Research Study on Quantum Key Distribution in Quantum Communication

Saurabh Dharmadhikari[1], Umeda Yeole[2]

[1]*Student, Department of Electrical & Electronics Engineering, Personal research Project, Nashik, India.*

[2]*Student, Department of Electronics & Telecommunication Engineering, Personal research Project, Nashik, India.*

Corresponding Author: ssdharmadhikari85@gmail.com

Abstract— This research paper explores the integration of Quantum Key Distribution (QKD) networks with Telecommunication Networking technology to enhance the security of communication. QKD, leveraging the principles of quantum physics, offers secure key exchange between users, detecting any potential eavesdropping during communication. Traditionally limited to point-to-point connections, the paper addresses the need for a unified control plane for efficient resource allocation in QKD networks. It discusses the challenges of multi-resource allocation, secret-key management, and survivability, offering potential solutions. The paper details recent progress in QKD networks and presents three practical cases illustrating the benefits of combining QKD with SDN. The paper concludes by summarizing the findings and emphasizing the significance of QKD networks in developing secure multi-user communication scenarios in the evolving landscape of information networks.

***Index Terms*—Quantum communication, Quantum key distribution, Telecommunication networks, quantum computing, quantum technology, photons, optics, electronics.**

1. Introduction

Quantum communication is one of the advanced fields in applied quantum physics.

Let us discuss 'What is quantum communication'? First, quickly jump into quantum physics,

Firstly, do you know what a quanta is?

It is a plural form of quantum. Moreover, quantum is called a packet of energy.

Secondly, we need to understand about photons. In simpler terms, photons are elementary particles representing a quantum of light or electromagnetic radiation.

What's next? Then, these tiny particles are called 'entangled photons'. They share quantum states with each other. 'Quantum state' is a mathematical entity of the quantum system.

After understanding the above factors of quantum physics here, we can define Quantum communication:

Manuscript revised December 04, 2023; accepted December 06, 2023. Date of publication December 08, 2023.
This paper available online at www.ijprse.com
ISSN (Online): 2582-7898; SJIF: 5.59

Quantum communication [7] is defined as a field of communication that uses quantum physics to transmit and protect data. Quantum communication is also a way of sending data from one place to another. This is the method of communication where data is transmitted in quantum bits instead of general data bits, as we use in everyday computers.

'Quantum bits' are also called 'Qubits'. These qubits transmit data in a unique path because qubits exist in multiple states. So, when data moves in quantum communication, it is not transmitted in 0s and 1s, but qubits can represent numerous possible combinations of 1, 0, or both at once. This ability to be in multiple states at once is also called a superposition.

This is one of the parts of quantum technology that derives benefit from identified properties revealed by quantum physics that help to new capabilities such as how we compute, communicate and sense.

'Quantum Key Distribution' [QKD][7] is a base of Quantum communication, where the states of particles, such as Photons, are used to create a sequence of 0's and 1's. This secure method enables both parties to produce a shared random secret key known only to them. This key is crucial for encryption and decryption purposes. The whole communication system is end-to-end encrypted.

Let us get an idea about how a basic secure communication system works:

- The sender transmits encrypted data to the receiver.
- The receiver can open data (message) if the receiver has a secret key.
- only one can open that data (message) with a secret key.

2. Literature Review

Quantum Key Distribution is an innovative technology that safeguards sensitive data during transferring in modern-era communication channels. Many researchers claim that simulating QKD can be used to ensure secure file communication across open-channel environments.[4]

Amrin M [1] suggested an algorithm to solve MITM attacks in BB84. It employs a computational security algorithm and an image algorithm to generate keys. The resulting hybrid key is used for ongoing communication, but the system lacks offline key establishment and scalability.

Sufyan T. [2] and Omer K. combined classical cryptography's unconditionally secure authentication techniques with QKD, creating two-party authenticated quantum key distribution protocols (based on BB84). This integration addresses issues from previous studies, reducing authentication costs. Two authentication modes, "partial" and "full," were considered for each QKD session, with the full mode significantly impacting the system's efficiency.

Marcin N. and Andrzej R. [11] acquainted themselves with an unconventional security measurement concept in QKD, which suggests a unique entropy of security. Quantum Key Distribution proposed basic and advanced security levels, allowing customization for end-users. Nevertheless, the system's resilience to intrusion attacks was not tested.

Chai-Wei Tsa [4] and Chun-Wei Yung [4] explain the method to distribute the security session key in the QKD network; the hop-by-hop method is necessary due to the limited distance for qubit communication. This means that any node along the routing path can be aware of the session keys distributed from the source node to the destination node.

Xiaobo Zheng and Zhiwen Zhao [12] introduced a two-way authentication method, examining the extent to which an eavesdropper can disrupt the negotiated key under the MDI scheme. The MDI supports the decoy state protocol, addressing equipment vulnerabilities against splitting attacks.

3. Concept And Protocol

Quantum Key Distribution (QKD) is a method used to securely share encryption keys for both symmetric and asymmetric ciphers. Its purpose is not to transmit any unencrypted data between the communicating parties, often referred to as the master and slave.

The initial protocol developed in the field of quantum cryptography was BB84. This protocol relies on the polarization of photons (particular states that help transmit classical information over a quantum channel) and is widely regarded as the most reliable solution in practical quantum cryptographic applications. Other protocols, like B92 or E91, are essentially adaptations of the BB84 protocol. For effective communication, both parties involved need devices or simulators capable of generating and detecting light pulses with various polarizations.

To create a secret quantum cryptographic key following the BB84 protocol, you need to go through two main phases.

Transmission: A randomly chosen qubit is sent based on photon polarization (from the Master side) [10].

Negotiation: Both communicating parties assess the compatibility of the keys they've obtained [1 0].

To generate the final secret key in this phase, four key stages must be accomplished as follows:

Raw Key Extraction (RK): RK aims to correct errors from qubit discussion in a quantum channel. Parties compare photon polarization to eliminate non-covalent bonds [10].

Error Estimation (EE): During the negotiation for a quantum key over a potentially noisy classical channel, the risk of key damage exists. To prevent this, the master and slave set an error threshold value ("Emax") based on the assumption of no attacks on the transmission medium. After each Quantum Key Distribution (QKD) round, they compare some qubits of their Raw Key (RK) to calculate a transmission error rate ("E"). If E exceeds Emax, it signals a potential attack [10].

Key Reconciliation (KR): When E≤Emax, errors can be present in the non-valent parts of the raw key. Error correction in KR minimizes these errors by dividing the raw key into K-bit blocks, computing parity bits, and comparing them in multiple rounds [10].

Privacy Amplification (PA): PA is the last step in the quantum key extraction protocol (BB84), reducing the bits an attacker might know from the raw key. Parties use a shrinking method on qubit sequences to cut authentication costs and deter attackers [10].

4. Schrodinger's Cat Theory

Schrodinger's Cat [5] is a famous thought experiment in quantum physics. Imagine placing a cat in a sealed box with a vial of poison, a radioactive atom, and a Geiger counter. If the atom decays, the Geiger counter detects it, breaking the vial and harming the Cat. If not, the Cat remains unharmed.

Here's the quantum twist: until we open the box and observe, the Cat exists in a superposition of states, both alive and dead simultaneously. It's a mystery highlighting the strange nature of quantum mechanics. According to quantum principles, particles can exist in multiple states until observed, and this experiment applies that idea to a macroscopic scale, challenging our classical intuitions about reality and observation in the quantum world. Schrodinger's Cat illustrates the peculiarities and complexities of quantum superposition, sparking ongoing discussions about the interpretation of quantum mechanics.

5. QKD Networks [Use Cases]

A. QKD Usage:

The quantum key generation process relies on transmitting photons between two parties over limited distances. This distance limitation poses challenges for authors and organizations, impacting real-world network communications technology. To address this, NIST and DIEHARD suites evaluate the randomness rates of resolved qubits based on p-values. The p-value reflects true randomness in qubit generation, changing with each round's content. This randomness characteristic makes QKD a valuable source for generating random numbers used in encryption algorithms, promoting the adoption of quantum technology [10].

B. Resources allocation in networks:

Quantum Key Distribution (QKD) networks have diverse resources, such as wavelength resources in existing fiber links and secret-key resources in Quantum Key Distribution Points (QKPs). While providing secret-key services, not only do we use secret keys continuously, but we also occupy a certain number of wavelength resources. This becomes crucial,

especially when the network has a limited number of wavelengths. Meeting communication security requirements and optimizing wavelength utilization is essential. To address these challenges, this section establishes a

multi-dimensional resource model in QKD networks. It designs a strategy for routing and resource allocation in the provision of secret-key services. Constantly updating secret keys is crucial to enhance security, as there is a risk of key leakage on both sides of communication [1 0].

6. Quantum Communication Future Possibilities

Government and banking: Ensuring the security and sovereignty of critical national data is vital for government agencies and the military. Quantum Key Distribution (QKD) emerges as a crucial tool in providing quantum-safe security. It can secure private communication links between government agencies, enabling the safe sharing of confidential data. Additionally, QKD-generated secret keys find applications in the banking sector, securing transactions and protecting customer data stored in bank data centers.

Government agencies and banks can implement trusted repeater-based local quantum networks to achieve end-to-end encryption with QKD [6].

Smart grid and national pipelines: Smart grids and national pipelines, crucial for any country's economy, may benefit from Quantum Key Distribution (QKD) to enhance security. QKD can safeguard smart grids, prevent blackouts, and protect pipelines from cyber threats, ensuring robust physical layer security for power line communication [6].

Healthcare: With the rise of e-healthcare during the pandemic, securing sensitive patient data is crucial. Quantum Key Distribution can provide unconditional security for storing, transmitting, and processing this information.

Wearable devices with biosensors can benefit from QKD-based encryption to ensure the confidentiality of intimate health data in the quantum computing era [6].

7. Conclusion

In simple terms, this paper concludes that quantum mechanics, studying the behavior of tiny particles, forms the basis of quantum physics. It explores how these particles display both wave and particle characteristics simultaneously. Quantum Key Distribution is currently the only cryptographic technique providing formally established unconditional security. Over the past 25 years, significant theoretical and experimental research has advanced QKD, with a focus on European implementations. Quantum cryptography has become an established academic field, and QKD technologies continually improve in performance and reliability. Looking ahead, cross-disciplinary collaborations and a focus on long-term security are vital for the future of, especially as it integrates into security infrastructures with network security research and industry partnerships.

References

[1]. Amreen Banu M. Shaikh, Parth D. Shah, BB84 and Identity Based Encryption (IBE) Based A Novel Symmetric Key Distribution Algorithm, Fifth International Conference on Advances in Recent Technologies in Communication and Computing, ARTCom, 2013

[2]. Sufyan T. Faraj Al-Janabi, Omar Kareem Jasim," Reducing the Authentication Cost in QuantumCryptography".

[3]. Dargan, J. How Can Quantum Entanglement Be Used for Secure Communication?

[4]. Tsai, C.-W.; Yang, C.-W.; Lin, J.; Chang, Y.-C.; Chang, R.-S. Quantum Key Distribution Networks: Challenges and Future Research Issues in Security. Appl. Sci. 2021, 11, 3767.

[5]. Fawzy, M. (2023) Quantum superposition and Schrodinger's cat.

[6]. Liu, R. et al. (2022) 'Towards the industrialisation of quantum key distribution in communication networks: A short survey', IET.

[7]. S. R. Hasan, M. Z. Chowdhury, M. Saiam and Y. M. Jang, "Quantum Communication Systems: Vision, Protocols, Applications, and Challenges," in IEEE Access, vol. 11, pp. 15855-15877, 2023.

[8]. Luo, W., Cao, L., Shi, Y. et al. Recent progress in quantum photonic chips for quantum communication and internet. Light Sci Appl 12, 175 (2023).

[9]. KAKU, M. (2023) Quantum Supremacy: How the Quantum Computer Revolution Will Change Everything. S.l.: VINTAGE.

[10]. Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty, Abdel-Badeeh M. Salem, Quantum Key Distribution: Simulation and Characterizations, Procedia Computer Science, Volume 65,2015.

[11]. Marcin Niemiec and Andrzej R. Pach, The measure of security in quantum cryptography, IEEE Global Communications Conference (GLOBECOM), 967 - 972,2012.

[12]. Zheng, X., Zhao, Z. Quantum key distribution with two-way authentication. Opt Quant Electron 53, 304 (2021).