JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-21, No.-03, March (2026) pp 104-122 ISSN (Print) 0973-8975

SECURE AND EFFICIENT CHANNEL ESTIMATION IN MU-MIMO-OFDM VIA SPARSE SPATIAL GRAPH NEURAL NETWORKS WITH FENNEC FOX OPTIMIZATION

Shovon Nandi[1], Madhumita Sarkar[2], Arindam Sarkar[3]

[1]Department of ECE, Techno Bengal Institute of Technology, Kolkata, India.

[2]Department of ECE, B. P. Poddar Institute of Management and Technology, Kolkata, India.

[3]Department of AEIE, Heritage Institute of Technology, Kolkata, India

Emails: [1]nandi.shovon@yahoo.in, [2]dr.msarkarece@gmail.com
[3]arin0007@gmail.com

Corresponding Author: **Shovon Nandi**

https://doi.org/10.26782/jmcms.2026.03.00008

(Received: January 02, 2026; Revised: February 19, 2026; Accepted: March 08, 2026)

Abstract

The integration of Sparse Spatial Graph Neural Network (SSGNN) is a promising approach for enhancing the security and performance of Multiple User - Multiple Input Multiple Output - Orthogonal Frequency Division Multiplexing (MU-MIMO-OFDM) systems. SSGNN can effectively model the sparse channel structure and estimate the channel state information (CSI) in real-time. This research introduces AI-driven solutions for next-generation wireless systems, focusing on a Sparse Spatial Graph Neural Network (SSGNN) optimized with Fennec Fox Optimization (FFO) for secure multi-user MIMO-OFDM channel estimation and interference mitigation. The proposed SSNGN-FFO approach achieves exceptional performance, with a remarkably low Bit Error Rate (BER) of 0.00012 and a high Peak Signal-to-Noise Ratio (PSNR) of 45dB, indicating its potential for reliable and high-quality wireless communication using MATLAB.

Keywords: Bit Error Rate, Channel Estimation, Channel State Information, Deep Learning, Inter-Carrier Interference, Mean Squared Error, MU-MIMO-OFDM, Peak Signal-to-Noise Ratio, Sparse Spatial Graph Neural Network

I. Introduction

The accelerated growth of wireless communication (WC) technologies, particularly the transition from fifth-generation (5G) to sixth-generation (6G) networks, has made them indispensable in today's digital society. These systems enable ultra-reliable connectivity, massive device access, and high-speed data services across diverse domains such as the Internet of Things (IoT), vehicular networks, and smart cities. Despite these capabilities, the integrity and confidentiality of wireless

transmission remain vulnerable to a variety of security threats. Among them, jamming and pilot spoofing attacks have emerged as particularly critical, as they can severely disrupt signal transmission and compromise network performance. Meanwhile, the demand for extremely high data rates, robust reliability, and efficient spectrum utilization has accelerated the adoption of Multiple User-Multiple Input Multiple Output-Orthogonal Frequency Division Multiplexing (MU-MIMO-OFDM). This technique integrates MIMO's multi-antenna architecture, which boosts throughput, with OFDM's multi-carrier modulation, which improves spectral efficiency. The overall system architecture is illustrated in fig. 1, where the block diagram highlights the essential components of MU-MIMO-OFDM transmission.

MIMO-OFDM technology provides significant advantages, including improved spectral efficiency, enhanced throughput, and resistance to frequency-selective fading [IV, XV]. However, it also introduces several challenges that limit its practical implementation. Complex channel estimation caused by Inter-Symbol Interference (ISI) and Inter-User Interference (IUI) remains a major issue. Furthermore, vulnerabilities such as pilot spoofing attacks can distort the Channel State Information (CSI), thereby compromising secure and reliable communication [II, XXXIX]. Consequently, developing robust channel estimation techniques and advanced interference mitigation mechanisms has become a primary focus for next-generation wireless systems.

In response to these challenges, deep learning (DL) has emerged as a powerful tool for addressing the limitations of traditional signal processing techniques. Leveraging their ability to learn intricate features and adapt to varying channel conditions, DL-based models can improve both performance and security in wireless networks [XXXVI, VII, XX]. Convolutional Neural Networks (CNNs) have been applied to extract spatial features, while Recurrent Neural Networks (RNNs) have been employed to model sequential dependencies in time-varying channel [XIX]. More recently, Graph Neural Networks (GNNs) have gained traction for their ability to capture the spatial and relational structure of communication networks [XIV], making them particularly promising for multi-user MIMO systems with sparse channel properties.

A Sparse Spatial Graph Neural Network (SSGNN) is particularly well-suited for MU-MIMO-OFDM systems because it efficiently models the sparse and structured nature of wireless channel by representing antennas, users, and subcarriers as nodes in a graph, while edges capture spatial and frequency-domain relationships. Beyond accurate channel modeling, SSGNNs can strengthen security in MU-MIMO-OFDM systems in three critical ways: (a) Anomaly detection, for identifying unusual patterns in signal transmission; (b) Intrusion detection, for recognizing unauthorized access attempts; and (c) Channel estimation, for improving accuracy and preventing eavesdropping [VI, XXXII, XXXVIII]. Moreover, SSGNNs offer scalability and adaptability across diverse users and channel conditions, outperforming CNNs, RNNs, and computationally heavy dense GNNs. These characteristics make SSGNN a strong candidate for next-generation wireless networks requiring both high efficiency and robust security.

Problem Statement and Research Gap

Although MU-MIMO-OFDM has emerged as a key enabler for next-generation wireless networks, its performance is hindered by several critical limitations. Traditional channel estimation methods are highly vulnerable to pilot

spoofing attacks, inter-user interference (IUI), and inter-symbol interference (ISI), which degrade reliability and compromise security. While deep learning approaches such as CNNs, RNNs, and conventional GNNs have been explored to address these issues, they suffer from notable shortcomings. CNNs are constrained by limited spatial feature extraction in large-scale antenna arrays, RNNs struggle with computational overhead in modeling long sequences, and dense GNNs introduce scalability challenges that limit their application in multi-user environments. Furthermore, existing solutions seldom incorporate security-aware learning mechanisms, leaving networks exposed to sophisticated attacks. Most importantly, there is a lack of hybrid frameworks that combine graph-based learning with adaptive optimization to simultaneously improve channel estimation accuracy, scalability, and robustness against adversarial threats.

Contributions

The key contributions of this research are summarized as follows:

Hybrid Framework for MU-MIMO-OFDM: Proposes a Sparse Spatial Graph Neural Network optimized with Fennec Fox Optimization (SSGNN-FFO), specifically designed to address channel estimation and interference mitigation challenges in MU-MIMO-OFDM systems.

Security Enhancement via SSGNN: Demonstrates how SSGNN effectively models antennas, users, and subcarriers as graph nodes, with edges capturing spatial and frequency-domain relationships, enabling robust anomaly detection, intrusion detection, and accurate channel estimation to safeguard against attacks such as pilot spoofing. This work evaluates worst-case estimator robustness under bounded distortions that are equivalent to low-power pilot contamination after baseband processing, consistent with recent learning-based physical-layer security.

Scalability and Adaptability: Establishes that SSGNN-FFO provides superior scalability compared to CNNs, RNNs, and dense GNNs, ensuring adaptability across diverse users, dynamic channels, and multi-user scenarios in next-generation networks.
Integration of Bio-Inspired Optimization: Introduces the Fennec Fox Optimization (FFO) algorithm for tuning SSGNN parameters, striking an effective balance between accuracy and computational complexity while improving resilience to adversarial conditions.

Performance Validation: Validates the proposed SSGNN-FFO framework using MATLAB 5G toolbox datasets, achieving a **Bit Error Rate (BER) of 0.00012** and a **Peak Signal-to-Noise Ratio (PSNR) of 45 dB**, which significantly outperforms existing DL-based methods.

Novelty Statement

Unlike existing CNN-, RNN-, and dense GNN-based approaches, the proposed SSGNN-FFO framework uniquely integrates a sparse spatial graph neural network with bio-inspired Fennec Fox Optimization, enabling scalable, secure, and highly accurate channel estimation in MU-MIMO-OFDM systems while simultaneously providing anomaly detection, intrusion detection, and robust interference mitigation.

The paper is organized as follows: Section II reviews literature; Section III presents the SSGNN-FFO architecture, system model, and optimization process; Section IV

discusses the dataset and performance metrics; Section V provides results and conclusions.

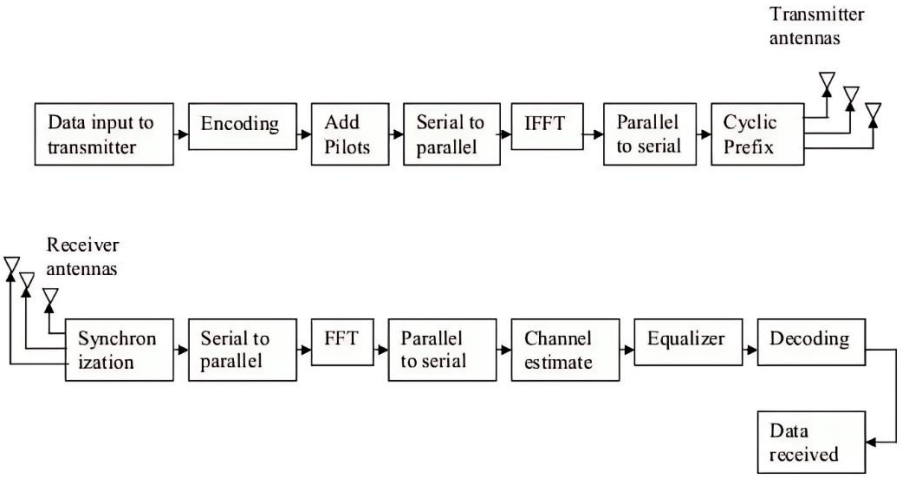

Fig. 1. The MIMO-OFDM System Block Diagram

II. Literature Review

According to [XI], Multiple Input Multiple Output (MIMO) systems exploit multiple antennas at either the transmitter or receiver to improve data throughput without requiring proportional increases in power or bandwidth. Building on this, Nandi et al. [XXIII-XXV] emphasized that the performance of MIMO systems is largely determined by spatial diversity and multiplexing gains, which depend on the number and configuration of antennas. Techniques such as Vertical-Bell Laboratories Layered Space-Time (V-BLAST) and Space-Time Coding have been widely applied to enhance detection efficiency at the receiver. Nevertheless, due to hardware constraints and antenna spacing requirements, practical deployments often limit the number of antennas to four, restricting scalability in real-world systems.

Shankar R. et al. [XXX] explained that MIMO technology leverages multipath propagation to transform signal variations into performance gains, thereby increasing data throughput and link reliability. Advanced implementations rely on coordinated transceivers and spatial processing to extend coverage and improve diversity. Furthermore, waveform enhancements such as Filtered-OFDM (F-OFDM) improve spectral efficiency by reducing out-of-band emissions, while Non-Orthogonal Multiple Access (NOMA) allows multiple users to simultaneously access shared spectrum resources, resulting in superior spectral efficiency and throughput compared to conventional orthogonal access schemes.

Orthogonal Frequency Division Multiplexing (OFDM) has also been recognized as a cornerstone modulation scheme for modern wireless systems. Sivadas [XIV] highlighted OFDM's effectiveness in handling multipath and frequency-selective fading by employing cyclic prefixes to eliminate Inter-Symbol Interference (ISI). However, the technique is sensitive to synchronization errors, with frequency offsets - caused by oscillator mismatches or relative motion between transmitter and receiver - posing a major challenge [XXXI, XXVI]. Complementing these findings, S. Nandi et

al. [XXII, XXVII] demonstrated that OFDM achieves robustness against frequency-selective fading by decomposing the channel into multiple flat-fading sub-channels through Inverse Fast Fourier Transform (IFFT) and Fast Fourier Transform (FFT) operations. This is accomplished by transmitting data over N overlapping but orthogonal subcarriers, thereby ensuring efficient modulation and demodulation with reduced ISI. Similarly, Jiang W. et al. [IX] reaffirmed that OFDM transforms time-varying, frequency-selective channels into parallel flat-fading sub-channels, while stressing the importance of precise time and frequency synchronization to maintain subcarrier orthogonality. Frequency offsets, often resulting from mobility or oscillator discrepancies, remain a persistent drawback of OFDM [XIII].

To address these challenges, deep learning (DL) techniques have gained attention for their ability to model complex channel behaviors and enhance wireless system performance. Convolutional Neural Networks (CNNs) have been widely applied for extracting spatial features from channel state information (CSI), enabling accurate detection and improved interference suppression [XX]. Recurrent Neural Networks (RNNs) and their variants, such as Long Short-Term Memory (LSTM) networks, have been employed to model temporal dependencies in time-varying fading channels, improving robustness in dynamic environments [XIX]. More recently, Graph Neural Networks (GNNs) have demonstrated superior performance by exploiting relational and topological structures of communication networks, making them particularly effective for multi-user MIMO systems with sparse spatial channel characteristics [XIV].

A further development is the Sparse Spatial Graph Neural Network (SSGNN), which efficiently represents antennas, users, and subcarriers as nodes, while edges capture spatial and frequency-domain relationships. As shown in recent studies [XXXII, XVIII, I], SSGNNs provide threefold benefits: (a) anomaly detection, by identifying unusual transmission patterns; (b) intrusion detection, by recognizing unauthorized access attempts; and (c) enhanced channel estimation, by improving accuracy to counter eavesdropping threats. Moreover, their scalability enables adaptation to diverse users and dynamic wireless conditions, outperforming CNNs, RNNs, and dense GNNs in terms of efficiency and robustness.

These advances establish the foundation for hybrid models that combine graph-based deep learning with bio-inspired optimization techniques to address unresolved challenges in MU-MIMO-OFDM systems, including scalability, security, and computational efficiency.

III. Proposed Architecture of SSGNN-FFO

The research uses known pilot frequency signals to analyze and optimize the wireless channel. It employs an SSGNN-FFO [XXXIV] to detect and mitigate attacks (Adversarial Attacks) on transmitted signals and utilizes FASP scheduling to prevent IUI. The block diagram for the proposed approach is shown in fig. 2.

A. SYSTEM MODEL

The terminal's signal, located on the MU-MIMO-OFDM time-frequency resource block, inserts the known pilot sequence of both the receiving and sending sides into the usable data before delivering the signal. Consequently, with the goal to determining the channel response at the pilot, the pilot signal as well as the usable data signal, respectively, can be recognized as the base station of the receiving end [XVI]. We explicitly define the adjacency matrix $A \in R^{N \times N,}$ where each entry A_{ij} denotes the presence or absence of a physical or logical connection between nodes i and j. Adjacency is established based on spatial proximity (antenna-user association) and frequency-domain correlation (adjacent subcarriers within the coherence bandwidth). Fig. 3 displays the architecture of the system. The terminal sends two frequency domain signals: F_s, that is the signal in the data frequency domain and F_p which is the pilot frequency domain signal. G is the additive white Gaussian noise, and CR represents the channel response. The base station receives the following signals: At the data location, R_S represents the estimated channel response based on the neural network, equation1 mentions R_p as the data frequency of the domain signal, C_S is the channel pilot frequency domain signal; at the pilot site, C_p represents the channel response. The recovered frequency domain signal is F, while the base station's antenna number is A.

$$R_p = \sum_{i=1}^{N} F_p R + G \tag{1}$$

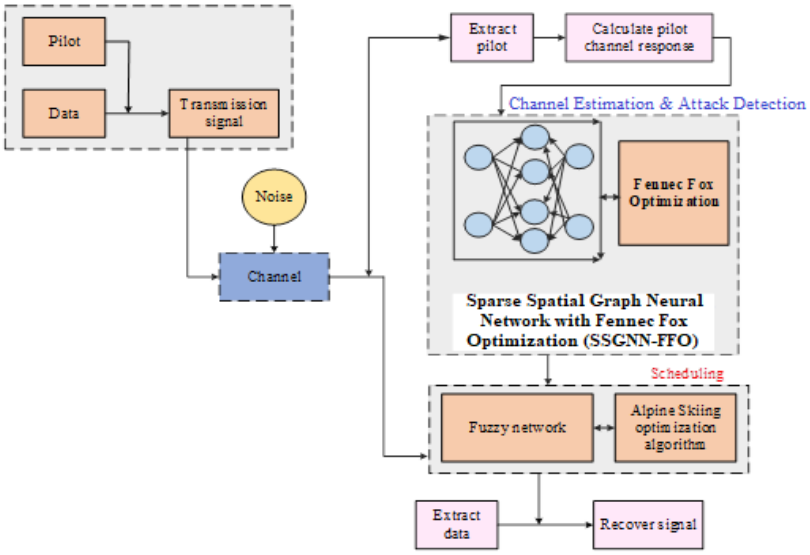

Fig 2. Proposed architecture

At the initial stage, the pilot's channel response is computed using the LS algorithm. The mathematical expression is represented by equation (2).

$$C_p = \frac{R_p}{F_p} \tag{2}$$

The LS technique does not account for noise while obtaining the channel response; noise is included in the produced information even if the algorithm's formula is

straightforward to compute. The data is then entered into the channel estimation model [XXIV] based on SSGNN-FFO after it has been obtained. In order to further recover the outgoing signal and go on to the security detection stage [XXXIX], the whole channel response estimation value can be achieved through training and learning.

B. Channel estimation and attack detection of SSGNN

The sparsity-awareness of SSGNN reduces computational complexity, making it ideal for real-time tasks like channel estimation, beamforming, and multi-user detection, while its graph-based architecture naturally handles irregular antenna configurations and dynamic interference patterns in MU-MIMO scenarios. The proposed system employs the SSGNN-FFO algorithm for channel estimation. This approach leverages the strengths of graph neural networks and the FFO algorithm to enhance the performance and security of WC Systems. The channel is represented as a graph, where nodes represent different elements such as antennas and subcarriers, and edges denote the relationships and dependencies between them [XII, XXIX, XXI, X].

The MU-MIMO-OFDM system is modeled as a graph $G = (V, \mathscr{E}, A)$, where V denotes the set of nodes, $\mathscr{E}$ denotes the set of edges, and $A \in R^{|V|\times|V|}$ is the adjacency matrix. Nodes represent users, antennas, and OFDM subcarriers. The adjacency matrix is fixed and defined as $A_{ij} = 1$, if a physically meaningful interaction exists, otherwise 0. The adjacency structure is fixed and deterministic, derived from system knowledge rather than learned during training.

Spatial connectivity links each user node u only to its serving antennas $S(u)$ [as $a \in S(u)$], while frequency-domain connectivity links subcarriers k, l satisfying $|f_k - f_l| \leq B_c$, where B_c is the coherence bandwidth. These physics-informed constraints enforce sparsity $\|A\|_0 \ll |V|^2$, reduce complexity, and prevent non-physical dependencies. For the SISO-OFDM configuration, the graph size is $|V| = N_u + N_s$. The sparse and interpretable graph structure that results facilitates the efficient transmission of messages while maintaining critical spatial-frequency correlations. The received signal at the MU-MIMO-OFDM [XXII] receiver can be expressed in equation (3):

$$y = Hx + n \tag{3}$$

where H is the channel matrix, n is the noise vector, and x is the transmitted signal vector.

The SSGNN uses a series of graph convolutional layers to learn the channel characteristics. The input to the network is the received pilot signal and the known pilot signal, which are used to train the network to predict the channel state information (CSI). Let $h_v^{(k)}$ represent the hidden state of node v at layer k in the graph neural network. SSGNN uses a series of self-nested layers with graph structures to model the complex relationships in the wireless channel [XVII, I, V]. The network leverages sparse spatial connections within the graph to efficiently process the received signals. The update rule for the hidden state can be expressed in equation (4):

$$h_v^{(k+1)} = \sigma\left(\sum_{u \in N(v)} a_{uv} W^{(k)} h_u^{(k)} + b^{(k)} \right) \tag{4}$$

where $\mathcal{N}(v)$ is the set of neighbours of node, a_{uv} is the edge weight between nodes u and v. $W^{(k)}$ and $b^{(k)}$ are the weight and bias parameters for layer and σ is the activation function.

The SSGNN-FFO model can detect attacks by identifying anomalies in the received signal. This is achieved by comparing the predicted CSI with the actual received signal.

A loss function can be used to measure the discrepancy between the predicted and actual CSI. The existence of an attack may be indicated if the loss crosses a specific threshold. An equation can be used to represent the loss function as shown below.

$$L(\theta) = \frac{1}{N}\sum_{i=1}^{N}|y_i - \hat{y}_i(\theta)| \tag{5}$$

Where Θ represents the parameters of the neural network, y_i and $\hat{y}_i$ are the actual, predicted signals, N represents the total number of samples respectively. We have identified the neighborhood $N_{(i)}$ explicitly from channel second-order statistics. Two nodes i and j are connected if their channel coefficients exhibit significant correlation:

$$N(i) = \{j | \frac{E[h_i h_j^*]}{\sqrt{E[|h_i|^2]\,E[|h_j|^2]}} \geq \tau\} \tag{6}$$

where τ is a correlation threshold derived from channel coherence properties. This statistically grounded neighbourhood ensures that message transmission occurs only across physically correlated channel components. Here, the edge weights are learnable but sparsity-masked, defined as $w_{ij} = A_{ij}\widetilde{w}_{ij}$; where $A_{ij} \in \{0,1\}$ is the fixed physics-informed adjacency matrix and $\widetilde{w}_{ij}$ is a trainable scalar parameter. This preserves physical sparsity while allowing adaptive weighting of correlated neighbours. Laplacian-normalized message passing employs the symmetrically normalized graph Laplacian to regulate information aggregation across nodes. The message-transmission rule using the normalized graph Laplacian is reformulated. Let,

$$L = I - D^{-1/2}AD^{-1/2} \tag{7}$$

where D is the degree matrix. The update rule in equation (8) is revised as (ensuring spectral stability and scale-invariant message propagation),

$$H^{(l+1)} = \sigma(D^{-1/2}AD^{-1/2}H^{(l)}W^{(l)} + b^{(l)}) \tag{8}$$

where $H^{(l)} \in R^{|V| \times F_l}$ is the node feature matrix at layer l, $A \in \{0,1\}^{|V| \times |V|}$ is the fixed physics-informed adjacency matrix derived from channel statistics; D is the degree matrix with $D_{ij} = \sum_j A_{ij}$; $W^{(l)} \in R^{F_l \times F_{l+1}}$ and $b^{(l)} \in R^{F_{l+1}}$ are trainable weights and bias respectably; σ(·) denotes a nonlinear activation function.

IV. Dataset and Performance Parameters for SSGNN-FFO Technique

The simulation experiment of this part is conducted in the 5G toolbox running in MATLAB, using the Rayleigh channel model. The SSGNN uses graph-projected representation, controlling dimensionality via sparse neighborhoods. Model capacity grows with graph integration, not just neuron count. Sparsity becomes a structural constraint with Laplacian-normalized propagation.

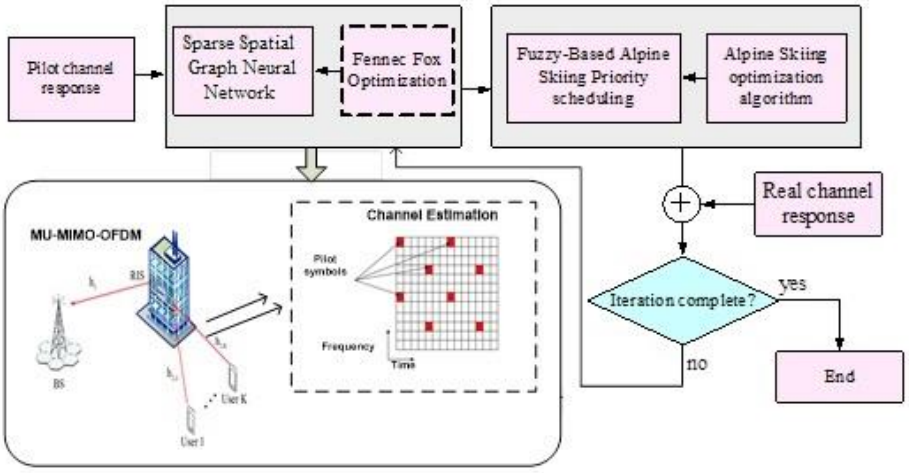

Fig 3. System architecture

During the training stage, when a certain number of signals is generated for a predetermined signal-to-noise ratio, 20,000 signals in total are generated as the training set. The training dataset is separated into validation and training sets to avoid overfitting. The validation data is used to track the trained neural network's performance at preset intervals, like five times per epoch, whereas the training set is used to train and test the model. The training process should conclude when the validation loss stops reducing and the model is no longer improving. In this research, training accounts for 80% of the dataset, with the remaining 20% being used for testing. The channel parameters and values are explained in Table 1. MATLAB 5G Toolbox permits customization and the SSGNN-FFO model requires datasets to create a variety of waveforms, antennas, and channel models. The dataset used in this research to train the DL-based channel estimation models was generated via the SSGNN-FFO Data Synthesis in 5G Channel Estimation [XXXV, III] reference example in MATLAB5G toolbox.

The single-input single-output (SISO) antenna approach is applied with the physical downlink shared channel (PDSCH) and demodulation reference signal (DM-RS) to generate the channel estimate. The reference example in the toolbox sends and receives the signal 256 times, generating 256 training datasets for the DL-based channel estimation system. Each dataset consists of 8568 data points (612 subcarriers × 14 OFDM symbols) with 1 antenna. To provide distinct inputs to the neural network during training, this approach transforms each complex-valued (I/Q) 612×14 matrix into a real-valued 612×14×2 matrix, separating the real and imaginary parts.

Systems for wireless communication rely on complex numbers. In digital wireless communication, complex numbers are used to modulate and demodulate wireless transmissions due to their ability to represent multiple dimensions. In contrast, adversarial machine learning attacks typically operate in the real number domain, using real numbers to overcome the decision boundaries of target deep learning models.

Table 1: Channel parameters

Parameters	Values
Modulation	16QAM
Number of transmit antennas	1
Number of receive antennas	1
Fading distribution	Rayleigh
Polarization	Co-polar
Direction of transmission	downlink
Windowing	36
Maximum Doppler shift	5-400 Hz
NFFT	1024
Delay spread	1-300ns

V. Result Analysis

The performance metrics that were evaluated in the proposed approach are given below,

(i) MSE

A performance indicator called Mean Squared Error (MSE) is used to assess and contrast with existing methods. The MSE formula is provided below. The mean squared deviation between the expected and observed values is computed. The MSE is equal to zero when a model is error-free. As the model error increases, so does the MSE value. The MSE value rises in tandem with the model error. This can be expressed in equation (6),

$$MSE" = \frac{\sum (k_m - \hat{k}_m)^2}{t} \tag{6}$$

where, t represents the total number of instances, k_m represents the actual m^{th} instance, and $\hat{k}_m$ represents the predicted m^{th} instance.

(ii) Attack Success Ratio (ASR)

Next, the ASR was used as the performance indicator. The ASR is the ratio of test samples that an attacker could misinterpret to the total number of test samples. The most effective attack is the one with the highest ASR. The formula for calculating ASR is as follows:

$$ASR" = \frac{1}{m"} \sum_{j=0}^{m"} \frac{MSE"(x_{(j)}^{adv}, K_{(j)}) - MSE(x_{(j)}, k_{(j)})}{MSE"(x_{(j)}^{adv}, k_{(j)})} \tag{7}$$

where, $m"$ represents the total number of test samples $x_{(j)}$ represents the original input data sample at index j $k_{(j)}$ represents the corresponding true label for the original input

data sample at index j, $x_{(j)}^{adv}$ represents the adversarial input data sample at index j which is crafted by perturbing the original input data to deceive the model.

(iii) Attack detections

Table 2 displays experimental results for the suggested strategy. According to the experimental findings, the suggested strategy can raise the channel estimate model's accuracy.

Table 2: Analysis in terms of attacks

Attack types	MSE		Attack Success Ratio (ASR)
	Benign input	Malicious input	
Basic Iterative Method (BIM)	0.027863	0.029183	0.066458
Fast Gradient Sign Method (FGSM)	0.027859	0.030103	0.095987
Momentum Iterative Method (MIM)	0.027857	0.029227	0.068912
Projected Gradient Descent (PGD)	0.027860	0.029178	0.066410
Carlini & Wagner (C&W)	0.027261	0.027405	0.00791

The results showcase the effectiveness of the proposed strategy in generating potent attacks, which in turn, improves the accuracy of the channel estimation model. Our findings indicate that the suggested approach outperforms existing methods, including FGSM, BIM, MIM, PGD, and C&W attacks. Notably, a defensive distillation-based deep learning model is employed to defend against all these attacks. The empirical results demonstrate the efficacy of the proposed mitigation strategy in enhancing the precision of the channel estimation model against various adversarial attacks. The adversarial model assumes bounded perturbations on pilot or CSI representations, mimicking low-power pilot contamination or interference. This study focuses on feature-domain attacks, providing a conservative estimate of estimator robustness under realistic distortion limits, rather than exploring waveform-domain spoofing.

Instead, FFO is used for low-dimensional hyperparameter and structural optimization, while gradient descent is used for network training. Table 3 outlines the optimization methods and dimensionality of various components in the SSGNN-FFO model. It shows that network weights are optimized using gradient descent (Adam) and have high dimensionality (hundreds), while components like graph sparsity level, learning rate, and dropout/regularization are optimized using FFO and have low dimensionality (1-3 or discrete/low values).

FFO optimizes hyperparameters θ_{hyper} to minimize loss L *(equation (8))*. Network weights (W) are optimized separately via gradient descent. This bilevel optimization approach allows FFO to focus on hyperparameter tuning.

$$\min_{\theta_{\text{hyper}}} \mathcal{L}\left(\mathbf{W}^*(\theta_{\text{hyper}})\right) \quad (8)$$
$$\Rightarrow \mathbf{W}^* = \arg\min_{\mathbf{W}} \mathcal{L}(\mathbf{W})$$

Table 3: Optimization Methods and Dimensionality of SSGNN-FFO Model Components

Component	Optimization Method	Dimensionality
Network weights (W, b)	Gradient descent (Adam)	High (hundreds)
Graph sparsity level (τ)	FFO	Low (1–3)
Learning rate (η)	FFO	Low
Hidden feature size	FFO	Discrete
Dropout / regularization	FFO	Low

Table 4 presents the performance of a communication systems at different signal-to-noise ratio (SNR) levels, measured in decibels (dB). As the SNR increases from 0 to 9 dB, both Bit Error Rate (BER) and Mean Squared Error (MSE) decrease significantly. Higher SNR levels result in lower BER and MSE values, indicating better system performance with fewer bit errors and more accurate predictions or estimations. This trend shows that improvements in SNR lead to enhanced quality and efficiency in signal transmission and processing.

Table 4: Analysis with respect to SNR

SNR (dB)	BER	MSE
0	0.88376	0.015667
3	0.034768	0.007870
5	0.010103	0.003915
7	0.002025	0.001950
9	0.000356	0.000976

Table 5: Comparative analysis between existing and proposed system

Approaches	Encryption time (s)	Decryption time (s)	Security level (%)
Diffie Hellman	1.63	1.25	82
Elliptic Curve Cryptography (ECC)	1.02	0.68	92
Modified ECC (MECC)	0.45	0.25	96.1
Proposed method	0.37	0.19	98.4

It is observed that from table 5, the proposed method outperforms existing cryptographic approaches (Diffie-Hellman, ECC, MECC) with the lowest encryption time (0.37s), the lowest decryption time (0.19s), and the highest security level (98.4%). Its exceptional speed and security make it a superior choice for cryptographic

applications. This method's efficiency and robust security positioning suggest potential for widespread adoption in secure data transmission. Overall, it offers a compelling solution for enhancing cryptographic performance.

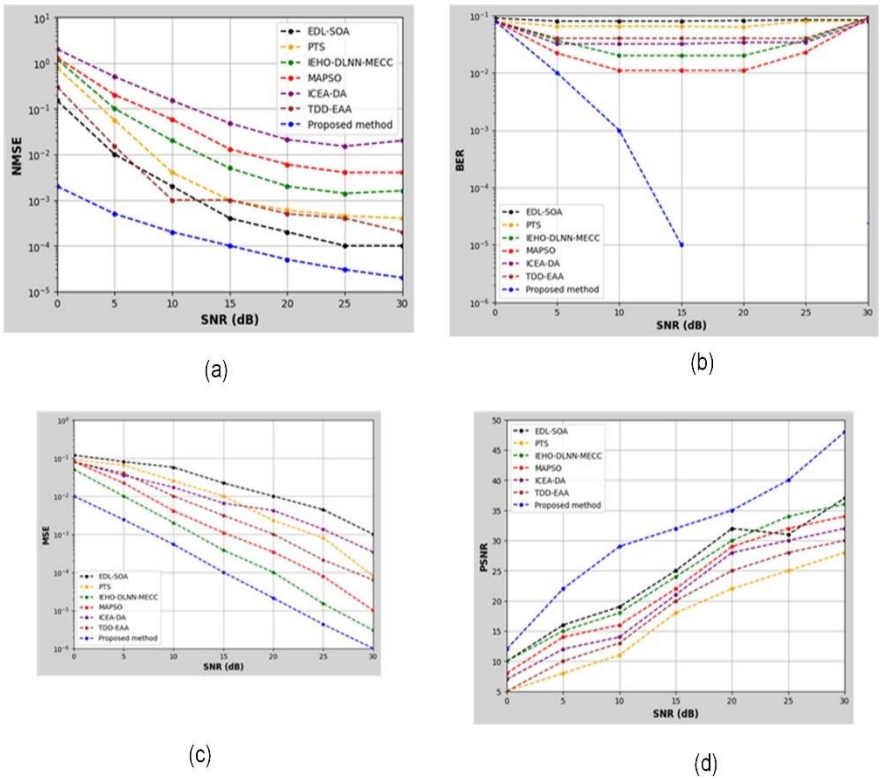

Fig 4. Comparison between Proposed and Existing Methods (a) NMSE vs SNR (b) SNR vs BER(c) MSE vs SNR (d) PSNR vs SNR

Fig. 4(a) compares the proposed methodology with existing approaches like Enhanced Deep Learning-based Signal Optimization Algorithm (EDL-SOA) and Pelican Tunicate Swarm (PTS) in terms of signal reconstruction quality (NMSE) and SNR (dB). The graph shows a negative correlation, where lower NMSE leads to lower BER, indicating better signal reconstruction. Notably, the proposed method achieves lower NMSE compared to most existing approaches, suggesting potentially better signal reconstruction and improved SNR.

Fig. 4(b) depicts a comparison of signal processing techniques, including the proposed methodology, in terms of SNR and BER. A negative correlation is visible - higher SNR coincides with lower BER, as a stronger signal is less susceptible to noise corruption. The proposed methodology outperforms existing approaches (EDL-SOA, PTS, etc.) with a higher SNR and lower BER, suggesting more efficient signal transmission with minimal errors. The clustered data points indicate consistency in performance.

Fig. 4(c) compares the proposed methodology with existing approaches (EDL-SOA, PTS, etc.) in terms of signal reconstruction quality (MSE) vs. SNR. The plot shows the expected trend: lower MSE (better reconstruction) corresponds to higher SNR (stronger

signal). The proposed methodology's data points cluster towards lower MSE and higher SNR, indicating superior performance in reconstructing signals with less error at higher noise levels.

Fig. 4(d) displays a comparative analysis of PSNR vs. SNR for the proposed methodology and established techniques (EDL-SOA, PTS, etc.). PSNR indicates received signal fidelity, while SNR represents signal power to noise ratio. The plot shows how the proposed approach fares against existing methods under varying noise conditions. Higher PSNR values signify superior signal quality, suggesting the proposed methodology enhances signal fidelity in MU-MIMO-OFDM systems.

Table 6: Comparison of BER, MSE NMSE and PSNR

Techniques	BER	MSE	NMSE	PSNR(dB)
EDL-SOA	0.04	0.000006	0.0000088	40
PTS	0.0009	0.0002	0.0005	30
IEHO-DLNN-MECC	0.007	0.00034	0.00008	30
MAPSO	0.0004	0.008	0.00006	38
ICEA-DA	0.00036	0.00049	0.03	43
TDD-EAA	0.00045	0.00078	0.001	39
PROPOSED METHOD	*0.00012*	*0.00023*	*0.001*	*45*

Table 6 compares techniques (EDL-SOA, PTS, MAPSO, ICEA-DA, TDD-EAA, Proposed Method) using BER, NMSE, MSE, and PSNR. EDL-SOA shows moderate results (BER: 0.04, PSNR: 40 dB). PTS has low BER (0.0009) but higher MSE (0.0002) and NMSE (0.0005). MAPSO and ICEA-DA have strong BER (0.0004, 0.00036) but elevated MSE/NMSE. TDD-EAA balances BER (0.00045), MSE (0.00078), PSNR (39 dB).

The proposed method outperforms others with the lowest BER (0.00012), low MSE (0.00023), NMSE (0.001), and highest PSNR (45 dB), showing exceptional accuracy and signal quality. Its minimal error rates and outstanding clarity make it most reliable for high-performance communication systems. This superior performance indicates potential for improved data transmission in real-world applications. The method's efficiency could benefit systems requiring robust signal processing.

VI. Conclusion

This study leveraged Sparse Spatial Graph Neural Networks (SSGNN) with Fennec Fox Optimization (FFO) for secure and efficient channel estimation in MU-MIMO-OFDM systems. The SSGNN-FFO model demonstrated exceptional performance, achieving a BER of 0.00012, MSE of 0.00023, NMSE of 0.001, and PSNR of 45 dB, outperforming existing approaches. The model showed robustness against adversarial attacks, with defensive distillation techniques further enhancing its

security. The proposed method ensures secure and efficient channel estimation, making it suitable for next-gen wireless networks. Future work can build on these findings to develop more robust AI-driven defenses and explore applications in IRS and spectrum sensing, ultimately paving the way for reliable and secure wireless communications. The SSGNN-FFO approach offers a promising solution for addressing channel estimation challenges in complex wireless environments. Its superior performance and security features position it as a key enabler for future wireless technologies. Overall, this research advances the state-of-the-art in MU-MIMO-OFDM channel estimation, contributing to the development of secure and efficient wireless systems.

Funding Declaration

The author(s) declare that no funds, grants, or other support were received during the preparation of this manuscript.

Conflict of Interest:

There was no relevant conflict of interest regarding this paper.

References

I. Bernstein, Daniel J., and Tanja Lange. "Faster Addition and Doubling on Elliptic Curves." *Advances in Cryptology – ASIACRYPT 2007*, edited by Kaoru Kurosawa, Lecture Notes in Computer Science, vol. 4833, Springer, 2007, pp. 29–50. 10.1007/978-3-540-76900-2_3.

II. Catak, F. O., et al. "Defensive Distillation-Based Adversarial Attack Mitigation Method for Channel Estimation Using Deep Learning Models in Next-Generation Wireless Networks." *IEEE Access*, vol. 10, 2022, pp. 98191–98203. 10.1109/ACCESS.2022.3206385.

III. Chitikena, R., and P. E. Rani. "Deep Learning-Based Channel Estimation and Secure Data Transmission Using IEHO-DLNN and MECC Algorithm in MU-MIMO OFDM System." *Wireless Personal Communications*, vol. 129, no. 4, 2023, pp. 2269–2289. 10.1007/s11277-023-10172-2.

IV. Dehmollaian, E., et al. "Using Channel State Information for Physical Tamper Attack Detection in OFDM Systems: A Deep Learning Approach." *IEEE Wireless Communications Letters*, vol. 10, no. 7, July 2021, pp. 1503–1507. 10.48550/arXiv.2011.03573.

V. Diffie, W., and M. Hellman. "New Directions in Cryptography." *IEEE Transactions on Information Theory*, vol. 22, no. 6, Nov. 1976, pp. 644–654, https://ee.stanford.edu/~hellman/publications/24.pdf.

VI. Farzamnia, A., N. W. Hlaing, M. K. Haldar, and J. Rahebi. "Channel Estimation for Sparse Channel OFDM Systems Using Least Square and Minimum Mean Square Error Techniques." *Proceedings of the 2017 International Conference on Engineering and Technology (ICET)*, Antalya, Turkey, 2017, pp. 1–5. IEEE. 10.1109/ICEngTechnol.2017.8308193.

VII. Gao, J., C. Zhong, G. Y. Li, and Z. Zhang. "Deep Learning-Based Channel Estimation for Massive MIMO with Hybrid Transceivers." *IEEE Transactions on Wireless Communications*, vol. 21, no. 7, 2022, pp. 5162–5174. 10.1109/TWC.2021.3137354.

VIII. Giannopoulos, T., and V. A. Paliouras. "A Low-Complexity PTS-Based PAPR Reduction Technique for OFDM Signals without Transmission of Side Information." *Journal of Signal Processing Systems*, vol. 56, 2009, pp. 141–153. 10.1007/s11265-008-0238-y.

IX. Jiang, W., et al. "Massive Connectivity over MIMO-OFDM: Joint Activity Detection and Channel Estimation with Frequency Selectivity Compensation." *IEEE Transactions on Wireless Communications*, vol. 21, no. 9, 2022, pp. 6920–6934. 10.1109/TWC.2022.3153106.

X. Kapileswar, N., and P. P. Kumar. "Optimized Deep Learning Driven Signal Detection and Adaptive Channel Estimation in Underwater Acoustic IoT Networks." *International Journal of Communication Systems*, vol. 37, no. 4, 2024, e5673. 10.1002/dac.5673.

XI. Ke, X. "Optical Wireless MIMO Technology and Space–Time Coding." *Handbook of Optical Wireless Communication*, Springer, 2023. 10.1007/978-981-97-1522-0_19.

XII. Khani, M., et al. "Adaptive Neural Signal Detection for Massive MIMO." *IEEE Transactions on Wireless Communications*, vol. 19, no. 8, Aug. 2020, pp. 5635–5648, https://www.studocu.com/row/document/tribhuvan-university/digital-control-system/adaptive-neural-signal-detection/98560254.

XIII. Kundu, N. K., et al. "Channel Estimation and Secret Key Rate Analysis of MIMO Terahertz Quantum Key Distribution." *IEEE Transactions on Communications*, vol. 70, no. 5, 2022, pp. 3350–3363. 10.1109/TCOMM.2022.3161008.

XIV. Liu, C., et al. "Comprehensive Graph Gradual Pruning for Sparse Training in Graph Neural Networks." *IEEE Transactions on Neural Networks and Learning Systems*, 2023. arXiv:2207.08629.

XV. Liu, Q., et al. "Adversarial Attack on DL-Based Massive MIMO CSI Feedback." *Journal of Communications and Networks*, vol. 22, no. 3, 2020, pp. 230-235. https://researchportal.hkust.edu.hk/en/publications/adversarial-attack-on-dl-based-massive-mimo-csi-feedback/.

XVI. Manohar, K., et al. "Data-Driven Sparse Sensor Placement for Reconstruction: Demonstrating the Benefits of Exploiting Known Patterns." *IEEE Control Systems Magazine*, vol. 38, no. 3, 2018, pp. 63–80. 10.1109/MCS.2018.2810460.

XVII. Mayouche, A., W. A. Martins, S. Chatzinotas, and B. Ottersten. "Data-Driven Precoded MIMO Detection Robust to Channel Estimation Errors." *IEEE Open Journal of the Communications Society*, vol. 2, 2021, pp. 1144–1157. 10.1109/OJCOMS.2021.3079643.

XVIII. Muni, N. B., et al. "Integrating Edge Computing with Swarm Intelligence for Efficient IoT Device Management." *Proceedings of the 3rd International Conference on Data Science and Information System (ICDSIS)*, Hassan, India, 2025, pp. 1–5. IEEE. 10.1109/ICDSIS65355.2025.11070424.

XIX. Nandi, S., A. Nandi, and N. N. Pathak. "Channel Estimation of Massive MIMO-OFDM System Using Elman Recurrent Neural Network." *Arabian Journal for Science and Engineering*, vol. 47, 2022, pp. 9755–9765. 10.1007/s13369-021-06366-0.

XX. Nandi, S., A. Nandi, and N. N. Pathak. "Deep Learning Assisted Technology for MIMO-OFDM 5G Application." *Proceedings of the International Conference on Computational Intelligence and Sustainable Technologies*, 2022. 10.1007/978-981-16-6893-7.

XXI. Nandi, S., A. Nandi, and N. N. Pathak. "Spectrally Efficient MIMO-OFDM for THz Communication in FANETs." *Proceedings of the 14th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Delhi, India, 2023, pp. 1–7. 10.1109/ICCCNT56998.2023.10306931

XXII. Nandi, S., et al. "Performance Analysis of Cyclic Prefix OFDM Using Adaptive Modulation Techniques." *International Journal of Electrical, Electronics and Computer Systems*, vol. 6, no. 8, 2017, pp. 214-220. https://zenodo.org/record/5274429/files/J1_2017_IJEECS.pdf.

XXIII. Nandi, S., N. N. Pathak, and A. Nandi. "A Novel Adaptive Optimized Fast Blind Channel Estimation for Cyclic Prefix Assisted Space–Time Block Coded MIMO-OFDM Systems." *Wireless Personal Communications*, vol. 115, 2020, pp. 1317–1333. 10.1007/s11277-020-07629-z.

XXIV. Nandi, S., N. N. Pathak, and A. Nandi. "Analysis of Hard Decision and Soft Decision Decoding Mechanism Using Viterbi Decoder in Presence of Different Adaptive Modulations." *International Journal of Future Generation Communication and Networking*, vol. 13, no. 3, 2020, pp. 3002–3012. 10.5281/zenodo.5273662.

XXV. Nandi, S., N. N. Pathak, and A. Nandi. "Avenues to Improve Channel Estimation Using Optimized CP in STBC Coded MIMO-OFDM System—A Global Optimization Approach." *Proceedings of the 5th International Conference on Microelectronics, Computing and Communication Systems (MCCS)*, Ranchi, India, 2020. 10.1007/978-981-16-0275-7_21.

XXVI. Nandi, S., N. N. Pathak, and A. Nandi. "Efficacy of Channel Estimation and Efficient Use of Spectrum Using Optimised Cyclic Prefix (CP) in MIMO-OFDM." *International Journal of Engineering and Advanced Technology*, vol. 9, no. 2, 2019, pp. 3032–3038. 10.35940/IJEAT.B4093.129219.

XXVII. Nandi, S., N. N. Pathak, and A. Nandi. "Implementation of Adaptive Optimized Fast Blind Channel Estimation of MIMO-OFDM Systems Using MFPA." *Intelligent Multi-Modal Data Processing*, Wiley, 2020, pp. 165–188. 10.1002/9781119571452.ch8.

XXVIII. Sarkar, M., and S. Ghosh. "Development of a Secured Optical Code Division Multiple Access System by Implementing Hybrid 2D Modified Walsh Code." *Optical Engineering*, vol. 59, no. 10, 2020, p. 106107. 10.1117/1.OE.59.10.106107.

XXIX. Sarkar, M., and S. Ghosh. "Implementation of Designed OCDMA Code in RoF for Future 5G Communication." *Journal of Optics*, 2024. 10.1007/s12596-024-01813-1.

XXX. Shankar, R., S. Nandi, and A. Rupani. "Channel Capacity Analysis of Non-Orthogonal Multiple Access and Massive Multiple-Input Multiple-Output Wireless Communication Networks Considering Perfect and Imperfect Channel State Information." *Journal of Defense Modeling and Simulation*, vol. 19, no. 4, 2021, pp. 771–781. 10.1177/15485129211000139.

XXXI. Sivadas, N. A. "PAPR Reduction of OFDM Systems Using H-SLM Method with a Multiplier-Less IFFT/FFT Technique." *ETRI Journal*, vol. 44, 2022, pp. 379–388. 10.4218/etrij.2020-0316.

XXXII. Soni, C., and N. Gupta. "An Optimized Sequence for Sparse Channel Estimation in a 5G MIMO System." *International Journal of Electronics*, 2024, pp. 1–23. 10.1080/00207217.2024.2408797.

XXXIII. Tang, R., C. Qi, and P. Zhang. "Block Sparse Channel Estimation Based on Residual Difference and Deep Learning for Wideband MmWave Massive MIMO." *Proceedings of the IEEE 97th Vehicular Technology Conference (VTC-Spring)*, Florence, Italy, 2023, pp. 1–6. 10.1109/VTC2023-Spring57618.2023.10200898.

XXXIV. Trojovská, E., M. Dehghani, and P. Trojovský. "Fennec Fox Optimization: A New Nature-Inspired Optimization Algorithm." *IEEE Access*, vol. 10, 2022, pp. 84417–84443. 10.1109/ACCESS.2022.3197745.

XXXV. Venkateswarlu, C., and N. V. Rao. "An Efficient MAPSO Model for Interference Cancellation and Optimal Channel Estimation in MIMO-OFDM System." *Wireless Personal Communications*, vol. 128, no. 1, 2023, pp. 283–307. 10.1007/s11277-022-09955-w.

XXXVI. Wu, H., X. Li, and Y. Deng. "Deep Learning-Driven Wireless Communication for Edge-Cloud Computing: Opportunities and Challenges." *Journal of Cloud Computing*, vol. 9, no. 1, 2020, p. 21. 10.1186/s13677-020-00168-9.

XXXVII. Yuan, Y., et al. "Alpine Skiing Optimization: A New Bio-Inspired Optimization Algorithm." *Advances in Engineering Software*, vol. 170, 2022, p. 103158. 10.1016/j.advengsoft.2022.103158.

XXXVIII. Zhang, M., and P. Li. "Nested Graph Neural Networks." *Advances in Neural Information Processing Systems*, vol. 34, 2021, pp. 15734-15747. 10.48550/arXiv.2110.13197.

XXXIX. Zheng, K., and X. Ma. "Designing Learning-Based Adversarial Attacks to MIMO-OFDM Systems with Adaptive Modulation." *IEEE Transactions on Wireless Communications*, 2023. https://www.scribd.com/document/744142171/Designing-Learning-Based-Adversarial-Attacks-to-MIMO-OfDM-Systems-With-Adaptive-Modulation.