INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 8, August 2026 | ISSN: 2456-4184 | IJNRD.ORG

A Lightweight Post-Quantum Cryptographic Framework for Secure Robot-to-Robot and Robot-to-Cloud Communication in Internet of Robotic Things

By

Oyebisi Lukman Oluremi loyebisi@gmail.com [1], **Fasina Temilade Temitope** temiladefasina@gmail.com [2], **Osedahunsi Victor Olayiwole** yungaaeronaut@gmail.com [3], **Dr. Sakpere Wilson** sakpere.wilson@lcu.edu.ng [4]

[1] Department of Computer and Information Science, Lead City University, Ibadan
[2] Department of Computer Scienc, Lead City University, Ibadan
[3] Department of Software Engineerin, Lead City University, Ibadan
[4] Department of Computer Science, Lead City University, Ibadan

Abstract

Internet of Robotic Things (IoRT) systems combine mobile robots, sensors, actuators, edge gateways and cloud services, but their communication channels expose them to packet sniffing, spoofed command injection, replay attacks and long-term cryptographic risk. This article suggests a lightweight post-quantum cryptographic system for secure communication between robots and cloud service in resource constrained IoRT environment. The framework integrates ML-KEM for quantum-resistant key establishment with Ascon-AEAD128 for low-overhead authenticated encryption of telemetry, command and control messages. It also maintains crypto-agility with a hybrid migration plan that enables classical elliptic-curve mechanisms to be interoperable with post-quantum key encapsulation during the transition period. The proposed architecture is evaluated conceptually by means of a simulation-ready benchmarking design, using ROS 2, Gazebo and microcontroller-class robotic nodes. The evaluation model compares the proposed ML-KEM/Ascon configuration with AES-GCM baselines and RSA/ECC baselines in terms of latency, throughput, random-access memory, packet overhead, energy cost and attack resilience. The article contributes a threat-driven architecture, an implementation model, a performance-evaluation matrix and deployment recommendations for autonomous, industrial and healthcare robots. It suggests that the quest for post-quantum security in a robot should not be considered a cloud-only challenge, as robots are often used for a long time, and they have safety-critical actuations and heterogeneous hardware constraints. The proposed framework offers a timely solution for secure, standards-compliant, and lightweight migration of cryptographic system in IoRT systems.

Keywords: *Internet of Robotic Things; post-quantum cryptography; ML-KEM; Ascon; ROS 2; lightweight security; robot communication*

INTRODUCTION

Robotics has evolved from a world of stand-alone programmable robots to a world of networked cyber-physical systems that share sensor data, instructions, maps and safety-critical control messages over local networks, edge gateways and cloud services. The Internet of Robotic Things (IoRT) is an extension of the IoT concept which integrates robotic autonomy with sensing, actuation, cloud analytics and human supervision. This convergence enhances scalability and intelligence but exposes greater vulnerability to cyberattacks: if a communication link is compromised, compromising the information is not the only concern, but so is the physical movement, service continuity, and human safety.

Recent surveys of the robotic cyber security landscape highlight network and operating system attacks, as well as attacks on the middleware, as top threat types, especially for robots that rely on ROS-based software, cloud interfaces and wireless communication. The works of Botta et al. (2023) and Zafir et al. (2024) highlight the need to consider security at multiple layers, including physical, operating-system, and network security, as well as security-by-design in IoRT. The results suggest that cryptographic protection cannot be integrated subsequently into the robot communication stack, but should be built in from the beginning.

The need to redesign cryptographic systems has increased due to quantum computing, which poses a threat to the mathematical basis of RSA and elliptic-curve cryptography. NIST has thus standardized post-quantum cryptography, such as ML-KEM for key encapsulation, and ML-DSA and SLH-DSA for digital signatures (Alagic et al., 2022; National Institute of Standards and Technology, 2024a, 2024b, 2024c). Meanwhile, there are devices that are constrained, yet still require lightweight symmetric cryptography. NIST SP 800-232 standardises the Ascon family, including Ascon-AEAD128, as a lightweight authenticated-encryption primitive for resource-constrained environments (National Institute of Standards and Technology, 2025; Turan et al., 2025).

This article tackles the research issue of providing quantum resistance to many IoRT deployments without simply swapping out existing cryptographic stacks with more computationally intensive ones. The proposed study therefore asks how a hybrid ML-KEM/Ascon framework can secure robot-to-robot and robot-to-cloud communication while remaining feasible for embedded robotic nodes. The goals are to design a lightweight post-quantum communication architecture, compare it with the baseline of RSA/ECC and AES-GCM, evaluate key performance metrics, and propose a deployment model for autonomous, industrial and healthcare robots.

2. BACKGROUND/LITERATURE REVIEW

2.1 Internet of Robotic Things and Communication Risk

Unlike conventional IoT systems, IoRT systems are capable of sensing, deciding and acting in a dynamic physical environment. A malicious packet can thus cause operational effects like unsafe navigation, false object recognition, misalignment of the manipulator or loss of teleoperation. In the field of long-term care, which requires safeguarding of private resident information and continuity of services, Chang et al., (2023) show the relevance of secure IoRT. Likewise, in industrial robotics and cloud robotics, communication is vital as remote analytics, fleet coordination and firmware updates rely on trusted communication channels.

Robotic middleware boosts interoperability but also provides a common attack surface. ROS 2 improves on ROS 1 by supporting DDS security plugins for authentication, encryption and access control, and its documentation emphasises policy-based protection using security artefacts and environment configuration (Open Robotics, 2024; Rescorla 2018). But with the security of DDS there is no reason why cryptographic agility can't be there as well. The key-exchange and certificate infrastructure surrounding a deployment might still rely on RSA or ECC, which could still be vulnerable in the future to quantum attacks. An IoRT design needs to thus include both current operational security and migration paths to post-quantum security.

2.2 Post-Quantum Cryptography for Robotic Systems

Post-quantum cryptography is designed to resist attacks by adversaries with cryptographically relevant quantum computers. The security of the ML-KEM is related to the Module Learning with Errors problem, and the parameter sets include ML-KEM-512, ML-KEM-768 and ML-KEM-1024 (National Institute of Standards and Technology, 2024a). For the IoRT, the value of ML-KEM is particularly significant, as it could be used to establish shared session secrets over an insecure channel, and then symmetric authenticated encryption could protect actual robot messages.

Digital signatures remain necessary for firmware, policy files, certificates and command authorisation. NIST FIPS 204 specifies ML-DSA, while FIPS 205 specifies SLH-DSA (National Institute of Standards and Technology, 2024b, 2024c). This article is not about firmware signing, but it places ML-KEM in a broader post-quantum migration agenda where the identities of robots, software updates and cloud gateways can gradually be switched to post-quantum signatures. The design also takes into account the fact that it is advisable to migrate in a hybrid fashion since it is not feasible to move all the legacy systems to post-quantum primitives at once.

2.3 Lightweight Cryptography and the Role of Ascon

Lightweight cryptography is essential where nodes have limited memory, battery capacity, processor speed and communication bandwidth. Ascon is important because it provides authenticated encryption with associated data, hashing and extendable-output functions using a compact permutation-based design. NIST SP 800-232 identifies Ascon-AEAD128, Ascon-Hash256, Ascon-XOF128 and Ascon-CXOF128 as standardised primitives suitable for constrained environments (National Institute of Standards and

Technology, 2025). Kaur et al. (2023) also discuss the implementation, attacks, and countermeasures of Ascon, emphasizing that lightweight security should not only focus on the algorithms' strength but also on attacks and side-channel and implementation security threats.

Ascon-AEAD128 is well suited to the IoRT requirements for short command packets, telemetry frames and sensor updates. Authenticated encryption protects confidentiality and integrity in one primitive and enables associated data such as topic name, robot identity, timestamp and sequence number to be authenticated even when it is not encrypted. This is useful for replay defence and command-context binding.

3. MAIN BODY OF TEXT

3.1 Threat Model

The proposed framework assumes an adversary who can observe, delay, replay, modify or inject packets over robot-to-robot, robot-to-edge and robot-to-cloud channels. The adversary can try to intercept the key establishment, replay old commands, send spoofed velocity or actuator commands, pretend to be a robot node, or eavesdrop on encrypted traffic for future decryption. The framework also does not cover full hardware tamper resistance, but it is possible to physically capture a low-end robot. Security objectives include: Confidentiality, Integrity, Origin Authentication, Freshness, Forward Looking Quantum Resistance, and Acceptable Performance on Constrained Nodes.

3.2 Proposed ML-KEM/Ascon Framework

The framework is organised into four layers. The identity layer associates cryptographic credentials with each robot node, gateway and cloud endpoint. The key-establishment layer is responsible for encapsulating a shared secret by means of ML-KEM, possibly followed by a classical ECDH secret during transition. The session-protection layer uses the shared secret to generate message keys, and uses Ascon-AEAD128 for command, telemetry and state messages. The monitoring layer records handshake status, failed authentication events, replay rejection and cryptographic cost for audit and anomaly detection. Figure 1 summarises the architecture.

Proposed post-quantum lightweight IoRT communication framework

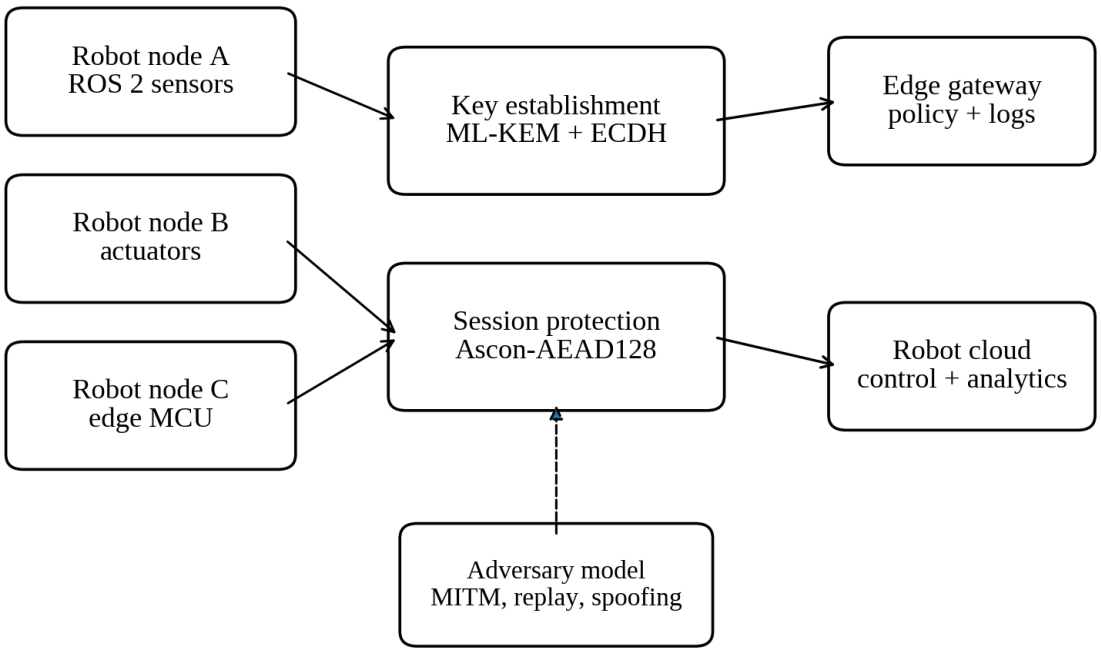

Figure 1: Proposed post-quantum lightweight communication framework for IoRT

A typical session begins when Robot A requests a secure channel with Robot B or a cloud endpoint. The receiver shares an ML-KEM public key or a short-lived certificate that includes the public key. Both parties use a key-derivation function to produce a session key; the sender uses ML-KEM to encrypt a shared secret and sends the ciphertext. In hybrid mode, a classical ECDH shared secret is concatenated with the ML-KEM secret before key derivation so that the channel remains protected if one family of assumptions is later weakened. After key confirmation, each packet is encrypted with Ascon-AEAD128 using a unique nonce, associated data and a session sequence number.

3.3 Algorithmic Design

The proposed protocol uses the following high-level sequence: (i) initialise robot identity and policy; (ii) exchange endpoint capabilities; (iii) perform ML-KEM encapsulation and decapsulation; (iv) derive two traffic keys for bidirectional communication; (v) encrypt all command and telemetry payloads using Ascon-AEAD128; (vi) reject packets with invalid tags, old sequence numbers or unauthorised topics; and (vii) rotate session keys after a configurable time or packet threshold. The framework intentionally

separates key establishment from message encryption to avoid having to perform the asymmetric post-quantum operation for each packet.

The design supports deployment in ROS 2 by placing the post-quantum handshake at the secure-transport boundary and using topic-level policy information as associated data. It can also be deployed to microcontroller-class nodes by performing ML-KEM operations on an edge gateway, while leaving Ascon-protected links between the edge gateway and resource-constrained devices. When a small sensor-actuator module is incapable of performing post-quantum operations directly, but still requires authenticated encryption, this split deployment can be helpful.

3.4 Evaluation Methodology

The recommended evaluation is experimental and simulation-based. A ROS2 and Gazebo testbed can simulate the exchange of navigation commands, sensor updates and status reports between a TurtleBot or differential-drive robot. The edge-class robots can be represented by a Raspberry Pi or similar single-board computer and the constrained actuator endpoints can be represented by an ESP32 or an Arduino device. Baseline configurations should include RSA/ECC-based key exchange with AES-GCM and the proposed ML-KEM/Ascon design. Man in the middle attacks, replay attacks, packet sniffing, spoofed command injection and unauthorised topic publication should be included in attack scenarios (Dworkin, 2007).

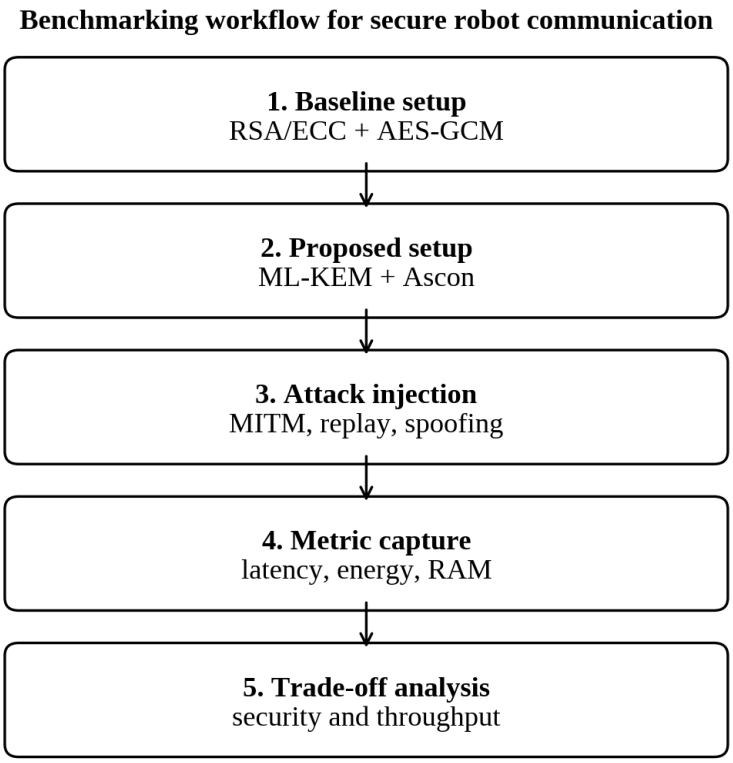

Figure 2: Benchmarking workflow for evaluating the proposed IoRT cryptographic framework

Metric	Operational definition	Relevance to IoRT
Handshake latency	Time between secure-channel request and usable session key	Affects robot start-up, failover and dynamic teaming
Packet latency	Time added by authenticated encryption and verification per message	Affects control-loop responsiveness
Energy consumption	Power cost per handshake and per encrypted packet	Determines battery impact on mobile robots
Memory footprint	RAM and flash required by cryptographic library and buffers	Determines feasibility on embedded nodes
Throughput	Encrypted payload delivered per second	Affects map, video and telemetry transfer
Attack rejection rate	Proportion of injected/replayed/spoofed packets rejected	Measures security effectiveness under adversarial traffic

Table 1: Proposed evaluation metrics for the ML-KEM/Ascon IoRT framework

3.5 Security Analysis

The framework provides better confidentiality by generating new session keys using ML-KEM and by encrypting each protected packet using authenticated encryption. It enhances integrity by ensuring that valid Ascon authentication tags and Ascon topic-bound associated data are provided. It enhances the freshness with nonces, sequence numbers and rejection windows. It also decreases future quantum exposure since the shared secret is created using a post-quantum KEM, not just RSA or ECC. This is particularly important for long-lived robots in healthcare, manufacturing and public infrastructure because recorded traffic may remain sensitive after current cryptographic assumptions weaken.

The framework does not aim to address all issues in robotic security. Physical capture, unsafe control logic, vulnerable firmware and poorly managed credentials can still undermine a deployment. So, the cryptographic model should be embedded in the secure boot, signed updates, least-privilege ROS 2 policies, network segmentation and runtime anomaly detection. However, the proposed design fills a major missing link: it provides a lightweight and standard way for IoRT deployments to enter the realm of post-quantum secure communication.

3.6 Deployment Recommendations

In cases where processor and memory resources are available, autonomous mobile robots should directly utilize the ML-KEM/Ascon. The framework should be implemented in a gateway-first approach, enabling the production cells to move in stages without impacting legacy controllers. However, due to the involvement of sensitive personal data and human safety, it is crucial that healthcare robots pay attention to certificate management, patient-data confidentiality and audit logging. In all cases, deployment should begin with a cryptographic inventory, followed by pilot benchmarking, hybrid mode, staged certificate migration and periodic key-rotation tests.

3.7 Limitations and Future Research

This article presents only a framework and benchmarking design—the actual implementation results will depend on the specific hardware, compiler, cryptographic library and middleware configuration. Future work should follow this framework by using liboqs, embedded Ascon libraries and ROS 2/DDS security hooks and report measured latency, memory, energy and attack-resilience values. Further studies should focus on side-channel resistance, secure key storage, post-quantum certificates and safety validation in which the cryptographic rejection of packets is coupled with real time control loops.

4. CONCLUSION

In this article, a lightweight post-quantum cryptographic framework for secure communication in IoRT systems is presented. The framework uses ML-KEM for quantum-resistant key establishment, authenticated encryption with Ascon-AEAD128, and maintains hybrid crypto-agility for ease of migration for practical use. It addresses the dual requirements for robustness to cryptographic attacks while being low overhead for use on constrained hardware. The architecture, threat model and evaluation matrix can be published and used for empirical tests in ROS 2, Gazebo and embedded robot platforms. The central contribution is a standards-aligned pathway for securing robot-to-robot and robot-to-cloud communication against present network attacks and future quantum threats

REFERENCES

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D., & Vassilev, A. (2022). Status report on the third round of the NIST Post-Quantum Cryptography Standardization Process. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8413

Botta, A., Rotbei, S., Zinno, S., & Ventre, G. (2023). Cyber security of robots: A comprehensive survey. *Intelligent Systems with Applications*, *18*, 200237.

Chang, S. H., Hsia, C. H., & Hong, W. Z. (2023). A secured internet of robotic things (IoRT) for long-term care services in a smart building. *The Journal of Supercomputing*, *79*(5), 5276-5290. https://doi.org/10.1007/s11227-022-04845-1

Dworkin, M. (2007). Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-38D

Kaur, J., Canto, A. C., Kermani, M. M., & Azarderakhsh, R. (2023). A comprehensive survey on the implementations, attacks, and countermeasures of the current NIST lightweight cryptography standard. *Cryptography*, 7(3), 31.

National Institute of Standards and Technology. (2024a). Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203). https://doi.org/10.6028/NIST.FIPS.203

National Institute of Standards and Technology. (2024b). Module-Lattice-Based Digital Signature Standard (FIPS 204). https://doi.org/10.6028/NIST.FIPS.204

National Institute of Standards and Technology. (2024c). Stateless Hash-Based Digital Signature Standard (FIPS 205). https://doi.org/10.6028/NIST.FIPS.205

National Institute of Standards and Technology. (2025). Ascon-Based Lightweight Cryptography Standards (SP 800-232). https://doi.org/10.6028/NIST.SP.800-232

Open Robotics. (2024). ROS 2 Security. https://docs.ros.org/en/rolling/Concepts/Intermediate/About-Security.html

Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. *RFC, 8446*, 1-160.

Turan, M. S., McKay, K., Chang, D., Bassham, L., & Kang, J. (2025). Ascon-Based Lightweight Cryptography Standards. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-232

Zafir, E. I., Akter, A., Islam, M. N., Hasib, S. A., Islam, T., Sarker, S. K., & Muyeen, S. M. (2024). Enhancing security of Internet of Robotic Things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques. *Internet of Things*, *28*, 101357. https://doi.org/10.1016/j.iot.2024.101357