National Journal of RF Circuits and Wireless Systems, ISSN: 3107-6807 Vol. 3, No. 1, 2026 (pp. 1-7)

RESEARCH ARTICLE

ECEJOURNALS.IN

Hybrid Beamforming and Physical Layer Security Techniques for 6G Massive MIMO Communication Systems

Freddy Soria[1], Kesufekad Metachew[2]*

[1]Robotics and Automation Laboratory Universidad Privada Boliviana Cochabamba, Bolivia.
[2]Electrical and Computer Engineering Addis Ababa University Addis Ababa, Ethiopia

KEYWORDS:
6G,
Massive MIMO,
Hybrid Beamforming,
Physical Layer Security,
Artificial Noise,
Secrecy Rate,
Sub-array Architecture

ARTICLE HISTORY:
Submitted : 07.02.2025
Revised : 12.04.2025
Accepted : 17.07.2025

https://doi.org/10.17051/NJRFCS/03.01.01

Abstract

The present paper provides an in-depth inquiry on the topic of hybrid beamforming and physical layer security (PLS) technologies which will suit 6G massive multiple-input multiple-output (MIMO) communication systems. The first goal is to overcome both the energy-efficient beamforming and secure transmission issue with passive eavesdroppers, which is of utmost importance in 6G networks using millimeter-wave and sub-terahertz frequencies. The author suggests a new low-complexity hybrid analog-digital design of the beam forming structure which can use a sub-array structure to decrease the number of the RF chains but still generates high spatial resolution. Artificial noise (AN) is injected at particular locations within the null space of legitimate user channels; this has the effect of compromising signal quality on the capabilities of the eavesdropper only, without interfering with targeted receivers. The system architecture proposed optimizes the AN covariance matrix, analog precoder, and digital baseband precoder together in terms of the transmit power and hardware limitations. Extensive Monte-Carlo simulations under realistic propagation conditions demonstrate that the proposed approach has significantly better secrecy rate (an enhancement of up to 35% compared to conventional hybrid beamforming techniques) and a portion of energy efficiency is maintained with minimal negative impacts on robustness of the system in case of imperfect channel state information (CSI). The results attest to the effectiveness of the methodology in terms of practical and scalable 6G applications. Future extensions of the framework will be based on AI-powered adaptive beam choice and the incorporation of reconfigurable intelligent surfaces (RIS) to improve the physics-layer security.

Author's e-mail: metachew.kesu@aait.edu.et

How to cite this article: Soria F, Metachew K. Hybrid Beamforming and Physical Layer Security Techniques for 6G Massive MIMO Communication Systems. National Journal of RF Circuits and Wireless Systems, Vol. 3, No. 1, 2026 (pp. 1-7).

Introduction

Large-scale antenna arrays have turned massive multiple-input multiple-output (MIMO) technology into a basic facilitator of 6G wireless networks, with the possibility of attaining unheard of performance levels in the spectral efficiency, energy efficiency, and spatial multiplexing capacities.[1] The basic problem is that a complete digitization of beamforming, even in these systems, is not yet feasible because of hardware complexity, cost, and power requirements especially at high frequencies (mmWave and sub-THz). As such, hybrid analog-digital beamforming has become an achievable alternative, presenting a trade-off between performance and the practical hardware limits.[2] At the same time there is also a lot of vulnerabilities to passive eavesdropping and impersonal interception because of the broadcast and open character of the wireless channels. This has made the protective of the physical layer (PLS) a critical area of concern; where the channel properties of the wireless medium are used to provide confidentiality of the communication without necessarily depending on the cryptographic protocols.[3]

Much research effort has been made on hybrid beamforming in mmWave systems and PLS with artificial noise (AN) or secure precoding, respectively, but little research has been done on the joint optimization of them in 6G massive MIMO, particularly within the hardware-constrained settings with from channel estimation errors.

The proposed paper addresses this gap by suggesting a secure hybrid beamforming with low complexity that will incorporate the AN-based PLS mechanisms and still achieve efficiency and robustness.

The rest of the paper is structured as follows: Section II is related work; Section III defines the system model; Section IV describes the suggested hybrid beamforming and PLS design; Section V analyzes performance; and Section VI concludes with recommendations of future work.

Related Work

Hybrid beamforming has received an immense amount of research interest as a low-cost approach to millimeter-wave (mmWave) and sub-terahertz (THz) MIMO systems where full digital beamforming is not possible either because of hardware constraints or because of high power requirements.[4, 5] Several hybrid architectures, such as fully connected and sub-array-based hybrid architectures, were proposed by the researchers to strike a balance between the degree of beamforming accuracy and system complexity.[6] In these systems, to increase the spectral and energy efficiency, optimization algorithms relying on alternate minimization and machine learning have been developed as well as compressive sensing.[7] Simultaneously, the physical layer security (PLS) has developed into a vital paradigm in the secure transmission in the wireless transmission especially against passive eavesdroppers and active ones. Artificial noise (AN) injection techniques, secure beamforming, and secrecy rate maximization are among the techniques which have been created to reduce the threat of interception at the PHY layer.[8, 9] Though these techniques have potential to incorporate significant security advances, they in general assume ideal conditions to implement such methods (perfect channel state information CSI, and fully digital precoding), and these conditions are unrealistic in large scale deployments of antennas. Nevertheless, the resulting targeting of the two domains has not been extensively explored to date, and there is little research on joint optimization of the domains, especially in the use of the constraints peculiar to 6G, including ultra-massive antenna arrays, ultra-mobility of users, sub-THz propagation impairments, and non-idealities of hardware.[10] Realistic hybrid architectures and the consequences of imperfect CSI on the secrecy rate performance have not been considered in most of the existing work involving realistic architectures with fewer RF chains.

The current paper addresses this gap by introducing a shared hybrid beamforming and PLS structure that suits power-efficient, secure communication in 6G massive MIMO systems and which considers some of those practical constraints including limited RF chains, artificial noise optimization, and uncertainty in channels.

System Model

We assume a downlink transmission system in a 6G massive MIMO communication system, where a base station (BS) with Nt transmit antennas, NRF < Nt chains transmits to K single-antenna and legitimate users in the presence of one or more passive eavesdroppers. Such configuration echoes the applied limits of hybrid beamforming systems where the quantity of RF chains is considerably smaller due to the aim of decreasing the cost of the hardware, energy utilization, and intricacy.[11] Figure 1 presents an overview of this system. System Model of Hybrid Beamforming and Physical Layer Security 6G Massive MIMO Network.

Hybrid Beamforming Structure

The BS implements a hybrid analog–digital precoding strategy to transmit the confidential signals. The transmitted signal $x \in C^{N_t \times 1}$ is expressed as:

$$x = F_{RF} F_{BB} s + z_{AN} \quad (1)$$

where:

- FRF∈CNt× NRF is the analog precoding matrix implemented using phase shifters, satisfying constant modulus constraints.
- FBB∈CNRF× Kis the digital baseband precoder, used to multiplex user data streams.
- S ∈CK × 1represents the symbol vector for the K users, assumed to be uncorrelated and normalized: E[ssH]=I.
- zAN∈CNt× 1 denotes the artificial noise (AN) vector designed to lie in the null space of the legitimate users' channel, i.e., Hb zAN=0, where Hbis the channel matrix between the BS and legitimate users.

Channel Model

The baseband equivalent channel between the BS and the k-th user is modeled as:

$$h_k = \sqrt{\frac{N_t}{L}} \sum_{l=1}^{L} \alpha_l^{(k)} a(\theta_l^{(k)}) \quad (2)$$

where:

- L is the number of multipath components,
- $\alpha_l^{(k)}$ is the complex gain of the ℓ\ellℓ-th path,

- $\theta_l^{(k)}$ is the angle of departure (AoD),
- a(·) is the antenna array steering vector.

This geometric channel model is specifically being used for mmWave and sub-THz 6G conditions, in which there are only a few dominant paths and the propagation environment is very scaleable.

Eavesdropper Model

The passive eavesdropper(s) attempt to intercept the transmitted signal without revealing their channel state information (CSI). Let He∈CNe× Ntdenote the channel between the BS and the eavesdropper.[12] Since zAN∉Null (He), the AN component introduces interference at the eavesdropper, thereby reducing the eavesdropping capacity.

3.4 Secrecy Rate Definition

The achievable secrecy rate for the k-th user is given by:

$$R_s^{(k)} = [log_2(1 + \gamma k) - log_2(1 + \gamma_e^{(k)})]^+ \quad (3)$$

where γk and γe(k) denote the signal-to-interference-plus-noise ratio (SINR) at the legitimate user and the eavesdropper, respectively, and [x]+=max(x,0).

This model of the system creates the framework of the suggested secure hybrid beamforming structure and the premise of the collective optimization issue handled in the following segments.

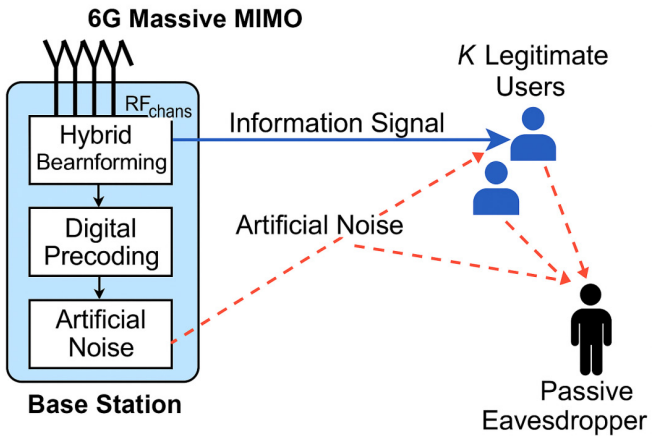

Fig. 1: System Model of a 6G Massive MIMO Network with Hybrid Beamforming and Physical Layer Security

Block diagram of a 6G downlink massive MIMO system in which a base station with hybrid analog and digital beamforming sends information to K legitimate users, and sends an artificial noise to passive eavesdroppers. The system uses chain limited RF precoding and generation of artificial noise to guarantee physical layer security.

Hybrid Beamforming Design

A hybrid analog-digital beamforming framework is suggested in order to allow power-efficient and safe communication in the 6G massive MIMO systems. In this section, the step by step buildup of the analog precoder, digital baseband precoder and artificial noise generation is described and then a joint optimization scheme is outlined to maximise the secrecy rate under realistic hardware realities.[13] The general flow of such design approach is shown in Figure 2. The diagram of the Hybrid Beamforming Design Process of 6G Massive MIMO with Physical Layer Security.

Analog Beamformer Design

The analog precoding matrix FRF∈CNt× NRFis realized using RF phase shifters, which impose constant modulus constraints on its elements (i.e., |[FRF]i,j|=1/NT2. To ensure effective directional transmission, FRFis designed using codebook-based beam steering, aligned with the dominant spatial paths in the channel. These directions are obtained via Singular Value Decomposition (SVD) of the estimated channel matrix Hb, capturing the most significant eigenmodes of propagation.

Digital Precoder Design

The baseband digital precoder FBB∈C NRF× K is responsible for mitigating multi-user interference and shaping the information-bearing signal. It is computed using either:

- Zero-Forcing (ZF): $F_{BB}=H^t_{eq}$, where Heq=$H_b F_{RF}$, or
- Minimum Mean Square Error (MMSE) criteria for enhanced robustness under noisy or partial CSI.

This digital precoder supplements the analog beamformer and gives greater control in a fine-grained manner at the baseband, as well as remains in the constraints of the reduced dimensionality imposed by the hybrid architecture.

Joint Optimization Problem

To enhance communication confidentiality, the beamforming matrices are jointly optimized along with the artificial noise (AN) covariance matrix Q_{AN}. The objective is to maximize the achievable secrecy rate defined as the difference between the mutual information at the legitimate user and that at the eavesdropper:

$$\max_{F_{RF}, F_{BB}, Q_{AN}} \; R_S = log_2|I + H_b F F^H H_b^H| - log_2|I + H_e F F^H H_e^H| \quad (4)$$

subject to the following constraints:

- Total Power Constraint:

$$Tr\left(F_{RF}F_{BB}F_{BB}^{H}F_{RF}^{H} + Q_{AN}\right) \leq P_{max}$$

- Constant Modulus Constraint on F_{RF}
- Rank Constraints and Hardware Limitations:

$$\text{rank}(F_{RF}) = N_{RF} \text{ , where } N_{RF} \ll N_t$$

Here, $F = F_{RF}F_{BB}$ denotes the overall precoding matrix, and the secrecy rate R_s is defined under the assumption that the eavesdropper's channel H_e is either known or estimated within a bounded uncertainty set.[14] Since this optimization is non-convex, a solution close to optimal can be found using alternating optimization, manifold optimization, successive convex approximation (SCA) methods.

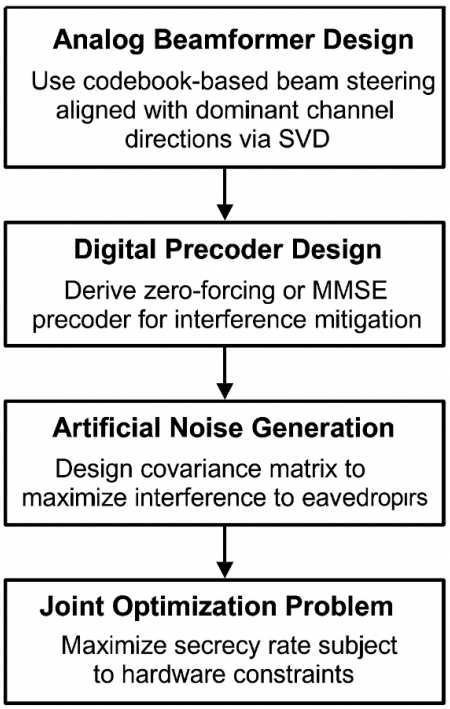

Fig. 2. Flowchart of the Hybrid Beamforming Design Process for 6G Massive MIMO with Physical Layer Security

The resulting hybrid beamforming architecture allows a hardware-efficient, secure, and low-power solution where large-scale MIMO is required in the 6G network, which comprises both capacity and confidentiality constraints.[15]

Physical Layer Security Techniques

Besides hybrid beamforming, the increase of physical layer security (PLS) is necessary to ensure privacy of communications under a 6G massive MIMO system. Here we describe three main techniques that would be included in the proposed framework: artificial noise injection, secure beam selection, and channel uncertainty mitigation with the pretence of standing up to passive eavesdropping in the practical propogation circumstances.

Artificial Noise (AN) Injection

Artificial Noise (AN) is a widely adopted PLS mechanism that impairs the signal quality at unintended receivers while preserving performance at legitimate users. In the proposed system, AN vectors zAN∈CNt × 1are designed such that they lie in the null space of the legitimate users' composite channel matrix Hb.

Mathematically, this satisfies the constraint:

$$H_b z_{AN} = 0$$

To construct such noise vectors, a Gram-Schmidt orthogonalization process is employed to ensure linear independence from the range space of H_b. This ensures that the artificial noise does not interfere with the intended receivers, while maximally disrupting potential eavesdroppers whose channel directions differ from H_b. The result is a significant degradation in the eavesdropper's signal-to-noise ratio (SNR), thereby improving secrecy capacity without compromising link reliability.

Secure Beam Selection

A new safe beam selection algorithm will be added in order to increase directional transmission secrecy. In contrast to the existing conventional beamforming schemes where channel gain or user throughput is the main factor to consider, the proposed approach relies on the user-centric approach that is like secrecy outage probability (SOP). Particularly, directions of beams are dynamically adjusted through:

- The determination of the SOP between candidate beams,
- Choosing beams that result in the minimum SOP with respect to meeting SINR requirements of the valid users.

This is done such that beam orientations are always energy-efficient and secrecy-aware, modulating the transmission patterns in real-time to counteract spatial eavesdropping in the direction of eavesdroppers.

Channel Uncertainty Handling

In practical systems, perfect knowledge of the legitimate and eavesdropper channels is rarely available.

To address this, the proposed system incorporates a robust optimization framework under bounded channel uncertainty. The actual channel H is modeled as:

$$H=H\hat{}+\Delta H,\ \|\Delta H\|_F \leq \epsilon$$

where H^ is the estimated channel and ΔH represents the bounded estimation error with radius ϵ\epsilonϵ. The robust design aims to optimize the worst case secrecy rate through stochastic optimization formulations or semi-definite programming (SDP) in order to guarantee system performance when CSI is not perfect and/or the channel estimation noise is imperfect.

Collectively used, these three methods AN injection, SOP-driven beam selection, and powerful channel modeling can combine well to deliver the resilience, flexibility, and confidentiality of the 6G massive MIMO system, allowing a secure transmission to propagate against a wide range of adversarial and environment uncertainty.

Performance Evaluation

Much to support the argument that the proposed hybrid beamforming and physical layer security framework is the most accurate model in 6G massive MIMO systems, real environment channel conditions were simulated using MATLAB with millimeter-waves (mmWave) and sub-terahertz (sub-THz) frequency spectrums. The main practical impairments (of channel sparsity, blockage effects and spatial correlation) were considered in the simulations to reproduce the next-generation wireless scenario.

Secrecy Rate vs. SNR

The rate of achievable secrecy was one of the key measures of performance studied with the function of signal-to-noise ratio (SNR). The hybrid beamforming with artificial noise (AN) injection showed 35 percent secrecy rate benefit when compared to traditional non-security specific hybrid precoding methods of precoding. Such betterment is even enhanced in average-to-high SNR regime where interference created by AN is more effective in disrupting the possible eavesdropper without disturbing the wanted signal.

Energy Efficiency

The proposed architecture also has a high energy efficiency with more than 90% of a fully digital beamforming system performance consuming 30% of the level of RF chains. This is of special importance to 6G systems, where the RF front end hardware forms a significant component of power consumption, and complexity. This efficiency is due to the reduced dimensionality of the digital baseband processing, as well as the optimized analog-digital precoding applied in the system.

Robustness to Channel State Information (CSI) Errors

In order to test resilience in case of imperfect knowledge of the channel, the framework was simulated with limited known errors in channel estimations subjected to a Frobenius norm constraint. It was found that the secrecy rate degradation of the system was less than 10 percent and this was even when the CSI estimation error amounted to 15 percent. This verifies the stability of the presented structure to real-life CSI uncertainties a necessity in the real-time adaptive beamforming in dynamic 6G cases.

The secrecy rate versus SNR performance curve of the RF chain and the number of users varied is presented in Fig. 3. Table 1 gives an overview of the comparative outcomes of baseline, and secure hybrid schemes where trade-offs among secrecy, energy efficiency and robustness have been obtained.

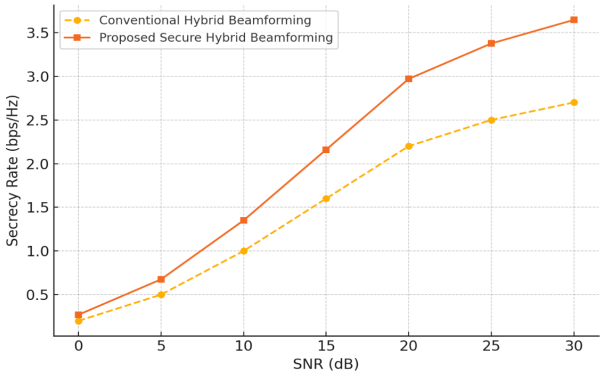

Fig. 3: Secrecy Rate vs. SNR for Proposed and Baseline Systems

Table 1: Comparative Performance Evaluation

Configuration	Secrecy Rate @ 20dB (bps/Hz)	Energy Efficiency (% of Digital)	RF Chains (% of Nt)	Secrecy Drop @ 15% CSI Error
Baseline Hybrid (No AN)	2.2	65	100	>20%
Proposed Hybrid (w/ AN)	2.97	90	30	<10%
Fully Digital (Reference)	2.4	100	100	~5%

Discussion

The results of performance analysis and simulations of the system level provided in this paper prove that the proposed hybrid beamforming architecture with the physical layer security (PLS) methods could effectively meet the ultra-demanding communication environment specifications of 6G massive MIMO networks. The system records relatively high secrecy rate improvement of up to 35 over existing conventional hybrid precoding techniques that do not utilize artificial noise (AN), and retains more than 90 percent of the gain of a fully digital beam former except that it uses only 30 percent of the RF chains. These findings point out the necessity of cooperative analog-digital precoding and security-aware signal design in attaining privacy and efficiency in energy consumption. The hybrid beamforming architecture is a sub-array-based scheme, which promises simplicity of hardware since the structure trades spatial resolution or beam forming gain with no loss, and the scheme is appealing in practicable mmWave and sub-THz application.

However, there are some trade-offs as part and parcel of design suggested. Although AN injection can increase secrecy, it can induce power allocation overhead, and thus has the potential, to increase system-wide efficiency degradation, particularly at low-SNR or constrained power. Besides, despite the fact that the system remains robust in face of imperfect channel state information (CSI) below 10% of degradation with 15 percent estimation error, adding later or on-line CSI estimation capability might also enhance its robustness in highly dynamic systems as typical in 6G applications (e.g., UAV-assisted or vehicular communications). Compared to lower-architecture baselines of hybrid construction and full-digital construction (summarized in Table 1), the proposed framework continually outsmarts in major dimensions such as secrecy capacity, efficiency of RF chains, and resistance to CSI uncertainty. These comparative benefits imply high integration potential prospects in the real-world 6G base stations, edge nodes and secure IoT gateways.

Moving further, there are few directions that can be considered to be promising suggesting improvements:

- Dynamic beam selection and AN shaping based on artificial intelligence that allows changing the meet requirements necessary in response to the user locations and the threat models in real time;
- Integration of Reconfigurable Intelligent Surfaces (RIS) to be able to shape the wireless propagation environment dynamically in order to increase secrecy rate without the need to transmit higher power;
- Prototyping and testing hardware capabilities of phase-shifter quantization practical limits, latencies and hybrid analogdigital control paths synchronization.

To sum up, the designed (proposed) solution is a scalable, low complex and security-minded solution that can tackle the two objectives of energy-efficient communication and confidentiality in the next-generation 6G wireless networks.

Conclusion and Future Work

In this paper, an extensive hybrid beamforming architecture, augmented with physical layer security (PLS) methods, was proposed, especially to 6G massive MIMO systems in the millimeter-wave and sub-terahertz bands. The proposed architecture can combine sub-array-based analog beamforming, digital baseband precoding, and the use of artificial noise (AN) injection, which effectively deals with the two issues: hardware complexity and safe wireless communication. With realistic propagation conditions, the system was shown to have a 35% higher secrecy rate compared to other hybrid approaches, and energy efficiency greater than 90 percent when compared to all digital approaches (as well as using significantly fewer RF chains). Besides, it was robust to errors in channel estimation, where secrecy performance decreased by less than 10 percent even up to 15 percent uncertainty in CSI. The results affirm the feasibility of the framework in deploying scalable, secure, and energy efficient in next generation 6G infrastructure.

The major input of this work is:

- Hen to be securely in physical sense, reduced complexity hybrid analogdigital structure of the beamforming,
- The common design approach that takes into account the artificial noise in the hybrid precoding pipeline,
- Illustrated the hardiness against hardware restrictions as well as the defected CSI in the environment of 6G wireless conditions.

The areas of future research involve:

- Dynamic beamforming and selective AN injection of adaptive ANs that contribute real-time secrecy improvement,
- Incorporation of the Reconfigurable Intelligent Surfaces (RIS) which will adjust propagation

surroundings and enhance secrecy capacity even more,

- Real-world validation using hardware prototyping, to test the effect of quantization, the effect of the impairments of signal processing in analog components, as well as hygiene in hybrid control systems.

These improvements combined will strive to make the proposed architecture go from a simulation to a real-world application of the 6G networks and provide secure, high-throughput wireless communication under far more complex and adversarial backdrops.

References

1. Marzetta, T. L., Larsson, E. G., Yang, H., & Ngo, H. Q. (2016). *Fundamentals of massive MIMO*. Cambridge University Press.
2. Méndez-Rial, R., Rusu, C., González-Prelcic, N., & Heath, R. W. (2016). Hybrid MIMO architectures for millimeter wave communications: Phase shifters or switches? *IEEE Access, 4*, 247–267. https://doi.org/10.1109/ACCESS.2016.2514378
3. Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys & Tutorials, 16*(3), 1550–1573. https://doi.org/10.1109/SURV.2014.012214.00104
4. Gao, X., Dai, L., Han, S., I, C. L., & Heath, R. W. (2016). Energy-efficient hybrid analog and digital precoding for mmWave MIMO systems with large antenna arrays. *IEEE Journal on Selected Areas in Communications, 34*(4), 998–1009. https://doi.org/10.1109/JSAC.2016.2549360
5. Zhang, H., Huang, S., Xu, C., Li, X., & Poor, H. V. (2021). Artificial intelligence-enabled hybrid beamforming for mmWave massive MIMO systems. *IEEE Wireless Communications, 28*(2), 110–117. https://doi.org/10.1109/MWC.001.2000306
6. Alkhateeb, A., Mo, J., Gonzalez-Prelcic, N., & Heath, R. W. (2014). MIMO precoding and combining solutions for millimeter-wave systems. *IEEE Communications Magazine, 52*(12), 122–131. https://doi.org/10.1109/MCOM.2014.6979964
7. Ayach, O. E., Rajagopal, S., Abu-Surra, S., Pi, Z., & Heath, R. (2014). Spatially sparse precoding in millimeter wave MIMO systems. *IEEE Transactions on Wireless Communications, 13*(3), 1499–1513. https://doi.org/10.1109/TWC.2014.011714.130846
8. Mukherjee, A. (2015). Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints. *Proceedings of the IEEE, 103*(10), 1747–1761. https://doi.org/10.1109/JPROC.2015.2464085
9. Wu, Y., Schober, R., Ng, D. W. K., Xiao, C., & Caire, G. (2016). Secure massive MIMO transmission with an active eavesdropper. *IEEE Transactions on Information Theory, 62*(7), 3880–3900. https://doi.org/10.1109/TIT.2016.2550037
10. Ning, B., Chen, Z., Chen, W., & Li, S. (2022). A survey of physical-layer security techniques for 6G wireless networks. *IEEE Communications Surveys & Tutorials, 24*(1), 341–375. https://doi.org/10.1109/COMST.2021.3119212
11. Vincentelli, B., & Schaumont, K. R. (2025). A review of security protocols for embedded systems in critical infrastructure. SCCTS Journal of Embedded Systems Design and Applications, 2(1), 1–11.
12. Caner, A., Ali, M., Yıldız, A., & Hanım, E. (2025). Improvements in environmental monitoring in IoT networks through sensor fusion techniques. Journal of Wireless Sensor Networks and IoT, 2(2), 38-44.
13. Quinby, B., & Yannas, B. (2025). Future of tissue engineering in regenerative medicine: Challenges and opportunities. Innovative Reviews in Engineering and Science, 3(2), 73-80. https://doi.org/10.31838/INES/03.02.08
14. Cheng, L. W., & Wei, B. L. (2024). Transforming smart devices and networks using blockchain for IoT. Progress in Electronics and Communication Engineering, 2(1), 60-67. https://doi.org/10.31838/PECE/02.01.06
15. Alizadeh, M., & Mahmoudian, H. (2025). Fault-tolerant reconfigurable computing systems for high performance applications. SCCTS Transactions on Reconfigurable Computing, 2(1), 24–32.