Análise de Desempenho e Eficiência Energética dos Protocolos MQTT e CoAP no contexto de IoT

Emanuel de Franceschi Vieira[1], **Murilo Cervi**[1],
Renato Preigschadt de Azevedo[1], **Tiago Antônio Rizzetti**[1]

[1]Colégio Técnico Industrial de Santa Maria (CTISM)
Universidade Federal de Santa Maria (UFSM)

{emanuel.vieira, cervi, renato, rizzetti}@redes.ufsm.br

Abstract. *This paper examines the performance and energy efficiency of MQTT, MQTT with TLS, and CoAP protocols in the context of the Internet of Things (IoT). Tests using ESP32 DevKit v1 microcontrollers in a controlled environment measured energy consumption and message throughput. The results indicate that CoAP offers higher throughput efficiency at maximum frequency, while MQTT exhibited moderate consumption without significantly impacting energy efficiency, even with encryption. The analysis underscores the importance of protocol selection, considering the constraints of each IoT application.*

Resumo. *Este artigo examina o desempenho e a eficiência energética dos protocolos MQTT, MQTT com TLS e CoAP no contexto da Internet das Coisas (IoT). Testes com microcontroladores ESP32 DevKit v1 em ambiente controlado mediram o consumo energético e a taxa de transferência de mensagens. Os resultados indicam que o CoAP possui maior eficiência na taxa de transferência em frequência máxima, enquanto o MQTT apresentou um consumo moderado, sem impactar significativamente a eficiência energética, mesmo com criptografia. A análise destaca a importância da escolha de protocolos, considerando as limitações de cada aplicação IoT.*

1. Introdução

A presença de dispositivos IoT pode gerar riscos significativos à privacidade, pois as interações com os usuários envolvem grandes quantidades de dados coletados sem um padrão definido [Liu et al. 2018, de Oliveira et al. 2019]. Para que as aplicações IoT operem de forma eficiente e confiável, é fundamental utilizar protocolos de comunicação adequados. Entre os principais, destacam-se o MQTT (*Message Queuing Telemetry Transport*) e o CoAP (*Constrained Application Protocol*), conhecidos por sua eficiência e confiabilidade. Protocolos de segurança, como TLS para MQTT e DTLS para CoAP, também são frequentemente implementados para proteger a comunicação.

Este estudo avalia o desempenho e a eficiência energética dos protocolos MQTT (com e sem TLS) e CoAP, levando em conta as limitações de recursos típicas de dispositivos IoT. Testes foram realizados em ambiente controlado utilizando microcontroladores *ESP32 DevKit v1* e uma máquina virtual com um *broker* MQTT e um servidor CoAP. Os dados coletados permitem uma análise comparativa que visa auxiliar na escolha dos protocolos mais adequados para aplicações IoT em termos de desempenho e consumo energético.

O restante deste artigo está organizado da seguinte forma. A Seção 2 descreve os trabalhos relacionados. A Seção 3 apresenta as principais características e funcionalidades dos protocolos MQTT e CoAP. Na Seção 4 é descrita a metodologia empregada no estudo. Os resultados obtidos nos experimentos realizados são apresentados na Seção 5 e, por fim, a Seção 6 conclui o artigo.

2. Trabalhos Relacionados

O artigo escrito por [Bayılmış et al. 2022] fornece uma visão geral dos protocolos MQTT, CoAP e WebSocket no contexto da IoT, avaliando taxas de transferência, consumo energético e tempo de atraso em um ambiente controlado. O estudo destaca que o CoAP, operando em UDP sem *handshake*, tem melhor desempenho em aplicações de alta carga com baixo consumo de energia. Já o trabalho de autoria de [Quincozes et al. 2021a] analisa a sobrecarga de mecanismos criptográficos nos protocolos MQTT e CoAP, focando no consumo energético, tempo de resposta e uso de memória com algoritmos AES128, AES256, TEA e DES. O MQTT com QoS-1 mostrou melhor desempenho em comparação com o CoAP.

Diferente dos trabalhos relacionados, o presente estudo emprega o uso de equipamentos de bancada para medir e calcular o consumo energético dos dispositivos. Além disso, são utilizados microcontroladores *ESP32 DevKit v1* como dispositivos IoT, proporcionando um cenário mais próximo da realidade de aplicação. Outro ponto divergente deste trabalho é o uso de TLS para o MQTT na avaliação dos impactos gerados pela implementação de ferramentas de criptografia de dados.

3. Protocolos de Comunicação e Criptografia de Dados

Protocolos de comunicação gerenciam a transferência de informações entre dispositivos. Em ambientes IoT, onde há restrições de recursos, a escolha do protocolo é fundamental. Dois protocolos amplamente utilizados são o MQTT e o CoAP [Martins and Zem 2015]. O MQTT, ideal para dispositivos com recursos limitados, é utilizado em setores como automotivo, telecomunicações e manufatura [MQTT 2022], transportando mensagens via TCP e podendo usar TLS para segurança [Seoane et al. 2021]. Ele utiliza o modelo *publish/subscribe*, que permite comunicação assíncrona, gerenciada por um *broker* central [Manandhar 2017]. O CoAP, desenvolvido pelo IETF, é um protocolo leve para ambientes com recursos limitados [Martins and Zem 2015]. Conforme a RFC7252, o CoAP usa UDP para comunicação assíncrona e DTLS para segurança [Shelby et al. 2014]. No modelo cliente/servidor, os clientes fazem requisições e os servidores respondem com dados e códigos de resposta. A Figura 1 apresenta, respectivamente, os modelos de Publicação/Assinatura e Cliente/Servidor, ilustrando a maneira como é feita a comunicação entre os dispositivos.

A privacidade e segurança em IoT são desafios críticos, com a criptografia de dados desempenhando um papel fundamental na proteção das informações transmitidas [Sklavos and Zaharakis 2016]. Ao lidar com informações no contexto digital, especialmente quando utilizamos a internet, é essencial que os sistemas computacionais atendam aos pilares da segurança da informação, como disponibilidade, integridade, controle de acesso, autenticidade, não-repúdio e privacidade [Oliveira 2012].

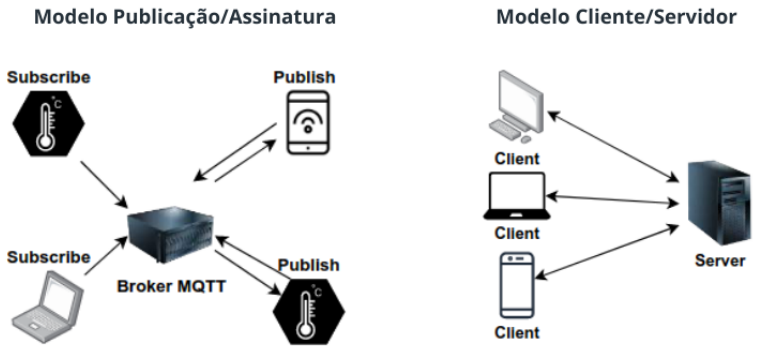


Figura 1. Modelos de funcionamento, adaptado de [Quincozes et al. 2021b].

A criptografia permite codificar os dados, tornando-os ilegíveis para qualquer pessoa não autorizada, assegurando a confidencialidade [Kim and Solomon 2014]. Existem duas principais abordagens para a criptografia: simétrica e assimétrica. Na criptografia simétrica, a mesma chave é usada para encriptar e decriptar os dados, oferecendo simplicidade e rapidez, mas exigindo uma troca segura de chaves previamente [Oliveira 2012]. Por outro lado, a criptografia assimétrica utiliza um par de chaves, uma pública e uma privada. A chave pública é compartilhada livremente, enquanto a chave privada é mantida em segredo, permitindo a decriptação de mensagens encriptadas com a chave pública correspondente [Kim and Solomon 2014].

4. Metodologia e Desenvolvimento

Para o desenvolvimento deste trabalho foi elaborado um ambiente de testes, no qual realizou-se a instalação de uma máquina virtual utilizando o *VM VirtualBox* com o sistema operacional Ubuntu *Server* 22.04 LTS. Essa escolha evitou que configurações anteriores interferissem nos testes. Na máquina virtual, foram instalados o *broker* MQTT Mosquitto, que suporta autenticação, certificados digitais e criptografia, e o servidor CoAP, criado com a biblioteca *libcoap*, que oferece recursos avançados e suporte a padrões como a RFC7552. Os microcontroladores ESP32 foram programados para funcionar como clientes tanto no envio quanto no recebimento de mensagens, permitindo a avaliação da eficiência e do desempenho dos protocolos MQTT e CoAP em diferentes cenários. No caso do MQTT, as bibliotecas *WiFi*, *PubSubClient*, e *WiFiClient* foram utilizadas, com *WiFiClientSecure* sendo empregada para o cenário com TLS. Para o CoAP, foram utilizadas as bibliotecas *WiFi* e *CoAP-simple-library*, configurando os dispositivos para atuarem como clientes e servidores, respectivamente.

4.1. Análise de Desempenho e Consumo Energético

Para avaliar o desempenho e o consumo energético dos protocolos MQTT e CoAP em dispositivos ESP32, foram realizados testes focando tanto na taxa de transferência quanto na eficiência energética. A análise de desempenho envolveu a medição da taxa de mensagens enviadas e recebidas por segundo, testando a capacidade desses protocolos em lidar com grandes volumes de dados. Foram transmitidas 1.000 mensagens de diferentes tamanhos (256, 512 e 1024 Bytes) utilizando *scripts* desenvolvidos para enviar as mensagens. Nos dispositivos que recebiam as mensagens, o tempo necessário para processar a chegada dessas mensagens foi registrado. De forma similar, nos clientes que enviavam as mensagens, foram analisados os tempos de transmissão.

A análise de consumo energético foi conduzida utilizando equipamentos de bancada, como o osciloscópio DPO2014 da *Tektronix* e a fonte de alimentação ajustável DP711 da *Rigol*, com o objetivo de aumentar a precisão das medições. O objetivo principal dessa análise foi avaliar o consumo de energia dos dispositivos ESP32 atuando nos diferentes cenários envolvendo os protocolos MQTT e CoAP. A fim de obter a média dos valores encontrados, os testes realizados foram repetidos cinco vezes para cada cenário, incluindo um teste basal sem troca de informações, que serve como referência de consumo energético em estado ocioso.

5. Resultados Obtidos

Os resultados dos testes de desempenho e consumo energético dos dispositivos IoT utilizando os protocolos MQTT, MQTT (TLS) e CoAP são apresentados a seguir. No cenário com MQTT sem criptografia, foi identificado um atraso significativo no recebimento de mensagens pelo ESP32 quando estas eram enviadas na frequência máxima, provavelmente devido à sobrecarga no *buffer* de recepção, resultando em perda de mensagens ou necessidade de retransmissão. Para resolver esse problema, foi implementado um atraso de 20 milissegundos entre o envio de cada mensagem, sincronizando o envio e o recebimento. Esse valor foi determinado através de testes preliminares, que mostraram que atrasos menores não eliminavam a perda de mensagens, enquanto atrasos maiores não ofereciam benefícios adicionais, apenas aumentando o tempo total de transmissão.

5.1. Desempenho

Por meio dos testes realizados foi possível obter algumas percepções significativas sobre o desempenho dos protocolos MQTT e CoAP. Os gráficos, na Figura 2, comparam o desempenho dos diferentes protocolos, destacando a quantidade de mensagens enviadas e recebidas por segundo em cada cenário. Esses gráficos permitem identificar diferenças na eficiência de transmissão, proporcionando observações relevantes sobre como cada protocolo se comporta em condições variadas.

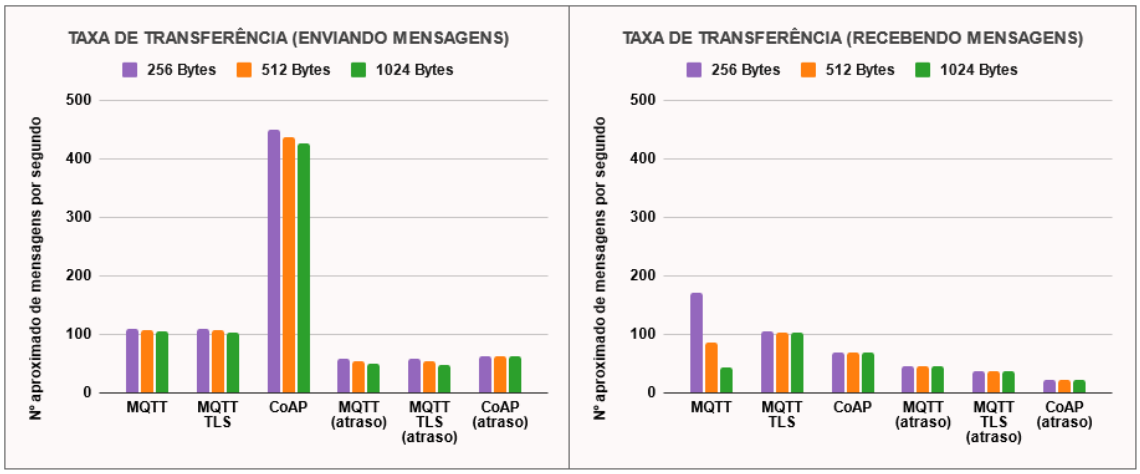


Figura 2. Gráficos comparativos da taxa de transferência

5.2. Consumo Energético

A análise do consumo energético permite avaliar o impacto dos protocolos MQTT e CoAP em dispositivos IoT, o que é crucial para otimizar a eficiência energética em

implementações práticas. Um aspecto importante é o efeito dos atrasos programados na transmissão de mensagens, que influenciam significativamente o consumo de energia. Utilizando um osciloscópio, foi possível identificar como esses atrasos afetam a onda de corrente, que, dado que a tensão é constante, reflete diretamente a potência dos dispositivos. No Apêndice, disposto ao final deste trabalho, é possível verificar registros referentes às ondas de corrente, comparando o cenário com e sem implementação de atraso.

Por meio da análise das métricas relacionadas ao consumo energético, é possível realizar uma comparação para identificar qual dos cenários foi mais eficiente. Os gráficos, na Figura 3, ilustram essa comparação, exibindo o consumo em Joules, obtido por meio da média do consumo energético em um intervalo de 40 segundos. A análise dos dados mostra que, no MQTT, a criptografia de dados tem uma influência moderada no consumo de energia, sem comprometer significativamente a eficiência dos dispositivos. Dispositivos operando em frequência máxima, sem atrasos, consomem mais energia devido à operação contínua. O CoAP, sem atrasos, também apresentou um consumo energético maior, mas reduziu o consumo com um atraso de 20ms. Assim, percebe-se que implementar atrasos programados pode otimizar o consumo energético, especialmente quando a frequência máxima não é necessária.

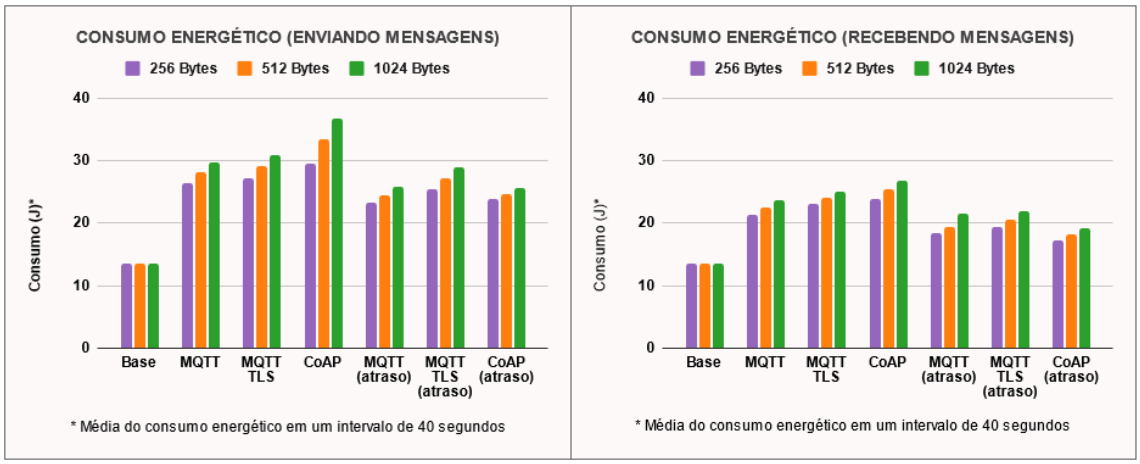


Figura 3. Gráficos comparativos do consumo energético

6. Conclusão

Este trabalho analisou os protocolos MQTT, MQTT com TLS e CoAP no contexto da IoT, com foco em desempenho e eficiência energética. Apesar de alguns desafios técnicos, como a dificuldade na implementação da criptografia DTLS com CoAP no ESP32, os testes realizados forneceram considerações valiosas sobre o comportamento dos dispositivos, especialmente em relação ao atraso no recebimento de mensagens com MQTT sem criptografia.

Embora nem todos os objetivos tenham sido plenamente alcançados, as dificuldades encontradas contribuíram para um entendimento mais profundo das particularidades dos protocolos analisados. O estudo oferece uma base sólida para futuras pesquisas e orienta a seleção adequada desses protocolos em diferentes contextos de implementação na IoT, ressaltando a importância de considerar as especificidades de cada cenário.

Agradecimentos

O presente trabalho foi realizado com apoio da Fundação Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES.

Referências

Bayılmış, C., Ebleme, M. A., Çavuşoğlu, Ü., Küçük, K., and Sevin, A. (2022). A survey on communication protocols and performance evaluations for internet of things. *Digital Communications and Networks*, 8(6):1094–1104.

de Oliveira, N. S., Gomes, M. A., Lopes, R., and Nobre, J. C. (2019). Segurança da informaçao para internet das coisas (iot): uma abordagem sobre a lei geral de proteçao de dados (lgpd). *Revista Eletrônica de Iniciação Científica em Computação*, 17(4).

Kim, D. and Solomon, M. G. (2014). *Fundamentos de segurança de sistemas de informação*. LTC.

Liu, J., Zhang, C., and Fang, Y. (2018). Epic: A differential privacy framework to defend smart homes against internet traffic analysis. *IEEE Internet of Things Journal*, 5(2):1206–1217.

Manandhar, S. (2017). Mqtt based communication in iot. Master's thesis.

Martins, I. R. and Zem, J. L. (2015). Estudo dos protocolos de comunicação mqtt e coap para aplicações machine-to-machine e internet das coisas.

MQTT (2022). MQTT. Acesso em 10 jun. 2023.

Oliveira, R. R. (2012). Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. *Segurança Digital [Revista online]*, 31:11–15.

Quincozes, V. E., Quincozes, S. E., and Kazienko, J. F. (2021a). Avaliando a sobrecarga de mecanismos criptograficos simétricos na internet das coisas: Uma comparação quantitativa entre os protocolos mqtt e coap. In *Anais do XX Workshop em Desempenho de Sistemas Computacionais e de Comunicação*, pages 13–24. SBC.

Quincozes, V. E., Quincozes, S. E., and Kazienko, J. F. (2021b). Desvendando a camada de aplicação na internet das coisas: Teoria, prática e tendências. *Sociedade Brasileira de Computação*.

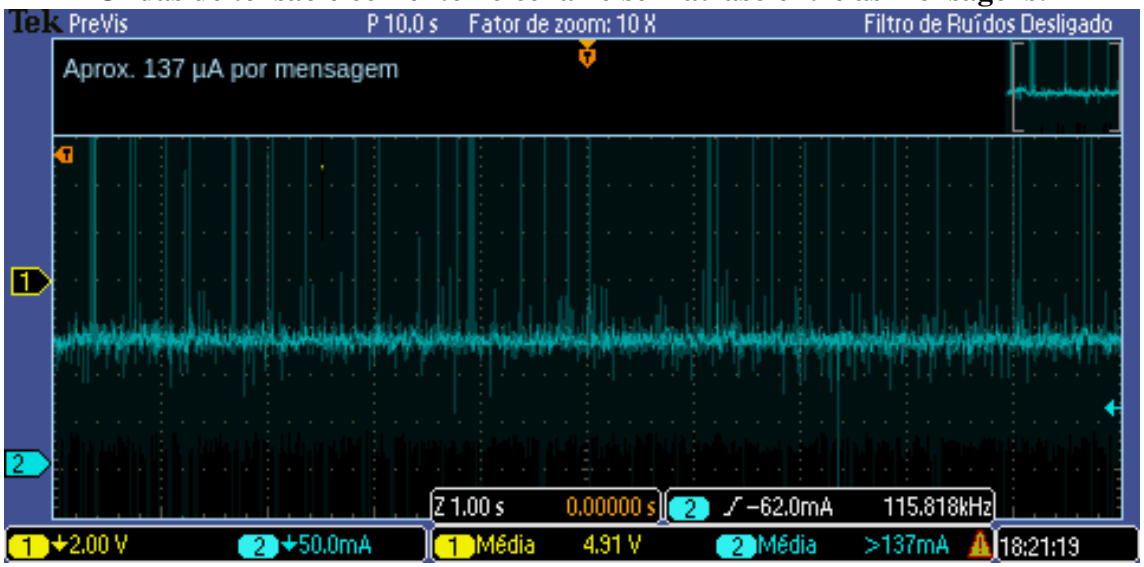
Seoane, V., Garcia-Rubio, C., Almenares, F., and Campo, C. (2021). Performance evaluation of coap and mqtt with security support for iot environments. *Computer Networks*, 197:108338.

Shelby, Z., Hartke, K., and Bormann, C. (2014). The Constrained Application Protocol (CoAP). RFC 7252.

Sklavos, N. and Zaharakis, I. D. (2016). Cryptography and security in internet of things (iots): Models, schemes, and implementations. In *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–2. IEEE.

APÊNDICE A

Ondas de tensão e corrente no cenário sem atraso entre as mensagens:



Ondas de tensão e corrente no cenário com atraso de 20ms entre as mensagens: