AI-Driven Adaptive Control and Optimization in Next-Generation Telecommunication Networks: Architectures, Algorithms, and Autonomous Fault Management for 5G/6G and Beyond

Abstract

This comprehensive survey delineates the transformative integration of artificial intelligence (AI) within adaptive control, telecommunications, and dynamic networking systems, emphasizing its pivotal role in advancing next-generation communication infrastructures such as 5G, 6G, and beyond. Motivated by escalating data volumes, heterogeneous device ecosystems, and stringent service demands, the work explores a broad spectrum of AI methodologies—including reinforcement learning, deep learning, federated learning, and gradient-based optimization—applied to critical domains like network traffic classification, software-defined networking (SDN), routing optimization, Open Radio Access Network (Open RAN), and autonomous fault management.

Key contributions include an in-depth examination of AI-driven adaptive traffic classification techniques that overcome traditional limitations posed by encryption and dynamic traffic patterns, highlighting trade-offs between accuracy, computational complexity, and real-time feasibility. The survey further analyzes AI-empowered SDN architectures that enhance resource allocation and anomaly detection, discussing scalability and security challenges alongside prospects for decentralized, privacy-preserving learning in 6G deployments. AI-based routing optimization is reviewed with a focus on reinforcement learning algorithms augmented by traffic prediction and anomaly detection, evidencing significant throughput and latency enhancements. Open RAN integration elucidates multilayer AI deployment for radio and network layer optimization, underscoring federated learning and hybrid communication modalities for improved performance and resilience. The incorporation of Large Language Model (LLM)-based agentic AI for autonomous fault management within O-RAN frameworks is also detailed, demonstrating substantial gains in fault detection accuracy, mitigation efficiency, and network uptime. Complementing these, the survey addresses AI-enhanced wireless networking elements such as reconfigurable intelligent surfaces (RIS) and perceptive mobile networks (PMNs), which benefit from advanced AI techniques for interference management and sensing.

The work critically appraises challenges enveloping computational overhead, latency constraints, data heterogeneity, privacy, interpretability, interoperability, and robustness against adversarial threats. It advocates scalable, distributed AI architectures combining edge-cloud synergy, federated and multi-agent learning paradigms, and explainable AI techniques to foster transparency, trust, and regulatory compliance. Gradient-based optimization methods and fast algorithmic updates are presented as foundational tools to enable real-time system adaptability in complex, stochastic network environments.

Concluding, the survey synthesizes cross-cutting themes and prospective research avenues—including hardware acceleration, quantum computing, blockchain-enhanced security, and multi-agent collaborative learning—that collectively underpin the evolution of autonomous, resilient, and intelligent telecommunication networks. By providing a holistic and rigorous exploration of AI-enabled adaptive control and networking, this work lays a robust foundation for future scholarly and practical advancements striving towards secure, scalable, and transparent AI integration in dynamic communication ecosystems.

ACM Reference Format:
. 2025. AI-Driven Adaptive Control and Optimization in Next-Generation Telecommunication Networks: Architectures, Algorithms, and Autonomous Fault Management for 5G/6G and Beyond. In . ACM, New York, NY, USA, 27 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

Artificial Intelligence (AI) has undergone significant advancements over recent decades, impacting various domains such as healthcare, finance, and autonomous systems [?]. Despite these achievements, ongoing challenges include scalability, interpretability, and integration with human decision-making processes [?]. Various methodologies have been proposed to address these issues, each with unique strengths and limitations.

For example, deep learning approaches have demonstrated exceptional performance in tasks involving large-scale data but often suffer from a lack of transparency and require substantial computational resources [?]. Alternatively, symbolic AI techniques offer better interpretability but struggle with scalability and adaptability to complex, real-world scenarios [?]. Hybrid models attempt to combine these advantages, yet integrating disparate paradigms remains nontrivial [?]. This survey critically analyzes these methods, comparing their relative merits and highlighting open research questions to guide future developments.

By synthesizing findings across multiple studies, this paper aims to provide a comprehensive overview that aids researchers in selecting appropriate AI techniques tailored to specific application needs.

1.1 Overview of AI-Driven Approaches in Adaptive Control, Telecommunications, and Networking Systems

The integration of artificial intelligence (AI) into adaptive control, telecommunications, and dynamic networking systems has

Conference'17, Washington, DC, USA
© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

catalyzed unprecedented advancements, fundamentally reshaping traditional paradigms by introducing data-driven adaptability and autonomous decision-making. Foundational studies have demonstrated AI's potential in optimizing networks via reinforcement learning, enabling autonomous control mechanisms within communication systems, and developing adaptive AI models designed for dynamic protocol adjustment [27, 28, 33**?**]. These approaches leverage the inherent dynamics of networks by utilizing system state information alongside historical interactions, thereby empowering networks to self-optimize under diverse and time-varying conditions [36**? ?**]. For instance, semantic communication frameworks that combine deep learning with knowledge graphs enable context-aware, efficient transmission by extracting and reconstructing semantic information, substantially enhancing communication reliability and semantic fidelity [36]. Additionally, deep learning techniques have been effectively applied to autonomously manage network parameters, detect anomalies, and predict system behaviors within telecom Self-Optimized Networks (SON), improving fault management and resource allocation [**?**].

Furthermore, AI techniques have addressed the complexities presented by distributed and heterogeneous network infrastructures, effectively tackling challenges such as resource contention, delay variability, and fault tolerance [2**? ?**]. Federated learning frameworks incorporating gradient sparsification, adaptive client selection, and joint bandwidth allocation optimize collaborative model training across wireless devices, balancing communication efficiency and learning accuracy under resource constraints [2**?**]. Reinforcement and federated learning methods enhance network slicing in next-generation wireless networks, enabling dynamic resource allocation and slice admission control to support diverse service requirements with improved throughput and latency [**?**]. Moreover, advancements in mobility management schemes within proxy mobile IPv6 domains have demonstrated significant reductions in signaling overhead and handover latency through hierarchical gateway structures and optimized signaling, thereby enhancing network performance and user experience [33].

Despite significant progress, persistent challenges remain, notably in managing computational overhead, sustaining real-time inference under tight latency requirements, and ensuring robustness against network uncertainties and adversarial perturbations [20**? ?**]. Large language models (LLMs) in telecommunications exemplify these challenges, requiring efficient deployment strategies and domain-specific adaptations to balance computational demands, privacy, and accuracy [**?**]. The breadth of AI integration spans from automated network traffic classification to autonomous fault management, covering both physical-layer optimization and higher-layer protocol adaptation [6, 7, 24]. Notably, AI-driven network management requires scalable frameworks that maintain accuracy while meeting stringent latency and reliability demands intrinsic to emerging applications like the Tactile Internet, which demands ultra-low latency and high reliability for real-time haptic communications [7]. This evolving landscape is underscored by the convergence of AI methodologies with emerging network architectures, highlighting the critical need for frameworks that balance performance gains while ensuring scalability and interoperability.

1.2 Motivation for AI Integration

The telecommunications and networking sectors are witnessing accelerated growth characterized by increasing data volume, heterogeneous device ecosystems, and complex service requirements, especially within vector databases, wireless networking infrastructures, software-defined networking (SDN), and Open Radio Access Network (Open RAN) architectures [1, 30, 37]. The transition to 5G/6G and beyond-6G (B6G) technologies demands adaptive, intelligent mechanisms capable of managing escalating complexity, enabling dynamic resource allocation, and optimizing real-time performance [22, 26]. AI techniques have demonstrated substantial benefits in these areas by facilitating model-free, context-aware decisions that optimize network slicing, enhance spectrum utilization, and enable hybrid fusion strategies such as combining visible light communication (VLC) and radio frequency (RF) systems [13, 16]. Additionally, AI-empowered sophisticated detection methods and adaptive interference cancellation schemes have proven effective in mitigating wireless channel impairments, thereby improving reliability and throughput [5, 25].

Real-world validations of these AI approaches affirm their practical applicability yet underscore ongoing challenges related to data heterogeneity, privacy preservation, and smooth integration with legacy systems. For example, AI-powered SDN frameworks have achieved up to 92% accuracy in traffic classification and substantial reductions in latency and false positives, but still face computational overhead and dataset scarcity [13]. Similarly, AI integration in Open RAN improves throughput, latency, and energy efficiency, yet demands resolving issues such as real-time inference latency, AI model convergence, and multi-vendor interoperability [5, 25]. Consequently, AI integration is driven not only by the pursuit of performance enhancements but also by the imperative to endow networks with self-adaptive intelligence essential to address the demands and uncertainties characteristic of next-generation telecommunication ecosystems.

1.3 Key AI Techniques and Their Roles

A diverse array of AI methodologies has been harnessed to enhance adaptability and performance within communication networks. Reinforcement learning (RL) constitutes a foundational technique for dynamic resource management, enabling agents to learn optimal policies related to bandwidth allocation, routing, and scheduling through continuous interaction with the environment, without requiring explicit environment modeling [32, 35]. These autonomic approaches facilitate self-configuration, self-optimization, and self-healing by embedding flexibility and adaptability into software-driven network infrastructures, although challenges such as scalability and interpretability remain. Gradient-based optimization methods, including stochastic dual gradient techniques and their variants, further enable efficient parameter updates in resource-constrained settings while offering provable convergence and queue stability for large-scale network control problems [**? ?**]. Such methods support the optimization of complex resource allocation and scheduling tasks critical in beyond-5G and 6G wireless systems.

Rapid algorithmic updates, often leveraging modular and distributed architectures, permit real-time adaptability essential for environments characterized by fluctuating traffic patterns and volatile channel conditions [**?**]. These approaches encompass security frameworks and policy-based rule enforcement crucial for defending against vulnerabilities in edge and cloud network deployments, ensuring network resilience.

Moreover, intelligent wireless technologies, including AI-powered reconfigurable intelligent surfaces (RIS), deep learning-driven interference management frameworks, and semantic communications, substantially enhance physical-layer operations by dynamically shaping signal propagation and improving robustness against noise and interference [6, 24, 38]. AI techniques applied to RIS enable adaptive channel estimation, beamforming, and resource allocation by learning optimal configurations from environmental feedback, thereby significantly improving spectral and energy efficiencies in complex wireless settings. Deep learning models, such as stacked autoencoders and deep neural networks, drive higher-layer tasks including customer churn prediction and traffic management, benefiting from their capacity to extract hierarchical features from raw data for robust decision-making [38]. Collectively, these AI techniques form a multi-layered intelligence framework, integrating decision-making from physical-layer signal optimization to network-layer control and application-specific adaptations, thus paving the way for more autonomous, reliable, and efficient future communication networks.

1.4 Challenges in AI-Enabled Networking

Despite these technological advances, AI-enabled networking faces critical challenges that hinder widespread implementation and effectiveness. Latency remains a stringent constraint, particularly relevant to ultra-reliable low-latency communications (URLLC) and tactile Internet applications, where inference delays and model update latencies may offset potential AI-driven optimization benefits [11, 14]. Scalability issues arise in large-scale, dynamic networks encompassing massive numbers of IoT and mobile devices; centralized AI architectures often face prohibitive computational burdens and excessive data transfer overhead [13, 31]. Privacy concerns are heightened by reliance on sensitive user data and distributed learning paradigms, stimulating the adoption of privacy-preserving algorithms such as federated learning—which nonetheless introduces additional complexities in synchronization and heterogeneity management [13**?**].

Interoperability remains challenging due to the diversity of vendor-specific implementations and the absence of standardized AI protocols, complicating seamless integration across multi-domain infrastructures [18**?**]. Additionally, ensuring robustness against dynamic network conditions and adversarial attacks is difficult, since AI models often assume stationary environments and may degrade significantly under previously unseen scenarios or malicious perturbations [6, 24, 39]. These multifaceted challenges underscore the necessity for scalable, secure, and interpretable AI frameworks capable of reliable operation within heterogeneous, dynamic network ecosystems.

1.5 Scope and Structure of the Survey

This survey systematically examines AI applications across pivotal networking domains, spanning from network traffic classification to autonomous fault management within software-driven infrastructures [17**?**]. It offers an in-depth exploration of AI methodologies tailored specifically for software-defined networking (SDN), routing optimization, Open RAN architectures, and dynamic network slicing, reflecting cutting-edge developments in these areas [21, 29**?**]. To rigorously assess the effectiveness of various AI approaches, the survey employs key performance metrics such as throughput, latency, accuracy, scalability, and robustness, which are critical for evaluating real-world network performance and AI-driven adaptability [13, 16].

Emphasizing both foundational frameworks and emerging trends, this work integrates insights from classical algorithmic control methods with contemporary deep learning and reinforcement learning techniques, fostering a comprehensive understanding of their complementary roles. Recent advances in learning-based optimization, distributionally robust models, and adaptive control are synthesized, alongside discussions on their associated trade-offs, limitations, and open research challenges. By elucidating these multifaceted contributions, the survey aims to provide a robust foundation to inform and guide future research and development in intelligent communication networks, focusing on enhancing network adaptability, operational efficiency, and resilience in increasingly complex and dynamic environments.

2 AI-Enabled Network Traffic Classification

In recent years, AI techniques have been widely adopted for network traffic classification due to their ability to handle the increasing complexity and volume of traffic data. These techniques encompass a variety of methods, including traditional machine learning algorithms, deep learning architectures, and online learning approaches, each offering distinct advantages and challenges.

To provide a comprehensive overview, Table 1 summarizes the key AI methods employed in traffic classification, along with their typical characteristics, strengths, and limitations.

Traditional machine learning techniques rely heavily on domain expertise to extract relevant handcrafted features, which can limit their adaptability to new or evolving traffic types. Deep learning methods address this by automating feature extraction directly from raw traffic data, enabling the recognition of complex and subtle patterns. However, deep models require substantial data for training and entail significant computational resources.

Online learning methods offer a promising avenue for scenarios where network traffic characteristics change rapidly. By updating models incrementally with new data, they maintain relevance over time. Nevertheless, these approaches necessitate careful design to prevent degradation due to noise or concept drift.

Beyond individual methods, comparative insights reveal that choosing an appropriate AI approach depends on application context, data availability, and computational constraints. There is a trade-off between accuracy, adaptability, and resource consumption that must be balanced. For example, while deep learning often achieves superior accuracy, traditional machine learning methods remain competitive in resource-limited environments or when labeled data is scarce.

In summary, the landscape of AI-enabled network traffic classification is diverse and evolving. Future research should focus on

Table 1: Summary of AI Methods for Network Traffic Classification

Method	Characteristics	Strengths	Limitations
Traditional ML (SVM, Random Forest, KNN)	Feature-based; requires manual feature engineering	Well-understood; efficient on small-to-medium datasets	Limited by feature quality; less effective on raw data
Deep Learning (CNN, RNN)	Automatically extracts features from raw data; capable of learning complex patterns	High accuracy; handles large-scale data; adaptive to complex traffic patterns	Requires large labeled datasets; computationally intensive
Online Learning	Models update incrementally with streaming data	Adaptable to evolving traffic patterns; suitable for real-time applications	Potentially less stable; risk of concept drift

hybrid approaches that combine the strengths of various AI methods, enhanced online learning schemes that robustly handle traffic dynamics, and comprehensive benchmarking to guide method selection for practitioners.

2.1 Limitations of Traditional Traffic Classification Methods

Traditional network traffic classification methods, including port-based identification and deep packet inspection (DPI), exhibit significant limitations in contemporary network environments. Port-based approaches rely heavily on static assumptions about port assignments, which are increasingly invalid due to the widespread adoption of dynamic port allocations, tunneling protocols, and applications obfuscating their use of ports. DPI offers finer granularity by examining packet payloads; however, its effectiveness is greatly diminished in the presence of encrypted traffic, since payload contents become inaccessible. Beyond ineffectiveness with encryption, DPI also raises privacy concerns and incurs substantial computational overhead, which can be prohibitive in high-throughput or resource-constrained systems. These constraints collectively reduce the practicality and scalability of conventional methods for managing encrypted, evolving, and complex traffic patterns encountered in modern networks. This has motivated the shift toward adaptive, data-driven classification techniques that leverage flow-level and statistical features, enabling more robust and flexible handling of encrypted and dynamic traffic [16].

2.2 Machine Learning Approaches for Traffic Classification

Advancements in artificial intelligence and machine learning (ML) introduce powerful alternatives that address the shortcomings of classical methods by utilizing statistical and behavioral traffic characteristics, which remain accessible even when payload encryption is enforced. Supervised learning algorithms—such as decision trees, random forests, support vector machines (SVM), k-nearest neighbors (k-NN), and neural networks—have been widely deployed to classify traffic flows based on features extracted from packet sizes, inter-arrival times, and flow durations [16]. These methods rely on labeled datasets to establish decision boundaries and have demonstrated high accuracy under controlled experimental conditions. Ensemble models like Random Forest and Gradient Boosting have shown particularly strong performance, balancing accuracy and robustness in diverse traffic scenarios [16].

In parallel, unsupervised learning techniques, especially clustering algorithms, identify anomalous or previously unseen traffic patterns without the necessity for labeled data. This capability is essential for adapting to new network behaviors and detecting emerging threats, complementing supervised classifiers by providing a dynamic and flexible detection framework [16]. Such approaches can mitigate challenges related to concept drift and evolving traffic, enhancing model adaptability in real-time environments.

Beyond traditional ML, deep learning methodologies leverage architectures such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to automatically learn hierarchical feature representations and capture temporal dependencies intrinsic to sequential packet flows. These models excel particularly in scenarios where encryption obfuscates payload data since they depend on flow-level statistical patterns to maintain classification effectiveness [16, 36**?**]. However, the increased computational complexity and training demands of deep learning models pose challenges for large-scale experimentation and real-time deployment, motivating ongoing research toward scalable, interpretable, and resource-efficient AI frameworks [16]. Future directions include exploring semi-supervised, federated, and edge learning paradigms to improve traffic classification's scalability, privacy preservation, and deployment feasibility in AI-driven networks [16].

2.3 Data Pipeline Processes

The success of AI-based traffic classification frameworks fundamentally depends on constructing a robust data pipeline that encompasses several crucial stages: traffic collection, preprocessing, feature extraction, model training, and performance evaluation.

Traffic collection must ensure comprehensive and representative sampling across diverse network conditions to capture the complexity of real-world traffic, addressing challenges such as encryption and dynamic port usage.

Preprocessing tackles issues including missing data, noise, and feature normalization to produce consistent input distributions that facilitate effective learning.

Feature extraction constitutes a critical phase that directly influences classifier performance. It involves computing statistical metrics derived from both flow-level and packet-level attributes; given encryption restrictions, many approaches rely on flow-based and statistical features rather than payload data when payload visibility is limited.

Model training requires large-scale, balanced datasets to mitigate bias toward dominant classes, enhance generalization, and address concept drift stemming from evolving traffic patterns.

Evaluation rigorously measures classifier performance through metrics such as accuracy, precision, recall, and processing latency [16]. Trade-offs between accuracy and real-time feasibility are carefully considered, especially when deploying complex models like deep learning in production environments.

Maintaining this lifecycle is essential to ensure classifier robustness, particularly in the face of evolving network conditions, domain shifts, and emerging challenges related to privacy preservation and scalability.

2.4 Performance Trade-offs

Implementing AI-powered classifiers in operational networks entails managing intrinsic trade-offs among accuracy, computational complexity, and real-time feasibility. Ensemble techniques, such as random forests and gradient boosting, provide robust and interpretable predictive performance with moderate computational costs. However, they may face challenges in handling encrypted traffic and adapting promptly to dynamic traffic changes [16]. Conversely, deep learning methods significantly enhance the ability to abstract features and model temporal dependencies, enabling superior classification of complex or obfuscated traffic patterns. These advantages typically come with increased inference latency and higher resource consumption, which can constrain scalability and suitability for edge deployment.

Real-time network operation requires a careful balance between detection speed and classification precision. Emerging adaptive frameworks that incorporate incremental and online learning strive to minimize the overhead of retraining while enabling rapid adaptation to concept drift and evolving traffic distributions. Although promising, these approaches remain subjects of active research [16].

2.5 Challenges and Emerging Directions

Despite substantial progress, AI-enabled network traffic classification continues to confront several key challenges.

Data imbalance poses a critical issue as common traffic classes disproportionately dominate datasets, biasing models and reducing sensitivity to rare or malicious traffic types. This imbalance hinders the detection of infrequent but potentially severe anomalies [16].

Encrypted traffic further complicates classification, as encryption techniques obscure payload contents, limiting the available feature space primarily to flow and statistical characteristics. This restriction demands advanced feature extraction and modeling approaches capable of inferring traffic types under constrained visibility [16].

Concept drift reflects the evolving nature of network behaviors over time, necessitating adaptive learning frameworks that can update models continuously to maintain classification accuracy amid changing patterns [16].

Dataset representativeness remains challenging since publicly available benchmarks often lack diversity in traffic sources, scales, and environments. This limitation affects the generalizability and transferability of trained models across heterogeneous network settings [16].

Addressing these challenges, promising future directions emphasize scalable and privacy-aware learning paradigms. **Semi-supervised learning** leverages abundant unlabeled data alongside limited labeled samples to improve model robustness and generalization, mitigating labeling costs and data scarcity issues [16, 24]. **Federated learning** enables decentralized, privacy-preserving model training by aggregating locally trained models without sharing raw traffic data, offering advantages for real-time edge inference and compliance with stringent data protection regulations [6, 16, 24].

Explainability has emerged as an indispensable aspect for deploying AI classifiers in network operations. Interpretable models and post-hoc explanation techniques help network operators understand model decisions, detect potential biases, and fulfill auditing requirements, thereby enhancing trust and accountability [16, 24].

Moreover, integrating AI with **edge computing** infrastructures fosters a paradigm shift by decentralizing inference closer to data sources. This proximity reduces latency and bandwidth consumption while enhancing scalability and robustness. The synergy between AI and edge computing facilitates more responsive, efficient, and privacy-preserving network traffic classification systems [6, 16].

In summary, AI-enabled traffic classification represents a transformative advancement over traditional methods by effectively adapting to encrypted, dynamic, and heterogeneous network traffic. Continued innovation targeting computational efficiency, data challenges, interpretability, and privacy is crucial to enable seamless integration within operational network environments and realize the full potential of AI-driven networking.

3 AI Integration in Software-Defined Networking (SDN) for 5G and Beyond

The convergence of Artificial Intelligence (AI) with Software-Defined Networking (SDN) presents transformative opportunities for advancing 5G and future network technologies. SDN's programmable architecture decouples the control plane from the data plane, enabling centralized network management and dynamic resource allocation. When integrated with AI, this programmable nature facilitates intelligent decision-making, automation, and network optimization tailored to diverse and stringent 5G requirements.

AI techniques, such as machine learning and deep learning, empower SDN controllers to analyze vast amounts of network data in real-time, supporting tasks like traffic prediction, anomaly detection, and self-healing. These capabilities enhance network performance by optimizing routing, load balancing, and quality of service while reducing latency and energy consumption. Moreover, AI-driven SDN frameworks can enable proactive resource management in dynamic 5G environments, adapting swiftly to user mobility and varying service demands.

Beyond basic performance improvements, integrating AI in SDN supports the implementation of network slicing—a foundational feature of 5G—by dynamically configuring and orchestrating isolated virtual networks customized for specific applications or industries. This integration further promotes security by enabling intelligent threat detection and automated mitigation mechanisms within the SDN architecture.

In summary, AI integration in SDN for 5G and beyond is pivotal for achieving intelligent, flexible, and scalable networks capable of meeting evolving technical challenges and diverse service requirements.

3.1 AI-Powered SDN Architectures

The integration of Artificial Intelligence (AI) within Software-Defined Networking (SDN) architectures has fundamentally transformed network control paradigms by enabling highly centralized, programmable, and intelligent decision-making frameworks. AI enhances the SDN controller's ability to dynamically adapt to fluctuating network conditions and heterogeneous traffic demands typical of 5G environments, thereby facilitating scalable and automated network management [13]. This architectural synergy leverages AI's pattern recognition and predictive analytics to optimize resource allocation and policy enforcement, while abstracting underlying hardware complexities.

Specifically, AI-powered SDN frameworks incorporate advanced supervised learning classifiers, such as Random Forest and Support Vector Machines (SVM), alongside deep learning models like Long Short-Term Memory (LSTM) networks within the SDN controller. These models facilitate real-time traffic classification, anomaly detection, and dynamic resource allocation, demonstrated to achieve up to 92% accuracy in traffic classification, 18% reduction in end-to-end latency, and 15% throughput improvement for enhanced Mobile Broadband (eMBB) applications [13]. These capabilities contribute significantly to meeting the stringent requirements of ultra-reliable low-latency communication (URLLC) and other 5G service categories.

Nonetheless, this integration poses challenges such as computational overhead, latency constraints, dataset scarcity, and vulnerability to adversarial AI attacks, which must be carefully managed for real-time network operations. Addressing these issues motivates ongoing research into lightweight AI models optimized for real-time response, federated learning approaches to enhance privacy, and robust AI techniques resilient to attacks, extending the applicability of AI-powered SDN architectures beyond 5G networks [13]. Overall, the AI-SDN synergy substantially improves scalability, flexibility, and automation in 5G and beyond network environments.

3.2 AI Techniques in SDN

Within SDN controllers, AI techniques primarily encompass supervised machine learning classifiers such as Random Forests and Support Vector Machines (SVM). These models effectively manage traffic classification and anomaly detection tasks by providing robust and interpretable decision boundaries suited to identifying diverse traffic patterns under varying network states [13]. In parallel, deep learning architectures—particularly Long Short-Term Memory (LSTM) networks—offer distinct advantages by capturing temporal dependencies and sequence dynamics in traffic flows, which are critical for modeling network behavior amidst temporal volatility [13]. The complementary utilization of shallow classifiers alongside deep recurrent networks creates a holistic framework that adapts to both static features and dynamic temporal shifts within network traffic. Empirical studies demonstrate that these AI-powered SDN frameworks can achieve up to 92% accuracy in traffic classification, reduce end-to-end latency by 18%, and increase throughput for enhanced Mobile Broadband (eMBB) services by 15%, while maintaining a false positive rate below 3% in anomaly detection [13]. Despite these benefits, training such complex models demands extensive labeled datasets and substantial computational resources, posing scalability challenges for practical deployments. Future work is directed toward developing lightweight AI models optimized for real-time response, incorporating federated learning to enhance privacy, and designing robust AI resilient to adversarial attacks, to further improve the scalability, flexibility, and automation of SDN in 5G and beyond networks [13].

3.3 Performance Improvements

Empirical studies confirm that AI-enhanced SDN architectures yield significant improvements across key network performance metrics. Specifically, the integration of supervised learning classifiers, such as Random Forest and SVM, alongside deep learning models like LSTM networks, within the SDN controller framework has achieved traffic classification accuracies up to 92%, markedly reducing misclassification errors that degrade service quality [13]. These accuracy enhancements translate directly into improved throughput, with experimental results indicating increases close to 15% in enhanced Mobile Broadband (eMBB) scenarios, owing to more precise resource scheduling and dynamic traffic steering enabled by AI-based decisions. Furthermore, AI's capability for rapid anomaly detection and real-time traffic adaptation has led to latency reductions of approximately 18% in end-to-end communications [13]. Equally critical is the reduction in false positive rates for anomaly detection to below 3%, which significantly minimizes unnecessary mitigation actions that could otherwise impair network efficiency. Collectively, these benefits underscore AI's pivotal role in elevating Quality of Service (QoS) metrics and responsiveness in the inherently volatile 5G network environments, promoting enhanced scalability, flexibility, and automation within the SDN architecture.

3.4 Challenges

Despite these advancements, deploying AI-powered SDN frameworks encounters several substantive obstacles that limit operational scalability and security. Foremost among these is the substantial computational overhead introduced by sophisticated AI models, which may hinder timely inference essential for ultra-low-latency applications such as those found in 5G and beyond networks [13]. Additionally, the scarcity of telecom-specific datasets presents a major barrier to supervised learning, given that annotated network traffic data is often limited, proprietary, or sensitive, thereby constraining model generalizability and robustness [**?**]. This scarcity is particularly challenging for training models that must adapt to diverse and dynamic network environments. Moreover, adversarial AI attacks pose significant security threats, as malicious actors may exploit vulnerabilities within AI models to induce erroneous decisions or evade detection, raising concerns over the reliability and trustworthiness of AI-enabled network control [18]. Interoperability challenges also arise due to heterogeneous vendor equipment and divergent technological standards, complicating seamless AI integration across multi-domain and multi-vendor SDN deployments [**?**]. Addressing these issues requires innovations not only in algorithmic design—such as lightweight AI models optimized for real-time response and robust defense mechanisms against adversarial threats—but also in collaborative frameworks that promote data sharing while preserving privacy, and standardize protocols across the telecom ecosystem to support scalable and secure AI-SDN integration.

3.5 Prospects Beyond 5G (6G)

Looking ahead, the evolution toward beyond 5G networks, particularly 6G, envisions the development of lightweight, privacy-preserving AI models specifically tailored for distributed SDN environments [6, 24]. Federated learning stands out as a promising approach, enabling collaborative model training across decentralized network nodes without exposing sensitive data, thereby addressing privacy and security concerns inherent in centralized data aggregation [13]. Anticipated advancements in multi-modal AI architectures—including large language models and multi-sensor data fusion—are expected to enhance situational awareness and optimize network performance beyond current temporal and spatial constraints [13]. Moreover, the integration of Reconfigurable Intelligent Surfaces (RIS) with AI techniques, such as machine learning and deep reinforcement learning, will likely play a pivotal role in dynamically controlling wireless environments to improve spectral and energy efficiency in 6G [6]. These intelligent wireless environments promise to boost coverage, robustness, and adaptability, critical for meeting 6G requirements like ultra-reliability, massive connectivity, and real-time intelligence. Nonetheless, achieving federated and privacy-aware AI solutions faces substantial computational, communication, and standardization challenges. High-dimensional configuration spaces and the need for low latency impose constraints on AI scalability and deployment [6, 24]. Addressing these challenges requires interdisciplinary research bridging AI, communications, and network engineering disciplines, alongside the development of lightweight distributed AI algorithms and robust models resilient to adversarial conditions [6, 13, 24]. The synergy of AI's algorithmic power with emerging wireless technologies will be essential in realizing the next generation of intelligent, autonomous, and scalable networks.

3.6 Summary

In summary, the integration of artificial intelligence (AI) techniques into Software Defined Networking (SDN) paradigms for 5G networks has driven notable advancements in enhancing network flexibility, adaptability, and overall performance. Despite these gains, significant challenges remain, particularly related to high computational demands and security vulnerabilities inherent in AI-enabled SDN deployments. Looking forward, the evolution toward 6G networks necessitates the development of optimized and distributed AI frameworks that effectively balance intelligent decision-making, computational efficiency, and stringent privacy requirements. These frameworks embody the forefront of research aiming to realize fully programmable, autonomous, and resilient network architectures in future communication systems.

3.7 AI-Driven Routing Optimization

AI-driven routing optimization leverages advanced algorithms to improve the efficiency and adaptability of routing in complex networks. These approaches use machine learning models to predict network conditions and dynamically adjust routing paths to optimize various performance metrics such as latency, throughput, and energy consumption [].

One of the critical algorithmic design challenges in AI-driven routing is balancing the trade-off between exploration and exploitation. Routing algorithms must explore new paths to discover optimal routes while exploiting known paths to maintain network stability. This challenge is compounded in highly dynamic environments, where network states change rapidly, requiring algorithms to adapt in real-time [].

Another significant challenge is the integration of heterogeneous data sources and real-time measurements into the decision-making process. AI models need to process diverse and sometimes incomplete information efficiently to generate accurate routing predictions. Moreover, ensuring scalability and low computational overhead remains a key concern, as routing optimization must operate seamlessly in large-scale networks [].

Additionally, handling uncertainty and variability in network conditions demands robust learning techniques. Algorithms often incorporate reinforcement learning mechanisms to continuously refine routing policies in response to feedback, enabling improved resilience against network disruptions [].

Although AI-driven routing promises substantial gains in network performance, the complexity of designing effective algorithms that can operate under stringent latency and reliability requirements remains an active area of research. Future work includes refining model interpretability, enhancing real-time responsiveness, and devising methods to guarantee performance bounds [].

In this section, we have synthesized the main algorithmic challenges in AI-driven routing optimization, highlighting the need for adaptable, scalable, and robust solutions to meet the demands of increasingly complex network environments.

3.7.1 *Limitations of Static Routing Protocols.*

Traditional static routing protocols lack the adaptability necessary for dynamic and heterogeneous network environments, leading to suboptimal performance under varying traffic patterns and network conditions. Originally designed for relatively stable and homogeneous infrastructures, these protocols exhibit limited real-time responsiveness to fluctuating workloads, mobility-induced topology changes, and unpredictable link failures. As a result, challenges such as increased latency, reduced throughput, and vulnerability to faults frequently arise in large-scale, multi-tenant networks typical of modern wireless and software-defined architectures [39]. Moreover, the rigidity inherent in static routing constrains efficient resource utilization and impedes the exploitation of cross-layer contextual information, which is critical for advancing 5G and beyond networks. These limitations underscore the need for adaptive routing mechanisms capable of dynamically responding to network state changes by learning from traffic patterns and anomalies, as proposed in emerging AI-driven approaches [39].

3.7.2 *Reinforcement Learning and Neural Networks for Routing.*

Artificial intelligence (AI) approaches, particularly reinforcement learning (RL) and neural networks (NNs), provide advanced tools to surpass the constraints of static routing by enabling adaptive, data-driven path optimization. RL algorithms iteratively explore and exploit routing policies to dynamically optimize multiple objectives such as throughput maximization, latency minimization, and fault tolerance enhancement [**?**]. This results in dynamic path prediction that directly responds to real-time network states. Neural networks complement this by learning complex nonlinear mappings from network metrics to optimal routing decisions, thereby generalizing from historical data and adapting to new conditions [27]—[**?**]. Together, these AI-driven methods empower autonomous routing frameworks that accommodate heterogeneous node capabilities and varying traffic demands, frequently outperforming traditional heuristics through superior robustness and scalability.

Nonetheless, key challenges remain. RL demands careful balancing of the exploration-exploitation trade-off, requiring meticulous algorithm design to avoid suboptimal policies. At the same time, maintaining model generalization without overfitting to specific network scenarios necessitates ongoing retraining and adaptation [39]. Empirical evidence indicates that AI-empowered routing schemes can improve network throughput and reduce latency by up to 30% relative to static routing protocols, while also enhancing fault tolerance via swift anomaly detection and rerouting [**?**]. Continuous research into scalability, training efficiency, and integration with legacy network infrastructure is essential to fully realize the potential of AI-driven routing in practical deployments.

3.7.3 Traffic Prediction and Anomaly Detection Integration. The incorporation of traffic prediction and anomaly detection into routing optimization marks a significant advancement by enabling proactive, rather than purely reactive, network management. Traffic prediction models—typically leveraging supervised learning and advanced time-series deep learning architectures such as RNNs and CNNs—forecast network load and congestion trends. These forecasts inform route selection decisions ahead of potential performance degradation, enhancing throughput and latency outcomes [24]. Concurrently, anomaly detection systems identify deviations from normal operation patterns, including link failures, cyberattacks, or misconfigurations, enabling rapid and accurate rerouting decisions that preserve service quality and network availability [39].

Integrating predictive traffic models with anomaly detection within AI-driven routing frameworks facilitates multi-objective optimization that addresses performance, reliability, and security simultaneously. This strategy enhances overall network resilience by preempting bottlenecks and limiting fault propagation, moving beyond traditional static routing limitations [39]. However, challenges remain in maintaining high accuracy under non-stationary and volatile network conditions, complicated by heterogeneous and voluminous data sources. Additionally, anomaly detection mechanisms must balance sensitivity and specificity effectively to minimize false positives, which could otherwise trigger unnecessary path changes and degrade performance.

Developing robust, generalizable models trained on diverse and representative datasets is essential to achieving this balance [24]. Furthermore, emerging research suggests benefits from integrating reinforcement learning techniques to dynamically adapt routing policies based on evolving network states and detected anomalies, thereby enhancing scalability and real-time responsiveness [39]. Overall, the convergence of traffic prediction and anomaly detection within AI-driven routing constitutes a transformative approach, promising self-optimization and robustness essential for complex modern and future network paradigms such as 5G, SDN, and beyond.

3.7.4 Empirical Gains and Challenges. Experimental validations of AI-driven routing protocols consistently demonstrate substantial gains, including increased throughput, reduced latency, and improved fault tolerance across diverse network topologies and traffic scenarios [**?**]. For example, reinforcement learning and neural networks enable dynamic adaptation to changing network conditions, yielding up to 30% improvements in throughput and latency, alongside enhanced resilience through rapid failure detection and rerouting [39]. However, scaling these AI models to large-scale, high-speed networks involves significant computational and communication overheads, particularly within centralized learning architectures, which can become bottlenecks [39]. These overheads are magnified by client heterogeneity and unreliable communication in wireless networks, prompting solutions such as gradient sparsification, error feedback, and adaptive client selection to improve efficiency and robustness [**?**].

Security vulnerabilities also arise from adversarial attacks that manipulate training data or model inference, potentially degrading routing performance and network stability. Mitigating these risks requires robust security protocols specifically tailored for network environments. Additionally, integrating AI models with legacy network infrastructures introduces further complexity. Hybrid or modular deployment strategies are necessary to ensure backward compatibility without service disruption, as networks must maintain continuous operation during incremental AI adoption [18].

Real-time inference demands combined with continuous model updates intensify these challenges, creating trade-offs among accuracy, responsiveness, and resource consumption. Addressing these limitations calls for advances in lightweight AI model designs, distributed and federated learning frameworks, and security-enhanced architectures fit for dynamic and heterogeneous network scenarios [39**?**]. Such innovations will be critical to fully realize the transformative potential of AI-driven routing in next-generation networks.

3.7.5 Future Trends. Emerging directions in AI-based routing optimization focus on decentralized and federated learning architectures to overcome scalability and privacy limitations inherent in centralized approaches. Federated learning enables distributed clients or network nodes to collaboratively train shared models without exposing sensitive local data, thus safeguarding privacy and reducing communication overheads [39]. Robust federated frameworks employ adaptive client selection and gradient sparsification to efficiently manage heterogeneous device capabilities and mitigate client dropout, enhancing convergence rates and accuracy under realistic wireless network conditions [6].

Moreover, hybrid algorithms that integrate AI techniques with conventional routing protocols exhibit promise for delivering adaptive yet lightweight routing solutions, facilitating seamless transitions and backward compatibility. These hybrid approaches leverage the heuristic strengths of traditional protocols while augmenting adaptability and predictive performance through machine learning components. Future research priorities include developing federated, privacy-preserving, and resource-efficient AI algorithms that address computational overhead and scalability challenges; integrating explainability and transparency features to foster operational trust; and expanding applicability to emerging paradigms such as 6G networks, massive MIMO, and edge computing ecosystems [39]. Collectively, these advancements are crucial for realizing fully autonomous, scalable, and resilient network routing architectures that can dynamically adapt to complex, evolving network environments.

4 AI in Open Radio Access Network (Open RAN) for 6G

4.1 Open RAN Architecture and AI Integration Layers

Open RAN introduces a transformative approach to wireless network infrastructure by disaggregating traditionally monolithic radio access components into three distinct units: the Radio Unit (RU), Distributed Unit (DU), and Centralized Unit (CU). This modular design fosters openness and programmability through well-defined interfaces, enabling accelerated innovation and increased vendor diversity. A pivotal advancement in Open RAN is the multilayer integration of artificial intelligence (AI), which enhances network intelligence by embedding AI capabilities at each architectural layer to systematically tackle unique operational challenges and holistically optimize performance [25].

At the RU level, AI models operate under stringent latency constraints to enable real-time radio signal processing and physical layer optimizations, such as adaptive beamforming and dynamic spectrum management. The DU leverages AI to manage scheduling, resource allocation, and localized interference mitigation, utilizing moderate computational resources alongside locally gathered datasets. Meanwhile, the CU aggregates network-wide telemetry data to execute sophisticated AI analytics that enable dynamic orchestration, fault detection, and long-term network optimization. This hierarchical AI deployment framework strategically balances computational complexity and latency requirements, ensuring scalability and responsiveness while supporting features like federated learning for user privacy and reinforcement learning for adaptive scheduling [25].

4.2 AI Techniques in Open RAN

A diverse array of AI techniques underpins Open RAN functionalities, each selected to meet specific operational objectives. Federated learning is particularly prominent, enabling distributed model training across the RU, DU, and CU layers without direct raw data sharing. This decentralization preserves user privacy while addressing the multi-vendor and multi-domain heterogeneity inherent to Open RAN environments, facilitating collaborative intelligence without compromising sensitive data [25]. Reinforcement learning (RL), especially deep RL, empowers autonomous decision-making for dynamic spectrum management, adaptive resource allocation, and interference mitigation by learning optimal policies through environment interaction. These AI-driven approaches enable the network to adapt effectively to changing conditions and optimize performance in real time [1, 37]. Deep neural networks (DNNs) are widely utilized for tasks requiring sophisticated pattern recognition and nonlinear mapping, such as fault detection and anomaly identification, leveraging the large volumes of standardized telemetry data collected in Open RAN ecosystems [22, 30].

Moreover, hybrid fusion techniques exemplify AI's adaptability in managing heterogeneous communication channels and mitigating interference. For instance, integrating visible light communication (VLC) and radio frequency (RF) modalities employs machine learning-based fusion and interference cancellation algorithms to enhance robustness in complex environments [26]. This VLC-RF hybrid approach capitalizes on the complementary characteristics of the two channels, improving overall communication reliability and throughput. Additionally, AI-driven sequence management strategies optimize high-capacity preamble sequence design for random access channels, significantly reducing collision probabilities. These designs increase the number of unique preambles with low cross-correlation, improving detection performance and decreasing retransmissions, which is critical for supporting massive IoT device connectivity in 5G and beyond [37]. Despite these advances, deploying AI in Open RAN faces challenges including the computational overhead of real-time model training, coordinating AI functionalities across diverse multi-vendor equipment, and ensuring scalability and interoperability in dynamic network environments [6, 25].

4.3 Performance Enhancements

Integrating AI into Open RAN architectures markedly improves key network performance metrics, including throughput, latency, energy efficiency, reliability, and resource utilization. AI-driven algorithms enable dynamic spectrum access and intelligent scheduling that adapt bandwidth allocation responsively to fluctuating traffic and complex interference conditions, thus boosting effective throughput and minimizing latency [25]. Energy efficiency is enhanced through AI-enabled resource optimization and hardware-aware scheduling schemes, which selectively power down idle components or scale computing tasks based on real-time network load, contributing to greener operations [6].

Reliability and connection robustness benefit from AI-based proactive fault detection and predictive maintenance, which facilitate early identification of anomalies before service degradation occurs. For example, reinforcement learning algorithms dynamically adjust handover parameters, reducing connection drops and improving mobility management [25]. Furthermore, AI improves resource utilization by analyzing extensive telemetry data to identify bottlenecks and redundant allocations, thereby facilitating efficient network slicing and large-scale multi-access edge computing (MEC) deployments [6].

Notably, the integration of Reconfigurable Intelligent Surfaces (RIS) combined with AI techniques leads to intelligent wireless environments that dynamically optimize the propagation environment, further enhancing coverage, spectral efficiency, and robustness [6]. These AI-powered enhancements collectively enable Open RAN to surpass traditional heuristic methods, adapting efficiently to dynamic network states and complex scenarios while managing challenges such as latency constraints, scalability, and interoperability [25]. This positions AI-empowered Open RAN as a cornerstone for resilient, efficient, and sustainable 6G networks.

4.4 Challenges

Despite these substantial gains, embedding AI within Open RAN poses several critical challenges. Model convergence remains a major concern, especially in dynamic and non-stationary wireless environments where partial observability can destabilize reinforcement learning and distributed training processes [25]. Additionally, the high computational demands for training and inference at edge units such as RUs and DUs, which have constrained processing capabilities, impose stringent resource limitations. Overcoming these demands requires advances in lightweight AI models and the development of efficient hardware accelerators tailored for edge deployment [18].

Multi-vendor interoperability also remains complex due to the heterogeneity of hardware capabilities, proprietary implementations, and disparate data formats, which complicate standardization and seamless integration of AI functionalities within the Open RAN ecosystem [6]. The deployment of AI further intensifies security and privacy risks; adversarial attacks targeting AI models, leakage of sensitive information during federated learning exchanges, and vulnerabilities in distributed AI protocols necessitate robust defense mechanisms alongside stringent regulatory compliance [24]. Furthermore, evolving telecommunications regulations—covering aspects such as data sovereignty, user privacy, and transparency—impose additional operational constraints on AI algorithm design, deployment, and governance [18].

Addressing these challenges requires multidisciplinary efforts spanning scalable and explainable AI frameworks, hardware-software co-design for edge intelligence, resilient and privacy-preserving learning methods, as well as coordinated standardization to ensure interoperability and regulatory adherence. These endeavors are essential to realize the full potential of AI-driven Open RAN architectures in delivering adaptive, secure, and efficient wireless networks for 6G and beyond.

4.5 Future Research Directions

Future research must prioritize explainability and transparency of AI decision-making within Open RAN to build trust, satisfy regulatory requirements, and facilitate efficient troubleshooting. Explainable AI (XAI) approaches will provide clear insights into AI-driven resource allocations and fault detection processes, which is especially crucial in multi-stakeholder environments where accountability and interpretability are paramount [25]. The development of multi-agent collaborative learning frameworks is expected to enhance distributed AI systems by enabling coordinated intelligence across RU, DU, and CU layers. This coordination is essential to effectively address the complex cross-layer optimization challenges intrinsic to 6G networks [18].

Designing lightweight AI models tailored specifically for resource-constrained edge units is critical to overcoming computational and energy limitations. Complementing these models with dedicated hardware accelerators will further mitigate bottlenecks, enabling real-time, efficient AI deployment at the network edge [24]. Emerging paradigms such as quantum computing offer promising avenues for solving complex optimization problems in Open RAN infrastructures, potentially surpassing classical approaches in speed and scale. Additionally, blockchain technologies can strengthen security, ensure data integrity, and support decentralized trust mechanisms, which are vital enablers for robust multi-vendor Open RAN ecosystems [25]. Integrating these cutting-edge technologies with AI capabilities will significantly advance Open RAN, paving the way for fully autonomous, resilient, and high-performance next-generation wireless networks.

5 Large Language Model-Driven Agentic AI for O-RAN Network Resilience

This section presents the integration of Large Language Models (LLMs) into agentic AI frameworks aimed at enhancing resilience in O-RAN networks. We discuss the architectures and operational flows of LLM-driven agents, emphasizing their role in dynamic decision-making and automation for network management.

By leveraging the powerful reasoning and adaptation capabilities of LLMs, agentic AI can proactively detect, diagnose, and mitigate network faults and anomalies, thus reinforcing O-RAN network reliability. The following subsections detail different aspects of LLM integration, including the structural design of agent architectures and the data flow mechanisms that support autonomous and context-aware operations.

In summary, the deployment of LLM-driven agentic AI constitutes a promising approach for resilient O-RAN systems by enabling smart, scalable, and adaptive network control.

5.1 Embedding LLM-Based Agents in RAN Intelligent Controller and SMO

The integration of Large Language Model (LLM)-based agents within the Open Radio Access Network (O-RAN) architecture—specifically within components such as the near Real-Time RAN Intelligent Controller (Near-RT RIC) and Service Management and Orchestration (SMO)—represents a significant advancement toward autonomous fault management. Embedding these agents enables continuous, context-aware monitoring of network telemetry alongside dynamic remediation strategies executed without human intervention. This autonomy exceeds traditional rule-based or supervised learning systems, which typically rely on predefined fault catalogs or manual threshold triggers. Leveraging LLMs' intrinsic capability to parse and synthesize diverse network state information, agentic AI systems can interpret a broad spectrum of fault manifestations and implement tailored corrective actions such as dynamic resource re-allocation and service re-configuration, all while adhering to stringent near-RT latency constraints [5].

Experimental evaluations have demonstrated that this LLM-driven agentic approach achieves a fault detection accuracy of 95%, a mitigation success rate of 91%, reduces network downtime by 40%, and decreases throughput degradation from 25% to 10% compared to conventional methods [5]. Furthermore, coupling LLM-based agents with the modular, open interfaces inherent to the O-RAN framework facilitates customizable agent behaviors and scalable deployments, thereby enhancing operational flexibility and significantly reducing mitigation time for complex fault scenarios. Nonetheless, challenges such as computational overhead, potential erroneous decisions, security risks, and vendor interoperability issues remain. Proposed solutions include hierarchical agent designs and rigorous validation processes to ensure reliability. Future work aims to optimize these LLM agents for edge deployment, enhance multi-agent coordination, incorporate explainability, and improve security robustness, underscoring the promising role of LLM-based agents in reinforcing O-RAN self-healing capabilities.

5.2 Natural Language Processing for Fault Interpretation and Interaction

A critical enabler of LLM-driven agentic AI efficacy is the application of advanced natural language processing (NLP) techniques for fault interpretation and human-machine interaction. Unlike traditional, deterministic fault detection frameworks that rely solely on numeric alarms or discrete indicators, LLMs process heterogeneous data outputs—including logs, alerts, and operator annotations—with nuanced semantic comprehension, enabling more sophisticated fault diagnosis. This advanced capability allows agents not only to detect and localize faults but also to contextualize root causes within operational narratives, thereby facilitating coherent, meaningful communication with human operators [5]. Such NLP-enabled interaction enhances transparency and fosters operator trust—vital factors given the inherent risks of erroneous decisions in fully autonomous systems. Moreover, these agents can articulate mitigation strategies, justify their decisions, and incorporate real-time operator feedback, ensuring integration of human oversight alongside agent autonomy. Experimental results demonstrate that this approach increases fault detection accuracy and mitigation success rates, significantly reducing network downtime and throughput degradation. This integrative process addresses critical concerns related to model interpretability, acceptance, and operational resilience during live network operations.

5.3 Experimental Achievements

Empirical evaluations confirm that integrating LLM-based agentic AI within the O-RAN architecture significantly enhances fault management capabilities. Experimental results show fault detection accuracy of up to 95%, a substantial improvement over baseline accuracies near 78% [3, 5, 14]. Mitigation success rates improve by more than 20%, while network downtime is reduced by approximately 40%. Concurrently, throughput degradation decreases from about 25% in baseline systems to around 10%, demonstrating more efficient network operation [5]. These improvements derive from the agents' abilities to proactively anticipate faults and execute diverse, context-aware responses, which outperform traditional heuristic or static rule-based approaches that often suffer from delayed or partial fault handling [14]. Furthermore, throughput enhancements reflect real-time resource optimization and adaptive reconfiguration orchestrated directly by agents embedded in the RIC and SMO layers, validating both the practical feasibility and operational effectiveness of this agent-based architectural framework [5]. These findings highlight promising advances in enhancing next-generation wireless network resilience through intelligent autonomous management.

5.4 Comparative Performance Analysis

When compared to conventional fault management techniques reliant on manual or semi-automated processes, LLM-driven agentic AI exhibits superior adaptability and resilience. Traditional methods frequently fail to capture the intricate interdependencies and temporal dynamics inherent in multi-source network data, resulting in suboptimal fault isolation and extended recovery times. In contrast, LLM agents synthesize multimodal inputs and apply contextual reasoning to enable expedited and more accurate fault classification and resolution pathways [5]. Furthermore, experimental evaluations demonstrate that LLM agentic AI achieves a fault detection accuracy of 95%, a mitigation success rate of 91%, and reduces downtime by 40%, significantly outperforming baseline approaches. Throughput degradation is also lowered from 25% to 10% in tested scenarios, illustrating enhanced network performance during fault conditions. Additionally, the continuous learning capabilities embedded in these agent architectures promote sustained performance improvements by adapting dynamically to evolving network topologies and traffic profiles. This operational advantage positions agentic AI as a markedly superior solution for managing the increasing heterogeneity and scale of next-generation wireless infrastructures.

5.5 Recognized Challenges

Despite these significant advancements, deploying LLM-based agentic AI within O-RAN architectures poses several critical challenges. First, the computational overhead associated with large-scale LLM inference raises concerns regarding latency and energy efficiency, particularly within resource-constrained edge environments [5, 18]. This challenge necessitates optimization of LLM architectures for real-time, low-power operation at the edge. Second, inaccuracies arising from incomplete or noisy input data, model bias, or adversarial conditions threaten network stability by potentially inducing erroneous decisions. Robust data preprocessing, model validation, and adversarial resilience mechanisms are essential to mitigate such risks. Third, AI-specific security vulnerabilities—including data poisoning and model inversion attacks—require stringent, multilayered safeguards to protect both data integrity and model confidentiality. Finally, ensuring seamless interoperability of LLM agents across heterogeneous multi-vendor ecosystems—each characterized by proprietary interfaces and diverse data semantics—remains an unresolved issue complicating standardized deployment [5, 18]. Hierarchical agent design and rigorous validation protocols may help address this complexity. Collectively, these challenges underscore the multifaceted difficulty of operationalizing agentic AI at scale while maintaining network performance and reliability.

5.6 Proposed Solutions and Optimizations

To address the aforementioned challenges, several strategies have been proposed. A hierarchical agent design paradigm advocates for lightweight, edge-deployable agents managing real-time, low-level tasks, while delegating more computationally intensive LLM operations to centralized or cloud environments. This approach effectively balances computational load with latency requirements and is critical for optimizing performance in resource-constrained edge environments [5]. Rigorous validation frameworks that incorporate simulated fault injection and continuous model retraining serve to reduce erroneous actions and bolster model robustness, ensuring reliable autonomous operation. Resource-constrained edge deployment benefits from advanced optimization techniques such as model pruning, quantization, and knowledge distillation, which significantly reduce computational demands without sacrificing

Table 2: Performance Comparison between Conventional Fault Management Baseline and LLM-Driven Agentic AI [5]

Metric	Baseline	LLM-Driven Agentic AI	Improvement
Fault Detection Accuracy	78%	95%	+17%
Mitigation Success Rate	70%	91%	+21%
Downtime Reduction	-	40%	-
Throughput Degradation	25%	10%	-15%

accuracy. Additionally, the adoption of standardized open interfaces and semantic data models within the O-RAN architecture enhances interoperability and facilitates seamless adaptation across multiple vendor implementations, thereby addressing the complexity inherent in multi-vendor ecosystems [5]. Collectively, these solutions form a comprehensive and scalable pathway toward practical deployment of LLM-driven agentic AI, enabling improved network resilience, fault detection, and self-healing capabilities demonstrated in recent experimental evaluations.

5.7 Future Directions

Future research endeavors focus on several pivotal areas aiming to advance agentic AI capabilities within complex O-RAN ecosystems. Enhancing multi-agent coordination to enable cooperative fault detection and mitigation across distributed RAN contexts promises improved resilience through collective intelligence [37]. To guide practical implementation, challenges including synchronization, backward compatibility, and computational complexity must be carefully addressed alongside novel algorithm design. Advancements in explainability methods remain critical to demystify agent decision-making processes, thereby fostering greater operator trust and aiding compliance with regulatory frameworks [18]. These methods could leverage interdisciplinary synergies between AI, control theory, and wireless signal processing to develop interpretable yet high-performance models. Strengthening security through adversarial training, secure model update protocols, and anomaly detection constitutes an imperative to safeguard agentic AI frameworks against emerging cyber threats [24]. Practical deployment will require scalable, real-time capable architectures balancing accuracy with latency and resource constraints.

Furthermore, integrating adaptive resource allocation and intelligent sequence management techniques offers potential for further optimization of network performance under dynamically changing conditions [37]. Such methods may yield disruptive innovations by shifting from static to fully autonomous, self-optimizing networks capable of real-time adaptation in massive IoT environments. Methodological frameworks combining reinforcement learning-based dynamic resource allocation with robust forecasting and anomaly detection models will be essential to guide researchers in this space [24]. Collectively, these future directions emphasize the increasing complexity of O-RAN networks and highlight the central role that sophisticated AI agents will play in ensuring their continued resilience, security, and operational excellence. Addressing the multifaceted challenges across AI explainability, security, coordination, and adaptive optimization will require interdisciplinary collaboration and holistic frameworks supporting sustainable deployment and evolution.

6 Adaptive Control and Reinforcement Learning in Networking Systems

Adaptive control and reinforcement learning (RL) have emerged as pivotal techniques for optimizing networking systems by dynamically adjusting control policies based on observed network conditions. These methods provide frameworks for handling uncertainties and non-stationarities typical in network environments, enabling efficient resource allocation, traffic management, and protocol adaptation.

A significant focus within this domain has been on gradient-based adaptive control methods. Gradient-based approaches utilize the gradient information of a performance metric or cost function with respect to control parameters to iteratively improve the system's behavior. For example, in network congestion control, gradient descent can adjust sending rates to optimize throughput and minimize delay, effectively adapting to network dynamics. The advantage of these methods lies in their relatively straightforward implementation and convergence properties under smooth cost landscapes.

Reinforcement learning adds an additional dimension by allowing network agents to learn optimal control policies through trial-and-error interactions with the environment, without requiring an explicit model. This is particularly useful in complex or partially observable network scenarios where modeling is infeasible. Model-free RL algorithms, such as Q-learning and policy gradient methods, have been applied to routing, resource allocation, and energy management in wireless networks.

To illustrate, consider a case study in adaptive routing where an RL agent optimizes path selection to minimize latency and packet loss over fluctuating network topologies. Using policy gradient methods, the agent incrementally improves its routing policy based on received rewards signaling successful data delivery, leading to adaptive, efficient routing in real time. This example highlights the synergy between gradient-based optimization and RL strategies in handling dynamic and stochastic network environments.

In addition to isolated techniques, the integration of gradient-based adaptive control within reinforcement learning frameworks has enabled the design of algorithms that combine the sample efficiency of gradient methods with the flexibility of RL. Such hybrid methods demonstrate promising results in network settings requiring rapid adaptation to changing conditions.

In summary, adaptive control and reinforcement learning provide powerful tools for enhancing performance and resilience in networking systems. Gradient-based methods offer a principled approach to continuous adaptation, while reinforcement learning facilitates operating under uncertainty and incomplete knowledge. The combination of these methodologies leads to robust, efficient network control solutions capable of meeting the demands of modern communication infrastructures.

The following sections delve deeper into specific gradient-based algorithms and reinforcement learning case studies, building on the concepts introduced here and illustrating their application across diverse networking scenarios.

6.1 Applications of Reinforcement Learning

Reinforcement learning (RL) has emerged as a crucial methodology for real-time adaptive control in dynamic and wireless networking environments. RL enables optimization of system performance under stochastic and time-varying conditions by learning policies that map network states to appropriate actions through direct interaction with the environment [2, 17, 21, 24, 29, 32**? ? ? ?**]. This capability contrasts with traditional model-based control methods that depend on fixed policies or heuristics, offering autonomous decision-making tailored to the complexities inherent in modern networks.

RL's versatility is demonstrated across diverse networking scenarios, including cellular self-organized networks (SON) and multihop wireless ad hoc systems, where it addresses critical challenges such as interference mitigation, handover optimization, and load balancing [17, 21, 29**? ?**]. In particular, deep RL (DRL) methods leverage deep neural networks to approximate value functions or policies, enabling rapid adaptation without explicit model dependencies. This feature is especially vital in heterogeneous and uncertain wireless contexts, such as multi-band communication networks where differing propagation and interference characteristics complicate control [32].

The effectiveness of RL-based adaptive control systems hinges on accurate and expressive state representations capable of handling high-dimensional and partially observable network environments. Recent literature highlights the synergy between RL and deep learning architectures—including convolutional, recurrent, and autoencoder networks—to extract pertinent features and exploit spatial-temporal correlations, thereby accelerating convergence and improving robustness [24**? ?**]. Additionally, novel analytical frameworks for optimal control on networked systems, such as modal decomposition based on network spectral properties, complement RL approaches by providing interpretable and computationally scalable solutions [17, 21].

Despite such advances, enduring challenges remain. Maintaining robustness amid non-stationary traffic patterns and fluctuating wireless channels demands adaptive generalization capabilities, motivating research into meta-learning and transfer learning to enhance policy reuse across varying network states [29]. Moreover, the deployment of RL in latency-sensitive and resource-constrained environments is limited by the computational overhead of inference and training. To overcome this, efforts focus on lightweight model architectures, hardware acceleration, and hybrid optimization algorithms that blend RL with traditional control methods [2**?**]. Collectively, these developments position reinforcement learning as a transformative tool for autonomous, efficient, and scalable management of increasingly complex wireless networks.

6.2 Deep Reinforcement Learning for Online Adaptation

Deep reinforcement learning (DRL) advances conventional RL by employing deep neural networks as function approximators for policies or value functions. This facilitates effective online adaptation for complex tasks such as decision-making, resource allocation, and adaptive bandwidth management in networking systems [20, 24**? ? ?**]. DRL is particularly valuable in environments characterized by high-dimensional state and action spaces where explicit policy engineering is infeasible, including dynamic spectrum allocation, power control, and admission control [20**?**].

By continuously learning from environmental interactions, DRL enables resource management policies to adapt dynamically to fluctuating network conditions, often outperforming heuristic or static strategies. Hybrid frameworks that integrate DRL with optimization techniques have shown improved convergence rates and enhanced performance in resource-constrained scenarios—for example, federated learning (FL) systems operating under heterogeneous wireless bandwidth constraints [24]. Incorporating domain-specific knowledge into DRL architectures further enhances the balance between exploration and exploitation, which is critical for achieving real-time adaptability.

However, deploying DRL in networking systems introduces challenges such as increased demand for training data, limited interpretability of learned models, risks of overfitting, and instability under non-stationary input distributions [**?**]. Mitigation strategies including experience replay buffers, target networks, and transfer learning are employed to address these issues. Nevertheless, achieving the optimal trade-off between model expressiveness and computational efficiency remains an ongoing area of research, especially given the stringent latency and scalability requirements inherent to next-generation wireless networks.

6.3 Challenges in Policy Design

The design of RL policies for networking systems necessitates a careful balance between exploration and exploitation in environments characterized by non-stationarity, such as wireless networks [18**? ? ?**]. Exploration is essential for discovering improved policies but can degrade performance and increase latency, which are critical concerns in mission-critical or ultra-reliable low-latency communication (URLLC) applications. Conversely, excessive exploitation risks converging to suboptimal policies when network traffic patterns or channel conditions change dynamically.

To mitigate these challenges, state-of-the-art techniques incorporate adaptive exploration rates that adjust based on environmental feedback, uncertainty-aware policy learning to account for incomplete and noisy information, and reward shaping that directly aligns with key networking performance metrics [**? ?**]. The stringent low-latency inference demands in networking impose constraints on model complexity and motivate efficient state acquisition strategies. However, accurate state information remains difficult to obtain due to measurement noise, delays, and partial observability inherent in distributed systems [18**?**].

Robust state estimation thus becomes essential, often realized through filtering methods or latent state representations learned jointly within RL frameworks. Furthermore, to ensure that policies generalize effectively across heterogeneous devices and diverse, dynamic network environments without sacrificing responsiveness, meta-reinforcement learning and multi-agent RL paradigms have been proposed [? ?]. These approaches enable rapid adaptation and cooperative decision-making suited for complex next-generation network architectures, such as AI-assisted network slicing and integrated optical wireless communications, which demand both reliability and agility [? ?].

6.4 Federated and Distributed Reinforcement Learning

Federated reinforcement learning (FRL) and distributed reinforcement learning paradigms have gained significant attention in networking systems due to their potential to enhance privacy, reduce computational burdens, and accelerate convergence within edge-cloud ecosystems [6, 24]. By decentralizing the training process, multiple clients—such as base stations or edge devices—collaboratively learn coordinated policies without sharing raw data, thereby inherently supporting privacy preservation and compliance with regulatory frameworks.

To address communication constraints typical in bandwidth-limited wireless environments, techniques like gradient sparsification and adaptive client selection are employed to reduce communication overhead [6]. State-of-the-art research demonstrates that FRL maintains robust policy performance in the presence of client dropout and heterogeneous data distributions by leveraging mechanisms such as error feedback and weighted aggregation of client updates [6]. Moreover, integrated resource allocation strategies jointly optimize bandwidth and computational resources, which accelerates training convergence and enhances accuracy in FL-based wireless networks [24].

Despite these advancements, key challenges remain, including the synchronization of distributed RL agents, mitigating delays caused by straggler clients, and defending against adversarial attacks. Future research directions focus on developing asynchronous FRL algorithms to improve efficiency, enhancing privacy through stronger mechanisms like differential privacy, and designing scalable architectures capable of handling the complexity of forthcoming 6G networks. Such developments are crucial to fully leverage the potential of FRL in next-generation wireless environments.

6.5 Integration Across Networking Frameworks

The efficacy of RL and adaptive control techniques is significantly amplified when integrated with complementary AI-driven networking frameworks, including network traffic classification, software-defined networking (SDN), and routing optimization [13, 16, 39]. Deep learning-based traffic classification models provide granular insight into network flow characteristics, overcoming limitations of traditional methods by effectively handling encrypted and dynamic traffic patterns. These models enable RL controllers to optimize resource allocation by prioritizing traffic types with enhanced accuracy and adaptability [16].

Within SDN architectures, RL-powered controllers dynamically adjust routing and admission control policies in response to real-time network state changes, thereby improving throughput, reducing latency, and enhancing fault tolerance. AI integration into SDN controllers combines supervised classifiers and deep learning models to enable real-time traffic classification, anomaly detection, and dynamic resource allocation, achieving significant performance gains in 5G and beyond network scenarios [13]. Similarly, RL-based routing protocols adaptively select communication paths to balance load and mitigate congestion and failures, enhancing network resilience and efficiency through continuous learning from traffic dynamics [39].

Such cross-framework synergies promote comprehensive network adaptation strategies in which RL agents leverage enriched contextual information and explicit control channels afforded by SDN. Nonetheless, integrating multiple AI modules introduces challenges including increased computational overhead, interoperability complexities, potential security vulnerabilities, and risks of cascading failures. Addressing these challenges requires concerted efforts toward standardization, development of modular and lightweight AI pipelines optimized for real-time response, and incorporation of explainable AI techniques to maintain transparency and manageability in autonomous network operations. Future research directions also emphasize privacy-aware federated and decentralized learning approaches to enhance scalability and security in heterogeneous network environments.

6.6 Gradient-Based Optimization and Fast Algorithmic Updates

Gradient-based optimization methods constitute a cornerstone in training and adapting artificial intelligence models. These approaches iteratively optimize an objective function by following the gradient of a loss landscape, enabling efficient convergence to optimal or near-optimal solutions. Key techniques include variants of gradient descent such as stochastic gradient descent (SGD), mini-batch gradient descent, and momentum-based methods, which improve computational efficiency and convergence stability.

Fast algorithmic updates leverage structural properties and approximations to accelerate these optimization processes. For instance, algorithms that exploit sparsity, employ adaptive learning rates, or approximate Hessian information enable rapid adaptation with reduced computational overhead. These advancements are crucial in large-scale settings and online learning scenarios where swift model updates are essential.

Integration of efficient gradient computations with fast update mechanisms has led to scalable frameworks, facilitating real-time learning and responsiveness in complex models. These methods continue to evolve, seeking improved trade-offs between computational speed and optimization accuracy, thereby enhancing the practical applicability of AI systems across diverse domains.

6.6.1 Gradient Descent and Variants. Gradient-based optimization constitutes a foundational approach for tuning control and network parameters in large-scale communication and data networks. Traditional gradient descent methods, alongside their accelerated variants, have proven effective for scalable optimization tasks. However, challenges such as high-dimensional uncertainty and the presence of integer decision variables considerably complicate these optimization processes. Specifically, while continuous control parameters allow for convergence guarantees under smoothness assumptions, incorporating integer or mixed-integer variables markedly increases computational complexity and complicates theoretical convergence analyses [34]. This challenge intensifies in settings characterized by large state spaces and expansive uncertainty sets, where computational demands grow exponentially with dimensionality.

To enhance scalability, recent algorithmic refinements such as stochastic gradient methods and adaptive learning rate schemes have been developed. These approaches enable efficient parameter updates even in vast, complex networks [7, 32, 35, 36, 38**? ?**]. Nonetheless, the inherently discrete nature of some optimization variables often necessitates hybrid or relaxation-based techniques, carefully balancing solution quality against computational tractability. The treatment of such integer-constrained optimization problems remains a dynamic research area, stimulating both theoretical advancements and practical algorithm design. Future directions include integrating machine learning-based heuristics and adaptive partitioning methods to better handle uncertainty and mixed-integer decision-making within communication networks.

6.6.2 Hybrid Model- and Data-Driven Gradient Approaches. In recognition of the limitations inherent to purely gradient-driven methods, recent research has advanced hybrid frameworks that integrate model-based insights with data-driven adaptations. These approaches capitalize on structural knowledge encoded within network models while concurrently exploiting real-time or historical data to inform adaptive gradient computations [2**? ?**]. This synergy enhances convergence speed and algorithmic flexibility by dynamically adjusting update rules and mitigating the discrepancies between modeled assumptions and evolving network conditions.

For example, in self-optimized wireless networks (SON), deep learning techniques have been combined with model-based control mechanisms to tune parameters robustly across diverse and variable environments [36]. This hybrid design leverages knowledge graphs and semantic information to enhance the understanding of network states, thereby improving responsiveness and stability. By integrating data-driven semantic representations with traditional model-based optimization, such frameworks address scalability and convergence challenges in complex, real-world systems effectively, and provide robustness against environmental variability.

6.6.3 Fast Algorithmic Update Techniques. The imperative for rapid recalibration of control policies in dynamic and stochastic network environments has motivated the development of fast algorithmic update methods focused on minimizing computational latency. Speed is critical for enabling online learning and real-time control systems [20, 35, 38**? ? ? ? ?**]. Typical methods involve incremental gradient updates, warm-starting solvers with prior solutions, and employing approximation heuristics that provide computationally efficient yet effective parameter adjustments.

In telecommunication networks, these techniques enable systems to respond swiftly to sudden changes in traffic patterns or channel conditions, thereby maintaining strict quality-of-service guarantees and improving resource allocation efficiency [7]. For example, ultra-low latency requirements for emerging paradigms like the Tactile Internet demand update mechanisms with latencies on the order of milliseconds, necessitating highly optimized algorithmic processes. However, striking the right balance between update speed and solution accuracy remains a core challenge: aggressive approximations risk degrading policy performance, while precise updates may incur computational delays incompatible with real-time constraints. To address this tension, recent advances incorporate parallel computation and distributed optimization frameworks that scale efficiently and facilitate timely responsiveness without compromising optimality [35**?**]. These algorithmic innovations are key for realizing adaptive, autonomous network management that can uphold rigorous performance metrics in highly dynamic telecom environments.

6.6.4 Case Studies and Benchmarks. Empirical validations of gradient-based optimization and fast update techniques within real-world telecommunication networks provide critical insight into their practical efficacy and constraints [7, 9, 36**? ?**]. Dynamic optimization strategies employing these methods have yielded measurable improvements in network throughput, latency reduction, and resource utilization across diverse scenarios. For instance, the integration of neural network-based information transfer (NNIT) approaches enables effective adaptation to dynamically changing network environments by transforming historical solutions into promising candidates, accelerating convergence in optimization [**?**]. Similarly, innovative federated learning schemes applying gradient sparsification and adaptive client selection enhance learning robustness and communication efficiency in resource-constrained wireless settings [**?**]. Applications to ultra-low latency scenarios, such as the 5G-enabled Tactile Internet, demonstrate how gradient-informed optimizations contribute to meeting stringent end-to-end delay requirements [7].

Despite these gains, scalability remains a key limitation, especially for very large instances with high heterogeneity and complex constraints. Challenges such as computational overhead and complex problem landscapes impede direct application of classical gradient-based methods, motivating the incorporation of hybrid metaheuristic approaches [9]. Benchmark studies reveal that while gradient-driven frameworks effectively handle moderately sized networks, augmenting them with metaheuristics—such as variable neighborhood search or population-based heuristics—enhances solution quality and exploration capacity for large-scale combinatorial problems. For example, variable neighborhood search algorithms have been successfully applied to complex hub location problems involving competitive pricing and demand shifts, offering robust and scalable performance [9].

These findings underscore the value of modular algorithmic strategies that adaptively integrate gradient information with heuristic exploration, thereby balancing computational efficiency with solution robustness. Such hybrid techniques hold promise for addressing the diverse challenges posed by dynamic, large-scale telecommunication network optimization scenarios.

6.6.5 Neural Network-Based Information Transfer (NNIT). Addressing the dynamic and time-varying nature of network environments necessitates mechanisms that not only optimize current parameters but also systematically leverage historical knowledge to expedite future adaptations. Neural Network-Based Information Transfer (NNIT) exemplifies this approach by learning mappings between evolving network states and corresponding optimal or near-optimal solutions, thus facilitating accelerated convergence and improved adaptability [4, 10, 23**?**].

NNIT architectures typically integrate population-based evolutionary algorithms with neural networks trained to predict promising regions of the solution space or to transform previous high-quality solutions into effective candidates for the current environment [?]. This information transfer effectively accelerates convergence in dynamic optimization problems by harnessing learned patterns of environmental changes, substantially reducing computational overhead. For instance, applications in supply chain decision frameworks—sharing complexity and dynamic characteristics with telecommunications networks—illustrate the computational advantages and robustness brought by NNIT methods [23].

Moreover, recent advances in interpretable AI have been incorporated within NNIT frameworks, enhancing transparency and trustworthiness by providing insight into solution landscapes [10]. This interpretability is vital for deployment in safety-critical and high-stakes network control systems, where understanding decision rationales is as important as optimization performance. Further promising extensions of NNIT include nonlinear stochastic decentralized adaptive controls, highlighting the method's versatility in addressing a broad spectrum of optimization challenges intrinsic to modern networked systems [4].

In summary, this section has delineated how gradient-based optimization techniques, when enriched by hybrid model-data-driven frameworks, rapid update strategies, and intelligent information transfer mechanisms such as NNIT, constitute a robust and versatile toolkit for tackling the profound complexity, scalability, and dynamism characteristic of contemporary and future network control tasks. Each method possesses unique advantages and challenges, motivating integrated algorithmic designs that exploit their complementary strengths to achieve superior optimization performance and adaptive capacity.

7 AI-Enhanced Wireless Networking and Sensing

Advancements in wireless networking and sensing have increasingly leveraged artificial intelligence (AI) techniques to enhance system performance, adaptability, and efficiency. Specifically, the integration of AI with reconfigurable intelligent surfaces (RIS) offers promising avenues for improved wireless communication by dynamically shaping the wireless environment.

In RIS-assisted wireless networks, AI algorithms enable intelligent configuration and control of the surface elements to optimize signal propagation, interference management, and network throughput. For example, reinforcement learning and deep learning models can predict channel state information and determine optimal phase shifts at the RIS, thereby enhancing link reliability and spectral efficiency under varying environmental conditions.

Moreover, AI-driven interference management frameworks utilize real-time data analytics to identify and mitigate interference patterns in dense wireless networks. These frameworks improve resource allocation and network scheduling, facilitating coexistence among multiple users and technologies without significant performance degradation.

Concrete benchmarking in recent studies has demonstrated substantial gains from integrating AI into RIS systems, including enhanced signal-to-noise ratios (SNR), reduced latency, and increased energy efficiency. These performance improvements have been observed across diverse scenarios, such as millimeter-wave communications and multi-user multiple-input multiple-output (MIMO) systems.

Overall, the synergy between AI and wireless sensing technologies empowers adaptive, context-aware networks capable of meeting the stringent requirements of next-generation wireless applications.

7.1 Reconfigurable Intelligent Surfaces (RIS)

Reconfigurable Intelligent Surfaces (RIS) have emerged as a transformative technology enabling programmable manipulation of wireless propagation environments. Unlike conventional wireless systems that treat the environment as a stochastic and uncontrollable factor, RIS impose deterministic control through engineered metasurfaces capable of dynamically altering incident electromagnetic waves. The integration of Artificial Intelligence (AI), particularly machine learning techniques, significantly enhances RIS functionality by enabling adaptive optimization over complex, high-dimensional configuration spaces. Supervised learning methods facilitate channel estimation by mapping measured channel state information (CSI) to optimal RIS configurations. Unsupervised approaches enable feature extraction from unlabeled channel data, improving generalization to dynamic environments. Moreover, deep reinforcement learning (DRL) offers an effective framework for sequential decision-making under uncertainty, enabling adaptive beamforming and resource allocation policies that maximize spectral efficiency and energy savings [6]. The synergy of these AI paradigms empowers RIS to overcome challenges posed by nonlinear and time-varying wireless channels, addressing issues such as high-dimensional configuration spaces, latency, scalability, and imperfect channel information. This combination ultimately achieves more robust and efficient wireless links, boosting coverage and energy efficiency. Future research directions emphasize lightweight distributed AI algorithms, federated learning for privacy preservation, and integration with emerging technologies such as millimeter wave (mmWave), massive MIMO, and edge computing, further advancing intelligent wireless environments [6].

7.2 Benefits and Challenges of RIS

The AI-enabled RIS paradigm offers multiple benefits. These include significantly enhanced spectral efficiency through improved directivity and interference management, augmented energy efficiency by reducing reliance on active radio frequency components, and extension of coverage by enabling signal reflection and focusing beyond line-of-sight barriers. Consequently, RIS facilitates connectivity in dense urban or obstructed environments. Notably, its robustness under imperfect channel conditions stems from AI's capacity to learn and compensate for noise and fading effects, thereby maintaining high communication quality [6].

Nevertheless, these advantages come with inherent challenges. The RIS configuration space is high-dimensional, making exhaustive search or traditional heuristic optimization impractical. Addressing this complexity requires scalable AI algorithms capable of effective dimension reduction while preserving performance integrity. Furthermore, latency and scalability constraints demand lightweight and distributed learning techniques, such as federated learning, to ensure practical deployment [6]. Security concerns also arise because adversaries could exploit RIS for unauthorized eavesdropping or signal manipulation. This risk necessitates the development of secure AI-driven configuration protocols alongside real-time anomaly detection mechanisms [6]. Balancing these benefits and challenges is central to advancing RIS deployment in real-world wireless networks.

7.3 Future Prospects in Wireless AI

Looking ahead, lightweight distributed AI architectures are poised to enable real-time and energy-efficient control of RIS, seamlessly integrated with pervasive wireless networks. Federated learning emerges as a key methodology, facilitating decentralized training of RIS optimization models across edge nodes while safeguarding data privacy and reducing communication overhead. This approach is especially vital given the growing heterogeneity of network topologies and the non-independent and identically distributed (non-i.i.d.) nature of data across devices. The convergence of federated AI with cutting-edge physical-layer technologies—such as millimeter-wave (mmWave) communications, massive multiple-input multiple-output (MIMO) antenna arrays, and edge computing platforms—will drive the advancement of edge intelligence [6]. These integrated frameworks are expected to jointly optimize sensing, communication, and computation resources while adhering to strict latency and energy constraints. To achieve these goals, future algorithmic innovations must carefully balance trade-offs among model complexity, convergence speed, and robustness against channel estimation errors. Moreover, emerging paradigms like neuromorphic computing and online continual learning offer promising avenues to enhance system adaptability in highly dynamic wireless environments.

7.4 Intelligent Interference Management in Perceptive Mobile Networks (PMNs)

Perceptive Mobile Networks (PMNs) represent a sophisticated integration of communication and sensing functionalities, enabling wireless infrastructure to simultaneously support data transmission and situational awareness. Managing interference effectively is vital because sensing waveforms and communication signals share spectral and spatial resources, leading to coexistence challenges. Recent advances have introduced AI-empowered interference mitigation frameworks that harness macro-diversity gains and coordinated beamforming strategies across multi-cell architectures [18]. Specifically, deep learning-based interference prediction models leverage both historical and real-time channel observations to forecast interference patterns accurately. This capability facilitates proactive and dynamic resource allocation, which maximizes the sensing signal-to-interference-plus-noise ratio (SINR) while ensuring that communication quality remains uncompromised. Such dynamic allocation schemes enhance the detection probability in sensing tasks and simultaneously reduce intra- and inter-cell interference, effectively balancing the dual objectives of communication and sensing within PMNs.

Despite these promising developments, several critical challenges remain to be addressed for practical and scalable PMN deployments. Key issues include maintaining low-latency inference necessary for real-time system adaptation, acquiring accurate channel state information in highly mobile user environments, and designing scalable cooperation schemes among multiple base stations without incurring prohibitive signaling overhead [18]. Overcoming these challenges is fundamental to realizing mature PMNs capable of harmonizing sensing and communication functions robustly. Future research directions highlighted in the literature emphasize the incorporation of multi-modal sensing, federated learning approaches for privacy preservation, and mechanisms to enhance robustness in dynamic network environments [18]. Overall, AI-driven intelligent interference management frameworks significantly enhance sensing performance while maintaining reliable communication within integrated sensing and communication networks.

7.5 Achievements and Challenges

AI-driven wireless sensing techniques have demonstrably enhanced detection probabilities and mitigated sensing interference, particularly through cooperative interference management strategies leveraging coordinated multipoint processing and macro-diversity [12, 18, 19]. These improvements enable robust detection performance in dense and heterogeneous network environments characterized by significant interference and channel uncertainty. Furthermore, privacy preservation has emerged as a critical concern within networked sensing, since sensitive environmental or user data may be indirectly inferred through side-channel attacks in cooperative frameworks. Recent studies propose privacy-aware AI algorithms that integrate differential privacy techniques and federated learning to alleviate these risks without significant deterioration of sensing performance [15, 18].

Robustness to heterogeneity in hardware capabilities, channel conditions, and user mobility patterns remains another outstanding challenge. Techniques incorporating model adaptation, transfer learning, and fast adaptation methods such as Zero-Shot Lagrangian Updates have shown promise in addressing such variability but require extensive validation in diverse real-world settings [8**?**]. Consequently, bridging the gap between theoretical AI frameworks and practical deployment necessitates continued research focused on scalable cooperation protocols, secure architectures, and self-tuning training paradigms that can operate reliably across heterogeneous wireless environments.

In summary, AI-enhanced wireless networking and sensing via RIS and intelligent interference management mark the advent of programmable, efficient, and context-aware wireless systems. This progress hinges on the intricate interplay of algorithmic sophistication—encompassing supervised, unsupervised, reinforcement, and federated learning—and physical-layer innovations [6]. Collectively, these advances establish a rich interdisciplinary frontier poised to shape future wireless ecosystems [6, 8, 12, 15, 18**?** , 19].

8 Explainability, Interpretability, and Trust in AI-Controlled Telecommunication Systems

Explainability and interpretability are critical for fostering trust in AI-controlled telecommunication systems, enabling stakeholders to comprehend, validate, and trust automated decisions. In operational telecom environments, explainability helps engineers and regulators to trace the rationale behind AI actions, improving reliability and compliance.

For instance, in multi-agent reinforcement learning-based network management, explainability frameworks such as attention mechanisms and feature attribution methods have demonstrated how agents coordinate resource allocation, offering insights that help network operators validate system behavior and detect anomalies. Such concrete frameworks provide interpretable feedback on agent cooperation patterns, directly impacting service quality and robustness.

Moreover, explainability methods contribute to regulatory compliance in telecommunications by aligning AI model decisions with established governance standards like GDPR and AI Act guidelines. Transparent AI decision-making processes ensure that automated actions can be audited for fairness, data privacy, and accountability, which is essential for meeting telecom regulatory requirements.

In practice, case studies from telecom operators show how interpretable AI has been applied to optimize traffic routing while maintaining explainable decision logs that satisfy internal compliance audits. These examples highlight the direct operational benefits of integrating explainability into AI systems.

To summarize, explainability in AI-controlled telecom systems bridges the gap between complex algorithmic decisions and stakeholder understanding, supporting trustworthy deployment that meets both technical and regulatory expectations.

8.1 Importance of Transparent AI Decision-Making

The incorporation of artificial intelligence (AI) in adaptive telecommunication and control systems introduces an unprecedented level of complexity, making transparent decision-making an essential attribute to cultivate trust among stakeholders and ensure compliance with evolving regulatory frameworks. Transparency serves as a cornerstone for certifying that AI-driven actions conform to desired operational, ethical, and legal standards, particularly within critical infrastructure sectors such as telecommunications [? ?]. The establishment of trust is inherently linked to the system's ability to provide interpretable rationales behind its decisions, thus enabling operators to verify, audit, and justify automated processes [?]. This transparency is crucial in highly dynamic and heterogeneous network environments, where AI models must continually adapt to varying contextual conditions without compromising reliability and safety [18]. Additionally, emerging AI governance regulations emphasize explainability as a fundamental principle, compelling telecommunication systems to exhibit clarity in their decision logic and mitigate risks associated with opaque AI behavior [24]. As AI-driven network management faces challenges such as balancing computational complexity with real-time processing requirements and ensuring robustness against adversarial conditions, transparent models help address these by revealing decision pathways and confidence levels. Consequently, transparent AI not only bolsters user confidence but also facilitates regulatory approvals and promotes the widespread adoption of AI-enhanced telecommunication technologies.

8.2 Methods for Interpretability and Explainability

Attaining interpretability within AI-driven telecommunication systems necessitates the integration of explainability mechanisms directly into core optimization and learning frameworks. Reinforcement learning (RL), a dominant paradigm for dynamic resource allocation and control, often poses challenges to transparency due to the complexity inherent in value function approximations and policy networks. Modern methodologies address this opacity through model-agnostic interpretability techniques and surrogate models that extract actionable insights from trained RL agents. These approaches clarify decision rationales by illuminating factors such as state-action value contributions and reward attributions [2?]. Embedding explainability frameworks within optimization algorithms further enhances understanding by elucidating solution trajectories and facilitating sensitivity analyses. This enables operators to comprehend how variations in system parameters influence resource management outcomes [20?]. Hybrid frameworks that couple deep learning with symbolic reasoning have been advanced to strike a balance between predictive performance and interpretability, thereby supporting effective human-in-the-loop validation [32]. Moreover, attention mechanisms and gradient-based attribution techniques embedded in neural network architectures highlight key features that influence AI decisions across tasks like traffic management, fault diagnosis, and spectrum allocation [?]. Collectively, these methods constitute a comprehensive toolset that mitigates the inherent opaqueness of sophisticated AI models, enhancing operational transparency while preserving system efficacy.

8.3 Future Directions

Looking forward, the evolution of explainable AI (XAI) within telecommunication and control systems is poised to tackle current limitations and emerging challenges through several pivotal advancements. A primary focus lies in the development of privacy-preserving XAI techniques that reconcile the need for transparency with strict data confidentiality requirements prevalent in telecommunication networks [18]. Federated explainability exemplifies such approaches by enabling interpretability without centralizing sensitive data, thereby aligning with privacy regulations and operational constraints.

Additionally, enhancing interpretability frameworks to be resilient against adversarial manipulation is imperative. Opaque AI systems are vulnerable to exploitation in hostile environments, jeopardizing network security and reliability [24]. Robust XAI methodologies must integrate anomaly detection and adversarial robustness to protect explanations from malicious interference [25].

Furthermore, scaling explainability to accommodate large-scale communication and control architectures—which span cloud, edge, and device layers as well as multi-agent systems—demands modular, hierarchical interpretation mechanisms capable of contextualizing AI decisions across multiple abstraction levels [5]. Cutting-edge AI paradigms such as multi-agent reinforcement learning and large language model-driven network intelligence require innovative explainability frameworks that capture complex cross-agent interactions and provide natural language interpretability, respectively.

To better guide research and practical implementation, Table 3 summarizes key future directions, associated challenges, and potential solutions in developing XAI for telecommunication and control systems. Practical pathways include leveraging federated learning to preserve data privacy, employing multi-agent models for distributed intelligence, and optimizing lightweight XAI models suitable for edge deployment to meet real-time constraints. Methodological frameworks should incorporate modular design and hierarchical explanations to manage complexity across heterogeneous network layers. The interplay between AI, control theory, and wireless technologies forms an interdisciplinary synergy essential to addressing emerging operational and security challenges.

The integration of these approaches will ultimately reinforce trustworthiness, enhance operational safety, and ensure regulatory compliance for AI-controlled telecommunication systems amid escalating complexity and heterogeneity. Anticipated disruptive innovations include agentic AI embedded with LLM-driven agents for autonomous fault detection and self-healing [5], and seamless AI integration within Open RAN architectures to enable adaptive, explainable control loops enhancing network resilience [25]. These paradigm shifts will foster transparent, robust, and efficient AI-driven telecommunications, facilitating a new generation of intelligent, self-optimizing networks.

8.4 Applications in Telecommunications and Networking

This section presents an overview of the key applications of artificial intelligence (AI) in telecommunications and networking, outlining the objectives, scope, and challenges inherent to these fields. The primary objective of this overview is to systematically examine how AI techniques contribute to enhancing network performance, reliability, and security, with a focus on major application domains such as network optimization, traffic management, resource allocation, and fault detection.

Table 4 summarizes the main AI application areas, associated challenges, and common evaluation metrics used within telecommunications and networking.

AI techniques have been extensively applied for network optimization by learning from historical data to dynamically adjust configurations, thereby improving throughput and reducing latency, while accounting for the heterogeneous and large-scale nature of modern networks. Traffic prediction models leverage machine learning to anticipate network congestion and enable proactive management, addressing challenges related to data volatility and sparsity. Resource allocation benefits from AI's capability to solve complex optimization problems under multiple constraints, promoting efficient and fair utilization of network resources. Additionally, AI-driven fault detection systems are designed to identify and diagnose anomalies within network operations, overcoming issues with imbalanced datasets and minimizing false alarms.

Although various approaches exist, including rule-based systems and traditional statistical methods, AI offers significant advantages in adaptability and scalability. However, a critical comparison reveals that, while some methods achieve higher accuracy, they may incur greater computational overhead, necessitating a trade-off analysis based on deployment requirements.

The discussion integrates these perspectives to provide a cohesive narrative of AI's transformative role in telecommunications, emphasizing the need for continued research to address scalability and interpretability challenges. Transitioning between topics, the presentation highlights how these AI applications are interrelated and collectively contribute to the robustness of modern communication networks.

8.4.1 AI-Driven Adaptive Control Applications. The integration of artificial intelligence (AI) techniques, particularly machine learning (ML) and deep learning (DL), has substantially transformed adaptive control mechanisms in telecommunications networks. These advancements have empowered functions such as dynamic resource allocation, congestion management, fault tolerance, and traffic prediction. Deep learning architectures—including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs)—exhibit remarkable capabilities in extracting complex spatial-temporal patterns from network data, thereby improving both predictive accuracy and control responsiveness [2, 7, 24, 35**? ? ? ? ? ?** , 36].

This progress reflects a paradigmatic shift from traditional static, heuristic-based methods toward data-driven adaptive frameworks, capable of learning from extensive historical and real-time network states. Reinforcement learning (RL), for instance, has been effectively applied to dynamic radio resource allocation, optimizing trade-offs between throughput and latency in heterogeneous wireless environments [36**?**]. Deep learning models such as CNNs and RNNs have demonstrated superior performance in traffic prediction by leveraging nonlinear dependencies and temporal correlations within network flows, outperforming classical statistical predictors [2**? ?**]. Additionally, GANs are instrumental in synthetic data generation and anomaly detection, thereby enhancing network fault management through identification of rare events and coping with sparse failure data [7**?**].

Nonetheless, deploying these sophisticated models entails significant challenges. The computational overhead associated with training and inference of complex deep learning models can impede real-time application, particularly in large-scale or resource-constrained edge environments [2**?**]. Federated learning (FL) has emerged as a promising solution to these challenges by enabling distributed model training while preserving data privacy and reducing communication overhead. Robust FL frameworks incorporate adaptive client selection, gradient sparsification, and efficient bandwidth allocation to address client dropout, limited bandwidth, and heterogeneous device capabilities [2**?**]. Moreover, generalization remains a critical issue, as models must adapt continuously to heterogeneous and evolving network conditions, requiring efficient retraining or adaptation mechanisms [**?**]. Privacy concerns, arising from the collection and processing of extensive network data, drive the adoption of privacy-preserving learning frameworks such as federated learning, which maintains data locality while collaboratively improving model performance [7, 35]. Despite these challenges, AI-driven adaptive control substantially enhances network self-optimization, reducing operational expenditures while improving quality of service (QoS) [24**?**].

Table 3: Summary of Future Directions, Challenges, and Solutions in Explainable AI for Telecommunications and Control

Future Direction	Challenges	Potential Solutions
Privacy-preserving XAI	Data confidentiality, regulatory compliance	Federated explainability, decentralized interpretation [18]
Adversarially robust explanations	Vulnerability to attacks, security risks	Integration of anomaly detection, adversarial training [24, 25]
Scalable, hierarchical interpretability	Multi-layer network architectures, complexity	Modular frameworks, hierarchical explanation models [5]
Multi-agent and LLM-driven XAI	Cross-agent interaction complexity, computational overhead	Agentic AI frameworks, lightweight LLM optimization [5]
Real-time edge deployment	Latency, resource constraints	Lightweight XAI models, hardware accelerators [25]
Interdisciplinary synergy	Integration of AI, control, wireless	Modular, layered frameworks bridging disciplines

Table 4: Summary of AI Applications, Challenges, and Evaluation Metrics in Telecommunications and Networking

Application Area	Challenges	Evaluation Metrics
Network Optimization	Scalability, real-time processing, heterogeneous data sources	Throughput, latency, resource utilization
Traffic Prediction and Management	Dynamic traffic patterns, data sparsity	Prediction accuracy, RMSE, MAE
Resource Allocation	Complex constraint satisfaction, fairness among users	Resource efficiency, fairness indices
Fault Detection and Diagnosis	Imbalanced data, anomaly identification	Detection rate, false positives, precision, recall

8.4.2 *Evaluation Metrics and Benchmarking.*

Comprehensive evaluation of adaptive algorithms in realistic communication and wireless scenarios necessitates metrics that integrate both classical network performance and AI-specific qualities, including robustness and semantic fidelity. Traditional benchmarks—such as throughput, latency, packet loss, and bit error rate (BER)—remain fundamental indicators of network health [2**?**]. However, the emergence of semantic communications emphasizes the need for novel metrics that transcend bit-level correctness by quantifying the semantic integrity of transmitted data.

In this context, semantic similarity metrics (e.g., BLEU scores when applied to textual or annotated image data) have been proposed to assess the fidelity of content following AI-enhanced compression and error correction schemes [24, 36**?**]. Such metrics align with the semantic communication framework combining deep learning with knowledge graphs that enhances semantic context consistency and error correction [36]. Incorporating these metrics addresses the inadequacies of strictly physical-layer evaluations, realigning optimization objectives with end-user perceived quality. Furthermore, adaptive algorithms are evaluated with respect to computational efficiency, convergence speed, and resilience to adversarial perturbations or network faults [2, 7**?**]. For example, latency models capturing transmission, propagation, processing, queueing, and retransmission delays are critical in Tactile Internet applications requiring ultra-low latency and high reliability [7].

Despite these advancements, standardized benchmarks leveraging established datasets and simulation frameworks remain sparse, impeding cross-comparison and reproducibility. This landscape highlights an urgent need for comprehensive evaluation frameworks that synergize physical, semantic, and operational performance measures, thereby establishing uniform criteria for assessing AI-driven network control across diverse wireless and edge-cloud environments [24]. Future evaluation protocols must furthermore balance trade-offs between accuracy and latency, consider interpretability of AI models, and address challenges like privacy and computational overhead in real-time processing [24**?**].

8.4.3 *Edge and Cloud Synergistic AI Solutions.*

The exponential growth of network data and the imperative for ultra-low-latency services have precipitated architectures that synergistically combine edge computing with cloud intelligence. By partitioning AI workloads between decentralized edge nodes and centralized cloud platforms, such hybrid frameworks optimize latency constraints while leveraging substantial computational resources to enhance network intelligence and robustness [6, 20, 24, 38**? ?**].

At the edge, AI models conduct real-time inference and process local data, which is critical for latency-sensitive applications including the Tactile Internet and autonomous vehicle control [7]. To accommodate resource limitations inherent to edge devices, lightweight deep learning models or compressed representations are employed [20**?**]. Concurrently, cloud-based AI systems aggregate global network insights, handle extensive training tasks, and disseminate updated models back to the edge, facilitating continuous learning and adaptive responsiveness [38**?**].

Federated learning exemplifies this edge-cloud synergy by enabling decentralized model training across heterogeneous devices without compromising data privacy or incurring prohibitive communication overhead [7]. Nonetheless, this approach faces challenges such as device heterogeneity, fluctuating wireless channel conditions, and synchronization complexities, which can impair model convergence and necessitate sophisticated resource allocation strategies that jointly optimize computation and communication [7**?**].

In addition, distributed AI architectures grapple with security vulnerabilities including adversarial attacks and data poisoning, prompting research into robust model design and trustworthy deployment at scale [6, 24]. Hence, the interplay between edge and cloud computing represents a crucial frontier for achieving intelligent, responsive, and secure network control in next-generation wireless systems.

8.4.4 *Resilient Control of Cyber-Physical Systems.*

Cyber-physical systems (CPS) underpinning telecommunications infrastructure require resilient control strategies capable of maintaining reliable operation despite actuator faults and sophisticated cyber attacks.

A prominent approach involves neural network-based finite-time resilient control methodologies for nonlinear time-delay systems, utilizing radial basis function neural networks (RBFNNs), advanced observer designs, and Lyapunov–Krasovskii functionals to ensure robustness and rapid convergence [3].

This framework models the system's unknown nonlinearities and fault signals through RBFNNs, where the nonlinear dynamics $f(x(t), x(t-\tau))$ are approximated as $W^T \Phi(x(t), x(t-\tau)) + \varepsilon$. The unknown weights W are estimated online using adaptive laws to compensate for uncertainties, delays, and disturbances. Concurrently, a designed observer estimates both the system states and fault signals, effectively handling discrepancies caused by unknown false data injections and measurement inconsistencies. This dual estimation enhances fault detection and isolation capabilities within the control loop [3].

The resulting adaptive control laws combine these state and fault estimates to guarantee finite-time convergence of the system states and estimation errors. This finite-time stabilization markedly improves the speed and robustness over traditional asymptotic control approaches. The theoretical foundation rests on Lyapunov–Krasovskii functionals tailored to incorporate time delays, which provide rigorous guarantees of closed-loop system stability despite uncertainties.

By integrating adaptive neural control with observer-based fault diagnosis and robust stability theory, this paradigm enables real-time mitigation of faults and cyber attacks through dynamic control input adjustments. It thus establishes a comprehensive resilience framework for CPS, addressing both component degradation and malicious interventions effectively. Nonetheless, ongoing challenges remain, such as extending these methods to stochastic systems with time-varying delays, accommodating multi-actuator and sensor configurations, and validating performance through hardware-in-the-loop experiments that emulate practical operational conditions [3].

8.4.5 Open Research Frontiers. Emerging research trajectories in telecommunications emphasize multi-agent systems, stochastic modeling, and hardware-in-the-loop simulation platforms as pivotal frontiers advancing adaptive control and AI integration [3]. Multi-agent frameworks foster scalable, decentralized decision-making across heterogeneous network entities, enhancing robustness and adaptability in complex, dynamic environments. The incorporation of stochastic models better captures wireless channel variability, environmental uncertainties, and human-in-the-loop behaviors, thereby necessitating adaptive control methodologies that judiciously balance performance against risk [3].

Hardware-in-the-loop platforms constitute indispensable testbeds that bridge algorithmic development and realistic hardware constraints, including timing delays, sensor inaccuracies, and communication limitations. These platforms facilitate expeditious prototyping, validation, and fine-tuning of resilient control schemes under conditions closely emulating actual network environments [3].

Complementary research efforts focus on explainable AI paradigms for network control to ensure transparency and interpretability, and on integrating reinforcement learning with classical control theory to combine long-term policy optimization with guaranteed system stability [24]. Addressing computational complexity through model compression, distributed AI frameworks, and energy-aware algorithms is also critical, especially for deployment within resource-constrained edge environments [6]. Collectively, these avenues herald transformative potential for next-generation telecommunications systems that are intelligent, autonomous, and resilient.

9 Cross-Cutting Themes and Integration Considerations

This section synthesizes the key challenges, solutions, and interactions across the various themes discussed in preceding sections, highlighting their intersections through concrete examples and case studies. By examining these cross-cutting issues, we aim to provide a more cohesive understanding of how different AI components and methods integrate, addressing their combined limitations and opportunities.

A primary challenge common across multiple themes is the trade-off between scalability and model interpretability. For instance, large-scale transformer models achieve impressive performance on natural language processing tasks but often sacrifice transparency in decision-making. This issue intersects with ethical AI considerations, where explainability is crucial for user trust and accountability. An example is the deployment of AI in healthcare diagnostics, where complex models must provide rationale for predictions to meet regulatory standards and clinical acceptance.

Another pervasive theme is the integration of learning paradigms, such as combining supervised learning with reinforcement learning to create robust agents capable of adapting in dynamic environments. A case study from autonomous driving illustrates this integration: perception modules trained on labeled images are combined with reinforcement learning policies that adapt to real-time driving conditions. This integration presents technical challenges such as aligning the learning objectives and managing the propagation of uncertainty, underscoring the need for unified frameworks.

Data privacy and security concerns also cut across themes. Federated learning techniques, originally developed to ensure privacy-preserving model training, have seen widespread application from mobile device personalization to collaborative healthcare research. The cross-cutting challenge lies in balancing data utility with privacy guarantees and computational efficiency. For example, while privacy-preserving federated methods limit data sharing, they can introduce biases if client participation is uneven, necessitating new algorithmic safeguards.

These examples demonstrate that cross-cutting themes are not isolated but deeply interconnected, requiring integrated approaches. Critically, many current solutions still address these challenges in siloed ways, limiting their efficacy in real-world applications where multiple themes converge. Future research must prioritize frameworks that jointly address scalability, interpretability, privacy, and adaptability.

In summary, the interplay of these cross-cutting themes points to the importance of holistic system design, where the limitations and strengths of individual components are balanced within an integrated architecture. Such approaches will better meet the complex demands of practical AI deployment.

9.1 Scalability and Real-Time AI Inference

The deployment of artificial intelligence (AI) within telecommunications demands scalable solutions capable of real-time inference across heterogeneous and dynamically evolving network environments. This requirement is challenging due to the high computational complexity of contemporary AI models, such as deep neural networks and large language models (LLMs), coupled with the variability of network resources and stringent latency constraints [6, 13, 39?]. For instance, incorporating AI into Open RAN architectures mandates efficient processing pipelines that adhere to tight timing budgets, enabling rapid control loop adaptations critical for tasks like spectrum management and interference mitigation [18].

Edge-cloud collaborative frameworks offer distinct advantages by distributing AI inference workloads to optimize latency and computational resource utilization; however, they face scalability constraints especially when coordinating multiple edge nodes or base stations [6]. To overcome these limitations, scalable AI architectures must integrate a combination of algorithmic compression techniques, model pruning, and hardware acceleration, alongside modular and parallel design principles. Additionally, synchronization and consistent model updating, particularly within federated or distributed learning paradigms, constitute significant challenges that affect maintaining real-time performance [13].

Addressing these complexities is especially crucial for perceptive mobile networks (PMNs), where AI-driven interference management and sensing require dynamic adaptation to fluctuating network loads without compromising communication quality [39]. Advanced AI frameworks in PMNs exploit coordinated beamforming and deep learning-based interference prediction across multi-cell architectures to maximize sensing signal-to-interference-plus-noise ratio (SINR) while preserving communication reliability [18]. Moreover, real-world implementations demonstrate that AI-enabled routing and traffic management can improve throughput and latency by adapting to network conditions in real time [39].

Overall, realizing scalable and real-time AI inference in telecommunications necessitates integrating lightweight, robust AI models optimized for dynamic network environments, efficient edge-cloud collaboration, and real-time synchronization mechanisms to fully harness the potential of AI for next-generation networks.

9.2 Privacy Preservation Strategies

Preserving privacy is a critical concern in telecommunications due to the sensitive nature of transmitted data and strict regulatory frameworks. Prominent strategies for privacy preservation include federated learning, edge computing, and lightweight distributed AI methods that localize data processing, thereby reducing exposure risks [6, 13, 18, 24]. Federated learning enables collaborative model training across decentralized entities while keeping raw data on-site, effectively mitigating risks inherent in centralized data collection [6]. Despite its advantages, federated learning faces challenges such as communication overhead, the heterogeneity of client devices, and susceptibility to inference attacks. Edge computing complements these approaches by performing AI inference near data sources, which reduces both the privacy attack surface and communication latency [13]. Deploying lightweight AI models at the edge—through techniques like quantization and knowledge distillation—further enhances privacy protection while improving computational efficiency [24]. Designing algorithms that rigorously balance privacy and model utility remains complex, often requiring integration of encryption methods, differential privacy mechanisms, and robustness against adversarial threats. Additionally, the rapid evolution of AI within open, multi-vendor ecosystems accentuates the need for standardized frameworks that embed stringent privacy safeguards while maintaining interoperability across diverse network infrastructures [13, 18].

9.3 Explainability and Trust

Establishing trust and transparency in AI-driven telecommunications systems is essential, given that automated decisions directly affect service quality and network reliability [18, 24? , 25]. Explainability techniques empower operators and stakeholders to interpret AI decision-making processes, identify erroneous outputs, and align these decisions with domain expertise. For instance, incorporating explainable AI within network management systems elucidates the rationale behind resource allocation or anomaly detection outcomes, thereby fostering confidence and enabling effective human-in-the-loop oversight [?]. Nonetheless, the predominant use of complex deep learning models often results in opaque, black-box systems, presenting a fundamental trade-off between prediction accuracy and interpretability [25]. Research advances include inherently interpretable models and post hoc explanation methods such as attention visualization, feature attribution, and counterfactual reasoning, which are progressing but remain immature in comprehensive telecom applications [24]. Moreover, explainability is critical for regulatory compliance verification and mitigating risks from erroneous AI decisions that could propagate cascading network failures [18]. In Open RAN and 6G networks, AI integration highlights additional trust challenges due to distributed and multi-agent learning frameworks, necessitating transparent AI mechanisms to ensure security, fault tolerance, and interoperability [25]. Therefore, enhancing AI system transparency remains a vital challenge that underpins systemic trust and responsible deployment in telecommunications.

9.4 Interoperability and Standardization Challenges

The integration of AI into telecommunications networks faces considerable interoperability and standardization challenges arising from diverse multi-vendor equipment, heterogeneous protocol stacks, and disparate technology domains [13, 18, 25]. Fragmented AI models and incompatible data schemas hinder seamless AI-driven control and coordination across Open RAN components, including radio units (RU), distributed units (DU), and centralized units (CU) [18]. The lack of unified AI interfaces and standardized telemetry data formats creates barriers to implementing distributed intelligence and federated learning, constraining scalability and limiting cross-vendor collaboration [13]. Additionally, varying regulatory requirements and privacy policies across jurisdictions and operators compound the fragmentation in AI adoption. Early efforts by standardization bodies to define AI-specific protocols, interfaces, and data representations are ongoing but remain in initial stages, despite their critical role in enabling modular, plug-and-play AI capabilities and ensuring reproducibility and reliability of AI-enhanced network functions [25]. Addressing these interoperability gaps demands interdisciplinary initiatives focused on harmonizing software stacks, unifying data semantics, and developing AI models robust to domain shifts and heterogeneity across multi-technology ecosystems.

9.5 Security and Robustness

As AI technologies permeate critical telecommunications infrastructure, ensuring security and robustness against adversarial threats, data poisoning, and erroneous model outputs is fundamental to operational reliability [5, 18, 24]. AI models are vulnerable to attacks exploiting weaknesses in training data, model parameters, and inference processes, potentially resulting in misclassifications, compromised routing decisions, or degradation of service quality. Such attacks are especially harmful in complex AI-enabled networks where flawed decisions may cascade, causing widespread disruptions across multiple layers and services [24]. Defensive strategies include adversarial training, development of robust model architectures, sophisticated anomaly detection systems, and hierarchical control mechanisms equipped with fallback options to mitigate AI failures [5]. Additionally, integrating explainability aids in the early detection of abnormal AI behaviors, while federated learning frameworks can minimize insider threats by limiting data exposure [18]. Nonetheless, achieving security without compromising performance or scalability remains challenging, particularly within resource-constrained edge environments typical in 5G and subsequent network generations [5].

Recent advances demonstrate the promise of agentic AI approaches leveraging large language models (LLMs) embedded within flexible Open Radio Access Network (O-RAN) architectures to enhance resilience. Such LLM-driven agents improve fault detection accuracy and mitigation success by autonomously monitoring network telemetry, interpreting complex faults through natural language understanding, and executing self-healing actions [5]. Experimental evaluations show fault detection accuracy rising from 78% to 95% and mitigation success increasing from 70% to 91%, alongside significant downtime reduction and throughput degradation improvements. However, these benefits must be balanced against challenges including computational overhead, potential erroneous decisions, security risks, and interoperability among multi-vendor environments, motivating hierarchical agent design and continuous validation frameworks [5].

Therefore, designing AI systems with intrinsic robustness, continuous validation processes, and adaptive security measures is imperative for their trustworthy integration into future telecommunication infrastructures. Scalability requires efficient AI architectures combining algorithmic compression, hardware acceleration, and modular design to meet real-time inference demands, while privacy preservation leverages federated learning, edge computing, and lightweight models balancing privacy-utility trade-offs under regulatory constraints [18, 24]. Explainability remains critical for building trust, auditability, and regulatory compliance amidst opaque deep models [24], and interoperability challenges arising from multi-vendor heterogeneity necessitate standardized AI interfaces and data formats supporting scalable collaboration [5]. Security demands robust defenses against adversarial attacks and errors, incorporating fallback mechanisms and continuous validation without sacrificing system performance.

Collectively, these emerging techniques and frameworks underscore that ensuring security and robustness in AI-driven telecommunications requires a multilayered approach combining advanced AI methodologies, network architecture flexibility, and rigorous operational safeguards.

10 Synthesis and Future Directions

The surveyed literature indicates a rapidly evolving landscape at the intersection of artificial intelligence, control theory, and wireless communication technologies. To guide future research and practical implementations, it is essential to synthesize the key methodological advancements and outline potential disruptive paradigm shifts, as well as address challenges encountered when transitioning from theory to real-world applications.

10.1 Methodological Contributions and Frameworks

The integration of AI techniques with control and wireless systems has given rise to novel frameworks that enable adaptive, resilient, and efficient operation in complex environments. Future research should focus on developing standardized methodological frameworks that unify these interdisciplinary approaches to facilitate comparison, reproducibility, and scalability. Such frameworks must incorporate robustness to uncertainties, real-time adaptability, and data-driven optimization while maintaining theoretical guarantees from control and communication domains.

10.2 Practical Implementation Pathways and Challenges

While theoretical advancements abound, practical implementation of AI-enabled control and wireless systems faces numerous challenges. These include computational resource constraints, latency requirements, robustness to dynamic environments, and integration with legacy infrastructure. Future efforts should prioritize the design of scalable algorithms compatible with edge computing and distributed architectures. Additionally, managing privacy, security, and ethical considerations will be paramount as AI systems are deployed in sensitive applications.

10.3 Potential Disruptive Innovations and Paradigm Shifts

Emerging trends suggest several potential disruptions in the field. The convergence of AI, control, and wireless communication technologies may lead to self-organizing and self-optimizing networks that dramatically improve efficiency and responsiveness. Paradigm shifts may also arise from the fusion of model-based and data-driven approaches, yielding hybrid methods that leverage the strengths of both. Further exploration into cross-layer design integrating AI at multiple system levels could transform traditional system architectures.

10.4 Comparative Summary of Key Approaches

To facilitate a clear understanding of the relative merits and limitations of the approaches discussed throughout this survey, Table 5 summarizes the principal characteristics, challenges, and application domains of representative methods.

10.5 Interdisciplinary Synergies

The symbiotic relationship between AI, control theory, and wireless communication will continue to deepen, leading to innovative system designs that transcend domain-specific limitations. Researchers should foster interdisciplinary collaborations that leverage advances in sensing, computing, and theoretical analysis to create holistic solutions. Emphasizing the synergy among these fields will accelerate progress towards autonomous, efficient, and resilient systems.

In summary, the roadmap for future work involves consolidating methodological advances into unified frameworks, addressing practical implementation challenges, anticipating paradigm shifts driven by novel hybrid and adaptive approaches, and reinforcing interdisciplinary collaborations. By targeting these directions, the community can advance the integration of AI with control and wireless technologies towards impactful real-world deployments.

10.6 Synergies Across AI, Resilient Control, and Wireless Technologies

The fusion of artificial intelligence (AI), resilient control strategies, and wireless technologies has driven substantial progress toward real-time, adaptive, and secure network management within dynamic and uncertain environments. A salient example of this interdisciplinary synergy is the development of adaptive neural network finite-time control methods designed for nonlinear systems with unknown time delays, actuator faults, and false data injection attacks. These frameworks employ radial basis function neural networks to approximate unknown nonlinearities and utilize online adaptive laws to estimate network weights and fault parameters in real-time. Coupled with observer-based fault detection mechanisms, this integration ensures fault-tolerant operations and finite-time convergence of state and estimation errors, significantly enhancing system resilience compared to traditional asymptotic control methods [3].

In parallel, AI has invigorated wireless communications through advanced paradigms such as Perceptive Mobile Networks (PMNs). These networks leverage coordinated beamforming and deep learning algorithms to predict and mitigate interference in complex multi-cell environments. By dynamically allocating resources based on learned interference patterns, these methods maintain communication quality while substantially improving sensing accuracy under heterogeneous, interference-prone conditions. This dynamic adaptation facilitates robust wireless resource orchestration amid fluctuating network loads, thereby enabling enhanced situational awareness and network performance [**?**].

Further extending this ecosystem, AI-driven optimization of reconfigurable intelligent surfaces (RIS) provides a powerful approach to shaping the wireless propagation environment. By learning mappings from channel state information to effective RIS configurations, these AI-empowered systems achieve improved spectral efficiency and robustness in uncertain, time-varying scenarios. This integration exemplifies how AI, control theory, and advanced wireless technologies collectively enable networks capable of context-aware, adaptive decision-making and resilient operation despite inherent cyber-physical uncertainties [18].

10.7 Critical Enablers

A set of pivotal enablers underpins the convergence of AI, control, and wireless technologies. These enablers not only address fundamental technical challenges but also represent active research areas with diverse approaches and trade-offs, as summarized in Table 6.

Below, we provide a critical discussion of each enabler with examples from current studies and highlight open research gaps:

Federated Learning. This approach facilitates collaborative model training across decentralized nodes without raw data exchange, addressing severe privacy concerns in wireless networks. For instance, in Open RAN contexts, federated learning enables dynamic spectrum management and fault detection by aggregating local AI insights [6]. However, challenges such as communication overhead, non-iid data distributions, and convergence difficulties remain points of debate in the field.

Privacy-Preserving AI. Tightly coupled with federated learning, privacy-preserving mechanisms—including differential privacy, secure multi-party computation, and homomorphic encryption—ensure that sensitive user and network information is secured. The trade-offs between privacy strength and model performance demand carefully balanced solutions, and the literature reveals ongoing controversy regarding the best approaches for different wireless scenarios.

Edge Intelligence. By decentralizing processing to network edge nodes, edge intelligence mitigates latency and bandwidth constraints inherent to centralized cloud architectures. Real-time tasks like interference mitigation and localized adaptive control benefit from this setup. Nonetheless, resource limitations and the need for coordinated inference across heterogeneous edge nodes introduce system design complexities and inconsistency risks.

Explainable AI. Given the increasing use of complex neural architectures and reinforcement learning agents in network management, explainability advances trust, regulatory compliance, and diagnostic capabilities [24]. Techniques to interpret decisions and visualize agent behavior enhance transparency, yet balancing interpretability with high prediction accuracy remains an active research challenge.

Scalable Distributed Architectures. To address the demanding scale of next-generation wireless systems, distributed frameworks combining multi-agent reinforcement learning and adaptive control are emerging. They enable resilience and fault tolerance across diverse network segments but raise issues related to scalability, system complexity, and interoperability.

In summary, these enablers collectively push AI's feasibility in wireless and cyber-physical systems by tackling privacy, interpretability, latency, and scalability challenges. Ongoing research is

Table 5: Comparative summary of key AI-based control and wireless methodologies

Approach	Methodological Strengths	Practical Challenges	Application Domains
Model-based control with AI integration	Theoretical robustness, interpretability	Computational complexity, model accuracy	Autonomous systems, robotics
Data-driven machine learning methods	Adaptability, scalability	Data requirements, lack of guarantees	Network optimization, resource allocation
Hybrid model-data fusion frameworks	Balance of theory and flexibility	Integration complexity, tuning	Smart grids, 5G/6G networks
Reinforcement learning for control	Real-time learning, policy optimization	Exploration-exploitation trade-offs	UAVs, IoT management
Edge AI and distributed architectures	Low latency, scalability	Communication overhead, privacy	Smart cities, industrial automation

Table 6: Summary and Analysis of Critical Enablers in AI-Driven Wireless Networks

Enabler	Function and Benefits	Challenges and Controversies	Illustrative Example
Federated Learning	Enables distributed intelligence while preserving privacy, e.g., collaborative spectrum management	Communication overhead, model convergence issues, heterogeneous data distributions	Open RAN dynamic spectrum allocation [6]
Privacy-Preserving AI	Protects sensitive user and network data, maintains user trust	Balancing privacy with model accuracy and efficiency; differential privacy vs. encryption trade-offs	Secure data exchange in multi-operator networks
Edge Intelligence	Decentralizes computation to reduce latency	Limited edge resources, coordination across nodes, model consistency	Real-time adaptive interference mitigation
Explainable AI	Provides transparency and interpretability for black-box models	Complexity of explanations, potential reduction in model accuracy [24]	Visualizing reinforcement learning decision paths
Scalable Distributed Architectures	Support multi-agent RL and adaptive control across heterogeneous segments	System complexity, scalability bottlenecks, interoperability issues	Large-scale network fault detection systems

crucial to resolve existing trade-offs between performance, complexity, and trustworthiness to realize fully intelligent and adaptive networks.

10.8 Identified Research Needs

Despite remarkable advancements, several critical research gaps persist that require focused investigation and innovative approaches.

Computational Complexity Reduction: Existing neural network-based control and AI inference frameworks must evolve to handle challenges such as time-varying delays and high-dimensional data inputs more efficiently. For example, adaptive neural network finite-time resilient control approaches have demonstrated robustness against unknown actuator faults and false data injection attacks, but often demand high neural network capacity and are sensitive to noise and parameter tuning [3]. Future methodologies should target new algorithms that significantly reduce computational resource consumption while maintaining or enhancing control performance, potentially through novel adaptive learning schemes or distributed architectures.

Robustness Against Uncertainties: AI models frequently remain vulnerable to adversarial perturbations, noisy telemetry, and imperfect channel state information. Robust design frameworks are essential for guaranteeing reliable operation amid uncertain and unmodeled disturbances, as highlighted in AI-empowered interference mitigation within networked sensing systems [18]. Research directions include the development of resilient AI algorithms that can adapt to dynamic and unpredictable environments, leveraging coordinated multi-agent cooperation and real-time adaptation to maintain sensing and control quality.

Latency Minimization: Achieving real-time inference latency is a critical requirement, especially in resource-constrained edge computing environments. Lightweight AI architectures and specialized hardware accelerators tailored for such conditions are imperative [24]. Emphasis should be placed on scalable AI models that balance accuracy and latency, integrating efficient reinforcement and deep learning methods for tasks like adaptive resource allocation and network optimization without compromising inference speed.

Interpretability Enhancement: Enhancing the transparency and interpretability of AI-driven decision-making processes remains vital for both operational acceptance and regulatory compliance, particularly within safety-critical domains. Future research should focus on explainable AI frameworks that provide clear insights into model predictions and control actions, fostering trust and facilitating debugging in complex cyber-physical systems.

Interdisciplinary Collaboration: Given the inherently multifaceted nature of cyber-physical systems and large-scale networks, collaborative frameworks that integrate control theory, wireless communications, and AI are essential. Such interdisciplinary efforts are crucial to holistically address challenges related to system dynamism, scalability, and security, enabling comprehensive solutions that span algorithmic, hardware, and network layers.

Addressing these research needs is critical to advancing the robustness, efficiency, and applicability of AI-enhanced resilient control and wireless systems. Further investigation into these directions will help bridge existing gaps, enabling resilient, scalable, and interpretable AI solutions that meet the rigorous demands of future cyber-physical infrastructures.

10.9 Anticipated Innovations

Looking forward, several key innovations are expected to drive the next phase of development. These innovations promise transformative capabilities but also present notable challenges and limitations that future research must address.

Multi-Agent Collaborative Learning: Distributed learning and decision-making across network nodes promise improved adaptability and fault tolerance in complex environments. Multi-agent reinforcement learning schemes have demonstrated enhanced resource allocation and anomaly detection in Open RAN settings [6]. However, challenges include the complexity of coordination among agents, communication overhead, scalability issues, and robustness to adversarial conditions. Federated and collaborative learning approaches must balance privacy, latency, and convergence speed for real-time applications.

Hardware Acceleration: Specialized AI accelerators embedded in edge devices can substantially reduce inference latency and energy consumption, enabling real-time adaptive control and interference mitigation [24]. The main limitations lie in hardware design complexity, cost constraints, and integration with heterogeneous network elements. Further, balancing energy efficiency with computational power remains a critical challenge, especially for resource-constrained edge environments.

Quantum Computing Integration: Quantum technologies indicate potential breakthroughs in optimization speeds and security measures, accelerating complex computations unreachable by classical methods. Despite this promise, practical deployment faces significant hurdles due to the nascent state of quantum hardware, error rates, and the need to develop quantum algorithms tailored for network optimization and security.

Blockchain Security Mechanisms: Blockchain-based solutions can enhance the security of decentralized AI agents by ensuring data integrity and providing transparent audit trails, thereby reinforcing trustworthiness in collaborative learning systems [25]. Yet, blockchain integration introduces trade-offs including latency overhead, scalability concerns, and increased computational demands. Aligning blockchain protocols with network performance requirements and privacy regulations remains an open research area.

These innovations collectively envisage fully autonomous intelligent networks characterized by self-healing capacities, context-aware adaptations, and proactive cyber-physical threat mitigation [5]. However, real-world deployment must carefully manage trade-offs among computational complexity, scalability, security, and interoperability. Advances such as explainable AI, hierarchical agent designs, and lightweight model development are critical to overcoming these limitations.

The following table summarizes the key innovations, their benefits, and associated challenges:

In summary, this synthesis elucidates the intricate, multi-dimensional progress and outstanding challenges at the intersection of AI, resilient control, and wireless technologies. By highlighting critical enablers and research gaps, it establishes a comprehensive roadmap for evolving secure, adaptive, and intelligent networked systems capable of addressing future demands and uncertainties.

11 Conclusion

The integration of artificial intelligence (AI) into various domains of telecommunication networks has markedly enhanced functionalities such as adaptive control, wireless networking, routing, software-defined networking (SDN), Open Radio Access Networks (Open RAN), and autonomous fault management. AI-driven adaptive control strategies utilize advanced predictive models to dynamically optimize network resource allocation, thereby improving the network's responsiveness to variable traffic loads and heterogeneous service demands. Within wireless networking and routing, machine learning techniques — especially ensemble methods like gradient boosting — have proven highly effective in capturing complex nonlinear patterns and addressing class imbalance issues endemic to network datasets. This capability fosters more accurate routing decisions and robust customer churn prediction, as demonstrated in recent studies [27]. Collectively, these advances underscore AI's critical contribution to enhancing efficiency and resilience in contemporary telecommunication infrastructures.

Looking ahead, the evolution of telecommunication networks is trending towards fully autonomous, self-optimizing systems capable of continuous self-monitoring and dynamic adjustment. Nevertheless, deploying AI solutions at scale introduces significant challenges: scalability concerns due to the computational demands of complex models such as gradient boosting; security and privacy risks related to adversarial attacks within AI-integrated control loops; interoperability difficulties arising from the heterogeneous, multi-vendor nature of modern networks; and the need for explainability and transparency to foster trust and accountability, especially with unsupervised learning algorithms. Promising methods—such as the neuralization framework that transforms clustering models into neural networks to reveal feature importances—offer pathways to improve interpretability in autonomous network operations [**?**].

In summary, the progression towards next-generation telecommunication networks is grounded in sophisticated AI methodologies that are autonomous, efficient, secure, and interpretable. The synergistic integration of AI across control, orchestration, and management layers signals a transformative phase where telecommunication infrastructures attain unprecedented levels of self-governance and resilience. Realizing this vision requires ongoing, interdisciplinary research to address integration complexities while ensuring scalability, security, and explainability of AI-driven solutions. Ultimately, this will pave the way for truly intelligent, adaptive, and trustworthy networks capable of meeting future communication demands.

To enhance reader takeaway, we provide a concise summary of key points:

Summary of Key Points:

• AI significantly improves telecommunication network functionalities including adaptive control, routing, and fault management through predictive and ensemble learning models.

• Gradient boosting methods outperform traditional algorithms in telecom customer churn prediction by effectively handling class imbalance and nonlinear relationships [27], but they require greater computational resources.

• Deploying AI at scale introduces challenges: scalability, security/privacy, interoperability, and explainability.

• Explainable AI frameworks, such as neuralization of clustering models [**?**], enhance transparency in autonomous network operations.

• Future telecommunication networks aim for fully autonomous, self-optimizing systems demanding interdisciplinary research efforts to overcome integration challenges.

This structured summary consolidates the survey's main contributions and highlights critical enablers and research directions necessary for advancing AI-driven telecommunications.

References

[1] S. Aboagye, M.-S. Alouini, and L. Dai. 2024. Multi-Band Wireless Communication Networks: Fundamentals, Challenges, and Resource Allocation. *IEEE Wireless Communications* 31, 5 (2024), 86–93. https://ieeexplore.ieee.org/document/10438479/

[2] A. Ahmed, T. M. Nguyen, and M. Elsayed. 2023. Deep Learning for Telecom Self-Optimized Networks. *IEEE Transactions on Communications* 71, 4 (2023), 2001–2014. https://ieeexplore.ieee.org/document/10811884

[3] Anonymous. 2025. Deep Learning in Wireless Communication Receiver: A Survey. arXiv preprint arXiv:2501.17184. https://arxiv.org/abs/2501.17184 Accessed: 2024-06-01.

Table 7: Summary of Anticipated Innovations: Benefits and Challenges

Innovation	Benefits	Challenges / Limitations
Multi-Agent Collaborative Learning	Enhanced adaptability, fault tolerance, and resource optimization [6]	Coordination complexity, scalability, communication overhead, adversarial robustness
Hardware Acceleration	Reduced latency and energy consumption enabling real-time control [24]	Hardware complexity, integration challenges, cost, balancing energy and compute
Quantum Computing Integration	Potential breakthroughs in optimization speed and security	Immature hardware, error rates, need for specialized quantum algorithms
Blockchain Security Mechanisms	Data integrity, auditability, trust enhancement in decentralized AI [25]	Latency overhead, scalability, computational demand, privacy and regulatory concerns

[4] M. W. Baidas. 2016. A Distributed Political Coalition Formation Framework for Multi-Relay Selection in Wireless Networks. *Wireless Communications and Mobile Computing* 16, 4 (2016), 2065–2082. doi:10.1002/wcm.2763

[5] Dimitris Bertsimas. 2023. Global optimization via optimal decision trees. *Journal of Global Optimization* 85, 1 (2023), 1–28. doi:10.1007/s10898-023-01311-x

[6] T. Chen, M. Hong, and Z. Su. 2018. Learn-and-Adapt Stochastic Dual Gradients for Network Optimization. *IEEE Transactions on Control of Network Systems* 5, 4 (2018), 1456–1467. https://ieeexplore.ieee.org/document/8110688

[7] Z. Chen, M. Zhao, and X. Wang. 2024. Robust Federated Learning for Unreliable and Resource-Constrained Wireless Networks. *IEEE Transactions on Wireless Communications* 23, 8 (2024), 9793–9809. https://ieeexplore.ieee.org/document/10444714/

[8] L. Dai, R. Jiao, F. Adachi, H. V. Poor, and L. Hanzo. [n. d.]. Deep Learning for Wireless Communications: An Emerging Interdisciplinary Paradigm. Online. https://arxiv.org/abs/2007.05952 Submitted Jul. 2020.

[9] X. Ding, Y. Jin, and J. Liu. 2023. Obstacle-Aware Fuzzy Clustering Protocol for Wireless Sensor Networks in 3D Terrain. *International Journal of Wireless Information Networks* 30, 1 (2023), 30–41. doi:10.1007/s10776-022-00595-8

[10] T. Febrianto, J. Hou, and M. Shikh-Bahaei. 2017. Cooperative Full-Duplex Physical and MAC Layer Design in Asynchronous Cognitive Networks. *Wireless Communications and Mobile Computing* 2017 (2017), 1–14. doi:10.1155/2017/8491920

[11] W. S. Fujo, I. J. Al-Mousa, and S. A. Hamed. 2024. Customer Churn Prediction in Telecommunication Industry Using Deep Learning. *Preprints.org* 2024, 0115 (2024). https://www.preprints.org/manuscript/202403.0585/v1

[12] A. Förster, F. Macabiau, and D. Grouset. 2024. A beginner’s guide to infrastructure-less networking concepts. *IET Networks* 13, 1 (2024), 14–22. doi:10.1049/ntw2.12094

[13] E. Hanasusanto, D. Kuhn, and K. N. Kallas. 2016. Multistage Robust Mixed-Integer Optimization with Adaptive Partitions. *Operations Research* 64, 4 (2016), 980–998. doi:10.1287/opre.2016.1515

[14] M. Imani. 2024. Comparing Traditional Machine Learning and Advanced Gradient Boosting Techniques in Customer Churn Prediction: A Telecom Industry Case Study. *Preprints.org* 2024, 0213 (2024). https://www.preprints.org/manuscript/202403.0213/v2

[15] K. D. Irianto and R. Chandra. 2020. Partial packet in wireless networks: a review of error recovery and loss mitigation techniques. *IET Communications* 14, 15 (2020), 2396–2409. doi:10.1049/iet-com.2019.0550

[16] D. Kuhn, P. Wiesemann, and T. Georghiou. 2019. Wasserstein Distributionally Robust Optimization: Theory and Applications in Machine Learning. *Operations Research* 67, 3 (2019), 814–831. doi:10.1287/opre.2018.1804

[17] Y. H. Kwon, K. J. Han, and Y. S. Choi. 2015. Efficient network mobility support scheme for proxy mobile IPv6. *EURASIP Journal on Wireless Communications and Networking* 2015, 1 (2015), 1–14. doi:10.1186/s13638-015-0437-8

[18] M. Li, Y. Hong, and B. Chen. 2021. A Unified Analytical Framework for Optimal Control Problems in Network Systems. *IEEE Transactions on Control of Network Systems* 8, 4 (2021), 1645–1656. https://ieeexplore.ieee.org/document/9454297

[19] Y. Li, Z. Zhang, L. Wu, and X. Wang. 2022. Real-World Wireless Network Modeling and Optimization: Recent Advances and Challenges. *Chinese Journal of Electronics* 31, 2 (2022), 263–280. https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/cje.2022.00.191

[20] Y. Liu, X. Liang, and P. Zhang. 2020. Data-Importance Aware Radio Resource Allocation. *IEEE Communications Letters* 24, 9 (2020), 2046–2050. https://ieeexplore.ieee.org/document/9098940

[21] R. F. Lopes. 2013. Performance of the modulation diversity technique for - fading channels in wireless communications. *EURASIP Journal on Wireless Communications and Networking* 2013, 1 (2013), 1–12. doi:10.1186/1687-1499-2013-17

[22] Y. Luo, C. Yang, and S. Yu. 2023. Recent Advances in Optical Wireless Communications for 6G Wireless Networks. *IEEE Wireless Communications* 30, 2 (2023), 58–65. https://ieeexplore.ieee.org/document/10325445/

[23] G. A. Mapunda, R. Ramogomana, L. Marata, B. Basutli, A. S. Khan, and J. M. Chuma. 2020. Indoor Visible Light Communication: A Tutorial and Survey. *Wireless Communications and Mobile Computing* 2020 (2020), 46. doi:10.1155/2020/8881305

[24] S. Nadarajah and A. A. Ciré. 2020. Network-Based Approximate Linear Programming for Discrete Optimization. *Operations Research* 68, 6 (2020), 1767–1786. doi:10.1287/opre.2019.1953

[25] A. Nagurney. 2022. Supply chain networks, wages, and labor productivity: insights from Lagrange analysis and computations. *Journal of Global Optimization* 83, 3 (2022), 615–638. doi:10.1007/s10898-021-01084-x

[26] F. Nisar and B. A. Rehman. 2025. An efficient security framework, vulnerabilities, and defense mechanisms in LoraWAN. *Computer and Telecommunication Engineering* 3, 2 (2025), Article ID 3072. https://aber.apacsci.com/index.php/CTE/article/view/3072

[27] D. Niyato. 2023. Editorial: Fourth Quarter 2023 IEEE Communications Surveys and Tutorials. *IEEE Communications Surveys & Tutorials* 25, 4 (2023), 3456–3463. https://ieeexplore.ieee.org/document/10325334/

[28] Dusit Niyato and et al. 2021. Survey on Wireless Communications. *IEEE Communications Surveys & Tutorials* 23, 1 (2021), 1–40. https://ieeexplore.ieee.org/document/9621329/

[29] S. Pawar, L. Bommisetty, and T. G. Venkatesh. 2022. A High Capacity Preamble Sequence for Random Access in 5G IoT Networks: Design and Analysis. *International Journal of Wireless Information Networks* 30, 1 (2022), 1–15. doi:10.1007/s10776-022-00593-x

[30] Y. Qian, H. Chen, and M. Dohler. 2022. Beyond 5G Wireless Communication Technologies. *IEEE Wireless Communications* 29, 1 (2022), 166–172. https://ieeexplore.ieee.org/document/9749229/

[31] E. Shaaban. 2023. Hyperparameter Optimization and Combined Data Certainty for Customer Churn Prediction in Telecommunication Industry. *Preprints.org* 2023, 1478 (2023). https://www.preprints.org/manuscript/202308.1478/v3

[32] X. Shen, Y. Liu, X. Du, and K. K. R. Choo. 2020. AI-assisted Network-slicing based Next-generation Wireless Networks. *IEEE Transactions on Wireless Communications* 19, 3 (2020), 1558–1571. https://ieeexplore.ieee.org/iel7/8782711/8889399/08954683.pdf

[33] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, and G. Fettweis. 2016. 5G-Enabled Tactile Internet. *IEEE Journal on Selected Areas in Communications* 34, 3 (2016), 460–473. https://ieeexplore.ieee.org/document/7403840/

[34] S. Thapaliya and P. K. Sharma. 2022. Cyber Forensic Investigation in IoT Using Deep Learning Based Feature Fusion in Big Data. *International Journal of Wireless Information Networks* 30, 1 (2022), 16–29. doi:10.1007/s10776-022-00588-7

[35] D. Wen, B. Zhang, and Y. Chen. 2020. Joint Parameter-and-Bandwidth Allocation for Improving Federated Learning Performance in Wireless Networks. *IEEE Transactions on Wireless Communications* 19, 10 (2020), 6780–6793. https://ieeexplore.ieee.org/document/9194337/

[36] Z. Weng, L. Lu, J. Chen, H. Zhang, and L. Hanzo. 2023. Deep Learning Enabled Semantic Communications With Knowledge Graph and Knowledge Base. *IEEE Journal on Selected Areas in Communications* 41, 9 (2023), 2192–2207. https://ieeexplore.ieee.org/document/10038754

[37] Z. Zhao, E. J. Schiller, E. Kalogeiton, T. Braun, S. Burkhard, and M. T. Garip. 2017. Autonomic Communications in Software-Driven Networks. *IEEE Journal on Selected Areas in Communications* 35, 11 (2017), 2431–2445. https://ieeexplore.ieee.org/document/8063402/

[38] H. Zhou, W. Saad, and D. Niyato. 2024. Large Language Model (LLM) for Telecommunications: A Comprehensive Survey on Principles, Key Techniques, and Opportunities. *IEEE Communications Surveys & Tutorials* 26, 2 (2024), 879–913. https://ieeexplore.ieee.org/document/10685369/

[39] D. D. Čvokić, Y. A. Kochetov, and A. Savić. 2022. A variable neighborhood search algorithm for the (r|p) hub–centroid problem under the price war. *Journal of Global Optimization* 83, 3 (2022), 405–444. doi:10.1007/s10898-021-01051-2