International Journal of Innovative Trends in Engineering Science and Technology
A Peer-Reviewed International Research Journal (IJITEST)
www.ijitest.org | E-ISSN: XXXX-XXXX

Quantum-Enabled Security Framework for 6G Communications Based on QKD-OFDM Integration

[1]Swapna Priya Chikatla,[2] Thorlapati Gulshan Sri Babu, [3]S Naga Mallik Raj
[1]Associate Professor,[2]Student,[3] Associate Professor
[1,3]Department of CSE, Vignan's Institute of Information Technology (A), Visakhapatnam, India.
[2]Department of CIVIL, Vignan's Institute of Information Technology (A), Visakhapatnam, India.
[1]swapnachsp@gmail.com, [2]gulshansribabu@gmail.com,[3]mallikblue@gmail.com

Abstract –Ultra-high data rates, efficient use of the terahertz spectrum, and significant connectivity are anticipated as Sixth Generation (6G) wireless communication emerges. However, traditional cryptographic algorithms like RSA and Elliptic Curve Cryptography, which are currently employed in wireless networks, are seriously threatened by the quick development of quantum computing. Future 6G systems must incorporate quantum-safe security measures to allay this worry. The incorporation of Quantum Key Distribution (QKD) into the physical layer of 6G communication networks is investigated in this paper. To facilitate secure key exchange and identify eavesdropping, QKD makes use of quantum concepts like superposition, entanglement, and the no-cloning theorem. Realistic wireless channel conditions are used to analyze the BB84 and E91 protocols. A proposed 6G channel model incorporates Nakagami-m fading, additive white Gaussian noise, and path loss. Detector noise and channel disturbances are taken into account when modeling the Quantum Bit Error Rate (QBER). In an OFDM framework, MATLAB simulations evaluate the secure key rate performance with respect to signal-to-noise ratio, transmission distance, and noise probability. The findings highlight the potential of QKD for secure 6G communications by showing that secure key generation is possible when the QBER stays below the theoretical threshold. Index Terms –5G and 6G wireless communications, Quantum Key Distribution, Fading Channels.

***Index Terms*— Cryptographic algorithms, Quantum Key Distribution, quantum computing, Fading Channels**

I. INTRODUCTION

Global connectivity has changed due to the development of wireless communication, which has progressed from simple analog systems to sophisticated broadband networks. Future networks are anticipated to offer exceptionally high data rates, lower latency, intelligent network management, and the capacity to connect a large number of devices as research advances toward sixth-generation (6G) communication. New applications like autonomous systems, remote medical services, immersive virtual environments, and smart infrastructure will be made possible by these features.

However, despite these advantages, there are significant security risks associated with the growing reliance on wireless technologies. High-frequency spectrum bands, large antenna arrays, intelligent surfaces, and distributed edge intelligence are anticipated to be utilized by the upcoming 6G systems. These advancements improve network performance, but they may also make communication systems vulnerable to sophisticated cyber-attacks, especially in vital industries like national security, healthcare, and transportation.

The majority of current security measures are based on conventional public-key cryptography methods, which depend on the difficulty of resolving difficult mathematical puzzles. However, the dependability of these security measures is seriously threatened by the continuous developments in quantum computing.

Strong quantum algorithms could solve these problems far more quickly than traditional computers, jeopardizing communication integrity and data confidentiality in next-generation networks. By utilizing the fundamental ideas of quantum mechanics rather than relying on computational complexity, quantum cryptography provides a workable substitute. By monitoring changes in error characteristics, quantum key distribution facilitates the safe creation of shared secret keys and allows authorized users to identify attempts at interception [1].

Quantum Key Distribution (QKD) and efficient modulation techniques [2], such as Orthogonal Frequency Division Multiplexing, make it possible to apply these ideas in real-world wireless settings, guaranteeing safe and effective data transfer. By simulating realistic channel conditions and evaluating secure key generation under various signal and noise levels, this study investigates the potential of quantum-based security measures for upcoming 6G systems. This project's goal is to support the development of resilient communication infrastructures that can withstand the novel difficulties presented by the quantum era.

This paper is structured as follows. Section II presents the system model and fundamentals of Quantum Key Distribution integrated with OFDM for 6G communication. Section III discusses performance analysis and simulation results, followed by conclusions and future research directions in Section IV.

II. RELATED WORK

All the related works that have been done by other researchers that are related to the current research problem should be summarized in this section [3] Notwithstanding the encouraging theoretical results, the majority of practical applications are confined to optical or partially integrated optical-wireless settings. Completely wireless quantum communication systems continue to be predominantly in the experimental phase.

Table 1: Comparison of existing systems with wireless QKD [4-16]

Feature	**Classical Physical Layer Security**	**Fiber-Based QKD**	**Free-Space / Satellite QKD**	**Wireless QKD (Emerging Research)**
Medium	RF / mmWave / THz	Optical fiber	Free-space optical (space ↔ ground)	Wireless RF/THz
Distance	Not applicable	Up to ~400 km	Thousands of km	Limited/experimental
Security Basis	Classical information theory	Quantum mechanics	Quantum mechanics	Quantum mechanics
Key Rate Performance	Not applicable	Moderate	Low (free-space loss)	Theoretical/limited data
Commercial Products	Yes	Yes	No (demo systems only)	No
Channel Impairments	Noise, fading	Fiber loss, dispersion	Atmospheric turbulence	Noise, fading, mobility
Eavesdropping Detection	No	Yes	Yes	Yes
Integration with Data Systems	Native	Yes	Hybrid optical-wireless	Under research
Examples	Artificial noise, beam-forming	SECOQC, Clavis, Toshiba QKD systems	Micius satellite QKD	Experimental RF/THz proposals

Quantum Key Distribution (QKD) has progressed from theoretical ideas to practical applications over the last two decades. Fiber-based QKD systems have successfully shown secure key exchanges by transmitting quantum states via optical cables, achieving extensive transmission distances under controlled environments. Moreover, several metropolitan quantum communication networks have illustrated the practicality of multi-node secure connectivity using the current fiber infrastructure. Free-space and satellite-based QKD experiments have further expanded the range of quantum-secure communication. Quantum signals sent between ground stations and space platforms have allowed for long-distance key sharing, overcoming the limitations of fiber attenuation. However, challenges such as atmospheric turbulence, beam alignment, weather sensitivity, and signal attenuation still pose risks to system reliability and key generation efficacy.

Recent studies have concentrated on hybrid quantum–classical communication systems in which Quantum Key Distribution (QKD) [17-19] produces secret keys that are subsequently utilized for the encryption of classical data transmissions.

The introduction of wireless QKD presents further challenges, such as multipath fading, path loss, interference, mobility effects, and the complexity of synchronization. These factors can have a substantial impact on the Quantum Bit Error Rate and the performance of secure key rates. Consequently, the integration of QKD with contemporary wireless technologies, including Orthogonal Frequency Division Multiplexing, massive MIMO, and terahertz communication, represents a significant avenue for research. Despite encouraging theoretical results, the majority of practical implementations are still confined to optical or partially integrated optical-wireless settings. Fully wireless quantum communication systems remain predominantly in the experimental phase.

III. PROPOSED METHODOLOGY

The suggested framework incorporates principles of quantum communication into Massive MIMO-OFDM by substituting traditional bit representation with qubit-based processing, thereby enhancing reliability and spectral efficiency[18]

Quantum-assisted channel estimation and error correction techniques are utilized to enhance BER and SNR performance under fading wireless conditions. MATLAB-based simulations are carried out to compare the efficiency of the qubit-driven architecture with conventional binary MIMO-OFDM systems.

3.1 Quantum Bit Representation

In QKD, classical bits are encoded into quantum states.
A qubit is represented as:

$$|\psi\rangle = \alpha|0\rangle+\beta|1\rangle \tag{1}$$

where

$$|\alpha|^2+|\beta|^2=1 \tag{2}$$

In BB84 protocol, two bases are used:
Rectilinear basis: $|0\rangle$, $|1\rangle$
Diagonal basis:

$$|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \qquad |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{3}$$

Each transmitted qubit randomly selects a basis.

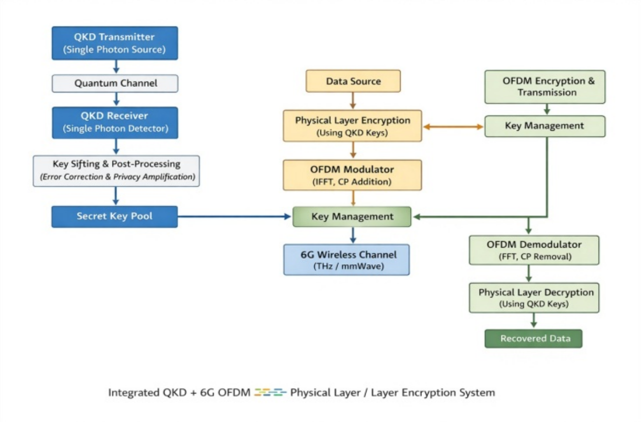

Figure 1: Block diagram of Proposed System

3.2. Quantum Channel Model

The quantum channel is affected by noise and loss. Let, η is the channel transmittance, p_d is dark count probability and $p_e$is the intrinsic error probability[19].
Therefore, the probability of successful photon detection is:

$$p_{\text{det}} = \eta + p_d \tag{4}$$

The Quantum Bit Error Rate (QBER) is defined as:

$$Q = \frac{N_{error}}{N_{total}} \tag{5}$$

Under noisy conditions:

$$Q = \frac{p_e\eta + \frac{p_d}{2}}{\eta + p_d} \tag{6}$$

If Q exceeds threshold Q_{th}, key is discarded.

3.3 Secure Key Rate Model

The asymptotic secure key rate for BB84 is

$$R = q \cdot P_{det}[1 - 2H_2(Q)] \tag{7}$$

where

$$q = \frac{1}{2} \text{ (basis matching probability)}$$

$$H_2(Q) \text{ = binary entropy function}$$

Binary entropy is:

$$H_2(Q) = -Qlog_2 Q - (1-Q)log_2(1-Q) \tag{8}$$

Thus:

$$R = \frac{1}{2}(\eta + p_d)[1 - 2H_2(Q)] \tag{9}$$

Secure key rate decreases as Q increases.

3.4 Distance-Dependent Channel Loss

In wireless 6G, path loss follows:

$$PL(d) = PL_0 + 10n\log_{10}\left(\frac{d}{d_0}\right) \tag{10}$$

Where,
$d$is the transmission distance, $n$is path loss exponent and $PL_0$is the reference path loss.
Channel transmittance can be expressed by

$$\eta(d) = 10^{-PL(d)/10} \tag{11}$$

ThusQBER becomes distance-dependent is related to

$$Q(d) = \frac{p_e\eta(d) + \frac{pd}{2}}{\eta(d) + p_d} \tag{12}$$

Key rate as function of distance can be expressed by

$$R(d) = \frac{1}{2}(\eta(d) + p_d)[1 - 2H_2(Q(d))] \tag{13}$$

3.5 AWGN Channel Model

The classical OFDM transmission over wireless channel:

$$y(t) = x(t) + n(t) \tag{14}$$

where
$x(t)$ is transmitted signal and $n(t) \sim \mathcal{N}(0, N_0)$
The Signal-to-Noise Ratio (SNR) of the AWGN Channel is

$$SNR = \frac{P_s}{N_0 B} \tag{15}$$

Noise increases error probability, impacting QBER indirectly.

3.6 Nakagami-m Fading Model

The modeling of the 6G fading channel under Nakagami Fading can be expressed by

$$f(r) = \frac{2m^m r^{2m-1}}{\Gamma(m)\Omega^m} exp(-\frac{mr^2}{\Omega}) \tag{16}$$

where

m fading parameter and Ω is the $E[r^2]$
Instantaneous SNR:

$$\gamma = r^2 \frac{P_s}{N_0} \tag{17}$$

Average key rate under fading:

$$R_{avg} = \int_0^\infty R(\gamma) f(\gamma) d\gamma \tag{18}$$

3.7 E91 Protocol Key Rate

For E91:

$$R_{E91} = P_{pair}[1 - H_2(Q) - H_2(Q_e)] \tag{19}$$

Where
The P_{pair} is the entangled pair generation probability and $Q_e$is the Eve's information. The Bell parameter can expressed by

$$S = E(a,b) + E(a,b') + E(a',b) - E(a',b') \tag{20}$$

If the absolute value of parameter **S** is greater than 2, it indicates violation of Bell's inequality, which confirms the presence of quantum entanglement and non-classical correlations.

3.8 OFDM System Model

Let the N is Number of subcarriers, Input symbol vector:

$$X = [X_0, X_1, ..., X_{N-1}] \tag{21}$$

Time domain OFDM signal:

$$x(n) = \frac{1}{N}\sum_{k=0}^{N-1} X_k e^{j2\pi kn/N} \tag{22}$$

After channel:

$$Y_k = H_k X_k + W_k \tag{23}$$

Encrypted symbol:

$$X_k^{enc} = X_k \oplus K_k \tag{24}$$

where K_k from QKD.

Total secure throughput can be expressed by

$$T_{secure} = R \cdot R_{OFDM} \tag{25}$$

where

$$R_{OFDM} = B\log_2(1+SNR)$$

Therefore

$$T_{secure}(d, SNR) = \frac{1}{2}(\eta(d) + pd)[1 - 2H_2(Q(d))] \cdot B\log_2(1+SNR) \tag{26}$$

The Error probability E_b and the noise variance σ^2 is related to $SNR = E_b/\sigma^2$, itcan also be written by

$$P_e = Q\left(\sqrt{2SNR}\right) \tag{27}$$

Where the Q-function can expressed by

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-t^2/2} dt \tag{28}$$

Thus

$$R(\sigma^2) = \frac{1}{2}(\eta + p_d)[1 - 2H_2(Q(\sigma^2))] \tag{29}$$

3.9 Security Condition

Secure key exists if: $R > 0$ which implies to

$$H_2(Q) < 0.5 \tag{30}$$

Threshold QBER:

$$Q_{max} \approx 0.11 \tag{31}$$

If $Q > 11\%$ the Key discarded.

However, the secure performance depends on

$$R(d, SNR, \sigma^2, m) \tag{32}$$

The system model assumes an ideal single-photon source and perfect synchronization between transmitter and receiver to simplify QKD performance analysis in a 6G wireless environment [20-24]. The public classical channel used for reconciliation and error correction is considered authenticated, allowing monitoring by an eavesdropper but preventing message modification. The adversary is assumed to possess unlimited computational capability, including quantum resources, yet remains constrained by fundamental quantum mechanical laws such as the no-cloning principle and measurement disturbance. These assumptions enable evaluation of unconditional security based on physical principles under controlled system conditions.

IV. RESULTS AND DISCUSSIONS

A comparative performance analysis of quantum key distribution (QKD) protocols in the presence of fading and eavesdropping shows how entanglement-based techniques improve the robustness of future wireless networks. In dynamic wireless environments, the BB84 protocol, which is renowned for its dependable and simple secure key generation, exhibits a more notable performance decline. In contrast, stronger quantum correlations are maintained by the E91 protocol, which results in lower error rates and higher secure key rates. Therefore, entanglement-based QKD is more appropriate for mobility-focused 6G settings that deal with fading and interference. Therefore, BB84 is still relevant for existing infrastructures even though E91 offers more promise for scalable wireless quantum security in the future.

For the BB84 and E91 protocols, Figure 2 shows how the secure key rate varies as the noise probability rises. Both protocols show a declining trend, indicating that the ability to produce secure quantum keys is reduced by an increase in channel noise. At low to moderate noise levels, the E91 protocol consistently achieves a significantly higher key rate than BB84, demonstrating superior robustness. In comparison to E91, BB84's performance drastically deteriorates and approaches a zero secure key rate at lower noise levels. Due to an excessive number of errors, both protocols are unable to produce secure keys in high noise environments.

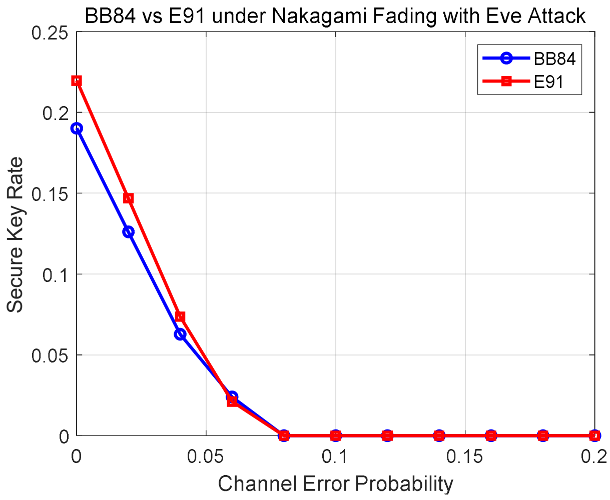

Figure 2: Comparison of BB84 vs E91 under Nakagami fading with Eve Attack

The operational viability of the BB84 and E91 quantum protocols across different levels of channel interference is evaluated in the related Figure 3. E91 consistently upholds a higher secure key rate throughout the range, despite both protocols experiencing a non-linear reduction in key generation efficiency as environmental noise intensifies.

According to the data, E91 has a higher noise threshold and continues to function at error levels where BB84 is completely insecure. For long-distance or high-interference quantum communication, entanglement-based systems such as E91 seem to be more robust. The crucial trade-off between protocol complexity and the capacity to maintain secure links in realistic, noisy environments is highlighted by this comparison.

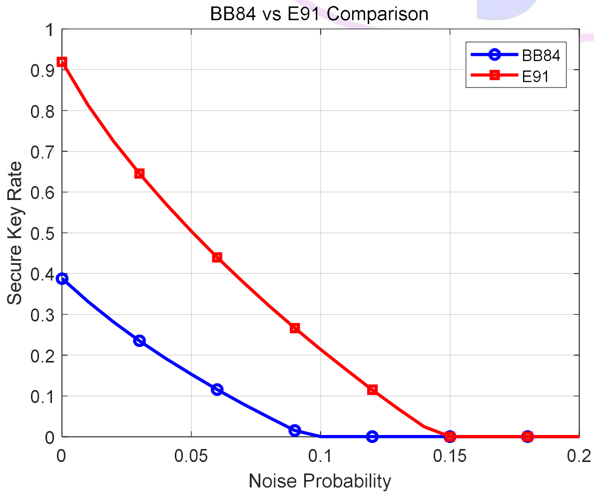

Figure 3: Comparison of BB84 vs E91 under Noise Probability

The durability of the BB84 and E91 protocols in the presence of Nakagami-m distributed noise is depicted in Figure 4. The results reveal that the E91 protocol achieves a considerably higher secure key rate across all tested noise probabilities when using a logarithmic scale. The entanglement-based E91 protocol is effective up to a threshold of 15%, whereas the BB84 protocol completely fails in key generation at around 10% noise levels.

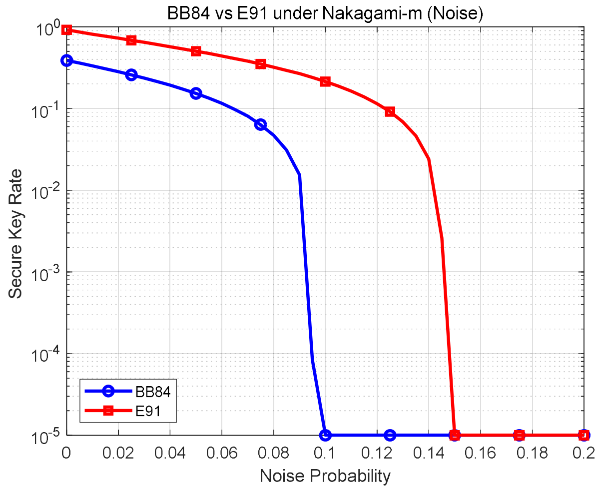

Figure 4: Noise Comparison of BB84 vs E91 under Nakagami-m fading

This illustration underscores the sensitivity of quantum channels to fading and external interference. In conclusion, the E91 protocol is shown to be more robust, providing a more trustworthy framework for secure communication in noisy conditions. The steep vertical drops indicate the specific limits where error correction can no longer address channel disturbances.

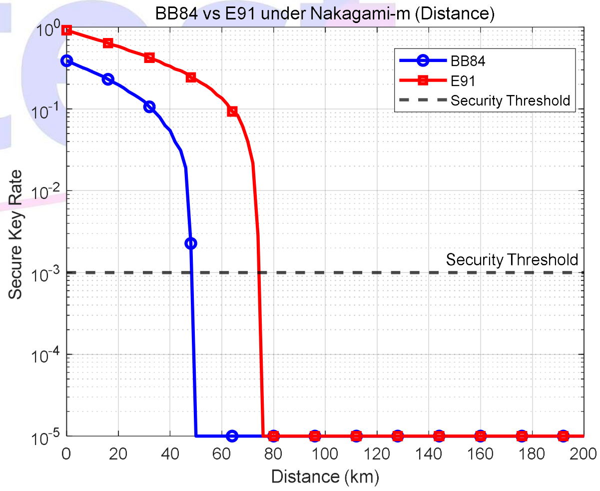

Figure 5: Distance Comparison of BB84 vs E91 under Nakagami-m fading

The impact of transmission distance on the BB84 and E91 protocols' secret key generation capacity under Nakagami-m fading conditions is shown in Figure 5.

There is a noticeable performance difference between BB84 and the E91 protocol, which maintains a viable key rate over a much larger geographic area. While the BB84 protocol fails to meet the minimum security threshold shortly after exceeding 45 kilometers, the E91 protocol's operational range approaches 75 kilometers. This extension shows how entanglement-based systems are more resilient to signal degradation and fading that happen with longer fiber or free-space links.

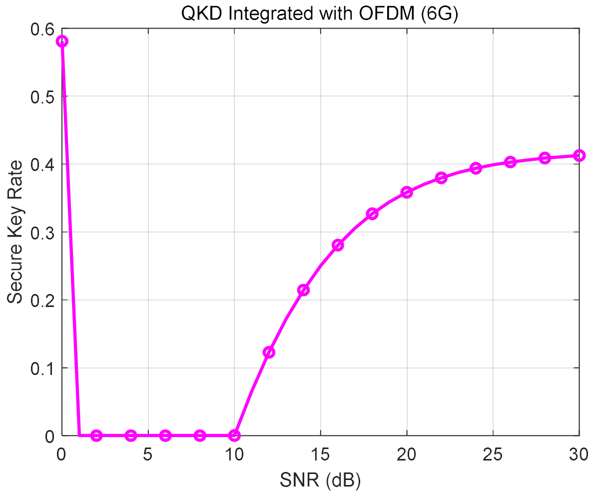

Figure 6: Efficiency of a QKD-OFDM integrated framework

The effectiveness of operations within a QKD-OFDM integrated framework designed for future 6G communication standards is evaluated in Figure 6. At lower signal-to-noise ratios, particularly in the range of 1 to 10 dB, the generation of secure keys is completely obstructed, indicating a distinct non-linear correlation.

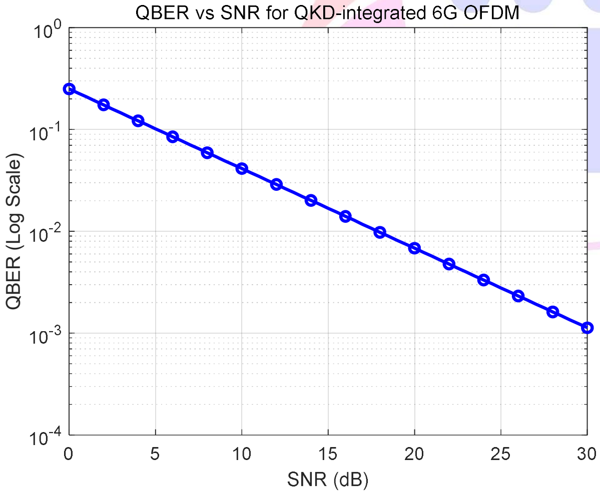

Figure 7: Error performance of a QKD integrated within a 6G OFDM

It is only when the signal strength surpasses the 10 dB mark that performance begins to improve, showing a consistent upward trajectory as channel conditions enhance. This pattern underscores the critical necessity of preserving high signal integrity in multi-carrier OFDM systems to ensure the feasibility of quantum security.

The error performance of a quantum key distribution system integrated within a 6G OFDM framework is illustrated in Figure 7.

The Quantum Bit Error Rate steadily decreases as the Signal-to-Noise Ratio increases from 0 to 30 dB. The diagram shows how the system can use a logarithmic scale to achieve high-precision transmissions at higher signal levels. According to the results, an SNR of more than 20 dB is typically required in this specific configuration in order to maintain the QBER below the critical threshold of 1%. These results are essential for determining how much power future wireless networks will need to ensure quantum security. This linear relationship shows that improving the quality of classical signals greatly increases the reliability of the core quantum cryptography process.

Figure 7 shows the error performance of a quantum key distribution system integrated into a 6G OFDM framework. The Quantum Bit Error Rate steadily decreases as the Signal-to-Noise Ratio increases from 0 to 30 dB. This example highlights how the system can use a logarithmic scale to achieve high-precision transmissions at higher signal levels. According to the data, an SNR of more than 20 dB is typically required in this specific configuration in order to maintain the QBER below the critical threshold of 1%. These results are essential for determining how much power future wireless networks will need to ensure quantum security. This linear trend shows that improving the integrity of classical signals greatly increases the reliability of the core quantum cryptography process.

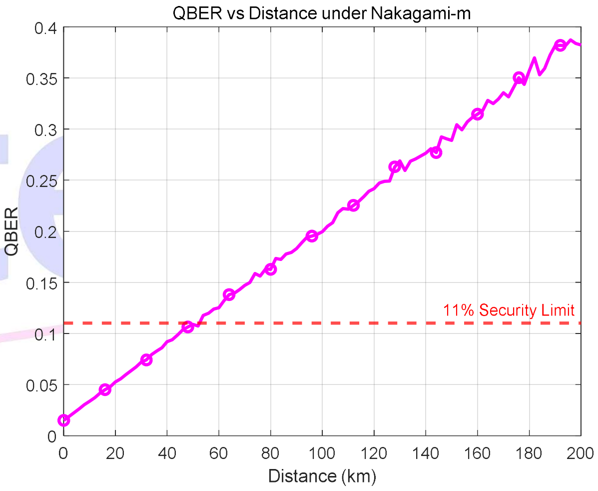

Figure 8:Impact of transmission distance on the QBER within a Nakagami-m fading

Figure 8 examines how transmission distance affects the Quantum Bit Error Rate in a Nakagami-m fading environment. At a distance of 200 kilometers, the QBER finally reaches 0.38, demonstrating a definite relationship between greater error rates and greater distance. The 11% security threshold, which represents the maximum permitted error for preserving confidentiality, is indicated by a horizontal reference line. The findings show that the security integrity of the system is maintained for roughly 50 kilometers. The quantum channel's resistance to possible intercept-resend attacks is compromised by the high error rates beyond this critical threshold. Determining the maximum range of unamplified quantum communication links in 6G systems requires these insights.

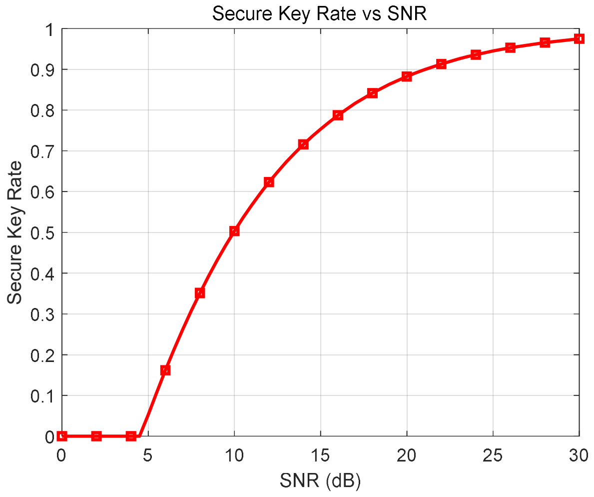

Figure 9: Performance thresholds of quantum key distribution within a 6G OFDM

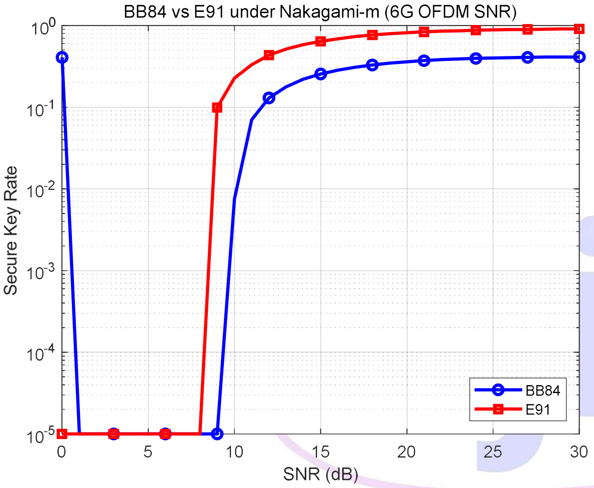

Figure 10: Performance thresholds of quantum key distribution within a 6G OFDM under Proposed Protocols

Figures 9 and 10 examine the performance thresholds of quantum key distribution within a 6G OFDM framework. The data indicates that secure key generation necessitates a minimum signal-to-noise ratio; notably, the E91 protocol requires a lower activation threshold compared to BB84. As the quality of the signal improves, E91 consistently shows a higher key rate on a logarithmic scale, achieving nearly ten times the efficiency of BB84. The entanglement-based E91 system reaches an almost optimal throughput of 1.0, whereas BB84 caps at a considerably lower capacity, even though both protocols gain from increased SNR. These findings underscore that E91 is better suited for high-speed 6G applications where optimizing secret key bitrate is essential. This analysis establishes a clear benchmark for choosing protocols based on the anticipated signal integrity of a wireless quantum channel.

IV. CONCLUSION

With an emphasis on noise, Nakagami-m fading, and transmission distance, this study examines the operational limits of the BB84 and E91 protocols under practical 6G channel conditions. The findings demonstrate that signal integrity has a major impact on the Secure Key Rate (SKR), which rises with SNR but falls precipitously as noise and distance increase. The 11% QBER level is acknowledged as a critical security threshold, above which secure communication becomes physically impossible. Data comparisons consistently show that the E91 protocol performs better than BB84, offering a 50% longer operational range and improved noise tolerance. Additionally, the analysis of Nakagami-m fading shows how a secure link may prematurely terminate due to stochastic signal variations. The resilience needed for high-interference wireless environments is effectively provided by E91's entanglement-based design. Therefore, strong fading mitigation and precise SNR management are essential for the effective integration of QKD into 6G architectures. These findings provide a thorough framework for choosing robust protocols to safeguard quantum networks of the future.

REFERENCES

[1] Termos*et al.*, “Quantum Authentication Evolution: Novel Approaches for Securing QKD,” *Entropy*, 2024.

[2] Termos*et al.*, “Quantum Authentication Evolution: Novel Approaches for Securing QKD,” *Entropy*, 2024.

[3] Y. Wang, “Research on 6G Communication Architecture Based on Quantum Key Encryption,” *Applied and Computational Engineering*, 2025.

[4] Y. Liang, “Integration of QKD in 6G Passive WDM Optical Fronthaul Architecture,” *Applied and Computational Engineering*, 2025.

[5] Hafeez *et al.*, “Quantum-Secured Routing in Drone Communication for 6G Mobility,” *Scientific Reports*, 2026.

[6] B. M. Kamil, “Enhancing 6G Network Security with Quantum Key Distribution,” *Al-Esraa University College Journal of Engineering Sciences*, 2025.

[7] V. Nair, “Exploring QKD Protocols for Secure Communication,” *Journal of Recent Trends in Computer Science and Engineering*, 2025.

[8] Balaji *et al.*, “AI-Driven Quantum-Secured 6G THz Networks,” *Scientific Reports*, 2025.

[9] A. C. Demeke, “Systematic Review: QKD for 6G Security,” 2026.

[10] M. A. Akbar, “6G Secure Quantum Communication Success Probability, Springer, 2024.

[11] M. A. Akbar *et al.*, “Role of Quantum Computing in 6G Technology,”*Information and Software Technology*, 2024.

[12] Behera *et al.*, “QNN-QRL: Quantum Neural Networks for QKD,” *arXiv preprint arXiv:2501.18188*, 2025.

[13] Ogrodnik*et al.*, “High-Dimensional QKD with Resource-EfficientDetection,” *arXiv preprint arXiv:2412.16782*, 2024.

[14] Brazaola-Vicario *et al.*, “High-Fidelity COW QKD Framework for 6G,” *arXiv preprint arXiv:2501.12043*, 2025.

[15] Zeydan*et al.*, “Quantum Technologies for Beyond 5G and 6G,” *arXiv preprint arXiv:2504.17133*, 2025.

[16] M. Goy *et al.*, “Ad-hoc Hybrid QKD Metropolitan Network,” *arXiv preprint arXiv:2412.07473*, 2024.

[17] ITU-T Recommendation Y.3800, “Overview on Networks Supporting Quantum Key Distribution,” International Telecommunication Union, 2019.

[18] 6GNet, “Post-Quantum 6G Framework Tutorials,” 6GNet Tutorial Series, 2025.

[19] Springer, “Quantum Network Applications in 6G Paradigm,” Springer Publications, 2025.

[20] Quantum Experiments at Space Scale (QUESS), “Global Quantum Key Distribution Experiments,” Research Reports.

[21] European Space Agency, “Eagle-1 Satellite Project: Future In-Orbit QKD Demonstration,” Project Documentation.

[22] *Financial Times*, “Secure Quantum Messages Sent over Telecom Network,” Technology Report.

[23] IJARASEM, “Quantum Cryptography for Securing Wireless Communication in 6G Networks,” *International Journal*, 2025.

[24] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, 1984.

Funding Declaration

The authors declare that no funds, grants, or other forms of financial support were received from any organization or institution for the conduct of this research.