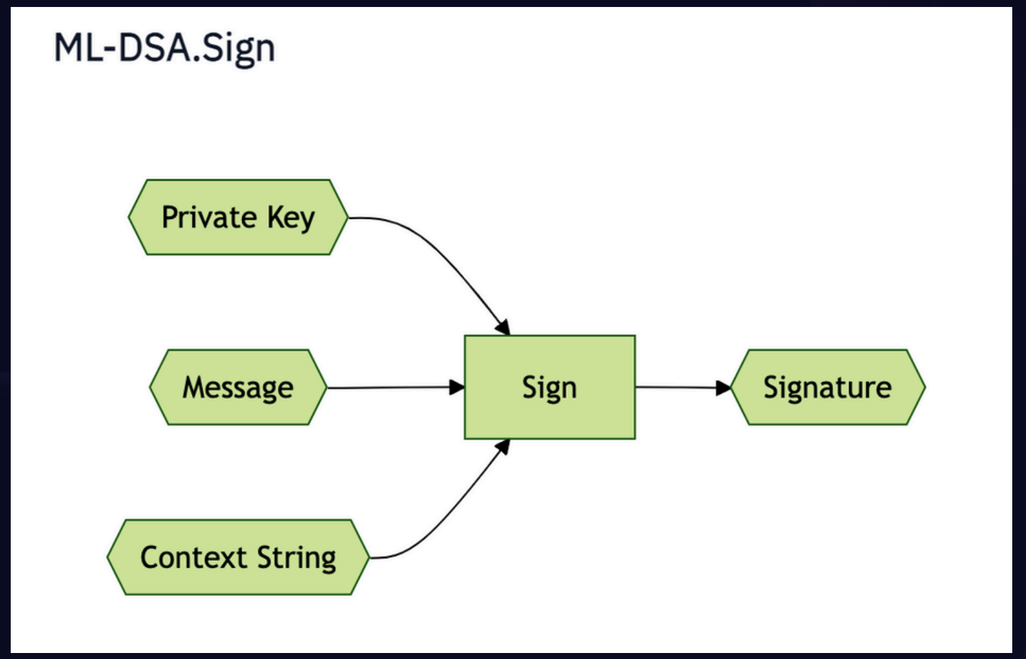
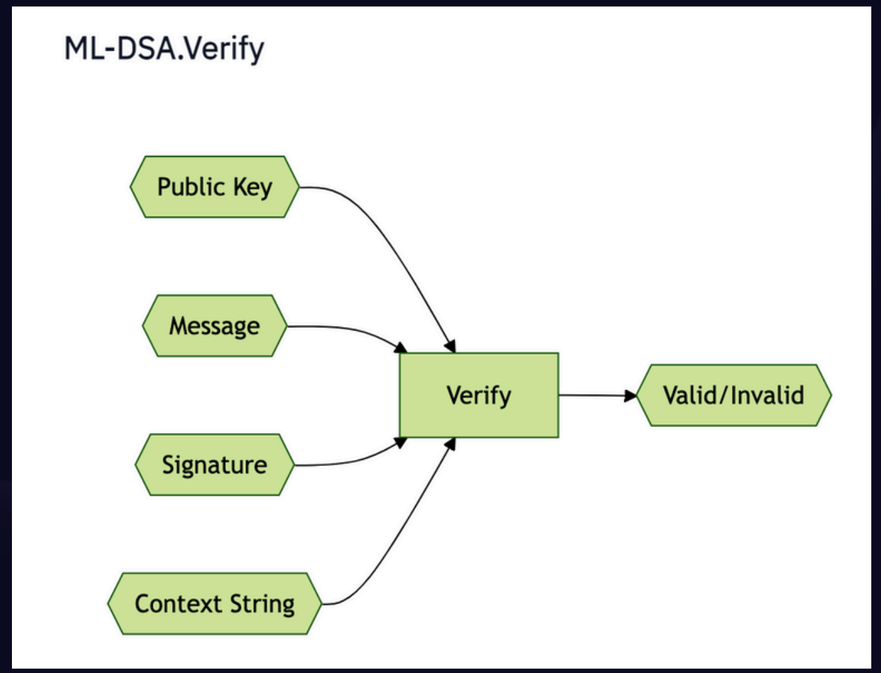
Performance Analysis of Post-Quantum Signatures (ML-DSA-44) for Securing Distributed Industrial Data

Implementation of PQC in a Vehicle Assembly Line (ML-DSA-44)

Rohith Ganesh Kanchi

S.D Madhumitha





Securing Industrial Systems in the Quantum

The Need for Data Integrity

Vehicle assembly lines generate critical data essential for safety, quality control, and regulatory compliance. Ensuring authenticity and integrity of such data is vital to operational trust.

The Quantum

Emerging quantum computers threaten classical public-key cryptography through Shor's Algorithm, rendering RSA and ECDSA insecure for signatures.

Post-Quantum Cryptography (PQC) Response

ML-DSA-44, based on CRYSTALS-Dilithium, is a leading quantum-resistant signature algorithm standardized by NIST (FIPS 204), targeting security comparable to AES-128.

Architecture 1: Centralized Orchestration

Process Workflow

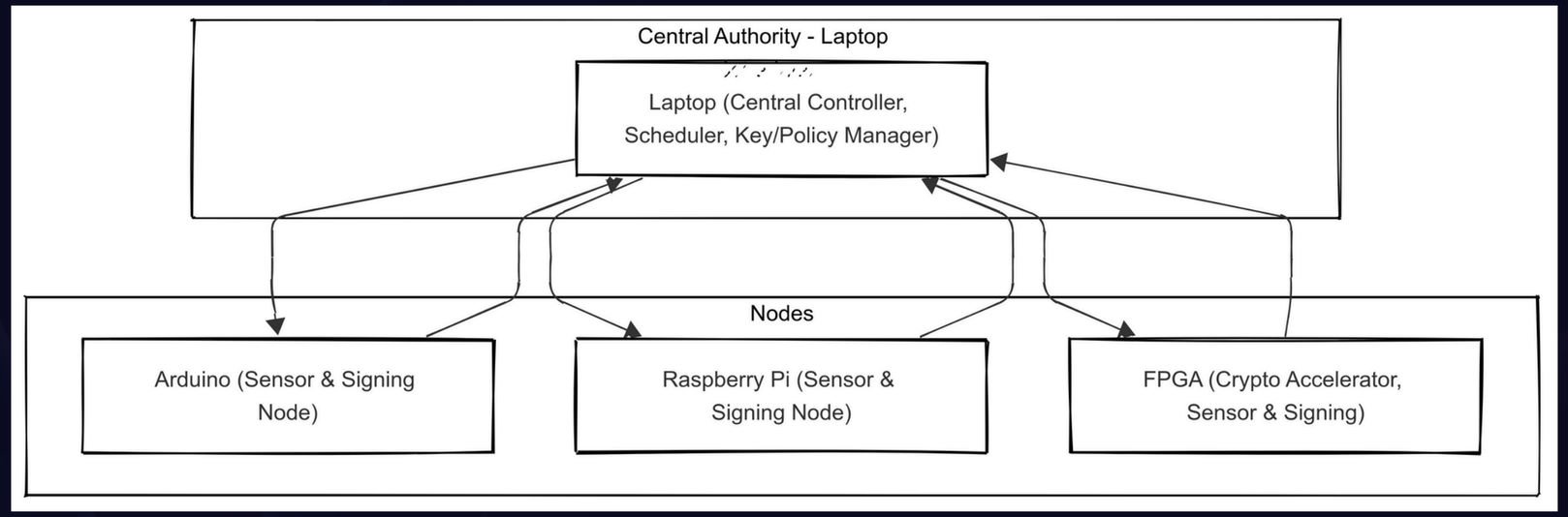
Sensors send unsigned data to a central Controller which delegates signing tasks to external Signer devices and gathers signatures for verification.

Advantages

- Enables sensors with limited computational capabilities.
- Utilizes dedicated powerful signing hardware.

Critical Flaws

- Unsigned data transmitted between sensor and Controller is vulnerable to tampering.
- Controller acts as a single complex bottleneck point.



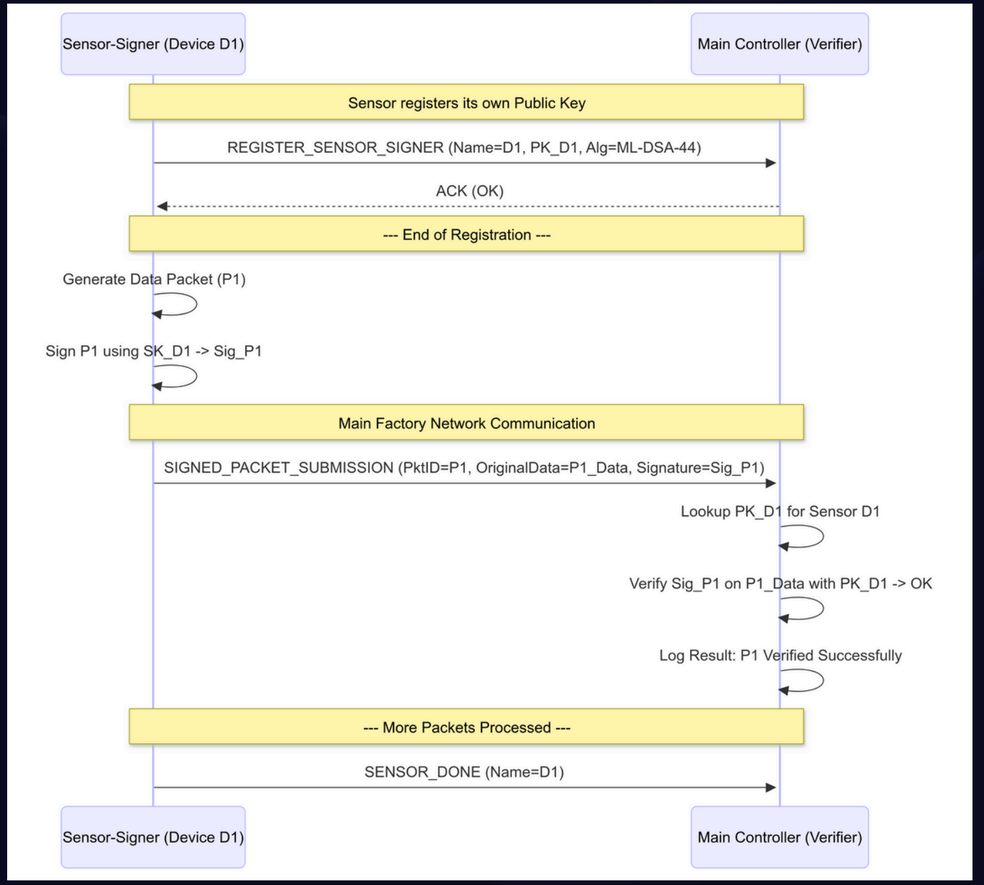
Architecture 2: Sensor-as-Signer (Direct Signing)

Secure-by-Design at Data Origin

Sensors locally sign entire data packets immediately upon generation, ensuring data integrity before transmission.

Benefits

- Detectable tampering during channel transmission.
- Simplified controller verification logic and less network traffic.



Limitations

Requires sensors to have substantial computational power to perform ML-DSA signing.

Architecture 3: Sensor Subsystem (Refined Model)

Design Concept

The sensor coordinates local trusted signers (e.g., Raspberry Pi or FPGA units) over a secure wired network, distributing signing load before sending authenticated data to the main Controller.

Advantages

- Protects data integrity within local subsystem.
- Offloads computational burden from sensor core.
- Leverages secure wired connections for subsystem communication.

Challenges

Increased system complexity for sensor coordination and subsystem infrastructure.

Note: This architecture (Arch 2 or Arch 3) was implemented in the simulation code for performance analysis.

Simulation Setup & Methodology

Core Technologies

Python 3 (asyncio) and pyca-oqs library for ML-DSA-44 algorithm implementation simulate signing and verification.

Components

- Sensor generates data and performs signing or coordination.
- Controller verifies signatures and logs results.
- Local signers operate in Arch 3 for distributed signing.

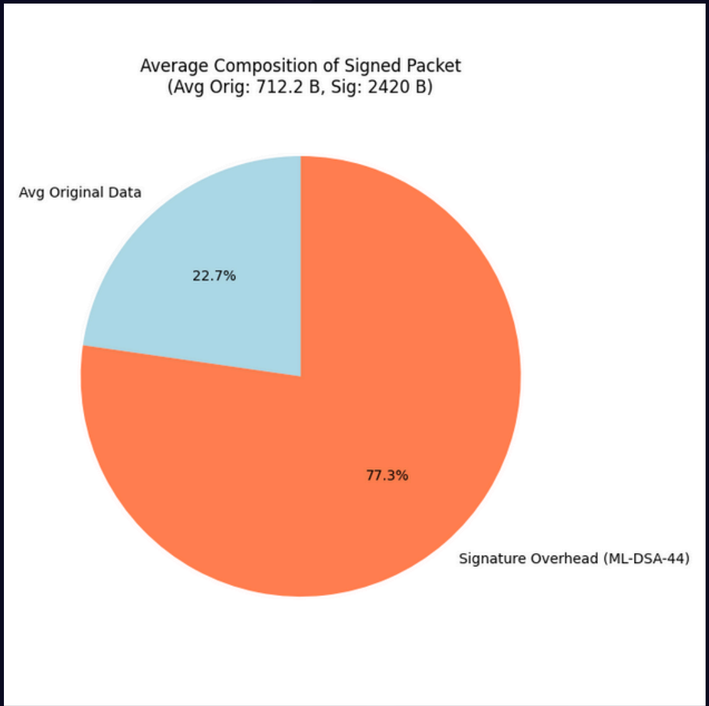
Network Simulation

Bandwidth constraints and latency modeled, reflecting realistic IoT communication delays. Logs from simulations analyzed using custom scripts.

Packet Size & Signature Overhead (ML-DSA-44)

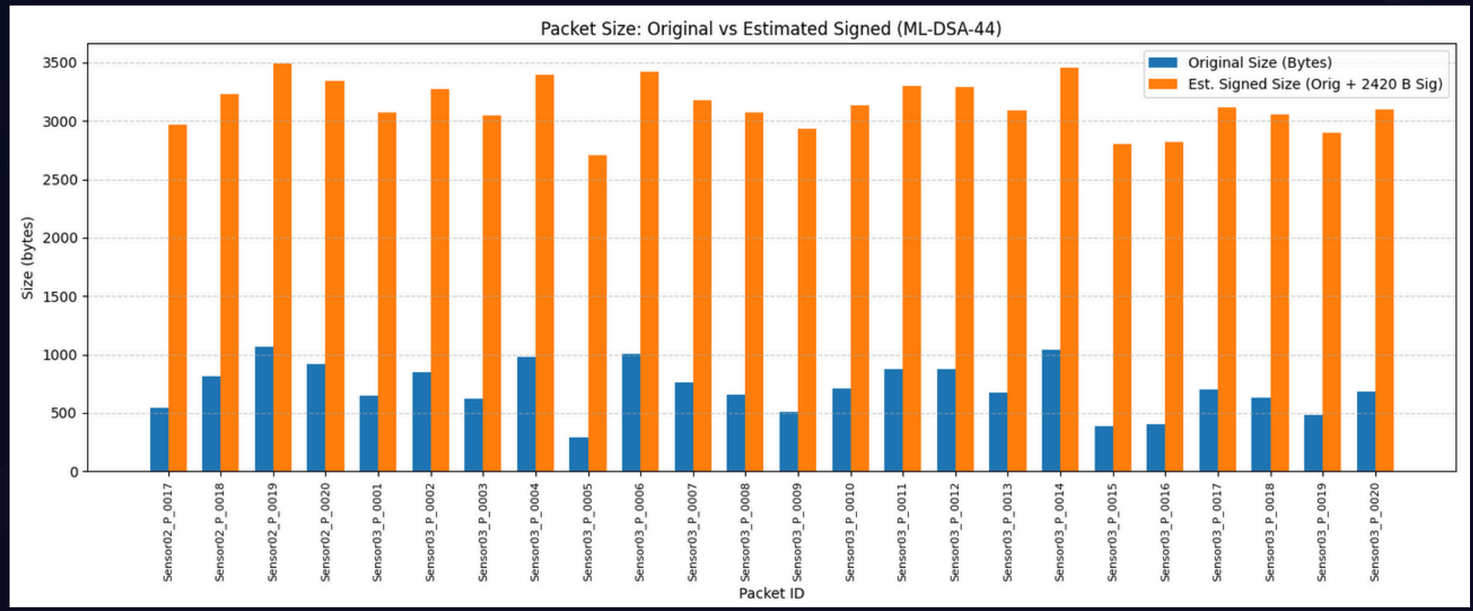
PQC Signature Impact

Each ML-DSA-44 signature adds 2420 bytes. This significantly inflates packet sizes, especially for small original sensor packets.

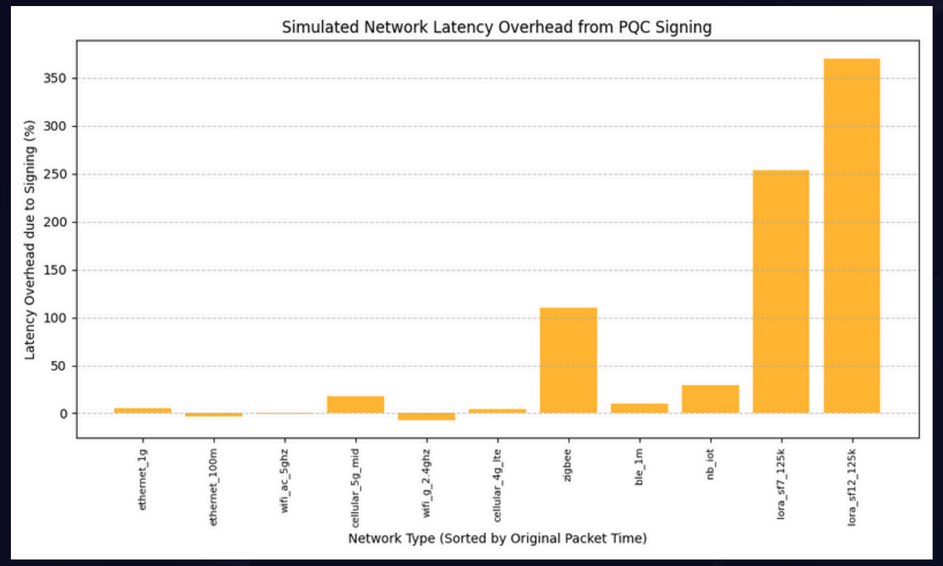


Simulation Insights

- Original average packet size: Varies by payload (50-900 bytes).
- Average number of signatures per packet depends on architecture.
- Overall packet size expansion ratio approaches ~4.8x in some cases

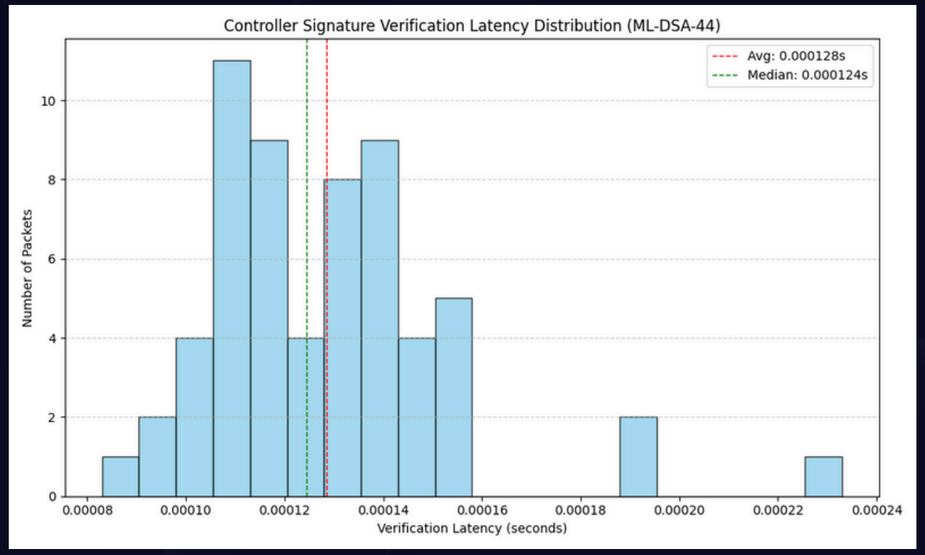


Performance Analysis: Latency & Network Impact



Network Transfer

The large PQC packet sizes significantly increase transmission times over constrained networks such as LoRa and NB-IoT, causing latency increases sometimes exceeding 1000%.



Verification Latency

Controller signature verification is highly efficient, averaging around 0.13 ms per packet, affirming fast computational performance of ML-DSA-44 on typical hardware.

Key Findings & Discussion

1

Security Imperative

Signing at source (Arch 2 or 3) is essential to prevent undetected data tampering, disproving the security of centralized baseline architecture.

2

Overhead Considerations

The 2.4 KB size per signature demands architectural optimization to mitigate network load and latency impact.

3

Hardware & Network Trade-

While verification is efficient, signing is computationally heavy and network bandwidth often constrains overall system latency.

4

Architecture Suitability

Choosing between Sensor-as-Signer and Sensor Subsystem models depends on device capability and scalability needs.