International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

AI Driven Security Threat Analysis for 5G Cognitive Radio Short Range Applications

Minilal M[1], Dr.Meena M*[2]

Submitted:18/03/2024 **Revised**: 29/04/2024 **Accepted**: 09/05/2024

Abstract: With 5G technologies, cognitive radio (CR) has become a possible answer to maximize spectrum utilization and efficiency. But in the case of short range application particularly, CR also brings significant security concerns in addition to benefits. Emphasizing short range use, this paper user 5G frame works to assess the security issue with cognitive radio systems. Among the discovered security hazards are primary user emulation attack, jamming attacks, SSDF attacks etc.; driven by reputation. Chaotic Deep Belief Networks (DBN) for detection and mitigation purpose is proposed to overcome these challenges using artificial intelligence (AI) approaches. Emphasizing the need of strong security measures to ensure the integrity and dependability of communication network, the analysis considers the unique characteristics of 5G –CR spectrum and short range applications .the result shows that the proposed chaotic DBN classification approach had accuracy ranging from 92.5 % to 94.2% in the testing set and an accuracy of 95.5% on the training set.

Keywords: *5G, Cognitive Radio, Short range application, Security analysis, Artificial intelligence, Chaotic deep belief networks*.

1. Introduction

As 5G technology is fast evolving and being used, the telecommunication industry is witnessing before unheard –of advances in data speed, network capacity and connectivity [1]-[2]. Cognitive radio which dynamically find empty radio areas to maximize spectrum use, in one of the major innovations around 5G.CR technology dramatically improves spectrum efficiency and communication dependability by allowing device to dynamically change their transmission parameters in real time and intelligibly discover available channels [3]-[4].

Even with all the benefits, including cognitive radios integration into 5G networks, certain security concerns arise. Short range applications including those present in IOT networks are especially vulnerable to numerous types of attacks because of their dense deployment and diverse structure [5]-[6]. Key security issues in CR systems are primary user emulation (PUE), jammer attack, and spectrum sensing and data falsification, reputation based attacks [7]-[8]. These threats damage data transmission integrity and confidence disrupt communication and affect network performance. Aiming for short range users, this work mostly addresses security issues in 5G Cognitive radio networks by means of detection and mitigation techniques [9]. Standard security measures are not enough for these environments since they cannot adapt to meet the dynamic and variable character of CR networks. Thus much needed are advanced security solutions able to quickly recognize and block hostile conduct in real time [10].

The objective of these researches is as follows:

1. To identify and investigate the security concerns specific to short range applications in 5G cognitive radio systems.
2. To use deep belief networks (DBNs) to build an artificial intelligence based detection systems spotting and reducing these security issues.
3. To evaluate the performance of the proposed DBN based approach about present security solutions.

This work introduces a new use of chaotic deep belief networks (DBNs) for security threat identification and mitigating in 5G cognitive radio networks. Since they can capture complex hierarchical representation of data unlike standard machine learning approaches. DBN are quite successful for anomaly identification in dynamic and heterogeneous environment. DBN can more specifically model and forecast nonlinear and unexpected patterns typical of network intrusion activities by means of Chaos theory.

This study makes contribution in:

1. Deals with the security threats particularly in short range applications in 5G Cognitive Radio Networks.
2. Depending on the chaotic deep belief networks, the development of a special artificial intelligence based security threat identification and mitigation strategy. This approaches increases robustness and detection accuracy by combining the strength of DBNs with chaos theory.

[1] *S.D.M.College of Eng. &Tech, Fort Collins – 8023, USA*
ORCID ID : 0000-3343-7165-777X
[2] *KLE.Institute of Technology, Tsukuba – 80309, JAPAN*
ORCID ID : 0000-3343-7165-777X
[3] *Computer Eng., Selcuk University, Konya – 42002, TURKEY*
ORCID ID : 0000-3343-7165-777X
** Corresponding Author Email: author@email.com*

Evaluation of the proposed method using a tailored dataset fit for 5G settings. Performance of the DBN based method with current techniques is compared against accuracy, detection rate, false positive rate, reaction time, run time and F-measure.

2. Related works

This work [11] investigates the possibility of cooperation between two transmitters in order to solve the security aware robust resource allocation in energy harvesting cognitive radio networks. This is done considering the value of the battery energy and the variations in channel gains. More precisely ,the main access point (AP) is the one that uses the time switching protocol to gather electricity from the renewable sources and then transfers it together with any data it has acquired to the secondary access point (SAP).In the process of doing so we address the question of how to maximize proportional fair energy efficiency (PEEE) while adhering to practical constraints ,all the while taking into considerations the fact that the channel gain and battery energy value are unknown. In addition to this it is considered that the eavesdroppers channel gain is unknown. We make advantage of the decentralized partially observable Markov decision process in order to find a solution to the resource allocation problem that is associated with it.

The MASRDDPG and RDPG approaches, which are multi-agent with single reward deterministic policy gradient, are employed in this process. When compared to these methodologies, contemporary approaches such as multi-agent and single agent DDPG are taken into considerations.Serving as virtual network functions (VNF) ,the module span a 5G network [12].while a cyber-threat –symptomizing (CTS)unit ,the DL module tracks network data utilizing the 5G network data analytic function (NWDAF).once it was determined the data was questionable .it was labelled as anomalous and attributed responsibility for end user service dissatisfaction and network bottleneck congestion.one might construct the DL security module for the most advanced proactive and adaptive cyber defence system (PACDS) by means of a logically ordered modular method.it has been made possible to improve the accuracy of outlier detection as well as response time ,and the complexity of the computation has been decreased. These improvements have been incorporated into the application over the course of its development.in addition to recommending an adaptive defence mechanism and describing its placement on a 5G network. Key performance indicators (KPI) have been suggested for the installation of security modules to protect intra slice and inter slice communication channels from both internal and external threats [13].These modules are intended to protect the communication channels between all of the slices. When it comes to the analysis of behaviour the CNN model distinguishes the best among the several deep learning models that were chosen. The botnet classification generated by the model has an accuracy of 99.74% and precision that is higher than that.

The spectrum of orthogonal frequency division multiplexing (OFDM) modulated transmission is used to capture sub band information, which is then used to build a generalized state vector (GS) with low dimensional in phase and quadrature components [14].effective control of state estimation and malicious attack capture is achieved with Markov jump particle filter. Studies on GS including more subcarrier followed later .Especially a deep learning method called variation auto encoders (VAE) transforms high dimensional radio signal into low dimensional latent space. Later on, the DBN is trained utilizing latent space information found in GS data by means of proposed method; one can detect anomalies resulting from cognitive devices or transmission jammers in a network subject to new transmission sources.

Based on deep learning, a fresh security architecture offered in [15] is aimed to control the specific risk given by 5G network and internet of things (IoT) channels. Our proposed method investigates network activity patterns both of which are vital for network security and detects any breaches in real time communications using deep neural networks. Deep learning can freely absorb complex information and pattern on its own, hence the proposed model can easily adapt to novel attack paths and traffic conditions .the method of machine learning makes this possible .the output of this work produced a hybrid model for the 5G communication intrusion detection. This approach uses an upgraded light weight CNNs design to mix Mobile Net V3-SVM with transfer Learning (TL).The proposed model learns from raw network data hierarchically by means of a framework comprising numerous layers. This enables one to sensibly separate good from negative behaviour. In resource limited environments, such those connected with the IoT and ultrafast 5G networks, we have used numerous creative ideas to raise the efficiency of intrusion detection. Using light weight Mobile network to manage network packets in real time while concurrently reducing the amount of processing overhead, the hybrid paradigm that has been shown fits very nicely for 5G edge devices and the IoT. The accuracy of the proposed model is improved through the utilisation of a mobile Net V3-SVM for the purpose of automatically classifying photographs of network intrusions. The experimental results demonstrate that the hybrid model that was developed is somewhat superior to the ones presently employed.

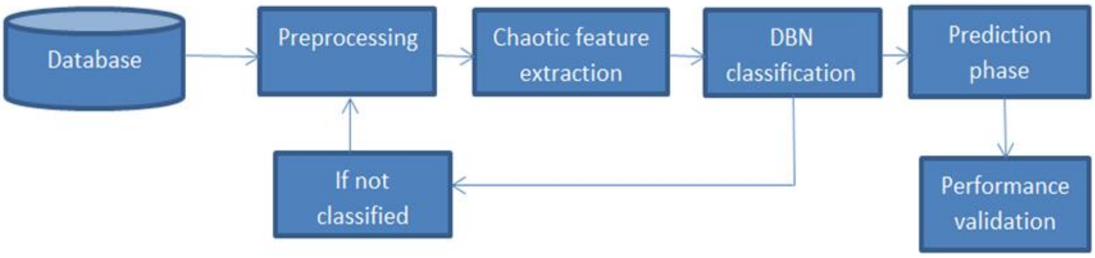


Fig 1: Proposed method

3. Proposed Method

We propose an artificial intelligence based solution using chaotic DBN to solve the security issues in 5G CR short range applications as in figure 1.using the chaotic mapping properties; this method increases the detection accuracy and resilience of the DBN in the dynamic 5G-CR environment. The approach is meant to find and minimize numerous security risks: primary user emulation attack, jamming attacks, SSDF attacks, Reputation based attacks.

Preprocessing: Preprocessing is the cornerstone of machine learning ,converting data into a usable form.in ensuring short range applications in 5G Cognitive radio using an AI based technology ,preprocessing consists data cleaning and normalizing to guarantee that the input to the DBN is both accurate and relevant.

- Data cleaning: Eliminating noise and irrelevant data from unprocessed data is the process known as data cleaning. This can cover outlier or erroneous value and filling in missing data. By employing the Z score method one can pinpoint data points that significantly deviates

$$z = \frac{(X-\mu)}{\sigma} \qquad (1)$$

Where

X- Data point

µ- mean of the data set

σ- standard deviation

Data points with |z| > 3 can be considered outliers and removed.

- Normalization : every feature equally supports the model usually [0,1] or [-1,1].the research adopts min-max normalization ,distinguished from others as:

$$X = \frac{[Xmax-Xmin]}{[X-Xmin]} \qquad (2)$$

X - is the original data point.

X_{min} and X_{max} - minimum and maximum values of the dataset.

X^1 – Normalized data point.

3.1 Pre-processing

Preprocessing is the cornerstone of machine learning ,converting data into a usable form.in ensuring short range applications in 5G Cognitive radio using an AI based technology ,preprocessing consists data cleaning and normalizing to guarantee that the input to the DBN is both accurate and relevant.

Data cleaning: Eliminating noise and irrelevant data from unprocessed data is the process known as data cleaning. This can cover outlier or erroneous value and filling in missing data. By employing the Z score method one can pinpoint data points that significantly deviates

$$z = \frac{(X-\mu)}{\sigma} \qquad (1)$$

Where

X- Data point

µ- mean of the data set σ- standard deviation

Data points with |z| > 3 can be considered outliers and removed.

- Normalization : every feature equally supports the model usually [0,1] or [-1,1].the research adopts min-max normalization ,distinguished from others as:

$$X = \frac{[Xmax-Xmin]}{[X-Xmin]} \qquad (2)$$

X - is the original data point

X_{min} and X_{max} - minimum and maximum values of the dataset

X^1 – Normalized data point.

3.2 Chaotic walk for feature extraction:

At its core feature extraction transforms raw data into higher value attributes for improved modeling.

Based on the innate uncertainity and complexity of chaotic systems ,chaotic walk based feature extraction turns input data into a feature space enhancing the distinction between normal and aberrant activity. This method is very useful for spotting network intrusions in a complex dataset including the SDN intrusion detection dataset,which include benign as well as several types of malicious traffic.often referred to as the butterfly effect ,chaos theory treats dynamically sensitive to initial condition dynamic systems.

For particular r values , the system exhibits chaotic behavior generally between 3.7 and 4.In feature extraction a chaotic walk is the repeated application of a chaotic map to produce a new feature space from the original data. This shift catches complex interactions and trends implying network invasions.

Let X={x_1,x_2,x_3……..x_{78}} be the set of 78 dataset quantitative features presented for every characteristics x_i is a chaotic walk transformation:

1. Initialize the chaotic map with random initial state xi,0 Є(0,1) and a control parameter rЄ[3.57, 4]
2. Apply the logistic map to each feature :
   Xi,n+1 = r $x_{i,n}$(1-$x_{i,n}$)
3. Generate the new feature set Y={y_1,y_2,…y_{78}} where each Y_i is the result of applying the chaotic map to X_i over n interactions.

   The research generates a sequence of pseudo random numbers using the chaotic map that subsequently weights the original properties ,hence enhancing their non linear interactions.

$$Yi,j = \sum_{K=1}^{N} Wk\, Xi,j\,(k) \qquad (3\,)$$

Where Wk –weights derived from the chaotic sequence and N is the number of interactions.

3.3 Deep Belief Network (DBN) Classification:

Deep belief networks are (DBN) are generative model consisting of multiple layered Restricted Boltzmann Machines(RBM).DBN handles feature learning ,dimensionality reduction and classification tasks.in network intrusion detection DBN may effectively learn hierarchical representation of input data ,hence improving the accuracy of classification of regular and atypical network activity.

The arrangement of the visible and hidden units assigns an energy defined by:

$$E(v,h) = -\sum_i \sum_j VihjWij - \sum_i bivi - \sum_j cjhj \qquad (4)$$

Where

Wij- weights between visible unit Vi and hidden unit hj

bi and cj biases of the visible and hidden units respectively.Each RBM is trained layer by layer using contrastive divergence.

$$P\,(h|v) = \pi jp(hj|v) \qquad (5)$$

Once pre – training is complete, entire DBN is fine-tuned using back propagation and gradient descent. This step adjusts the weights to minimize the classification error. For classification the DBN the learned features to predict the class of input data. The output layer which is typically a softmax layer provides the probabilities for each class. During the forward pass , the input data is propagated through each RBM layer. The activation for the hidden layer h_j is computed as

$$hj = \sigma(\sum_i ViWij + Cj \qquad (6)$$

Where σ is the sigmoid activation function. For the final classification, the output layer uses the softmax function:

$$p(y = k|x) = \sum_j exp(WjTh + bj)\exp\,(WkTh + bk) \qquad (7)$$

Where Wk and b_k are the weights and biases for the output layer.

4. Performance evaluations:

High performance computing cluster with 20 nodes, each equipped with Intel Xeon E5-26988 v4 Processors and 256 GB RAM is used for simulating the code of MATLAB R2021a.Python 3.8 is used for supplementary analysis. Tensor flow is for AI model implementation. The proposed method is compared with existing methods including MASRDDPG, DBN-MJPF and NWDAF-PACDS in terms of Accuracy: Detection Rate: False Positive Rate: Response Time: Run time and F measure: confusion matrix. The experimental setup is collectively provided in table 2.

Performance metrics:

- Accuracy: Measure of collectively identified threats.
- Detection rates: Proportion of actual threats correctly detected.
- False Positive Rate: Proportion of normal instances incorrectly identified as threats.
- Response time: time taken to detect and mitigate threats.

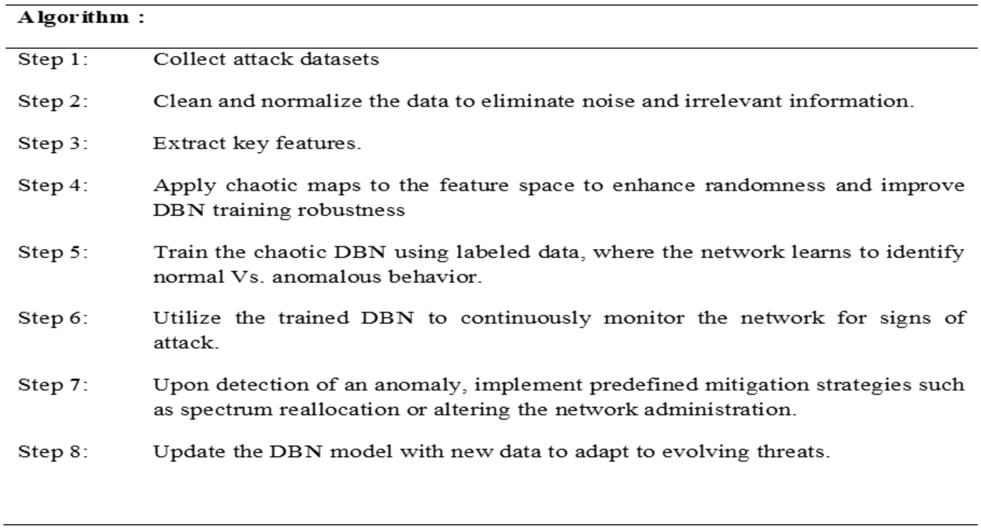
Dataset: DBN intrusion detection dataset includes labeled instances of normal and anomalous activities within a simulated 5G –CR environment. It contains various features relevant signal analysis and threat detection. The data contains 79 quantitative and qualitative features out of which one feature represents the qualitative attributes and 78 features represent the quantitative attribute.

The proposed DBN classification method demonstrates superior performance across all evaluation metrics compared to the existing methods(MASRDDPG,DBN-MJPF,NWDAF-PACDS).For the training data set the DBN classification achieved an accuracy of 95.5%,a detection rate of 95.0% and a false positive rate of 2.0%the response time was 28ms,and run time was 180 seconds with an f-measure of 0.950.the components of the confusion matrix consisted in 10800 true positives (TP),9000 true negatives (TN),350 false positives(FP) and 600 false negatives(FN). The NWDAF-PACDS method by contrast reported an F-measure of 0.935,a response time of 30ms,a run duration of 200 seconds ,a training accuracy of 94.2%,a detection rate of 93.5%,a false positive rate of 2.5% and so on. DBN-MJPF and MASRDDPG methods showed worse performance with regard to accuracy rates of 93.8% and 92.5% respectively. These results show how precisely and successfully the proposed DBN networks finds network leaks.

5. Discussion

The proposed work presents an examination of securing short range applications in 5G cognitive radio networks using an artificial intelligence based technique. Particularly with arrival of 5G technologies, the main focus is on addressing the security concerns related to cognitive radio systems.

Table 1: Proposed Algorithm



Algorithm :	
Step 1:	Collect attack datasets
Step 2:	Clean and normalize the data to eliminate noise and irrelevant information.
Step 3:	Extract key features.
Step 4:	Apply chaotic maps to the feature space to enhance randomness and improve DBN training robustness
Step 5:	Train the chaotic DBN using labeled data, where the network learns to identify normal Vs. anomalous behavior.
Step 6:	Utilize the trained DBN to continuously monitor the network for signs of attack.
Step 7:	Upon detection of an anomaly, implement predefined mitigation strategies such as spectrum reallocation or altering the network administration.
Step 8:	Update the DBN model with new data to adapt to evolving threats.

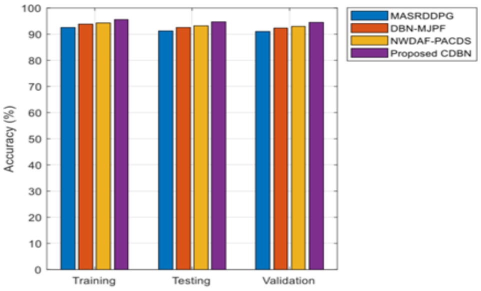


Figure 2: Accuracy(%)

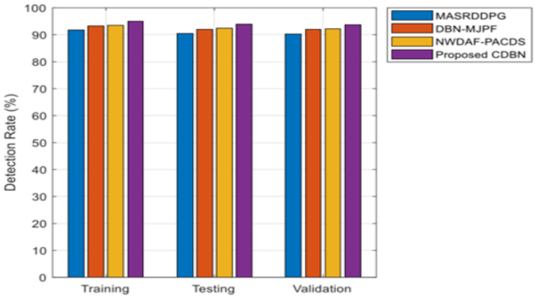


Figure 3: detection rate (%)

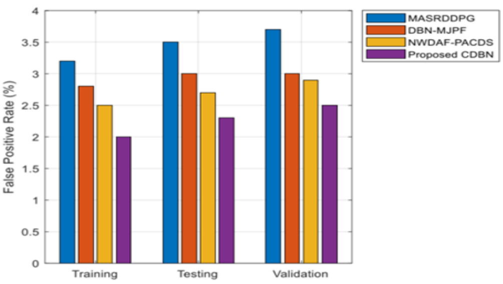


Figure 4: False Positive Rate(%)

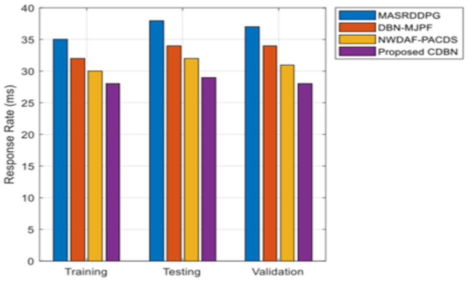


Figure 5: Response Time (ms)

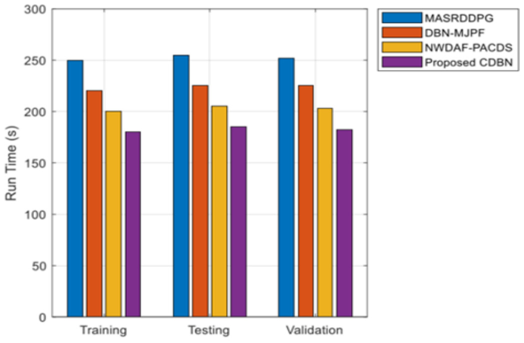


Figure 6: Run Time(s)

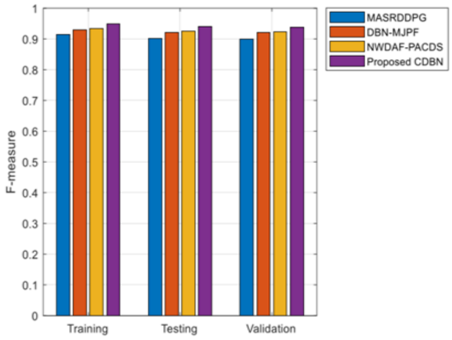
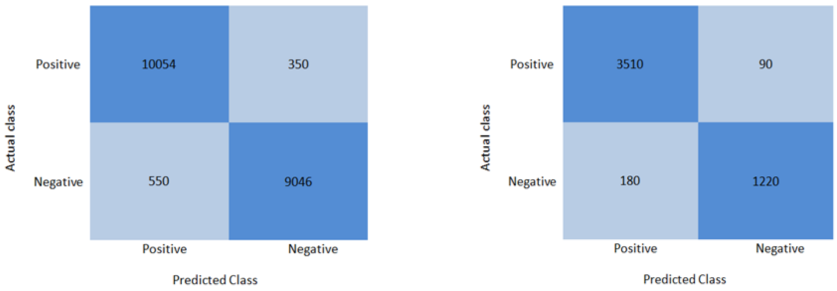


Figure 7: F-measure



(a) Training (b) Testing

Figure 8: Confusion matrix of proposed method

Table 2: Experimental set up

Parameter	Value
Simulation area	: 1000m X 1000m
Number of nodes	: 100
Spectrum bands	: 5(2.4Ghz, 3.5 GHz, etc.;)
Signal to noise ratio(SNR)	: 20dB
Transmission power	: 30dBm
Node mobility speed	: 5m/s
Attack type simulated	: 5 (PUE,jamming,etc)
Training data size	: 21,500 samples
Test data size	: 5000 samples
DBN layer	: 5
Neuron per layer	: 100
Chaotic Map Type	: Logistic map
Chaos control parameter	: 3.9
Mitigation strategy	: Dynamic spectrum allocation
Detection threshold	: 0.5
Evaluation period	: 60 seconds

DBN method with reaction time of 28ms and a runtime of 180seconds exhibits efficiency in both detection speed and

general processing time. The DBN classification method showed to be rather 10054 true positives. The method proved its dependability in spotting benign traffic by showing a high percentage of true negatives of 9046, which demonstrated its accuracy and dependability were indicated by the significantly lower false positives (350) and false negatives (550) than in previous techniques.

The remarkable performance of the DBN classification approach over all relevant criteria shows its stability as a solution for securing 5G cognitive radio networks. Its power to create higherarchial representations and capture complex trends in the data helps it to be rather efficient in spotting and lowering network intrusion .this approach not only ensure accuracy and dependability of intrusion detection but also assures prompt reactions to such threats since maintaining network security in real time depends on fast answers to possible attacks.

Table 3: Performance Analysis

Method	Dataset	Accuracy (%)	Detection rate (%)	False positive rate(%)	Response time (ms)	Run time(s)	F-measure	Loss
MASRDDPG	Training	92.5	91.8	3.2	35	250	0.915	7.5
	Testing	91.2	90.5	3.5	38	255	0.902	8.8
	Validation	91.0	90.2	3.7	37	252	0.900	9.0
DBN-MJPF	Training	93.8	93.2	2.8	32	220	0.930	6.2
	Testing	92.6	92.0	3.0	34	225	0.921	7.4
	Validation	92.4	91.8	3.2	33	223	0.919	7.6
NWDAF-PACDS	Training	94.4	93.5	2.5	30	200	0.935	5.8
	Testing	93.1	92.4	2.7	32	205	0.925	6.9
	Validation	92.9	92.2	2.9	31	203	0.923	7.1
Proposed DBN classification	Training	95.5	95.0	2.0	28	180	0.950	4.5
	Testing	94.6	94.0	2.3	29	185	0.940	5.4
	Validation	94.4	93.8	2.5	28	182	0.938	5.6

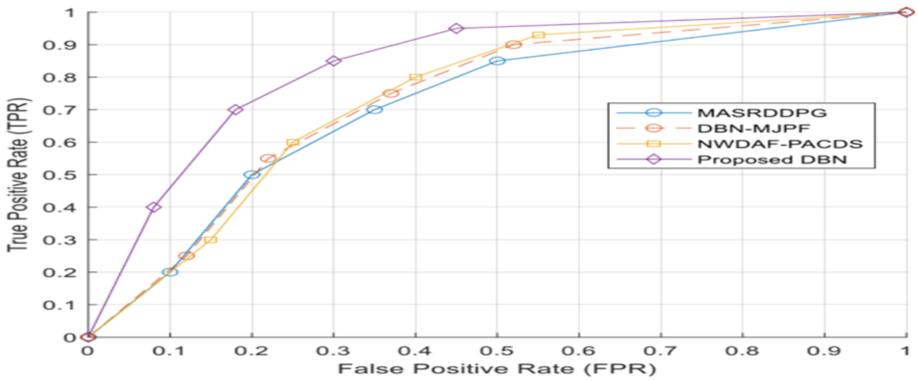


Fig 9: ROC Curve

6. Conclusion:

Under the frame work of SDN intrusion detection, the proposed DBN classification systems outperforms current sytems.Maintaining good run times it reduces false positive rates, increases detection rates and guarantee more accuracy. These advancements are critically essential in real time network security scenarios when fast and accurate anomaly detection is essential to lowering prospective dangers. Since the DBN technique can capture hierarchical representations inside the data and complicated patterns, thereby improving its performance ,it is good tool for network intrusion detection.DBN classification method offers a workable way to strengthen 5G cognitive radio network security against emerging threats.

7. Future works:

Future research will focus on including more complex neural network topologies and studying ensemble learning technique to improve detection accuracy and reduce false positive rates hence enhancing the DBN model. Moreover, including other types of networks attacks and benign traffic to the dataset would be vital to ensure the resilience and adaptability of the model to many practical scenarios.

References:

[1] Pirinen, P. (2014, November). A brief overview of 5G research activities. In *1st International Conference on 5G for Ubiquitous Connectivity* (pp. 17-22). IEEE.

[2] Badoi, C. I., Prasad, N., Croitoru, V., & Prasad, R. (2011). 5G based on cognitive radio. *Wireless Personal Communications*, *57*, 441-464.

[3] Gandotra, P., & Jha, R. K. (2017). A survey on green communication and security challenges in 5G wireless communication networks. *Journal of Network and Computer Applications*, *96*, 39-61.

[4] Ahmad, W. S. H. M. W., Radzi, N. A. M., Samidi, F. S., Ismail, A., Abdullah, F., Jamaludin, M. Z., & Zakaria, M. (2020). 5G technology: Towards dynamic spectrum sharing using cognitive radio networks. *IEEE access*, *8*, 14460-14488.

[5] Parvin, S., Hussain, F. K., Hussain, O. K., Han, S.,

Tian, B., & Chang, E. (2012). Cognitive radio network security: A survey. *Journal of Network and Computer Applications*, *35*(6), 1691-1708.

[6] Siddikov, I., Khujamatov, K., Reypnazarov, E., & Khasanov, D. (2021, November). Crn and 5g based iot: Applications, challenges and opportunities. In *2021 international conference on information science and communications technologies (ICISCT)* (pp. 1-5). IEEE.

[7] Hlavacek, D., & Chang, J. M. (2014). A layered approach to cognitive radio network security: A survey. *Computer Networks*, *75*, 414-436.

[8] El-Hajj, W., Safa, H., & Guizani, M. (2011). Survey of security issues in cognitive radio networks. *Journal of Internet Technology*, *12*(2), 181-198.

[9] Badoi, C. I., Prasad, N., Croitoru, V., & Prasad, R. (2011). 5G based on cognitive radio. *Wireless Personal Communications*, *57*, 441-464.

[10] Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, *22*(1), 196-248.

[11] Sheikhzadeh, S., Pourghasemian, M., Javan, M. R., Mokari, N., & Jorswieck, E. A. (2021). Ai-based secure NOMA and cognitive radio-enabled green communications: Channel state information and battery value uncertainties. *IEEE Transactions on Green Communications and Networking*, *6*(2), 1037-1054.

[12] Yuan, Y., Gehrmann, C., Sternby, J., & Barriga, L. (2022, July). Insight of Anomaly Detection with NWDAF in 5G. In *2022 International Conference on Computer, Information and Telecommunication Systems (CITS)* (pp. 1-6). IEEE.

[13] Odarchenko, R., Iavich, M., Iashvili, G., Fedushko, S., & Syerov, Y. (2023). Assessment of security KPIs for 5G network slices for special groups of subscribers. *Big Data and Cognitive Computing*, *7*(4), 169.

[14] Krayani, A., Farrukh, M., Baydoun, M., Marcenaro, L., Gao, Y., & Regazzoni, C. S. (2019, September). Jammer detection in M-QAM-OFDM by learning a Dynamic Bayesian Model for the Cognitive Radio. In *2019 27th European Signal Processing Conference (EUSIPCO)* (pp. 1-5). IEEE.

[15] Lilhore, U. K., Dalal, S., & Simaiya, S. (2024). A cognitive security framework for detecting intrusions in IoT and 5G utilizing deep learning. *Computers & Security*, *136*, 103560