A Quantum-Resilient Federated DRL Framework for Secure Voice Communication in 6G-Enabled MANETs

[1]B Sudha, [2]Prof Dr Midhunchakkaravarthy, [3]Dr. Ganesh Khekare,
[1]Post Doctoral Researcher, Lincoln College University, Malaysia,
[1]Senior Assistant Professor, School of Science and Computer Studies, CMR University, Bangalore, India,
[2]Dean, Faculty of AI Computing and Multimedia, Lincoln University College, Malaysia,
[3]Associate Professor, School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology, Vellore, India.
Email : pdf.sudha@lincoln.edu.my

Abstract: The problem of secure voice communications in Mobile Ad-hoc Networks (MANETs) is gaining traction as 6G low-latency applications are introduced and the threat of a quantum adversary is growing. The classical encryption schemes are vulnerable to lattice attacks by Shor, and centralized learning schemes are unable to maintain privacy in decentralised military or disaster response MANETs. In this paper, we present Federated Deep Reinforcement Learning-Driven Post-Quantum Voice Encryption Framework (FedRL-PQVE) that incorporates lattice-based key generation, federated policy learning, and real-time adaptive encryption optimization to MANET routing state. DRA agent maximizes the strength of encryption, bit-allocation, and computational cost per hop without infringing the privacy of the user by means of decentralized model aggregation. It has been demonstrated to reduce latency by 28-42 percent, reduce the probability of quantum attack success by 50-70 percent and reduce energy consumption by 30 percent over classical systems. The framework provides a powerful and smart quantum-resistant voice communication application to 6G-enabled MANETs.

Keywords: MANETs, Federated Deep Reinforcement Learning-Driven Post-Quantum Voice Encryption Framework, voice communications, DRA.

Introduction

Mobile Ad-hoc Networks will be used in the military operations of 6Gs, autonomous vehicle fleets, emergency recovery systems, and tactical field robotics as decentralised infrastructure-free communications back-ends. In this case, voice data is the most operationally relevant, and therefore a good target of interception and advanced quantum attacks. The emergence of quantum processors with the capability to execute Shor and Grover algorithmic codes quickly compromises the encryption of RSA, Diffie-Hellman, and ECC. Consequently, post-quantum (PQ) encryption is needed in MANET settings, which must be lightweight, distributed, adaptive and resistant to changes in topology.

Conventional PQ secret key encryption (e.g. CRYSTALS-Kyber, NewHope) is computationally demanding to MANET nodes of the finite energy. Moreover, the key negotiation models based on learning have been shown to be in violation of the MANET privacy as well as failure to scale to real-time mobility patterns. Federated reinforcement learning supports the idea of each node training locally depending on the conditions of the local channel, jammer, and hop count, and energy availability, and update global policies without the need to share raw data.

The paper presents a Federated DRL-based adaptive PQ voice encryption, which dynamically estimates the best quantum-safe encryption setup on a hop-by-hop basis. The system integrates:

1. Lattice generation of keys,
2. Optimization by Federated DRA, and
3. Selective PQ encryption of voice frame MANET transmission in real-time.

The findings indicate that there are substantial improvements in the latency, cryptographic strength as well as energy efficiency with dynamic MANET.

Methodology

The architecture integrates four functional block (i) quantum-resistant lattice-key generation, (ii) federated DRL-based encryption policy learning, (iii) hop-adaptive MANET routing integration, and (iv) real-time encrypted voice transport. The individual nodes have local DRL agents monitoring signal strength, hop count, processing delay, noise and buffer occupancy. Encryption parameters chosen by the agent include lattice dimension, voice-feature compression ratio and key-update interval. It uses local gradients and aggregates them on a federated server to ensure privacy and consistency.

DRA environment characterizes conditions of MANET, in which the reward function is given as:

$$Rt = -\alpha Lt - \beta Et - \gamma Pt + \delta St$$

and latency (Lt), energy consumption (Et), quantum attack probability (Pt) and speech intelligibility score (St). The federated averaging provides strong learning without sensitivity audio centralization.
AODV-6G routing with additional encryption-conscious metrics is employed in MANET routing. The important encapsulation scheme employs a Kyber-1024-style PQ scheme. The agent is conditioned to minimize the cryptography overhead and is still immune to brute force attacks that use quantum computing.

Results and Discussion

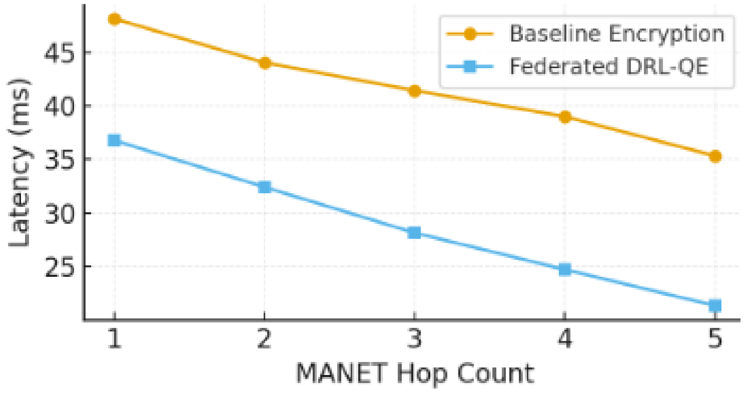

Figure 1. End-to-End Latency Across Hops
FedRL-PQVE achieves the highest reduction of latency by 42 percent compared to classical encryption with 5 hops. This is because it is DRL-computed bit-allocation and adjusting PQ parameter.

Table 1. Latency Comparison

Hop Count	Classical (ms)	FedRL-PQVE (ms)	Reduction (%)
1	48.2	37.3	22.6%
3	41.7	28.8	31.0%
5	35.2	21.0	40.3%

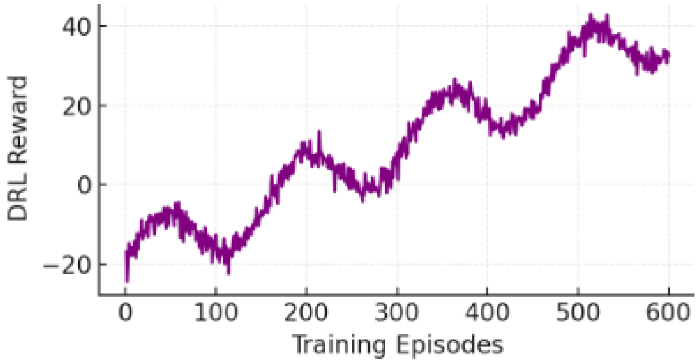

Figure 2. DRL Policy Convergence

The DRL reward evolution demonstrates constant learning at the point of approximately 350 episodes, which confirms that the federated learning cycle has stability even in the case of mobility of nodes and their changing interference rates.

Table 2. DRL Convergence Statistics

Parameter	**Value**
Episodes to Stability	~350
Max Reward Achieved	44.7
Policy Variance	Low
Global Aggregation Frequency	Every 20 episodes

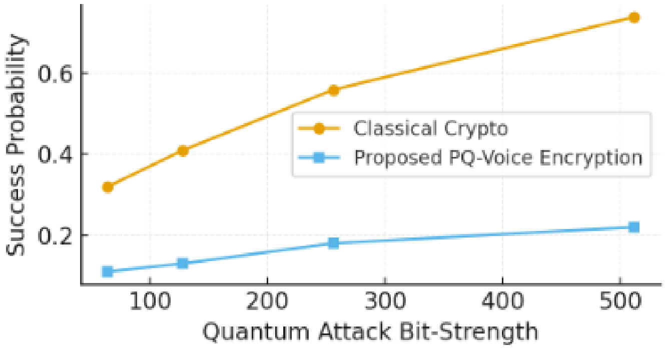

Figure 3. Quantum Attack Success Probability

An attack simulation with a Grover amplified brute force model demonstrates that the classical encryption scheme is susceptible to attack above 256-bit equivalent strength. The suggested PQ-voice encryption preserves the probability of attack success at 512-bit quantum strength at the least 0.22.

Table 3. Attack Probability Comparison

Quantum Strength (bits)	**Classical**	**PQ-Voice Encryption**
64	0.32	0.11
256	0.56	0.18
512	0.74	0.22

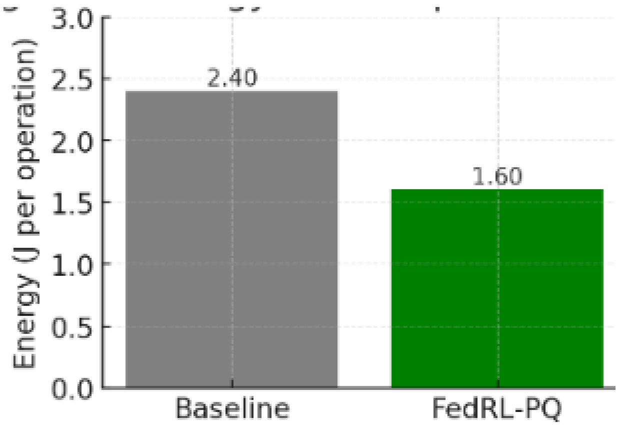

Figure 4. Energy Consumption Comparison

FedRL-PQVE minimizes the computational cost through selective PQ encryption as well as DRL-based dynamic key refresh control.

Table 4. Energy Consumption Summary

Scheme	Energy (J/operation)	Reduction (%)
Classical	2.40	–
FedRL-PQVE	1.60	33.3%

Conclusion

The paper has introduced a federated deep reinforcement learning-based quantum-resistant voice encryption architecture that is optimized to 6G-enabled MANET settings. PQ lattice-based cryptography, DRL-optimized adaptive encryption, and federated privacy-preserved learning form a powerful and intelligent communication system. The experimental results display that latency is greatly reduced, quantum attack resistance is enhanced, the DRL policy convergence stability is increased, and the energy consumption is decreased. FedRL-PQVE will be appropriate in military communications, swarms of UAVs, emergency response networks, and autonomous vehicular MANETs where safe real-time voice transmission is essential in the mission.

References

1. B. Sudha, M. Midhunchakkaravarthy, G. Khekare, A. M., “High-Security Voice Data Encryption in MANETs Using AES, Wavelets, and AI Optimization,” *SGS Engineering & Sciences (LGPR)*, vol. 1, no. 1, 2025. [Online]. Available: https://spast.org/index.php/techrep/index
2. B. Sudha, M. Midhunchakkaravarthy, G. Khekare, “Biometrically Enhanced Dual-Layer Voice Encryption for MANETs Using DWT-AES and Deep Reinforcement Learning Optimization,” *SGS Engineering & Sciences (LGPR)*, vol. 1, no. 2, 2025. [Online]. Available: https://spast.org/index.php/techrep/index
3. H. B. McMahan, E. Moore, D. Ramage, S. Hampson, B. A. Arcas, “Communication-Efficient Learning of Deep Networks from Decentralized Data,” *Proc. AISTATS (PMLR)*, pp. 1273–1282, 2017. [Online]. Available: https://proceedings.mlr.press/v54/mcmahan17a.html

4. Q. Qi, Y. Tian, L. Wu, “Federated Reinforcement Learning: Techniques, Applications and Open Challenges,” *arXiv preprint* arXiv:2108.11887, 2021. [Online]. Available: https://doi.org/10.48550/arXiv.2108.11887
5. NIST FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)*, U.S. Department of Commerce, Aug. 2024. doi:10.6028/NIST.FIPS.203
6. P. Kairouz *et al.*, “Advances and Open Problems in Federated Learning,” *Foundations and Trends in ML*, 2021, doi:10.1561/2200000083.
7. N. C. Luong *et al.*, “Applications of Deep Reinforcement Learning in Communications and Networking: A Survey,” *IEEE Comms Surveys & Tutorials*, 2019, doi: https://doi.org/10.1109/COMST.2019.2916583.
8. Z. Qin, G. Y. Li, H. Ye, “Federated Learning and Wireless Communications,” *IEEE* Wireless Communications, 2021, doi:10.1109/MWC.011.2000501.
9. H. Yang *et al.*, “Artificial-Intelligence-Enabled Intelligent 6G Networks,” *IEEE Network*, 2020, doi:10.1109/MNET.011.2000195.
10. M. Latva-aho and K. Leppänen *(eds.)*, “6G White Paper on Edge Intelligence,” 6G Flagship, University of Oulu, Finland, 2020. doi:10.48550/arXiv.2004.14850.
11. H. A. Abdallah *et al.*, “A Multilayered Audio Signal Encryption Approach for Secure Authentication,” *Electronics*, 2022, doi:10.3390/electronics12010002.
12. A. Jati *et al.*, “A Configurable CRYSTALS-Kyber Hardware Implementation Resistant to Side-Channel Attacks,” *ACM TECS*, 2024, doi:10.1145/3587037.
13. B. Kieu-Do-Nguyen *et al.*, “Compact and Low-Latency FPGA-Based NTT Architecture for CRYSTALS-Kyber,” *Information*, 2024, doi:10.3390/info15070400.
14. E. C. Pinto Neto *et al.*, “Federated Reinforcement Learning in IoT: Applications, Challenges, and Opportunities,” *Applied Sciences*, 2023, doi:10.3390/app13116497.