

LIMITES OPERACIONAIS DO PROTOCOLO MQTT PARA SEGURANÇA INDUSTRIAL EM AMBIENTES IIoT

João Gustavo Mota Ramos¹; João Pedro da Cunha Machado²; Wesley Novaes Fioreze Costa³; Anderson Adelson de Matos⁴

¹ Escola e Faculdade de Tecnologia Senai Felix Guisard – joaogustavo2202@gmail.com

² Escola e Faculdade de Tecnologia Senai Felix Guisard – jotapepe.machado@gmail.com

³ Escola e Faculdade de Tecnologia Senai Felix Guisard – wesley.fioreze@docente.senai.br

⁴ Escola e Faculdade de Tecnologia Senai Felix Guisard – anderson.matos@sp.senai.br

Resumo: A quarta revolução industrial consolidou a Internet Industrial das Coisas (IIoT) como componente fundamental para a digitalização de plantas fabris, permitindo o monitoramento de ativos em tempo real e, com isso, a implementação de estratégias de manutenção preditiva. Não obstante, a transição de sistemas de controle tradicionais, condicionados a cabeamento estruturado e protocolos determinísticos, para redes sem fio baseadas em protocolos de internet, como o Message Queuing Telemetry Transport (MQTT), introduz desafios relacionados à incerteza temporal. Em ambientes industriais e em sistemas críticos, a integridade da operação depende não apenas da entrega do dado, mas do cumprimento de janelas temporais rigorosas. O fenômeno da latência e, principalmente, a variabilidade do atraso (jitter), podem comprometer a eficácia de sistemas de intertravamento de segurança (safety interlocking), onde um comando de parada de emergência deve ser processado em milissegundos para evitar falhas em maquinários ou riscos à integridade física de operadores. O presente estudo tem como objetivo analisar o comportamento e a confiabilidade do protocolo MQTT em cenários de monitoramento de ativos críticos sob condições de estresse de rede. Buscou-se mensurar a latência ponta-a-ponta, e o jitter em diferentes níveis de Qualidade de Serviço (QoS), identificando o ponto de ruptura em que a degradação da rede potencialmente inviabiliza o uso de comandos de segurança. Para a validação experimental, propõe-se uma arquitetura baseada em microcontroladores de baixo custo (ESP32), atuando como nós sensores de vibração e temperatura em um motor industrial simulado. A comunicação foi estabelecida via protocolo MQTT, utilizando o middleware de código aberto Eclipse Mosquitto instalado em um servidor local. O delineamento experimental consistiu na submissão da rede Wi-Fi a cenários controlados de congestionamento de banda e injeção de latência via ferramentas de emulação de rede. O foco da análise concentrou-se no cálculo estatístico do jitter, visando identificar a dispersão do atraso em mensagens de emergência enviadas durante picos de tráfego. Os resultados indicam uma correlação entre o aumento do nível de QoS e o incremento da latência média, evidenciando o trade-off entre a garantia de entrega e o determinismo temporal. Em alinhamento com os Objetivos de Desenvolvimento Sustentável (ODS), em especial o ODS 9 (Indústria, Inovação e Infraestrutura), ao fomentar uma indústria resiliente e inovadora, conclui-se analisando os resultados e discussões propostos neste trabalho, que o monitoramento de máquinas, aliado a uma rede otimizada, é oportuno e indicado para a maturidade digital, promovendo um ambiente fabril mais seguro e eficiente.

Palavras-chave: IIoT; Latência; MQTT; Sistemas Críticos;

OPERATIONAL LIMITS OF THE MQTT PROTOCOL FOR INDUSTRIAL SECURITY IN IIoT ENVIRONMENTS

João Gustavo Mota Ramos¹; João Pedro da Cunha Machado²; Wesley Novaes Fioreze Costa³; Anderson Adelson de Matos⁴

¹ Escola e Faculdade de Tecnologia Senai Felix Guisard – joagustavo2202@gmail.com

² Escola e Faculdade de Tecnologia Senai Felix Guisard – jotapepe.machado@gmail.com

³ Escola e Faculdade de Tecnologia Senai Felix Guisard – wesley.fioreze@docente.senai.br

⁴ Escola e Faculdade de Tecnologia Senai Felix Guisard – anderson.matos@sp.senai.br

Abstract: The fourth industrial revolution has consolidated the Industrial Internet of Things (IIoT) as a fundamental component for the digitization of manufacturing plants, enabling real-time asset monitoring and, with it, the implementation of predictive maintenance strategies. Nevertheless, the transition from traditional control systems, conditioned by structured cabling and deterministic protocols, to wireless networks based on Internet protocols, such as Message Queuing Telemetry Transport (MQTT), introduces challenges related to temporal uncertainty. In industrial environments and critical systems, the integrity of the operation depends not only on the delivery of data, but also on compliance with strict time windows. The phenomenon of latency and, especially, delay variability (jitter) can compromise the effectiveness of safety interlocking systems, where an emergency stop command must be processed in milliseconds to prevent machinery failures or risks to the physical integrity of operators. The present study aims to analyze the behavior and reliability of the MQTT protocol in critical asset monitoring scenarios under network stress conditions. We sought to measure end-to-end latency and jitter at different Quality of Service (QoS) levels, identifying the breaking point at which network degradation potentially renders the use of safety commands unfeasible. For experimental validation, we propose an architecture based on low-cost microcontrollers (ESP32), acting as vibration and temperature sensor nodes in a simulated industrial motor. Communication was established via the MQTT protocol, using the open-source Eclipse Mosquitto middleware installed on a local server. The experimental design consisted of subjecting the Wi-Fi network to controlled scenarios of bandwidth congestion and latency injection via network emulation tools. The focus of the analysis was on the statistical calculation of jitter, aiming to identify the dispersion of delay in emergency messages sent during traffic peaks. The results indicate a correlation between the increase in QoS level and the increase in average latency, highlighting the trade-off between delivery guarantee and temporal determinism. In line with the Sustainable Development Goals (SDGs), in particular SDG 9 (Industry, Innovation, and Infrastructure), by fostering a resilient and innovative industry, it is concluded by analyzing the results and discussions proposed in this work that machine monitoring, combined with an optimized network, is timely and appropriate for digital maturity, promoting a safer and more efficient manufacturing environment.

Keywords: IIoT; Latency; MQTT; Critical Systems;