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 the Quantum computing technologies is imposing greater threats on the existing cryptographic algorithms that rely heavily on the mathematical problems, creating a growing demand for quantum safe Communication. Even though Quantum Key Distribution (QKD) is a theoretically proven secure key exchange method against quantum attacks, it also faces several deployment challenges like scalability, cost, and interoperability limitations. A systematic review was conducted to examine the recent advancements in QKD technologies by analyzing the peer reviewed studies Published between 2021 to 2025 and classified according to protocol design, network architecture and deployment readiness. The review analyzed articles for a Comparison of the recent advancements in the field of Twin Field QKD, Continuous Variable QKD, Hybrid classical quantum networks and long-distance secure communication systems. Furthermore, the review also examined the Conjunction of QKD with the emerging security applications of 5G Networks, IOT environments, edge computing, fog Computing and Multimedia security systems. Despite of the significant technological advancements, the deployment of QKD is still under the constraints of scalability, lower key generation rates, cost of deployment, Synchronization issues, stability complexities, interoperability problems and standardization issues. Through a comprehensive evaluation of QKD protocols and network architectures, this study highlights the critical research gaps and provides future directions for the practical deployment of the QKD enabled secure communication networks.

Keywords: NA

1. Introduction

The rapid development of the modern Communication infrastructure has significantly increased the demand for securing information exchange against increasingly sophisticated cyber threats. The digital ecosystem underpins a wide variety of services including government operations, financial transactions, industrial automation, health care systems, and cloud computing platforms. To ensure confidentiality, integrity, and authenticity of the information, cryptographic mechanisms have become an unavoidable component of modem 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 serve the Communication system. However, the efficiency and long-term security of these algorithms are being challenged by the emerging quantum computational paradigms.

Copyright: © 2026 by the authors

The rapid development of quantum computing is leading to an increased pace of the transition to quantum-safe communication technologies on a global scale. 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 challenges, thus presenting a credible long-term threat to modern public-key cryptography standards like RSA and ECC [1],[2]. This motivates government standardization bodies, research institutions, and industry actors to jointly work towards developing cryptography solutions that adequately safeguard future communication infrastructure from quantum-enabled adversaries. Perhaps the most prominent achievement 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, the NIST approved lattice-based and hash-based cryptographic algorithms to replace the vulnerable public-key protocols in next-generation security infrastructures.

This process has spurred a rapid, worldwide migration to quantum-resistant cryptographic implementations in governments, banks, cloud providers, and critical infrastructures. While all these techniques are designed to be secure against classical and quantum attackers within polynomial time computational resources, the security of PQC still remains based on the hardness of the underlying mathematical problems which researchers have recognized not to afford information-theoretic security, motivating additional methods like QKD to be supported by the theory of quantum mechanics[1]. Alongside the standards for PQC, the international community has also been actively working towards the development of standards for interoperable quantum communication networks [2], [3]. The European Telecommunications Standards Institute (ETSI) has been the key organization, working on standards for the design and analysis of practical QKD systems, from technical specifications and reference architecture to security requirements, interoperability and network requirements. These standards seek to facilitate the introduction of QKD into existing telecommunication networks while also providing support for vendor interoperability and large-scale deployment.

The International Telecommunication Union Telecommunication Standardization Sector has also launched activity on standards for quantum communication networks, which work on the architecture of QKD networks, network interfaces and operational structure. This joint effort by both EU and international standard bodies demonstrates the importance of standards for the advancement of quantum communication techniques and integrating them into widespread telecommunication systems. Another significant motivation for research on recent QKD systems is the rise of quantum internet. Different from the classical internet, the goal of the quantum internet is to implement quantum information transmission among geographically separated quantum devices over quantum networks for various applications such as distributed quantum computing, quantum sensing communication and quantum cloud [4], [5], [6]. QKD has been recognized as one of the first practical applications in the new era of quantum internet, with continued research on quantum repeaters, quantum memories, quantum network and quantum internet, we could see a transition from the isolated point-to-point QKD to the single-link to global interconnected quantum network. Collectively, these factors have pointed out that shifting to quantum-safe global practices are compatible with a simple replacement of current ciphers. Rather, it is essentially providing an integrated security environment where post-quantum cryptography, quantum communication networks, standards at the international level, and QKD are incorporated to offer strong layers of protection to future digital infrastructures. This transformation has created a new demand for research on scalable, interoperable, and deployment-ready QKD technologies and, as such, has driven the comprehensive review presented in this paper.

QKD has emerged as one of the most promising technologies for secure key establishments. QKD derives its security from the fundamental laws of quantum physics and differs in this aspect with the traditional cryptographic algorithms, whose security depends on the computational complexity of mathematical problems. QKD operates on the basis of the quantum phenomena like the uncertainty principle, and the non-cloning theorem, which prevents any attempt to intercept or duplicate quantum information by introducing detectable disturbances. This unique feature enables the legitimate users to identify the eavesdropper's presence and to establish secret keys information theoretic security. owing to these unique properties QKD has attracted significant research interest and has got evolved to practical Communication systems. The introduction of the BB84 and E91 protocols also helped in the significant

evolving of the QKD, and the development of numerous protocols, network architectures and deployment Strategies to improve the transmission performance, deployment scalability and integration with existing Communication infrastructures [7], [8]–[9], [10].

The progression of the development of the QKD technologies is through several stages, reflecting the demand for secure and scalable quantum communication Systems. Since the introduction of the pioneering BB84 and E91 protocols established the theoretical foundations of quantum secure key exchange and demonstrating the feasibility of exploiting quantum mechanical properties for cryptographic applications. However, practical deployment challenges motivated the development of enhanced protocols. Significant research efforts have focused on Continuous Variable QKD (CV-QKD), Measurement -Device Independent QKD, and Twin Field QKD, which eventually aims for key generation performance, resistance to attacks and long-distance communication activities. Simultaneously, advancements in quantum computing also witnesses the shift from isolated point-to-point systems to large scale architectures. These collective developments illustrate the transformation of QKD from a theoretical concept to a promising technology for future secure communication systems.

Recent years, QKD has made great strides in development which has caused to produce several review articles, highlighting different characteristics of quantum-secure communications. The reviews available cover the history of QKD protocols, namely discrete-variable (DV), continuous-variable (CV), measurement-device-independent, twin-field, device-independent QKD. They have analyzed the working, described the mechanisms that make the keys secure, discussed the limitations that have to be resolved experimentally, and the ways that they were realized. Sometimes other works mainly focus on QKD network and communication infrastructures: they consider trusted-node systems, quantum communication assisted by satellite, quantum-enabled software-defined networking, hybrid classical quantum networks, quantum repeaters, and the developing quantum internet [11]- [13]. Recently, a number of 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 started to pay much attention to other aspects like industrial deployment, commercialization, coexisting deployment of Post-Quantum Cryptography (PQC) with QKD, artificial intelligence assisted quantum communications, integrated photonic chip technologies, and physical-layer quantum communication techniques [15]. These collectively shows that the quantum communication research is difficult to find the review papers covering all these topics, because most of the researchers focus upon only one aspect like protocol development, network architectures, application domains, or deployment strategies. With the emergence of QKD being transitioned from laboratory experiments to deployment-ready communication infrastructures, it has become increasingly important to do the synthesis of these different research areas. This paper aims to respond to such a demand by offering a multidisciplinary overview of QKD technologies, through the study of protocol development, network architectures, challenges in real-world deployment, standardization efforts, implementation tendencies, and research trends pointing toward the future all taken under the structure of unified perspective [1], [4], [7]-[13], [15].

At present, there is a big gap in QKD literature. Majority of the papers just dive straight into their own research topic like developing new protocols, creating network topology, application-oriented solutions, or security proofs without linking all these parts together that are deeply entwined. And, with QKD now rapidly moving from lab-scale experiments to actual deployed communication systems, we face a whole new wave of problems around scalability interoperability, standardization, industry adoption, and compatibility with new quantum-safe solutions such as Post-Quantum Cryptography (PQC). These changes are really encouraging both scholarly work and industrial interest but looks like there does not exist yet a single thorough review paper which connects protocol upgrades with network structures, deployment-related issues, global standardization activities, level of implementation readiness, and upcoming technology trends. So, there is a greater need for a single review article that can summarize the most recent breakthroughs in the field, and on the other side, be a thought-provoking piece of work which can expose the existing problems and the unresolved needs of this area while guiding the research toward more scalable, interoperable, and deployable quantum communication systems.

Driven by these research gaps, our paper is aimed at presenting an in-depth review of QKD technologies that encompasses protocol evolution, network architectures, practical deployment challenges, international standardization, and implementation strategies all within one single setup. In addition, the study also highlights the most promising emerging research trends, pointing out key challenges that remain unsolved, and presents visions for the future that would lead to fully deployed and interoperable quantum communication systems on a larger scale.

The major contributions of this study are summarized as follows:

1. A comprehensive review on the recent advancements and developments in the QKD technologies covering foundational protocols as well as contemporary advancements, including Continuous-Variable (CV), Measurement-Device-Independent (MDI), Twin-Field (TF), and Device-Independent (DI) QKD.
2. Presents a detailed evaluation of QKD network architectures and communication infrastructures, including trusted-node networks, satellite-assisted quantum communication, Software-Defined Networking (SDN)-enabled QKD, hybrid classical–quantum communication systems, and the emerging Quantum Internet.
3. Compared and examined various QKD Deployment models and network architectures by examining 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 the Internet of Things (IoT).
4. Identified and discussed the key challenges affecting the large-scale deployment including transmission loss, scalability, interoperability, hardware limitations, security vulnerabilities, implementation complexity, and deployment readiness.
5. Highlighted the emerging trends and future research directions in quantum secure communications and integration of Post-Quantum Cryptography (PQC) with QKD, artificial intelligence-assisted quantum communications, integrated photonic technologies, and next-generation quantum communication infrastructures.

The remainder of this paper is outlined as follows: Section I presents the Systematic methodology, Section III reviews the evolution and classification of QKD protocols, Section IV analyses the network architectures and deployment approaches. Section V discusses the application domains and efforts for real-world implementation. Section VI presents deployment challenges, research gaps, and future directions. Finally, section VII concludes the review and highlights the key findings.

2. Systematic Methodology

This study carries out a systematic literature review to gain insights into and critically appraise the developments in QKD over the past few years. The research is mainly focused on how the quantum key distribution protocols have changed over time, network layout, actual deployment fields, strategies for deployment, and novel developments in quantum communication technology. Apart from this, the paper also seeks to find research areas where more studies and exploration are needed, to analyze limitations which are common with today's QKD systems and at the same time point out the potential ways in which one can work towards making available scalable, interoperable and deployment-ready quantum secured communication networks.

2.1 Search Strategy

An in-depth search was made of scientific papers through five widely used research databases: IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, and Web of Science. The selection of these databases was due to their wide range of top-quality peer-reviewed publications on quantum information science, quantum communications and cryptography as well as optical communications and secure networking. To capture the latest and most impactful work, citation tracking as well as backward reference search were also used to pinpoint any additional relevant materials.

The search method was systematic and it relied on the use of combinations of keywords that were representative of each main topic covered here. 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 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

To select quality work that is current and relevant, the articles are included if they:

1. Published in peer-reviewed journals or reputable international conference proceedings.
2. Primarily published between 2021 and 2026, while including seminal publications of historical significance where necessary (e.g., foundational QKD protocols).
3. Focused on one or more aspects of Quantum Key Distribution, 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 comparative evaluation.
5. Available in full text and published in English. Studies were excluded if:

1. Were duplicate publications.
2. Were not published in English.
3. Contained insufficient technical or experimental information.
4. Focused primarily on quantum computing or cryptographic topics unrelated to QKD.
5. If they consist of editorials, abstracts, thesis, patents, non-peer-reviewed reports, or other non-scholarly publications.

2.3 Data Extraction and Quality Assessment

The studies were filtered through a multi-phase selection process which includes removal of duplicates, filtering through titles, abstracts, and finally full text of the paper. The authors have checked their relevance to the topic, quality of the methods of originality, experimental verification, and their impact on the domain of QKD.

The studies that were considered relevant were analyzed manually, and their content was systematically collected into a database organized by topics. 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 a comparative analysis and discover the current state and trends of research the selected studies were divided into six major groups:

- QKD protocol evolution
- QKD network architectures
- Practical implementation and application domains
- Deployment strategies and industrial initiatives
- Standardization and interoperability

• Emerging research directions and future trends

The study selection process is illustrated using the PRISMA diagram in Fig.1 ensuring transparency and reproducibility throughout the process.

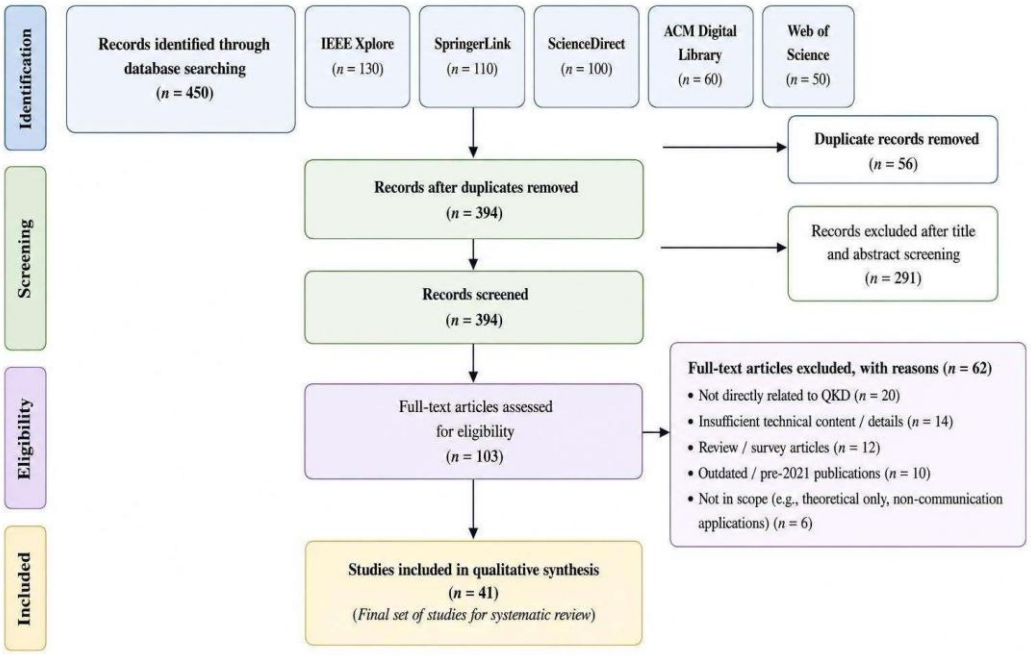

Fig.1. PRISMA study selection process

3. Evolution and Classification of QKD Protocols

3.1 Evolution of QKD Protocols

The history of QKD protocols can mainly be explained by the desire to make communications more secure, covering longer distances in transmission, make implementation more practical, and promote large scale adoption. After the presentation of the BB84 scheme in 1984, QKD gradually went from being an idea to an advanced technology that, it already supports secured communication systems [1]. Instead of public-key cryptography systems whose safety relies on the difficulty of the computational tasks, security of QKD is information-theoretic even against the adversaries with unlimited computational powers.

The progression of QKD protocols was through the identification of limitations of prior protocols and addressing them, as shown in Fig. 2. By setting the standard for quantum secret exchange, the fundamental BB84 protocol was just the first phase, while E91 was the first protocol which used the quantum entangled state of the particles in communication to secure the channel with the Bell's inequality experiment [7], [10]. Later, the SARG04 protocol was launched to make the weak coherent pulse based implementations more secure through the number of photon splitting attacks [8], [16]. In line with the increasing communication requirements, CV-QKD was one of the most interesting approaches. It allows one to exploit continuous quadratures of coherent light states, which leads to the advantage of seamless integration with existing optical communication networks [9], [17]- [19]. Recently released QKD protocols like MDI-QKD and TF-QKD are aimed at fixing the weaknesses of the detectors and overcoming the issue of limited transmission distance, respectively [20]- [23]. All such technological changes have been a sign of QKD research gradually moving from the level of theoretical security protocol toward real-life, deployable quantum communication systems that can support future quantum networks.

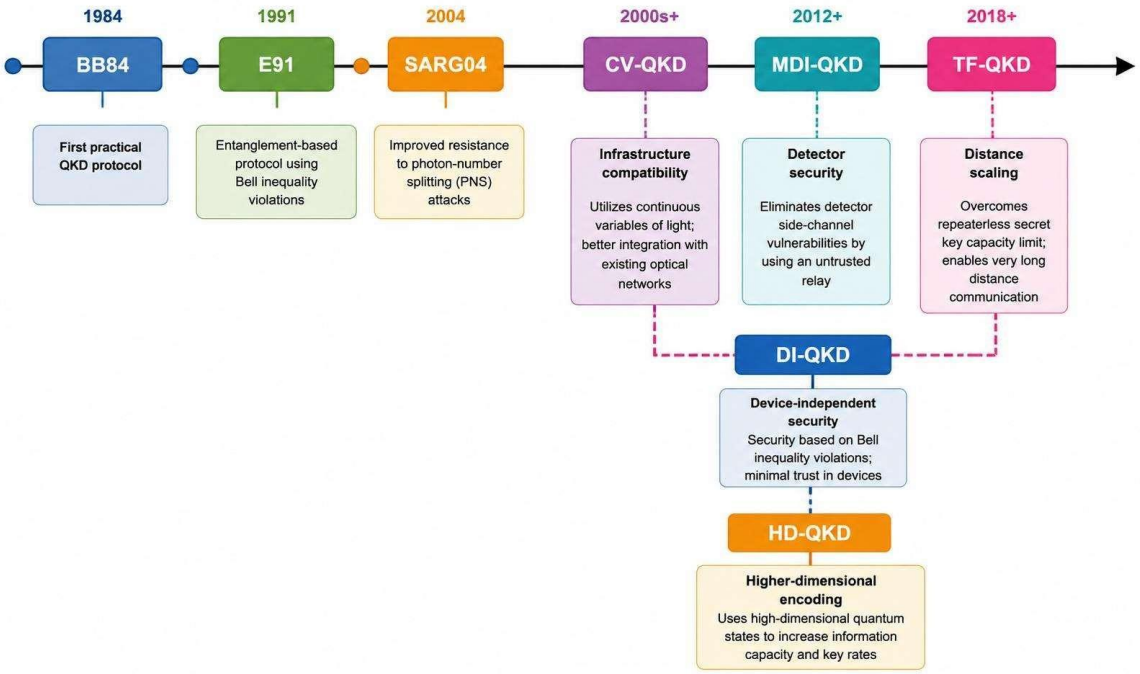

Fig. 2. Evolution of QKD protocols and the problems addressed by each generation

3.2 Discrete Variable QKD Protocols

Discrete-Variable QKD (DV-QKD) is the first generation of practical QKD and is also the most widely studied family of quantum key distribution protocols. In these protocols, quantum information is encoded into discrete quantum states, usually the polarization or phase of a single photon.

Within the many DV-QKD protocols proposed over the past four decades, three of these protocols BB84, E91, and SARG04 have greatly impacted the development of secure quantum communications [1], [7], [8]. The BB84 protocol laid the foundation of the contemporary QKD by illustrating that principle secret-key generation can be achieved over a communication channel by sending a series of quantum non-orthogonal states [1], [24].

Due to its conceptual simplicity, provable security and successful implementation by several experiments, the BB84 remains the standard of practical QKD. The performance of this system is limited by the losses in transmission, the non-ideal detectors, and the limited distance between the communicating stations. In principle, to deepen the theoretical security, quantum entanglement was added in the E91 protocol to be the foundation of secure keys generation [25].

The security was guaranteed by the violation of Bell inequality, which required no assumption on state preparation and can detect eavesdroppers [26]. The entanglement-based systems exhibit even stronger theoretical security, but require more complicated quantum sources, and more narrow synchronization and entangled-photon generation techniques. The SARG04 protocol was then designed as a natural improvement of the BB84 protocol for practical implementation of weak coherent pulse systems [27]. The classical shifting step is changed, so that the protocol still works over current optical systems but offers much better resilience to PNS attack.

However, this proposed protocol is less elegant, more complicated during the post-processing stage, and not widely implemented as the BB84. 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 distance [26]. These problems have led to the

development of more advanced QKD protocols capable of offering greater scalability, stronger implementation security, and extended communication distance.

3.3 Advanced QKD Protocols

The drawbacks of traditional DV-QKD protocols have led to the proposal of the more sophisticated QKD schemes as seen in figure 3, aiming for better performance in practical security, longer transmission distance, and easier implementation. Also, the proposed CV-QKD, MDI-QKD, TF-QKD, and DI-QKD are currently the four most important developments of modern quantum communication systems. Differing from the DV-QKD approach, in the CV-QKD protocols, the quantum information is encoded in continuous quadrature variables corresponding to the phase and amplitude of a coherent light state [9], [17], [18].

This method allows the use of simple telecommunication components which operate on optical fiber communication infrastructures, as the greatest advantage. Several recent experiments have implemented non-Gaussian operations (such as quantum scissors and photon-catalysis) which greatly improve the fidelity and transmission distance without sacrificing the quality of the information sent [19], [28].

These protocols are unfortunately hard to implement in practice owing to the noise of the channel, the calibration of detectors and the finite-size issues. Thus, MDI-QKD was proposed to address the presence of detector side-channel attack, arguably the most important effect affecting the security of any real implementation of QKD [20]– [22]. By removing the measurement operations entirely from the trusted user through the transition of all measurement operations to an untrusted relay, MDI-QKD can provide unconditional security while not trusting measurement devices even though, the implementation security is enhanced.

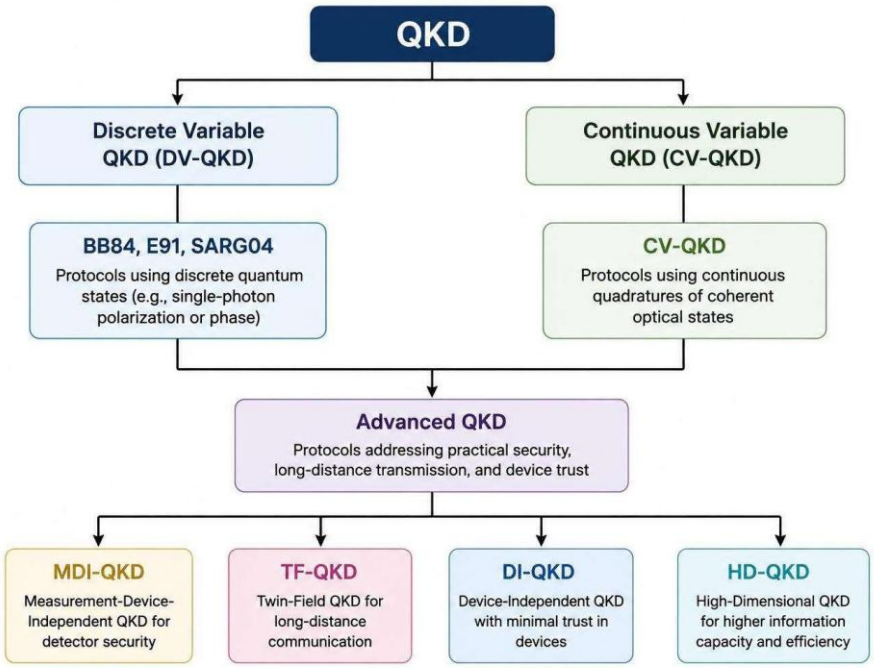

Figure 3. Classification of QKD protocols

However, the system still needs to be carefully synchronised, with high interference visibility while revealing fragility in stability due to more complicated system. TF-QKD is the most important recent achievement in long-distance quantum communication. Utilizing single-photon interference in an intermediate measurement station, TF-QKD beats the repeaterless secret-key capacity limit and has experimentally demonstrated secure information transmission up to a fiber length of more than 800 km [23], [29]. But it is difficult to implement in practice due to

strict phase stabilization, synchronization and calibration issues. Hence, Device-independent QKD (DI-QKD) is the most secure scheme at present for quantum key distribution.

Instead of trusting the quantum devices, this scheme offers unconditional security via Bell inequality violations, even if the measurement devices are untrusted or false. Despite of the current limitations in technology due to the requirements of high detection efficiencies, low channel loss and entangled-photon generation, DI-QKD maintains an attractive conclusion on practical use [30], [31].

All together, these sophisticated protocols reflect the growing maturity of QKD toward scalable, secure, and deployable quantum communication systems. Instead of competing with conventional protocols, every scheme focuses on particular problems arising from communication range, implementation security, integration with classical communications, or system scaling.

3.4 Comparison and 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
Protocol	**Security Strength**	**Distance Capability**	**Deployment Maturity**	**Major Limitation**
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

Table 1. Comparison and Analysis of QKD Protocols

The comparison of modern QKD protocols in Table 1 shows that there is no protocol that can at the same time optimize communication distance, secret-key generation rate, implementation simplicity, deployment cost, and security robustness. Though BB84 is still considered as the most developed and most experimentally verified protocol, its actual performance is hampered by channel attenuation and hardware imperfections. But, SARG04 is more immune to photon-number-splitting attacks, while E91 offers stronger theoretical security because of the usage of quantum entanglement. Even though, in CV-QKD the interface and compatibility between quantum communication systems are facilitated but at the same time, these remain highly susceptible to the limitations of channel conditions. In MDI-QKD the removal of the detectors as side-channel attacks, improves the level of security whereas the TF-QKD communication goes over the secret-key capacity limit for communication without quantum repeaters. Finally, DI-QKD delivers the most profound security guarantees theoretically, its experimental realizations remain 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 deployment environment. As a result, upcoming QKD research should concentrate on

developing flexible and scalable protocol setups which will be able to support diverse quantum communication infrastructures while also making a compromise between, security, performance, and practical deployability.

The development of QKD protocols clearly shows that it is not only possible to achieve large scale quantum-secure communication by the means of protocol-level innovations. The practical deployment of such systems will also require the development of efficient network architectures that are able to handle scalable key distribution, heterogeneous communication environments, and interoperability among different quantum communication technologies on one hand and the management of resources on the other hand. However, to this end, the next section reviews the historical development of different QKD network architectures and analyzes their roles in establishing practical quantum communication networks.

4. Network Architectures for QKD

The evolution of the QKD network architectures demonstrates how the quantum key distribution technology has moved from experimental point-to-point links to full-scale and interconnected communication structures. First QKD implementations made use of only direct point-to-point links or introduced trusted repeaters in between to achieve the range. Despite the simplicity of the setups and the ability to successfully realize practical QKD experiments, those systems have limited scalability due to transmission losses, requirements of infrastructure, high deployment cost and the necessity to have either a dedicated or a trusted communication channel.

So, in case one needs more users or has to cover greater areas, the systems that allow users to make more flexible choices about the ways in which keys are generated stored managed and delivered to them, the ones that can operate smoothly together with the classical systems already in place are the only ones that can satisfy the demand. In line with this, researchers in recent times have come to the idea of multi-user and general-purpose network architecture that will quite a bit enhance scalability as well as the ease-of operations of QKD systems. The qTDM-QKDN concept, for example, brings a method whereby several users can utilize QKD resources in a time-division-based way by making use of common transceiver resources only. Through this, it is possible to achieve major hardware cost savings on dedicated links as it was the case for the QKD devices.

As Software-Defined Networking (SDN)-enabled QKD setups come into play, one gains the ability to programmable network control coupled with a centralized orchestration model allowing dynamic resource allocation, path management, and network monitoring. Key Management System (KMS)-based systems are yet one means of operational integration of QKD and classical communication networks that supports in providing a complete range of functionality such as key storage distribution, lifecycle management, and application-level access. These technological shifts from stand-alone secure links to multi-user, managed, and deployment-oriented QKD networks.

4.1 Architectural Approaches for QKD Systems

Point-to-point QKD is the most basic network setting, where two nodes interested in communication set up a quantum channel directly between themselves to generate the secret key. Due to its relatively small scale and well-developed technology, it brings a good starting point for the short-distance, metropolitan environment. Though, to connect a large number of users, the infrastructure cost of setting up direct links grows exponentially. Trusted-node architectures overcome this problem by linking users through a chain of quantum key distribution links. The intermediate node creates or receives a key from the network link to the adjacent node and using these keys they can enable end-to-end secure transmission of information.

Such networks provide a way of scaling quantum key distribution beyond the range of a single link and establish one of the most feasible routes for early implementation at a large scale [11], [15]. The intermediate nodes must be trusted as the key material to be processed and stored at these locations. Once compromised, the security of communication related to the trusted node will be compromised. To optimize the use of QKD resources, multi-user architectures like qTDM-QKDN have been proposed [32].

They enable two or more communicating users to share the quantum communication resources using a time division based access to the system, transceiver hardware for each pair is reduced, sharing of the system can optimize the system infrastructure and deployment cost. And the number of users co-operative scheduling synchronization resource allocation and network management are crucial. SDN-enabled QKD architectures offer an alternative by allowing centralized protocol control to improve network flexibility [33]. Decoupling control functions from the communication infrastructure allows the controller to centrally manage the use of quantum links, position key-generation resources and flexibly configure a QKD network to suit communication traffic.

But implementations of such architectures will require interoperable interfaces between (standardized) QKD hardware, traditional network elements, and the SDN control layer. KMS based QKD architectures can also complement these network strategies by overseeing the usage and handling of keys generated over QKD links [12], [34]. A KMS can facilitate key generation coordination storage retrieval, distribution and services to upper-layer applications.

The combination of QKD with the concept of KMS hardware is also relevant for interconnection of quantum key-generation infrastructure with classical security systems [35]. Even though, issues for interoperability, standard interface, secured storage of keys, and proper key lifecycle management are still important for large-scale application.

4.2 Regional and Global QKD Architectures

However, extending QKD to broader communication contexts on regional and global scales presents new issues. 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. So, 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 EuroQCI and MadQCI highlight the importance of establishing a networked quantum communication ecosystem [33]. These projects emphasize on combining QKD with current communication infrastructure and establishing compatible quantum-secure services within networked environments. Both of them reflect an initial shift from demonstrating QKD to establishing regional QCI.

Satellite aided QKD introduces the prospect of complementing the distance limitations of a terrestrial fiber network [36], [37]. This is achieved when the use of free space optical link between satellites and ground stations is utilized. In addition, a satellite architecture has the flexibility to connect physically separated terrestrial QKD networks, not only over long distances but on an inter-continental sense.

Satellite based architectures demand the fulfilment of technical and operational conditions, such as pointing and tracking requirements, effects of the atmosphere, required synchronizations, photon loss considerations, weather dependence, and the creation and operation of appropriate ground-station infrastructure. This way, regional and global architectures of QKD emerge as having more demands than simply enhancing the quantum key generation efficiency. They demand efficient control of the large-scale networks, standardised interfaces, interoperate equipment, relevant key management mechanisms, and integration between 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 will be dependent upon the infrastructure needs for trust-node systems, and on the assumptions of the final set of trusted nodes for trusted-node systems. In the longer term, it is anticipated that the quantum repeater based networks will offer a scalable method for extending quantum communication over distances beyond the practical limits of direct transmission. Quantum repeaters seek to establish quantum entanglement across a number of network segments using techniques such as entanglement generation and

quantum memory, rather than a more traditional amplification of an unknown state [5], [6]. Quantum repeater network projects are also related to the quantum internet. The concept of quantum internet is aimed at connecting

physically distributed quantum devices using quantum communication links and sharing quantum information and entanglement using the network [4]-[6], [11].

QKD is one of the first anticipated applications of quantum internet, while future applications include distributed quantum computing, quantum sensing and secure quantum communication. Transition from proof-of-principle demonstration to infrastructure needs improvements in quantum memories, repeater efficiency, entanglement distribution, multiplexing synchronization, network control and quantum classical interfaces. Repeater-based architectures like trusted-node networks attempt to minimize the reliance on fully trusted intermediate infrastructure.

Currently, practical quantum repeater networks are technically less mature due to hardware limitations, quantum memory lifetime, entanglement creation efficiency, transport and maintenance of fidelity, synchronization, and hardware integration. As such, repeater-based QKD and the quantum internet should currently be viewed as directions for future architecture exploration rather than immediate alternatives for mature trusted-node and terrestrial QKD networks.

4.4 Comparative Analysis and Architectural Trade-offs

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	Reduced	Very Long	Experimental	Quantum memory/repeater technology
Quantum Internet	Very High	Reduced	Global	Long-term	Immature infrastructure

Table 2. Comparative Analysis of QKD Network Architectures

Major QKD network architectures are addressing various requirements like scalability, extent of geographical coverage, degree of trust, usage of existing infrastructure, and the maturity of deployment. Point-point system is simplest and mature but has a limited capacity. Trusted-node networks are a feasible solution to the problem of QKD extension over regional distances although their functioning needs are to be carried through a trusted intermediary infrastructure. qTDM-QKDN system works more efficiently at sharing resources among different users while SDN architecture offers the users an improved flexibility being controlled in the central place. KMS-based methods can be a way to connect QKD-generated keys to regular communication infrastructures. Satellite-assisted QKD allows for wider coverage which isn't possible with terrestrial fibre limitations. Additionally, quantum repeater networks and the quantum internet are examples of the long-term directions that could bring large-scale, quantum connection. Based on the comparison given in Table 2, different QKD network architectures may excel in different areas such as scalability,

interoperability, cost efficiency, security assumptions, and operational simplicity at the same time. This way, deployment of network will likely be a combination of terrestrial trusted-node networks, multi-user resource-sharing mechanisms, SDN orchestration, KMS integration, and satellite-assisted links in the early stages. Furthermore, technology continues to develop with quantum repeaters and quantum internet, there is a possibility to get architectures that are less trust-dependent and cover much more geography. So, from practical viewpoint QKD's development is not only about upgrading separate protocols but also about coming up with an interoperable, and easily expandable network architecture. Therefore, QKD deployment should be studied for security infrastructure environment, and application. This is the foundation to identify the areas and situations where QKD technologies are currently in use and the possibilities of deployment.

5. Practical Applications and Deployment Trends

Progression in QKD technology has slowly seen the range of its application emerge from pure laboratory demonstrations to real world usecases for secure communications and infrastructure. The essential role of the key-distribution aspect of QKD in these real world settings is its provision of a method of generating shared cryptographic keys through a quantum communication channel that does not rely on hardness assumptions on which conventional public key-establishment methods rely. QKD has attracted increased focus for sensitive information, critical systems, and long term secure communications against the potential threat of future quantum computers.

5.1 Emerging Application Domains

A significant potential application area for QKD is in future, including fifth and sixth-generation communication networks. These new communication networks, Mostly the 5G and 6G networks, will have to support sensitive data transmission and inter-network communication, and require a means to establish secure keys [13], [38]. During this task, the use of QKD with other communication and core-network infrastructure, targeted to develop secure keys, is considered to be promising, and of world-wide attention. QKD can be combined with other current network security mechanisms to offer a second layer of defense against security breaches originating from attacks on current cryptographic key-establishment mechanisms.

For a desirable practical use, adequate integrated QKD-to-telecom basic infrastructure will have to be realized. This infrastructure has to deliver keys with low bottleneck latency, manage keys efficiently, operate seamlessly with existing protocol layers in the network, and plan QKD resources based on existing network and topology. With the proliferation of Internet of Things devices, edge and fog computing use cases still comes to an increased need for secure communications architectures [14], [39]. As the number of devices and locations involved increases and these architectures will tend to 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 the transmission in such contexts, for example gateways edge nodes, or other infrastructure nodes capable of supporting quantum communication hardware. Integrating QKD at the level of resource-constrained IoT devices is difficult because of hardware requirements, communication bandwidth, and cost considerations.

Therefore, any 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 eternal privacy of sensitive information is at the paramount. Financial institutions could use quantum secure key distribution to establish confidentiality on valuable transactions and links, and healthcare facilities can use confidential key establishment to secure sensitive medical data and distributed healthcare apparatus.

Defense and government communications systems are leading in the application field within the QKD proposition, again due to the need for protection of sensitive data for many years. QKD is also being considered for

critical infrastructure, such as smart grids and industrial automation, where the threat of communication disruption will have significant impacts on the availability of the services.

The overall landscape of applications reflects that the QKD can operate successfully in various communication setups that it is not only a single one. The areas in which it finds possible applications are: the telecommunication sector, financial systems, healthcare, defense, IoT industry, edge computing, smart grids, and industrial infrastructures [2], [14]. Thus the degree to which QKD fits in each area varies greatly and is based not only on the distance of communication but also on the minimum security level, the existing communication network (if any), latency requirements, and most of all, whether the quantum communication hardware can be physically or logically integrated into current systems [40]. The major Application domains are summarized in Fig.4.

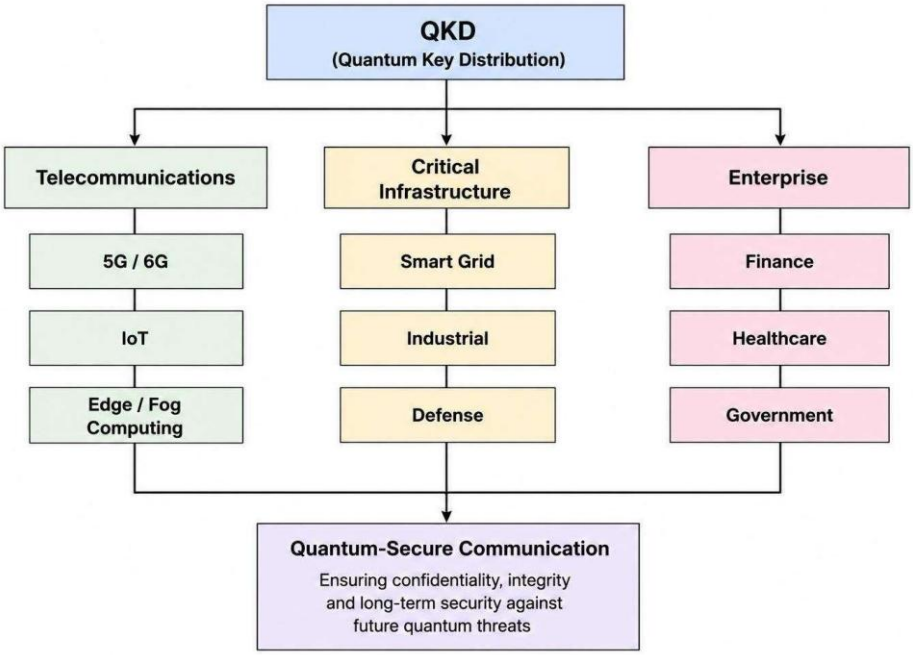

Figure 4. QKD Application Domains

5.2 Real-World QKD Deployment Initiatives

This transition from proof of concept to on-site deployment is more and more exemplified by local, national and international levels of QKD networks and key distribution projects. Such networks not only give a clear

picture on how to fit QKD in 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 China quantum communication infrastructure [41], Madrid Quantum Communication Infrastructure (MadQCI) [33] and the European Quantum Communication Infrastructure (EuroQCI) is representative of otherwise similar approach to building operational quantum communication infrastructures.

Ground fiber-based QKD continues to be a significant option for metro and regional networks as it leverages existing optical communication networks and can offer a fairly stable communication environment. The back bone attenuation of fiber dictates intrinsic constraints on the maximum length achievable without the installation of intermediate nodes; This way this architecture continues to be relevant within existing deployments. Satellite supported QKD can work as a complementary method to overcome the distance limitations of fiber-based, terrestrial QKD networks.

Space-ground configurations can physically interconnect spatially distant ground stations and be the basis for long-range or even inter-continental quantum links [37]. This approach entails further specifications about synchronization, point and track on to satellites, weather and atmosphere, distance and transmission losses, infrastructure on the ground, and operational aspects. Because of this, satellite-based QKD or fiber-based terrestrial solutions should not be seen as competing deployment strategies but as components to a common infrastructure to enable large-scale quantum communication networks [36].

These regional and national initiatives also highlights the increasing relevance of interoperability and integration with current communication systems. Leaps from stand alone quantum links to the inclusion of essential management systems, classical communication channels, network orchestration, and standard interfaces are becoming progressively more prevalent. These records the advances that suggests genuine QKD deployment is transitioning from demonstrations to integrated quantum-secure communication infrastructures [15].

5.3 Deployment Readiness and Critical Assessment

While recent deployment efforts highlight remarkable advances in technology, the widespread commercial acceptance of QKD is still facing several interconnected challenges. The costs of infrastructure and hardware, mostly in dedicated quantum transmitters, receivers, trusted nodes, or specific optical devices are required, still continues to be the limitation. The reliance on trusted intermediate nodes in most terrestrial schemes introduces extra layers of operational and security considerations, the need for interoperability among equipment from different sources, integration into current telecommunication systems, and the lack of harmonized interfaces and standards may hinder large scale deployment. Operational scalability is another significant issue.

A QKD network is required to generate, store, distribute, and administer keys constantly per the needs of various applications and users. So, performance of a pragmatic QKD implementation cannot be judged simply with 'secret-key rate' or 'transmission distance'. It should also take into account network operability, key management efficiency, utilization of resources synchronization maintenance, interoperability and integration to classical security systems.

The deployment initiatives assessed in this paper indicates an important shift from experimental QKD links towards the development of more sophisticated and dispersed quantum communication network architectures. The use of terrestrial networks enables the deployment in urban and regional contexts, while the use of satellites ensures a broader geographical reach. In parallel, initiatives such as EuroQCI, MadQCI or large scale national quantum communication initiatives suggest an increased acknowledgement of the relevance of implementing QKD in operational communication networks. One should note that the deployment landscape is still made of a mixture of research, government-led and early industrial deployments in this area rather than embedded in commercially available networks.

So, current QKD technology may be described as mature in some aspects but it is not mature as a globally scalable communication service. Additional advancements are necessary to bring QKD to a useable technology for different applications, communications networks, key management, interoperability and interface standards cost and deployment setups. All these factors also highlight that the future QKD uses will probably not be as a stand-alone security technology but as part of a sufficiently broad set of quantum-based technologies, that would include the PQC.

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 Terrestrial + Satellite	Long-distance secure communication	Global coverage	Satellite deployment cost

Table 3. Comparative Assessment of QKD Deployments

The comparative assessment in Table 3 clearly demonstrates the development of QKD from the experimental level to large-scale operational quantum communication infrastructures. The successful validation of QKD with existing communication networks, while supporting secure services for government, industries and critical infrastructures, has been done through regional and national initiatives. Additionally, satellite-assisted developments also expanded the communication limits. Even though these deployment initiatives have several advantages, they are facing challenges related to infrastructure development, interoperability, standardization, and operational scalability. These evaluations strongly indicate that while QKD deployments have still reached a significant technical maturity, they still require continuous advancements in both technology and deployment strategies for large-scale adoption.

6. Challenges, Research Gaps and Future Research Perspectives

6.1 Challenges in Real-World QKD Deployment

Although there has been significant progress on QKD protocols, network architectures and deployment projects in the last 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, those issues do not seem to stem from any single limitation, but rather from the interplay of quantum-channel properties, hardware restrictions, network scalability, interoperability and deployment

aspects. At the physical and protocol levels, the transmission loss, the non-zero rate of secret-key generation, the detectors imperfections, the finite-key effect, the noise of the channel and the synchronization conditions are all factors limiting the performances of the QKD [1], [17], [19], [26], [29]. The feasible distance and the key-generation rate strongly depend on the specific protocol, the transmission medium, the specifications of the source and the technology of the receiver.

Protocols like the MDI-QKD and the TF-QKD can overcome some distance and security issues, but at the expense of an overall more complex system including higher specifications in term of synchronization, phase stabilization, interference and calibration [20]– [23]. Hardware and infrastructure requirements is another important barrier. Successful real-world implementation of QKD measures demand for additional hardware components such as optical source detectors for quantum communication components in parallel with classical control infrastructure.

The equipment involved and its processing needs high costs, in particular 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 telecom environment. Network level challenges include scalability, interoperability, key-management and the presence of a trusted-node [11], [12], [34], [39]. Key management across multiple users in a large scale QKD network needs to ensure there are enough keys for each user and that the network performance remains unaffected.

Interoperability and compatibility of QKD systems supplied by different vendors and the integration of QKD with existing conventional communication networks need to be addressed for large scale distribution. Based on current terrestrial QKD networks, the reliance on trusted intermediate nodes can impose further physical and operational security restrictions. Standardization and common interfaces are crucial in enabling heterogeneous QKD component networks to work as a communication [30], [31].

6.2 Research Gaps and Open Issues

Systematic review of the selected literatures reveals that the field of QKD has matured in its progress still, there are observed research gaps that straddle the areas of protocol performance, network scalability, deployment preparedness, and system integration. Most the studied literature are preoccupied with protocol, scientific, or experimental level solutions that optimize individual metrics that include, but are not limited to, transmission distance, security, key-generation, efficiency, detector robbery, counter-measurement, or network infrastructure dimensioning; with few comparative studies of these parameters together that consider realistic conditions for large-scale deployment [1], [2], [4], [7]- [13], [15]. This presents a research gap in how directly observed improvements at the protocol or experimental level are reflected in an operational quantum communication network infrastructure. Another notable shortfall is the lack of comprehensive long-term, large-scale performance assessments [12], [15], [33], [41].

While regional and national QKD programs have explored the practicality of establishing quantum networks in real-world settings, most of the systems tested are operational at a pilot scale, or experimental research. More in-depth assessment is needed to evaluate the robustness, maintenance requirements, key availability, operating costs, network expansion potential and performance under large traffic in long term operation. Interoperability is still not satisfactorily studied. More diverse protocols, transmission media, hardware platforms, network architectures, and key management schemes are projected in the next QKD

network. And interactions among these diverse parts are quite difficult. Standardized interface protocols, ubiquitous network management facilities and interoperable key management schemes have to be in place in order not to keep isolated QKD networks. Another significant gap is in the combination of QKD with other quantum-safe solutions.

While there is a growing amount of research directed towards hybrid QKD PQC solutions, there has to be much work done on practical implementation approaches, system tradeoffs, key-management systems, and interworking concerns [2], [3]. To evaluate a full end-to-end quantum-secure communications system (rather than individual QKD nodes), the combination of QKD with SDN, intelligent network management, edge computing, and automated resource management is still in an early phase [6], [33]. These gaps illustrate that future work needs to look at solving the integration of specific QKD stages, and long-term system capabilities, rather than optimal solutions for individual components.

6.3 Future Research Directions

Based on the discussed problems and research gaps, future QKD research should give more emphasis on integrated, scalable, and deployment-oriented communication structures. Instead of optimizing protocols separately, future research should design a comprehensive QKD communication system by considering protocol selection, network architecture, key management infrastructure security, and application, simultaneously to adapt heterogeneous deployment environment and heterogeneous application requirement.

Extending communication distance will also be a key research topic. Progress will be needed in the areas of quantum repeaters, quantum memories, entanglement distribution, and network architectures based on repeaters to surpass the fundamental constraints on direct quantum transmission that exist today [4]- [6].

Development of the quantum internet is ongoing, but significant technological issues may preclude global networks of quantum communications from being realized in the near term. Hybrid quantum-safe security is another valuable directions: integrating QKD and PQC can offer replacing, augmenting, or reinforcing the respective use cases of each technology, and provide additional value by including the use of physical security derived from the properties of quantum communication, plus the computational security stemming from cryptography [2], [3].

Further investigations should be done on practical hybrid architecture, key-establishment mechanisms, cryptography agility, performance overhead and migration path for achieving integration QKD and PQC into current communication infrastructures.

Another way of enhancing QKD network management is by applying the emerging technologies of AI and SDN [12], [33]. AI-based support may be used for the traffic prediction, anomaly detection, resource allocation and to enable a dynamic and adaptive system, while SDN may allow programmable and flexible management of various quantum and classical network resources [6]. They should still be among the main areas of investigation. QKD future networks will need standardized interfaces, interoperable hardware devices, standardized key-management protocols, and compatibility with current communication protocols.

At the same time, affordable quantum hardware and integrated photonic technology will could greatly reduce the physical and deployment costs of QKD systems [30], [31]. Also, field-trial and long-term

operation experiments are required to examine the reliability scalability cost-effectiveness, and security [15], [33], [41]. All of this directions suggest that the future progression of QKD will be forced by the need for a manageable, cost-effective, application-aware quantum-secure communication infrastructure, that gives interoperability rather than solely on increasing key rates or transmission distances.

7. Conclusion

The systematic literature review summarizes the trends in QKD innovations from initiation with the core protocols, to modern quantum communication technologies, and on to the new and developing practical deployment environments and infrastructure. The outcome of this review includes coverage of progress by discrete-variable and advanced QKD protocols, evolution in type and categories of network architecture, areas of practical use implementations, regions and countries of implementations, and review of the challenges encountered by these innovations in building toward large scale practical use [33], [37], [41]. The evidence shows QKD innovations have advanced appreciably past the purely theoretical and laboratory initiatives to where experimental testing and deployment are becoming more prevalent through terrestrial, satellite assisted, and new quantum network types of practical environments.

The study also reveals that there are still considerable hurdles to overcome before we can see QKD as a practical, deployable and cost effective secure technology. Transmission loss, performance in key-generation, hardware exclusivity, scalability, interoperability, trust entity relied, operational difficulty, and lack of standards still impede practical deployability [12], [15], [30], [34]. Currently, not a single QKD protocol and network architecture among them in the early-stage networks can achieve the best of all worlds for secure distance security, cost-of-use, scalability, and maturity.

So, subsequent QKD infrastructure may be a reasoned combination of protocols hardware network architectures, trusted-nodes, key management, standards, application standardization and deployment. The review also emphasizes on the need for combination of QKD with other technologies like PQC, SDN, quantum repeaters, quantum memories and intelligent network management [2], [3], [6], [30], [33]. The hybrid and interoperable techniques are expected to be significant in moving from isolated QKD deployments into heterogeneous quantum-secure communication networks.

For this reason, ongoing large-scale field trials, standardization, hardware development, and long-term performance trials will be required to demonstrate the practicability and economic viability. Basically, the evolution of QKD has been described as moving from a focus on protocols to network, integrated, and deployment oriented quantum communication infrastructures. Future trajectory of development will result from the interdisciplinary effort in QIS, optical communication engineering cybersecurity networking, and standardization, also researchers will create the technological building blocks of large-scale resilient quantum-secure communication networks to enable future information infrastructure.

REFERENCES

1. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Reviews of Modern Physics, vol. 92, no. 2, Art. no. 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, P. Anusha, N. R. Vullam, J. Jala, V. S. Bellapu, and A. S. Vindhya, "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 Communications Surveys & Tutorials, 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," Physical Review A, vol. 103, no. 3, Art. no. 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," Physical Review Applied, vol. 21, no. 2, Art. no. 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, Z. Yan, H. Yang, Q. Lu, Z. Lu, L. Cheng, et al., "Information reconciliation of continuous-variables quantum key distribution: Principles, implementations and applications," EPJ Quantum Technology, vol. 10, Art. no. 40, 2023, doi: 10.1140/epjqt/s40507-023-00197-8.
10. V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, "Advances in device-independent quantum key distribution," npj Quantum Information, 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 Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839–894, 2022, doi: 10.1109/COMST.2022.3144219.
12. E. Dervisevic, A. Tankovic, E. Fazel, R. Kompella, P. Fazio, M. Voznak, and M. Mehic, "Quantum key distribution networks—Key management: A survey," ACM Computing Surveys, vol. 57, no. 10, Art. no. 257, pp. 1–36, 2025, doi: 10.1145/3730575.
13. M. Mehic, L. Michalek, E. Dervisevic, P. Burdiak, M. Plakalovic, J. Rozhon, et al., "Quantum cryptography in 5G networks: A comprehensive overview," IEEE Communications Surveys & Tutorials, 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), 2025, 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 Communication, 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," Physics 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," Applied Physics Reviews, 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, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, et al., "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," Physical Review Letters, vol. 125, no. 1, Art. no. 010502, 2020, doi: 10.1103/PhysRevLett.125.010502.
20. M. C. 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.
21. Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, et al., "Long-distance free-space measurement-device-independent quantum key distribution," Physical Review Letters, vol. 125, no. 26, Art. no. 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," Physical Review Applied, vol. 20, no. 2, Art. no. 024029, 2023, doi: 10.1103/PhysRevApplied.20.024029.
23. Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, et al., "Experimental twin-field quantum key distribution over 1000 km fiber distance," Physical Review Letters, vol. 130, no. 21, Art. no. 210801, 2023, doi: 10.1103/PhysRevLett.130.210801.
24. S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, et al., "Twin-field quantum key distribution over 830-km fibre," Nature Photonics, vol. 16, pp. 154–161, 2022, doi: 10.1038/s41566-021-00928-2.

25. A. Hreibi, A.-K. Kniggendorf, A. Kuhl, J. Kronjäger, H. Schnatz, and S. Kück, "Entanglement-based intercity quantum key distribution: Metrology and implementation," Measurement: Sensors, vol. 38, Art. no. 101777, 2025, doi: 10.1016/j.measen.2024.101777.
26. 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 in Optics, vol. 16, Art. no. 100718, 2024, doi: 10.1016/j.rio.2024.100718.
27. 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.
28. 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 in Physics, vol. 56, Art. no. 107276, 2024, doi: 10.1016/j.rinp.2023.107276.
29. 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.
30. W. Luo, L. Cao, Y. Shi, L. Wan, H. Zhang, S. Li, et al., "Recent progress in quantum photonic chips for quantum communication and internet," Light: Science & Applications, vol. 12, Art. no. 175, 2023, doi: 10.1038/s41377-023-01173-8.
31. M. Zahidy, M. T. Mikkelsen, R. Müller, B. Da Lio, M. Krehbiel, Y. Wang, et al., "Quantum key distribution using deterministic single-photon sources over a field-installed fibre link," npj Quantum Information, vol. 10, Art. no. 2, 2024, doi: 10.1038/s41534-023-00800-x.
32. J. C. Hernandez-Hernandez, D. Larrabeiti, M. Calderon, I. Soto, B. Cimoli, H. Liu, and I. Tafur Monroy, "Designing optimal quantum key distribution networks based on time-division multiplexing of QKD transceivers: qTDM-QKDN," Future Generation Computer Systems, vol. 164, Art. no. 107557, 2025, doi: 10.1016/j.future.2024.107557.
33. V. Martin, J. P. Brito, L. Ortíz, R. B. Méndez, J. S. Buruaga, R. J. Vicente, et al., "MadQCI: A heterogeneous and scalable SDN-QKD network deployed in production facilities," npj Quantum Information, vol. 10, Art. no. 80, 2024, doi: 10.1038/s41534-024-00873-2.
34. 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.
35. J. M. Lukens, N. A. Peters, and B. Qi, "Hybrid classical-quantum communication networks," Progress in Quantum Electronics, vol. 103, Art. no. 100586, 2025, doi: 10.1016/j.pquantelec.2025.100586.
36. W. Jiang, Y. Zhang, H. Han, and J. Mu, "Quantum communication in self-organizing satellite networks: Challenges and opportunities," IEEE Communications Standards Magazine, vol. 9, no. 3, pp. 15–25, 2025, doi: 10.1109/MCOMSTD.2025.3578320.
37. Y. -A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, 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.
38. A. Atutxa, A. Sanz, J. Sasiain, J. Astorga, and E. Jacob, "Towards a quantum-safe 5G: Quantum key distribution in core networks," Computer Communications, vol. 224, pp. 145–158, 2024, doi: 10.1016/j.comcom.2024.06.005.
39. 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," Computers, Materials & Continua, vol. 84, no. 1, pp. 25–55, 2025, doi: 10.32604/cmc.2025.062966.
40. 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," Engineering Science and Technology, an International Journal, vol. 70, Art. no. 102167, 2025, doi: 10.1016/j.jestch.2025.102167.
41. H. -Z. Chen, M.-H. Li, Y. Z. Wang, Z.-G. Zhao, C. Ye, F.-L. Li, et al., "Implementation of carrier-grade quantum communication networks over 10000 km," npj Quantum Information, vol. 11, Art. no. 137, 2025, doi: 10.1038/s41534-025-01089-8.