iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VII **Month of publication:** July 2025

DOI: https://doi.org/10.22214/ijraset.2025.72926

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

A Deep Neural Network Assisted Physical Layer Security Mechanism for Wireless Networks

Vinit Kumar Singh[1], Dr. Ranu Pandey[2]
[1]*Research Scholar, Department of Cyber Forensics, Shri Rawatpura Sarkar University, Raipur, Chhattisgarh*
[2]*Associate Professor, Department of Computer Science and Engineering, Shri Rawatpura Sarkar University, Raipur, Chhattisgarh*

Abstract: ***The physical layer in wireless systems is inherently susceptible to eavesdropping, jamming, spoofing, and signal injection attacks because wireless signals propagate through open space. Unlike wired networks, where physical access is more controlled, wireless communication can be intercepted by any nearby device. Attackers can exploit features such as channel reciprocity, power control, or modulation characteristics to compromise communications. These vulnerabilities make it imperative to secure the physical layer, especially in applications involving sensitive data like military, healthcare, and IoT-based services, which rely primarily on wireless data transmission. This paper presents a machine learning assisted security aware channel assignment protocol against possible adversarial eavesdropping attacks. The ML parameters such as gradient, iterations to convergence and cost function have been computed and presented. The final error rate with and without the proposed system under adversarial attacks is also presented. It can be observed that the proposed approach is close to the no adversarial attack condition clearly indicating the efficacy of the approach to proactively thwart potential attacks. The error rates are also significantly lower than existing approach in the domain. Additionally, to enhance the QoS of the system, a handoff mechanism is also proposed in conjugation with equalization. The metrics for evaluation of the performance of the system are the BER, scatter and MSE.***

Keywords: Physical Layer Security, Wireless Networks, Machine Learning, Channel Assignment, BER, MSE, Accuracy.

I. INTRODUCTION

Network security and authentication paradigms are undergoing a metamorphosis with the advent of deep learning and quantum computing, especially with the possibility of implementing machine learning algorithms on quantum computers which may lead to breaking of existing encryption and security algorithms [1]. This lead to see the security of networks as a three layered approach based on the OSI model typically introducing security patches at:

- Physical layer
- Network Layer
- Application Layer

Physical layer security is one of the most crucial aspect of security in wireless networks. Due to continued sharing of resources, wireless networks often come under security attacks, most common of which are eavesdropping attacks. In the case of eavesdropping attacks, deliberately designed random eavesdropping data is added to the channel. These eavesdropping along with noise result in packet losses and low throughput, degrading the overall performance of the cognitive network. In this work, a security aware eavesdropping rejection mechanism is proposed which detects suspicious signals in the channel frequency response and employs discrete equalization to recover transmitted data [2]. However, the inherent characteristics of wireless communication, such as open transmission medium and mobility, introduce significant security challenges. Ensuring the security of wireless networks is crucial to protect sensitive information, maintain privacy, and ensure the reliable operation of network services. This essay explores the primary security challenges faced by wireless networks, including threats, vulnerabilities, and potential countermeasures [3].

Channel assignment in wireless networks involves selecting the appropriate frequency channels for communication to minimize interference and optimize network performance. Traditional channel assignment strategies primarily focus on factors such as bandwidth efficiency and signal strength [4]. However, as cyber threats evolve, it is essential to incorporate security considerations into channel assignment. Security-aware channel assignment addresses potential vulnerabilities and mitigates risks such as eavesdropping, jamming, and unauthorized access [5].

Wireless networks face a variety of security threats that can compromise communication integrity and confidentiality. Eavesdropping involves intercepting wireless communications to gain unauthorized access to sensitive information [6].

©IJRASET: All Rights are Reserved

Jamming attacks disrupt network operations by overwhelming channels with interference. Unauthorized access and man-in-the-middle attacks exploit weak authentication mechanisms to hijack communications. Security-aware channel assignment aims to counter these threats by considering security metrics in the channel selection process [7]. Thus, future research is focussing on developing lightweight, efficient algorithms for real-time security-aware channel assignment. Advances in artificial intelligence and distributed computing can enhance the adaptability and scalability of these solutions [8]. Additionally, collaborative frameworks that involve cross-layer security measures and industry standards can ensure comprehensive protection for wireless networks.

II. THE OSI MODEL AND PHYSICAL LAYER SECURITY

One of the fundamental security challenges in wireless networks is the open nature of the transmission medium. While traditional security mechanisms are implemented at higher OSI layers (such as encryption at the application or transport layer), Physical Layer Security provides first-line defense against unauthorized access by leveraging the inherent randomness and characteristics of the wireless channel. PLS can work in tandem with higher-layer security protocols or operate independently in resource-constrained environments. This layered security approach is more robust and flexible, especially for devices that cannot handle computationally expensive cryptographic algorithms [9].

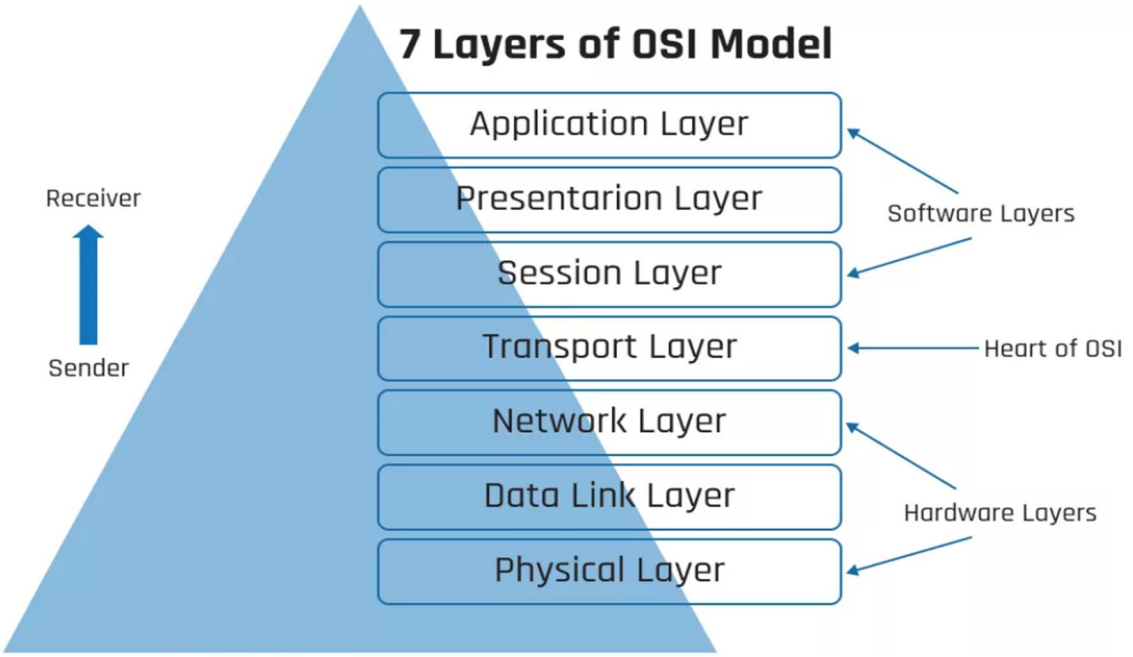


Fig.1 The OSI Model

Figure 1 depicts the OSI model [10].

OSI, or Open Systems Interconnection Model, is a conceptual model used to describe the functioning of a networking system. Developed by the ISO (International Organization for Standardization) in 1984, it is used to standardize network design and equipment manufacturing principles. This means diverse technologies can communicate seamlessly using standard rules of communication and protocols. Until the OSI model was launched, network architecture lacked the protocols for effective data communication and design infrastructure. This made installing, configuring, and setting up new equipment in existing networks challenging [11].

Smart cognitive wireless networks represent the next evolution in wireless communication, leveraging artificial intelligence (AI) and machine learning (ML) to dynamically manage spectrum usage and optimize network performance. These networks are designed to be adaptive, learning from the environment to make intelligent decisions about spectrum access . However, their advanced capabilities also introduce new security challenges. Attack avoidance is critical in ensuring the reliability and integrity of these networks.

The major characteristics of cognitive wireless are given as [12]:

1) Cognitive ability: It is the ability of Cognitive Systems to sense or catch the data from the radio surroundings of the radio technology. It can be said that cognitive radio constantly observes nature, orients itself, makes plans, decides, and then acts.

2) Reconfigurability: It is continuously adapting to the changes in the spectrum that change the properties of the channel. Thus it can be said that it is the utilization of the channel state information. (frequency, transmission power, modulation scheme, communication protocol) of radio [13].

Spectrum sensing is a fundamental task in cognitive wireless networks, enabling devices to detect available frequency bands and avoid interference with primary users. Traditional methods often struggle with accuracy and reliability, especially in low signal-to-noise ratio environments. Machine learning models, such as supervised learning (e.g., support vector machines, k-nearest neighbors) and unsupervised learning (e.g., clustering algorithms), have been employed to enhance spectrum sensing [14]. These models can learn from historical data to identify patterns and anomalies, improving the detection of vacant channels and reducing false alarms. The open and adaptive nature of CWNs introduces various security challenges, such as spectrum sensing data falsification and denial of service attacks. Machine learning models play a critical role in enhancing network security. Anomaly detection algorithms, including clustering and neural networks, can identify suspicious behavior and detect attacks in real-time. Moreover, ML-based intrusion detection systems (IDS) can analyze network traffic patterns to detect and mitigate malicious activities. By continuously learning and adapting to new threats, these models help maintain the integrity and reliability of cognitive wireless networks [15].

While ML models offer numerous benefits for cognitive wireless networks, several challenges remain [16]. These include the need for large labeled datasets, computational complexity, and the risk of model overfitting. Additionally, the dynamic and unpredictable nature of wireless environments poses challenges for the generalization and adaptability of ML models. Future research is likely to focus on developing lightweight and adaptive ML algorithms, enhancing transfer learning and federated learning techniques, and addressing ethical considerations such as privacy and fairness [17].

III. ADVERSERIAL EAVESDROPPING

Eavesdropping are the most common form of attack for cognitive radio mehanisms where the attacker tries to jam the spectrum in order to deny access with high accuracy. This can be categorized in 3 cases:

1) Low eavesdropping

2) Moderate eavesdropping

3) High eavesdropping

The eavesdropping activity changes the channel response of system from an ideal nature to non-ideal natue. The eavesdropping activity can be gauged based on the channel state information (CSI) of the system. Howeber there are some challenges in utilizing the CSI. Main Challenges faced in Spectrum Sensing in Cognitive Radio Systems [18]:

a) Wireless channels change randomly over time, therefore sensing wireless channels before they change is tough [19].

b) Determining eavesdropping activity may be tough due to the addition of noise.

c) Due to addition of noise in the transmitted signal, detection of spectrum holes may be practically tough [20]

d) Due to dynamic spectrum allocation, there exists a chance of ‘Spectrum Overlap’ causing interference between users [21].

e) Designing cognitive radio systems to perform error free in real time may be complex to design i.e. reduced throughput of the system. (bits/sec).

Predictive modeling uses historical data to forecast future network conditions and user behavior. In CWNs, predictive models, such as time series analysis and regression models, can predict spectrum availability, traffic load, and user mobility patterns. These predictions enable proactive network management, allowing cognitive radios to anticipate and adapt to changes before they occur. This proactive approach enhances network efficiency, reduces latency, and improves user experience [22].

IV. ML ASSISTED CHANNEL ASSIGNMENT

Machine learning plays a pivotal role in detecting and mitigating attacks in cognitive wireless networks. ML-based intrusion detection systems can analyze vast amounts of network data to identify suspicious patterns and anomalies [23]. Techniques such as supervised learning, unsupervised learning, and deep learning can be applied to develop models that distinguish between normal and malicious behavior. Continual learning algorithms can update these models in real-time, adapting to new threats and minimizing false positives.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

Spectrum sensing is crucial for cognitive radios to detect available channels and avoid interference with primary users. However, this process is vulnerable to attacks such as primary user emulation (PUE), where an attacker mimics a primary user to deceive cognitive radios [24]. Another threat is spectrum sensing data falsification (SSDF), where attackers feed false data into the network. To avoid these attacks, robust spectrum sensing techniques, such as collaborative sensing and machine learning-based anomaly detection, can be employed. These methods enhance the reliability of sensing by cross-verifying data from multiple sources and identifying abnormal patterns [25]

Collaboration among devices and network entities can enhance security in cognitive wireless networks. By sharing threat intelligence and cooperating in defense strategies, the network can respond more effectively to attacks. Collaborative approaches, such as cooperative spectrum sensing and distributed intrusion detection, leverage the collective capabilities of multiple devices to improve security. Trust management frameworks can be implemented to ensure that only reliable and trustworthy nodes participate in collaborative activities [26].

The security aware channel assignment algorithm is mathematically expressed as:

Algorithm

1. Generate Random binary data packets.

2. Design noisy channel condition as:

$$N(f) = \frac{K}{2} \forall f$$

3. Simulate Attack Conditions under low and moderate magnitudes.

4. Design ML Model and train it with:

Pilot Tx Bits

Received Rx Bits

Time Samples

SINR

5.Define maximum number of iterations as $maxitr$.

6. Define least squares (LS) cost function to be minimized as:

$$f_{cost} = \underbrace{min}_{maxitr} \quad \frac{1}{n}\sum_{i=1}^{n}(t_i - \hat{t}_i)^2$$

7. Design a deep neural network and initialize weights randomly.

for i=1:maxitr,

{

Update weights as:

$$w_{i+1} = w_i - \alpha \nabla f_{cost}(w_i) - \left[\begin{bmatrix} \frac{\partial^2 e_1}{\partial w_1^2} & \cdots & \frac{\partial^2 e_1}{\partial w_m^2} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 e_n}{\partial w_1^2} & \cdots & \frac{\partial^2 e_n}{\partial w_m^2} \end{bmatrix} * \begin{bmatrix} \frac{\partial^2 e_1}{\partial w_1^2} & \cdots & \frac{\partial^2 e_1}{\partial w_m^2} \\ \vdots & \ddots & \vdots \\ \frac{\partial^2 e_n}{\partial w_1^2} & \cdots & \frac{\partial^2 e_n}{\partial w_m^2} \end{bmatrix}^T + \alpha I \right]_i^{-1} * (t_i - \hat{t}_i)$$

}

8.: if ($i == maxitr$ *or* f_{cost} *stabilizes over k-fold, validation)*

{

Truncate training

else

Update weights

}

9.Obtain channel state information (CSI).

10. Leverage CSI to choose bandwidth with secure channel assignment.

11. Compare error rate for no attack, low attack an moderate to high attack scenarios to validate results.

©IJRASET: All Rights are Reserved

$H(freg)$ represents the channel frequency response.
$f(freq)$ denotes a function of frequency.

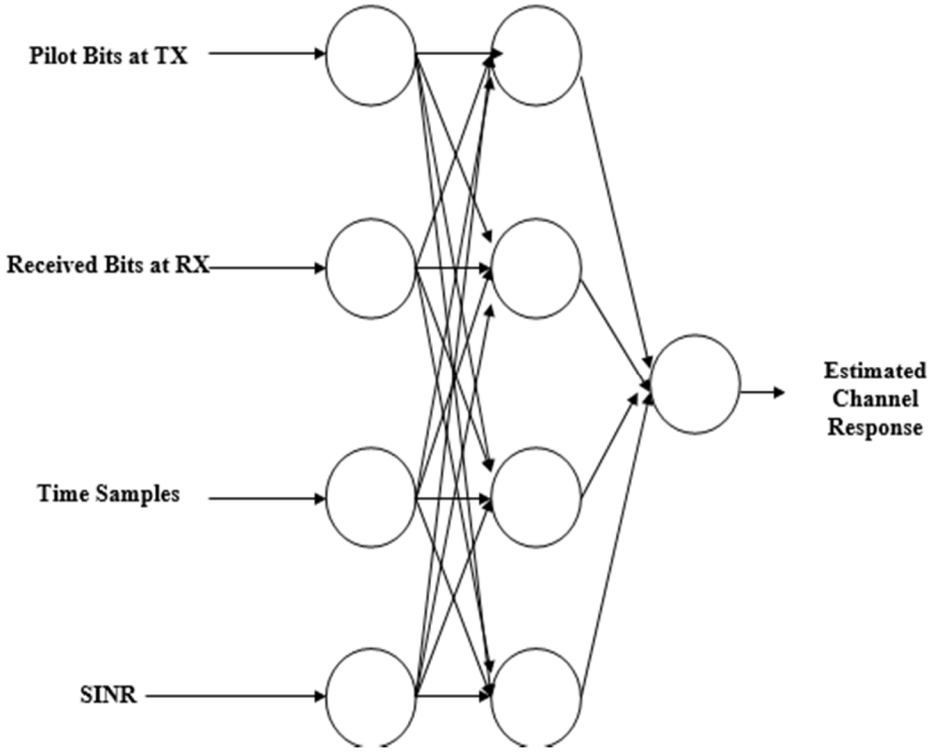


Fig.2 System Model

Figure 2 depicts the system model to estimate attacks proactively. The chances for a false alarm occur when there is collision present but the CSI suggest that collision is absent or vice versa. The chances of false alarm increase when there is actual addition of noise in the desired spectrum. It is noteworthy that such noise effects may lead to a false interpretation that there is collision noise being injected in the signal spectrum and it is the act of eavesdropping by the adversary. This however is not true and leads to misleading and inaccurate results. The effect can be summarized as follows:
Let the threshold for collision to be present by 'T'
If $h(t) > T; Collision\ presnet$
However,
If $h(t) + n(t) > T$ holds true;

Then there is a clear chance of false alarm often computed as the probability of false alarm of collision threat. Security-aware channel assignment is vital for protecting wireless networks against evolving cyber threats while maintaining optimal performance. By integrating security considerations into channel selection processes, wireless networks can achieve enhanced security, improved performance, resilience, and user trust [27]
Based on the model presented in figure 2, a handoff or handover mechanism can be initiated among orthogonal multiple access and its non-orthogonal counterpart under limited secure bandwidth conditions. The BER can be chosen as the evaluation metric for initiating handover [28].
While receiving the complex DataStream at the receiving end, let the composite binary data stream for the wireless network be designated as $S_{composite}(t)$, Orthogonal Access as O-ACCESS and Non-Orthogonal Access as NO-ACCESS, then:

$$S_i = sign\{real[S_{composite}(t)]\}$$

$$S_q = sign\{real[S_{composite}(t)]\}$$

Here,
I represents the in-phase component
To, initiate handover, the following condition can be used:
if $(BER_{NO-Access} < BER_{O-ACCESS})$
{
Choose NO-ACCESS as the transmission technique
else
{
Fall back to O-ACCESS
}

V. RESULTS

The results have been obtained using random data generation. The results have been presented next.

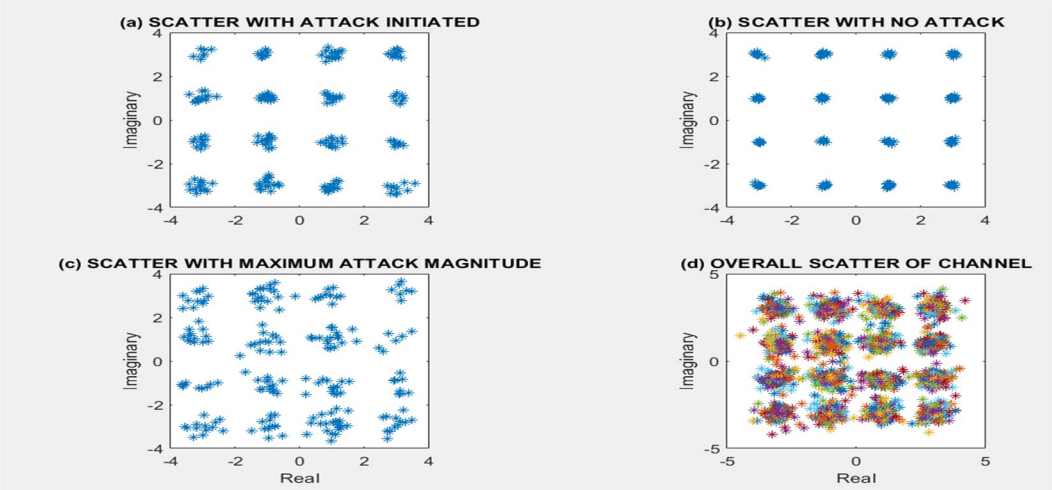


Fig.3 Scatter Plots Under Conditions of Attack

Figure 3 depicts the scatter for no attack, initial attack, maximum attack and overall scatter conditions.

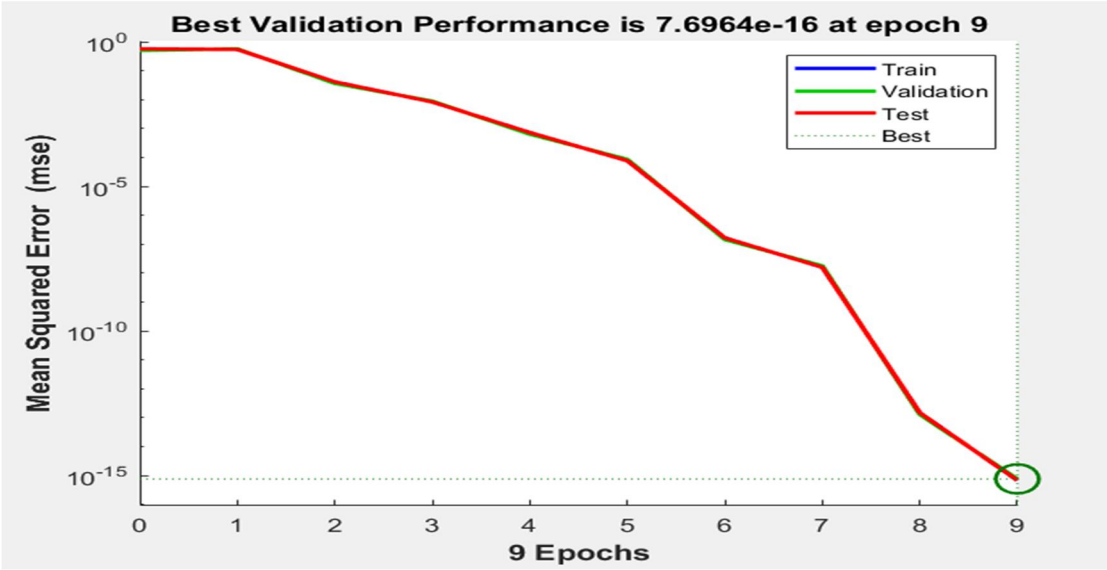


Fig.4 Convergence of ML Model

From figure 4, it can be observed that the deep neural network model attains convergence at 9 iterations with the MSE being $7.69 * 10^{-16}$

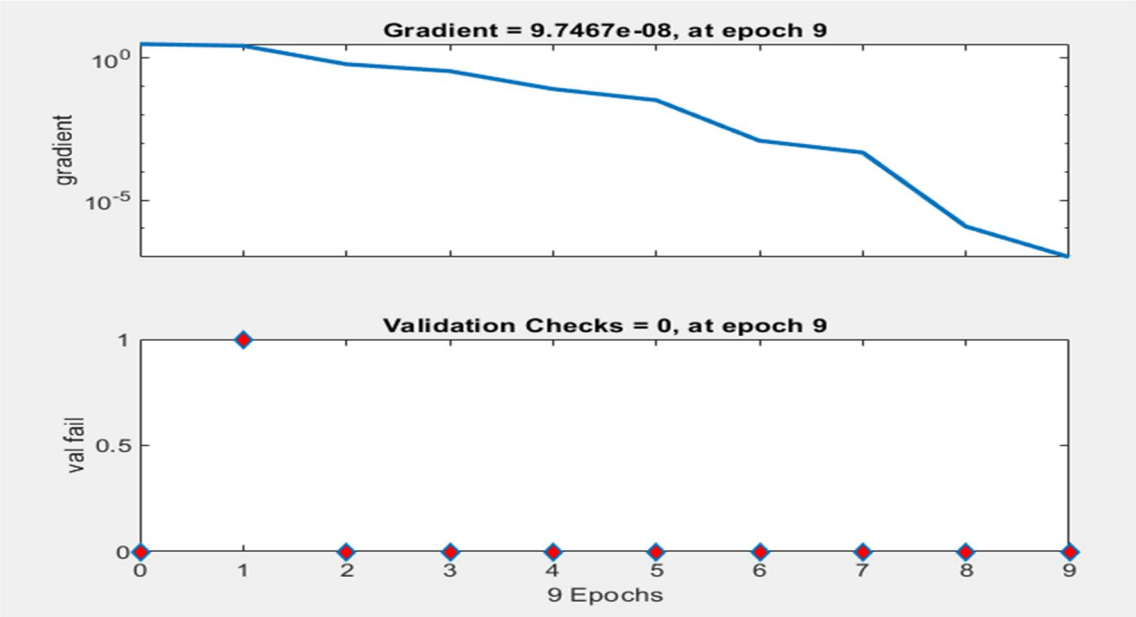


Fig.5 Gradient and Validation Checks for ML Model

From figure 5, it can be observed that the deep neural network model attains gradient of $9.7467 * 10^{-8}$ at 9 iterations.

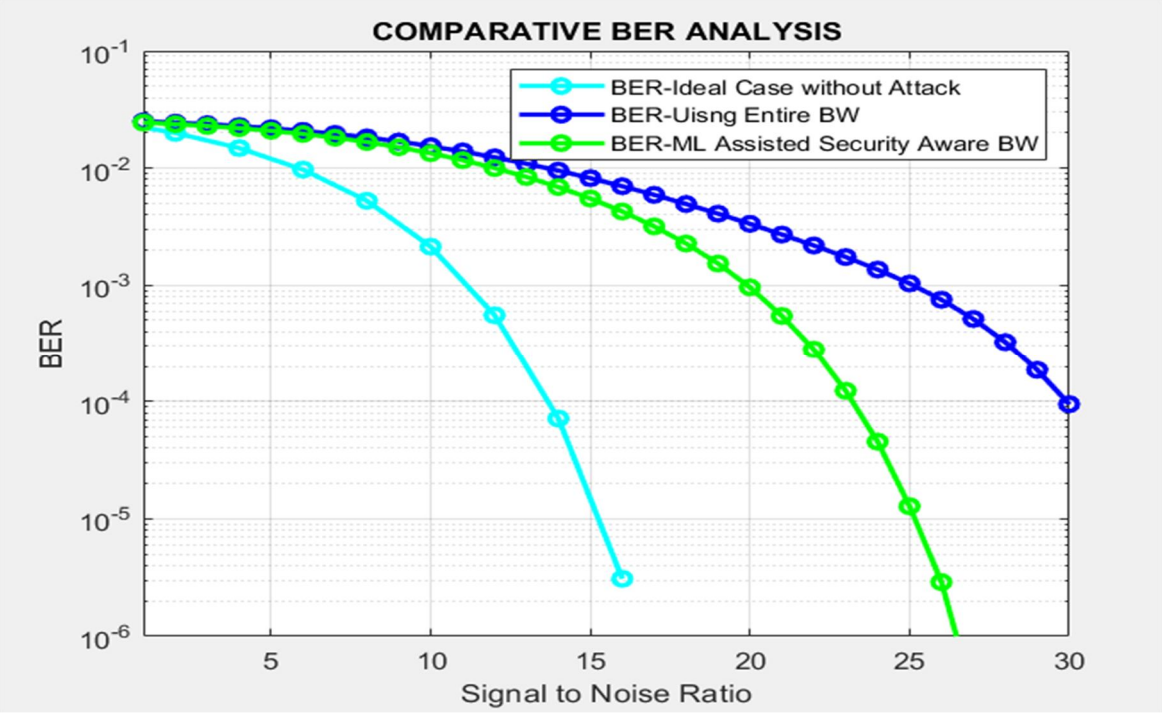


Fig.6 Error Rates for Different Conditions

Figure 6 depicts the BER of the proposed system under idea no attack condition, BER utilizing the entire bandwidth and the ML assisted Bandwidth of the system.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

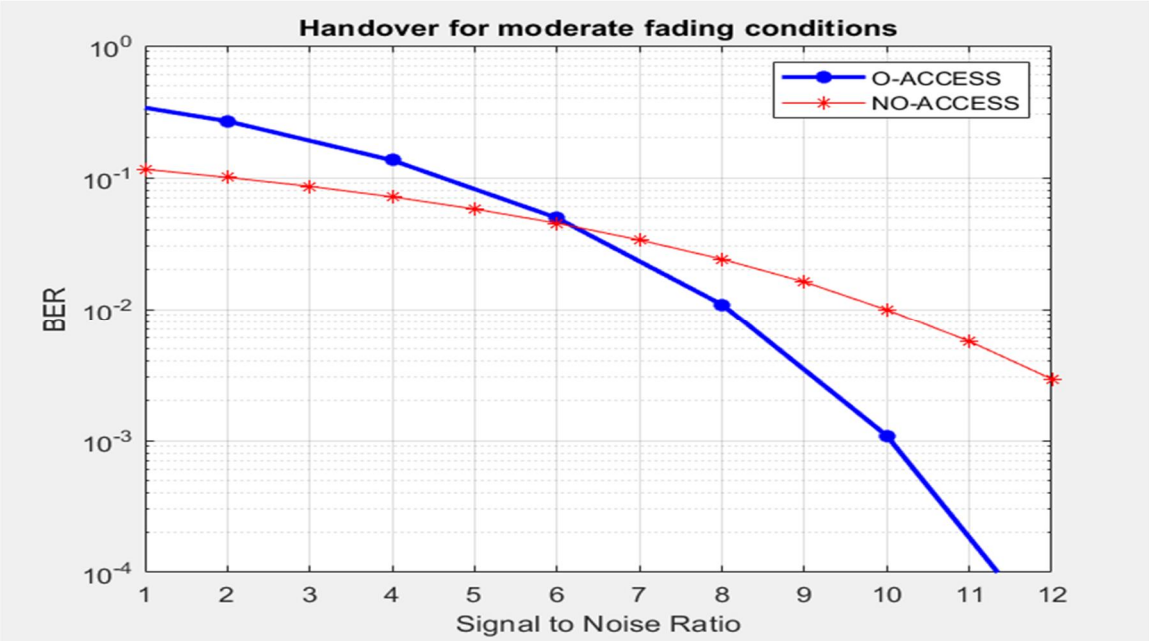


Fig.7 Error Rates for Handoff

Figure 7 depicts the handoff BER under moderate fading conditions for the system.

It can be observed from the previous results that the system designed in this approach emulates a real life scenario of varying adversarial attacks on the bandwidth for data transmission for the network. Moreover, the scatter plot of the network maps the levels of attack with the channel scatter. The performance of the machine learning model can be seen to attain quick convergence with low MSE values. Moreover, there are no resets in the validation phase. The error rate for the proposed system almost reaches 10^{-6} thereby indicating high accuracy for the system. The handover or handoff BER for the system reaches 10^{-4} A summary of the results is presented in table I.

Table I.
Summary of Results

S.No	Parameter	Value
1	Data generation	Random
2	Carries per packet	32
3	Channel	0.3
4	Iterations to convergence	Gaussian
5	Resets	0
6	BER reached	10^{-6}
7	Error Rate of Previous Work [29]	10^{-4}
8	Error Outage of Previous Work [30]	10^{-3}
9	Handoff BER	10^{-4}
10	BER at Handoff Previous Work [31]	10^{-3}

The results clearly indicate that the proposed ML assisted security framework not only introduces proactive security but also improves upon the system QoS by attaining very low error rates. The BER of the system can be seen to be significantly lesser compared to existing work in the domain.

VI. CONCLUSION

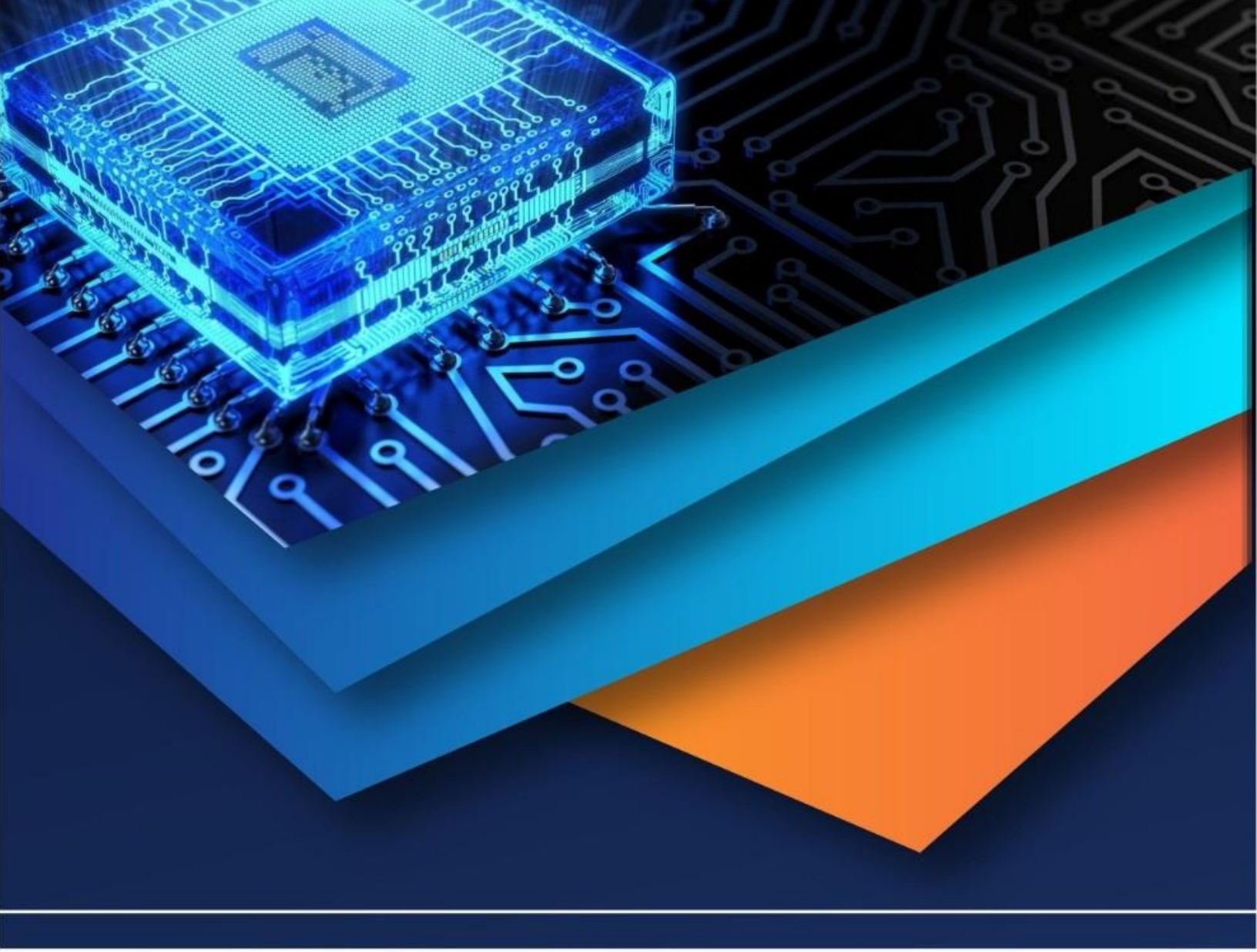
It can be concluded that Physical Layer Security is an essential aspect in the context of wireless networks, offering a foundational and complementary layer of protection against emerging threats. By capitalizing on the unique characteristics of wireless channels, PLS provides efficient and robust security, particularly in environments where traditional methods fall short. As wireless communication continues to underpin critical applications, the importance of integrating physical layer security across network design and implementation becomes not only beneficial but imperative. The ability of ML models to learn from data and adapt to changing environments makes them indispensable for the efficient and reliable operation of CWNs. As research and technology continue to advance, the integration of more sophisticated ML techniques will further enhance the capabilities and resilience of cognitive wireless networks, paving the way for smarter and more adaptive wireless communication systems. The proposed approach uses a machine learning based security aware channel assignment protocol for thwarting potential adversarial attacks. The proposed approach attains fast convergence at low BER rates, thereby rendering high improved security. Additionally, the handoff also improves the QoS of the system under variable channel conditions encountering attacks.

REFERENCES

[1] SK Singh, S Kumar, A Chhabra, A Sharma, “Advancements in secure quantum communication and robust key distribution techniques for cybersecurity applications”, Cyber Security and Applications, Elsevier 2025, 100089.
[2] K. St. Germain and F. Kragh, “Physical-Layer Authentication Using Channel State Information and Machine Learning,” IEEE, Jun. 2020.
[3] A. Senigagliesi, L. Baldi and E. Gambi, “Performance of Statistical and Machine Learning Techniques for Physical Layer Authentication,” arXiv, 2020.
[4] A. Albehadili et al., “Machine Learning-Based PHY-Authentication for Mobile OFDM Transceivers,” in Proc. IEEE VTC 2020-Fall, 2020.
[5] G. Gao, N. Ni, D. Feng, X. Jing and Y. Cao, “Physical Layer Authentication Under Intelligent Spoofing in Wireless Sensor Networks,” Signal Processing, vol. 166, 2020.
[6] L. Liao et al., “Multiuser Physical Layer Authentication in Internet of Things with Data Augmentation,” IEEE Internet of Things J., vol. 7, no. 3, pp. 2077–2088, Mar. 2020.
[7] H. Fang, X. Wang, Z. Xiao and L. Hanzo, “Autonomous Collaborative Authentication with Privacy Preservation in 6G: From Homogeneity to Heterogeneity,” IEEE Network, vol. 36, no. 6, pp. 28–36, Jul. 2022.
[8] R. Xie et al., “A Generalizable Model-and-Data Driven Approach for Open-Set RFF Authentication,” IEEE Trans. Inf. Forensics Security, vol. 16, pp. 4435–4450, Aug. 2021.
[9] A Soni, R Upadhyay, A Jain “Internet of Things and wireless physical layer security: A survey”, Computer Communication, Networking and Internet Security, Springer 2017, pp.115-123.
[10] https://certera.com/blog/what-is-the-osi-model-layers-benefits-and-applications/
[11] S. Sullivan, A. Brighente, S. A. P. Kumar and M. Conti, "5G Security Challenges and Solutions: A Review by OSI Layers," in IEEE Access, vol. 9, pp. 116294-116314, 2021
[12] X. Zeng, C. Wang and Z. Li, “CVCA: A Complex-Valued Classifiable Autoencoder for mmWave Massive MIMO Physical Layer Authentication,” presented at IEEE INFOCOM Workshops, 2023
[13] AA Sharifi, M Sharifi, MJM Niya, “Secure cooperative spectrum sensing under primary user emulation attack in cognitive radio networks: Attack-aware threshold selection approach”, vol.70, issue.1, Elsevier 2020.
[14] Syed Hashim Raza Bukhari ,Sajid Siraj,Mubashir Husain Rehmani,“ NS-2 based simulation framework for cognitive radio sensor networks”, SPRINGER 2019/.
[15] K. J. Prasanna Venkatesan ,V. Vijayarangan, “Secure and reliable routing in cognitive radio networks”, SPRINGER 2018.
[16] K Gai ,Meikang Qiu ,Hui Zhao, “Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data”,IEEE 2017.
[17] Ju Ren ,Yaoxue Zhang ,Qiang Ye , Kan Yang ; Kuan Zhang ,Xuemin Sherman Shen,” Exploiting Secure and Energy-Efficient Collaborative Spectrum Sensing for Cognitive Radio Sensor Networks”, IEEE 2016.
[18] R.K. Sharma ;,Danda B. Rawat,” Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey”,IEEE
[19] A. Khamaiseh, I. Alsmadi, and A. Al-Alaj, “Deceiving Machine Learning-based Saturation Attack Detection Systems in SDN,” in Proc. IEEE NFV-SDN, 2020.
[20] M. Assis, L. F. Carvalho, J. Lloret, and M. L. Proença Jr., “A GRU Deep Learning System Against Attacks in Software Defined Networks,” J. Network and Computer Applications, vol. 177, p. 102942, 2021.
[21] J. Bhayo et al., “A Time-Efficient Approach Toward DDoS Attack Detection in IoT Network Using SDN,” IEEE Internet of Things J., vol. 9, no. 5, pp. 3612–3630, Mar. 2022.
[22] A. Bahashwan, M. Anbar, S. Manickam, T. Al-Amiedy, M. Aladaileh, and I. H. Hasbullah, “A Systematic Literature Review on Machine Learning and Deep Learning Approaches for Detecting DDoS Attacks in Software-Defined Networking,” Sensors, vol. 23, no. 9, p. 4441, May 2023. ijisae.org.
[23] N. Niknami and J. Wu, “Advanced ML/DL-Based Intrusion Detection Systems for Software-Defined Networks, in Network Security Empowered by Artificial Intelligence, Y. Chen et al., Eds., Adv. in Inf. Security, vol. 107, Springer, Cham, pp. 59-84, Feb.2024.
[24] C. Zhao et al., "Generative AI for Secure Physical Layer Communications: A Survey," in IEEE Transactions on Cognitive Communications and Networking, vol. 11, no. 1, pp. 3-26, Feb. 2024.
[25] B. Ozpoyraz, A. T. Dogukan, Y. Gevez, U. Altun and E. Basar, "Deep Learning-Aided 6G Wireless Networks: A Comprehensive Survey of Revolutionary PHY Architectures," in IEEE Open Journal of the Communications Society, vol. 3, pp. 1749-1809, 2022
[26] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, “DDoSNet: A Deep-Learning Model for Detecting Network Attacks,” in Proc. IEEE 21st WoWMoM, Aug. 2020

[27] N. Abuzainab, M. Alrabeiah, A. Alkhateeb and Y. E. Sagduyu, "Deep Learning for THz Drones with Flying Intelligent Surfaces: Beam and Handoff Prediction," 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 2021, pp. 1-6.
[28] S. Alraih, R. Nordin, A. Abu-Samah, I. Shayea and N. F. Abdullah, "A Survey on Handover Optimization in Beyond 5G Mobile Networks: Challenges and Solutions," in IEEE Access, vol. 11, pp. 59317-59345, 2023
[29] Ara and B. Kelley, "Physical Layer Security for 6G: Toward Achieving Intelligent Native Security at Layer-1," in IEEE Access, 2024, vol. 12, pp. 82800-82824.
[30] T. N. Nguyen et al., "Cooperative Satellite-Terrestrial Networks With Imperfect CSI and Multiple Jammers: Performance Analysis and Deep Learning Evaluation," in IEEE Systems Journal, vol. 18, no. 4, pp. 2062-2073, Dec. 2024,
[31] A. Tusha, S. Doğan and H. Arslan, "A Hybrid Downlink NOMA With OFDM and OFDM-IM for Beyond 5G Wireless Networks," in IEEE Signal Processing Letters, 2020, vol. 27, pp. 491-495

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)