International Journal of Safety and Security Engineering
Vol. 15, No. 3, March, 2025, pp. 479-489
Journal homepage: http://iieta.org/journals/ijsse

SIOPA-DLMUC: A Self-Improved Orca Predation Algorithm with Deep Learning for Enhancing 5G Enabled Cognitive Radio Network Security

M. Minilal, M. Meena*

Department of ECE, Vels Institute of Science Technology and Advanced Studies, Chennai 600117, India

Corresponding Author Email: meena.se @velsuniv.ac.in

https://doi.org/10.18280/ijsse.150307

Received: 5 February 2025
Revised: 19 March 2025
Accepted: 25 March 2025
Available online: 31 March 2025

Keywords:
5G networks, malicious user detection, Cognitive Radio Networks, deep learning, hyperparameter tuning, spectrum sensing, network security, metaheuristic optimization

ABSTRACT

Cognitive Radio Networks (CRN) are pivotal in the 5G era, ensuring efficient spectrum usage for data-intensive applications while their cognitive abilities adapt to the environment, reducing interference and enhancing connectivity. However, amidst the promise of these advancements lies a critical challenge - the detection of malicious users (MUs) within CRNs. A dynamic and cooperative nature of CRNs, where unlicensed secondary consumers share spectrum with licensed primary consumers that opens door to potential vulnerabilities. Detecting and mitigating presence of MUs are vital for maintaining the reliability of network and preventing illegal spectrum access. To address these security challenges and enhance accuracy of decision-making within CRNs, this study introduces Self-improved Orca Predation Algorithm with Deep Learning Driven Malicious User Detection (SIOPA-DLMUC). This novel technique focuses on robust detection and classification of MUs. It operates in two distinct stages: in the first stage, the long short-term memory (LSTM) algorithm is employed for automated MU detection. LSTM, known for its ability to analyze temporal behavior and communication patterns of users within CRNs, plays a critical role in identifying deviations from normal behavior, thus improving the accuracy of MU detection. In the second stage, the SIOPA-based hyperparameter tuning process optimizes LSTM parameters to enhance detection performance further. To validate the effectiveness of the SIOPA-DLMUC algorithm, extensive testing has been performed on a diverse dataset, including four distinct types of attacks: Byzantine attacks, Jamming Attacks, Spectrum Sensing Data Falsification (SSDF) attacks, and Primary User Emulation (PUE) attacks along normal samples. The results consistently demonstrate superior performance of SIOPA-DLMUC algorithm when compared to other deep learning models, showcasing its potential to bolster security and reliability in CRNs operating within the 5G landscape. With its capacity to adapt to a wide range of threats and provide robust security, the SIOPA-DLMUC algorithm represents a promising solution for ensuring the integrity of 5G-assisted Cognitive Radio Networks. The proposed model achieves an impressive accuracy of 93.93% demonstrate an exceptional performance surpassing the traditional models.

1. INTRODUCTION

The emergence of 5G and Cognitive Radio Networks (CRNs) heralds a new era in wireless transmission, offering innovative solutions to the challenges of wireless connectivity. The fifth generation (5G) wireless technology brings with it the promise of ultra-low latency and blazing-fast data speeds, positioning it as the ideal choice for applications like augmented reality, autonomous vehicles, and the Internet of Things (IoT) [1]. Concurrently, CRNs introduce the concept of dynamic spectrum access, allowing devices to intelligently harness and adapt available spectrum resources. Integrating CRN into the architecture of 5G presents a compelling opportunity to address interference issues and optimize spectrum utilization, ensuring that the 5G network operates at its peak even in congested and dynamic environments. Moreover, the fusion of CRNs with 5G emphasizes resilience and adaptability. In an ever-evolving wireless landscape, CRN offers intelligent interference management, bolstering the overall robustness of the 5G network by dynamically allocating spectrum resources in real-time [2]. These technologies also promote spectrum sharing and facilitate greater cooperation among diverse wireless systems, fostering effective coexistence between different technologies. This collaborative synergy between 5G and CRNs holds the potential to create a more reliable, agile, and efficient wireless transmission system, essential for meeting the diverse demands of contemporary applications and services. For a visual representation of the general architecture of 5G-enabled CRNs, refer to Figure 1.

Within the realm of Cognitive Radio Networks (CRNs), task of identifying accessible spectrum resources involves a method that employs secondary users (SUs). These SUs lack the necessary permissions but play a pivotal role in monitoring

and controlling the voluntary spectrum utilized by primary users (PUs) who possess valid permissions [3]. PUs, as licensed users, hold exclusive rights to specific spectrum bands. Attacks targeting PUs typically revolve around interference, unauthorized access, or disrupting their legitimate communications. On the other hand, SUs are opportunistic or unlicensed users that dynamically access spectrum resources not in use by PUs. The success of a CRN hinges on the network's ability to accurately detect presence or nonappearance of essential signal within licensed band, which is opportunistically utilized. To achieve this, Cooperative Spectrum Sensing (CSS) recognized for its capacity to deliver enhanced detection precision, particularly in environments with low signal-to-noise ratios (SNR). In context of infrastructure-based CRNs, CSS involves collecting detecting information from individual users (nodes) within the Fusion Center (FC). The FC employs aggregation rules like OR and AND to formulate the final detection decision [4]. This decision is subsequently disseminated to the individual nodes. Reporting can take two forms: (i) binary, where '0' indicates the absence of the essential signal and '1' denotes its presence, and ii) continuous, where distinct nodes transmit the freshly detected values (such as energy levels) to the FC for further processing [5].

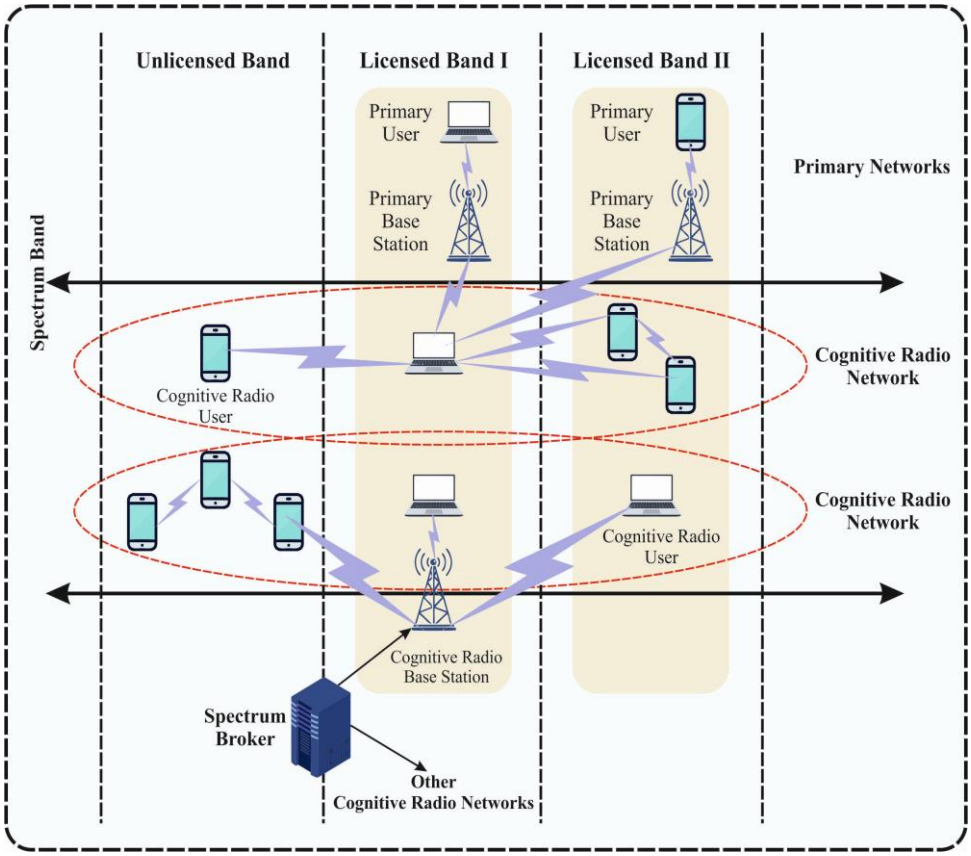

Figure 1. Architecture of 5G enabled CRNs

In the quest for more robust spectrum sensing capabilities, central and distributed collaborative networks have emerged as promising approaches [6]. In the central network, secondary users (SUs) work together by sharing their sensing information with a Fusion Center (FC) that aggregates sensing reports from all SUs to make an optimum decision regarding spectrum occupancy of primary users (PUs) [7]. Conversely, in the distributed network, SUs collaborates by sharing their sensing data amongst themselves, independently making final decision on PU spectrum occupancy without need for FC communication [8]. While collaborative networks offer significant advantages, they are liable to possible threats posed by malicious users (MUs), who may engage in unwanted intrusions among PUs and SUs, thereby compromising accurateness of spectrum sensing process.

To address these challenges, recent advancements have seen the utilization of Machine Learning (ML) methods, which aim to mitigate some of the limitations associated with traditional approaches [9]. ML, a prominent area within Artificial Intelligence, empowers machines with ability to learn autonomously. ML models are supervised learning, which involves a training procedure with labeled input data, and unsupervised learning, where training occurs with unlabeled input data [10]. These ML methods offer promising avenues for enhancing spectrum sensing in collaborative networks, thereby improving the overall resilience and accuracy of the system.

In this study, we develop a new Self-Improved Orca Predation Algorithm with Deep Learning-Driven Malicious User Detection (SIOPA-DLMUC) technique for 5G assisted CRNs. The main goal of SIOPA-DLMUC system is to classify and detect occurrence of MUs in the CRN. The SIOPA-DLMUC technique involves a long short-term memory (LSTM) model for detection of MUs in CRN. In addition, SIOPA-based hyperparameter tuning process can be executed to improve performance of LSTM approach. To observe outcome of SIOPA-DLMUC system, a comprehensive set of simulations is carried out on our database, comprising four kinds of attacks namely byzantine attack, jamming attack, SSDF attack, and Primary User Emulation (PUE) attack with normal samples.

2. RELATED WORK

In reference [11], a combination of GRU and SVM algorithms was proposed for Cognitive Radio Networks. These models were utilized to train and test datasets comprising spectrum sensing results. GRU, a simplified variant of the Long Short-Term Memory (LSTM) network, was employed due to its lower computational complexity and higher efficiency when dealing with small datasets. SVM was applied at the output layer to classify users as either authorized or malicious within the cognitive radio environment.

In reference [12], a hybrid approach integrating the Secure Hash Algorithm 1 (SHA-1) and Neural Networks (NN) was introduced. This model leverages Direction of Arrival (DoA) and Received Signal Strength (RSS) data to determine the positioning between primary and secondary users. The primary objective of this method is to reduce the claim ratio within the communication system.

Benazzouza et al. [13] proposed a novel model based on two machine learning approaches. This algorithm employs a chaotic compressive sensing-based authentication technique to extract low-dimensional features, along with a collaborative machine learning method for user identification. Furthermore, a deep learning technique is proposed that utilizes scalogram images as inputs for identifying primary users in the spectrum.

Paul and Choi [14] presented combined SU and CSS information communications in Energy Harvesting enabled CRN in SSDF threats. The current study utilizes collecting approach to detach the hateful SU from truthful set of SU utilizing reputational rate and other features. The recognized hateful and weak SU is controlled by resourceful Device-to-Device (D2D) transmission in CRN. A Collaborative Learning approach is also projected.

In reference [15], an AI method used to protect transmission on VWN is presented. An effective cyberattack recognition technique is examined utilizing an AI method in the Bayesian learning method for recognition. The outcomes of deep neural network (DNN) and Random Forest methods are examined to identify the cyberattacks on a VWN, having measured essential communication control as a beginning value to the classification of mistrustful actions.

Ajay and Nesasudha [16] proposed an enhanced ANN based on the aggressor identification method. The presentation of ANN is enhanced by the Immune plasma optimizer (IPO) technique which is enthused by the human immune system reaction to COVID19 infection. Consequences specify that the projected IP-enhanced ANN generates the best outcomes relating to hacker recognition accuracy, packet delivery ratio, delay of the network, and energy.

Zhang et al. [17] presented a result for the recognition of irregular use of spectrum from the sub-sampled data stream, an MLP/FFNN. The projected result will be learning the outline of authentic and unauthentic practices independently without the notice of the specialists. The projected NN architecture has displayed rapid recognition speed and a lesser recognition error rate. Brinda and Bhuvaneshwari [18] developed a Boundary recognition technique that utilizes the projected position of each SU, which is attained by employing the RNN method. Next Malicious User Detection by Ordering (MUDO) method can be projected, in which additional employers are evaluated utilizing Basic Probability Analysis (BPA), and depend on commands in which SUs combined by equivalent PU. The SUs with minimum commands rejected as they might be malevolent employers.

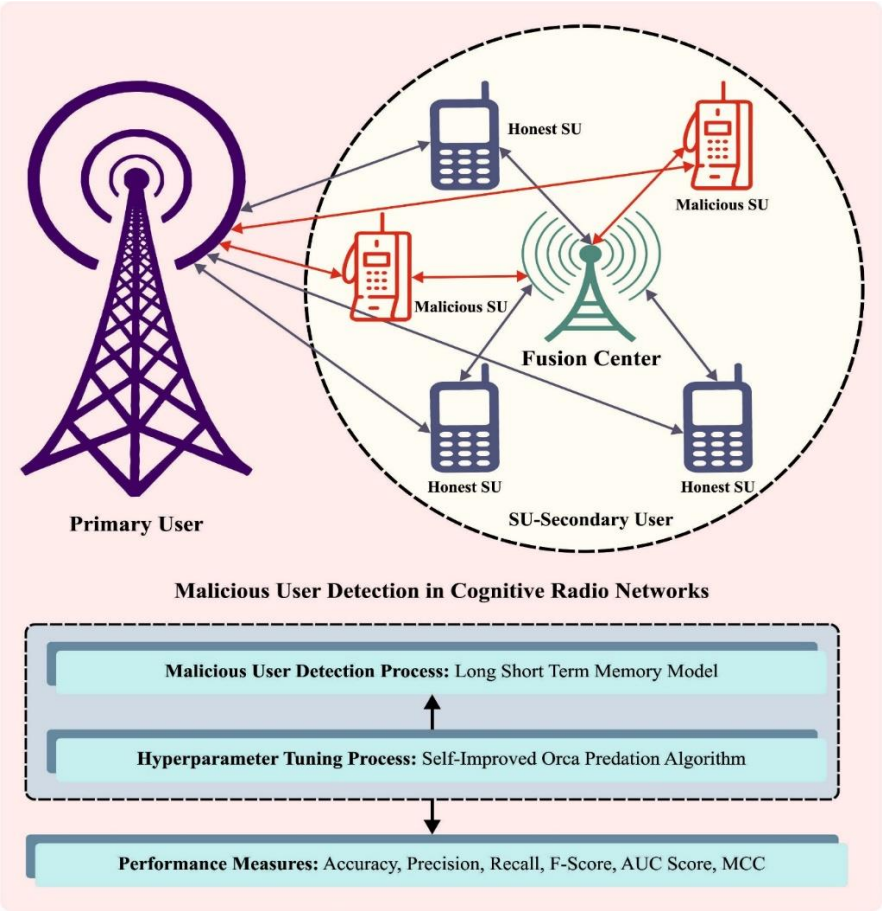

Figure 2. Workflow of SIOPA-DLMUC approach

3. THE PROPOSED MODEL

In this article, we introduced an automated solution, the Self-Improved Orca Predation Algorithm with Deep Learning Driven Malicious User Detection (SIOPA-DLMUC), tailored to address the pressing challenge of detecting Malicious Users (MUs) within the context of 5G-assisted Cognitive Radio Networks (CRN) susceptible to various attacks. The SIOPA-DLMUC operates through two critical stages: firstly, it harnesses Long Short-Term Memory (LSTM) to detect MUs effectively, offering the capability to identify temporal patterns associated with Byzantine attacks, Jamming Attacks, Spectrum Sensing Data Falsification (SSDF) attacks, and Primary User Emulation (PUE) attacks, as well as normal network behavior. The second stage utilizes the SIOPA to fine-tune hyperparameters, enhancing the model's adaptability to detect these specific attacks. SIOPA leverages advanced features, including an acceleration mechanism, memory, learning, and social interactions, to navigate the complex landscape of CRNs under the influence of these disruptive attacks. The model also incorporates a 'BubbleNet' mechanism that refines encircling behaviors, bolstering its ability to detect MUs and ensuring the security of CRNs operating within the dynamic 5G environment.

The SIOPA-DLMUC system aims to classify and detect the occurrence of the MUs in the CRN. To achieve this, SIOPA-DLMUC algorithm follows two phases of processes namely LSTM-based detection and SIOPA-based hyperparameter tuning. Figure 2 portrays workflow of SIOPA-DLMUC methodology.

3.1 Stage I: MU detection process

The detection of the MUs in the CRN is performed by the use of the LSTM model. LSTM works by employing a gating mechanism, consisting of forget, input, and output gates, to selectively process and store information in memory cells, allowing it to effectively capture and analyze temporal patterns in the data [19].

The LSTM is a kind of in-between NN model. LSTM comprises 4 neural system layers that interface in an optimum manner. LSTM adds or removes information to memory unit, using the "Gateway". It includes multiplication and layering work of sigmoid NN. The sigmoid layer opposites feature data by sigmoid ability and estimates outcome in range of [0, 1], representing what amount of information elements can be experienced. “1” represents that each data is permitted that sent. “0” denotes that no date is allowed that sent. The gating mechanism in the LSTM is related to the forgetting gate information gateway and an output gate.

The Forget gate selects what data to be discarded or retained from the memory:

$$F_G = \sigma[w^F(F_t, Y_{t-1}) + c^F] \quad (1)$$

In Eq. (1), F_G is forget gate. C and w are controlled and weighted borders. F_t addresses input at existing timestamp; $Y_t - 1$ shows outcome at t-1 timestamp in prior square of LSTM. σ shows sigmoid function.

The input gate I_G selects the data that must be saved:

$$I_G = \sigma[w^I(F_t, Y_{t-1}) + C^I] \quad (2)$$

Lastly, the resultant gate defines which portion of the memory can be retained:

$$O_G = \sigma[w^O(F_t, Y_{t-1}) + c^o] \quad (3)$$

Additional candidate memory cell M_t is made by the $\tan H$ layer and is represented by:

$$M_t = \tan H[w^M(F_t, Y_{t-1}) + c^M] \quad (4)$$

In Eq. (4), $\tan H$ permits LSTM to remove or add information in the final input. The information gateway chooses the memory unit, and the forget gate is used to delete or hold data for creating the last memory.

$$M_t = F_G * M_{t-1} + I_G * M_t \quad (5)$$

In Eq. (5), M_t signifies memory unit at existing timestamp (t).

$$Y_t = O_G * \tan H(M_t) \quad (6)$$

In Eq. (6), $*$ denotes element-wise multiplication, y_t indicates the output attained by the softmax resultant layer to obtain the output predictive in the existing blocks. Lastly, the loss function is estimated by selecting the MSE as the error calculation:

$$Loss = \sum_{t=1}^{N} (Y_t - T_t)^2 \quad (7)$$

In Eq. (7), Tt shows desired outcome. N indicates prediction made in instance of n data point. Figure 3 demonstrates infrastructure of LSTM.

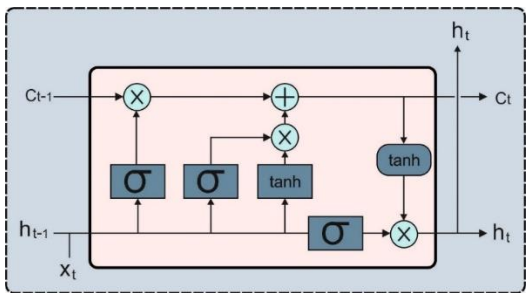

Figure 3. LSTM architecture

3.2 Stage II: Hyperparameter tuning process

For hyperparameter tuning of LSTM method, SIOPA used. An OPA is a current metaheuristic optimization model that sketched inspiration from natural hunting strategy of orcas (killer whales) [20]. It stimulates the hunting behavior of orca to resolve the problem of the optimization algorithm. In the OPA, initialize the population of virtual orca, and each orca signifies the best possible solution to the optimization problems.

Driving phase

Current advancement has introduced the incorporation of social interaction, acceleration mechanism, memory, and learning during the driving stage. This increases the capabilities and performance of the model. The acceleration mechanism has been integrated to enhance the exploitation

and exploration. Orcas collectively improve their intelligence by exchanging and communicating data about the best possible solution, which facilitates the convergence towards the best solution.

i) Acceleration

The acceleration mechanism has been integrated to improve exploitation and exploration capabilities. This mechanism enables orcas to finetune movement speed dynamically according to solution quality, leading to effective navigation of searching space. Sequentially, this enables better exploration of promising outcomes and exploitation of potential areas. During the chase phase, the velocity update equation can be used as follows:

$$Vtchase, 1, i = a * \big(d * xtbest - F * (b * Mt + c * xti)\big) + w * Vtchase, 1, i — 1 \quad (8)$$

$$Vtchase, 2, i = e * (xtbest - xti) + w * Vtchase, 2, i — 1 \quad (9)$$

Now, the acceleration or weight feature w controls impact of previous velocity on existing velocity.

ii) Memory and learning

Here, memory and learning mechanism incorporated to allow orcas to exploit previous knowledge. This allows for making appropriate decisions in future iterations and retaining the memory of successful outcomes, gradually increasing performance of model. In chase stage, velocity update equation is adapted to integrate memory and learning as follows:

$$Vtchase, 1, i = a * \big(d * xtbest - F * (b * Mt + c * xti)\big) + w * Vtchase, 1, i - 1 + m * (Xbest - xti) \quad (10)$$

In Eq. (10), weight or learning factor m defines impact of prior optimum location ($Xbest$) on the existing velocity. Orcas could successfully learn from previous experience and accordingly adapt the movement by adjusting these weights.

iii) Social interaction

During driving process, social interactions amongst orcas established to enable collaboration as well as data sharing. This f to cooperate and exchange valuable information, resulting in better exploitation and exploration of the searching space. During chase phase, velocity updating formula is modified to integrate social interaction:

$$Vtchase, 1, i = a * \big(d * xtbest - F * (b * Mt + c * xti)\big) + w * Vtchase, 1, i - 1 + s * (Xsocial - xti) \quad (11)$$

The social or weight factor s defines the impact of social information, $Xsocial$, on existing velocity.

Encircling phase

A “BubbleNet” mechanism is employed in encircling stage, to enable encircling behaviors of orcas. The orca works together in encircling stage, to encircle target performance by forming a virtual "net" around it. The orca creates a cooperative force that successfully encircles target outcome by coordinating the action.

i) BubbleNet formation

The orcas exploit a BubbleNet development in the encircling stage, based on the supportive hunting strategy used by orcas. The BubbleNet development assists in concentrating and corraling the target solution in a certain region, which improves efficiency of the collective hunting. The location updating formula for the 3rd chasing method, integrating the BubbleNet creation shown as follows:

$$xtchase, 3, i, k = xtd1, k + u * (xtd2, k - xtd3, k) + b * Bt \quad (12)$$

$$Bt = \frac{\sum N\, n(xtbest - xti)}{Nn} \quad (13)$$

After choosing the third chasing technique, $xtchase, 3, i, k$ shows the updated location with BubbleNet development. The BubbleNet creation can be obtained by adding the weighted sum of differences among the past best location ($xtbest$) and the existing location of orcas (xti). The weight b defines the impact of BubbleNet formation on the movement and allows for coordination of the position for creating the virtual net. The differences between the historical best position and the existing positions for each orca are divided and summed by the overall number of orcas (Nn) to compute the BubbleNet force (Bt).

ii) BubbleNet position modifications

In encircling stage, orca location is modified according to BubbleNet formation, taking fitness function into account. The location updating equation is given below:

$$xtchase, i = xtchase, i \; if \; f(xtchase, i) < f(xti) \quad (14)$$

After integrating the BubbleNet formation ($xtchase, i$), if the fitness values of the location are superior to the fitness values of the existing location (xti), the location remains the same. This ensures that the orca maintains the position if BubbleNet formation does not result in an enhancement in fitness value.

$$xtchase, i = xti \; if \; f\,(xtchase, i) \geq f(xti) \quad (15)$$

After integrating BubbleNet development, if the fitness value of the location is equal or not superior to the fitness values of the existing location, then the location can be upgraded to that existing location. This prevents the orca from moving towards a lesser optimum location.

iii) Adaptive attack speed

During attacking stage, adaptive attack speed is established to change movement rapidity dynamically based on vicinity of the prey and the existing iteration. These facilities improve the probability of catching the prey and improve their attack strategy. $S(t)$, denotes the adaptive attack speed function and evaluates the correct attack speed according to factors including convergence criteria, distance to the prey, and prey movement. During the attacking phase, the velocity update for the orca is expressed as follows:

$$Vtattack, 1, i = \frac{(xt1+xt2+xt3+xt4)}{4} - xtchase, i * S(t) \quad (16)$$

$$Vtattack, 2, i = \frac{(xtchase,d1+xtchase,d2+xtchase,d3)}{3} - xti * S(t) \quad (17)$$

Now, velocity upgrade for orca in 1st and 2nd attacking strategies are, $Vtattack, 1, i$ and $Vtattack, 2, i$. According to the orca position, the updates are calculated and their chase target, considering the adaptive attack speed as (t). During the attacking phase, the updated location of the orca is defined as follows:

$$xtattack, i = xtchase, i + g1 * Vtattack, 1, i + g2 * Vtattack, 2, i \quad (18)$$

In Eq. (18), the upgrade place of the orcas is $xtattack, i$ considering the chase location, the velocity update, and the weighted $g1$ and $g2$. Both weights controlling the impact of the velocity update on the movement, enabling to finetune the attack strategy.

The fitness optimum is an important feature in SIOPA algorithm. An encoded performance has been organized to assess superior efficiency of candidate results. Currently, accuracy value is a main form used to project an FF.

4. RESULTS AND DISCUSSION

This section inspects MU detection outcomes of SIOPA-DLMUC approach tested on a dataset, generated by our own. Table 1 represents the details of the dataset. Indoor CRN attacks involve threats like spectrum sensing data falsification, where attackers manipulate sensing information to mislead network, and primary user emulation, where malicious devices impersonate authentic users to disrupt spectrum allocation. Sybil attacks include creating fake identities to gain undue control over spectrum resources, hindering network efficacy, whereas Jamming attacks are common indoors, intending to cause interference. Outdoors, spectrum misuse, primary user emulation, and eavesdropping on communication attacks remain a concern. Furthermore, attackers may exploit vulnerabilities in cross-technology integration, perform Denial of Service (DoS) attacks, and manipulate location information, imposing strong security systems and regulations to defend CRN performance and integrity. In this work, indoor and outdoor attacks are involved. We have generated a dataset comprising 25000 samples with five classes namely Byzantine attack, Jamming Attack, SSDF attack, Primary User Emulation (PUE) attack, and Normal. Each class holds a total of 5000 samples.

Table 1. Details on database

Classes	No. of Samples
Byzantine Attack	5000
Jamming Attack	5000
SSDF Attack	5000
PUE Attack	5000
Normal	5000
Total Samples	**25000**

The class labels are defined as follows:

•Byzantine attack occurs when certain nodes, including secondary users, intentionally provide conflicting or false information about spectrum availability. This deception disrupts efficient spectrum utilization, posing a significant threat to network reliability and security. Detecting and preventing Byzantine attacks is crucial for safeguarding Cognitive Radio Networks.

•A jamming attack in 5G Cognitive Radio involves the deliberate interference with radio signals, typically by secondary users, disrupting communication.

$$Fitness = \max(P) \quad (19)$$

$$P = \frac{TP}{TP + FP} \quad (20)$$

where, FP and TP imply false and true positive values

•Attackers generate high power signals exceeding expected levels or introduce signal variances to disrupt network operations. Detecting and mitigating jamming attacks is vital to maintain communication reliability in Cognitive Radio Networks.

•Spectrum Sensing Data Falsification (SSDF) is deliberate manipulation of spectrum sensing data in cognitive radio systems. It involves misreporting presence or nonappearance of primary users to disrupt spectrum allocation. Detecting and countering SSDF is essential for network reliability and security.

•In realm of 5G Cognitive Radio, Primary User Emulation (PUE) entails a deceptive practice where secondary users mimic primary users' signal behavior, potentially causing harmful interference. Attackers may imitate signal characteristics, posing a challenge for distinguishing between genuine and emulated primary users. Detecting PUE attacks is critical for preserving the integrity and performance of Cognitive Radio Networks.

•In the context of CRN in 5G, "normal" refers to the standard and expected behavior of nodes within the network. It signifies the absence of malicious activities like Byzantine attacks, jamming attacks, Primary User Emulation (PUE), or other deceptive actions “Normal” behavior includes legitimate spectrum sensing, communication, and network operations that follow established protocols and do not disrupt the efficient utilization of the radio spectrum.

This study employed a carefully crafted set of simulation parameters to generate a comprehensive dataset for research in the domain of 5G-assisted Cognitive Radio Networks. The parameters encompass various attack scenarios, including Byzantine Attacks, Jamming Attacks, Primary User Emulation (PUE) Attacks, and Spectrum Sensing Data Falsification (SSDF) Attacks, all operating within the 2.4 GHz frequency band. These attacks were executed with distinct modulation schemes, such as QPSK for Primary Users (PUs) and BPSK for Secondary Users (SUs). To ensure dataset's fidelity, the simulation considered critical factors like expected signal power, modulation schemes, and specific detection thresholds tailored to each attack type. By capturing the dynamics of malicious behaviors and their impact on the network, this dataset serves as a valuable resource for advancing research in the security and resilience of 5G Cognitive Radio Networks. The simulation settings of the attacks are given in Table 2.

Figure 4 shows confusion matrices attained by SIOPA-DLMUC technique at 80:20 and 70:30 of TR phase /TS phase. The simulated values reported effective recognition with all five classes.

Table 2. Simulation parameter setting

Attack Type	Parameter	Value
Byzantine Attack	Frequency Band	2.4 GHz
	Modulation Scheme	QPSK for PUs, BPSK for SUs
	Expected Signal Power (P_expected)	-70 dBm
	Expected Modulation Scheme (M_expected)	QPSK for PUs, BPSK for SUs
	Threshold for Byzantine Attack Detection	At least 20% of nodes provide conflicting information within 1 second
Jamming Attack	Frequency Band	2.4 GHz
	Modulation Scheme	QPSK for PUs, BPSK for SUs
	Expected Signal Power (P_expected)	-70 dBm
	Expected Modulation Scheme (M_expected)	QPSK for PUs, BPSK for SUs
	Threshold for Sudden Spike	P(t) > P_expected + 5 dB
	Threshold for High Variance	Variance > 10 dB
	Threshold for Sudden Increase in Nodes	N_actual > N_expected * 1.2 within 1 second
PUE Attacks	Frequency Band	2.4 GHz
	Modulation Scheme	QPSK for PUs, BPSK for SUs
	Maximum Transmission Power for SUs (P_max_SU)	-60 dBm
	Maximum Transmission Power for PUs (P_max_PU)	-30 dBm
	Threshold for PUE Attack Detection	Significant overlap in signal behavior between SUs and PUs
SSDF Attacks	Frequency Band	2.4 GHz
	Modulation Scheme	QPSK for PUs, BPSK for SUs
	Maximum Transmission Power for SUs (P_max_SU)	-60 dBm
	Maximum Transmission Power for PUs (P_max_PU)	-30 dBm
	Threshold for SSDF Attack Detection	Energy levels exceeding -40 dBm within a certain time window

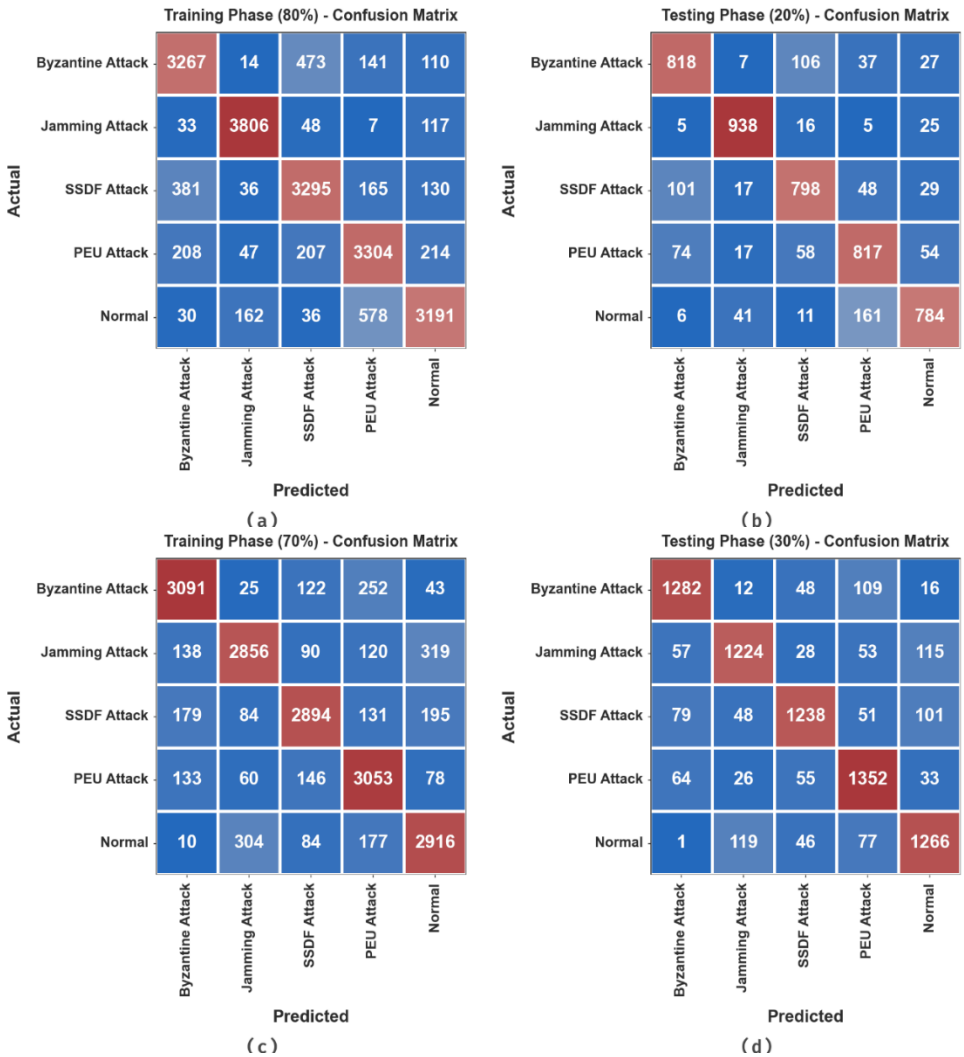

Figure 4. Confusion matrices of (a-c) TR phase of 80% and 70% and (b-d) TS phase of 20% and 30%

Table 3. MU recognition outcome of SIOPA-DLMUC method at 80:20 of TR phase/TS phase

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}	MCC
			TR Phase (80%)			
Byzantine Attack	93.05	83.36	81.57	82.46	88.75	78.13
Jamming Attack	97.68	93.63	94.89	94.25	96.63	92.80
SSDF Attack	92.62	81.18	82.23	81.70	88.73	77.08
PUE Attack	92.16	78.76	83.02	80.83	88.73	75.95
Normal	93.12	84.82	79.83	82.25	88.13	78.04
Average	**93.73**	**84.35**	**84.31**	**84.30**	**90.19**	**80.40**
			TS Phase (20%)			
Byzantine Attack	92.74	81.47	82.21	81.84	88.78	77.31
Jamming Attack	97.34	91.96	94.84	93.38	96.40	91.73
SSDF Attack	92.28	80.69	80.36	80.52	87.80	75.71
PUE Attack	90.92	76.50	80.10	78.26	86.90	72.55
Normal	92.92	85.31	78.17	81.58	87.39	77.32
Average	**93.24**	**83.19**	**83.14**	**83.12**	**89.45**	**78.93**

Table 4. MU detection outcome of SIOPA-DLMUC approach at 70:30 of TR phase/TS phase

Class	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}	AUC_{score}	MCC
			TR Phase (70%)			
Byzantine Attack	94.85	87.05	87.49	87.27	92.10	84.04
Jamming Attack	93.49	85.79	81.07	83.36	88.84	79.37
SSDF Attack	94.11	86.75	83.09	84.88	89.97	81.25
PUE Attack	93.73	81.78	87.98	84.77	91.57	80.92
Normal	93.09	82.12	83.53	82.82	89.50	78.49
Average	**93.85**	**84.70**	**84.63**	**84.62**	**90.39**	**80.81**
			TS Phase (30%)			
Byzantine Attack	94.85	86.45	87.39	86.92	92.03	83.71
Jamming Attack	93.89	85.65	82.87	84.24	89.73	80.47
SSDF Attack	93.92	87.49	81.61	84.45	89.33	80.75
PUE Attack	93.76	82.34	88.37	85.25	91.75	81.38
Normal	93.23	82.69	83.90	83.29	89.74	79.05
Average	**93.93**	**84.92**	**84.83**	**84.83**	**90.52**	**81.07**

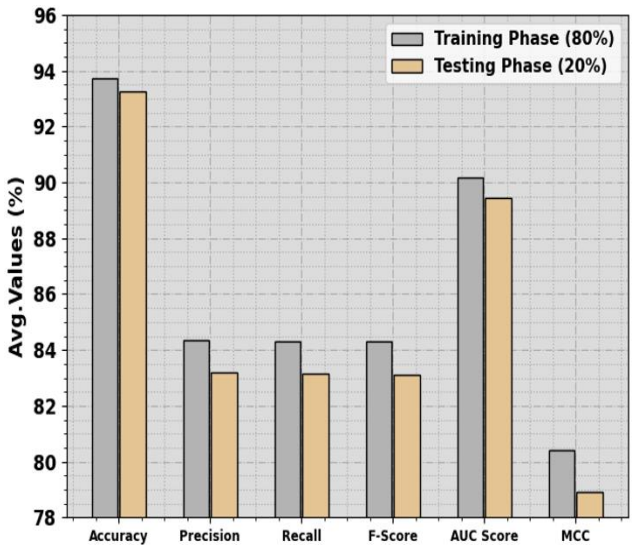

Figure 5. Average of SIOPA-DLMUC approach at 80:20 of TR phase/TS phase

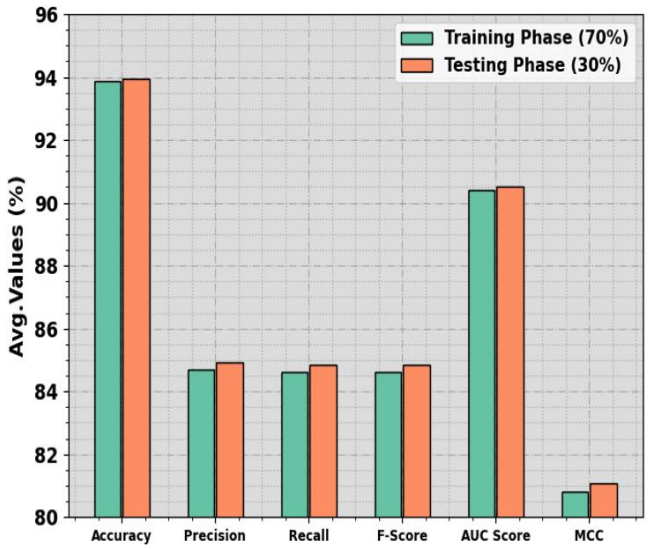

Figure 6. Average of SIOPA-DLMUC technique at 70:30 of TR phase/TS phase

In Table 3 and Figure 5, MU detection results of SIOPA-DLMUC model at 80:20 of TR Phase/TS Phase are illustrated. The simulated values indicate that SIOPA-DLMUC model attains enhanced performance under all five classes. With 80% of TR Phase, SIOPA-DLMUC method achieves an average $accu_y$ of 93.73%, $prec_n$ of 84.35%, $reca_l$ of 84.31%, F_{score} of 84.30%, AUC_{score} of 90.19%, and MCC of 80.40%. At the same time, based on 20 % of the TS Phase, SIOPA-DLMUC system attains an average $accu_y$ of 93.24%, $prec_n$ of 83.19%, $reca_l$ of 83.14%, F_{score} of 83.12%, AUC_{score} of 89.45%, and MCC of 78.93%.

In Table 4 and Figure 6, MU detection outcome of SIOPA-DLMUC model with 70:30 of TR Phase/TS Phase is demonstrated. The simulated values highlighted that SIOPA-DLMUC method achieves improved performance by all five classes. According to 70% of the TR Phase, the SIOPA-DLMUC methodology gets an average $accu_y$ of 93.85%, $prec_n$ of 84.70%, $reca_l$ of 84.63%, F_{score} of 84.62%,

AUC_{score} of 90.39%, and Mathew Correlation coefficient (MCC) of 80.81%. Simultaneously, with 30 % of TS Phase, SIOPA-DLMUC system attains an average $accu_y$ of 93.93%, $prec_n$ of 84.92%, $reca_l$ of 84.83%, F_{score} of 84.83%, AUC_{score} of 90.52%, and MCC of 81.07%.

To determine the performance of the SIOPA-DLMUC method with 70:30of TR Phase/TS Phase, TR and TS $accu_y$ curves are well-defined, as represented in Figure 7. TR and TS $accu_y$ curves reported performance of SIOPA-DLMUC model over various epochs. This figure provides important particulars about learning tasks and generalization abilities of SIOPA-DLMUC methodology. With a growth in epoch amount, it is observed that TR and TS $accu_y$ curves get upgraded. It is showed that SIOPA-DLMUC algorithm extents enriched testing accuracy can potentially recognize patterns in TR and TS data.

Figure 7. $Accu_y$ curve of SIOPA-DLMUC approach at 70:30 of TR phase/TS phase

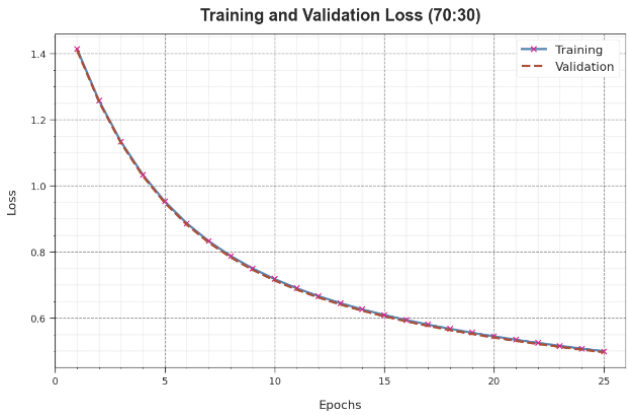

Figure 8. Loss curve of SIOPA-DLMUC approach at 70:30 of TR phase/TS phase

Figure 8 represents complete TR and TS loss values of SIOPA-DLMUC methodology with 70:30 of TR Phase /TS Phase over epochs. TR loss displays model loss gets decreased over epochs. Primarily, loss values become reduced as model adjusts weight to diminish predicted error on TR and TS data. The loss curves shows that extent to which the model fits training data. It is observed that TR and TS loss progressively diminished as well as defined that SIOPA-DLMUC technique efficiently learns patterns exhibited in TR and TS data. It is also remarked that SIOPA-DLMUC model modifies parameters for minimizing difference between real and predicted training labels.

The PR analysis of SIOPA-DLMUC methodology with 70:30 of TR Phase/TS Phase is described by scheming exactness beside recall as represented in Figure 9. The simulated values reported that SIOPA-DLMUC model acquires enhanced PR values with every 5 class. The figure exhibits that method learns for recognizing diverse classes. SIOPA-DLMUC technique gains enriched outcomes in detection of positive samples by reduced false positive.

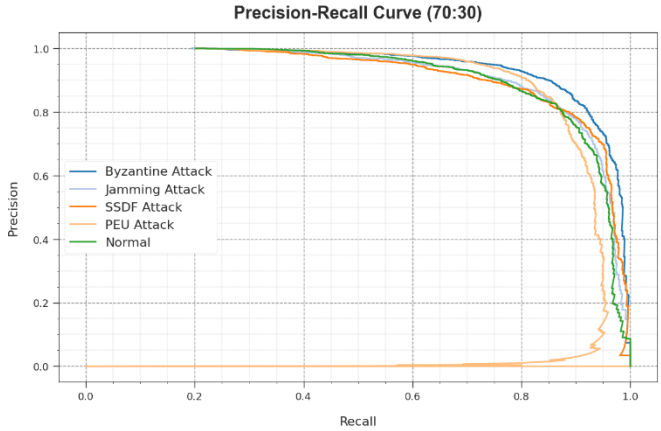

Figure 9. PR curve of SIOPA-DLMUC approach at 70:30 of TR phase/TS phase

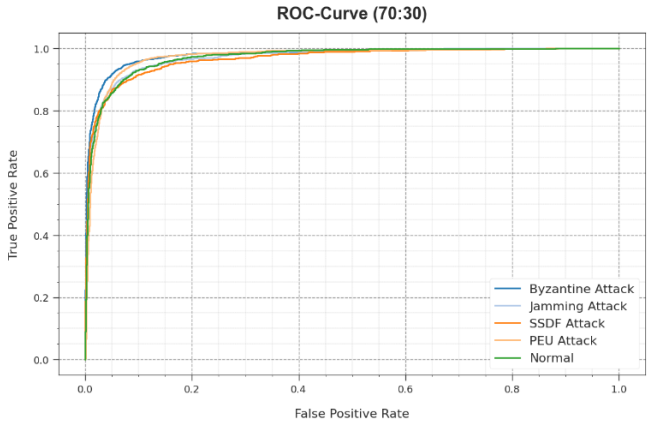

Figure 10. ROC curve of SIOPA-DLMUC approach at 70:30 of TR phase/TS phase

The ROC analysis offered by SIOPA-DLMUC system with 70:30 of TR Phase/TS Phase is showed in Figure 10, which has ability to differ class labels. The figure states respected visions into trade-off between TPR and FPR rates over dissimilar categorization thresholds as well as modifying epoch counts. It offers correct forecast result of SIOPA-DLMUC method on classifier of separate five classes.

The comparative results of SIOPA-DLMUC approach with current methods are made in Table 5 and Figure 11 [13]. The simulated values highlighted that SVM model reaches poor performance. Similarly, NB, stacking, and DBN techniques portrayed slightly improvised results. Meanwhile, LR model has resulted in near-optimal performance with $accu_y$, $prec_n$, and $reca_l$ of 93%, 82%, and 84% respectively. Finally, the SIOPA-DLMUC technique demonstrates maximum results over other models with higher $accu_y$, $prec_n$, and $reca_l$ of 93.93%, 84.92%, and 84.83% respectively. These results show that the SIOPA-DLMUC technique accomplishes improved performance on the MU detection process in the CRN.

Table 5. Comparative outcome of SIOPA-DLMUC method with current systems

Models	$Accu_y$	$Prec_n$	$Reca_l$
SVM Model	70.00	66.00	75.00
Logistic Regression	93.00	82.00	84.00
Naïve Bayes	92.00	84.00	84.00
Stacking Model	92.70	83.90	83.00
DBN Model	92.89	82.98	83.50
SIOPA-DLMUC	93.93	84.92	84.83

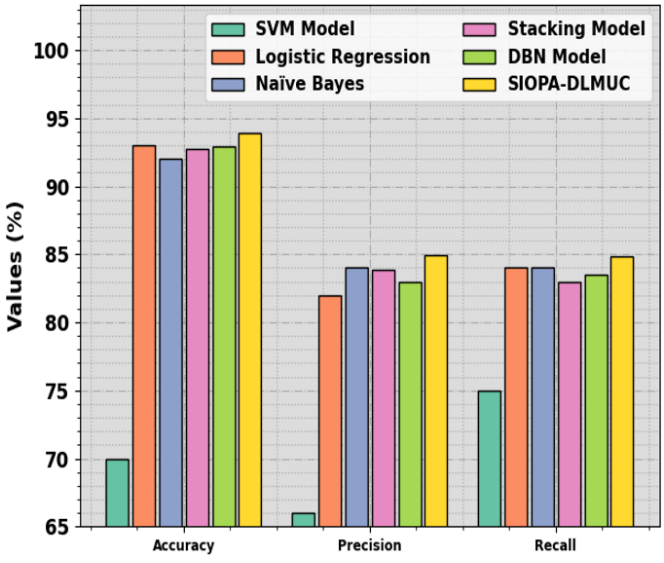

Figure 11. Comparative outcome of SIOPA-DLMUC approach with recent methods

5. CONCLUSION

In this study article, an automated SIOPA-DLMUC approach has been established for the MU detection process in the 5G assisted CRN. The chief goal of SIOPA-DLMUC method is to classify as well as detect occurrence of MUs in the CRN. To accomplish this, SIOPA-DLMUC approach follows 2-stage processes namely LSTM-based detection and SIOPA-based hyperparameter tuning. In this work, LSTM is utilized for analyzing temporal behaviour and communication patterns of users in CRN. To better outcome of LSTM system in MU detection process, SIOPA-DLMUC technique is used for optimal hyperparameter selection process. To examine solution of SIOPA-DLMUC approach, a complete set of simulations carried out on our database, comprising four kinds of attacks namely Byzantine Attacks, Jamming Attacks, Primary User Emulation (PUE) Attacks, and Spectrum Sensing Data Falsification (SSDF) Attacks alongside normal samples. An extensive result stated that an optimum outcome of the SIOPA-DLMUC technique based on other DL models. Ensuring the robustness of 5G-assisted Cognitive Radio Networks (CRNs) in face of evolving security challenges is of paramount importance. While simulations provide valuable insights and a controlled environment for testing security measures, transition to real-world deployment is a pivotal step in validating effectiveness of these security mechanisms. Future research could also focus on development of blockchain-based protocols and smart contracts tailored to unique requirements of CRNs in 5G, ensuring trust, transparency, and resilience against attacks.

REFERENCES

[1] Alqahtani, A.S., Changalasetty, S.B., Parthasarathy, P., Thota, L.S., Mubarakali, A. (2023). Effective spectrum sensing using cognitive radios in 5G and wireless body area networks. Computers and Electrical Engineering, 105: 108493. https://doi.org/10.1016/j.compeleceng.2022.108493

[2] Jain, A., Gupta, N., Sreenu, M. (2023). Blockchain based smart contract for cooperative spectrum sensing in cognitive radio networks for sustainable beyond 5G wireless communication. Green Technologies and Sustainability, 1(2): 100019. https://doi.org/10.1016/j.grets.2023.100019

[3] Bourebaa, F., Benmohammed, M. (2021). A Deep neural network model for malware detection. International Journal of Informatics and Applied Mathematics, 4(1): 1-14.

[4] Dewangan, N., Kumar, A., Patel, R.N. (2023). A framework for secure cooperative spectrum sensing based with blockchain and deep learning model in cognitive radio. In 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, pp. 1-6. https://doi.org/10.1109/ICECONF57129.2023.10083887

[5] Ray, K.S., Kusshwaha, R. (2021). Detection of malicious URLs using deep learning approach. In the" Essence" of Network Security: An End-to-End Panorama, pp. 189-212. https://doi.org/10.1007/978-981-15-9317-8_8

[6] Muñoz, E.C., Pedraza, G.C., Cubillos-Sánchez, R., Aponte-Moreno, A., Buitrago, M.E. (2023). PUE attack detection by using DNN and entropy in cooperative mobile cognitive radio networks. Future Internet, 15(6): 202. https://doi.org/10.3390/fi15060202

[7] Zhang, N., Tan, Y.A., Yang, C., Li, Y. (2021). Deep learning feature exploration for android malware detection. Applied Soft Computing, 102: 107069. https://doi.org/10.1016/j.asoc.2020.107069

[8] Liyakat, K.K.S. (2023). Detecting malicious nodes in IoT networks using machine learning and artificial neural networks. In 2023 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, pp. 1-5. https://doi.org/10.1109/ESCI56872.2023.10099544

[9] Imtiaz, S.I., ur Rehman, S., Javed, A.R., Jalil, Z., Liu, X., Alnumay, W.S. (2021). DeepAMD: Detection and identification of android malware using high-efficient deep artificial neural network. Future Generation Computer Systems, 115: 844-856. https://doi.org/10.1016/j.future.2020.10.008

[10] Yalçın, S. (2023). An artificial intelligence-based spectrum sensing methodology for LoRa and cognitive radio networks. International Journal of Communication Systems, 36(5): e5433. https://doi.org/10.1002/dac.5433

[11] Clement, J.C., 2023.GRU-SVM based threat detection in cognitive radio network. Sensors, 23(3): 1326. https://doi.org/10.3390/s23031326

[12] VasanthaReddy, R.M., Lingareddy, S.C. (2021). Detection and prevention of primary user emulation attack in cognitive radio networks using secure hash algorithm. International Journal of Intelligent Engineering & Systems, 14(2): 136-146.

https://doi.org/10.22266/ijies2021.0430.12
[13] Benazzouza, S., Ridouani, M., Salahdine, F., Hayar, A. (2022). A novel prediction model for malicious users detection and spectrum sensing based on stacking and deep learning. Sensors, 22(17): 6477. https://doi.org/10.3390/s22176477
[14] Paul, A., Choi, K. (2023). Joint spectrum sensing and D2D communications in cognitive radio networks using clustering and deep learning strategies under SSDF attacks. Ad Hoc Networks, 143: 103116. https://doi.org/10.1016/j.adhoc.2023.103116
[15] Sapavath, N.N., Muhati, E., Rawat, D.B. (2021). Prediction and detection of cyberattacks using AI model in virtualized wireless networks. In 2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Washington, DC, USA, pp. 97-102. https://doi.org/10.1109/CSCloud-EdgeCom52276.2021.00027
[16] Ajay, V.P., Nesasudha, M. (2022). Detection of attackers in cognitive radio network using optimized neural networks. Intelligent Automation & Soft Computing, 34(1): 193-204. https://doi.org/10.32604/iasc.2022.024839
[17] Zhang, H., Yang, J., Chen, J., Gao, Y. (2023). Spectrum usage anomaly detection from sub-sampled data stream via deep neural network. Journal of Communications and Information Networks, 8(1): 13-23. https://doi.org/10.23919/JCIN.2023.10087244
[18] Brinda, V., Bhuvaneshwari, M. (2022). Identifying malicious secondary user presence within primary user range in cognitive radio networks. Wireless Personal Communications, 122(3): 2687-2699. https://doi.org/10.1007/s11277-021-09025-7
[19] Siva, R., S, K., Hariharan, B., Premkumar, N. (2024). Automatic software bug prediction using adaptive golden eagle optimizer with deep learning. Multimedia Tools and Applications, 83(1): 1261-1281. https://doi.org/10.1007/s11042-023-16666-2
[20] Jebur, R.S., Zabil, M.H.B.M., Hammood, D.A., Cheng, L.K., Al-Naji, A. (2023). Image denoising using hybrid deep learning approach and self-improved orca predation algorithm. Technologies, 11(4): 111. https://doi.org/10.3390/technologies11040111