A report on the survey of QKD

SAMADRITA BHAUMIK
SUMMER RESEARCH INTERN AT NIT ROURKELA
ELECTRONICS AND COMMUNICATION ENGINEERING
SUPERVISOR: SADANANDA BEHERA
DATE OF SUBMISSION: 04/07/2025

***Abstract*—**
***Index Terms*—Quantum Key Distribution,**

I. Literature Survey

This paper [1] presents a comprehensive survey on the integration of Quantum Key Distribution (QKD) into optical fiber networks to enhance communication security. It explores how QKD enables information-theoretic security by leveraging quantum properties of photons, addressing vulnerabilities such as lightpath attacks in classical optical networks. The paper examines key challenges in implementing QKD in existing infrastructures, including quantum-classical signal coexistence, photon loss, and the need for trusted repeater nodes for long-distance key distribution. It also covers issues related to routing, wavelength and time-slot allocation, as well as architectural considerations for deploying QKD across metropolitan and long-haul networks. Furthermore, the survey discusses photonic and physical layer constraints, protocols like BB84 and decoy-state methods, and the role of advanced components such as detectors and optical pulses. Lastly, it outlines ongoing standardization efforts and future directions, including the use of software-defined networking (SDN), quantum repeaters, and hybrid quantum-classical architectures, making it a valuable resource for researchers and engineers in secure optical networking.

This article [2] surveys various QKD protocols and presents a small experimental analysis of some discussed protocols.Conventional cryptography relies on mathematical complexity for security, but weak key distribution undermines it. In 1994, Peter Shor introduced a quantum algorithm that threatens such cryptographic systems by efficiently factoring large integers. As a response, Quantum Key Distribution (QKD) has gained attention for its potential to offer unconditionally secure communication based on quantum mechanics.The survey emphasizes the strengths and weaknesses of protocols like BB84 and B92 in real-world scenarios. It also discusses implementation challenges such as photon loss, noise, and hardware limitations.

This paper [3] proposes a scalable and robust architecture for Quantum Key Distribution (QKD) networks by adopting a modular, SDN-inspired design. The architecture introduces clearly defined functional modules and standardized interfaces to support integration, automation, and interoperability within telecom-grade infrastructures. It enables dynamic resource allocation, monitoring, and orchestration across multiple domains, facilitating efficient network slicing, fault tolerance, and the sharing of quantum devices—particularly beneficial in metropolitan networks. The authors demonstrate the feasibility of their approach through a testbed implementation, showcasing how QKD networks can be transformed from isolated point-to-point systems into fully managed, large-scale quantum-secure communication infrastructures. Their work supports ongoing efforts toward QKD standardization and integration with classical telecommunications networks.

This paper [4] provides a comprehensive overview of how QKD has progressed from simple point-to-point links to complex, scalable network architectures aimed at realizing a future quantum internet. It outlines the technical evolution through stages such as optical-switch networks, trusted-relay models, and the anticipated use of quantum repeaters. The paper explores both the physical and network layers involved in QKD networks, including components like single-photon detectors and quantum routing protocols. It highlights ongoing standardization efforts by organizations and discusses real-world applications. Finally, it addresses key challenges such as scalability, interoperability, and cost-effectiveness, offering design guidelines for building secure, modular, and future-ready QKD networks that pave the way toward the Qinternet.

This paper [5] explores the fundamental challenges in building scalable and robust quantum networks. It highlights key limitations such as photon loss, decoherence, and the inability to amplify or clone quantum signals, which severely constrain long-distance quantum communication. The study focuses on the role of quantum repeaters, showing that even with their use, there exists a practical limit on the network diameter for tasks like device-independent quantum key distribution (QKD), governed by the quality of entanglement. Using graph-theoretic models, the authors analyze the robustness of quantum networks, identifying critical points where repeater placement significantly enhances connectivity and resilience. They evaluate practical use-cases, including satellite-based links and on-chip quantum architectures, and examine their performance in essential tasks like entanglement distribution, teleportation, and delegated computing under realistic noise and loss conditions. The paper also presents optimization strategies for network topology, shortest-path entanglement routing, and quantum resource allocation, offering a comprehensive view of the constraints and design considerations for a future quantum internet.

This paper [6] presents a model for enabling long-distance secure communication using Quantum Key Distribution (QKD) enhanced by the deployment of quantum repeaters. It addresses the limitations of QKD over large distances due to photon loss and decoherence by proposing an optimized strategy for placing trusted quantum repeater nodes. The authors incorporate factors like node reliability, quantum memory limitations, and transmission delay, applying algorithms such as Dijkstra's and Yen's to identify optimal communication paths. Their simulation results demonstrate improved reliability, reduced delays, and efficient resource utilization, making the approach viable for secure quantum communication over large-scale networks, particularly in Internet of Things (IoT) applications.

In the paper [7], the authors propose a novel approach to quantum key distribution (QKD) over long distances by integrating quantum error correction and sequential entanglement swapping in repeater-based networks. Most existing proposals for entanglement distribution rely on a connection-oriented paradigm, where resources along a path are pre-reserved. However, this does not align well with the current Internet infrastructure, which operates primarily through connectionless packet switching. In contrast, this work explores a hop-by-hop teleportation-based protocol that enables entanglement distribution without prior resource reservation. The authors study the achievable secret key generation rate between two users using a repeater chain, analyzing both unencoded and encoded scenarios. Specifically, they apply a three-qubit repetition code for error detection in the encoded case, allowing the system to tolerate realistic operational errors. The use of adaptive optics and optical packet switching is also considered to support practical implementation. Simulation and theoretical analyses demonstrate that quantum error detection can significantly extend the viable range for trust-free key distribution, highlighting its potential for robust and scalable quantum networks. Overall, the paper provides valuable insights into deploying QKD using encoded quantum repeaters with sequential swapping, offering a feasible and flexible solution for future quantum-secured communication infrastructures.

The paper [8] explores the use of satellite-based Quantum Key Distribution (QKD) as a secure communication method that leverages quantum mechanics to protect data. QKD typically faces limitations over long distances due to signal attenuation, which requires the use of quantum repeaters—technologically challenging but feasible—or the more recently demonstrated Twin-Field QKD (TF-QKD). As quantum technologies evolve, they are expected to play a significant role in enhancing network security. The paper focuses on the integration of QKD with satellite and space technologies, highlighting its potential for secure communication between ground stations and satellites. It also addresses challenges such as atmospheric losses, beam divergence, and satellite alignment, and discusses technological strategies including the use of repeaters and trusted nodes. Furthermore, the study offers an overview of CubeSats and other satellites that currently implement QKD, emphasizing the growing importance of space-based quantum cryptography in the context of 5G and future global communications infrastructure.

The paper [9] presents a comparative evaluation of quantum key distribution (QKD) protocols within satellite-based communication frameworks, focusing on their applicability to both uplink (ground-to-satellite) and downlink (satellite-to-ground) transmissions. Satellite-based QKD represents a significant advancement in secure communication by utilizing quantum mechanics to generate unbreakable cryptographic keys. The study classifies QKD systems into three categories—optical QKD, wireless QKD, and semiwireless QKD—and assesses their performance in quantum dialogue and quantum conference settings. Key challenges such as photon loss, atmospheric turbulence, and alignment precision are examined to understand their impact on system performance. Simulations of critical metrics including bit error rate (BER), throughput, and loss tolerance provide insights into the trade-offs between robustness, efficiency, and scalability across different protocol implementations. Special attention is given to the role of adaptive optics and the effects of transmission direction, showing that downlink channels generally outperform uplinks in terms of BER and throughput. Additionally, the research highlights the viability of semi-QKD approaches for scenarios involving non-quantum receivers, illustrating a path for hybrid integration of quantum and classical systems. Overall, the findings emphasize the transformative potential of satellite QKD in enabling secure, scalable, and flexible communication networks for the quantum era.

The paper [10]presents a new type of quantum hacking that targets quantum key distribution (QKD) systems by taking advantage of a weakness in their laser sources. Instead of using the usual method of injecting light at the laser's working wavelength (around 1550nm), the authors show that shining a continuous beam of light at a shorter wavelength (1310nm) into Alice's laser diode can noticeably change how the laser works. This optical-pumping attack increases the pulse energy by approximately 10 percentage and the average output power by about 20 percentage without being detected by standard monitoring mechanisms. Even very low injection powers (23nW) are shown to cause noticeable distortions in pulse shape and timing jitter. The altered output leads to misestimated key rates, compromising the security assumptions of QKD protocols such as BB84. Experimental validation using a commercial QKD transmitter confirmed the attack's feasibility and effectiveness, especially in systems with insufficient isolation at non-operational wavelengths. The authors stress that while some systems may have enough spectral isolation to resist such attacks, many others—particularly those with passive state preparation—remain vulnerable. They recommend countermeasures such as broadband optical isolators, spectral filters, and thorough characterization of QKD source components across a wide wavelength range to detect and prevent such loopholes. This study highlights the importance of defending QKD systems against unconventional side-channel attacks that target physical-layer imperfections.

REFERENCES

[1] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash and A. K. Mishra, "Quantum Key Distribution Secured Optical Networks: A Survey," in IEEE Open Journal of the Communications Society, vol. 2, pp. 2049-2083, 2021, doi: 10.1109/OJCOMS.2021.3106659.

[2] A. I. Nurhadi and N. R. Syambas, "Quantum Key Distribution (QKD) Protocols: A Survey," 2018 4th International Conference on Wireless and Telematics (ICWT), Nusa Dua, Bali, Indonesia, 2018, pp. 1-5, doi: 10.1109/ICWT.2018.8527822.

[3] M. Peev et al., "Quantum Key Distribution Network Architectures," 2024 International Conference on Quantum Communications, Networking, and Computing (QCNC), Kanazawa, Japan, 2024, pp. 320-326, doi: 10.1109/QCNC62729.2024.00056.

[4] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng and L. Hanzo, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839-894, Secondquarter 2022, doi: 10.1109/COMST.2022.3144219.

[5] "Practical Limitations on the Quantum Internet," 2024 16th International Conference on COMmunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2024, pp. 729-731, doi: 10.1109/COMSNETS59351.2024.10427077.

[6] S. Baskar, M. K. Roberts and K. P. Sridhar, "Long-Distance Secure Communication Based on Quantum Repeater Deployment with Quantum-Key Distribution," 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT), Vellore, India, 2024, pp. 1-6, doi: 10.1109/AIIoT58432.2024.10574780.

[7] J. Rey-Domínguez and M. Razavi, "Quantum key distribution over an encoded repeater chain with sequential swapping," 2025 International Conference on Quantum Communications, Networking, and Computing (QCNC), Nara, Japan, 2025, pp. 323-330, doi: 10.1109/QCNC64685.2025.00058.

[8] F. Lauterbach, M. Vanëk, M. Mehic and M. Voznak, "A Study on Quantum Key Distribution Satellite Communications," 2023 15th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Ghent, Belgium, 2023, pp. 128-133, doi: 10.1109/ICUMT61075.2023.10333106.

[9] J. Grow, J. Dutta, S. Chakravarty and I. Ahmed, "Comparison of Quantum Protocols for Satellite-Terrestrial Networks," SoutheastCon 2025, Concord, NC, USA, 2025, pp. 1050-1052, doi: 10.1109/SoutheastCon56624.2025.10971651.

[10] M. Fadeev, A. A. Ponosova, R. Shakhovoy and V. Makarov, "Laser-pumping attack on QKD sources," 2024 International Conference Laser Optics (ICLO), Saint Petersburg, Russian Federation, 2024, pp. 562-562, doi: 10.1109/ICLO59702.2024.10624559.