Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.024839
Article

Tech Science Press

Detection of Attackers in Cognitive Radio Network Using Optimized Neural Networks

V. P. Ajay[1,*] and M. Nesasudha[2]

[1]Department of Electronics and Communication Engineering, Kumaraguru College of Technology, Coimbatore, 641049, Tamilnadu, India
[2]Electrical Sciences, Karunya Institute of Technology and Sciences, Coimbatore, 641114, Tamilnadu, India
[*]Corresponding Author: V. P. Ajay. Email: ajayvpphd@gmail.com
Received: 01 November 2021; Accepted: 07 January 2022

Abstract: Cognitive radio network (CRN) is a growing technology targeting more resourcefully exploiting the available spectrum for opportunistic network usage. By the concept of cognitive radio, the wastage of available spectrum reduced about 30% worldwide. The key operation of CRN is spectrum sensing. The sensing results about the spectrum are directly proportional to the performance of the network. In CRN, the final result about the available spectrum is decided by combing the local sensing results. The presence or participation of attackers in the network leads to false decisions and the performance of the network will be degraded. In this work, an optimized artificial neural network (ANN) based aggressor classification algorithm is proposed. The performance of ANN improved by using the Immune plasma optimization (IPO) algorithm which is inspired by human immune system response for COVID-19 disease. Results indicate that the proposed IP optimized ANN produces better results in terms of attacker detection accuracy, energy, packet delivery ratio and delay of the network. The results show that the proposed method has 32% accuracy rate improvement's, 16% energy savings, 40% packet delivery ratio improvements and 30% overall delay reductions than the existing methods.

Keywords: ANN; cognitive; IPE; Covid-19

1 Introduction

The open and dynamic nature of CRN causes cognitive radio systems to be susceptible to numerous malicious attacks [1]. The main aim of attackers in the network is to lower the performance in terms of privacy, obtainability, and access control [2]. Cognitive radio networks allow secondary user (SU) or unlicensed users to use a licenced user or Primary user (PU) spectrum opportunistically when the spectrum is in an idle state [3,4]. So, compared to other networks, all types of attacks do occur in CRN.

In other networks, the security for communication is provided by using encryption and decryption algorithms. In CRN, the SU's and PU's are separated without signalling exchange. So, there is a huge need for security algorithms to protect a network from attack.

In CRN, the spectrum sensing accuracy increased by using the concept of collaborative spectrum sensing whereas the local sensing results of SU's combined to make a decision about available spectrum or channel. The presence of attackers in a network leads to making a wrong decision about spectrum and the entire performance of the network will be degraded. One of the main data falsification attacks in CRN called the spectrum sensing data falsification (SSDF) attack which is effectively participated to falsify the local sensing results [5]. The types Of SSDF attacks can be classified into three types: Always 'yes' attack, Always 'no' attack and always adverse attack. In the always **yes** attack, the sensing results by SU's always one irrespective of actual results. Conversely, in always **no** attack, the sensing results by SU's always zero irrespective of actual results. In adverse attacks, the sensing results are an inversion of original results always.

Recently, the use of machine learning (ML) algorithms is motivated by various researchers due to their accuracy and learning capacities like Support vector machines (SVM), random forest (RF) and Neural networks (NN). ML is a subset of artificial intelligence used for various applications like data mining, speech and image processing [6]. The main drawback of ML algorithms suffers from training complexity and parameter tuning. In this work, NN based attacker detection algorithm is proposed for CRN. The performance of ANN is improved by using IPO algorithms.

Section 2, describes the related work. In Section 3, the proposed algorithm with IP optimized NN is explained. In Section 4, system models and experimental results are discussed. Finally, conclude the paper in Section 5.

2 Related Work

In this section, security algorithms are reviewed for detecting attackers in CRN. Kaligineedi et al. 2020 [7], have proposed a malicious user detection scheme to identify malicious users and reduce their performance of the sensing system. The proposed method doesn't require any PU acknowledgement for detection and increases the detection rate by knowing the partial response of the authentication unit. Comparing the data function scheme, the proposed scheme via simulating cooperation system makes the equal gain at the access point.

Alahmadi et al. 2014 [8] have proposed an AES-Assisted DTV scheme to share confidential data between source and destination. By using this process, a reference signal is generated at end of the destination which is used to identify the accurate information or authorized user data. A malicious user can be identified preciously even the primary user is absent by combining the analysis on the autocorrelation. The proposed system mainly implies that it can directly apply to HDTV systems. Yuan et al. 2013 [9] have developed a defence scheme using Belief Propagation (BP). The main aim of the proposed model is to record the feedback while moving from one to another on the route. Based on final credit values, the source node is to detect the malicious node. Xu et al. 2016 [10] have proposed an algorithm for physical layer security. By using the metric of transmission secrecy outage probability, the randomly distributed attackers are easily identified. It jointly considers both security and reliability problems.

Zhang et al. 2021 [11], have proposed an ML-based power scheduling model for attacker design in CR. NN is used to identify malicious nodes and to increase the secrecy rate of SU's. The main of the proposed ML is to solve the power scheduling problem with increased security. Results show that the proposed model achieves a 92% secrecy rate with lesser computation time. Wang et al. 2018 [12] have proposed a PU boundary detection based attacker detection algorithm to increase network security. The self-organizing map is used to find the boundary of PU. The presence of attacker patterns in a network is classified by using the SVM algorithm. Results show that kernel-based SVM is superior to linear SVM in terms of classification accuracy.

Laghate et al. 2015 [13] have introduced an algorithm for detecting malicious nodes in a group of nodes using Bayesian network model. The correlated data from collected SU's are processed by a loopy belief propagation algorithm to separate attackers from the group. The classification error is very less when compared to other methods. Rawat et al. 2011 [14] have proposed a Byzantine attack detection method by comparing the local decisions of SU's. The FC performs counting mismatch between received results to identify the attacks. The delay and throughput performance of the network improved due to the elimination of attackers in the network.

Alahmadi et al. 2014 [15] have presented an encryption technique to prevent attacker communication in a network. Advanced encryption standard (AES) has been used to encrypt a reference signal for SU to PU communication. But, the encryption processes adds complexity to the network communication. Abrardo et al. 2016 [16] have developed a game-theoretic approach to take an optimum decision in the fusion centre. The combined hidden Markov Model and chair varshney rule is used to study the observed results of SU's. The false detection probability is very less when compared to other approaches.

3 IPO Optimized NN Based Malicious Node Detection Algorithms

The proposed malicious node detection algorithm is divided into three steps: data pre-processing, NN model construction and Optimized NN based classification. The data pre-processing method involves the observing of sensed results using the exponentially weighted moving average method. Then, the NN model is trained and optimized by using IP optimization. The optimized model accurately classifies the attacker nodes in the network.

Data pre-processing

The local sensing data from SU's collected at the FC. FC executes fusion rule for result or decision making. In this rule, the final result is 'ONE' if [n/2] SUs send the result as 'ONE' to the FC. Else, the result is 'ZERO'. The frequency property of events is used for decision making with dissimilar events at each slot for each SU. There are four possible events to have occurred (00, 01, 10, 11).

In a slot, Event 00 is happened, for an SU if the common result is ZERO and the SU reports ZERO. Similarly, Event 01 is happened, for an SU if the common result is ZERO and the SU's send the result as 'ONE'. Four random variables X0, X1, X2 and X3 were used to denote the frequency of the four occurrence types correspondingly. In a slot, the events of 00 and 11 happened frequently, it is to expect that SU is an authentic one who or which acts as the majority SUs. Similarly, the events of 01 and 10 occurred frequently, it is to expect that SU is an aggressor who or which falsify the original decision result.

The past reply or behaviour of SU's contribute a major role in classifying whether it is genuine or not. In this work, the exponentially weighted moving average method is used to calculate the value of x(t) which represents the frequency with which the matching occurrence category happens in the new past.

$$X_i(t) = \begin{cases} \beta + (1-\beta)X_i(t-1) & \text{if } i^{th} \text{event type occurs at } t \\ (1-\beta)X_i(t-1) & \text{otherwise} \end{cases} \quad (1)$$

where t denotes the time slot. β is the factor to be used for giving priority to the observations. The performance of classification improved by assigning more weights to recent observations.

Immune plasma optimization (IPO)

The immune plasma therapy approach has been used successfully in various viral diseases for example Crimean-Congo haemorrhagic fever (CCHF), H1N1 flu, SARS and MERS and ebola. This method is instantly available from persons who have recovered, are viral free, and can give immune plasma (IP) comprising higher neutralizing antibodies. Immune Plasma (IP) algorithm is a new meta-heuristic

optimization algorithm inspired by the treatment process of Immune Plasma or convalescent plasma for COVID-19 patients or some other disease [17].

In this optimization, each person in the population is considered as a possible solution to be optimized. The immune response of the corresponding person specifies the excellence of the corresponding solution. The defence operation for generating antibodies at the starting of infection is related to the exploration or diversification stages of optimization. The identification of persons who recovered from the disease shortly contribute to the exploitation stage of the IP algorithm. The basic concept IP algorithm is including three steps: Producing initial persons. Infection distribution and immune system response and Plasma Extraction and Transfer.

Producing initial persons

Initially, each person in a population is considered as a possible solution for the problem. The produced population with decision parameters is given in the equation.

$$s_{kj} = s_j^{low} + rand(0,\ 1)(s_j^{high} - s_j^{low}) \text{ Where } k = \{1,\ 2,\ \ldots,\ PS\} \text{ and } j = \{1,\ 2,\ \ldots,\ D\} \tag{2}$$

s_j^k is coordinated with the jth decision parameter of the s_k.

s_j^{low} and s_j^{high} denotes the minimum and maximum limits of the jth parameter, rand(0, 1) denotes the random number varies between 0 to 1.

Infection distribution and immune system response

A minimum percentage of diseased persons can affect the entire population. The secretions from the infected persons entered into another person easily. the immune system of the affected person gives a specific response to corresponding antigens by developing antibodies. The spreading rate of disease and corresponding immune system response mathematically modelled and expressed as follows

$$s_{kj}^{inf} = s_{kj} + rand(-1, +1)(s_{kj} - s_{mj}) \tag{3}$$

where $k = \{1, 2, \ldots, N\}$ and $m = \{1, 2, \ldots, N\}$-{k}

s_{kj} is the randomly calculated jth variable of the s_k person being diseased.

s_{kj}^{inf} is the recently estimated jth variable of the s_k^{inf} that is used on behalf of the infectious s_k person. The s_{mj} is also the jth variable of the earlier diseased and randomly designated s_m person.

In the IP algorithm, the amount of produced antibodies is directly related to the objective function. The person with the highest antibody generation rate is considered as the best solution for the corresponding fitness function. In every iteration, the present solution is compared with the previous solution based on anti-body generation rate. The jth parameter of the s_k individual remains without change is given in equation

$$s_{kj} = \begin{cases} s_{kj}^{inf};\ if\ f(s_{kj}^{inf}) < f(s_k) \\ s_{kj};\ \ if\ f(s_{kj}^{inf}) \geq f(s_k) \end{cases} \tag{4}$$

Plasma Extraction and Transfer

The response of the immune system for antigen is different for different persons. While some of the diseased people may recover fast, some of the people need intensive care units to recover from the disease. In the plasma method, the antibodies generated from the recovered person are transferred to the affected person to create immunity. The plasma transmission operation is initiated by identifying the number of donors and receivers persons. The number of eligible donors and receivers is also identified in this stage. The plasma transfer from donors to receivers is mathematically expressed as the following equation:

$$s_{kj}^{rcv-p} = s_{kj}^{rcv} + rand(-1,+1)(s_{kj}^{rcv} - s_{mj}^{dnr})\text{j} \ = \{1,\ 2,\ \ \ldots,\ \text{D}\} \tag{5}$$

s_k^{rcv-p} individual denotes the s_k^{rcv} after plasma treatment and s_{kj}^{rcv-p} is matched with the jth variable of the s_k^{rcv-p} individual.

The plasma treatment is completed when the immunity of the patient is increased. The response or immunity of the s_k^{rcv} is not improve for the dose, then, the s_k^{rcv} of receiver improved by adjusting controlling parameters. The dose of plasma is transferred from donor to receiver until reach a guaranteed immunity.

Once the plasma treatment is completed, IP algorithms use a controlled-randomised process for altering calculated donor persons in the last iterations. The random number varies from zero to one and it is smaller than the proportion between current fitness evaluation (t_{cr}) and precalculated maximum fitness evaluations (t_{max}). Each variable is updated based on the guidance of previously used values and it is expressed as follows:

$$x_{mj}^{dnr} = x_{mj}^{dnr} + rand(-1,+1)x_{mj}^{dnr} \tag{6}$$

For concluding the working of IP algorithm, generates initial persons, control the spreading of infection, find out immune responses, chooses donor and receiver persons, transfers plasmas for the receivers and lastly updates donors.

3.1 ANN

Artificial neural networks (**ANNs**), also called **neural networks** (**NNs**) are intelligent systems encouraged by the biological neural networks that can perform in a manner similar to the human nervous system. It contains an input layer, hidden layers, and an output layer to process the neurons. The output of each is connected to the next layer with the different nonlinear activation functions as shown in Fig. 1.

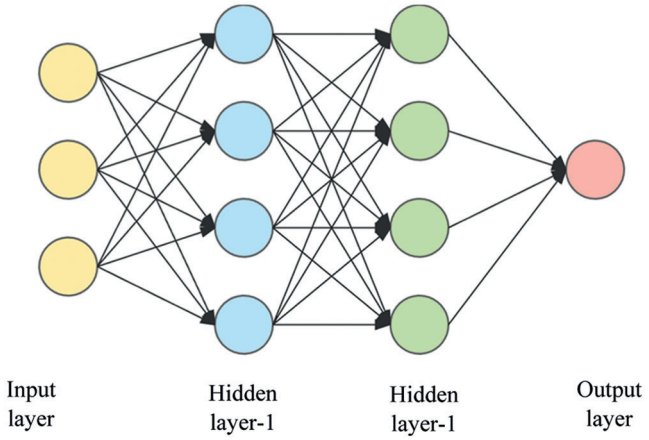

Figure 1: Structure of NN

ANN is a subcategory of supervised learning where the information is in the form of a connected network unit. It involves the extraction of features from data sets for learning. The data set for learning is separated into two sections: training and testing. Training sets are used to teach the ANN model with known input and outputs. the most common data set division methods are random sampling, hold-out method and cross-validation.

The training process of NN depends on four factors: learning rate, weight, bias and parameter tuning. The learning process started with some initial values and then updated based on the error rate for every

iteration. The training of NN is a complex task and more time-consuming. The proper optimization algorithm is needed to adjust the weight of the network by considering parameter tuning as a combinatorial problem. In ANN, the weights of neurons are responsible for perfect classification and prediction. These Neurons are also identified as tuned parameters. The tuning of correct weight in the network helps to get exact classification or prediction results. The cost function of each network is derived to optimize the tuning parameters to give an effective result. The proposed ANN optimization and attacker detection algorithm is given below.

Pseudocode for proposed attack detection

Initialize PS, D, NoD and NoR control parameter

Set number of PU and SU's

Randomly initialize all NN parameters

For all nodes

{

SU(Sensing results)

Perform ← Exponentially weighted moving average

}

For all results

NN (hyper parameters)

{

Find classification error

Optimized NN

ATTACKER classification

}

Call IP

}

IP optimization (Parameters)

{

Update using the response of immune system equation

Update using plasma transfer equation

Update using the previous best solution

Determine donor and receiver person's

Identify best tuning parameters

}

4 System Model and Experimental Results

The proposed attacker detection algorithm is implemented using MATLAB. The total number SU's is set to 500. For sensing, co-operative spectrum sensing is performed. Each SU senses spectrum availability independently and FC perform decision making based on binary classification. The reports of 100 slots are used to create a data set. The frequency of four events is applied for each slot. The nodes are programmed to behave as s attacker randomly with the probability of α and labelled as 'attacker'. The

remaining nodes are labelled to be genuine. The probability for the existence of PU's is set to 0.6. The probability of false alarm used for sensing error calculation. The parameters considered for NN optimization are: number of neurons, epochs and batch size.

The performance parameters considered are: Accuracy, Precision and Recall. The accuracy of attacker detection results denotes the ratio of the sum of TP and TN out of all the detections. Recall rate denotes the ratio of TP to the summation of TP and FN. Precision rate denotes the ratio of TP to the summation of TP and FP. Both precision and recall rate is a valuable measure of the success of detection when the classes are very imbalanced.

$$\text{Accuracy} = \frac{\text{TP} + \text{FN}}{TP + FP + TN + FN} \tag{7}$$

$$\text{Precision} = \frac{\text{TP}}{TP + FP} \tag{8}$$

$$\text{Recall} = \frac{\text{TP}}{TP + FN} \tag{9}$$

- **True Positive (TP)**: True positive represents the rate of exact attacker detections of positives out of actual positive cases.
- **False Positive (FP)**: False-positive represents the rate of inexact positive detections.
- **True Negative (TN)**: True negative represents the rate of exact detections of negatives out of real negative cases.
- **False Negative (FN)**: False-negative represents the rate of inexact negative detections.

For a fair comparison, the proposed algorithm compared with other standard classification algorithms of Support Vector Machine (SVM), Naïve Bayes and traditional neural network. The detection accuracy of the proposed method for Always **YES** attack, Always **NO** attack and Adverse attacks as a function of increasing attacker nodes percentage given in Tabs. 1–3 and graphically shown in Figs. 2–4. The proposed optimized model shows higher classification accuracy percentage for all types of attacks. It assures the reliability of the proposed protocol for the further processing of routing and clustering.

Table 1: Always **YES** attack

Percentage of attackers (%)	SVM	NB	NN	Optimized NN
10	98	99	100	100
20	95	97	97	100
30	90	95	96	99
40	87	91	94	99
50	87	90	94	98

Table 2: Always **NO** attack

Percentage of attackers (%)	SVM	NB	NN	Optimized NN
10	94	98	98	99
20	90	96	97	99
30	86	94	97	99
40	82	90	93	99
50	81	83	90	97

Table 3: Adverse attack

Percentage of attackers (%)	SVM	NB	NN	Optimized NN
10	90	98	96	100
20	84	96	96	99
30	84	94	95	98
40	83	90	92	98
50	81	90	92	96

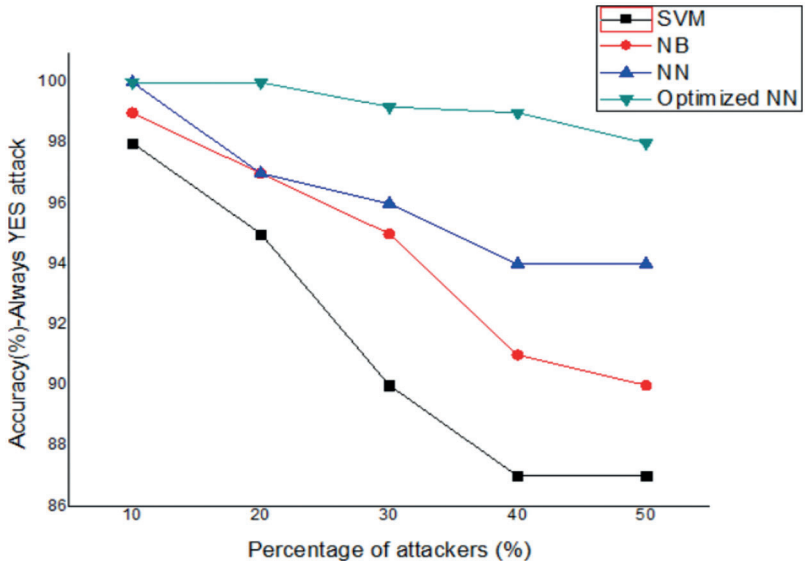

Figure 2: Always **YES** attack

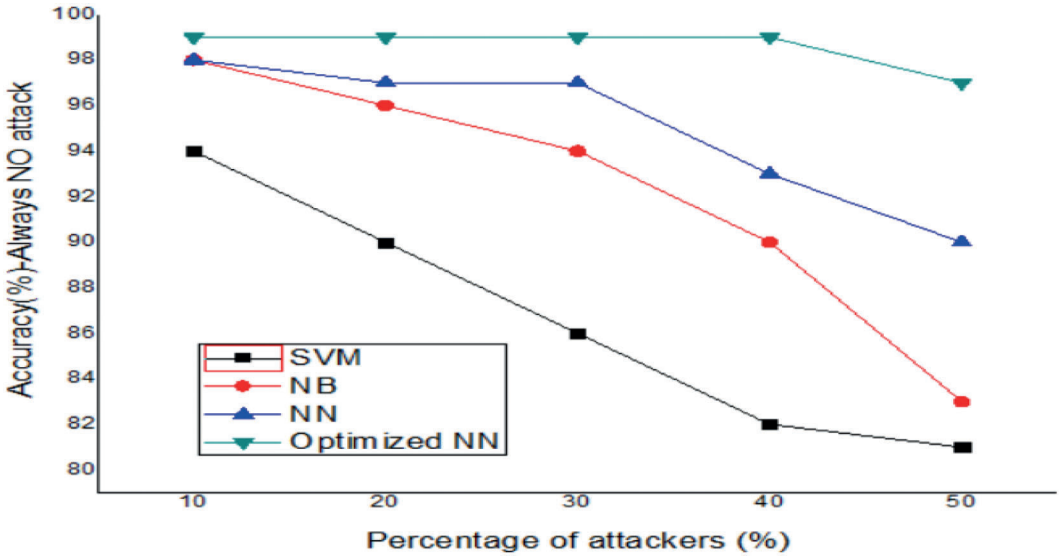

Figure 3: Always **NO** attack

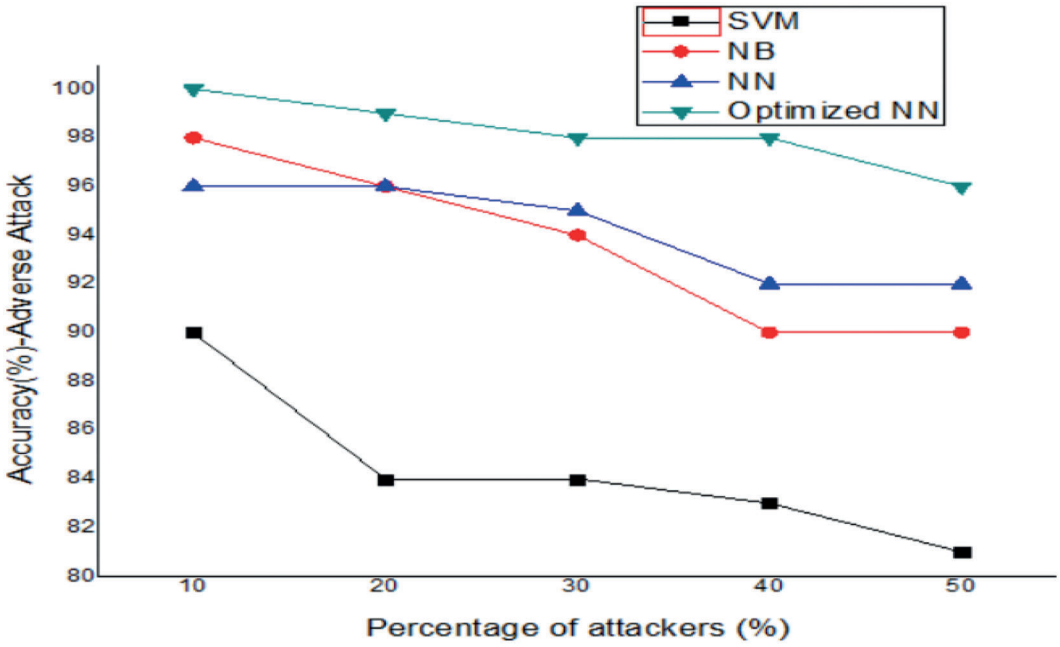

Figure 4: Always **YES** attack

The precision and recall rate of the proposed method as a function of increasing attacker nodes percentage is given in Tabs. 4 & 5 and graphically shown in Figs. 5 & 6. The overall precision and recall rate of the proposed optimized NN model is higher than other methods due to the selection of optimal selection parameters.

Table 4: Precision analysis

Percentage of attackers (%)	SVM	NB	NN	Optimized NN
10	85	95	96	97
20	85	92	93	97
30	79	91	89	93
40	78	88	87	92
50	75	86	86	89

Table 5: Recall rate analysis

Percentage of attackers (%)	SVM	NB	NN	Optimized NN
10	72	79	82	89
20	72	77	77	88
30	65	70	73	88
40	60	70	73	87
50	60	66	70	87

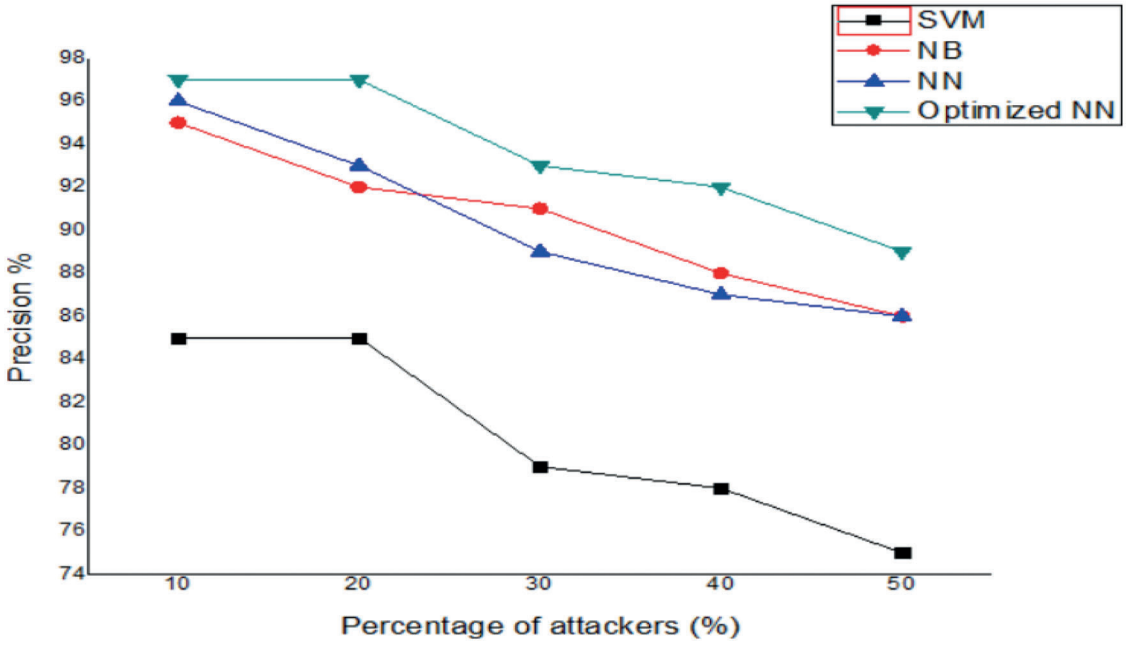

Figure 5: Precision analysis

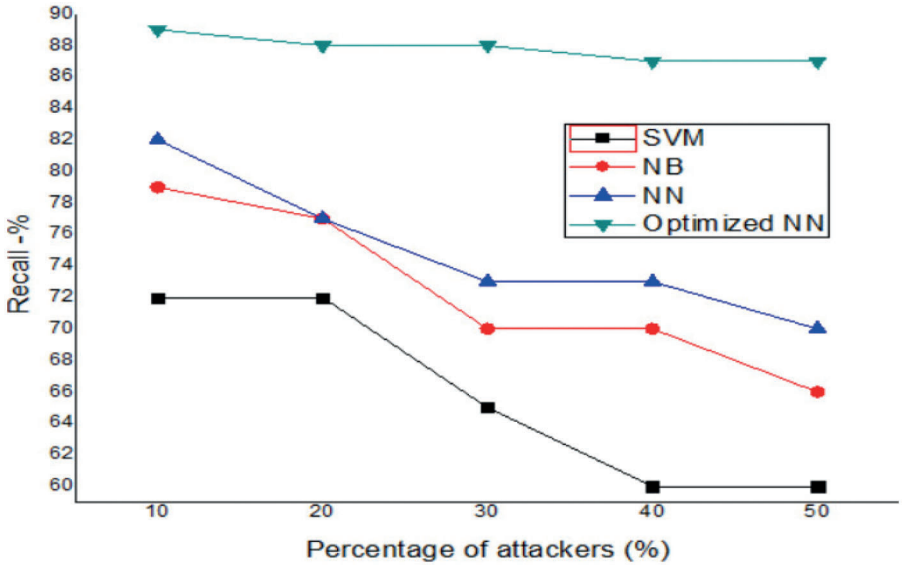

Figure 6: Recall analysis

The classification results of proposed NN by a varying number of neurons, epochs and batch sizes are given in Tab. 6. Results show that the increasing layers and batch sizes lead to increased accuracy of detection. Compared to other methods, the proposed model achieved an overall accuracy of about 99.2% as given in Tab. 7.

Table 6: Validation for varying parameters

Neurons	Epochs'	Batch size	Accuracy
8	200	20	88
16	150	10	96.5
32	100	10	100

Table 7: Over all analysis

Method	Accuracy
SVM	89.2
NB	94
NN	94.8
Optimized NN	99.2

5 Conclusion

The cognitive radio concept is introduced to overcome the drawback of a static spectrum allocation policy by using a dynamic spectrum allocation strategy. CR utilize the available spectrum efficiently by offering opportunistic access to SU's. But, security in CRN is a critical issue due to its inherent vulnerabilities. This work proposed a malicious node detection algorithm for attacker free communication in CRN. ML algorithm of ANN combined with optimization is used to detect an attacker in a network. The proposed method compared with well-known algorithms of SVM, NB and traditional ANN. Results show that the proposed model achieves a higher detection rate than other methods.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems," *IEEE Transaction on Wireless Communication*, vol. 10, no. 1, pp. 274–283, 2011.

[2] X. ChunSheng and M. Song, "Detection of PUE attacks in cognitive radio networks based on signal activity pattern," *IEEE Transactions on Mobile Computing*, vol. 13, no. 5, pp. 1022–1034, 2014.

[3] S. M. Mishra, A. Sahai and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. IEEE Conf. Communication. (ICC'06)*, Istanbul, Turke, pp. 1658–1663, 2006.

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

[5] X. Xu, J. Bao, Y. Wang and L. Li, "A spectrum sensing data falsification countermeasure strategy in energy-efficient CRN," in *2016 8th Int. Conf. on Wireless Communications & Signal Processing (WCSP)*, Yangzhou, China, 2016.

[6] H. Zhu, T. Song, J. Wu and X. Li, "Cooperative spectrum sensing algorithm based on support vector machine against SSDF attack," in *Proc. IEEE ICC Workshops*, Kansas, USA, pp. 1–6, 2018.

[7] P. Kaligineedi, M. Khabbazian and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2488–2497, 2015.

[8] A. Alahmadi, M. Abdelhakim, J. Ren and T. Li, "Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 772–781, 2014.

[9] Z. Yuan, Z. Han, Y. L. Sun, H. Li and J. B. Song, "Routing-toward-primary-user attack and belief propagation-based defense in cognitive radio networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp. 1750–1760, 2013.

[10] X. Xu, B. He, W. Yang, X. Zhou and Y. Cai, "Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 373–387, 2016.

[11] M. Zhang, "Exploiting deep learning for secure transmission in an underlay cognitive radio network," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 726–741, 2021.

[12] H. Wang and Y. Yao, "Primary user boundary detection in cognitive radio networks: Estimated secondary user locations and impact of malicious secondary users," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4577–4588, 2018.

[13] M. Laghate and D. Cabric, "Cooperative spectrum sensing in the presence of correlated and malicious cognitive radios," *IEEE Transactions on Communications*, vol. 63, no. 12, pp. 4666–4681, 2015.

[14] A. S. Rawat and P. Chen, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, 2011.

[15] A. Alahmadi, M. Abdelhakim and J. Jian Ren, "Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 772–781, 2014.

[16] A. Abrardo, M. Barni and B. Tondi, "A game-theoretic framework for optimum decision fusion in the presence of byzantines," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1333–1345, 2016.

[17] S. Aslan and S. Demirci, "Immune plasma algorithm: A novel meta-heuristic for optimization problems," *IEEE Access*, vol. 1, no. 1, pp. 220227–220245, 2020.