DETERMINISTIC EDGE CONTROL FOR AI AGENTS VIA MODEL CONTEXT PROTOCOL OVER MQTT

Simeon Monov, Emre Myumyun

Abstract. *The integration of Artificial Intelligence (AI) agents with the Internet of Things (IoT) represents a paradigm shift from static, rule-based automation to dynamic physical orchestration [1]. However, bridging probabilistic Large Language Models (LLMs) with deterministic hardware endpoints introduces severe reliability challenges, most notably the risk of models generating structurally invalid parameters during execution. To address this, we propose a standardized integration architecture utilizing the Model Context Protocol (MCP) over the Message Queuing Telemetry Transport (MQTT) protocol [2]. By explicitly constraining the AI's action space with strict JSON schemas, the framework prevents hallucinated or malformed commands. Transmitting these structured JSON-RPC payloads over MQTT ensures minimized jitter, high temporal consistency, and the deterministic low latency required for safe, reliable real-time edge computing.*

Key words: Autonomous Agents, Large Language Models, LLM, Model Context Protocol, MCP, MQTT, JSON-RPC, Edge Computing, IoT

Acknowledgments

This study is supported by the project SP25-FMI-008 "Research and implementation of modern language models and artificial neural networks for automated processing, forecasting, and structuring of data and texts in specific application domains" at the Paisii Hilendarski University of Plovdiv.

References

[1] A. Athanasopoulou, N. Fotiou, A. Chatzopoulos, Interacting with IoT Data Spaces Using LLMs and the Model Context Protocol, Sensors, vol. 26, pp. 1193, 2026

[2] N. Yang, G. Lyu, M. Ma, Y. Lu, Y. Li, Z. Gao, H. Ye, J. Zhang, T. Chen, Y. Chen, IoT-MCP: Bridging LLMs and IoT Systems Through Model Context Protocol, arXiv, Ithaca, 2025

Simeon Monov[1,*], Emre Myumyun[1]

[1] Paisii Hilendarski University of Plovdiv,
Faculty of Mathematics and Informatics,
236 Bulgaria Blvd., 4027 Plovdiv, Bulgaria
Corresponding author: smonov@uni-plovdiv.bg