

A Deep Learning Based Approach for Security Enhancement of MIMO-IOT Networks

Shrishti

Assistant Professor, Department of Computer Science and Engineering
Sushila Devi Bansal College of Technology, Indore

Abstract:- The rapid growth of the Internet of Things (IoT) has transformed the way devices communicate and interact in modern digital environments. IoT systems consist of billions of interconnected sensors, smart devices, vehicles, healthcare equipment, industrial machines, and home automation systems that continuously exchange data through wireless networks. As the number of connected devices increases, conventional wireless communication technologies face significant challenges such as limited bandwidth, network congestion, high latency, reduced energy efficiency, and unreliable connectivity. To overcome these limitations and support large-scale machine-type communications, advanced wireless technologies are required. One of the most promising technologies for enhancing IoT system performance is Massive Multiple Input Multiple Output (Massive MIMO), which has become a key component of modern 5G and beyond wireless communication systems. In the proposed work, a deep learning based approach for enhancing the security of MIMO-IoT systems has been proposed. It has been shown that the proposed approach outperforms existing approaches in terms of error performance and spectral efficiency.

Keywords— *Internet of Things (IoT), Multiple Input Multiple Output (MIMO), Deep Learning, Data Security, Bit Error Rate (BER), Spectral Efficiency, Quality of Service (QoS).*

I. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has created a strong demand for advanced wireless communication technologies capable of supporting billions of interconnected devices. IoT systems are widely used in smart cities, healthcare, industrial automation, agriculture, transportation, environmental monitoring, and home automation. These applications involve continuous communication among sensors, controllers, machines, and cloud platforms. Traditional wireless communication systems often struggle to handle the enormous number of connected devices, high data traffic, and strict quality-of-service requirements of modern IoT environments [1]. Therefore, Massive Multiple Input Multiple Output (Massive MIMO) technology has become essential for improving the efficiency, reliability, and scalability of IoT communication systems. One of the primary reasons for the need for Massive MIMO in IoT systems is the massive growth in connected devices. Conventional wireless networks have limited capacity and cannot efficiently support simultaneous communication among thousands or millions of IoT devices. Massive MIMO uses a large number of antennas at the base station to communicate with multiple devices at the same time using the same frequency spectrum. This capability significantly increases network capacity and enables large-scale machine-type communication, which is a fundamental requirement for IoT ecosystems [2].



Fig.1 The Conceptual Framework for IoT systems

Figure 1 depicts the IoT framework. IoT systems also require efficient utilization of limited wireless spectrum resources. As the number of wireless devices increases, spectrum congestion becomes a major challenge. Massive MIMO improves spectral efficiency through spatial multiplexing, where multiple independent data streams are transmitted simultaneously within the same bandwidth. This efficient spectrum usage allows IoT networks to achieve higher data transmission rates and better communication quality without requiring additional spectrum resources. As a result, Massive MIMO becomes highly beneficial for dense urban IoT deployments and smart city infrastructures. Another important need for Massive MIMO in IoT systems is improved energy efficiency [3]. Many IoT devices are battery-powered and are expected to operate for long durations without frequent charging or battery replacement. Massive MIMO employs beamforming techniques that direct wireless signals precisely toward intended devices instead of broadcasting energy in all directions [4]. This focused transmission reduces unnecessary power consumption and improves signal strength. Consequently, IoT devices consume less energy during communication, thereby extending battery life and enhancing the sustainability of IoT networks [5].

Massive MIMO refers to a wireless communication technique in which a base station is equipped with a very large number of antennas, often hundreds, to simultaneously serve many users or devices within the same frequency band. Unlike traditional MIMO systems that use a small number of antennas, Massive MIMO significantly improves spectral efficiency, energy efficiency, and network capacity [6]. By employing advanced beamforming and spatial multiplexing techniques, Massive MIMO can direct signals precisely toward intended IoT devices while minimizing interference to other devices. This capability is particularly important in dense IoT environments where thousands of devices may operate simultaneously in smart cities, industrial automation systems, intelligent transportation networks, and healthcare monitoring applications. One of the major advantages of Massive MIMO in IoT systems is its ability to increase network capacity. In conventional wireless networks, the simultaneous connection of numerous devices often leads to congestion and packet loss [7]. Massive MIMO addresses this problem by serving multiple IoT devices concurrently using the same time-frequency resources. Through spatial multiplexing, different data streams are transmitted independently to multiple devices, thereby improving throughput and reducing communication delays. This enhanced capacity allows IoT systems to support a massive number of connected devices without significant degradation in performance, making Massive MIMO highly suitable for large-scale IoT deployments [8].

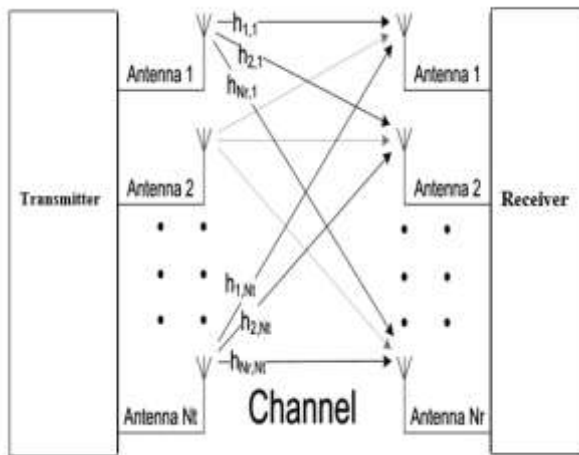


Fig.2. The MIMO System

Figure 2 depicts the MIMO system. The MIMO based system has multiple transmitter and multiple receivers which create parallel data paths for transmission and reception which in turn allows enhanced data rates for the same limited bandwidth. Typically, the channel capacity is enhanced as per the following relation [9]:

$$C = f\{kBlpg_2 \left[1 + \frac{h_{ij}^2 S}{N} \right]\} \quad (1)$$

Here,

C is the channel capacity

B is the channel bandwidth

S is the signal power

N is the noise power

k is a constant depending on system parameters

f is a function depending on system parameters

h is the MIMO channel matrix

i is the number of transmitters

j is the number of receivers

Here,

x1, x2 ... xn are the different sub-carriers for OFDM transmission

n is the total number of carriers

T is the period of the carriers

Another important benefit of Massive MIMO is improved spectral efficiency. Spectrum resources are limited and expensive, especially in highly populated urban environments where wireless traffic is continuously increasing. Massive MIMO utilizes the available spectrum more efficiently by transmitting multiple parallel data streams over the same bandwidth. This efficient spectrum utilization increases data transmission rates and improves overall communication quality. In IoT applications such as smart transportation systems, autonomous vehicles, and industrial control systems, high spectral efficiency ensures reliable and real-time data transmission, which is critical for maintaining operational safety and performance. Massive MIMO also enhances energy efficiency in IoT networks [10]. Many IoT devices are battery-powered and operate under strict energy constraints. Frequent battery replacement or charging may not be feasible in remote or large-scale deployments. Massive MIMO improves energy efficiency by focusing transmission energy toward specific devices through beamforming techniques instead of broadcasting signals in all directions. This targeted transmission reduces power consumption at both the transmitter and receiver ends while maintaining strong signal quality. Consequently, IoT devices can achieve longer battery life and improved operational sustainability, which is especially beneficial for sensor networks, environmental monitoring systems, and wearable healthcare devices [11].

II. SPACE TIME BLOCK CODING FOR MIMO SYSTEMS

To implement this MIMO based transmission scheme practically, Space Time Block Coding (STBC) is often employed in which the data stream is arranged as a matrix with the number of columns equating to the number of MIMO transmitters and the number of rows equating to the number of time slots of transmission. The symbols of STBC transmission can be estimated as [12]:

$$H^+ = (H^H H)^{-1} H^H \quad (2)$$

Here,

H^+ represents the Moore-Penrose pseudo inverse since the channel matrix,

H is the channel matrix and it may not always be square for the STBC matrix.

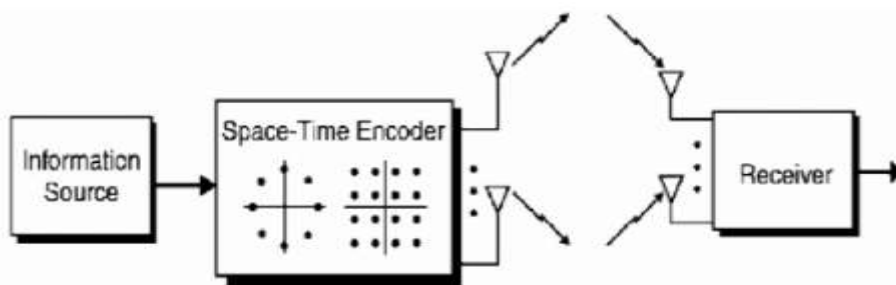


Fig.3 The STBC Scheme for MIMO

Figure 3 depicts the STBC scheme for MIMO systems. Space-Time Block Coding (STBC) is a signal processing and transmission technique used in Multiple Input Multiple Output (MIMO) wireless communication systems to improve transmission reliability and reduce the effects of fading and interference in wireless channels. In modern wireless communication networks, signals transmitted through the air are often affected by multipath fading, noise, attenuation, and interference, which can significantly degrade communication quality. STBC was developed to overcome these challenges by utilizing multiple transmitting and receiving antennas to provide spatial diversity and enhance signal robustness. MIMO technology employs multiple antennas at both the transmitter and receiver to improve wireless communication performance [13]. However, simply using multiple antennas is not sufficient to guarantee reliable communication in fading environments. STBC introduces coding across both space (multiple antennas) and time (multiple transmission intervals) to ensure that redundant copies of the transmitted data are sent through independent communication paths. This redundancy allows the receiver to recover the original information even when some signal paths experience severe fading or interference [14]. The fundamental principle of STBC is to transmit multiple copies of a data stream using different antennas over different time slots according to a predefined coding matrix. One of the most widely used STBC schemes is the Alamouti Scheme, which is designed for systems with two transmit antennas and one or more receive antennas. In the Alamouti scheme, two symbols are transmitted simultaneously from two antennas during two consecutive time intervals using a special orthogonal coding structure. This orthogonality enables simple decoding at the receiver while providing full diversity gain without increasing transmission bandwidth or power [15].

Wireless IoT environments are often affected by signal fading, interference, and noise due to obstacles, mobility, and dense device populations. Massive MIMO employs diversity gain and advanced signal processing methods to mitigate these communication impairments. By using multiple antennas, the system can combine signals from different propagation paths, thereby improving signal strength and reducing error rates. This results in more reliable communication links and enhanced quality of service for critical IoT applications such as emergency response systems, smart grid monitoring, and industrial process automation. Low latency communication is another essential requirement for modern IoT systems, particularly in applications involving real-time decision-making and control. Examples include autonomous driving, robotic automation, remote surgery, and intelligent traffic management systems. Massive MIMO reduces communication latency by increasing channel capacity and enabling efficient simultaneous transmissions. The improved signal quality and reduced retransmissions further contribute to faster data delivery [16]. As a result, IoT systems powered by Massive MIMO can support time-sensitive applications with greater accuracy and responsiveness. Massive MIMO also plays a significant role in enhancing the scalability of IoT networks. As IoT ecosystems continue to expand, communication infrastructures must accommodate rapidly growing numbers of devices without compromising network

performance. Massive MIMO provides scalable connectivity by efficiently managing multiple user connections within a single cell. This scalability is particularly important in smart city environments where millions of sensors and connected devices continuously exchange information related to traffic, pollution, surveillance, and public services [17]. The ability of Massive MIMO to support large-scale connectivity ensures sustainable network growth and improved operational efficiency. Despite its numerous advantages, the implementation of Massive MIMO in IoT systems also presents several challenges. One major issue is the increased hardware complexity associated with deploying large antenna arrays and advanced signal processing units. Channel estimation and synchronization become more complicated as the number of antennas increases. Additionally, pilot contamination, which occurs when similar pilot signals are reused in neighboring cells, can degrade system performance. High computational requirements and energy consumption at base stations also pose implementation challenges [18]. Researchers are actively exploring machine learning techniques, hybrid beamforming strategies, and intelligent resource allocation methods to overcome these limitations and optimize Massive MIMO performance in IoT networks. The integration of Massive MIMO with emerging technologies such as artificial intelligence, edge computing, cloud computing, and 6G communication systems is expected to further enhance IoT performance in the future. Artificial intelligence algorithms can optimize antenna selection, beamforming, and resource management in real time, while edge computing can reduce latency by processing IoT data closer to end devices [19]. The combination of Massive MIMO with millimeter-wave communication and intelligent reflecting surfaces may provide ultra-high-speed connectivity and improved coverage for next-generation IoT applications. These technological advancements will enable smarter, more efficient, and highly connected digital ecosystems.

III. A DEEP LEARNING BASED SECURITY FRAMEWORK FOR MIMO-IOT SYSTEMS

The integration of MIMO with IoT systems creates highly efficient communication infrastructures known as MIMO-IoT systems. However, the increasing connectivity and open wireless environment also expose these systems to various security threats such as eavesdropping, spoofing, denial-of-service attacks, malware injection, signal jamming, and unauthorized access. To address these challenges, researchers have proposed Deep Learning based security frameworks that provide intelligent, adaptive, and automated protection mechanisms for MIMO-IoT systems [20]. A Deep Learning based security framework for MIMO-IoT systems refers to an intelligent cybersecurity architecture that uses deep neural networks and advanced machine learning algorithms to detect, classify, and prevent malicious activities within wireless IoT communication environments. Unlike traditional security mechanisms that rely on predefined rules and signatures, deep learning models can automatically learn complex patterns and hidden relationships from large volumes of network data. This capability enables the framework to identify both known and unknown cyber threats with higher accuracy and adaptability [21].

The architecture of a Deep Learning based security framework for MIMO-IoT systems generally consists of several layers, including the sensing layer, communication layer, data processing layer, security analysis layer, and application layer. In the sensing layer, IoT devices and sensors collect environmental or operational data and transmit it through MIMO-enabled wireless communication channels[22]. The communication layer uses MIMO techniques such as beamforming, spatial multiplexing, and diversity transmission to enhance data transmission efficiency and reliability [23]. The collected network traffic and communication parameters are then forwarded to the data processing layer, where preprocessing techniques such as normalization, feature extraction, dimensionality reduction, and noise filtering are applied before feeding the data into deep learning models. 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 [24]. 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.

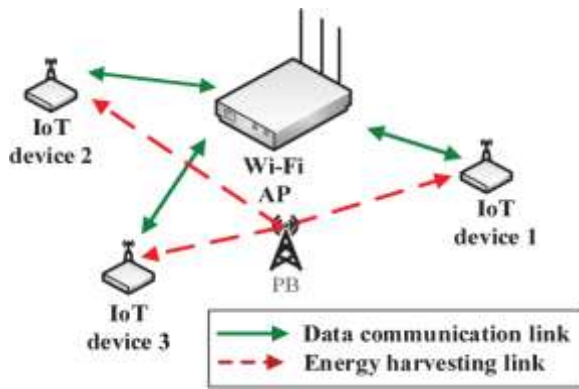


Fig.4 Typical Energy Harvesting at Hub of IoT Network

Figure 4 depicts the MIMO-IoT energy harvesting technique at the hub/gateway of the MIMO-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 [25] 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 for MIMO-IoT 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:*

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

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

for i=1:maxitr,

{

Update weights as:

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

}

8.: if ($i == \text{maxitr}$ 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.

 $H(\text{freq})$ represents the channel frequency response.

 $f(\text{freq})$ denotes a function of frequency.

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. In such a case, an equalization mechanism, such as Zero Forcing Equalization (ZFE) can be incorporated. Considering correctness at the output of the ZFE, the output is given by [26]:

$$\gamma_{ZF-BLE}(k, n) = E\{|d_n^k|^2\}|\Sigma|_{i,j}^2 \quad (3)$$

The Minimum Mean Square Error (MMSE) algorithm tries to minimize the mean square error as the objective function (G)

Here, the errors in channel estimation can be minimized by employing the following relation [27]:

$$G = \text{minimize} \left(\frac{1}{n} \sum_{i=1}^n e_i^2 \right) \quad (4)$$

Here,

G denotes the objective function

e denotes current error sample value

n denotes the number of error samples

The zero forcing equalizer tries to force the mean square error (mse) of the channel estimation to zero. Mathematically, equalization is performed if [28]

$$x(k) = [0_M \quad I_M] \begin{bmatrix} u(k-1) \\ u(k) \end{bmatrix} + E \frac{w_M}{\sqrt{M}} Z_r r(k) \quad (5)$$

Here,

$M \times M$ is the matrix size

u is the received signal

x is the recovered or equalized signal

W are the weights of the equalizer

E is the expectation or average value

IV. SIMULATION RESULTS

The system has been designed on Matlab, on a PC with 16GB of RAM and Intel i7 processor. The total number of bits in the simulation are 10 million bits, generated randomly through simulation.

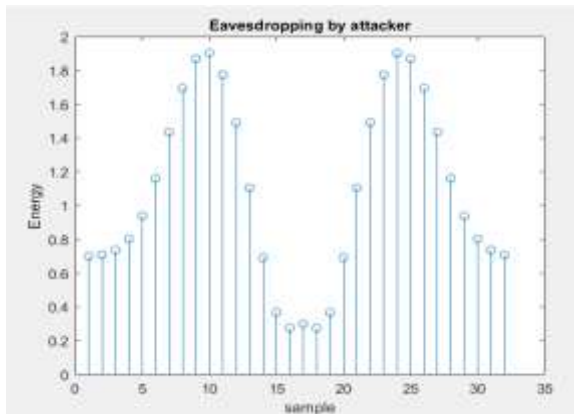


Fig.5 Condition of Attack

Figure 5 depicts the channel response for the MIMO-IoT Network under adversarial attack.

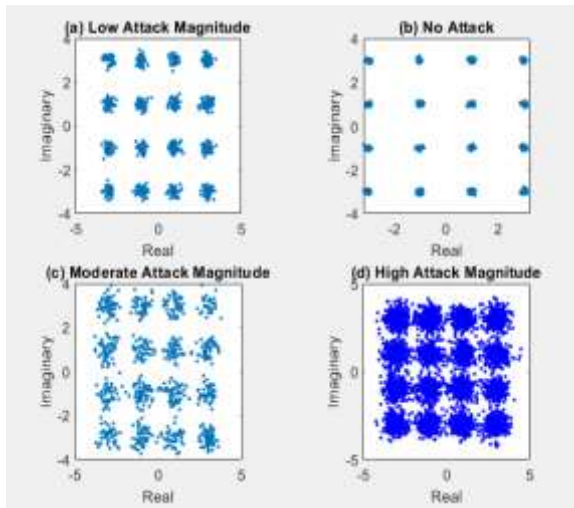


Fig.6 Scatter Plots

Figure 6 depicts the scatter plot of the model.

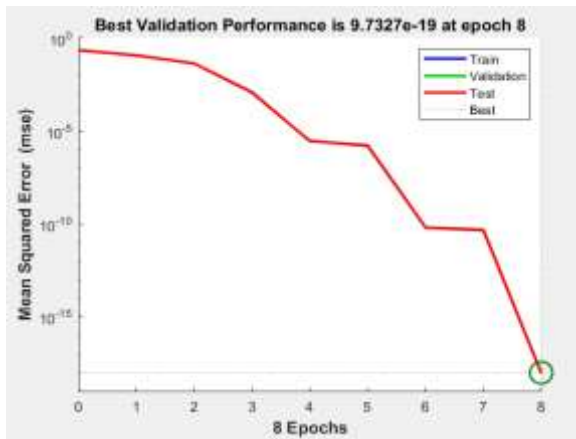


Fig.7 Convergence of Deep Learning Model

Figure 7 depicts the convergence of the model.

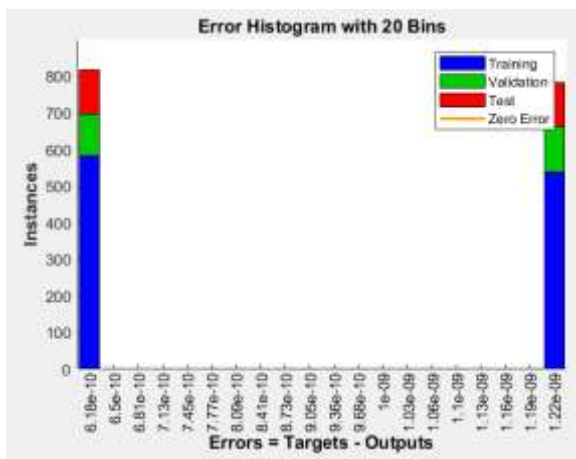


Fig.8 Error Histogram for ML Model

Figure 8 depicts the error histogram.

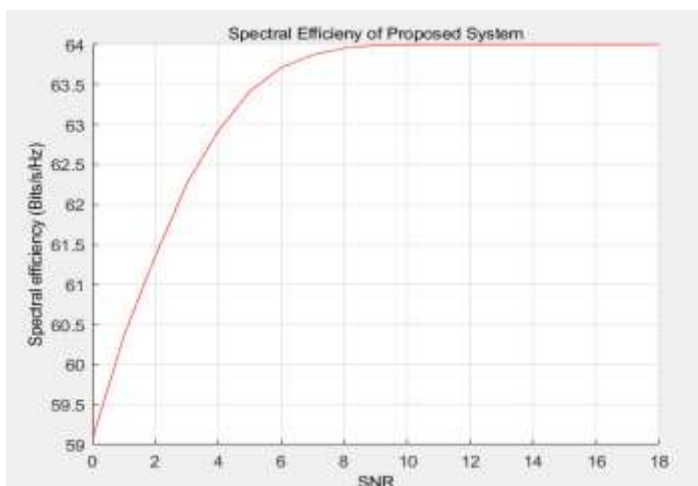


Fig.9. Spectral Efficiency of Proposed System

Figure 9 depicts the spectral efficiency of the model.

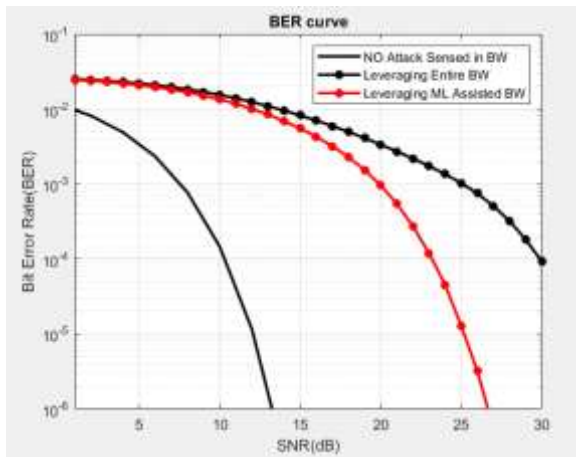


Fig.10 Error Rates for Different Conditions

Figure 10 depicts the error rate of the model. 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. 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	10 million Random
2	Carries per packet	32
3	Ideal Channel Gain	0.3
4	Iterations to convergence	8
5	Resets	0
6	BER reached (Proposed Work)	10^{-6}
7	BER (Lee et al.), [28]	10^{-2}
8	BER (Guo et al.), [27]	10^{-3}

The experimental results confirm that the proposed deep learning based security framework improves overall system performance in terms of convergence speed, communication stability, and error reduction. The framework effectively enhances the reliability and security of MIMO-IoT communication networks while supporting large-scale data transmission and intelligent threat detection. These outcomes demonstrate the suitability of the proposed model for future secure IoT applications such as smart cities, industrial automation, healthcare monitoring, intelligent transportation systems, and next-generation wireless communication networks.

V. CONCLUSION

It can be concluded that, Massive MIMO has emerged as a highly effective technology for enhancing the performance of IoT-based systems. Its ability to improve network capacity, spectral efficiency, energy efficiency, reliability, scalability, and low-latency communication makes it an essential component of modern wireless communication infrastructures. Although certain implementation challenges remain, ongoing research and technological innovations continue to improve the practicality and effectiveness of Massive MIMO in IoT environments. As the demand for intelligent and interconnected systems continues to grow, Massive MIMO will play a crucial role in enabling efficient, reliable, and large-scale IoT communications in future smart environments. a Deep Learning based security framework for MIMO-IoT systems provides an advanced and intelligent solution for protecting wireless IoT communication environments against modern cyber threats. By combining the communication efficiency of MIMO technology with the adaptive learning capabilities of deep neural networks, the framework enhances intrusion detection, anomaly identification,

authentication, physical layer security, and malware prevention. Although certain implementation challenges remain, ongoing research and technological innovations continue to improve the effectiveness and scalability of these security frameworks. As IoT networks continue to expand in size and complexity, deep learning based security mechanisms will play a critical role in ensuring safe, reliable, and secure communication in next-generation MIMO-IoT systems. The proposed work is shown to attain lower error rate and thereby improved system performance compared to existing work in the domain.

REFERENCES

- [1] Ullah, A., Choi, W., Berhane, T. M., Sambo, Y., & Imran, M. A. (2024). Soft-output deep LAS detection for coded MIMO systems: a learning-aided LLR approximation. *IEEE Transactions on Vehicular Technology*
- [2] E. Balevi, A. Doshi and J. G. Andrews, "Massive MIMO Channel Estimation With an Untrained Deep Neural Network," in *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 2079-2090, March 2020
- [3] M. -S. Baek, S. Kwak, J. -Y. Jung, H. M. Kim and D. -J. Choi, "Implementation Methodologies of Deep Learning-Based Signal Detection for Conventional MIMO Transmitters," in *IEEE Transactions on Broadcasting*, vol. 65, no. 3, pp. 636-642, Sept. 2019.
- [4] David Borges, Paulo Montezuma, Afonso Ferreira, Rui Dinis, "Two Low Complexity MRC and EGC Based Receivers for SC-FDE Modulations with Massive MIMO Schemes", *Journal of Signal Processing Systems*, volume 90, pp:1357–1367, Springer 2018.
- [5] [2] C Thrampoulidis, W Xu, Babak Hassibi, "Symbol error rate performance of box-relaxation decoders in massive mimo", Volume: 66 , Issue: 3, pp: 3377-3392, *IEEE Transactions on Signal Processing* 2018.
- [6] Prabina Pattanayak, Vinay Kumar Trivedi, Sayan Chakraborty, Preetam Kumar, "BER Performance of Multi User Scheduling for MIMO-STBC and MIMO-OFDM Broadcast Network with Imperfect CSI", *Proceedings in 2017 4th International Conference on Signal Processing and Integrated Networks (SPIN)*, IEEE 2017.
- [7] Y Li, C Tao, G Seco-Granados, "Channel estimation and performance analysis of one-bit massive MIMO systems", Volume: 65 , Issue: 15, pp:4075-4089, *IEEE Transactions on Signal Processing*, 2017.
- [8] S Park, A Alkhateeb, RW Heath, "Dynamic subarrays for hybrid precoding in wideband mmWave MIMO systems", Volume: 16 , Issue: 5, pp: 2907-2920, *IEEE Transactions on Wireless Communications* 2017.
- [9] C Chen, Z Liu, K Xie, Y Liu, Y Zhang, "Adaptive fuzzy asymptotic control of MIMO systems with unknown input coefficients via a robust Nussbaum gain-based approach", Volume: 25 , Issue: 5, pp:1252-1263, *IEEE Transactions on Fuzzy Systems* 2017.
- [10] X Gao, L Dai, S Han, I Chih-Lin, "Energy-efficient hybrid analog and digital precoding for mmWave MIMO systems with large antenna arrays", Volume: 34 , Issue: 4, pp: 998-1009, *IEEE Journal on Selected Areas in Communications* 2016.
- [11] X Yu, JC Shen, J Zhang, "Alternating Minimization Algorithms for Hybrid Precoding in Millimeter Wave MIMO Systems", *IEEE* 2016
- [12] J Mo, RW Heath, "Capacity analysis of one-bit quantized MIMO systems with transmitter channel state information", Volume: 10 , Issue: 3, pp: 485-500, *IEEE Journal of Selected Topics in Signal Processing* 2015.
- [13] A Pitarokoilis, SK Mohammed, "Uplink performance of time-reversal MRC in massive MIMO systems subject to phase noise", Volume: 14 , Issue: 2, pp: 711-723, *IEEE Transactions on Wireless Communications* 2015.
- [14] EG Larsson, O Edfors, F Tufvesson, "Massive MIMO for next generation wireless systems", Volume: 52 , Issue: 2, pp: 186-195, *IEEE Communications Magazine* 2014
- [15] E Björnson, J Hoydis, M Kountouris, "Massive MIMO systems with non-ideal hardware: Energy efficiency, estimation, and capacity limits", Volume: 60 , Issue: 11, pp: 7112-7139, *IEEE Transactions on Information Theory* 2014
- [16] HQ Ngo, EG Larsson, "Energy and spectral efficiency of very large multiuser MIMO systems", Volume: 61 , Issue: 4, pp: 1436 – 1449, *IEEE Transactions on Communications* 2013

- [17] X Chen, X Wang, X Chen, "Energy-efficient optimization for wireless information and power transfer in large-scale MIMO systems employing energy beam-forming", Volume: 2 , Issue: 6 , pp:667-670, IEEE Wireless Communications Letters 2013
- [18] M. S. Oh, S. Hosseinalipour, T. Kim, C. G. Brinton, and D. J. Love, "Channel Estimation via Successive Denoising in MIMO OFDM Systems: A Reinforcement Learning Approach," in Proceedings of the IEEE International Conference on Communications (ICC), Jun. 2021, pp. 1–6.
- [19] O El Ayach, RW Heath, S Abu-Surra, "Low complexity precoding for large millimeter wave MIMO systems", Proceedings in 2012 IEEE International Conference on Communications (ICC).
- [20] N. T. Nguyen, K. Lee, and H. Dai, "Application of Deep Learning to Sphere Decoding for Large MIMO Systems," IEEE Transactions on Wireless Communications, vol. 20, no. 7, pp. 4204–4217, 2021.
- [21] X. Ma, Z. Gao, F. Gao, and M. Di Renzo, "Model-Driven Deep Learning Based Channel Estimation and Feedback for Millimeter-Wave Massive Hybrid MIMO Systems," IEEE Journal on Selected Areas in Communications, vol. 39, no. 8, pp. 2388–2406, Aug. 2021
- [22] O El Ayach, RW Heath, S Abu-Surra, "The capacity optimality of beam steering in large millimeter wave MIMO systems", Proceeding in 2012 IEEE 13th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC).
- [23] D. Korpi, M. Honkala, J. M. J. Huttunen, and V. Starck, "DeepRx MIMO: Convolutional MIMO Detection with Learned Multiplicative Transformations," arXiv preprint arXiv:2010.16283, 2020.
- [24] Y. Qiang, X. Shao, and X. Chen, "A Model-Driven Deep Learning Algorithm for Joint Activity Detection and Channel Estimation," IEEE Communications Letters, vol. 24, no. 11, pp. 2508–2512, Nov. 2020
- [25] Q. Hu, F. Gao, H. Zhang, G. Y. Li and Z. Xu, "Understanding Deep MIMO Detection," in IEEE Transactions on Wireless Communications, vol. 22, no. 12, pp. 9626-9639, Dec. 2023
- [26] Wang, Y., Gao, Z., Chen, S., Hu, C., & Zheng, D. (2024). Deep learning-based channel extrapolation and multiuser beamforming for RIS-aided terahertz massive MIMO systems over hybrid-field channels. Intelligent Computing, 3, 0065
- [27] J. Guo, T. Chen, S. Jin, G.Y. Li, X. Wang, X. Hou, "Deep learning for joint channel estimation and feedback in massive MIMO systems", Digital Communications and Networks, Elsevier 2024, vol.10, pp.83-93.
- [28] S. Lee and D. Sim, "Deep Learning-Based Channel Estimation Method for MIMO Systems in Spatially Correlated Channels," in IEEE Access, 2024, vol. 12, pp. 79082-79090.