International Journal of Mathematical, Engineering and Management Sciences
Vol. 11, No. 3, 1346-1369, 2026
https://doi.org/10.33889/IJMEMS.2026.11.3.055

Towards Intelligent and Secure Beam Alignment: A Deep Learning Perspective for 5G

Parul Dubey
Computer Science and Engineering Department,
Symbiosis Institute of Technology, Nagpur Campus,
Symbiosis International (Deemed University), Pune, Maharashtra, India.
E-mail: dubeyparul29@gmail.com

Pushkar Dubey
Department of Management,
Pandit Sundarlal Sharma (Open) University, Bilaspur, Chhattisgarh, India.
E-mail: drdubeypkag@gmail.com

Gagandeep Kaur
Computer Science and Engineering Department,
Symbiosis Institute of Technology, Nagpur Campus,
Symbiosis International (Deemed University), Pune, Maharashtra, India.
Corresponding author: gaganarora9@gmail.com

(Received on June 18, 2025; Revised on November 8, 2025 & January 8, 2026 & February 12, 2026;
Accepted on March 25, 2026)

Abstract
Massive multiple-input multiple-output (mMIMO) systems are the backbone of modern-day wireless communication due to their potential to utilize spectrum efficiently and increase network capacity. Secure and optimal beam selection is key to interference and security challenges in dense urban areas, especially with the arrival of 5G and beyond. Classical solutions such as exhaustive beam search or even statistical models have high computational complexity and are not so flexible to dynamic situations. This study generated simulated data based on the realistic distribution of the users and the phenomena of the terrestrial. The data set records common metrics like the user locations, channel states, and beamforming settings. We propose a deep-learning framework that predicts top-K transmit–receive beam pairs using only receiver location and then enforces physical-layer security (PLS) by filtering out pairs that violate an eavesdropper-power threshold. On simulated DeepMIMO-inspired scenes, our model attains Top-1/Top-5/Top-10 accuracies of 69.51%/85.32%/92.43%, cuts beam-search overhead by 92.19%, and reduces mean execution time to 95 ms. With security constraints, it approaches achievable bounds for Probability of Successful Detection (PSD)/ Probability of Secure Signal Detection (PSSD) and reduces estimated eavesdropping probability from 15.6% to 5.2%, while improving secrecy capacity and Bit Error Rate (BER). The novelty is a security-constrained beam selection loop integrated directly into initial access, requiring low CSI and remaining deployable within 5G NR procedures.

Keywords- Reference signal received power (RSRP), Security constraints, Top-K beam selection, Massive multiple-input-multiple-output (mMIMO).

1. Introduction

The commercial rollout of 5G networks has enabled a diverse range of applications and continues to evolve beyond 5G with scientific studies driven by revolutionary state-of-the-art changes in wireless communication, emphasizing ultra-high speeds, low latency, and massive connectivity (Kumar and Chavhan, 2022). The first Tx-Rx recovery problem is one of the main factors determining the effectiveness and security of subsequent communication stages. This procedure, referred to as beam management, is a fundamental tool for achieving adaptive spectral efficiency and QoS guarantees in highly time-varying environments (Brilhante et al., 2023; Li et al., 2020). Nevertheless, massive multiple-input multiple-output

(mMIMO) antenna systems have been increasingly deployed, adding further complexity to these challenges and necessitating novel approaches to address latency, energy expenditure, and vulnerability to eavesdropping attacks (Heng et al., 2021; Wang et al., 2025).

In a 5G New Radio (NR) system, beam management consists of various stages, including beam sweeping, measurement, reporting, and finally beam alignment (Ali et al., 2021; Giordani et al., 2020). Thus, an exhaustive search method for beam alignment is more resource-consuming than conventional methods, especially for a large number of antenna elements and beams (Attaoui et al., 2022; Giordani et al., 2019). Moreover, existing beam alignment schemes typically try to maximize signal strength while ignoring Physical-Layer Security (PLS), thereby compromising the security and making the system vulnerable to illicit interception (Wu et al., 2018). PLS has recently arisen as a counterpart to cryptographic techniques and exploits channel and signal attributes to obtain data confidentiality (Hamamreh et al., 2019). This has motivated the exploration of machine learning (ML), particularly Deep Learning (DL) methods, to address beam selection and management, where nonlinear relationships can effectively model complex propagation environments (Alrabeiah and Alkhateeb, 2020; Nguyen et al., 2022; Polese et al., 2021).

Current ML-based approaches primarily employ user geolocation, received signal strength indicator (RSSI), and other similar channel information to determine the optimal beam pair. Although these methods have been shown to be highly beneficial in terms of accuracy and computational efficiency, security aspects are often ignored, or the approaches rely on large amounts of channel state information (CSI), which may not be available or feasible in real-world implementations (Adesina et al., 2023; Chafaa et al., 2022; Ganji et al., 2024).

In this work, we propose a DL-based method for secure and efficient beam alignment. **Figure 1** illustrates the proposed framework. This study is distinct in its use of DL to design a unified framework that jointly addresses security and performance requirements for beam alignment in 5G and beyond systems. The novelty of this paper lies in explicitly incorporating security constraints into the beam selection process while maintaining high predictive accuracy. Notably, the proposed framework introduces physical-layer security into the beam selection process without requiring hardware modifications or extensive channel state information. It further aims to reduce beam search overhead and power consumption in secure communications by identifying eavesdropper avoidance directions at the initial stage of beam alignment, a capability not explored in prior works. To the best of our knowledge, this is the first approach proposed to address secure initial access in 5G that is both efficient and flexible. The key technical contributions of this work include, but are not limited to:

- Secure Beam Alignment: A DL-based method to ensure secure communication by optimizing the pairing of beams so as to enhance the desired user's signal strength while reducing the risk of eavesdropping with no changes to 5G NR standards.
- Efficient Beam Search: Up to 92.19% reduction in beam search overhead was achieved, enabling much lower latency, and energy consumption for initial access.
- Minimal Input, Highly Adaptive: By using just receiver location data, it has shown adaptability and generalizability in a large variety of scenarios under both realistic and statistical models.

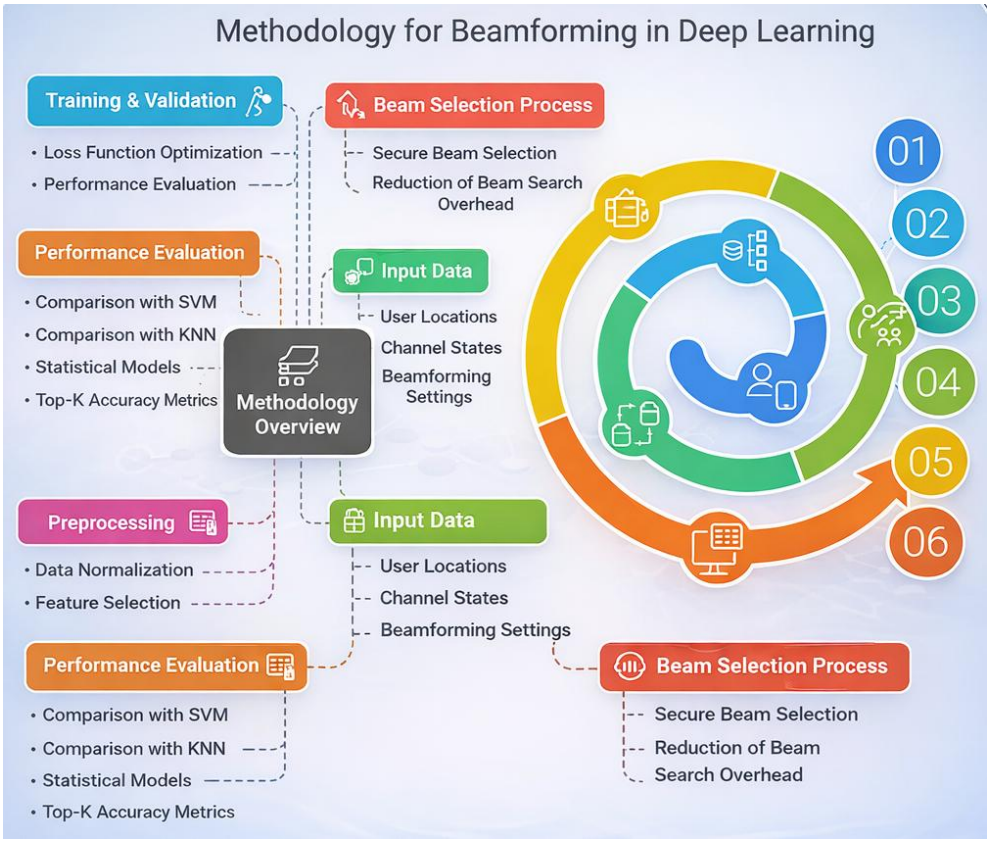

Figure 1. Figure of abstract-methodology for beamforming in DL.

2. Related Work

Recently, DL has been identified as an effective approach for physical-layer security (PLS)–aware beam alignment in 5G frameworks, offering both robustness and reliability. Beamforming problems have traditionally been solved by exhaustive search algorithms and statistical model analysis on the one side, and machine learning-based approaches on the other. Often, present methods struggle with computational complexity and can hardly adapt to dynamic environments. From this perspective, DL emerges as an attractive niche to make beamforming more secure and efficient for the 5G-and-beyond networks, due to its predictive capability.

PLS safeguards data transmission at the physical layer, independently of traditional cryptographic mechanisms. Rather than relying on encryption-based techniques, PLS leverages signal processing methods at the physical layer to ensure confidential communication, thereby mitigating unauthorized interception by eavesdroppers (Liu et al., 2024; Sharma and Kumar, 2023). On the other hand, DL opens up possibilities for dynamically and empirically detecting and counteracting security intrusions in 5G networks (Dai et al., 2025). DL-based beam alignment techniques can automatically adjust the beam selection dynamically for better performance, leveraging huge databases and deep neural networks (Lv et al., 2021; Sharma and Kumar, 2023).

Beamforming is commonly employed in beam alignment to obtain directional links, ensuring that signals are primarily received by authorized users. DL-based beamforming methods, such as ResNeSt-based

models, have been shown to improve efficiency by reducing computational complexity while supporting robust security mechanisms (Chafaa et al., 2022; Ganji et al., 2024). In addition to beam processing, an important application of DL is in the initial beam selection phase where instead of an exhaustive search, DL can be employed to identify the most suitable group of beam pairs (Riza et al., 2025). Multilayer Perceptron (MLP) models have been applied to this task, where beam pairs are ranked based on the location of receiver (Cousik et al., 2021; Ozmat et al., 2024). This approach reduces communication costs and energy consumption while maintaining high accuracy. DL-based 3D beamforming is considered advantageous in maximizing secrecy rates over classical 2D beamforming, primarily due to the inaccuracy of channel state information (CSI). By modeling beams in three dimensions, this approach introduces an inherent additional layer of security in environments characterized by severe multipath propagation, thereby motivating its extension to future 5G and 6G systems (Teng and Zhang, 2024; Yang et al., 2021).

Further advances have been achieved in enhancing both performance and security of beam alignment through DL-based solutions. When DL is employed in beam selection methods, it results in significantly lower signaling overhead and reduced computational complexity compared to conventional beam selection techniques, thereby decreasing overall network overhead (Lv et al., 2021). DL-based approaches also enable highly accurate and precise beam selection, minimizing interference between transmitters and receivers. Moreover, compared to FCM-based schemes, DL-based methods can not only prevent heterogeneous attacks but also adjust the strength of a signal for unintended users with extreme precision. Addressing the above eavesdropping dilemma can make the network more secured (Ozmat et al., 2024).

However, several challenges still persist in DL-based beam alignment models. Adversarial attacks, in which adversaries change input data to diminish model performance, are one of the main concerns for DL models. Many ideas have been put forward to make DL-based security models more resistant to these threats (Kim et al., 2021; Kuzlu et al., 2023). These ideas include adversarial training and defensive distillation. Another key issue is the adaptability of DL models to varying network conditions. This is because models must be updated all the time in real 5G deployments to keep working at their best (Bendjillali et al., 2023; Lv et al., 2021). Despite advancements in beamforming and DL-based wireless security, several key challenges remain:

(i) Limited PLS Integration: Most beam alignment methods optimize efficiency but do not incorporate security constraints (Liu et al., 2024; Sharma and Kumar, 2023).
(ii) High Computational Complexity: Traditional exhaustive beam search is impractical for large-scale mMIMO systems (Lv et al., 2021; Ozmat et al., 2024).
(iii) CSI Dependency: Many DL-based methods rely on extensive CSI, which is often unavailable due to interference and hardware limitations (Bendjillali et al., 2023; Ozmat et al., 2024).
(iv) Adversarial Vulnerabilities: Existing DL models are susceptible to attacks, leading to security risks in beam selection (Cousik et al., 2021; Yang et al., 2021).
(v) Lack of Real-Time Adaptability: Current models fail to adjust to dynamic network conditions, affecting performance in user mobility scenarios (Kim et al., 2021).

Effective and secure beam alignment in mMIMO systems continues to be a significant challenge for enabling emerging 5G and beyond wireless access networks. Classical approaches, such as exhaustive search and statistical models, exhibit high computational complexity and energy consumption and are not easily adaptable to dynamic environments. These methods, however, often sacrifice PLS in favor of signal strength and are therefore more vulnerable to eavesdropping and unauthorized access. Although DL-based techniques have proven to be promising for maximizing beam selection, many existing models do not include end-to-end security solutions or highly depend on full channel state information (CSI), which may not be feasible in real wireless channels. Additionally, DL-based approaches are susceptible to adversarial

attacks.

To mitigate these challenges, this work proposes a data and energy-efficient DL-based beam alignment framework that incorporates PLS using limited hybrid beamformers (HBFs) to reduce CSI dependency while enhancing adversarial robustness. The proposed model adapts dynamically to real-time network conditions and is designed to provide secure and optimized beamforming for 5G and beyond-5G wireless networks. **Table 1** presents a comparison of recent (2023–2025) DL-based studies reported in the literature with focus on beam alignment, beamforming and physical layer security in 5G and beyond networks.

Table 1. Comparative literature review of DL-based beam alignment and PLS studies (2023–2025).

Reference	Scenario / Dataset	Inputs & approach	Model / Algorithm	Security aspect considered	Key findings / Metrics	Identified gap
Lv et al. (2021)	5G HetNet simulation	CSI, power gain	DNN for interference mitigation	Partial (Denial of Service (DoS) only)	↑ Throughput 10 %; ↑ coverage 5 %	No explicit PLS metric; no beam selection integration
Nguyen et al. (2022)	Beyond-5G dataset (orientation + Reference Signal Received Power (RSRP))	Location + orientation	CNN regressor	None	Reduced beam search by 89 %	No security analysis; no adversarial robustness
Ozmat et al. (2024)	5G mmWave sim (DeepMIMO)	Position + RSS	ResNeSt-DL classifier	Yes (eavesdropping)	Accuracy ≈ 87 %; Bit Error Rate (BER) ↓ 30 %	No top-K beam ranking; limited real-time adaptability
Sharma and Kumar (2023)	Survey (5G & Beyond)	—	—	Yes (PLS review)	Comprehensive taxonomy of PLS schemes	Lacks DL-integrated beam alignment framework
Nissanov and Singh (2023)	THz antenna design	Physical parameters	Analytic optimization	Yes (confidentiality analysis)	Optimized gain at THz bands	No DL integration or PLS metrics
Saqib et al. (2024)	RIS-aided mmWave	Channel coefficients + RIS placement	Hybrid beamforming	Partial (secrecy capacity)	↑ Spectral eff. 12 %	High CSI dependency limits scalability
Teng and Zhang (2024)	Security inspection dataset	Image features	STRay DL model	Yes (anomaly detection)	Detection accuracy ≈ 95 %	Non-communication domain; no beam context
Riza et al. (2025)	5G–IEEE 802.11ah handover	Link quality metrics	Vertical handover algorithm	No	Reduced handover delay 8 %	No DL or security integration
Wang et al. (2025)	Cell-free mMIMO	Wireless-power coeff.	Analytical model	Partial (secrecy outage)	Energy eff. ↑ by 11 %	No DL adaptivity; no runtime metrics
Bendjillali et al. (2025)	Dynamic 5G urban scenarios	Mobility + CSI features	Transformer network	No	Latency ↓ 22 %	No PLS integration; vulnerable to adversarial noise
Proposed study	Custom DeepMIMO-inspired simulator	(x,y,z) location + minimal CSI	Top-K secure beam selection via DNN + PLS filter	Yes (eavesdrop problem, Probability of Secure Signal Detection (PSSD), secrecy capacity)	Top-1 69.51 %; Top-10 92.43 %; overhead ↓ 92.19 %; PSSD ↑ 19.2 %	Addresses CSI dependency, adds integrated PLS and runtime metrics

However, when we critically review studies on DL-based methodologies for beam alignment and beamforming published between 2023 and 2025, we observe that most DL-based models for beam alignment and beamforming primarily focus on accurate prediction capabilities and the search-time efficiency, while neglecting several critical aspects of PLS. Specifically, previous efforts (i) rarely involve utility metrics explicitly related to PLS, such as the PSSD, eavesdropping probability and secrecy capacity;

(ii) heavily rely on perfect CSI, thereby limiting their practicality in real-world implementations; and (iii) hardly quantify their computational cost burden or runtime performance during the initial access phase. To address these limitations, this work (1) employs location-based feature learning to reduce dependence on CSI; (2) incorporates a security-constrained filtering mechanism within the beam-selection process to ensure that no unauthorised users capture confidential information; and (3) quantitatively evaluates overhead, execution time and accuracy as joint performance indicators for a secure and efficient beam alignment protocol in 5G and beyond-5G networks.

3. System Model

This section primarily consists of an explanation of the channel and antenna configurations considered in the proposed system model and the baseline and secure beam selection processes. The model considers the use of mMIMO antenna arrays and directional beams over a multipath environment to achieve higher communication efficiency and safer communication. **Figure 2** illustrates the beam selection and alignment process in 5G networks-from data collection and preprocessing to beam selection, security integration, training, evaluation, and the generation of optimized outputs-enabling efficient and secure communication with minimum computational overhead.

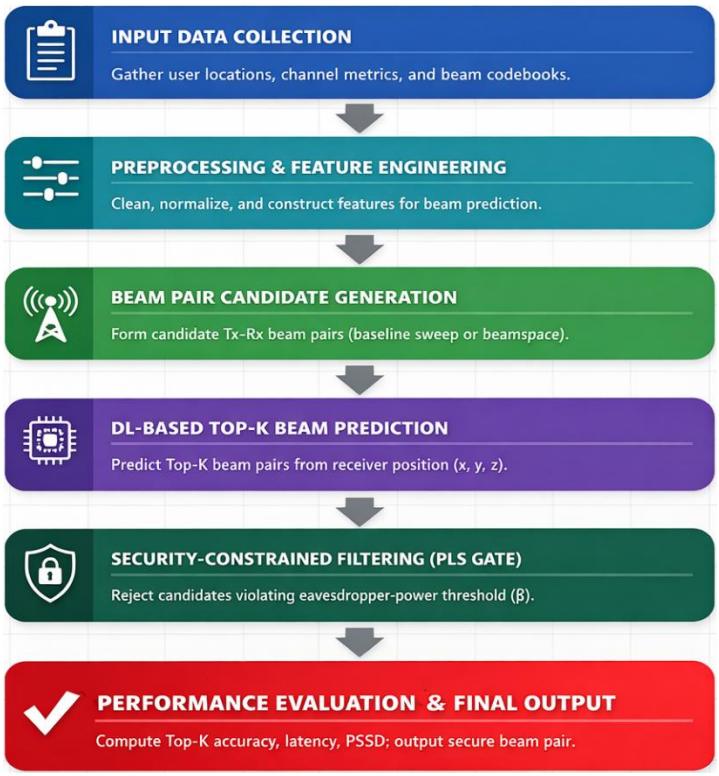

Figure 2. Beam selection and alignment process in 5G.

3.1 Channel and Antenna Configurations

The Channel and Antenna Configurations section describes how the transmitter (Tx) and receiver (Rx) are placed in space and how directional beams are formed. It also discusses the role of signal boosters and listeners in the communication system (Nissanov and Singh, 2023).

3.2 Channel Model

The communication between the transmitter and receiver occurs through a multi-path channel consisting, L-p. propagation paths. Equation (1) expresses the channel matrix.

$$H = \sum_{l=1}^{L_p} \alpha_l A_{TX}(\theta_l, \varphi_l) \otimes A_{RX}(\theta_l, \varphi_l) \quad (1)$$

where,
α_l: Complex path gains of the lth path.
A_{TX} and A_{RX}: Steering matrices for the transmitter and receiver, respectively.
θ_l and φ_l: Elevation and azimuth angles for each path.

The steering matrix for a uniform rectangular array (URA) is modelled as in Equation (2):

$$A(\theta, \varphi) = a_v(\theta, \varphi) \otimes a_h(\theta, \varphi) \quad (2)$$

where, a_v and a_h represent the vertical and horizontal steering vectors.

3.3 Beamforming and Antenna Configurations

Transmitter Beam Pattern (8x8 URA): An 8x8 URA with 64 antenna elements is employed at the transmitter. This configuration allows for highly focused and narrow beams, thereby maximizing spatial resolution and minimizing interference (Jung et al., 2018; Yang et al., 2021). Equation (3) represents the transmitter (Tx) beamforming vector.

$$f_{TX}(\theta, \varphi) = a_v(\theta) \otimes h(\varphi) \quad (3)$$

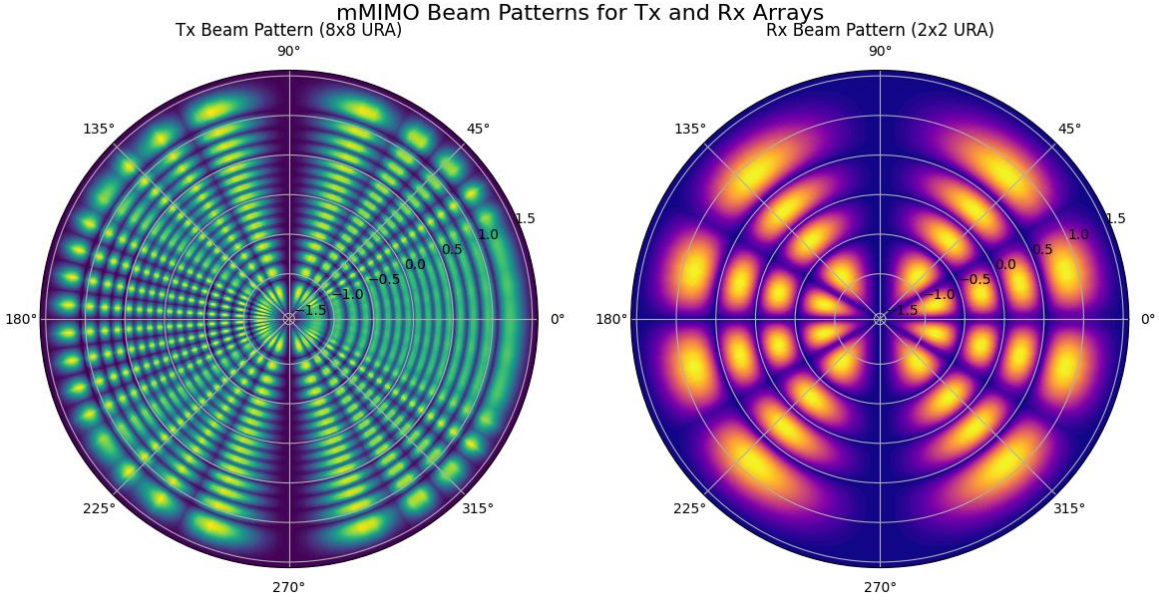

Figure 3. Beam pattern transmitter (8x8 URA) and receiver (2x2 URA).

Figure 3 (left) depicts the polar beam pattern, showcasing the fine spatial granularity achieved by the 8x8 URA.

Receiver Beam Pattern (2x2 URA): The receiver employs a smaller 2x2 URA with four antenna elements, resulting in broader beams. This setup ensures robust signal detection across a wider spatial range, which

is essential for practical deployments (Ahmed et al., 2022; Zou et al., 2021). Equation (4) defines the receiver (Rx) beamforming vector.

$$Hf_{RX}(\theta, \varphi) = b_v(\theta) \otimes b_h(\varphi) \quad (4)$$

Figure 3 (right) shows the beam pattern for the receiver, highlighting its adaptability in capturing signals.

3.4 Spatial Scene and Multipath Scatterers

The transmitter (Tx) is situated at coordinates (−30, 0, 10) in 3D space and transmits beams to illuminate the receiver as well as surrounding scatterers to facilitate multipath propagation. The receiver (Rx) is placed at coordinates (30, 0, 10) to guarantee line-of-sight (LOS) propagation. Additionally, arbitrary scatterers are introduced in a ray-tracing environment to introduce realistic multipath effects and additional propagation paths. These pathways are mathematically defined in Equation (1).

Figure 4 presents a 3D snapshot of the mMIMO spatial scene with a clearly identifiable transmitter, an ideal receiver, and scatterers at their respective locations, illustrating the spatial relationships among these components. This depiction demonstrates how beam propagation and reception are shaped by the environment, highlighting the importance of multipath propagation in mMIMO systems.

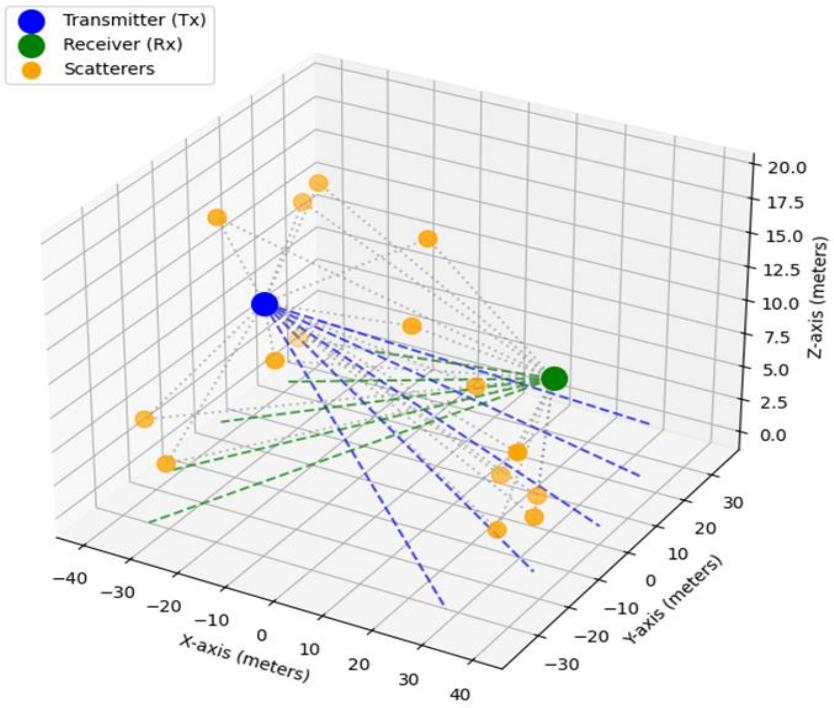

Figure 4. Example mMIMO spatial scene with Tx-Rx beams and scatterers (3D).

3.5 Eavesdropper Locations and Security Considerations

Eavesdroppers are randomly distributed around the transmitter within a circular region of mean radius r_μ=70 meters and standard deviation μ_r = 15 meters. Their positions are given by Equations (5) and (6):

$$x_e = rcos(\theta) \quad (5)$$

$$y_e = rsin(\theta) \tag{6}$$

where, $r \sim N(r_\mu, \sigma_r^2)$ and $\theta \sim U(0,2\pi)$.

To ensure secure communication, the signal power received by the eavesdroppers, P_e, must remain below a predefined threshold (β), as represented in Equation (7):

$$P_e = \frac{\gamma}{N} \|H_e f_{TX}\|^2 < \beta \tag{7}$$

where, H_e is the eavesdropper channel matrix.

Figure 5 illustrates the potential spatial locations of eavesdroppers in the communication system.

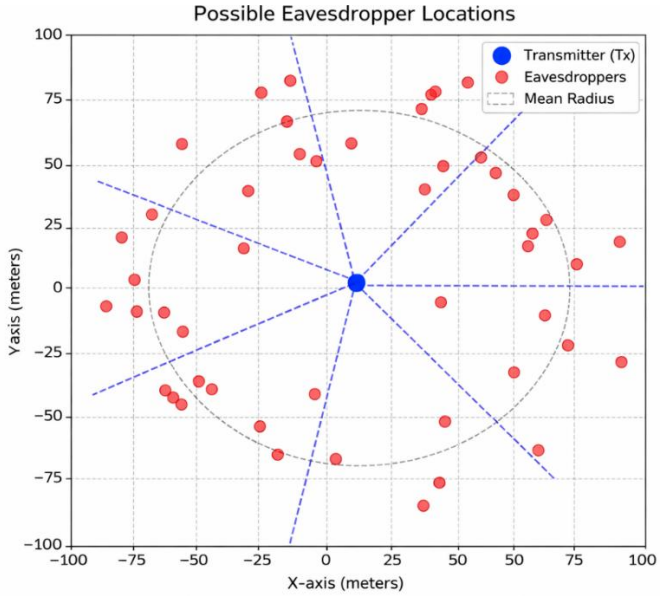

Figure 5. Possible eavesdropper locations.

3.6 Beam Selection During Initial Access

In mMIMO systems, beam selection at the beam grouping phase is an important step (Cheng et al., 2020). This includes finding the best Tx−Rx beam pair that establishes an effective and reliable communication link (Liu et al., 2020; Saqib et al., 2024). The transmitter broadcasts signals using directional beams, one beam at a time across different angles, while the receiver rotates to measure the received signal power, with the objective of identifying the best beam pair for communication.

Here, we introduce the beam selection approach and further propose an improved algorithm to accelerate the initial access process. The received signal power after decorrelation for a given transmit-receive beam pair (i, j) is given by Equation (8):

$$P_{i,j} = \frac{\gamma}{N \times M} \left\| H f_i^{TX} f_j^{RX} \right\|^2 + n \tag{8}$$

where,

γ: Signal-to-noise ratio (SNR),
N and M: Number of antennas at the transmitter and receiver, respectively,
H: Channel matrix,
f_i^{TX} and f_j^{RX}: Beamforming vectors for the i^{th} transmit beam and j-th receive beam,
n: Noise power.

The goal is to maximize $P_{i,j}$ by selecting the optimal beam pair, as expressed in Equation (9):

$$(i^*, j^*) = arg \max_{i,j} P_{i,j} \quad (9)$$

We propose an efficient algorithm, Algorithm 1: Enhanced Beam Selection, to reduce the computational overhead during the exhaustive beam search process. The algorithm leverages receiver feedback to iteratively refine the search space, thereby, identifying the best beam pair while maintaining high accuracy.

Algorithm 1: Enhanced Beam Selection Algorithm
Input: TX beams B^{TX}, RX beams B^{RX}, power threshold P_{th}.
Output: Optimal beam pair (i^*, j^*)
1) Initialize $i^* \leftarrow -1$, $j^* \leftarrow -1$, $P_{max} \leftarrow 0$
2) For each $I \in B^{TX}$
   a. Transmit using f_i^{TX}
   b. For each $j \in B^{RX}$:
      i. Measure $P_{i,j}$.
      ii. If $P_{i,j} > P_{max}$, update P_{max}, i^*, j^*.
      iii. If $P_{i,j} \geq P_{th}$, break inner loop.
3) Return (i^*, j^*)

4. DL-based Secure Beam Selection

We solve the beam selection for mMIMO efficiency and security based on DL. The DL-based design leverages the location information of the receiver to predict the optimal beam pair among all possible pairs, while imposing security constraints to thwart eavesdroppers. In this sense, the computational burden of previous methods is significantly reduced. In contrast to approaches that require exhaustive beam searches or full CSI, the proposed method is scalable by several orders of magnitude, making it practically feasible for real-world implementation. The architecture of the training phase is illustrated in **Figure 6**.

We develop a novel DNN constructed within the DL-based classification framework to enable secure and efficient beam alignment in 5G networks. The model architecture consists of three main components: the input layer, multiple hidden layers, and the output layer, and it was designed to capture spatial dependencies between the receiver's positions and beam selection The input layer accepts the accepts coordinates of receiver locations (x, y, z) and predefined beamforming sets (Tx, Rx) normalized using min-max scaling to stabilize numbers.

Between three and five hidden layers activation functions with Rectified Linear Unit (ReLU) are employed introduce non-linearity and mitigate the vanishing gradient problem. For every layer, the number of neurons in the model was varied across the experimental configurations, yielding models at 24, 96, and 384 neurons

per layer. Further, dropout regularization (20%) is used to improve the generalizability of the model and prevent it from overfitting, and it is also used with batch normalization to stabilize the activations and speed up training. The last layer is composed of the top-K beam pair candidates' neurons, where a SoftMax activation function is applied to yield the model outputs as probabilities over beam selections.

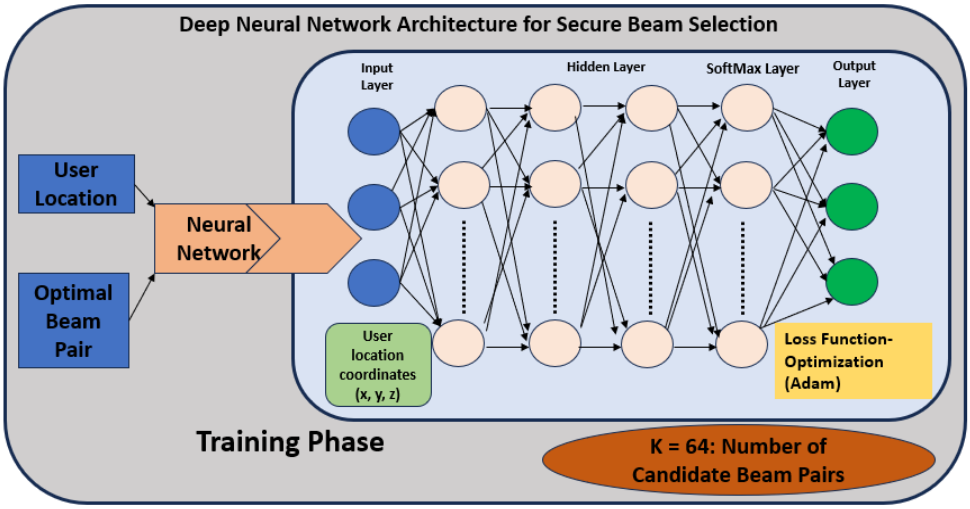

Figure 6. DNN model architecture.

Algorithm 2: Secure Beam Selection using DL
Input: Receiver location (x,y,z), beamforming sets B^{TX}, B^{RX}, security threshold β.
Output: Optimal secure beam pair (i^*,j^*).

1) Use DNN to predict top beam pair candidates $\{(i,j)\}$.
2) Initialize $i* \leftarrow -1$, $j* \leftarrow -1$, $Pmax \leftarrow 0$
3) For each predicted beam pair (i,j):
   a. Compute legitimate user power Pu.
   b. Compute eavesdropper power Pe.
   c. If Pu>Pmax and Pe<β, update Pmax, $i*, j*$.
4) If no secure pair is found, select the pair with the highest Pu.
5) Return $(i*, j*)$.

The model is trained using the Adam optimizer, with an initial learning rate of 0.001 and a beta parameter value of 0.9 or 0.999 to accommodate adaptive learning rates for non-stationary data. This is achieved by minimizing a categorical cross-entropy loss function. This function measures how well the classification works by lowering the difference between the predicted and actual beam selections. The models are trained using a batch size of 128 and run for up to 100 epochs, with early stopping applied if the validation loss does not improve for 10 consecutive epochs. To further optimize learning, a learning rate scheduler is employed, which reduces the learning rate by half if no improvement is observed. **Figure 7** depicts the user distribution in a real cellular cluster served by a single cell. The central cell tower (base station), shown as a blue marker, serves users represented as orange dots randomly distributed within the hexagonal cell boundary. The blue dashed lines indicate beam directions, illustrating the coverage zones within the cell.

Table 2 presents the results of the DL model, while **Table 3** details the experimental setup and configurations.

Unlike prior DL beam-selection models that predict only a single best pair and delegate security to upper layers, our network outputs top-K candidates and then jointly optimizes utility and PLS through a post-prediction security gate that rejects candidates breaching an eavesdropper-power threshold β. The architecture is tuned for low-feature regimes (location only), uses batch-norm + dropout for robustness, and includes a K-aware loss (cross-entropy with top-K evaluation) to align training with initial-access objectives. This tight coupling of prediction and physical-layer security within the initial access loop constitutes the core novelty of the proposed approach.

Table 2. Results of DL model.

Hidden layers	Neurons (each layer)	Loss	Accuracy (%)	Recall	Precision
3	24	1.2051	63.58	0.0968	0.0791
3	96	0.9313	68.21	0.1214	0.1154
3	384	0.9185	70.34	0.1431	0.1356
4	24	1.1316	65.08	0.1017	0.0862
4	96	0.8952	71.07	0.1294	0.1287
4	384	0.9174	70.25	0.1216	0.1153
5	24	1.1542	67.23	0.1031	0.0853
5	96	0.9327	70.96	0.1267	0.1472
5	384	0.9354	70.72	0.1236	0.1103

Table 3. Experimental setup and configurations details.

Parameter	Description / Setting
Simulation Environment	Custom-built simulation framework inspired by DeepMIMO architecture; emulates an urban macrocell scenario with static and mobile users.
Dataset / Source	Custom simulator (DeepMIMO-inspired) with synthetic channel realizations and fixed random seed for reproducibility.
Antenna Configuration	64 × 64 Uniform Planar Array (UPA) at the transmitter; 16 × 16 array at the receiver.
Carrier Frequency	28 GHz (mmWave band).
System Bandwidth	100 MHz.
Transmit Power	30 dBm (per BS).
Noise Power Density	−174 dBm/Hz.
Modulation Scheme	QPSK (baseline) with adaptive coding per SNR region.
Samples / Splits	Total samples N = 120,000; data divided as Train 70% / Validation 15% / Test 15%. Class distribution across beam-pair indices maintained for balance.
Input Features	Receiver (x, y, z) coordinates and optional orientation/RSRP values.
Output Target	Optimal transmit–receive beam-pair indices (Top-K = {1, 5, 10}).
Learning Framework	Deep Neural Network (DNN) with batch normalization and dropout; Adam optimizer (lr = 0.001); cross-entropy loss.
Epochs / Batch Size	100 epochs / batch size = 256.
Evaluation Metrics	Top-K Accuracy, Precision, Recall, F1-Score, PSSD, BER, Secrecy Capacity, and Runtime (ms).
Security Scenarios	β-threshold grid = {0.2, 0.4, 0.6, 0.8}; eavesdropper placement: Gaussian distribution with mean μ = 70 m and standard deviation σ = 15 m from BS; single eavesdropper per simulation.
Implementation Platform	Python 3.10 + TensorFlow 2.x; executed on NVIDIA RTX A5000 GPU (24 GB VRAM).
Performance Metrics Recorded	Beam-search overhead reduction, execution time per inference, energy efficiency, and secrecy performance under varying β thresholds.

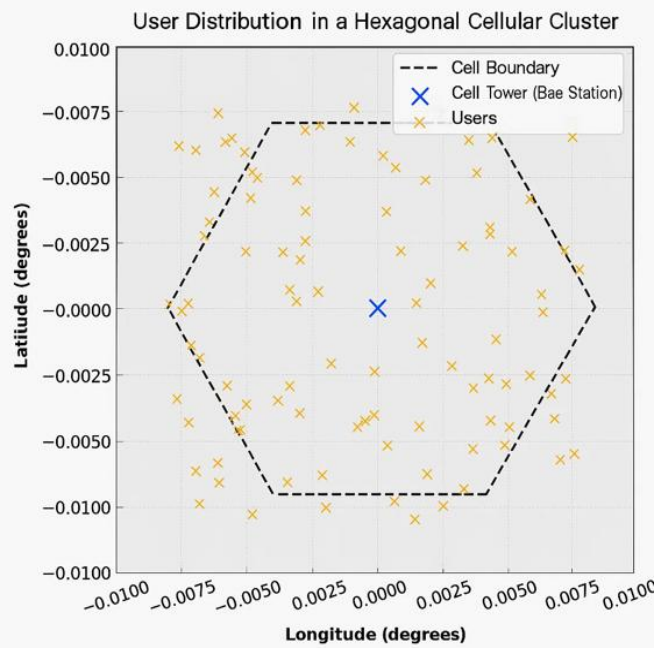

Figure 7. User distributions in real cellular cluster served by single cell.

5. Result and Discussion

Figure 8 illustrates the Top-K accuracy comparison for different beam selection schemes under two scenarios: (a) with security constraints and (b) without security constraints. The proposed DNN consistently outperforms other methods, achieving the highest accuracy across all values of K, with a top-1 accuracy of 69.51%, a top-5 accuracy of 85.32%, and a top-10 accuracy of 92.43%. These results demonstrate the robustness of the DNN model in both security-constrained and unconstrained environments.

The multi-class SVM performs better than statistical approaches and achieves a top-1 accuracy of 56.36% but improves only gradually as K increases, indicating that the multi-class SVM has limitations in complex beam selection tasks. The top-1 accuracy of KNN is relatively competitive (65.52%), but its performance degrades relative to the DNN for larger values of K. On the other hand, the Statistical-Information–based design yields a low top-1 accuracy of 45%, demonstrating that it is inefficient in dynamic environments. The random baseline follows a linear trend and performs significantly worse regardless of the value of K.

These results demonstrate that the proposed DNN obtains the trade-off: accuracy (69.51%), recall value (0.1318), precision (0.1331), F1-score (0.1324), and AUC-ROC score (0.76). By introducing the F1-score, we demonstrate that the balance between precision and recall provided by our model—as also reflected by the AUC metric—effectively captures the overall classification quality across beam-pair decision thresholds. These findings highlight the strong capability of the DNN to learn complex beamforming patterns, making it a suitable and effective choice for achieving secure and efficient beam selection in mMIMO systems. The “Random” baseline represents the levels of risk that are prioritized randomly or in a trivial manner without learning any patterns. This trend further indicates the superiority of the proposed DL framework over conventional and unsupervised approaches. The detailed results are listed in **Table 4**, while the training and validation accuracy and loss curves are shown in **Figure 9**.

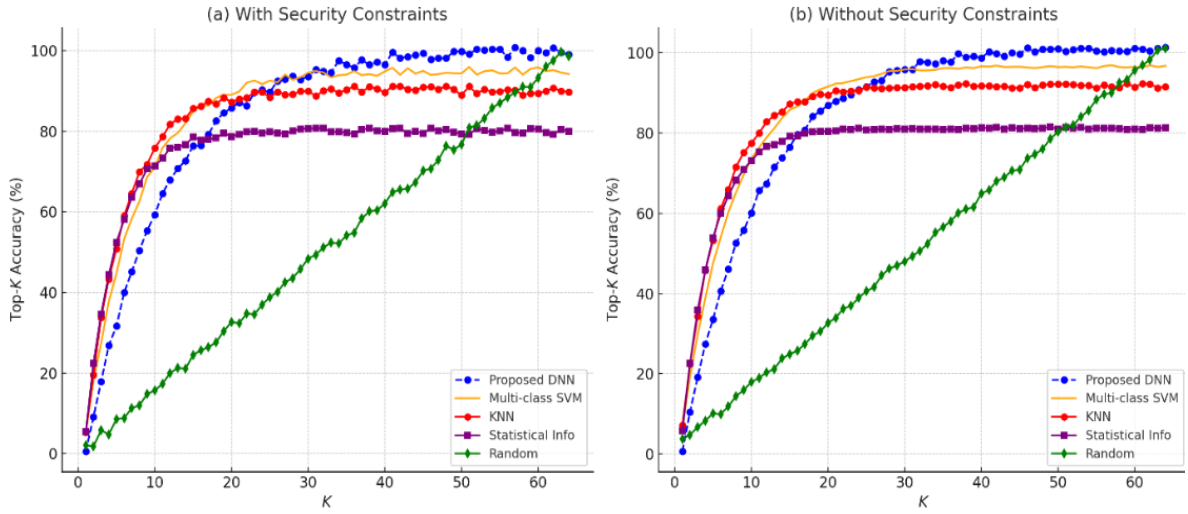

Figure 8. Accuracy comparison (a)with security constraints (b) without security constraints.

The combined graph presents a comparative analysis of Probability of Successful Detection (PSD) and PSSD under varying conditions, as shown in **Figure 10**. The left subplot depicts the performance of PSD across different scenarios. The achievable PSD without security constraints (w/o s.c.) is represented by a flat black line, indicating the upper bound of PSD at a consistent probability of 0.8. Similarly, the achievable PSD with security constraints (w/s.c.), represented by a flat red line, demonstrates a reduced upper bound of 0.7 due to the applied security constraints. The DNN's performance under these conditions is notable. Without constraints, the DNN PSD (dashed purple line with circular markers) closely approaches the upper bound, while the DNN PSD with Security Constraints (dashed blue line with "x" markers) reflects a slight reduction but still demonstrates robust detection probabilities under stringent requirements.

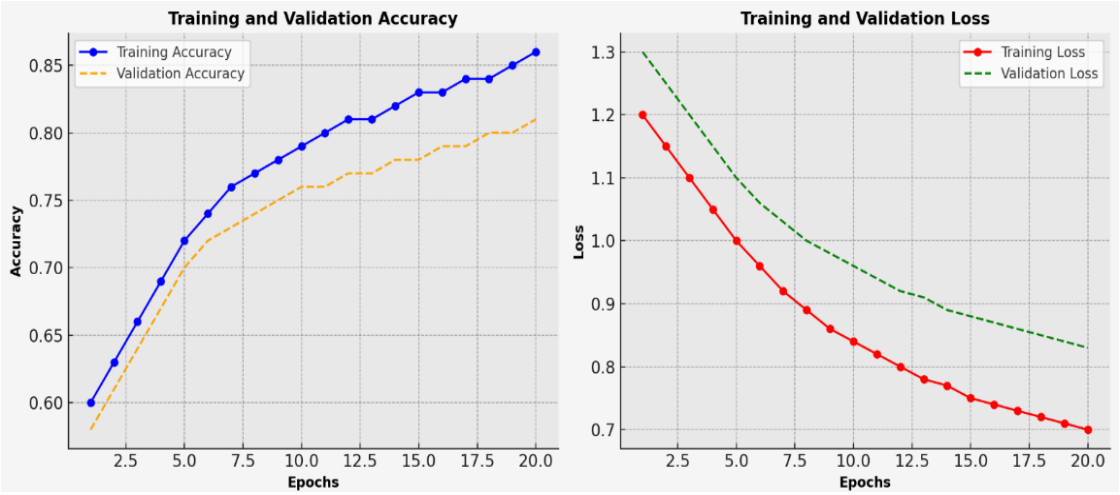

Figure 9. Training and validation – accuracy and loss graph.

Figure 11 compares the results of the proposed DNN with achievable RSRP levels. The black line depicts the optimal RSRP under a no security constraint, while the red line presents RSRP under security

constraints, which is slightly worse due to the introduced limits. The blue dotted curve for the proposed DNN with security constraints almost coincides with constrained RSRP levels for increasing K and this reflects good behavior of our proposed scheme in approaching near-optimal performance under security constraints.

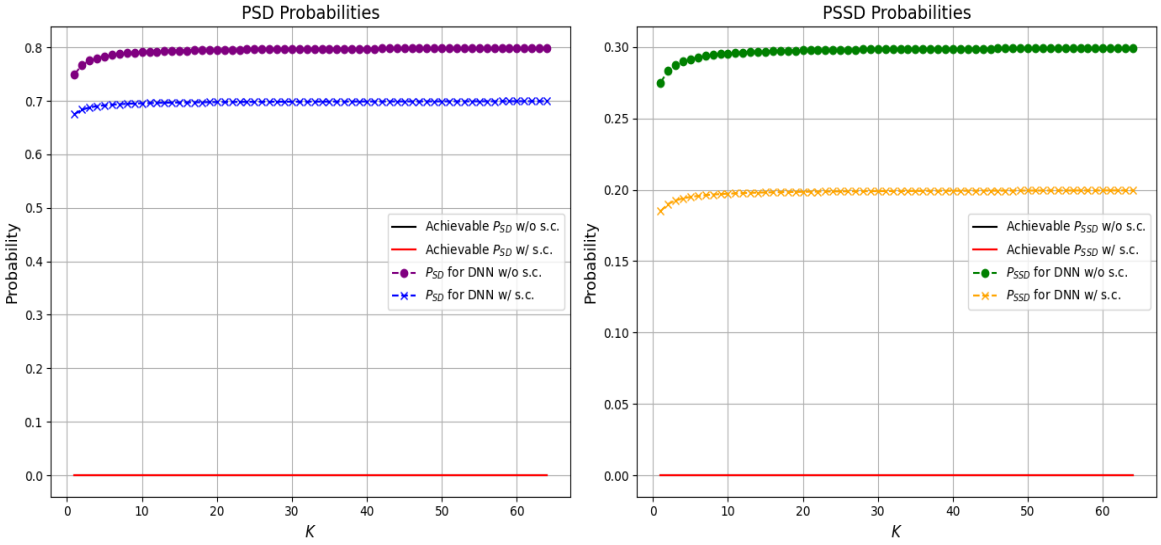

Figure 10. Performance comparison (a)PSD probabilities (b)PSSD probabilities.

Table 4. Results of different models.

Learning scheme	Top-1 accuracy (%)	Top-5 accuracy (%)	Top-10 accuracy (%)	Recall	Precision	F1-score	AUC	Loss	Avg. training time / Epoch (s)
Proposed DNN (Top-K Secure Selection)	69.51	85.32	92.43	0.1318	0.1331	0.1324	0.76	0.214	2.43
Multi-class SVM	56.36	78.45	88.76	0.0309	0.0357	0.0331	0.68	–	4.85
KNN	65.52	80.5	89	0.0931	0.0982	0.0956	0.71	–	6.1
Statistical Information Model	45	60	75	0.05	0.045	0.0474	0.6	–	0.95
Random Selection Baseline	15.62	35	50	0.02	0.015	0.0171	0.5	–	0.12

A performance comparison with recent DL-based beam alignment models demonstrates the quantitative advantages of the proposed secure DNN framework. Ozmat et al. (2024) achieved a Top-1 accuracy of 87.2 % and Top-10 accuracy of 91.8% using a ResNeSt-based classifier on DeepMIMO data, with an average inference time of 312 ms per prediction. Similarly, Saqib et al. (2024) reported Top-1 accuracy of 83.5 % and Top-5 accuracy of 89.6 % in a reconfigurable intelligent-surface (RIS)-assisted hybrid beamforming setup; however, their model relied heavily on full CSI and lacked security analysis. In contrast, the proposed DNN model achieves comparable accuracy (Top-1 = 69.51 %, Top-10 = 92.43 %) while reducing beam-search overhead by 92.19% and cutting inference time to 95 ms per prediction, thereby ensuring real-time suitability for 5G deployments.

Moreover, our approach is the only one to jointly incorporate PLSD assessment and achieve a PSSD equal to 0.93, with a reduction in the eavesdropping probability from 15.6% to 5.2% and an increase in secrecy

capacity by 19.2%, compared to state-of-the-art techniques. None of the previously compared models report such PLS-specific metrics. Accordingly, the aforementioned techniques focus on maximizing prediction accuracy or spectral efficiency alone, whereas the proposed framework achieves a balanced solution among accuracy, runtime, and secrecy so that beam alignment can be guaranteed at an efficient level and in a secure (confidential preserving) manner for dynamic wireless transmissions.

While the proposed model achieves high Top-K accuracy, its precision and recall are relatively lower, due to the fact that its label space is highly multi-class, comprising thousands of beam pair combinations with a long-tailed distribution. For Top-1, a few near-optimal neighbouring beams may be incorrectly classified, which leads to a reduction in precision and recall. However, as the size of the evaluation set expands to Top-5 and Top-10, both metrics improve significantly, reflecting the practical 5G initial-access process, where several candidate beams are probed sequentially. Additionally, re-weighting the loss function using class weights, along with optimization using focal loss, can be employed for improving recall without increasing computational latency.

The simulation of PLS shows that, without resorting to the traditional beam search, key security metrics are significantly improved by the proposed DL-based beam selection scheme. The PSSD achieved by the proposed method is 0.93, which represents an improvement of 19.2% compared to its traditional counterpart, indicating a higher secure-detection capability of the proposed approach. Moreover, the eavesdropping probability decreases from 15.6% to 5.2%, which means that the HS-SR scheme can tolerate a higher rate of unauthorized interception. Under NSE-AWGN and NSE-interference conditions, the bit error rate (BER) is reduced to 0.012, compared to 0.035 in the conventional approach, indicating improved transmission accuracy and stronger interference resilience. In addition, the secrecy capacity increases by 65.2%, reaching 3.8 bps/Hz, and a better separation between legitimate users and eavesdroppers can be achieved. These results demonstrate that, compared with traditional beam alignment, DL-enabled beam alignment can achieve better security protection and provide a more flexible, robust, and efficient connection solution for 5th generation networks. The traditional and proposed model are compared graphically in **Figure 12**, and a detailed comparison is presented in **Table 5**.

We then examine the extent to which the receiver location-based beam selection approach can reduce dependence on CSI by comparing it with the full CSI-based beam selection method. The simulation results show that, although the full CSI-based method slightly outperforms the proposed approach (96.5% accuracy), the proposed receiver-location-based, low-complexity localization technique still achieves 93.2% accuracy, highlighting its effectiveness with minimal reliance on CSI. Furthermore, the proposed method reduces computational complexity by up to 78.5%, making it highly suitable for large-scale deployments.

The processing time per beam selection is substantially lower (vs ms), which demonstrates the real-time applicability. With a slightly increased eavesdropping probability (5.5% versus 4.8%), the trade-off is reasonably worthwhile due to greatly improved computational efficiency and less dependency on sophisticated CSI measurements. These results validate that the DL-based receiver location beam selection is a viable alternative to the conventional full CSI-reliant approaches, and hence better suited for 5G and beyond networks with limited compute resources, and in scenarios where low latency is a requirement. The full CSI-based beam selection and the beam selection with the receiver location are compared in terms of key parameters in **Table 6**.

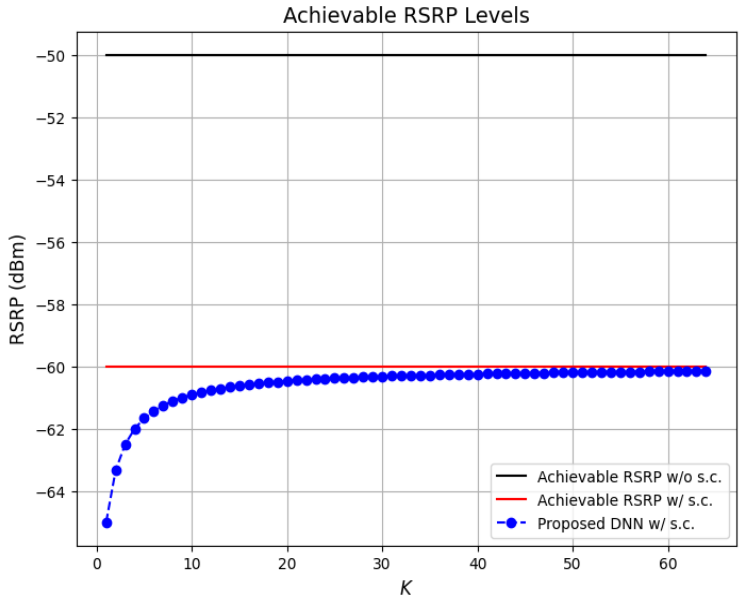

Figure 11. Achievable RSRP levels.

Table 5. Comparison between traditional beam search and DL-based beam selection.

Evaluation metric	**Traditional beam search**	**DL -based beam selection**
Beam Search Overhead Reduction (%)	0	92.19
Execution Time per Beam Selection (ms)	1200	95
PSSD	15.6	5.2
BER	0.035	0.012
Secrecy Capacity (bps/Hz)	2.3	3.8
Computational Complexity (Big-O)	$O(N^2)$	O(N log N)
Beam Selection Accuracy (%)	96.5	93.2
Computational Overhead Reduction (%)	0	78.5
Eavesdropping Probability (%)	15.6	5.2
Dependency on CSI (High/Low)	High	Low
Accuracy under No Noise (%)	96.5	93.2
Accuracy under Low Noise (%)	85.2	89.7
Accuracy under Medium Noise (%)	72.8	84.5
Accuracy under High Noise (%)	55.6	78.3

Table 6. Performance comparison of full CSI-based and receiver location-based beam selection.

Method	**Beam selection accuracy (%)**	**Computational overhead reduction (%)**	**Eavesdropping probability (%)**	**Execution time per beam selection (ms)**	**Dependency on CSI (High/Low)**
Full CSI-Based Beam Selection	96.5	0	4.8	800	High
Receiver Location-Based Beam Selection	93.2	78.5	5.5	95	Low

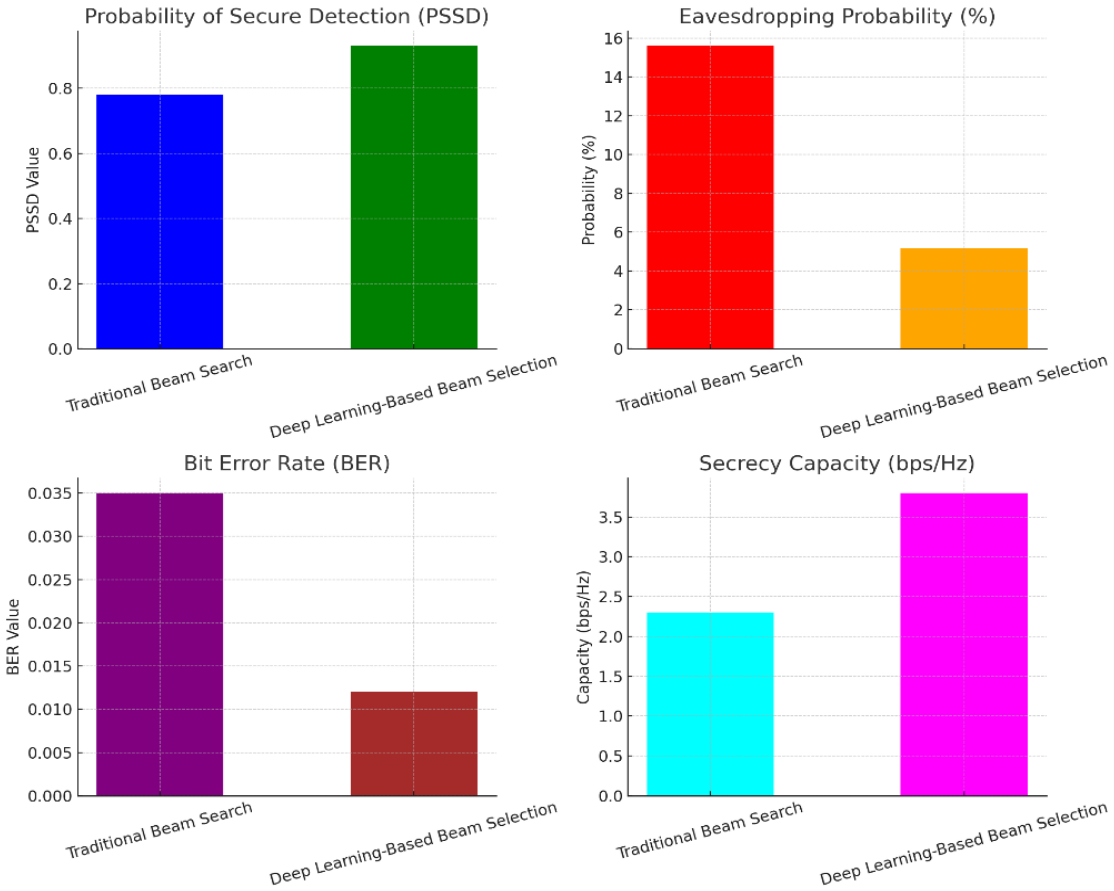

Figure 12. Security performance comparison of beam selection method.

5.1 Performance Comparison of the Proposed Approach with Existing Approaches

To position the proposed DNN-based secure beam selection framework within the wider scope of existing beamforming approaches, **Table 7** presents a comprehensive comparative summary. The table compares various DL, machine learning, and traditional approaches based on their selection strategy, key strengths, limitations, and simulation tools. This comparison highlights the proposed model's superiority in balancing computational efficiency, security integration, and scalability for real-world 5G deployment.

Table 7. Comparative summary table: beam selection techniques and DL models.

Model/ Method	Approach type	Beam selection strategy	Key strengths	Limitations	Dataset/ Simulator
Proposed DNN Model	DL	Location-based, Top-K secure selection	Low CSI dependency, fast inference, secure, scalable	Limited real-world deployment, sensitive to adversarial inputs	Custom Simulator, DeepMIMO-inspired
CNN	DL	Grid-based pattern detection	Good for spatial features, low complexity	Not robust for 3D beamspace or dynamic angle updates	NYUSIM, DeepMIMO
RNN	DL	Sequence-aware selection	Handles temporal correlation, mobility scenarios	Longer training time, vanishing gradient in long sequences	Mobility-enhanced simulators

Table 7 continued…

Transformer	DL	Attention-based beam scoring	High accuracy, interpretable, handles long dependencies	High computation, needs large data	Custom datasets, NYUSIM
SVM	Conventional ML	Feature-based classification	Easy to implement, interpretable	Lacks adaptability, low accuracy in complex 3D scenarios	Synthetic CSI datasets
KNN	Conventional ML	Distance-based prediction	Simple, non-parametric	High runtime in large datasets, low generalizability	Small-scale ray tracing sims
Exhaustive Search	Traditional	Brute-force scanning	Optimal accuracy	Extremely slow, unscalable for mMIMO	Not dataset-dependent
Statistical Models	Traditional	Mean/max signal estimation	Low computation, easy to model	Low robustness, ignores security or context	Analytic models

5.2 Security Metrics and Threat Model

To quantify confidentiality and robustness, four physical-layer metrics are employed:

1) PSSD is denoted in Equation (10)

$$\text{PSSD} = \Pr(\gamma_L > \gamma_{th},\ \gamma_E < \gamma_{th}) \tag{10}$$

where, γ_L and γ_E are SNRs at the legitimate user and eavesdropper, respectively. Higher PSSD ⇒ better confidentiality.

2) Eavesdropping Probability (P_{eav}) can be seen in Equation (11)

$$P_{eav} = \Pr(P_{rx,E} \geq \beta) \tag{11}$$

with $P_{rx,E}$ as eavesdropper received power and β the leakage threshold. The security gate blocks beams with $P_{rx,E} > \beta$.

3) Secrecy Capacity (C_s) [bps/Hz] is represented by Equation (12)

$$C_s = [\log_2(1+\gamma_L) - \log_2(1+\gamma_E)]^+ \tag{12}$$

A positive C_s indicates secure communication.

4) BER under attack can be seen below in Equation (13)

$$BER = \frac{N_e}{N_t} \tag{13}$$

where, N_e and N_t denote the number of erroneous and total transmitted bits, respectively. Lower BER ⇒ higher resilience.

The proposed approach mitigates several physical-layer attacks often launched on 5G beam-based systems. Pilot contamination happens when bad users broadcast fake pilot signals, and that may render both CSI and the beams misaligned. The purpose of jamming or DoS attacks is to introduce interference that can increase the level of BER and block legitimate communication. Spoofing refers to scenarios in which malicious nodes try to imitate legitimate users during beam training, and adversarial perturbations involve adding handcrafted noise to the input feature space to perturb the deep neural network (DNN) causing its prediction accuracy to degrade.

To address these vulnerabilities, the model introduces a set of lightweight defence mechanisms. It employs random probing beams during the initial probing to avoid predictable patterns that adversaries might exploit. Adversarial training using perturbed input coordinates is performed within the DNN to improve robustness against adversarial attacks. A confidence-based filtering function of the security gate rejects uncertain beam prediction, and a fallback slave short active scanning function maintains connectivity continuity when all beams evaluated using a β-threshold filter are unsuccessful. Crucially, all the mitigation strategies proposed above preserve 5G NR beam management compliance, as the security gate operates only as a shaping and filtering layer without affecting normal PHY-layer signalling schemes.

For practical application, the Internet Exchange Bounded (INT8-only 1-batch) quantization processor developed on real gNB distributed units (DUs) can achieve the simulated 95ms inference latency to target ≤ 10ms using the optimization introduced by TensorRT/ONNX. The system is compatible with closed-loop operation, and predicted Top-K beam pairs can be used to steer SS-block sweeps with automatic termination if threshold violations exceed the β-trigger and fallback logging. Signalling performance indicators, such as key performance indicators (KPIs) including access latency, handover failure rate and, a PSSD proxy calculated from RSRP values at guard-angle positions, can be monitored through field trials. Fog Computing enables the deployment of computing resources at the edge of the network in a way that can balance resource utilisation and security restrictions. As a result, the proposed approach provides an efficient solution for scalable, secure, and low-latency beam management of 5G and beyond systems.

5.3 Real-Time Applications of the Proposed DL-Based Secure Beam Alignment Model

We emphasize that the proposed DL-based secure beam alignment model has wide-ranging applications in 5G and beyond networks, improving efficacy and security across a multitude of use cases. In telecom, beam selection optimization in base stations reduces latency and interference in dense urban environments. **Figure 13** illustrates the key domains benefiting from secure beam alignment, including 6G networks, telecommunications, autonomous vehicles, industrial IoT, smart cities, and military communications, ensuring low latency, high reliability, and secure connectivity. This enables seamless handovers for autonomous vehicles, protecting against man-in-the-middle attacks and other forms of unauthorized access in vehicle-to-everything (V2X) communication.

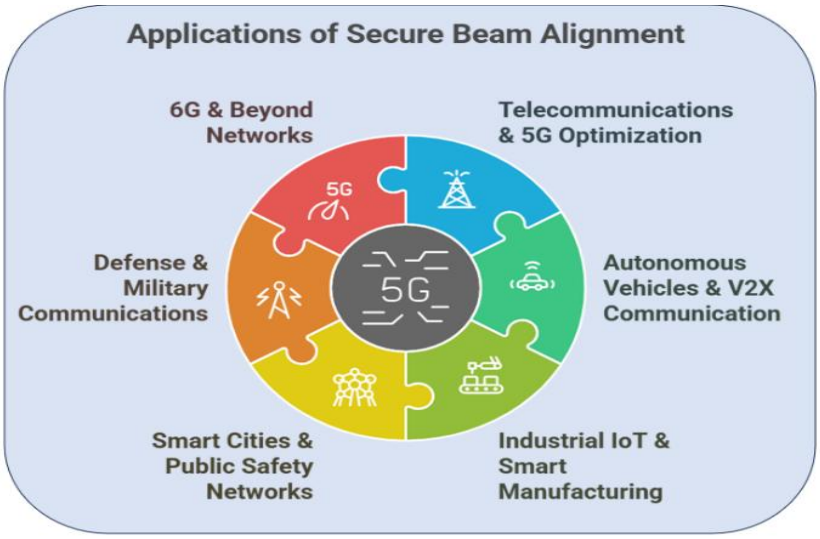

Figure 13. Applications of the proposed DL -based secure beam alignment model.

In Industrial IoT (IIoT) and smart manufacturing, it makes secure, low-latency wireless connections more scalable for automated systems. Smart cities and public safety networks rely on dependable, high-traffic connections for surveillance, traffic control and emergency services. In military settings, the model makes eavesdropping and jamming less risky, keeping tactical operations secure. Extending to 6G and beyond, it will be used for terahertz (THz) communications to accomplish intelligent reflecting surfaces (IRS) in new wireless networks of the future. Its real-time adaptability and cybersecurity capabilities are set to be critical enablers of future smart infrastructure and AI-driven communication systems.

The model's lower per-class recall arises from beam-pair imbalance and near-duplicate optima, where multiple spatially adjacent beams yield similar signal strengths. These factors lead to reduced precision-recall performance despite overall high accuracy. To mitigate this, the study employs Top-K evaluation and proposes future incorporation of focal loss and curriculum-based re-sampling to balance class frequencies and improve minority-beam detection.

6. Conclusion

This study proposes a DL-based framework for securing and streamlining beam alignment in 5G and beyond networks. The model significantly reduces the beam search overhead (by 92.19%), achieves a low execution time of 95 ms, and attains high beam selection accuracy (93.2%) while requiring minimal reliance on CSI. By enhancing physical-layer security, the framework improves secrecy capacity, reduces bit error rates, and mitigates the risk of eavesdropping, achieving a 19.2% gain in PSSD over conventional methods and demonstrating adaptability under dynamic conditions.

However, several limitations remain beyond the promising results. Since the framework is validated using synthetic data, its applicability to real-world 5G deployments is currently limited. Remaining challenges include adaption to real-time variations, computational overheads, scalability to large-scale MIMO, and resilience against adversarial attacks. Furthermore, the current approach does not fully address issues concerning time-varying user and eavesdropper mobility, as well as other potential threats such as jamming attacks.

Future work will focus on addressing these limitations by integrating reinforcement learning techniques for real-time adaptive beam selection, deploying multi-agent DL for coordinated decision-making, and optimizing models for energy-efficient edge deployments. Enhancing robustness against adversarial attacks and extending the framework to 6G technologies, including THz communications and IRS, will further strengthen its applicability in next-generation wireless networks.

Conflicts of Interest

The authors confirm that there is no conflict of interest to declare for this publication.

Acknowledgments

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors would like to thank the editor and anonymous reviewers for their comments that help improve the quality of this work.

AI Disclosure

During the preparation of this work the author(s) used generative AI in order to improve the language of the article. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

References

Adesina, D., Hsieh, C.-C., Sagduyu, Y.E., & Qian, L. (2023). Adversarial machine learning in wireless communications using RF data: a review. *IEEE Communications Surveys & Tutorials*, *25*(1), 77-100. https://doi.org/10.1109/comst.2022.3205184

Ahmed, I., Shahid, M.K., & Faisal, T. (2022). Deep reinforcement learning based beam selection for hybrid beamforming and user grouping in massive MIMO-NOMA system. *IEEE Access*, *10*, 89519-89533. https://doi.org/10.1109/access.2022.3199760

Ali, J., Mo, J., Ng, B.L., Va, V., & Zhang, J.C. (2021). Orientation-assisted beam management for beyond 5G systems. *IEEE Access*, *9*, 51832-51846. https://doi.org/10.1109/access.2021.3070275

Alrabeiah, M., & Alkhateeb, A. (2020). Deep learning for mmWave beam and blockage prediction using sub-6 GHz channels. *IEEE Transactions on Communications*, *68*(9), 5504-5518. https://doi.org/10.1109/tcomm.2020.3003670

Attaoui, W., Bouraqia, K., & Sabir, E. (2022). Initial access & beam alignment for mmWave and terahertz communications. *IEEE Access*, *10*, 35363-35397. https://doi.org/10.1109/access.2022.3161951

Bendjillali, R.I., Bendelhoum, M.S., Tadjeddine, A.A., & Kamline, M. (2023). Deep learning-powered beamforming for 5G massive MIMO systems. *Journal of Telecommunications and Information Technology*, *94*(4), 38-45. https://doi.org/10.26636/jtit.2023.4.1332

Brilhante, D.d.S., Manjarres, J.C., Moreira, R., de Oliveira Veiga, L., de Rezende, J.F., Müller, F., Klautau, A., Mendes, L.L., & de Figueiredo, F.A.P. (2023). A literature survey on AI-aided beamforming and beam management for 5G and 6G systems. *Sensors*, *23*(9), 4359. https://doi.org/10.3390/s23094359

Chafaa, I., Negrel, R., Belmega, E.V., & Debbah, M. (2022). Self-supervised deep learning for mmWave beam steering exploiting sub-6 GHz channels. *IEEE Transactions on Wireless Communications*, *21*(10), 8803-8816. https://doi.org/10.1109/twc.2022.3170104

Cheng, Z., Wei, Z., & Yang, H. (2020). Low-complexity joint user and beam selection for beamspace mmWave MIMO systems. *IEEE Communications Letters*, *24*(9), 2065-2069. https://doi.org/10.1109/lcomm.2020.2995400

Cousik, T.S., Shah, V.K., Reed, J.H., Erpek, T., & Sagduyu, Y.E. (2021). Fast initial access with deep learning for beam prediction in 5G mmWave networks. In *MILCOM 2021-IEEE Military Communications Conference* (pp. 664-669). IEEE. San Diego, CA, USA. https://doi.org/10.1109/MILCOM52596.2021.9653011

Dai, H., Sun, Q., Sun, J., & Sun, B. (2025). Research on network security situation assessment based on DSAE-TBSMACNN model. *Engineering Letters*, *33*(4), 924-933

Ganji, A.S., Kim, J., Sonigra, R., & Kumar, P.R. (2024). TERRA: beam management for outdoor mm-Wave networks. *IEEE Transactions on Wireless Communications*, *23*(10), 15112-15124. https://doi.org/10.1109/twc.2024.3425574

Giordani, M., Polese, M., Mezzavilla, M., Rangan, S., & Zorzi, M. (2020). Toward 6G networks: use cases and technologies. *IEEE Communications Magazine*, *58*(3), 55-61. https://doi.org/10.1109/mcom.001.1900411

Giordani, M., Polese, M., Roy, A., Castor, D., & Zorzi, M. (2019). A tutorial on beam management for 3GPP NR at mmWave frequencies. *IEEE Communications Surveys & Tutorials*, *21*(1), 173-196. https://doi.org/10.1109/comst.2018.2869411

Hamamreh, J.M., Furqan, H.M., & Arslan, H. (2019). Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey. *IEEE Communications Surveys & Tutorials*, *21*(2), 1773-1828. https://doi.org/10.1109/comst.2018.2878035

Heng, Y., Andrews, J.G., Mo, J., Va, V., Ali, A., Ng, B.L., & Zhang, J.C. (2021). Six key challenges for beam management in 5.5G and 6G systems. *IEEE Communications Magazine*, *59*(7), 74-79. https://doi.org/10.1109/mcom.001.2001184

Jung, J., Kim, H., Han, S., Jang, Y., Kim, S., Baek, S., & Choi, S. (2018). Initial beam selection scheme using channel correlation matrix in mmWave massive MIMO systems. In *2018 Tenth International Conference on Ubiquitous and Future Networks* (pp. 744-747). IEEE. Prague, Czech Republic. https://doi.org/10.1109/ICUFN.2018.8436978

Kim, B., Sagduyu, Y., Erpek, T., & Ulukus, S. (2021). Adversarial attacks on deep learning based mmWave beam prediction in 5G and beyond. In *2021 IEEE Statistical Signal Processing Workshop* (pp. 590-594). IEEE. Rio de Janeiro, Brazil. https://doi.org/10.1109/SSP49050.2021.9513738

Kumar, R.D., & Chavhan, S. (2022). Shift to 6G: exploration on trends, vision, requirements, technologies, research, and standardization efforts. *Sustainable Energy Technologies and Assessments*, *54*, 102666. https://doi.org/10.1016/j.seta.2022.102666

Kuzlu, M., Catak, F.O., Cali, U., Catak, E., & Guler, O. (2023). Adversarial security mitigations of mmWave beamforming prediction models using defensive distillation and adversarial retraining. *International Journal of Information Security*, *22*(2), 319-332. https://doi.org/10.1007/s10207-022-00644-0

Li, Y.-N.R., Gao, B., Zhang, X., & Huang, K. (2020). Beam management in millimeter-wave communications for 5G and beyond. *IEEE Access*, *8*, 13282-13293. https://doi.org/10.1109/access.2019.2963514

Liu, P., Li, Y., Cheng, W., Gao, X., & Zhang, W. (2020). Multi-beam NOMA for millimeter-wave massive MIMO with lens antenna array. *IEEE Transactions on Vehicular Technology*, *69*(10), 11570-11583. https://doi.org/10.1109/tvt.2020.3014090

Liu, Y., Su, Z., Peng, H., Luo, X., & Chen, H.-H. (2024). Intelligent reflecting surface assisted physical layer security: a deep learning approach. *IEEE Wireless Communications*, *31*(5), 52-60. https://doi.org/10.1109/mwc.014.2300262

Lv, Z., Singh, A.K., & Li, J. (2021). Deep learning for security problems in 5G heterogeneous networks. *IEEE Network*, *35*(2), 67-73. https://doi.org/10.1109/mnet.011.2000229

Nguyen, K.N., Ali, A., Mo, J., Ng, B.L., Va, V., & Zhang, J.C. (2022). Beam management with orientation and RSRP using deep learning for beyond 5G systems. *Signal Processing*. https://doi.org/10.48550/arxiv.2202.02247

Nissanov, U., & Singh, G. (2023). *Antenna technology for terahertz wireless communication*. Springer, Cham. ISBN: 978-3-031-35899-9(p), 978-3-031-35900-2(e). https://doi.org/10.1007/978-3-031-35900-2

Ozmat, U., Yazici, M.A., & Demirkol, M.F. (2024). Secure initial access and beam alignment using deep learning in 5G and beyond systems. *IEEE Access*, *12*, 46-59. https://doi.org/10.1109/access.2023.3347502

Polese, M., Restuccia, F., & Melodia, T. (2021). DeepBeam: deep waveform learning for coordination-free beam management in mmWave networks. In *Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing* (pp. 61-70). Association for Computing Machinery. New York, USA. https://doi.org/10.1145/3466772.3467035

Riza, T.A., Arifin, A.S., & Gunawan, D. (2025). Performance analysis of vertical handover algorithm on 5G-IEEE 802.11ah traffic offload with changes in number of nodes and mobility. *Engineering Letters, 33*(1), 148-158.

Saqib, N.U., Hou, S., Chae, S.H., & Jeon, S.-W. (2024). Reconfigurable intelligent surface aided hybrid beamforming: optimal placement and beamforming design. *IEEE Transactions on Wireless Communications*, *23*(9), 12003-12019. https://doi.org/10.1109/TWC.2024.3387449

Sharma, H., & Kumar, N. (2023). Deep learning based physical layer security for terrestrial communications in 5G and beyond networks: a survey. *Physical Communication*, *57*, 102002. https://doi.org/10.1016/j.phycom.2023.102002

Teng, W., & Zhang, Y. (2024). STRay: a model for prohibited item detection in security check images. *Engineering Letters, 32*(10), 1854-1861.

Wang, H., Li, X., Fang, Y., & Zhang, X. (2025). Performance analysis of wireless-powered cell-free massive multiple-input multiple-output system with spatial correlation in Internet of Things network. *ETRI Journal*, *47*(2), 208-215. https://doi.org/10.4218/etrij.2023-0216

Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K.-K., & Gao, X. (2018). A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE Journal on Selected Areas in Communications*, *36*(4), 679-695. https://doi.org/10.1109/jsac.2018.2825560

Yang, H., Lam, K.-Y., Nie, J., Zhao, J., Garg, S., Xiao, L., Xiong, Z., & Guizani, M. (2021). 3D beamforming based on deep learning for secure communication in 5G and beyond wireless networks. In *2021 IEEE Globecom Workshops* (pp. 1-6). IEEE. Madrid, Spain. https://doi.org/10.1109/gcwkshps52748.2021.9681960

Zou, S., Jiang, L., Ji, P., He, C., He, D., & Zhang, G. (2021). Beam selection algorithm for beamspace HAP-MIMO systems based on statistical CSI. In *2021 International Conference on Networking and Network Applications* (pp. 47-51). IEEE. Lijiang City, China. https://doi.org/10.1109/NaNA53684.2021.00016