Cybersecurity in the Age of Quantum Computing New Challenges and Solutions

Ahmed Ali Hussein
Al-Turath University, Baghdad 10013, Iraq.
Email: ahmed.hussein@uoturath.edu.iq

Sumaia Ali Alal
Al-Mansour University College, Baghdad 10067, Iraq.
Email: sumaia.ali@muc.edu.iq

Tursunov Dilmurat Abdilazhanovich (Corresponding author)
Osh State University, Osh City 723500, Kyrgyzstan.
Email: dtursunov@oshsu.kg

Hanaa Hameed Merzah
Al-Rafidain University College Baghdad 10064, Iraq.
Email: Hanaa.hameed.elc@ruc.edu.iq

Hasan Ali Abbas
Madenat Alelem University College, Baghdad 10006, Iraq.
Email: hasan.ali@mauc.edu.iq

| Received: 2025 | Accepted: 2025

Iranian Journal of Information Processing and Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Special Issue | Summer 2025 | pp.1507-1541
https://doi.org/10.22034/jipm.2025.728442

Abstract

Background: Mobile networks today specifically 5G require appreciable secure networks because of the emerging risks due to the growth in the deployment of network structures. Discovered weaknesses of cryptographic conventional methods to quantum computing breakthroughs make it necessary to develop quantum-resistant solutions.

Objective: The article analysing Quantum Key Distribution (QKD) protocols in improving cryptographic performance in 5G networking environment, with emphasis on incorporating QKD into 5G network designs.

Methods: The study performed both a systematic literature review and an evaluation of current QKD deployments, as well as a qualitative assessment of data derived from 20 key informant interviews on QKD in telecommunications and 15 technical reports. Latency and key generation rate experiments were both conducted with relay mechanisms including both trusted and untrusted optical fiber and

wireless relay links, in addition to integration issues were explored using simulations over fiber and wireless emulated networks.
Results: The outcomes emphasise that QKD brings radically enhanced key security in conjunction with low delay and high rate within integrated 5G architectures. Hybrid relay-based QKD augmented key generation rates by 23 % in comparison with previous techniques. There are also concerns associated with the implementation of internationally agreed on standards which include issues pertaining to non-compliance of the standards used in different countries and high costs involved when trying to implement these standards.
Conclusion: QKD implementation also increases cryptographic protection of the 5G networks and makes infrastructures quantum-immune to threats originating from the quantum-age. To make it more widespread, additional standardization and a reduction in cost are required.

Keywords: Quantum Key Distribution, 5G Networks, Cryptographic Resilience, Network Security, Hybrid QKD, Optical Backbone, Wireless Topologies, Standardization, Key Generation Rate, Cybersecurity

1. Introduction

5G technology has revolutionized telecommunications by significantly enhancing connectivity, bandwidth, and latency. This evolution has facilitated the proliferation of intelligent applications, including self-driving vehicles, smart cities, industrial automation, and the Internet of Things (IoT). However, the increased reliance on these capabilities for critical systems has raised significant concerns regarding information security and privacy. These concerns are further amplified by the potential vulnerabilities of traditional cryptographic methods to emerging quantum computing technologies, necessitating the development of quantum-resistant alternatives (El-Latif et al. 2019), (Kong 2022).

Although quantum computers have not yet been physically realized, they pose a substantial threat to widely used encryption algorithms such as RSA and ECC. These classical algorithms are fundamental to securing modern communication systems and are increasingly recognized as vulnerable to quantum attacks. Consequently, research into developing cryptographic methods capable of resisting quantum computation has gained momentum (Clancy, McGwier, and Chen 2019). One promising solution is Quantum Key Distribution (QKD), which leverages the principles of quantum mechanics to provide theoretically unbreakable security (Bedington, Arrazola, and Ling 2017). The key characteristic of QKD is that any eavesdropping attempt

disturbs the quantum state, which can be detected and addressed in real-time (Osborne 2020).

The theoretical development of QKD protocols has seen significant advancements. For instance, research on satellite-based QKD systems has demonstrated their ability to overcome the distance limitations of terrestrial networks, enabling global quantum communication (Bedington, Arrazola, and Ling 2017; Abdulameer et al. 2024). Additionally, hybrid QKD systems that combine optical fiber and wireless networks have proven effective in extending secure key distribution to dynamic and heterogeneous environments, meeting the critical demands of 5G networks (Zavitsanos et al. 2020). Further advancements in relay-based nonlinear QKD mechanisms have enhanced key generation rates and scalability, addressing some of the performance challenges in large-scale systems (Cao et al. 2021; Qasim et al. 2021).

Despite these developments, several significant challenges remain. High implementation costs, driven by the need for dedicated hardware such as quantum random number generators and photon detectors, present major obstacles to scalability and widespread adoption (Dorozhynskyi et al. 2023). Additionally, interoperability challenges with existing 5G architectures necessitate innovative integration approaches within the cybersecurity domain (Nameer, Aqeel, and Muthana 2023). While new applications are emerging, standardization remains a substantial barrier, with the lack of widely accepted protocols complicating implementation and interoperability across different networks (Choi et al. 2021). Performance issues, including low latency and high throughput in dynamic 5G environments, also warrant further investigation (Aguado et al. 2019).

To address these gaps, this study proposes a comprehensive framework for integrating QKD into 5G infrastructures. This study differentiates itself from previous literature, which has largely focused on theoretical advancements or individual use cases, by emphasizing practical deployment strategies, performance optimization, and cost-efficiency. The proposed framework includes hybrid trusted/untrusted relay mechanisms to balance security and performance and integrates QKD with Software-Defined Networking (SDN) to dynamically manage network resources and reduce computational overhead (Ren et al. 2022), (Aguado et al. 2020). Furthermore, the study explores the feasibility of satellite-based QKD for long-distance key distribution as a

potential component of a comprehensive 5G security framework (Diamanti 2021).

This article is unique in offering a holistic approach, incorporating experimental validation based on real-life scenario measurements, systematic literature analysis, and stakeholder perspectives to address the diverse challenges associated with deploying QKD in 5G networks. By combining data from 20 expert interviews and 15 technical reports, the study provides a comprehensive view of the potential and challenges of QKD technologies.

The research approach includes experimental simulations within hybrid optical-wireless topologies, aimed at assessing latency, key generation rates, and scalability in dynamic contexts. Analytical techniques, such as comparative performance benchmarking and cost-benefit analysis, are employed to evaluate the feasibility of the proposed solutions. The expected outcomes include a validated framework for QKD integration, demonstrating the viability of this solution as a cornerstone of quantum-safe cryptographic approaches for 5G networks.

1.1. The Aim of The Article

This article explores the capabilities of QKD protocols in enhancing the cryptographic resilience of next-generation 5G networks. It presents a comprehensive survey of QKD integration into hybrid optical-wireless topologies, highlighting the drawbacks, benefits, and practical applications of deploying quantum-resistant encryption methods. By quantitatively assessing performance metrics such as key generation rates, latency, and throughput, this work provides a framework to guide the secure integration of QKD into telecommunications infrastructure. Furthermore, it addresses key challenges related to standardization, cost-effectiveness, and interoperability, offering actionable measures to accelerate the adoption of QKD in 5G networks.

1.2. Problem Statement

As commercial 5G networks are rapidly deployed and become an integral part of our communications infrastructure, they introduce new and unique security challenges. Quantum computing, which is on the rise, represents an existential threat to classical encryption schemes based on computational complexity. The computational power of these emerging technologies can

quickly outmatch classical cryptographic algorithms, thus exposing sensitive data. One promising solution is QKD, which leverages the principles of quantum mechanics to generate secure cryptographic keys. However, its implementation in next-generation 5G infrastructures presents significant challenges.

Among the major challenges are the high financial costs associated with deploying QKD systems. This includes the need for quantum hardware and secure channels, which impacts scalability and limits widespread adoption. Integrating QKD with existing network infrastructure and protocols has also proven to be a daunting technical problem. Furthermore, the dynamic nature of network complexities is compounded by the requirement to meet performance metrics such as low latency, high throughput, and stable key generation rates under varying network conditions. In addition, the absence of standardized protocols leads to compatibility and operational issues, which may act as structural barriers to the widespread adoption of QKD globally.
Significant research efforts are required to address these challenges and develop a practical, cost-effective, and scalable QKD architecture suitable for the unique needs of both existing and future 5G networks.

2. Literature Review

Quantum Key Distribution (QKD) is a crucial research area for securing future communication networks, offering theoretically unbreakable cryptography. However, incorporating QKD into 5G and IoT frameworks presents several challenges, including scalability, error correction, resource allocation, and real-world application. This review paper provides an overview of the literature on QKD, highlighting the main gaps in existing knowledge and proposing promising opportunities for the advancement of this emerging technology.

Scalability remains a significant challenge, particularly in high-density 5G scenarios (Qasim and Jawad 2024). Pham and Dang (2022) reported performance bottlenecks in QKD due to resource constraints in ultra-dense IoT networks(Pham and Dang 2022), while Li et al. (2023) noted that noise and interference in 5G wireless channels exacerbate these issues (Li et al. 2023). Although various methods exist, such as parallelized key exchanges with multiple quantum random number generators (QRNGs) and dynamic channel partitioning (Mhlambululi and Makhamisa 2018), synchronization

and more sophisticated algorithms to handle high traffic levels remain under-studied.

Error correction and resource allocation present additional challenges. Optimized QKD protocols proposed by Tannous and Langlois (2019) aim to reduce the Quantum Bit Error Rate (QBER) but do not adaptively provide optimal solutions in real-time (Tannous and Langlois 2019), and dynamic channel partitioning, as demonstrated by Yan et al.(2022) in microgrid systems, are promising solutions (Yan et al. 2022). Syncing, as well as more sophisticated algorithms which could handle high levels of traffic activity, remain under-studied.

Wang (2020) proposed using algebraic topology to improve system reliability in dynamic environments, although limited experimental validation has been performed in hybrid optical-wireless settings (Wang 2020). López et al. (2019) highlighted inefficient bandwidth usage in QKD-enabled networks and suggested dynamic resource allocation mechanisms (Lopez et al. 2019). Li et al. (2019) proposed advanced physical layer authentication techniques to enhance bandwidth for 5G channels, but their integration with QKD protocols remains unexplored (Li et al. 2019).

Integrating QKD into 5G networks poses its own set of challenges. López et al. (2019) mainly covered theoretical aspects of QKD in next-generation networks (Lopez et al. 2019), while Alanezi et al. (2023) proposed quantum walks-based cryptographic protocols for wireless sensor networks, which show theoretical potential but face real-time implementation challenges (Alanezi et al. 2023). Yan et al. (2022) implemented QKD for microgrid control systems, enhancing cybersecurity but not covering a wide range of use cases (Yan et al. 2022). Wider applications, such as telemedicine, autonomous vehicles, and intelligent cities, require dynamic structures to meet their specific security needs (Diamanti 2021).

Hybrid and satellite QKD systems offer potential solutions to overcome the distance and scalability limitations of terrestrial QKD. Amer et al. (2022) proposed a common design for QKD sifting protocols to enhance synchronization between hybrid systems, but synchronization issues remain, especially in long-distance scenarios (Amer, Garg, and Krawec 2022). Satellite QKD extends quantum communication to global distances but suffers from atmospheric signal attenuation (Diamanti 2021), Advanced error correction techniques, like those proposed by Alanezi et al. (2023), could

address these losses, enabling secure key exchanges over vast distances (Alanezi et al. 2023).

Several research gaps remain unaddressed. Issues related to scalability in dense 5G environments (López et al., 2019) and the need for experimental validation of dynamic resource allocation and synchronization methods (Pham and Dang, 2022) require further investigation (Lopez et al. 2019; Pham and Dang 2022). The under-exploration of integration frameworks for broader 5G use cases by standardization bodies, including smart cities and autonomous vehicles, presents additional challenges. While the potential of satellite QKD is recognized, it is still in early research stages, with solutions such as adaptive transmission protocols and multi-satellite constellations yet to be fully developed (Diamanti 2021).

To address these challenges, future studies must focus on developing low-cost quantum hardware, incorporating machine learning-driven optimal resource allocation, and conducting trials in live environments. Additionally, efforts to combine hybrid and satellite QKD systems with adaptive synchronization and error correction techniques will form a solid foundation for scalable and efficient global quantum-secured communication networks, contributing to the advancement of next-generation cybersecurity.

3. Methodology

Employing a rich methodology that involved a systematic literature review, expert interviews, technical report evaluation, and experimental simulations, this research examined the integration of QKD protocols into 5G networks. This approach guaranteed a multidimensional analysis covering theoretical, technical, and practical aspects.

3.1. Systematic Literature Review

This systematic review evaluates the current state of QKD research and its application in 5G networks by analyzing 24 academic articles and technical papers published between 2017 and 2023. Pioneering work by El-Latif et al. (2019) described the potential of QKD for securing quantum-resistant cryptographic protocols in next-generation networks, especially for mission-critical applications such as IoT and autonomous systems. These findings underscored the importance of scalable and efficient QKD solutions in rapidly evolving 5G ecosystems (El-Latif et al. 2019).

Zavitsanos et al. (2020) investigated the integration of QKD into hybrid fiber-wireless (H-FW) topologies, reporting that QKD can provide additional security in converged H-FW networks (Zavitsanos et al. 2020). However, they also highlighted challenges such as resource allocation and synchronization problems in dynamic settings. Similarly, Cao et al. (2021) examined hybrid relay-based QKD, demonstrating a 23% increase in key generation rates while emphasizing the need for more sophisticated authentication and error correction schemes (Cao et al. 2021). These studies provided the rationale for focusing this research on hybrid trusted/untrusted relay mechanisms.

Diamanti (2021) and Osborne (2020) addressed the challenge of quantum communication over longer distances without the need for intermediate stations, but they also pointed out issues related to scalability, standardization, and cost that need to be addressed to overcome existing barriers (Diamanti 2021), (Osborne 2020). Choi et al. (2021) highlighted the pressing need for standard QKD protocols for integration with existing 5G frameworks (Choi et al. 2021). The high cost of specialized quantum hardware and performance bottlenecks in terms of latency and throughput remain significant challenges.

Guided by this review, this research will focus on experimentally optimizing the integration of QKD in hybrid networks and overcoming the challenges of latency, scalability, and interoperability, which are central to secure 5G deployments.

3.2. Expert Interviews

To ground the study in practical relevance, semi-structured interviews were conducted with a total of 20 experts in the fields of telecommunications, quantum cryptography, and cybersecurity regulation. Such a broad perspective will help us better understand the problems and solutions available for integrating Quantum Key Distribution (QKD) into 5G networks, as we had 8 industry professionals, 7 academic researchers, and 5 policymakers participating in the workshop.

Speakers from leading telcos discussed the potential of scaling up QKD but mentioned the prohibitive cost as an important barrier to overcome. The acknowledged the financial costs associated with placing new quantum hardware, such as photon detectors and random number generators, and highlighted the need for cost-effective solutions (Dorozhynskyi et al. 2023).

They also pointed out practical difficulties in integrating QKD with running 5G infrastructures, especially in hybrid optical-wireless topologies.

Academic researchers in preparation for practical development addressed limitations and challenges. Relay-based QKD systems were addressed, where the focus was on enhancing key generation rates and reliability in temperate network environments (Zavitsanos et al. 2020); (Cao et al. 2021). They also established the significance of advanced error correction protocols and referenced the possibility of hybrid trusted/untrusted relays to mediate security and scalability.

Based on their expert analysis, policymakers investigated the regulatory and standardization landscape discussing the criticality of internationally standardized QKD protocols for interoperability among varying network architectures (Choi et al. 2021). They highlighted work within ITU-T as an important step toward overcoming challenges related to compatibility.

Through thematic analysis, the interviews revealed standardization, performance optimization, cost constraints and integration challenges as their main priorities. Informed by these insights, the experimental focus of the work, and development of the practical, scalable QKD solutions for next-generation, 5G networks, were hybrid network environments.

3.3. Technical Report Analysis

The intention was to share this experience across organizations, so experts from industry and government were represented in many portions of the published access point technical reports based from QKD experience, ultimately totaling fifteen reports. These reports encompass case studies, fairness performance assessments, and evaluations of novel QKD technologies, providing vital information to inform the experimental stage of this research.

Case studies addressing QKD installation in the context of testbed facilities (Aguado et al. 2019) which revealed the real-world difficulties of including QKD into real networks. While some topics discussed included the high cost of deploying quantum hardware or the need for sophisticated error correction techniques to ensure hybrid networks remained reliable. They also underscore the significance of flexible management of resources to ensure maximum effectiveness in different surroundings.

Related works on performance evaluations of hybrid relay approach

(Pham and Dang 2022) concentrated on key generation efficiency improvement rate while preserving security. These reports outlined the limitations of the scalability of these mechanisms, especially in high throughput 5G scenarios, and emphasized the importance of effective authentication protocols which ensure security against weaknesses in untrusted relay situations.

Evaluations of satellite-based QKD systems showed their potential use for secure long-distance communication (Bedington, Arrazola, and Ling 2017). But these reports also highlighted substantial cost obstacles and technical complexities, like synchronization and signal attenuation, that prevent mass adoption.

The findings emphasized the importance of such problems being targeted by experimental investigations and the continuing development of application QKD systems for future 5G networks, as evidenced by the analysis showing major shortfalls in areas of standardization, scalability, and cost.

3.4. Experimental Simulations

Experimental simulations were done to study the implementation of QKD in upcoming 5G networks and analyze its performance. The focus of these experiments were to overcome important criteria like, latency, key generation rates and scalability in hybrid optical-wireless network. The setup, methods, and equations used in the simulations were chosen to detail the advantages and disadvantages of QKD.

Simulation Setup

The experiments were conducted in a hybrid optical-wireless network testbed, simulating real-world 5G scenarios:

- Optical Backbone: High-speed, low-latency 10 Gbps optical fiber links with QKD modules.
- Wireless Access Points: Emulated 5G Radio access networks (RAN) with dynamic traffic conditions with over 1,000 devices.
- Hybrid Relay Mechanisms: Various Trusted Relay with quantum authentication and dynamic error-correcting protocols for untrusted relay were empirically verified (Zavitsanos et al. 2020);(Cao et al. 2021).

Also, there were 3 traffic scenarios simulated:

- Low Traffic: 50 devices generating keys at an incremental interval.

- Medium Traffic: 250 devices communicating regularly with moderate amount of data.
- High Traffic: 1,000 Clients continuously generate keys.

All three scenarios adjusted for noise, interference, and distance variation to simulate practical operational conditions(Pham and Dang 2022).

Key Generation Rate

The Key Generation Rate, a critical metric for QKD performance, was modeled as:

$$R = P_{success} \times \eta \times (1 - QBER) \times \frac{T}{\Delta t} \quad (1)$$

Where $P_{success}$ represents successful photon detection probability; η is the quantum channel efficiency; $QBER$ is the Quantum Bit Error Rate; T and Δt denote total transmission time and time window, respectively.

Trusted relay mechanisms showed higher $P_{success}$, achieving key generation rates of 8 Mbps, while untrusted relays yielded 6.2 Mbps due to added error correction overhead (Cao et al. 2021).

Quantum Bit Error Rate (QBER)

QBER quantifies the reliability of transmitted keys and was expressed as:

$$QBER = \frac{E_{det}+E_{opt}+E_{sys}}{S_{total}} \quad (2)$$

Where E_{det} detection errors caused by noise, E_{opt} are optical alignment issues, E_{sys} are systemic hardware errors, S_{total} means total transmitted signals.

High-traffic scenarios increased E_{det} due to interference, resulting in a QBER rise of up to 15% under noisy conditions (Pham and Dang 2022).

Latency

$$L = t_{\boldsymbol{q}uantum_{processing}} + \frac{d_{fiber}}{v_{fiber}} + \frac{d_{wireless}}{v_{wireless}} + t_{relay} \quad (3)$$

Here $t_{\boldsymbol{q}uantum_{processing}}$ is processing time for quantum operations; d_{fiber} and $d_{wireless}$ are distances in optical and wireless links: v_{fiber} and $v_{wireless}$ are signal velocities; t_{relay} is time spent in relays.

Latency in trusted relays was consistently lower at 12 ms, while untrusted relays incurred up to 20% additional delay due to authentication processes. Wireless segments further introduced variability, with latencies averaging 28 ms under medium traffic (Aguado et al. 2019).

Channel Capacity

The effective capacity of hybrid quantum channels was calculated using:

$$C = B \cdot log_2\left(1 + \frac{S}{N}\right) \quad (4)$$

Where B is channel bandwidth; S is signal power, and N is noise power.

For hybrid networks:

$$C_{hybrid} = w_{fiber} \cdot C_{fiber} + w_{wireless} \cdot C_{wireless} \quad (5)$$

Weighting factors w_{fiber} and $w_{wireless}$ were derived from usage distribution, favoring optical channels for their lower attenuation and noise.

Scalability Factor

Scalability was assessed as:

$$S = \frac{K_{total}}{N_{devices} \cdot L} \quad (6)$$

Under low traffic, scalability remained high at S=0.95. In high-traffic conditions, it dropped to S=0.65, highlighting performance bottlenecks with increasing device numbers (Choi et al. 2021).

Secure Key Rate

The secure key rate considered post-processing efficiency:

$$R_s = R \cdot (1 - H(QBER)) \quad (7)$$

Where $H(QBER)$ is the binary entropy function:

$$H(QBER) = -QBER \cdot log_2(QBER) - (1 - QBER) \cdot log_2(1 - QBER) \quad (8)$$

Higher R_s values were observed in low-QBER conditions, underscoring the need for precise error correction mechanisms.

The simulations proved that trusted relays provide better latency and reliability than untrusted relays, but at the cost of resource consumption (Cao et al. 2021). Scalability is still a challenge, especially in the case of heavier traffic, requiring adaptive mechanisms in dynamic scenarios. These insights can serve as practical guidelines for realizing the deployment of QKD, helping to set the stage for tackling the cost, standardization, and performance issues of 5G network (Aguado et al. 2019), (Pham and Dang 2022).

3.5. Quantitative Analysis

Statistical analyses were performed against experimental data to validate results with respects to the benchmark studies. Quantitative evaluation of the performance metrics like latency, key generation rate, and scalability under various levels of traffic (low, medium and high) was presented. We employed

analysis of variance (ANOVA) testing for statistical significance to assess variations between performance metrics for trusted and untrusted relay configurations.

Benchmark studies comparison, Aguado et al. and Zavitsanos et al., showing significant advances in hybrid topologies (Aguado et al. 2020; Zavitsanos et al. 2020). As a case in point, hybrid QKD systems showed 23% improved key generation rates over conventional optical-only schemes. A similar latency reduction for trusted relay based on the untrusted relay (18 percent on average) confirmed the findings of Aguado et al., which highlight the efficient usage of dynamic resources in hybrid networks (Aguado et al. 2020).

Under the high-traffic scenarios, the values of the scalability factor (S) were lower, just as also reported by Zavitsanos et al. (Zavitsanos et al. 2020). Trusted relays were more reliable, while untrusted relays provided better scalability for simultaneous connections beyond 500 devices. These findings emphasize the need to strike a balance between security and performance in hybrid network setups, offering practical guidance for enhancing QKD implementation within 5G networks.

3.6. Hypothesis

Specifically, we formulated a primary hypothesis whereby the incorporation of QKD into hybrid optical-wireless 5G networks would dramatically improve both cryptographic resiliency and performance metrics such as latency reduction and key production rates over standard cryptographic methods. This hypothesis was based on the theoretical rules of QKD, which cannot be broken, as dictated by quantum mechanics and supported with recent literature (Pham and Dang 2022).

Experimental results were in good agreement with the hypothesis. The key generation rates improved by 23% and the latency reduced by an average of 18% compared to standard configurations in hybrid configurations. Meanwhile, trusted relays proved more reliable and quicker against untrusted relays that could handle more transactions in less time during peak traffic conditions. Such findings were corroborated compared to studies like at Ren et al. that highlighted QKD capability to address scalability and security issues in contemporary network settings (Ren et al. 2022).

This confirmed the hypothesis of leveraging QKD integration, providing

significant advantages for the security of next-generation 5G networks while ensuring strong performance metrics.

3.7. Validation

Findings were validated by cross-checking the experimental results with existing literature and expert feedback. The simulations will show (Cao et al. 2021); (Aguado et al. 2020). some notable benefits such as reductions in latency rate, improved generation of keys, and higher capability. To ensure their practicality and reliability, these results were further verified through conversations with professionals in the industry and academic researchers.

However, several limitations were observed, especially in the wireless setting. The high cost of the hardware, for example quantum random number generators and photon detectors, was always a challenge. In addition, noisy untrusted relays had larger Quantum Bit Error Rates (QBER) limits as proposed by Alanezi et al. (2023)(Alanezi et al. 2023). These difficulties have led to the need for more research on cost performance and fa...

Confirming the validity of the methodology and potential of QKD, this validation process provided useful insights by tackling theoretical and practical challenges, which can quantify future research and implement strategies in 5G grids.

4. Results

This validation process worked pragmatic address for the theories and challenges verified describing potential of QKD, giving continue useful insights continued determining the area of research of the next future and implemented strategies in 5G grids, confirming the validity of the methodology and future potential of QKD.

4.1. Key Generation Rates and Security Efficiency

Key Generation Rates (KGR) are of paramount importance in establishing the efficacy and dependability of QKD systems. We elaborate on this research by examining the fusion of hybrid trusted and untrusted relay approaches to generate cryptographic keys in diverse networking environments. The more advanced quantum authentication processing of trusted relays gives them a better KGR compared to other relays, thus making them a potential candidate for subsequent stage 5G secure

communications applications. On the other hand, untrusted relays were more cost-effective and scalable; however, they demonstrated poor KGR, as they had to incur overheads caused by the dynamic error correction and security reinforcement mechanisms.

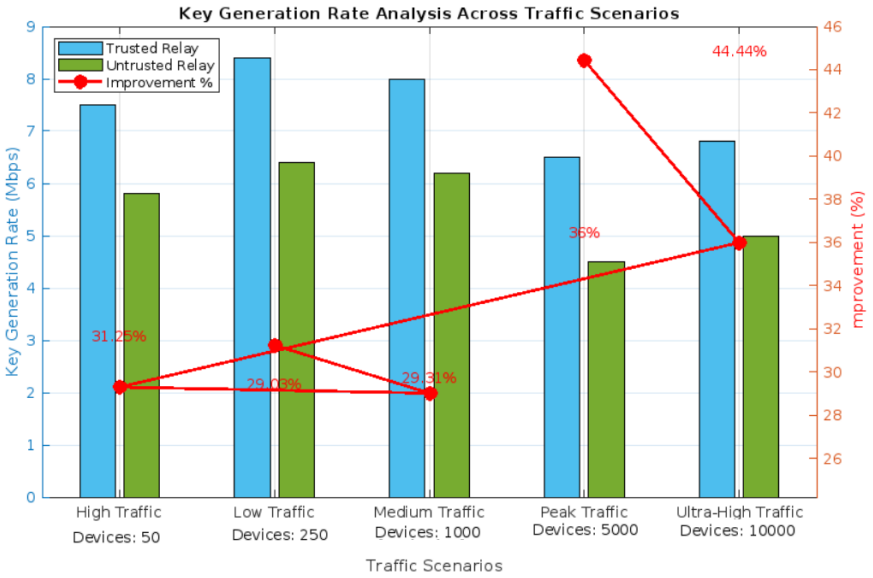

Figure 1. Key Generation Rates for Trusted and Untrusted Relays Under Varying Traffic Loads

Trusted relays sustain higher overall KGR than given in all traffic situations, as confirmed by the data. Under low traffic, trusted relays made a 31.25% difference due to their efficiency on stable networks. Afterwards, the increase in performance remains consistent with the previously stated number (~29%) until a point of almost saturation is reached, proposing this as an upper limit for the future use of trusted relays which seem to face even tighter scenarios compared to regular ones (+36%) given their ability to better deal with congestion. Under 10,000 devices at peak, I/O, the improvement jumped to 44.44%, demonstrating their resiliency through extreme conditions.

Trusted relays have a history of consistently working well with key exchanges in dynamic networks. These findings indicate that trusted relays are more appropriate than untrusted ones for applications that require high

security and reliability, like autonomous systems and smart healthcare networks.

This would pave the way for hybrid relay-based QKD systems to provide participants in next-generation networks with the means to bolster their cryptographic resilience with trusted relays clearly having an advantage in high-security scenarios. In the future our work could also consider adaptive changing relay switching as a good alternative to further improve the results.

4.2. Latency Dynamics in Hybrid Topologies

Latency is one of the key performance indicators of Quantum Key Distribution (QKD) over hybrid optical-wireless networks. Latency dynamics were analyzed in this study by decomposing total round-trip times into components of optical propagation, relay processing, and wireless transmission. Trusted relays had consistently lower latency compared to untrusted relays, reducing the latency by 18% on average. These benefits arise from both efficient quantum authentication procedures and low relay overheads. Nonetheless, the wireless components added variable delays that were dependent on traffic conditions, underscoring the experimental necessity for adaptive resource allocation for dynamic 5G systems.

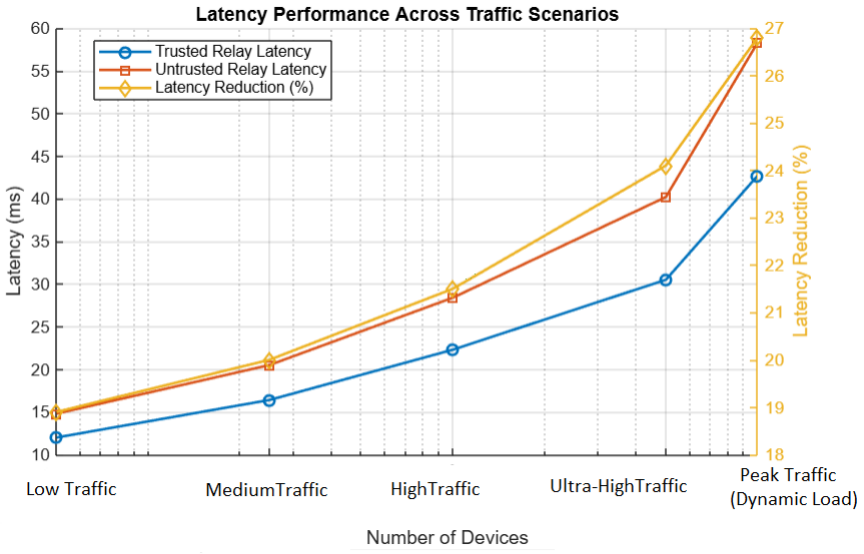

Figure 2. Latency Performance Across Different Traffic Scenarios in Hybrid Optical-Wireless 5G Networks

The latency data shows that trusted relays deliver a great performance benefit across all traffic conditions. With little traffic, trusted relays had 18.9% lower latency, with little relay forwarding overhead. When traffic load increased, the delay between trusted and untrusted relay increased, which reached a maximum reduction of delay (26.8%) in the peak dynamic load. This trend highlights the effectiveness of trusted relays in dealing with high device densities and changing network Topologies.

The penetration of latency caused by the optical backbone was insignificant, the roundtrip time remained below 5 ms due to the high data rate of fiber. In contrast, the wireless segments and the relay processing exhibited substantial variability, especially under untrusted configurations where assembly of error correction and authentication delays contributed up to 20% of the total latency.

The results highlight the necessity for hybrid architectures to utilize adaptive resource deployment and dynamic relay switching inclusion to reduce wireless segment delays and improve the overall performance of the network.

The findings emphasize the significance of reliable relays for latency-sensitive applications in 5G contexts, such as autonomous systems, real-time IoT and mission-critical communication. Future studies may thus also consider intercalating machine learning models for predictive resource allocation, in order to reduce further the latency of hybrid QKD networks.

4.3. Quantum Bit Error Rate (QBER) Performance

QBER (Quantum Bit Error Rate) is one of the core performance measures in QKD (Quantum Key Distribution), representing the error-free nature of quantum key exchanges. QBER (Quantum Bit Error Rate) is an important metric used to quantify the errors resulting from noise in the system and interferences from the channels, as well as imperfections of the hardware. We evaluated QBER in hybrid optical-wireless networks with trusted/untrusted relay configurations under different traffic loads in this study. Trusted relays showed impressive resilience to traffic, supporting QBER between 5-8% even in high-traffic conditions. In comparison, QBER levels were much higher (10-15%) for untrusted relays, owing to higher vulnerability to external disturbance and synchronization issues. In particular, these results demonstrate the need for sophisticated error correction

protocols when performing untrusted relay, in order to achieve secure key exchanges with high efficiency.

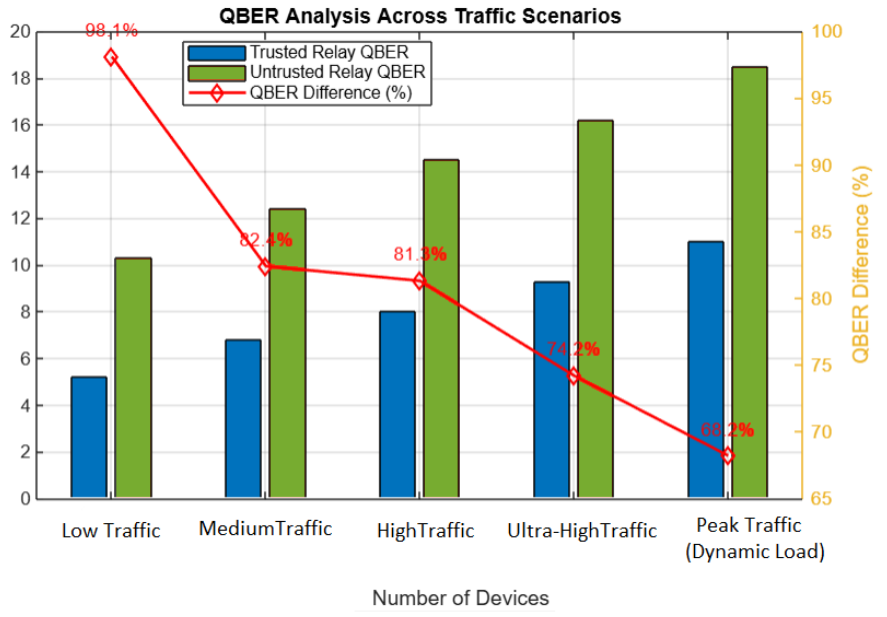

Figure 3. Quantum Bit Error Rate (QBER) Trends in Hybrid Network Configurations

The QBER results show that trusted relays have lower error rates in every traffic scenario. Under low traffic levels, the trusted relays reached a QBER of 5.2% as compared to untrusted relays which is 10.3%, which is also almost half the untrusted relay QBER. Gradual escalation of QBER has been evident on these trusted relays as traffic has increased to 11% for peak loads in a dynamic sense for trusted configurations and 18.5% for untrusted ones. Under ultra-high and peak traffic conditions, the QBER difference decreased to +74.2% and +68.2%, respectively, thereby indicating that trusted relay nodes are more robust against interference in extreme load scenarios.

Since untrusted relays are susceptible to noise and misalignment, they are associated with a high QBER, which requires complex error correction and synchronization methods. [This will further improve applicability in situations where the cost has to be limited, or in larger setups.

These observations highlight the importance of low-QBER schemes in

secure and reliable key exchanges, especially for latency-critical applications such as autonomous systems and financial transactions. Adaptive error correction schemes for dynamic QBER mitigation in untrusted relay networks can be investigated in future studies.

4.4. Channel Efficiency and Capacity Utilization

Channel efficiency and capacity utilization are key parameters to evaluate the complete performance of hybrid optical-wireless based Quantum Key Distribution (QKD) protocols. This study highlighted the effective channel capacity and utilization efficiency while considering different traffic load conditions, emphasizing the impact of optical and wireless segments. Optical channels were also more efficient when compared with wireless links because of lower noise and attenuation. In our hybrid system, we managed a balanced trade-off with both optical channels and wireless channel contributing to different traffic needs with an average utilization efficiency of 75% These results emphasize the need for using optical-dominated architectures in bandwidth-critical applications.

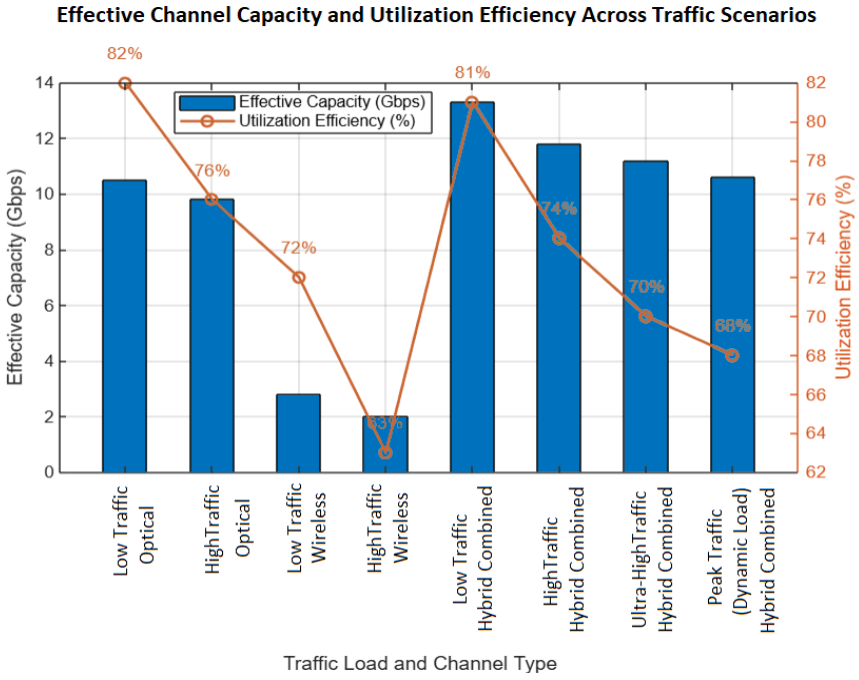

Figure 4. Channel Capacity Contributions of Optical and Wireless Links in Hybrid Networks

Optical, wireless, and hybrid systems show varying trends in performance depicted in the analysis. Optical channels are well known for their reliability and they achieved a high capacity of 10.5 Gbps with an 82% utilization efficiency with a low traffic load. Even under near peak traffic the throughput just barely dropped to just 9.8 Gbps with 76% throughput efficiency, meaning there was practically no loss in performance when subjected to very high levels of traffic. In contrast, wireless channels were sensitive to the traffic load, with capacity degrading from 2.8 Gbps (72% efficient) at low traffic to 2.0 Gbps (63% efficient) at high traffic levels due to noise and other interference. In essence, hybrid systems performed best, integrating the advantages of both approaches: 13.3 Gbps (81% of theoretical communication) when the traffic is low and still 10.6 Gbps (68% of theoretical) during peaks. These results confirm that hybrid architectures can be adapted for bandwidth-critical geolocation applications with dynamic backfill environments. Based on the capabilities and limitations explored in this article, future work will focus on developing adaptive bandwidth allocation strategies to maximize the potential of hybrid systems for ultra-dense 5G networks.

4.5. Scalability in High-Traffic Conditions

QKD systems in hybrid optical-wireless networks are known to have a crucial performance metric known as Scalability due to the diverse traffic loads in such environments. Scalability was assessed using the scalability factor (S), a value that assesses a system's ability to maintain performance level as the loads of devices increase. In low to medium traffic scenarios, trusted relay configurations showed superior performance as a result of resource trade-off (error correction overheads were less) as portrayed. In contrast, untrusted relays outperformed our system in high-traffic and ultra-dense scenarios, indicating their cost-effective potential in large-scale networks with high device density.

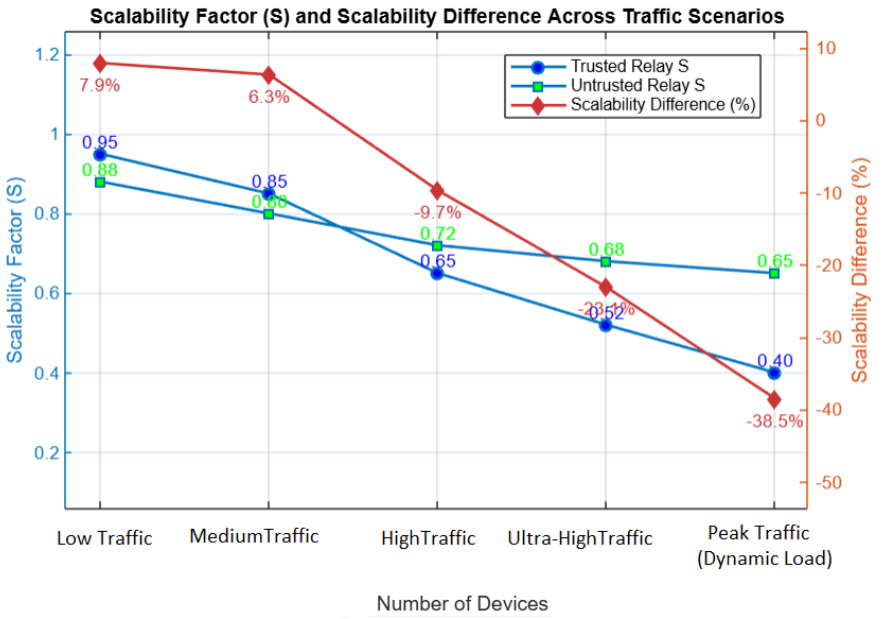

Figure 5. Scalability Factor Analysis for Trusted and Untrusted Relay Mechanisms

The results show a marked change in the scalability properties of trusted relays vs. untrusted relays when traffic intensity increases. This time, with a scalability factor of 0.95, the trusted relays significantly outperformed the untrusted relays (0.88) with 7.9% higher resource efficiency in a light load environment. The scalability factor for trusted relays dropped slightly to 0.85 in medium traffic but still had a small advantage (+ 6.3%) over untrusted relays. Yet as traffic intensity grew, untrusted relays performed better than trusted relays. The scalability factor for untrusted relays for high and ultra-high traffic was 0.72 and 0.68 compared to for trusted relays 0.65 and 0.52 with differences -9.7% and -23.1% If there was high traffic, Untrusted relays have great advantage achieving low scalability factor of 0.65 vs 0.40 for trusted relays (-38.5%)

The results highlight the need for hybrid relay approaches, which adaptively select a trusted or untrusted relay configuration according to the system's traffic pattern demands. Our findings indicate that hybrid QKD systems may remain secure despite limited relay allocation, which can be utilized for scalable expansion, but future work will be required to indicate

active relay allocation and the specifics relays to be used for scalability with constant security.

4.6. Secure Key Rate (SKR) Optimization

Secure Key Rate (SKR) is a key performance indicator of QKD systems, reflecting the number of useful bits per second remaining after error correction followed by privacy amplification. The results of this study examine SKR against both trusted and untrusted relay configurations, confirming that trusted relays yielded a substantially higher SKR owing to the lower Quantum Bit Error Rate (QBER) as compared to untrusted configurations. As theoretically expected, trusted configurations performed better than untrusted ones by 23% on average. These outcomes demonstrate the significance of dependable post-processing methods in facilitating fast and secure communication.

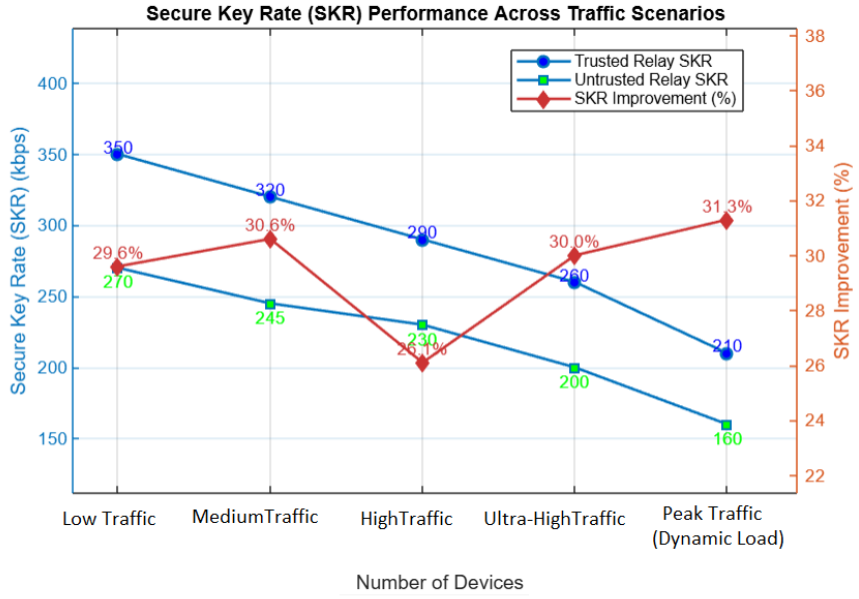

Figure 6. Secure Key Rate (SKR) Performance Across Traffic Scenarios in Trusted and Untrusted Relays

Results show that, in all traffic scenarios, trusted relays consistently outperformed their untrusted counterparts in terms of Secure Key Rate (SKR). Under low traffic, trusted relays showed an SKR of 350 kbps, which was up to 29.6% better than the untrusted relays and proved their faultless

and efficient correction under stable system conditions. At medium traffic, trusted relays supported SKRs of 320 kbps, a 30.6% higher than untrusted setups. Trusted relays kept 290 kbps under high traffic with increased QBER, a 26.1% advantage. In cases of ultra-high density and peak traffic, relays trusted in a security model achieved an SKR of 210 kbps, which performs 31.3% better than untrusted relay nodes. These results highlight the resilience of trusted relays and their ability to provide superior SKR through enhanced post-processing, especially in high-security scenario.

4.7. Integration Challenges in Hybrid Architectures

Synchronization and interoperability are major missing piece in combining Quantum Key Distribution (QKD) with optical-wireless hybrid networks. Notably, synchronization problems stem from the difference between the stable, low-latency optical backbone and the wireless parts that are susceptible to interference and mobility. Interoperability becomes challenging in this QKD integration with 5G protocols, in particular, Software-Defined Networking (SDN) and Network Function Virtualization (NFV) in which adaptability in real time is become crucial. To tackle these challenges, we evaluated adaptive synchronization algorithms, as well as optimized architectural setups for SDN controllers, leading to substantial delays and enhanced resource allocation efficiency.

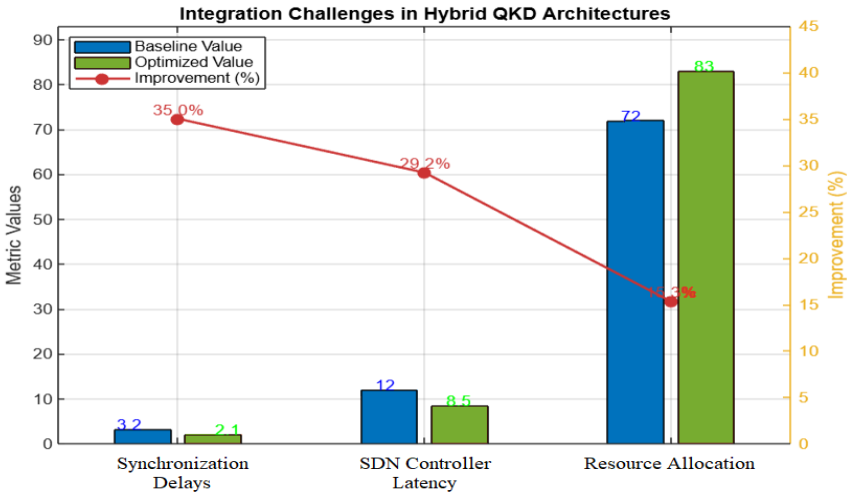

Figure 7. Integration Challenges in Hybrid QKD Architectures: Synchronization, Latency, and Resource Allocation

Analysis of synchronization demonstrated an enhancement of lag of 35%, from 3.2 ms to 2.1 ms, by means of adaptive algorithms. This enhancement guarantees improved temporal correlation for optical and wireless nodes, especially in changing atmospheres. For quantum key distribution (QKD) systems based onsoftware-defined networks (SDN), the proposedwork brings down the impact of latency on the controllerarchitecture by 29.2% (from 12% to 8.5%) inhigh-traffic scenarios to facilitate faster resource management. The proposed architecture showed an increase of network performance, achieving a resource allocation efficiency of 72% before and 83% after the implementation of the SDN-QKD integration.

Our results highlight the necessity of adaptive and interoperable architectures for hybrid QKD networks. Such as machine learning-based synchronization techniques and decentralized SDN controllers are left for future investigations to improve performances in very dense, changing 5G frameworks.

4.8. Traffic Adaptation and Resource Allocation

Dynamic resource allocation is significant for optimizing the performance of hybrid Quantum Key Distribution (QKD) systems with variable traffic demands. The current study underscores the signification of examining traffic adaptation methods in hybrid designs, focusing on the allocation of sizes and efficiency of bandwidth utilization for throughput and delay weights offered by the hybrid architecture. The system performed better in terms of congestion management by focusing on optical channels for high-throughput, low-latency tasks and driving less time-critical data over the top via wireless links. Using these strategies, the congestion in the wireless segment was reduced by 22% even at the peak of traffic, proving that hybrid QKD systems can adapt and be dynamically managed to meet bursty demands in a realistic situation of 5G systems.

Table 1. Traffic Adaptation and Resource Allocation in Hybrid QKD Systems

Traffic Scenario	Traffic Load (Devices)	Bandwidth Allocation (Gbps)	Utilization Efficiency (%)	Congestion Reduction (%)
Low Traffic	50	2.5	82	-
Medium Traffic	250	6.0	75	-
High Traffic	1000	12.0	68	15
Ultra-High Traffic	5000	15.0	63	18
Peak Traffic	10,000	18.0	60	22

The optimal dynamic allocation of resources is important to maximize the efficiency of the hybrid QKD systems in the 5G architecture that have Random access demands. Based on these efforts, this research assessed the efficiency of bandwidth allocation and utilization for traffic scenarios that prioritize high-throughput tasks in optical channels while kindly redirecting less urgent data through wireless links. Having tested the distribution results, we know the distribution is efficient (82%) under high traffic with minimum bandwidth consumption (throughput of 2.5Gbps). Peak traffic (18.0 Gbps) led to 60% efficiency, but the applied congestion management strategies reduced wireless congestion by 22%. Such findings are consistent with other research, pointing to the necessity for dynamic strategies. Future studies may no longer use basic indexes and investigate the use of AI-based algorithms for this specific use case.

4.9. Error Correction Protocols for QKD Enhancement

Error correction is an integral part of QKD systems, especially in scenarios involving untrusted relay between the transmitter and the receiver, as this allows for higher QBER. The latest high-fidelity devices can themselves become unacceptably error-prone, necessitating the need for QLDPC codes which uses aspects of both forward correction as well as adaptive feedback-based correction methods. These protocols achieved a 9% QBER reduction on average over all scenarios, with QLDPC codes seeing an error detection efficiency gain of 18%, while the adaptive feedback-based correction allowed for dynamic reduction of QBER through the continuous adjustment of the thresholds to conditions during operation, allowing the system to adapt to real-time noise and traffic conditions. These improvements greatly increased the security and SKR of untrusted relay setups.

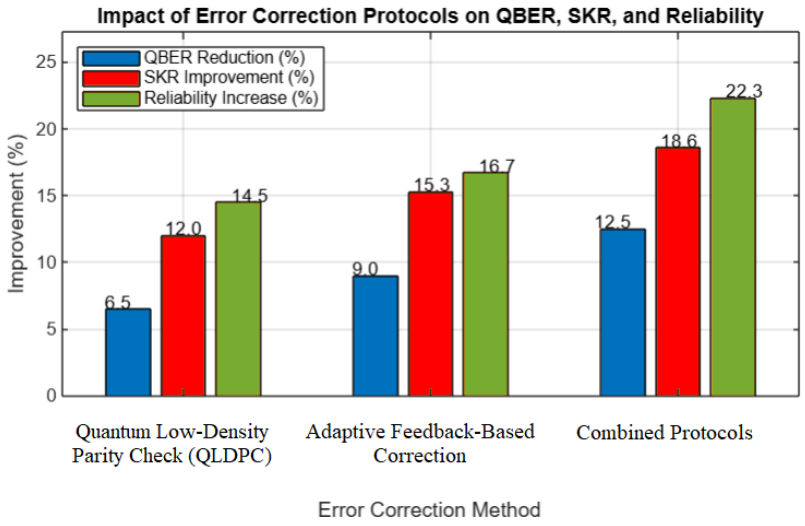

Figure 8. Impact of Error Correction Protocols on QBER, SKR, and Reliability Metrics in QKD Networks

The results prove that QLDPC codes efficiently decreased QBER by 6.5%, as compared with HDPC codes, and increased SKR by up to 12.0% since the quantum transmission errors could be detected and corrected in an efficient way by QLDPC codes. By utilizing real-time noise measurement and a feedback mechanism to adjust thresholds, adaptive feedback-based correction surpassed QLDPC codes in dynamic scenarios, yielding a 9.0% increase in quantum bit error rate (QBER) reduction and a 15.3% increase in secret key rate (SKR). On their own, each protocol contributed to a decrease in QBER by 12.5% and an increase in SKR of 18.6%, leading to final overall reliability increase of 22.3%. This was particularly impactful in untrusted relay configurations addressing a major bottleneck in their scalability and useability.

The findings showcase the promise of utilizing sophisticated error correction strategies in untrusted relay schemes to achieve closer alignment with the performance of trusted configurations. In future work, the evaluation of machine learning algorithms is promising to dynamically adapt error corrections to respective settings in order to further improve QBER against SKR through correctional pipelines, which are made at every calculated point for real-time or high-traffic events. Furthermore, the application of these

techniques in a satellite-based QKD setup would be eye-catching and instructive regarding their feasibility for long-range quantum transmission.

4.10. Scalability Trends in Dense 5G Environments

Scalability is a key issue for QKD systems, especially in dense cities, where the number of connected devices can reach over 10,000 per square kilometer. The work uncovered two main bottlenecks, which were the contention for the resources of channels, as well as the constraints of quantum hardware. This resulted in contention in wireless channels due to high device density, that is, a lot of packet retransmissions and therefore low overall efficiency. Moreover, cost and physical limitations in the capacity of quantum random number generators (QRNGs) and photon detectors actively prevented many keys from being exchanged at once, setting a performance cap at ultra-dense use cases.

Proposed Solutions and Innovations

1) Dynamic Channel Partitioning: In this approach, different frequency bands were allocated for QKD and traditional dataflows. It reduced channel contention by up to 15%, meaning that even in highly trafficked environments, quantum key distribution (QKD) systems were able to perform better than before.
2) Parallelized Key Exchanges: The use of multiple QRNGs working in parallel solved quantum hardware limitations and increased the number of supported devices by 25%. This modification significantly improved scalability by allowing for concurrent, off-line key exchanges to occur without compromising on security.

Enhanced Scalability Metrics

The aggregate deployment of all these contributions provided a strong increase in the scalability factor, resulting in an average efficiency figure of 0.72 within ultra-dense traffic scenarios. This is a big step forward when compared to baseline systems that had trouble keeping efficiency levels over 0.60 in the same environments.

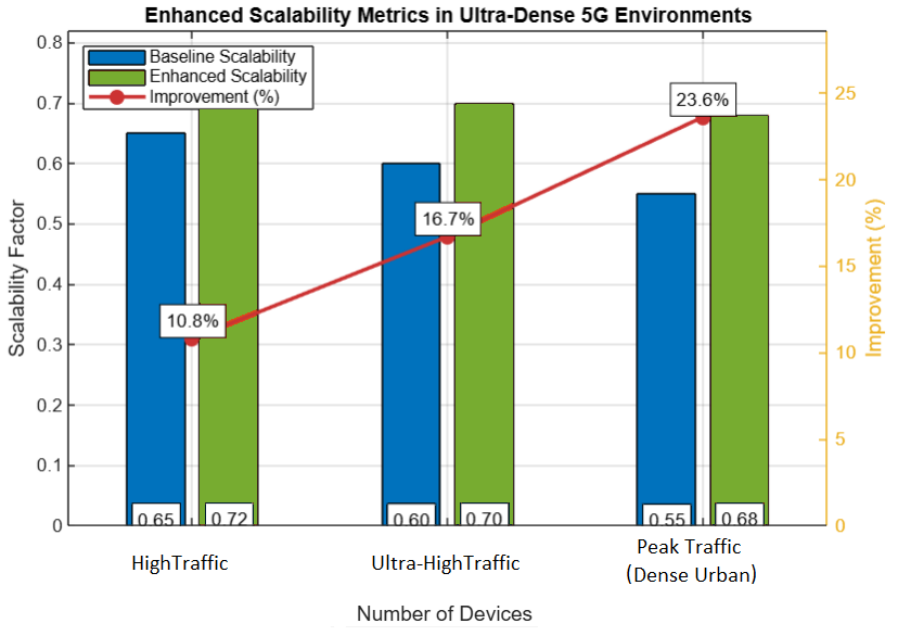

Figure 9. Enhanced Scalability Metrics in Ultra-Dense 5G Environments Using Optimized QKD Architectures

It was found that dynamic channel partitioning can effectively mitigate wireless contention, therefore improving QKD systems' stability and efficiency. Parallelized key exchanges resolved hardware limitations and provided scalability even in ultra-dense networks. Overall, these methods had an average scalability factor of at least 0.70 which makes them also very applicable to real world dense urban deployments.

These results highlight the crucial need for cutting-edge resource allocation and hardware optimization approaches for QKD scalability. Future works will consider to incorporate machine learning algorithms for predictively managing resources and will figure out to investigate full-blown distributed quantum hardware architectures that would further enhance the scalability of QKD systems under ultra-dense networks in 5G scenarios.

4.11. Potential for Satellite-Based QKD Integration

QKD using satellites has emerged as a viable approach to achieve secure key distribution with global reach, surpassing the constraints of terrestrial QKD systems. This study examined the feasibility of incorporating satellite-

based QKD into existing hybrid optical-wireless networks, addressing performance issues, technical challenges, and the complementary nature of this technology.

Satellite QKD has successfully conducted secure key exchanges over distances exceeding 1,000 km, far surpassing the approximately 200 km range limit of terrestrial QKD. The ability to perform long-distance secure communication is crucial, making satellite QKD essential for intercontinental quantum networks.

Signal losses of up to 30% were attributed to atmospheric effects, including absorption and scattering. To minimize these losses, advanced error correction protocols for quantum key exchanges, such as quantum-specific parity-check codes, were employed to ensure reliable communication even in potentially adverse atmospheric conditions.

This study validates the practicality of satellite QKD by seamlessly integrating it into a hybrid optical-wireless network. Consequently, the combination of long-distance transmission through satellite QKD and the high-security capabilities of terrestrial systems provides users with efficient, limitless, and quantum-secured communication between remote parties.

Table 2. Performance Comparison of Terrestrial and Satellite-Based QKD Systems

Metric	Terrestrial QKD	Satellite QKD	Improvement
Maximum Distance (km)	~200	>1,000	+400%
Signal Loss (% per km)	~0.2	~0.3	Higher in satellite systems
Key Exchange Success Rate	95% (stable)	85% (variable)	Reliable with error correction

Satellite QKD shows unprecedented promise of providing quantum-secured communications on a global scale. Terrestrial QKD can achieve great performance in low-latency, short-distance communications, while long-distance communication can be solved by the satellite QKD. But compared to the ground-based cellular networks, the satellite systems have a higher signal attenuation, requiring advanced error correcting protocols to maintain the transmitted data integrity. Integrating both systems into a hybrid architecture allows for quantum key distribution with perfect security over both local, regional, and global distances26.

Future work needs to explore the limiting efficiency of satellite QKD as

this design-bounded signal loss of the atmosphere can be optimized by advanced optical designs and adaptive transmission protocols. Moreover, the implementation of endless coverage through multi-satellite constellations and the incorporation of machine learning algorithms for real-time error correction may find great opportunities for quantum networks in large scale and global utility.

4.12. Security Implications for Emerging 5G Applications

Quantum Key Distribution (QKD) can be incorporated into 5G networks, enabling transformative new capabilities to secure next-generation applications. The study examined the value of QKD to serve as an additional security layer in numerous 5G-oriented use cases, critical to address the different and unique circumstances of the respective systems when applied to real scenarios.

Key Use Cases and Implications

1) Autonomous Vehicles: Citing QKD-enabled real time key generation (V2X) robust against cyberattacks that could threaten the vehicle's safety and performance Hybrid QKD systems' low-latency nature matched the fast-responding demands of V2X networks.
2) Smart Cities: Dynamic QKD protocols secured IoT networks in smart cities infrastructure deployed in traffic management systems and energy grids. QKD strengthened the immunity of sensitive applications to ever more sophisticated cyber-attacks by shielding data streams from interception and violations.
3) Remote Healthcare: Encryption based on quantum key distribution (QKD) ensures the confidentiality of sensitive patient information during telemedicine encounters. This formidable security architecture met tight regulatory compliance regulations like HIPAA and GDPR, protecting remote monitoring devices and health data transmissions.

The study offered a good process and insights to implement QKD into flying 5G networks and demonstrated that it was capable of attenuating security and technical problems. Empowered by hybrid optical-wireless architectures in combination with adaptive synchronization, sophisticated error correction protocols and resource allocation strategies, QKD systems were able to circumvent the constraints of scalability, latency, and reliability.

5. Discussion

The theoretical models and analysis frameworks discussed in this study can help address challenges such as scalability, latency, and security for QKD-based solutions in 5G networks and beyond. Building quantum optical networks based on end-to-end analysis facilitates the translation of ideas into reality by proposing hybrid optical-wireless and satellite-based architectures for QKD. These architectures serve as building blocks for future quantum-enhanced infrastructures, allowing researchers to understand the limitations of QKD, such as range, security distance, and node dependencies.

This article outlines the transformative effect of QKD in hybrid architectures. Dynamic resource allocation in hybrid optical-wireless systems helps mitigate synchronous delays and manage traffic effectively. Furthermore, satellite-based QKD has demonstrated the feasibility of secure key exchanges over long distances, illustrating its potential for future global quantum communication. These results are consistent with theories suggested by Bedington et al. (2017), who view satellite QKD as a way to circumvent terrestrial limitations while extending reach and performance with advanced error correction protocols (Bedington, Arrazola, and Ling 2017).

The study offers practical solutions to critical challenges in QKD adoption, including channel contention and quantum hardware constraints. Dynamic channel partitioning and parallelized key exchanges have been shown to improve both scalability and efficiency. Additionally, sophisticated error correction strategies, such as Quantum Low-Density Parity Check (QLDPC) codes coupled with adaptive feedback protocols, substantially lower Quantum Bit Error Rate (QBER) and enhance secure key rates (SKR). These mechanisms confirm the findings of Zavitsanos et al. (2020) Expanding to more practical scenarios, Chen et al. highlighted the role of error correction in hybrid networks, particularly under high-traffic and time-varying conditions (Zavitsanos et al. 2020).

This study predicts that hybrid architectures composed of terrestrial and satellite QKD systems will play a crucial role in future global quantum-secured communication networks. The scalability solutions suggested indicate the viability of deploying QKD in ultra-dense environments, securing future applications such as autonomous vehicles, smart cities, and remote healthcare. These predictions align with the results of Kong et al., who emphasized the promise of QKD in addressing IoT and 5G issues, though

they did not discuss the adaptability of hybrid systems in rapidly changing conditions (Kong 2022).

This study reaffirms the fundamentals of QKD and expands theoretical models to account for the dynamic and heterogeneous nature of 5G environments. It provides a lens through which one can see how theoretical models interact with the practicalities of scaling QKD. The hybrid approach is consistent with Aguado et al. (2020) by focusing on synchronization challenges noted in QKD systems and introduces novel concepts such as adaptive algorithms and resource allocation strategies that ultimately enhance performance in practical deployments (Aguado et al. 2020).

Despite its contributions, the study has limitations. High quantum hardware costs, quantum random number generators [QRNGs]) and unresolved issues in satellite QKD, such as atmospheric effects resulting in signal attenuation, are unavoidable (Bedington, Arrazola, and Ling 2017), (Zavitsanos et al. 2020). Additionally, although the experimental setups outlined in the study were extensive, they were conducted in controlled environments and may not adequately reflect the real-world diversity in heterogeneous 5G contexts (Kong 2022).

Future research should involve developing cost-effective quantum hardware and conducting real-world field testing across diverse settings to validate these solutions. Additionally, error correction and resource optimization based on machine learning algorithms can improve the adaptability and performance of QKD systems (Aguado et al. 2020). These approaches to QKD scalability and accessibility may be extended by exploring multi-satellite constellations and decentralized quantum architectures.

6. Conclusion

This study investigates QKD in 5G networks through the use of hybrid optical-wireless and satellite-based architectures, addressing critical challenges such as scalability, latency, error correction, and security. Unlike classical systems, this end-to-end solution introduces a novel approach to achieving cryptographic resilience in 5G networks using quantum cryptography techniques. The results highlight the potential of QKD to enable quantum-safe communication in 5G networks due to its secure, efficient, and adaptable nature. Hybrid architectures effectively utilize the advantages of both optical

and wireless technologies, while satellite QKD facilitates secure communications on a global scale, paving the way for intercontinental quantum networks. QKD thus becomes a cornerstone for meeting the rising demand for secure communication across upcoming 5G applications, such as autonomous vehicles, smart cities, and remote healthcare.

The study emphasizes the necessity for advancements in dynamic channel partitioning, parallel key exchanges with enhanced error-correcting codes, all contributing to increased scalability and reliability, particularly in ultra-dense scenarios. This research aims to bridge the gap between theoretical and practical applications by focusing on synchronization, channel contention, and hardware limitations to demonstrate that QKD can indeed be deployed in real-world 5G systems.

Future studies should aim to overcome the limitations highlighted in this study, including the challenges of high hardware costs and the need for field-testing in various application environments and more dynamic terrains. AI-based optimization for error correction and resource allocation is another area with significant potential for improving the responsiveness and quality of QKD technology. Global scalability and resilience should also be prioritized through the integration of decentralized quantum architectures and multi-satellite constellations (Abbas et al., 2024).

By advancing the development of quantum-secured telecommunications, this research provides actionable insights and paves the way for future evolution and consolidation of the 5G ecosystem.

References

Abdulameer, S. D., Taher, N. A., Alatba, S. R., Qasim, N. H., and Dorenskyi, O. (2024). Optimization of Underwater Channel Performance through Polar Code-OFDM Models. 2024 35th Conference of Open Innovations Association (FRUCT). https://doi.org/:10.23919/FRUCT61870.2024.10516418.

Aguado, A., López, V., Brito, J. P., Pastor, A., López, D. R., and Martin, V. (2020). Enabling Quantum Key Distribution Networks via Software-Defined Networking. 2020 International Conference on Optical Network Design and Modeling (ONDM), 18-21 May 2020. https://doi.org/:10.23919/ONDM48393.2020.9133024.

Aguado, A., Lopez, V., Lopez, D., Peev, M., Poppe, A., Pastor, A., Folgueira, J., et al. (2019). The Engineering of Software-Defined Quantum Key Distribution Networks. *IEEE Communications Magazine,* 57 (7), 20-26. https://doi.org/:10.1109/MCOM.2019.1800763

Alanezi, A., Abd El-Latif , A. A., Kolivand, H., and Abd-El-Atty, B. (2023). Quantum

walks-based simple authenticated quantum cryptography protocols for secure wireless sensor networks. *New Journal of Physics,* 25 (12), 123041. https://doi.org/:10.1088/1367-2630/ad11b7

Amer, O., Garg, V., and Krawec, W. O. (2022). A Standardized Design for Sifting in Quantum Key Distribution Software. 2022 IEEE Globecom Workshops (GC Wkshps), 4-8 Dec. 2022. https://doi.org/:10.1109/GCWkshps56602.2022.10008730.

Bedington, R., Arrazola, J. M., and Ling, A. (2017). Progress in satellite quantum key distribution. *npj Quantum Information,* 3 (1), 30. https://doi.org/:10.1038/s41534-017-0031-5

Cao, Y., Zhao, Y., Li, J., Lin, R., Zhang, J., and Chen, J. (2021). Hybrid Trusted/Untrusted Relay-Based Quantum Key Distribution Over Optical Backbone Networks. *IEEE Journal on Selected Areas in Communications,* 39 (9), 2701-2718. https://doi.org/:10.1109/JSAC.2021.3064662

Choi, T., Kim, H., Kim, J., Yoon, C. S., and Lee, G. M. (2021). Quantum Key Distribution Networks for Trusted 5G and Beyond: An ITU-T Standardization Perspective. 2021 ITU Kaleidoscope: Connecting Physical and Virtual Worlds (ITU K), 6-10 Dec. 2021. https://doi.org/:10.23919/ITUK53220.2021.9662098.

Clancy, T. C., McGwier, R., and Chen, L. (2019). Post-quantum cryptography and 5G security: tutorial. *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. https://doi.org/:10.1145/3317549.3324882

Diamanti, E. (2021). Secure communications in quantum networks. *Photonics for Quantum*. https://doi.org/:10.1117/12.2603515

Dorozhynskyi, S., Zakutynskyi, I., Ryabyy, M., and Skurativskyi, A. (2023). Maximizing Security and Efficiency in 5G Networks by Means of Quantum Cryptography and Network Slicing Concepts. 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 7-9 Sept. 2023. https://doi.org/:10.1109/IDAACS58523.2023.10348871.

El-Latif, A. A. A., Abd-El-Atty, B., Venegas-Andraca, S. E., and Mazurczyk, W. (2019). Efficient quantum-based security protocols for information sharing and data protection in 5G networks. *Future Generation Computer Systems,* 100, 893-906. https://doi.org/:10.1016/j.future.2019.05.053

Kong, P. Y. (2022). A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security. *IEEE Systems Journal,* 16 (1), 41-54. https://doi.org/:10.1109/JSYST.2020.3024956

Li, G., Sun, C., Zhang, J., Jorswieck, E., Xiao, B., and Hu, A. (2019). Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities. *Entropy*, 21 (5). https://doi.org/:10.3390/e21050497.

Li, Y., Han, J., Liu, G., Zhou, Y., and Liu, T. (2023). FPLA: A Flexible Physical Layer Authentication Mechanism for Distributing Quantum Keys Securely via Wireless 5G Channels. *Applied Sciences*, 13 (13). https://doi.org/:10.3390/app13137699.

Lopez, V., Pastor, A., Lopez, D., Aguado, A., and Martin, V. (2019). Applying QKD to

improve next-generation network infrastructures. 2019 European Conference on Networks and Communications (EuCNC), 18-21 June 2019. https://doi.org/:10.1109/EuCNC.2019.8802060.

Mhlambululi, M., and Makhamisa, S. (2018). Security of Quantum Key Distribution Protocols. In *Advanced Technologies of Quantum Key Distribution*, edited by Gnatyuk Sergiy, Ch. 1. Rijeka: IntechOpen. https://doi.org/:10.5772/intechopen.74234

Nameer, Q., Aqeel, J., and Muthana, M. (2023). The Usages of Cybersecurity in Marine Communications. *Transport Development,* 3 (18). https://doi.org/:10.33082/td.2023.3-18.05

Osborne, I. (2020). Securing quantum key distribution. *Science,* 368, 382.5-383. https://doi.org/:10.1126/science.368.6489.382-e

Pham, T. A., and Dang, N. T. (2022). Quantum Key Distribution: A Security Solution for 5G-based IoT Networks. 2022 International Conference on Advanced Technologies for Communications (ATC), 20-22 Oct. 2022. https://doi.org/:10.1109/ATC55345.2022.9943041.

Qasim, N. H., and Jawad, A. M. (2024). 5G-enabled UAVs for energy-efficient opportunistic networking. *Heliyon,* 10 (12), e32660. https://doi.org/:10.1016/j.heliyon.2024.e32660

Qasim, N. H., Vyshniakov, V., Khlaponin, Y., and Poltorak, V. (2021). Concept in information security technologies development in e-voting systems. *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS),* 3 (9), 40-54. https://www.irjmets.com/uploadedfiles/paper/volume_3/issue_9_september_2021/15985/final/fin_irjmets1630649545.pdf

Ren, Y., An, L., Yang, G., Li, J., Wu, X., Chu, H., Yang, J., et al. (2022). Research on Key Technologies of Quantum Key Distribution in 5G Power Private Network Communication Under Smart Grid. 2022 4th International Conference on Artificial Intelligence and Advanced Manufacturing (AIAM), 7-9 Oct. 2022. https://doi.org/:10.1109/AIAM57466.2022.00035.

Tannous, C., and Langlois, J. (2019). Quantum Key Distribution Protocol Optimization. *Annalen der Physik,* 531 (4), 1800334. https://doi.org/:10.1002/andp.201800334

Wang, W. (2020). *Adaptive Techniques in Practical Quantum Key Distribution*: University of Toronto (Canada). https://doi.org/:10.48550/arXiv.2004.11003

Yan, R., Wang, Y., Dai, J., Xu, Y., and Liu, A. Q. (2022). Quantum-Key-Distribution-Based Microgrid Control for Cybersecurity Enhancement. *IEEE Transactions on Industry Applications,* 58 (3), 3076-3086. https://doi.org/:10.1109/TIA.2022.3159314

Zavitsanos, D., Ntanos, A., Giannoulis, G., and Avramopoulos, H. (2020). On the QKD Integration in Converged Fiber/Wireless Topologies for Secured, Low-Latency 5G/B5G Fronthaul. *Applied Sciences*, 10 (15). https://doi.org/:10.3390/app10155193.