# Leveraging Deep Learning Based CSI Estimation for Securing Wireless and IOT Networks

**Dilip Mandliya[1], Arpana Jaiswal[2] , Pranay Ramdiya[3]**

**Abstract: Wireless networks have a great potential in supporting time-critical data delivery among diverse devices and for emerging applications such as smart cities and automation. 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. 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.**

*Keywords:- Wireless Networks, Machine Learning, Channel Assignment, Proactive Security, Error Rate*

## I.Introduction

Wireless networks have become ubiquitous in modern society, providing convenient and flexible connectivity for various devices and applications [1]. 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 [2]. 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]. 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. Characteristics of Smart Wireless Networks

One of the fundamental security challenges in wireless networks is the open nature of the transmission medium. Unlike wired networks, where signals are confined to physical cables, wireless signals propagate through the air, making them susceptible to eavesdropping and interception by unauthorized parties. Attackers can easily capture wireless signals using readily available tools, posing risks to the confidentiality and integrity of the transmitted data. Hence smart or cognitive wireless network architectures are being developed [9]

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 [10]. 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 [11]:

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 [12].

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:

1)      Wireless channels change randomly over time, therefore sensing wireless channels before they change is tough.

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

3)      Due to addition of noise in the transmitted signal, detection of spectrum holes may be practically tough

4)      Due to dynamic spectrum allocation, there exists a chance of 'Spectrum Overlap' causing interference between users.

5)      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.

## IV. Security Aware Channel Assignment Based on Machine Learning

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. 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. 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. 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. Figure 1 depicts the IoT-energy harvesting technique at the hub/gateway of the network:
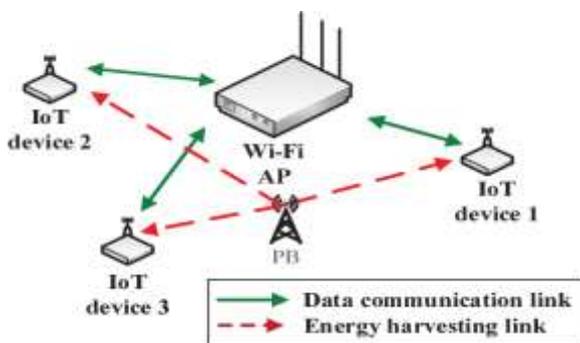


**Fig.1 Typical Energy Harvesting at Hub of IoT Network**

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.

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

*7. Design a deep neural network and initialize weights randomly.*
*for i=1:maxitr,*
*{*
*Update weights as:*

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

*}*

*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.*

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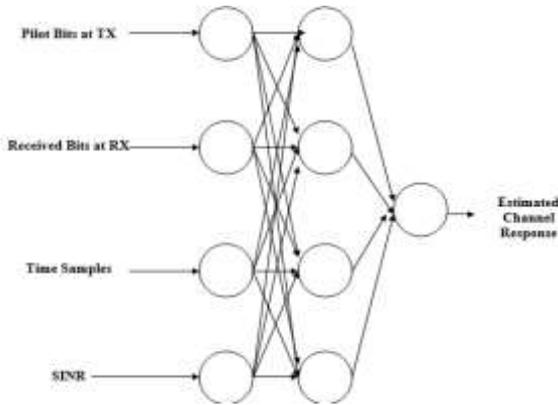$f(freq)$ denotes a function of frequency.



**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.

## V. Results:

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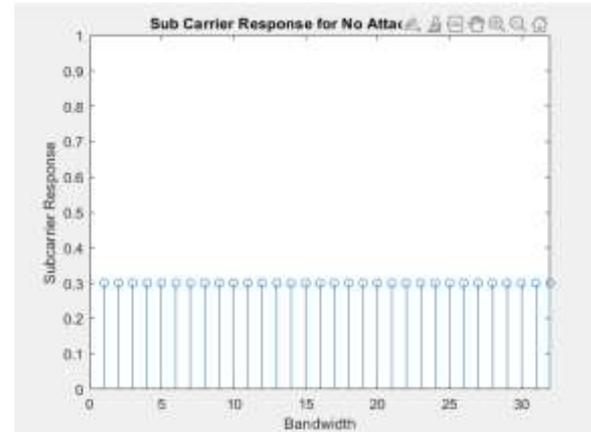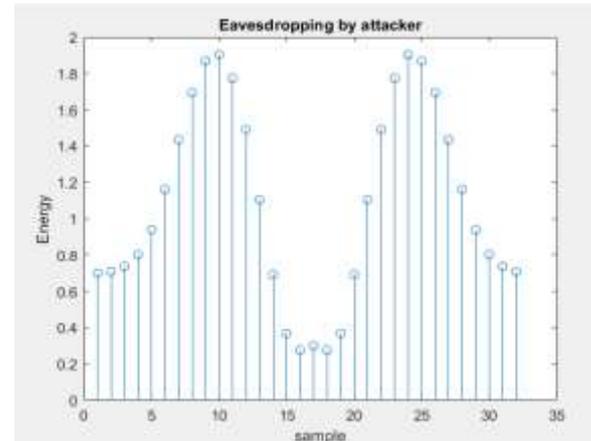


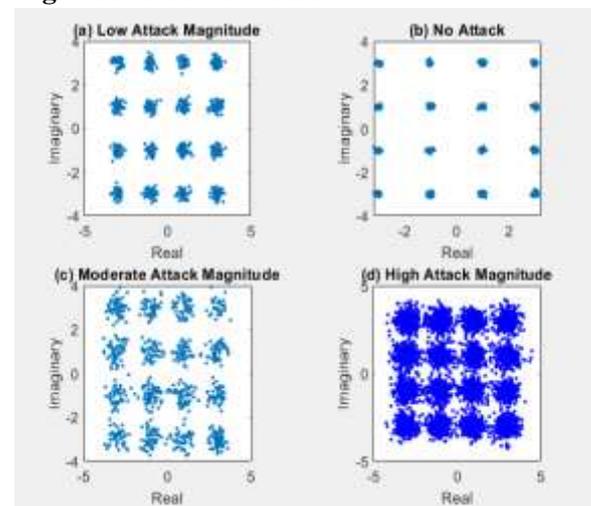**Fig.3 Ideal Transmission with No attack**



**Fig.4 Condition of Attack**



**Fig.5 Scatter Plots**
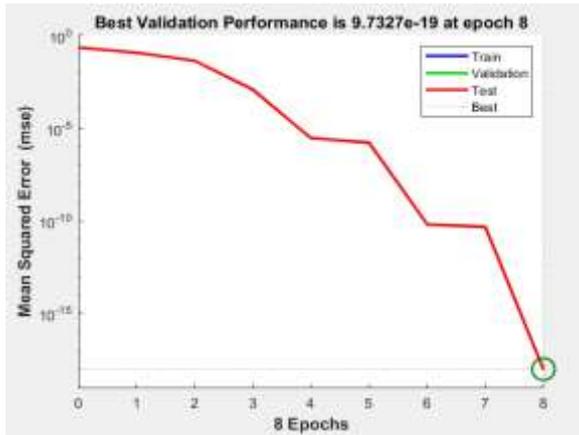
**Fig.6 Convergence of ML Model**



**Fig.7 Gradient and Validation Checks for ML Model**



**Fig.8 Error Histogram for ML Model**



**Fig.9 Error Rates for Different Conditions**
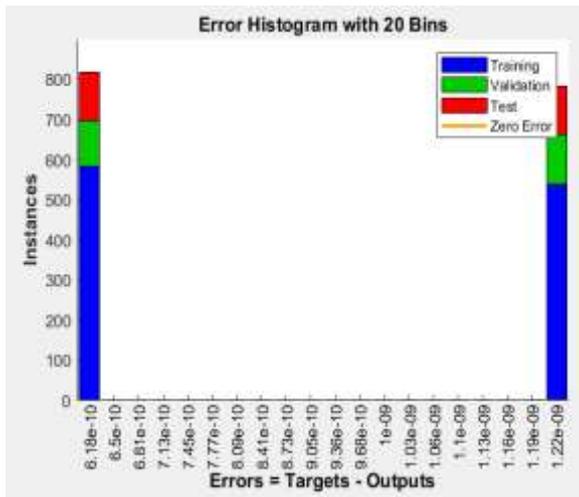
It can be observed from the previous results that the system designed in this approach emulates a real life scenario of varying adversarial attacks on the bandwidth for data transmission for the network. Moreover, the scatter plot of the network maps the levels of attack with the channel scatter.

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. 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 | Ideal Channel Gain | 0.3 |
| 4 | Iterations to convergence | 8 |
| 5 | Resets | 0 |
| 6 | BER of Proposed Work | $10^{-6}$ |
| 7 | BER of Previous Work [1] | $10^{-4}$ |

**Conclusion: It can be concluded form the above discussions that Machine learning models have revolutionized cognitive wireless networks by enhancing spectrum sensing, decision-making, resource allocation, and security. 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 quality of service (QoS).

### References

1. I. 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.

2. H. Huang, Y. Zhang, H. Zhang, C. Zhang and Z. Han, "Illegal Intelligent Reflecting Surface Based Active Channel Aging: When Jammer Can Attack Without Power and CSI," in IEEE Transactions on Vehicular Technology, vol. 72, no. 8, pp. 11018-11022, Aug. 2023.

3. T Burton, K Rasmussen, "Private data exfiltration from cyber-physical systems using channel state information" ACM SIGSAC Conference on Computer and Communications Security, ACM 2021, PP.223-235.

4. 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

5. Syed Hashim Raza Bukhari ,Sajid Siraj,Mubashir Husain Rehmani," NS-2 based simulation framework for cognitive radio sensor networks", SPRINGER 2019

6. K. J. Prasanna Venkatesan ,V. Vijayarangan, "Secure and reliable routing in cognitive radio networks", SPRINGER 2018

7. Keke Gai ,Meikang Qiu ,Hui Zhao, "Security-Aware Efficient Mass Distributed Storage Approach for Cloud Systems in Big Data",IEEE 2017

8. 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

9. Rajesh K. Sharma ;,Danda B. Rawat," Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey",IEEE 2015.

10. Maged Elkashlan ,Lifeng Wang ,Trung Q. Duong , George K. Karagiannidis ,Arumugam Nallanathan, "On the Security of Cognitive Radio Networks",IEEE 2015

11. Erol Gelenbe," A Software Defined Self-Aware Network: The Cognitive Packet Network", IEEE 2014

12. Mahmoud Khasawneh ,Anjali Agarwal," A survey on security in Cognitive Radio networks", IEEE 2014

13. Yulong Zou, Xianbin Wang ,Weiming Shen," Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks",IEEE 2013

14. Muhammad Faisal ,Amjad,Baber Aslam ,Cliff C. Zou, ," Reputation Aware Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks", IEEE 2013

15. Gianmarco Baldini ,Taj Sturman ,Abdur Rahim Biswas ,Ruediger Leschhorn ,Gyozo Godor ,Michael Street," Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead", IEEE 2012

16. Alvaro Araujo ,Javier Blesa,Elena Romero,Daniel Villanueva, "Security in cognitive wireless sensor networks. Challenges and open problems", SPRINGER 2012

17. Yiyang Pei ,Ying-Chang Liang, Kah Chan Teh ,Kwok Hung Li, "Secure Communication in Multiantenna Cognitive Radio Networks With Imperfect Channel State Information", IEEE 2011