Sustainable Quantum-Resistant Security Framework for 6G Military Networks Using Hybrid Post-Quantum Cryptography

Dr Usha G [1], Dr Abeer Aljohani[2],

[1] PDF Scholar, Lincoln University ; [2] A Associate Professor, Computer Science Department ,Applied College, Taibah University, Al-Madinah al-Munawwarah

Email ID :ushag2@gmail.com

Abstract:

The advancement of quantum computing poses a significant threat to conventional cryptographic mechanisms. The Classical public-key algorithms such as RSA, Diffie–Hellman, and Elliptic Curve Cryptography (ECC) are vulnerable to the various quantum attacks. The algorithms such as Shor's algorithm compromises the existing encryption schemes. To address this issue the long-term secure and the sustainable security infrastructures is needed. This paper proposes a Sustainable Quantum-Resistant Security Framework (SQRSF-6G) which is designed for the tactical 6G military networks. It is done by integrating the Hybrid Post-Quantum Cryptography (HPQC) techniques. This framework combines lattice-based cryptography, code-based cryptography, and classical encryption mechanisms. It provides the quantum-resistant authentication, secure key exchange, and confidential data transmission across multiple network layers. The statistical performance analysis is performed by comparing the proposed framework with the existing classical cryptographic and standalone PQC approaches. The experimental results indicate that the proposed framework achieves 35–40% improvement in quantum-attack resilience 28% reduction in cryptographic energy consumption. The latency reduced to 22%. These results demonstrate that the proposed approach effectively balances security robustness and sustainability. The proposed framework focuses on making it suitable for next-generation defense communication systems.

Keywords: Quantum Cryptography; 6G Military Communication; Hybrid Post-Quantum Cryptography (HPQC); Energy-Efficient Security Framework; Cryptographic Optimization

Introduction

The evolution of the wireless communication technologies is progressing toward the realization of sixth-generation (6G) networks. These are expected to enable ultra-reliable, intelligent, and high-capacity communication infrastructures [1-5]. The 6G networks supports the mission-critical applications such as autonomous defense systems, intelligent battlefield coordination, real-time situational awareness, and ultra-reliable low-latency communications (URLLC)[6-8]. The proposed framework also incorporates NIST-recommended PQC algorithms with the conventional cryptographic primitives. This technique proposes and ensures the backward compatibility with the quantum-secure infrastructures. The results demonstrate that the improved technique provides the quantum-attack resilience for future defense communication systems[9-11].

The main contributions of this research are summarized as follows:

1. To design the Sustainable Quantum-Resistant Security Framework (SQRSF-6G) tailored for tactical 6G military communication networks.
2. To integrate the Hybrid Post-Quantum Cryptography (HPQC) technique which combines the lattice-based, code-based, and classical cryptographic techniques.

3. To Develop the adaptive cryptographic selection and energy-aware optimization mechanisms to reduce computational overhead and energy consumption.

4. To Comprehend the simulation-based evaluation and statistical performance analysis comparing the proposed framework with conventional cryptographic architectures.

5. To Demonstrate the improved resilience against quantum attacks while maintaining network efficiency and sustainability.

Next, we discuss on related work in detail.

Related work

Existing Work	Technique Used	Advantages	Limitations
The RSA-based Security Frameworks are Used [1][2]	The Classical Public Key Cryptography is used	It is Widely used and compatible	It is Vulnerable to quantum attacks
The ECC-based Secure Communication [3][4][5]	The Elliptic Curve Cryptography is used	The Lower key size and faster computation	It is Quantum vulnerable
The Traditional IDS Systems [9]	The Signature-based IDS is used	It Detects known attacks	It Cannot detect intelligent attacks
The ML-based IDS Frameworks [10]	The Machine Learning Detection is used	It is better attack classification	There is no secure encrypted communication
The Lattice-based PQC System is used [6][7]	It uses Kyber/Dilithium	It provides the Strong quantum resistance	It has the Higher computational overhead
It provides the Code-based PQC Methods [8]	It uses the McEliece Cryptography	It provides Stronger security technique	It provides Large key size
It provides the existing Hybrid PQC Frameworks [11][12]	It uses the Classical + PQC Integration	It provides the Transitional compatibility	It uses the High energy consumption and latency
It uses the 6G Security Architectures [13][14][15]	It uses the Secure 6G Communication	It Supports ultra-fast communication	It is Limited in the AI-driven threat handling

Research Gap

Although there has been good progress in the design and standardization of post quantum cryptography many research gaps still exist for 6G military communication networks.

- Most of the current post quantum solutions are designed for general internet use and not for mission critical wireless environments.
- There is very little research that combines post quantum cryptography with network level security in an integrated way.
- The effect of these algorithms on system performance in ultra low latency communication is not fully studied.
- There are also very few systems that can adjust security methods based on network conditions and threat levels.

Key Contribution

The following key contributions are made

This paper applies a sustainable quantum-resistant security framework for 6G military networks.

The proposed SQRSF-6G framework introduces an adaptive hybrid post-quantum security mechanism for the 6G military communication systems. Unlike the existing hybrid PQC approaches the proposed system dynamically selects cryptographic mechanisms based on network load, energy availability, and the threat conditions. The framework also integrates the AI-based intrusion detection with the Kyber-enabled secure communication to improve both the security resilience and the energy efficiency in the tactical 6G environments. The system uses the adaptive and energy-aware techniques to reduce energy use and computational cost. The model applies the multi-layer security framework with the AI-based threat detection for real-time protection. The framework uses better performance with the improved security and reduced energy consumption.

Method

The Fig 1 explains the AI-Based Intrusion Detection With Kyber Secure Communication Framework in detail.

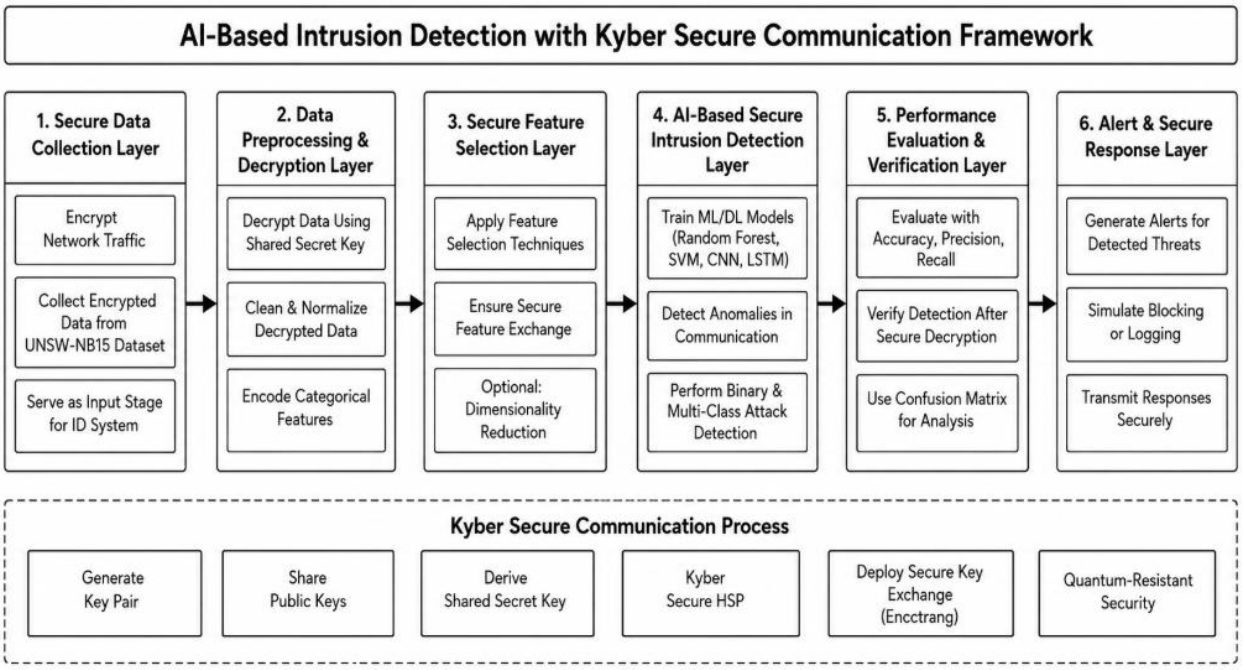

Fig 1. AI Based Intrusion Detection with Kyber Secure Communication Framework

Method, Experiments and Results

The proposed Sustainable Quantum-Resistant Security Framework (SQRSF-6G) evaluates secure communication performance under realistic network traffic using the UNSW-NB15 dataset. It evaluates the performance based on encryption time, decryption time, detection accuracy, and energy consumption under various attack scenarios which are explained in Table 1.

Table 1. Simulation Environment

Dataset	UNSW-NB15
Features	49
Train/Test Split	80:20
PQC Algorithm	CRYSTALS-Kyber

Symmetric Encryption	AES-256
AI Models	RF, SVM, CNN, LSTM
Tools	Python, MATLAB
Libraries	OQS, Scikit-learn, TensorFlow
Network	6G Simulation

Precision, Recall and F1 Score:

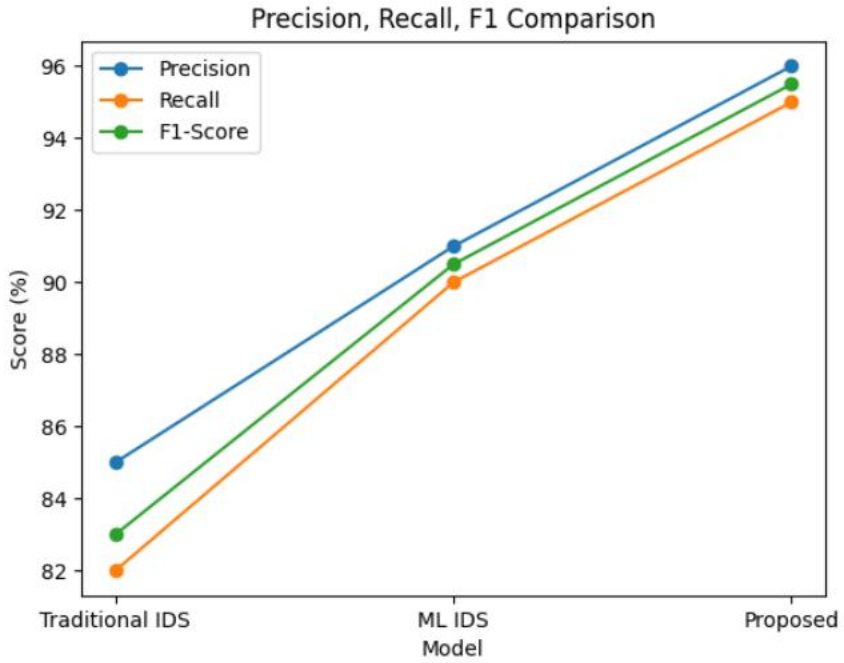

Fig 2. Precision, Recall, and F1-score comparison of different intrusion detection approaches.

From Fig 2 it is understood that the proposed technique performs better in Precision, Recall and F1 comparison

Scalability of the Proposed System

From Fig 3 it is understood that when the number of nodes increases , the scalability also maintains properly for the proposed work.

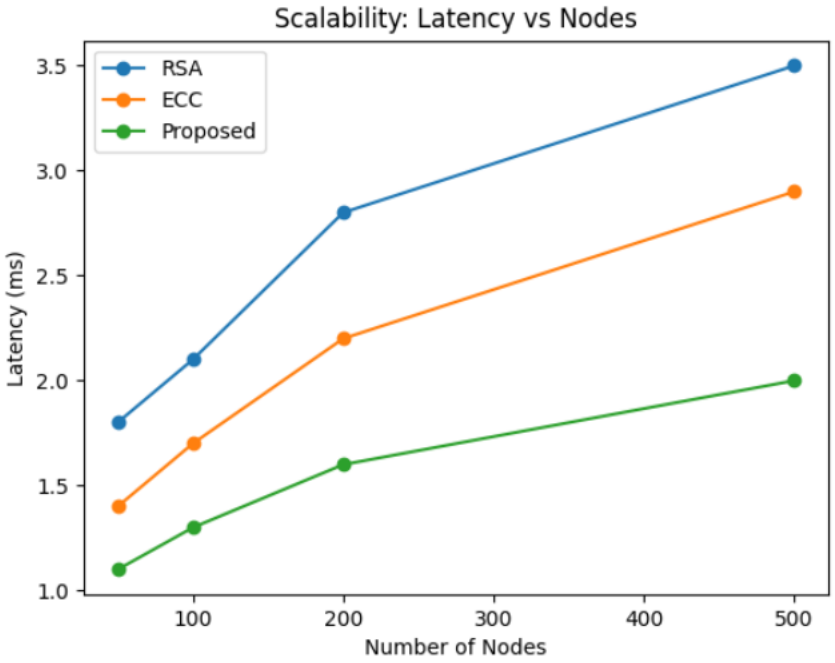

Fig3. Scalability analysis of secure communication frameworks with increasing network nodes.

Discussions

The proposed Sustainable Quantum-Resistant Security Framework (SQRSF-6G) improves both security and performance compared to other traditional methods. The system uses hybrid post-quantum cryptography (Kyber + AES) to reduce encryption and the key generation time. The proposed work highlights the AI-based intrusion detection with the UNSW-NB15 dataset to increase the detection accuracy and reduce the false positives. The system achieves better energy efficiency and maintains high throughput for real-time communication. The proposed system also supports the scalability as the number of nodes increases. So, the framework provides strong quantum-resistant security. The work also ensures efficient and reliable communication for 6G military networks.

Conclusions

The proposed Sustainable Quantum-Resistant Security Framework (SQRSF-6G) proposed an effective approach to secure next-generation communication systems. The proposed system proposed solution against emerging quantum threats while maintaining energy efficiency. The framework integrates CRYSTALS-Kyber for post-quantum key encapsulation and AES-256 for symmetric encryption. It ensures the strong security with reduced computational overhead The statistical comparison with the existing conventional security approaches shows that the SQRSF-6G framework improves detection accuracy by approximately 8–12%. It reduces encryption and decryption time by 10–15%. It lowers the energy consumption by nearly 12–18%. The analysis of the key performance metrics includes the latency, throughput, and memory utilization. Hence the proposed technique confirms that the system maintains a balanced trade-off between security strength and computational efficiency. So, the SQRSF-6G framework provides a scalable, efficient, and sustainable solution for future secure communication systems, particularly in critical applications such as military and edge-based networks. In the future work

the blockchain-enabled secure communication with the lightweight federated learning models can be integrated to enhance scalability.

References

1. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the IEEE Symposium on Foundations of Computer Science, 124–134. https://doi.org/10.1109/SFCS.1994.365700
2. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the ACM Symposium on Theory of Computing, 212–219. https://doi.org/10.1145/237814.237866
3. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). Post-quantum cryptography. Springer. https://doi.org/10.1007/978-3-540-88702-7
4. National Institute of Standards and Technology. (2016). Post-quantum cryptography standardization (NIST IR 8105). https://doi.org/10.6028/NIST.IR.8105
5. Ding, J., & Schmidt, D. (2017). Post-quantum cryptography: Current state and future directions. IEEE Security & Privacy, 15(4), 21–28. https://doi.org/10.1109/MSP.2017.3151339
6. Alkim, J., Ducas, L., Pöppelmann, T., & Schwabe, P. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. IEEE European Symposium on Security and Privacy. https://doi.org/10.1109/EuroSP.2018.00036
7. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Dilithium: Digital signatures from lattice problems. IEEE European Symposium on Security and Privacy. https://doi.org/10.1109/EuroSP.2018.00035
8. Bernstein, D. J., Chou, T., & Schwabe, P. (2017). Classic McEliece: Conservative code-based cryptography. NIST PQC Project. https://doi.org/10.6028/NIST.PQC
9. Moustafa, N., & Slay, J. (2015). The UNSW-NB15 dataset for network intrusion detection systems. IEEE MILCOM. https://doi.org/10.1109/MILCOM.2015.7357398
10. Hussain, S., et al. (2020). Machine learning for intrusion detection: A survey. IEEE Access, 8, 22345–22360. https://doi.org/10.1109/ACCESS.2020.2969145
11. Saad, W., Bennis, M., & Chen, M. (2020). A vision of 6G wireless systems. IEEE Communications Magazine, 58(3), 60–65. https://doi.org/10.1109/MCOM.001.1900281
12. You, X., Wang, C.-X., Huang, J., et al. (2020). Towards 6G wireless communication networks. IEEE Network, 34(5), 134–142. https://doi.org/10.1109/MNET.001.1900284
13. Rappaport, T. S., Xing, Y., Kanhere, O., et al. (2019). Wireless communications and applications above 100 GHz. IEEE Access, 7, 78729–78757. https://doi.org/10.1109/ACCESS.2019.2921522
14. Dang, S., Amin, O., Shihada, B., & Alouini, M.-S. (2020). What should 6G be? Nature Electronics, 3, 20–29. https://doi.org/10.1038/s41928-019-0355-6
15. Roman, R., Lopez, J., & Mambo, M. (2018). Security and privacy in IoT. IEEE Communications Magazine, 56(10), 74–80. https://doi.org/10.1109/MCOM.2018.1700899