNN
[74]	PUEA	LSTM
[75]	Spectrum anomaly	GAN
[76]	PUEA	GAN
[77]	PUEA	GAN
[78]	Abnormal signals in CRN	Conditional generative adversarial network (C-GAN) and dynamic Bayesian network (DBN)
[79]	Malicious user	GAN
[80]	PUEA and jamming attack	Sparse coding method
[81]	PUEA	Adaptive learning
[82]	Random jamming attack	Autoencoder
[83]	Jamming attack	Deep reinforcement learning
[84]	Jamming attack	Deep reinforcement learning

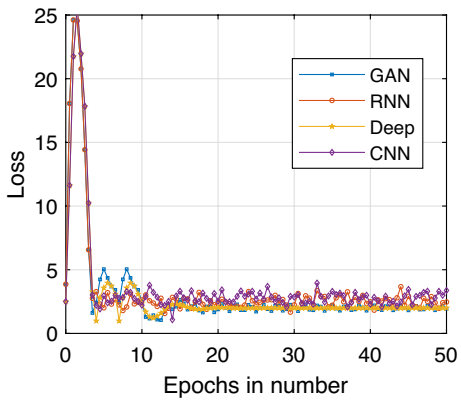

Fig. 7 Training loss verses number of epochs. GAN outperforms other deep learning models that it converges with minimum loss within a few epochs

of intruders to the smart sensors associated with the connected vehicles. They have proposed a blockchain-based framework for various security criteria, namely user's fake request and smart devices' compromise. Their results are analysed to have 70 % improvement in the success rate of identifying the intruders.

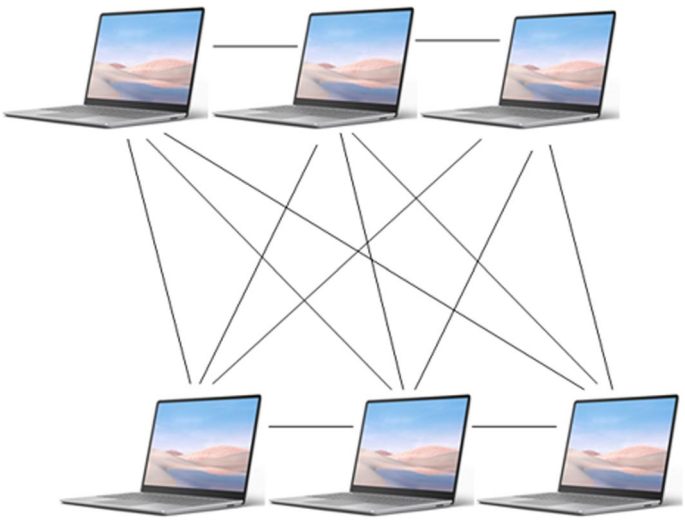

Fig. 8 Peer-to-peer distributed system. Different nodes involved in the peer-to-peer distributed system

Proactive blockchain-based spectrum sharing (ProBLeSS) protocol has been proposed in [87] to combat the SSDF attack in cognitive radio (CR)-based Internet of Battlefield Things (IoBT) networks. Compared to proactive learning-based MAC protocol (PROLEMus) [88], there is reduction in channel utilization, sensing delay and backoff rate of 2.74%, 5.5% and 8.3%, respectively.

In [89], Ying-Chang has discussed the blockchain technology for dynamic spectrum management and the challenges faced in applying blockchain to spectrum management. Malicious attacks have also been discussed to ensure security of the network.

The authors of [90] have proposed two-threshold-based voting (TTBV) algorithm to exclude the malicious helpers who wish to take part in spectrum sensing contract only to get the money, not to perform sensing. A running prototype of spectrum sensing has been developed on Ethereum blockchain, and the source code is shared on the public repository.

In order to avoid collusion attacks in cognitive radio network, Guowei Zhang [91] have used blockchain technology, which maintains the history of users' interaction as a public ledger and monitors the collusion attack of the users. It provides confidence for the secondary users to make a proper judgement. Blockchain-based cognitive sensing improves the sensing efficiency and the identification of the attack.

In [92], the authors have proposed a mobile edge computing-enabled spectrum blockchain for the Internet of spectrum devices, where the consensus mechanism is done in three stages for a secure spectrum sharing. Byzantine attack has been mitigated with high detection probability.

In [93], the authors have proposed a dynamic spectrum acquisition technique with smart contract-based permissioned blockchain to mitigate the double-spending attack and Byzantine attack for a wireless downlink communication system with multiple MVNOs (multiple mobile virtual network operators (MVNOs).

The authors of [94] have designed the multioperator spectrum sharing (MOSS) smart contract on the constructed permissioned blockchain for spectrum sharing and trading

among the multioperators and designed a mechanism to penalize the malicious operators. The privacy and openness are proved to be better than the traditional methods.

Careem [95] in his doctoral dissertation, leverage the distributed consensus mechanism applied with blockchain network to make accurate inferences even from the malicious agents. This leads to an autonomous and highly reliable spectrum enforcement approach, which outperforms the static crowdsourced enforcement strategies.

Blockchain-enabled cooperative spectrum sensing-based dynamic spectrum access has been proposed in [96], where data integrity and validity are guaranteed by the use of hashing and digital signatures of blockchain, so that the activity of the malicious users imitating the authorized users can be controlled. It also provides incentives for secondary users for their cooperation with tokens. Blockchain stores the sensing results which helps in spectrum monitoring and sharing.

Based on certificateless public key cryptography, a novel framework is proposed in [97] to protect the CSS from internal and external security threats in CR-IIoTs (cognitive radio-based Industrial Internet of Things). It performs better than state of the art in throughput, communication overhead and packet delivery ratio by 8.5%, 19.9% and 6.7%, respectively. It outperforms state of the art by 19.7% in data tampering attack, 13.4% in DDoS attack, 11.3% in on–off attack and 21.1% in SDF attack.

The authors of [98] have proposed a weighted fusion decision algorithm using the technology of blockchain. It produces reliable sensing output with less number of assistants and sampling rate, and resists the collusion attacks of the malicious users effectively, thus improving the accuracy and security of the cognitive radio networks.

Rajesh Babu and Amutha [99] have proposed a model, which performs three processes, viz. extreme learning machine (ELM) technique-based spectrum sensing, blockchain-based spectrum access and malicious user (MU) identification and blocking. It has obtained a maximum detection rate of 0.68 under SNR of -20dB, while the OR rule and KNN methods have attained a minimum detection rate of 0.5 and 0.58, respectively.

In [100], distributed consensus mechanism in blockchain technology has been applied to find whether the Byzantine malicious sensing attack has falsified the spectrum data in the Internet of spectrum devices. Effective robust prevention of SSDF attack is proved in the experimental results. In [101], during signal transmission between primary and secondary users, active and passive attacks occur, which can be mitigated by hybrid RSA (Riverest, Shaimer and Adleman) and HMAC (Hash Message Authentication Code) algorithms. The performance shows greater efficiency in throughput, encryption time, decryption time, energy consumption and packet delivery ratio compared to other algorithms.

5 Conclusion

In this survey, we have focussed on the detection of malicious users in cognitive radio network during spectrum sensing. Two major attacks that cause the CRN vulnerable are primary user emulation attack and SSDF attack. Three advanced mitigation strategies, viz. machine learning, deep learning and blockchain, have been discussed and reviewed.

Abbreviations

CRN	Cognitive radio network
PUEA	Primary user emulation attack
SSDF	Spectrum sensing data falsification attack
SVM	Support vector machine
ROC	Region of convergence
KNN	K-nearest neighbour
CNN	Convolutional neural network
RNN	Recurrent neural network
GAN	Generative adversarial network

Acknowledgements
We acknowledge and thank our institution for giving us the resources, opportunity and support to carry out the work successfully.

Author contributions
Author 1 has contributed in the design of the study of the literature survey and drafted the manuscript. Author 2 has contributed to the analysis, synthesis and simulations done in the survey. All authors read and approved the final manuscript.

Funding
The author did not receive support from any organization for the submitted work.

Availability of data and materials
Data sharing is not applicable to this article.

Declarations

Competing interests
The authors declare that there are no conflicts of interest.

Received: 13 April 2022 Accepted: 7 August 2023
Published online: 30 September 2023

References

1. N. Mishra, S. Srivastava, S.N. Sharan, in *2019 2nd international conference on intelligent communication and computational techniques (ICCT)* (IEEE, 2019), pp. 333–338
2. S.B. Sadkhan, D.M. Reda, in *2019 2nd International Conference on Engineering Technology and its Applications (IICETA)* (IEEE, 2019), pp. 117–122
3. I.A. Sohu, A.A. Rahimoon, A.A. Junejo, A.A. Sohu, S.H. Junejo, in *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)* (IEEE, 2019), pp. 1–4
4. G.K. Kurt, Ö. Cepheli, in *Towards Cognitive IoT Networks* (Springer, 2020), pp.101–123
5. S. Thangjam, N. Kumar, S. Kumar et al., in *IOP Conference Series: Materials Science and Engineering*, vol. 1033 (IOP Publishing, 2021), p. 012021
6. T. Singal, Int. J. Eng. Appl. Sci. Technol. (2020)
7. S.P. Chaturvedi, T. Singal, Int. J. Tech. Res. Sci. 92–99 (2020)
8. Y. Sudha, Int. J. Innov. Texhnol. Res. (2019)
9. S. Shrivastava, A. Rajesh, P. Bora, B. Chen, M. Dai, X. Lin, H. Wang, IET Commun. **15**(7), 875 (2021)
10. F. Salahdine, N. Kaabouch, Phys. Commun. **39**, 101001 (2020)
11. D.H. Tashman, W. Hamouda, IEEE Netw. (2020)
12. N. Mishra, S. Srivastava, S.N. Sharan, Wirel. Pers. Commun. **115**(1), 827 (2020)
13. G. Rathee, N. Jaglan, S. Garg, B.J. Choi, K.K.R. Choo, IEEE Trans. Cognit. Commun. Netw. **6**(3), 959 (2020)
14. M.A. Aref, S.K. Jayaweera, E. Yepez, IET Commun. **14**(18), 3110 (2020)
15. A.M. Joykutty, B. Baranidharan, in *2020 International Conference on Smart Electronics and Communication (ICOSEC)* (IEEE, 2020), pp. 878–884
16. Y. Sudha, Int. J. Innov. Technol. Res. (2020)
17. M.B. Weiss, K. Werbach, D.C. Sicker, C.E.C. Bastidas, IEEE Trans. Cognit. Commun. Netw. **5**(2), 193 (2019)
18. Z. Li, W. Wang, Q. Wu, in *International Conference on Blockchain and Trustworthy Systems* (Springer, 2020), pp. 575–587
19. S. Han, X. Zhu, in *2019 IEEE 19th International Conference on Communication Technology (ICCT)* (IEEE, 2019), pp. 936–940
20. M.S. Khan, L. Khan, N. Gul, M. Amir, J. Kim, S.M. Kim, Wireless Communications and Mobile Computing **2020** (2020)
21. E. Cadena Muñoz, L.F. Pedraza Martínez, J.E. Ortiz Triviño, Electronics **9**(8), 1282 (2020)
22. W.F. Fihri, H. El Ghazi, B. Abou El Majd, F. El Bouanani, IEEE Access **8**, 227349 (2020)
23. S. Fu, G. Zhang, L. Yang, Clust. Comput. **22**(2), 2667 (2019)
24. M.S. Hossain, M.S. Miah, Mach. Learn. Appl. 100052 (2021)
25. V. Sangeetha, A. Prakash, in *Materials Today: Proceedings* (2021)
26. M.A. Inamdar, H. Kumaraswamy, in *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184)* (IEEE, 2020), pp. 490–495

27. R. Sarmah, A. Taggu, N. Marchang, Wirel. Netw. **26**(8), 5939 (2020)
28. N. Gul, M.S. Khan, S.M. Kim, J. Kim, A. Elahi, Z. Khalil, Electronics **9**(6), 1038 (2020)
29. Y. Zhang, Q. Wu, M. Shikh-Bahaei, in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)* (IEEE, 2020), pp. 1–6
30. H.B. Salameh, S. Otoum, M. Aloqaily, R. Derbas, I. A. Ridhawi, Y. Jararweh, Ad Hoc Netw. **98**, 102035 (2020)
31. A. Albehadili, A. Ali, F. Jahan, A.Y. Javaid, J. Oluochy, V. Devabhaktuniz, in *2019 Wireless Telecommunications Symposium (WTS)* (IEEE, 2019), pp. 1–7
32. U. Samantsinghar, S. Sethi, D.C. Panda, R.K. Sahoo, in *2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)* (IEEE, 2020), pp. 1–6
33. M.S. Miah, M.A. Hossain, K.M. Ahmed, M. Rahman, A. Calhan, M. Cicioglu et al., (2021)
34. A.A. Ltd., *Detecting the Primary User Emulation Attack Using the Logistic Regression and MLE*. Ph.D. thesis (2018)
35. J.L.M. Tephillah. S International Journal of Future Generation Communication and Networking **14**(1), 426 (2021)
36. S. Zhang, Y. Wang, P. Wan, J. Zhuang, Y. Zhang, Y. Li, IEEE Access **8**, 5777 (2020)
37. N. Saini, N. Pandey, A.P. Singh, Int. J. Inf. Comput. Secur. **13**(1), 73 (2020)
38. A. Taggu, N. Marchang, in *2019 4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON)* (IEEE, 2019), pp. 1–5
39. F. Zhao, S. Li, J. Feng, Wirel. Commun. Mob. Comput. **2019** (2019)
40. A. Chakraborty, J.S. Banerjee, A. Chattopadhyay, J. Mech. Cont. Math. Sci. **15**(1), 39 (2020)
41. R. Neelaveni, B. Sridevi, Soft. Comput. **23**(18), 8389 (2019)
42. A. Banerjee, S.P. Maity, Trans. Emerg. Telecommun. Technol. **30**(5), e3567 (2019)
43. V. Sangeetha et al., Int. J. Modern Agric. **10**(2), 1270 (2021)
44. Z. Cheng, J. Zhang, T. Song, J. Hu, X. Bao, IEEE Trans. Cognit. Commun. Netw. **7**(2), 553 (2020)
45. W. Fassi Fihri, H. El Ghazi, B. Abou El Majd, F. El Bouanani, Int. J. Commun. Syst. **32**(15), e4026 (2019)
46. Y. Fu, Z. He, IEEE Syst. J. **14**(2), 1764 (2019)
47. M. Farrukh, A. Krayani, M. Baydoun, L. Marcenaro, Y. Gao, C.S. Regazzoni, in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (IEEE, 2019), pp. 380–385
48. A. Krayani, M. Farrukh, M. Baydoun, L. Marcenaro, Y. Gao, C.S. Regazzoni, in *2019 27th European Signal Processing Conference (EUSIPCO)* (IEEE, 2019), pp. 1–5
49. Z. Luo, S. Zhao, Z, Lu, J. Xu, Y. Sagduyu, IEEE Trans. Mobile Comput. (2020)
50. S. Vimal, L.Kalaivani, M. Kaliappan, A. Suresh, X.Z. Gao, R. Varatharajan, Neural Comput. Appl. **32**(1), 151 (2020)
51. T.T. Anh, N.C. Luong, Z. Xiong, D. Niyato, D.I. Kim, arXiv preprint arXiv:2001.03336 (2020)
52. D. Ganesh, T.P. Kumar, M.S. Kumar, IET Commun. (2021)
53. L. Jiang, X. Zhang, in *Journal of Physics: Conference Series*, vol. 1827 (IOP Publishing, 2021), p. 012008
54. M. Dabaghchian, *Security and Intelligence Measure in Online Machine Learning-Based Dynamic Spectrum Sharing Networks*. Ph.D. thesis (George Mason University, 2019)
55. M.H. Ling, K.L.A. Yau, in *2019 International conference on information networking (ICOIN)* (IEEE, 2019), pp. 296–300
56. S.S.M. Slehat, *Investigation of Security and Spectrum Management Issues in Cognitive Radio Aided by Machine Learning*. Ph.D. thesis (2020)
57. M. Hossain, J. Xie, in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications* (IEEE, 2019), pp. 613–621
58. N. Sureka, K. Gunaseelan, J. Ambient Intell. Humaniz. Comput. 1–10 (2021)
59. S.A. Balamurugan, S.S. kumar, Int. J. Commun. Syst. **33**(6), e4289 (2020)
60. A.H.S. Magdalene, L. Thulasimani, in *Artificial Intelligence Trends for Data Analytics Using Machine Learning and Deep Learning Approaches* (CRC Press, 2020), pp. 87–110
61. H. Yao, G. Zhu, Y. Yang, in *2021 8th International Conference on Automation and Logistics (ICAL)* (2021), pp. 49–53
62. B. Chhetry, N. Marchang, arXiv preprint arXiV:2106.10964 (2021)
63. V. Ponnusamy, K. Kottursamy, T. Karthick, M. Mukeshkrishnan, D. Malathi, T.A. Ahanger, Comput. Electr. Eng. **88**, 106849 (2020)
64. R.M. VasanthaReddy, S.C. Lingareddy, Int. J. Intell. Eng. Syst. (2020)
65. G. Rathee, N. Jaglan, S. Garg, B.J. Choi, D.N.K. Jayakody, IEEE Internet Things Mag. **3**(4), 20 (2020)
66. A.A. Ltd., *An Artificial Neural Network Approach for Detecting Spectrum Sensing Data Falsification Attacks*. Ph.D. thesis (2018)
67. Z.S.S. Marvasti, O. Abedi, *Fundamental Research in Electrical Engineering* (Springer, Berlin, 2019), pp.865–877
68. A. Toma, T. Nawaz, Y. Gao, L. Marcenaro, C.S. Regazzoni, IET Commun. **13**(10), 1336 (2019)
69. S. Srinivasan, K. Shivakumar, M. Mohammad, Int. J. Distrib. Sens. Netw. **15**(9), 1550147719860365 (2019)
70. M.A. Aygül, H.M. Furqan, M. Nazzal, H. Arslan, in *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)* (IEEE, 2020), pp. 1–5
71. N. Saini, N. Pandey, Int. J. Commun. Netw. Distrib. Syst. **22**(4), 385 (2019)
72. B. Varatharajan, B. Mariappan, Wireless personal communications
73. Y. Zhang, Q. Wu, M. Shikh-Bahaei, in *2020 IEEE Globecom Workshops (GC Wkshps* (IEEE, 2020), pp. 1–6
74. Q. Dong, Y. Chen, X. Li, K. Zeng, in *2018 IEEE International Smart Cities Conference (ISC2)* (IEEE, 2018), pp. 1-9
75. A. Toma, A. Krayani, L. Marcenaro, Y. Gao, C.S. Regazzoni, in *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications* (IEEE, 2020), pp. 1–7
76. D. Roy, T. Mukherjee, M. Chatterjee, E. Pasiliao, in *2019 IEEE Global Communications Conference (GLOBECOM)* (IEEE, 2019), pp. 1–6
77. D. Roy, *Machine Learning Based RF Transmitter Characterization in the Presence of Ddversaries*. Ph.D. thesis (University of Central Florida, 2020)
78. A. Toma, A. Krayani, M. Farrukh, H. Qi, L. Marcenaro, Y. Gao, C.S. Regazzoni, IEEE Trans. Cognit. Commun. Netw. **6**(1), 21 (2020)
79. A. Toma, *PHY-Layer Security in Cognitive Radio Networks Through Learning Deep Generative Models: An AI-Based Approach*. Ph.D. thesis (Queen Mary University of London, 2020)
80. H.M. Furqan, M.A. Aygul, M. Nazzal, H. Arslan, EURASIP J. Wireless Commun. Netw. **2020**(1), 1 (2019)

81. S. Arun, G. Umamaheswari, Circuits Syst. Signal Process. **39**(2), 1071 (2020)
82. K. Kottursamy et al, Wireless Personal Communications (2021)
83. S. Vimal, M. Khari, R.G. Crespo, L. Kalaivani, N. Dey, M. Kaliappan, Comput. Commun. **154**, 481 (2020)
84. J. Xu, H. Lou, W. Zhang, G. Sang, IEEE Access **8**, 202563 (2020)
85. J.C. Clement, K. Sriharipriya, P. Prakasam, et al., Multimedia Tools Appl. 1–23 (2023)
86. A. Sajid, B. Khalid, M. Ali, S. Mumtaz, U. Masud, F. Qamar, Future Gener. Comput. Syst. **108**, 816 (2020)
87. M. Patnaik, G. Prabhu, C. Rebeiro, V. Matyas, K. Veezhinathan, IEEE Netw. Lett. **2**(2), 67 (2020)
88. M. Patnaik, V. Kamakoti, V. Matyáš, V. Řchák, IEEE Trans. Cognit. Commun. Netw. **5**(2), 400 (2019)
89. Y.C. Liang, *Dynamic Spectrum Management* (Springer, Berlin, 2020), pp.121–146
90. S. Bayhan, A. Zubow, A. Wolisz, in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)* (IEEE, 2018), pp. 1–10
91. G. Zhang, in *Journal of Physics: Conference Series*, vol. 1578 (IOP Publishing, 2020), pp. 012–045
92. Y. Jian, D. Guoru, C. Xi, Z. Linyuan, S. Jiachen, Z. Hangsheng, in *Proceedings of the 12th EAI International Conference on Mobile Multimedia Communications* (2019)
93. M. Jiang, Y. Li, Q. Zhang, G. Zhang, J. Qin, IEEE Trans. Signal Process. **69**, 986 (2021)
94. S. Zheng, T. Han, Y. Jiang, X. Ge, IEEE Access **8**, 88547 (2020)
95. M.A.A. Careem, *Autonomous Spectrum Enforcement: A Blockchain Approach* (State University of New York at Albany, New York, 2019)
96. Y. Pei, S. Hu, F. Zhong, D. Niyato, Y.C. Liang, in *2019 IEEE Global Communications Conference (GLOBECOM)* (IEEE, 2019), pp. 1–6
97. G. Indra, S.K. Dhurandher, R. Raj, Int. J. Commun. Syst. **33**(18), e4582 (2020)
98. X. Xie, Z. Hu, M. Chen, Y. Zhao, Y. Bai, Electronics **10**(11), 1346 (2021)
99. C. Rajesh Babu, B. Amutha, Trans. Emerg. Telecommun. Technol. **33**, e4174 (2020)
100. Y. Jian, C. Xi, D. Guoru, Z. Hangsheng, J.S. Linyuan ZHANG, J. Commun. **41**(3), 1 (2020)
101. S. Srinivasan, K. ShivaKumar, M. Muazzam, J. Intell. Fuzzy Syst. **36**(5), 4449 (2019)

Publisher's Note