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, 43 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 remain in three key areas: scalability, interpretability, and integration with human decision-making [**?**]. Throughout this survey, we critically examine existing methodologies by focusing on their strengths, limitations, and suitability for different applications.

To provide a clear overview for readers, this survey is organized as follows. Section **??** reviews prominent AI techniques, including machine learning, neural networks, and symbolic reasoning, highlighting their typical applications. Section **??** discusses the main challenges faced in AI research and practice, such as scalability issues when dealing with large datasets, the need for interpretability to ensure transparency, and methods for integrating AI systems with human decision-making processes. Finally, Section **??** explores future directions and potential solutions to these challenges.

For readers less familiar with some technical terms, we provide brief explanations where these terms first appear. For example, "scalability" refers to an AI system's ability to maintain performance as the size of data or complexity of tasks increases, while "interpretability" means how easily humans can understand the reasoning behind AI outputs. This approach aims to make the survey accessible to a broader audience.

This structured breakdown and the inclusion of clarifying examples throughout the paper should help guide the reader effectively through the landscape of AI research.

Conference'17, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM

https://doi.org/10.1145/nnnnnnn.nnnnnnn

1.1 Current AI Methodologies

Deep learning approaches have demonstrated exceptional performance on large-scale datasets, enabling breakthroughs in perception and pattern recognition [**?**]. However, these methods often lack transparency due to their black-box nature and demand substantial computational resources, which hinders their deployment in resource-constrained or high-stakes settings requiring interpretability and efficiency.

Symbolic AI techniques offer superior interpretability and align well with human reasoning processes [**?**]. Yet, their scalability and adaptability to complex, unstructured data remain limited, restricting their effectiveness across a broad range of real-world applications where flexibility and learning from raw data are crucial.

Hybrid models aim to leverage the complementary advantages of both paradigms by integrating symbolic reasoning with deep learning [**?**]. Despite their promise, such integration is nontrivial due to challenges in harmonizing fundamentally different representations and learning mechanisms, including the need to reconcile symbolic logic's discrete structures with neural networks' continuous representations, as well as ensuring end-to-end differentiability for training efficiency.

1.2 Scope and Contributions

This survey synthesizes findings across a diverse range of AI techniques, providing a detailed comparative analysis that elucidates their unique capabilities, inherent trade-offs, and situational advantages. By systematically highlighting open research challenges and prospective future directions, it furnishes valuable guidance for researchers aiming to select, adapt, or advance AI methodologies tailored to specific application contexts and requirements.

1.3 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 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].

A comparative evaluation of these diverse AI-driven approaches reveals notable trade-offs. For example, semantic communication methods [36] achieve superior semantic fidelity and noise robustness but incur substantial computational overhead and complexities in dynamic knowledge updating. Deep learning techniques applied in SON [**?**] enhance autonomous management capabilities but face challenges in model robustness across heterogeneous network environments and increased resource consumption. Federated learning frameworks [2**?**] effectively balance data privacy and communication efficiency, yet may encounter scalability and synchronization issues in highly dynamic wireless settings. Reinforcement learning applied to network slicing [**?**] provides adaptive resource allocation with improved throughput and latency but often requires extensive training data and careful tuning to avoid convergence issues.

Moreover, specific limitations and pitfalls need explicit consideration. The hierarchical mobility management strategies [33], while reducing signaling overhead, may face scalability concerns in ultra-dense networks with high mobility users, and integrating them seamlessly with standardized protocols remains nontrivial. The deployment of LLMs [**?**] in telecom environments must carefully manage the trade-off between inference latency, model size, and privacy, with existing methods still grappling with domain adaptation and hallucination mitigation. Finally, AI-driven frameworks

for emerging ultra-reliable low-latency networks, such as the Tactile Internet [7], demand stringent real-time guarantees, exposing tensions between AI model complexity and latency requirements.

Overall, this evolving landscape underscores the importance of advancing scalable, interpretable, and resource-aware AI frameworks that effectively balance performance gains against computational costs, latency constraints, and deployment complexity. Future research should focus on developing hybrid models combining the strengths of multiple AI paradigms, enhancing robustness to network uncertainties, and integrating explainability to foster trust and effective operation within mission-critical telecommunication systems.

1.4 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]. For instance, advances in 5G IoT random access leverage novel high-capacity preamble sequences to handle massive device connectivity while minimizing collisions [37]. Similarly, in cyber forensic investigations within IoT, deep learning-based feature fusion methods effectively handle heterogeneous big data and improve security analysis [1], and obstacle-aware protocols enhance wireless sensor network resilience in complex 3D terrains [30]. 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]. For example, machine learning-based network traffic classification models improve accuracy and adaptability despite encrypted, dynamic traffic patterns. Such models employ diverse supervised and deep learning algorithms that can automatically learn from flow and statistical features, achieving high accuracy while addressing challenges like data imbalance and concept drift [16]. Similarly, AI-powered SDN frameworks integrate supervised and deep learning methods into SDN controllers to perform real-time traffic classification, anomaly detection, and dynamic resource allocation. Experimental validations report up to 92% accuracy in traffic classification, an 18% reduction in latency, and a 15% increase in throughput in 5G environments, significantly enhancing network management and resource efficiency [13]. 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 while highlighting ongoing challenges related to data heterogeneity, privacy preservation, computational overhead, and smooth integration with legacy systems. For example, despite AI's promise, SDN frameworks still face computational challenges and dataset scarcity issues [13]. AI integration in Open RAN notably enhances throughput, latency, and energy efficiency, employing federated learning, reinforcement learning, and deep neural networks, yet demands resolving challenges such as real-time inference latency, AI model convergence, multi-vendor interoperability, and energy constraints at the edge [5, 25]. Quantitative evaluations demonstrate improvements in fault detection accuracy up to 95% and mitigation success rates up to 91%, significantly reducing downtime and throughput degradation in Open RAN environments [5].

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.

1.5 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, self-healing, and self-protection by embedding flexibility and adaptability into software-driven network infrastructures, particularly leveraging software-defined networking (SDN) and network function virtualization (NFV). While such frameworks significantly improve network resilience, throughput, latency, and operational cost, challenges such as scalability, device heterogeneity, interpretability of machine learning models for real-time decisions, and security vulnerabilities remain [35]. Addressing these issues calls for enhanced AI and big data analytics, adaptive trust and security mechanisms, and comprehensive standardization to ensure wide interoperability and robust network autonomy.

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 [**? ?**]. These approaches are crucial for optimizing complex resource allocation and scheduling tasks required in beyond-5G (B5G) and 6G wireless systems, supporting ultra-low latency, massive connectivity, and improved spectral and energy efficiency. Such optimization techniques also assist in integrating emerging technologies like optical wireless communications, ensuring robustness despite diverse channel conditions and network densification [**?**]. The optimization frameworks are integral to realizing key technologies such as cell-free massive MIMO and hybrid spectrum sharing envisioned in B5G systems, balancing performance with computational and hardware constraints.

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 incorporate security frameworks and policy-based rule enforcement critical for defending against vulnerabilities in edge and cloud network deployments.

Through simulation and practical validations, such frameworks have demonstrated effectiveness in mitigating network attacks and enhancing both internal and external security postures, thereby improving overall network resilience.

Moreover, intelligent wireless technologies incorporating AI have demonstrated substantial improvements at the physical layer. AI-powered reconfigurable intelligent surfaces (RIS) dynamically control the wireless environment by enabling adaptive channel estimation, beamforming, and resource allocation through learned environmental feedback [6, 38]. This integration boosts spectral and energy efficiency in complex wireless settings and adapts effectively to imperfect channel information. Deep learning-driven interference management frameworks enable robust signal processing against noise and interference, while semantic communications further optimize information flow. Deep learning models such as stacked autoencoders and deep neural networks are applied beyond the physical layer for higher-level tasks including customer churn prediction and traffic management [38]. These models efficiently extract hierarchical features from raw data, facilitating robust decision-making and improved operational performance, although challenges related to computational cost, data requirements, and interpretability persist.

Collectively, these AI techniques form a multi-layered intelligence framework that integrates decision-making from physical-layer signal optimization to network-layer control and application-specific adaptations. This cohesive approach advances autonomous, reliable, and efficient future communication networks, addressing many of the challenges anticipated in next-generation wireless systems [6, 24, 35]. Future research directions emphasize explainable AI models, edge-cloud synergy, and enhanced robustness against adversarial conditions to fully realize intelligent and secure network ecosystems.

1.6 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]. For instance, in URLLC scenarios, AI models integrated within Software-Defined Networking (SDN) controllers must execute traffic classification and anomaly detection swiftly; any lag in inference can degrade the promised low-latency service [13]. 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. An example is AI-powered SDN frameworks in 5G that, despite improving traffic classification accuracy and throughput, struggle with computational overhead and dataset scarcity when scaling to billions of devices [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. For example, federated learning applied to AI-enhanced interference mitigation in networked sensing must balance privacy with the heterogeneity of local data distributions and communication constraints [13, 18**?**].

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. In practical deployments, integrating AI models trained on heterogeneous wireless communication protocols often requires ad hoc adaptation, hindering smooth multi-vendor coordination [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. For example, AI-optimized Reconfigurable Intelligent Surfaces (RIS) and network routing algorithms demonstrate strong performance under controlled settings but remain vulnerable to adversarial perturbations and sudden environmental changes, affecting coverage and resilience [6, 24, 39].

Addressing these challenges requires developing scalable AI-SDN frameworks that optimize resource allocation and traffic management while preserving privacy [13], as well as creating robust AI algorithms capable of adapting dynamically to network changes and threats [6, 24, 39]. For instance, AI-driven routing solutions that adapt to traffic fluctuations and detect failures in real-time can enhance throughput and latency but need to balance computational complexity and privacy concerns [39]. These multifaceted challenges underscore the necessity for scalable, secure, and interpretable AI frameworks capable of reliable operation within heterogeneous, dynamic network ecosystems.

1.7 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 combining classical analytical frameworks with state-of-the-art data-driven methods, the survey highlights how AI models improve network adaptability and operational efficiency while addressing challenges such as model interpretability, computational overhead, and security vulnerabilities.

Ultimately, this work 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

This section aims to provide a structured and measurable overview of AI techniques applied to network traffic classification, evaluating their characteristics, performance, and limitations. The measurable objectives are: (1) to categorize main AI approaches used in traffic classification, (2) to compare their strengths and weaknesses with quantitative benchmarks where available, (3) to discuss recent datasets and evaluation protocols, and (4) to highlight open challenges and future directions.

2.1 Taxonomy of AI Methods

AI techniques for network traffic classification broadly fall into three categories: traditional machine learning, deep learning, and online learning. Each category differs in feature extraction methodology, adaptability, and computational requirements.

2.2 Performance Benchmarks and Datasets

Recent benchmarking efforts emphasize evaluation on publicly available datasets such as MIRAGE [**?**], ISCX VPN-nonVPN [**?**], and UCDAVIS [**?**] which provide labeled flows for encrypted and unencrypted traffic. Standardized evaluation protocols use accuracy, F1-score, and runtime metrics on these datasets to enable fair method comparison.

Empirical studies often report that deep learning models, especially CNNs and RNNs, outperform traditional methods by 5-15% in accuracy on encrypted traffic datasets, as shown in MIRAGE evaluations. Online learning methods maintain competitive performance in streaming scenarios but require well-designed drift detection mechanisms to sustain accuracy. Unfortunately, data scarcity and heterogeneity remain key bottlenecks in benchmarking, with calls for more comprehensive, up-to-date datasets continuing.

2.3 Discussion and Research Directions

AI-based traffic classification faces ongoing challenges, including accurate classification amidst encrypted and obfuscated traffic, limited labeled data, and maintaining model robustness in evolving network environments. Hybrid approaches combining deep feature extraction with online incremental learning show promise for balancing accuracy and adaptability.

Furthermore, the field would benefit from meta-analyses comparing AI methods across standardized datasets, clearly defined evaluation protocols, and extended benchmarks incorporating real-world traffic dynamics. Publicly available, large-scale, and up-to-date datasets are critical to advancing research and practical deployments.

In summary, the AI-enabled network traffic classification landscape demands integrated solutions that effectively address data availability, model interpretability, resource constraints, and the evolving nature of network traffic patterns.

2.4 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. Additionally, traditional methods struggle with evolving traffic patterns and concept drift, limiting their adaptability and accuracy over time.

These constraints collectively reduce the practicality and scalability of conventional techniques 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]. Moreover, emerging hybrid or semi-supervised methods have been proposed to alleviate limitations inherent to purely supervised approaches. These methods combine limited labeled data with abundant unlabeled data to enhance classification performance and adaptability, especially under evolving network conditions and scarcity of annotated traffic samples. Such hybrid techniques represent a promising direction to overcome traditional challenges by improving generalization and reducing reliance on costly manual labeling [16].

2.5 Machine Learning Approaches for Traffic Classification

This section provides a focused overview of machine learning methodologies applied to network traffic classification, emphasizing their objectives, comparative advantages, and how they address key challenges such as encrypted payloads, dynamic traffic patterns, and the need for real-time deployment.

Advancements in artificial intelligence and machine learning (ML) offer powerful alternatives to traditional methods by exploiting statistical and behavioral traffic characteristics that remain accessible despite payload encryption. Supervised learning algorithms—including decision trees, random forests, support vector machines (SVM), k-nearest neighbors (k-NN), and neural networks—have been widely used to classify traffic flows based on features extracted from packet sizes, inter-arrival times, and flow durations [16]. These approaches depend on labeled datasets to establish classification boundaries and have shown high accuracy under controlled conditions. Ensemble models, such as Random Forest and Gradient Boosting, demonstrate particularly strong performance across diverse and evolving traffic datasets by effectively balancing accuracy and robustness [16].

Unsupervised learning techniques, especially clustering algorithms, complement supervised models by identifying anomalous

Table 1: Summary of AI Methods for Network Traffic Classification

Method	Characteristics	Strengths	Limitations	Typical Performance
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 and encrypted traffic	Accuracy ranges from 75% to 90% depending on feature set and dataset
Deep Learning (CNN, RNN)	Automatically extracts features from raw data; capable of learning complex patterns	High accuracy; scalable; effective with encrypted traffic	Requires large labeled datasets and high computational resources; interpretability challenges	Accuracy often exceeds 90%, including on encrypted traffic classification
Online Learning	Incremental model updates with streaming data	Adaptable to evolving traffic; suitable for real-time scenarios	Model stability concerns; susceptible to noisy data and concept drift	Accuracy varies, typically 85–90% in dynamic conditions with robust adaptation

or previously unseen traffic patterns without requiring labeled data. This ability is crucial for adapting to new network behaviors and detecting emerging threats, thus addressing the challenge of concept drift and evolving traffic characteristics. As a result, unsupervised methods enhance model adaptability and enable dynamic detection in real-time environments [16].

Beyond conventional ML, deep learning methodologies employ architectures such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to automatically learn hierarchical feature representations and capture temporal dependencies inherent in sequential packet flows. These models perform particularly well when encryption obscures payload content, relying instead on flow-level statistical patterns to sustain classification effectiveness [16, 36**?**]. Although deep learning achieves superior accuracy on complex and encrypted traffic, it incurs higher computational complexity and training demands, challenging large-scale experimentation and real-time deployment. This trade-off motivates ongoing research toward scalable, interpretable, and resource-efficient AI frameworks [16].

Comparative analyses with recent datasets indicate that ensemble supervised models offer a favorable balance between computational cost and classification performance. Deep learning models provide enhanced robustness against encryption and traffic variability but require greater resources. Unsupervised methods improve adaptability and anomaly detection, which are critical for managing non-stationary and previously unknown traffic behaviors.

Emerging directions focus on semi-supervised, federated, and edge learning paradigms to enhance scalability, privacy preservation, and deployment feasibility in AI-driven network traffic classification. These approaches collectively address challenges such as data imbalance, limited payload visibility, concept drift, and the need for real-time inference. Ultimately, they aim to enable more autonomous, efficient, and privacy-aware network management solutions [16].

2.6 Data Pipeline Processes

The success of AI-based traffic classification frameworks fundamentally depends on constructing a robust data pipeline encompassing 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 significant challenges such as encryption, dynamic port usage, and evolving traffic behaviors.

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

Feature extraction constitutes a critical phase that directly influences classifier performance. Given restrictions on payload visibility due to encryption, most approaches rely on flow-based and statistical features extracted from both flow-level and packet-level attributes, such as packet sizes, inter-arrival times, and flow durations. These features provide meaningful insights while preserving user privacy.

Model training requires large-scale, balanced datasets to mitigate bias toward dominant classes, enhance generalization, and address concept drift caused by continuously evolving traffic patterns. Techniques such as data augmentation—including methods like oversampling minority classes or generating synthetic samples—and resampling may be employed to improve dataset representativeness and robustness.

Evaluation rigorously measures classifier performance through metrics including accuracy, precision, recall, and processing latency [16]. Trade-offs between classification accuracy and real-time feasibility are carefully considered, particularly when deploying complex models like deep learning in operational environments. The selection of appropriate evaluation criteria depends on specific application requirements and deployment constraints.

Maintaining this lifecycle is essential to ensure classifier robustness amid evolving network conditions, domain shifts, and emerging challenges related to privacy preservation and scalability. Future work emphasizes scalable, generalizable models that support real-time inference while respecting privacy and resource constraints.

2.7 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].

2.8 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, often leading to skewed performance metrics and inadequate responses to security threats [16].

Encrypted traffic further complicates classification, as encryption techniques obscure payload contents and dynamic port usage restrict traditional inspection methods. Consequently, classification relies mainly on flow-based and statistical features, which demands innovative feature extraction and modeling strategies capable of accurately inferring traffic types under constrained visibility and complex encryption schemes [16].

Concept drift reflects the evolving nature of network behaviors over time, requiring adaptive learning frameworks that can update models incrementally or continuously. Without such adaptability, models may become obsolete or inaccurate as traffic patterns shift due to new applications, protocols, or attacker strategies [16].

Dataset representativeness remains challenging since publicly available benchmarks often lack diversity in terms of traffic sources, network scales, environments, and temporal coverage. This limitation restricts the generalizability and transferability of trained models across heterogeneous and real-world network scenarios [16].

To address these challenges, promising future directions emphasize scalable, privacy-aware, and interpretable learning paradigms. **Semi-supervised learning** leverages abundant unlabeled network data alongside limited labeled samples, effectively improving model robustness, mitigating labeling costs, and alleviating data scarcity issues. This approach balances the benefits of supervised and unsupervised learning to adapt to dynamic and partially labeled environments [16, 24].

Federated learning offers decentralized, privacy-preserving model training by aggregating locally trained models rather than sharing raw traffic data. This paradigm is particularly advantageous for real-time edge inference and compliance with stringent data protection regulations, enabling collaborative learning across distributed networks while safeguarding sensitive information [6, 16, 24].

Explainability has emerged as a crucial requirement for deploying AI classifiers in operational network environments. Interpretable models and post-hoc explanation techniques provide insights into model decisions, help detect potential biases, and support auditing and regulatory compliance. Enhancing explainability fosters trust, accountability, and safer network operations [16, 24].

Moreover, integrating AI with **edge computing** infrastructures enables decentralization of inference closer to data sources. This proximity reduces latency and bandwidth consumption, improves scalability, and enhances robustness against failures and attacks. The synergy between AI and edge computing facilitates more responsive, efficient, and privacy-preserving network traffic classification systems suitable for dynamic real-world deployments [6, 16].

In summary, AI-enabled network traffic classification represents a transformative advancement over traditional methods by effectively adapting to encrypted, dynamic, and heterogeneous traffic patterns. Continued innovation focusing on computational efficiency, data imbalance, interpretability, privacy, and adaptability is essential to realize AI's full potential and seamless integration within operational network environments.

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 critical tasks like traffic prediction, anomaly detection, fault diagnosis, and self-healing. These capabilities enhance overall network performance by optimizing routing, load balancing, and quality of service (QoS) provisioning, while simultaneously reducing latency and energy consumption. Moreover, AI-driven SDN frameworks enable proactive resource management in the dynamic and heterogeneous 5G environments, adapting swiftly to fluctuating user mobility patterns, varying network conditions, and diverse service demands.

Beyond performance and efficiency improvements, integrating AI with SDN fundamentally supports 5G's network slicing capabilities—a foundational feature that allows the creation of multiple logically isolated virtual networks customized for specific applications, industries, or services. AI techniques facilitate the dynamic configuration, orchestration, and real-time adaptation of these slices, ensuring flexible, on-demand resource allocation and maintaining stringent and differentiated QoS requirements. Furthermore, this integration advances security within the SDN architecture by enabling intelligent threat detection, comprehensive real-time anomaly analysis, and automated mitigation mechanisms that proactively safeguard the network against emerging cyber threats.

In summary, AI integration in SDN for 5G and beyond is pivotal for achieving intelligent, flexible, and scalable networks capable of effectively meeting evolving technical challenges and the diverse requirements posed by next-generation applications and services.

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, an anomaly detection false positive rate below 3%, an 18% reduction in end-to-end latency, and a 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, thereby 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]. 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 promising results, practical deployment of such complex AI models faces several challenges. Training these models demands extensive labeled datasets and substantial computational resources, which may limit scalability and real-time responsiveness. Additionally, safeguarding AI models against adversarial attacks is critical to maintaining network reliability and security. Addressing these concerns, current research efforts focus on developing lightweight AI models optimized for real-time operation, employing federated learning techniques to preserve user privacy, and enhancing AI robustness against adversarial manipulations. These strategies not only improve the scalability and flexibility of AI in SDN but also facilitate automation in dynamic and heterogeneous network environments.

In summary, integrating AI techniques into SDN controllers enables more intelligent traffic management and anomaly detection, significantly improving quality of service in 5G and beyond networks. Continued advancements in model efficiency, privacy preservation, and security resilience are essential to realize the full potential of AI-powered SDN frameworks for future wireless 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 improvements directly enhance throughput, with experimental results indicating increases close to 15% in enhanced Mobile Broadband (eMBB) scenarios, attributable to more precise resource scheduling and dynamic traffic steering enabled by AI-driven decisions. Moreover, AI's capacity for rapid anomaly detection and real-time traffic adaptation has contributed to reductions of approximately 18% in end-to-end communication latency [13]. Equally important is the reduction in false positive rates for anomaly detection to below 3%, significantly minimizing unnecessary mitigation actions that might otherwise impair network efficiency. Collectively, these benefits emphasize AI's pivotal role in elevating Quality of Service (QoS), scalability, flexibility, and automation within inherently volatile 5G SDN environments, thereby enhancing responsiveness and adaptability to dynamic and heterogeneous traffic demands [13].

3.4 Challenges

This subsection identifies and analyzes key challenges hindering the deployment and operational scalability of AI-powered SDN frameworks, explicitly linking them to methodologies discussed earlier and illustrating each with pertinent examples and case studies.

The primary challenge is the substantial computational overhead associated with sophisticated AI models embedded in SDN controllers, which impacts the real-time processing required for ultra-low-latency scenarios such as enhanced Mobile Broadband (eMBB) and ultra-reliable low-latency communication (URLLC) in 5G and beyond networks [13]. For instance, deep learning models such as LSTM networks, when integrated for traffic classification and anomaly detection, have demonstrated improvements in accuracy and throughput but impose increased inference latency [13]. The tradeoff between model complexity and latency underscores the need for algorithmic innovations that compress models to maintain accuracy while significantly reducing processing time. Effective mitigation strategies include model pruning and knowledge distillation to achieve lightweight architectures, enabling deployment in latency-sensitive SDN environments.

Data scarcity remains a significant barrier due to the proprietary and sensitive nature of telecom-specific datasets, which restricts the training of supervised AI models and limits their generalizability across heterogeneous network conditions [**?**]. For example, large language models (LLMs) hold promise for automating telecom tasks such as network configuration and traffic classification, but their data-intensive nature demands vast, domain-specific corpora that are currently difficult to access [**?**]. Federated learning frameworks

have emerged as practical solutions to this problem, enabling collaborative model training across multiple operators without direct data exchange, thus preserving privacy and expanding data utility [**?**]. However, balancing privacy, utility, and communication overhead in such distributed approaches requires further investigation.

Security threats from adversarial AI attacks pose critical risks to AI-SDN systems, as attackers may exploit model vulnerabilities to trigger erroneous decisions or evade detection, undermining network reliability [18]. Interference mitigation frameworks in perceptive mobile networks exemplify these challenges, where AI-driven resource allocation improves sensing performance but remains vulnerable to adversarial manipulation that could degrade signal-to-interference-plus-noise ratio (SINR) and sensing accuracy [18]. Robust defense mechanisms tailored to dynamic telecom conditions, including adversarial training and anomaly-aware model updating, are essential to enhance system resilience.

Interoperability issues emerge from heterogeneous vendor equipment and inconsistent technological standards, complicating the seamless integration of AI models across multi-domain SDN deployments [**?**]. The lack of unified data formats and protocols hinders consistent AI control and data exchange across diverse network segments. Table 3 summarizes key standards initiatives addressing these challenges, noting their focus areas and current limitations. For example, while ETSI ENI emphasizes AI orchestration, it lacks comprehensive AI model interoperability support; similarly, 3GPP SA2 targets 5G architectures but is evolving in defining AI use cases and data sharing practices.

To facilitate holistic understanding, Table 2 below summarizes identified challenges alongside corresponding mitigation strategies and examples.

The top three critical research priorities identified are: (1) developing computationally efficient AI models enabling ultra-low-latency inference in real-world SDN deployments; (2) designing secure and robust AI frameworks resilient to diverse adversarial threats specific to telecom environments; and (3) advancing standardized, interoperable architectures and protocols facilitating scalable AI integration across heterogeneous multi-vendor telecom infrastructures.

Addressing these priorities requires holistic approaches combining algorithmic innovation, comprehensive security frameworks, collaborative data paradigms, and ecosystem-wide standardization efforts. Central research questions guiding future work include: How can AI models be compressed and accelerated without degrading accuracy under dynamic network loads? What tailored adversarial defense strategies effectively counter telecom-specific attack vectors while maintaining operational efficiency? How can federated learning designs optimize privacy-utility tradeoffs in multi-vendor SDNs with minimal communication overhead? How might emerging standards be shaped to ensure seamless interoperability and extensibility for AI-powered network control?

In summary, overcoming these challenges through integrated technological and procedural solutions is vital to harness the full potential of AI-enabled SDN architectures in next-generation wireless networks, ultimately advancing network intelligence, scalability, security, and automation.

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 emerges as a key 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 significantly enhance situational awareness and optimize network performance beyond existing temporal and spatial constraints [13].

Moreover, integrating Reconfigurable Intelligent Surfaces (RIS) with AI techniques such as machine learning and deep reinforcement learning is poised to play a pivotal role in dynamically controlling wireless environments to improve spectral and energy efficiency in 6G networks [6]. AI-enabled RIS systems optimize critical functions like channel estimation, beamforming, and resource allocation by learning from complex and dynamic channel state information, outperforming traditional heuristic methods. This synergy promises to enhance coverage, robustness, and adaptability, which are vital for meeting 6G requirements such as ultra-reliability, massive connectivity, and real-time intelligence [6].

Nonetheless, realizing federated and privacy-aware AI solutions entails overcoming substantial computational, communication, and standardization challenges. High-dimensional RIS configuration spaces and stringent low-latency demands impose constraints on AI scalability and real-time deployment [6, 24]. To address these challenges, interdisciplinary research bridging AI, communications, and network engineering is essential. This includes developing lightweight distributed AI algorithms and robust models resilient to adversarial conditions, as well as scalable frameworks capable of operating efficiently amid heterogeneous network traffic and dynamic environments [6, 13, 24]. The fusion of advanced AI algorithms with emerging wireless technologies will be critical to achieving intelligent, autonomous, and scalable next-generation 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. Key performance metrics observed in recent studies include reductions in end-to-end latency by up to 30%, improvements in throughput exceeding 20%, and energy efficiency gains around 15%, underscoring the practical benefits of AI-empowered SDN frameworks. Notably, reinforcement learning methods enable dynamic adaptability by learning optimal routing policies through interaction with the network environment, albeit with considerable training time and computational complexity [36]. Heuristic optimization offers faster convergence by applying problem-specific rules or approximations, trading off some optimality for efficiency. Deep learning-based approaches leverage high-accuracy prediction capabilities, for instance by modeling traffic patterns or faults to improve routing decisions, but

Table 2: Summary of AI-SDN Challenges with Corresponding Mitigation Strategies and Examples

Challenge	Mitigation Strategies	Illustrative Examples/Case Studies
Computational Overhead	Model compression (pruning, distillation), lightweight architectures, real-time optimization	LSTM integration in SDN controllers for URLLC scenarios with latency reduction techniques [13]
Data Scarcity	Federated learning, privacy-preserving data sharing, synthetic data generation	Collaborative training of LLMs across operators using federated approaches to address telecom data scarcity [?]
Security Vulnerabilities	Adversarial training, anomaly detection, robust AI model design	AI-enabled interference mitigation frameworks enhanced with adversarial resilience to maintain sensing SINR [18]
Interoperability	Standardization of AI model interfaces and protocols, vendor-neutral APIs	ETSI ENI and 3GPP SA2 standards advancing multi-vendor AI-SDN integration though still evolving [?]

Table 3: Summary of Current Standards Initiatives Relevant to AI-SDN Integration

Standard Initiative	Scope	Limitations
ETSI ENI (Experiential Networked Intelligence)	Framework for AI-driven network management and automation	Focuses on orchestration; limited coverage of AI model interoperability
3GPP SA2 AI/ML Work Items	AI/ML integration for 5G system architecture and management	Primarily targets 5G; evolving definitions for AI use cases and data sharing
TIP OpenRAN AI/ML	AI/ML aspects for OpenRAN architectures	Concentrates on RAN domain; vendor-specific implementations limit generalizability
IETF ANIMA (Autonomic Networking)	Autonomic networking protocols supporting AI-driven control	Early stage; interoperability challenges remain across multi-vendor environments
IEEE P2894 (AI/ML Data Formatting)	Standardization of data representations for AI/ML in networks	Emerging standard; adoption in telecom industry is limited so far

require significant computational resources [**?**]. Evolutionary algorithms provide robust adaptation to network changes through iterative improvement, though they typically converge more slowly.

Despite these innovations, challenges such as high computational demands and security vulnerabilities persist, impacting scalability and trustworthiness. Addressing these issues is critical for widespread adoption and practical deployment.

Table 4 presents a concise comparison of prominent AI-based routing methods within SDN environments, highlighting their key strengths, empirical performance gains, and inherent limitations. This overview clarifies trade-offs involved in method selection for specific network scenarios.

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 represent the forefront of research aimed at realizing 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 [].

The main algorithmic challenges in AI-driven routing can be categorized into four key areas: accurate prediction of dynamic network states, efficient path computation under varying constraints, real-time adaptation to network changes, and scalability in large heterogeneous environments.

For example, machine learning models can forecast traffic congestion or link failures, enabling preemptive rerouting to maintain quality of service. Case studies in software-defined networking (SDN) environments demonstrate how reinforcement learning algorithms iteratively improve routing policies based on network feedback, leading to reduced latency and higher throughput.

Despite these advances, there remain open challenges. One critical example is the trade-off between the computational overhead of complex AI models and the need for fast, real-time routing decisions. Additionally, transferring trained models across different network topologies without significant retraining is still problematic. Addressing these issues requires further research into lightweight models and domain adaptation techniques.

In summary, AI-driven routing optimization offers promising improvements by predicting and responding to network dynamics more effectively than traditional static methods. However, the balance between model complexity, execution speed, and adaptability to diverse network scenarios continues to be a key focus for future research.

3.7.1 Balancing Exploration and Exploitation. One critical challenge in routing algorithms is effectively balancing the trade-off between exploration and exploitation. Exploration involves probing new paths to discover potentially better or more optimal routes, while exploitation focuses on leveraging known, reliable paths to maintain consistent and stable network performance. Achieving this balance becomes especially challenging in highly dynamic environments, where network conditions and topologies change rapidly, requiring routing algorithms to adapt swiftly and make real-time decisions []. Properly addressing this balance is essential to optimize routing efficiency, minimize latency, and ensure robustness in dynamic networks.

3.7.2 Integration of Heterogeneous and Real-Time Data. Integrating heterogeneous data sources and real-time measurements remains a significant obstacle. AI models must efficiently process diverse and sometimes incomplete information—including traffic patterns, link quality, and node status—to produce accurate routing predictions. Ensuring scalability and maintaining low computational overhead are essential, as routing optimization must operate smoothly in large-scale networks [].

3.7.3 Handling Uncertainty and Variability. Robustness against uncertainty and variability in network conditions is paramount. Reinforcement learning techniques are commonly employed to continuously refine routing policies based on feedback, thereby enhancing resilience to dynamic network disruptions and failures [].

3.7.4 Meeting Latency and Reliability Requirements. Designing algorithms that meet stringent latency and reliability constraints remains a significant research challenge in AI-driven routing optimization. Ensuring timely and dependable network performance requires lightweight, adaptive models capable of real-time decision making under dynamic conditions. Future research directions

Table 4: Comparison of AI-Based Routing Techniques in SDN for 5G Networks

Method	Key Strengths	Performance Gains	Limitations
Reinforcement Learning	Learns optimal policies via environment interaction; adapts dynamically to network changes	Latency reduction up to 30%	High training time and computational complexity
Heuristic Optimization	Applies domain-specific rules for fast convergence	Throughput improvements over 20%	May yield sub-optimal routing decisions
Deep Learning-based	High accuracy in traffic and fault prediction enabling proactive routing	Energy efficiency gains of 15%	Requires significant computational resources and data
Evolutionary Algorithms	Robust adaptation to dynamic network conditions via iterative improvement	Enhanced fault tolerance	Slower convergence compared to other methods

include improving model interpretability to facilitate debugging and trust, enhancing responsiveness for real-time adaptation, and developing rigorous formal methods that provide guarantees on latency and reliability performance bounds [].

In summary, addressing these challenges requires adaptable, scalable, and robust solutions tailored to the complexities of modern network environments. This section has synthesized the primary algorithmic hurdles and outlined promising avenues for future work to unlock the full potential of AI-driven routing optimization.

3.7.5 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. Consequently, 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 pressing need for adaptive routing mechanisms that can dynamically respond to changes in network state by learning from traffic patterns and anomalies. Emerging AI-driven approaches leverage machine learning techniques, including reinforcement learning and neural networks, to optimize routing decisions in real-time. These methods address routing as a multi-objective optimization problem that balances throughput, latency, and fault tolerance [39]. Empirical evidence shows such AI-based routing solutions can achieve up to 30% improvements in throughput and latency while enhancing resilience through rapid failure detection and rerouting.

However, these advancements come with challenges such as increased computational overhead, scalability concerns, the necessity for representative training data, and the complexity of integrating AI-driven protocols with existing network infrastructure. Future research directions emphasize decentralized and federated learning methods to enable scalable, privacy-aware routing, as well as the development of hybrid AI-conventional schemes that benefit from both adaptive intelligence and established routing stability [39]. Overall, transitioning from static to intelligent, AI-based routing frameworks holds significant promise for the robust and efficient operation of next-generation networks.

3.7.6 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 requires careful design to balance exploration and exploitation to avoid suboptimal policies. Moreover, maintaining model generalization without overfitting specific network scenarios demands ongoing retraining and adaptation [39]. Empirical evidence indicates that AI-empowered routing schemes can improve network throughput and reduce latency by up to 30% compared to static routing protocols, while also enhancing fault tolerance through rapid anomaly detection and rerouting [**?**]. Continuous research is essential to address scalability, computational efficiency, and seamless integration with legacy network infrastructure to fully realize AI-driven routing's potential in real-world deployments.

3.7.7 Traffic Prediction and Anomaly Detection Integration. This subsection aims to elucidate the integration of traffic prediction and anomaly detection within AI-driven routing for enhanced network performance and resilience. It critically discusses the methodologies, performance trade-offs, and practical deployment challenges encountered in this emerging paradigm.

The integration of traffic prediction and anomaly detection into routing optimization represents a pivotal advancement, enabling proactive network management that anticipates and mitigates performance degradation rather than responding solely after it occurs. Traffic prediction models primarily leverage supervised learning combined with advanced time-series deep learning architectures, such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs), to forecast network load and congestion patterns. These models achieve high accuracy by capturing complex temporal dependencies but introduce trade-offs between prediction latency and computational complexity, which can impact real-time routing decisions and scalability [24]. For example, while RNNs provide detailed temporal modeling, their inference latency may not suit ultra-low-latency environments, necessitating simpler models or hardware acceleration.

Simultaneously, anomaly detection systems continuously monitor network operations to identify deviations caused by link failures,

Table 5: Summary of AI-Driven Routing Optimization Challenges and Solutions

Challenge	Description	Common Approaches
Exploration vs. Exploitation	Balancing discovery of new optimal routes with stability of known paths	Reinforcement learning, multi-armed bandits
Integration of Heterogeneous Data	Processing diverse and real-time network information	Data fusion, online learning
Uncertainty and Variability	Coping with dynamic and unpredictable network conditions	Robust learning, continual adaptation
Latency and Reliability Requirements	Ensuring performance under strict timing and availability constraints	Lightweight models, real-time optimization

cyber-attacks, or misconfigurations. These systems must balance sensitivity and specificity to minimize false positives, which, if excessive, can trigger unnecessary route recalculations resulting in network instability and performance degradation [39]. Techniques range from statistical thresholding to deep autoencoders, each presenting trade-offs between detection speed and accuracy.

Combining predictive traffic modeling with anomaly detection within AI-driven routing frameworks facilitates multi-objective optimization that simultaneously addresses performance, reliability, and security dimensions. This comprehensive approach enhances overall network resilience by preempting bottlenecks and containing fault propagation, surpassing the limitations of traditional static routing methods [39]. Empirical results from recent studies demonstrate up to a 30

Key challenges persist, including maintaining model accuracy under highly dynamic and non-stationary network conditions characterized by heterogeneous and large-scale data sources. Moreover, practical deployment faces limitations such as computational overheads of complex models, the need for representative and diverse training datasets to avoid overfitting, and integration with existing network infrastructures that may lack flexibility [24, 39]. Addressing these requires robust, generalizable models along with adaptive training strategies.

Recent advancements advocate incorporating reinforcement learning techniques, enabling routing policies to dynamically adjust based on evolving traffic states and detected anomalies. Such techniques improve scalability and real-time responsiveness, critical for modern network environments including 5G and software-defined networking (SDN) [39]. However, reinforcement learning introduces additional complexity in training and convergence guarantees, posing deployment hurdles.

In summary, the convergence of traffic prediction and anomaly detection within AI-driven routing paradigms presents a transformative framework underpinning self-optimization and enhanced robustness necessary for complex and emerging network architectures. Balancing model performance, computational demands, and integration challenges remains essential for practical widespread adoption.

3.7.8 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 [39**?**]. For instance, 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]. Specifically, [39] formulates routing as a multi-objective optimization integrating traffic prediction and anomaly detection, producing these empirical gains.

However, these benefits entail significant computational and communication overheads, especially in centralized learning architectures, which can become bottlenecks for real-time operation and scalability [39]. Addressing communication overhead, [**?**] proposes a robust federated learning framework employing gradient sparsification with error feedback mechanisms and adaptive client selection. This approach reduces communication costs from 120 MB to 55 MB and accelerates convergence from 200 to 150 rounds while maintaining test accuracy above 85% under adverse conditions such as 40% client dropout. The method balances communication efficiency against potential accuracy loss, exposing a nuanced tradeoff between compression levels and model performance.

These mechanisms demonstrate a viable path to mitigating the scalability challenge by exploiting client heterogeneity and unreliable wireless links common in real-world deployments. Moreover, adaptive client selection strategies selectively engage devices with sufficient resources and stable connectivity, maximizing effective participation without overwhelming network bandwidth. Such detailed comparative studies highlight how communication-efficient federated learning can sustain accuracy and robustness in resource-constrained environments.

Security vulnerabilities also arise from adversarial attacks targeting either training data or model inference stages, potentially degrading routing performance and compromising network stability [39**?**]. Mitigating these risks requires adopting robust, network-specific security protocols tailored for AI-integrated routing environments. Additionally, the integration of AI models within legacy network infrastructures introduces further complexity. Hybrid or modular deployment strategies are necessary to maintain backward compatibility and avoid service disruption, enabling continuous network operation alongside incremental AI adoption [18].

The demand for real-time inference combined with continuous model updates intensifies these challenges, forcing trade-offs among inference accuracy, responsiveness, and resource consumption. Lightweight AI model designs along with distributed and federated learning frameworks enhanced by security-aware mechanisms are essential to navigating these trade-offs [39**?**]. Continued innovation in adaptive compression techniques, coded computing, and privacy-preserving methods is critical to fully realizing the transformative potential of AI-driven routing in highly dynamic and heterogeneous next-generation networks.

3.7.9 Future Trends. Emerging directions in AI-based routing optimization increasingly emphasize decentralized and federated learning architectures to address the scalability and privacy challenges of

centralized methods. Federated learning allows multiple distributed clients or network nodes to collaboratively train a shared model without exchanging sensitive local data, thereby enhancing privacy and reducing communication overhead [39]. Advanced federated frameworks incorporate adaptive client selection and gradient sparsification techniques to efficiently handle heterogeneous device capabilities and client dropout, improving convergence speed and accuracy in real-world wireless environments [6].

Hybrid routing algorithms that combine AI techniques with conventional protocols show significant promise for delivering adaptive yet resource-efficient solutions. These hybrid schemes benefit from the heuristic strengths and stability of traditional protocols while leveraging machine learning components to enhance adaptability and predictive accuracy.

To provide a more concrete roadmap, near-term research (1-3 years) will focus on developing scalable federated learning models with privacy-preserving mechanisms and investigating their integration into existing SDN-based network infrastructures [39]. Within 3-5 years, efforts will likely shift towards optimizing hybrid AI-conventional routing algorithms that balance adaptability with computational efficiency, incorporating explainability and transparency methods to build operator trust. Longer-term challenges (5+ years) include extending AI-based routing to emerging paradigms such as 6G networks, massive MIMO, and edge computing ecosystems [6, 39], where the dynamic, high-dimensional nature of network environments demands fully autonomous, resilient, and scalable routing strategies.

Recent pioneering studies emphasize exploiting Reconfigurable Intelligent Surfaces (RIS) combined with AI as a promising avenue to dynamically optimize radio environments, which can be incorporated into routing decisions to enhance spectral and energy efficiency [6]. Parallel work demonstrates AI-driven routing frameworks using reinforcement learning to achieve up to 30% improvements in throughput and latency by adapting to real-time network states and failures [39].

Collectively, these advancements will play a critical role in achieving fully autonomous, scalable, and resilient routing architectures capable of dynamically adapting to complex, evolving network conditions, addressing key challenges such as computational overhead, scalability, and trustworthiness.

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

Open Radio Access Network (Open RAN) represents a significant paradigm shift in mobile network architecture by promoting openness, flexibility, and intelligence, which are fundamental for the evolution to 6G. The integration of Artificial Intelligence (AI) into Open RAN enables more efficient and adaptive network management, dynamic resource allocation, and optimized service delivery, all critical to meeting the stringent requirements of 6G such as ultra-low latency, massive connectivity, energy efficiency, and enhanced reliability.

AI techniques in Open RAN empower intelligent radio resource management by dynamically optimizing spectrum usage, power control, and interference mitigation across disaggregated and virtualized network components. Advanced machine learning models can predict traffic demand, user mobility, and network anomalies, allowing proactive and real-time adaptation of network functions to consistently satisfy 6G performance targets. Moreover, AI-driven automation facilitates robust self-organizing and self-healing capabilities within the RAN, significantly reducing operational expenditures while enhancing user Quality of Experience (QoE).

Beyond operational efficiency, AI integration enhances the security posture of Open RAN by continuously monitoring for anomalies, detecting cyber threats, and enabling rapid response mechanisms. This security aspect is especially critical as 6G networks are expected to underpin safety-critical applications including autonomous vehicles, remote healthcare, and industrial automation. The modular and open interface architecture of Open RAN further supports continuous deployment and online training of AI models, accelerating innovation cycles and enabling customized solutions tailored to diverse deployment contexts in 6G ecosystems.

In summary, embedding AI within Open RAN is a cornerstone for unlocking the full potential of 6G networks. It provides adaptive, intelligent orchestration and control that align with the complex, dynamic, and heterogeneous demands of future wireless communication systems, paving the way toward sustainable, resilient, and high-performing 6G infrastructures.

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. It supports advanced techniques such as federated learning, which preserves user privacy by enabling distributed intelligence without sharing raw data, and reinforcement learning, which adapts scheduling policies dynamically in response to changing network conditions. Leveraging standardized telemetry data, AI agents perform real-time analytics and closed-loop control that significantly improve throughput, latency, energy efficiency, connection reliability, and resource utilization [25].

Overall, multilayer AI integration in Open RAN marks a paradigm shift towards automated, optimized, and innovative next-generation networks, laying a robust foundation for resilient and user-centric 6G systems, while addressing challenges related to computational overhead, interoperability, and data quality.

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 plays a pivotal role by enabling distributed model training across the RU, DU, and CU layers without exchanging raw data, thus preserving user privacy and effectively managing the multi-vendor and multi-domain heterogeneity characteristic of Open RAN ecosystems. This decentralization fosters collaborative intelligence while securing sensitive information [25]. Reinforcement learning (RL), particularly deep RL, facilitates autonomous decision-making for dynamic spectrum management, adaptive resource allocation, and interference mitigation by learning optimal policies through interactions with complex, time-varying network environments. These AI-driven methods empower the network to continuously adapt and optimize performance in real time [1, 37]. Deep neural networks (DNNs) are extensively employed for tasks demanding sophisticated pattern recognition and nonlinear function approximation, such as fault detection and anomaly identification, utilizing large volumes of standardized telemetry data harvested within Open RAN infrastructures [22, 30].

Furthermore, hybrid fusion techniques showcase AI's flexibility in handling heterogeneous communication modalities and interference mitigation. For example, combining visible light communication (VLC) and radio frequency (RF) channels leverages machine learning-based fusion and interference cancellation algorithms to bolster robustness in challenging propagation conditions [26]. This VLC-RF hybrid strategy exploits the complementary physical properties of both communication methods, enhancing overall communication reliability and throughput. Additionally, AI-informed sequence management approaches optimize the design of high-capacity preamble sequences for random access channels. These advancements markedly reduce collision probabilities by increasing the number of unique preambles exhibiting low cross-correlation and strong auto-correlation properties, thereby improving detection accuracy and decreasing retransmission overhead. Such capabilities are vital for supporting the massive IoT device connectivity demands intrinsic to 5G and beyond [37].

Despite these technological advances, practical deployment of AI within Open RAN confronts several significant challenges. These include the computational burdens imposed by real-time model training and inference, complexities in coordinating AI functionalities across heterogeneous multi-vendor equipment, and ensuring scalability and seamless interoperability within fluid, dynamic network conditions. Addressing these obstacles is essential to fully realize the potential of AI-powered Open RAN networks [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]. AI methods, such as supervised, unsupervised, and deep reinforcement learning, play a pivotal role in optimizing RIS functions including channel estimation, beamforming, and resource allocation by learning complex mappings from channel states to optimal RIS configurations. These AI-driven 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].

However, despite these promising improvements, AI integration in Open RAN is not without its limitations and challenges. Some deployments have experienced issues related to the high computational overhead and latency introduced by complex AI models, which can impact real-time decision-making and network responsiveness [25]. Additionally, model convergence difficulties and data quality variability sometimes lead to suboptimal or inconsistent performance gains. In environments with multi-vendor components, interoperability challenges further complicate seamless AI orchestration across the Open RAN ecosystem [25]. Security vulnerabilities arising from AI model attacks or misconfigurations remain an important concern that can affect network reliability and integrity. Moreover, while AI-enabled RIS shows significant theoretical gains, practical implementations must address the high-dimensional configuration spaces and stringent latency requirements, which may limit performance improvements or increase deployment complexity [6].

Acknowledging these trade-offs, ongoing research emphasizes lightweight AI models tailored for edge deployment, federated learning to enhance privacy and scalability, and robust fault tolerance mechanisms [25]. This balanced approach aims to maximize performance enhancements while mitigating the risks and challenges identified in less successful deployments. Thus, AI-empowered Open RAN holds great promise as a cornerstone for resilient, efficient, and sustainable 6G networks, contingent upon continued

advances in model efficiency, standardization, and security practices.

4.4 Challenges

The integration of AI into Open RAN architectures introduces several critical challenges that must be systematically addressed to realize its full potential. This subsection clarifies these challenges through illustrative examples, ties them explicitly to previously discussed methodologies, and proposes directions for overcoming them. Our objective is to provide a clear understanding of the technical and operational barriers hindering AI-driven Open RAN deployments and identify top research priorities.

4.4.1 Model Convergence in Dynamic Environments. A primary challenge lies in ensuring AI model convergence within the dynamic, non-stationary nature of wireless channels characterized by partial observability. Reinforcement learning approaches, while promising for adaptive resource management, can experience instability due to rapidly fluctuating radio conditions, as demonstrated in [25]. For instance, a reinforcement learning scheduler may fail to stabilize when channel statistics shift unexpectedly, leading to suboptimal network throughput and increased latency. This raises key research questions: how to design reinforcement learning algorithms with robust convergence properties under transient states, and how to enable real-time adaptation mechanisms that guarantee reliable decision-making despite environmental uncertainties?

4.4.2 Computational and Energy Constraints at the Edge. Deploying complex AI models at the edge units such as RUs and DUs presents significant limitations due to processing capacity and energy constraints [18, 25]. For example, interference mitigation using deep learning demands low-latency inference on resource-constrained hardware, creating a trade-off between model complexity and operational feasibility. Results in [18] show that AI-driven interference prediction can reduce sensing interference by 30% but only if latency remains within strict bounds. Hence, lightweight AI architectures and hardware-software co-design are critical. Research must balance inference latency, energy consumption, and accuracy, interrogating how novel accelerators and compact models can optimize this balance without sacrificing performance.

4.4.3 Multi-Vendor Interoperability. The heterogeneity of Open RAN components from multiple vendors complicates interoperable AI deployment [6, 25]. For instance, integrating intelligent Reconfigurable Intelligent Surfaces (RIS) optimized by AI requires harmonizing diverse hardware interfaces and data formats, as detailed in [6]. The absence of unified standards impedes seamless AI model sharing and operation across vendors, affecting scalability and maintenance. This challenge prompts exploration of middleware frameworks and standardization efforts capable of aligning data representation and AI interfaces while preserving security and efficiency.

4.4.4 Security and Privacy Risks. Increased AI complexity amplifies vulnerabilities to adversarial attacks and privacy breaches within Open RAN [24, 25]. AI models trained via federated learning risk information leakage, and adversaries can exploit weaknesses to mislead AI-driven network management. For example, [24] discusses emerging threats like adversarial intrusions that degrade service quality and confidentiality. Thus, developing real-time intrusion detection, robust AI architectures resilient to attacks, and privacy-preserving learning protocols is paramount. These efforts must also navigate regulatory compliance across jurisdictions.

4.4.5 Regulatory and Governance Challenges. Finally, regulatory requirements for data sovereignty, user privacy, and algorithmic transparency dictate stringent constraints on AI deployment [18, 25]. Explainable AI frameworks and auditability mechanisms become essential to ensure trust and accountability, especially given evolving policies across global operators.

4.4.6 Top Research Priorities. Based on the discussion above, the three most critical research priorities are: (1) developing scalable and explainable AI algorithms that ensure stable learning and adaptation in time-varying environments, (2) creating efficient edge AI solutions via co-designed hardware and lightweight models to meet stringent latency and energy requirements, and (3) advancing interoperable AI frameworks coupled with rigorous security and privacy safeguards conforming to regulatory mandates. Addressing these priorities requires multidisciplinary initiatives that integrate communications theory, AI, hardware design, and regulatory insight.

In summary, overcoming the outlined challenges calls for both theoretical innovations and practical engineering. Integrating insights from [6, 18, 24, 25] highlights that while AI significantly enhances Open RAN capabilities, realizing these benefits demands robust convergence techniques, efficient edge deployment strategies, seamless multi-vendor support, and comprehensive security and governance models. Only through such coordinated efforts can AI-driven Open RAN systems deliver adaptive, secure, and efficient wireless networks suited 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]. To measure progress, development of standardized evaluation metrics and benchmarks tailored to Open RAN scenarios is essential. These could include quantifiable indicators such as explanation fidelity, user trust scores, and impact on fault resolution times. Furthermore, pilot studies and experimental platforms simulating multi-vendor Open RAN environments should be established to validate XAI methods and assess their operational effectiveness in realistic settings.

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

Table 6: Summary of Challenges in AI-Driven Open RAN and Potential Mitigation Strategies

Challenge	Description	Potential Mitigation Strategies
Model convergence	Instability of AI models in dynamic, partially observed wireless environments [25]	Design robust reinforcement learning algorithms; Real-time adaptation mechanisms; Multi-agent collaboration
Edge resource constraints	Limited computation and energy in RUs/DUs hindering complex AI inference [18, 25]	Lightweight AI architectures; Hardware-software co-design; Specialized AI accelerators
Multi-vendor interoperability	Diverse hardware and data formats impeding unified AI deployment [6, 25]	Middleware frameworks; Adoption of open standards (e.g., O-RAN, 3GPP); Standardized AI model interfaces
Security and privacy	Vulnerabilities to adversarial attacks and data leakage in federated/distributed learning [24, 25]	Real-time intrusion detection; Robust and privacy-preserving learning protocols; Federated learning with differential privacy
Regulatory compliance	Compliance with data sovereignty, privacy laws, and need for transparency [18, 25]	Explainable AI; Auditability frameworks; Policy-aware AI model design

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].

To structure these efforts effectively, future research goals can be categorized into short-, mid-, and long-term milestones. In the short term, objectives include developing robust explainable AI models with appropriate evaluation metrics, conducting pilot studies on multi-agent collaborative frameworks to improve transparency and coordination, and formulating specific research questions such as: "How can XAI techniques optimize AI decision interpretability without compromising performance in Open RAN?" or "What mechanisms best facilitate multi-agent collaboration across distributed RAN units?" Mid-term priorities focus on creating and deploying lightweight AI algorithms alongside hardware accelerators to meet the demands of edge computing in Open RAN environments. Key research hypotheses might explore trade-offs between model complexity and latency in resource-constrained settings. Long-term ambitions target the integration of emerging technologies such as quantum computing and blockchain to revolutionize optimization, security, and trustworthiness in Open RAN. Achieving these milestones will provide measurable improvements, including enhanced AI interpretability, reduced computational latency, increased network resilience, and stronger multi-vendor interoperability.

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 aims to provide a comprehensive overview of how Large Language Models (LLMs) can be integrated within agentic AI frameworks to enhance the resilience of Open Radio Access Network (O-RAN) systems. The key objectives include outlining the architectural design of LLM-driven agents, analyzing their operational roles in dynamic network management, and comparing their capabilities against alternative AI methods for fault detection and mitigation. Additionally, we discuss deployment feasibility, cost considerations, and emerging paradigm intersections to offer a well-rounded perspective on autonomous resilience in O-RAN environments.

5.1 Overview and Objectives

Agentic AI systems possess autonomous perception, reasoning, and decision-making abilities to operate independently toward specified goals. When enhanced by LLMs, these agents gain advanced natural language understanding and contextual reasoning, enabling sophisticated analysis of complex network states. The primary functions of LLM-driven agents in O-RAN include proactive fault and anomaly detection, diagnostic root-cause analysis, and automated mitigation through reconfiguration commands. By integrating these capabilities, the agents aim to improve network reliability and adaptability with scalable control strategies.

5.2 Architectural Design and Data Flow

At a high level, the agentic AI architecture incorporates multi-source data inputs such as telemetry metrics and performance indicators, which the LLM processes to construct situational awareness. This enriched context feeds into decision-making modules responsible for selecting optimal actions that influence network state via O-RAN control interfaces. A continuous feedback loop supports learning and responsiveness to evolving conditions, ensuring the agent maintains relevance as network dynamics shift. The structured data flow and agent components enable adaptive control while preserving operational transparency.

5.3 Comparative Analysis with Alternative AI Approaches

Unlike traditional machine learning and rule-based systems commonly used for fault management, LLM-driven agentic AI offers enhanced reasoning capabilities and flexibility. This allows for more nuanced interpretation of network anomalies and context-aware decision-making beyond simple pattern recognition. However, compared to established methods, challenges remain in computational overhead and real-time responsiveness, especially in edge deployments. Balancing these trade-offs involves considering operational scale, latency requirements, and available computational resources.

5.4 Deployment Feasibility and Cost Considerations

Implementing LLM-based agents in edge O-RAN environments raises practical concerns including hardware constraints, latency sensitivity, and resource consumption. While LLMs deliver superior reasoning, their computational demands may exceed edge device capacities without optimization strategies such as model pruning or distillation. Cost implications also stem from the need for robust connectivity and maintenance overhead. Future efforts must explore lightweight model adaptations and hybrid architectures combining

LLM reasoning with conventional control algorithms to enable feasible, cost-effective deployment.

5.5 Emerging Paradigms and Future Directions

The integration of LLM-driven AI with emerging technologies such as quantum computing and blockchain presents promising avenues to further enhance network resilience. Quantum computing could accelerate complex reasoning tasks, while blockchain may ensure secure, tamper-evident agent interactions and decision audit trails. Investigating these synergies could yield more robust, trustworthy autonomous systems capable of managing next-generation O-RAN infrastructures.

In summary, LLM-driven agentic AI provides a powerful approach for autonomous, adaptive network control in O-RAN. By addressing deployment challenges and exploring complementary technologies, future research can advance this paradigm towards stable, scalable, and cost-efficient resilience solutions.

Cross-references to the following subsections detail the structural design of agent architectures and the data flow mechanisms that support these autonomous and context-aware operations, thereby highlighting the practical pathways for implementing LLM-driven resilience strategies.

5.6 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)—marks a significant advancement toward achieving autonomous fault management. Embedding these agents enables continuous, context-aware monitoring of diverse network telemetry data combined with dynamic remediation strategies executed without human intervention. This autonomy surpasses traditional rule-based or supervised learning systems, which typically depend on predefined fault catalogs or manual threshold triggers. Leveraging LLMs' intrinsic ability to parse and synthesize heterogeneous 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 performed on a simulated O-RAN testbed demonstrate 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]. Table 7 summarizes key performance improvements over baseline techniques, showcasing the method's enhanced robustness and efficacy in handling complex fault scenarios. Furthermore, the modularity and open interfaces inherent to the O-RAN framework facilitate seamless integration of LLM-based agents, enabling customizable behaviors and scalable deployments that significantly enhance operational flexibility and reduce mitigation times.

Despite these promising results, several challenges remain critical. These include the computational overhead of running LLMs in near-RT environments, the risk of occasional erroneous decisions affecting network stability, security vulnerabilities exposing the system to adversarial threats, and interoperability issues among different vendor implementations. Proposed mitigations encompass hierarchical agent architectures to distribute computational loads efficiently, rigorous validation frameworks to ensure reliability of decisions, and robust security mechanisms to safeguard against attacks. Future research directions focus on optimizing these LLM agents for deployment at edge environments, enhancing multi-agent coordination techniques, incorporating explainability features to improve transparency and trust, and reinforcing security robustness. Collectively, these advancements underscore the promising role of LLM-based agents in strengthening O-RAN self-healing capabilities and operational resilience in next-generation networks.

5.7 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 from a simulated O-RAN environment demonstrate that this approach increases fault detection accuracy from 78% to 95% and improves mitigation success rates from 70% to 91%, significantly reducing network downtime by 40% and decreasing throughput degradation from 25% to 10% [5]. Table 10 summarizes these performance improvements, illustrating the substantial gains achieved by incorporating LLM-driven NLP for fault interpretation.

This integrative process addresses critical concerns related to model interpretability, acceptance, and operational resilience during live network operations, while also highlighting challenges such as computational overhead and ensuring robustness against erroneous decisions. The use of hierarchical agent designs and rigorous validation methods has been proposed to mitigate these challenges, promoting reliable and transparent AI-human collaborative fault management [5].

5.8 Experimental Achievements

Empirical evaluations demonstrate that integrating LLM-based agentic AI within the O-RAN architecture significantly enhances fault management capabilities. Experimental results indicate fault detection accuracy reaching up to 95%, representing a substantial

Table 7: Performance Comparison of LLM-Based Agentic AI Approach vs. Baseline in O-RAN Fault Management

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

Table 8: Performance Comparison of LLM-driven Agentic AI in O-RAN Fault Management [5]

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

improvement over baseline accuracies of approximately 78% [3, 5, 14]. Mitigation success rates improve by more than 20%, while network downtime is reduced by nearly 40%. Additionally, throughput degradation decreases from about 25% in baseline systems to approximately 10%, illustrating more efficient and resilient network operation [5].

These enhancements result from the agentic AI's capability to proactively anticipate faults and execute diverse, context-aware responses, outperforming traditional heuristic or static rule-based methods which often produce delayed or partial fault handling [14]. Improvements in throughput further reflect real-time resource optimization and adaptive network reconfiguration autonomously performed by agents embedded within the RIC and SMO layers, validating both the practical feasibility and operational effectiveness of the proposed architecture [5].

Table 10 summarizes the key performance improvements observed experimentally, highlighting significant gains in detection accuracy, mitigation success, downtime reduction, and throughput degradation compared to baseline O-RAN implementations.

These results underscore the potential of LLM-driven agentic AI to enhance the resilience of next-generation wireless networks by enabling intelligent, autonomous fault management that dynamically adapts to network contexts. While challenges such as computational overheads and security considerations remain, ongoing work focuses on mitigation strategies including hierarchical agent design and rigorous validation to address these issues [5].

5.9 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.

Notably, the continuous learning capabilities embedded in these agent architectures promote sustained performance improvements by dynamically adapting to evolving network topologies and traffic profiles. This adaptive proficiency positions agentic AI as a markedly superior solution for managing the increasing heterogeneity and scale of next-generation wireless infrastructures. Additionally, by integrating LLM-based agents within key O-RAN components such as the Near-RT RIC and SMO, the system autonomously monitors network telemetry, interprets faults using natural language processing, and executes mitigation strategies including dynamic resource re-allocation and self-healing operations [5]. These capabilities collectively contribute to enhanced resilience and robustness beyond that achievable with traditional approaches.

5.10 Recognized Challenges

Despite these significant advancements, deploying LLM-based agentic AI within O-RAN architectures poses several critical challenges. First, the computational overhead inherent to large-scale LLM inference raises pressing concerns regarding latency and energy efficiency, especially within resource-constrained edge environments [5, 18]. Addressing this issue requires targeted optimization of LLM architectures to enable real-time, low-power operation suitable for edge deployment, as highlighted in recent work focusing on AI-powered interference management and efficient network sensing [5, 18]. Second, the potential for inaccuracies arising from incomplete or noisy input data, entrenched model biases, or adversarial conditions threatens network stability by causing erroneous decision-making. Mitigating these risks necessitates robust data preprocessing techniques, stringent model validation, and advanced adversarial resilience mechanisms to ensure reliability. Third, AI-specific security vulnerabilities—including data poisoning and model inversion attacks—demand comprehensive, multilayered

Table 9: Performance Comparison of Agentic AI-Enabled O-RAN vs. Baseline Systems

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

Table 10: 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%

safeguards to protect data integrity and preserve model confidentiality. Lastly, ensuring seamless interoperability of LLM agents within heterogeneous, multi-vendor ecosystems characterized by proprietary interfaces and diverse data semantics remains an unresolved challenge, complicating standardized deployment [5, 18]. Approaches such as hierarchical agent design combined with rigorous validation protocols have shown promise in tackling this complexity. Collectively, these challenges underscore the multifaceted difficulty of operationalizing agentic AI at scale while maintaining network performance, reliability, and security.

5.11 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 incorporating 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, significantly reducing computational demands without sacrificing 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. These evaluations have shown fault detection accuracy improvements from 78% to 95%, mitigation success rates increasing from 70% to 91%, a 40% reduction in network downtime, and a significant decrease in throughput degradation from 25% to 10% [5]. Table 11 summarizes these performance gains, underscoring the effectiveness of the proposed optimization strategies in enhancing O-RAN self-healing and operational reliability.

5.12 Future Directions

This subsection outlines clear objectives and a detailed roadmap for advancing agentic AI capabilities in complex O-RAN ecosystems. The goal is to develop scalable, resilient, secure, and interpretable AI frameworks that enable autonomous, real-time adaptation in distributed and resource-constrained network environments.

5.12.1 Multi-Agent Coordination. Future research should focus on enabling efficient and robust cooperation among distributed AI agents for fault detection and mitigation across RAN nodes. Key objectives include designing synchronization protocols that maintain ultra-low latency and ensuring backward compatibility without performance losses. Concrete milestones involve developing lightweight consensus mechanisms and experimentally validating their scalability in large-scale deployments [37]. Addressing computational complexity in real-time processing remains critical to practical applicability.

5.12.2 Explainability and Operator Trust. Advancing explainability techniques is essential for fostering operator confidence and regulatory compliance. Research should aim to integrate AI interpretability with control theory and wireless signal processing to develop hybrid models that deliver actionable insights with minimal latency [18]. A central challenge lies in balancing model complexity and clarity, and innovating visualization tools tailored to operator workflows. Short-term goals include prototyping operator-centric dashboards and conducting user studies to assess effectiveness.

5.12.3 Security and Robustness. Safeguarding O-RAN AI agents against evolving cyber threats is paramount. Priorities include developing adversarially robust training methods, secure and efficient model update protocols, and real-time anomaly detection at the network edge [24]. Research should quantify overhead thresholds for security mechanisms under typical edge resource constraints and anticipate emerging attack vectors in dynamic network topologies.

Table 11: Performance Improvements of LLM-Driven Agentic AI in O-RAN Self-Healing [5]

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

Milestones incorporate deploying prototype defenses in realistic O-RAN testbeds and benchmarking their impact on network performance.

5.12.4 Deployment Architectures. Addressing the tradeoffs between accuracy, latency, and resource utilization necessitates novel architectural frameworks that synergize edge and cloud computing [24]. Key research questions involve orchestrating decentralized AI inference alongside centralized model updates with minimal communication overhead. Roadmap activities include defining standardized interfaces for modular AI components and empirically measuring system-level latency and throughput under varying traffic loads.

5.12.5 Adaptive Resource Allocation and Network Autonomy. To support massive IoT deployments and dynamic network conditions, there is a pressing need to transition from static policies to fully autonomous, self-optimizing networks [37]. Integrating reinforcement learning for dynamic resource allocation with robust forecasting and anomaly detection frameworks is a promising approach. Open challenges include modeling temporal dependencies and environmental uncertainties effectively. Immediate research goals involve developing benchmark datasets and simulation platforms to evaluate RL algorithms' adaptability and robustness.

5.12.6 Implementation Pathways and Benchmarking. A concrete implementation pathway entails developing open-source toolkits and standardized benchmarks to evaluate agentic AI methods in O-RAN contexts. Such initiatives would accelerate reproducibility, facilitate cross-comparison of techniques, and foster community collaboration. Proposed benchmarks should cover metrics across latency, throughput, energy efficiency, security resilience, and explainability quality, aligned with the challenges summarized in Table 12.

In summary, these directions form an interconnected roadmap that explicitly links practical implementation considerations with theoretical challenges addressed in prior sections. Achieving these objectives will require interdisciplinary collaboration, scalable system design, and iterative validation to realize sustainable, trustworthy, and high-performance AI-enabled O-RAN networks.

6 Adaptive Control and Reinforcement Learning in Networking Systems

This section aims to provide a focused overview of adaptive control and reinforcement learning (RL) techniques applied to networking systems, highlighting their capabilities, limitations, and roles within modern communication environments such as O-RAN and 6G networks. We clarify key concepts, discuss representative case studies, and examine the synergy between gradient-based adaptive control and RL for dynamic network management.

Adaptive control and 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 emphasis is placed on gradient-based adaptive control methods. These approaches use 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 adjusts sending rates to optimize throughput and minimize delay, effectively responding to network dynamics. The strengths of gradient-based methods include their straightforward implementation and well-understood convergence properties under smooth cost landscapes. However, these methods can face challenges when the cost surface is complex or non-differentiable, potentially limiting their applicability in highly dynamic or stochastic networking environments.

Reinforcement learning extends beyond model-based approaches by enabling network agents to learn optimal control policies through direct environment interaction without requiring explicit models. This model-free nature suits complex or partially observable network scenarios where accurate modeling is infeasible. Classical RL algorithms, such as Q-learning and policy gradient methods, have been successfully applied to routing optimization, resource allocation, and energy-efficient management in wireless networks. Nonetheless, RL approaches often suffer from limitations including sample inefficiency, difficulty in handling high-dimensional state and action spaces, and challenges in ensuring safety and robustness during exploration, especially in mission-critical networking contexts.

To illustrate these concepts, consider a case study in adaptive routing where an RL agent optimizes path selection with the goal of minimizing latency and packet loss across fluctuating network topologies. Employing policy gradient methods, the agent incrementally refines its routing policy based on reward signals tied to successful data delivery, enabling adaptive and efficient routing in real time. This example demonstrates how gradient-based optimization and RL can synergize to handle dynamic and stochastic network environments effectively.

Integrating gradient-based adaptive control methods within reinforcement learning frameworks further enhances performance by blending the sample efficiency and theoretical guarantees of gradient methods with the flexibility of RL policies. Hybrid algorithms have shown promise in scenarios demanding rapid adaptation to

Table 12: Summary of Future Research Challenges and Concrete Objectives in Agentic AI for O-RAN

Research Area	Key Challenges	Concrete Objectives and Milestones
Multi-Agent Coordination	Synchronization latency, backward compatibility, computational complexity	Design scalable low-latency synchronization protocols validated on large deployments; Develop lightweight consensus algorithms ensuring compatibility [37]
Explainability	Model complexity vs. interpretability, operator visualization, real-time constraints	Integrate control theory with signal processing for interpretable models; Prototype operator dashboards and conduct usability evaluations [18]
Security	Adversarial robustness, secure updates, edge anomaly detection	Implement adversarial training and secure model update protocols; Benchmark defenses in edge resource-constrained scenarios [24]
Deployment Architecture	Edge-cloud synergy, latency, resource management	Develop modular AI component interfaces; Measure latency and throughput in hybrid edge-cloud setups [24]
Adaptive Resource Allocation	Dynamic environments, temporal modeling, real-time learning	Create benchmarks and simulation platforms to test RL-based allocation; Model temporal dependencies and environmental uncertainty [37]

changing network conditions, yet these combined methods also inherit and sometimes amplify the individual limitations such as computational complexity and sensitivity to hyperparameters.

Despite these advances, significant challenges remain for deploying RL and adaptive control in open radio access networks (O-RAN) and emerging 6G systems. Issues include the curse of dimensionality in state and action spaces, requirements for low-latency, real-time decision-making under partial observability, and the need to maintain robust performance amid the openness and heterogeneity intrinsic to O-RAN infrastructures. Moreover, balancing exploratory learning with stringent safety requirements to avoid degraded service is critical but difficult. Addressing these challenges motivates ongoing research into scalable, safe, and interpretable RL algorithms tailored to the unique constraints of these advanced network architectures.

Adaptive control methods also play a crucial complementary role by ensuring continuous parameter tuning and system stability, vital for integrating learning-based agents into operational network cycles. This synergy becomes increasingly relevant with the incorporation of large language model (LLM)-driven agent architectures, where LLMs provide high-level reasoning that can guide RL agents' exploration and adaptation strategies. The integration of adaptive control, reinforcement learning, and LLM-driven intelligence holds promise for creating more responsive, interpretable, and robust network management agents suited to the complexities of next-generation communication systems.

In summary, adaptive control and reinforcement learning form a powerful combined toolkit for enhancing the performance and resilience of networking systems. Gradient-based methods offer principled mechanisms for continuous adaptation, while RL facilitates operation in uncertain and partially known environments. The advancement and integration of these methodologies with cutting-edge LLM-driven architectures produce robust, efficient network control solutions capable of meeting the evolving demands of infrastructures such as O-RAN and 6G. However, critical challenges related to scalability, safety, and interpretability must be addressed to realize their full potential in real-world deployments.

The following sections build upon these foundational concepts by delving into specific gradient-based algorithms and reinforcement learning case studies, illustrating their application across a broad range of networking scenarios with improved clarity and depth.

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 the 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 multi-hop 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—such as convolutional and recurrent architectures—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, which utilize frequency bands from sub-6 GHz to millimeter-wave and terahertz bands with widely differing propagation and interference characteristics, complicating control and necessitating flexible RL-driven resource allocation strategies [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, advanced analytical frameworks for optimal control on networked systems, such as modal decomposition grounded in network spectral properties, complement RL approaches by providing interpretable and computationally scalable solutions [17, 21]. For example, modal decomposition techniques decouple network dynamics into independent eigenmodes, facilitating efficient control design with reduced complexity and enhanced scalability, often achieving significant cost reductions and faster computations compared to classical methods.

Despite these 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, deploying RL in latency-sensitive and resource-constrained environments is limited by the computational overhead of both inference and training. To address this, efforts focus on lightweight model architectures, hardware acceleration, and hybrid optimization algorithms that blend RL with classical control and optimization methods [2**?**]. For instance, combining RL with learn-and-adapt stochastic dual gradient algorithms exploits the strengths of both learning-based adaptation and analytical optimization for improved network resource management and queue stability under uncertainty.

Collectively, these developments position reinforcement learning as a transformative tool for autonomous, efficient, and scalable management of increasingly complex wireless networks, particularly within emerging 5G and 6G paradigms where dynamic adaptability and intelligent resource allocation are paramount [24**?**]. Continued integration of RL with domain-specific knowledge, advanced optimization frameworks, and real-time analytical models promises further enhancements in performance, robustness, and interpretability of network control solutions.

6.2 Deep Reinforcement Learning for Online Adaptation

Deep reinforcement learning (DRL) enhances traditional reinforcement learning by utilizing deep neural networks as function approximators for policies or value functions, enabling effective online adaptation in complex networking tasks such as decision-making, resource allocation, and adaptive bandwidth management [20, 24**? ? ?**]. DRL is especially beneficial in high-dimensional state and action spaces where explicit policy design is impractical, covering applications like dynamic spectrum allocation, power control, and admission control [20**?**].

Through continuous interaction with the environment, DRL facilitates dynamic adaptation of resource management policies that respond to fluctuating network conditions, frequently outperforming heuristic or static methods. Hybrid frameworks that combine DRL with optimization techniques have demonstrated faster convergence and improved performance in resource-constrained settings—for instance, federated learning (FL) systems operating over wireless networks with heterogeneous bandwidth capabilities [24]. Moreover, embedding domain-specific knowledge into DRL architectures helps balance exploration and exploitation, a critical factor for real-time adaptability.

Nevertheless, employing DRL in networking systems introduces challenges, including substantial requirements for training data, limited interpretability of learned models, risks of overfitting, and stability issues in non-stationary environments [**?**]. To mitigate these concerns, mechanisms such as experience replay buffers, target networks, and transfer learning are commonly applied. Achieving an optimal balance between model expressiveness and computational efficiency remains an active research focus, particularly given the stringent latency and scalability demands of emerging wireless networks. Future developments will likely center on adaptive AI models capable of real-time optimization, cross-layer integration, and enhanced robustness, aiming to fulfill ultra-low latency and massive connectivity objectives envisioned for beyond-5G and 6G systems [24**?**].

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 [**? ?**].

Notably, [**?**] highlights that AI-assisted network slicing frameworks leverage RL to dynamically allocate resources and control slice admission, adapting to the fluctuating traffic and QoS requirements characteristic of next-generation wireless networks. This approach integrates advanced learning methods including federated learning and deep learning for traffic prediction, allowing intelligent, adaptive slicing with improved throughput, latency, resource utilization, and QoS provisioning. Similarly, advances in optical wireless communications (OWC) for 6G networks [**?**] present additional challenges due to channel variability and device heterogeneity, necessitating RL policies that can swiftly adapt while maintaining robustness. The integration of OWC with conventional RF systems faces difficulties such as atmospheric effects and system alignment, which RL can help address through adaptive policies sensitive to environmental changes.

These case studies underscore the importance of integrating domain-specific knowledge with advanced RL strategies to meet the rigorous demands of emerging network technologies and to balance AI model complexity with the operational constraints of ultra-reliable, low-latency network applications.

6.4 Federated and Distributed Reinforcement Learning

Federated reinforcement learning (FRL) and distributed reinforcement learning paradigms have attracted considerable interest in networking systems due to their capacity 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 regulatory compliance.

To tackle communication constraints typical of bandwidth-limited wireless environments, techniques like gradient sparsification and

adaptive client selection are deployed to minimize communication overhead [6]. Recent research has shown that FRL preserves robust policy performance despite client dropout and heterogeneous data distributions by employing mechanisms such as error feedback and weighted aggregation of client updates [6]. Additionally, integrated resource allocation approaches simultaneously optimize bandwidth and computational resources, resulting in accelerated training convergence and improved accuracy in FL-based wireless networks [24].

Nonetheless, significant challenges persist, including the synchronization of distributed RL agents, mitigating delays arising from straggling clients, and defending against adversarial attacks. Future research is expected to focus on developing asynchronous FRL algorithms to enhance training efficiency, incorporating stronger privacy-preserving techniques such as differential privacy to protect sensitive information, and designing scalable architectures capable of handling the complexity of forthcoming 6G networks. These directions align with broader AI-driven network optimization objectives and are essential for fully realizing FRL's potential in next-generation wireless environments.

6.5 Integration Across Networking Frameworks

The efficacy of reinforcement learning (RL) and adaptive control techniques is significantly enhanced when integrated with complementary AI-driven networking frameworks such as network traffic classification, software-defined networking (SDN), and routing optimization [13, 16, 39]. Deep learning-based traffic classification models provide granular insights into network flow characteristics, effectively overcoming the limitations of traditional methods—such as port-based and deep packet inspection approaches—that struggle with encrypted and dynamic traffic patterns. These advanced models enable RL controllers to optimize resource allocation with greater accuracy and adaptability by prioritizing traffic types based on detailed classification results [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 learning classifiers (e.g., Random Forest, SVM) and deep learning models (e.g., LSTM networks) to perform real-time traffic classification, anomaly detection, and dynamic resource allocation. This integration results in significant performance improvements, as demonstrated by up to 92% traffic classification accuracy, an 18% reduction in end-to-end latency, and increased throughput in 5G and beyond network scenarios [13]. Similarly, RL-based routing protocols adaptively select communication paths by continuously learning from traffic dynamics, balancing load, mitigating congestion and failures, and thereby enhancing network resilience and efficiency [39].

These cross-framework synergies facilitate comprehensive network adaptation strategies, where RL agents leverage enriched contextual information and explicit control channels provided by SDN. However, the integration of multiple AI modules introduces challenges such as elevated computational overhead, interoperability complexities, potential security vulnerabilities, and risks of cascading failures. Addressing these challenges necessitates efforts toward standardization and the development of modular, lightweight AI pipelines optimized for real-time operation. Moreover, incorporating explainable AI technologies is vital for maintaining transparency and manageability in autonomous network operations. Future research directions emphasize privacy-aware federated and decentralized learning approaches to enhance scalability and security within 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 enhance computational efficiency and convergence stability.

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

The integration of efficient gradient computations with fast update mechanisms has produced scalable frameworks that facilitate real-time learning and responsiveness in complex models. Continuous developments strive to improve the balance between computational speed and optimization accuracy, thereby augmenting 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.

Table 13: Summary of AI Integration Across Networking Frameworks: Benefits and Challenges

Framework	AI Techniques	Key Benefits	Challenges
Network Traffic Classification [16]	Supervised ML (Random Forest, SVM), Deep Learning (CNN, RNN)	High accuracy in encrypted/dynamic traffic classification; Enables prioritized resource allocation	High computational cost; Data imbalance; Encryption limits payload visibility; Concept drift
Software-Defined Networking (SDN) [13]	Supervised classifiers (Random Forest, SVM), LSTM networks	Up to 92% traffic classification accuracy; 18% latency reduction; Increased throughput; Real-time traffic management	Computational overhead; Dataset scarcity; Interoperability; Security risks; Need for lightweight models
AI-Driven Routing Optimization [39]	Reinforcement Learning, Neural Networks	Adaptive path selection; 30% throughput and latency improvement; Enhanced fault tolerance	Scalability; Model training data representativeness; Security vulnerabilities; Integration complexity

Table 14: Summary of Gradient-Based Optimization Techniques and Fast Update Algorithms

Technique	Key Characteristics	Advantages	Typical Use Cases
Stochastic Gradient Descent (SGD)	Updates parameters using noisy gradient estimates from random samples	Computationally efficient; scalable to large datasets	Large-scale supervised learning
Mini-batch Gradient Descent	Uses small batches for gradient estimation	Balances convergence speed and stability	Deep neural network training
Momentum Methods	Incorporate exponentially weighted gradients to accelerate convergence	Improved convergence speed and reduced oscillations	Training deep networks, convex and non-convex optimization
Sparsity-Exploiting Algorithms	Utilize sparse data or parameter structures	Reduced computational overhead and memory usage	Large sparse models, online learning
Adaptive Learning Rate Methods	Dynamically adjust step sizes based on past gradients	Robust convergence and reduced hyperparameter tuning	Online learning, variable data distributions
Hessian Approximation Algorithms	Approximate second-order information for faster convergence	Improved convergence rates; handle ill-conditioned problems	Large-scale optimization, curvature-informed updates

Future directions include integrating machine learning-based heuristics—such as deep learning models that extract hierarchical features from network data [38]—and adaptive partitioning methods [34] to better handle uncertainty and mixed-integer decision-making within complex communication networks. Such integrations hold promise for achieving improved robustness and efficiency in optimization under realistic network constraints, including those arising in next-generation wireless and software-driven environments, where adaptability and real-time performance are critical [7, 35]. Combining these techniques with autonomous network management and advanced resource allocation strategies can further enhance optimization performance in 5G/6G and beyond systems [32**?**].

6.6.2 Hybrid Model- and Data-Driven Gradient Approaches. Recognizing the limitations of purely gradient-driven methods, recent research has focused on hybrid frameworks that integrate model-based insights with data-driven adaptations. These approaches leverage structural knowledge embedded in network models while simultaneously exploiting real-time or historical data to inform adaptive gradient computations [2**? ?**]. This integration enhances convergence speed and algorithmic flexibility by dynamically adjusting update rules and reducing discrepancies between model assumptions and evolving network conditions.

For instance, in self-optimized wireless networks (SON), deep learning techniques are combined with model-based control mechanisms to robustly tune parameters across diverse and dynamic environments [36]. This hybrid approach utilizes knowledge graphs and semantic information extracted via deep neural networks and graph neural networks to provide a contextual understanding of network states, thereby improving system responsiveness and stability. By fusing data-driven semantic representations with traditional model-based optimization, these frameworks effectively address scalability and convergence challenges inherent in complex, real-world networks. Moreover, the integration confers robustness to environmental variability by embedding semantic context consistency and enabling error correction through inference of missing or distorted semantic elements within the knowledge graph structure [36]. Such hybrid methods thus present a promising direction for achieving intelligent, flexible, and resilient network optimization beyond conventional gradient-based approaches.

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 approaches include incremental gradient updates that adjust parameters based on streaming data, warm-starting solvers with prior solutions to reduce convergence time, and employing approximation heuristics that offer computationally efficient yet effective parameter refinements.

In telecommunication networks, these techniques allow systems to respond swiftly to sudden changes in traffic patterns, user demands, or channel conditions, thereby maintaining strict quality-of-service (QoS) guarantees and improving resource allocation efficiency [7]. For instance, the emerging Tactile Internet paradigm imposes ultra-low latency requirements on the order of milliseconds, necessitating update mechanisms that can execute within extremely tight time budgets [7]. Achieving this demands highly optimized algorithmic procedures that carefully balance computational complexity with accuracy, where the end-to-end latency components, including transmission, propagation, processing, queueing, and retransmission delays, collectively remain below the stringent thresholds.

A central challenge in fast algorithmic updates is managing the trade-off between update speed and solution precision. Aggressive approximations risk degrading policy performance and potentially violating QoS constraints, whereas fully precise updates may incur computational delays incompatible with real-time demands. To mitigate this tension, recent advances incorporate parallel computation and distributed optimization frameworks, which enable decomposition of the update problem across multiple processing units or network nodes. Such architectures scale efficiently with system size and facilitate timely responsiveness without substantially compromising optimality [35**?**].

Furthermore, fast update techniques are increasingly integrated within AI-driven control and optimization frameworks that underpin autonomic and self-optimizing networks [35**? ?**]. These combined approaches enhance real-time adaptability, robustness, and operational efficiency by leveraging machine learning for predictive modeling and decision-making, alongside rapid algorithmic recalibration to meet dynamic network conditions. Consequently, these innovations provide a foundation for adaptive, autonomous network management capable of maintaining rigorous performance metrics amid 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, thereby accelerating convergence in optimization [**?**]. This method effectively learns environmental evolution patterns through training on solutions from both previous and new environments, facilitating rapid adjustment to shifting network conditions.

Similarly, innovative federated learning schemes applying gradient sparsification with error feedback and adaptive client selection enhance learning robustness and communication efficiency in resource-constrained wireless settings [**?**]. By minimizing a weighted global loss with error feedback, employing sparsification operators, and selectively choosing clients based on their resource availability and reliability, these techniques maintain high accuracy and reduce communication overhead significantly—even under high dropout rates. Experiments on standard benchmarks such as MNIST and CIFAR-10 demonstrate improved test accuracy and convergence speed compared to previous federated learning methods.

Applications to ultra-low latency scenarios, such as the 5G-enabled Tactile Internet, illustrate how gradient-informed optimizations contribute to meeting stringent end-to-end delay requirements [7]. The Tactile Internet, powered by 5G innovations like Multi-access Edge Computing (MEC) and network slicing, demands radical redesigns in optimization frameworks to ensure that transmission, propagation, processing, queueing, and retransmission delays collectively remain below one millisecond. This enables revolutionary use cases such as remote surgery and immersive virtual reality that require ultra-reliable, low-latency communication.

Despite these gains, scalability remains a key limitation, especially for very large instances with high heterogeneity and complex constraints. Computational overhead and intricate 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 are effective for moderately sized networks, augmenting them with metaheuristics—such as variable neighborhood search (VNS) or population-based heuristics—enhances solution quality and exploration capacity for large-scale combinatorial problems.

For example, VNS algorithms have been successfully applied to complex hub location problems involving competitive pricing and demand shifts, offering robust and scalable performance [9]. This approach adapts multiple neighborhood structures, including hub swapping, client reallocation, and price adjustments, coupled with shaking and local search strategies to escape local optima and robustly explore diverse solution spaces. Computational results demonstrate superior scalability and solution robustness relative to classical heuristics.

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 and dynamic challenges posed by 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 requires methods that not only optimize parameters in the current setting but also leverage learned knowledge from previous environments to accelerate adaptation. Neural Network-Based Information Transfer (NNIT) exemplifies this strategy by employing neural networks to learn mappings between evolving network states and their corresponding optimal or near-optimal solutions, thereby facilitating faster convergence and enhanced adaptability [4, 10, 23**?**].

Typically, NNIT integrates population-based evolutionary algorithms with neural networks trained to predict promising regions of the solution space or to transform historical high-quality solutions into effective candidates for the current environment [**?**]. By learning the structural patterns inherent in dynamic environments, such methods substantially reduce computational overhead associated with repeated optimization from scratch. For instance, in supply chain networks—characterized by complexity and dynamic features akin to telecommunications systems—NNIT techniques leverage variational inequalities and Lagrange multiplier analysis to model supply chain equilibria, offering numerical guidance for informed solution transfer [23]. This framework captures equilibrium behaviors where firms optimize profit under wage and labor constraints, and sensitivity analysis via Lagrange multipliers aids strategic decisions on resource allocation and wage policy, thus enhancing robustness and computational efficiency in dynamic optimization.

Moreover, recent advances in interpretable AI have been integrated into NNIT architectures to enhance transparency and trustworthiness by revealing insights into the solution landscape [10]. These methods employ optimal decision trees with hyperplanes to approximate nonlinear, black-box constraints and objectives within a mixed-integer optimization framework. This approach provides global approximate models that transparently depict feasible regions and objective surfaces, enabling decision-makers to explore and validate solutions effectively—an essential feature for deployment in safety-critical and high-stakes network control scenarios.

NNIT also shows considerable promise in nonlinear stochastic decentralized adaptive control applications, underscoring its versatility across a wide range of network optimization problems [4]. The underlying control-theoretic framework formulates optimal interventions to mitigate adverse dynamics such as economic shock propagation in networked systems. By optimally allocating control resources under budgetary and delay constraints, this approach reduces shock severity and economic loss, demonstrating scalability and strategic efficacy. Such frameworks complement NNIT's hybrid paradigm by incorporating control insights that enhance both solution quality and practical applicability.

In summary, NNIT represents a robust and hybrid paradigm that synergistically combines population-based optimization, learned

knowledge transfer via neural networks, interpretable modeling with optimal decision trees, and control-theoretic principles. This integration effectively addresses the complexity, scalability, and dynamism inherent in contemporary and future network control tasks. By exploiting these complementary strengths, NNIT-based algorithmic designs achieve superior optimization performance and adaptive capacity across diverse dynamic and uncertain environments.

7 AI-Enhanced Wireless Networking and Sensing

This section explores how artificial intelligence (AI) techniques improve wireless networking and sensing, with a particular focus on their integration with reconfigurable intelligent surfaces (RIS). We begin by outlining the main objectives, followed by detailed discussion of methodologies, benefits, challenges, and future directions. A summary table is also provided to aid clarity and retention.

Reconfigurable intelligent surfaces (RIS) are planar structures composed of numerous passive reflecting elements with adjustable electromagnetic properties, such as phase shifts, which can be programmatically controlled to dynamically manipulate wireless signal propagation. By smartly configuring these elements, RIS can enhance signal quality, extend coverage, and reduce interference in wireless environments. This fundamental capability makes RIS a promising enabler for next-generation adaptive wireless networks.

AI integration with RIS aims to achieve dynamic environment control for enhanced communication reliability, efficiency, and adaptability in wireless networks. Key objectives include optimizing signal propagation, managing interference, and improving resource allocation in diverse and challenging scenarios.

AI algorithms in RIS-assisted networks primarily utilize reinforcement learning and deep learning to configure surface elements such as phase shifts. These configurations enhance channel state prediction, link reliability, and spectral efficiency under variable conditions.

In addition, AI-driven interference management frameworks leverage real-time data analytics to detect and mitigate interference, thereby improving network scheduling and resource utilization. This is critical for enabling the coexistence of multiple users and technologies without significant performance loss.

Recent benchmarking results demonstrate that AI-powered RIS systems achieve notable enhancements in signal-to-noise ratio (SNR), latency reduction, and energy efficiency, applicable to environments such as millimeter-wave communications and multi-user MIMO setups.

Integration with existing wireless standards remains an essential challenge, as RIS and AI techniques require compatibility with protocols such as 5G NR and emerging 6G frameworks. Moreover, large-scale deployment of RIS arrays necessitates scalable AI algorithms with low computational complexity and real-time adaptability to cope with dynamic channel conditions and diverse application requirements.

In summary, AI-driven enhancements in RIS-based wireless sensing and networking empower adaptive and context-aware systems that meet stringent requirements of next-generation applications. However, challenges remain in scaling AI techniques for large-scale deployments, ensuring robustness, and integrating AI seamlessly with evolving wireless standards. Addressing these will be critical for realizing the full potential of AI-enhanced wireless environments.

7.1 Reconfigurable Intelligent Surfaces (RIS)

Reconfigurable Intelligent Surfaces (RIS) have emerged as a transformative technology that enables programmable manipulation of wireless propagation environments, marking a shift from treating the environment as a stochastic, uncontrollable factor to one subject to deterministic control. This is realized through engineered metasurfaces capable of dynamically altering incident electromagnetic waves, providing unprecedented flexibility in wireless communications. The integration of Artificial Intelligence (AI), particularly machine learning techniques, significantly enhances RIS capabilities by optimizing complex, high-dimensional configuration spaces adaptively. Supervised learning methods assist in channel estimation by mapping measured channel state information (CSI) to optimal RIS configurations, while unsupervised learning facilitates feature extraction from unlabeled channel data, thereby improving generalization in dynamic and uncertain environments. Furthermore, deep reinforcement learning (DRL) provides an effective framework for sequential decision-making under uncertainty, enabling adaptive beamforming and resource allocation strategies that optimize spectral efficiency and energy savings [6]. The combination of these AI paradigms empowers RIS to address key challenges such as high-dimensional configuration spaces, latency constraints, scalability issues, and imperfect channel information, resulting in more robust and efficient wireless links with enhanced coverage and energy efficiency. Future research directions prioritize the development of lightweight, distributed AI algorithms specifically tailored for RIS, the adoption of federated learning techniques to preserve user privacy, and the seamless integration of RIS with emerging technologies such as millimeter wave (mmWave), massive MIMO, and edge computing. Collectively, these advancements are poised to accelerate the realization of intelligent wireless environments that substantially improve network performance and sustainability [6].

7.2 Benefits and Challenges of RIS

The AI-enabled RIS paradigm offers multiple benefits that significantly enhance wireless communication systems. These include notable improvements in spectral efficiency achieved through enhanced directivity and more effective interference management. For instance, experimental studies have shown that AI-enabled RIS can adaptively optimize beamforming strategies to outperform traditional heuristic methods, leading to measurable gains in coverage and data rates [6]. Additionally, RIS reduces reliance on active radio frequency components, thereby augmenting energy efficiency and contributing to greener communications. It also extends coverage by enabling signal reflection and focusing beyond line-of-sight barriers, which facilitates connectivity in dense urban environments or scenarios with significant obstacles. An important advantage of AI integration is robustness under imperfect channel conditions, as AI algorithms can learn and compensate for noise and fading effects, thereby maintaining high communication quality [6].

Table 15: Summary of AI Techniques and RIS Benefits in Wireless Networking and Sensing

Aspect	AI Methodologies	Benefits	Challenges and Future Directions
RIS Configuration	Reinforcement Learning, Deep Learning	Adaptive phase shift optimization, improved channel state prediction	Scalability in large RIS arrays, real-time learning efficiency
Interference Management	Real-time Data Analytics, Machine Learning	Enhanced interference identification, resource allocation, network scheduling	Robustness to dynamic environments, multi-user coexistence complexity
Performance Gains	AI-assisted RIS control	Increased SNR (up to 10-15 dB), reduced latency (up to 30%), improved energy efficiency	Integration with diverse wireless standards (5G/6G), hardware limitations
Application Scenarios	Millimeter-wave, multi-user MIMO systems	Context-aware adaptivity, improved spectral efficiency	Deployment cost, reliability under harsh propagation conditions

However, these benefits come with inherent challenges that must be addressed to realize practical deployment. The RIS configuration space is typically high-dimensional—sometimes involving thousands of elements—rendering exhaustive search or conventional heuristic optimization methods impractical. This complexity necessitates the development of scalable AI algorithms capable of effective dimensionality reduction while preserving performance. For example, deep reinforcement learning and unsupervised learning approaches have been proposed to efficiently map channel states to near-optimal RIS configurations [6]. Moreover, practical deployment requires AI techniques that meet stringent latency and scalability constraints, motivating the use of lightweight and distributed learning methods such as federated learning, which also offers privacy benefits by avoiding centralized data aggregation. Security is another critical concern, as adversaries might exploit RIS to perform unauthorized eavesdropping or signal manipulation. To mitigate these risks, secure AI-driven configuration protocols and real-time anomaly detection mechanisms are essential [6]. Balancing and addressing these benefits and challenges is central to advancing RIS deployment and realizing intelligent wireless environments.

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 under strict latency and energy constraints. Achieving these objectives requires future algorithmic innovations that carefully balance trade-offs among model complexity, convergence speed, and robustness to channel estimation errors. Moreover, emerging paradigms like neuromorphic computing and online continual learning offer promising routes to enhance system adaptability and resilience in highly dynamic wireless environments.

7.4 Intelligent Interference Management in Perceptive Mobile Networks (PMNs)

Perceptive Mobile Networks (PMNs) represent an advanced integration of communication and sensing functionalities, enabling wireless infrastructure to simultaneously support data transmission and situational awareness. Effective interference management is essential because sensing waveforms and communication signals coexist in shared spectral and spatial domains, leading to complex coexistence challenges. Recent advances have introduced AI-empowered interference mitigation frameworks that exploit macro-diversity gains and coordinated beamforming strategies across multi-cell architectures [18]. In particular, deep learning-based interference prediction models leverage both historical and real-time channel observations to accurately forecast interference patterns. This predictive capability enables proactive and dynamic resource allocation, maximizing the sensing signal-to-interference-plus-noise ratio (SINR) while preserving the quality of communication links. These dynamic allocation schemes improve sensing detection probability by approximately 20% and simultaneously reduce intra- and inter-cell interference by about 30%, thereby achieving a balanced optimization of communication and sensing objectives in PMNs [18].

Despite these promising developments, several critical challenges remain for practical and scalable PMN deployments. Key issues include achieving low-latency inference to support real-time system adaptation, acquiring precise channel state information in highly mobile environments, and designing scalable cooperation schemes among multiple base stations without incurring excessive signaling overhead [18]. Addressing these challenges is pivotal to realizing robust PMNs that can harmonize sensing and communication functionalities effectively. Future research directions highlighted in recent literature emphasize integrating multi-modal sensing capabilities, adopting federated learning for privacy-preserving interference management, and developing mechanisms that enhance robustness under dynamic and heterogeneous network conditions [18]. Collectively, AI-driven intelligent interference management frameworks offer substantial improvements in 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 methods dynamically optimize resource allocation and beamforming configurations by integrating AI with physical-layer innovations, resulting in robust detection performance within dense and heterogeneous network environments marked by significant interference and channel uncertainty. Moreover, privacy

preservation has emerged as a critical concern in networked sensing, as sensitive environmental or user data may be indirectly inferred via side-channel attacks inherent to cooperative frameworks. To address this, recent studies propose privacy-aware AI algorithms that incorporate differential privacy mechanisms and federated learning paradigms, effectively mitigating privacy risks while maintaining sensing performance [15, 18].

Robustness to heterogeneity in hardware capabilities, channel conditions, and user mobility patterns remains a major challenge. Approaches leveraging model adaptation, transfer learning, and fast adaptation methods such as Zero-Shot Lagrangian Updates have demonstrated potential in coping with such variability [8**?**]. For instance, Zero-Shot Lagrangian Update offers computationally efficient network optimization by directly updating Lagrange multipliers without iterative primal solves, enabling real-time adaptability in dynamic wireless environments [8]. Additionally, explainability-focused AI methods enhance trustworthiness and interpretability within heterogeneous setups [**?**]. Nonetheless, these techniques demand extensive validation in diverse real-world scenarios to ensure broad applicability and reliability. Bridging the gap between theoretical AI frameworks and practical deployment therefore necessitates continued research on scalable cooperation protocols, secure architectures, and self-tuning training paradigms capable of operating reliably across heterogeneous wireless environments.

In summary, AI-enhanced wireless networking and sensing via RIS and intelligent interference management herald 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 trace the rationale behind AI actions, improving reliability and ensuring compliance.

8.1 Explainability Frameworks in Network Management

In multi-agent reinforcement learning-based network management, explainability frameworks such as attention mechanisms—which highlight important inputs influencing decisions—and feature attribution methods—which quantify the impact of individual features—have demonstrated how agents coordinate resource allocation. These methods offer insights that help network operators validate system behavior and detect anomalies. Such frameworks provide interpretable feedback on agent cooperation patterns, directly impacting service quality and robustness.

8.2 Regulatory Compliance and Transparency

Explainability methods also contribute to regulatory compliance in telecommunications by aligning AI model decisions with governance standards including GDPR and the AI Act. Transparent AI decision-making enables automated actions to be audited for fairness, data privacy, and accountability, which is essential for meeting both internal and external telecom regulatory requirements.

8.3 Practical Applications in Telecom Operations

Practical case studies from telecom operators illustrate how interpretable AI techniques optimize traffic routing while maintaining explainable decision logs that satisfy internal compliance audits. For example, an explainable resource scheduling model allowed operators to identify unexpected decision triggers and adjust system parameters to improve network throughput without sacrificing transparency. Another application is in fault diagnosis systems, where interpretable models guide operators through root cause analysis by highlighting relevant system states and events, thus accelerating remediation and minimizing downtime.

8.4 Summary and Impact

In summary, explainability in AI-controlled telecom systems bridges the gap between complex algorithmic decisions and stakeholder understanding. By supporting trustworthy deployment that meets both technical and regulatory expectations, these methods ensure AI systems are reliable, auditable, and aligned with operational goals.

8.5 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 confronts challenges such as balancing computational complexity with real-time processing needs 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. This alignment with regulatory expectations and operational transparency is essential for advancing next-generation networks, including beyond 5G (B5G) and 6G systems, which rely fundamentally on AI for adaptive, secure, and efficient management [24**?** **?**].

8.6 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, enabling operators to comprehend how variations in system parameters influence resource management outcomes [20**?**]. For example, optimization-based resource allocation methods can be analyzed to reveal the impacts of system parameters on convergence and performance metrics, assisting network designers in balancing trade-offs between efficiency and fairness.

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]. Such approaches are particularly relevant in multi-band wireless communication networks, where complex channel dynamics and diverse frequency bands present challenges for transparent decision-making. By integrating expert knowledge through symbolic components, these hybrid models enhance explainability while maintaining accuracy in resource allocation.

Moreover, attention mechanisms and gradient-based attribution techniques embedded in neural network architectures highlight key features that influence AI decisions across tasks such as traffic management, fault diagnosis, and spectrum allocation [**?**]. These methods provide insight into which input features or network conditions critically affect model outputs, thereby facilitating operational transparency in sophisticated AI-driven systems.

Collectively, these interpretability and explainability methods form a comprehensive toolset that mitigates the inherent opaqueness of sophisticated AI models, enhancing operational transparency while preserving system efficacy. This balance is crucial for advancing trustworthy AI applications in next-generation wireless networks, enabling robust, adaptive, and understandable decision-making under dynamic and heterogeneous environments.

8.7 Future Directions

This subsection outlines key objectives to guide the development of explainable AI (XAI) in telecommunications and control systems, emphasizing the balance between transparency, privacy, security, and scalability in next-generation networks. The objectives include advancing privacy-preserving interpretability, enhancing robustness against adversarial threats, enabling scalable explanations for complex multi-layer architectures, and integrating multi-agent and LLM-driven AI paradigms with practical deployment considerations in edge and cloud environments.

Looking forward, the evolution of explainable AI (XAI) within telecommunication and control systems is poised to address current limitations and emerging challenges through several pivotal advancements. A primary focus is the development of privacy-preserving XAI techniques that balance transparency with stringent data confidentiality requirements common in telecommunication networks [18]. For instance, federated explainability enables interpretability without centralizing sensitive data, thereby supporting privacy regulations and operational constraints as demonstrated in multi-cell perceptive mobile networks where coordinated deep learning mitigates interference while preserving user privacy [18].

Enhancing interpretability frameworks to be resilient against adversarial manipulation is another critical direction. AI systems deployed in hostile network environments are vulnerable to exploitation that threatens security and reliability [24]. Robust XAI methodologies should integrate anomaly detection and adversarial training to safeguard explanations from malicious interference, as highlighted in AI-driven network management surveys and recent Open RAN implementations [25]. For example, integrating adversarially robust explanations with multi-agent learning can thwart attacks aiming to distort resource allocation or fault diagnosis [24, 25].

Scaling explainability to handle large-scale communication and control architectures that span cloud, edge, and device layers, as well as multi-agent systems, requires modular, hierarchical interpretation mechanisms capable of providing contextualized explanations across abstraction levels [5]. Emerging AI paradigms, including multi-agent reinforcement learning and large language model (LLM)-driven network intelligence, demand innovative explainability frameworks that capture complex cross-agent interactions and supply natural language interpretability. An illustrative case is the LLM-driven agentic AI approach in Open RAN, which autonomously identifies and mitigates faults with high accuracy while providing interpretable natural language explanations [5].

Practical implementation pathways to realize these future directions involve leveraging federated learning techniques to preserve data privacy without compromising explanation fidelity, employing multi-agent coordination models to distribute intelligence efficiently, and optimizing lightweight XAI models tailored for real-time edge deployment within stringent latency and resource constraints identified in 6G and beyond Open RAN networks [25]. Methodological frameworks advocating modular and hierarchical explanations facilitate managing complexity across heterogeneous network layers while promoting interoperability. Additionally, open-source initiatives and benchmarking platforms focusing

on privacy, robustness, and explainability can accelerate research and deployment efforts.

To further aid comprehension, Table 16 summarizes these future directions, highlighting associated challenges and potential solutions. This synthesis links practical challenges explicitly to earlier thematic discussions on network privacy, security, scalability, and AI integration, thereby providing a cohesive roadmap.

Key research questions and hypotheses for advancing XAI in this domain include: How can federated XAI methods guarantee privacy protections without sacrificing explanation fidelity and user trust? What are the most effective defenses against adaptive adversarial attacks targeting explainability in dynamic, real-time network analytics? How can hierarchical XAI frameworks be standardized to ensure seamless interoperability across diverse telecom layers and vendors? Which optimization strategies best balance computational overhead against interpretability for LLM-driven agentic AI deployed in resource-constrained edge environments? Addressing these questions requires interdisciplinary, collaborative efforts combining insights from AI, control theory, wireless communications, and cybersecurity.

Anticipated disruptive innovations encompass agentic AI systems embedded with LLM-driven agents that enable autonomous fault detection and self-healing capabilities [5]. Empirical results demonstrate performance gains such as a 17% increase in fault detection accuracy and a 40% reduction in network downtime compared to traditional methods [5]. Seamless AI integration within Open RAN architectures fosters adaptive, explainable control loops that enhance network resilience, throughput, and resource efficiency [25]. Such paradigm shifts collectively promote transparent, robust, and efficient AI-driven telecommunications, facilitating the emergence of intelligent, self-optimizing networks dynamically responsive to evolving environmental and operational conditions.

8.8 Applications in Telecommunications and Networking

This section provides a comprehensive overview of the key applications of artificial intelligence (AI) in telecommunications and networking. We detail the primary objectives, scope, and challenges specific to these domains, systematically examining how AI techniques enhance network performance, reliability, and security. The discussion focuses on four major application areas: network optimization, traffic prediction and management, resource allocation, and fault detection and diagnosis. Each area leverages AI methodologies to address specific problems: network optimization improves routing and load balancing to increase throughput and reduce latency; traffic prediction and management utilize machine learning models to forecast network demand and mitigate congestion; resource allocation applies AI for dynamic and efficient distribution of bandwidth and computing power; and fault detection and diagnosis employ intelligent algorithms to monitor, detect, and promptly resolve network failures, thereby enhancing system robustness.

8.8.1 Network Optimization. AI techniques have been extensively applied for network optimization by learning from historical data to dynamically adjust configurations in complex and large-scale networking environments. This adaptive approach enhances throughput and reduces latency while efficiently managing the heterogeneous nature of modern networks. Despite these advantages, challenges remain in achieving scalable real-time processing and integrating diverse and often noisy data sources. Compared to traditional rule-based and statistical approaches, AI methods provide superior adaptability and scalability; however, they may introduce extra computational overhead and require careful design and deployment strategies to balance performance gains with resource constraints.

8.8.2 Traffic Prediction and Management. Traffic prediction models leverage machine learning to anticipate network congestion, enabling proactive management strategies that improve overall service quality. These models face challenges stemming from dynamic traffic patterns and data sparsity, which may limit prediction accuracy. While AI methods often outperform conventional statistical techniques in capturing complex temporal patterns, their reliance on large volumes of high-quality data can be a limitation in practice. Commonly used evaluation metrics include prediction accuracy, root mean square error (RMSE), and mean absolute error (MAE), which together provide a comprehensive assessment of model performance across different dimensions.

8.8.3 Resource Allocation. AI-driven resource allocation tackles complex constraint satisfaction problems inherent in network resource management, aiming to optimize the utilization of limited resources while satisfying diverse user demands. These approaches enhance efficiency and fairness by dynamically balancing competing objectives such as throughput maximization, latency minimization, and equitable user service. Despite their advantages, challenges remain related to achieving fairness guarantees, managing the computational complexity of AI models, and ensuring the interpretability and practical deployment of these solutions. Compared to traditional heuristic methods, AI-based techniques often demonstrate improved resource efficiency and fairness indices, yet further research is needed to address trade-offs between performance, complexity, and transparency in real-world network environments.

8.8.4 Fault Detection and Diagnosis. AI-based fault detection systems are designed to identify and diagnose anomalies within network operations, effectively handling imbalanced datasets and minimizing false alarms. Their ability to detect subtle and rare events significantly enhances network resilience. However, balancing the detection rate and false positive rate remains a critical challenge, particularly in real-world environments where false alarms can disrupt service continuity. To comprehensively evaluate these systems, metrics such as detection rate, precision, recall, and false positive rate are indispensable.

While AI methods offer substantial benefits over traditional techniques in adaptability and performance, they also introduce challenges related to computational overhead, data requirements, model interpretability, and deployment complexity. Overcoming these limitations is vital to unlock AI's full transformative potential in telecommunications. Future research directions should emphasize scalability, real-time implementation, fairness, and explainability to

Table 16: Summary of Future Directions, Challenges, and Solutions in Explainable AI for Telecommunications and Control

Future Direction	Challenges	Potential Solutions
Privacy-preserving XAI	Ensuring data confidentiality while maintaining explanation fidelity	Federated explainability, decentralized interpretation frameworks [18]
Adversarially robust explanations	Vulnerability to attacks compromising network security and explanation integrity	Integration of anomaly detection, adversarial training, and robust model design [24, 25]
Scalable, hierarchical interpretability	Managing complexity across multi-layer network architectures and distributed agents	Modular frameworks with hierarchical explanation models providing multi-level context [5]
Multi-agent and LLM-driven XAI	Complexity in cross-agent interactions and computational overhead on constrained devices	Agentic AI frameworks leveraging lightweight LLM optimization and multi-agent coordination [5]
Real-time edge deployment	Meeting latency and resource constraints for timely explanations	Development of lightweight XAI models optimized for edge devices, hardware acceleration [25]
Interdisciplinary synergy	Integrating AI, control theory, and wireless communication disciplines	Modular, layered frameworks bridging theoretical and practical gaps across domains

Table 17: 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, minimizing false alarms	Detection rate, false positives, precision, recall

ensure the development of robust and efficient AI-enabled network systems.

This structured overview highlights the interconnected nature of AI applications, underscoring their collective role in enhancing the robustness and intelligence of modern communication networks.

8.8.5 AI-Driven Adaptive Control Applications. This section presents an overview of the objectives, key AI techniques, applications, and challenges in employing AI-driven adaptive control within telecommunications networks. The primary goal is to enhance network management through dynamic, data-driven optimization strategies that improve quality of service (QoS), resource utilization, and fault resilience while maintaining privacy and computational efficiency.

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 enable critical 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. For example, reinforcement learning (RL) 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, enhancing network fault management through identifying rare events and addressing sparse failure data [7**?**].

Despite these advances, deploying sophisticated AI models introduces significant challenges. The computational overhead involved in training and inference of complex deep learning models can impede real-time application, especially in large-scale or resource-constrained edge environments [2**?**]. Federated learning (FL) emerges as a promising solution by enabling distributed model training while preserving data privacy and reducing communication overhead. Robust FL frameworks integrate gradient sparsification, error feedback, and adaptive client selection to handle client dropout, limited bandwidth, and heterogeneous device capabilities [**?**]. Moreover, joint optimization of model parameter size and bandwidth allocation improves FL efficiency, decreasing training time and boosting accuracy in wireless networks with diverse device and channel conditions [2].

Generalization remains a critical issue, as AI models must continuously adapt to heterogeneous and evolving network conditions, necessitating efficient retraining or adaptation mechanisms [**?**]. Privacy concerns related to collecting and processing extensive network data motivate the adoption of privacy-preserving learning frameworks such as FL, which maintain data locality while collaboratively enhancing model performance [7, 35]. Despite these challenges, AI-driven adaptive control mechanisms significantly advance network self-optimization, reducing operational expenditures while improving QoS [24**?**].

In summary, AI-driven adaptive control in telecommunications networks aims to automate and optimize network operations in a dynamic, data-informed manner by harnessing advanced ML and DL techniques. While these approaches offer considerable benefits in efficiency and performance, addressing computational constraints, privacy, and model generalization is essential for their practical deployment.

8.8.6 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 closely with semantic communication frameworks that combine deep learning and knowledge graphs to enhance semantic context consistency and enable more effective error correction [36]. Incorporating these semantic-level evaluations addresses the inadequacies of strictly physical-layer assessments, thereby realigning optimization objectives with end-user perceived quality. Moreover, adaptive algorithms are evaluated with respect to computational efficiency, convergence speed, and resilience to adversarial perturbations or network faults [2, 7**?**]. For instance, latency models capturing transmission, propagation, processing, queueing, and retransmission delays play a critical role in Tactile Internet applications that require ultra-low latency and high reliability [7].

Despite these advancements, the field still lacks widely adopted standardized benchmarks leveraging established datasets and simulation frameworks, hindering cross-comparison and reproducibility. Existing repositories such as MNIST and CIFAR-10 are frequently employed in supervised and federated learning evaluations [2], yet these datasets fall short in representing the complex demands of semantic communications or edge-cloud interactions. This gap underscores the urgent need for novel datasets and repositories specifically tailored to semantic fidelity, multimodal data integration, and dynamic, real-time adaptive networking scenarios that better reflect practical communication challenges.

To foster uniformity and comparability, best practices for evaluation protocols should mandate clearly defined metrics that capture semantic, physical-layer, and operational performance, complemented by consistent testbed configurations and open-source simulation tools [24]. Such protocols must balance accuracy with computational and latency constraints while integrating interpretability and privacy considerations intrinsic to AI-driven systems [24**?**]. The establishment of comprehensive, standardized evaluation frameworks will be pivotal in enabling rigorous performance benchmarking, enhancing reproducibility, and accelerating the deployment of AI-enabled network control across wireless and edge-cloud environments.

8.8.7 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 perform real-time inference and handle local data processing, crucial for latency-sensitive applications such as 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, enabling efficient on-device execution without compromising responsiveness [20**?**]. Meanwhile, cloud-based AI systems aggregate global network insights, manage intensive training processes, and distribute updated models back to edge nodes, supporting continual learning and adaptive decision-making [38**?**].

Federated learning exemplifies this edge-cloud synergy by facilitating decentralized model training across heterogeneous devices while preserving data privacy and reducing communication overhead [7]. Addressing device heterogeneity involves adaptive model compression and personalized federated optimization techniques that match model complexity to individual device capabilities. Synchronization challenges caused by diverse update frequencies and intermittent connectivity are mitigated through asynchronous federated learning protocols and hierarchical aggregation schemes. For example, grouping devices based on similarities in data distribution or computational power promotes more stable and efficient training rounds [7**?**].

Additionally, distributed AI systems confront security challenges including adversarial attacks and data poisoning, spurring research into robust model architectures and trustworthy deployment strategies at scale [6, 24]. The dynamic interplay between edge and cloud computing thus represents a critical frontier for delivering intelligent, responsive, and secure network control in next-generation wireless ecosystems, with ongoing developments guided by advancements in AI model design, communication protocols, and network architecture [6, 7, 24**?**].

8.8.8 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 $W^T\Phi(x(t), x(t-\tau)) + \varepsilon$. Here, W represents unknown weights, Φ denotes the basis functions, and ε is the approximation error. The unknown weights W are estimated online using adaptive laws, which enable real-time compensation for system uncertainties, time delays, and external disturbances. Concurrently, a specifically designed observer estimates both the system states and fault signals, effectively managing discrepancies caused by unknown false data injections (FDI) and measurement inaccuracies. This dual estimation mechanism significantly 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. Unlike traditional asymptotic controllers that achieve stability over an indefinite period, finite-time stabilization ensures all errors vanish within a known finite interval, markedly improving responsiveness and robustness under adversarial conditions. The theoretical foundation relies on

Lyapunov–Krasovskii functionals carefully constructed to incorporate the effects of time delays, providing rigorous guarantees of closed-loop system stability despite the presence of unknown nonlinearities and disturbances.

To contextualize, consider a nonlinear system subject to unknown actuator faults and malicious false data injection attacks causing erroneous sensor measurements. The proposed approach uses RBFNNs to approximate nonlinearities appearing in the system's delayed states and employs an observer to dynamically identify both the current system state and any present faults or attacks. By adjusting the control inputs based on these real-time estimates, the controller quickly compensates for faults and maintains system operation within desired performance bounds. Simulations on benchmark nonlinear systems have validated this methodology, displaying superior fault tolerance and faster stabilization compared to classical adaptive controls [3].

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, effectively addressing both component degradation and malicious interventions. 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 emulating practical operational scenarios [3].

In summary, this resilient control strategy provides a promising avenue toward enhancing CPS security and reliability, leveraging real-time learning and estimation to not only detect but actively counteract faults and cyber threats in critical infrastructure systems.

8.8.9 Open Research Frontiers. Emerging research trajectories in telecommunications underscore the significance of multi-agent systems, stochastic modeling, and hardware-in-the-loop simulation platforms as foundational frontiers advancing adaptive control and AI integration [3]. Multi-agent frameworks enable scalable, decentralized decision-making across heterogeneous network entities, thereby enhancing robustness and adaptability in complex, dynamic environments. The integration of stochastic models provides a nuanced characterization of wireless channel variability, environmental uncertainties, and human-in-the-loop behaviors, which necessitates adaptive control methodologies capable of balancing performance with risk management effectively [3].

Hardware-in-the-loop platforms serve as critical testbeds bridging the gap between algorithmic development and real-world hardware constraints such as timing delays, sensor inaccuracies, and communication limitations. These platforms expedite prototyping, validation, and fine-tuning of resilient control schemes under conditions closely aligned with realistic network environments [3].

Complementary research areas focus on developing explainable AI paradigms in network control to ensure transparency and interpretability, as well as integrating reinforcement learning with classical control theory to merge long-term policy optimization with provable system stability guarantees [24]. Tackling computational complexity remains a pivotal concern with efforts directed towards model compression techniques, distributed AI frameworks, and energy-efficient algorithms, which are imperative for deploying intelligent control in resource-constrained edge environments [6]. Collectively, these research directions underscore a transformative potential for next-generation telecommunications systems characterized by intelligence, autonomy, and resilience.

To delineate a structured research roadmap, near-term objectives include designing and benchmarking adaptive multi-agent control strategies endowed with robust fault tolerance, leveraging hardware-in-the-loop platforms for realistic validation [3]. Concurrently, efforts aim to advance explainable AI methods and fuse reinforcement learning with classical control techniques to achieve interpretable and stable network management solutions [24]. Addressing computational challenges via lightweight distributed AI and energy-aware algorithms establishes a foundation for practical deployment in edge computing scenarios [6].

Long-term research goals envision the seamless integration of distributed resilient control mechanisms for complex multi-agent networks operating under dynamic, uncertain wireless conditions. This involves extending stochastic adaptive control techniques to accommodate time-varying delays and enhance resilience against cyber-physical attacks, as demonstrated by frameworks incorporating adaptive neural network-based fault detection and mitigation [3]. Future investigations aspire to realize fully autonomous, intelligent wireless systems by harmonizing adaptive control, explainable AI, and scalable reinforcement learning frameworks while ensuring robustness, scalability, and sustainability within next-generation telecommunications infrastructures.

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 provide a 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 example, large-scale transformer models achieve state-of-the-art performance on natural language processing tasks but often lack transparency in their decision-making processes. This issue intersects with ethical AI considerations where explainability is critical for user trust and accountability. In healthcare diagnostics, for instance, complex models must provide clear rationales for predictions to comply with regulatory standards and gain clinical acceptance.

Another pervasive theme involves integrating learning paradigms, such as combining supervised learning with reinforcement learning to develop robust agents capable of adapting in dynamic environments. A relevant case study from autonomous driving illustrates this integration: perception modules trained on labeled images are fused with reinforcement learning policies that adapt to real-time driving conditions. This integration surfaces technical challenges including aligning heterogeneous learning objectives and managing uncertainty propagation, emphasizing the need for unified frameworks that bridge these aspects effectively.

Data privacy and security are also essential cross-cutting concerns. Federated learning techniques, originally designed for privacy-preserving model training, have found applications ranging from mobile device personalization to collaborative healthcare research. The main challenge lies in balancing data utility with privacy guarantees and computational efficiency. For example, privacy-preserving federated methods often limit data sharing but can suffer from bias due to uneven client participation, necessitating algorithmic safeguards tailored to these contexts.

Despite increasing recognition of these interconnected challenges, most existing solutions address them in isolation. To foster AI systems capable of holistic performance, we propose a research roadmap focused on three priorities. First, developing unified conceptual frameworks that explicitly model the interactions among scalability, interpretability, privacy, and adaptability. Such frameworks would support joint optimization by capturing trade-offs and synergies across these dimensions. Second, designing modular architectures that enable flexible integration of diverse learning paradigms and privacy-preserving techniques while preserving interpretability standards. Third, establishing standardized benchmarks and evaluation protocols that assess multi-dimensional criteria—including transparency, robustness, and privacy—under realistic deployment conditions.

From a methodological perspective, integrated AI system design should incorporate explicit multi-objective optimization strategies to balance competing demands. For instance, optimization methods can simultaneously address model accuracy, explainability, privacy preservation, and computational cost. Embedding uncertainty quantification within modular pipelines can help control error propagation when composing heterogeneous components. Moreover, adaptive learning schemes that dynamically respond to environmental feedback can enhance system robustness and foster user trust.

In summary, addressing cross-cutting themes in AI requires moving beyond siloed approaches toward comprehensive system-level thinking. Emphasizing joint frameworks, modular design, and multi-criteria evaluation will better align AI capabilities with the complex requirements of practical deployment, fostering transparency, privacy, and adaptability in concert.

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 address these challenges, scalable AI architectures must combine algorithmic compression methods, such as model pruning and quantization, with hardware acceleration and modular, parallel system designs. Synchronization and consistent model updating—particularly in federated or distributed learning paradigms—are critical for maintaining real-time performance while preserving data privacy and handling heterogeneous network conditions [13].

These complexities are especially pronounced in 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 leverage 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]. Cooperative sensing among multiple base stations enhances robustness under high network loads, demonstrating up to 20% improvement in detection probability and significant interference reduction.

Moreover, real-world AI-enabled routing and traffic management systems dynamically adapt to network conditions, achieving improvements of up to 30% in both throughput and latency [39]. Similarly, AI-powered software-defined networking (SDN) frameworks deploy machine learning models—including Random Forest classifiers and LSTM networks—for real-time traffic classification, anomaly detection, and resource allocation; experiments show up to 92% classification accuracy alongside an 18% reduction in end-to-end latency in emulated 5G scenarios [13]. These results highlight the practical scalability and real-time responsiveness achievable through integrated AI-SDN architectures.

Furthermore, the integration of AI with Reconfigurable Intelligent Surfaces (RIS) optimizes wireless environment control to improve spectral and energy efficiency. AI techniques, such as deep reinforcement learning, enable dynamic RIS configuration and resource allocation by learning mappings from channel states to optimal configurations, thus addressing high-dimensional optimization challenges and latency constraints in scalable deployments [6].

Overall, realizing scalable and real-time AI inference in telecommunications necessitates lightweight yet robust AI models optimized for dynamic network environments, efficient edge-cloud collaboration, and real-time synchronization mechanisms that support distributed learning while preserving privacy and system responsiveness. These case studies underscore the critical importance of algorithmic compression, distributed inference, adaptive learning, and hardware-aware designs in meeting scalability demands without sacrificing real-time performance, thereby unlocking AI's full potential for next-generation network applications.

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].

Moreover, integration of encryption techniques plays a vital role in securing data transmissions and model parameters within telecommunications networks. End-to-end encryption ensures that data remains confidential during communication between distributed entities, effectively preventing unauthorized access and eavesdropping. Homomorphic encryption allows computations to be performed directly on encrypted data without decryption, enabling privacy-preserving model training and inference [24]. Combined with differential privacy mechanisms, which add calibrated noise to shared model updates, these approaches rigorously protect individual data contributions from leakage while maintaining overall model utility. In Software-Defined Networking (SDN)-enabled 5G and beyond frameworks, these encryption and privacy-preserving algorithms are embedded alongside AI models within SDN controllers, facilitating real-time traffic classification and anomaly detection without compromising data confidentiality [13]. However, designing algorithms that balance encryption overhead, privacy guarantees, and model accuracy remains complex, particularly under stringent latency and computational constraints.

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]. Such frameworks integrate encryption, secure multiparty computation, and federated learning protocols, enabling seamless and privacy-respecting collaboration among heterogeneous stakeholders in telecommunications systems.

9.3 Explainability and Trust

This subsection aims to elucidate the critical role of explainability in fostering trust and transparency within AI-driven telecommunications systems, emphasizing current advancements, challenges, and their operational and regulatory implications.

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 [**?**]. Empirical studies demonstrate that AI-empowered frameworks can meaningfully improve network performance while maintaining system transparency. For example, the interference management framework in perceptive mobile networks applies AI to dynamically allocate resources based on explainable interference predictions, resulting in a 20% improvement in detection probability and a 30% reduction in sensing interference while preserving communication quality [18]. Such explainable insights assist operators in validating AI decisions against operational constraints, reducing inadvertent network disruptions.

Despite these benefits, the widespread use of complex deep learning models often creates opaque, black-box systems, revealing a fundamental trade-off between prediction accuracy and interpretability [25]. Current research includes developing inherently interpretable models and post hoc explanation methods such as attention visualization, feature attribution, and counterfactual reasoning. While these methods have shown progress, they remain immature for comprehensive telecommunications applications and require further adaptation to meet domain-specific needs [24]. Moreover, explainability is essential not only for operational transparency but also for regulatory compliance and risk mitigation, as erroneous AI decisions could trigger cascading network failures [18]. The evolving ecosystems of Open RAN and emerging 6G networks introduce additional trust challenges because of their distributed and multi-agent learning frameworks, necessitating transparent AI mechanisms to ensure security, fault tolerance, and interoperability [25].

In summary, advancing explainability in AI systems is a vital challenge underpinning systemic trust, responsible deployment, and regulatory adherence in telecommunications. Continued efforts toward interpretable AI models, tailored explanation techniques, and integration of trust frameworks are imperative for the reliable and transparent operation of next-generation networks.

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.

Table 18: Current Standards Initiatives Addressing AI Interoperability and Standardization in Telecommunications

Standards Body	Initiative/Group	Scope and Focus
O-RAN Alliance	AI/ML Working Group	Defines AI model interfaces, standardized telemetry data formats, and protocols for Open RAN components (RU, DU, CU) to realize distributed intelligence and federated learning [25].
3GPP	SA6 (Enhancements for AI)	Integration of AI data models and interfaces in 5G/6G network management for seamless AI control across heterogeneous network slices [13].
ETSI	Experiential Networked Intelligence (ENI)	Framework for context-aware AI management, standardizing AI-driven closed-loop automation workflows and interoperability between network elements [13].
IEEE Standards Association	P1931.1 (Interoperability for AI Systems)	Developing guidelines for AI component interoperability, data exchange formats, and reproducibility standards applicable to telecommunications infrastructures [18].
ITU-T	Focus Group on Machine Learning for Future Networks	Standardizing machine learning workflows, data representation, and privacy frameworks for multi-vendor network environments [25].

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].

Given the resource constraints common at the network edge in 5G and beyond, emerging lightweight security solutions are essential. These include model compression techniques such as pruning and quantization to reduce computational overhead while preserving robustness, enabling deployment of secure AI on edge devices [18, 24]. Lightweight anomaly detection models and efficient encryption schemes tailored for edge environments enhance protection without imposing significant latency or energy costs [24]. Moreover, federated learning and edge computing synergize to protect data privacy and reduce centralized vulnerabilities, balancing the privacy-utility trade-offs crucial under regulatory frameworks [18]. These approaches facilitate real-time inference with acceptable security guarantees in constrained settings, addressing a critical challenge for scalable AI-driven network management [24].

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 increasing from 78% to 95%, and mitigation success rate rising from 70% to 91%, alongside a 40% reduction in downtime and a drop in throughput degradation from 25% to 10%, significantly enhancing network performance. These improvements are summarized in Table 19. However, these benefits must be balanced against challenges including computational overhead, potential erroneous decisions, security risks, and interoperability issues among multi-vendor environments, motivating hierarchical agent designs 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. In the following, we connect each future research challenge to prior thematic discussions presented in this survey, propose detailed roadmaps, suggest concrete milestones, and highlight actionable research questions that can foster progress in AI-enabled wireless control systems.

Implementing these research directions requires a coordinated effort bridging AI algorithm design, control theory, wireless protocol development, and practical system engineering. For example, scalability challenges connect back to distributed learning methods in Section 3 and resource-aware wireless schemes in Section 4, while robustness aspects rely heavily on control-theoretic guarantees discussed in Section 5. The integration of AI and classical control, emphasized throughout Section 6, remains a core research avenue demanding new theoretical insights and interdisciplinary validation. Low-latency demands specifically leverage advances in AI-aided scheduling from Section 4, and security concerns draw from privacy-preserving and adversarial defense mechanisms in Section 7.

Beyond research, practical implementation pathways must incorporate open-source platforms and standardized benchmarks to

Table 19: Performance Improvements of LLM-Driven Agentic AI in O-RAN Resilience [5]

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

Table 20: Summary of Future Research Challenges and Opportunities in AI-Enabled Wireless Control Systems

Research Challenge	Opportunity	Actionable Research Questions / Milestones
Scalability and Complexity	Development of scalable AI algorithms for large-scale networks	How can AI models be optimized for computational complexity and energy efficiency in massive deployments? Milestones: Prototype scalable distributed control algorithms; evaluate computational overhead and energy consumption in large network simulations and testbeds; design adaptive models that gracefully degrade performance under limited resources. Links to Section 3 on distributed AI frameworks and Section 4 on resource-aware wireless protocols.
Robustness to Real-World Variability	Robust control against environmental dynamics and hardware uncertainties	What theoretical and empirical frameworks ensure robustness of AI-driven control under non-ideal conditions including channel fading, interference, and hardware variability? Milestones: Develop uncertainty-aware AI methods integrating control-theoretic robustness (Section 3); conduct experimental validation on diverse testbeds to assess performance degradation; define standardized robustness metrics for benchmarking.
Integration of AI and Control Theory	Synergistic methods combining AI learning with classical control	How to design hybrid frameworks that provide formal stability guarantees while enabling the adaptability of AI? Milestones: Propose architectures that tightly couple online learning with model predictive control or Lyapunov-based methods; validate through stability proofs and simulation studies (Section 9); explore interpretability to enable safety-critical deployment.
Low-Latency and Reliability	AI approaches enabling ultra-reliable low-latency communications (URLLC)	What specialized AI-driven scheduling and resource allocation techniques can ensure URLLC requirements in wireless control loops? Milestones: Develop latency-aware AI models that predict channel states and network conditions for dynamic scheduling (Section 4); benchmark delay-reliability trade-offs in real-time control scenarios; integrate with adaptive control policies to mitigate packet loss.
Data Privacy and Security	AI methods preserving privacy and ensuring network security	How to safeguard data privacy and defend against adversarial attacks in AI-enabled wireless control systems? Milestones: Formulate secure federated learning and differential privacy mechanisms within control frameworks; analyze vulnerabilities to adversarial inputs and propose robustified models (Section 7); demonstrate through simulated and physical attacks resilience metrics and mitigation strategies.
Real-World Deployment	Bridging theory-to-practice gap through prototyping and field trials	What are the practical barriers such as hardware constraints, scalability issues, and unforeseen environmental factors that hinder real-world adoption? Milestones: Deploy pilot AI-enabled wireless control systems in industrial or urban environments; collect and analyze empirical performance and failure cases; develop open-source toolkits and standardized benchmarks to promote reproducibility and community engagement (links to all sections).

enable transparent and systematic evaluation. Existing initiatives such as [placeholder for relevant open-source frameworks] can be expanded to incorporate wireless control scenarios, enabling the community to share datasets, algorithms, and deployment experiences. Field trials and industrial collaborations will be vital to validate theoretical predictions, uncover hidden challenges, and guide algorithmic refinements toward deployable AI-enabled wireless control systems.

This synthesis articulates a comprehensive roadmap that tightly links future opportunities with concrete research questions and milestones, grounded in the thematic structure of this survey. Such clarity and specificity are crucial for advancing the state of the art and accelerating adoption of robust, scalable, and secure AI-driven wireless control in real-world applications.

10.1 Methodological Contributions and Frameworks

The integration of AI techniques with control and wireless systems has led to innovative frameworks that enable adaptive, resilient, and efficient operation in complex environments. To advance this field, future research should prioritize the development of standardized methodological frameworks that unify these interdisciplinary approaches. Such frameworks would facilitate consistent benchmarking, reproducibility, and scalability of results across diverse applications. Key characteristics of these frameworks include robustness against system uncertainties, real-time adaptability to dynamic and stochastic conditions, and data-driven optimization strategies. Importantly, these frameworks must also preserve the theoretical guarantees foundational to control theory and wireless communications, ensuring reliability and safety in AI-enabled systems. By establishing comprehensive and standardized methodological frameworks, research can bridge current gaps between disparate methodologies, streamline integration efforts, and accelerate the practical deployment of intelligent control and wireless systems in real-world scenarios.

10.2 Practical Implementation Pathways and Challenges

While theoretical advancements abound, the practical implementation of AI-enabled control and wireless systems confronts several critical challenges. These challenges include computational resource constraints, stringent latency requirements, maintaining robustness amid dynamic and uncertain environments, and seamless integration with existing legacy infrastructure. To address these issues, future research should prioritize the development of scalable and efficient algorithms that are compatible with edge computing paradigms and distributed architectures, thereby reducing latency and resource demands. Furthermore, as AI systems are increasingly deployed in sensitive and mission-critical applications, it is essential to rigorously manage privacy, security, and ethical considerations throughout the design and deployment phases to ensure trustworthy and responsible AI operation.

10.3 Potential Disruptive Innovations and Paradigm Shifts

Emerging trends indicate several potential disruptions in the field, each with transformative implications. One significant innovation is the convergence of AI, control, and wireless communication technologies, which may enable self-organizing and self-optimizing networks capable of dramatically enhancing efficiency and responsiveness. For example, autonomous network management systems utilizing reinforcement learning can dynamically adapt resource allocation without human intervention, improving latency and throughput under varying conditions.

Another paradigm shift is expected from the fusion of model-based and data-driven approaches, producing hybrid methods that exploit the complementary strengths of both paradigms. Such approaches combine theoretical guarantees from model-based designs with the adaptability and scalability of data-driven methods, as demonstrated in recent prototypes for channel estimation and signal processing that achieve superior robustness and performance.

Additionally, further research into cross-layer design that integrates AI across multiple system levels holds promise for transforming traditional system architectures. By enabling holistic optimization from physical to application layers, these designs facilitate more adaptive and intelligent communication systems. For instance, AI-enabled cross-layer protocols have shown improved quality of service in next-generation networks by jointly optimizing routing, scheduling, and power control.

These emerging innovations illustrate a shift toward highly integrated, intelligent network systems that can autonomously manage complex environments, marking a substantial departure from

conventional approaches and pointing toward new frontiers in communication system design.

10.4 Comparative Summary of Key Approaches

To facilitate a clear understanding of the relative merits, limitations, and practical considerations of the approaches discussed throughout this survey, Table 21 provides a detailed comparative summary. It highlights the principal characteristics, implementation challenges, and key application domains of representative methods, enabling readers to grasp their contextual suitability and trade-offs.

10.5 Interdisciplinary Synergies

The symbiotic relationship between AI, control theory, and wireless communication is poised to deepen significantly, paving the way for innovative system designs that overcome traditional domain-specific boundaries. To foster impactful progress, researchers should actively encourage interdisciplinary collaborations that integrate advances across sensing technologies, computational methodologies, and theoretical frameworks. These collaborations are essential for developing comprehensive and robust solutions that effectively tackle complex real-world challenges by leveraging complementary strengths from each field.

Moving forward, consolidating diverse methodological advances into unified frameworks that seamlessly integrate AI, control, and wireless communication technologies will be crucial. This integration must explicitly address practical implementation challenges, such as scalability, latency, and reliability, to facilitate the translation of theoretical innovations into deployable systems. Furthermore, anticipating and adapting to emerging paradigm shifts—including hybrid models and adaptive, data-driven control strategies—will promote the creation of more flexible and resilient system architectures. By emphasizing and strengthening these interdisciplinary synergies, the research community can accelerate the development of autonomous, efficient, and dependable systems with broad and meaningful impact across diverse applications.

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 (FDI) attacks. As detailed in [3], such systems are modeled with unknown, possibly time-varying delays and combined faults/attacks affecting actuators and sensors. Radial basis function neural networks are employed to approximate the unknown nonlinear dynamics by representing the nonlinear function $f(x(t), x(t-\tau))$ as $W^T\Phi(x(t), x(t-\tau)) + \varepsilon$, where W are adaptive weights estimated online. An observer-based fault detection mechanism is integrated to estimate system states and faults despite measurement discrepancies introduced by FDI attacks. Through an adaptive control law incorporating these elements, finite-time convergence of state and estimation errors is achieved, which significantly enhances resilience compared to traditional asymptotic techniques by enabling faster system responses under substantial unknown disturbances.

Definition 10.1 (Finite-Time Convergence). Finite-time convergence refers to the property of a system's state or estimation error to reach an equilibrium point exactly within a finite time interval, as opposed to asymptotic convergence which approaches the equilibrium asymptotically over infinite time.

In parallel, AI has invigorated wireless communications through advanced paradigms such as Perceptive Mobile Networks (PMNs). These networks integrate coordinated beamforming with deep learning algorithms to predict and mitigate interference in complex multi-cell environments [**?**]. Specifically, the AI-empowered framework dynamically allocates resources based on learned interference patterns by exploiting macro-diversity and array gains through coordinated sensing across multiple base stations. This adaptive approach maintains communication quality while substantially improving sensing accuracy under heterogeneous and interference-prone conditions. The system dynamically adjusts beamforming strategies and resource scheduling to optimize the sensing signal-to-interference-plus-noise ratio (SINR) and communication performance simultaneously, facilitating robust wireless resource orchestration despite challenges such as low-latency inference and channel acquisition.

Definition 10.2 (Perceptive Mobile Networks (PMNs)). PMNs are wireless networks that combine communication and sensing functionalities by leveraging advanced signal processing and AI to provide both data transmission and environment perception capabilities.

Further extending this ecosystem, AI-driven optimization of reconfigurable intelligent surfaces (RIS) offers a powerful approach to shaping the wireless propagation environment. By learning mappings from channel state information to effective RIS configurations, these AI-empowered systems enhance spectral efficiency and system robustness under uncertain and time-varying channel conditions [18]. This integration of AI, control theory, and advanced wireless technologies exemplifies how networks can achieve context-aware, adaptive decision-making and resilient operation despite inherent cyber-physical uncertainties, advancing toward next-generation secure and adaptive wireless systems.

Definition 10.3 (Reconfigurable Intelligent Surfaces (RIS)). RIS are planar surfaces consisting of numerous small elements whose electromagnetic properties can be dynamically manipulated to control the propagation of wireless signals in the environment.

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 22.

Below, we provide a critical discussion of each enabler with examples from current studies and highlight open research gaps, including relevant performance observations and application impacts:

Table 21: Comparative summary of key AI-based control and wireless methodologies

Approach	Methodological Strengths	Practical Challenges	Application Domains
Model-based control with AI integration	Strong theoretical foundations and interpretability facilitate reliability and safety assurances	High computational complexity and the need for accurate system models may limit adaptability	Autonomous systems, robotics, and safety-critical control
Data-driven machine learning methods	High adaptability and scalability enable handling complex, dynamic environments	Requires large volumes of data and may lack formal performance guarantees	Network optimization, resource management, and traffic prediction
Hybrid model-data fusion frameworks	Combines theoretical rigor with flexibility to improve robustness	Complexity in integration and parameter tuning poses practical hurdles	Smart grids, 5G/6G communication networks, and cyber-physical systems
Reinforcement learning for control	Enables real-time learning and policy optimization in uncertain environments	Balancing exploration and exploitation remains challenging, along with convergence guarantees	Unmanned aerial vehicles (UAVs), Internet of Things (IoT) device management
Edge AI and distributed architectures	Supports low-latency processing and scalable deployment across network edges	Communication overhead and privacy concerns require careful management	Smart cities, industrial automation, and distributed sensing

Table 22: 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; trade-offs among differential privacy, encryption, and secure computation	Secure data exchange in multi-operator networks
Edge Intelligence	Decentralizes computation to reduce latency and optimize resource usage at the network edge	Limited edge resources, coordination across nodes, model consistency, heterogeneity of devices	Real-time adaptive interference mitigation
Explainable AI	Provides transparency and interpretability for black-box models, enhancing trust and regulatory compliance	Complexity of explanations, potential trade-off between interpretability and accuracy [24]	Visualizing reinforcement learning decision paths
Scalable Distributed Architectures	Support multi-agent RL and adaptive control across heterogeneous and large-scale network segments	System complexity, scalability bottlenecks, interoperability issues	Large-scale network fault detection systems

Federated Learning. This approach facilitates collaborative model training across decentralized nodes without raw data exchange, addressing stringent privacy concerns inherent in wireless networks. In Open RAN contexts, federated learning enables dynamic spectrum management and fault detection by aggregating local AI insights, leading to improved spectral efficiency and robustness [6]. Experimental analyses demonstrate that AI-enabled methods using federated learning outperform traditional heuristics by effectively adapting to dynamic channel conditions. However, challenges such as communication overhead, non-iid data distributions, and convergence difficulties still limit scalability and require further algorithmic enhancements to optimize trade-offs between learning accuracy and resource consumption.

Privacy-Preserving AI. Closely related to federated learning, privacy-preserving mechanisms—including differential privacy, secure multi-party computation, and homomorphic encryption—protect sensitive user and network information while maintaining user trust. These methods must carefully balance privacy guarantees against model accuracy and computational overhead. In wireless network scenarios, this balancing act is crucial to operating within constrained latency and processing budgets. Ongoing research focuses on identifying optimal configurations that minimize the impact on inference performance while securing data, especially in multi-operator environments where data sharing is sensitive.

Edge Intelligence. By decentralizing processing to network edge nodes, edge intelligence significantly reduces latency and bandwidth consumption compared to centralized cloud architectures. Applications such as real-time interference mitigation and localized adaptive control benefit from edge deployment, achieving faster response times and more fine-grained network adaptation. Yet, limited computational resources and the heterogeneity of edge devices pose constraints on model complexity and scalability. Coordinating distributed inference while maintaining model consistency and coping with device diversity remain open challenges, requiring innovative distributed learning algorithms and system designs to harness the edge advantage without sacrificing accuracy.

Explainable AI. Given the widespread deployment of complex neural architectures and reinforcement learning agents in network management [24], explainability enhances system transparency, fosters user trust, and supports compliance with regulatory standards. Techniques that interpret AI decisions and visualize agent behaviors enable operators to identify system weaknesses and biases, thus improving reliability. Performance studies highlight the trade-off that often exists between interpretability and prediction accuracy, necessitating new model designs tailored for wireless applications that maintain both high performance and explainability. This is vital as network decisions impact service quality and security.

Scalable Distributed Architectures. Addressing the scale and complexity of next-generation wireless systems demands distributed frameworks that combine multi-agent reinforcement learning and adaptive control. Such architectures provide resilience and fault tolerance across diverse, heterogeneous network segments. Evaluations of large-scale deployment scenarios reveal that these frameworks can improve fault detection accuracy and system responsiveness. Nonetheless, challenges related to system complexity, scalability bottlenecks, and interoperability among varied network components remain. Research efforts are devoted to developing scalable, interoperable, and efficient distributed frameworks that preserve performance while managing networking and computational overhead.

In summary, these enablers collectively advance AI's feasibility in wireless and cyber-physical systems by tackling privacy, interpretability, latency, and scalability challenges. Performance insights from recent studies demonstrate notable gains in spectral efficiency, network robustness, and management accuracy attributable to these technologies. However, ongoing research is essential to resolve existing trade-offs between performance, complexity, and trustworthiness, ultimately enabling the realization of fully intelligent and adaptive wireless networks.

10.8 Identified Research Needs

This section outlines the key research gaps that must be addressed to advance AI-enhanced resilient control and wireless systems. The primary objectives are to develop computationally efficient, robust, low-latency, interpretable, and interdisciplinary AI frameworks that achieve resilient and scalable performance in dynamic cyber-physical environments. Addressing these challenges will enable reliable operation, real-time responsiveness, and user trust in next-generation cyber-physical infrastructures. To guide research focus, the needs are ranked by urgency and potential impact as shown in Table 23.

Computational Complexity Reduction: Highest urgency is assigned here due to the critical need for deployable solutions on resource-constrained devices. Current adaptive neural network finite-time resilient control approaches for nonlinear time-delay

Table 23: Summary of Key Research Challenges Ranked by Urgency and Potential Impact, with Specific Illustrative Techniques

Rank	Research Need	Challenges	Potential Solution Paths and Illustrations
1	Computational Complexity Reduction	High neural network capacity, sensitivity to noise, time-varying delays	Adaptive dynamic pruning (e.g., magnitude-based pruning), distributed resilient control via multi-agent consensus, neural network quantization and low-rank factorization, hardware-efficient algorithms leveraging FPGA and ASIC implementations [3]
2	Robustness Against Uncertainties	Vulnerability to adversarial perturbations, noisy telemetry, imperfect channel info	Resilient AI with robust training (e.g., adversarial training), cooperative multi-agent reinforcement learning, real-time adaptation via online learning, interference mitigation using coordinated beamforming and AI-based channel estimation [18]
3	Latency Minimization	Real-time inference demands, resource constraints, trade-offs between accuracy and speed	Lightweight architectures such as MobileNets, hardware accelerators with GPUs and TPUs, scalable reinforcement and deep learning optimizing network management, edge-cloud synergy for adaptive offloading [24]
4	Interpretability Enhancement	Lack of transparency in AI decisions, regulatory and operational trust issues	Explainable AI frameworks including SHAP and LIME, model introspection techniques like layer-wise relevance propagation, visualization tools of decision paths, domain-aware explanations tailored to control and networking contexts
5	Interdisciplinary Collaboration	Integrating diverse expertise across control, communications, and AI	Holistic multi-layer frameworks combining algorithmic design, hardware optimization, and network layering; fostering joint research and development platforms and consortia

systems exhibit robustness to unknown actuator faults and cyber-attacks but require high neural network capacity and are sensitive to noise and parameter settings [3]. Concrete strategies involve dynamic pruning methods that remove less significant network connections during training to reduce complexity, and distributed resilient control frameworks leveraging multi-agent consensus protocols to share computation load. Neural network compression techniques such as quantization and low-rank decompositions, along with FPGA or ASIC tailored implementations, further contribute to hardware-efficient inference and control.

Robustness Against Uncertainties: Ranked second due to the substantial impact of adversarial conditions on system reliability. AI models in networked sensing and control remain vulnerable to adversarial perturbations, noisy measurements, and imperfect channel information [18]. Robust AI training methodologies like adversarial training and domain randomization can improve resilience. Cooperative multi-agent reinforcement learning enhances robustness by exploiting diversity and coordination for interference mitigation via coordinated beamforming and AI-based channel estimation techniques. Real-time adaptive learning mechanisms enable systems to counteract evolving disturbances and adversarial inputs dynamically.

Latency Minimization: Placed third reflecting real-time operational demands critical in edge deployments. The challenge lies in balancing inference speed and accuracy under limited computational resources [24]. Development of lightweight neural network architectures such as MobileNets or EfficientNets facilitates fast inference. Dedicated hardware accelerators including GPUs, TPUs, and specialized ASICs significantly reduce computation times. Scalable reinforcement and deep learning algorithms optimize resource allocation dynamically, while synergistic edge-cloud computing enables adaptive offloading of intensive tasks to satisfy stringent latency requirements.

Interpretability Enhancement: This need supports operational trust and regulatory compliance in safety-critical systems. Explainable AI approaches such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) provide insight into model decision rationale. Model introspection techniques like layer-wise relevance propagation and visualization of decision pathways facilitate effective debugging and validation. Tailoring explanations to domain contexts in control and wireless communications enhances usability and fosters trust.

Interdisciplinary Collaboration: Though ranked last, it remains essential for holistic progress. Synergistic efforts combining control theory, wireless communications, and AI are imperative to tackle complex cyber-physical challenges. Joint frameworks integrating algorithmic, hardware, and network layers with shared research initiatives accelerate innovation toward resilient, scalable AI-empowered infrastructures.

In summary, the prioritized research objectives presented here target the development of resilient, scalable, interpretable, and efficient AI solutions for complex cyber-physical environments. Clear elucidation of challenges with concrete illustrative techniques aims to focus research efforts and bridge key gaps, empowering future systems to achieve dependable real-world operations with enhanced reliability and trustworthiness.

10.9 Anticipated Innovations

This section explicitly highlights the key objectives of forthcoming advancements within AI-empowered wireless networks, focusing on transformative innovations that promise enhanced autonomy, security, and efficiency while addressing current implementation challenges. The synthesis frames these innovations within a conceptual model emphasizing the interplay of technological capabilities, operational constraints, and mitigation pathways, balanced by current feasibility considerations and expected development timelines.

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, notably within Open RAN contexts, have demonstrated significant gains in resource allocation, anomaly detection, and network resilience [6, 25]. However, challenges such as coordination complexity, communication overhead, scalability, and adversarial robustness remain substantial. To address these, future research may explore hierarchical agent architectures that reduce coordination burdens and lightweight consensus mechanisms minimizing latency and computational costs. Federated learning frameworks incorporating privacy-preserving and adaptive convergence protocols are expected to evolve within the next 3–5 years, offering a balanced trade-off between privacy, latency, and real-time responsiveness. These advancements are crucial for scalable, decentralized AI-enabled networks.

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 tasks essential for next-generation wireless systems [24]. The complexity of hardware design and integration challenges necessitates modular accelerator architectures offering configurable performance-to-energy ratios tailored to resource-constrained environments. Cost-effective fabrication methods and open accelerator standards will be pivotal for widespread adoption and interoperability with heterogeneous network elements. Progress in this area is anticipated to mature steadily within the upcoming 2–4 years, driven by collaborations between hardware designers and network researchers. Such innovation supports the critical demand for efficient edge AI deployment.

Quantum Computing Integration: Quantum technologies hold promise for breakthroughs in optimization speed and security, enabling accelerated resolution of complex network computation tasks beyond classical capabilities. Despite significant challenges, including immature hardware technology, high quantum error rates,

and the need for application-specific quantum algorithms, ongoing research and experimental prototypes present viable mitigation strategies. Hybrid quantum-classical architectures, leveraging early quantum processors for specialized optimization sub-tasks while maintaining classical control, offer a near-term approach to integration. Concurrently, the development of noise-resilient quantum algorithms and error-correction protocols tailored to network optimization and security is a crucial research direction, likely progressing beyond 5 years from now, as hardware and algorithmic maturity improves. This trajectory emphasizes practical deployment readiness through phased quantum adoption.

Blockchain Security Mechanisms: Blockchain-based approaches enhance the security of decentralized AI agents by ensuring data integrity and providing transparent audit trails, thereby reinforcing trustworthiness in collaborative learning systems [25]. Main challenges include blockchain-associated latency overhead, scalability limitations, increased computational demands, and privacy/regulatory compliance concerns. Scalable consensus protocols, such as variants of proof-of-stake, along with off-chain processing techniques, can alleviate throughput bottlenecks and reduce latency impacts. Privacy-preserving blockchain implementations combined with compliance-aware smart contracts promise alignment with data protection regulations. Careful architectural alignment of blockchain solutions with network performance imperatives is essential to minimize effects on latency-sensitive operations. These solutions are expected to mature within a 3–6 year horizon, integrating seamlessly with evolving AI-controlled network environments.

Collectively, these anticipated innovations envision fully autonomous intelligent networks characterized by self-healing capacities, context-aware adaptations, and proactive cyber-physical threat mitigation [5]. Achieving this vision requires managing trade-offs among computational complexity, scalability, security, and interoperability through integrated frameworks. Techniques such as explainable AI improve transparency and trust, hierarchical agent designs enhance multi-agent coordination, and lightweight model development supports efficient edge deployment. This conceptual synthesis underscores critical enablers and actionable research directions to overcome identified challenges, situating each innovation within a realistic development and deployment trajectory.

The following table summarizes the key innovations, their benefits, associated challenges, and prospective mitigation strategies with improved clarity and readability:

In summary, this nuanced synthesis elucidates the multi-dimensional progress and outstanding challenges at the intersection of AI, resilient control, and wireless technologies. By explicitly linking benefits with challenges and forward-looking mitigation approaches, and situating innovations within practical feasibility and development timelines, it establishes a comprehensive and actionable roadmap. This roadmap guides the evolution of secure, adaptive, and intelligent networked systems capable of effectively addressing future demands and operational uncertainties.

11 Conclusion

This survey aimed to comprehensively review the integration of artificial intelligence (AI) techniques into telecommunication networks, focusing on their roles in adaptive control, wireless networking, routing, software-defined networking (SDN), Open Radio Access Networks (Open RAN), and autonomous fault management. Our objectives included synthesizing state-of-the-art AI methods, evaluating their benefits and challenges, and identifying future research directions to guide the evolution towards fully autonomous, self-optimizing network systems.

11.1 Key Contributions and Findings

The integration of AI into various telecommunication domains has markedly enhanced functionalities such as adaptive control, wireless networking, routing, SDN, 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. For instance, as demonstrated in recent work [27], gradient boosting methods such as CatBoost and LightGBM significantly outperform traditional algorithms in telecom customer churn prediction. These methods effectively manage nonlinearities and class imbalances without external resampling, although this improved accuracy comes at the cost of increased computational requirements. This illustrates the trade-off between predictive performance and resource efficiency in practical deployments.

Collectively, these advances underscore AI's critical contribution to enhancing efficiency and resilience in contemporary telecommunication infrastructures.

11.2 Challenges and Future Directions

Looking ahead, the evolution of telecommunication networks is trending towards fully autonomous, self-optimizing systems capable of continuous self-monitoring and dynamic adjustment. However, deploying AI solutions at scale introduces significant challenges:

- **Scalability concerns**: The computational demands of complex models such as gradient boosting need to be balanced with the requirement for real-time responsiveness. - **Security and privacy vulnerabilities**: AI-integrated control loops may be susceptible to adversarial attacks, posing risks to network stability and data confidentiality. - **Interoperability difficulties**: The heterogeneous and multi-vendor nature of telecom environments complicates seamless AI solution integration. - **Explainability and transparency**: Particularly with unsupervised learning algorithms, lack of interpretability can hinder trust and accountability.

Promising explainable AI (XAI) frameworks offer pathways to address some of these challenges. For example, the neuralization approach that reformulates clustering models as neural networks

Table 24: Summary of Anticipated Innovations: Benefits, Challenges, and Mitigation Approaches

Innovation	Benefits	Challenges / Limitations	Potential Mitigation Strategies
Multi-Agent Collaborative Learning	Enhanced adaptability, fault tolerance, and optimized resource management [6, 25]	Coordination complexity, scalability, communication overhead, adversarial robustness	Hierarchical agent designs, lightweight consensus protocols, federated privacy-preserving frameworks
Hardware Acceleration	Reduced inference latency and energy consumption enabling real-time adaptive control [24]	Design complexity, integration challenges, cost considerations, balancing energy and compute resources	Modular configurable architectures, open standards, cost-effective fabrication processes
Quantum Computing Integration	Potential for accelerated optimization, enhanced security in network operations	Immature hardware, high error rates, need for specialized quantum algorithms	Hybrid quantum-classical systems, noise-resilient quantum algorithms, advanced error correction
Blockchain Security Mechanisms	Enhanced data integrity, auditability, and trust in decentralized AI [25]	Latency overhead, scalability constraints, high computational demand, privacy and regulatory concerns	Scalable consensus mechanisms, off-chain computation, privacy-preserving protocols, compliance-aware smart contracts

reveals feature importances and makes cluster assignments interpretable [**?**], thereby improving transparency and trust in autonomous network operations.

11.3 Holistic Perspective and Interdisciplinary Importance

Our unique synthesis conceptualized the interplay between AI methodologies and telecom network layers—control, orchestration, and management—highlighting how AI integration across these strata facilitates unprecedented levels of self-governance and resilience. This holistic view emphasizes the necessity of interdisciplinary research to manage integration complexity, and the careful balancing of scalability, security, and explainability.

11.4 Summary of Key Points

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

Summary of Key Points:

• This survey reviewed AI's transformative impact on telecommunication functionalities including adaptive control, routing, and fault management, focusing on predictive and ensemble learning models.

• Gradient boosting methods outperform traditional algorithms in customer churn prediction by effectively managing class imbalance and nonlinear relationships [27], albeit with higher computational costs.

• Key deployment challenges include scalability, security/privacy, interoperability, and explainability.

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

• The envisioned future involves fully autonomous, self-optimizing networks, necessitating interdisciplinary research to surmount integration obstacles.

This structured and explicitly stated summary consolidates the survey's main contributions and emphasizes critical enablers and research avenues necessary to advance AI-driven telecommunications.

11.5 Concluding Remarks

In summary, the progression towards next-generation telecommunication networks is grounded in sophisticated AI methodologies that are autonomous, efficient, secure, and interpretable. Realizing this vision demands continued advancement of AI-driven frameworks that can operate robustly at scale and with transparency, fulfilling the stringent requirements of future communication infrastructures.

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.

[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 infrastructureless 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