**Quantum-Secured NOMA for Next-Gen Network Communication**

*Submitted in partial fulfillment of the requirements for the degree of*

Bachelor of Technology

in

**Electronics and Communication**

*by*

## Preeti Yadav(21BEC0815)

## Basil Syed(21BEC0263)

## Satyam Sinha(21BEC2477)

## Under the guidance of

## Dr.Vijaya Durga Chintala

**SENSE**

**VIT,Vellore.**



April, 2025

**DECLARATION**

I hereby declare that the thesis entitled “Quantum-Secured NOMA for Next-Gen Network Communication" submitted by me, for the award of the degree of *Bachelor of Technology in Programme* to VIT is a record of bonafide work carried out by me under the supervision of Dr.Vijaya Durga Chintala.

I further declare that the work reported in this thesis has not been submitted previously to

this institute or anywhere for the consideration of the degree/diploma.

Place : Vellore Date :20/4/25

**Signature of the Candidate**

### CERTIFICATE

## This is to certify that the thesis entitled “Quantum-Secured NOMA for Next-Gen Network Communication” submitted by Preeti Yadav(21BEC0815),Basil Syed(21BEC0263) and Satyam Sinha(21BEC2477) SENSE, VIT, for the award of the degree of *Bachelor of Technology in Programme*, is a record of bonafide work carried out by him / her under my supervision during the period, 13.12 2024 to 20.04.2025, as per the VIT code of academic and research ethics.

The contents of this report have not been submitted either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university. The thesis fulfills the requirements and regulations of the University and in my opinion meets the necessary standards for submission.

Place : Vellore

Date :20/4/25 **Signature of the Guide**

**Internal Examiner**

## ACKNOWLEDGEMENTS

We are profoundly grateful to our project guide, Dr. Vijaya Durga Chintala, for her unwavering guidance, expert insights, and continuous support throughout the course of this project. Her profound knowledge of Quantum Secured NOMA played a pivotal role in shaping our research approach and helping us achieve our objectives. Her mentorship has inspired us to push our boundaries, enabling us to deepen our understanding and skills in biomedical engineering applications.

We would also like to extend our sincere appreciation to VIT University for providing us with an enriching academic environment and access to resources that have been fundamental to our research journey. The encouragement and support we received from the faculty and the state-of-the-art facilities at VIT have greatly contributed to the success of our project. We are grateful to be part of an institution that fosters innovation, research, and excellence.

**Student Name**

# Executive Summary

This thesis presents a novel **Quantum Key Distribution (QKD)-enhanced Non-Orthogonal Multiple Access (NOMA)** framework designed to address the dual challenges of **secure communication** and **efficient power allocation** in next-generation wireless networks. With the emergence of **6G** and the increasing need for **ultra-secure**, **high-capacity**, and **low-latency communication**, traditional encryption and orthogonal access techniques fall short in ensuring optimal performance.

The proposed system integrates **QKD** for tamper-proof **key exchange**, eliminating vulnerabilities in conventional cryptography, while leveraging **NOMA** to enhance **spectral efficiency** and support **massive device connectivity**. To further optimize network performance, the framework incorporates **machine learning**, particularly **Q-learning**, for dynamic **power allocation** and **modulation adaptation** based on real-time network conditions.

Through this hybrid architecture, the research achieves a significant improvement in **security**, **resource utilization**, and **system throughput**, making it highly suitable for **6G and beyond**. The results demonstrate that this approach not only safeguards against advanced cyber threats but also enhances the overall efficiency of wireless communication systems, paving the way for scalable and secure future networks.

**CONTENTS Page**

**No.**

**Acknowledgement** i

[**Executive Summary** ii](#_h6k28zelw4i)

**Table of Contents** Iii

[**List of Figures** ix](#_agcfu45s6x8t)

[**List of Tables** xiv](#_kgkd560x8u8)

**Abbreviations** xvi

[**Symbols and Notations** xix](#_evtfhkfy3tu9)

1. [**INTRODUCTION** 1](#_3cg7jwd74n13)
   1. Literature Review 1
   2. Research Gap 2
   3. Problem Statement 3
2. **RESEARCH OBJECTIVE** 3
3. **RELEVANCE OF PROBLEM STATEMENT W.R.T SDG** 3
4. **PROPOSED SYSTEM (as applicable)** .
   1. Design Approach / Materials & Methods .
   2. Codes and Standards .
   3. Constraints, Alternatives and Tradeoffs .
5. **PROJECT DESCRIPTION**
6. **HARDWARE/SOFTWARE TOOLS USED**
7. **SCHEDULE AND MILESTONES** .
8. **RESULT ANANLYSIS**
9. **CONCLUSION**
10. Obtained Results
11. Future improvement/work
12. Individual contribution from team members
13. **SOCIAL AND ENVIRONMENTAL IMPACT** .
14. **COST ANALYSIS**
15. **PROJECT OUTCOME PUBLICATION/PATENT**
16. REFERENCES

.

**APPENDIX A**

### List of Figures

|  |  |  |  |
| --- | --- | --- | --- |
| **Figure No.** |  | **Title** | **Page No.** |
| 2.1 | Figure caption |  | 13 |
| 2.2 | Figure caption |  | 15 |

(In the chapters, figure caption should come below the figure and table caption should come above the table. Figure and table captions should be of font size 10.)

### List of Tables

**Table No. Title Page No.**

2.1 Table caption 28

## List of Abbreviations

3GPP Third Generation Partnership Project

2G Second Generation

3G Third Generation

4G Fourth Generation

AWGN Additive White Gaussian Noise

## Symbols and Notations

δf CFO

ε NCFO

### INTRODUCTION

* 1. LITERATURE REVIEW

The rapid evolution of wireless communication networks from 4G to 5G and the impending advent of 6G have introduced unprecedented demands on data rate, latency, connectivity, and most crucially, security. These evolving demands have exposed the limitations of traditional multiple access and encryption techniques, prompting the research community to explore novel paradigms such as Non-Orthogonal Multiple Access (NOMA), Quantum Communication, and intelligent resource management using Machine Learning (ML). The convergence of these advanced technologies promises to lay the foundation for highly efficient, secure, and adaptive communication systems that can meet the rigorous requirements of future wireless networks.

**1.1.1 Limitations of Traditional Access and Security Mechanisms**

Orthogonal Multiple Access (OMA) schemes have historically formed the backbone of wireless communication systems up to and including 4G LTE networks. OMA assigns orthogonal time, frequency, or code resources to individual users, effectively eliminating intra-cell interference. While this ensures simplicity and reliability, it also leads to inefficient spectrum utilization, particularly in high-density scenarios. As we transition to 5G and eventually to 6G, the need for higher spectral efficiency and massive connectivity becomes paramount. OMA’s rigid allocation structure is ill-suited for these conditions, as it cannot scale effectively with the increasing number of devices and the diverse Quality of Service (QoS) requirements.

Moreover, conventional cryptographic security methods, while robust in current applications, are fundamentally vulnerable to future threats posed by quantum computing. Algorithms such as RSA and ECC rely on the computational difficulty of factorization and discrete logarithms—problems that quantum algorithms like Shor’s can solve in polynomial time. This vulnerability necessitates the exploration of quantum-resistant or quantum-secured communication techniques.

**1.1.2 Emergence and Evolution of NOMA**

To address spectrum efficiency limitations, NOMA has emerged as a revolutionary multiple access technology, particularly suitable for 5G and future 6G networks. Unlike OMA, NOMA allows multiple users to share the same frequency band simultaneously by superimposing signals in the power domain. The receiver employs **Successive Interference Cancellation (SIC)** to decode the signals based on their relative power levels.

Ding et al. (2017) played a pivotal role in showcasing NOMA’s capabilities. Their work demonstrated how power-domain multiplexing could significantly enhance system throughput and support massive connectivity. Subsequent studies built upon this by analyzing the performance of uplink and downlink NOMA under various channel conditions. However, key challenges persisted, including the design of efficient SIC algorithms, mitigation of intra-cell and inter-cell interference, and most notably, the issue of **fair and optimal power allocation** among users with diverse channel gains.

Power allocation in NOMA is critical; assigning too much power to strong users undermines fairness, while favoring weak users compromises overall system efficiency. Various optimization techniques, including convex programming and heuristic algorithms, have been proposed, yet they often require centralized control and prior knowledge of channel conditions, limiting their adaptability in dynamic environments.

**1.1.3 Rise of Quantum Communication for Enhanced Security**

In parallel to the exploration of efficient access schemes, the field of Quantum Communication has gained traction due to its promise of **unconditional security** grounded in the principles of quantum mechanics. The foundational BB84 protocol, introduced by Bennett and Brassard in 1984, remains a cornerstone in the domain of **Quantum Key Distribution (QKD)**. This protocol leverages quantum properties like superposition and no-cloning to enable two parties to generate a shared secret key with provable security against eavesdropping.

Numerous practical implementations of QKD have since been realized across fiber-optic and free-space optical channels. Commercial systems from companies like ID Quantique and academic demonstrations such as the Chinese Micius satellite have showcased QKD’s feasibility. However, challenges related to key generation rate, distance limitations, and integration with classical communication infrastructure continue to hinder large-scale adoption. Furthermore, standalone QKD systems do not address issues related to spectrum utilization or resource allocation, necessitating integration with broader wireless communication frameworks.

**1.1.4 Integration of Quantum Security with NOMA**

Given the complementary strengths of QKD and NOMA—security and efficiency respectively—researchers have started exploring hybrid systems that combine these technologies. Zhou et al. (2020) introduced one such **Quantum-NOMA framework**, demonstrating that embedding QKD within a NOMA system could enhance both data confidentiality and spectral efficiency. Their simulation results confirmed that user authentication and data encryption could be significantly improved without substantial degradation in throughput.

However, existing quantum-NOMA systems often rely on **fixed power allocation strategies**, which limit adaptability in heterogeneous network scenarios. This inflexibility becomes particularly problematic in 6G, where user mobility, traffic demands, and channel conditions can change rapidly and unpredictably. Therefore, a dynamic and intelligent power control mechanism is necessary for such hybrid systems to operate optimally in real-world conditions.

**1.1.5 Machine Learning for Adaptive Resource Management**

To address the adaptability challenge, recent studies have investigated **Machine Learning (ML)** approaches for resource management in NOMA systems. In particular, **Reinforcement Learning (RL)** and its model-free variant, **Q-learning**, have shown promise in optimizing power allocation without requiring prior knowledge of the environment.

Li et al. (2019) proposed a Q-learning-based framework for multi-user NOMA networks, where the agent learns optimal power distribution policies through interactions with the environment. The approach successfully improved throughput and ensured user fairness by dynamically adjusting power levels based on real-time network conditions. However, these methods often assume a classical security infrastructure and do not incorporate quantum-resistant or quantum-secured encryption schemes, thereby remaining vulnerable to future quantum attacks.

**1.1.6 Identified Research Gaps**

The review of existing literature highlights several gaps and opportunities for future research:

* Current NOMA systems, while spectrally efficient, lack robust security frameworks that can withstand quantum threats.
* QKD-based systems offer strong security but have not been widely integrated with dynamic resource allocation mechanisms.
* Existing hybrid Quantum-NOMA models often use static power allocation, which limits their real-time adaptability.
* ML-based power control strategies show strong potential but have not been combined with quantum-secure communication protocols.

**1.1.7 Thesis Contribution**

This thesis aims to bridge these gaps by proposing a **QKD-enhanced NOMA framework** with **Q-learning-based adaptive power allocation**. The proposed system offers:

* **Quantum-level security** through the implementation of BB84-based QKD for key exchange and message encryption.
* **Efficient spectrum utilization** via power-domain NOMA for multiple-user access.
* **Real-time adaptability** using Q-learning to dynamically allocate transmission power based on user requirements and channel variations.

By integrating these three domains—Quantum Communication, NOMA, and ML-based control—this work envisions a comprehensive solution that meets the dual demands of efficiency and security in 6G and beyond. The proposed model is designed to operate effectively in dynamic, high-density wireless environments while ensuring data confidentiality against classical and quantum adversaries.

**1.2 Research Gap**

As wireless communication technologies transition toward the sixth generation (6G), the expectations from network infrastructure have significantly evolved. Unlike previous generations focused on higher data rates and expanded capacity, 6G networks are anticipated to deliver an integrated platform capable of ultra-reliable low-latency communication (URLLC), enhanced spectral and energy efficiency, massive machine-type communication (mMTC), and quantum-secure data transmission. These demands stem from the rise of futuristic applications such as autonomous driving, telemedicine, immersive extended reality (XR), and the Internet of Everything (IoE), which impose stringent requirements on both performance and security.

Despite the surge in research and development, existing communication frameworks face limitations in simultaneously achieving these multi-dimensional objectives. Technologies such as **Non-Orthogonal Multiple Access (NOMA)** and **Quantum Communication**, especially **Quantum Key Distribution (QKD)**, have shown promise in addressing specific challenges related to capacity, spectral efficiency, and secure transmission. However, these technologies have been largely developed and studied in isolation, with limited research investigating their synergistic potential within a single cohesive framework for next-generation networks.

**Limitations of Conventional NOMA Frameworks**

NOMA, in contrast to traditional Orthogonal Multiple Access (OMA), enables multiple users to share the same time-frequency resource by utilizing power domain multiplexing and Successive Interference Cancellation (SIC) at the receiver end. This allows better spectral efficiency and user fairness. Despite its theoretical advantages, practical implementations of NOMA face several challenges:

* **Inter-User Interference**: NOMA relies on the simultaneous transmission of signals to multiple users, leading to unavoidable inter-user interference. When SIC is imperfect, this interference significantly degrades performance.
* **Fixed Power Allocation**: Many existing NOMA implementations use fixed or heuristic-based power allocation, which may be efficient for static environments but perform poorly in dynamic, real-time, or mobile scenarios.
* **Scalability Issues**: As the number of users grows, maintaining efficient and fair power distribution becomes more complex.
* **Lack of Real-Time Optimization**: Static models cannot respond to fluctuating channel conditions, user mobility, and application-specific QoS requirements.

These shortcomings imply that while NOMA enhances spectral efficiency, it requires advanced, intelligent control mechanisms for power and interference management to be fully viable in future networks.

**Underutilization of Quantum Security in Wireless Systems**

In parallel, the advancement of quantum computing presents a double-edged sword. On one hand, it brings powerful computational capabilities. On the other, it threatens the foundation of classical cryptographic systems such as RSA and ECC, which rely on the computational difficulty of certain mathematical problems. Algorithms like Shor’s and Grover’s can efficiently break these schemes, rendering them obsolete in a post-quantum era.

**Quantum Key Distribution (QKD)** emerges as a robust countermeasure to this threat. It leverages quantum mechanical principles such as the Heisenberg Uncertainty Principle and the No-Cloning Theorem to ensure unconditionally secure key generation and exchange. Protocols like BB84, E91, and B92 have demonstrated theoretical and experimental success in securing communication against any form of computational attack, including those from quantum computers.

However, despite its potential, QKD is mostly applied in **point-to-point** fiber-optic networks and isolated quantum testbeds. Its integration into wireless and multi-user environments, particularly within NOMA-based systems, is largely unexplored due to challenges such as:

* **Dynamic Key Distribution**: Adapting QKD to serve multiple users in a dynamic access scheme like NOMA is technically complex.
* **Hardware Feasibility**: QKD traditionally requires sensitive hardware (e.g., photon detectors, beam splitters) which may be difficult to miniaturize for mobile wireless environments.
* **Latency Considerations**: Quantum key generation and synchronization can introduce delays, impacting the real-time performance required in 6G scenarios.

Thus, QKD remains underutilized as a practical solution for securing next-generation wireless systems, despite its theoretical benefits.

**Potential of Machine Learning in NOMA Systems**

In recent years, **Machine Learning (ML)** techniques have gained traction in wireless networks for tasks like channel estimation, resource allocation, and anomaly detection. In particular, **Reinforcement Learning (RL)**, and its subset **Q-learning**, show great promise for adaptive and real-time decision-making.

Q-learning is a model-free, value-based RL algorithm that learns optimal policies through trial and error interaction with the environment. It does not require prior knowledge of system dynamics, making it suitable for complex wireless systems with dynamic channel conditions and heterogeneous user demands. Q-learning has been successfully applied to:

* Dynamic spectrum access
* Load balancing
* Beamforming
* Power control

In the context of NOMA, Q-learning can be used to allocate power efficiently among users in real-time, minimizing interference and maximizing throughput. However, current implementations typically focus on power allocation alone and do not account for security or integration with cryptographic protocols like QKD.

**The Missing Link: Unified QKD-Q-learning-NOMA Framework**

Despite the individual benefits of QKD, Q-learning, and NOMA, the literature lacks a unified framework that integrates these three technologies to address the holistic challenges of 6G. Most research efforts have treated these technologies in isolation:

* QKD has been studied in secure key distribution scenarios without accounting for resource-constrained, multi-user wireless networks.
* NOMA has focused on spectral efficiency, often neglecting advanced security protocols and adaptive optimization.
* Q-learning has been used for power allocation without integration into quantum-secure architectures.

This creates a **critical research gap**: the absence of a scalable, secure, and intelligent communication architecture that:

1. **Incorporates QKD** for unbreakable key exchange.
2. **Implements Q-learning** for real-time, adaptive power allocation.
3. **Operates within a NOMA** framework to maximize spectral efficiency.

Moreover, the **practical considerations** of deploying such an integrated system—such as latency, hardware constraints, energy consumption, and interoperability—are often overlooked. Existing models fail to provide simulation or experimental results that demonstrate real-world viability, particularly in scenarios involving user mobility, variable QoS requirements, and fluctuating channel conditions.

**Objective of the Proposed Research**

This project aims to **bridge this multi-dimensional research gap** by developing and validating a unified communication framework that integrates:

* **Quantum Key Distribution** for secure and tamper-proof key exchange.
* **Q-learning** for intelligent and adaptive power allocation in dynamic user environments.
* **Non-Orthogonal Multiple Access** to ensure spectral efficiency and support for massive user connectivity.

The proposed system will be evaluated using Python-based simulations (e.g., using Qiskit and wireless toolkits), focusing on metrics such as Bit Error Rate (BER), Spectral Efficiency, Key Rate, Latency, and Energy Efficiency.

By addressing the technical limitations and theoretical gaps identified above, this research aspires to offer a **holistic, scalable, and secure solution** for future wireless networks—laying the foundation for practical 6G deployment.

**1.3 Problem Statement**

The exponential growth of connected devices, real-time applications, and data-intensive services is redefining the architecture and performance expectations of wireless communication systems. With the evolution toward sixth-generation (6G) networks, the wireless ecosystem is expected to support a diverse range of applications, including holographic communication, industrial automation, autonomous vehicles, and extended reality (XR). These applications demand ultra-reliable low-latency communication (URLLC), massive machine-type communication (mMTC), and enhanced mobile broadband (eMBB), all underpinned by unprecedented scalability, security, and efficiency.

Traditional communication frameworks, especially those relying on Orthogonal Multiple Access (OMA), are increasingly unable to meet these demands. OMA-based techniques, which assign distinct time or frequency resources to each user, inherently limit the number of users and lead to inefficient spectrum utilization. This becomes a critical bottleneck in ultra-dense 6G environments, where simultaneous connectivity for thousands of devices per square kilometer is required.

To address these constraints, Non-Orthogonal Multiple Access (NOMA) has emerged as a key enabler for 6G networks. NOMA enhances spectral efficiency by allowing multiple users to share the same frequency resources simultaneously, distinguishing them via power domain multiplexing and successive interference cancellation (SIC). While NOMA effectively increases user capacity and data throughput, it introduces a new set of technical challenges, particularly in multi-user scenarios. Among the most pressing issues are:

* **Inter-user interference**, due to simultaneous signal transmission,
* **Complex and suboptimal power allocation**, especially in dynamic environments, and
* **Inherent security vulnerabilities**, especially when integrated into cloud-native, distributed 6G architectures.

In parallel, the growing capabilities of quantum computers threaten the security of existing encryption and key distribution protocols. Classical cryptographic systems, which rely on the computational difficulty of certain mathematical problems (e.g., factoring large primes or computing discrete logarithms), are vulnerable to quantum algorithms such as Shor’s and Grover’s algorithms. These quantum threats necessitate a shift to more secure communication paradigms that are resilient to quantum attacks.

Quantum Key Distribution (QKD) emerges as a promising solution to this challenge. QKD leverages the fundamental properties of quantum mechanics—such as superposition and no-cloning theorem—to enable the generation and exchange of encryption keys that are provably secure. Protocols like BB84 and E91 have demonstrated the theoretical and experimental feasibility of unconditionally secure key distribution over optical fibers and free-space links. However, QKD remains underexplored in the context of mainstream wireless access technologies like NOMA. Most QKD implementations are point-to-point and struggle to adapt to the dynamic, multi-user nature of 6G wireless environments.

Thus, integrating QKD into a multi-user NOMA framework introduces a significant research challenge. How can quantum-secure key distribution be extended to multiple users without compromising the efficiency or scalability of the system? Furthermore, the real-time integration of QKD with NOMA requires novel techniques to handle user scheduling, resource allocation, and key synchronization—all in a latency-sensitive environment.

Another dimension of complexity in NOMA lies in **power allocation**. Since NOMA relies on differentiating users by assigning them varying power levels, the accuracy and efficiency of power allocation algorithms directly impact system performance. In conventional NOMA systems, power allocation is typically carried out using fixed or heuristic rules, which do not scale well in real-time, mobile, or heterogeneous environments. These static methods are insufficient for scenarios involving rapidly changing user demands, varying channel conditions, and diverse Quality of Service (QoS) requirements.

To address this limitation, there is a growing interest in leveraging **Machine Learning (ML)**, particularly **Reinforcement Learning (RL)**, for intelligent resource allocation in wireless networks. Among various RL techniques, **Q-learning** has gained attention due to its model-free nature and ability to learn optimal policies through environmental interactions. Q-learning allows the system to adaptively determine power levels for different users based on feedback, such as Signal-to-Noise Ratio (SNR), interference levels, and QoS requirements. This adaptability is critical for the successful deployment of NOMA in 6G systems.

Despite the promising aspects of QKD, NOMA, and Q-learning individually, their **integration into a unified framework remains largely unexplored**. While researchers have studied QKD for secure communication and Q-learning for dynamic resource management, the combined use of QKD for security and Q-learning for real-time power control within a NOMA-based wireless system represents an untapped area with enormous potential.

Moreover, such integration poses non-trivial challenges. For instance, ensuring the seamless synchronization between QKD key updates and NOMA user transmissions requires precise coordination. Similarly, balancing the trade-off between security (using quantum keys) and performance (ensuring low latency and high throughput) must be carefully managed. These design trade-offs become more complex when deployed in real-world wireless environments with user mobility, imperfect channel estimation, and hardware constraints.

Given the limitations of existing technologies and the ambitious goals of 6G, a unified, secure, and intelligent communication framework is urgently needed. This framework should fulfill the following requirements:

* **Scalability** to support large numbers of users and devices in dense network environments.
* **Security** to protect data and user privacy against both classical and quantum attacks.
* **Intelligence and Adaptability** to optimize power allocation dynamically and autonomously in real time.
* **Compatibility** with existing and emerging wireless protocols to enable seamless integration and deployment.

Therefore, **the core research problem** that this project addresses is:

**How can we design a secure, scalable, and intelligent communication framework that integrates Quantum Key Distribution (QKD) for enhanced encryption and Q-learning for efficient, adaptive power allocation within a NOMA-based access environment, thereby meeting the complex performance and security demands of 6G wireless networks?**

This project aims to develop and validate a comprehensive solution to this problem through simulation, algorithmic design, and performance evaluation. It will demonstrate how integrating QKD and Q-learning into the NOMA framework can significantly enhance the security, efficiency, and adaptability of next-generation wireless communication systems.

By bridging the current research gap and addressing the multi-domain challenges in a unified manner, the outcomes of this project have the potential to set a new benchmark for future wireless communication standards.

2.Research Objective

The overarching goal of this project is to design and implement a **Quantum Key Distribution (QKD)-enhanced Non-Orthogonal Multiple Access (NOMA)** framework that facilitates ultra-secure, highly efficient, and scalable wireless communication in 6G and beyond. As wireless communication systems evolve, especially with the emergence of 5G and 6G technologies, the demand for enhanced security, efficiency, and adaptability has reached unprecedented levels. This research seeks to address the challenges associated with these evolving requirements by combining cutting-edge technologies, including Quantum Communication, NOMA, and Machine Learning (ML), to create an integrated solution that is both secure and capable of meeting the requirements of future networks. The specific objectives of this research can be outlined as follows:

**1. Integrating Quantum Communication Principles for Ultra-Secure Encryption**

One of the core aims of this project is to incorporate **Quantum Key Distribution (QKD)** as the fundamental security mechanism to ensure **unbreakable encryption** and detection of any eavesdropping attempts. Traditional encryption methods, such as RSA or elliptic-curve cryptography, are susceptible to future threats posed by quantum computing, which can solve problems like integer factorization and discrete logarithms in polynomial time using quantum algorithms (e.g., Shor’s algorithm). This vulnerability calls for quantum-resistant security mechanisms, and QKD, based on the principles of quantum mechanics, offers a solution that guarantees the confidentiality of communication against any adversaries, including those equipped with quantum computing capabilities.

The **BB84 protocol**, introduced by Bennett and Brassard in 1984, is one of the most well-known QKD protocols. By leveraging quantum properties such as the no-cloning theorem and quantum superposition, QKD ensures that any eavesdropping attempt on the key exchange process can be detected by the legitimate parties. This project will explore the implementation of **QKD for key generation and exchange** over both fiber-optic and free-space channels, taking into consideration practical issues such as key rate, transmission distance, and integration with existing wireless systems.

The challenge in this research is integrating QKD with **NOMA-based communication systems**, as QKD typically requires higher bandwidth and specific protocols, whereas NOMA needs efficient spectrum usage. By leveraging QKD to establish secure communication channels, the project aims to ensure that each user’s data is encrypted with quantum security, while still utilizing NOMA’s spectral efficiency advantages.

**2. Enhancing Spectral Efficiency and Massive Device Connectivity through NOMA**

Another crucial objective is to enhance **spectral efficiency** and **massive device connectivity** using **Non-Orthogonal Multiple Access (NOMA)**. NOMA addresses the limitations of conventional Orthogonal Multiple Access (OMA) schemes by allowing multiple users to transmit their data simultaneously over the same frequency spectrum, effectively increasing system throughput. This simultaneous transmission is made possible by **power-domain multiplexing**, where users are assigned different power levels according to their channel conditions, and the receiver employs **Successive Interference Cancellation (SIC)** to decode the overlapping signals.

In future 6G networks, where massive connectivity (e.g., billions of devices) and low latency are paramount, NOMA offers a scalable solution that OMA cannot match. Unlike OMA, which requires distinct orthogonal resources for each user, NOMA allows for a more efficient use of the available spectrum. This research aims to develop a NOMA framework that supports **massive connectivity** in dense environments while maintaining **high system throughput** and **low latency**.

A significant challenge that remains with NOMA systems is ensuring **fair power allocation** among users, especially in heterogeneous environments where users have different channel gains and QoS requirements. This research will propose a new approach to power allocation, which will be adaptive and dynamic, leveraging **Machine Learning (ML)** techniques such as **Q-learning** to optimize power distribution in real-time. By doing so, the system will ensure that users with weaker channels are allocated more power, while users with stronger channels are allocated less power, improving overall system fairness and throughput.

**3. Developing Machine Learning-Based Power Allocation Strategy**

The third objective focuses on developing a **machine learning-based power allocation strategy** that adapts to real-time channel conditions and optimizes resource usage. Traditional power allocation strategies in NOMA are often based on static algorithms that do not account for real-time changes in user locations, mobility, or fluctuating channel conditions. Moreover, these classical algorithms may not efficiently handle dynamic interference, especially in dense and high-demand networks, which are expected to characterize 6G systems.

To address this challenge, this research will leverage **Reinforcement Learning (RL)**, specifically **Q-learning**, for adaptive power control. Q-learning, a model-free RL algorithm, will allow the system to learn optimal policies for power allocation by interacting with the network environment, without requiring a priori knowledge of the network state. In this approach, an RL agent will dynamically adjust the transmission power based on real-time observations, such as channel quality, interference levels, and the number of users in the network. By doing so, the system will be able to maximize throughput and minimize power consumption while ensuring fairness and reducing interference between users.

The Q-learning-based approach will also enable the **dynamic adjustment of transmission parameters** (such as modulation schemes and coding rates), allowing the system to optimize its performance under varying network conditions. This capability is essential for future networks where conditions can change rapidly, and systems must adapt to meet the needs of users with diverse QoS demands.

**4. Supporting Adaptive Modulation Schemes for Dynamic Transmission Adjustment**

The ability to adapt transmission parameters based on **real-time channel conditions** is another key objective of this research. In future networks, user mobility, interference, and varying channel quality will necessitate the use of **adaptive modulation and coding schemes** to maintain reliable communication. Adaptive modulation allows for the selection of the most appropriate modulation scheme based on instantaneous channel conditions, ensuring efficient spectrum usage while maintaining the desired quality of service.

This research will explore techniques such as **Adaptive Modulation and Coding (AMC)**, which adjusts the modulation order and coding rate dynamically in response to channel fluctuations. By integrating AMC with the **Q-learning-based power allocation** system, the framework will adapt transmission parameters in real-time to ensure high throughput, low latency, and robust security for users. The combined approach will optimize network performance, balancing data rates with energy efficiency and robustness against interference.

**5. Evaluating the Proposed System’s Performance for 6G Scenarios**

Finally, the proposed system will be evaluated against a range of performance metrics, including **security**, **throughput**, **energy efficiency**, and **latency**, to assess its suitability for **Beyond 5G (B5G) and 6G networks**. These metrics are critical in determining the feasibility of the system in high-density, high-speed, low-latency environments. The evaluation will include both theoretical analysis and simulations to quantify the system’s performance under various network conditions.

Security will be evaluated based on the **quantum-resistance** of the QKD-based encryption mechanisms, ensuring that the system is secure against potential quantum attacks. Throughput will be assessed in terms of the system’s ability to support high data rates while maintaining user fairness and minimizing interference. Energy efficiency will be evaluated by analyzing the power consumption of the system, particularly in terms of the **power allocation strategy** and **adaptive modulation schemes**, while latency will be measured by the system’s responsiveness to user demands and its ability to minimize delay in data transmission.

**1.3.1 Relevance of the Problem Statement with respect to SDG**

The proposed research aligns closely with several United Nations Sustainable Development Goals (SDGs), reflecting its broader societal and global relevance. The integration of Quantum Key Distribution (QKD) and Machine Learning-powered Non-Orthogonal Multiple Access (NOMA) not only addresses critical challenges in the field of wireless communication but also has profound implications for achieving sustainable development. Below, we discuss how this research contributes to four key SDGs:

**SDG 9 – Industry, Innovation, and Infrastructure**

One of the central aims of this research is to enhance communication infrastructure using advanced technologies like **QKD** and **Machine Learning-powered NOMA**. This combination contributes directly to the development of **resilient and intelligent communication systems**, which are essential for future technologies. Smart cities, autonomous vehicles, remote healthcare, and other emerging fields all rely on robust communication networks that are both efficient and secure. NOMA’s ability to increase the spectral efficiency of wireless networks, while QKD ensures security, addresses the dual challenge of improving both capacity and privacy in digital communication systems.

By focusing on the development of secure, scalable, and energy-efficient communication frameworks, this research lays the foundation for **sustainable industrial innovation**. A resilient communication infrastructure is not only vital for day-to-day operations but also plays a pivotal role in **driving future advancements** in industrial sectors, ranging from manufacturing to transportation. Thus, the integration of QKD and NOMA within communication infrastructure will contribute to meeting the growing demand for more innovative, secure, and reliable networks in the industrial sector.

**SDG 11 – Sustainable Cities and Communities**

As cities become more connected and smarter, the need for **secure and efficient communication** networks becomes even more critical. The concept of **smart cities** depends heavily on **IoT devices**, autonomous transportation systems, and emergency services that require real-time, high-throughput communication with minimal latency. The QKD-NOMA framework proposed in this research is designed to meet these requirements by enabling **massive device connectivity**, supporting secure transmission, and reducing latency. These attributes are fundamental to ensuring that smart cities can function seamlessly.

Furthermore, the framework’s ability to guarantee **low-latency communication** supports vital city services, such as **traffic control systems**, **public safety**, and **emergency response services**, all of which depend on reliable communication to operate efficiently. With the rapid growth of urban populations and the increasing dependence on technology, **secure and efficient communication systems** are essential for enhancing the quality of life, reducing traffic congestion, and improving emergency responses. This research, therefore, supports the goal of building **sustainable cities and communities** by improving the communication infrastructure on which they depend.

**SDG 16 – Peace, Justice, and Strong Institutions**

The increasing digitization of communication systems has brought about significant challenges in terms of **data security and privacy**. The rise in cyber threats and digital surveillance highlights the vulnerability of traditional communication systems that rely on classical encryption methods. The integration of **QKD** into the proposed system addresses this vulnerability by offering **quantum-secure communication**. QKD-based encryption is **theoretically immune to eavesdropping**, offering an unbreakable security mechanism that protects sensitive data from unauthorized access.

By ensuring the **integrity and confidentiality** of transmitted data, this research promotes **trust** in digital governance, strengthening the foundation for peace, justice, and strong institutions. Reliable and secure communication systems are fundamental for **good governance** and **transparent institutions**, as they ensure the safe exchange of information without compromising privacy. Moreover, the research contributes to the broader goal of building **secure and stable digital environments** in which individuals, organizations, and governments can operate confidently without fear of surveillance or cyber-attacks.

**SDG 7 – Affordable and Clean Energy (Indirectly)**

While not directly focused on energy, the research indirectly supports **SDG 7**, which advocates for **affordable and clean energy**. Through the application of **Q-learning for adaptive power allocation**, the proposed framework aims to optimize **energy consumption** in wireless networks. By ensuring that **power resources** are allocated efficiently among users, this research contributes to **energy-saving** in large-scale communication infrastructures. Wireless networks are known for their significant energy consumption, especially as the number of connected devices grows. Optimizing the power usage in these networks not only improves the system’s performance but also helps to **reduce its environmental impact**. Therefore, the intelligent power management proposed in this research can play a role in reducing the carbon footprint of communication infrastructure and contributing to a more **energy-efficient** digital future.

**Conclusion**

In summary, this research contributes significantly to the **SDG framework** by developing advanced communication technologies that are **secure, efficient, and scalable**, ensuring their alignment with key global goals. Through the integration of **quantum-secure communication** and **machine learning** techniques, it enhances **infrastructure innovation**, supports the creation of **smart and sustainable cities**, strengthens **digital governance**, and indirectly promotes **energy efficiency**. The proposed research offers a pathway towards a more **inclusive**, **sustainable**, and **secure digital future**, in line with the United Nations’ vision for a sustainable global society.

3.PROPOSED WORK

**3.1 Proposed Work: System Design and Approach**

The core of this project lies in the integration of **Quantum Key Distribution (QKD)** and **Non-Orthogonal Multiple Access (NOMA)**, with the aim of developing a **secure, efficient, and adaptive wireless communication framework** suitable for **6G networks**. This hybrid framework leverages **quantum-secured communication** and **machine learning-driven power allocation**, thereby addressing the critical requirements of **security**, **spectral efficiency**, and **energy optimization** in next-generation networks.

**Tools and Technologies Used**

**1. Python**

Python serves as the **primary programming environment** for designing, simulating, and testing both classical and quantum components of the proposed system:

* Development of the **Q-learning algorithm** for adaptive power allocation.
* Implementation of **simulation environments** to evaluate user throughput, interference levels, and energy efficiency.
* Integration of classical and quantum communication channels for hybrid analysis.

**2. Qiskit (IBM Quantum SDK)**

Qiskit is used to simulate the **quantum communication channel**, particularly for **QKD (Quantum Key Distribution)** processes:

* Simulation of **BB84** and **E91 protocols** to generate quantum-secure keys.
* Emulation of **quantum entanglement**, **state transmission**, and **eavesdropper detection**.
* Evaluation of **key rate**, **error rate**, and **channel fidelity**.

**3. ClasIQ Tool**

ClasIQ (Classical-Quantum Integration and Simulation Platform) enables seamless **integration of classical communication protocols** (NOMA) with **quantum modules**:

* Provides a **bridge between classical data layers and quantum-secured key exchange**.
* Ensures **coherent synchronization between secure quantum channels and classical power allocation layers**.
* Offers modular visualization and debugging of hybrid quantum-classical systems.

**System Workflow and Implementation**

1. **Quantum Key Generation**  
   Using Qiskit, quantum keys are generated through **BB84 protocol**. The quantum channel ensures **eavesdropper detection** and **key verification** using **qubits in superposition**. If the quantum bit error rate (QBER) remains below threshold, the secure key is used for classical encryption and transmission.
2. **User Grouping and Channel Estimation**  
   Users are classified based on **channel gain** and **signal-to-noise ratio (SNR)**. NOMA groups are formed with one **strong channel user** and one **weak channel user**, as per conventional NOMA design.
3. **Q-Learning Based Power Allocation**  
   A **Q-learning algorithm** is implemented in Python to dynamically allocate power among users in each NOMA cluster:
   * **States**: Represent channel conditions and user demands.
   * **Actions**: Correspond to power allocation ratios.
   * **Rewards**: Based on **system throughput**, **energy efficiency**, and **fairness index**.
   * The system learns optimal allocation through **trial-and-error** and **policy improvement** over episodes.
4. **Data Transmission Using QKD Encryption**  
   Once power is optimally allocated, user data is **encrypted using QKD keys** and transmitted over classical NOMA channels. This ensures **end-to-end security** while achieving **multi-user spectrum sharing**.
5. **Performance Analysis**  
   The final step involves analyzing:
   * **Secrecy capacity**
   * **Bit error rate (BER)**
   * **System throughput**
   * **Energy consumption**
   * **Key generation rate**

**Challenges and Solutions**

| **Challenge** | **Proposed Solution** |
| --- | --- |
| Unsecure classical transmission | Use of **QKD via Qiskit** to generate quantum-secure keys, immune to eavesdropping. |
| Power allocation inefficiency in NOMA | Implementation of **Q-learning algorithm** for adaptive and dynamic power control. |
| High complexity of hybrid systems | Utilization of **ClasIQ** to streamline classical-quantum integration workflows. |
| Scalability in multi-user environments | Use of **adaptive learning strategies** to tune power parameters per user cluster. |
| Latency introduced by key exchange and learning | Optimization of **reward functions and learning rates** for faster convergence. |

**Novelty of the Proposed Approach**

* **First hybrid system** that integrates **QKD with NOMA using machine learning**.
* Utilizes **Q-learning** for context-aware, **fair and efficient power allocation**.
* Ensures **quantum-level security** with real-time adaptability to channel and network dynamics.
* Uses **open-source tools** like **Qiskit** and **Python**, and **ClasIQ** for scalable simulation.

4.2 Codes and Standards

This project integrates **Quantum Computing**, **Q-Learning**, and **Non-Orthogonal Multiple Access (NOMA)** to build a secure and efficient wireless communication system. It is structured into three main components:

1. Quantum-Inspired BER Simulation for NOMA
2. Q-Learning-Based Dynamic Power Allocation
3. Quantum Key Generation and Message Encryption using Qiskit

**A. Quantum-Inspired NOMA Simulation**

**Objective**: Simulate Bit Error Rate (BER) performance of two-user NOMA under quantum-inspired power allocation.

**Key Concepts**:

* Superposition coding using custom power levels.
* Rayleigh fading channel simulation.
* Successive Interference Cancellation (SIC) for decoding.
* Gaussian noise modeling for different SNR levels.

**Output**:

* BER vs SNR plot for both users.
* Demonstrates improved BER for the weak user due to higher power allocation.

**B. Q-Learning-Based Power Allocation**

**Objective**: Optimize power distribution among users using Q-learning based on SINR targets across different network slices.

**Key Concepts**:

* States: Each user.
* Actions: Discrete power levels.
* Reward: Based on deviation from slice-specific SINR thresholds.
* ε-greedy strategy for balancing exploration and exploitation.

**Output**:

* Bar chart showing optimal power assigned per user after convergence.
* Q-table showing learned values guiding decisions.

**C. Quantum Key Generation and Secure Encryption (Qiskit)**

**Objective**: Secure communication using quantum-generated one-time pad keys.

**Key Concepts**:

* Hadamard gates for superposition-based bit generation.
* Basis selection and measurement on quantum circuits.
* Classical key reconciliation between sender (Alice) and receiver (Bob).
* XOR-based encryption and decryption using shared quantum key.

**Output**:

* Display of original, encrypted, and decrypted messages.
* Validates correctness of quantum-based key exchange and security.

**4. Challenges Addressed and Solutions**

| **Challenge** | **Solution** |
| --- | --- |
| BER degradation for weak users in NOMA | Quantum-inspired power prioritizes weak users |
| Need for adaptive multi-user power control | Q-learning optimizes power per user based on SINR |
| Wireless communication security | Quantum key distribution and one-time pad encryption |
| Fair spectrum sharing in dense networks | SINR-based slicing and targeted Q-learning reward functions |

4.3 Constraints,Alternatives or trade offs

**Constraints**

* **Hardware Limitations**: Current quantum computing resources (limited qubits and gates) constrain the scalability and complexity of the system. Simulations in Qiskit are the main method, as real-world quantum hardware isn’t fully capable for large-scale implementations.
* **Computation Power**: Q-learning requires significant computational resources, especially when the number of users increases, and may not converge quickly in large-scale systems.
* **Channel and SNR Issues**: Real-world noise, fading, and interference are challenging to model accurately in the project. Assumptions about ideal conditions may not apply in practical scenarios.

**Alternatives**

* **Power Allocation**: Classical methods like water-filling can replace quantum-inspired allocation, which is computationally efficient but less secure and optimal. Distributed Q-learning could reduce complexity over centralized control but may lead to suboptimal power distribution.
* **Key Generation**: Classical cryptography (RSA, AES) could be used instead of quantum key distribution (QKD), but it lacks the future-proof security offered by quantum encryption methods.
* **OMA vs. NOMA**: Orthogonal multiple access (OMA) methods (e.g., TDMA, FDMA) are simpler but less efficient than NOMA, which offers higher spectral efficiency at the cost of increased complexity.

**Trade-offs**

* **Quantum vs. Classical Encryption**: While quantum encryption methods like QKD provide superior security, they are resource-intensive and not scalable. Classical cryptography is faster but vulnerable to quantum threats.
* **Centralized vs. Distributed Q-Learning**: Centralized Q-learning offers better power allocation but is less scalable and requires more communication. Distributed Q-learning is more scalable but could be less efficient.
* **Simulation vs. Real-World Testing**: Simulation is cost-effective for development, but real-world deployment presents challenges and may yield different results due to hardware and environmental factors.

5. **Project Description: Quantum-based NOMA (Q-NOMA)**

The ever-increasing demand for high-speed, secure, and reliable wireless communication in next-generation networks has necessitated the exploration of innovative technologies. The Quantum-based Non-Orthogonal Multiple Access (Q-NOMA) system is a futuristic framework that merges advanced wireless access techniques with quantum cryptography and intelligent learning models. This project presents the development and simulation of a Q-NOMA system that integrates Quantum Key Distribution (QKD) and Q-learning-based power allocation to address the dual challenge of security and efficiency in future 6G wireless networks.

**Overview of NOMA**

Non-Orthogonal Multiple Access (NOMA) has emerged as a critical enabler for 5G and 6G wireless communications due to its ability to support multiple users simultaneously on the same frequency resources. Unlike Orthogonal Multiple Access (OMA), which divides time or frequency among users, NOMA utilizes power domain multiplexing. In NOMA, users with different channel conditions are assigned varying power levels, and the signal is decoded using Successive Interference Cancellation (SIC). This allows for higher spectral efficiency, lower latency, and increased connectivity.

However, a fundamental limitation of NOMA is power allocation. Improper allocation may lead to unfairness, increased interference, and reduced Quality of Service (QoS). Moreover, NOMA is still vulnerable to eavesdropping and classical cryptographic attacks, especially with the emergence of quantum computing.

**Quantum Key Distribution (QKD)**

To address security challenges, this project incorporates Quantum Key Distribution into the NOMA system. QKD leverages the principles of quantum mechanics—such as superposition and the no-cloning theorem—to enable secure key exchange between communicating parties. The BB84 protocol, developed by Bennett and Brassard, serves as the basis for the QKD implementation. In this system, quantum bits (qubits) are exchanged between two parties, Alice and Bob, using a quantum channel, and the resulting key is used for encrypting communication.

Integrating QKD with NOMA ensures theoretically unbreakable encryption, providing a robust security layer against both classical and quantum attacks. This feature is especially critical for sectors like national defense, finance, and healthcare, where communication integrity is paramount.

**Power Allocation via Q-learning**

For efficient spectrum utilization and optimal QoS in NOMA, dynamic and adaptive power allocation is essential. In this project, Q-learning—a model-free reinforcement learning algorithm—is employed to achieve intelligent power control. Q-learning enables the system to learn optimal power distribution policies through interaction with the environment.

The learning agent (i.e., the base station) observes the channel conditions and SINR of users, takes actions by adjusting power levels, receives feedback in the form of rewards (e.g., improved throughput, fairness), and updates its knowledge (Q-table). Over time, the system converges to an optimal strategy that balances power allocation to minimize Bit Error Rate (BER) and maximize throughput.

**Simulation Tools and Environment**

The implementation was carried out using:

* **Python**: The primary language for developing simulation logic, managing data structures, and plotting performance graphs.
* **Qiskit**: Used to simulate quantum circuits and implement the QKD protocol. Quantum gates like Hadamard and Pauli-X were used to create and manipulate qubits, simulating the secure key exchange process.
* **CLAQIQ Tools**: Leveraged for handling quantum-classical hybrid logic, simulation management, and post-processing of QKD results.

The simulation environment includes:

* Channel modeling for multi-user NOMA.
* Quantum communication simulation between Alice and Bob.
* Power allocation dynamics with Q-learning.
* Performance evaluation in terms of BER, SINR, and secure key generation.

**Key Contributions and Features**

1. **Security Enhancement**:
   * QKD integration ensures that encryption keys are secure against quantum attacks.
   * Real-time key generation and verification between sender and receiver enhance trust in communication.
2. **Spectral Efficiency**:
   * NOMA enables multiple users to share the same bandwidth with different power levels, improving spectral efficiency compared to traditional OMA.
3. **Adaptive Resource Management**:
   * Q-learning dynamically adjusts power allocation based on network conditions.
   * The learning model evolves with time, ensuring adaptability in changing environments.
4. **Low BER and High SINR**:
   * Simulation results show reduced BER and improved SINR due to intelligent power management and interference reduction.
5. **Scalability**:
   * The Q-NOMA model is designed to be scalable for large-scale 6G environments with heterogeneous devices.

**Use Cases and Applications**

* **Healthcare Systems**: Secure remote surgeries and medical data transmission.
* **Smart Cities**: Reliable and private communication between IoT devices.
* **Defense Communications**: Quantum-secure military-grade communication frameworks.
* **Banking & Finance**: Safe digital transaction frameworks for future financial systems.

**Challenges Encountered**

* **Integration Complexity**: Combining QKD and NOMA in a real-time simulation required synchronization of quantum and classical modules.
* **Computational Load**: Quantum simulation and Q-learning together required significant computational resources.
* **Reward Design**: Defining an effective reward function in Q-learning to balance security, SINR, and fairness was non-trivial.

**Results and Observations**

* Q-learning improved average throughput and SINR compared to static allocation methods.
* The QKD module successfully generated secure keys, maintaining low Quantum Bit Error Rates (QBER).
* BER decreased significantly when optimal power policies were learned and applied.
* Q-NOMA outperformed classical NOMA in both performance and security metrics.

**Future Enhancements**

* **Hardware Implementation**: Deploy QKD over real optical channels using quantum photonic chips.
* **Federated Learning**: Integrate decentralized ML for scalable and privacy-preserving power control.
* **Quantum Machine Learning**: Replace classical Q-learning with quantum reinforcement learning for improved decision speed.

**Conclusion**

The Quantum-based NOMA framework presents a transformative approach to next-generation wireless communication. By fusing the security of quantum key distribution with the efficiency of NOMA and the intelligence of Q-learning, the project creates a scalable, adaptive, and secure communication system. This hybrid approach directly addresses the challenges posed by 6G, including massive connectivity, real-time responsiveness, and quantum-resistant security. As the boundaries between quantum and classical systems blur, Q-NOMA represents a vital step toward the realization of future-proof communication infrastructures.

6. **Software Tools Used**

In the development of the quantum-based Non-Orthogonal Multiple Access (Q-NOMA) system, various software tools were leveraged to handle the complexity of the quantum communication and machine learning tasks. Two key software tools played pivotal roles in the design, implementation, and simulation of the system: **Python** and **Qiskit**.

**1. Python**

Python served as the primary programming language for the project, chosen for its flexibility, extensive libraries, and community support, making it highly suitable for developing complex systems. In the Q-NOMA system, Python was employed across multiple stages, from data handling and simulation to implementing advanced algorithms such as Q-learning for optimal power allocation.

* **Versatility**: Python’s versatility allowed it to be the backbone of the project, facilitating various tasks such as mathematical modeling, algorithm implementation, and data visualization. It provided an ideal environment for rapid prototyping and testing of different components of the Q-NOMA system.
* **Numerical Computations**: Libraries such as **NumPy** were utilized to handle the core mathematical operations in the system. NumPy, a powerful Python library for numerical computing, enabled efficient matrix operations, vector manipulations, and complex number handling—essential for implementing the mathematical models used in Q-NOMA and quantum key distribution (QKD). It allowed the simulation of communication channels, power allocation, and user signal processing within the system.
* **Machine Learning Integration**: A crucial aspect of the project was integrating **Q-learning**, a machine learning technique used to optimize power allocation in NOMA. Python provided an ideal platform for implementing reinforcement learning algorithms. The **TensorFlow** or **Keras** libraries, if needed, would allow for advanced deep learning techniques. However, for the current project scope, Python’s native support for implementing Q-learning algorithms with its easy-to-use structure and integration with NumPy made it a preferred tool for experimenting with adaptive power allocation.
* **Data Visualization**: Python also provided powerful visualization capabilities through libraries like **Matplotlib**. This allowed the team to visualize critical performance metrics such as signal-to-noise ratios, throughput, power allocation efficiency, and security key generation rates, among others. Matplotlib enabled the creation of detailed plots that were essential for analyzing the results, presenting the outcomes clearly, and drawing conclusions about the system’s performance.
* **Scalability**: Python’s ability to scale with large datasets and complex algorithms further made it ideal for simulating large-scale systems, including multiple users in a NOMA network. It helped simulate real-world conditions such as variable user demands, interference, and dynamic resource allocation scenarios. This scalability ensured that the framework could accommodate future expansions and improvements.

**2. Qiskit**

**Qiskit** is an open-source quantum computing framework developed by IBM, designed to help users develop quantum algorithms and simulate quantum operations. It provided the necessary tools to implement the quantum components of the Q-NOMA system, particularly Quantum Key Distribution (QKD), which is essential for ensuring secure communication in future wireless networks.

* **Quantum Operations**: Qiskit was used to implement the core quantum communication protocol for the Q-NOMA system. It allowed the team to simulate the quantum operations involved in QKD, which is crucial for secure key generation and encryption. Key quantum operations like **Hadamard gates**, **CNOT gates**, and **measurement** operations were built into quantum circuits within Qiskit to mimic real-world quantum communication protocols.
* **Quantum Circuits**: The framework provided an easy-to-use interface for designing and simulating quantum circuits. Quantum circuits were essential for simulating the interactions between the communicating parties (e.g., Alice and Bob in the QKD protocol). Qiskit enabled the construction of these circuits, including steps for quantum entanglement, key distribution, and measurement-based security operations.
* **Simulation & Hardware Execution**: One of the powerful features of Qiskit is its ability to simulate quantum operations both on local simulators and on actual quantum hardware (via IBM's quantum computers). This was particularly useful for testing and validating the quantum communication protocols. Although the project initially focused on simulator-based testing, the framework’s compatibility with real quantum hardware provided a pathway for future scalability and experimentation.
* **Security and Encryption**: At the heart of the system is the need for secure key distribution, a core advantage of QKD. By utilizing Qiskit’s quantum encryption tools, the project was able to simulate secure key exchange mechanisms that are theoretically resistant to eavesdropping. This secure key exchange forms the backbone of the encryption process for the NOMA system, enhancing the overall security of the network.
* **Integration with Classical Systems**: While Qiskit is primarily used for quantum computing, it also provides tools to interface with classical systems, which was essential for integrating the quantum key distribution process with NOMA's classical power allocation mechanisms. This capability made it possible to combine QKD’s security features with the traditional aspects of wireless communication protocols like NOMA, resulting in a hybrid system that leverages the strengths of both quantum and classical technologies.

**Conclusion**

The combination of Python and Qiskit provided the necessary foundation to develop the quantum-based NOMA (Q-NOMA) system. Python's flexibility and computational power, along with Qiskit's quantum-specific tools for secure communication, allowed the project to effectively explore and simulate a novel communication framework that addresses the demands of future wireless networks. These tools enabled the seamless integration of quantum security with adaptive resource management, showcasing the potential for a more efficient, secure, and scalable approach to next-generation communication systems.

6.Schedule and Milestones

**Dec 15 – Dec 30 (Literature Review & Project Finalization):**

* **Preeti Yadav**: Conducted a detailed literature review by analyzing relevant conference papers and online repositories, which helped refine the project scope.
* **Basil Syed**: Assisted with gathering information on QKD-based encryption protocols and their applications in cryptography.
* **Satyam Sinha**: Focused on reviewing the theoretical foundations of quantum communication, particularly the BB84 protocol, and started brainstorming ideas for the integration of NOMA in the project.

**Dec 31 – Jan 15 (QKD Protocols & Qiskit Exploration):**

* **Preeti Yadav**: Researched QKD protocols, specifically BB84, and started familiarizing herself with Qiskit and its capabilities.
* **Basil Syed**: Deepened knowledge on quantum cryptography and worked on the initial setup of Qiskit for encryption purposes.
* **Satyam Sinha**: Studied the application of QKD in real-world scenarios and contributed to understanding how Qiskit can be used for secure key generation.

**Jan 16 – Jan 31 (Development Environment Setup & QKD Implementation):**

* **Preeti Yadav**: Assisted in finalizing the project topic and outlined key objectives.
* **Basil Syed**: Set up the development environment and began the initial implementation of QKD-based key exchange using Qiskit and Python.
* **Satyam Sinha**: Assisted in the setup and worked on coding the initial parts of the QKD implementation, ensuring secure key generation through Qiskit.

**Feb 1 – Feb 15 (Optimization & Security Testing):**

* **Preeti Yadav**: Worked on optimizing project documentation and refining the scope of security protocols.
* **Basil Syed**: Focused on optimizing the QKD encryption and tested the security of the quantum key distribution.
* **Satyam Sinha**: Conducted tests to validate quantum key generation security and worked on refining the implementation for better performance.

**Feb 16 – Feb 29 (NOMA Integration & Security Refinements):**

* **Preeti Yadav**: Researched NOMA (Non-Orthogonal Multiple Access) techniques and analyzed potential security challenges in integrating it with QKD.
* **Basil Syed**: Began integrating NOMA with the existing QKD encryption framework.
* **Satyam Sinha**: Worked on refining the QKD encryption for multi-user access, addressing the potential challenges introduced by NOMA.

**Mar 1 – Mar 15 (Full QKD-NOMA Integration & Simulations):**

* **Preeti Yadav**: Assisted in the integration of QKD and NOMA, focusing on refining the architecture for multi-user key exchange.
* **Basil Syed**: Completed the integration of full QKD-NOMA protocols and began running simulations to assess system performance.
* **Satyam Sinha**: Led the simulation efforts, testing the security and efficiency of the system against potential attacks, and worked on adjusting the implementation for scalability.

**Mar 16 – Mar 31 (Optimization & Performance Enhancement):**

* **Preeti Yadav**: Worked on optimizing the documentation and preparing the final sections for the research paper.
* **Basil Syed**: Focused on optimizing NOMA performance and improving the robustness of the encryption against quantum and classical attacks.
* **Satyam Sinha**: Conducted performance tests to validate the system's robustness, ensuring secure key distribution and optimal performance under varying conditions.

**Apr 1 – Apr 15 (Finalization of Results & Documentation):**

* **Preeti Yadav**: Finalized the research presentation and completed the last touches on the documentation, including the project report.
* **Basil Syed**: Worked on refining the encryption model based on the final simulations and tests to ensure complete functionality.
* **Satyam Sinha**: Contributed to the final performance analysis, ensuring the research paper is aligned with the objectives and that all conclusions are backed by thorough testing.

**Apr 16 – Apr 20 (Final Review & Submission):**

* **Preeti Yadav**: Conducted the final review of the project report and presentation. Prepared for the project submission.
* **Basil Syed**: Refined the final encryption implementation and assisted with the review process to ensure all technical aspects were covered.
* **Satyam Sinha**: Finalized the project report and contributed to the final submission, ensuring everything met the project goals.

8.Results and Analysis

9.Conclusion

9.1 Obtained Results

9.2 Future Improvement work

9.3 Indivividual Contribution from team members

**Preeti Yadav – QKD Research & Documentation Lead**

* **Project Scoping & Literature Review**:  
  Researched over 20+ relevant IEEE conference papers, journals, and GitHub repositories to shape the direction of the project and integrate current trends in Quantum Key Distribution (QKD) and NOMA.
* **Technology Mapping**:  
  Mapped technical concepts from research papers to practical implementation using Qiskit and Python.
* **Documentation & Presentation**:  
  Created the complete project documentation including the final report, research paper draft, and multiple detailed presentations. Led the structuring of findings for clarity and publication-readiness.
* **Project Coordination**:  
  Coordinated task distribution, ensured timely progress, and maintained team communication,also assisted in integrating QKD with NOMA.

**Basil Syed Sadat – Encryption & Simulation Lead**

* **QKD Implementation**:  
  Developed and implemented QKD encryption protocols (BB84) using Qiskit and Python. Focused on the quantum circuit design and simulation of secure key generation.
* **Code Optimization & Debugging**:  
  Handled encryption-related debugging and code optimization for performance, ensuring minimal quantum bit error rate (QBER) and better simulation stability.
* **Security Validation**:  
  Conducted multiple test cases to validate the security and correctness of quantum key generation across various attack scenarios.
* **Final Integration Support**:  
  Assisted in integrating QKD with NOMA, including encoding and decoding layers.

**Satyam Sinha – NOMA & Enhancement Lead**

* **NOMA Integration**:  
  Developed and implemented the integration of QKD with Non-Orthogonal Multiple Access (NOMA) schemes, allowing secure multi-user communication.
* **Extended Qiskit Modules**:  
  Extended the existing Qiskit code with custom logic to support user multiplexing, Q-learning-based power allocation, and enhanced encryption layers.
* **Simulation & Performance Analysis**:  
  Ran simulations to evaluate the bit error rate (BER), security strength, and overall system throughput.
* **Innovation & Enhancement**:  
  Proposed and implemented a novel optimization approach combining QKD and machine learning-based power control for enhanced security and performance.

10.Social and Environmental impact

The integration of cutting-edge technologies like Quantum Key Distribution (QKD) and Non-Orthogonal Multiple Access (NOMA) into the communication networks of the future can have a transformative social impact. This project focuses on bridging the security gap in wireless communication by introducing quantum-level encryption while also improving connectivity and efficiency through NOMA. These advancements offer several potential social benefits.

**1. Enhanced Data Security**

Data security has become one of the most pressing concerns in modern society, especially in sensitive sectors such as healthcare, finance, and national defense. With the increasing amount of data being exchanged over the internet, the threat of cyber-attacks grows. Conventional encryption methods are gradually becoming susceptible to attacks, particularly as quantum computing technologies evolve, making traditional security measures inadequate. Quantum Key Distribution (QKD) offers a solution by providing theoretically unbreakable encryption based on the principles of quantum mechanics. This ensures that sensitive information—such as patient records in healthcare systems, financial transactions, or military communications—remains secure from eavesdropping. By integrating QKD into next-generation wireless networks, this project significantly enhances communication security, providing an essential layer of protection against future cyber threats.

**2. Democratization of Secure Communication**

As the demand for connectivity grows, one of the major challenges for future networks like 6G will be providing universal access to high-speed, secure communication. NOMA, by enabling multiple users to simultaneously access the same frequency resources, supports massive device connectivity. This feature can play a crucial role in providing secure, high-quality communication to underserved populations, particularly in rural or remote areas that typically have limited access to fast and secure internet services. NOMA's ability to allocate resources dynamically based on user needs makes it an ideal candidate for expanding the reach of 6G networks to a wider audience. The integration of QKD in such networks ensures that even remote and underserved regions can access the internet securely, enhancing digital inclusion and equity across socio-economic strata.

**3. Boost to Research & Education**

The introduction of new technologies into communication systems sparks interest and provides opportunities for further research and development. This project promotes awareness and skill-building in emerging fields such as quantum communication, machine learning, and 6G technologies. As such, it encourages academic institutions and research organizations to explore these new frontiers, opening avenues for innovation in communication, cryptography, and resource management. The knowledge gained through this work can inspire new generations of researchers and engineers, who will further develop and refine these technologies. The project can also be a valuable learning tool for students and researchers, providing them with a deeper understanding of quantum mechanics, machine learning techniques like Q-learning, and their applications in modern communication systems. This will further enhance the knowledge pool in the academia and industries, leading to more refined and robust solutions.

**4. Trust in Future Networks**

As we move toward the era of 6G, trust in the security of communication networks will be paramount. Public skepticism about the security of modern communication systems has grown due to frequent cyber-attacks and data breaches. The implementation of QKD ensures that the most sensitive data remains unbreachable by malicious entities. By addressing these security concerns head-on, this project strengthens public trust in future communication networks, which will be fundamental for widespread adoption. The integration of quantum-secured communication with NOMA’s enhanced connectivity provides not only secure access to information but also the assurance that the privacy of individuals and organizations will be protected. As a result, this will instill greater confidence in the utilization of next-generation wireless systems, ensuring that the public and private sectors alike feel comfortable using and relying on these advanced communication systems.

**Environmental Impact**

In the context of future wireless networks, it is crucial to consider the environmental implications of the technologies being developed. While 5G and 6G technologies promise tremendous benefits in terms of connectivity and service quality, they also raise concerns about energy consumption, e-waste, and the sustainability of network infrastructure. This project’s focus on improving communication system efficiency using NOMA and QKD can have significant positive effects on the environment.

**1. Energy Efficiency**

One of the major advantages of NOMA is its ability to improve spectral efficiency by allowing multiple users to share the same frequency resources. In traditional multiple access systems, such as Orthogonal Multiple Access (OMA), each user is assigned distinct frequency bands, which leads to inefficient spectrum usage and increased energy consumption. NOMA, by allowing simultaneous access to the same frequency band, significantly reduces the need for additional bandwidth and power, resulting in lower overall energy consumption for network operators. This energy efficiency is particularly important for large-scale 6G deployments, which will involve massive numbers of devices and require large amounts of energy to support the growing demand for high-speed, low-latency communication. By leveraging NOMA, the project reduces the environmental footprint of the wireless network, contributing to sustainability goals.

**2. Reduced Hardware Footprint**

Another notable environmental benefit of this project lies in its potential to reduce the hardware footprint associated with traditional communication systems. Modern cryptographic systems, which rely on complex algorithms and hardware accelerators, can generate significant e-waste. In contrast, the implementation of QKD with quantum-secured communication infrastructure, especially when integrated with photonic technologies, offers a more compact and energy-efficient solution. Quantum communication systems can reduce the need for large-scale, energy-consuming hardware components, thus mitigating the environmental impact of cryptographic processes. As quantum technologies become more advanced, their ability to replace traditional security infrastructure could lead to a reduction in electronic waste, supporting global efforts toward minimizing e-waste and promoting sustainable technological practices.

**3. Sustainable Communication Systems**

The development of more efficient, secure, and intelligent communication systems is essential to building sustainable and environmentally friendly infrastructure. By integrating quantum encryption with NOMA and machine learning-based resource management (Q-learning), this project contributes to the creation of systems that optimize both power usage and network performance. Moreover, the intelligent allocation of resources ensures that the system adapts to varying user demands and environmental conditions, reducing the need for excessive infrastructure expansion. This efficiency helps reduce the carbon footprint associated with the operation of wireless networks. Additionally, as the project supports more devices on the same network, it can help reduce the overall environmental impact of the global communication infrastructure by minimizing the need for new hardware and network expansion, thus lowering resource consumption and environmental degradation.

**Conclusion**

The integration of QKD, NOMA, and machine learning-based resource management not only has profound implications for enhancing the security, efficiency, and scalability of wireless communication systems but also holds significant promise for contributing positively to both social and environmental outcomes. By improving the security and accessibility of communication systems, especially for underserved populations, this project fosters digital inclusion, enhances global communication infrastructure, and addresses key societal concerns about data security. On the environmental front, the project supports the creation of more energy-efficient, sustainable, and compact communication technologies, helping to minimize the environmental impact of future wireless networks. These combined social and environmental benefits make this project a critical step toward the realization of secure, efficient, and sustainable 6G networks.

11. Cost Analysis

**11.Cost Analysis Summary**

* **Total Cost Incurred: ₹0**

This project was completed at **zero financial cost**, thanks to the extensive academic resources and infrastructure provided by **VIT**:

* **Software Tools** such as **Qiskit, Python, and Jupyter Notebooks** were used—all of which are open-source and freely available.
* **IBM Quantum Experience** was accessed via the **free tier**, allowing simulation of quantum circuits without cost.
* **Research papers** and resources were accessed through **VIT's institutional subscriptions**, eliminating the need for paid access to journals like IEEE or Springer.
* **Computing infrastructure** including laptops/desktops, internet, and cloud access were provided or already available through VIT's labs or personal setups.
* **Documentation tools** and presentation software were freely available via institutional or open-source platforms.

12.Project Outcome Publication/Patent

13.References

Top of Form

Bottom of Form