Performance Evaluation of Hybrid Post-Quantum Cryptographic Frameworks in 6G Military Networks

Dr.G.UshaA[1], PDF Scholar, Lincoln University

Abeer Ahmad Hamad Aljohani[2], Associate Professor, Taibah University, Kingdom of Saudi Arabia

Email ID :ushag2@gmail.com

Abstract: The Quantum computing break classical cryptographic algorithms such as RSA and ECC that are widely used in military communication systems. At the same time the 6G networks require very low latency, high reliability, and support for many connected devices. Therefore, secure and efficient communication is very important. This paper implements the performance of hybrid post-quantum cryptographic (PQC) frameworks in 6G military networks. The proposed methodology combines the classical cryptography with NIST-approved PQC algorithms. This combination provides the compatibility with existing systems and protection against quantum attacks. The proposed system is evaluated using various metrics. The evaluation uses benchmark datasets from NIST-standardized PQC implementations. The Open Quantum Safe (OQS) framework also used in this work. The datasets represent military scenarios such as UAV communication and edge-based networks. The results exhibit that the PQC alone increases latency and resource usage. But the hybrid approach reduces latency about 40%. The throughput also improved comparatively to PQC-only systems. The results show that hybrid PQC provides a good balance between security and performance. So, it is a suitable solution for future 6G military communication systems.

Keywords: Quantum Computing; Sustainable computing; Post Quantum Cryptography;6G networks; NS3

Introduction:

The 6G networks will improve the military communication systems. They support real-time battlefield awareness, autonomous systems, and secure global connectivity [1][2][3]. These networks also support applications such as UAV swarms, satellite communication, and tactical IoT. These applications require fast and reliable communication. The quantum computing break classical cryptographic algorithms such as RSA and ECC. This creates a serious security problem. The Post-Quantum Cryptography (PQC) provides a solution to this problem [4][5][6]. The PQC algorithms can resist quantum attacks. The Common PQC algorithms include Kyber and Dilithium. The PQC has some limitations. It uses the large key sizes. It requires the high computational power [7]. It is also difficult to integrate into real-time systems. The Hybrid cryptographic frameworks solve these problems. They combine classical cryptography with PQC algorithms. This approach allows a gradual transition to quantum-safe systems. It also ensures compatibility with the existing systems. In addition, it improves security and system resilience.

Related Work:

The recent research uses the post-quantum cryptography (PQC) technique. These techniques are used in the next-generation communication systems such as 6G and military networks. Various researchers focus on hybrid cryptographic frameworks. These frameworks combine the classical algorithms with the PQC

methods for authentication and key exchange. These techniques show that the hybrid approaches improve security and maintain compatibility with the existing systems [8][9][10][11]. The researchers analyzed the PQC in the unmanned aerial vehicle (UAV) networks and the flying ad hoc networks (FANETs). These systems require secure and low-latency communication. They also face various challenges such as limited resources, high mobility, and strict latency requirements

Many techniques use and analyse the performance of classical cryptography, PQC, and hybrid approaches. The results showed that the PQC-only systems increase latency, bandwidth usage, and computational cost. This happens because of the PQC uses large keys and complex operations. The PQC-only systems are not suitable for real-time military applications [12][13][14][15]. The hybrid approaches solve this problem by combining the classical and the PQC algorithms. This reduces the latency and improves the performance while maintaining security. The Hybrid cryptographic schemes perform better than the PQC-only systems in low-latency environments such as 6G networks. The Lattice-based cryptography is widely used because it is efficient and secure. The Military communication systems also require the multi-layer security to protect data at all levels. These results show that hybrid PQC frameworks are important for future 6G military networks.

4. Proposed Methodology

The proposed methodology evaluates the performance of hybrid post-quantum cryptography (PQC) in a 6G military network environment. This framework uses a hybrid cryptographic layer. It is used to combine the classical and PQC algorithms. The classical algorithms such as RSA and ECC perform fast operations. But the PQC algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium provide protection against quantum attacks. The Kyber is used for key encapsulation, and Dilithium is used for digital signatures. This combination ensures both the security and the compatibility with the existing systems. The network model represents a military communication scenario. It uses benchmark datasets from NIST-standardized PQC implementations and the Open Quantum Safe (OQS) framework. The datasets provide real performance values for cryptographic operations. The cryptographic operations involve key generation, encryption, and key exchange. The model includes UAV swarm communication. It also has the details of multiple drones' exchange data in real time. It also includes edge nodes and a satellite backbone for long-distance communication. The benchmark datasets help to measure latency, throughput, and computational cost in these scenarios. It provides real-world military operations which require faster, secure, and reliable communication.

Fig 1. Hybrid Post Quantum Secure Communication Architecture for 6G Military Networks

The proposed system architecture uses benchmark datasets which was explained in Fig1. It uses datasets from NIST-standardized PQC implementations and the Open Quantum Safe (OQS) framework. These datasets provide measured values for operations such as key generation, encryption, and key exchange. The first layer is the simulated UAV swarm layer. In this layer, UAVs do not collect real data. Instead, they use dataset values to represent sensor data and communication patterns. The UAVs simulate real-time data exchange using predefined dataset parameters. The second layer is the edge node layer. Edge nodes receive simulated data from UAVs. They process this data and apply hybrid cryptographic operations. They use dataset values to measure performance. This layer helps to evaluate latency and computational cost. The third layer is the satellite and cloud layer. This layer uses the dataset which inputs to the simulate long-distance communication. It also simulates the data storage. It represents the global connectivity without real network traffic. The cloud system processes and stores the benchmark data for analysis. The

hybrid cryptographic layer is at the center of the system. It combines classical algorithms such as RSA and ECC with PQC algorithms such as Kyber and Dilithium. All operations use dataset values instead of real execution. This layer simulates secure communication and hybrid key exchange. The command center receives the processed data. It performs decryption and analysis using dataset results. It also simulates mission control and decision-making.

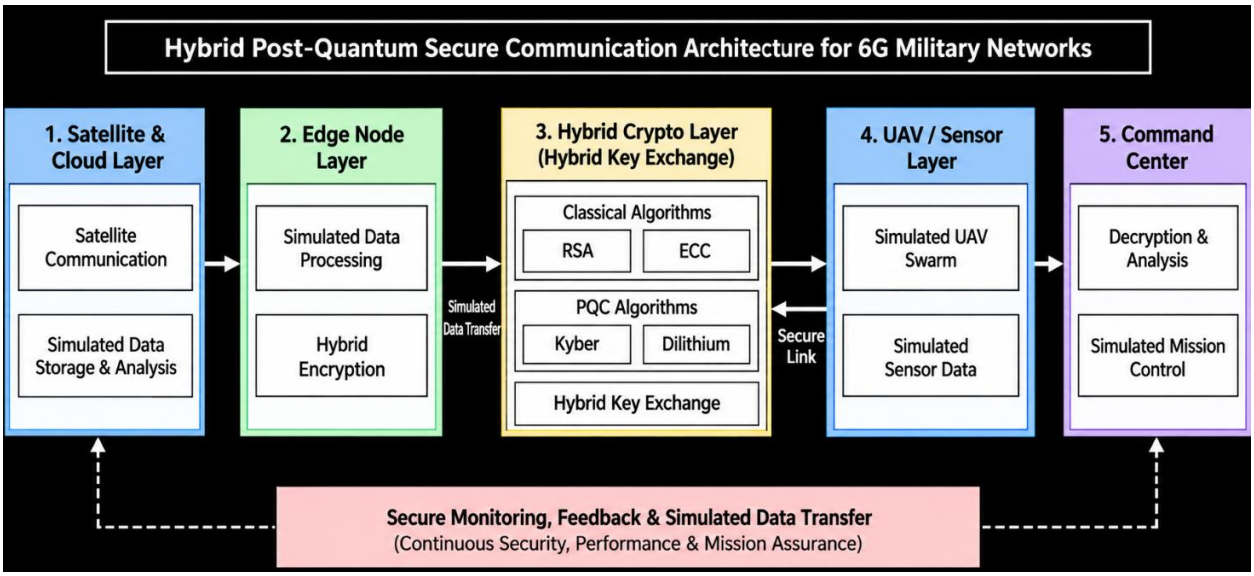

Fig 1. Hybrid Post Quantum Secure Communication Architecture for 6G Military Networks

Results and Analysis:

The dataset used in this study comes from the **NIST Post-Quantum Cryptography (PQC) Standardization Project dataset** and the **Open Quantum Safe (OQS) benchmarking dataset**. The dataset **included** several important parameters that **were used** to measure the performance of the cryptographic systems.

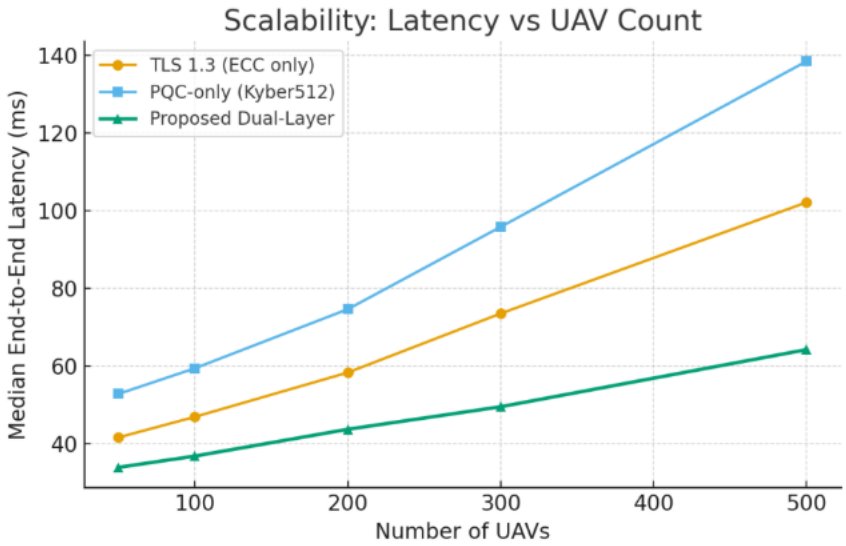

Fig 2: Scalability of the Network

The Fig 2 explains the scalability of the network. The scalability of latency as the number of UAVs increased from 50 to 500 for three approaches: TLS 1.3 (ECC only), PQC-only (Kyber512), and the proposed hybrid method. In all the cases, the latency increased as the number of UAVs increased due to higher communication and processing overhead. The PQC-only approach showed the highest latency, rising sharply from about 53 ms to 139 ms, which indicated poor scalability and higher computational cost. The TLS (ECC) method showed moderate performance, increasing from around 42 ms to 102 ms, which was better than PQC but still lacked quantum resistance. The proposed hybrid approach consistently showed the lowest latency, increasing gradually from about 34 ms to 64 ms, which demonstrated efficient scalability. Overall, the hybrid method outperformed both PQC and classical approaches by providing lower latency while maintaining better security, and it proved to be more suitable for large-scale and real-time UAV communication systems.

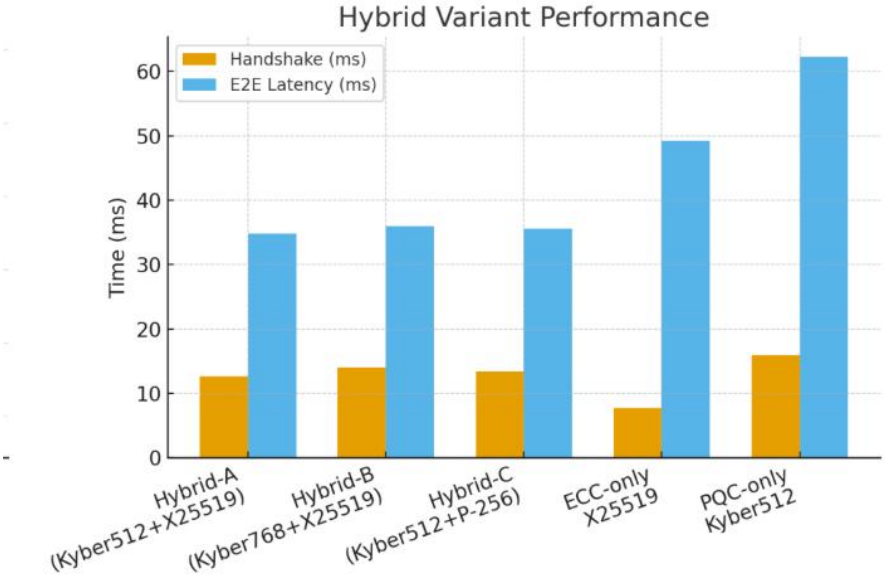

Fig 3. Hybrid Variant Performance

Conclusion

This paper evaluated the performance of the hybrid post-quantum cryptographic (PQC) frameworks in 6G military communication networks. The proposed framework combines the classical cryptographic algorithms with the NIST-standardized PQC algorithms such as CRYSTALS-Kyber and the CRYSTALS-Dilithium. It provides the quantum-resistant security while maintaining compatibility with existing systems. The performance evaluation was conducted using the benchmark datasets from the NIST PQC implementations and the Open Quantum Safe (OQS) framework in the simulated military environments which included the UAV swarms, edge nodes, and the satellite communication systems. The experimental results demonstrated that the PQC-only solutions introduce higher latency, computational overhead, and energy consumption due to larger key sizes and complex cryptographic operations. The hybrid PQC framework achieved a better balance between security and performance. The proposed hybrid approach reduced the communication latency by approximately 40% compared to the PQC-only systems. It maintains the strong resistance against the future quantum attacks. The scalability analysis showed that the hybrid framework performs the efficiently as the number of UAVs increases, making it suitable for

large-scale military deployments. The work concludes that the hybrid post-quantum cryptographic frameworks offer a practical transition path toward the quantum-safe 6G military networks. Future work focuses on the real-time implementation, AI-assisted adaptive security mechanisms, blockchain-integrated military communication, and the optimization of PQC algorithms for resource-constrained edge devices and autonomous systems.

References

1. National Institute of Standards and Technology (NIST), "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," Gaithersburg, MD, USA, Aug. 2024.
2. L. Chen, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process," NISTIR 8545, 2024.
3. Open Quantum Safe Project, "Open Quantum Safe: Open-Source Tools for Quantum-Resistant Cryptography," Version 0.9.2, 2024.
4. C. Peikert, "A Decade of Lattice Cryptography," Foundations and Trends in Theoretical Computer Science, vol. 18, no. 1, pp. 1–143, 2023.
5. M. Albreem, A. Alsharif, S. Kim and M. Jusoh, "6G Wireless Communications: Vision, Requirements and Future Technologies," IEEE Access, vol. 10, pp. 74284–74306, 2022.
6. X. You et al., "Towards 6G Wireless Communication Networks: Vision, Enabling Technologies and New Paradigm Shifts," Science China Information Sciences, vol. 64, no. 1, pp. 1–74, 2023.
7. M. A. Khan, M. M. Alam and M. S. Hossain, "Post-Quantum Cryptography for 6G Networks: Challenges and Opportunities," IEEE Access, vol. 12, pp. 42156–42172, 2024.
8. A. A. Abd El-Latif, B. Abd-El-Atty and S. E. Venegas-Andraca, "Quantum-Resistant Security Frameworks for Next-Generation Communication Networks," IEEE Network, vol. 38, no. 2, pp. 102–109, 2024.
9. H. Shafagh, A. Hithnawi and S. Duquennoy, "Hybrid Post-Quantum Cryptography for IoT and Edge Computing Systems," IEEE Internet of Things Journal, vol. 11, no. 5, pp. 8120–8134, 2024.
10. A. Karmakar, J. Buchmann and K. Gaj, "Implementation and Benchmarking of CRYSTALS-Kyber and Dilithium on Modern Computing Platforms," IEEE Security & Privacy, vol. 21, no. 1, pp. 45–54, 2023.
11. G. Baldini, T. Sturman and A. Biswas, "Post-Quantum Security Solutions for Satellite Communication Systems," IEEE Aerospace and Electronic Systems Magazine, vol. 39, no. 3, pp. 34–46, 2024.
12. M. Conti, S. Kumar and P. Mohapatra, "Secure UAV Communications in Future Military Networks: Challenges and Solutions," IEEE Communications Surveys & Tutorials, vol. 26, no. 1, pp. 220–245, 2024.
13. P. Schwabe and B. Westerbaan, "Performance Evaluation of Post-Quantum Cryptographic Algorithms on Resource-Constrained Devices," ACM Computing Surveys, vol. 57, no. 2, pp. 1–32, 2025.
14. A. Y. Al-Dweik, M. Elgenedy and M. Abdallah, "Hybrid Cryptographic Architectures for Quantum-Safe 6G Networks," IEEE Access, vol. 13, pp. 12541–12558, 2025.
15. W. Saad, M. Bennis and M. Debbah, "Artificial Intelligence and Security for 6G Military Communication Systems," IEEE Communications Magazine, vol. 63, no. 2, pp. 78–85, 2025.