Proceedings of CONF-SEML 2025 Symposium: Strategic Learning in Machine Intelligence
DOI: 10.54254/2755-2721/2025.BA23841

Quantum-Enhanced Converged Wireless-Fiber 5G Fronthaul System: Security and Performance Optimization

Haonan Dong

University of Electronic Science and Technology of China, Chengdu, China
1748357466@qq.com

Abstract: With the global deployment of 5G networks, the demand for high bandwidth and low latency has driven innovations in fronthaul architectures. However, traditional solutions face challenges related to security and signal interference. This paper proposes an innovative quantum-enhanced converged wireless-fiber 5G fronthaul system that integrates quantum key distribution (QKD) technology with a passive wavelength division multiplexing (WDM) architecture to achieve physical-layer secure communication. The system deploys the quantum transmitter (Alice) at the active antenna unit (AAU) side and the receiver (Bob) at the distribution unit (DU) side, leveraging the Heisenberg Uncertainty Principle, quantum measurement collapse theory, and the no-cloning theorem to detect eavesdropping attempts. Simulation results demonstrate the significant impact of noise detection probability, fiber loss, and transmission distance on both the secure key rate and quantum bit error rate (QBER). Key findings highlight the need to minimize fiber loss, reduce transmission distance, lower filter loss, decrease noise detection probability, and improve detection efficiency. These optimizations collectively enhance the secure key rate while reducing the QBER, thereby improving overall system reliability. Remarkably, this solution achieves these security enhancements without requiring large-scale modifications to existing infrastructure, offering a practical and cost-effective upgrade path for current 5G deployments while providing a future-proof foundation for emerging 6G networks. The architecture's inherent scalability and compatibility make it particularly suitable for high-security applications, including government communications, financial transactions, and critical infrastructure protection—bridging the gap between theoretical quantum security and practical wireless network implementation.

Keywords: QKD, 5G fronthaul, Wireless-fiber convergence, Secure Key Rate, QBER

1. Introduction

5G has been rapidly deployed worldwide since its commercial launch in 2019, significantly enhancing connectivity and enabling smarter industries. The core features and advantages of 5G can be summarized into four aspects: high speed (data transmission rates of up to 10 Gbps), low latency (as low as 1 millisecond), massive device connectivity, and high spectral efficiency [1]. In terms of key technologies, 5G comprises both wireless and fiber-optic components. The wireless segment includes millimeter-wave technology, which enables higher data rates; small cells that enhance

DOI: 10.54254/2755-2721/2025.BA23841

signal coverage and network capacity; Massive MIMO (multiple input, multiple output) to improve spectral efficiency by increasing the number of antennas; beamforming for precise signal direction control; full-duplex technology, which allows simultaneous transmission and reception on the same frequency [2]; edge computing to reduce latency by processing data closer to end users; and network slicing to provide customized virtual networks for diverse applications.

However, the evolution of wireless communication does not stop there. The advent of 6G promises to extend these boundaries even further, offering unprecedented performance and capabilities. Key advantages of 6G include significantly higher data transmission speeds, ultra-low latency, and enhanced device connectivity [3]. While 5G achieves speeds of up to 10 Gbps, 6G is expected to reach terabit-per-second (Tbps) data rates, enabling seamless support for data-intensive applications such as holographic communication and immersive virtual reality. Additionally, 6G aims to reduce latency to sub-millisecond levels—well below 5G's 1-millisecond threshold—which will be critical for real-time applications such as remote surgery and autonomous systems [4]. Furthermore, 6G will support an even greater number of connected devices while maintaining high-quality service in densely populated areas, thereby surpassing the capabilities of 5G.

The key technologies driving 6G can be categorized into three main areas: wireless communication, network architecture, and security. In wireless communication, 6G will utilize terahertz frequency bands, which offer significantly greater bandwidth than the millimeter-wave bands used in 5G [5]. Reconfigurable intelligent surfaces (RIS) will dynamically adjust signal paths to optimize coverage and quality, while holographic MIMO will build on 5G's Massive MIMO by leveraging holographic principles to further enhance spectral efficiency. Moreover, ultra-low-latency communication will achieve sub-millisecond delays, setting a new benchmark for real-time applications.

In terms of network architecture, 6G will integrate distributed computing and cloud computing to facilitate faster and more efficient data processing. AI-driven adaptive networks will autonomously optimize resource allocation and network performance based on real-time demand. Network slicing, already implemented in 5G, will be further refined to deliver highly customized services tailored to specific use cases. Additionally, satellite and high-altitude platform systems (HAPS), such as satellite internet, will play a crucial role in extending global coverage, particularly in remote and underserved areas [6].

Data privacy will also be a critical concern in 6G networks. Given the vast amounts of personal and sensitive data being transmitted—such as location information, health records, and biometric identifiers—ensuring user privacy is paramount [7]. To this end, 6G must employ advanced privacy-preserving techniques, including differential privacy and homomorphic encryption, to protect data throughout its lifecycle, from transmission to storage. Furthermore, regulatory and compliance frameworks will be essential for enforcing rigorous data protection standards across all 6G-enabled ecosystems.

The emergence of quantum computing presents an additional challenge to 6G security. Traditional cryptographic methods used in 5G and earlier generations may become obsolete as quantum computers acquire the capability to break current encryption algorithms [8]. To mitigate this threat, 6G will need to adopt quantum-resistant communication technologies, such as quantum key distribution (QKD), to ensure secure data transmission even in the presence of quantum-enabled attacks. This transition will be essential for maintaining robust, long-term security in a post-quantum world.

2. Related works

DOI: 10.54254/2755-2721/2025.BA23841

Research on 6G in top-tier journals over the past five years reveals a field rich in innovation and marked by significant challenges. Current efforts are not only centered on technological breakthroughs but also explore practical applications and the resolution of associated issues. Overall, 6G research is evolving from conceptual frameworks to the investigation of concrete implementation pathways [9]. This transition reflects a growing consensus among researchers, industry leaders, and policymakers that 6G must not only outperform its predecessors technologically but also deliver meaningful value across diverse sectors such as healthcare, education, smart cities, and industrial automation.

Firstly, in terms of spectrum utilization, researchers are investigating the THz band as a core frequency range for next-generation wireless communication. Compared to the millimeter-wave bands used in 5G, THz frequencies offer significantly higher data transmission rates and broader bandwidth. However, they also present new technical challenges, such as severe signal attenuation and limited propagation distances. To overcome these obstacles, technologies such as RIS and advanced antenna systems—particularly holographic MIMO—have become key areas of focus. These innovations aim to enhance signal coverage and improve spectral efficiency, thereby optimizing overall network performance. Additionally, hybrid architectures combining sub-THz and optical communications are being explored to ensure seamless connectivity and support ultra-reliable low-latency communications (URLLC).

Secondly, the design of 6G network architectures is increasingly prioritizing flexibility and intelligence. With the advancement of edge computing, distributed cloud computing, and AI-driven network management, future 6G networks will dynamically adapt to the requirements of diverse application scenarios. For example, AI-based adaptive configurations can adjust resource allocation in real time to accommodate traffic fluctuations, thereby enhancing user experience [10]. Furthermore, machine learning algorithms are being integrated into network optimization processes to predict demand patterns and proactively manage resources. Additionally, improvements in network slicing technology will enable the delivery of tailored services for specific applications, supporting a wide variety of business models and enhancing service quality. These advancements are expected to foster greater interoperability among heterogeneous networks and lay the foundation for a truly autonomous and self-optimizing communication ecosystem.

In terms of security and privacy protection, 6G faces unprecedented challenges. On one hand, the emergence of quantum computing threatens to render existing encryption algorithms ineffective. On the other hand, the highly interconnected nature of 6G networks means that a vulnerability in a single node could jeopardize the stability of the entire system. Consequently, researchers are developing new security mechanisms based on QKD and exploring the integration of blockchain technology to enhance data security and user privacy. Moreover, zero-trust architecture and federated learning techniques are being investigated to safeguard sensitive information while preserving data utility. The goal is to build an inherently secure infrastructure where threats can be detected and mitigated in real time, ensuring both confidentiality and integrity in an increasingly complex digital landscape.

Finally, it is important to note that 6G research extends beyond terrestrial communication systems to include satellite internet and HAPS. These systems offer viable solutions to the limitations of ground-based infrastructure, particularly in remote regions and maritime environments [11]. By integrating satellite and terrestrial networks, 6G aims to achieve seamless global connectivity, which will greatly facilitate global information sharing and socio-economic development. Airborne base stations, drones, and non-terrestrial networks are being studied as complementary components of a

DOI: 10.54254/2755-2721/2025.BA23841

unified communication framework, enabling ubiquitous access regardless of geographic location or environmental conditions.

In summary, current 6G research encompasses a broad spectrum of topics, ranging from the physical layer to advanced application layers [12]. Although numerous technical and implementation challenges remain, ongoing research and technological innovation are paving the way for transformative societal changes. This trajectory underscores the critical importance of interdisciplinary and international collaboration in steering 6G toward a smarter, more efficient, and secure future [13].

3. Quantum-Enhanced Converged Wireless and Fiber 5G Fronthaul System

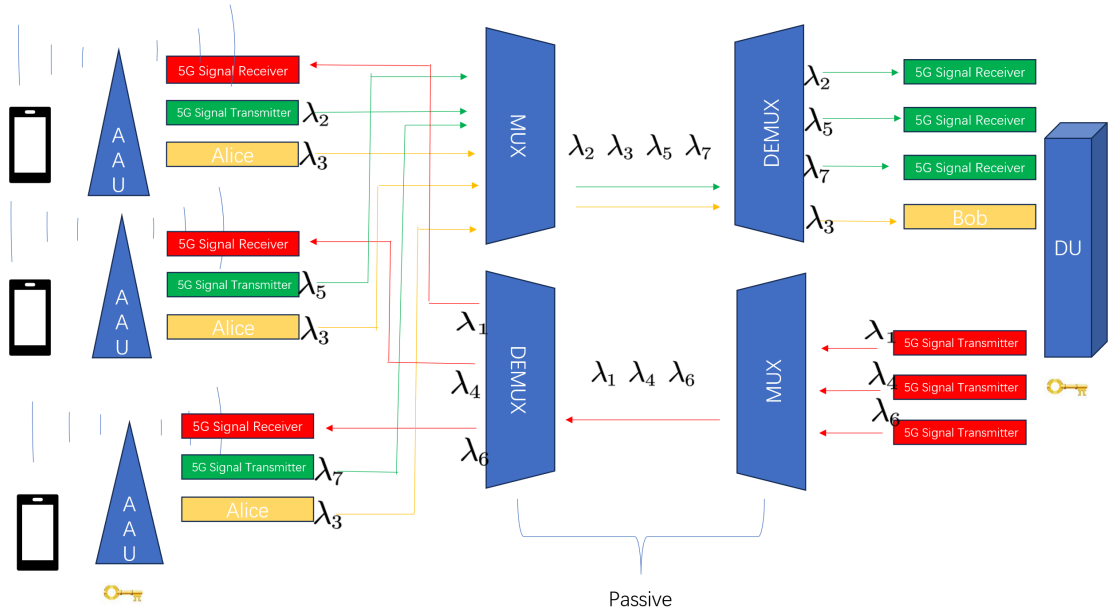

Figure 1: Quantum-Enhanced Converged Wireless and Fiber 5G Fronthaul System

We propose a Quantum-Enhanced Converged Wireless-Fiber 5G Fronthaul System, a 5G fronthaul solution based on passive wavelength division multiplexing (WDM). In this architecture, a photon transmitter (Alice) is deployed at the Active Antenna Unit (AAU) side, while a photon receiver (Bob) is positioned at the Distribution Unit (DU) side. This design enables the transmission of both classical and quantum signals over the same link, enhancing the security of information transmission at the physical layer. The core objective of this system is to ensure secure communication. When an eavesdropper attempts to intercept or duplicate transmitted information, such intrusions can be detected by monitoring the quantum bit error rate (QBER). If the error rate exceeds a predefined threshold, it indicates a potential eavesdropping attempt on the communication link.

To understand the eavesdropping detection mechanism, it is essential to consider three fundamental principles of quantum mechanics:

1. Heisenberg Uncertainty Principle: Two non-commuting quantum observables cannot be simultaneously measured with arbitrary precision.

2. Measurement Collapse Principle: When a quantum system is measured, its state collapses to one of the eigenstates of the measurement operator. Unless the system is already in an eigenstate, measurement will irreversibly alter the quantum state.

DOI: 10.54254/2755-2721/2025.BA23841

3. No-Cloning Theorem (derived from the principles above): It is impossible to create an exact copy of an unknown quantum state without altering the original. Any attempt to intercept or measure the quantum state introduces disturbances, which can be detected when Alice and Bob compare their measurement bases and check for consistency [14].

To prevent interference between quantum and classical signals, time-division multiplexing techniques can be employed. This ensures that photons are transmitted during designated time slots, separate from those used for conventional signal transmission [15].

The proposed architecture offers several key advantages:

1. QKD technology is grounded in the laws of quantum mechanics, providing security that is theoretically unbreakable. Any eavesdropping on the quantum channel can be detected in real time, ensuring the confidentiality and integrity of the communication. Unlike classical cryptographic methods, which rely on computational complexity and are vulnerable to advances in computing power—especially with the rise of quantum computing—QKD guarantees information-theoretic security. This makes it particularly suitable for securing critical infrastructure, military communications, and sensitive financial transactions where long-term data protection is essential.

2. Since the photon transmitter (Alice) is more expensive than the receiver (Bob), placing Alice at the AAU side—where there are multiple units—and Bob at the DU side—where the number of units is fewer—effectively reduces deployment costs. This strategic allocation allows a single high-cost Alice device to serve multiple lower-cost Bob units, optimizing resource utilization across the network. Furthermore, this setup simplifies maintenance and management by centralizing the more complex components within fewer physical locations, thereby reducing operational overhead and improving system reliability.

3. This solution fully leverages existing communication infrastructure, eliminating the need for extensive modifications or equipment replacement. By integrating QKD into current fiber-optic networks, security enhancements can be introduced incrementally without disrupting ongoing services. This step-by-step transition strategy protects existing investments and enables flexible adaptation to evolving security requirements, significantly enhancing the feasibility and scalability of the proposed solution. Additionally, the compatibility with software-defined networking (SDN) and network function virtualization (NFV) technologies allows for dynamic reconfiguration of secure channels based on real-time traffic demands and threat assessments. As a result, the architecture not only supports current network operations but also lays a solid foundation for future-proof, secure, and intelligent communication systems.

4. Simulation analysis

In the preceding sections, we discussed the current development status and potential challenges of 5G, and proposed a novel quantum-enhanced wireless-fiber fronthaul architecture. In this chapter, we present a simulation-based performance analysis of Quantum Key Distribution (QKD), focusing on the influence of key parameters—including noise detection probability, fiber loss, detection efficiency, transmission distance, and filter loss—on the secure key rate and quantum bit error rate(QBER).

DOI: 10.54254/2755-2721/2025.BA23841

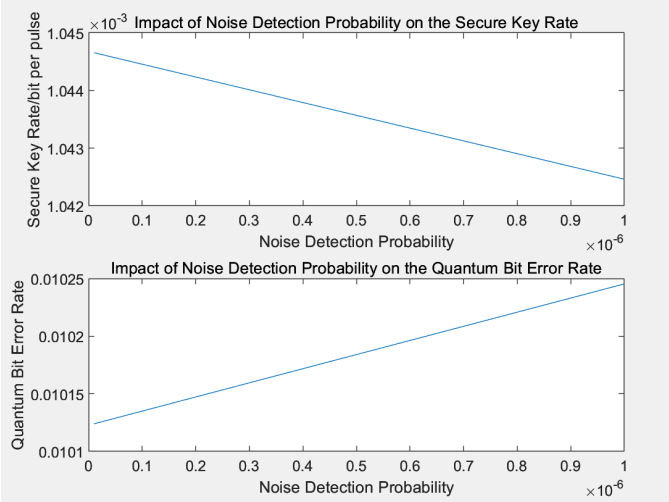

Figure 2: The impact of noise detection portability on QKD performance

Figure 2 illustrates the effect of noise detection probability on both the secure key rate and QBER. The results indicate that as noise detection probability increases, the secure key rate decreases linearly, while QBER increases linearly. This highlights the importance of minimizing noise detection probability in practical applications to achieve a higher secure key rate and lower QBER.

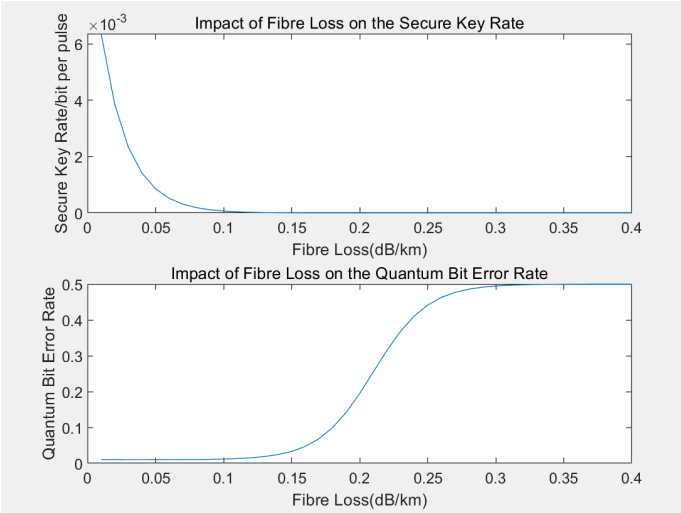

Figure 3: The impact of fiber loss on QKD performance

Figure 3 demonstrates the influence of fiber loss on QKD performance. As fiber loss increases, the secure key rate declines rapidly, approaching zero when fiber loss exceeds 0.1 dB/km. Concurrently, QBER rises significantly between 0.1 dB/km and 0.3 dB/km, eventually stabilizing around 0.5 beyond this point. These findings underscore the need to minimize fiber loss in practical deployments to optimize secure key rate and reduce QBER.

DOI: 10.54254/2755-2721/2025.BA23841

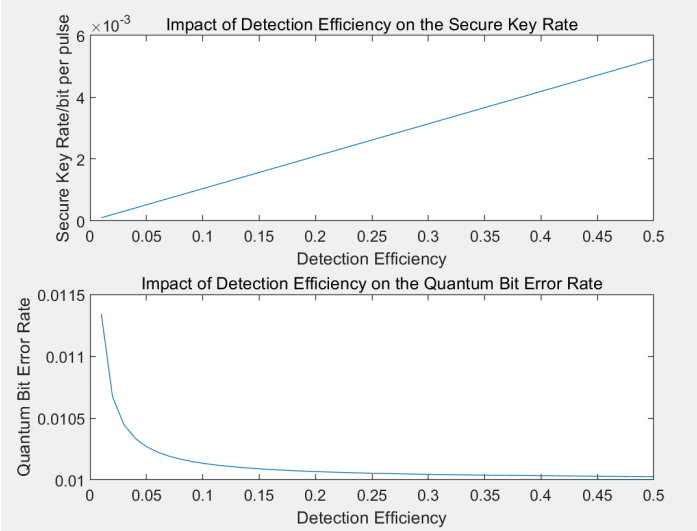

Figure 4: The impact of detection efficiency on QKD performance

Figure 4 shows the impact of detection efficiency on QKD performance. The simulation reveals that as detection efficiency increases, the secure key rate improves linearly, while QBER declines sharply. Beyond a detection efficiency of 0.1, the rate of QBER decrease slows. This emphasizes the importance of enhancing detection efficiency to boost the secure key rate and suppress QBER.

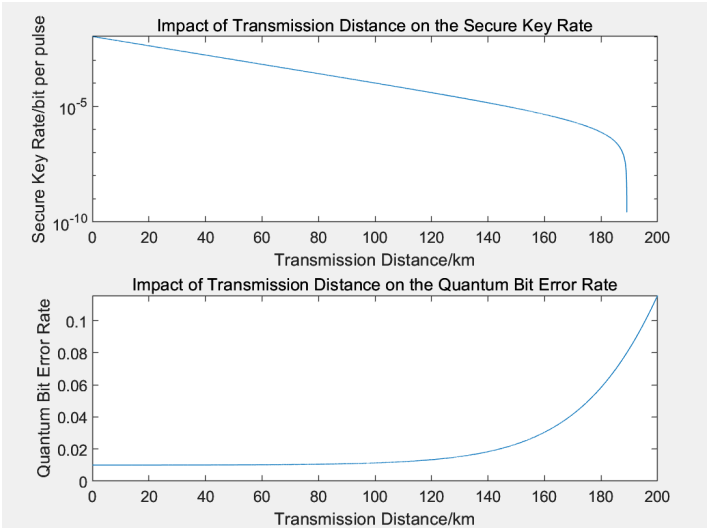

Figure 5: The impact of transmission distance on QKD performance

Figure 5 presents the effect of transmission distance on secure key rate and QBER. The secure key rate decreases linearly with distance up to approximately 180 km, after which it declines more steeply. In contrast, QBER rises gradually for distances under 140 km but exhibits exponential growth beyond this range. Therefore, minimizing transmission distance is crucial for maintaining a high secure key rate and low QBER.

DOI: 10.54254/2755-2721/2025.BA23841

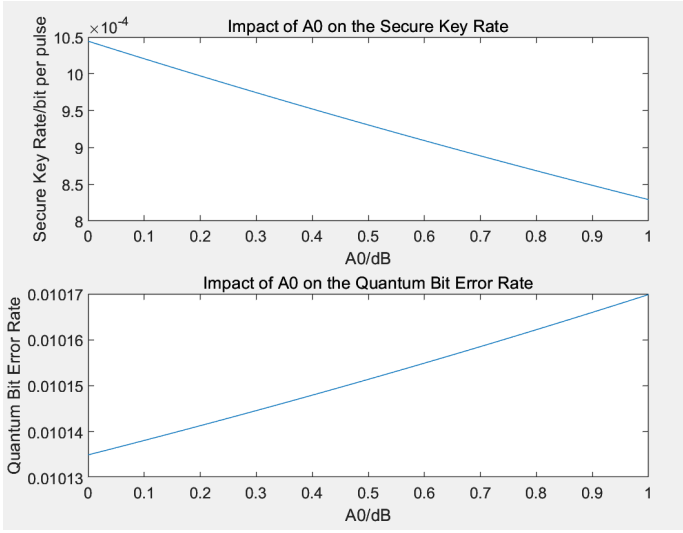

Figure 6: The impact of filter loss on QKD performance

Figure 6 evaluates the impact of filter loss on QKD performance. Filter loss is categorized into three components: base filter loss, first-stage additional loss, and tunable filter loss. Since all three exhibit identical effects on the secure key rate and QBER, they are collectively represented as A0 in the simulation. As filter loss increases, the secure key rate decreases linearly, and QBER increases linearly. These findings suggest that minimizing filter loss is essential to optimize QKD performance in practical scenarios.

The simulation results presented in the figures collectively confirm the impact of various system parameters—namely, noise detection probability, fiber loss, detection efficiency, transmission distance, and filter loss—on both the secure key rate and QBER in QKD systems. As demonstrated, increases in noise detection probability, fiber loss, and filter loss each lead to a linear decline in the secure key rate, accompanied by a linear increase in QBER. Transmission distance follows a similar pattern: the secure key rate decreases linearly up to approximately 180 km before dropping sharply, while QBER rises slowly up to 140 km and then increases exponentially beyond that point. In contrast, improved detection efficiency contributes to a linear increase in the secure key rate and a rapid decrease in QBER, particularly when the efficiency exceeds 0.1. These findings underscore the critical importance of minimizing noise detection probability, fiber loss, transmission distance, and filter loss, while maximizing detection efficiency, in order to optimize both the security and performance of practical quantum communication systems.

5. Research summary and prospect

This research has successfully demonstrated the feasibility and advantages of a quantum-enhanced converged wireless-fiber 5G fronthaul system through rigorous theoretical analysis and comprehensive numerical simulations. The proposed architecture constitutes a significant advancement in addressing the pressing security challenges of next-generation mobile networks, while preserving compatibility with existing communication infrastructure.

The core innovations of this study are encapsulated in three key contributions. First, the novel integration of quantum key distribution (QKD) technology with passive wavelength division multiplexing (WDM) architecture enables the concurrent transmission of quantum and classical signals without mutual interference. Second, the adoption of an asymmetric deployment strategy—

DOI: 10.54254/2755-2721/2025.BA23841

placing the quantum transmitter (Alice) at the Active Antenna Unit (AAU) and the quantum receiver (Bob) at the Distributed Unit (DU)—achieves an optimal balance between security performance and cost-efficiency. Third, the modular and incremental deployment capability of the system allows for seamless integration into existing networks, significantly reducing both capital and operational expenditures.

The simulation results yield several critical quantitative insights that provide practical guidance for real-world deployment. Notably, a fiber loss threshold of 0.1 dB/km emerges as a pivotal design constraint, beyond which secure key rate performance declines sharply. Similarly, a maximum effective transmission distance of 140 km serves as a benchmark for network planning in various deployment contexts. Furthermore, the nonlinear relationship between detection efficiency and QBER reveals that even incremental improvements in detection technology—especially beyond an efficiency of 0.1—can produce significant performance benefits. Lastly, both noise detection probability and filter loss demonstrate linear correlations with QBER and secure key rate, highlighting the necessity of minimizing these parameters to ensure the reliability and robustness of the proposed architecture.

The practical implications of this research span multiple sectors. For telecommunications operators, it provides a cost-effective pathway to enhance the security of existing 5G networks. Moreover, for government and financial institutions, the architecture offers quantum-safe communication capabilities to mitigate emerging cyber threats. In the industrial domain, the proposed system enables ultra-reliable, low-latency communication, which is essential for the success of Industry 4.0 applications. Finally, for the future development of 6G, this work lays the groundwork for integrating classical and quantum communication paradigms [16].

Looking ahead, this research opens several promising avenues for further exploration. These include the integration of advanced post-quantum cryptography algorithms, optimization for terahertz communication bands, and the development of hybrid quantum-classical network management protocols. The proposed architecture not only addresses current security challenges but also offers a flexible framework for the integration of future quantum communication technologies as they evolve.

6. Conclusion

This study makes substantial contributions to both academic research and practical network deployment by demonstrating that quantum-enhanced security can be effectively implemented within existing network infrastructures, without incurring prohibitive costs or technical challenges. The findings provide compelling evidence that quantum technologies are poised to play a transformative role in securing next-generation wireless communication systems.

References

[1]Shin, H. , Park, S. , Kim, L. , Kim, J. , Kim, T. , & Song, Y. , et al. (2024). The future service scenarios of 6g telecommunications technology. Telecommunications Policy, 48(2).

[2]Haque, M.A., et al. (2024). 6G Wireless Communication Networks: Challenges and Potential Solution. International Journal of Business Data Communications and Networking. 19. 27.

[3]M. Na et al., (2024)."Operator's Perspective on 6G: 6G Services, Vision, and Spectrum," in IEEE Communications Magazine, vol. 62, no. 8, pp. 178-184, doi: 10.1109/MCOM.001.2400060.

[4]Guo, J. (2024).“Upgrading roadmaps for state-of-art communications systems: from 5G TO 6G” IET Conference Proceedings, v 2024, n 24, p 504-8, 09

DOI: 10.54254/2755-2721/2025.BA23841

[5]Yang, N., Hyrynsalmi, S., Siemon, D. (2025). A Conceptual Analysis of Emerging 6G Ecosystem. In: Petrik, D., Saltan, A., Helferich, A. (eds) Digital Product Management in the Era of Data Economy, Artificial Intelligence, and Ecosystems. ICDPM 2024. Lecture Notes in Business Information Processing, vol 528. Springer, Cham.

[6]Trichias, K. (2024). "6G Global Landscape: A Comparative Analysis of 6G Targets and Technological Trends," 2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Antwerp, Belgium, pp. 1-6.

[7]Dai, H. (2024), "Analysis of the upgrading from 5G to 6G," 2nd International Conference on Mechatronic Automation and Electrical Engineering (ICMAEE 2024), Hybrid Conference, Nanjing, China, pp. 456-459

[8]Smyth, P. (2024) “What Should 6G Be” Evolution or Revolution? A converged view of cellular, Wi-Fi, computing and communication. Telecommunications (111), p 507-65

[9]Gersing, P., Doll, M., Huschke, J., & Holschke, O. (2024). Architecture Proposal for 6G Systems Integrating Sensing and Communication. ArXiv, abs/2411.10138.

[10]Wymeersch, H. (2025) "6G Positioning and Sensing Through the Lens of Sustainability, Inclusiveness, and Trustworthiness," in IEEE Wireless Communications, vol. 32, no. 1, pp. 68-75

[11]M. Wei, J. Wu, H. Liu, L. Lin, Z. Zhang and M. Sun, (2025) "Envisioning the Potential of 6G Use Cases—A Dual Perspective of Innovation and Business," in IEEE Access, vol. 13, pp. 9831-9843

[12]Garg, T. (2024) “Protocol Security in 6th Generation (6G) Networks” Computational Intelligence and Network Systems: First International Conference, CINS 2023, Proceedings. Communications in Computer and Information Science (1978), p 47-62

[13]Konstantinos T. (2024)“6G Global Landscape: A Comparative Analysis of 6G Targets and Technological Trends” 2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), p 1121-1126,

[14]Wei, C. (2008) “Experimental Research on Fiber Quantum Key Distribution” Doctoral dissertation, University of Science and Technology of China

[15]Chen LX. (2025) “Research on Co-propagation System Integrating Quantum Key Distribution and Classical Communication” Study on Optical Communications

[16]Zhang, GW. (2025) “Research Progress of Integrated Quantum Key Distribution” Laser & Optoelectronics Progress