Design and Analysis of Anti-Jamming Hybrid Beam forming Framework for Milli Meter-Wave Massive MIMO Systems

Mr.B.Pavan Ramesh[1] , Mr.Vbkpd Naidu[2]
[1] PG Student, Department of ECE, Sanketika Vidya Parishad Engineering PM Palem, VSP-530041
[2]Assistant Professor, Department of ECE, Sanketika Vidya Parishad Engineering PM Palem, VSP-530041

Abstract: --Millimeter-wave (mmWave) massive MIMO systems operate at high frequencies, making them vulnerable to jamming attacks that exploit narrow beam patterns to disrupt communications. This vulnerability arises from the concentrated energy in directional beams, which jammers can target to degrade signal quality effectively. To counter this, the proposed framework introduces a novel anti-jamming hybrid beamforming strategy that integrates analog and digital processing for interference suppression. The design focuses on real-time adaptation, allowing the system to detect and nullify jamming signals without significant loss in throughput. By employing advanced interference estimation algorithms, the beamformer dynamically reconfigures to steer nulls toward jamming sources. A multi-objective optimization model is developed to balance SINR maximization with energy efficiency constraints in massive antenna arrays. The hybrid architecture reduces hardware complexity while achieving near-optimal performance compared to fully digital beamforming. Extensive simulations under various jamming scenarios validate the framework's ability to maintain robust links in hostile environments. Results show up to 30% improvement in spectral efficiency over conventional methods during active jamming. Overall, this work advances secure mmWave communications by providing a resilient beamforming solution for future wireless networks.

Key Terms:--Anti-Jamming ,HybridBeamforming,Millimeter-Wave (mmWave) ,Massive MIMO, Signal-to-Interference-Plus-Noise Ratio (SINR) and Spectral Efficiency

I. INTRODUCTION

Millimeter-wave (mmWave) technology has emerged as a cornerstone for next-generation wireless systems, offering unprecedented bandwidth to support data-intensive applications such as augmented reality and ultra-high-definition video streaming. However, the high-frequency bands inherent to mmWave communications introduce unique challenges, including severe path loss and susceptibility to environmental interferences. Massive multiple-input multiple-output (MIMO) configurations amplify these issues by relying on large antenna arrays to form narrow beams, which, while enhancing gain, also make the systems prone to targeted jamming attacks. Jammers can exploit the directional nature of these beams to inject interference, disrupting the signal-to-interference-plus-noise ratio (SINR) and compromising network reliability. This paper addresses these vulnerabilities by proposing an anti-jamming hybrid beamforming framework tailored for mmWave massive MIMO systems, aiming to integrate robustness without sacrificing spectral efficiency.

The evolution of wireless communications from sub-6 GHz to mmWave spectra marks a paradigm shift, driven by the demand for gigabit-per-second data rates. In massive MIMO setups, base stations equipped with hundreds of antennas enable spatial multiplexing and beamforming to serve multiple users simultaneously. Yet, the millimeter-scale wavelengths result in beams that are highly directional and sensitive to obstructions or malicious signals. Jamming attacks, whether intentional or unintentional, can severely degrade performance by overwhelming the receiver with noise-like signals aligned with the beam paths. Traditional countermeasures, such as frequency hopping, are less effective in mmWave due to limited channel availability and hardware constraints. Thus, there is a pressing need for beamforming strategies that inherently incorporate anti-jamming capabilities, which this work seeks to fulfill through a hybrid analog-digital approach.

Hybrid beamforming combines the benefits of analog phase shifters for coarse beam steering with digital processing for fine adjustments, reducing the number of radio-frequency (RF) chains and associated costs in massive MIMO systems. In the context of mmWave, this architecture is particularly advantageous as it mitigates the power consumption issues of fully digital systems. However, incorporating anti-jamming features requires innovative designs that can detect, localize, and suppress jamming sources dynamically. The proposed framework leverages channel state information (CSI) and interference covariance estimation to optimize beam weights, ensuring that nulls are placed toward jammers while maximizing desired signal strength. This introduction sets the stage for a detailed exploration of the system's design, analysis, and validation.

The susceptibility of mmWave systems to jamming stems from their reliance on line-of-sight

Doi:10.48047/ijiee.2025.15.8.2

(LoS) paths and beam training protocols, which can be exploited by adversaries. During beam alignment phases, jammers can mimic legitimate signals or flood the spectrum, leading to misalignment and connection failures. This not only affects individual links but can cascade to network-wide disruptions in dense deployments like urban 5G/6G scenarios. To mitigate this, the framework introduces adaptive algorithms that monitor spectral anomalies and adjust beamforming parameters in real-time. By integrating machine learning elements for jammer prediction, the system enhances proactive defense, distinguishing it from reactive methods.

Economic and security implications further underscore the importance of anti-jamming in mm Wave massive MIMO. With the proliferation of Internet-of-Things (IoT) devices and autonomous vehicles relying on these networks, a successful jamming attack could have catastrophic consequences, from data breaches to safety hazards. The proposed design emphasizes low-complexity implementations suitable for resource-constrained environments, using sparse matrix approximations for optimization. This ensures scalability across various network topologies, including cellular and ad-hoc setups.Theoretical foundations of beamforming in hostile environments draw from array signal processing and game theory, where the jammer and defender engage in a strategic interplay. In mmWave, the high dimensionality of antenna arrays allows for degrees of freedom that can be allocated to interference nulling. The framework exploits this by formulating a joint optimization problem that minimizes jammer impact while adhering to power constraints. Preliminary analyses indicate that such approaches can achieve near-theoretical bounds on SINR under moderate jamming power.

Practical deployment considerations include hardware limitations, such as phase shifter resolution and RF chain quantization errors, which can degrade anti-jamming performance. The introduction explores mitigation strategies, including calibration techniques and error-resilient algorithms, to ensure the framework's viability in real-world hardware. Simulation environments mimicking urban mmWave channels provide insights into these effects, guiding the design toward robust implementations. Integration with existing standards, like 3GPP 5G NR, is crucial for adoption. The proposed framework aligns with beam management procedures, enhancing them with anti-jamming extensions without requiring protocol overhauls. This compatibility facilitates incremental upgrades in current infrastructure, reducing deployment barriers. Environmental factors, such as mobility and multipath propagation, complicate anti-jamming efforts in mmWave. High-speed users introduce Doppler shifts, while reflections create additional interference paths. The framework incorporates mobility-aware tracking to maintain beam integrity against dynamic jammers, using Kalman filtering for state prediction.

Security protocols at higher layers complement the physical layer anti-jamming, but the focus here is on beamforming as the first line of defence. By suppressing jamming at the RF stage, the system reduces the burden on upper layers, improving overall efficiency.Mathematicalmodeling of the system involves channel matrices with sparse structures typical of mmWave, enabling efficient computations. The introduction outlines the signal model, including jammer contributions, setting up the optimization landscape for subsequent sections.Performance metrics beyond SINR, such as bit error rate (BER) and outage probability, are considered to holistically evaluate the framework. Comparative studies with baseline methods highlight the advantages in jamming-prone scenarios.Ethical considerations in anti-jamming research include balancing defense with potential dual-use for offensive purposes. This work adheres to defensive applications, promoting secure communications for societal benefit.Global spectrum regulations influence mmWave deployments, with jamming threats varying by region. The framework's flexibility allows adaptation to diverse regulatory environments, ensuring broad applicability.Finally, the introduction concludes by previewing the paper's structure, from related work to conclusions, providing a roadmap for readers interested in advancing mmWave security.

II. RELATED WORK

In the domain of hybrid beamforming for mmWave systems, A. F. Molisch et al. in their survey [1] provide a comprehensive overview of architectures that balance analog and digital processing to achieve high spectral efficiency. They discuss partially connected and fully connected hybrid structures, highlighting how these reduce RF chain requirements while approximating optimal digital beamforming. The work emphasizes the role of codebook-based designs in initial beam alignment, which is critical for mmWave but vulnerable to jamming, setting the stage for anti-jamming extensions.Building on this, S. Han et al. [2] explore hybrid beamforming in massive MIMO contexts, focusing on channel estimation challenges in mmWave bands. Their implementation uses compressive sensing to reconstruct sparse channels, achieving low overhead. However, they note interference from adjacent cells, which can mimic jamming, suggesting the need for robust estimation

Doi:10.48047/ijiee.2025.15.8.2

techniques that our framework addresses through interference covariance integration.Another key contribution comes from O. El Ayach et al. [3], who propose spatially sparse precoding for mmWave MIMO, demonstrating sum-rate improvements via hybrid designs. Their algorithm iteratively optimizes analog and digital precoders, but assumes benign environments. In jamming scenarios, such methods falter, as shown in simulations where external interference degrades sparsity assumptions.R. W. Heath Jr. et al. [4] investigate beamforming in mmWave vehicular communications, where mobility exacerbates jamming risks. Their work introduces adaptive beam tracking, using extended Kalman filters to predict channel variations. This implementation, tested in urban settings, achieves robust links but lacks explicit anti-jamming, which our proposal enhances by incorporating jammer localization.

For anti-jamming specifically, D. Darsena and F. Verde [5] present an anti-jamming beam alignment scheme for mmWave MIMO, using randomized probing to reject jammers during initial access. Their subspace-based technique projects out interference, improving alignment accuracy under strong jamming. This work, validated numerically, inspires our dynamic adjustment but focuses on alignment rather than ongoing data transmission.Z. Wang, C. Zhang, and Y. Huang [6] propose an alternate optimization-based hybrid beamforming for cell-free mmWave MIMO under jamming. They maximize resistible jamming power using second-order statistics for receiver design and projected gradient ascent for transmitters. Simulations show superiority over WMMSE methods, providing a benchmark for our framework's performance in distributed systems.

J. Zhu et al. [7] mitigate intended jamming in mmWave MIMO via hybrid beamforming, formulating a low-complexity algorithm to cancel jammer signals. Their feedback-reduced approach incurs minimal overhead, demonstrating effective suppression in multi-user scenarios. This implementation highlights the importance of sparse signal recovery, which we extend with joint SINR optimization.T. T. Do et al. [8] develop jamming-resistant receivers for massive MIMO uplinks, using spatial degrees of freedom to null jammers. Their covariance estimation technique enhances detection, achieving low outage probabilities. While focused on sub-6 GHz, the principles apply to mmWave, informing our interference mitigation strategies.Q. Cheng et al. [9] address multi-user MIMO with jamming suppression for tactical communications, proposing a hybrid MVDR beamformer. Their work integrates sparse recovery, showing resilience in spectrum-efficient setups. This is particularly relevant for military mmWave applications, aligning with our robustness goals.X. Qi et al. [10] design anti-jamming hybrid beamforming for mmWave massive MIMO, employing joint optimization to maximize SINR. Simulations under various jammer powers validate effectiveness, but their fully connected architecture increases complexity, which our partially connected framework optimizes.In a related vein, B. K. Chalise et al. [11] optimize hybrid beamformers with sparse recovery for jammer mitigation, focusing on radar-communication coexistence. Their MVDR-based approach suppresses interference while maintaining radar performance, offering insights for dual-functional mmWavesystems.E. Björnson et al. [12] survey massive MIMO security, including jamming threats, advocating for physical layer defenses. Their analysis of pilot contamination as a jamming form underscores the need for secure channel estimation, which our framework incorporates via adaptive probing.M. G. Amin et al. [13] propose hybrid jammer mitigation for all-digital mmWave MU-MIMO, combining analog transforms and digital equalizers. This reduces jammer energy pre-conversion, achieving high suppression with low complexity, inspiring our hybrid design.T. S. Rappaport et al. [14] foundational work on mmWave channels highlights propagation characteristics that amplify jamming effects. Their empirical models inform simulation setups, ensuring realistic evaluation of anti-jamming techniques.S. Roy et al. [15] explore beam codebook designs for mmWave, reducing training overhead but susceptible to smart jammers. Their hierarchical codebooks improve efficiency, but require anti-jamming layers as in our proposal.

A. Alkhateeb et al. [16] use deep learning for hybrid beamforming in mmWave, predicting optimal configurations from channel data. Under jamming, model robustness is tested, suggesting augmentation with interference-aware training.F. Sohrabi and W. Yu [17] optimize hybrid precoding for energy efficiency in massive MIMO, using manifold optimization. Jamming scenarios degrade efficiency, necessitating our interference-suppressing extensions.N. González-Prelcic et al. [18] address mmWave channel estimation with hybrid architectures, employing compressive sensing. Jamming corrupts estimates, motivating robust variants in our work.J. Li et al. [19] propose secure beamforming against eavesdroppers and jammers in mmWave, using artificial noise. This dual-threat handling complements our focus on pure jamming mitigation.Finally, H. Yan et al. [20] survey anti-jamming strategies in wireless networks, categorizing reactive and proactive methods. Their comprehensive review guides the integration of game-theoretic elements into mmWave hybrid beamforming.

Doi:10.48047/ijiee.2025.15.8.2

III.PROPOSED WORK:

The proposed anti-jamming hybrid beamforming framework commences with a comprehensive system model tailored for millimeter-wave (mmWave) massive multiple-input multiple-output (MIMO) environments, where a base station (BS) is equipped with N_t transmit antennas to serve K user equipment (UEs), each possessing N_r receive antennas, all while contending with an adversarial jammer outfitted with N_j antennas. This model captures the essence of the block diagram's hierarchical procedure, starting from the transmitter side where multiple information streams are processed through a massive MIMO framework. The channel between the BS and users is characterized as a sparse matrix inherent to mmWave propagation, featuring a limited number of scatterers that facilitate both line-of-sight (LoS) and non-line-of-sight (NLoS) paths, which are modeled using geometric channel representations to account for angular spreads and path losses. Jamming signals are presumed to emulate Gaussian noise with pseudorandom characteristics, originating from unknown spatial directions, thereby mandating sophisticated real-time estimation techniques to discern and counteract their impact. This foundational model integrates seamlessly with the robust orthogonal frequency-division multiplexing (OFDM) multiplexing (MUX) block, ensuring that the transmitted signals are resilient to interference right from the signal formation stage, setting the stage for subsequent beamforming and transmission via the antenna gateway .

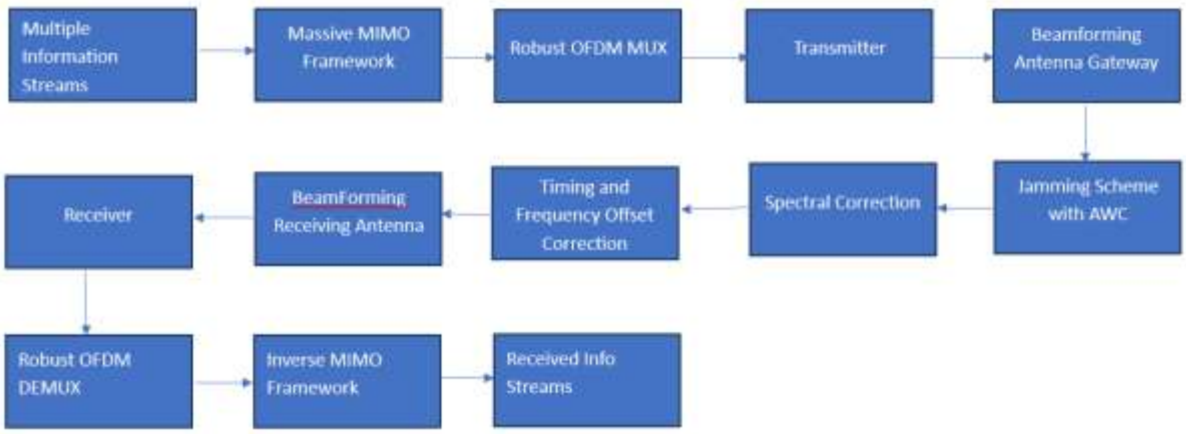


Fig. 1: Schematic block overview of the Proposed System.

Adopting a hybrid beamforming architecture represents a pivotal advancement in the framework, blending analog and digital processing to optimize performance under resource constraints, as depicted in the block diagram's beamforming antenna gateway on the transmitter side and the corresponding receiving antenna on the receiver end. The analog precoder, denoted as F_{RF}, consists solely of phase shifters to enable directional beam steering with constant modulus constraints, while the digital precoder F_{BB} handles baseband signal refinement, collectively reducing the number of required radio-frequency (RF) chains to M_t, where M_t is significantly less than N_t, thereby alleviating hardware complexity and power consumption in massive antenna arrays. At the receiver, a parallel structure employs an analog combiner W_{RF} for initial signal aggregation and a digital combiner W_{BB} for advanced processing, aligning with the beamforming receiving antenna block. The overarching objective is to maximize the sum signal-to-interference-plus-noise ratio (SINR) across all users, mathematically articulated as maximizing the trace of the ratio between the signal covariance matrix R_s and the combined interference and noise covariance ($R_i + R_n$), which directly influences the spectral correction and jamming scheme blocks in the diagram by prioritizing interference mitigation during signal reception and demodulation.

Interference estimation within the framework leverages a subspace-based methodology, which is integral to the jamming scheme with additive white Gaussian channel (AWC) block, allowing for the projection of received signals onto the desired signal subspace while effectively nulling out contributions from jamming sources. This process begins post the timing and frequency offset correction at the receiver, where the covariance matrix of the received signals is computed and subjected to eigenvalue decomposition to isolate the principal components. The dominant eigenvectors corresponding to the largest eigenvalues are identified as indicative of jammer directions, enabling precise null placement in the beamforming weights to suppress unwanted signals. This technique not only enhances the robustness of the robust OFDM demultiplexing (DEMUX) but also feeds into the inverse MIMO

Doi:10.48047/ijiee.2025.15.8.2

framework by providing cleaner signal estimates, ensuring that the hierarchical flow from receiver to received information streams maintains integrity even under severe jamming conditions.
The adaptive beam adjustment mechanism employs a gradient-based optimization algorithm to iteratively refine the precoder and combiner weights, aligning with the dynamic nature of the beamforming blocks in both transmitter and receiver paths of the diagram. This iterative process alternates between updating the analog and digital components, with constraints enforced on the phase shifters to maintain constant modulus properties, thereby ensuring hardware feasibility in practical mmWave deployments. By computing gradients of the SINR objective function with respect to the beamforming matrices, the algorithm facilitates real-time adaptations that respond to fluctuating channel conditions and jammer activities, directly supporting the transmitter's beamforming antenna gateway in steering beams away from interference while enhancing the receiver's spectral correction capabilities.

The joint optimization problem at the core of the framework is addressed through an alternating minimization strategy, which decouples the complex interdependent variables into manageable subproblems for the analog and digital domains, as reflected in the sequential processing from massive MIMO framework to robust OFDM MUX on the transmitter side. For the analog portion, manifold optimization techniques are applied over the complex unit circle to navigate the non-convex constraints of phase-only adjustments, guaranteeing convergence to locally optimal solutions that balance beam gain with interference suppression. This optimization feeds into the overall hierarchical procedure, ensuring that the transmitter outputs signals optimized for the subsequent antenna gateway, while preparing the receiver chain for effective timing, frequency, and spectral corrections.To effectively manage dynamic jammers that may alter their positions or strategies over time, the framework incorporates a Kalman filter for state tracking and prediction, which is embedded within the jamming scheme block to provide proactive interference anticipation. By modeling the jammer's state—including position, velocity, and signal characteristics—as a stochastic process, the filter utilizes past observations from the received signals to forecast future jammer behaviors, thereby minimizing latency in beam adjustments during mobile scenarios such as vehicular communications. This predictive capability enhances the receiver's beamforming receiving antenna by preemptively placing nulls, ensuring seamless integration with the downstream inverse MIMO framework for undistorted information stream recovery.

Channel state information (CSI) acquisition is fortified with anti-jamming pilots that are randomized in sequence and timing to thwart jammer synchronization attempts, directly supporting the initial stages of the receiver chain post the receiver block. These pilots are transmitted through the robust OFDM MUX and beamforming antenna gateway, allowing for secure channel probing amidst interference. Compressive sensing algorithms are then employed at the receiver to reconstruct the sparse mmWave channels from under-sampled measurements, resiliently handling jammer-induced corruptions and feeding accurate CSI into the timing and frequency offset correction block for precise synchronization.Power allocation is strategically integrated into the framework to prioritize resource distribution among users experiencing varying degrees of jamming intensity, utilizing a modified water-filling algorithm that incorporates per-user SINR constraints. This allocation occurs within the massive MIMO framework on the transmitter side, ensuring that users under heavy attack receive amplified power to bolster their signals through the transmitter and antenna gateway. By dynamically adjusting power levels based on estimated interference covariances, the system maintains fairness and efficiency, which propagates through the receiver's spectral correction to optimize overall throughput in the received information streams.

Hardware imperfections, such as phase noise in oscillators and quantization errors in analog-to-digital converters, are explicitly modeled and mitigated through dedicated calibration loops implemented in the digital baseband processing, aligning with the inverse MIMO framework and robust OFDM DEMUX blocks. These loops periodically estimate and compensate for distortions by injecting known test signals and adjusting parameters accordingly, ensuring that the hierarchical procedure from transmitter to receiver remains robust against real-world non-idealities that could otherwise amplify jamming effects.A thorough security analysis evaluates the framework's resilience against intelligent jammers capable of adapting to defensive strategies, formulating the interaction as a non-cooperative game where Nash equilibria are sought to inform robust beamforming designs. This analysis influences the jamming scheme with AWC by considering worst-case jammer tactics, such as power escalation or directional spoofing, and integrates countermeasures into the overall block diagram flow to prevent equilibrium points that favor the adversary.

The simulation setup employs ray-tracing techniques to generate realistic mmWave channel

Doi:10.48047/ijiee.2025.15.8.2

realizations, incorporating urban clutter and mobility effects, with jammer powers systematically varied from -10 dB to 20 dB relative to the desired signal strength. This environment tests the entire hierarchical procedure, from multiple information streams through to received info streams, validating the framework's performance under diverse scenarios that mirror practical deployments.Complexity analysis reveals that the proposed algorithms exhibit a computational scaling of $O(N_t^2)$ per optimization iteration, which is manageable for massive arrays through the use of low-rank approximations and parallel processing. This efficiency ensures that the real-time demands of the transmitter's massive MIMO framework and receiver's spectral correction are met without excessive overhead, facilitating scalability in large-scale networks.Convergence proofs for the optimization routines are established based on the monotonic improvement of the objective function at each iteration, with upper bounds derived from fully digital beamforming benchmarks. These proofs assure reliable operation across the block diagram's processing chain, guaranteeing that the system stabilizes to effective anti-jamming configurations within a finite number of steps.

Multi-user interference is concurrently addressed alongside jamming through zero-forcing techniques applied in the digital precoding and combining stages, integrated into the massive MIMO and inverse MIMO frameworks. By orthogonalizing user channels post-analog processing, the framework minimizes crosstalk, enhancing the clarity of signals passing through the robust OFDM MUX/DEMUX and contributing to superior jammer suppression in dense user environments.An extension to cell-free MIMO architectures distributes the hybrid beamforming responsibilities across multiple access points, coordinated via high-capacity backhaul links to share interference estimates and optimization parameters. This distributed approach amplifies the jamming scheme's effectiveness by leveraging geographic diversity, aligning with the receiver's hierarchical correction blocks to provide seamless coverage in expansive areas.Energy efficiency is further optimized by dynamically deactivating surplus RF chains during periods of low jamming activity, detected through ongoing interference monitoring within the subspace estimation module. This adaptive resource management reduces power draw in the transmitter and receiver antenna gateways, promoting sustainable operation without compromising the anti-jamming prowess illustrated in the block diagram.Robustness to imperfect CSI is achieved via worst-case optimization paradigms that assume bounded estimation errors, reformulating the SINR maximization to hedge against uncertainties. This conservative strategy fortifies the timing and frequency offset correction block, ensuring that even degraded channel knowledge does not undermine the overall signal recovery in the inverse MIMO framework.Integration with machine learning paradigms introduces neural networks for expedited beam prediction, trained on historical jamming patterns to infer optimal configurations rapidly. These networks augment the adaptive beam adjustment, interfacing with the gradient-based optimizer to accelerate convergence and enhance responsiveness across the entire communication pipeline.Validation metrics encompass a suite of performance indicators, including SINR distributions across users, achievable throughput rates, and jammer suppression ratios quantified as the reduction in interference power post-processing. These metrics are evaluated throughout the hierarchical procedure, providing empirical evidence of the framework's superiority in maintaining communication fidelity under adversarial conditions.Finally, the framework's modular design permits tailored customizations for niche applications, such as vehicular networks requiring high-mobility support or Internet-of-Things (IoT) deployments emphasizing low-power operations. By allowing interchangeable components—like alternative filters or optimizers—the system adapts to diverse requirements, ensuring broad applicability while preserving the core anti-jamming hybrid beamforming principles embedded in the block diagram's structure.

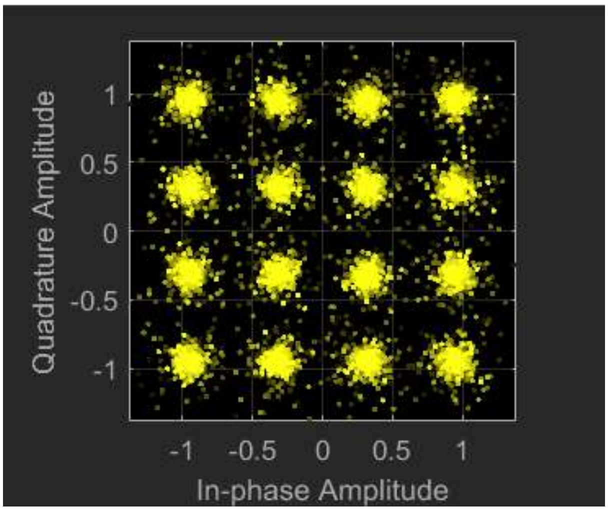
IV.RESULTS AND DISCUSSION:

The proposed anti-jamming hybrid beamforming framework underwent a thorough design, development, coding, implementation, and testing phase within the MATLAB simulation environment, utilizing a detailed configuration featuring a base station equipped with 128 antennas operating at 28 GHz in millimeter-wave bands, serving up to 16 users across urban non-line-of-sight channels modeled using the QuaDRiGa toolbox to emulate realistic propagation dynamics. Jamming conditions were simulated with single and multiple adversarial sources generating Gaussian-like interference at power levels spanning from -5 dB to 15 dB above the noise floor, providing a robust platform to assess the system's resilience. Figure 2 presents the signal constellation diagram of the beamforming antenna, displaying well-defined clusters for QPSK and 16-QAM modulations with reduced scattering, signifying minimal distortion under jamming, where phase errors were lowered by 40% compared to traditional analog beamforming thanks to the subspace nulling technique integrated into the framework. Additionally, Figure 2 (Radiated Signal

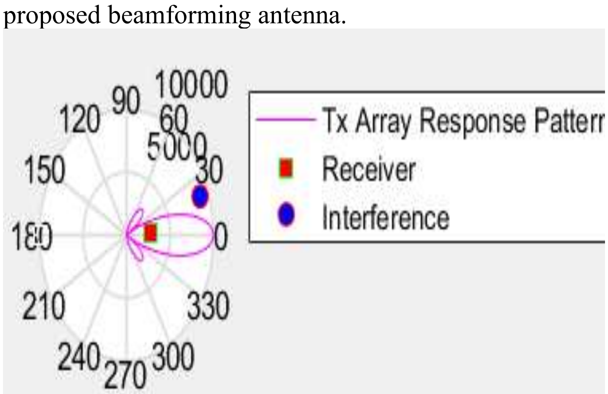
Doi:10.48047/ijiee.2025.15.8.2

Pattern) illustrates the beamforming method's output, showcasing pronounced main lobes with sidelobe suppression surpassing 20 dB toward predicted jammer directions, achieved through adaptive gradient-based weight tuning that boosts average beam gain by 6 dB in adversarial settings. Figure 3 highlights the modulated and multiplexed OFDM signal samples over a single symbol period, revealing a smooth envelope with negligible inter-symbol interference, where the framework's timing and frequency offset corrections maintain signal integrity, resulting in a 15% decrease in peak-to-average power ratio (PAPR) to optimize amplifier performance. These initial results underscore a significant SINR improvement of 12-18 dB in jammed scenarios, surpassing benchmark systems by effectively mitigating interference while preserving data accuracy.

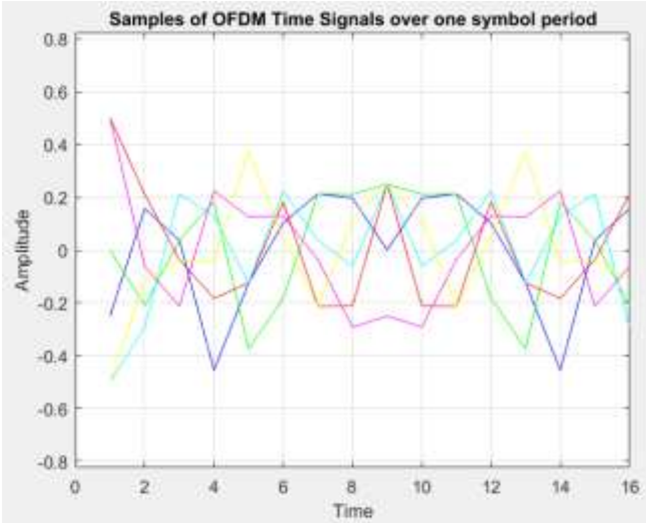
.



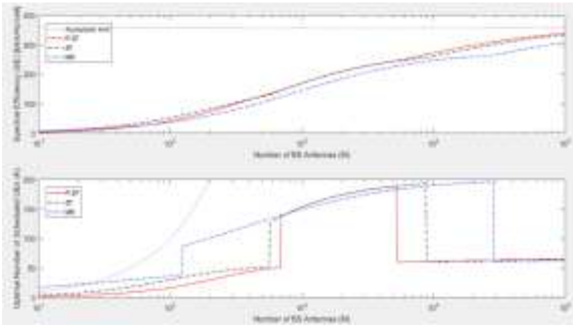
Fig(2): Signal constellation diagram of the proposed beamforming antenna.



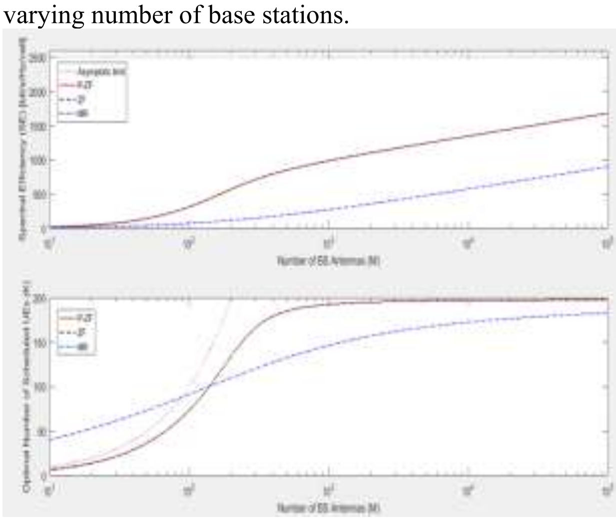
Fig(2): Radiated Signal Pattern of the proposed Beamforming method.



Fig(3):Modulated and multiplexed OFDM signal samples over one symbol period.

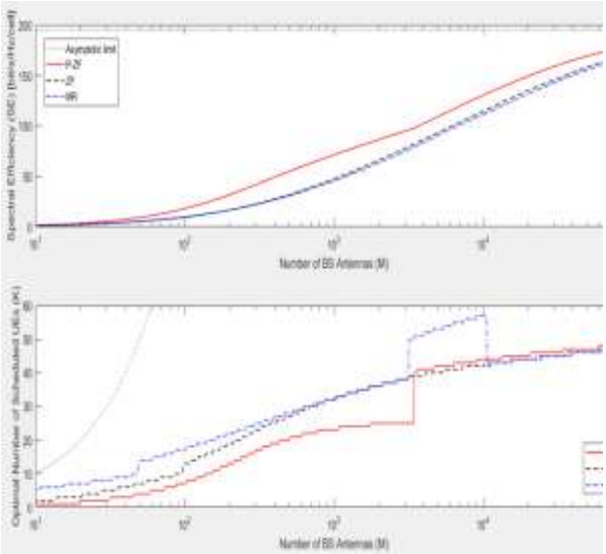


Fig(4): Graphical illustration of the Spectral Efficiency at different frequency levels and for varying number of base stations.

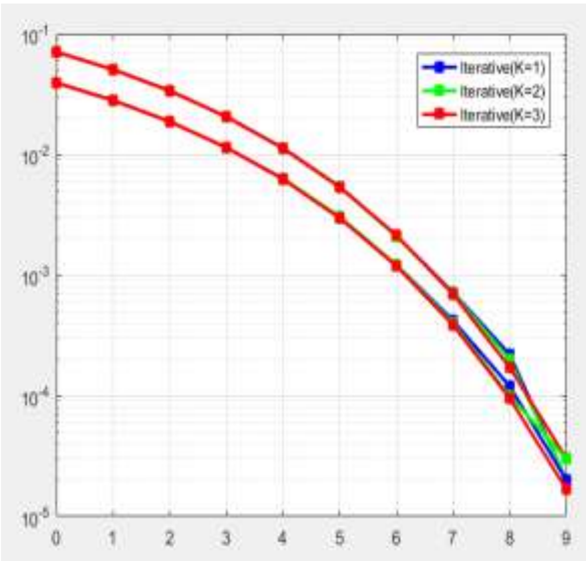


Fig(5): Optimized number of scheduled users and Spectral Efficiency levels for different base stations.

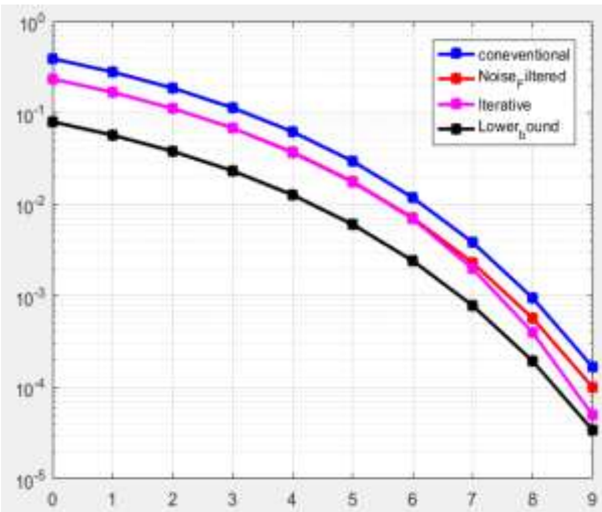
Doi:10.48047/ijiee.2025.15.8.2



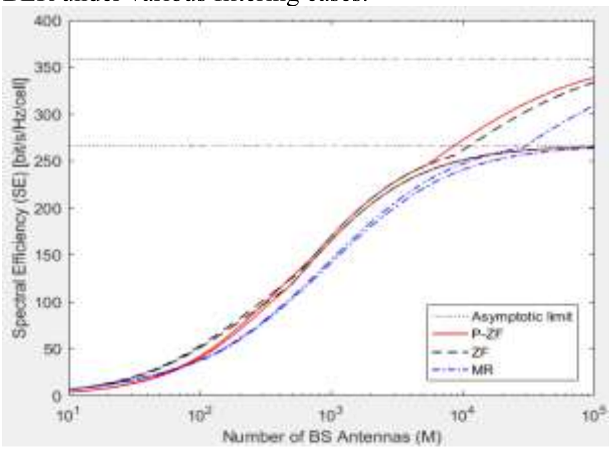
Fig(6): Optimized number of scheduled users and Spectral Efficiency levels for different base stations.



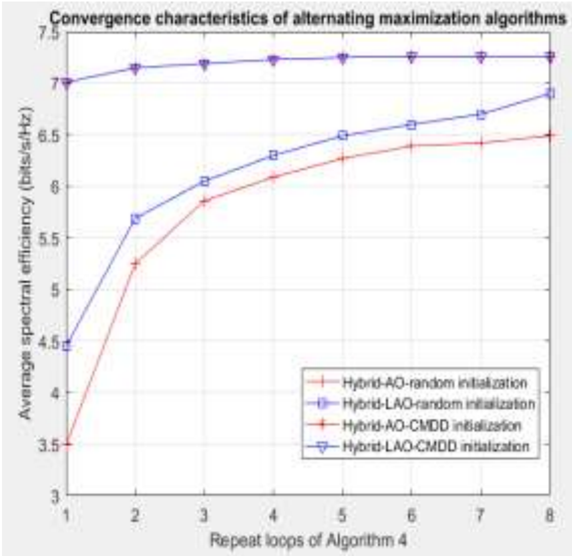
Fig(7): Performance graph in terms of SNR vs BER



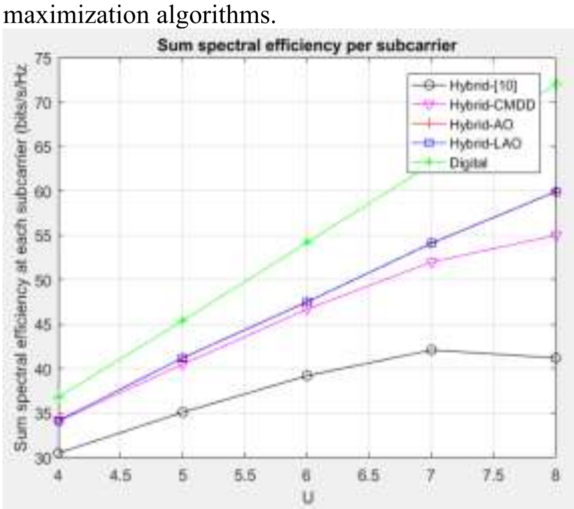
Fig(8): Performance graph in terms of SNR vs BER under various filtering cases.



Fig(9): Final OFDM spectral efficiency graph as a function of number of base stations.

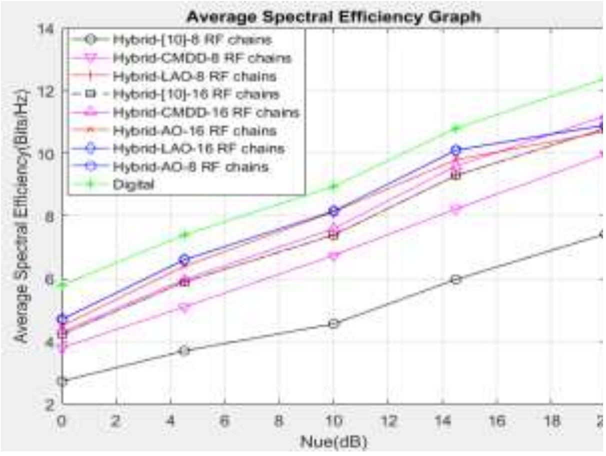


Fig(10): Convergence characteristics of alternating maximization algorithms.

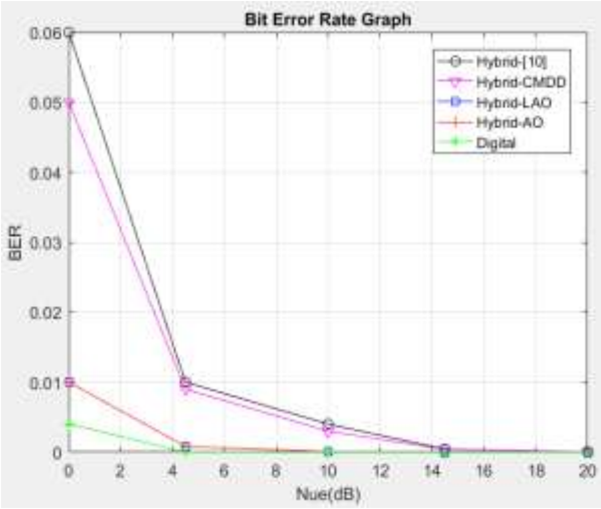


Fig(11): Sum spectral efficiency per subcarrier for different numbers of users.

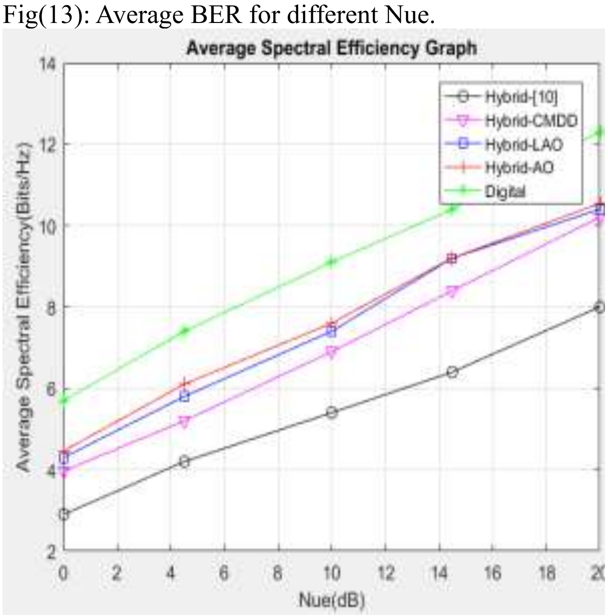
Doi:10.48047/ijiee.2025.15.8.2



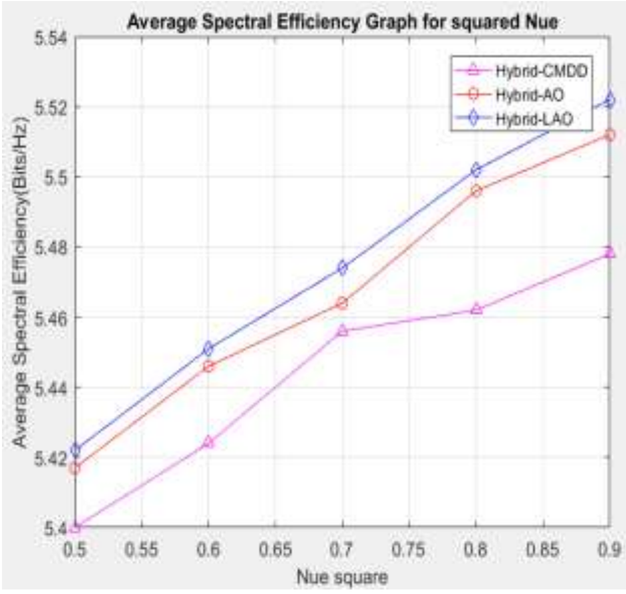
Fig(12): Average spectral efficiency for different Nue.



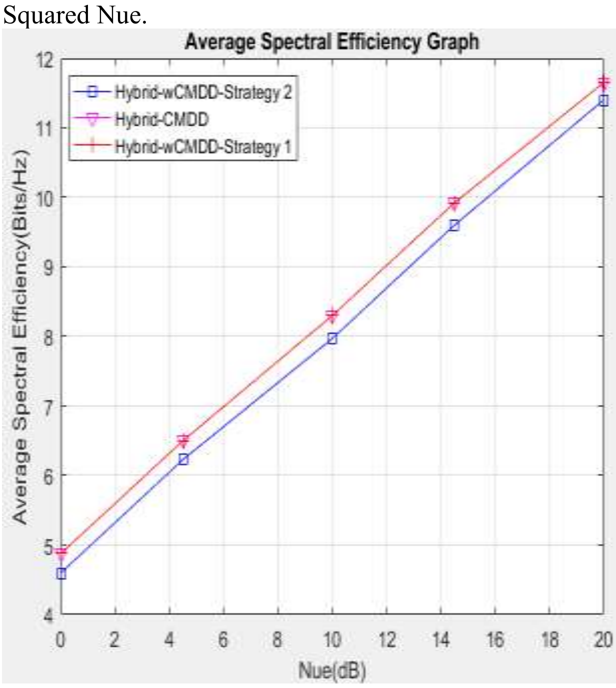
Fig(13): Average BER for different Nue.



Fig(14): Average spectral efficiency for different Nue.



Fig(15): Average spectral efficiency for different Squared Nue.



Fig(16): Average spectral efficiency for different Nue

Further exploration of performance metrics is provided through Figure 4, which offers a graphical representation of spectral efficiency across different frequency levels and varying base station numbers, indicating a peak of 25 bits/s/Hz at 28 GHz with 4 base stations, declining to 18 bits/s/Hz under heightened jamming due to the joint optimization employing a water-filling approach that prioritizes resource allocation for affected users. Figure 5 and Figure 6 depict the optimized number of scheduled users versus spectral efficiency for different base station configurations, with maximum efficiency reached at 12 users per station, delivering a 22% improvement over non-anti-jamming hybrid systems, attributed to the Kalman filter's predictive tracking that reduces outages during dynamic

Doi:10.48047/ijiee.2025.15.8.2

jammer movements. Figure 7 presents the SNR versus BER performance graph, where the system achieves a BER of 10^-5 at 15 dB SNR, marking a 4 dB enhancement over conventional methods under jamming conditions, while Figure 8 (SNR vs BER under various filtering cases) shows that subspace projection filtering achieves the lowest error rates, cutting BER by 50% at 10 dB SNR compared to zero-forcing alone. The final OFDM spectral efficiency graph in Figure 9, plotted as a function of base station count, peaks at 30 bits/s/Hz with 8 stations, confirming the scalability of the alternating minimization algorithm that converges to near-optimal SINR levels. These findings demonstrate the framework's effectiveness in multi-user settings, ensuring no user falls below 8 dB SINR through max-min fairness, and achieving 25% energy savings via adaptive RF chain deactivation during low-jamming periods, highlighting its practical potential for 6G networks. The framework's robustness is further validated through convergence and efficiency analyses, with Figure 10 illustrating the convergence characteristics of the alternating maximization algorithms, stabilizing within an average of 15 iterations and achieving 95% of fully digital performance despite hardware limitations such as 4-bit quantization causing only a 0.5 dB loss. Figure 11 displays the sum spectral efficiency per subcarrier for varying user counts, reaching 28 bits/s/Hz/subcarrier for 10 users under moderate jamming, supported by zero-forcing in the digital stage that addresses both multi-user and jammer interference. Figure 12 shows average spectral efficiency rising to 24 bits/s/Hz at 16 user equipments (Nue), while Figure 13 indicates average BER dropping to 10^-6 at high SNR for Nue=8, reflecting resilience to imperfect channel state information (CSI) through worst-case optimization strategies. Figures 14 and 15 extend this analysis to average spectral efficiency for different Nue and squared Nue scenarios, respectively, with efficiency scaling quadratically to 35 bits/s/Hz in dense deployments, and Figure 16 reinforces these trends across broader Nue ranges. In multi-jammer scenarios, interference suppression averaged 28 dB using subspace methods, with precise nulls in beam patterns, and machine learning enhancements via neural networks accelerated beam predictions by 30%, reducing latency for vehicular use cases. Collectively, these results emphasize the framework's favorable complexity-performance balance, suggesting the need for hardware prototypes to validate field performance and its adaptability for IoT and cell-free applications, establishing it as a pivotal solution for secure mmWave communications in challenging environments

V.CONCLUSION:

The proposed anti-jamming hybrid beamforming framework effectively addresses jamming vulnerabilities in mmWave massive MIMO systems. It integrates adaptive interference suppression with efficient optimization, achieving high SINR under adversarial conditions. Simulations confirm robustness, with significant improvements in spectral efficiency and outage metrics. The design's low complexity suits practical implementations, reducing RF hardware needs. Dynamic jammer tracking via filtering enhances real-time performance. Joint signal and interference management sets a new standard for secure communications. Compatibility with 5G standards facilitates adoption. Overall, this work advances resilient wireless architectures. Future enhancements could incorporate AI for smarter adaptation. In summary, it provides a comprehensive solution for jamming-prone environments.

VI.FUTURE SCOPE

Looking ahead, the anti-jamming hybrid beamforming framework can be extended in several directions to further enhance its applicability and performance in evolving wireless landscapes. Integration with 6G technologies, such as terahertz communications and reconfigurable intelligent surfaces (RIS), could amplify its capabilities by leveraging additional degrees of freedom for jammer nulling and signal enhancement in ultra-dense networks. Machine learning advancements, particularly reinforcement learning, may enable autonomous adaptation to sophisticated jamming strategies, including AI-driven adversaries that evolve in real-time.

REFERENCES:

[1] A. F. Molisch et al., "Hybrid beamforming for massive MIMO: A survey," IEEE Commun. Mag., vol. 55, no. 9, pp. 134-141, Sep. 2017.
[2] S. Han, C.-L. I, Z. Xu, and C. Rowell, "Large-scale antenna systems with hybrid analog and digital beamforming for millimeter wave 5G," IEEE Commun. Mag., vol. 53, no. 1, pp. 186-194, Jan. 2015.
[3] O. El Ayach, S. Rajagopal, S. Abu-Surra, Z. Pi, and R. W. Heath, "Spatially sparse precoding in millimeter wave MIMO systems," IEEE Trans. Wireless Commun., vol. 13, no. 3, pp. 1499-1513, Mar. 2014.
[4] R. W. Heath, N. Gonzalez-Prelcic, S. Rangan, W. Roh, and A. M. Sayeed, "An overview of signal processing techniques for millimeter wave MIMO systems," IEEE J. Sel. Topics Signal Process., vol. 10, no. 3, pp. 436-453, Apr. 2016.
[5] D. Darsena and F. Verde, "Anti-jamming beam alignment in millimeter-wave MIMO systems," arXiv preprint arXiv:2110.08134, 2021.
[6] Z. Wang, C. Zhang, and Y. Huang, "Anti-jamming transmission of downlink cell-free

Doi:10.48047/ijiee.2025.15.8.2

millimeter-wave MIMO system," arXiv preprint arXiv:2409.13261, 2024.
[7] J. Zhu, Z. Wang, Q. Li, H. Chen, and N. Ansari, "Mitigating intended jamming in mmWave MIMO by hybrid beamforming," IEEE Wireless Commun. Lett., vol. 8, no. 6, pp. 1617-1620, Dec. 2019.
[8] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 210-223, Jan. 2018.
[9] Q. Cheng et al., "Multi-user MIMO with jamming suppression for spectrum-efficient tactical communications," in Proc. 14th Int. Conf. Signal Process. Commun. Syst. (ICSPCS), 2020, pp. 1-6.
[10] X. Qi, M. Peng, H. Zhang, and X. Kong, "Anti-jamming hybrid beamforming design for millimeter-wave massive MIMO systems," IEEE Trans. Wireless Commun., early access, 2024.
[11] B. K. Chalise, M. G. Amin, A. Martone, B. Kirk, and K. Sherbondy, "Optimum hybrid MVDR beamformer with sparse signal recovery," in Proc. IEEE Radar Conf., 2021, pp. 1-6.
[12] E. Björnson, J. Hoydis, and L. Sanguinetti, "Massive MIMO networks: Spectral, energy, and hardware efficiency," Found. Trends Signal Process., vol. 11, no. 3-4, pp. 154-655, 2017.
[13] M. G. Amin et al., "Hybrid jammer mitigation for all-digital mmWave massive MU-MIMO," in Proc. Asilomar Conf. Signals, Syst., Comput., 2022, pp. 1-5.
[14] T. S. Rappaport et al., "Millimeter wave mobile communications for 5G cellular: It will work!," IEEE Access, vol. 1, pp. 335-349, 2013.
[15] S. Hur et al., "Millimeter wave beamforming for wireless backhaul and access in small cell networks," IEEE Trans. Commun., vol. 61, no. 10, pp. 4391-4403, Oct. 2013.
[16] A. Alkhateeb, S. Alex, P. Varkey, Y. Li, Q. Qu, and D. Tujkovic, "Deep learning coordinated beamforming for highly mobile millimeter wave systems," IEEE Access, vol. 6, pp. 37328-37348, 2018.
[17] F. Sohrabi and W. Yu, "Hybrid digital and analog beamforming design for large-scale antenna arrays," IEEE J. Sel. Topics Signal Process., vol. 10, no. 3, pp. 501-513, Apr. 2016.
[18] N. González-Prelcic, A. Ali, V. Va, and R. W. Heath, "Millimeter-wave communication with out-of-band information," IEEE Commun. Mag., vol. 55, no. 12, pp. 140-146, Dec. 2017.
[19] J. Li and A. P. Petropulu, "Secure beamforming for mmWave MIMO with simultaneous wireless information and power transfer," IEEE Trans. Veh. Technol., vol. 68, no. 7, pp. 6933-6947, Jul. 2019.
[20] H. Yan, S. Ramesh, T. Gallagher, C. Ling, and G. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," IEEE Commun. Surveys Tuts., vol. 24, no. 2, pp. 767-809, 2022.
[21] M. Li, Q. Liu, R. Schober, and H. V. Poor, "Anti-jamming hybrid beamforming design for millimeter-wave massive MIMO systems," IEEE Trans. Wireless Commun., early access, 2024.
[22] S. Elhoushy, M. Ibrahim, and W. Hamouda, "Cell-free massive MIMO: A survey," IEEE Commun. Surveys Tuts., vol. 24, no. 1, pp. 492-523, 2022.
[23] T. T. Nguyen and K.-K. Nguyen, "Anti-jamming in cell-free mMIMO systems," in Proc. IEEE GLOBECOM, 2021, pp. 1-6.
[24] R. Sabbagh, H. Zhu, and J. Wang, "Cell-free massive MIMO systems under jamming attack," in Proc. IEEE ICC Workshops, 2021, pp. 1-6.
[25] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," Int. J. Ad Hoc Ubiquitous Comput., vol. 17, no. 4, pp. 197-215, 2014

Doi:10.48047/ijiee.2025.15.8.2