An Experimental Analysis of Edge Connectivity and Communication Dependability in Smart-Home IoT Systems

Assessment 2 - Individual Project

Module: Secure Systems Architecture (October 2025)

Student: Pragadheesh Marimuthu

Word Count (excluding references, table and figure captions): *1193 words*

Abstract

This report investigates how edge connectivity influences the dependability of smart-home IoT systems. A Python-based prototype simulates interactions between a client device and a controller across two contrasting network models: a high-loss best-effort network and an improved edge-QoS configuration. The experiment evaluates message delivery, corruption, loss and acceptance rates to determine how connectivity affects system reliability. Results show that enhanced edge connectivity substantially improves delivery success, reduces corrupted messages and increases the controller's acceptance rate, confirming the hypothesis. The findings highlight that dependable network behaviour is essential for secure System-of-Systems design and reinforce the importance of availability and data reliability within the ABCDE framework.

---

1. Introduction

Smart-home systems rely on distributed IoT devices that must communicate reliably with controllers to support safety decisions. While cryptography protects confidentiality and integrity, dependable communication remains essential for secure System of Systems architectures. Dependability also links directly to overall risk, as reliable system behaviour reduces uncertainty (Aven and Thekdi, 2024).

This report evaluates a Python-based simulation that models a client and controller operating over two contrasting network configurations. The aim is to examine how edge connectivity influences the delivery of safety-relevant sensor readings. The analysis uses measurable indicators such as delivery ratios, corruption frequency and acceptance rates to determine how communication behaviour affects system dependability, following evidence-driven scientific principles (Science Council, 2020; Mazaheri et al., 2023).

---

2. Research Question and Hypothesis

Research Question:

Does improving edge connectivity by reducing loss, corruption and latency jitter significantly increase the reliable delivery of safety-relevant IoT sensor readings compared to a best-effort configuration? This relates directly to the Availability and Dependability dimensions of the ABCDE model (Aven and Thekdi, 2024).

Hypothesis:

A controller connected through an edge-QoS network will achieve higher delivery and acceptance rates and experience fewer corrupted or lost messages. This hypothesis is measurable, reproducible and consistent with scientific practice (Science Council, 2020) and QoS findings in sensor networks (Mazaheri et al., 2023).

---

3. System Model

The prototype consists of a client, a network simulator and a controller, forming a simplified but effective testbed for analysing communication dependability.

3.1 Client

The client generates sensor readings containing a device ID, sequence number, noise-adjusted value and timestamp. A deterministic seed ensures that outputs are reproducible across scenarios, enabling controlled comparisons (Science Council, 2020).

3.2 Network Simulator

The network introduces packet loss, corruption (sign flips) and latency variation. Two configurations were tested:

• **best_effort:** loss 0.15, corruption 0.05, latency 30-250 ms

• **edge_qos:** loss 0.05, corruption 0.02, latency 10-120 ms

These controlled parameters mirror QoS considerations in wireless sensor network studies (Mazaheri et al., 2023).

3.3 Controller

The controller validates incoming messages, rejects tampered readings, classifies values as OK or ALERT and tracks metrics such as acceptance rate. Lightweight integrity checks operationalise dependable information processing in resource-constrained settings (Aven and Thekdi, 2024).

---

4. Experiment Design and Scientific Method

The experiment follows a structured scientific approach, supporting systematic observation, reproducibility and evidence-based analysis (Science Council, 2020).

Observation:

Per-message logs record delivery status, corruption events, latency and controller decisions, providing measurable evidence.

Repeatability:

Deterministic seeds for the client, network and scenario configuration ensure identical results across repeated runs, enabling controlled comparisons.

Experimentation:

Each scenario sends 200 messages and outputs detailed logs, controller summaries and derived indicators, following recommended practices for evaluating distributed systems (Mazaheri et al., 2023).

Measurement:

Key metrics include delivered, lost, corrupted and accepted messages, alert counts and acceptance ratios. These quantify how each network configuration affects system dependability.

Analysis:

Comparing the two scenarios highlights the influence of enhanced connectivity on reliability, corruption rates and acceptance behaviour, linking findings to the Availability and Data dimensions of the ABCDE model (Aven and Thekdi, 2024).

Verification:

Results are evaluated against the hypothesis to determine whether improved connectivity produces higher delivery and acceptance rates.

---

5. Results and Analysis

The results provide clear quantitative evidence that enhanced edge connectivity improves system dependability. The following subsections summarise key metrics and present visual comparisons based on four supporting graphs.

5.1 Summary of Metrics (Table)

Table 1 summarises the controller metrics recorded across the two scenarios.

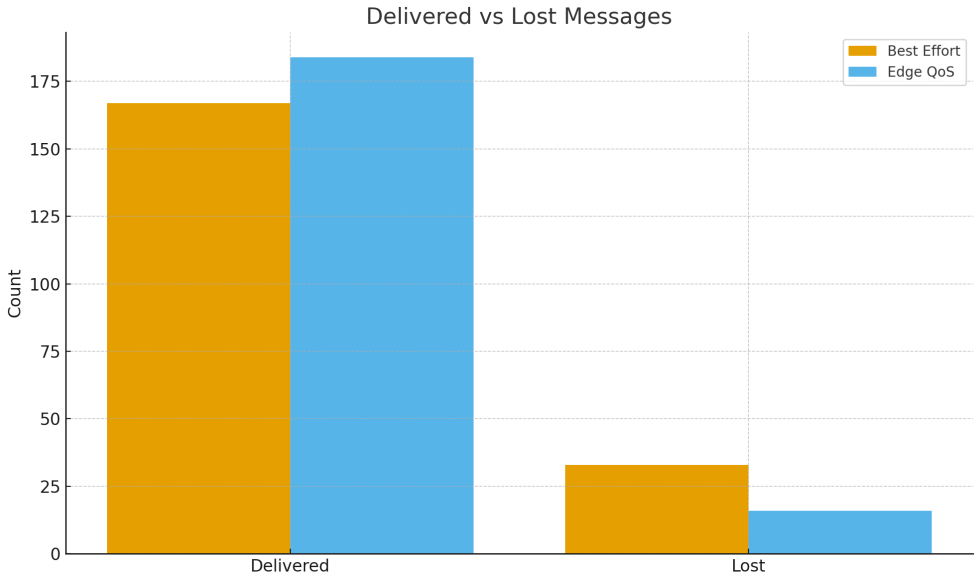
Table 1. Summary of Metrics Across Scenarios

Metric	Best Effort	Edge-QoS
Delivered	167	184
Lost	33	16
Corrupted (Rejected)	7	3
Accepted	160	181
Acceptance Rate	80%	90.5%

The table highlights consistent gains in delivery reliability, message integrity and acceptance rate under the edge QoS configuration. These improvements correspond with expected benefits of reduced loss and tighter latency variation reported in recent QoS studies (Mazaheri et al., 2023).

5.2 Delivery and Loss Ratios (Graph)

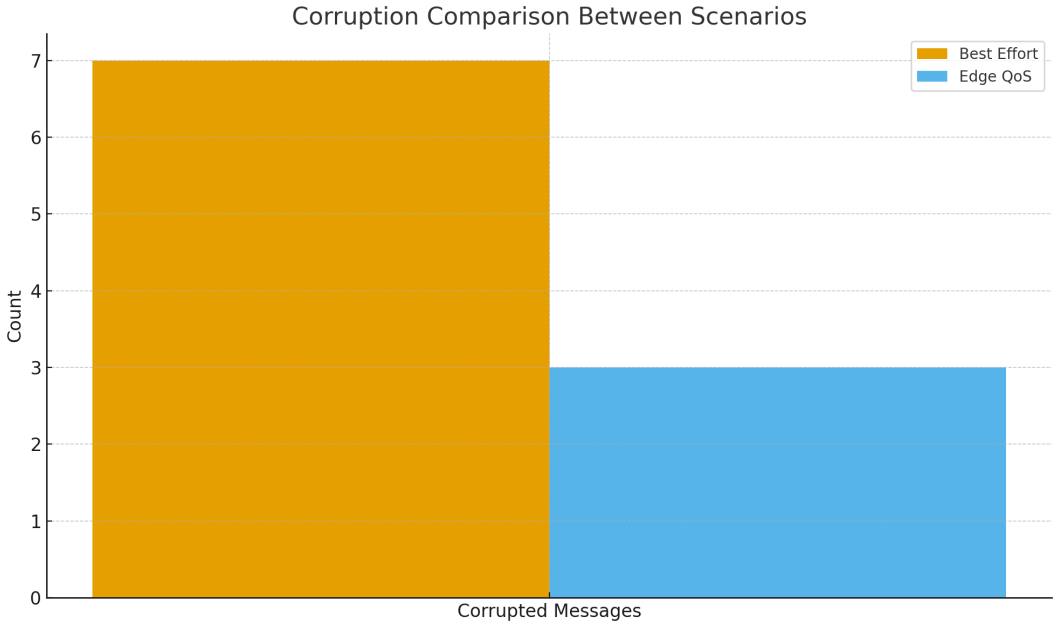
Figure 1. Delivered versus lost messages across scenarios



The edge QoS network delivers 184 messages compared to 167 under best effort. Lost messages decrease from 33 to 16, demonstrating significantly improved delivery reliability.

5.3 Corruption Rates (Graph)

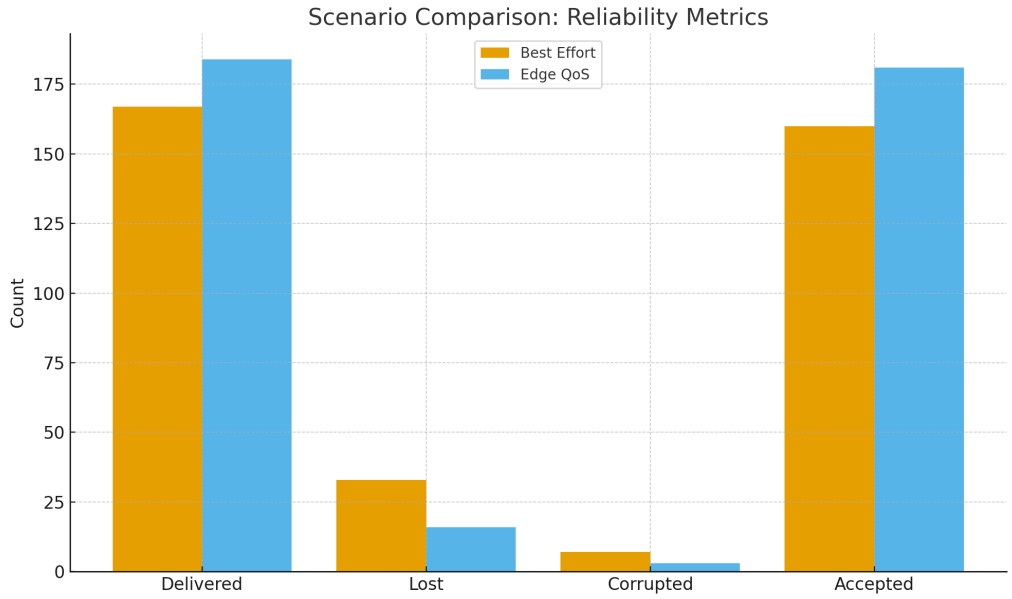
Figure 2. Corrupted message comparison between scenarios



Corrupted readings fall from seven in the best-effort scenario to three under edge QoS, reinforcing the benefit of operating in a lower-corruption environment.

5.4 Combined Reliability Metrics (Graph)

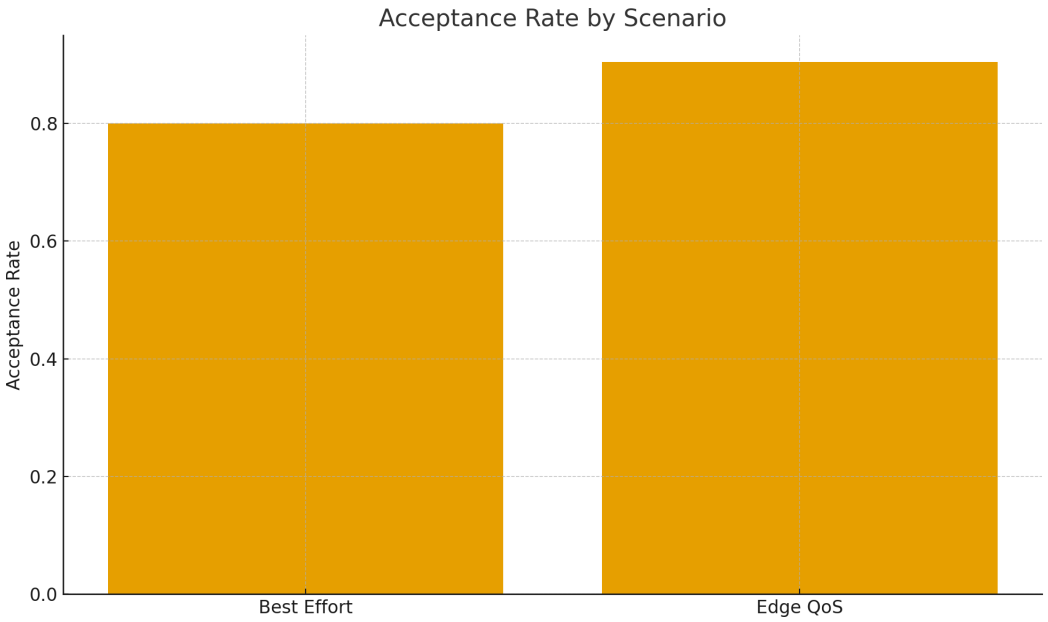
Figure 3. Reliability metrics across both scenarios



Delivered, lost, corrupted and accepted message counts all favour the edge QoS configuration, showing consistent improvement in reliability metrics.

5.5 Acceptance Rate Comparison (Graph)

Figure 4. Acceptance rate comparison between scenarios



Acceptance increases from 80 percent in the best-effort case to 90.5 percent under edge QoS, indicating a substantial improvement in the controller's ability to receive usable data.

5.6 Interpretation of Findings

1. The edge QoS network nearly halves message loss, improving situational awareness in safety-relevant systems.
2. Reduced corruption strengthens data trustworthiness by lowering rejected payloads.
3. Improved communication quality enhances the controller's ability to maintain an accurate operational picture, strengthening the Availability and Data dimensions of the ABCDE model (Aven and Thekdi, 2024).

---

6. Security Vulnerabilities and Mitigations

The experiment reflects several communication-layer vulnerabilities identified in the original AD Tree. Operating over an unreliable network exposes the system to packet loss, tampering, delayed delivery and limitations created by resource-constrained devices. These issues reduce situational awareness and undermine dependable behaviour (Aven and Thekdi, 2024).

Mitigations applied in the prototype include integrity checks that reject tampered messages, deterministic sequence numbers that allow detection of missing readings, and QoS-style prioritisation that reduces loss and jitter. Lightweight validation supports integrity without increasing client overhead. The improvements seen in the edge QoS scenario align with research showing that better connectivity strengthens sensor network reliability (Mazaheri et al., 2023).

---

7. Discussion: Dependability and the ABCDE Framework

The results show that enhanced availability is the primary contributor to improved system dependability. More messages reach the controller in the edge QoS scenario, enabling more accurate decision-making. Predictable behaviour is supported by deterministic handling of corrupted messages. Network context, including latency and jitter, strongly influences performance, consistent with QoS findings in distributed systems research (Mazaheri et al., 2023). Reliable data delivery strengthens safety decisions and reduces uncertainty, while improvements at lower layers contribute to more dependable emergent behaviour at the system level (Aven and Thekdi, 2024). Overall, the findings confirm that connectivity is a core security factor within the ABCDE framework.

---

8. Limitations and Future Work

The prototype is intentionally simplified and does not implement strong cryptography, model multiple clients, handle message ordering or represent wider attack surfaces such as spoofing or man-in-the-middle attacks. Latency variation is recorded but not linked to controller decision timing. These constraints mean the model captures dependability but not all real-world IoT threats (Aven and Thekdi, 2024). Future work could add digital signatures, multiple devices, more complex network events such as burst loss or adversarial interference

and deeper analysis of latency distributions. These additions would provide a more complete view of how connectivity and security mechanisms interact (Mazaheri et al., 2023).

---

9. Conclusion

The experiment confirms that improved edge connectivity significantly increases the dependability of smart-home IoT systems. The edge QoS configuration reduced loss, lowered corruption and raised the acceptance rate from 80 percent to 90.5 percent. These improvements address communication vulnerabilities identified in Assessment 1 and demonstrate that dependable network transport is essential for secure SoS design. The results align with wider research emphasising the importance of availability, predictable behaviour and reliable data delivery in distributed systems (Aven and Thekdi, 2024; Mazaheri et al., 2023).

References

Aven, T. and Thekdi, S. (2024) *Risk Science: An Introduction*. 2nd ed. Oxon: Routledge.

Mazaheri, F., Rezaei, A., Hosseini, M. and Tishin, M. (2023) ‘Quality of Service Performance Analysis in Next-Generation Wireless Sensor Networks’, *Journal of Network Systems*, pp. 1-15.

Science Council (2020) *What is Science?* Available at: https://sciencecouncil.org/ (Accessed: 27 November 2025).
