Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2025) 000–000

Procedia Computer Science

www.elsevier.com/locate/procedia

The 20th International Conference on Future Networks and Communications (FNC)
August 4-6, 2025, Leuven, Belgium

Robust Protection of 5G MIMO Networks from Jamming Attacks via Adaptive Beamforming

Konstantinos Tsachrelias[a], Chrysostomos-Athanasios Katsigiannis[a], Vasileios Kokkinos[a], Christos Bouras[a]*, Apostolos Gkamas[b], Philippos Pouyioutas[c]

[a]*Computer Engineering & Informatics Dept., University of Patras, Patras, Greece*
[b]*Department of Chemistry, University of Ioannina, Ioannina, Greece*
[c]*Computer Science Department, University of Nicosia, Nicosia, Cyprus*

Abstract

Ensuring reliable and secure communication in 5G networks is critical, especially against jamming attacks that can significantly impair network performance. This paper presents a method to enhance the resilience of 5G Multiple Input Multiple Output (MIMO) networks through adaptive beamforming, specifically targeting jamming mitigation. The approach involves dynamically adjusting signal transmission direction to differentiate between legitimate communication and interference. Simulation results demonstrate that adaptive beamforming effectively reduces the impact of jamming, maintaining service quality even under adverse conditions. This method provides a practical and scalable solution for improving the security of 5G networks, addressing a key challenge in wireless communication systems.

Keywords—Beamforming; Spatial Filtering; 5G Networks Jamming attack; Security; Multiple Input Multiple Output (MIMO)

1. Introduction

The development of 5G technology has transformed mobile communication, offering faster data rates, lower latency, and greater connectivity. Key to these advancements are Multiple Input Multiple Output (MIMO) systems and adaptive beamforming, which improve spectral efficiency and network performance. However, as 5G networks become integral to critical infrastructure, they face increasing threats from sophisticated jamming attacks that disrupt communication by overwhelming the network with interference.

Jamming attacks have become a critical concern for the security and performance of 5G networks. This issue is especially pronounced in MIMO systems, where the use of multiple antennas significantly improves network capacity but also introduces new points of vulnerability. Due to the complex Base Station (BS) arrangements, attackers have greater flexibility to interfere with legitimate signals, creating disruption by deliberately injecting unwanted signals into the communication channel. As a result, legal communication experiences reduced quality, increased error rates, and decreased overall throughput. In extreme cases, jamming can completely block the ability of devices to connect, resulting in a total loss of communication. Addressing these threats requires careful analysis and the development of effective defensive methods that can maintain network stability and protect the integrity of data transmitted over 5G networks.

This paper proposes a method to defend 5G MIMO networks against jamming attacks using adaptive beamforming. By adjusting the direction of signal transmission, adaptive beamforming can isolate legitimate communication from jamming signals, ensuring consistent service quality even in the presence of interference. Previous research has focused on beamforming for improving spectral efficiency and reducing interference under normal conditions [1].

*Corresponding author. Tel.: +30-2610-996951.
E-mail address: bouras@upatras.gr

Additionally, extensive research has investigated advanced beamforming techniques to improve the efficiency and scalability of 5G MIMO networks. For instance, paper [2] proposes a method that uses a sparse MIMO array combined with a Spatial Filter Bank (SFB) to tackle challenges such as antenna complexity and beamwidth variation at different scanning angles. By spacing antenna elements farther apart, this approach reduces the number of elements needed without compromising performance, making it easier to implement in practical applications. The spatial filter bank helps to maintain a consistent beamwidth across the entire observation field and allows the generation of multiple beams, which enhances scanning efficiency. This combination of sparse arrays and SFB offers a solution that simplifies hardware design while improving spatial resolution, making it a useful technique for modern 5G applications.

Paper [3] has investigated methods to secure data transmission in 5G networks, particularly in the face of eavesdropping threats. One approach, known as Multi-cell Original Symbol Phase Rotated (MOSPR), has been proposed to protect against eavesdroppers in a multi-cell MIMO environment. Unlike traditional methods that focus on single-cell scenarios, this technique involves multiple BSs serving multiple users across different cells. The MOSPR method enhances security by increasing the Symbol Error Rate (SER) of the eavesdropper, making it harder for unauthorized parties to intercept the data. Simulations show that MOSPR is 8% more efficient than techniques like Artificial Noise (AN) generation, especially when the number of antennas at the BSs (BSs) is large. This research highlights the effectiveness of MOSPR in safeguarding data transmissions in 5G networks, even against sophisticated MIMO eavesdroppers, by keeping the SER high and ensuring secure communication across different cells.

Another study in the area of interference mitigation is presented in [4] and investigating defensive strategies against beam training attacks specifically in millimeter-wave (mmWave) 5G networks used in industrial settings. The research explores a scenario where an Automated Guided Vehicle (AGV) and a BS conduct beam training to establish and maintain mmWave connections within smart factories. Acknowledging the vulnerability of beam training to jamming attacks aimed at disrupting communications, the authors propose a defensive approach comprising two stages: detection and mitigation. Both stages employ autoencoder-based machine learning models, enabling detection accuracy of over 80% and significant improvements in signal-to-interference-plus-noise ratio (SINR), reaching enhancements of up to 15 dB. This research highlights practical, machine-learning-driven defense mechanisms, directly compatible with current 5G New Radio standards, and suggests potential extensions for scenarios involving multiple vehicles and hybrid beamforming techniques.

In addition, paper [5] studying anti-jamming techniques during the Beam Alignment (BA) phase in mmWave MIMO communications. Specifically addressing vulnerabilities in the 5G New Radio BA procedure, the paper highlights that a malicious jammer could exploit known spatial and time-frequency resources to severely degrade the accuracy of beam selection. To counteract such threats, the authors propose a defensive approach utilizing randomized probing combined with jamming cancellation. Their method intentionally introduces randomness into the probing sequences, enabling the legitimate receiver to differentiate between genuine signals and interference through orthogonal projections. Numerical experiments provided by the authors confirm that this method maintains beam alignment accuracy remarkably close to normal conditions without interference. They also identify future research directions, such as addressing adaptive smart jammers capable of dynamically modifying their attack patterns, necessitating more robust and flexible interference mitigation solutions.

This research introduces a practical method for protecting 5G MIMO networks from jamming attacks by using adaptive beamforming. Rather than depending on static setups or additional specialized equipment, the method fully utilizes the beamforming functionality already present in modern wireless communication systems. Through extensive and clearly defined simulations, the paper demonstrates that adaptive beamforming effectively identifies interference caused by jammers and dynamically adjusts the transmission direction to minimize its impact. This allows legitimate signals to maintain their strength and quality, ensuring stable communication despite the presence of intentional interference. The key novelty of this study lies in adapting existing beamforming methods specifically to counteract deliberate jamming in 5G scenarios. Previous research primarily explored beamforming to improve general communication performance under normal conditions, without directly addressing deliberate interference. This study, however, directly targets the issue of security and network stability under malicious interference, showing for the first time that adaptive beamforming alone can serve as an efficient and robust defensive measure. The detailed simulations provide clear evidence of this capability, filling a significant gap in current 5G security approaches and contributing directly to enhancing reliability and resilience in real-world network deployments [6], [7], [8].

The rest of the paper is organized as follows: In Section 2, the mathematical model utilized in the simulation environment is introduced. Moving to Section 3, the algorithm analysis that forms the basis for constructing the experiment scenarios is delved into. Section 4 outlines the simulation setup and methodology employed to assess the performance of Spectral Efficiency in MIMO 5G Heterogeneous Networks (HetNets). Following that, in Section 5, the simulation results are presented, and a comprehensive analysis of the findings is conducted. Lastly, Section 6 concludes the paper and offers insights into potential avenues for future research.

2. Mathematical Model

This section gives a detailed explanation of the mathematical model used to set up and carry out the simulations in the subsequent scenario. In the mathematical model proposed, the main elements are the representation of signal transmission, the interference from jammers, the path loss calculations, and the evaluation metrics such as SINR. Each of these components contributes to understanding the behavior of the network under different conditions and the effectiveness of the applied beamforming techniques.

The model begins with a 5G MIMO system setup, where a BS equipped with multiple antennas communicates with several User Equipment (UE) like mobile phones and etc, each also equipped with multiple antennas. The BS has Nt transmit antennas, while each UE has Nr receive antennas. The interaction between the BS and each UE is represented by a channel matrix H, which captures the effects of the wireless propagation environment, including factors such as fading and multipath propagation. The transmitted signal s is defined as:

$$x = W_s \tag{1}$$

where x represents the transmitted signal vector, W is the beamforming matrix, and s is the data symbol intended for the UE. The beamforming matrix W directs the transmitted signal energy towards the intended UE while minimizing interference in other directions. Each element of W is designed based on the channel characteristics to optimize signal transmission.

When the transmitted signal reaches a particular UE, the received signal at that UE is influenced not only by the desired signal but also by the interference from multiple jammers. The received signal at the i-th UE, considering K jammers, can be expressed as [9]:

$$y_i = H_i + \sum_{k=1}^{K} H_{ji} x_k + n_i \tag{2}$$

In this expression, Hi is the channel matrix between the BS and the i-th UE, and Hji represents the channel from the k-th jammer to the i-th UE. The term xk denotes the transmitted signal from the k-th jammer, and ni is the noise at the i-th UE, typically modeled as Gaussian noise with zero mean and a covariance matrix. This equation captures the interplay of desired signals, interference, and noise at the receiver, which is critical for evaluating the system's performance.

The model also includes a path loss equation to describe how the power of a transmitted signal attenuates as it travels through the propagation medium. This attenuation is influenced by both distance and frequency. In this study, a standard path loss model used for 5G networks is applied, expressed as [10]:

$$\mathrm{PL}(d) = 32.4 + 20\log_{10}(d) + 20\log_{10}(f_c) \tag{3}$$

In this equation, PL(d) denotes the Path Loss in decibels (dB) at a distance d (in meters) from the BS, and fc is the carrier frequency in gigahertz (GHz). The constant 32.4 accounts for free-space path loss, while the logarithmic terms represent the attenuation due to distance and frequency. This equation is used to calculate the received power Pr at each UE by subtracting the path loss from the transmitted power Pt [11]:

$$\mathrm{P_r} = P_{\mathrm{t}} - \mathrm{PL(d)} \tag{4}$$

This relationship shows that the received power decreases as PL increases, which occurs with greater distances or higher frequencies. The received power serves as a baseline for evaluating communication quality before introducing interference.

In the presence of jammers, the signal received at each UE is further degraded by interference. The model accounts for this by calculating the interference power using a similar path loss model. The overall impact of jammers is reflected in the received power at each UE, which decreases significantly compared to the baseline value. To evaluate the performance of the network under these conditions, the SINR is used as a key metric. The SINR at the i-th UE before applying any interference mitigation technique is given by [12]:

$$\mathrm{SINR_{before}} = \frac{\mathrm{P_{r,i}}}{\sum_{\mathrm{k}=1}^{\mathrm{K}} I_{\mathrm{ji}} + \sigma^2} \tag{5}$$

In this expression, Pr,i is the received power at the i-th UE, $\sum_{k=1}^{K} I_{ji}$ represents the total interference power from all K jammers, and $\sigma 2$ is the noise power. The SINR value provides a measure of signal quality by comparing the desired signal power to the sum of interference and noise power.

After applying beamforming or other interference mitigation techniques, the SINR is recalculated, reflecting the improvement in performance due to the suppression of interference. The improved SINR is denoted as SINRafter, which indicates how effectively the mitigation technique enhances communication quality.

The difference between SINRbefore and SINRafter demonstrates the effectiveness of the applied mitigation technique in restoring or enhancing signal quality. This mathematical model provides a comprehensive framework for analyzing the performance of a 5G MIMO network under various conditions, making it suitable for evaluating the results obtained from the experiments described in subsequent sections.

Furthermore, the Bit Error Rate (BER) is also evaluated to further assess communication quality at each UE. BER measures the reliability of data transmission by calculating the ratio of erroneous bits received to the total number of bits transmitted. A higher BER indicates poor transmission quality, while a lower BER reflects better communication performance.

Before applying any interference mitigation technique, the BER at each UE is directly influenced by the interference from the jammers and the overall signal quality. As interference increases, the BER value rises, indicating a higher number of errors in data transmission.

After applying beamforming, the BER is recalculated to measure the improvement in transmission quality. A lower BER value after beamforming compared to the initial BER value demonstrates the effectiveness of the beamforming technique in reducing transmission errors and enhancing overall communication reliability. This decrease in BER shows that the applied mitigation strategy successfully counteracts interference and improves network performance under adverse conditions.

3. Algorithm Analysis

This section provides an in-depth analysis of the theoretical algorithm, which was evaluated through a series of simulations. Algorithm 1 begins by setting up the 5G MIMO network environment, configuring key parameters, and visualizing the network topology. It proceeds through several stages, including interference simulation, beamforming application, and performance evaluation. Each step in the algorithm is structured to demonstrate the impact of jamming on communication quality and the effectiveness of beamforming techniques in mitigating such interference.

Algorithm 1 Evaluating Beamforming-Based Interference Mitigation in 5G MIMO Networks Under Jamming Conditions

Step.1 Network Initialization and Parameter Configuration:
- Clear all previous variables, close any open figures, and set up the necessary parameters for the simulation.
- Define the number of UE, jammers, and antennas at both the BS and the UE.
- Set transmission power, carrier frequency, and bandwidth values, which are representative of a realistic 5G MIMO network.

Step.2 Network Topology Visualization:
- Define fixed positions for the BS, UE, and jammers within a two-dimensional space.
- Create a figure to visually represent the network topology, where the BS is plotted at the origin, and UE and jammers are plotted at their respective positions.
- Label each entity for clear identification and set plot boundaries for better visualization.

Step.3 Baseline Received Signal Power Calculation:
- Compute the distances between the BS and each UE.
- Use a standard path loss model to calculate the received power at each UE, which serves as a baseline without any interference.
- Generate a bar plot to illustrate the received signal power at each UE under these ideal conditions.

Step.4 Simulating Jamming Effects:
- Introduce jammers with higher transmission power than the BS to disrupt communication.
- Assume that jamming reduces the received power at each UE by a fixed amount, simulating the negative impact of interference.
- Create a bar plot to demonstrate the significant reduction in received power at each UE due to jamming.

Step.5 Beamforming to Mitigate Jamming:
- Construct an adaptive beamforming matrix based on the positions of the UE relative to the BS.
- Calculate a steering vector for each UE to focus signal energy on them while minimizing interference in the directions of the jammers.
- Recalculate the received power at each UE after applying beamforming to observe the improvement.
- Display the new received power values using a bar plot, highlighting the effectiveness of beamforming in restoring communication quality.

Step.6 SINR Calculation and Comparison:
- Calculate the SINR at each UE before applying beamforming to quantify the signal quality under jamming conditions.
- Recalculate the SINR after beamforming to evaluate the improvement in communication quality.
- Generate a grouped bar plot to compare SINR values before and after beamforming.

Step.7 Step: BER Calculation and Comparison
- Calculate the BER at each UE before applying beamforming. The BER serves as a measure of the quality of communication, representing the proportion of bit errors relative to the total number of bits transmitted under jamming conditions.
- Apply beamforming at the BS to mitigate interference from the jammers.
- Recalculate the BER at each UE after applying beamforming to observe the improvement in communication quality.
- Generate a grouped bar plot to compare the BER values before and after beamforming. This comparison highlights the effectiveness of beamforming in reducing transmission errors and improving communication reliability.

Step.8 Comparison of Signal Quality Across Different Scenarios:
- Compare the received signal power at each UE across three different scenarios: without jamming, with jamming, and after beamforming.
- Generate a line plot to visualize these comparisons, providing a comprehensive view of the overall system performance under varying conditions.
- Highlight the improvements achieved through beamforming and the restored communication quality, as shown in the final plot.

The Algorithm 1 has been developed to theoretically assess the performance of a 5G MIMO network under interference, with a particular emphasis on the impact of jamming and the potential of adaptive beamforming to mitigate its effects. Initially, the simulation environment is set up by clearing previous variables and closing any open figures, followed by the configuration of key parameters such as the number of UE, jammers, and antennas at both the BS and the UEs. Transmission power, carrier frequency, and bandwidth values are established to reflect realistic network conditions. The network topology is then visualized by positioning the BS at a fixed location and placing the UEs and jammers within a two-dimensional grid, with clear labeling to facilitate accurate representation of the scenario.

Following this, the algorithm calculates the baseline received signal power by determining the distances between the BS and each UE and applying a standard path loss model. This baseline provides a reference point for optimal communication performance in the absence of interference. When jamming is introduced—simulated by deploying jammers with higher transmission power than the BS—a significant reduction in received signal power is observed, along with a corresponding drop in SINR and an increase in the BER. These changes effectively illustrate the disruptive influence of jamming on network performance. To counteract these negative effects, the algorithm applies adaptive beamforming. An adaptive beamforming matrix is constructed based on the relative positions of the UEs, and a steering vector is calculated for each user to concentrate the transmitted signal energy while minimizing interference from the jammers. As a result, after beamforming is applied, the received signal power at each UE increases substantially, and the SINR values improve, returning nearly to the baseline levels observed before interference. In addition, the bit error rate is markedly reduced, highlighting the effectiveness of beamforming in enhancing communication reliability.

Finally, the algorithm conducts a comprehensive comparison of the signal quality across different scenarios without jamming, with jamming, and with beamforming applied using various visual representations such as bar and line plots. This comparative analysis clearly demonstrates that adaptive beamforming not only restores the degraded signal quality but also maintains robust communication even under challenging interference conditions. Overall, the algorithm provides a structured framework that confirms the potential of adaptive beamforming to significantly improve network performance by counteracting the adverse effects of jamming in 5G MIMO networks.

4. Simulation Environment

This section describes the simulation environment used to evaluate the performance of the proposed adaptive beamforming method under jamming conditions. The 5G MIMO network was modeled within a two-dimensional area measuring 60×60 meters. A Macro BS, equipped with 64 antennas, was placed centrally within this area. Four UEs (UE1, UE2, UE3, and UE4), each configured with 4 antennas to enable spatial multiplexing, were positioned strategically around the BS. Additionally, two jammers were deployed at predetermined locations to generate intentional interference. The simulation parameters included a carrier frequency of 6 GHz, commonly used in sub-6 GHz 5G scenarios, and a channel bandwidth of 100 MHz. Detailed simulation parameters such as transmit power levels, antenna gains, and jammer characteristics are summarized in Table I, while the specific spatial positions of the BS, UEs, and jammers are illustrated clearly in Fig. 1.

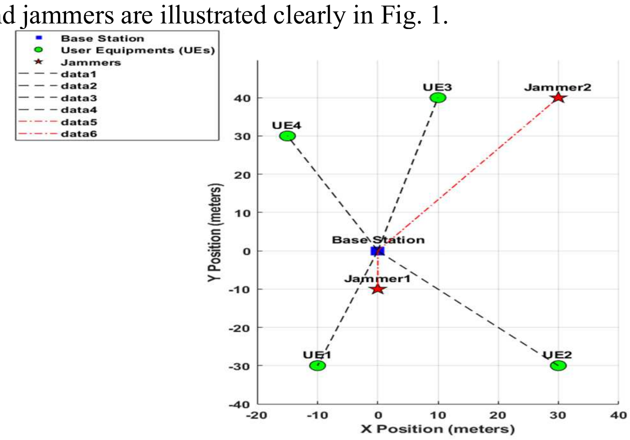

Fig.1. MIMO Network Topology

TABLE I. Simulation Parameters

Parameter	Value
Transmit Power (BS) (dbm)	40 dBm
Transmit Power-Jammer (dbm)	45 dBm
Carrier Frequency (GHz)	3.5 GHz
Channel Bandwidth (MHz)	100 MHz
Number of BS Antennas	Pnoise= -74+10log(Bandwidth(hz))
Number of UEs-Jammers	4, 2
Power Noise	-174 dBm/Hz
Subcarrier Spacing	120 kHz
Grid Dimensions	60 x 60 meters

To accurately simulate real-world conditions, the MATLAB-based implementation first calculated the horizontal distances between the BS and each UE. Using these distances, the Free-Space Path Loss (FSPL) values were computed, directly influencing the received signal power at the UEs under interference-free conditions. To represent jamming interference realistically, a predefined reduction of 5 dB was then applied to the calculated signal power at each UE. Subsequently, adaptive beamforming was introduced, providing a directional gain of 15 dB, significantly increasing the received signal strength towards the UEs and reducing the impact of the jammers. The effectiveness of the adaptive beamforming approach was quantified by evaluating three distinct scenarios: baseline conditions without jamming, degraded conditions under jamming, and restored conditions after beamforming was applied. SINR and received power levels were measured and compared across these scenarios, clearly illustrating the capability of the adaptive beamforming technique to enhance network performance under adverse interference conditions.

5. Performance Evaluation

The results from the experiments conducted provide a comprehensive understanding of the impact of jamming on the network performance and the effectiveness of beamforming techniques in mitigating this interference. The network topology Fig. 1 illustrates the spatial distribution of the BS, UE, and jammers within a defined area. The connections between the BS, UE, and jammers are depicted by lines to visualize the transmission paths and the potential interference links. This visualization helps set the stage for analyzing how interference propagates through the network and how beamforming can redirect signal energy to avoid jamming.

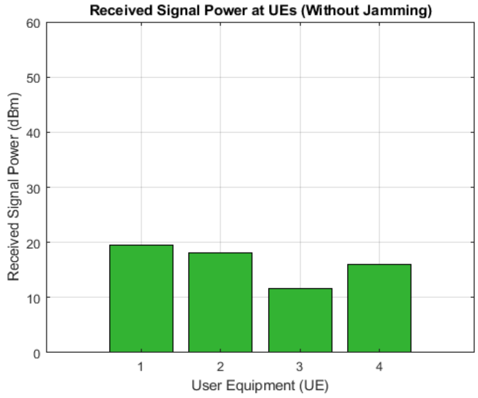

Fig.2. Received Signal Power at UE Without Jamming

Fig. 2 displays the received signal power at four user equipment devices (UE1, UE2, UE3, UE4) under normal conditions, with no interference present. The x-axis shows the UE labels, and the y-axis measures the power in dBm. The bars indicate that the received power levels are generally around 20 dBm for most UEs. For example, UE1 measures close to 19.5 dBm, and UE2 registers a similar value. UE3 is slightly lower than the others, indicating small variations across the network. These readings serve as a baseline for the network's performance, showing how the system operates in the absence of external disruptions.

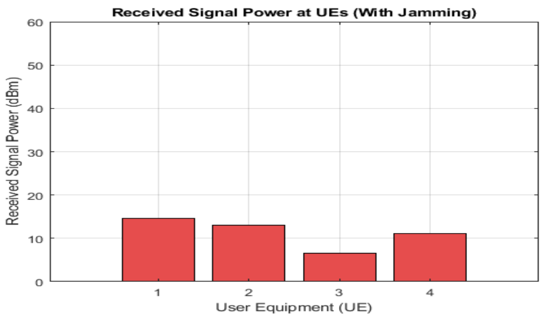

Fig.3. Impact of Jamming on Received Signal Power

Next, the fig. 3 illustrates the impact of introducing high-power jammers into the network. As before, the x-axis represents the four UEs, and the y-axis shows the measured signal power in dBm. The bars show a noticeable decrease of about 5 dBm for most UEs when compared to the baseline in Figure 2. For instance, the power level at UE1 drops from approximately 19.5 dBm to around 14.5 dBm. This reduction highlights how jamming signals interfere with the communication link between the BS and each UE. Even though the exact power loss varies slightly among the UEs, they all experience some decline, underscoring the disruptive effect of the jammers across the network.

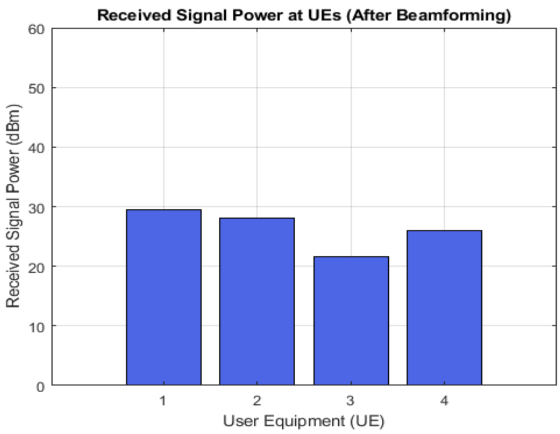

Fig.4. Received Signal Power After Applying Beamforming

Figure 4 demonstrates the improvements achieved by applying beamforming at the BS to counteract the jammers. The axes remain the same, with UEs on the x-axis and received power in dBm on the y-axis. The bars in this figure are higher than both the baseline (Fig. 2) and the jammed scenario (Fig. 3). Specifically, UE1's power level rises from around 14.5 dBm under jamming conditions to about 29.5 dBm after beamforming. Similar gains are observed by the other UEs, whose signal powers also exceed their initial (non-jammed) values. These results indicate that beamforming effectively concentrates signal energy toward each UE, reducing the impact of interference from the jammers and enhancing overall network performance.

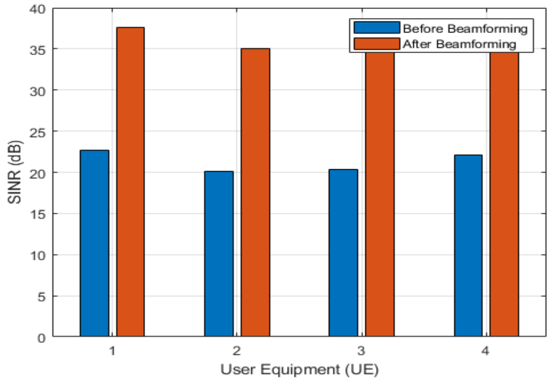

Fig.5. SINR Comparison Before and After Beamforming

The effectiveness of beamforming is further illustrated by the comparison of SINR values before and after applying beamforming, as presented in Fig. 5. Prior to beamforming, the SINR values were lower due to the interference caused by the jammers. For instance, the SINR for UE1 was approximately 22 dB, whereas, after applying beamforming, the SINR improved, increasing to 37.6 dB. This enhancement in SINR demonstrates the ability of beamforming to mitigate interference and establish a clear communication channel.

Additionally, the effectiveness of beamforming in reducing transmission errors is shown in Fig. 6. The BER values before beamforming were due to jamming interference. For instance, UE3 had a BER of approximately 0.25, indicating transmission errors. After beamforming, the BER dropped to approximately 0.06, a fourfold reduction in errors.

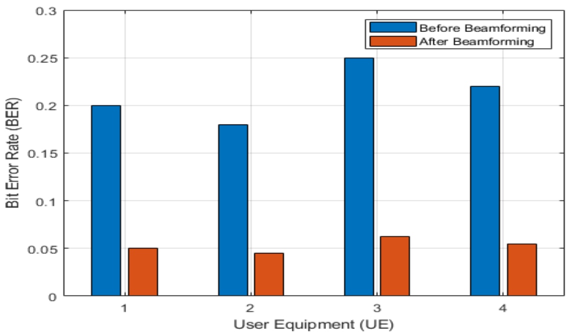

Fig.6. BER Comparison Before and After Beamforming

This decrease in BER highlights the ability of beamforming to focus the transmitted energy toward the intended UE, thereby minimizing interference and enhancing communication quality. The same trend is observed across all UE, confirming that beamforming improves the overall reliability and performance of the 5G MIMO network under jamming conditions.

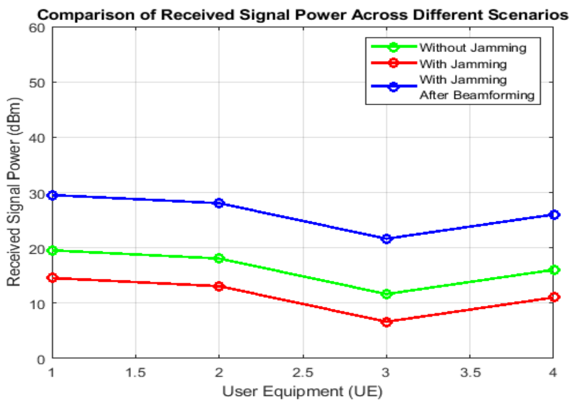

Fig.7. Comparison of Signal Quality Across Different Scenarios

Finally, Fig. 7 provides a holistic view of the received signal power across three scenarios: without jamming, with jamming, and with jamming after applying beamforming. The results indicate that while jamming reduces signal power by approximately 5 dBm for all UE, beamforming restores the signal power to levels noticeably higher than the baseline. For instance, the received signal power for UE1 dropped from 19.5 dBm (baseline) to 14.5 dBm under jamming but increased up to almost 29.5 dBm after applying beamforming.

Overall, in summary, the experiments reveal the severe impact of jamming on network performance, as evidenced by the significant reductions in received signal power and SINR. However, the application of beamforming techniques successfully counteracts these disruptions, restoring communication quality to near-optimal levels. These findings underscore the critical role of beamforming in maintaining the reliability and performance of 5G MIMO networks under interference conditions.

6. Conclusion and Future Work

In conclusion, this research presented an adaptive beamforming strategy specifically designed to address interference caused by jamming attacks in 5G MIMO networks. Through detailed simulations and analysis, the effectiveness of adaptive beamforming was demonstrated, highlighting clear improvements in received signal strength, SINR values, and communication reliability. The adaptive technique effectively reduced interference by dynamically steering the signal toward intended users, thereby counteracting the negative impacts introduced by jamming signals.

Additionally, the outcomes of this research underline the practical applicability of adaptive beamforming without the need for extra hardware or complex modifications to existing infrastructure. By clearly illustrating scenarios before and after beamforming implementation, the study provides concrete evidence of improved network performance under realistic interference conditions. This contributes directly to solving a critical security and reliability issue in modern wireless communications, making adaptive beamforming a strong candidate for practical adoption in 5G networks.

Looking forward, several promising directions for future research emerge from this study. One area of particular interest is exploring machine-learning techniques to enhance the real-time responsiveness and accuracy of adaptive beamforming adjustments. Additionally, future studies could examine beamforming performance within more complex multi-cell environments, considering scenarios with increased user mobility and dynamic interference patterns. Moreover we plan to investigate the impact of beamforming on system energy consumption. Investigating combined methods involving power control, cooperative communications, or hybrid mitigation approaches could also offer valuable improvements, further strengthening the resilience and reliability of next generation 5G systems.

Acknowledgment

The research project was supported by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the "2nd Call for H.F.R.I. Research Projects to support Faculty Members & Researchers" (Project Number: 02440).

References

[1] T. Konstantinos, et al, “Enhancing Spectral Efficiency in 5G MIMO Networks Through Adaptive Beamforming Techniques”, 2024 7th International Conference on Advanced Communication Technologies and Networking (CommNet), Rabat, Morocco, 2024, pp. 1-7

[2] D. Nguyen, M. Zomorrodi, N. Karmakar and K. Ho, “Efficient Beamforming Technique Based on Sparse MIMO Array and Spatial Filter Bank”, in IEEE Antennas and Wireless Propagation Letters, vol. 19, no. 7, pp. 1147-1151, July 2020

[3] R. Chitauro, M. Brzozowski, O. Yener and P. Langendörfer, “Real-Time Jamming Detection, Classification and Logging Using Computer Vision in 5G Private Networks”, 2024 19th International Symposium on Wireless Communication Systems (ISWCS), Rio de Janeiro, Brazil, 2024, pp. 1-6

[4] S. Dinh-Van, et al, “A Defensive Strategy Against Beam Training Attack in 5G mmWave Networks for Manufacturing”, in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2204-2217, 2023

[5] D. Darsena and F. Verde, “Anti-Jamming Beam Alignment in Millimeter-Wave MIMO Systems,” in IEEE Transactions on Communications, vol. 70, no. 8, pp. 5417-5433, Aug. 2022

[6] E. Bout, V. Loscri and A. Gallais, “Energy and Distance evaluation for Jamming Attacks in wireless networks”, 2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT), Prague, Czech Republic, 2020, pp. 1-5

[7] C. Örnek and M. Kartal, “An Efficient EVM Based Jamming Detection in 5G Networks”, 2022 4th IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Amman, Jordan, 2022, pp. 130-135

[8] H. Pirayesh and H. Zeng, “Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey”, in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 767-809, Secondquarter 2022

[9] A.Molisch., and F. Tufvesson, “Propagation channel models for next-generation wireless communications systems”, IEICE Transactions on Communications 97.10 (2014): 2022-2034.

[10] F.E. Shaibu., et al, “Performance of path loss models over mid-band and high-band channels for 5G communication networks: A review”, Future Internet 15.11 (2023): 362.

[11] T. Oladimeji., P Kumar, and M. Elmezughi, “An improved path loss model for 5G wireless networks in an enclosed hallway”. Wireless Netw 30, 2353–2364 (2024).

[12] H. Tataria, et al, “Standardization of propagation models: 800 MHz to 100 GHz--a historical perspective”, arXiv preprint arXiv:2006.08491 (2020).