Proceedings of the 3rd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/145/2025.21874

Integration of Quantum Key Distribution in 6G Passive WDM Optical Fronthaul Architecture

Yongjian Liang[1,a,*]

[1]*School of Electrical and Information Engineering Shandong University (Weihai) No.180 Wenhua West Road, Weihai, Shandong, China*
a. yongjianliang959@gmail.com
**corresponding author*

Abstract: The advancement of 6G networks demands high-capacity, ultra-low latency, and secure communication infrastructure. Traditional fronthaul solutions face significant challenges in meeting these demands due to increasing data traffic, network densification, and security vulnerabilities. To address these issues, this paper proposes an innovative 6G passive Wavelength Division Multiplexing (WDM) fronthaul architecture integrated with Quantum Key Distribution (QKD). By leveraging quantum cryptographic principles, our approach ensures unbreakable security and protects network transmissions from potential cyber threats and eavesdropping attacks. The proposed architecture effectively combines high-speed optical transmission with quantum-secured key exchange, optimizing network reliability and reducing security risks. Through comprehensive simulations, we evaluate key performance factors, including secure key rate (SKR), quantum bit error rate (QBER), detector efficiency, and quantum transmission loss. Results indicate that our architecture maintains high SKR with minimal QBER, even under challenging transmission conditions, ensuring robust quantum-secured communication. Additionally, the passive nature of WDM significantly reduces power consumption and maintenance costs, improving network sustainability. This research establishes a practical pathway for integrating quantum security into next-generation optical fronthaul networks, enabling highly secure, scalable, and efficient data transmission for future 6G applications, including autonomous vehicles, smart cities, and industrial IoT.

Keywords: 6G Fronthaul, Passive WDM, Quantum Key Distribution (QKD), Secure Communication

1. Introduction

5G is the new generation of communication technology. The emergence of 5G is driven by the rapid development of cutting-edge technologies such as the Internet of Things (IoT), artificial intelligence (AI), virtual reality (VR), and autonomous driving, all of which place higher demands on network performance. Among these developments, the 5G fronthaul represents a new and evolving network architecture compared to 4G and faces enormous pressure. Its importance and complexity have made it a research focus and hot spot in 5G bearer networks [1]. Moreover, 5G technology can offer peak speeds that are up to 10 times faster than those of 4G, support millions of simultaneous connections, and deliver ultra-low latency. It will greatly enhance massive IoT connectivity and provide highly

DOI: 10.54254/2755-2721/145/2025.21874

reliable, low-delay connections. Furthermore, 5G will promote the deep integration of communication networks, the Internet, and the Internet of Things, thereby enabling more convenient, faster, and more extensive connectivity and interaction among people, devices, and services.

6G is the next revolutionary development in mobile communication technology. While 5G is well known for network cloudification with a microservice-based architecture, next-generation networks—or the 6G era—are closely coupled with intelligent network orchestration and management [2]. Compared with 5G, 6G will push the boundaries of communication technology even further. Its goal is to achieve nearly ubiquitous ultra-fast networks, with data transmission rates reaching 100 Gbps or more and latency reduced to the microsecond level. Key features of 6G include extensive ultra-high frequency (THz band) communications, large-scale AI integration, intelligent network management, and integration with quantum computing. It will enable seamless support for various devices and applications—especially in fields such as autonomous driving, drones, augmented reality (AR), virtual reality (VR), and more. Additionally, 6G will place greater emphasis on network intelligence and automation by integrating cutting-edge technologies such as quantum and terahertz communications to provide higher reliability and a lower-latency experience. It will also focus on environmentally friendly technologies by optimizing energy use and reducing the carbon footprint of network operations.

The most significant driving force behind the 6G leap is the inherent connected intelligence within telecommunications networks, accompanied by advanced networking and artificial intelligence (AI) technologies. However, the close integration of 6G and AI does not necessarily guarantee improved security and privacy; in some cases, it may even serve as a means to compromise them [3]. The security requirements for 6G include not only traditional cyberattack protections—such as data encryption and firewall defenses—but also emerging challenges like the threat posed by quantum computing to existing encryption technologies and security issues related to smart devices. Because 6G will involve a greater number of devices and terminals—thereby increasing the attack surface—more robust authentication and access control mechanisms will be required. Furthermore, the proliferation of IoT devices and the implementation of 6G systems increase the risk that unauthorized users might impersonate legitimate primary users to access the spectrum for malicious purposes. Addressing these security issues is essential for maintaining network integrity and reliability [4]. Moreover, because 6G will make extensive use of artificial intelligence and machine learning algorithms, AI can be employed not only to detect and respond to cyberattacks but also to facilitate self-repair. In addition, 6G communications will involve a wider range of frequency bands—especially the terahertz band—which renders the propagation characteristics of signals more complex and susceptible to interference. The application of quantum communication technology will serve as one of the security guarantees for 6G, as quantum encryption can provide nearly unhackable security.

Quantum communication is a technology that utilizes the principles of quantum mechanics to enable information transmission. Its core concept is to use quantum bits (qubits) in place of classical bits. An important advantage of quantum communication is its security during information transmission, particularly through quantum key distribution (QKD). In general, quantum communications leverage principles such as the no-cloning theorem and entanglement to achieve quantum-resistant secure communications. For example, QKD achieves information-theoretically secure key agreement between two nodes [5]. The classic representative protocol is the BB84 protocol, which generates a shared key via qubit transmission. Its absolute security stems from the non-cloning theorem, which states that quantum states cannot be completely copied or stolen. Consequently, any attempt to eavesdrop on a quantum communication inevitably alters the quantum state, thereby alerting the communicating parties. This level of security is superior to that provided by classical encryption methods. Therefore, in QKD, if an eavesdropper attempts to intercept the key information, the quantum state will be altered, and the communicating parties can detect the intrusion by

DOI: 10.54254/2755-2721/145/2025.21874

comparing portions of the key, thus ensuring its security. Moreover, QKD is resistant to interference: any attempt to monitor or alter information during quantum transmission will result in noticeable changes that are quickly detected. Unlike traditional communications, even if an adversary intercepts the signal, no useful information can be obtained unless the communication is actively interfered with—a modification that would itself be readily detected.

2. Related Works

Recent research on 6G has achieved significant progress in areas such as architecture design, intelligent network structures, and network management. Reference [6] examines the evolution of 6G architecture, highlighting that 6G will support a vast array of new services with stringent key performance indicators (KPIs) and quality-of-service (QoS) requirements. Consequently, network resources must be optimized to meet these demands. Reference [7] delves into the overall development trends of 6G. It is anticipated that by 2030, 6G will provide global coverage, enhance spectrum efficiency, promote energy savings and cost-effectiveness, while simultaneously improving security features and supporting diverse application scenarios.

Reference [8] focuses on the pivotal role of deep learning (DL) in the sixth generation of mobile communications. The paper outlines a comprehensive vision for deep learning in 6G, emphasizing its contributions to adaptive resource allocation, intelligent network management, advanced signal processing, ubiquitous edge intelligence, and intrinsic security mechanisms.

In addition, further research has focused on the efficiency and security of communications. Reference [9] investigates the potential of integrating quantum computing and blockchain technology to bolster both the security and efficiency of 6G systems. The study proposes a novel framework, known as the Quantum-Blockchain-6G (QBG) framework, which aims to harness the computational power of quantum computing alongside the security, privacy, and transparency offered by blockchain technology. This framework seeks to enhance urban management and meet the unique demands of the 6G era.

With the advent of 6G, new approaches are required to identify and address cybersecurity, trust, and privacy risks that emerge as network and computing infrastructures become increasingly virtualized. In response, this paper introduces a novel security-enabling mechanism deployed in the data plane that employs network slicing as a means of security mitigation. In this manner, legitimate traffic can be isolated from harmful traffic, leaving attackers with few vulnerabilities to exploit [10].

3. 6G Passive WDM Optical Network Fronthaul Architecture Based on QKD

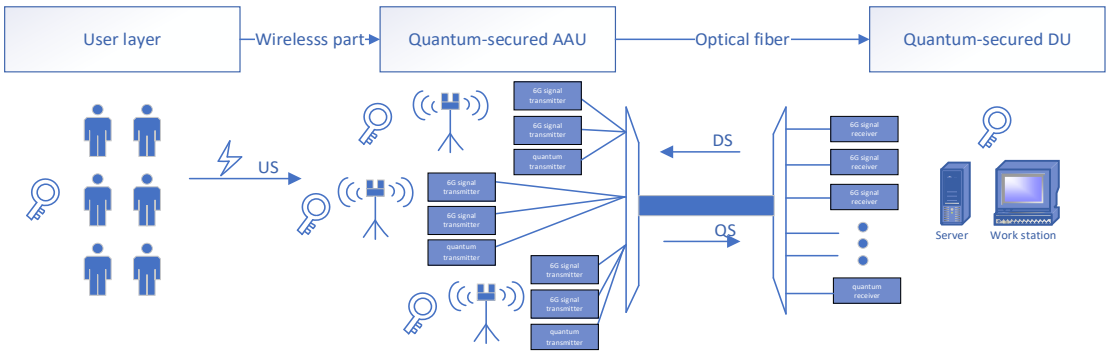

Figure 1: 6G Passive WDM Optical Network Fronthaul Architecture Based on QKD (US: upstream signal; DS: downstream signal; QS: quantum signal)

Designed for 5G signal transmission using a Passive WDM (Passive Wavelength Division Multiplexing) architecture, the system comprises a user layer, an AAU (Active Antenna Unit) site,

DOI: 10.54254/2755-2721/145/2025.21874

and a DU (Distributed Unit). At the AAU site, the system incorporates a quantum transmitter (Alice) and a quantum receiver (Bob).

The transmitted signals primarily include upstream signals from the client to the AAU site and from the AAU site to the DU site. The primary device is the wavelength division multiplexer (MUX), which merges multiple signals with the optical line terminal to facilitate signal reception and demodulation. The system's main function is twofold. First, it transmits users' requests and various types of information (including data, voice, and video) from the client to the operator. Second, for downlink transmission, the DU station sends signals of different wavelengths through the optical line terminal; subsequently, the MUX combines these multiwavelength signals into a single optical fiber, and an optical splitter allocates them to different users based on power levels. Additionally, optical signals are used to remotely monitor the status of the optical fiber—for example, tracking power loss, fault locations, and providing synchronization signals to ensure clock alignment across systems. Protective signals are also transmitted to enhance the overall reliability of the optical network.

In the wireless access segment, the AAU employs a massive MIMO antenna array and utilizes the millimeter-wave frequency band to achieve high-density user access and high-speed transmission via beamforming technology. Moreover, the AAU converts wireless signals into digital baseband streams, which are then forwarded to the DU through an optical fiber fronthaul network. In the optical fiber transmission segment, the DU modulates the baseband signal, synchronization signal, and the quantum key (generated by QKD) onto the C-band and O-band, respectively, before transmitting them to the AAU via the MUX using a single optical fiber.

The architecture offers high capacity; a single fiber supports 40 channels of 100 Gbps classic service plus a 10 Gbps quantum key channel, resulting in a total capacity of over 4 Tbps. This configuration meets the demands of ultra-high-density 6G connections, conserves fiber resources, and significantly reduces the number of optical fibers required for forward transmission. Moreover, the 6G architecture can directly leverage the existing 5G infrastructure, and its passive devices require no external power supply or maintenance. The deployment is relatively simple, and the probability of failure is low. When adding AAU sites, only the wavelength assignment needs to be adjusted, with no requirement for additional optical fiber.

Finally, the implementation of the BB84 quantum key distribution protocol can significantly enhance system security and confidentiality. Furthermore, by exploiting differences in transmission bands, quantum signals can be separated from classical WDM channels through wavelength isolation filtering. Therefore, through technical optimization, QKD can be integrated into the 6G passive WDM architecture to enable safe and efficient quantum key distribution, thereby laying the foundation for the deep integration of the quantum Internet with classical optical networks.

4. Simulation Analysis

According to the architecture diagram, this study conducted a simulation analysis of the secure key rate (SKR) and quantum bit error rate (QBER) of the system. The study primarily explores the effects of detector efficiency, quantum transmission loss, average photon number per pulse, and noise on SKR and QBER at different transmission distances, providing practical guidance.

DOI: 10.54254/2755-2721/145/2025.21874

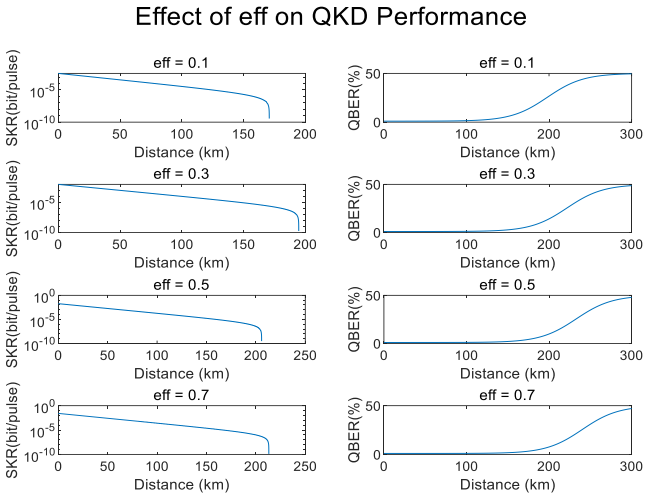

Figure 2: Effect of Detector Efficiency on QKD Performance
(SKR: Secure Key Rate; QBER: Quantum Bit Error Rate)

Photon detection efficiency is one of the most critical parameters in quantum key distribution (QKD) systems. Higher detection efficiency allows the detector to capture more photon signals, improving signal quality and enhancing the key generation rate. However, increasing detection efficiency is often associated with higher technical requirements and costs. High-efficiency detectors typically require more sophisticated photodetectors, leading to increased equipment costs and potentially imposing higher demands on durability, sensitivity, and operational conditions.

In different application scenarios, photon detection efficiency must be balanced according to system requirements and cost constraints. For example, in short-range communications or applications with high-security requirements, high-efficiency detectors may be preferred to maximize key generation rates and enhance security. In long-distance transmission or cost-sensitive applications, less efficient equipment may be selected to reduce system construction costs, while optimizing other parameters to compensate for performance losses caused by lower detection efficiency.

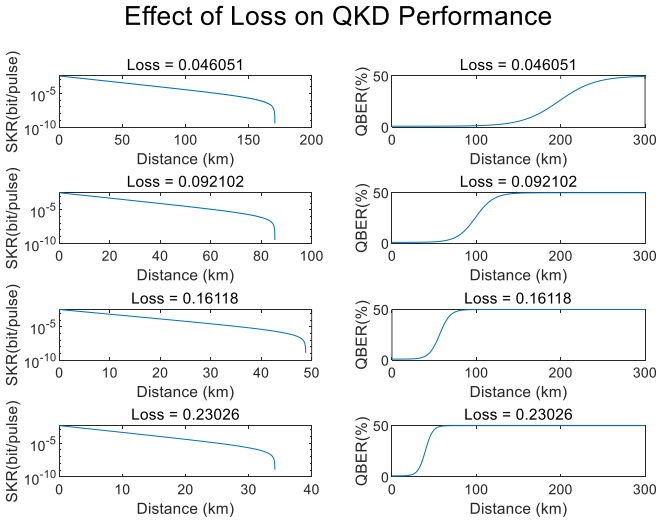

Figure 3: Effect of Quantum Transmission Loss on QKD Performance

DOI: 10.54254/2755-2721/145/2025.21874

Channel loss directly impacts the transmission quality of quantum signals and the overall performance of the system. In QKD, channel loss is not only limited to physical channel attenuation but also includes signal attenuation in optical fibers, air, or other transmission media. Due to the non-clonability of quantum signals, selecting low-loss transmission channels is particularly crucial. Using a path with minimal channel loss reduces signal attenuation during transmission, thereby increasing the probability of detecting valid signals at the receiving end.

To address excessive signal loss in long-distance transmission, relay devices can be employed to extend the transmission range. Repeaters amplify and restore the signal quality, ensuring that transmission losses remain effectively controlled. However, the inclusion of relay devices increases system complexity, introduces additional delays, and adds to overall costs. Therefore, when designing a QKD system, a balance must be achieved between transmission distance, loss, signal amplification, and the use of relay devices. In the long term, selecting low-loss channels can significantly improve system stability and key generation rates. For long-distance communication, reducing channel loss in combination with relay-based signal amplification is a key strategy to ensure the optimal functioning of quantum communication networks.

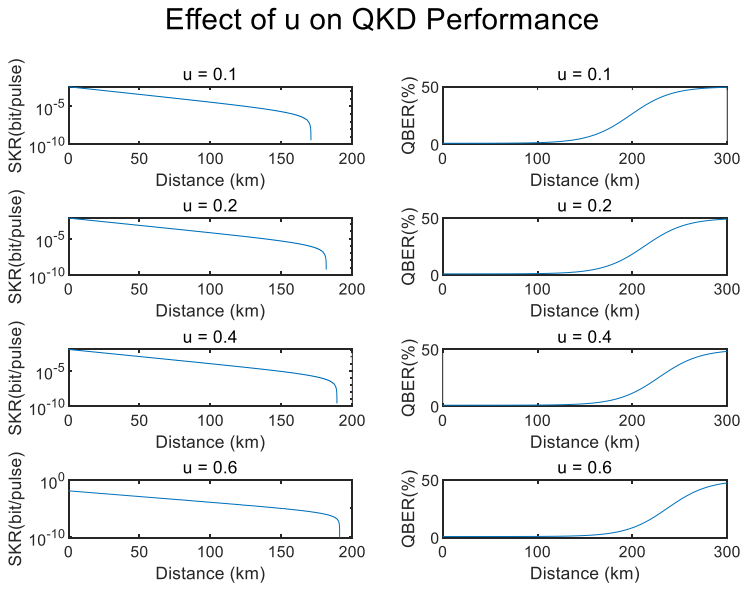

Figure 4: Effect of Average Photon Number per Pulse on QKD Performance

In QKD, the average photon number per pulse (μ) represents the number of photons carried in each pulse. Although increasing the photon count can enhance transmission rates, an excessively high photon number may lead to issues such as multiphoton interference and increased signal processing complexity. Experimental results indicate that an optimal photon number achieves a balance between stability and performance.

For quantum communication systems, an excessive increase in photon count may result in signal distortion and degradation of key generation quality. Therefore, a higher photon count does not necessarily equate to better performance. In practical applications, this parameter should be optimized according to the specific characteristics of the quantum device. Quantum device manufacturers typically provide reference standards or recommended optimal photon number ranges for experimental design. The goal of this optimization is to determine an appropriate intermediate value that ensures a low bit error rate, stable signal quality, and strong robustness against environmental fluctuations.

DOI: 10.54254/2755-2721/145/2025.21874

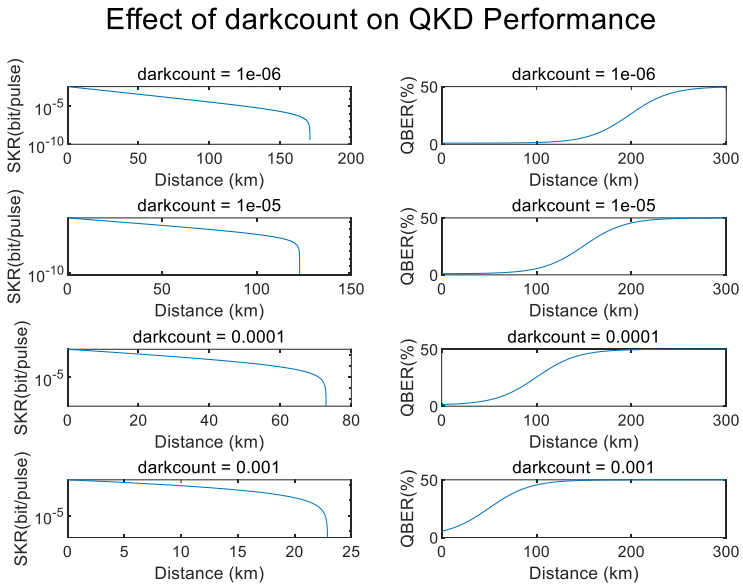

Figure 5: Effect of Noise on QKD Performance

Dark counts are false signals produced by quantum detectors that do not originate from real photons but rather from intrinsic noise within the detector itself. In quantum key distribution, dark counts directly impact signal quality and increase the bit error rate (BER). A lower dark count results in a lower system noise level and a higher signal-to-noise ratio, thereby improving key generation efficiency.

As transmission distance increases, the impact of dark counts on system performance becomes more pronounced. Photon signal attenuation increases over longer distances, making the system more sensitive to noise. At this point, dark counts act as background noise, gradually overwhelming real signals and leading to a rise in the bit error rate. To enhance system performance, it is essential to minimize dark counts.

5. Conclusions

This paper introduces a novel 6G fronthaul architecture that leverages Passive WDM (Wavelength Division Multiplexing) and Quantum Key Distribution (QKD) to address critical security and efficiency challenges in next-generation communication networks. Our approach combines the high-capacity transmission capabilities of WDM with quantum encryption, ensuring ultra-secure communication with low maintenance and high scalability. Simulation results confirm that our architecture achieves a high secure key rate (SKR) while maintaining an ultra-low quantum bit error rate (QBER), even under varying transmission conditions. The integration of QKD significantly enhances data confidentiality, making the system resilient to cyber threats and eavesdropping attacks. Moreover, the passive WDM framework reduces power consumption and infrastructure costs, offering an energy-efficient solution for future 6G networks.

From an application perspective, this architecture is particularly well-suited for security-critical scenarios such as smart cities, autonomous driving, and financial transactions, where data integrity and real-time security are paramount. By seamlessly integrating quantum encryption with classical optical networking, this study paves the way for a secure, sustainable, and high-performance 6G communication ecosystem, bridging the gap between traditional and quantum-enhanced networking technologies.

DOI: 10.54254/2755-2721/145/2025.21874

References

[1] R.Wei and X. Luo, "Exploration 5G Fronthaul Technology & Networking Solutions," 2024 International Conference on Electrical Drives, Power Electronics & Engineering (EDPEE), Athens, Greece, 2024, pp. 522-524, doi: 10.1109/EDPEE61724.2024.00103.

[2] Y.Siriwardhana, P. Porambage, M. Liyanage and M. Ylianttila, "AI and 6G Security: Opportunities and Challenges," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 2021, pp. 616-621, doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.

[3] P.Porambage, G. Gür, D. P. Moya Osorio, M. Livanage and M. Ylianttila, "6G Security Challenges and Potential Solutions," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 2021, pp. 622-627, doi: 10.1109/EuCNC/6GSummit51104.2021.9482609.

[4] P.Deepanramkumar and A. Helen Sharmila, "AI-Enhanced Quantum-Secured IoT Communication Framework for 6G Cognitive Radio Networks," in IEEE Access, vol. 12, pp. 144698-144709, 2024, doi: 10.1109/ACCESS.2024.3471711.

[5] C. Wang and A. Rahman, "Quantum-Enabled 6G Wireless Networks: Opportunities and Challenges," in IEEE Wireless Communications, vol. 29, no. 1, pp. 58-69, February 2022, doi: 10.1109/MWC.006.00340.

[6] Akgul, Ozgur Umut, et al. "Discussion on 6G Architecture Evolution: Challenges and Emerging Technology Trends." 2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). IEEE, 2024.

[7] Ran, Yuhan , and D. Zhang ."The Overall Development Trend of 6G."2023 5th International Academic Exchange Conference on Science and Technology Innovation (AECST) 0.

[8] Jiao, Licheng, et al. "Advanced deep learning models for 6G: overview, opportunities and challenges." IEEE Access (2024).

[9] Zohaib, Muhammad, Fahad S. Altuwaijri, and Sami Hyrynsalmi. "Integrating quantum computing and blockchain: Building the foundations of secure, efficient 6g technology." Proceedings of the 1st ACM International Workshop on Quantum Software Engineering: The Next Evolution. 2024.

[10] Escolar, Antonio Matencio, et al. "Network slicing as 6G security mechanism to mitigate cyber-attacks: the RIGOUROUS approach." 2024 IEEE 10th International Conference on Network Softwarization (NetSoft). IEEE, 2024.