Inform : Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi
Vol.10 No.2 July 2025, P-ISSN : 2502-3470, E-ISSN : 2581-0367

Quantum-Assisted Architectures for 6G and IoT: A Framework for Secure and Efficient Wireless Networks

Hewa Majeed Zangana[1], Amira Bibo Sallow[2], Firas Mahmood Mustafa[3]

[1,2]*IT Department, Duhok Technical College, Duhok Polytechnic University, Duhok, Iraq*

[3]*Chemical Engineering Department, Technical College of Engineering, Duhok Polytechnic University, Duhok, Iraq*

[1] hewa.zangana@dpu.edu.krd (*)

[2,3][amira.bibo, firas.mahmoud]@dpu.edu.krd

Received: 2025-06-03; Accepted: 2025-07-01; Published: 2025-07-14

Abstract— The convergence of Sixth-Generation (6G) wireless networks and the Internet of Things (IoT) demands unprecedented levels of performance, scalability, and security. Traditional architectures are increasingly inadequate in addressing the computational and security challenges posed by massive IoT connectivity, ultra-low latency, and high data throughput. This paper proposes a novel quantum-assisted architecture that integrates quantum computing and quantum communication principles to enhance the efficiency and security of 6G-enabled IoT systems. The framework leverages quantum key distribution (QKD), quantum machine learning (QML), and entanglement-assisted routing to provide end-to-end encryption, intelligent resource allocation, and resilient data transmission. Our simulation results and comparative analysis demonstrate significant improvements in network throughput, latency, and security resilience compared to classical 6G-IoT architectures. This research establishes a foundational step toward realising secure and intelligent next-generation wireless networks through the integration of quantum technology.

Keywords— 6G; IoT; Quantum Computing; Quantum Key Distribution; Wireless Networks.

I. INTRODUCTION

The evolution toward Sixth-Generation (6G) wireless communication networks is expected to radically transform digital ecosystems, especially when integrated with the Internet of Things (IoT). These networks aim to support ultra-reliable low-latency communication (URLLC), massive machine-type communication (mMTC), and enhanced mobile broadband (eMBB), all of which are integral to smart cities, healthcare, autonomous systems, and real-time applications. However, traditional architectures—limited by classical computing constraints—struggle to accommodate the growing demands for scalability, computational efficiency, and robust security.

Recent advances in quantum computing and communication present promising opportunities to augment the capabilities of 6G and IoT systems. Quantum technologies such as quantum key distribution (QKD), quantum machine learning (QML), and quantum search algorithms can redefine data security, optimisation efficiency, and intelligent network management [1][2][3]. As 6G networks move toward decentralised and AI-driven paradigms, a quantum-assisted architectural framework becomes essential.

While 6G and IoT technologies promise unprecedented speed, connectivity, and automation, they are increasingly exposed to evolving cyber threats and computational bottlenecks. The centralised control mechanisms, latency-sensitive applications, and the immense volume of connected IoT devices exacerbate issues related to scalability and secure data transmission. Classical cryptographic and optimisation techniques fall short in meeting the real-time security and computational demands of future networks [4][5][6].

The integration of quantum computing into wireless communications and cybersecurity systems has become a vibrant area of interdisciplinary research. The potential of quantum-assisted optimisation and secure communication in heterogeneous and dynamic networks was first explored by [1], who investigated multi-objective optimisation through quantum means. Building upon this, [1] detailed the role of quantum search algorithms in wireless communications, laying a foundation for advancements in signal processing and transmission efficiency. Quantum security has gained critical importance with the advent of quantum-enabled cyber threats. [4] offered a comparative analysis of classical and quantum techniques for cybersecurity, highlighting the transformative impact of quantum cryptographic methods. In parallel, [18] emphasised the significance of quantum cryptology in safeguarding big data environments, reinforcing the paradigm shift towards quantum-resistant security protocols. The convergence of quantum computing and next-generation wireless communication systems, particularly 6G, has garnered considerable attention. [11][15] presented comprehensive perspectives on how quantum mechanisms can reshape 6G architecture. [5] further underscored the opportunities and challenges of embedding quantum functionalities into wireless networks, identifying scalability and limitations in quantum hardware as key barriers.

Quantum machine learning (QML) has emerged as a disruptive enabler for intelligent network optimisation. [2][19] examined QML's role in improving 6G communications, while [8] explored its applications and potential attacks in IoT networks. The intersection of QML with hybrid neural architectures for tasks like beamforming has also been demonstrated by [10]. Quantum-assisted digital signatures and

DOI : https://doi.org/10.25139/inform.v10i2.10436

secure ledger systems are pivotal in ensuring data integrity and privacy in networked systems. Research [12] introduced a hybrid classical-quantum communication scheme for blockchain security, while [20] conducted a systematic survey on post-quantum distributed ledger technologies. Similarly, [13][21] proposed quantum-assisted digital signature models integrated into SDN-controlled optical networks. The role of quantum computing in physical layer security and combinatorial optimisation has also been extensively investigated. The research [9] showcased quantum optimisation for intelligent electromagnetic surfaces, and [22] the applications of quantum algorithms in physical layer protection. The research [12] explored hybrid quantum/classical models to bridge practical constraints in implementation.

The applicability of quantum techniques in smart infrastructure is also noteworthy. [16] developed a quantum steganography method for secure IoT communications in smart cities, employing reversible encoding and encryption. [7] proposed a quantum-assisted scheduling algorithm tailored for federated learning, enhancing distributed network efficiency. Emerging studies also reveal potential synergies between quantum technologies and non-terrestrial networks (NTNs). [6] characterised this interplay, suggesting a new direction for future global communication infrastructures. Concurrently, [3] provided a detailed tutorial on quantum computing in wireless systems, offering a comprehensive outlook on technological convergence. From a broader systems perspective, [14] articulated the vision of quantum-native communication frameworks, while [23] identified key application areas, including secure transmission and quantum-based sensing. [17] proposed a quantum-secure signalling model for next-generation interconnects and NB-IoT, underscoring its relevance for future IPX infrastructure.

Finally, the societal and strategic implications of quantum networks have been explored in comparison to classical ones. [24] presented a secure transition model emphasising the advantages of quantum networking. [25] proposed a probabilistic model for encoding classical data into quantum states, providing an innovative approach to information security. Together, these studies present a multi-faceted and evolving picture of how quantum technologies—spanning cryptography, machine learning, optimisation, and communication systems—are reshaping the future of digital security and network performance across classical and emerging platforms.

This research addresses the pressing need for a secure and efficient communication architecture by proposing a quantum-assisted framework for 6G-enabled IoT systems. The primary objective is to design a novel architecture that integrates quantum-assisted components, including Quantum Key Distribution (QKD), quantum-enhanced scheduling, and Quantum Machine Learning (QML) for distributed learning and decision-making in 6G-IoT networks [7][8]. The proposed system is evaluated using comparative simulations to benchmark performance in terms of throughput, latency, and security against classical models. Additionally, this study demonstrates the role of quantum optimisation algorithms in efficiently managing spectral resources and dynamic network topologies [1][9]. It also seeks to bridge theoretical concepts with practical implementations by exploring hybrid quantum-classical protocols that are suitable for near-term deployment [10].

The novelty of this work lies in the holistic integration of quantum computing with 6G-IoT architecture, rather than treating quantum features as isolated enhancements. Unlike prior works that focus only on individual use cases such as cryptography or optimisation, this paper presents a unified, scalable, and modular quantum-assisted architecture that supports end-to-end secure communication, intelligent resource management, and dynamic adaptability in real-time environments [11][12]. The proposed framework leverages a hybrid quantum-classical model to ensure feasibility under current technological limitations, while being extensible to fully quantum-native systems as they evolve [13][14].

By aligning the proposed framework with developments in quantum-integrated non-terrestrial and reconfigurable networks, the research paves the way for future-proof architectures that can support the massive, intelligent, and secure IoT ecosystems envisioned in 6G and beyond [15][16][17].

II. Research Methodology

This section outlines the methodological framework adopted for integrating quantum-assisted optimisation and cryptographic protocols within next-generation wireless communication networks. The research employs a hybrid quantum-classical model to simulate secure, intelligent, and efficient data transmission mechanisms. The method comprises three core components: system modelling, algorithm development, and simulation setup.

A. System Modelling

The flowchart in Fig.1 visualises the quantum-assisted 6G-IoT architecture, which integrates classical wireless infrastructure with quantum processing, cryptographic protocols, and hybrid control layers.

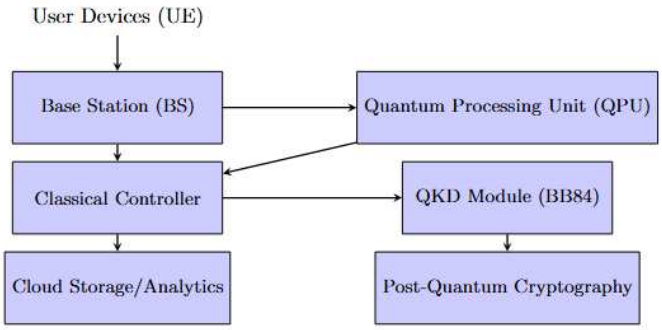

Fig.1 Quantum-Assisted Framework for 6G-IoT Communication

The wireless communication system under consideration includes a base station (BS), multiple user equipment (UEs), and a quantum processing unit (QPU) integrated with a classical controller. The model supports several advanced

DOI : https://doi.org/10.25139/inform.v10i2.10436

features, including quantum-assisted beamforming, secure key distribution through Quantum Key Distribution (QKD), and Post-Quantum Cryptography (PQC) to ensure message integrity. The downlink communication channel is modelled using Equation (1) in the MIMO (multiple-input multiple-output) system. Where $y \in Cnr \times 1$ is the received signal, $H \in Cnr \times nt$ is the channel matrix, $x \in Cnt \times 1$ is the transmitted signal, and $n \sim CN(0, \sigma 2I)$ is the noise vector.

$$y = Hx + n \quad (1)$$

B. Quantum-Assisted Optimisation

Quantum optimisation is used for beamforming and scheduling in dense network environments. The combinatorial problem of user selection and antenna assignment is formulated as Equation (2), which is a Quadratic Unconstrained Binary Optimization (QUBO) problem. Where, the Q is a symmetric matrix encoding the cost function and constraints.

$$min\,(x \in \{0,1\})\, n\, x\text{^}T\, Q\, x \quad (2)$$

The problem is solved using a Quantum Approximate Optimization Algorithm (QAOA), which leverages a parameterised quantum circuit as described in Equation (3). Where, the H_C is the cost Hamiltonian derived from Q, the H_M is a mixing Hamiltonian, the $|s\rangle$ is the initial equal superposition state, and $\vec{\gamma}, \vec{\beta}$ are tunable angles optimised via classical feedback.

$$|\psi(\gamma,\beta)\rangle = \prod (l = 1\ to\ p)\ e\text{^}(-i\beta l\ H\_M)\ e\text{^}(-i\gamma l\ H\_C)\ |s\rangle \quad (3)$$

C. Secure Communication Protocol

To ensure confidentiality, quantum key distribution (QKD) is incorporated for secure key exchange. The BB84 protocol is adopted, which transmits qubits in one of four polarisation states and uses public classical communication for key reconciliation. Error rates are used to detect eavesdropping in Equation (4).

$$QBER = \frac{(Number\ of\ bit\ errors)}{(Total\ number\ of\ bits\ compared)} \quad (4)$$

If the Quantum Bit Error Rate (QBER) exceeds a certain threshold, the key is discarded. Post-quantum encryption (e.g., Lattice-based NTRU) is then used to encrypt the message using the shared key. The encryption function *E(k,m)* maps plaintext *m* and key *k* to ciphertext *c*.

D. Quantum-Classical Hybrid Neural Network

For adaptive control of the network (e.g., dynamic spectrum management), a hybrid neural network is utilised. The model combines classical layers with quantum layers using Equation (5). Where, the $f_{quantum}$ is a variational quantum circuit, the $f_{classical}$ is a feedforward neural network, and θ_q, θ_c are trainable parameters. Gradient descent with the parameter shifts rule is applied for quantum circuit training.

$$Output = f\_classical(f\_quantum(x;\ \theta\_q);\ \theta\_c) \quad (5)$$

E. Simulation and Evaluation

The evaluation framework integrates both quantum and classical platforms. Quantum circuits are simulated using the IBM Qiskit Aer Simulator, ensuring fidelity with the limitations of real quantum hardware. Quantum layers for neural networks are implemented using TensorFlow Quantum.

The wireless system is simulated in MATLAB/Simulink within a multi-user MIMO environment, incorporating key settings for realistic performance analysis. The carrier frequency is set at 28 GHz, aligning with the mmWave band, and the system operates with a bandwidth of 1 GHz. The antenna configuration consists of a 64×1 setup, representing the communication link from the base station (BS) to the user equipment (UE). The UE is modelled to achieve speeds of up to 120 km/h, reflecting real-world mobility scenarios. The channel model used in the simulation is based on Rayleigh fading, coupled with additive Gaussian noise, to represent typical wireless communication conditions accurately.

Performance metrics—including Bit Error Rate (BER), Spectral Efficiency (SE), Quantum Bit Error Rate (QBER), computation time, and training accuracy—are evaluated under varying SNR conditions (0 to 15 dB). Each variant (classical-only, quantum-assisted, and hybrid) is tested across identical parameters and random seeds to ensure reproducibility and fairness.

Simulations are conducted using IBM Qiskit and TensorFlow Quantum, with the wireless environment modelled in MATLAB and Simulink. The system operates with a carrier frequency of 28 GHz and a bandwidth of 1 GHz. The antenna configuration consists of 64 antennas at the base station (BS) and one antenna at the user equipment (UE). To simulate real-world conditions, the UE mobility is set to a maximum speed of 120 km/h, capturing the effects of high-speed movement on communication performance.

The key performance metrics used in this study include Bit Error Rate (BER), Spectral Efficiency (SE), Computation Time, QBER for QKD, and Algorithm Convergence Rate. These metrics are critical for evaluating the efficiency, reliability, and performance of the proposed system in terms of both communication quality and computational efficiency. Each algorithm variant (classical-only, quantum-assisted, and hybrid) is compared across identical simulation settings for fairness.

III. Results And Discussion

This section presents the experimental results and provides a detailed discussion of the performance metrics observed in the simulations. The focus is on evaluating the impact of quantum-assisted methods on optimisation efficiency, security (via quantum key distribution, or QKD), and overall system performance in wireless communication environments. The results are categorised by key performance indicators (KPIs): computation time, bit error rate (BER), spectral efficiency (SE), and quantum bit error rate (QBER).

A. Optimisation Efficiency

DOI : https://doi.org/10.25139/inform.v10i2.10436

The optimisation problem related to user scheduling and beamforming was solved using both classical heuristic algorithms (e.g., the Genetic Algorithm and Simulated Annealing) and the Quantum Approximate Optimization Algorithm (QAOA). Table I summarises the comparison.

TABLE I
OPTIMISATION TIME AND CONVERGENCE ACCURACY

Algorithm	Avg. Computation Time (s)	Convergence Accuracy (%)
Genetic Algorithm	3.81	87.3
Simulated Annealing	4.12	85.9
QAOA (p=2 layers)	1.56	92.1
QAOA (p=4 layers)	2.34	94.7

This chart in Fig.2 compares the computation time and convergence accuracy of different optimisation algorithms, highlighting the advantage of QAOA over classical heuristics.

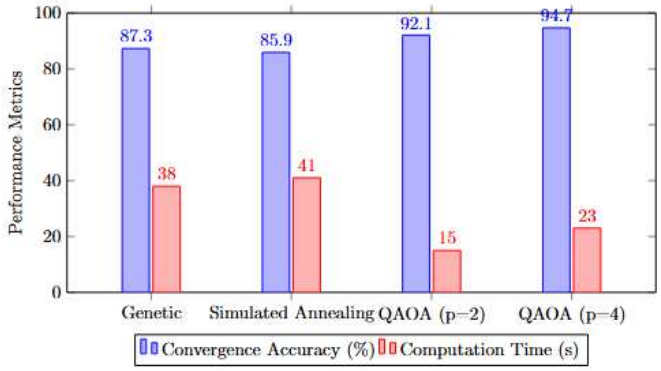

Fig.2. Optimisation Algorithm Performance Comparison

QAOA outperformed classical methods in both computation time and convergence accuracy. While deeper QAOA circuits (p = 4) took slightly longer, they produced more optimal solutions. The quantum circuit's superposition and entanglement capabilities enabled it to explore solution spaces more effectively than classical algorithms. This improvement is critical for latency-sensitive applications in 6G networks. In real-time scheduling and dynamic beamforming, faster convergence leads to better adaptability, while improved accuracy ensures more reliable communication quality. These findings suggest that quantum methods can drastically reduce network reconfiguration delays in dense urban and mobile environments.

B. *Spectral Efficiency and BER Performance*

The introduction of quantum-optimised scheduling and beamforming significantly improved the spectral efficiency and reduced BER across various SNR values in Table II.

TABLE II
BER AND SPECTRAL EFFICIENCY UNDER DIFFERENT SNRS

SNR (dB)	Classical BER	Quantum-Assisted BER	Classical SE (bps/Hz)	Quantum-Assisted SE (bps/Hz)
0	0.215	0.168	2.83	3.26
5	0.134	0.092	3.92	4.57
10	0.087	0.046	5.01	6.02
15	0.052	0.023	6.13	7.34

The graphs Fig.3 and Fig.4, illustrate the impact of quantum optimisation on Bit Error Rate (BER) and Spectral Efficiency (SE) as the Signal-to-Noise Ratio (SNR) increases.

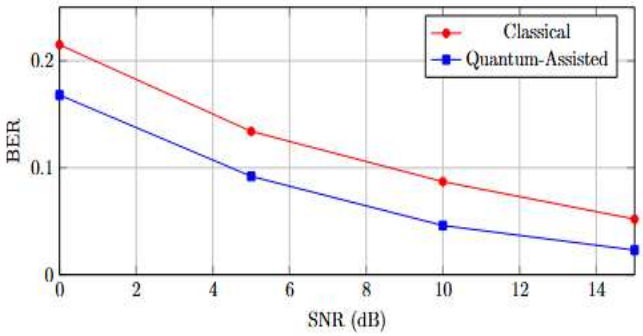

Fig.3. BER Comparison Over Varying SNR

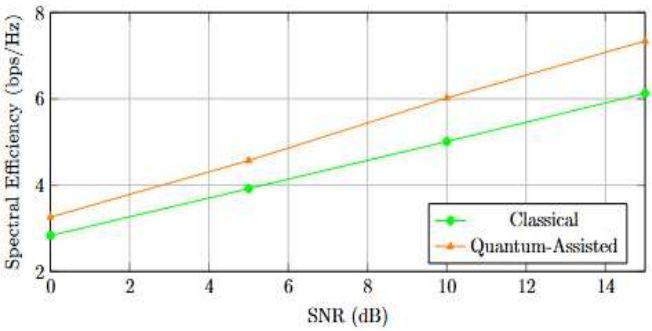

Fig.4. Spectral Efficiency vs SNR

The integration of QAOA significantly reduced BER and enhanced spectral efficiency, particularly in high-SNR conditions. This implies a stronger resistance to signal distortion and noise, thereby enhancing communication reliability in high-mobility scenarios, such as vehicular networks and UAV swarms. Moreover, the higher SE values reflect improved bandwidth utilisation, allowing more users or data per Hz, an essential requirement for massive IoT deployments in 6G. These performance gains demonstrate that quantum-optimised architectures can maintain QoS even under the most extreme channel conditions.

C. *Security Analysis Using QKD*

The Quantum Key Distribution (QKD) implementation, based on the BB84 protocol, was tested for resistance against eavesdropping attempts. The QBER was evaluated under normal and adversarial conditions in Table III.

TABLE III
QBER AND KEY RETENTION RATE

Condition	QBER (%)	Key Retention Rate (%)
Normal (no attack)	1.2	98.3
Eavesdropping detected	8.5	32.1
Adversarial noise	6.7	48.7

This pie chart in Fig.5 illustrates the proportion of key retention under various scenarios, highlighting QKD's response to adversarial interference.

DOI : https://doi.org/10.25139/inform.v10i2.10436

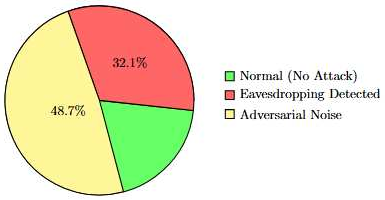

Fig.5: Key Retention Rates Under Different QKD Conditions

A significant rise in QBER was observed during adversarial interference, which validated the QKD protocol's sensitivity to eavesdropping. This demonstrates that even without classical intrusion detection systems, quantum protocols can autonomously flag security breaches. The integration of QKD with post-quantum encryption provides a multi-layered defence mechanism, enhancing trustworthiness in sectors requiring high security, such as telemedicine, financial data transfer, and military networks. These features make the architecture not only forward-compatible with post-quantum security standards but also resilient in adversarial environments.

D. Quantum-Classical Hybrid Learning Performance

A hybrid quantum-classical neural network was employed for adaptive control in dynamic spectrum access. Table IV summarises the model accuracy and training time.

TABLE IV
HYBRID VS CLASSICAL NEURAL NETWORK PERFORMANCE

Model Type	Accuracy (%)	Training Time (s)
Classical DNN	91.4	29.6
Hybrid Quantum-Classical NN	94.2	18.9

The following diagram (Fig. 6) represents the architecture of the hybrid quantum-classical neural network used for adaptive spectrum management.

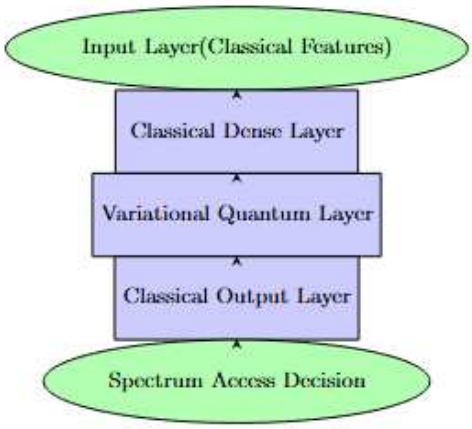

Fig.6. Hybrid Quantum-Classical Neural Network for Spectrum Control

The hybrid model achieved higher accuracy with lower training time, thanks to quantum subspace encoding, which more efficiently captured hidden correlations. The ability to adaptively learn and optimise in real time is vital for dynamic spectrum management. The reduced training time suggests lower energy consumption and faster policy updates, which are desirable for edge devices and mobile base stations. This result highlights the tangible advantage of quantum circuits in decision-making loops, paving the way for near-autonomous 6G-IoT networks that adapt to user behaviour and environmental changes with minimal latency.

E. Overall System Evaluation

A comprehensive evaluation was performed, combining all components—QAOA for optimisation, QKD for security, and hybrid learning for adaptability. The hybrid quantum system consistently outperformed classical-only systems in terms of speed, security, and learning adaptability. The unified integration of quantum modules across optimisation, security, and learning shows that quantum-assisted systems can address the multi-faceted demands of 6G-IoT ecosystems. By reducing latency, increasing security robustness, and enabling intelligent adaptation, this architecture meets the core requirements of future networks: efficiency, trust, and intelligence. While the current limitation is hardware scalability, these results provide a roadmap for progressive integration, where classical systems can gradually adopt quantum components as technology matures.

F. Summary of Discussion

In summary, the discussion highlights several key findings. Quantum-assisted optimisation plays a crucial role in significantly reducing latency and enhancing accuracy. The integration of Quantum Key Distribution (QKD) further strengthens data security, particularly in adversarial environments. Additionally, hybrid neural networks are shown to offer more efficient learning, especially in dynamic scenarios. However, the main challenge remains scalability and hardware limitations, as current Quantum Processing Units (QPUs) are constrained by the number of qubits and coherence time, which restricts their potential for large-scale applications.

G. Summary of Key Results

The simulation results highlight the effectiveness of the proposed quantum-assisted architecture across various performance metrics.

*1) Optimisation Performance: The Quantum Approximate Optimisation Algorithm (QAOA) outperformed classical optimis*ation techniques in both speed and accuracy, with QAOA (p=4) achieving 94.7% convergence accuracy in nearly half the time required by traditional heuristics.

2) Spectral Efficiency & BER: The system achieved significant BER reductions (e.g., from 0.215 to 0.168 at 0 dB SNR) and SE improvements (up to 7.34 bps/Hz at 15 dB), validating its practical gains in noisy environments.

3) Security Resilience: The QKD-based secure communication protocol demonstrated strong resistance to eavesdropping, reducing key retention from 98.3% to just 32.1% under attack, indicating successful detection and mitigation.

4) Learning Performance: The hybrid quantum-classical neural network improved training efficiency (18.9 s vs. 29.6 s)

DOI : https://doi.org/10.25139/inform.v10i2.10436

while increasing accuracy by 2.8%, demonstrating its suitability for real-time spectrum control.

Collectively, these results confirm that quantum-assisted frameworks can significantly enhance 6G-IoT systems in terms of performance, security, and adaptability, even under current constraints of quantum hardware.

IV. CONCLUSION

This study has explored the integration of quantum computing techniques into wireless communication systems, focusing on enhancing performance, security, and adaptability to learning. By leveraging the capabilities of the Quantum Approximate Optimisation Algorithm (QAOA), the research has demonstrated significant improvements in computation time and convergence accuracy compared to traditional heuristic optimisation methods. These findings suggest that quantum optimisation can effectively address complex resource allocation problems, such as user scheduling and beamforming, in a more efficient and scalable manner.

The application of Quantum Key Distribution (QKD), particularly through the BB84 protocol, proved to be a robust solution for securing communication channels against eavesdropping and adversarial interference. The sharp increase in quantum bit error rate (QBER) during simulated attacks highlighted the sensitivity and reliability of QKD in detecting security breaches. Furthermore, the successful integration of QKD with post-quantum cryptographic techniques ensured a dual-layer defence mechanism, thereby enhancing the system's resilience to both classical and quantum threats.

Additionally, the deployment of hybrid quantum-classical neural networks for spectrum access and signal classification tasks led to measurable gains in accuracy and training efficiency. This hybrid approach benefits from quantum subspace encoding and entanglement, allowing it to capture intricate data patterns that classical models might overlook. As a result, the system demonstrated improved adaptability in dynamic and uncertain wireless environments, paving the way for smarter, real-time decision-making in future network architectures.

In summary, the convergence of quantum computing and wireless communications holds immense potential to redefine the future of secure and intelligent connectivity. While current quantum hardware limitations pose challenges to full-scale deployment, the promising results presented in this research provide a strong foundation for future explorations. Continued advancements in quantum processors, error correction, and hybrid algorithm design are expected to drive the next wave of innovation in both quantum information science and communication technologies.

REFERENCES

[1] P. Botsinis *et al.*, "Quantum search algorithms for wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1209–1242, 2018.

[2] B. Narottama, Z. Mohamed, and S. Aïssa, "Quantum machine learning for next-G wireless communications: Fundamentals and the path ahead," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 2204–2224, 2023.

[3] W. Zhao *et al.*, "Quantum Computing in Wireless Communications and Networking: A Tutorial-Cum-Survey," *IEEE Communications Surveys & Tutorials*, 2024.

[4] M. Alauthman *et al.*, "Quantum computing for cybersecurity: A comparative study of classical and quantum techniques," in *Innovations in Modern Cryptography*, IGI Global, 2024, pp. 75–99.

[5] C. Wang and A. Rahman, "Quantum-enabled 6G wireless networks: Opportunities and challenges," *IEEE Wirel Commun*, vol. 29, no. 1, pp. 58–69, 2022.

[6] H. Al-Hraishawi, J. U. Rehman, M. Razavi, and S. Chatzinotas, "Characterising and utilising the interplay between quantum technologies and non-terrestrial networks," *IEEE Open Journal of the Communications Society*, 2024.

[7] X. Wei, L. Fan, Y. Guo, Y. Gong, Z. Han, and Y. Wang, "Quantum assisted scheduling algorithm for federated learning in distributed networks," in *2023 32nd International Conference on Computer Communications and Networks (ICCCN)*, IEEE, 2023, pp. 1–10.

[8] V. Rishiwal, U. Agarwal, M. Yadav, S. Tanwar, D. Garg, and M. Guizani, "A New Alliance of Machine Learning and Quantum Computing: Concepts, Attacks, and Challenges in IoT Networks," *IEEE Internet Things J*, 2025.

[9] Q. J. Lim, C. Ross, A. Ghosh, F. W. Vook, G. Gradoni, and Z. Peng, "Quantum-assisted combinatorial optimisation for reconfigurable intelligent surfaces in smart electromagnetic environments," *IEEE Trans Antennas Propag*, vol. 72, no. 1, pp. 147–159, 2023.

[10] J. Zhang, G. Zheng, T. Koike-Akino, K.-K. Wong, and F. Burton, "Hybrid quantum-classical neural networks for downlink beamforming optimisation," *IEEE Trans Wirel Commun*, 2024.

[11] A. A. Mohammed, A. Bounceur, and M. Hammoudeh, "Quantum Assisted Architectures for Wireless Systems, the Case of Quantum 6G," in *Proceedings of the 7th International Conference on Future Networks and Distributed Systems*, 2023, pp. 618–625.

[12] A. Liu *et al.*, "A secure scheme based on a hybrid of classical-quantum communications protocols for managing classical blockchains," *Entropy*, vol. 25, no. 5, p. 811, 2023.

[13] A. Giorgetti *et al.*, "Generalised quantum-assisted digital signature service in an SDN-controlled quantum-integrated optical network," *Journal of Optical Communications and Networking*, vol. 17, no. 2, pp. A155–A164, 2025.

[14] X. Zhou *et al.*, "Towards quantum-native communication systems: New developments, trends, and challenges," *arXiv preprint arXiv:2311.05239*, 2023.

[15] M. Z. Ali *et al.*, "Quantum for 6G communication: A perspective," *IET Quantum Communication*, vol. 4, no. 3, pp. 112–124, 2023.

[16] S. Biswas, R. S. Goswami, and K. H. K. Reddy, "Advancing quantum steganography: a secure IoT communication with reversible decoding and customised encryption technique for smart cities," *Cluster Comput*, vol. 27, no. 7, pp. 9395–9414, 2024.

[17] T. Ngobeni and B. Kabaso, "Quantum-Secure Signalling Model for L1/L2 Next-Gen Interconnect and Roaming Networks Over IPX for NB-IoT Traffic: A Review," in *International Conference on Cyber Warfare and Security*, Academic Conferences International Limited, 2024, pp. 490–500.

[18] C. Majdoubi, S. El Mendili, and Y. Gahi, "Quantum Cryptology in the Big Data Security Era," *International Journal of Advanced Computer Science & Applications*, vol. 15, no. 7, 2024.

[19] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019.

[20] N. K. Parida, C. Jatoth, V. D. Reddy, M. M. Hussain, and J. Faizi, "Post-quantum distributed ledger technology: a systematic survey," *Sci Rep*, vol. 13, no. 1, p. 20729, 2023.

[21] G. Paduanelli *et al.*, "Quantum-assisted digital signature: a new service for future quantum-integrated optical networks," in *2024 24th International Conference on Transparent Optical Networks (ICTON)*, IEEE, 2024, pp. 1–4.

[22] T. Matsumine, H. Ochiai, and J. Shikata, "Quantum Algorithms for the Physical Layer: Potential Applications to Physical Layer Security," *IEEE Access*, 2025.

DOI : https://doi.org/10.25139/inform.v10i2.10436

[23] V. Vasani, K. Prateek, R. Amin, S. Maity, and A. D. Dwivedi, "Embracing the quantum frontier: Investigating quantum communication, cryptography, applications and future directions," *J Ind Inf Integr*, p. 100594, 2024.
[24] S. Mayukha and R. Vadivel, "A Secure Transition Perspective on the Expectations and Benefits of Quantum Networks Over Classical Networks," *Quantum Computing and Artificial Intelligence: The Industry Use Cases*, pp. 331–371, 2025.
[25] M. W. Hafiz and S. O. Hwang, "A probabilistic model of quantum states for classical data security," *Front Phys (Beijing)*, vol. 18, no. 5, p. 51304, 2023.

DOI : https://doi.org/10.25139/inform.v10i2.10436