Quantum Networking: Explore QKD and quantum internet

Project for

Advanced Networks Master's program course

Written By: Nikolaos Mouzakitis MTP321

Date Last Edited: January 15, 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 distributed computing. 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 methodology section, a simulation-based approach utilizing QuTiP showcases examples to study the key elements of quantum networking. The results section presents findings from the simulations, highlighting performance metrics such as communication fidelity and error rates under varying network conditions. 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.

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 a broader vision for the quantum internet.

Chapter 3

Methodology

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)[2], 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 [3]. It realizes a secure communication of a secret cryptographic key alongside two entities, over an insecure medium/channel by using principles of quantum mechanics.

In this simulation, whose code is listed in Listing 1 of Appendix A,

Chapter 4

Results

Chapter 5

Discussion

Chapter 6

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] 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).

[3] 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.

Appendix A: BB84 Quantum Key Distribution 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")
'''Visualization 3: Key Distribution (Histogram) '''
key_bits = [bob_results[i] for i in range(num_qubits) if matching_bases[i]]
plt.figure(figsize=(8, 6))
plt.hist(key_bits, bins=2, color='purple', edgecolor='black', rwidth=0.85)
plt.title('Distribution of Key Bits')
plt.xlabel('Key Bit')
plt.ylabel('Frequency')
plt.xticks([0, 1])
plt.savefig("Distribution of Key Bits.png")
```