International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 18(23s) 2026 pp. 460-479

https://doi.org/10.70917/ijcisim-2026-5587
Article

Trends in Quantum Key Distribution Technologies: A Systematic Review of Protocols, Network Architectures, and Deployment Challenges

Anugraha Saji[1] , Anju Pratap[2]

[1]Department of Computer Science and Engineering, Saintgits College of Engineering (Autonomous), Kottayam, Kerala, India.
Email ID: anugraha.se2527@saintgits.org

[2]Department of Computer Science and Engineering, Saintgits College of Engineering (Autonomous), Kottayam, Kerala, India.
Email ID: anju.pratap@saintgits.org

Corresponding Author: Anugraha Saji, Email ID: anugraha.se2527@saintgits.org

Abstract

The emergence of quantum computing technologies poses increasing threats to existing cryptographic algorithms that rely on mathematical hardness, creating a growing demand for quantum-safe communication. Although quantum key distribution can provide secure key establishment under appropriate security assumptions, it faces deployment challenges related to scalability, cost, and interoperability. A systematic review was conducted to examine recent advancements in quantum key distribution technologies by analyzing peer-reviewed studies and classifying them according to protocol design, network architecture, and deployment readiness. The review examined the convergence of quantum key distribution with emerging security applications in fifth-generation networks, Internet of Things environments, edge computing, and fog computing. Through a comprehensive evaluation of protocols and network architectures, this study highlights critical research gaps and provides future directions for the practical deployment of quantum key distribution-enabled secure communication networks.

Keywords: Quantum Key Distribution, Quantum Networks, Quantum Communication, Post-Quantum Cryptography, Quantum Internet

1 Introduction

The rapid development of modern communication infrastructure has significantly increased the demand for securing information exchange against growing cyber threats. The digital ecosystem underpins a wide variety of services, including government operations, financial transactions, industrial automation, healthcare systems, and cloud computing platforms. To ensure the confidentiality, integrity, and authenticity of information, cryptographic mechanisms have become an indispensable component of modern communication systems. For several decades, traditional public-key cryptographic algorithms, including RSA, Elliptic Curve Cryptography (ECC), and Diffie–Hellman key exchange, have been extensively deployed to secure communication systems. However, the efficiency and long-term security of these algorithms are being undermined by emerging quantum computational capabilities. The rapid development of quantum computing is accelerating the transition toward quantum-safe communication technologies on a global scale.



Copyright: © 2026 by the authors

While large-scale fault-tolerant quantum computers are still not commercially available, quantum algorithms such as Shor's algorithm are theoretically capable of efficiently solving integer factorization and discrete logarithm problems, thus presenting a credible long-term threat to modern public-key cryptography standards such as RSA and ECC [1], [2]. This motivates government standardization bodies, research institutions, and industry actors to collaborate on developing cryptographic solutions that adequately safeguard future communication infrastructure against quantum-enabled adversaries. A prominent development in this transition is the standardization of post-quantum cryptography (PQC) by the National Institute of Standards and Technology (NIST). After several years of global scrutiny, NIST finalized standards for lattice-based and hash-based cryptographic algorithms to replace vulnerable public-key protocols in next-generation security infrastructure.

This process has spurred worldwide migration toward quantum-resistant cryptographic implementations in governments, banks, cloud providers, and critical infrastructure. While these techniques are designed to remain secure against classical and quantum attackers under specified computational assumptions, PQC remains based on the hardness of underlying mathematical problems and therefore does not provide information-theoretic security, motivating complementary approaches such as Quantum Key Distribution (QKD), whose security is grounded in quantum mechanics [1].

Alongside PQC frameworks, the international community has also been actively working toward standards for interoperable quantum communication networks [2], [3]. The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) has also initiated standardization activities for quantum communication networks, focusing on QKD network architecture, network interfaces, and operational structures. These joint efforts by international standards bodies demonstrate the importance of standards for advancing quantum communication technologies and integrating them into widespread telecommunication systems. These standards are also relevant to the development of interoperable quantum communication networks and the emerging quantum internet [4]-[6].

Collectively, these factors indicate that the transition to quantum-safe practices is not merely a simple replacement of current ciphers. Rather, it requires an integrated security environment in which post-quantum cryptography, quantum communication networks, international standards, and QKD are incorporated to provide layered protection for future digital infrastructure. This transformation has created a growing demand for scalable, interoperable, and deployment-ready QKD technologies and, as such, has motivated the comprehensive review presented in this study.

QKD has emerged as one of the prominent technologies for secure key establishment. QKD derives its security from fundamental laws of quantum physics and differs in this respect from traditional cryptographic algorithms, whose security depends on the computational complexity of mathematical problems. QKD operates on the basis of quantum phenomena such as the uncertainty principle and the no-cloning theorem, which can make interception or duplication of quantum information detectable under appropriate protocol assumptions. This feature enables legitimate users to detect potential eavesdropping and establish secret keys with information-theoretic security. Owing to these properties, QKD has attracted significant research interest and has evolved into practical communication systems.

The introduction of the BB84 and E91 protocols also contributed to the evolution of QKD, followed by the development of numerous protocols, network architectures, and deployment strategies to improve transmission performance, scalability, and integration with existing communication infrastructure [7]-[10]. However, inherent practical deployment challenges motivated the development of enhanced protocols. The development of QKD technologies has progressed through several stages, reflecting the demand for secure and scalable quantum communication systems. Significant research efforts have focused on Continuous-Variable Quantum Key Distribution (CV-QKD), Measurement-Device-Independent QKD (MDI-QKD), and Twin-Field Quantum Key Distribution (TF-QKD), which aim to enhance key-generation rates, implementation security, and long-distance communication reach. Simultaneously, advances in quantum networking have driven the shift from isolated point-to-point systems toward larger-scale architectures. These developments illustrate the transformation of QKD from a theoretical concept into a promising technology for future secure communication systems.

In recent years, QKD has made substantial progress, leading to the publication of several review articles highlighting different aspects of quantum-secure communication. Existing reviews cover the history of QKD protocols, including Discrete-Variable QKD (DV-QKD), CV-QKD, MDI-QKD, TF-QKD, and Device-Independent QKD (DI-QKD) variants. They have analyzed protocol operation, the mechanisms that provide key security, experimental limitations, and experimental realizations. Other studies focus primarily on QKD networks and communication infrastructure, considering trusted-node systems, satellite-based quantum

communication, quantum-enabled software-defined networking (SDN), hybrid classical-quantum networks, quantum repeaters, and the evolving quantum internet [11]-[13]. Recently, review papers have discussed scalable key-management systems, network interoperability, international standardization, and the integration of QKD with emerging technologies such as 5G/6G networks, Internet of Things (IoT), cloud computing, edge computing, and critical infrastructure protection [2], [13], [14]. Researchers have also examined industrial deployment, commercialization, coexistence of PQC with QKD, artificial-intelligence-assisted quantum communication, integrated photonic technologies, and physical-layer quantum communication techniques [15].

At present, there is a significant gap in the QKD literature. The majority of papers focus exclusively on isolated domains, such as protocol development, network topology, application-oriented solutions, or security proofs, without integrating these intrinsically linked dimensions. Furthermore, as QKD moves from laboratory-scale experiments toward practical communication systems, new challenges arise around scalability, interoperability, standardization, industry adoption, and compatibility with quantum-safe solutions such as PQC. These changes have catalyzed both scholarly work and industrial interest; however, a comprehensive review that synthesizes protocol developments with network structures, deployment-related issues, global standardization activities, implementation readiness levels, and emerging technology trends remains limited.

Consequently, there is a critical need for a review article that not only summarizes recent developments but also critically evaluates unresolved challenges while guiding research toward more scalable, interoperable, and deployable quantum communication systems. Driven by these research gaps, this study aims to present an in-depth review of QKD technologies that encompasses protocol evolution, network architectures, practical deployment challenges, international standardization, and implementation strategies within a unified framework. In addition, the study highlights emerging research trends, identifies key unresolved challenges, and presents future directions toward fully deployed, interoperable, and large-scale quantum communication systems.

The major contributions of this study are summarized as follows:

1. Provides a comprehensive review of recent advancements and developments in QKD technologies, covering foundational protocols as well as contemporary approaches, including CV-QKD, MDI-QKD, TF-QKD, and DI-QKD.
2. Evaluates QKD network architectures and communication infrastructures, including trusted-node networks, satellite-based quantum communication, SDN-enabled QKD, hybrid classical-quantum communication systems, and the emerging quantum internet.
3. Compares QKD deployment models and network architectures by evaluating key-management systems, international standardization initiatives, industrial implementation efforts, deployment challenges, and the integration of QKD with modern communication technologies such as 5G/6G networks, cloud computing, edge computing, and IoT.
4. Identifies and discusses key challenges affecting large-scale QKD deployment, including transmission loss, scalability, interoperability, hardware limitations, security vulnerabilities, implementation complexity, and deployment readiness.
5. Highlights emerging trends and future research directions in quantum-secure communications, including the integration of PQC with QKD, artificial-intelligence-assisted quantum communications, integrated photonic technologies, and next-generation quantum communication infrastructure.

The remainder is organized as follows: Section 2 presents the systematic methodology; Section 3 reviews the evolution and classification of QKD protocols; Section 4 analyzes network architectures and deployment approaches; Section 5 discusses application domains and real-world implementation efforts; Section 6 presents deployment challenges, research gaps, and future directions; and Section 7 concludes the review and highlights the key findings.

2 Systematic Methodology

This study conducted a systematic literature review to critically assess recent developments in QKD. The research focused primarily on the evolution of QKD protocols, network topologies, deployment domains, deployment strategies, and emerging developments in quantum communication technology. Furthermore, the study sought to identify critical research gaps, analyze limitations of contemporary QKD architectures, and propose a viable pathway toward scalable, interoperable, and deployment-ready quantum-secured communication networks.

2.1 Search Strategy

A systematic literature search was conducted through five widely used research databases: IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, and Web of Science. These databases were selected because of their comprehensive coverage of peer-reviewed publications in quantum information science, quantum communications, cryptography, optical communications, and secure networking. Furthermore, citation tracking and backward reference chaining were used to identify additional relevant studies and support comprehensive coverage of the literature.

The search strategy was systematic, employing keyword combinations representative of each core thematic domain. The keywords included "Quantum Key Distribution", "BB84", "E91", "B92", "BBM92", "SARG04", "Continuous-Variable QKD", "Measurement-Device-Independent QKD", "Twin-Field QKD", "Device-Independent QKD", "Satellite QKD", "Quantum Networks", "Quantum Internet", "Quantum Repeaters", "Software-Defined Networking-enabled QKD", "Hybrid Quantum Communication", "Post-Quantum Cryptography", and "Quantum-Safe Communication". Boolean operators (AND, OR) and phrase-based search combinations were utilized to improve search precision and maximize retrieval relevance.

2.2 Selection Criteria

Studies were included if they met the following criteria:

1. Published in peer-reviewed journals or reputable international conference proceedings.
2. Published primarily between 2021 and 2025, with earlier studies retained when essential for foundational, theoretical, or experimental context.
3. Focused on core aspects of QKD, including protocol development, network architectures, deployment strategies, implementation techniques, applications, standardization, or future quantum communication technologies.
4. Provided sufficient theoretical, experimental, or analytical details to support a comprehensive comparative evaluation.
5. Available in full text and published in English.

Studies were excluded if they met any of the following criteria:

1. Duplicate publications.
2. Publications not available in English.
3. Studies not directly related to QKD, including quantum computing or cryptographic topics unrelated to QKD or to QKD-PQC integration.
4. Studies containing insufficient technical or experimental information.
5. Narrative or tutorial reviews lacking a systematic methodology or critical synthesis.
6. Publications before 2021 that were not essential for foundational context.
7. Studies outside the review scope, such as purely theoretical work with no communication relevance or non-communication applications.
8. Editorials, abstracts, theses, patents, non-peer-reviewed reports, or other non-scholarly publications.

2.3 Data Extraction and Study Assessment

The studies were filtered through a multi-phase selection process that included duplicate removal and screening of titles, abstracts, and full-text articles. The screening process was performed in successive stages, beginning with title and abstract screening followed by full-text assessment of potentially relevant studies. Studies were retained only when they satisfied all predefined eligibility criteria and directly contributed to one or more objectives of the review. The studies were qualitatively assessed based on relevance to the review objectives, methodological clarity, originality, experimental or analytical validation, and contribution to the QKD domain.

The studies that were considered relevant were analyzed manually, and their content was systematically collected into a database organized by topics. Following the screening and eligibility assessment, 41 studies were selected for detailed analysis. The parameters recorded from the research works were year of publication, type of publication, QKD protocol, architecture of the network, communication medium, communication distance, key rate, application domain, deployment model, implementation platform, key research contributions, identified limitations, and potential research directions. To enable comparative analysis and identify

contemporary trends in research, the selected studies were classified into six major groups:

1. QKD protocol evolution
2. QKD network architectures
3. Practical implementation and application domains
4. Deployment strategies and industrial initiatives
5. Standardization and interoperability
6. Emerging research directions and future trends

The review used a qualitative study-assessment approach rather than a standardized numerical risk-of-bias instrument. Accordingly, the assessment criteria were used to inform study selection and comparative interpretation, and the resulting synthesis should be interpreted as a structured qualitative review rather than a quantitative meta-analysis. The study selection process is illustrated using the PRISMA diagram in Figure 1 to support transparent reporting of the identification, screening, eligibility assessment, and final inclusion stages.

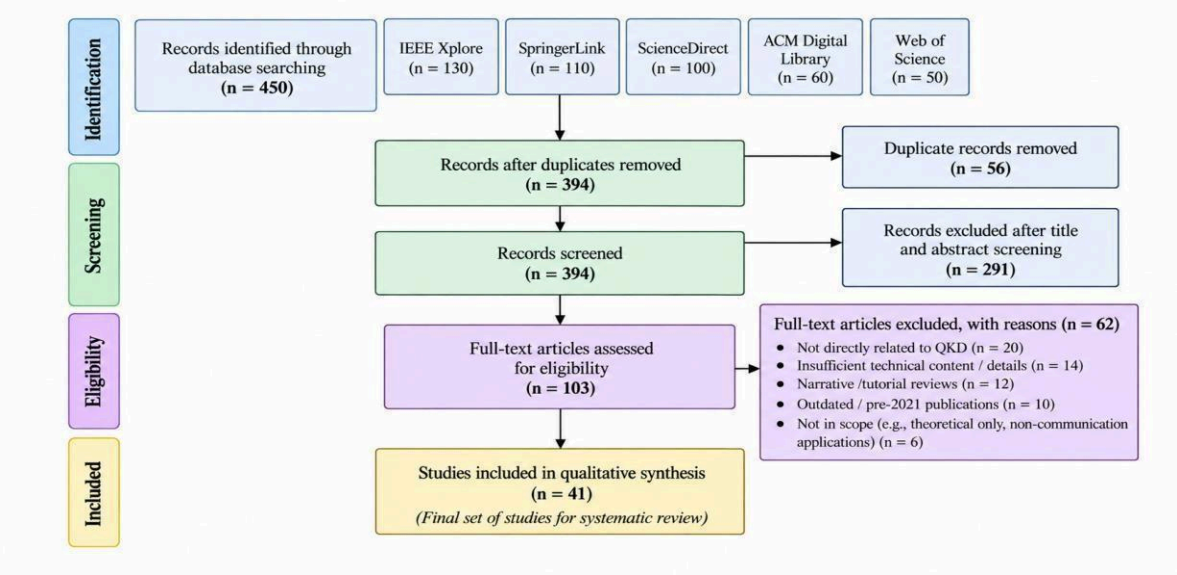


Figure 1. PRISMA study selection process

3 Evolution and Classification of QKD Protocols

The evolution of QKD protocols has been driven by the need to improve communication security, extend transmission distances, simplify practical implementation, and support large-scale adoption. Since the introduction of the BB84 scheme in 1984, QKD has gradually evolved from a theoretical concept into an advanced technology capable of supporting secure communication systems [1]. Unlike public-key cryptography systems whose security relies on the computational complexity of hard mathematical problems, QKD can provide information-theoretic security under appropriate assumptions, including security of the implementation and authenticated classical communication.

The progression of QKD protocols has been driven by efforts to identify and address the limitations of earlier frameworks, as shown in Figure 2. BB84 established the foundation for practical quantum key distribution, while entanglement-based QKD, of which E91 was the first example, later informed device-independent approaches [7], [10]. Later, SARG04 was introduced to improve the security of weak-coherent-pulse implementations against photon-number-splitting attacks [8], [16]. In line with increasing communication requirements, CV-QKD emerged as a promising approach that exploits continuous quadratures of coherent light and can integrate with existing optical communication networks [9], [17]–[19]. MDI-QKD and TF-QKD were subsequently developed to address detector side-channel vulnerabilities and long-distance transmission limitations, respectively [20]-[23]. These developments illustrate the gradual transition of QKD research from theoretical security protocols toward real-world, deployable quantum communication systems that can support future quantum networks.

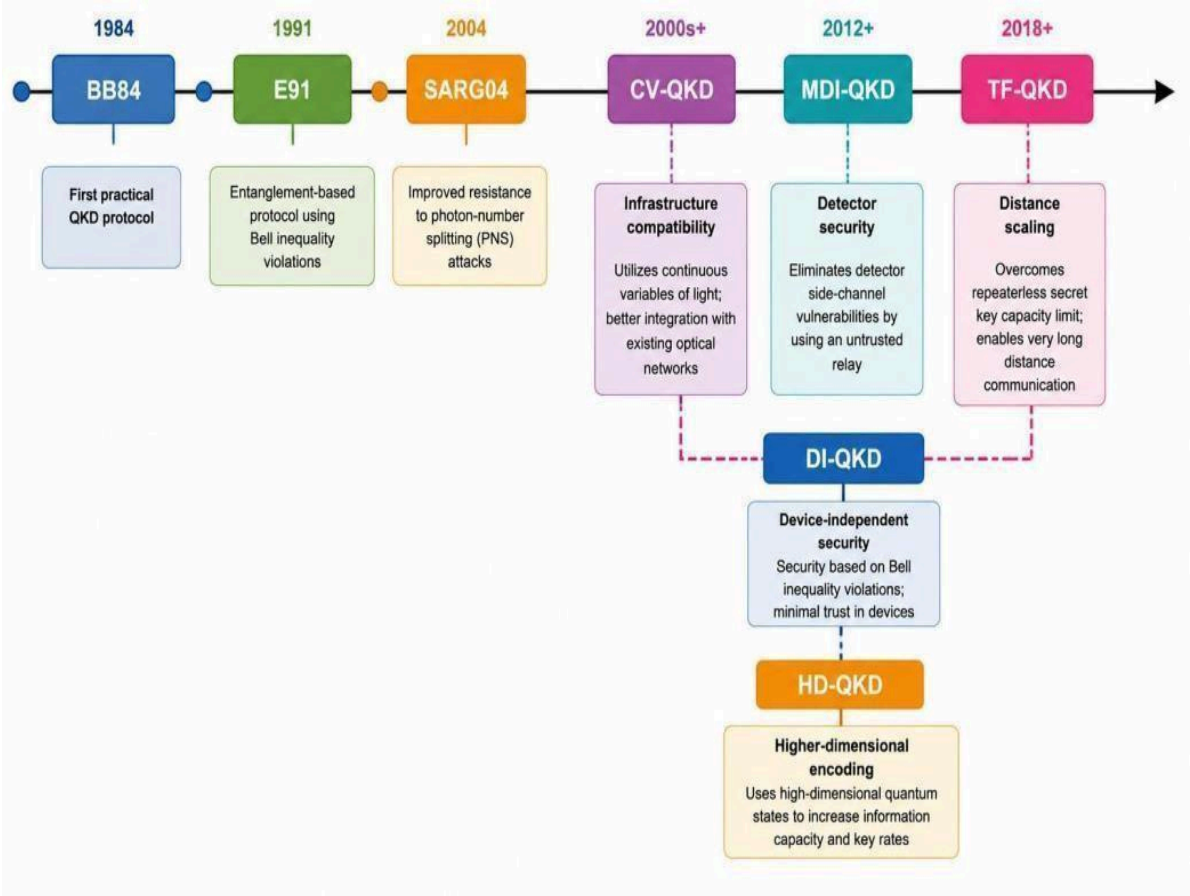


Figure 2. Evolution of QKD protocols and the problems addressed by each generation

3.1 Discrete-Variable QKD Protocols

DV-QKD is an important family of practical QKD protocols and remains one of the most widely studied approaches. In these protocols, quantum information is encoded into discrete quantum states, usually using the polarization or phase of a single photon. Among the many DV-QKD protocols proposed over the past four decades, BB84, E91, and SARG04 have significantly influenced the development of secure quantum communications [1], [7], [8]. Due to its conceptual simplicity, provable security, and successful experimental implementation, BB84 remains one of the most mature QKD protocols. Its performance is limited by transmission losses, non-ideal detectors, and limited communication distance. To strengthen the theoretical security model, quantum entanglement was introduced in the E91 protocol as a foundation for secure key generation [7]. The entanglement-based approach has also been extended to practical intercity implementations that combine precise timing metrology with distributed entangled-photon sources [24].

Security in E91 is associated with the violation of Bell inequalities, which can reveal the presence of an eavesdropper under the protocol assumptions [10]. Entanglement-based systems can provide strong theoretical security guarantees but require more complex quantum sources, tighter synchronization, and advanced entangled-photon generation techniques. The SARG04 protocol was designed as an improvement over BB84 for practical weak-coherent-pulse implementations [8]. Its sifting procedure is modified to improve resilience against photon-number-splitting attacks while remaining compatible with optical communication systems. Compared with BB84, SARG04 introduces more complex post-processing and has seen more limited implementation. Although DV-QKD protocols have reached a certain level of maturity and have been implemented extensively, they are still affected by fundamental issues caused by photon losses, detector imperfections, finite-key effects, and limited communication distances [25]. These problems have led to the development of more advanced QKD protocols capable of offering greater scalability, stronger implementation security, and extended communication distances.

3.2 Advanced QKD Protocols

The drawbacks of traditional DV-QKD protocols have led to the proposal of more sophisticated QKD schemes,

as shown in Figure 3, aiming to enhance practical security, transmission distance, and implementation feasibility. CV-QKD, MDI-QKD, TF-QKD, and DI-QKD represent four important approaches in modern quantum communication. High-dimensional QKD (HD-QKD) uses higher-dimensional quantum states to increase information capacity and can potentially improve key-generation efficiency, although implementation complexity remains a challenge. Unlike DV-QKD, CV-QKD encodes quantum information in continuous quadrature variables corresponding to the phase and amplitude of coherent light [9], [17], [18]. CV-QKD allows the use of telecommunication components that operate on optical-fiber communication infrastructure, which is a primary advantage. Recent experiments have implemented non-Gaussian operations, such as quantum scissors and photon catalysis, that can improve fidelity and transmission distance [19], [26].

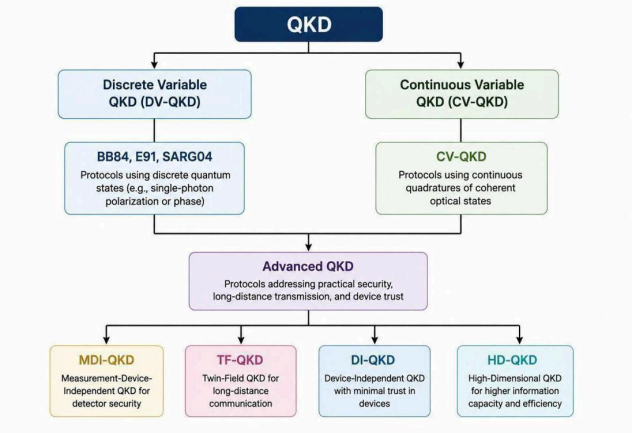


Figure 3. Classification of QKD protocols

CV-QKD implementations are challenging in practice owing to channel noise, detector calibration errors, and finite-size effects. MDI-QKD was proposed to address detector side-channel attacks, which are a major vulnerability in practical QKD implementations [20]-[22]. By moving the measurement operation to an untrusted relay, MDI-QKD removes the need to trust the measurement device while retaining security under the protocol assumptions.

However, MDI-QKD systems still require careful synchronization and high interference visibility and can be operationally sensitive because of their complex architecture. TF-QKD represents a major development in long-distance quantum communication. By utilizing single-photon interference at an intermediate measurement station, TF-QKD can overcome the repeaterless secret-key capacity limit and has been experimentally demonstrated over 830 km of fiber [27] and recently, over 1000 km of fiber [23]. However, practical implementation remains challenging because of strict phase stabilization, synchronization, and calibration requirements. DI-QKD provides a strong device-independent security model by reducing reliance on assumptions about the internal operation of quantum devices. Instead of trusting the quantum devices, this approach derives security from Bell-inequality violations under suitable assumptions, even when measurement devices are untrusted or compromised. Despite current technological limitations, including requirements for high detection efficiencies, low channel losses, and advanced entangled-photon generation, DI-QKD remains significant for practical research and future applications [28], [29]. Altogether, these sophisticated protocols reflect the growing maturity of QKD toward scalable, secure, and deployable quantum communication systems. Although they differ from one another, each protocol addresses specific challenges related to implementation security, integration with classical communications, or system scaling.

3.3 Comparison and Analysis of QKD Protocols

The comparison of modern QKD protocols in Table 1 shows that no protocol simultaneously optimizes communication distance, secret-key generation rate, implementation simplicity, deployment cost, and security robustness.

Table 1. Comparative analysis of QKD protocols

Protocol	Security Strength	Distance Capability	Deployment Maturity	Major Limitation
BB84	High	Medium	Very High	Transmission loss
E91	High	Medium	Medium	Entanglement generation
SARG04	High	Medium	Medium	Limited adoption
CV-QKD	High	Medium–High	Medium	Noise sensitivity
MDI-QKD	Very High	High	Emerging	Implementation complexity
TF-QKD	Very High	Very High	Emerging	Synchronization requirements
DI-QKD	Very High	Limited	Experimental	Detection efficiency
HD-QKD	High	Application-dependent	Emerging	Implementation complexity

BB84 is among the most mature and extensively verified protocols, but its performance is constrained by channel attenuation and hardware imperfections. SARG04 provides improved resilience against photon-number-splitting attacks, while E91 uses quantum entanglement as part of its security model. CV-QKD facilitates compatibility with classical optical infrastructure but remains sensitive to channel conditions. In MDI-QKD, eliminating detector side-channel vulnerabilities improves implementation security, whereas TF-QKD can overcome the repeaterless secret-key capacity limit without quantum repeaters. Finally, DI-QKD offers strong device-independent security guarantees, although its experimental realization remains highly demanding.

Based on these points, it is clear that the choice of a protocol is greatly influenced by the specifications of an application such as communication distance, network architecture, implementation complexity, availability of hardware, level of security, and the deployment environment. As a result, upcoming QKD research should concentrate on developing flexible and scalable protocol configurations capable of supporting diverse quantum communication infrastructures while balancing security, performance, and practical deployability. The development of QKD protocols demonstrates that achieving large-scale quantum-secure communication relies on more than protocol-level innovations. Practical deployment will also require efficient network architectures capable of supporting scalable key distribution, heterogeneous communication environments, interoperability among different quantum communication technologies, and effective resource management. Accordingly, the next section reviews the historical development of QKD network architectures and analyzes their roles in establishing practical quantum communication networks.

4 Network Architectures for QKD

This section compares major QKD network architectures, including point-to-point, trusted-node, SDN-enabled, hybrid classical-quantum, and satellite-based configurations, with emphasis on scalability, interoperability, key management, and deployment requirements.

4.1 Architectural Approaches for QKD Systems

The point-to-point configuration represents the baseline QKD architecture, with a dedicated quantum link connecting two communicating nodes. Due to its relatively small scale and well-developed technology, it provides a good starting point for short-distance metropolitan environments. However, to connect a large number of users, the number of required direct links grows quadratically, resulting in rapidly increasing infrastructure costs. Trusted-node architectures overcome this problem by linking users through a chain of QKD links. The intermediate node creates or receives a key from the network link to the adjacent node, thereby enabling end-to-end secure transmission. Such networks provide a means of extending QKD beyond the range of a single link and represent one of the feasible routes toward large-scale implementation [11], [15]. The intermediate nodes must be trusted because key material is processed and stored at these locations. If a trusted node is compromised, the security of communications relying on that node can be jeopardized. To optimize QKD resource use, multiuser architectures such as qTDM-QKDN (quantum Time-Division Multiplexing QKD

Network) have been proposed [30].

These architectures enable two or more communicating users to share quantum communication resources through time-division-based access. Consequently, the required transceiver hardware for each pair can be reduced, optimizing infrastructure use and deployment cost. As the number of users grows, cooperative scheduling, synchronization, resource allocation, and network management become crucial. SDN-enabled QKD architectures offer an alternative by allowing centralized protocol control to improve network flexibility [31]. Decoupling control functions from the communication infrastructure allows the controller to centrally manage quantum links, provision key-generation resources, and configure the QKD network according to communication traffic. However, implementations of such architectures require interoperable interfaces between standardized QKD hardware, traditional network elements, and the SDN control layer. Key Management System (KMS)-based QKD architectures can complement these network strategies by overseeing the use and handling of keys generated over QKD links [12], [32]. A KMS can facilitate key generation, coordination, storage, retrieval, distribution, and access by upper-layer applications.

4.2 Regional and Global QKD Architectures

Extending QKD to broader communication contexts on regional and global scales presents new challenges. Optical attenuation through fiber channels limits the maximum point-to-point range of fiber-based QKD networks and renders the development of large-scale terrestrial networks more reliant on existing infrastructure. As a result, regional development projects and satellite-based protocols have gained prominence for the expansion of quantum-secure communication over large areas. Regional quantum communication projects, including the European Quantum Communication Infrastructure (EuroQCI) and the Madrid Quantum Communication Infrastructure (MadQCI) [31], highlight the importance of establishing a networked quantum communication ecosystem. The projects emphasize combining QKD with current communication infrastructure and establishing compatible quantum-secure services within networked environments. Both initiatives reflect an initial shift from demonstrating QKD to establishing regional Quantum Communication Infrastructure (QCI).

Satellite-based QKD introduces the prospect of overcoming the distance limitations of a terrestrial fiber network [33], [34]. This is achieved by utilizing free-space optical links between satellites and ground stations. In addition, a satellite architecture has the flexibility to connect physically separated terrestrial QKD networks, not only over long distances but on an intercontinental scale. Satellite-based architectures require technical and operational capabilities such as pointing and tracking, mitigation of atmospheric effects, synchronization, photon-loss management, weather resilience, and appropriate ground-station infrastructure. Consequently, regional and global QKD architectures require more than improvements in quantum key-generation efficiency. They also require efficient control of large-scale networks, standardized interfaces, interoperable equipment, effective key-management mechanisms, and integration of satellite and terrestrial links.

4.3 Quantum Repeater Networks and the Quantum Internet

Trusted-node and satellite-based networks offer practical methods for extending QKD networks, but their scalability depends on infrastructure requirements and the security assumptions associated with trusted nodes. In the longer term, quantum-repeater-based networks may provide a scalable method for extending quantum communication beyond the practical limits of direct transmission. Quantum repeaters seek to establish quantum entanglement across multiple network segments using techniques such as entanglement generation and quantum memory rather than conventional amplification of an unknown quantum state [5], [6].

Quantum repeater network projects are also related to the quantum internet. The quantum internet aims to connect physically distributed quantum devices using quantum communication links and to share quantum information and entanglement across the network [4]-[6], [11]. QKD is one of the anticipated applications of the quantum internet, while future applications include distributed quantum computing, quantum sensing, and secure quantum communication. Transitioning from proof-of-principle demonstrations to deployed infrastructure requires improvements in quantum memories, repeater efficiency, entanglement distribution, multiplexing, synchronization, network control, and quantum-classical interfaces.

Quantum-repeater-based architectures, unlike trusted-node networks, seek to reduce reliance on fully trusted intermediate infrastructure. Experimental quantum repeater networks are currently less mature because of hardware limitations, quantum memory lifetime, entanglement-generation efficiency, fidelity preservation, synchronization, and hardware integration. Therefore, repeater-based QKD and the quantum internet should currently be viewed as directions for future architectural development rather than immediate alternatives to mature trusted-node and terrestrial QKD networks.

4.4 Comparative Analysis and Architectural Trade-offs

Major QKD network architectures address requirements such as scalability, geographical coverage, degree of trust, use of existing infrastructure, and deployment maturity. Point-to-point systems are the simplest and most mature but suffer from limited capacity. Trusted-node networks provide a feasible solution for extending QKD over regional distances, although they require trusted intermediate infrastructure. qTDM-QKDN improves resource sharing among users, while SDN architectures offer greater flexibility through centralized control. KMS-based methods can connect QKD-generated keys to conventional communication infrastructures. Satellite-based QKD provides wider coverage than terrestrial fiber alone. Quantum repeater networks and the quantum internet represent longer-term directions that could enable large-scale quantum connectivity.

Based on the comparison in Table 2, different QKD network architectures may excel in different areas, including scalability, interoperability, cost efficiency, security assumptions, and operational simplicity. Consequently, early-stage network deployment will likely combine terrestrial trusted-node networks, multiuser resource-sharing mechanisms, SDN orchestration, KMS integration, and satellite-based links. As quantum repeaters and the quantum internet advance, architectures that are less dependent on trusted nodes and capable of covering wider geographical ranges may become feasible. From a practical viewpoint, QKD development is therefore not only about improving individual protocols but also about developing interoperable and scalable network architectures. Deployment should ultimately be evaluated in terms of security, infrastructure environment, and application requirements to identify current use cases and future deployment possibilities.

Table 2. Comparative analysis of QKD network architectures

Architecture	Scalability	Coverage	Deployment Cost	Key Advantage	Limitation
Point-to-Point	Low	Local	High	Simple implementation	Poor scalability
Trusted Node	Medium	Regional	Medium	Longer communication range	Security relies on trust assumption
qTDM-QKDN	High	Regional	Low	Resource sharing efficiency	Complicated scheduling
SDN-QKD	High	Regional	Medium	Flexibility and central control	Dependence on controller
Satellite QKD	High	Global	High	Larger coverage	Costly infrastructure
Quantum Repeater	Very High	Extended	Very High	Extends communication beyond repeaterless limits	Quantum memory/Repeater technology immaturity
Quantum Internet	Very High	Global	Very High	Long-term, general-purpose connectivity	Immature infrastructure

5 Practical Applications and Deployment Trends

Progress in QKD technology has gradually expanded its applications from laboratory demonstrations to real-world use cases for secure communications and infrastructure. The essential role of QKD in these settings is to generate shared cryptographic keys through a quantum communication channel without relying on the computational hardness assumptions central to conventional public-key-based key-establishment methods. QKD has attracted increasing attention for sensitive information, critical systems, and long-term secure communications in anticipation of potential threats from future quantum computers.

5.1 Emerging Application Domains

A significant potential application area for QKD is in next-generation networks, including 5G and 6G communication networks. These new communication networks must support sensitive data transmission and inter-network communication, and require a means to establish secure keys [13], [35]. To achieve this, the use

of QKD with other communication and core-network infrastructure, targeted to develop secure keys, is considered a promising approach that has gained worldwide attention. QKD can be combined with current network security mechanisms to offer a second layer of defense against security breaches originating from attacks on current cryptographic key-establishment mechanisms.

For practical use, an integrated QKD-telecom infrastructure must be established. This infrastructure must deliver keys with low latency, manage keys efficiently, operate seamlessly with existing protocol layers, and allocate QKD resources according to the network topology. With the proliferation of IoT devices, edge and fog computing use cases drive an increasing need for secure communications architectures [14], [36]. As the number of devices and locations involved increases, these architectures inherently incorporate interconnected heterogeneous devices with diverse computational capabilities and communication protocols. Traditional security mechanisms are not suited to this complex environment, and QKD may provide a flexible means of establishing secure keys during transmission across nodes capable of supporting quantum communication hardware, such as gateways and edge nodes. Integrating QKD at the level of resource-constrained IoT devices is difficult because of hardware requirements, communication bandwidth, and cost considerations. Therefore, practical implementation of QKD in an IoT environment will most likely take the form of a hybrid network architecture in which keys generated by QKD are stored and distributed by a capable infrastructure node. Beyond communication networks, QKD may have applications for other sectors where long-term privacy of sensitive information is paramount. Financial institutions and healthcare facilities can use quantum-secure key distribution to establish confidentiality of sensitive data and links.

Defense and government communications are among the leading application areas for QKD because of the need to protect sensitive data over long periods. QKD is also being considered for critical infrastructure, such as smart grids and industrial automation, where communication disruption could significantly affect service availability. The reviewed literature indicates that QKD has potential applications across diverse communication environments. Potential application domains identified in the literature include telecommunications, financial systems, healthcare, defense, IoT, edge computing, smart grids, and industrial infrastructure [2], [14]. The suitability of QKD for each domain depends not only on communication distance but also on the required security level, the existing communication network, latency requirements, and, most importantly, whether quantum communication hardware can be physically or logically integrated into current systems [37]. The major application domains are summarized in Figure 4.

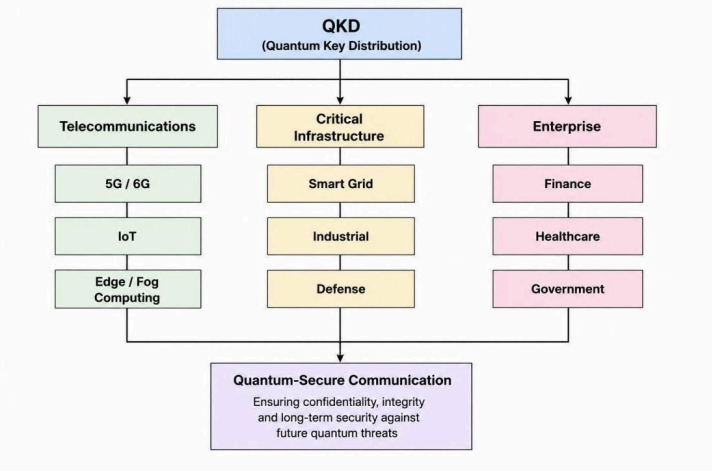


Figure 4. QKD application domains

5.2 Real-World QKD Deployment Initiatives

Recent deployment initiatives demonstrate a gradual movement beyond laboratory validation toward regional, national, and cross-border QKD infrastructure. Such networks not only give a clear picture of how to fit QKD into the existing telecommunication network infrastructure, but also allow the scientific community as well as network operators to assess operational constraints, number of nodes, interoperability, and performance at a realistic scale. Large-scale initiatives such as the Quantum Communication Network – China [38], MadQCI [31], and EuroQCI represent related approaches to building operational quantum communication infrastructures. Ground-based fiber QKD remains a significant option for metropolitan and regional networks because it leverages existing optical communication infrastructure and can provide a stable communication environment.

The backbone attenuation of fiber dictates intrinsic constraints on the maximum length achievable without the installation of intermediate nodes; consequently, this architecture continues to be relevant within existing deployments. Satellite-based QKD can work as a complementary method to overcome the distance limitations of fiber-based, terrestrial QKD networks.

Space-ground configurations can physically interconnect distant ground stations and provide a basis for long-range or even intercontinental quantum links [34]. However, this approach entails additional requirements regarding synchronization, satellite pointing and tracking, atmospheric conditions, transmission losses, ground infrastructure, and operational aspects. Because of this, satellite-based QKD and fiber-based terrestrial solutions should not be seen as competing deployment strategies but as components of a common infrastructure to enable large-scale quantum communication networks [33]. These regional and national initiatives also highlight the increasing relevance of interoperability and integration with current communication systems. The transition from standalone quantum links to systems incorporating key-management systems, classical communication channels, network orchestration, and standard interfaces is becoming increasingly prevalent. This progress suggests that QKD deployment is gradually transitioning from isolated demonstrations toward integrated quantum-secure communication infrastructures [15].

5.3 Deployment Readiness and Critical Assessment

While recent deployment efforts highlight substantial technological advances, widespread commercial adoption of QKD continues to face several interconnected challenges. Infrastructure and hardware costs, particularly for dedicated quantum transmitters, receivers, trusted nodes, and specialized optical devices, remain significant limitations. Reliance on trusted intermediate nodes in many terrestrial schemes introduces additional operational and security considerations. Interoperability among equipment from different vendors, integration with existing telecommunication systems, and the lack of harmonized interfaces and standards may also hinder large-scale deployment. Operational scalability is another significant issue.

A QKD network must generate, store, distribute, and manage keys continuously according to the needs of various applications and users. Therefore, the performance of a practical QKD implementation cannot be judged solely by secret-key rate or transmission distance. It should also account for network operability, key management efficiency, resource utilization, synchronization, maintenance, interoperability, and integration with classical security systems. The deployment initiatives assessed in this study indicate an important shift from experimental QKD links toward more sophisticated and distributed quantum communication network architectures. Terrestrial networks support deployment in urban and regional contexts, while satellites provide broader geographical reach. In parallel, initiatives such as EuroQCI, MadQCI, and other large-scale national quantum communication initiatives indicate increasing recognition of the importance of implementing QKD in operational communication networks. However, the deployment landscape still consists of a mixture of research, government-led, and early industrial deployments rather than globally embedded commercial networks.

Therefore, current QKD technology may be described as mature in some respects but not yet mature as a globally scalable communication service. Additional advances are necessary to make QKD a practical technology for different applications and communication networks, including improvements in key management, interoperability and interface standards, cost, and deployment configurations. These factors also indicate that future QKD use will probably not be a standalone security technology but part of a broader set of quantum-safe technologies that includes PQC. The comparative assessment in Table 3 demonstrates the development of QKD from experimental systems toward large-scale operational quantum communication infrastructures.

Regional and national initiatives have validated the integration of QKD with existing communication networks while supporting secure services for governments, industries, and critical infrastructures. Satellite-based developments have also extended potential communication distances. However, these deployment initiatives continue to face challenges related to infrastructure development, interoperability, standardization, and operational scalability. Furthermore, ongoing research is focusing on improving network integration, reducing deployment costs, and developing efficient key management mechanisms to support practical implementation. Collaboration among research institutions, governments, and industrial stakeholders is also essential for establishing reliable QKD networks and accelerating their adoption across different sectors. These findings indicate that although QKD deployments have reached significant levels of technical maturity, continued advances in both technology and deployment strategies are required for large-scale adoption.

Table 3. Comparative assessment of QKD deployments

Deployment Initiative	Scale	Infrastructure	Primary Application	Strength	Challenge
Quantum Communication Network – China	National	Fiber, Satellite	Critical infrastructure security	Long-distance operation	High infrastructure cost
EuroQCI	Regional	Fiber, Satellite	Cross-border security	Interoperability	Standardization
MadQCI	Regional	Hybrid	Urban quantum infrastructure	Practical validation	Complexity in integration
Space-Ground QKD Networks	Global	Fiber, Satellite	Long-distance secure communication	Global coverage	Satellite deployment cost

6 Discussion: Challenges, Research Gaps, and Future Research Perspectives

Although there has been significant progress in QKD protocols, network architectures, and deployment projects in recent years, a range of technical and operational issues still impede the evolution of QKD toward scalable and commercially feasible quantum-secure communication networks. Based on the papers analyzed, these issues do not stem from a single limitation but rather from the interplay of quantum-channel properties, hardware restrictions, network scalability, interoperability, and deployment factors. At the physical and protocol levels, transmission loss, limited secret-key generation rates, detector imperfections, finite-key effects, channel noise, and synchronization conditions limit QKD performance [1], [17], [19], [25], [39]. The feasible distance and key-generation rate depend strongly on the specific protocol, transmission medium, source characteristics, and receiver technology.

Protocols such as MDI-QKD and TF-QKD can address some distance and security challenges, but at the expense of greater system complexity, including stricter requirements for synchronization, phase stabilization, interference, and calibration [20]-[23]. Hardware and infrastructure requirements are another important barrier. Successful real-world implementation of QKD systems requires additional hardware components such as optical sources, detectors, and quantum communication components alongside classical control infrastructure.

The equipment involved and its associated processing requirements can be costly, particularly when large terrestrial networks and trusted intermediate stations are involved. These challenges are further amplified when QKD is deployed in complex heterogeneous networks spanning metropolitan areas, longer fiber links, satellite systems, and telecommunications environments. Network-level challenges include scalability, interoperability, key management, and the presence of trusted nodes [11], [12], [30], [33]. Key management across multiple users in a large-scale QKD network must ensure sufficient key availability for each user while maintaining network performance.

Interoperability and compatibility among QKD systems supplied by different vendors, as well as integration of QKD with existing conventional communication networks, must be addressed for large-scale deployment. In current terrestrial QKD networks, reliance on trusted intermediate nodes can impose additional physical and operational security restrictions. Standardization and common interfaces are crucial for enabling heterogeneous QKD components to operate as a coherent communication infrastructure, network, or ecosystem [12], [31]-[33].

6.1 Research Gaps and Open Issues

The systematic review of the selected literature reveals that the field of QKD has matured significantly; however, research gaps remain across protocol performance, network scalability, deployment preparedness, and system integration. Most of the studied literature focuses on solutions that optimize individual metrics, including transmission distance, security, key-generation efficiency, detector side-channel countermeasures, or network infrastructure dimensioning, with relatively few comparative studies considering these parameters together under realistic large-scale deployment conditions [1], [2], [4], [7]-[13], [15]. This presents a research gap in understanding how improvements observed at the protocol or experimental level translate into operational quantum communication network infrastructure. Another notable shortfall is the lack of comprehensive long-term, large-scale performance assessments [12], [15], [31], [38].

While regional and national QKD programs have explored the practicality of establishing quantum networks in

real-world settings, most tested systems remain at pilot scale or function as experimental testbeds. More in-depth assessment is needed to evaluate robustness, maintenance requirements, key availability, operating costs, network expansion potential, and performance under heavy traffic loads during long-term operation. Interoperability also remains insufficiently explored. More diverse protocols, transmission media, hardware platforms, network architectures, and key-management schemes are expected in the next generation of QKD networks. However, interactions among these diverse components are difficult to manage. Standardized interfaces, effective network-management mechanisms, and interoperable key-management schemes must be established to prevent the isolation of individual QKD networks.

Another significant gap concerns the combination of QKD with other quantum-safe solutions. While research on hybrid QKD-PQC solutions is growing, substantial work remains necessary on practical implementation approaches, system trade-offs, key-management systems, and interworking concerns [2], [3]. The integration of QKD with SDN, intelligent network management, edge computing, and automated resource management remains at an early stage, and few studies evaluate full end-to-end quantum-secure communication systems rather than individual QKD nodes [6], [29]. These gaps indicate that future work needs to focus on integrating individual QKD components into long-term system architectures rather than optimizing isolated components.

6.2 Limitations of the Review

Defense and government communications are among the leading application areas for QKD because of the need to protect sensitive data over long periods. QKD is also being considered for critical infrastructure, such as smart grids and industrial automation, where communication disruption could significantly affect service availability. The reviewed literature indicates that QKD has potential applications across diverse communication environments. Potential application domains identified in the literature include telecommunications, financial systems, healthcare, defense, IoT, edge computing, smart grids, and industrial infrastructure [2], [14]. The suitability of QKD for each domain depends not only on communication distance but also on the required security level, the existing communication network, latency requirements, and, most importantly, whether quantum communication hardware can be physically or logically integrated into current systems [37]. The major application domains are summarized in Figure 4.

In addition, the review did not employ a standardized numerical risk-of-bias instrument. These limitations may affect the generalizability and comparability of the synthesized findings and should be considered when interpreting the comparative assessments and identified research gaps.

6.3 Future Research Directions

The reviewed studies collectively suggest that future QKD research should shift from isolated protocol optimization toward integrated communication architectures that jointly address scalability, key management, interoperability, and deployment constraints. Instead of optimizing protocols in isolation, future initiatives should focus on designing comprehensive QKD communication systems. This requires considering protocol selection, network architecture, key management, infrastructure security, and application layers simultaneously to adapt to heterogeneous deployment environments and diverse application requirements.

Extending communication distance remains a critical research frontier. Substantial progress is needed in the development of quantum repeaters, quantum memories, entanglement distribution, repeater-based network architectures, and decoherence-mitigation strategies to overcome the fundamental physical constraints currently limiting direct quantum transmission [4]-[6], [40]. While long-term evolution toward a full quantum internet is underway, significant technological hurdles may delay the realization of global quantum communication networks. Hybrid quantum-safe security is another vital direction: integrating QKD and PQC can provide complementary security properties by combining the physical security derived from quantum-mechanical principles with the computational security provided by modern cryptography [3].

Further investigations should focus on practical hybrid architectures, robust key-establishment mechanisms, cryptographic agility, performance-overhead mitigation, and migration pathways to achieve seamless integration of QKD and PQC into existing communication infrastructures. Another avenue for enhancing QKD network management involves leveraging emerging technologies such as SDN [31]. AI-based frameworks can optimize traffic prediction, anomaly detection, and resource allocation to enable dynamic, adaptive systems, while SDN paradigms allow programmable and flexible management of coexisting quantum and classical network resources [41].

In addition, future QKD networks will require standardized interfaces, interoperable hardware devices, standardized key-management protocols, and compatibility with current telecommunication standards. Concurrently, commercialization of affordable quantum hardware and integrated photonic technologies could

reduce the physical footprint and deployment costs of QKD systems [29]. Finally, extensive field trials and long-term operational experiments are required to rigorously validate the reliability, scalability, cost-effectiveness, and real-world security of these systems [31], [38]. Broadly, these directions suggest that the future progression of QKD will be driven by the need for manageable, cost-effective, and application-aware quantum-secure communication infrastructure that prioritizes interoperability rather than focusing solely on independent improvements to key-generation rates or transmission distances.

7 Conclusion

This systematic literature review summarizes the evolution and trends in QKD, tracking progress from foundational protocols to modern quantum communication technologies and emerging practical deployment environments. The review covers advancements in discrete-variable and advanced QKD protocols, the evolution of network architectures, real-world deployment use cases across various regions and countries, and a critical analysis of the technical and operational challenges encountered during scale-up [34], [38]. The evidence demonstrates that QKD has progressed beyond purely theoretical and laboratory initiatives, with experimental testing and pilot deployments becoming increasingly prevalent across terrestrial, satellite-based, and next-generation quantum network testbeds.

However, the study also reveals that considerable hurdles remain before QKD can be widely adopted as a practical, deployable, and cost-effective security technology. Key barriers include transmission loss, limited key-generation rates, hardware constraints, scalability limitations, interoperability issues, reliance on trusted entities, operational complexity, and a lack of unified industry standards [15], [28], [32]. Based on the literature reviewed, no single QKD protocol or network architecture simultaneously optimizes transmission distance, security, deployment cost, scalability, and technological maturity.

Consequently, future QKD infrastructures will likely depend on a pragmatic combination of diverse protocols, hardware configurations, network architectures, trusted-node topologies, key-management systems, and standardized application interfaces. The review further emphasizes the need to integrate QKD with complementary technologies, including PQC, SDN, quantum repeaters, quantum memories, and intelligent network-management frameworks [3], [6], [28], [31]. Developing these hybrid and interoperable paradigms will be essential for transitioning from isolated QKD links into heterogeneous, large-scale quantum-secure communication networks.

Large-scale field trials, interoperable standards, lower-cost quantum hardware, and long-term operational evaluations remain necessary before QKD can become a broadly deployable security service. In summary, the evolution of QKD is undergoing a paradigm shift from an exclusive focus on isolated protocols toward the engineering of networked, integrated, and deployment-oriented quantum communication infrastructures. The future trajectory of this field will be shaped by interdisciplinary efforts spanning quantum information science, optical communication engineering, cybersecurity, networking, and international standardization bodies. Through these collaborative efforts, researchers and engineers can establish the technological building blocks necessary to develop resilient, large-scale quantum-secure architectures for future global information infrastructures.

Acknowledgment

The authors would like to express their sincere gratitude to Saintgits College of Engineering (Autonomous), Kottayam, Kerala, India, for providing the academic environment, facilities, and support necessary to carry out this systematic review. The authors also acknowledge the support and encouragement received from the Department of Computer Science and Engineering throughout this work. The authors would also like to acknowledge the researchers and scholarly communities whose published work provided the foundation for this systematic review.

References

[1] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realistic devices,” *Rev. Mod. Phys.*, vol. 92, no. 2, p. 025002, 2020, doi: 10.1103/RevModPhys.92.025002.

[2] D.-E. Shahwar, M. Imran, A. B. Altamimi, W. Khan, S. Hussain, and M. Alsaffar, “Quantum cryptography for future networks security: A systematic review,” *IEEE Access*, vol. 12, pp. 180048–180078, 2024, doi: 10.1109/ACCESS.2024.3504815.

[3] S. S. Vellela *et al.*, “Quantum cryptography and key distribution for secure communication in the

post-quantum world," in *Proc. Int. Conf. Sustainable Communication Networks and Application (ICSCN)*, 2025, pp. 619–624, doi: 10.1109/ICSCN67106.2025.11308316.

[4] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini, "Quantum Internet—applications, functionalities, enabling technologies, challenges, and research directions," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2218–2247, 2021, doi: 10.1109/COMST.2021.3109944.

[5] K. Goodenough, D. Elkouss, and S. Wehner, "Optimizing repeater schemes for the quantum internet," *Phys. Rev. A*, vol. 103, no. 3, p. 032610, 2021, doi: 10.1103/PhysRevA.103.032610.

[6] S. Haldar, P. J. Barge, S. Khatri, and H. Lee, "Fast and reliable entanglement distribution with quantum repeaters: Principles for improving protocols using reinforcement learning," *Phys. Rev. Applied*, vol. 21, no. 2, p. 024041, 2024, doi: 10.1103/PhysRevApplied.21.024041.

[7] I. W. Primaatmaja, K. T. Goh, E. Y.-Z. Tan, J.-T. F. Khoo, S. Ghorai, and C. C.-W. Lim, "Security of device-independent quantum key distribution protocols: A review," *Quantum*, vol. 7, Art. no. 932, 2023, doi: 10.22331/q-2023-03-02-932.

[8] A. A. Abushgra, "Variations of QKD protocols based on conventional system measurements: A literature review," *Cryptography*, vol. 6, no. 1, Art. no. 12, 2022, doi: 10.3390/cryptography6010012.

[9] S. Yang *et al.*, "Information reconciliation of continuous-variables quantum key distribution: Principles, implementations and applications," *EPJ Quantum Technol.*, vol. 10, Art. no. 40, 2023, doi: 10.1140/epjqt/s40507-023-00197-8.

[10] V. Zapatero *et al.*, "Advances in device-independent quantum key distribution," *npj Quantum Inf.*, vol. 9, Art. no. 10, 2023, doi: 10.1038/s41534-023-00684-x.

[11] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the Qinternet," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, 2022, doi: 10.1109/COMST.2022.3144219.

[12] E. Dervisevic *et al.*, "Quantum key distribution networks—key management: A survey," *ACM Comput. Surv.*, vol. 57, no. 10, Art. no. 257, pp. 1–36, 2025, doi: 10.1145/3730575.

[13] M. Mehic *et al.*, "Quantum cryptography in 5G networks: A comprehensive overview," *IEEE Commun. Surveys Tuts.*, vol. 26, no. 1, pp. 302–346, 2024, doi: 10.1109/COMST.2023.3309051.

[14] G. D. Makkar and S. Pant, "Quantum cryptography for securing the Internet of Things: A comprehensive literature survey," in *Proc. 5th Int. Conf. Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Dehradun, India, 2025, Art. no. 11402714, doi: 10.1109/IOT-SIU65919.2025.11402714.

[15] R. Liu, G. G. Rozenman, N. K. Kundu, D. Chandra, and D. De, "Towards the industrialisation of quantum key distribution in communication networks: A short survey," *IET Quantum Commun.*, vol. 3, no. 3, pp. 151–163, 2022, doi: 10.1049/qtc2.12044.

[16] C. Sekga and M. Mafu, "Security of quantum-key-distribution protocol by using the post-selection technique," *Phys. Open*, vol. 7, Art. no. 100075, 2021, doi: 10.1016/j.physo.2021.100075.

[17] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future," *Appl. Phys. Rev.*, vol. 11, no. 1, Art. no. 011318, 2024, doi: 10.1063/5.0179566.

[18] V. L. da Silva, M. A. Dias, N. A. F. Neto, and A. B. Tacla, "From coherent communications to quantum security: Modern techniques in CV-QKD," in *Proc. 2024 SBFoton International Optics and Photonics Conference (SBFoton IOPC)*, 2024, pp. 1–5, doi: 10.1109/SBFotonIOPC62248.2024.10813518.

[19] Y. Zhang *et al.*, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Phys. Rev. Lett.*, vol. 125, no. 1, p. 010502, 2020, doi: 10.1103/PhysRevLett.125.010502.

[20] M. A. C. T. Ribeiro, A. B. Tacla, F. de Melo, and R. O. Vallejos, "A comparative review between measurement-device-independent QKD protocols," in *Proc. XI Int. Symp. Innovation and Technology (SIINTEC)*, Salvador, Brazil, 2025. [Online]. https://doity.com.br/anais/senaicimatec/trabalho/473609 .

[21] Y. Cao *et al.*, "Long-distance free-space measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 125, no. 26, p. 260503, 2020, doi: 10.1103/PhysRevLett.125.260503.

[22] M. Sun, C.-H. Zhang, H.-J. Ding, X.-Y. Zhou, J. Li, and Q. Wang, "Practical decoy-state memory-assisted measurement-device-independent quantum key distribution," *Phys. Rev. Applied*, vol. 20, no. 2, p. 024029, 2023, doi: 10.1103/PhysRevApplied.20.024029.

[23] Y. Liu *et al.*, "Experimental twin-field quantum key distribution over 1000 km fiber distance," *Phys. Rev. Lett.*, vol. 130, no. 21, p. 210801, 2023, doi: 10.1103/PhysRevLett.130.210801.

[24] A. Hreibi, A.-K. Kniggendorf, A. Kuhl, J. Kronjäger, H. Schnatz, and S. Kück, "Entanglement-based intercity quantum key distribution: Metrology and implementation," *Meas.: Sens.*, vol. 38, Art. no. 101777, 2025, doi: 10.1016/j.measen.2024.101777.

[25] M. Rahmanpour, A. Erfanian, A. Afifi, M. Khaje, and M. H. Fahimifar, "A new quantum key distribution

protocol to reduce afterpulse and dark counts effects," *Results Optics*, vol. 16, Art. no. 100718, 2024, doi: 10.1016/j.rio.2024.100718.

[26] K. Jafari, M. Golshani, and A. Bahrampour, "Long-distance high-fidelity continuous-variable quantum key distribution with non-Gaussian operations: An exact closed form solution," *Results Phys.*, vol. 56, Art. no. 107276, 2024, doi: 10.1016/j.rinp.2023.107276.

[27] S. Wang *et al.*, "Twin-field quantum key distribution over 830-km fibre," *Nature Photon.*, vol. 16, pp. 154–161, 2022, doi: 10.1038/s41566-021-00928-2.

[28] W. Luo *et al.*, "Recent progress in quantum photonic chips for quantum communication and internet," *Light Sci. Appl.*, vol. 12, Art. no. 175, 2023, doi: 10.1038/s41377-023-01173-8.

[29] M. Zahidy *et al.*, "Quantum key distribution using deterministic single-photon sources over a field-installed fibre link," *npj Quantum Inf.*, vol. 10, Art. no. 2, 2024, doi: 10.1038/s41534-023-00800-x.

[30] J. C. Hernandez-Hernandez *et al.*, "Designing optimal quantum key distribution networks based on time-division multiplexing of QKD transceivers: qTDM-QKDN," *Future Gener. Comput. Syst.*, vol. 164, Art. no. 107557, 2025, doi: 10.1016/j.future.2024.107557.

[31] V. Martin *et al.*, "MadQCI: A heterogeneous and scalable SDN-QKD network deployed in production facilities," *npj Quantum Inf.*, vol. 10, Art. no. 80, 2024, doi: 10.1038/s41534-024-00873-2.

[32] P. James, S. Laschet, S. Ramacher, and L. Torresetti, "Key management systems for large-scale quantum key distribution networks," in *Proc. 18th Int. Conf. Availability, Reliability and Security (ARES)*, Benevento, Italy, 2023, pp. 1–9, doi: 10.1145/3600160.3605050.

[33] W. Jiang, Y. Zhang, H. Han, and J. Mu, "Quantum communication in self-organizing satellite networks: Challenges and opportunities," *IEEE Commun. Standards Mag.*, vol. 9, no. 3, pp. 15–25, 2025, doi: 10.1109/MCOMSTD.2025.3578320.

[34] Y.-A. Chen *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, pp. 214–219, 2021, doi: 10.1038/s41586-020-03093-8.

[35] A. Atutxa, A. Sanz, J. Sasiain, J. Astorga, and E. Jacob, "Towards a quantum-safe 5G: Quantum key distribution in core networks," *Comput. Commun.*, vol. 224, pp. 145–158, 2024, doi: 10.1016/j.comcom.2024.06.005.

[36] S. Y. Moon, B. H. Jo, A. E. Azzaoui, S. K. Singh, and J. H. Park, "Edge-Fog enhanced post-quantum network security: Applications, challenges and solutions," *Comput. Mater. Continua*, vol. 84, no. 1, pp. 25–55, 2025, doi: 10.32604/cmc.2025.062966.

[37] M. R. I. Rifat, M. M. Rahman, M. A. K. Nayon, M. S. Azad, and M. R. C. Mahdy, "QSAC: Quantum-assisted secure audio communication using quantum entanglement, audio steganography, and classical encryption," *Eng. Sci. Technol., Int. J.*, vol. 70, Art. no. 102167, 2025, doi: 10.1016/j.jestch.2025.102167.

[38] H.-Z. Chen *et al.*, "Implementation of carrier-grade quantum communication networks over 10000 km," *npj Quantum Inf.*, vol. 11, Art. no. 137, 2025, doi: 10.1038/s41534-025-01089-8.

[39] M. Mafu, C. Sekga, and M. Senekane, "Security of Bennett–Brassard 1984 quantum-key distribution under a collective-rotation noise channel," *Photonics*, vol. 9, no. 12, Art. no. 941, 2022, doi: 10.3390/photonics9120941.

[40] M. A. Khan, S. Ghafoor, S. M. H. Zaidi, H. Khan, and A. Ahmad, "From quantum communication fundamentals to decoherence mitigation strategies: Addressing global quantum network challenges and projected applications," *Heliyon*, vol. 10, no. 14, Art. no. e34331, 2024, doi: 10.1016/j.heliyon.2024.e34331.

[41] P. Sharma, S. Gupta, V. Bhatia, and S. Prakash, "Deep reinforcement learning-based routing and resource assignment in quantum key distribution-secured optical networks," *IET Quantum Comput.*, vol. 4, no. 3, pp. 136–145, doi: 10.1049/qtc2.12063.