Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.084949

REVIEW

A Survey on AI-Enabled Network Protocols for Quantum-Resilient Communication

Bareera Anam, Muhammad Asim, Muhammad Nadeem Ali and Byung-Seo Kim*

Department of Software and Communications Engineering, Hongik University, Sejong Campus, Sejong-si, Republic of Korea

*Corresponding Author: Byung-Seo Kim. Email: jsnbs@hongik.ac.kr

Received: 02 May 2026; Accepted: 07 July 2026; Published: 13 August 2026

ABSTRACT: The rapid evolution of communication networks, driven by the expansion of heterogeneous environments such as 6G, Internet of Things (IoT), and edge computing, has exposed a critical research gap in the lack of unified frameworks that jointly address intelligent network control and quantum-resilient security. Existing networking protocols were originally designed under static configurations and classical security assumptions, making them increasingly inadequate for dynamic, large-scale, and intelligent infrastructures exposed to quantum-enabled threats. At the same time, the emergence of Quantum Computing (QC) introduces severe security risks, as widely used cryptographic mechanisms supporting protocols such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec) become vulnerable to quantum attacks. This paper presents a structured survey based on a systematic classification of recent literature across AI-enabled networking, Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and protocol-level integration approaches. The review categorizes existing works into AI-driven network optimization, quantum-resilient security mechanisms, and hybrid AI–QRC architectural frameworks, enabling a unified comparison of design strategies and deployment models. Furthermore, this survey analyzes how Artificial Intelligence (AI) techniques enable autonomous network operations while Quantum-Resilient Cryptography (QRC) approaches provide post-quantum security guarantees, highlighting their complementary roles in next-generation network design. The study further synthesizes key findings for a tightly coupled AI–QRC co-design, which remains an open challenge due to mismatched assumptions in control latency, cryptographic overhead, and protocol adaptability. Additionally, this review emphasizes the need for integrated frameworks that combine intelligence and quantum security to develop adaptive, scalable, and resilient network protocols for the post-quantum era.

KEYWORDS: Artificial intelligence; quantum-resilient communication; post-quantum cryptography; network protocols; autonomous networks; quantum Internet; secure networking; reinforcement learning; TLS; QKD

1 Introduction

Communication networks form the backbone of modern digital infrastructure. From cloud computing and financial systems to industrial automation, telemedicine, and national defence, nearly every sector now relies on secure and efficient communication. Over the past five decades, the Internet has evolved from a small-scale research initiative into a globally interconnected system serving billions of users and a rapidly growing number of devices [1]. Incremental refinements have driven this evolutionary trajectory to the classic network protocols such as Internet Protocol (IP), Transmission Control Protocol (TCP), Border Gateway Protocol (BGP), TLS, and their successors, designed in an era defined by relatively constrained threat models, predictable traffic patterns, and computational environments that rendered brute-force cryptographic attacks infeasible. The foundational assumptions embedded in these protocols-deterministic

and rule-based behaviour, static or slowly evolving threat models, public-key cryptography secure against classical adversaries, and limited requirements for autonomous decision-making defined a technological paradigm that served well for decades [2].

That paradigm is now under simultaneous pressure from two disruptive technological forces. First, the rapid maturation of QC threatens to invalidate the mathematical hardness assumptions underlying ECC (Elliptic Curve Cryptography), RSA (Rivest-Shamir-Adleman), and Diffie-Hellman key exchange. Shor's algorithm, executable in polynomial time on a sufficiently large fault-tolerant quantum processor, can factor large integers and solve discrete logarithm problems efficiently [3]. Grover's algorithm effectively halves the security level of symmetric cryptographic schemes. Adversaries engaged in Harvest-Now-Decrypt-Later (HNDL) attacks may already be collecting and storing large volumes of encrypted traffic with the expectation that future advances in QC could enable retrospective decryption of currently secure communications [4,5]. Second, AI has achieved remarkable capabilities in domains marked by high dimensionality, non-stationarity, and uncertainty. RL agents have demonstrated superhuman performance in sequential decision-making tasks; deep neural networks provide state-of-the-art classification and anomaly detection; and Federated Learning (FL) enables distributed model training without centralizing sensitive data. These advances open the prospect of networks capable of autonomous, intent-driven operations [6]. Despite growing research activity across both domains, existing work remains fragmented. Studies on AI-driven networking predominantly focus on performance optimization and traffic engineering, generally assuming classical cryptographic security remains adequate [7]. Conversely, research on QRC emphasizes cryptographic primitives and QKD, with limited attention to protocol intelligence or adaptive behaviour [8]. This disciplinary separation produces three principal gaps: lack of holistic protocol co-design, insufficient integrated survey coverage, and limited architectural guidance for AI-enabled protocols over quantum-resilient frameworks. This survey addresses the convergence of transformative forces, AI-driven network intelligence and quantum-resilient security, in the context of next-generation network protocol design. We synthesize contributions across Deep Reinforcement Learning (DRL), FL [9,10], PQC [11–14], QKD [15–18], graph neural networks [19], privacy-preserving Machine Learning (ML) [20,21], and Quantum Machine Learning (QML) [22,23], providing a unified reference for researchers and practitioners. The motivation for this survey is twofold. First, existing surveys tend to address AI-driven networking or PQC in isolation, without systematically examining how these fields must co-evolve to meet the security and performance requirements of future networks [24,25]. Second, practical integration of PQC and QKD within operational network protocols, particularly within Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) based architectures [26,27], remains an emerging area, and a systematic review of progress and challenges in this space is warranted [18,28]. The uniqueness of this survey's contribution rests on specific characteristics that, taken together, are not provided by existing surveys in the literature. First, whereas prior surveys examine AI-driven network optimization [24] or post-quantum cryptographic algorithms [25] as separate research threads, this survey systematically examines their co-design requirements, specifically how AI state representations, reward functions, and action spaces must be restructured to account for PQC-induced handshake latency, increased certificate sizes, and QKD key pool constraints, none of which appear as variables in existing AI networking formulations. Second, the survey addresses protocol-layer integration concretely and specifically by examining how Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM), Module-Lattice-Based Digital Signature Algorithm (ML-DSA), and QKD effect TLS 1.3, Quick UDP Internet Connections (QUIC), Internet Key Exchange version 2 (IKEv2), Domain Name System Security Extensions (DNSSEC), and BGP at the handshake, certificate, and key management levels, rather than treating PQC as an abstract algorithm substitution problem. Third, the survey provides a unified treatment of the full AI-quantum protocol stack, from physical-layer QKD key

generation through SDN control-plane orchestration to application-layer anomaly detection, within a single analytical framework. Fourth, the (HNDL) threat is analyzed not merely as a cryptographic concern but as an operational protocol design constraint that makes PQC migration of currently deployed TLS, IPsec, and BGP sessions an immediate priority rather than a deferred research question.

1.1 Positioning of This Survey

Table 1 summarizes existing surveys across three dimensions: AI-driven networking coverage, quantum-resilient security coverage like PQC, QC, QKD, and protocol-level integration. This survey is unique in jointly addressing all dimensions. To provide a consistent and transparent comparison, the qualitative ratings reported in Table 1 are assigned according to the depth and breadth of coverage provided by each survey. Specifically, 'High' indicates a comprehensive discussion involving multiple subtopics with detailed technical and protocol-level analysis; 'Medium' denotes moderate coverage with discussion of key concepts but limited technical depth or scope; 'Low' represents only brief coverage or passing mention of the topic; and 'None' indicates that the topic is not substantively discussed. These ratings were assigned based on the content presented in the respective surveys and are intended to provide a qualitative overview of their relative coverage rather than a quantitative performance evaluation.

Table 1: Comparison of related survey scope and coverage.

Survey	AI-Driven Networking Coverage	PQC Coverage	QC Coverage	QKD Coverage	Protocol-Level Integration
Luong et al. [29]	High	Low	Low	Low	Low
Xiao et al. [30]	High	None	None	None	Low
Ríos-Guiral et al. [31]	High	None	None	None	Low
Tam et al. [32]	High	None	None	None	Low
Bikkasani and Yerabolu [33]	High	None	None	None	Low
Farris et al.; Bakhiet et al. [34,35]	Medium	Low	Low	Low	Medium
Abdi et al. [36]	High	Low	Low	Low	Medium
Pattaranantakul et al. [37]	Low	None	None	None	Medium
Nguyen et al. [38]	Medium	None	None	None	High
Siddiqi et al. [39]	High	None	None	None	Medium
Luong et al.; Xiao et al. [29,30]	High	Low	Low	Low	Low
Chawla & Mehra; Chhetri et al.; Sharath et al. [40–42]	Low	High	High	High	Medium
This Survey	**High**	**High**	**High**	**High**	**High**

Note: Rating Criteria: High = comprehensive coverage with substantial technical depth, multiple subtopics, and protocol-level analysis; Medium = partial coverage with moderate technical discussion; Low = limited coverage or brief mention of the topic; None = topic not addressed.

1.2 Methodology

To ensure rigour, transparency, and reproducibility, this study adopts a structured literature search and screening process, with the literature review conducted in reference to the transparency principles of the PRISMA guidelines. The literature search was conducted across major scientific databases, including IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and arXiv, and was supplemented with official reports, standards, and technical documentation from National Institute of Standards and Technology (NIST), Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI), and International Telecommunication Union-Telecommunication Standardization Sector (ITU-T). Search queries were constructed using combinations of keywords related to AI, ML, PQC, QKD, quantum communication, network protocol design, SDN, NFV, autonomous networking, IoT, edge computing, and quantum-resilient communication systems. A PRISMA-guided study selection process was employed. Initially, records were identified through database searches and additional sources. Duplicate records were removed before screening. Subsequently, titles and abstracts were examined to assess relevance to AI-enabled networking, PQC, quantum communication technologies, or their integration within network protocol architectures. Full-text assessment was then performed to determine final eligibility. Studies were included if they addressed AI-driven network management, post-quantum cryptographic mechanisms, quantum communication technologies, quantum networking architectures, or hybrid approaches combining these domains within communication systems. Eligible sources included peer-reviewed journal articles, conference papers, standards documents, and technical reports containing sufficient methodological or technical detail to support analysis. Studies were excluded if they were outside the scope of communication networks and protocols, focused solely on theoretical cryptographic constructions without networking relevance, lacked adequate technical detail, represented duplicate publications, or were otherwise unrelated to the objectives of this survey. The retained literature was systematically categorized along three complementary dimensions: (i) security mechanism, including PQC, QKD, and hybrid security approaches; (ii) AI methodology, including supervised learning, DRL, FL, graph neural networks, and anomaly detection techniques; and (iii) networking domain, including transport-layer protocols, routing and control-plane mechanisms, IoT and edge networks, and emerging quantum networking infrastructures. This three-dimensional classification framework guided the organization of the survey and facilitated cross-domain comparison of existing research efforts. Given the substantial heterogeneity of experimental methodologies, datasets, performance metrics, deployment environments, and threat models across the selected studies, a structured narrative synthesis approach was adopted in preference to quantitative meta-analysis. The analysis focuses on identifying prevailing research trends, methodological limitations, deployment challenges, performance trade-offs, and open research opportunities, with particular emphasis on the emerging convergence of AI-driven network control and quantum-resilient communication protocols. Further details are provided as supplementary material, where the study selection process is summarized using a PRISMA flow diagram in the supplementary file.

1.3 Paper Structure

We summarize the structure of this survey in Fig. 1. We begin with the preliminary research landscape in Section 2. Then, we examine the evolution of network protocols in Section 3. Next, Section 4 discusses quantum threats and quantum-resilient communication approaches. Section 5 focuses on the role of AI in network protocols. Section 6 presents the integration of AI and quantum-resilient mechanisms within SDN and NFV environments. Section 7 introduces the mathematical foundations for AI-driven and quantum-resilient networking. Section 8 outlines key challenges and open problems. Section 9 highlights research gaps and future directions. Finally, Section 10 concludes the paper.

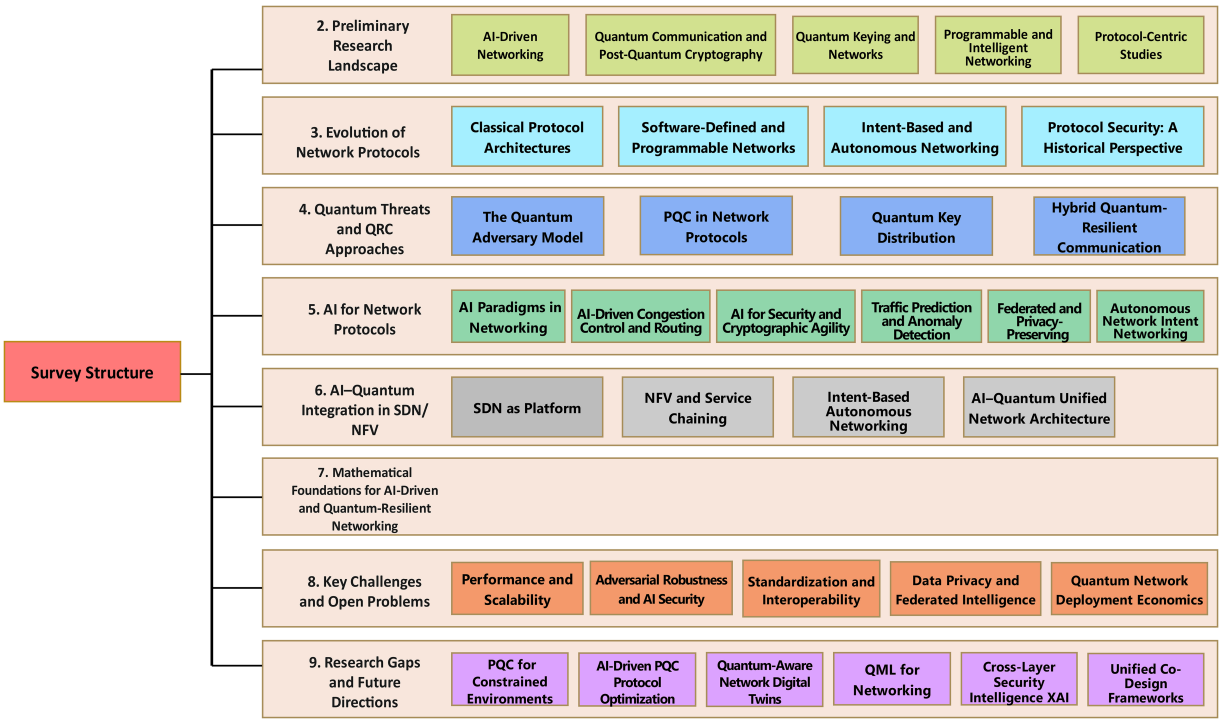

Figure 1: Outline of this survey paper.

2 Preliminary Research Landscape

Many studies have looked at the different areas discussed in this work. However, most of them treat AI-driven networking and quantum-resilient security separately, with little focus on combining the two. This section gives an overview of the existing research and highlights the main gaps.

2.1 AI-Driven Networking

A substantial body of survey literature addresses AI applications in communication networks. AI-driven networking has rapidly evolved from single-agent controllers to multi-agent and distributed AI for large, dynamic networks. The integration of AI into networking has driven significant advancements in optimization, automation, and adaptive control across modern communication systems. Reference [7] provides a comprehensive review of deep learning applications in networking, including traffic classification, routing, and congestion control. A study [29] surveys DRL approaches, examining their role in resource management, routing, and network slicing. Another paper [24] presents a broad overview of ML techniques for network management, encompassing supervised, unsupervised, and Reinforcement Learning (RL) methods. A manuscript [9] reviews the application of FL in wireless networks, with an emphasis on privacy preservation. Recent work on multi-agent DRL and knowledge sharing protocols shows that agents can coordinate to optimize traffic and congestion under varying conditions, improving convergence and stability in complex topologies [43–45]. In 5G and 6G, AI is increasingly used for joint optimization of routing, resource allocation, and traffic engineering, often atop SDN/NFV substrates that expose programmable control and telemetry [46–49]. However, these AI frameworks generally assume classical security primitives and do not account for PQC-induced changes in packet sizes, handshake latencies, or control plane scalability, leaving a gap in end-to-end secure, AI-managed network design [13]. A common limitation across this body of work is the assumption of classical cryptographic security. None of the reviewed AI

networking surveys explicitly addresses the impact of quantum threats on the protocols being optimized, nor do they explore how quantum-resilient security mechanisms interact with AI-driven adaptation. Post-quantum cryptographic primitives introduce qualitatively different computational overhead, latency profiles, and key management requirements that materially alter the optimization landscape for AI-driven protocols.

Quantum communication literature reflects a well-established body of work encompassing both quantum cryptography and PQC. Foundational developments in quantum cryptography are addressed in [15], while Ref. [11] covers post-quantum cryptographic approaches, including lattice-based, code-based, multivariate, and hash-based constructions. Advancements in QKD, including protocol design, security analyses, and experimental deployments, are detailed in [16]. In August 2024, NIST finalized three of its initial PQC standards: CRYSTALS-Kyber as FIPS 203 (ML-KEM), CRYSTALS-Dilithium as FIPS 204 (ML-DSA), and SPHINCS+ as FIPS 205 (SLH-DSA) [50]. FALCON was kept in development. It was formalized under the designation FN-DSA (FIPS 206) and represents an ongoing standardization and refinement process. These works primarily emphasize the mathematical and cryptographic foundations of quantum-resistant algorithms, with comparatively limited attention to protocol layer integration. Practical deployment challenges, including handshake latency, increased certificate sizes, and key management overhead, remain insufficiently explored systematically.

The NIST status reports [12,50] and the foundational NIST report on PQC [51] form the core references for the PQC standardization process, outlining candidate algorithms and evaluation methodologies across multiple rounds. The broader post-quantum cryptographic landscape is further characterized in [11]. Transition challenges from classical to PQC at the IETF protocol level are examined in [28], providing a framework for migration planning aligned with emerging standards. Performance implications of integrating PQC algorithms into widely used protocols such as TLS 1.3 [52] and Secure Shell (SSH) are quantified in [13], offering empirical insights for protocol design. This analysis is extended in [14] through the inclusion of Open Quantum Safe (OQS) library implementations [53], enabling evaluation across a wider range of algorithmic candidates. Hybrid cryptographic approaches are explored in [54] through the proposal of PQ-HPKE, addressing transitional requirements between classical and post-quantum systems. Implementation considerations at the hardware level, particularly for constrained environments, are investigated in [55], demonstrating Field-Programmable Gate Array (FPGA) based realizations of lattice-based key exchange. Enterprise readiness for quantum-safe cybersecurity is examined in [56], highlighting the gap between organizational awareness and practical deployment preparedness. Additionally, Universally Composable (UC) security frameworks in [57] provide a rigorous foundation for analyzing the security of PQC protocols in composed and real-world environments. Beyond foundational PQC and QKD surveys, newer work concentrates on system-level performance and deployment readiness. Multiple studies benchmark PQC algorithms and their integration into TLS and SSH across heterogeneous environments, quantifying handshake inflation, CPU load, and bandwidth overhead, and proposing optimizations and migration frameworks for cloud and IoT deployments [13]. Parallel efforts design hybrid and code-based PQC–TLS frameworks and side-channel-aware implementations, emphasizing cryptographic diversity and compatibility with existing infrastructure [8,9]. In quantum networks, research shifts from protocol taxonomy to practical key management [58], relay trust models, and SDN-based control architectures for scalable QKD networks, yet these works are rarely coupled with AI-driven network control [11,15]. This separation of concerns reinforces the need for a unified view in which PQC/QKD constraints explicitly shape learning-based control policies.

2.2 Quantum Keying and Networks

Quantum cryptography has been extensively studied, with early foundational work in [15] covering BB84 [59], E91, continuous-variable schemes, and the underlying physics of quantum channels. Subsequent developments in [16] expand this scope to include discrete-variable and continuous-variable QKD, device-independent and measurement-device-independent QKD, as well as emerging quantum network architectures. From a networking standpoint, it also focuses on key management, trusted relay architectures, and integration with classical network infrastructure, highlighting aspects most relevant to protocol design. Beyond QKD, Ref. [8] explores a broader range of quantum cryptographic primitives, including quantum oblivious transfer, quantum coin flipping, and quantum secure computation, reflecting the diversity of the quantum cryptographic toolkit. Practical advancements further demonstrate feasibility at scale, with satellite-based QKD enabling global communication capabilities [60] and long-distance fibre-based implementations achieving record performance [17]. The progression toward a fully realized quantum internet is outlined in [61], describing a layered roadmap from current QKD networks to future quantum internetworks. Additionally, challenges in quantum network control are addressed through entanglement routing strategies in [62], providing algorithmic foundations for efficient quantum communication. Recent QKD surveys extend early protocol-centric views by examining network-level key management, trust models, and performance trade-offs. Comprehensive reviews categorize QKD network architectures, testbeds, and standards, while highlighting that key management is often a bottleneck and still underspecified compared to link-layer QKD implementations [11,15,16]. Follow-on work explores partially trusted and untrusted relays, proposing trust taxonomies and key routing algorithms that relax full trust assumptions [63] and improve key distribution success rates [64], often with collaborative or threshold-based strategies [11,12,15]. SDN-inspired control for QKD networks has also emerged, introducing virtualized KMS entities and centralized controllers for relay path computation, but these mechanisms are not yet co-optimized with AI-based traffic engineering or slice-level orchestration [16]. Satellite and long-distance fibre demonstrations continue to push physical layer reach, but their integration with programmable and AI-driven network stacks remains largely unexplored [11,15].

2.3 Programmable and Intelligent Networking

The evolution of programmable and intelligent networking has been shaped by several foundational developments across SDN, NFV, and autonomic systems. Ref. [26] introduced OpenFlow and the SDN paradigm, establishing the architectural foundation for programmatic network control. The evolution of programmable networking concepts is further contextualized in [65], situating SDN within a broader trajectory of network programmability research. Network function virtualization is comprehensively addressed in [27], covering architecture, management, orchestration, and associated research challenges. Data plane programmability is enabled through the introduction of P4 in [66], a domain-specific language designed for protocol-independent packet processing that complements SDN control plane flexibility. The concept of autonomic computing in [67] establishes the foundation for self-managing systems, encompassing self-configuration, self-optimization, self-healing, and self-protection, which continues to influence zero-touch network management research. This paradigm is further extended to edge environments in [6], where cognitive IoT integrates perception, learning, and adaptation within resource-constrained device networks. Beyond classic SDN/NFV surveys, newer work emphasizes policy-based orchestration, service function chaining, and Service Level Agreement (SLA) aware flow placement. NFV-aware orchestration frameworks use optimization and heuristics to place VNFs and service chains while minimizing latency and maximizing reliability, often leveraging central SDN control for traffic steering [56,68]. Studies on flow management in SDN-based NFV environments detail the single- and multi-flow orchestration algorithms, showing how

joint control of routing and VNF placement can meet QoS constraints and enable Network-as-a-Service abstractions [6,56,68]. Special issues and overviews highlight SDN/NFV's role in 5G, MEC, and security, including reinforcement-learning-based edge offloading and secure SDN control planes; yet, they rarely consider PQC overheads or QKD-based key provisioning as first-class design constraints. This underscores a missing link between programmable data/control planes, AI-driven management, and quantum-safe security primitives at scale.

2.4 Protocol-Centric Studies

Protocol-focused work on PQC and AI typically treats security and intelligence as separate concerns. A growing body of work explores adaptations of network protocols in response to emerging security and intelligence requirements. A study [53] investigates the integration of post-quantum key encapsulation mechanisms into TLS 1.3, while [13] evaluates the performance overhead of PQC in QUIC. On the AI-driven side, RL techniques for traffic engineering are proposed in [69], knowledge-defined networking paradigms are introduced in [70], and intent-based networking using natural language processing is explored in [25]. Despite these advancements, the joint consideration of AI-driven intelligence and quantum-resilient security as a unified co-design problem remains largely unaddressed, forming the central focus of this survey. On the PQC side, multiple studies embed NIST PQC candidates into TLS 1.3 and SSH, measuring realistic handshake latency, throughput, and certificate-chain behaviour, and proposing multi-algorithm chains, hybrid KEMs, and window-size tuning to keep overhead acceptable even in constrained environments [7,8,24]. Other contributions design hybrid TLS frameworks that integrate code-based schemes and QRNGs, and evaluate deployment across heterogeneous testbeds, showing that careful design can preserve near-classical performance while improving cryptanalytic robustness. A study by Zafar and Iqbal demonstrates that a dual-handshake hybrid TLS combining classical and code-based McEliece/BIKE cryptography achieves approximately 30% lower latency and reduced resource overhead compared to pure post-quantum TLS, maintaining near-classical efficiency levels [52]. Another study by Sosnowski et al. benchmarks NIST PQC algorithms in TLS 1.3 and explicitly reports no performance drawback from using hybrid algorithms, concluding they are suitable for adoption in today's systems [71], whereas Sikeridis et al. integrate post-quantum signature schemes into TLS 1.3 and show that Dilithium- and Falcon-based hybrid configurations incur only approximately 6%–8% median handshake overhead relative to classical RSA/ECDSA, keeping latency compatible with real-world web use [72]. Giron et al. extend KEMTLS with hybrid post-quantum and elliptic-curve KEMs and find the performance penalty of the hybrid configuration over PQ-only KEMTLS to be negligible [73]; and Döring and Geitz confirm empirically that carefully selected PQ or hybrid TLS configurations can match or even surpass classical cryptography performance envelopes [74]. On the AI side, protocol-level DRL is applied to traffic engineering, routing, and congestion control in SDN and knowledge-defined networking, often with multi-agent or graph-based architectures that exploit fine-grained telemetry [2,3,50]. However, none of these protocol-centric efforts co-design the learning objectives, state representations, and reward functions with PQC/QKD-induced changes in handshake frequency, key-rotation cost, or key-pool dynamics, leaving open how to build AI-optimized yet quantum-resilient protocol stacks.

3 Evolution of Network Protocols

The architecture of modern communication networks has evolved through several distinct generations, each defined by increasing complexity, heterogeneity, and scale. The original Internet architecture, formalized in the TCP/IP reference model [75] and elaborated model [2], emphasized simplicity, interoperability, and end-to-end transparency. The DARPA specifications [76] established the foundational datagram model

that persists in IPv4/IPv6. Network protocols were designed with the implicit assumption that the underlying infrastructure was relatively stable and that security could be layered atop existing transport and application mechanisms [77,78]. The transition to 4G/5G cellular networks introduced concepts such as network slicing [33], virtual network functions, and service-based architectures (SBA) that began to challenge traditional protocol assumptions. The anticipated deployment of 6G systems targeting data rates on the order of terabits per second, sub-millisecond latency, and native AI integration at the air interface and network core represents a qualitative departure from prior generations. Blockchain-based trust mechanisms and cognitive IoT frameworks [6] are being explored as complementary architectural components in heterogeneous 6G environments. The Fig. 2 shows the transition from classical network architectures to future intelligent and quantum-resilient systems under the influence of disruptive technologies. It highlights how advances in QC and AI are reshaping foundational assumptions of network protocol design.

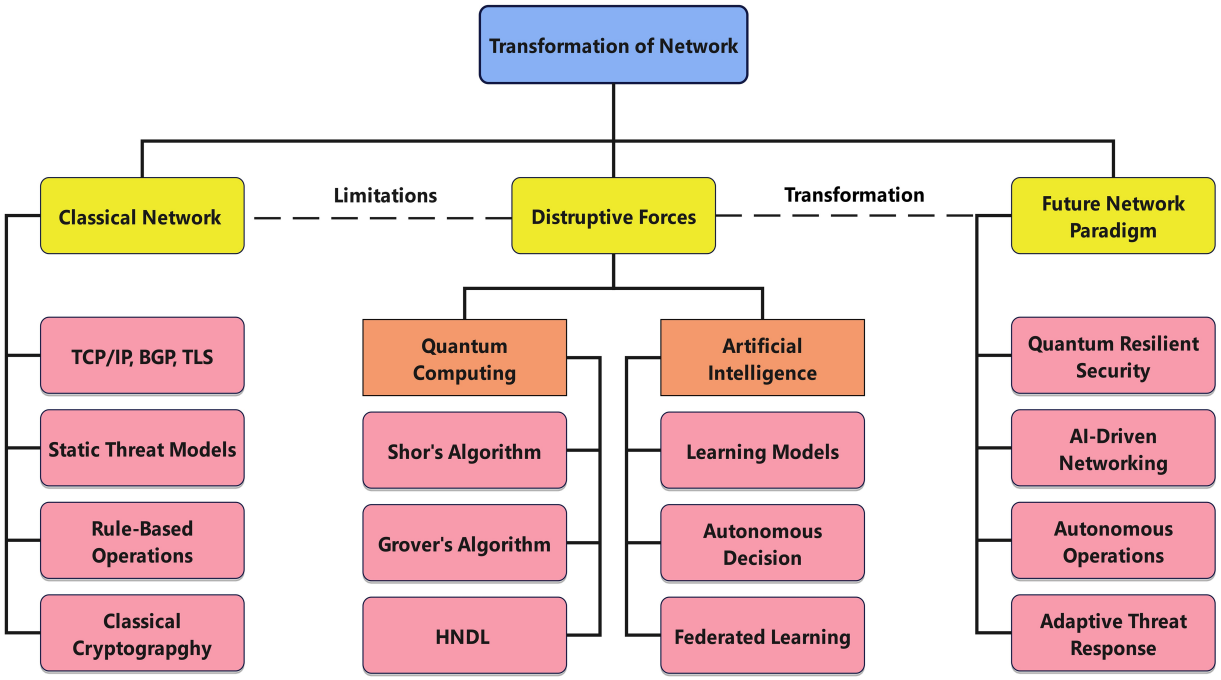

Figure 2: Network evolution under AI and quantum disruption.

3.1 Classical Protocol Architectures

The design of classical network protocols has been governed by principles of modularity, interoperability, and scalability encapsulated in the TCP/IP and OSI reference models. The layered abstraction separates concerns across the physical, data link, network, transport, and application layers, enabling independent evolution and broad interoperability across heterogeneous implementations [76]. This architecture proved extraordinarily successful, scaling from a four-node experimental network in 1969 to a global infrastructure supporting billions of simultaneous connections. However, inherent limitations have become increasingly apparent. Protocol behaviour is fundamentally reactive and rule-based: congestion control algorithms respond to observed losses and delays but cannot anticipate future conditions [79]. Routing protocols such as BGP converge over timescales of minutes, ill-suited to millisecond-scale modern traffic engineering [80]. Security mechanisms are tightly coupled to specific cryptographic primitives requiring complex, slow-moving standards updates. Cross-layer optimization is structurally impeded by strict encapsulation.

3.2 Software-Defined and Programmable Networks

SDN represented the first fundamental architectural departure from classical protocol design, decoupling the control plane from the data plane and introducing centralized programmability [26]. The OpenFlow protocol defined a standardized interface enabling policy-driven forwarding rule installation without hardware-specific programming [65]. Network Function Virtualization (NFV) complemented SDN by moving network functions from specialized hardware to software instances on commodity servers [27]. P4 extended data plane programmability further, allowing custom packet parsing pipelines [66]. These developments collectively established the architectural groundwork for AI integration.

3.3 Intent-Based and Autonomous Networking

The vision of autonomous networking self-configuring, self-optimizing, and self-healing systems is realized through intent-based networking (IBN), where operators specify high-level goals and the network automatically translates, implements, and monitors them [81]. AI is the enabling technology, learning to translate abstract intents into concrete configurations, predict network state evolution, detect anomalies, and optimize resources across multiple time scales [82]. Table 2 summarizes the evolution of network protocol paradigms.

Table 2: Evolution of network protocol paradigms.

Era	Paradigm	Key Technologies	Control Model	Security Model
1970s–1990s	Classical	TCP/IP, BGP, DNS, TLS	Distributed, static rules	Perimeter-based, add-on
2000s–2010s	Programmable	SDN, NFV, OpenFlow, P4	Centralized controller	Policy-driven, classical PKI
2015–2022	Intelligent	RL, DRL, IBN, FL	Adaptive, data-driven	ML-assisted, classical cryptography
2022–2026	Quantum-AI	PQC, QKD, hybrid approaches, autonomous AI	Autonomous, intent-driven	Post-quantum, AI-managed
Projected Future (Beyond 2026)	Quantum-Native (Emerging)	Quantum Internet, entanglement routing, distributed quantum networking	Highly autonomous, quantum-aware orchestration	QKD-enabled and information-theoretic security mechanisms

3.4 Protocol Security: A Historical Perspective

The security architecture of classical network protocols evolved reactively, with security mechanisms typically added after initial deployment. IP itself provides no inherent security; IPsec was introduced as a retrofitted extension [77]. TLS adoption across the web required over twenty years to achieve near-universal coverage [78]. This reactive posture means the cryptographic primitives embedded in deployed protocols represent technical debt: the transition to PQC requires renegotiating handshake protocols, certificate formats, PKI hierarchies, and hardware acceleration support across an immense installed base. The Fig. 3 illustrates the reactive evolution of protocol security, where mechanisms such as IPsec and

TLS were incrementally layered over initially insecure designs. It highlights how accumulated cryptographic dependencies create significant technical debt, complicating the transition to post-quantum secure communication systems.

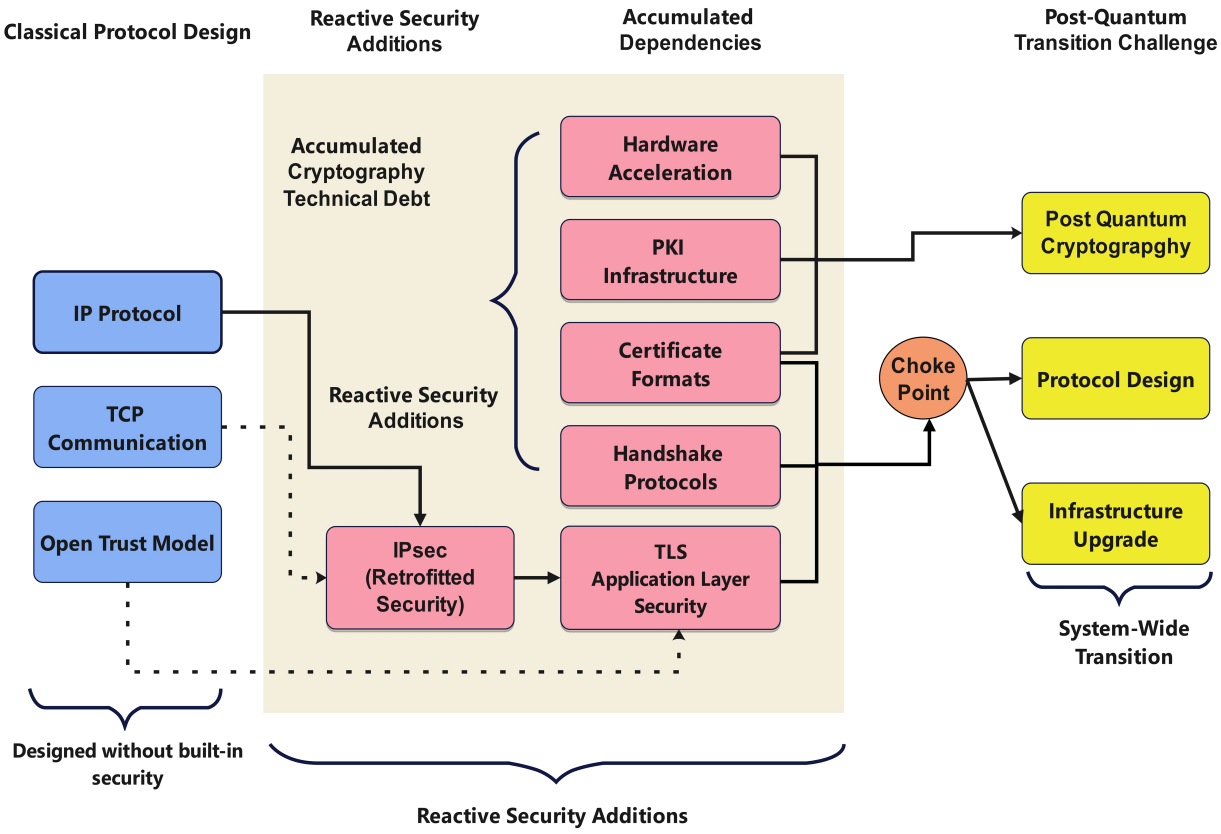

Figure 3: Reactive security evolution with technical debt accumulation.

4 Quantum Threats and QRC Approaches

Quantum threats are emerging risks from QC, that can compromise widely used cryptographic schemes, breaking RSA and ECC via Shor's algorithm, and weakening symmetric encryption through Grover's algorithm. QRC approaches address these challenges by employing PQC, QKD, and hybrid security mechanisms to ensure long-term secure communication against quantum-capable adversaries [83].

4.1 The Quantum Adversary Model

Quantum-capable adversaries fundamentally alter the cryptographic threat model. Shor's algorithm, executable in polynomial time on a fault-tolerant quantum processor, can efficiently solve both the integer factorization problem underlying RSA and the discrete logarithm problem underlying elliptic-curve cryptography [3]. A fault-tolerant processor with approximately 4000 logical qubits would suffice to break RSA-2048 and 256-bit ECC [84], thereby compromising all deployed asymmetric cryptographic systems, including TLS key exchange and key encapsulation, certificate-based digital signatures, VPN authentication, and routing protocol security. Critically, the impact of Shor's algorithm must be understood in a use-case-specific manner: RSA and ECDH employed for key exchange and key encapsulation require replacement by a Key Encapsulation Mechanism (KEM) such as ML-KEM (FIPS 203), while RSA and ECDSA employed for

digital signatures require replacement by a signature scheme such as ML-DSA (FIPS 204) or the forthcoming FN-DSA; a single post-quantum algorithm cannot serve both roles interchangeably.

Grover's algorithm provides a quadratic quantum speedup for unstructured search and reduces the effective security of symmetric encryption by half [85]: AES-128 drops to 64-bit effective post-quantum security, which is considered insufficient, while AES-256 retains 128-bit effective security and requires no replacement. For hash functions, it is important to distinguish between two distinct quantum threats. Grover's algorithm applies to preimage search, halving preimage resistance. For example, reducing SHA-256 preimage security from 2^{256} to 2^{128} quantum queries. Collision resistance, however, is governed by a separate and more powerful quantum attack: the Brassard–Høyer–Tapp (BHT) algorithm achieves collision search in $O(2^{n/3})$ quantum queries with quantum random access memory (QRAM), reducing SHA-256 collision resistance to approximately 2^{85}, which meaningfully weakens collision security below the classical birthday bound of 2^{128} and motivates upgrading to SHA-384 or SHA-512 for collision-sensitive applications. HNDL attacks represent an immediate and present threat even before large-scale fault-tolerant quantum computers are realized [56]: adversaries are actively harvesting encrypted network traffic today with the intent of decrypting it retroactively once sufficient quantum capability becomes available, making the transition to PQC an urgent operational priority rather than a deferred concern. Table 3 provides a comprehensive summary of the quantum vulnerability of classical cryptographic algorithms, organized by cryptographic function across key exchange, digital signatures, symmetric encryption, and hash functions, together with their recommended post-quantum replacements and effective post-quantum security levels.

Table 3: Classical cryptographic algorithms: quantum vulnerability and post-quantum replacements.

Algorithm	Use Case	Classical Security	Quantum Attack	Effective Post-Quantum Security	PQC Replacement
RSA-2048	Key Encapsulation	112-bit	Shor (polynomial time)	Broken	ML-KEM-768
RSA-4096	Key Encapsulation	140-bit	Shor (polynomial time)	Broken	ML-KEM-1024
ECDH P-256	Key Exchange	128-bit	Shor (polynomial time)	Broken	ML-KEM-768
ECDH P-384	Key Exchange	192-bit	Shor (polynomial time)	Broken	ML-KEM-1024
RSA-2048	Digital Signature	112-bit	Shor (polynomial time)	Broken	ML-DSA-65/FN-DSA-512
RSA-4096	Digital Signature	140-bit	Shor (polynomial time)	Broken	ML-DSA-87/FN-DSA-1024
ECDSA P-256	Digital Signature	128-bit	Shor (polynomial time)	Broken	ML-DSA-65/FN-DSA-512
ECDSA P-384	Digital Signature	192-bit	Shor (polynomial time)	Broken	ML-DSA-87
AES-128	Symmetric Encryption	128-bit	Grover (square-root speedup)	64-bit	AES-256
AES-256	Symmetric Encryption	256-bit	Grover (square-root speedup)	128-bit	AES-256 (retain)
SHA-256	Hash Function	256-bit (preimage)	Grover/BHT	128-bit preimage, 85-bit collision	SHA-384 or SHA-512

(Continued)

Table 3 (continued)

Algorithm	Use Case	Classical Security	Quantum Attack	Effective Post-Quantum Security	PQC Replacement
SHA-384	Hash Function	384-bit (preimage)	Grover	192-bit preimage, 128-bit collision	SHA-384 (retain)
SHA-3/SHAKE-256	Hash Function	256-bit (preimage)	Grover (limited impact)	128-bit	SHA-3/SHAKE-256 (retain)

4.2 PQC in Network Protocols

Unlike classical asymmetric schemes whose security rests on integer factorization and discrete logarithm problems and is efficiently broken by Shor's algorithm on a fault-tolerant quantum processor, PQC [86] builds on hardness assumptions believed to resist quantum attack, such as the Learning With Errors (LWE) problem in lattice-based constructions and collision resistance in hash-based schemes. Following a multi-year standardization process, NIST finalized three initial PQC standards in August 2024: CRYSTALS-Kyber (ML-KEM, FIPS 203) for key encapsulation; CRYSTALS-Dilithium (ML-DSA, FIPS 204) for digital signatures; and SPHINCS+ (SLH-DSA, FIPS 205) as a stateless hash-based signature scheme [50]. FALCON, designated FN-DSA and corresponding to the forthcoming FIPS 206, was not finalized in this round and is proceeding along a separate standardization path, with final publication still pending at the time of writing. Where a currently finalized signature standard is required, ML-DSA (FIPS 204) remains the recommended substitute pending the completion of FIPS 206. Integration into TLS 1.3 requires incorporating post-quantum key encapsulation mechanisms (KEMs) into the handshake while maintaining interoperability and backward compatibility with existing deployments. Hybrid key exchange approaches that combine classical ECDH with ML-KEM have been proposed as a practical migration strategy [53] and are actively being studied within the context of TLS standardization efforts [87]. Performance evaluations indicate that the integration of post-quantum KEMs can substantially increase handshake message sizes, in some cases by up to seven times compared with classical TLS handshakes, while post-quantum-only configurations may exhibit 22%–55% higher handshake latency than pure ECDHE deployments [88]. However, hybrid ECDHE+PQC configurations introduce only marginal additional delays (approximately 0.3–0.4 ms), with the relative overhead becoming less significant under typical Internet round-trip times [88]. Furthermore, experiments involving KpqC and ML-KEM-based hybrid TLS deployments reported larger latency increases in localhost environments, while the relative overhead decreased to approximately 30%–40% under local-area network conditions [89].

For routing security, BGPsec and RPKI rely on digital signatures for route origin validation. Post-quantum signatures with larger key and signature sizes require updates to BGP message formats and increased router memory [54]. DNSSEC faces analogous challenges, with post-quantum signatures potentially exceeding UDP packet size limits, thereby increasing fragmentation and deployment complexity in DNSSEC environments [90]. IPsec and IKEv2 require algorithm suite updates, with performance bottlenecks in hardware security modules not yet accelerated for lattice operations [91]. The Fig. 4 illustrates the integration of post-quantum cryptographic mechanisms across multiple network protocol layers, including TLS, DNSSEC, BGPsec, and IPsec. It highlights the associated performance and scalability trade-offs, emphasizing the challenges of achieving quantum resilience while maintaining backward compatibility.

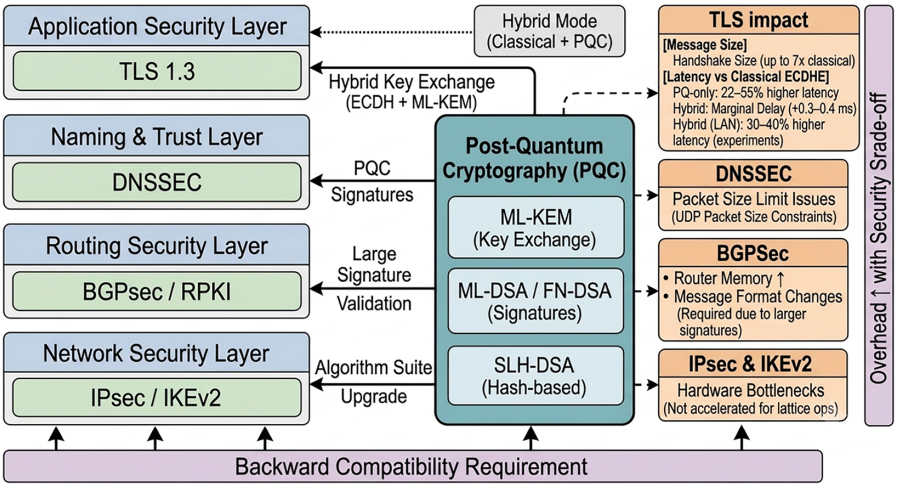

Figure 4: PQC integration across network protocol stack with performance impact overlay.

4.3 Quantum Key Distribution

QKD provides quantum-resilient key establishment based on the physical properties of quantum mechanics rather than computational hardness. Beginning with BB84, QKD protocols enable two parties to establish a shared secret whose security is guaranteed by physics: any eavesdropping attempt unavoidably introduces detectable disturbances. Contemporary implementations achieve key distribution rates of several megabits per second over metropolitan distances up to 100 km [17]; satellite-based QKD extends reach to intercontinental scales [60]. However, QKD faces substantial integration challenges for packet-switched networks. The quantum channel is fundamentally point-to-point; multi-hop key distribution requires trusted relay nodes, representing security vulnerabilities. Key generation rates are limited by photon detection efficiencies. Cost and infrastructure requirements currently limit deployment to high-value applications. Integrating QKD-generated key material with network cryptographic architectures requires standardized interfaces not yet fully developed [18].

4.4 Hybrid Quantum-Resilient Communication

Hybrid approaches combining PQC, classical cryptography, and selective QKD deployment are increasingly recognized as the most practical path forward [14]. A hybrid framework may combine classical ECDH for backwards compatibility, ML-KEM for computational quantum resistance, and QKD for information-theoretic security in high-assurance segments. The resulting composite key inherits the security of the strongest component. Hybrid approaches also provide cryptographic agility—the ability to substitute cryptographic components as the threat model evolves or as new vulnerabilities are discovered [51]. A comparison of PQC and QKD approaches is given in Table 4.

Table 4: Comparison of PQC and QKD approaches.

Criterion	PQC	QKD
Security Basis	Computational hardness (quantum-safe) [11,51]	Physical laws of quantum mechanics [15,59]
Infrastructure	Software-only, existing Internet [13,28]	Dedicated quantum channels [17,18]

(Continued)

Table 4 (continued)

Criterion	PQC	QKD
Key Rate	On-demand (asymmetric) [14]	Rate-limited: kbps–Mbps [17,60]
Distance	Unlimited (Internet-scale) [53]	~100–421 km per hop [17,60]
Standardization	NIST finalized: ML-KEM, ML-DSA, SLH-DSA [12,50]	ETSI, ITU-T, ISO/IEC in progress [18]
Deployment Maturity	High (software integration) [13,14]	Low–medium (hardware intensive) [60,61]
Cost	Low (software updates) [28]	High (dedicated hardware) [18]
Adversarial Risk	Algorithm-level (cryptanalysis) [11]	Side-channel, photon-number-splitting (PNS) attacks [16]
AI Integration	PQC-TLS overhead prediction [13,54]	AI-driven entanglement routing [62]

5 AI for Network Protocols

AI is being used in network protocols to make networks smarter and more adaptive. It helps improve tasks like routing, traffic control, and resource use, making networks more efficient and reliable [92].

5.1 AI Paradigms in Networking

The application of AI to network protocols spans several ML paradigms. Supervised learning is well-suited to classification tasks such as traffic type identification, anomaly detection, and intrusion classification. Unsupervised learning enables clustering-based traffic analysis and novel attack pattern detection [93]. RL is particularly well-matched to sequential decision-making inherent in network protocols: routing decisions, congestion window adjustments, and cryptographic algorithm selection. DRL combines RL with deep neural network function approximators for traffic engineering, adaptive bitrate selection, and network slice management. FL enables distributed model training without centralizing sensitive data. Graph neural networks naturally represent network topologies for routing and anomaly propagation modelling [19]. Table 5 summarizes key AI techniques and their principal application domains within network protocol intelligence.

Table 5: AI techniques and their application domains in network protocol intelligence.

AI Technique	Paradigm	Protocol Application	Strengths	Limitations
Deep Neural Networks	Supervised	Traffic classification, Intrusion Detection System (IDS), flow prediction	High accuracy, scalable	Requires labeled data, black-box nature
Deep RL (DQN, PPO)	Reinforcement	Congestion control, routing, resource management	No labeled data required	Slow convergence, instability
FL	Distributed	Distributed protocol models, PQC-FL	Privacy-preserving	Vulnerable to poisoning attacks
LSTM/Transformer	Supervised/Self-supervised	Traffic forecasting, intent translation	Strong temporal modeling	High computational cost, large models

(Continued)

Table 5 (continued)

AI Technique	Paradigm	Protocol Application	Strengths	Limitations
Autoencoders/VAE	Unsupervised	Anomaly detection, protocol debugging	No labels required	Higher false positive rate
Graph Neural Networks	Supervised	Routing, topology inference, attack propagation	Graph-native modeling	Scalability challenges in large networks
Bayesian Networks	Probabilistic	Uncertainty-aware security decisions	Interpretable	Limited scalability
Generative Adversarial Networks	Generative	Adversarial traffic simulation, data augmentation	Diverse data generation	Training instability

5.2 AI-Driven Congestion Control and Routing

AI-driven approaches learn optimal control policies from observed network dynamics. Learning-based congestion control represents a compelling application of AI to transport-layer protocol design. Orca [94] trains a deep RL agent to control TCP congestion windows, outperforming BBR on heterogeneous networks. PCC Vivace [95] employs online convex optimization. Aurora [96] demonstrates RL-based congestion control generalizing across diverse network conditions. For routing, DQRN applies deep Q-networks to adaptive routing in SDN, achieving near-optimal paths in dynamic topologies. A critical limitation is sensitivity to distribution shift: agents trained in one environment may perform poorly elsewhere. This is particularly concerning for post-quantum networks, where PQC computational overhead alters timing profiles in ways that may invalidate assumptions embedded in learned policies. Transfer learning strategies are required to address this challenge [97].

5.3 AI for Security and Cryptographic Agility

AI techniques are increasingly applied to network security functions directly relevant to quantum-resilient protocol design. Anomaly detection using autoencoders or isolation forests can identify suspicious network-level behavioural signatures potentially indicative of quantum-facilitated threats, including anomalous TLS handshake completion rates, unexpected cipher suite negotiation patterns inconsistent with legitimate client populations, statistically irregular key exchange parameter distributions, and atypical certificate validation sequences that may signal active protocol downgrade attempts or HNDL interception activity [98]. IDS leveraging RNNs or CNNs can detect patterns in packet traces betraying exploitation of cryptographic weaknesses [99]. Of particular relevance is AI application to cryptographic agility, dynamic selection and adaptation of cryptographic algorithms based on threat intelligence, performance conditions, and security posture [100]. An AI agent trained to balance security level, computational overhead, and communication latency can autonomously select appropriate combinations of classical and post-quantum primitives for each connection context. However, adversarial ML attacks can manipulate AI security classifiers, inducing undesirable algorithm selections [101]. Model poisoning in FL can subvert distributed AI models, potentially compromising cryptographic agility logic across network segments [102].

5.4 Traffic Prediction and Anomaly Detection

Accurate traffic prediction enables proactive resource management and pre-positioned security responses. LSTM and transformer architectures achieve superior forecasting over classical ARIMA methods. GNN-based spatio-temporal models capture both temporal dynamics and spatial network correlations [19].

For anomaly detection, Ref. [98] provide the foundational taxonomy. Goldstein and Uchida [93] offer comparative evaluation of unsupervised algorithms. Buczak and Guven [99] surveyed ML methods for cybersecurity intrusion detection, establishing the state of the art. Adversarial robustness of AI detectors [101,102] is a critical concern: adversarial examples [101] can evade neural IDS systems, necessitating certified defences [102] and formal verification.

5.5 Federated and Privacy-Preserving Intelligence

FL enables network nodes to collaboratively train shared models without exchanging raw traffic data. Integration of FL with QRC requires post-quantum secure aggregation protocols to prevent quantum adversaries from reconstructing local model updates or manipulating aggregated models [20]. As illustrated in Fig. 5, distributed edge devices collaboratively train a shared model under a federated architecture in which a central server aggregates local updates without accessing raw data, while PQC-secured aggregation is applied at the server to protect against quantum-capable adversaries intercepting or tampering with the aggregation channel.

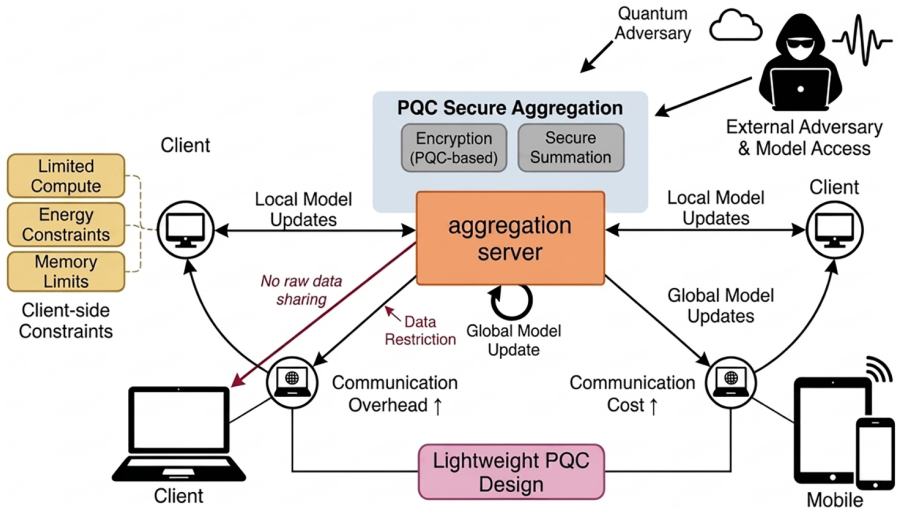

Figure 5: FL with PQC-secured aggregation under resource constraints.

However, introducing PQC-secured aggregation leads to concrete and quantifiable costs across multiple dimensions that remain insufficiently explored in the literature. Communication overhead increases because ML-KEM public keys (1184 bytes for ML-KEM-768) and ciphertexts (1088 bytes) are significantly larger than classical ECDH parameters (32–65 bytes for P-256), which increases per-round bandwidth consumption for each participating edge device; in high-frequency federated training over bandwidth-constrained wireless links, this overhead accumulates across both rounds and participants. This also affects model convergence, as higher per-round communication latency reduces the number of aggregation rounds that can be completed within a fixed training window, potentially slowing convergence, particularly under Non-Independent and Identically Distributed (non-IID) data distributions where more rounds are typically required to reach comparable model performance. Energy consumption at edge devices also increases due to the lattice-based arithmetic used in ML-KEM and ML-DSA, which requires higher CPU cycle counts per aggregation step compared to classical ECDH and ECDSA, thereby increasing per-round energy usage in battery-constrained IoT and edge environments; this motivates ongoing research into lightweight PQC variants, including optimized lattice constructions and hardware-accelerated polynomial arithmetic suitable for FL workloads.

Finally, aggregation latency increases due to the combined effect of larger PQC payloads and additional server-side cryptographic computation, which raises end-to-end round-trip time per federated round and may degrade performance in time-sensitive network control applications such as DRL-based congestion control or intent-based routing when latency exceeds control-plane reaction budgets.

Many studies introduced federated averaging (FedAvg) as the foundational FL algorithm enabling distributed model training without raw data sharing. Ref. [10] surveyed FL challenges including non-IID data, communication efficiency, and Byzantine robustness. Ref. [9] addressed the joint optimization of communication and learning in wireless federated settings. Ref. [20] proposed practical secure aggregation for privacy-preserving federated ML. Differential privacy [21] provides formal privacy guarantees by injecting calibrated noise into model updates. Network compression techniques [103] reduce communication cost in federated model distribution. Neuromorphic computing [104] offers an energy-efficient inference substrate for edge-deployed network AI models.

5.6 Autonomous Network Management and Intent-Based Networking

The vision of autonomous networks [67] is operationalized through intent-based networking frameworks [25,81] that translate high-level operator intent into protocol configurations. Ref. [81] formalized IBN concepts and definitions in IETF, RFC 9315. Cognitive IoT [6] extends autonomous management to the edge. Large language models and QML [22] are beginning to emerge as tools for intent translation and configuration generation.

6 AI–Quantum Integration in SDN/NFV

The SDN/NFV paradigm was architected around the assumption of lightweight, low-latency control-plane operations, where OpenFlow rule installations, NFV service chain reconfigurations, and controller-to-switch communications are all optimized for classical cryptographic overhead. The introduction of PQC and QKD into these environments disrupts this assumption at multiple layers simultaneously. ML-KEM key encapsulation produces ciphertexts of 1088 bytes compared to 32 bytes for ECDH P-256, directly inflating OpenFlow secure channel handshakes; ML-DSA signatures at 3309 bytes impose authentication overhead on every controller-to-switch TLS session re-establishment; and QKD-constrained key pools introduce hard limits on re-keying frequency that conflict with the rapid session turnover characteristic of high-throughput SDN deployments. NFV service function chains compound this further, as each inter-VNF hop may require independent PQC-authenticated sessions, multiplying cryptographic overhead across the chain length. Addressing these tensions requires more than algorithm substitution: it demands co-design of AI-driven control logic including DRL-based controllers, intent-based networking engines, and federated orchestration frameworks, with explicit awareness of PQC handshake costs, QKD key consumption rates, and the resulting state-space and reward-function implications for learned control policies. This section examines how such integration can be realized across the SDN control plane, the NFV management and orchestration layer, and the network security enforcement fabric. By embedding intelligence into control and orchestration layers, networks can autonomously optimize performance, detect anomalies, and enforce security policies in real time. Moreover, the modular nature of SDN/NFV enables seamless upgrades from classical to post-quantum cryptographic primitives without requiring complete infrastructure overhauls. Such architectures also support cross-layer optimization, where AI models consider both networking performance metrics and cryptographic overhead. As QC advances, these integrated designs ensure long-term confidentiality, integrity, and availability of communication systems. Ultimately, architectural co-design is not just beneficial but essential for achieving scalable and secure future Internet infrastructures.

6.1 SDN as Platform

The architectural properties of Software-Defined Networking make it a uniquely capable platform for deploying AI-driven, quantum-resilient protocol stacks at operational scale. By physically separating the control plane from the data plane and exposing network state through programmable northbound APIs, SDN concentrates the decision-making surface into a controller that can be instrumented with AI inference engines, cryptographic policy managers, and real-time threat intelligence feeds, capabilities that are architecturally infeasible in distributed, device-by-device classical network management. OpenFlow [26] and the SDN paradigm [65] realize this separation through a standardized southbound protocol that allows the controller to install, modify, and revoke forwarding rules across heterogeneous switching hardware without per-device configuration, giving AI-driven control logic a uniform enforcement fabric across the entire network domain. Knowledge-defined networking [70] extends this architecture further by adding a knowledge plane above the control plane, enabling continuous learning-driven protocol adaptation in which observed network behaviour feeds back into updated control policies without human intervention. P4 [66] pushes programmability deeper still, into the data plane itself, enabling per-packet ML inference within forwarding hardware and allowing cryptographic header inspection, anomaly scoring, and algorithm negotiation to occur at line rate without controller round-trips. From a quantum-security perspective, the SDN control channel, which is the communication path between controller and data-plane devices over HTTPS, NETCONF, and RESTCONF, represents a high-value interception target whose compromise would give a quantum-capable adversary complete visibility into and control over network-wide forwarding policy; securing these channels with PQC-TLS [13,28,54] is therefore not an optional hardening measure but a foundational requirement for any quantum-resilient SDN deployment.

Beyond these capabilities, the SDN controller architecture provides a uniquely advantageous platform for managing the operational complexities introduced by quantum-resilient protocol deployment, complexities that distributed per-device cryptographic management cannot address with comparable efficiency or consistency. PQC-TLS session management is one such capability. An SDN controller maintaining a real-time, network-wide registry of TLS negotiation outcomes can enforce quantum-safe cipher-suite policies at scale without requiring per-device reconfiguration. Recent work has demonstrated the feasibility of integrating classical cryptography, PQC, and QKD-derived keys into TLS 1.3 within SDN environments while preserving crypto-agility and backward compatibility [105]. Such centralized visibility enables the controller to monitor negotiated cryptographic parameters, identify non-compliant or downgraded sessions, and enforce policy decisions through dynamic OpenFlow rule updates. QKD key availability management represents another critical function. Unlike conventional cryptographic systems, QKD generates secret keys at rates constrained by photon transmission characteristics and channel loss. Consequently, QKD keys constitute a scarce network resource that must be allocated efficiently. SDN-enabled QKD architectures address this challenge through centralized controllers that maintain global knowledge of network state, key availability, and device status, enabling coordinated routing and key management decisions [106]. Similarly, QKD-as-a-Service frameworks maintain real-time information regarding secret-key generation rates and available key resources [107], allowing centralized allocation of keys in response to application demands [58]. The controller can therefore continuously monitor key pool occupancy, schedule session establishments according to available key resources, pre-distribute keys to edge devices during anticipated demand spikes, and trigger hybrid PQC fallback mechanisms when QKD key pools become depleted. This transforms QKD key management from a local reactive process into a globally optimized resource-allocation problem [58]. Cryptographic policy enforcement can likewise be centralized through the SDN control plane. Intent-based cryptographic policies specifying minimum security levels, approved PQC algorithms, hybrid classical/PQC requirements, and per-slice quantum-safe configurations can be defined at the controller level

and enforced consistently across the network. Experimental studies in 5G network slicing have demonstrated SDN orchestrators selecting different security mechanisms [108], including classical cryptography, QKD-protected communication, and quantum-resistant algorithms, according to slice-specific requirements [109]. More recently, intent-based networking architectures integrating PQC and machine-learning-driven threat detection have shown how high-level security intents can be translated automatically into network-wide cryptographic configurations [110]. These capabilities allow security-sensitive slices, such as critical infrastructure or financial services, to operate under stricter quantum-safe policies while less sensitive traffic employs hybrid or PQC-only protection mechanisms. Security fallback orchestration further strengthens network resilience. When the controller detects PQC negotiation failures, QKD link outages, key-pool exhaustion, or anomalous cryptographic behaviour indicative of downgrade attacks, it can automatically initiate predefined recovery procedures. These actions may include switching affected flows to approved hybrid cryptographic modes, reallocating QKD resources, rerouting traffic through alternative quantum-safe paths, or isolating suspicious flows for further inspection. Practical deployments have demonstrated SDN orchestration across multiple controllers and heterogeneous key-management systems to coordinate QKD key delivery across vendor-diverse environments, highlighting the feasibility of centralized quantum-safe resource management at scale [111]. Collectively, these capabilities establish the SDN controller as a critical coordination layer for integrating PQC, QKD, and AI-driven security management into future quantum-resilient network infrastructures.

6.2 NFV and Service Chaining

Network Function Virtualization (NFV) is a technology that virtualizes network services traditionally run on proprietary hardware, allowing them to operate as software-based functions on general-purpose infrastructure. NFV [27] decouples network functions from dedicated hardware, enabling on-demand VNF/CNF instantiation orchestrated by AI-driven management systems [7,24]. DRL-based VNF placement [96] determines optimal VNF locations and resource allocations. Homomorphic encryption [100] enables computation on encrypted VNF state without decryption, supporting privacy-preserving VNF migration. Virtualized security functions (VPN gateways, IDS VNFs) relying on classical cryptography must be migrated to PQC-enabled implementations [27,28]; the software-defined nature of NFV facilitates this through VNF image upgrades.

In addition, NFV enhances scalability and flexibility by allowing rapid provisioning and scaling of network services based on demand. AI-driven orchestration can predict workload patterns and proactively allocate resources, reducing latency and improving quality of service. Service Function Chaining (SFC) further enables the dynamic composition of multiple VNFs, forming customized security and routing pipelines tailored to application requirements. This is particularly important for integrating quantum-safe cryptographic modules into existing service chains without disrupting operations [112]. NFV also supports multi-tenant environments, where different tenants can adopt varying levels of quantum security based on their needs. Moreover, virtualization enables efficient testing and validation of new PQC algorithms before large-scale deployment. Overall, NFV acts as a key enabler for transitioning toward quantum-resilient and AI-driven network infrastructures.

6.3 Intent-Based Autonomous Networking

Intent-Based Networking (IBN) is an advanced networking approach where high-level user intents or policies are automatically translated into network configurations using AI-driven systems. Intent-based networking [25,81] enables operators to specify high-level policy objectives that AI systems translate into low-level protocol configurations. Kephart and Chess [67] established the foundational self-managing

system model. Explainable Artificial Intelligence (XAI) [113] is essential for making autonomous protocol decisions auditable in regulated environments. Model compression [103] enables deployment of AI protocol management agents on resource-constrained network elements. Neuromorphic computing [104] offers a neurologically inspired, energy-efficient substrate for always-on network intelligence at the edge.

Additionally, IBN significantly reduces the complexity of network management by abstracting low-level configurations into human-understandable intents. AI models continuously monitor network states and ensure that the implemented configurations align with the specified intents, even under dynamic conditions. This is particularly valuable in quantum-resilient networks, where security policies must adapt to emerging threats and cryptographic transitions. Autonomous management systems can detect inconsistencies between intent and actual behaviour, triggering corrective actions without human intervention. The integration of XAI enhances trust by providing transparency into decision-making processes, which is critical in security-sensitive environments. Additionally, edge-based intelligence enabled by neuromorphic computing reduces latency and improves responsiveness. These capabilities collectively pave the way for fully autonomous, self-healing, and quantum-secure networks. The Fig. 6 presents a simplified intent-based networking loop where high-level user intents are translated into protocol configurations by AI-driven controllers. Continuous monitoring and feedback enable autonomous adaptation, while explainable and lightweight AI ensures transparency and efficient deployment.

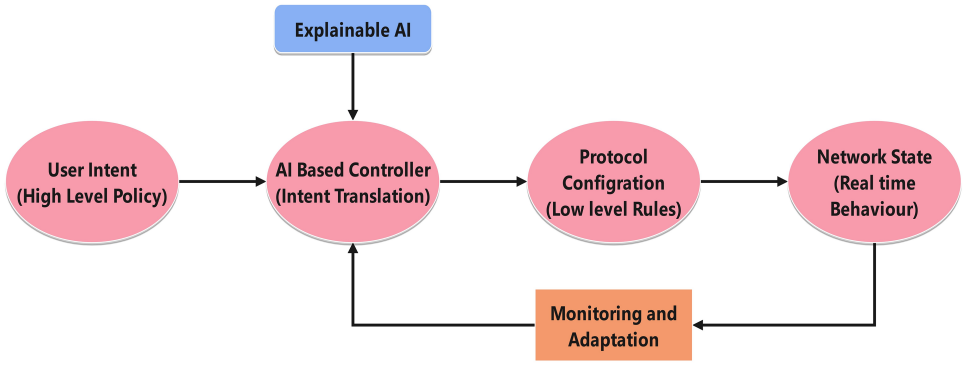

Figure 6: Intent-based autonomous networking control loop.

6.4 AI–Quantum Unified Network Architecture

A reference co-design architecture is a conceptual framework that integrates AI-driven intelligence and quantum-safe security mechanisms into a unified multi-layer network design. A proposed reference architecture for co-designed AI-quantum-safe network management incorporates four principal planes: (i) the AI-driven Network Intelligence Plane, hosting traffic analysis, DRL-based routing [69,96], anomaly detection [98,99], and intent translation [25,81] models; (ii) the Quantum-Safe Cryptographic Services Layer, providing PQC-based key management [12,28] and optional QKD key injection [18,62]; (iii) the SDN/NFV Orchestration Layer [26,27], enabling programmable control of data plane elements and security function instantiation; and (iv) the Network Telemetry and Observability Framework, providing standardized data feeds for AI model training, inference, and security auditing.

This co-design architecture ensures tight coupling between intelligence, control, and security, enabling holistic network optimization. The separation into distinct planes promotes modularity, allowing independent evolution of AI models and cryptographic mechanisms. Real-time telemetry feeds enable continuous learning and adaptation, improving both performance and threat detection capabilities. The integration of PQC and QKD ensures layered security, combining computational and information-theoretic protections.

Additionally, orchestration layers enable automated deployment and lifecycle management of network services, reducing operational complexity. Such architectures also support interoperability across heterogeneous environments, including IoT, edge, and satellite networks. Ultimately, this unified design paradigm provides a scalable and future-proof foundation for AI-enabled QRC architecture. The Fig. 7 presents a minimal co-design framework where AI intelligence, quantum-safe security, and network control interact as tightly coupled components. A central telemetry core enables continuous data-driven adaptation across all elements, supporting scalable and autonomous network operation.

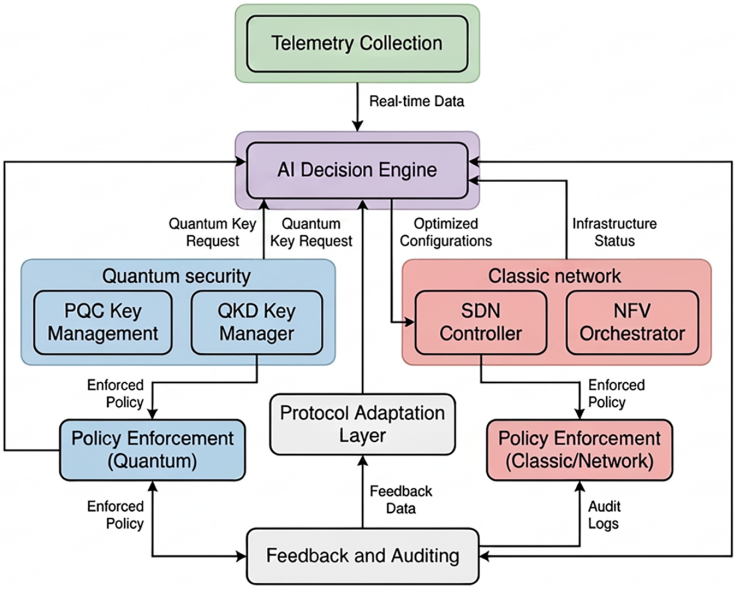

Figure 7: Co-design framework diagram.

7 Mathematical Foundations for AI-Driven and Quantum-Resilient Networking

This section reviews the mathematical models and analytical formulations that underpin AI-driven network optimization and quantum-resilient security mechanisms, as reported in the literature. These formulations provide a formal basis for understanding how intelligent decision-making and quantum-safe cryptographic techniques are modelled, analyzed, and evaluated within modern network protocols. Critically, each formulation is explicitly connected to the protocol design and evaluation challenges of AI-enabled quantum-resilient networking identified throughout this survey, including PQC handshake latency, QKD key availability constraints, cryptographic agility decisions, and privacy-preserving federated intelligence.

Within AI-enabled network control, the problem is commonly formulated as a Markov Decision Process (MDP) $M = (S, A, P, R, \gamma)$ [114]. Here, S represents the state space, A denotes the action space, $P(s'|s, a)$ is the transition probability, $R(s, a)$ is the reward function, and $\gamma \in (0, 1]$ is the discount factor. The objective is to learn an optimal policy that maximizes long-term expected reward:

$$\pi^* = \arg\max_{\pi} \mathbb{E}\left[\sum_{t=0}^{\infty} \gamma^t \cdot R(s_t, a_t) \mid \pi\right] \tag{1}$$

In the context of AI-enabled quantum-resilient protocol design, the state space S must be extended beyond classical network variables such as link utilization and queue lengths to incorporate PQC-specific protocol state: current handshake latency per flow (which increases by 20–50 ms under ML-KEM relative

to ECDH in measured deployments), residual QKD key pool occupancy per link, the active cryptographic algorithm suite per session, and the time since last key rotation. The reward function $R(s, a)$ must correspondingly penalize PQC handshake latency and key-rotation overhead while rewarding cryptographic compliance and QKD key pool sustainability, enabling the learned policy π^* to explicitly trade off routing cost, latency, and quantum-resilient security in a principled, quantifiable manner.

DRL methods such as Deep Q-Networks (DQN) approximate the action-value function $Q(s, a; \theta)$ using neural networks [115], trained via temporal-difference learning [116]:

$$L(\theta) = \mathbb{E}\left[\left(r + \gamma \cdot \max_{a'} Q(s', a'; \theta^-) - Q(s, a; \theta)\right)^2\right] \tag{2}$$

where θ^- denotes the parameters of a target network. For cryptographic agility applications, the action space A includes discrete algorithm selection decisions, such as switching from a hybrid classical/ML-KEM configuration to a QKD-secured session or falling back to a pre-approved classical cipher suite upon QKD key pool exhaustion, and the immediate reward r must reflect both the security gain of the selected configuration and the latency cost of the resulting handshake, directly linking the DQN training objective to the protocol-level trade-offs analyzed in Sections 4.2 and 6.1.

Complementing RL, federated learning has emerged as a distributed optimization paradigm for privacy-preserving network intelligence [68,117]. Multiple clients collaboratively minimize a global loss function:

$$w^* = \arg\min_w \sum_{k=1}^{N} \frac{n_k}{n} \cdot F_k(w) \tag{3}$$

where $F_k(w) = \dfrac{1}{n_k} \sum_{i \in D_k} \ell(x_i, y_i; w)$ and $n = \sum n_k$. The FedAvg algorithm performs iterative aggregation:

$$w_{t+1} = \sum_{k=1}^{N} \frac{n_k}{n} \cdot w_k^{(t+1)} \tag{4}$$

As discussed in Section 5.5, integrating PQC-secured aggregation into this framework inflates the effective per-round communication cost $F_k(w)$: ML-KEM-768 introduces 1088-byte ciphertexts per establishment of the aggregation channel compared to 32 bytes for ECDH P-256, which compounds between N clients and between training rounds, directly affecting convergence speed in bandwidth-constrained wireless federated settings. This formulation thus provides the quantitative basis for evaluating the communication-convergence trade-off introduced by the PQC-secured aggregation identified in Section 5.5.

To ensure privacy, differential privacy mechanisms introduce calibrated noise into local updates [118,119]:

$$w_k^{(t+1)} \leftarrow w_k^{(t+1)} + \mathcal{N}(0, \sigma^2 C^2 I) \tag{5}$$

In quantum-resilient federated deployments, the noise parameter σ must be jointly calibrated against both the privacy budget ε and the additional perturbation risk of model update introduced by quantum-capable adversaries capable of intercepting aggregation channels, motivating the PQC-secured aggregation protocols discussed in Section 5.5.

From a security standpoint, PQC schemes rely on computational hardness assumptions believed to resist quantum attacks [11]. The quantum attack cost against LWE-based schemes such as ML-KEM is approximated as [120]:

$$\text{Cost}_{\text{quantum}}(n, q, \sigma) \approx 2^{(0.265 \cdot \beta)} \tag{6}$$

where β is the dimension of the BKZ block required to solve the underlying lattice problem. This formula directly informs parameter selection in protocol design: ML-KEM-768 targets β values corresponding to approximately 178-bit quantum security, while ML-KEM-1024 targets approximately 218-bit quantum security, providing the formal basis for matching algorithm parameter sets to the security level requirements of specific protocol deployments, such as mandatory ML-KEM-1024 for high-sensitivity SDN control channels as discussed in Section 6.1.

In symmetric cryptography, Grover's algorithm reduces brute-force search complexity, effectively halving key strength [85]:

$$\text{PostQuantum\_Security}(\text{AES-}k) = \frac{k}{2} \tag{7}$$

This formula directly justifies the protocol-level recommendation, discussed in Section 4.1, to replace AES-128 with AES-256 in all quantum-resilient network protocol deployments: AES-128 provides only 64-bit effective post-quantum security under Grover's attack, which falls below accepted security thresholds, while AES-256 retains 128-bit effective security.

In contrast, QKD provides information-theoretic security grounded in quantum mechanics [15,59]. The secure key rate is bounded by the Devetak–Winter theorem [121]:

$$K \geq 1 - h(e_{\text{bit}}) - h(e_{\text{phase}}) \tag{8}$$

where $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary entropy function, and e_{bit}, e_{phase} are the bit and phase error rates, respectively. Practical QKD key rate degrades with channel length:

$$K(L) = K_0 \cdot 10^{-\alpha L/10} \tag{9}$$

These two formulas together provide the formal underpinning for the SDN controller QKD key availability management function described in Section 6.1: $K(L)$ quantifies the key generation rate available on each QKD link as a function of fibre length and loss coefficient α, while the Devetak–Winter bound constrains the maximum achievable secure rate under measured channel error rates. An SDN controller with telemetry of both e_{bit} and link occupancy can compute real-time key availability estimates and schedule sessions or trigger PQC fallback accordingly, directly translating these formulas into operational control-plane decisions.

Anomaly detection in network environments is modelled as a one-class classification problem [98]. Autoencoder-based approaches quantify anomalies via reconstruction error:

$$\text{Score}(x) = \|x - \text{Decoder}(\text{Encoder}(x))\|^2 \tag{10}$$

A threshold-based mechanism flags inputs exceeding a calibrated reconstruction error as anomalous. As discussed in Section 5.3, in quantum-resilient network deployments the input feature vector x must be specifically constructed to include PQC-relevant protocol observables, TLS handshake completion rates, cipher suite negotiation outcomes, key exchange parameter size distributions, and certificate validation

sequence patterns, so that the autoencoder learns a normal manifold reflective of compliant PQC-negotiated traffic, enabling detection of protocol downgrade attempts, HNDL interception activity, and anomalous cryptographic negotiation patterns as flagged behavioural deviations from this manifold. Performance is evaluated using ROC-AUC metrics. Table 6 lists the details of mathematical models and formulations across various applications.

Table 6: Mathematical models and their applications in AI-enabled quantum-resilient networking.

Model/Framework	Formulation	Application
MDP for routing [122]	$M = (S, A, P, R, \gamma)$	DRL-based routing control
DQN loss [123–125]	$L(\theta) = \mathbb{E}[(r + \gamma Q(s', a'; \theta^-) - Q(s, a; \theta))^2]$	Congestion control, resource management
FedAvg objective [126]	$w^* = \arg\min \sum(n_k/n) \cdot F_k(w)$	Distributed network AI training
Differential privacy [127]	Gaussian noise: $\mathcal{N}(0, \sigma^2 C^2 I)$	Privacy-preserving FL
Quantum gate cost	Cost $\approx 2^{(0.265\beta)}$	PQC security estimation
Grover security	PostQ-security = $k/2$ bits	Symmetric key migration
QKD key rate [128–131]	$K \geq 1 - h(e_{\text{bit}}) - h(e_{\text{phase}})$	Fiber-based QKD performance
QKD distance decay [128,131,132]	$K(L) = K_0 \cdot 10^{(-\alpha L/10)}$	Repeater design, link budget analysis
Autoencoder scoring [131,133]	Score = $\|x - \text{Dec}(\text{Enc}(x))\|^2$	Network anomaly detection

8 Key Challenges and Open Problems

Key challenges and open problems are unresolved technical, operational, and research issues that impede large-scale deployment of AI-enabled and quantum-resilient network protocols. The integration of AI with quantum-safe communication mechanisms introduces a complex set of interdisciplinary challenges spanning networking, ML, and cryptography. These challenges arise not only from computational and architectural constraints but also from evolving threat models and standardization gaps. As networks transition toward quantum-resilient infrastructures, issues such as scalability, interoperability, and economic feasibility become increasingly critical. Moreover, the dynamic nature of AI systems introduces additional concerns related to robustness, explainability, and trustworthiness. Addressing these challenges requires coordinated efforts across academia, industry, and standardization bodies. Existing studies highlight that no single solution is sufficient; instead, a combination of optimization, secure design, and policy frameworks is necessary. This section surveys the major open problems that define the current research frontier in this domain.

8.1 Performance and Scalability

Deploying PQC and AI-driven control jointly within high-throughput network protocol stacks introduces a coupled performance bottleneck that neither research community has systematically addressed in

isolation. PQC algorithms impose measurable overhead in key and signature sizes and computation time relative to classical algorithms [13,14]. ML-KEM-768 ciphertexts at 1088 bytes and ML-DSA-65 signatures at 3309 bytes directly inflate TLS handshake sizes, increase fragmentation risk under standard MTU limits, and raise per-session cryptographic computation costs. Simultaneously, AI model inference latency, particularly for per-flow DRL routing decisions [69,96], must be compatible with the microsecond-scale timing budgets of high-speed switching environments. The integration of ML-KEM into high-throughput network protocols requires careful benchmarking and optimization [14,55]. The difficulty is structural and multi-layered. PQC algorithms are built on lattice arithmetic, specifically Number Theoretic Transform (NTT) polynomial multiplication, whose computational cost does not reduce with clock speed improvements in the same way classical modular exponentiation does. When PQC and AI are deployed jointly, their overheads interact. PQC handshake latency delays the state observations available to the DRL agent, while DRL policy computation delays cryptographic session establishment, creating a feedback loop that neither PQC nor AI research has addressed in isolation. In resource-constrained environments such as IoT and edge networks, increased key sizes further amplify bandwidth consumption and storage overhead, making the joint deployment problem qualitatively harder than either challenge alone. FPGA acceleration for NTT operations [55] has demonstrated significant throughput improvements for ML-KEM polynomial arithmetic. Model compression techniques [103] reduce AI inference overhead. Edge AI and hierarchical model deployment strategies have been explored to reduce centralized bottlenecks. Adaptive mechanisms that dynamically adjust cryptographic parameters and AI model complexity based on network conditions are also emerging as promising directions. Co-optimized benchmarking frameworks that jointly evaluate PQC cryptographic overhead and AI inference latency under realistic, high-throughput traffic conditions remain absent. Existing benchmarks treat PQC and AI performance independently, failing to capture their coupled interaction in deployed protocol stacks. Standardized evaluation methodologies for PQC-AI integrated systems across IoT, edge, and core network segments do not yet exist, making cross-study comparison unreliable. Future research should develop unified co-optimization frameworks that jointly model PQC handshake cost and AI inference latency as coupled variables in network protocol design. Hardware-software co-design approaches combining FPGA-accelerated NTT with lightweight DRL inference engines are a promising direction. Adaptive parameter selection mechanisms, dynamically choosing between ML-KEM-512, ML-KEM-768, and ML-KEM-1024 based on real-time link conditions and latency budgets, represent an important open problem requiring co-optimization across cryptographic and networking layers.

8.2 Adversarial Robustness and AI Security

AI-driven network components operating within quantum-resilient protocol stacks face an adversarial threat surface that extends well beyond classical ML attacks. At the classical layer, AI components are susceptible to data poisoning, model evasion, and model extraction [101,102]. At the quantum layer, AI anomaly detectors must be extended to recognize quantum-specific attack vectors, including side-channel attacks on QKD implementations [16] and photon-number splitting (PNS) attacks on weak coherent pulse QKD systems [15]. Critically, an adversary who successfully manipulates the AI cryptographic agility controller into selecting a downgraded cipher suite gains a cryptographic advantage without ever attacking the cryptographic primitive itself, making the AI control layer a high-value attack target in its own right. Reference [101] demonstrated the fragility of neural networks to imperceptible input perturbations, and this fragility carries qualitatively more severe consequences when the neural network controls cryptographic session parameters. Misclassification consequences extend from traffic misrouting to full session key compromise. Hybrid classical-quantum protocol stacks introduce new adversarial entry points at every integration boundary, between the AI controller and the PQC negotiation layer, between the QKD key

management system and the SDN controller, and between FL aggregation and cryptographic agility logic. Quantum-specific vectors such as side-channel information leakage from QKD optical hardware [16,134] are physically grounded threats that classical adversarial ML defences were never designed to detect. The integration of AI into critical network infrastructure further amplifies the potential impact of such attacks, where adversarial manipulation of routing or security decisions can lead to large-scale service disruptions or data breaches. Certified defences [102] and formal verification provide provable robustness guarantees within bounded perturbation sets. Adversarial training and robust optimization are being actively explored to mitigate evasion and poisoning risks. Explainability techniques [113] are essential for operational deployment in regulated environments and provide insight into AI decision-making processes. Continuous monitoring and adaptive learning strategies are being investigated for real-time threat detection. No existing adversarial robustness framework simultaneously addresses: (a) classical adversarial ML attacks on the AI control layer, (b) quantum-specific side-channel and PNS attacks on the QKD physical layer, and (c) the cryptographic consequences of AI misclassification in algorithm selection. The interaction between model poisoning in FL and cryptographic agility logic, where a poisoned aggregated model could systematically select weaker cipher suites network-wide, represents a particularly critical and unaddressed gap. Future work should develop quantum-aware adversarial robustness frameworks that jointly model classical adversarial ML threats and quantum-physical attack vectors within a unified threat model. Formal verification of AI cryptographic agility controllers, proving that no adversarial input can induce selection of a non-compliant cipher suite, is an important open direction. Byzantine-robust federated aggregation protocols that are simultaneously PQC-secured and poisoning-resistant require dedicated research combining FL theory with post-quantum cryptographic protocol design.

8.3 Standardization and Interoperability

The transition to quantum-resilient networking requires simultaneous, coordinated standardization across multiple protocol layers and multiple independent standards bodies, a degree of cross-organizational alignment that has no precedent in prior cryptographic transitions. PQC integration must be standardized across TLS [13], IKEv2 [77], SSH [13], and DNSSEC through IETF working groups, while NIST-finalized standards [12,50] provide the cryptographic primitive layer. For QKD, ETSI, ITU-T, and International Organization for Standardization (ISO) and the International Electrotechnical Commission (ISO/IEC) standardization efforts [18] must harmonize with Network Configuration Protocol (NETCONF) and Yet Another Next Generation (YANG) network management standards [81]. UC security [57] provides formal tools for analyzing composed PQC-classical protocol security, but its application to deployed hybrid protocol stacks remains limited. The standardization landscape is fragmented across bodies operating on different timelines, with different technical scopes and without a unified coordination mechanism. Production networks simultaneously consist of legacy systems running classical cryptography, modern SDN/NFV infrastructures, and emerging quantum communication components, all of which must interoperate during a transition period of indeterminate length. Cross-layer standardization, specifying interfaces between AI orchestration modules and cryptographic services, or between QKD key management systems and YANG/NETCONF management planes, falls outside the primary scope of any single standardization body, creating a coordination gap at precisely the integration points where security vulnerabilities are most likely to emerge. Backward compatibility with existing protocols must be maintained throughout, further constraining the design space. NIST finalized FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) in August 2024 [12,50], providing the cryptographic primitive layer. IETF working groups are actively developing hybrid PQC extensions for TLS 1.3, IKEv2, and SSH. ETSI and ITU-T have published QKD interface standards [18]. Backward compatibility considerations are being addressed through hybrid classical/PQC transitional mechanisms in several IETF

drafts. Collaborative initiatives between standardization bodies and industry stakeholders are accelerating adoption in critical sectors. Unified cross-layer standards that simultaneously specify PQC algorithm integration at the protocol layer, QKD key management interfaces, and AI module integration points within SDN/NFV management frameworks do not yet exist. Current deployments are necessarily bespoke, creating fragmentation and security vulnerabilities at integration boundaries. Formal composability analysis using tools such as UC security [57] of hybrid PQC-classical protocols as they will actually be deployed in heterogeneous production networks remains largely absent from standardization documents. Future work should develop globally accepted, cross-layer standards integrating PQC algorithm specifications, QKD key management interfaces, and AI orchestration APIs within a unified framework. Formal backward-compatible hybrid transition specifications for each major protocol, including TLS, IKEv2, SSH, DNSSEC, and BGP, that define negotiation fallback behaviour under mixed classical/PQC environments are urgently needed. International coordination mechanisms between NIST, IETF, ETSI, and ITU-T to align timelines and technical scope represent an important institutional priority.

8.4 Data Privacy and Federated Intelligence

Multi-domain FL for network AI must simultaneously satisfy three conflicting requirements: strong privacy guarantees under data sovereignty constraints, acceptable model accuracy under non-IID data distributions, and quantum-resilient aggregation channel security, a three-way tension that no existing framework jointly addresses. Multi-domain FL [10] must operate under strict data sovereignty constraints. Differential privacy [21] and secure aggregation [20] provide partial solutions but impose accuracy-privacy trade-offs. The quantum threat extends to FL infrastructure. Gradient aggregation protocols relying on classical authenticated channels require PQC migration [28,54]. Homomorphic encryption [100] enables computation on encrypted model updates, supporting privacy-preserving FL without trusted aggregators. Differential privacy noise injection degrades model accuracy, and this accuracy loss is amplified when federated rounds are reduced in frequency by PQC aggregation overhead. Since ML-KEM-768 introduces 1088-byte ciphertexts per aggregation channel establishment compared to 32 bytes for ECDH P-256, overhead compounds across participants and rounds. Inference attacks and gradient leakage mean that even without sharing raw data, federated participants can reconstruct sensitive information from model updates. Regulatory requirements impose additional sovereignty constraints that conflict with the global aggregation assumptions of standard FedAvg. As QC matures, classical authenticated aggregation channels become vulnerable, requiring PQC migration of the aggregation protocol itself and adding further overhead to an already bandwidth-constrained process. Differential privacy [21] provides formal privacy guarantees via calibrated noise injection. Practical secure aggregation [20] enables privacy-preserving model aggregation. Homomorphic encryption [100] supports computation on encrypted updates, eliminating trusted aggregators. Network compression [103] and neuromorphic computing [104] reduce communication and energy overhead. Secure multi-party computation is also being explored as an alternative aggregation mechanism. Quantum-resilient FL frameworks with formally bounded and jointly optimized privacy-accuracy-latency trade-offs do not yet exist. Current approaches address these dimensions independently, failing to model their coupled interaction under PQC-secured aggregation. PQC-compatible secure multi-party computation protocols with practical overhead bounds for resource-constrained edge devices remain an open problem. The specific vulnerability of federated cryptographic agility models to Byzantine poisoning, where a compromised participant systematically biases the global model toward weaker cipher suite selections, has not been formally analyzed. Future research should develop co-optimization frameworks that jointly minimize privacy loss, model accuracy degradation, and PQC aggregation overhead within a unified FL objective.

PQC-secured variants of secure multi-party computation with edge-device-compatible computational budgets require dedicated protocol design. Formal analysis of Byzantine robustness in federated cryptographic agility systems, proving bounds on cipher suite degradation achievable by a bounded number of poisoned participants, represents an important open theoretical problem.

8.5 Quantum Network Deployment Economics

QKD deployment imposes infrastructure requirements including dedicated dark fibre or wavelength allocations, specialized single-photon detectors, strict environmental controls [17,18,60], and physically secured trusted relay nodes that create a cost structure fundamentally different from classical cryptographic infrastructure and cannot be reduced to software or algorithmic improvements alone. Quantum repeater technology [61,62] remains in early development, constraining practical QKD to limited distances. The combination of QKD and PQC, referred to as quantum hybrid security, is recommended for critical infrastructure [18,54], providing defence-in-depth, but the economic justification for this dual deployment requires rigorous cost-benefit modelling that the literature has not yet provided. The economic difficulty is partially physics-constrained rather than purely market-driven. QKD key generation rates are bounded by photon transmission rates and channel loss, as expressed by $K(L) = K_0 \cdot 10^{-\alpha L/10}$, meaning key generation capacity decreases exponentially with fibre distance regardless of hardware improvements. This creates an irreducible cost floor for long-distance QKD that cannot be engineered away without quantum repeaters, which themselves remain experimentally immature [61,62]. Trusted relay nodes introduce physical security requirements including tamper-evident facilities, personnel vetting, and continuous monitoring that are absent from classical network infrastructure. The high cost of quantum communication infrastructure also requires skilled personnel and maintenance resources whose availability varies significantly across regions. Hybrid PQC/QKD architectures [18,54] provide a practical pathway by leveraging existing classical infrastructure for PQC while selectively deploying QKD on the highest-sensitivity links, reducing total QKD coverage required. Trusted relay deployments have been demonstrated in national-scale testbeds in China, Europe, and Japan. Public-private partnerships and government initiatives are playing a key role in subsidizing early deployment costs. Cost-benefit analyses for specific high-value sectors including defence, finance, and critical infrastructure have been conducted to justify selective adoption. Rigorous, generalizable techno-economic models for hybrid quantum-classical network deployments across diverse contexts including metropolitan, national, and cross-border environments do not exist. Existing economic analyses are case-specific and do not provide transferable models for deployment decision-making. The economic implications of quantum repeater maturation, specifically how repeater availability would alter the cost structure of long-distance QKD and reshape the PQC/QKD deployment balance, have not been formally modelled. Region-specific deployment economics accounting for fibre infrastructure availability, regulatory environments, and threat models are also absent from the literature. Future research should develop generalizable techno-economic models for hybrid PQC/QKD network deployment parameterized by coverage distance, traffic sensitivity classification, QKD key generation rate, and quantum repeater availability. Scalable deployment architectures that minimize QKD coverage requirements by intelligently identifying which links require QKD vs. PQC-only protection, potentially using AI-driven risk classification of traffic flows, represent an important co-design opportunity. Long-term roadmaps integrating quantum repeater maturation timelines with deployment economics planning are needed to guide investment decisions by network operators and policymakers.

9 Research Gaps and Future Directions

Despite significant advancements, the integration of AI with quantum-safe communication mechanisms remains in its early stages, with multiple open research challenges. These gaps arise due to limitations in scalability, computational efficiency, interoperability, and the lack of unified design frameworks. At the same time, rapid developments in AI, cryptography, and quantum communication present new opportunities for innovation. Addressing these gaps requires interdisciplinary approaches that combine networking, ML, and quantum technologies. However, future research must focus on practical deployment considerations, including resource constraints, real-time adaptability, and security assurance. The surveyed literature highlights that bridging these gaps is essential for achieving robust, scalable, and future-proof communication architecture. This section outlines key research directions that can shape the next generation of intelligent and quantum-resilient networks.

Table 7 summarizes the identified research gaps, their relevant domains, assigned priority levels, anticipated time frames, and key supporting references. Across, Priority levels are assigned based on a composite assessment of deployment urgency, security impact, research gap severity, technical feasibility, and standardization dependency. Deployment urgency reflects how immediately a gap affects currently deployed or imminently standardized systems. Security impact represents the severity of the cryptographic or operational consequences if the gap remains unaddressed. Research gap severity captures the extent to which the issue remains insufficiently explored in the literature relative to its practical importance. Technical feasibility encompasses the likelihood of achieving meaningful progress in the near term given current algorithmic, hardware, and protocol maturity. Standardization dependency considers whether the gap directly blocks or enables ongoing NIST, IETF, ETSI, or ITU-T standardization efforts. A research gap is classified as Critical when it exhibits high deployment urgency, substantial security impact, and significant research-gap severity, indicating that insufficient progress could pose an immediate risk to quantum-resilient network deployments. High-priority gaps represent important near-term research challenges with strong implications for security, deployment, or standardization. Medium-priority gaps remain important but are either partially addressed, dependent on infrastructure maturation, or associated with less immediate security consequences. Low-priority gaps are generally exploratory, long-term in nature, or dependent on foundational advances in related research areas.

Table 7: Research gap taxonomy: priority, timeframe, and key references.

Research Gap	Research Question	Evaluation Metrics	Key References	Priority	Timeframe
Lightweight PQC for IoT	Can ML-KEM/ML-DSA run on constrained devices under strict resource limits?	Latency; RAM usage; energy/operation; code size	[6,14,28,55]	Critical	Near-term
AI-PQC Protocol Optimization	How to adapt DRL for PQC-aware TLS/QUIC performance?	Handshake latency; throughput; DRL convergence	[13,14,54,96]	High	Near-term
Adversarially Robust Net-AI	Can AI systems resist both classical and quantum-era attacks?	Attack success rate; ROC-AUC; downgrade rate	[99,101,102,113]	High	Near-term

(Continued)

Table 7 (continued)

Research Gap	Research Question	Evaluation Metrics	Key References	Priority	Timeframe
PQC/QKD Standardization	How to unify PQC and QKD standards across protocols?	Interoperability rate; adoption time; failure rate	[12,18,28,81]	High	Near-term
Quantum-Aware Digital Twins	Can twins accurately model QKD + PQC network behaviour?	Prediction error; sim latency; accuracy	[18,26,61,62]	Medium	Mid-term
Privacy-Preserving Federated AI	Can FL be PQC-secure, private, and efficient together?	Ciphertext overhead	[10,20,21,68]	Medium	Mid-term
Cross-Layer Security AI	Can AI detect cross-layer quantum-era attacks?	Heterogeneous data; XAI cost	[16,28,57,98]	Medium	Mid-term
Unified Co-Design Frameworks	Can AI, PQC, and QKD be jointly optimized?	No unified model; multi-objective complexity; missing UC integration	[12,18,57,61]	Critical	Mid-term
Quantum ML for Networking	Can QML outperform classical DRL in networking?	NISQ noise; no quantum advantage proof; benchmarking limits	[22,23,84]	Medium	Long-term
Quantum Repeater Networks	Can repeaters enable scalable QKD networks?	Decoherence; high cost; immature tech	[17,60–62]	High	Long-term
Neuromorphic Edge AI	Can neuromorphic chips support PQC-aware edge AI?	Programming maturity; accuracy gap vs. DNNs	[22,103,104]	Low	Long-term

Note: Critical = immediate research need; High = substantial near-term importance; Medium = moderate urgency or mid-term relevance; Low = emerging long-term research direction

9.1 Lightweight PQC for Constrained Environments

Lightweight PQC encompasses the design of resource-efficient post-quantum cryptographic algorithms suitable for devices with limited computational, memory, and energy capabilities. IoT and edge devices [6] face severe resource constraints incompatible with current PQC key and signature sizes [14,28,55]. Research on algorithm variants and hardware-software co-design for Class 0/1 constrained devices is urgently needed [55]. Cognitive IoT frameworks [6] may provide adaptive security protocol selection based on device capability and threat context. In addition, the deployment of PQC in constrained environments requires significant optimization to balance security and efficiency. Current PQC schemes often introduce large key sizes and computational overhead, making them impractical for low-power devices. Lightweight cryptographic primitives and hybrid approaches are being explored to address these limitations. Hardware acceleration, such as Application-Specific Integrated Circuit (ASIC) and FPGA-based implementations, can further reduce latency and energy consumption. Adaptive frameworks that dynamically select cryptographic algorithms based on device context and network conditions offer promising solutions. Moreover, standardization efforts must consider the unique requirements of IoT ecosystems. Ensuring secure yet efficient communication in constrained environments remains a critical research challenge.

9.2 AI-Driven PQC Protocol Optimization

AI-driven PQC protocol optimization leverages the use of ML techniques to dynamically optimize the selection and configuration of post-quantum cryptographic protocols. DRL agents could dynamically select PQC algorithm variants, key sizes, and hybrid configurations [54] based on security requirements and network conditions [69,96]. AI models trained on PQC handshake telemetry [13,14] could predict and preemptively mitigate PQC-induced latency anomalies. Transfer learning [97] could enable rapid adaptation of PQC-aware protocol agents across heterogeneous network environments. Also, integrating AI into cryptographic protocol management introduces new opportunities for adaptive and context-aware security. AI models can continuously learn from network behaviour and optimize cryptographic operations in real time. This enables efficient handling of dynamic workloads and varying threat levels. Predictive analytics can identify potential performance bottlenecks before they impact system performance. However, ensuring the reliability and security of AI-driven decisions remains a challenge. The integration of AI with cryptographic systems also raises concerns about explainability and trust. Developing robust, interpretable, and efficient AI-driven optimization frameworks is an important future direction.

9.3 Quantum-Aware Network Digital Twins

Quantum-aware network digital twins are virtual replicas of networks that model both classical and quantum communication components, enabling simulation, analysis, and optimization of hybrid quantum–classical infrastructures. Network digital twins must evolve to incorporate QKD channel models, quantum memory performance parameters, and repeater network topologies [61,62]. Quantum-aware digital twins would enable safe simulation of hybrid PQC-QKD protocol configurations and AI-driven orchestration strategies without risking operational network stability. In addition, digital twins provide a powerful platform for testing and validating new network protocols in a controlled environment. By incorporating quantum-specific parameters, these models can simulate realistic quantum communication scenarios. This enables researchers to evaluate performance, security, and scalability before deployment. AI-driven optimization strategies can also be tested and refined within digital twin environments. Also, digital twins support predictive maintenance and fault analysis, improving network reliability. The integration of real-time data enhances model accuracy and responsiveness. Developing comprehensive quantum-aware digital twins is essential for accelerating innovation and reducing deployment risks.

9.4 QML for Networking

QML constitutes the application of QC principles to enhance ML algorithms and solve complex optimization problems. QML [22] and quantum-inspired classical algorithms [23] may offer computational advantages for specific network optimization problems—particularly those involving high-dimensional optimization spaces or combinatorial structure. The theoretical foundations of quantum ML [22,23] suggest potential speedups for clustering, recommendation, and linear systems problems that have network optimization analogues, though near-term Noisy Intermediate-Scale Quantum (NISQ) limitations [84] constrain practical applicability.

Beyond theoretical potential, QML represents a promising direction for addressing computationally intensive networking problems. Hybrid quantum-classical models can leverage the strengths of both paradigms to achieve improved performance. Applications such as traffic optimization, anomaly detection, and resource allocation may benefit from quantum speedups. However, current quantum hardware limitations restrict large-scale deployment. Research is needed to identify practical use cases where quantum advantages can be realized. Additionally, integration with existing network infrastructure poses significant challenges. Despite these limitations, QML remains a key area for future exploration.

9.5 Cross-Layer Security Intelligence and XAI

Achieving quantum-resilient network security requires coordinated threat detection and response across protocol layers that currently operate with independent security models [135], a gap that single-layer AI security approaches cannot close. Future architectures should integrate AI-driven security intelligence operating across physical (QKD side-channel indicators [16]), network (PQC authentication status [28]), and application (behavioural anomaly signals [98,99]) layers, enabling AI models to correlate observables across layers to identify complex attack patterns, such as a coordinated QKD side-channel probe coinciding with a TLS cipher suite downgrade attempt, that are invisible to any single-layer detector operating in isolation.

Explainability [113] is essential for operational acceptance of autonomous security decisions, particularly in regulated environments where accountability for cryptographic policy enforcement must be auditable. An XAI-equipped AI security controller that can produce human-interpretable justifications for algorithm selection or session termination decisions is not merely preferable; it is a prerequisite for deployment in critical infrastructure contexts where unexplained autonomous cryptographic decisions carry legal and operational liability. Formal verification [102] of AI-driven protocol controllers provides correctness guarantees analogous to classical protocol verification, bounding the set of inputs under which the controller can produce a non-compliant cryptographic output. However, achieving seamless cross-layer integration of explainability and formal verification within a single operational security framework remains an open and technically demanding research challenge.

9.6 Unified Co-Design Frameworks

The most critical gap in the AI-quantum networking research landscape is the absence of frameworks that co-design AI-driven intelligence and quantum-resilient security from first principles, rather than integrating them as independently developed components retrofitted onto each other. This distinction matters because the state representations, reward functions, and optimization objectives of AI-driven controllers must be fundamentally restructured to account for PQC-induced handshake costs, QKD key pool constraints, and key-rotation frequency, restructuring that cannot be achieved by simply layering AI on top of an existing PQC/QKD deployment. UC security [57] provides formal tools for analyzing the composed security of AI-protocol-PQC systems, ensuring that the security properties of individual components are preserved when integrated into a larger architectural whole and specifically that composed architectures remain robust against adaptive adversaries who can exploit integration boundaries. The quantum internet layered development roadmap [61] provides an architectural template for phased co-design, defining capability levels from prepare-and-measure QKD through entanglement distribution that can structure the timeline and scope of co-design framework development. QML [22] and privacy-preserving FL [20,21] must be integrated into this framework as first-class components, not added as extensions, so that their learning objectives and privacy constraints are jointly optimized with the cryptographic security and protocol performance requirements of the target deployment. Establishing such comprehensive co-design methodologies, validated through formal security analysis and empirical protocol benchmarking, represents one of the most consequential open research directions identified in this survey and one whose resolution is a prerequisite for the remaining gaps identified in Table 7 to be addressed coherently.

10 Conclusion

This survey has presented a comprehensive and critical review of research at the intersection of AI and quantum-resilient communication, viewed through the lens of network protocol design. We traced the evolutionary trajectory of network protocols from classical layered architectures through programmable SDN-era systems to the emerging vision of AI-driven autonomous operation. The quantum threat landscape,

including Shor's and Grover's algorithms and HNDL attacks, was analyzed alongside the principal quantum-resilient mechanisms: NIST-standardized PQC (ML-KEM, FIPS 203; ML-DSA, FIPS 204; SLH-DSA, FIPS 205), QKD, and hybrid approaches. The survey reveals that existing research largely treats AI intelligence and quantum-resilient security as separate concerns. Little attention has been devoted to jointly designing AI learning objectives, state representations, reward functions, and decision spaces alongside PQC-induced latency, QKD key management constraints, and cryptographic lifecycle requirements. This lack of integrated design remains one of the most significant barriers to the development of truly intelligent and quantum-resilient network protocols. The analysis also highlights the urgency of migration efforts in response to HNDL threats, as sensitive communications protected by classical cryptography today may already be vulnerable to future quantum decryption. The identified research gaps indicate that lightweight PQC mechanisms for constrained IoT and edge environments, AI-assisted cryptographic agility, adversarial robust network intelligence, cross-layer security orchestration, and unified co-design methodologies deserve particular attention. Progress in these areas will require tighter integration of protocol engineering, cryptographic design, ML, and formal security analysis. Future research should also focus on efficient PQC deployment within widely used protocols such as TLS and QUIC, trustworthy and explainable AI-driven security controllers, privacy-preserving learning architectures, scalable quantum networking infrastructures, and interoperable hybrid PQC/QKD systems capable of supporting practical deployment scenarios. The findings of this survey also carry important implications for protocol designers, standardization organizations, and network operators. Protocol designers must carefully evaluate the performance and security trade-offs introduced by PQC algorithms and redesign AI-enabled protocol components to account for quantum-resilient security requirements. Standardization bodies should continue developing interoperable migration frameworks that bridge cryptographic, networking, and AI-management requirements across emerging deployments. Network operators, meanwhile, should begin preparing for hybrid environments that combine classical and quantum-resilient mechanisms while addressing the operational challenges associated with cryptographic agility, key management, and automated policy enforcement. Overall, the convergence of AI and quantum-resilient networking represents one of the most technically demanding and strategically important research frontiers in modern network protocol design. Continued progress will depend on coordinated advances in cryptography, networking, AI, and standardization. By identifying current capabilities, persistent limitations, and promising research directions, this survey provides a foundation for the development of secure, intelligent, and quantum-resilient communication infrastructures for the post-quantum era.

Acknowledgement: Not Applicable.

Funding Statement: This research was supported in part by the Strategic Networking & Development Program funded by the Ministry of Science and ICT through the National Research Foundation of Korea (RS-2026-25549127) and supported by the 2026 Hongik University Innovation Support Program Fund.

Author Contributions: The authors confirm contributions to the paper as follows: Conceptualization, Bareera Anam; investigation, Bareera Anam; writing original draft preparation, Bareera Anam and Muhammad Asim; writing—review and editing, Bareera Anam, Muhammad Asim and Muhammad Nadeem Ali; visualization, Bareera Anam, Muhammad Asim and Muhammad Nadeem Ali; supervision, Byung-Seo Kim. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: Not Applicable.

Ethics Approval: Not Applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Supplementary Materials: The supplementary material is available online at https://www.techscience.com/doi/10.32604/cmc.2026.084949/s1.

Abbreviations

AI	Artificial Intelligence
IDS	Intrusion Detection System
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
SSH	Secure Shell
PNS	Photon Number Splitting
NIST	National Institute of Standards and Technology
IPsec	Internet Protocol Security
IETF	Internet Engineering Task Force
ETSI	European Telecommunications Standards Institute
ITU-T	International Telecommunication Union–Telecommunication Standardization Sector
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
YANG	Yet Another Next Generation
NETCONF	Network Configuration Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UC	Universally Composable
DRL	Deep Reinforcement Learning
QRC	Quantum-Resilient Cryptography
IoT	Internet of Things
ML	Machine Learning
XAI	Explainable Artificial Intelligence
FPGA	Field-Programmable Gate Array
ASIC	Application-Specific Integrated Circuit
Non-IID	Non Independent and Identically Distributed
QML	Quantum Machine Learning
NISQ	Noisy Intermediate-Scale Quantum
SLA	Service Level Agreement
SDN	Software-Defined Networking
BGP	Border Gateway Protocol
TLS	Transport Layer Security
QC	Quantum Computing
ECC	Elliptic Curve Cryptography
RSA	Rivest–Shamir–Adleman
HNDL	Harvest-Now-Decrypt-Later
FL	Federated Learning
NFV	Network Functions Virtualization
ML-KEM	Module-Lattice-Based Key Encapsulation Mechanism
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
QUIC	Quick UDP Internet Connections
IKEv2	Internet Key Exchange Version 2
DNSSEC	Domain Name System Security Extensions
RL	Reinforcement Learning

References

1. Mehra J, Madaan S, Balu N, Selvakumar P, Manjunath TC. The ubiquitous internet and smart computation available 24/7 for anyone and anywhere. In: Educational AI humanoid computing devices for cyber nomads. Hershey, PA, USA: IGI Global Scientific Publishing; 2025. p. 247–7.
2. Clark D. The design philosophy of the DARPA Internet protocols. In: Proceedings of the Symposium on Communications Architectures and Protocols; 1988 Aug 16–18; Stanford, CA, USA. p. 106–14.
3. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science; 1994 Nov 20–22; Santa Fe, NM, USA. p. 124–34.
4. Blanco-Romero J, Mendoza FA, Gárcia-Rubio C, Campo C, Sánchez DD. On the practical feasibility of harvest-now, decrypt-later attacks. arXiv:2603.01091. 2026.
5. Kagai F, Branch P, But J, Allen R. Harvest-now, decrypt-later: a temporal cybersecurity risk in the quantum transition. Telecommunications. 2025;6(4):100.
6. Giuliano A, McCafferty-Leroux A, Yawney J, Gadsden SA. Cognitive internet of things: a review of theory, applications, and recent advances. IEEE Commun Surv Tutor. 2025;28:446–84.
7. Mao H, Alizadeh M, Menache I, Kandula S. Resource management with deep reinforcement learning. In: Proceedings of the 15th ACM Workshop on Hot Topics in Networks; 2016 Nov 9–10; Atlanta, GA, USA. p. 50–6.
8. Broadbent A, Schaffner C. Quantum cryptography beyond quantum key distribution. Des Codes Cryptogr. 2016;78(1):351–82. doi:10.1007/s10623-015-0157-4.
9. Chen M, Yang Z, Saad W, Yin C, Poor HV, Cui S. A joint learning and communications framework for federated learning over wireless networks. IEEE Trans Wirel Commun. 2020;20(1):269–83. doi:10.1109/twc.2020.3024629.
10. Li T, Sahu AK, Talwalkar A, Smith V. Federated learning: challenges, methods, and future directions. IEEE Signal Process Mag. 2020;37(3):50–60.
11. Bernstein DJ, Lange T. Post-quantum cryptography. Nature. 2017;549(7671):188–94. doi:10.1038/nature23461.
12. Alagic G, Apon D, Cooper D, Dang Q, Dang T, Kelsey J, et al. Status report on the third round of the NIST post-quantum cryptography standardization process. NIST. 2022. doi:10.6028/NIST.IR.8413.
13. Sikeridis D, Kampanakis P, Devetsikiotis M. Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH. In: Proceedings of the 16th International Conference on Emerging Networking Experiments and Technologies; 2020 Dec 1–4; Virtual. p. 149–56.
14. Paquin C, Stebila D, Tamvada G. Benchmarking post-quantum cryptography in TLS. In: International Conference on Post-Quantum Cryptography. Berlin/Heidelberg, Germany: Springer; 2020. p. 72–91.
15. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Mod Phys. 2002;74(1):145. doi:10.1103/revmodphys.74.145.
16. Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, et al. Advances in quantum cryptography. Adv Opt Photonics. 2020;12(4):1012–236. doi:10.1364/aop.361502.
17. Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M, et al. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett. 2018;121(19):190502. doi:10.1103/physrevlett.121.190502.
18. Mehic M, Niemiec M, Rass S, Ma J, Peev M, Aguado A, et al. Quantum key distribution: a networking perspective. ACM Comput Surv. 2020;53(5):1–41. doi:10.1145/3402192.
19. Wu Z, Pan S, Chen F, Long G, Zhang C, Yu PS. A comprehensive survey on graph neural networks. IEEE Trans Neural Netw Learn Syst. 2020;32(1):4–24. doi:10.1109/tnnls.2020.2978386.
20. Bonawitz K, Ivanov V, Kreuter B, Marcedone A, McMahan HB, Patel S, et al. Practical secure aggregation for privacy-preserving machine learning. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security; 2017 Oct 30–Nov 3; Dallas, TX, USA. p. 1175–91.
21. Dwork C, Roth A. The algorithmic foundations of differential privacy. Found Trends Theor Comput Sci. 2014;9(3–4):211–487. doi:10.1561/0400000042.
22. Biamonte J, Wittek P, Pancotti N, Rebentrost P, Wiebe N, Lloyd S. Quantum machine learning. Nature. 2017;549(7671):195–202. doi:10.1038/nature23474.
23. Tang E. A quantum-inspired classical algorithm for recommendation systems. In: Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing; 2019 Jun 23–26; Phoenix, AZ, USA. p. 217–28.

24. Boutaba R, Salahuddin MA, Limam N, Ayoubi S, Shahriar N, Estrada-Solano F, et al. A comprehensive survey on machine learning for networking: evolution, applications and research opportunities. J Internet Serv Appl. 2018;9(1):1–99. doi:10.1186/s13174-018-0087-2.
25. Leivadeas A, Falkner M. A survey on intent-based networking. IEEE Commun Surv Tutor. 2022;25(1):625–55. doi:10.1109/comst.2022.3215919.
26. McKeown N, Anderson T, Balakrishnan H, Parulkar G, Peterson L, Rexford J, et al. OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Comput Commun Rev. 2008;38(2):69–74.
27. Mijumbi R, Serrat J, Gorricho JL, Bouten N, Turck FD, Boutaba R. Network function virtualization: state-of-the-art and research challenges. IEEE Commun Surv Tutor. 2015;18(1):236–62.
28. Hoffman PE. The transition from classical to post-quantum cryptography. Fremont, CA, USA: Internet Engineering Task Force; 2019.
29. Luong NC, Hoang D, Gong S, Niyato D, Wang P, Liang YC, et al. Applications of deep reinforcement learning in communications and networking: a survey. IEEE Commun Surv Tutor. 2018;21(3):3133–74. doi:10.1002/9781119873747.ch1.
30. Xiao Y, Liu J, Wu J, Ansari N. Leveraging deep reinforcement learning for traffic engineering: a survey. IEEE Commun Surv Tutor. 2021;23(4):2064–97. doi:10.1109/comst.2021.3102580.
31. Ríos-Guiral S, Lahmadi A, Botero JF, Gutiérrez SA. Leveraging reinforcement learning for traffic engineering in programmable networks: a survey. IEEE Commun Surv Tutor. 2025;28:1318–50. doi:10.1109/comst.2025.3632870.
32. Tam P, Ros S, Song I, Kang S, Kim S. A survey of intelligent end-to-end networking solutions: integrating graph neural networks and deep reinforcement learning approaches. Electronics. 2024;13(5):994.
33. Bikkasani DC, Yerabolu M. AI-driven 5G network optimization: a comprehensive review of resource allocation, traffic management, and dynamic network slicing. Am J Artif Intell. 2024. doi:10.20944/preprints202410.2084.v1.
34. Farris I, Taleb T, Khettab Y, Song J. A survey on emerging SDN and NFV security mechanisms for IoT systems. IEEE Commun Surv Tutor. 2018;21(1):812–37. doi:10.1109/comst.2018.2862350.
35. Bakhiet MBMT, Alofe OM, Azad MA, Lallie H, Fatema K, Sharif T. A comprehensive survey on secure software-defined network for the internet of things. Trans Emerg Telecommun Technol. 2021;33(1):e4391. doi:10.1002/ett.4391.
36. Abdi AH, Audah L, Salh A, Alhartomi MA, Rasheed H, Ahmed S, et al. Security control and data planes of SDN: a comprehensive review of traditional, AI, and MTD approaches to security solutions. IEEE Access. 2024;12:69941–80.
37. Pattaranantakul M, He R, Song Q, Zhang Z, Meddahi A. NFV security survey: from use case driven threat analysis to state-of-the-art countermeasures. IEEE Commun Surv Tutor. 2018;20:3330–68.
38. Nguyen VG, Brunstrom A, Grinnemo KJ, Taheri J. SDN/NFV-based mobile packet core network architectures: a survey. IEEE Commun Surv Tutor. 2017;19(3):1567–602. doi:10.1109/comst.2017.2690823.
39. Siddiqi S, Naeem F, Khan S, Khan KS, Tariq M. Towards AI-enabled traffic management in multipath TCP: a survey. Comput Commun. 2021;181:412–27.
40. Chawla D, Mehra PS. A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: challenges, opportunities and solutions. Internet Things. 2023;24(1):100950. doi:10.1016/j.iot.2023.100950.
41. Chhetri G, Somvanshi S, Hebli P, Brotee S, Das S. Post-quantum cryptography and quantum-safe security: a comprehensive survey. arXiv:2510.10436. 2025.
42. Sharath HA, Vrindavanam J, Dana S, Prasad SN. Quantum-resilient cryptography: a survey on classical and quantum algorithms. IEEE Access. 2025;13:172854–77.
43. Li Z, Zhang G, Dong S, Xu C. Network-wide traffic signal control optimization using a multi-agent deep reinforcement learning. Transp Res Part C Emerg Technol. 2021;125(3):103059. doi:10.1016/j.trc.2021.103059.
44. Alhachem C, Kellil M, Bouabdallah A. A multi-agent deep reinforcement learning approach for traffic management in complex communication networks. In: Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC); 2025 May 12–16; Abu Dhabi, United Arab Emirates. p. 1678–85.

45. He Q, Wang Y, Wang X, Xu W, Li F, Yang K, et al. Routing optimization with deep reinforcement learning in knowledge defined networking. IEEE Trans Mob Comput. 2024;23(2):1444–55. doi:10.1109/tmc.2023.3235446.
46. Li Y, Chen M. Software-defined network function virtualization: a survey. IEEE Access. 2015;3:2542–53. doi:10.1109/access.2015.2499271.
47. Papavassiliou S. Software defined networking (SDN) and network function virtualization (NFV). Future Internet. 2020;12(1):7. doi:10.3390/fi12010007.
48. Giotis K, Kryftis Y, Maglaris B. Policy-based orchestration of NFV services in software-defined networks. In: Proceedings of IEEE NetSoft; 2015 Apr 13–17; London, UK. p. 1–5.
49. Huang PH, Wen CH. Flow management and orchestration for virtualized network functions in software-defined networks. In: Programmable networks for IP service deployment. London, UK: The Institution of Engineering and Technology; 2017. p. 287–312.
50. Alagic G, Bros M, Ciadoux P, Cooper D, Dang Q, Dang T, et al. Status report on the first round of the additional digital signature schemes for the NIST post-quantum cryptography standardization process. NIST. 2024. doi:10.6028/NIST.IR.8528.
51. Chen L, Jordan S, Liu YK, Moody D, Peralta R, Perlner R, et al. Report on post-quantum cryptography. NIST. 2016. doi:10.6028/NIST.IR.8105.
52. Zafar A, Iqbal SS. Integrating code-based post-quantum cryptography into SSL TLS protocols through an interoperable hybrid framework. Discov Comput. 2025;28(1):202. doi:10.1007/s10791-025-09735-7.
53. Stebila D, Mosca M. Post-quantum key exchange for the internet and the open quantum safe project. In: International Conference on Selected Areas in Cryptography. Berlin/Heidelberg, Germany: Springer; 2016. p. 14–37.
54. Anastasova M, Kampanakis P, Massimo J. PQ-HPKE: post-quantum hybrid public key encryption. Cryptology ePrint Archive. 2022.
55. Oder T, Güneysu T. Implementing the NewHope-Simple key exchange on low-cost FPGAs. Lect Notes Comput Sci. 2017;11368(3):128–42. doi:10.1007/978-3-030-25283-0_7.
56. Le TD, Do PH, Dinh TD, Pham VD. Are enterprises ready for quantum-safe cybersecurity? arXiv:2509.01731. 2025.
57. Canetti R. Universally composable security: a new paradigm for cryptographic protocols. In: Proceedings of the IEEE Symposium on Foundations of Computer Science; 2001 Oct 14–17; Las Vegas, VA, USA. p. 136–45.
58. Dervisevic E, Tankovic A, Fazel E, Kompella R, Fazio P, Voznák M, et al. Quantum key distribution networks—key management: a Survey. ACM Comput Surv. 2024;57:1–36.
59. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11.
60. Liao SK, Cai WQ, Liu WY, Zhang L, Li Y, Ren JG, et al. Satellite-to-ground quantum key distribution. Nature. 2017;549(7670):43–7. doi:10.1038/nature23655.
61. Wehner S, Elkouss D, Hanson R. Quantum internet: a vision for the road ahead. Science. 2018;362(6412):eaam9288.
62. Shi S, Qian C. Concurrent entanglement routing for quantum networks: model and designs. In: Proceedings of the ACM SIGCOMM Conference; 2020 Aug 10–14; Virtual. p. 62–75.
63. Vyas N, Mendes P. Relaxing trust assumptions on quantum key distribution networks. In: Proceedings of EuCNC/6G Summit; 2024 Jun 3–6; Antwerp, Belgium. p. 709–14.
64. Stan C, Verchère D, Olmos JV, Monroy IT, Rommel S. Dynamic-threshold-based pre-relaying for enhanced key allocation in quantum-secured networks. J Opt Commun Netw. 2025;17(3):233–48. doi:10.1364/jocn.544857.
65. Feamster N, Rexford J, Zegura E. The road to SDN: an intellectual history of programmable networks. ACM SIGCOMM Comput Commun Rev. 2014;44(2):87–98. doi:10.1145/2602204.2602219.
66. Bosshart P, Daly D, Gibb G, Izzard M, McKeown N, Rexford J, et al. P4: programming protocol-independent packet processors. ACM SIGCOMM Comput Commun Rev. 2014;44(3):87–95.
67. Kephart JO, Chess DM. The vision of autonomic computing. Computer. 2003;36(1):41–50. doi:10.1109/mc.2003.1160055.
68. McMahan B, Moore E, Ramage D, Hampson S, Y Arcas BA. Communication-efficient learning of deep networks from decentralized data. Proc Mach Learn Res. 2017;54:1273–82.

69. Valadarsky A, Schapira M, Shahaf D, Tamar A. Learning to route. In: Proceedings of the 16th ACM Workshop on Hot Topics in Networks; 2017 Nov 30–Dec 1; Palo Alto, CA, USA. p. 185–91.
70. Mestres A, Rodriguez-Natal A, Carner J, Barlet-Ros P, Alarcón E, Solé M, et al. Knowledge-defined networking. ACM SIGCOMM Comput Commun Rev. 2017;47(3):2–10. doi:10.1145/3138808.3138810.
71. Sosnowski M, Wiedner F, Hauser E, Steger L, Schoinianakis D, Gallenmüller S, et al. The performance of post-quantum TLS 1.3. In: Proceedings of the 19th International Conference on Emerging Networking EXperiments and Technologies (CoNEXT Companion); 2023 Dec 5–8; Paris, France.
72. Sikeridis D, Kampanakis P, Devetsikiotis M. Post-quantum authentication in TLS 1.3: a performance study. In: Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2020; 2020 Feb 23–26; San Diego, CA, USA.
73. Giron A, Nascimento JPAD, Custódio R, Perin LP. Post-quantum hybrid KEMTLS performance in simulated and real network environments. Lect Notes Comput Sci. 2023;14168(7671):293–312. doi:10.1007/978-3-031-44469-2_15.
74. Döring R, Geitz M. Post-quantum cryptography in use: empirical analysis of the TLS handshake performance. In: Proceedings of the NOMS 2022—IEEE/IFIP Network Operations and Management Symposium; 2022 Apr 25–29; Budapest, Hungary. p. 1–5.
75. Cerf V, Kahn R. A protocol for packet network intercommunication. IEEE Trans Commun. 1974;22(5):637–48. doi:10.1109/tcom.1974.1092259.
76. Postel JB. DARPA internet program: internet and transmission control protocol specifications. Fremont, CA, USA: Internet Research Task Force location; 1981.
77. Kent S, Seo K. Security architecture for the Internet protocol. Fremont, CA, USA: Internet Research Task Force location; 2005.
78. Felt AP, Barnes R, King A, Palmer C, Bentzel C, Tabriz P. Measuring HTTPS adoption on the web. In: Proceedings of the 26th USENIX Security Symposium; 2017 Aug 16–18; Vancouver, BC, Canada. p. 1323–38.
79. Cardwell N, Cheng Y, Gunn CS, Yeganeh SH, Jacobson V. BBR: congestion-based congestion control. Commun ACM. 2017;60(2):58–66.
80. Labovitz C, Ahuja A, Jahanian F. Experimental study of internet stability and backbone failures. In: Proceedings of the 29th Annual International Symposium on Fault-Tolerant Computing; 1999 Jun 15–18; Madison, WI, USA. p. 278–85.
81. IETF RFC 9315. Intent-based networking: concepts and definitions. Fremont, CA, USA: Internet Research Task Force location; 2022.
82. Silver D, Huang A, Maddison CJ, Guez A, Sifre L, van den Driessche G, et al. Mastering the game of Go with deep neural networks and tree search. Nature. 2016;529(7587):484–9. doi:10.1038/nature16961.
83. Durr-E-Shahwar I M, Altamimi AB, Khan W, Hussain S, Alsaffar M. Quantum cryptography for future networks security: a systematic review. IEEE Access. 2024;12(5):180048–78. doi:10.1109/access.2024.3504815.
84. Preskill J. Quantum computing in the NISQ era and beyond. Quantum. 2018;2:79. doi:10.22331/q-2018-08-06-79.
85. Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing; 1996 May 22–24; Philadelphia, PA, USA. p. 212–9.
86. Mehic M, Michalek L, Dervisevic E, Burdiak P, Plakalovic M, Rozhon J, et al. Quantum cryptography in 5G networks: a comprehensive overview. IEEE Commun Surv Tutor. 2024;26(1):302–46. doi:10.1109/comst.2023.3309051.
87. Chen J, Peng W, Wang Y, Bian Y. On the security and efficiency of TLS 1.3 handshake with hybrid key exchange from CPA-Secure KEMs. Entropy. 2025;27(12):1242. doi:10.3390/e27121242.
88. Abbasi M, Cardoso F, Váz P, Silva J, Martins P. A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. Cryptography. 2025;9(2):32. doi:10.3390/cryptography9020032.
89. Sim M, Song G, Lee M, Yoon S, Baksi A, Seo H. Integrating and benchmarking KpqC in TLS/X.509. Electronics. 2025;14(18):3717. doi:10.3390/electronics14183717.
90. Goertzen JR, Stebila D. Post-quantum signatures in DNSSEC via request-based fragmentation. arXiv:2211.14196. 2022.

91. Mao S, Zhang H, Wu W, Liu J, Li S, Wang H. A resistant quantum key exchange protocol and its corresponding encryption scheme. China Commun. 2014;11(9):124–34. doi:10.1109/cc.2014.6969777.
92. Parra OJS, Sanchez LC, Gomez J. The evolution of VANET: a review of emerging trends in artificial intelligence and software-defined networks. IEEE Access. 2025;13:49187–213.
93. Goldstein M, Uchida S. A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PLoS One. 2016;11(4):e0152173. doi:10.1371/journal.pone.0152173.
94. Abbasloo S, Yen CY, Chao HJ. Classic meets modern: a pragmatic learning-based congestion control for the internet. In: Proceedings of the ACM SIGCOMM Conference; 2020 Aug 10–14; Virtual. p. 632–47.
95. Dong M, Li Q, Zarchy D, Godfrey PB, Schapira M. PCC: re-architecting congestion control for consistent high performance. In: Proceedings of the 12th USENIX Symposium on Networked Systems Design and Implementation; 2015 May 4–6; Oakland, CA, USA. p. 395–408.
96. Jay N, Rotman N, Godfrey B, Schapira M, Tamar A. A deep reinforcement learning perspective on internet congestion control. In: International Conference on Machine Learning; 2019 Jun 9–15; Long Beach, CA, USA; 2019. p. 3050–9.
97. Pan SJ, Yang Q. A survey on transfer learning. IEEE Trans Knowl Data Eng. 2009;22(10):1345–59. doi:10.1109/tkde.2009.191.
98. Chandola V, Banerjee A, Kumar V. Anomaly detection: a survey. ACM Comput Surv. 2009;41(3):1–58.
99. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutor. 2015;18(2):1153–76. doi:10.1109/comst.2015.2494502.
100. Acar A, Aksu H, Uluagac AS, Conti M. A survey on homomorphic encryption schemes: theory and implementation. ACM Comput Surv. 2018;51(4):1–35. doi:10.1145/3214303.
101. Goodfellow IJ, Shlens J, Szegedy C. Explaining and harnessing adversarial examples. arXiv:1412.6572. 2014.
102. Seshia SA, Desai A, Dreossi T, Fremont DJ, Ghosh S, Kim E, et al. Formal specification for deep neural networks. In: International Symposium on Automated Technology for Verification and Analysis; 2018 Oct 7–10; Los Angeles, CA, USA. p. 20–34.
103. Han S, Pool J, Tran J, Dally WJ. Learning both weights and connections for efficient neural networks. Adv Neural Inf Process Syst. 2015;28:1–9.
104. Roy K, Jaiswal A, Panda P. Towards spike-based machine intelligence with neuromorphic computing. Nature. 2019;575(7784):607–17. doi:10.1038/s41586-019-1677-2.
105. Buruaga JS, Méndez RB, Brito J, Martín V. Hybrid quantum-safe integration of TLS in SDN networks. Comput Netw. 2025;267(6):111355. doi:10.1016/j.comnet.2025.111355.
106. Horoschenkoff P, Rödiger J, Wilske M. A new control and management architecture for SDN-enabled quantum key distribution networks. J Opt Commun Netw. 2024;17(3):209–20. doi:10.1364/jocn.547074.
107. Yu X, Liu Y, Zou X, Cao Y, Zhao Y, Nag A, et al. Secret-key provisioning with collaborative routing in partially-trusted-relay-based quantum-key-distribution-secured optical networks. J Light Technol. 2022;40(12):3530–45. doi:10.1109/jlt.2022.3153992.
108. Allaw Z, Zein O, Ahmad AM. Cross-layer security for 5G/6G network slices: an SDN, NFV, and AI-based hybrid framework. Sensors. 2025;25:3335.
109. Wright P, White C, Parker RC, Pegon JS, Menchetti M, Pearse J, et al. 5G network slicing with QKD and quantum-safe security. IEEE/OSA J Opt Commun Netw. 2020;13(3):33–40. doi:10.1364/jocn.413918.
110. Roy KS, Singh S, Goswami H, Panchal S, Hassan SM. Design and evaluation of a resilient IBN architecture: integrating post-quantum cryptography with adaptive threat detection using machine learning. PLoS One. 2026;21:e0348293.
111. Sim DH, Shin J, Kim MH. Software-defined networking orchestration for interoperable key management of quantum key distribution networks. Entropy. 2023;25(6):943. doi:10.3390/e25060943.
112. Sanz A, Atutxa A, Franco D, Astorga J, Jacob E, Lopez D. Toward quantum-safe scalable networks: an open, standards-aware key management framework. arXiv:2509.09453. 2025.

113. Ribeiro MT, Singh S, Guestrin C. "Why should I trust you?" explaining the predictions of any classifier. In: Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining; 2016 Aug 13–17; San Francisco, USA. p. 1135–44.
114. Feriani A, Hossain E. Single and multi-agent deep reinforcement learning for AI-enabled wireless networks: a tutorial. IEEE Commun Surv Tutor. 2021;23(2):1226–52. doi:10.1109/comst.2021.3063822.
115. Mnih V, Kavukcuoglu K, Silver D, Rusu AA, Veness J, Bellemare MG, et al. Human-level control through deep reinforcement learning. Nature. 2015;518(7540):529–33. doi:10.1038/nature14236.
116. Sutton RS. Learning to predict by the methods of temporal differences. Mach Learn. 1988;3(1):9–44. doi:10.1007/bf00115009.
117. Yang Q, Liu Y, Chen T, Tong Y. Federated machine learning: concept and applications. ACM Trans Intell Syst Technol. 2019;10(2):1–19. doi:10.1145/3298981.
118. Abadi M, Chu A, Goodfellow I, McMahan HB, Mironov I, Talwar K, et al. Deep learning with differential privacy. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security; 2016 Oct 24–28; Vienna, Austria. p. 308–18.
119. McMahan HB, Ramage D, Talwar K, Zhang L. Learning differentially private recurrent language models. arXiv:1710.06963. 2017.
120. Regev O. On lattices, learning with errors, random linear codes, and cryptography. J ACM. 2009;56(6):1–40. doi:10.1145/1060590.1060603.
121. Devetak I, Winter A. Distillation of secret key and entanglement from quantum states. Proc R Soc A. 2005;461(2053):207–35. doi:10.1098/rspa.2004.1372.
122. Rajasekhar N, Radhakrishnan TK, Samsudeen N. Exploring reinforcement learning in process control: a comprehensive survey. Int J Syst Sci. 2025;56(14):3528–57. doi:10.1080/00207721.2025.2469821.
123. Yang Z, Xie Y, Wang Z. A theoretical analysis of deep Q-learning. Proc Mach Learn Res. 2020;120:486–9.
124. Wang S, Liu H, Gomes P, Krishnamachari B. Deep reinforcement learning for dynamic multichannel access in wireless networks. IEEE Trans Cogn Commun Netw. 2018;4(2):257–65. doi:10.1109/tccn.2018.2809722.
125. Qi Q. Universal approximation theorem of deep Q-networks. arXiv:2505.02288. 2025.
126. Zheng Z, Zhang H, Xue L. Federated Q-learning with reference-advantage decomposition: almost optimal regret and logarithmic communication cost. arXiv:2405.18795. 2024.
127. Zhou X. Differentially private reinforcement learning with linear function approximation. Proc ACM Meas Anal Comput Syst. 2022;6(1):1–27. doi:10.1145/3508028.
128. Li Q, Wang Y, Mao H, Yao J, Han Q. Mathematical model and topology evaluation of quantum key distribution network. Opt Express. 2020;28(7):9419–34. doi:10.1364/oe.387697.
129. Reiß S, van Loock P. Deep reinforcement learning for key distribution based on quantum repeaters. Phys Rev A. 2022;108(1):012406. doi:10.1103/physreva.108.012406.
130. Liu ZP, Zhou MG, Liu WB, Li CL, Gu J, Yin HL, et al. Automated machine learning for secure key rate in discrete-modulated continuous-variable quantum key distribution. Opt Express. 2022;30(9):15024–36. doi:10.1364/oe.455762.
131. Mafu M. Advances in AI and machine learning for quantum communication applications. IET Quantum Commun. 2024;5(3):202–31. doi:10.1049/qtc2.12094.
132. Kamil BM. Advanced 6G network protection using quantum key distribution: a systematic review. Babylon J Netw. 2025;2025:80–96. doi:10.58496/bjn/2025/007.
133. Shingne H, Chikmurge D, Parkhi P, Agrawal P. Design of an integrated model using deep reinforcement learning and variational autoencoders for enhanced quantum security. MethodsX. 2025;15(5):103445. doi:10.1016/j.mex.2025.103445.
134. Sharma P, Agrawal A, Bhatia V, Prakash S, Mishra A. Quantum key distribution secured optical networks: a survey. IEEE Open J Commun Soc. 2021;2:2049–83. doi:10.1109/ojcoms.2021.3106659.
135. Nwaga PC, Nwagwughiagwu S. Exploring the significance of quantum cryptography in future network security protocols. World J Adv Res Rev. 2024;24(3):817–33. doi:10.30574/wjarr.2024.24.3.3733.