International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 25s,2025
https://theaspd.com/index.php

Survey On Adaptive AI Techniques For Qos And Privacy Preservation In Multi-User 6G Networks

G M Anand Reddy[1], Dr. Chandramouli H [2]
[1] Research Scholar, Department of Computer Science and Engineering, East Point College of Engineering and Technology, Bangalore, Karnataka, India. Email: anandsaireddy.gm@gmail.com
[2] Professor, Department of Computer Science and Engineering, East Point College of Engineering and Technology, Bangalore, Karnataka, India. Email: hcmcool123@gmail.com

Abstract: *The emergence of sixth-generation (6G) wireless networks promises unprecedented advancements in communication technologies, offering ultra-low latency, high throughput, and massive connectivity—especially for the Internet of Things (IoT) ecosystem. However, delivering consistent Quality of Service (QoS) in ultra-dense, heterogeneous, and security-sensitive 6G environments presents significant challenges. Orthogonal Frequency Division Multiple Access (OFDMA), though foundational, faces limitations in dynamic spectrum allocation, latency control, and interference mitigation under such complex scenarios. This survey explores the role of Artificial Intelligence (AI), particularly Deep Reinforcement Learning (DRL), in addressing these challenges by enabling adaptive optimization of transmission parameters, intelligent beam forming, and real-time traffic scheduling. Furthermore, the survey investigates AI-enhanced security and privacy-preserving mechanisms, which are crucial to mitigate threats from untrusted devices while maintaining QoS integrity. We examine recent advancements in integrated resource management, beam forming control, anomaly detection, and secure spectrum allocation across multi-user 6G IoT frameworks. By systematically analyzing existing methods, their advantages, and their limitations, this work highlights critical research gaps—including the lack of unified, real-time adaptive frameworks for joint QoS and security optimization. The survey concludes by outlining future directions aimed at developing scalable, intelligent, and robust AI-driven architectures to meet the demanding requirements of next-generation IoT-driven 6G communications.*
Keywords: *Quality of Serivce (QoS), Artificial Intelligence (AI), Deep Reinforcement Learning (DRL), 6G Networks.*

1. INTRODUCTION

The evolution towards 6G networks will bring new challenges and opportunities in Quality of Service (QoS) management. With anticipated capabilities such as ultra-low latency, high throughput, and massive connectivity (IoTs), QoS mechanisms need to adapt to meet the rigorous requirements of potential future applications, while end-to-end QoS includes services that demand very high performance requirements. However, the future system must be deployed in a cost-effective manner and must not require over-deployment of network resources [1].

The exponential growth in wireless communication and the rapid proliferation of Internet of Things (IoT) devices have spurred the evolution toward sixth-generation (6G) networks. Unlike its predecessors, 6G aims to deliver ultra-reliable, low-latency, and high-throughput communication services that can seamlessly support emerging applications such as autonomous vehicles, real-time augmented reality, telemedicine, and intelligent industrial automation. In this hyper-connected landscape, the efficient and intelligent management of **Quality of Service (QoS)** becomes a cornerstone of 6G design. Traditional approaches to QoS, which rely on static resource provisioning and predefined policies, are insufficient to address the dynamic, heterogeneous, and security-sensitive environments of 6G [2].

OFDMA (Orthogonal Frequency Division Multiple Access) has long been the foundation of multi-user communication in cellular networks. However, in ultra-dense IoT deployments expected in 6G, OFDMA systems face several challenges such as latency degradation, suboptimal throughput, and inefficient interference management. As a result, there is a critical need for **adaptive and intelligent optimization frameworks** that can dynamically allocate resources, maintain service-level agreements, and enhance overall network performance [3].

Recent advances in **Artificial Intelligence (AI)**, particularly **Deep Reinforcement Learning (DRL)**, offer promising solutions to this challenge. DRL algorithms like **Deep Deterministic Policy Gradient (DDPG)** have demonstrated the ability to learn optimal strategies through interaction with the environment, making them well-suited for dynamic resource allocation, intelligent beamforming, and real-time traffic scheduling. These learning-based techniques enable 6G networks to autonomously adapt to varying channel conditions, user mobility, and interference levels—significantly enhancing QoS outcomes [4].

Beyond throughput and latency, **security and privacy** have emerged as critical dimensions of QoS in 6G networks. The presence of both trusted and untrusted devices in shared environments poses new threats, such as eavesdropping and signal interference. Traditional encryption methods, while necessary, are insufficient on their own. Hence, AI-enabled security frameworks are required to detect anomalies, mitigate threats, and preserve user confidentiality while ensuring uninterrupted service delivery [5].

Another key challenge lies in the **optimization of spectrum and power resources**. Static allocation schemes lead to inefficiencies and fail to scale with the increasing density of connected devices. A self-learning, AI-driven spectrum allocation strategy can maximize spectral efficiency and fairness, dynamically adjusting to real-time network demands. Furthermore, such strategies can also enhance **energy efficiency**, a vital requirement for sustainable 6G operation [6].

Given these multifaceted challenges, this research proposes a **comprehensive AI-driven optimization framework** that integrates DRL for QoS enhancement, adaptive security mechanisms, and intelligent spectrum management. By leveraging DDPG-based learning and actor-critic neural architectures, the proposed system aims to provide a holistic solution that dynamically balances throughput, latency, interference, and security in OFDMA-based 6G IoT networks [7].

This work not only contributes to the academic understanding of AI applications in wireless communications but also addresses real-world deployment challenges by focusing on adaptability, scalability, and cross-layer integration. The goal is to enable robust, efficient, and secure communication in the complex, high-density environments of future 6G networks

- **Network Slicing**

Network slicing will be an integral part of 6G QoS management, allowing the creation of multiple virtual networks on a single existing physical infrastructure. Each part of the unbundled network can be optimized for different types of traffic and services, enabling tailored or on-demand QoS for applications with diverse requirements. This attempt to decompose the physical network into several virtual parts seeks to specify one part to a specific job or a specific type of service. This segmentation ensures that key services are given the necessary resources and priority, while less key services do not consume too much bandwidth or disrupt more important traffic [8].

- Isolation: Each network entity operates independently, ensuring that problems in one part of the network do not affect the others. It is essential to maintain the reliability and performance of critical applications.
- Scalability: Network slices can adapt in time to match demand allowing resources to be used effectively and accommodating changing traffic patterns.
- Comprehensive Management: Slicing covers everything from the network to the periphery guaranteeing quality of service from the server room all the way to the end user.

Resource Management: Bandwidth, processing power, and storage can be assigned to each slice based on its requirements enhancing network efficiency

- **Optimizes Latency**

6G networks will combine edge computing, network slicing, enhanced radio access technologies, URLLC, AI and machine learning, rapid link throughput, and distributed architecture in an effort to fulfill the real-time performance demands of new applications [9]. By combining these approaches, latency is optimized and 6G networks are made sufficiently stable and dependable to handle the upcoming wave of cutting-edge, time-sensitive applications. 6G networks are expected to achieve latency times on the order of a few milliseconds to meet the real-time performance requirements of applications such as telemedicine and interaction, and these future networks should ensure QoS and reliability. 6G networks will combine edge computing, network slicing, enhanced radio access technologies, URLLC, AI and machine learning, rapid link throughput, and distributed architecture in an effort to fulfill the real-time performance demands of new applications. By combining these approaches, latency is optimized and 6G networks are made sufficiently stable and dependable to handle the upcoming wave of cutting-edge, time-sensitive applications. 6G networks are expected to achieve latency times on the order of a few milliseconds to meet the real-time performance requirements of applications such as telemedicine and interaction. And these future networks should ensure QoS and reliability.

- **Reliability Guarantees**

Some services will require extreme reliability, such as industrial automation and autonomous vehicles. They will need appropriate robust service quality mechanisms to ensure total reliability. Approaches will include error rehearsal and correction methods to ensure consistent performance.

- **AI and Machine Learning (Cognitive Radio)**

In 6G, AI and machine learning will play a key role in dynamic QoS management. These technologies will enable QoS parameters to be analyzed predictively, optimized in real time, and adjusted automatically according to network conditions and traffic patterns [5].

- **High Bandwidth Applications**

Emerging applications such as augmented reality (AR) and virtual reality (VR) will require high bandwidth and light interference. QoS mechanisms will need to formally support these services and manage bandwidth allocation (Cognitive Radio) to ensure optimal performance.

- **Quality of Service and Security**

Maintaining quality of service while ensuring network security will be a key challenge. Security measures must be integrated into QoS protocols to avoid degradation of QoS due to malicious activity. Achieving quality of service for 6G is not a task that can be handled by any single player in the telecom industry alone. It will require effective coordination between telecoms operators, device manufacturers, and application designers. An interdisciplinary partnership such as this one is necessary to articulate the standards of QoS that would work effectively for all the involved parties.

End-to-end QoS includes services that demand very high levels of performance and that need to be delivered across specific deployment zones: geographically wide, local, delimited, and, in the case of nomadic services, dynamic. Of course, all this must be achieved in a cost-effective way that does not require over-deployment of network resources [10]. Radio Access Network (RAN) and Core Network (CN) architectures will be based on a high level of modularity and virtualization of network functions. Transport will therefore have to support this process by automatically ensuring the appropriate connectivity between each network function.

In data transport, there is a need for high availability [11]. This implies that the network should be able to function even in cases of failure, regardless of whether it is hardware or software. This involves redundancy systems, failover mechanisms, and resilience design principles—ensuring continuous accessibility of services. On the other hand, resilience deals with quick recovery from unexpected attacks: designing systems to gracefully handle failures, adapt to changing conditions while still keeping up performance standards under different scenarios that might occur [12]. Self-healing networks can reconfigure themselves to maintain QOS and reduce downtime as much as possible; unexpected attacks need to be considered. This has to be considered about programmability. On the basis of real-time emerging requirements, it allows network operators to change network resources and behavior dynamically [13]. It is an integration of network function virtualization (NFV) with software-defined networking (SDN), which will make this possible [14]. The other crucial aspect is flexibility. The objective is to adapt swiftly to new technologies, applications, and user needs with minimal reconfiguration. Alternatively, it will provide fast changes and improvements in response to changing demands, ensuring that the network has a wide range of dynamic use cases it can serve effectively.

In a low latency network like 6G [15] it is also a challenge to maintain proper Quality of Service in message delivery. The 6G network is an amalgamation of the multiple network system having diversified protocols and standard interoperability between different protocols is also a big challenge.

1.1. Motivation and Contribution

The motivation behind this research stems from the pressing need to address the multifaceted challenges of Quality of Service (QoS) in the rapidly evolving 6G IoT ecosystem. Traditional OFDMA-based communication systems are increasingly inadequate in managing the dynamic and ultra-dense nature of modern networks, where diverse IoT devices demand low latency, high reliability, secure data exchange, and efficient spectrum utilization. As applications like autonomous vehicles, telemedicine, and real-time augmented reality proliferate, the stakes for seamless and intelligent QoS management continue to rise. Current static optimization strategies fail to scale or adapt to real-time traffic fluctuations, interference, and energy constraints. Simultaneously, the presence of untrusted devices introduces complex security and privacy concerns that cannot be solved through conventional encryption alone. These challenges highlight the urgent need for an intelligent, self-learning framework that can simultaneously optimize throughput, latency, security, and resource allocation. Leveraging deep reinforcement learning (DRL), particularly the Deep Deterministic Policy Gradient (DDPG) approach, this research aspires to fill these critical gaps and contribute to the development of robust, adaptive, and scalable QoS architectures for the future of 6G communications.

- **AI-Driven QoS Optimization Framework:**

This research introduces a novel Deep Reinforcement Learning (DRL)-based framework using the Deep Deterministic Policy Gradient (DDPG) algorithm to dynamically optimize Quality of Service (QoS) parameters such as throughput, latency, and interference in OFDMA-based 6G IoT networks. The framework adapts in real-time to varying network conditions, enabling intelligent beamforming, power control, and traffic scheduling across ultra-dense device environments.

- **Integrated Security and Privacy Mechanisms:**

A robust security model is embedded within the proposed framework to address threats from untrusted or semi-trusted devices. By incorporating AI-driven anomaly detection and adaptive eavesdropping prevention strategies, the system ensures secure and privacy-preserving communication without compromising QoS performance.

- **Efficient Spectrum and Resource Allocation Strategy:**

The research proposes a self-learning, energy-aware spectrum and resource allocation mechanism that ensures fair and efficient utilization of bandwidth and power in large-scale 6G IoT deployments. This includes the formulation of a joint optimization strategy that balances spectral efficiency, user fairness, and energy consumption under diverse and dynamic network loads.

2. RELATED WORK

As the 6G landscape evolves to support ultra-dense IoT deployments, Quality of Service (QoS) provisioning has become increasingly complex. Traditional OFDMA-based networks struggle to handle the dynamic nature of 6G traffic demands, particularly under ultra-low latency and high reliability requirements. Recent studies emphasize the role of Deep Reinforcement Learning (DRL), especially Deep Deterministic Policy Gradient (DDPG), as a scalable solution to dynamically manage transmission parameters such as power levels, beamforming weights, and user scheduling strategies. Shen et al. introduced a simulation platform incorporating such mechanisms to model high-density 6G scenarios efficiently. However, real-time adaptation to channel variations and interference remains a challenging gap [16].

Adaptive beamforming and power control have been identified as critical enablers for improving signal quality and mitigating interference in multi-user scenarios. Sharma et al. proposed a multi-agent DRL-based solution for terahertz-enabled femtocells that optimized beamforming vectors and power settings to enhance the secrecy rate and throughput. Additionally, Cao et al. demonstrated that joint design of active and passive beamforming could significantly reduce latency and improve SINR in mmWave systems. These findings support the need for AI-based algorithms that can continuously adapt transmission strategies to optimize end-to-end QoS [17].

Security and privacy are vital considerations in 6G IoT environments, especially due to the rise in untrusted or semi-trusted users. Traditional encryption approaches fall short in multi-user and dynamic spectrum-sharing contexts. AI-based anomaly detection, combined with secrecy rate optimization, is gaining traction as an effective strategy. For example, Khan et al. proposed an AI-enhanced multi-attribute utility function to enable secure decision-making in ultra-dense heterogeneous 6G networks. These models utilize real-time network states to detect threats and dynamically secure communications while maintaining QoS [18].

Modern works are exploring the use of DRL to model privacy-preserving resource allocationstrategies. The ability of DRL agents to learn from adversarial behaviors in multi-agent settings allows for efficient threat detection and mitigation. In particular, the proposed DDPG framework by Anilkumar et al. integrates active monitoring of trusted and untrusted devices, adapting beamforming and spectrum usage to limit the signal leakage to potential eavesdroppers [19].

QoS and security are often at odds: stronger encryption or redundant communication methods can introduce latency and reduce throughput. Mao et al. explored AI-based joint optimization of QoS and security for 6G energy harvesting IoT systems, demonstrating the viability of using learning models to strike a dynamic balance between performance and protection. Such joint objectives are critical for scalable and resilient 6G networks [20].

Resource allocation lies at the heart of 6G performance optimization. Bhajantri and colleagues reviewed resource allocation across fog, edge, and cloud layers, highlighting the importance of latency-aware distributed computing strategies. Meanwhile, Nguyen et al. introduced federated DRL for spectrum and computing resource allocation across edge nodes, ensuring scalability in real-world vehicular networks [21].

Efficient spectrum allocation is a persistent challenge in ultra-dense deployments. Zhao et al. introduced an interference-inference-based scheduling model that leveraged historical network data for real-time resource management. The use of Double DQN and novel energy-aware metrics enabled fair spectrum distribution while maximizing user satisfaction and minimizing interference [22].

Conventional static allocation schemes are inadequate for dynamic and decentralized environments like 6G. Reinforcement learning has shown promise in joint spectrum-power optimization, especially in scenarios with imperfect CSI or untrusted users. The iterative learning strategy employed in DDPG frameworks enables real-time correction and policy refinement, addressing both spectrum scarcity and fairness [23].

Real-time adaptability is crucial for the sustainability of QoS strategies. Many traditional models fail to scale with user density or adjust to channel degradation. Simulation platforms introduced by Guo et al. and Shen et al. allowed controlled testing of adaptive AI-based models, though they point to the lack of large-scale real-world validations of these techniques in operational networks [24].

Energy efficiency is directly linked to QoS, particularly in battery-powered IoT devices. Game-theoretic approaches and AI-enhanced models have been proposed to reduce power consumption without compromising user performance. Huang et al. presented a game-theoretic optimization model for UAV communication that balanced energy use and QoS delivery in real-time [25].

An often-overlooked area in QoS research is dynamic traffic scheduling. Load balancing strategies powered by machine learning can predict congestion and reallocate traffic flows intelligently. These strategies are especially useful in OFDMA systems where subcarrier assignments must be tightly controlled to avoid channel contention and minimize delay [26].

Mobility and congestion introduce unpredictability in channel conditions. Existing OFDMA networks do not adequately adapt to such variations. Cao et al. and Ma et al. advocate for the use of self-learning channel estimation models that can respond to changes in mobility patterns and interference profiles on the fly, ensuring stable QoS delivery [27].

To fully optimize QoS in 6G, cross-layer and interdisciplinary strategies must be considered. Recent works integrate AI with blockchain for secure identity management, combine DRL with fog computing for adaptive load handling, and propose hybrid OFDMA-NOMA models for enhanced multiplexing capabilities. These hybrid approaches show promise in maintaining QoS across diverse application domains [28].

Evaluation of AI-based QoS frameworks often involves performance indicators like throughput, latency, energy efficiency, and secrecy rate. However, Zhao et al. proposed a novel metric called effective energy efficiency, which combines service quality and power consumption into a unified performance score. Incorporating such metrics is crucial for a holistic understanding of AI-driven frameworks in real-world deployments [29].

While numerous efforts have advanced the theoretical underpinnings of QoS in 6G networks, several gaps persist: limited real-world deployment of AI-based OFDMA optimizations, lack of multi-objective frameworks that address both security and QoS, and insufficient support for adaptive, real-time scheduling. Addressing these challenges forms the foundation of your proposed objectives and highlights the relevance of your research [30]. A Survey on AI Techniques for QoS and Privacy Preservation in Multi-User 6G Networks is as shown in Table 1.

Table 1: A comprehensive Survey on AI Techniques for QoS and Privacy Preservation in Multi-User 6G Networks

Ref	Method	Advantages	Disadvantages	Research Gap
[8]	Spectrum and interference management in heterogeneous 6G networks	Comprehensive analysis of resource strategies; supports multi-user environments	Lacks real-time AI integration for adaptive resource allocation	No dynamic, AI-based optimization approach for changing traffic conditions
[9]	Resource management in fog/edge/cloud for IoT	Enables distributed computing for improved QoS	Static resource estimation; lacks adaptive scheduling	No self-learning model to support dynamic edge resource management
[10]	Wireless resource simulation for dense IoT	Models high-density IoT scenarios effectively	Simulation-based only; not validated in real-world settings	Absence of DRL-based optimization in practical 6G testbeds
[11]	Four-tier edge architecture for massive IoT	Reduces latency and boosts coverage	Doesn't integrate AI for real-time adaptation	No intelligent QoS control in hierarchical edge systems
[13]	Federated DRL for vehicular IoT	Optimizes spectrum and compute distribution efficiently	Requires high computation; limited to vehicular context	Lacks scalability validation in ultra-dense heterogeneous IoT settings
[15]	IRS-assisted OFDMA channel estimation	Enhances spectral and energy efficiency	Complex implementation in mobile scenarios	Doesn't consider QoS-security trade-offs
[20]	Game-theoretic spectrum sharing for UAVs	Balances spectrum use and energy efficiency	Focused only on UAV communication	No support for real-time AI-based multi-user spectrum adaptation
[21]	DRL for secrecy rate optimization in femtocells	Improves secure communication in dynamic settings	High model complexity; resource-intensive	Not generalized for broader OFDMA 6G IoT environments
[23]	AI-enhanced context-aware decision model	Boosts secure network selection using multi-attribute utility	Limited in handling real-time adversarial threats	No reinforcement learning for adaptive anomaly mitigation
[24]	Interference-inference-based scheduling with Double DQN	Achieves energy-efficient and fair resource allocation	Relies on past data; delayed response to new threats	Doesn't support joint optimization of QoS and privacy in real time

Research Gaps

- **Lack of Real-Time Adaptive QoS Optimization in OFDMA-Based 6G Networks:**

Most existing QoS enhancement techniques in OFDMA systems rely on static or heuristic-based optimization, which are not capable of adapting to rapidly changing network conditions such as dynamic user mobility, interference, and traffic fluctuations.

- **Insufficient Integration of AI in End-to-End QoS Management:**

While AI and machine learning have shown promise in isolated use cases (e.g., scheduling or routing), there is a gap in unified AI-driven frameworks that simultaneously manage multiple QoS parameters—latency, throughput, and interference—in an end-to-end fashion.

- **Inadequate Security and Privacy Measures in Multi-User OFDMA Networks:**

Existing security mechanisms primarily focus on encryption and authentication, neglecting dynamic threats like eavesdropping from untrusted nodes. There is limited research on AI-based, real-time security models that preserve privacy while maintaining high QoS.

- **Lack of Joint Optimization for QoS and Security Trade-Offs:**

Few studies consider the trade-offs between strong security and QoS performance. Strong encryption or redundant secure paths may degrade latency and throughput. A multi-objective, AI-driven optimization model that balances both aspects is missing in the literature.

- **Limited Research on AI-Based Beamforming and Power Control in Ultra-Dense Environments:**

Current beamforming and power allocation strategies in OFDMA systems are largely predefined or rule-based, and do not exploit reinforcement learning for adaptive signal optimization in ultra-dense, high-interference 6G scenarios.

- **Scalability Challenges in High-Density IoT Deployments:**

Existing QoS management solutions often fail to scale efficiently with the exponential growth of IoT devices in 6G environments. There is a gap in scalable AI-based frameworks capable of ensuring fair and efficient resource distribution among thousands of heterogeneous nodes.

- **Minimal Real-World Validation of AI-Driven Resource Allocation Strategies:**

Many proposed models remain in the simulation or conceptual phase with limited deployment in testbeds or real-world 6G scenarios. There is a lack of empirical evidence validating the practicality, robustness, and efficiency of AI-driven QoS frameworks in operational settings.

3. CONCLUSION

The evolution of 6G networks is poised to revolutionize the communication landscape, particularly in enabling ultra-dense IoT environments with stringent requirements for latency, reliability, and security. This survey has comprehensively reviewed the recent advancements in AI-driven QoS optimization techniques for multi-user OFDMA-based 6G IoT networks. It emphasizes the critical role of Deep Reinforcement Learning (DRL), especially the Deep Deterministic Policy Gradient (DDPG) approach, in facilitating intelligent, adaptive control over beamforming, power allocation, traffic scheduling, and resource distribution. In addition, the integration of AI into security and privacy-preserving mechanisms has shown strong potential for defending against emerging threats from untrusted users and dynamic environments, ensuring trustworthy and efficient communication. Despite notable progress, several key challenges remain unaddressed. Current solutions lack scalability, real-time adaptability, and unified frameworks that jointly optimize QoS and security. The survey identifies these research gaps and underscores the need for holistic, AI-powered models capable of simultaneously managing performance, energy efficiency, and data privacy. Future research should focus on real-world validations, cross-layer optimization, and lightweight learning models suitable for edge and IoT devices. Ultimately, the insights from this survey lay the foundation for developing robust an.

REFERENCES:

- Z. M. Fadlullah, B. Mao, and N. Kato, "Balancing QoS and Security in the Edge: Existing Practices, Challenges, and 6G Opportunities with Machine Learning," IEEE Communications Surveys & Tutorials, 2022.
- B. Mao, Y. Kawamoto, and N. Kato, "AI-Based Joint Optimization of QoS and Security for 6G Energy Harvesting IoT," IEEE IoT Journal, vol. 7, no. 8, 2020.
- M. R. Mahmood et al., "A Review on AI/ML for Empowering IoT Toward 6G Era," IEEE Access, vol. 10, 2022.
- H. T. Nguyen et al., "DRL-Based Intelligent Resource Allocation for QoS in 5G/6G Vehicular Networks," Wireless Communications and Mobile Computing, 2021.
- F. Guo et al., "Enabling Massive IoT Toward 6G: A Survey," IEEE IoT Journal, vol. 8, 2021.
- H. Sharma et al., "Secrecy Rate Maximization in THz-Aided Heterogeneous Networks: A DRL Approach," IEEE Transactions on Vehicular Technology, 2023.
- Y. Zhao et al., "Intelligent Scheme for Energy-Efficient Uplink Resource Allocation in 6G," IEEE TNSM, 2024.
- S. Zhang et al., "Deep Learning-Based RIS Channel Extrapolation," arXiv preprint, 2021.
- X. Ma et al., "Joint Channel Estimation and Data Rate Maximization in IRS-Assisted THz MIMO," IEEE Access, vol. 8, 2020.
- B. Zheng et al., "IRS-Assisted Multi-User OFDMA: Channel Estimation and Design," IEEE Transactions on Wireless Communications, 2020.
- X. Shen et al., "Wireless Resource Management for 6G-Enabled IoT," IEEE Wireless Communications, vol. 29, no. 1, 2022.

- Y. Cao et al., "Joint Power Control and Beamforming in IRS-Assisted Uplink mmWave," IEEE Transactions on Cognitive Communications and Networking, vol. 7, 2021.
- L. B. Bhajantri and G. S., "Resource Management in IoT: A Survey," J. Telecommun. Inf. Technol., 2021.
- T. Huang et al., "Spectrum Sharing for 6G Air-Ground Integrated Networks," IEEE TNSM, 2025.
- W. U. Khan et al., "NOMA-Enabled Optimization in Small-Cell IoV," IEEE Transactions on Intelligent Transportation Systems, vol. 23, 2022.
- S. Manap et al., "Survey on Radio Resource Management in 5G HetNets," IEEE Access, vol. 8, 2020.
- D. G. S. Pivoto et al., "Relevance Analysis of Enabling Technologies for 6G Architectures," IEEE Access, vol. 11, 2023.
- M. Z. Chowdhury et al., "6G Wireless Systems: Applications, Requirements, Technologies," IEEE Open J. of Communications Society, 2020.
- J. G. Andrews et al., "What Will 6G Be?" IEEE Journal on Selected Areas in Communications, vol. 38, no. 8, 2020.
- M. Agiwal et al., "Next Generation 6G Wireless Networks: A Comprehensive Survey," Elsevier Computer Networks, 2021.
- M. S. Khan et al., "AI-Enhanced Secure Decision-Making in 6G: Multi-Attribute Utility Function," IEEE Transactions on Consumer Electronics, 2024.
- K. S. Munagala et al., "Secure and Reliable Communication in 6G Networks," IEEE Access, 2022.
- Y. Pimpalkar et al., "A Novel E2E Path Selection Algorithm for QoS and QoE in 6G," IEEE TNSM, 2024.
- X. Ma et al., "Channel Estimation for IRS-Enabled Terahertz Systems," IEEE ICC Workshops, 2020.
- R. Abbas et al., "Machine Learning for 6G Wireless Networks: Challenges and Opportunities," IEEE Vehicular Technology Magazine, 2021.
- S. Zhang et al., "Security and Privacy for 6G: A Machine Learning Perspective," IEEE Wireless Communications, vol. 29, 2022.
- J. Tang et al., "AI for Dynamic Spectrum Management in Next-Gen Networks," IEEE Network, 2021.
- N. Zhao et al., "Beamforming Techniques in IRS-Aided Networks: A Survey," IEEE Communications Surveys & Tutorials, 2023.
- M. Vegni and V. Loscri, "A Survey on Security in 6G Communications," Ad Hoc Networks, 2022.
- M. Elsayed et al., "AI for 6G: A Framework and Open Research Directions," IEEE Network, vol. 36, no. 4, 2022.