Quantum Networking: Explore QKD and quantum internet

Project for

Advanced Networks Master's program course

Written By: Nikolaos Mouzakitis MTP321

Date Last Edited: January 16, 2025

Abstract

Quantum networking represents a transformative advancement in secure communication, with Quantum Key Distribution (QKD) and the quantum internet standing at its core. Unlike the widely available and adopted classical systems, QKD leverages certain mechanical principles from the field of quantum physics in order to theoretically guarantee unbreakable encryption schemes, addressing critical vulnerabilities in modern cryptographic methods. In the early days of its rise, quantum internet promises a global network enabling unprecedented levels of secure communication, distributed quantum computing, and advanced scientific applications.

Contents

Chapter 1

Introduction

Quantum networking stands as the next frontier in communication technology, which is expected to leverage principles of quantum mechanics for achieving unprecedented levels in security, as well as in computational capability. In contrast to ordinary classical networks, quantum networks rely on quantum states of the likes of superposition and entanglement to achieve operations impossible for the classic networking schemes. These attributes become of vital importance in application areas like secure communications, where quantum key distribution (QKD) promises provable security against eavesdropping, and in distributed computing in cases where quantum nodes could collaborate to solve problems beyond the reach of classical networks. In the modern world, where the requirement for global data security keeps following an increasing trend, quantum networking is considered as a robust solution for protecting sensitive informations. Moreover, it is possible that mixed architectures combining classical and quantum network elements could provide a feasible solution for the future communication systems.

Challenges arise although; despite the promising potential in quantum networking, it faces technical and theoretical obstacles that need to be surpassed in order to achieve and enable an entirely practical implementation and adoption. Because of the very nature of quantum mechanichs, quantum internet is opted to utilize concepts without classical counterparts with the likes of quantum entanglment, no-cloning theorem, quantum measurement and teleportation. In contrast to the classical and well known model of computation experienced so far, where we deeply rely on the fact that information can be read and copied, this concept that does not hold for quantum networking. The scalability remains one of the main issues, because as current quantum networks are limited in the number of nodes and the distances they can span without degradation. This limitation comes from the fragile nature of the quantum states, which are very sensitive on environmental noise and

decoherence especially over long distances. As a countermeassure, in order to avoid these limitations the development of reliable quantum repeaters and advanced error-correction schemes are required.

Additionally, the efficient generation, distribution and storage of entanglement across a network pose critical hurdles, as maintaining high fidelity in entangled states is necessary for the network's functionality.

Another key challenge lies in integrating quantum systems with classical infrastructure, which requires seamless coordination between vastly different operational paradigms. Addressing these challenges is crucial for moving quantum networking beyond the experimental phase and into real-world applications. The computing power of a quantum computer is exponentialy related to the number of qubits that comprise it; where a qubit is the quantum counterpart of the classical bit and is the building block of a quantum computers.

In this project the current state of quantum networking is explored alongside its potential applications. The introduction provides a broad overview of the field, emphasizing its importance in secure communication and presents a brief description of the most common terminology of quantum networking. In the related work section recent advancements in quantum networking are presented, with a focusing on technologies such as quantum key distribution, entanglement distribution, and quantum repeaters. In the combined methodology and results section, a simulation-based approach utilizing QuTiP showcases examples to study the key elements of quantum networking, presenting the findings from the simulations. The discussion section interprets these findings in the context of existing literature, identifying both strengths and limitations of current technologies. In the end, the conclusion section summarizes the project's work.

1.1 A brief description of the most common terms in quantum networking

A **quantum network** consists of a set of quantum processors/devices connected to each other. **Qubits** can be particles such as photons or electrons, carrying certain properties derived from quantum mechanics called *state*. A state's can express the spin of an electron or a photon's polarization. The particular state of a qubit is unknown prior to its measurement, since it is in a superposition (*as an analogy one can think the linear combination of two variables)* of states. After its measurement the qubit collapses in one state, which actually can not be determined before since it is related with the basis

that is used in the measurement.

Quantum superposition consists one of the ground principles in quantum mechanics. It presents the property that quantum system has, of existing in multiple states at the same time, until it gets measured. Superposition denotes that prior to measurement, the system does not exist in any state but in a combination of both states. States in quantum mechanics are denoted as $|\psi\rangle$ and represent a vector in a complex Hilbert space. A system in superposition is described as a linear combination of basis states:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle,$$

where:

- $|0\rangle$ and $|1\rangle$ are the basis states, and
- a_0 ,a_1 belong to complex numbers and satisfy the following equation:

$$|a_0|^2 + |a_1|^2 = 1.$$

Coefficient $|a_0|^2$ represent the probability of measuring the system state as $|0\rangle$ and $|a_1|^2$ the probability to measure it as $|1\rangle$. After describing its properties, we can understand why superposition constitutes a basic difference in between quantum and classical mechanics.

Quantum entanglement is the situation where two qubits become correlated in a way that any modification on the state of the first at once affect the state, and is reflected on the second qubit, without any consideration of their actual distance. Because of the no-cloning theorem, there it is not even possible for a third qubit to be entangled with either of those qubits.

The **no-cloning theorem** is a fundamental principle in quantum mechanics which states that it is impossible to create an exact copy of an unknown quantum state. This theorem has important consequences in quantum information theory and especially in quantum cryptography and networking. The theorem therefore guarantees the secure quantum communication in protocols such as Quantum Key Distribution (QKD) because it is impossible for any eavesdropper who copies quantum states in order to intercept informations to operate unnoticed.

1.2 QKD

Quantum Key Distribution is an approach of sharing and establishing a secret cryptographic key among two communicating entities[8]. In order to achieve

the desired outcome it utilizes both a quantum channel and a classical channel of communication. The quantum one is used to transmit qubits among the entities while the classical one operates for establishing the final key and for encrypted data exchanges following the classical paradigm. QKD is only used for the generation of the initial key.

1.3 Quantum Repeaters

Quantum repeaters are devices which are designed to extend the range of quantum communication networks. They are required to enable QKD in long distances and for supporting the construction of a future quantum internet. In the classical way of communication, the repeaters are used in order to amplify signals for avoiding signal loss, but due to the no-cloning theorem which prohibits duplication of quantum states, this is not applicable on quantum communication. So a quantum repeater in constrast, utilizes entanglement distribution and error correction schemes to achieve the establishment of a quantum connection over long distance.

The main issues that quantum repeaters address are the following: **a)** Photon Loss (Attenuation): tens of kilometers [4]. In fact, quantum repeaters are used for

In fiber-based quantum communication, photons carrying quantum information experience loss as they propagate through the medium. This limits the range of QKD to about 100-200 km without repeaters. Quantum repeaters overcome this by segmenting the communication channel into shorter links. Entanglement is created and stored in each segment, and through entanglement swapping, the links are extended to form a long-distance connection. Decoherence:

Quantum states are highly sensitive to environmental noise, which can cause them to lose coherence. This degrades the fidelity of the transmitted quantum information. Quantum repeaters use quantum memories to store entangled states temporarily, allowing error correction or entanglement purification to maintain the quality of the entanglement. Scalability of Quantum Networks:

Without repeaters, quantum networks would be limited to small, localized regions due to the constraints of photon transmission. Quantum repeaters enable the scalable construction of quantum networks by bridging long distances and connecting multiple network nodes. Error Accumulation:

Errors accumulate over long distances in quantum communication systems. Classical error correction cannot be directly applied to quantum states. Quantum repeaters incorporate error correction protocols such as entangle-

ment purification to address this issue. How Quantum Repeaters Work

Segmented Links:

The total communication distance is divided into smaller segments where entanglement is established. Entanglement Generation:

Pairs of entangled photons are created and distributed between nodes in adjacent segments. Entanglement Swapping:

Entanglement is extended across multiple segments by performing a Bell state measurement at intermediate nodes. Quantum Memory:

Nodes in the network store entangled states temporarily using quantum memories, allowing time for the rest of the network to synchronize. Entanglement Purification:

Imperfections in the entanglement are corrected by combining multiple imperfect pairs to produce fewer high-quality pairs. Applications of Quantum Repeaters

Secure Long-Distance Communication: Quantum repeaters are critical for enabling QKD over continental and intercontinental distances, ensuring unbreakable encryption.

Quantum Internet: They play a foundational role in connecting quantum processors and sensors across vast networks, enabling distributed quantum computing and sensing.

Advanced Scientific Experiments: Long-distance entanglement enabled by quantum repeaters can support experiments testing the foundations of quantum mechanics over unprecedented scales.

Quantum repeaters are thus the cornerstone of overcoming the practical challenges of long-distance quantum communication, paving the way for robust and scalable quantum networks.

Chapter 2

Related Work

In recent years, quantum networking has gained significant attention due to its potential to ignite a revolution in secure communications and distributed computing. Khristo et al. [1] have provided an overview of the field's current status but also of the desired future directions. In their work the key advancements and challenges in the development of quantum networks have been discussed while in addition explored the integration of the quantum key distribution (QKD) and presented a broader vision for the quantum internet.

Van Meter et al. [2] proposed a complete architecture for a scalable unified quantum communications. They utilize a two-pass connection setup and recursive protocol to allow scalability and extensibility for future internetworking of many quantum devices. Authors also presented protocols-algorithms for connection establishments,desicion making, routing and allocation of resources inside the quantum network and its consisting layers. Cacciapuoti et al. [5] also explored the concept of quantum internet. In their work the key differences among quantum and classical networks ar underlined, and point out quantum teleportation as the most fundamental method of transporting informations in a quantum system. Authors proposed a framework for tackling the challenges of a quantum network creation In contrast to traditional quantum repeaters who require the use of entaglement swapping and quantum memory, all-photonic quantum repeaters are based on light particles(photons) for the transfer of quantum information.Authors in [4] propose an all photonic quantum repeater based on RGS (repeater graph states) achieving a higher repetition rate compared to traditional quantum repeaters, and does not require the use of quantum memories. Their proposed scheme offers a fast Bell pair generation ration with only limitation the time required for the creation of the repeater graph state.

There ... [8]

Chapter 3

Methodology and Results

For the purposes of this project, a simulation approach using software tools have been employed in order to enable the demonstration of selected concepts in quantum networking. QuTiP(Quantum Toolbox in Python)[6], an open source framework written in Python, has been used for the simulations.

3.1 BB84 Quantum Key Distribution Protocol

BB84 protocol is a foundational work in the field of quantum key distribution (QKD) protocols, been proposed back in 1984 [7]. It realizes a secure communication of a secret cryptographic key alongside two entities, over a potenitally insecure medium/channel by using principles of quantum mechanics.

In this simulation (code is listed in Listing 1 of Appendix A), two entities entitled Alice and Bob, execute the QDK using the BB84 protocol in order to share a secret key over a potentially non-secure medium. Initially Alice creates a number of qubits (100 in this example) randomly in one of the two possible bases (either 'x' or 'z') and sends them to Bob. Bob on his side, randomly selects a base per qubit and measures it. In the next step, they are comparing their used bases over a classical communication channel and they discard all the bits generated as an outcome from the measured qubits whose bases were not matching. The remaining bits which obtained from matching bases among the two entities are kept and create the shared secret key.

As we can observe in Figure 3.3, the relation of success rate is plotted against the utilized number of qubits in the protocol. The simulation was run for up to 10000 qubits. Success rate is converging to value 0.5, as the probability of Alice and Bob choosing the same base ('x' or 'z') is 50%.

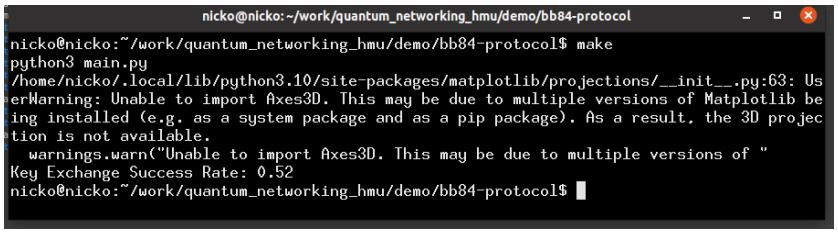

Figure 3.1: Execution of code of Listing 1 of Appendix A.

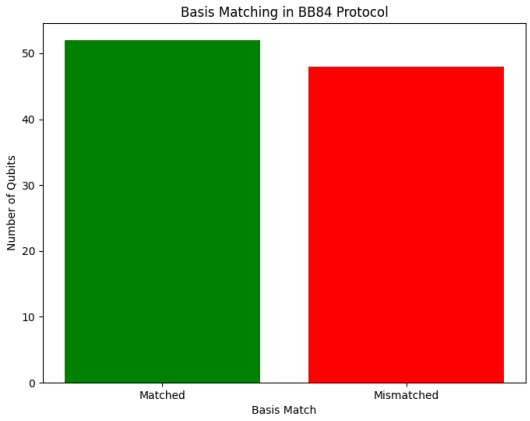

Figure 3.2: Bases matched on the example where 100 qubits used.

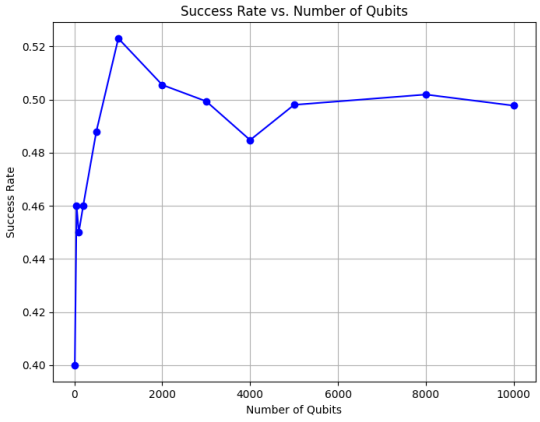

Figure 3.3: Success rate vs number of qubits used.

Chapter 4

Discussion

Chapter 5

Conclusion

Bibliography

[1] Khristo, Y., Asaad, B. and Abdelbaki, N. "Quantum Networking, where it is headed", in *Proc. 16th Int. Computer Engineering Conf. (ICENCO)*, Cairo, Egypt, Dec. 2020, pp. 1–4.

[2] Van Meter, R., Satoh, R., Benchasattabuse, N., Teramoto, K., Matsuo, T., Hajdušek, M., Satoh, T., Nagayama, S. and Suzuki, S. "A Quantum Internet Architecture", *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, 2022, pp. 341-352.

[3] Valls, V., Promponas, P. and Tassiulas, L. "A Brief Introduction to Quantum Network Control", in *Comm. Mag.* 62, 10 (October 2024), pp. 48–53

[4] Benchasattabuse, N., Hajdušek, M. and Meter, R. V. "Protocols for All-Photonic Quantum Repeaters" *2023 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Bellevue, WA, USA, 2023, pp. 314–315.

[5] Cacciapuoti, A. S., Caleffi, M., Tafuri, F., Cataliotti, F. S., Gherardini, S. and Bianchi, G. "Quantum Internet: Networking Challenges in Distributed Quantum Computing," in *IEEE Network*, vol. 34, no. 1, pp. 137-143, January/February 2020

[6] Johansson, J. R., Nation, P. D. and Nori, F. *"QuTiP 2: A Python framework for the dynamics of open quantum systems", Comp. Phys. Comm. 184*, 1234 (2013).

[7] Bennett, C. H and Brassard, G. "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, 1984, pp. 175–179.

[8] Zhou, Y., Tang, Z., Nikmehr, N., Babahajiani, P., Feng, F., Wei, T. C., Zheng, H., and Zhang, P., "Quantum computing in power systems," *iEnergy*, 2022, vol 1, issue 2: 170-187

Appendix A: Simulation Code

Listing 1: BB84 for QKD

```
from qutip import basis, ket2dm
import numpy as np
zero = basis(2, 0)   ''' |0> '''
one = basis(2, 1)    ''' |1> '''
plus = (zero + one).unit()   ''' |+> '''
minus = (zero - one).unit()  ''' |-> '''
''' Alice's qubits'''
def generate_bb84_states(num_qubits):
    states = []
    bases = []
    for _ in range(num_qubits):
        basis_choice = np.random.choice(['z', 'x'])
        bit = np.random.choice([0, 1])
        if basis_choice == 'z':
            states.append(zero if bit == 0 else one)
        else:
            states.append(plus if bit == 0 else minus)
        bases.append(basis_choice)
    return states, bases
'''Measurement'''
def measure_state(state, basis):
    if basis == 'z':
        projection = [zero, one]
    else:  ''' 'x' '''
        projection = [plus, minus]
    probabilities = [abs(proj.overlap(state))**2 for proj in projection]
    return np.random.choice([0, 1], p=probabilities)
'''Simulation'''
num_qubits = 100
alice_states, alice_bases = generate_bb84_states(num_qubits)
bob_bases = np.random.choice(['z', 'x'], num_qubits)
''' Measure and compare '''
bob_results = [measure_state(state, bob_bases[i]) for i, state in enumerate(
    ↪ alice_states)]
matching_bases = [alice_bases[i] == bob_bases[i] for i in range(num_qubits)]
shared_key = [bob_results[i] for i in range(num_qubits) if matching_bases[i
    ↪ ]]
''' Calculate success rate'''
success_rate = len(shared_key) / num_qubits
print(f"Key Exchange Success Rate: {success\_rate:.2f}")
import matplotlib.pyplot as plt
''' Visualization 1: Basis Matching (Bar Chart)'''
matched = sum(matching_bases)
mismatched = num_qubits - matched
plt.figure(figsize=(8, 6))
plt.bar(['Matched', 'Mismatched'], [matched, mismatched], color=['green', '
    ↪ red'])
plt.title('Basis Matching in BB84 Protocol')
plt.xlabel('Basis Match')
plt.ylabel('Number of Qubits')
plt.savefig('Basis Matching in BB84 Protocol.png')
''' Visualization 2: Success Rate vs. Number of Qubits (Line Chart) '''
num_qubits_list = [10, 50, 100, 200, 500, 1000, 2000, 3000, 4000, 5000, 8000
    ↪ , 10000]
success_rates = []
for nq in num_qubits_list:
    alice_states, alice_bases = generate_bb84_states(nq)
```

```
    bob_bases = np.random.choice(['z', 'x'], nq)
    bob_results = [measure_state(state, bob_bases[i]) for i, state in
        ↪ enumerate(alice_states)]
    matching_bases = [alice_bases[i] == bob_bases[i] for i in range(nq)]
    shared_key = [bob_results[i] for i in range(nq) if matching_bases[i]]
    success_rate = len(shared_key) / nq
    success_rates.append(success_rate)
plt.figure(figsize=(8, 6))
plt.plot(num_qubits_list, success_rates, marker='o', color='b')
plt.title('Success Rate vs. Number of Qubits')
plt.xlabel('Number of Qubits')
plt.ylabel('Success Rate')
plt.grid(True)
plt.savefig("Success Rate vs Number of Qubits.png")
```