IX Encontro de Iniciação Científica e Tecnológica
IX EnICT
ISSN: 2526-6772
IFSP – *Campus* Araraquara
6 de dezembro de 2025

Análise do impacto da variação de tamanho de pacotes em protocolos MQTT e CoAP no contexto de ataques DoS

[1] Graduando em Tecnologia em Análise e Desenvolvimento de Sistemas pelo Instituto Federal de São Paulo (IFSP) – Câmpus Bragança Paulista. E-mail: inacio.fernandes@aluno.ifsp.edu.br

[2] Doutor em Computação Aplicada pelo Instituto Nacional de Pesquisas Espaciais (INPE). Docente do Instituto Federal de São Paulo (IFSP) – Câmpus Bragança Paulista. E-mail: luiz.veras@ifsp.edu.br

Área de conhecimento: **Redes de Computadores – 1.03.04.04-5.**

RESUMO: Novos protocolos de comunicação têm sido desenvolvidos para melhorar as trocas de informações entre dispositivos IoT. Este trabalho investiga como a variação do tamanho dos pacotes impacta os protocolos CoAP e MQTT em dispositivos IoT. Para isso, simulações foram realizadas para avaliar o desempenho dos protocolos em diversos cenários de rede, considerando métricas como latência, taxa de entrega de pacotes e consumo de energia. Foi considerado um cenário com 1000 dispositivos enviando 1000 mensagens cada, a cada 10 milissegundos. Os resultados indicam que pacotes maiores podem causar maior atraso devido ao tempo de processamento. Este estudo oferece parâmetros que ajudam no desenvolvimento de aplicações eficientes para IoT, com a escolha do protocolo e rota de pacotes ideal para cada cenário. O estudo também considera a robustez dos protocolos contra-ataques de negação de serviço (DoS), fornecendo informações sobre a resistência e segurança desses protocolos em redes IoT.

PALAVRAS-CHAVE: iot; mqtt; coap; ataque dos; redes.

1. INTRODUÇÃO

A Internet das Coisas, em inglês, Internet of Things (IoT), está revolucionando a indústria ao interconectar dispositivos e sistemas por meio da Internet. O uso dessa tecnologia tem inúmeros benefícios, mas traz desafios e, em especial, preocupações com a segurança. Em geral, a eficiência e a segurança da comunicação são essenciais para garantir o funcionamento adequado das operações em ambientes IoT.

Protocolos como o Message Queuing Telemetry Transport (MQTT) e o Constrained Application Protocol (CoAP) são amplamente adotados devido à sua eficiência e baixo consumo de recursos, sendo ideais para dispositivos IoT. No entanto, a segurança desses protocolos enfrenta diversas ameaças, destacando-se os ataques de negação de serviço (do inglês, Denial of Service – DoS). Esses ataques visam sobrecarregar servidores com um volume massivo de requisições maliciosas, resultando na interrupção ou indisponibilidade do serviço para usuários legítimos [Singh et al. 2015; Thangavel et al. 2014].

Este estudo concentra-se na avaliação do impacto dos diferentes tamanhos de mensagens nos protocolos MQTT e CoAP em cenários de DoS. Investigar como esses protocolos respondem a cargas variadas de pacotes é crucial não apenas para compreender sua eficiência operacional, mas também para avaliar sua resistência contra potenciais ataques

cibernéticos. A análise empírica desses aspectos contribui significativamente para o desenvolvimento de estratégias robustas de segurança e otimização de desempenho em aplicações IoT [Thangavel et al. 2014; Cosmi e Mota 2019].

2. FUNDAMENTAÇÃO TEÓRICA

2.1 Protocolos MQTT e CoAP

O MQTT, demonstrado pela Figura 1, é um protocolo de publicação/assinatura sobre TCP, centralizado em um *broker* e com três níveis de Qualidade de Serviço (QoS) para garantir a entrega [Locke 2010; Banks e Gupta 2014]. Em contraste, o CoAP, demonstrado pela Figura 2, é um protocolo RESTful desenvolvido pela IETF, baseado em UDP, que utiliza um modelo cliente/servidor [Shelby et al. 2014]. Por não ter a garantia do TCP, o CoAP implementa sua própria confiabilidade com mensagens Confirmáveis (CON) e Não-confirmáveis (NON) [Shelby et al. 2014]. O cabeçalho do CoAP (4 bytes) é maior que o do MQTT (2 bytes), mas ambos são projetados para baixo *overhead* [Banks e Gupta 2014; Shelby et al. 2014].

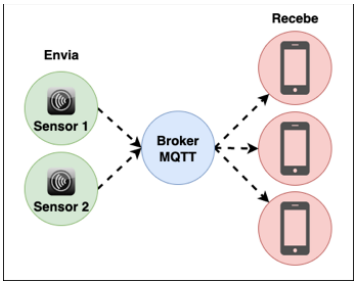

Figura 1 – Arquitetura MQTT

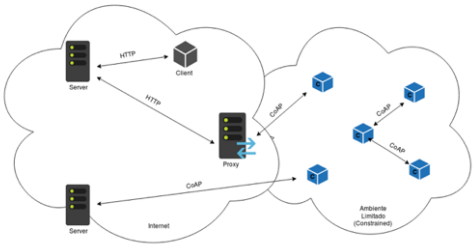

Figura 2 – Arquitetura CoAP

2.2 Ataque de Negação de Serviço em IoT

Em protocolos IoT, os ataques DoS exploram características específicas do modelo de comunicação No MQTT, por ser baseado em TCP, os ataques comuns incluem o *CONNECT flood* (esgotar a capacidade de conexões do *broker*) e o *flood*(enviar um volume massivo de mensagens, especialmente com *payloads* grandes) [Vucinic et al. 2016].

No CoAP, por ser baseado em UDP, as ameaças são diferentes. Ele é vulnerável a ataques de inundação de pacotes simples e, mais criticamente, a ataques de amplificação de DDoS [Seitz et al. 2018]. Nesses ataques, um atacante com IP *spoofado* envia uma pequena requisição a servidores CoAP, que respondem com respostas muito maiores para a vítima [Seitz et al. 2018]. A variação no tamanho dos pacotes, como investigado neste estudo, é um vetor direto para a eficácia desses ataques.

3. TRABALHOS RELACIONADOS

Estudos prévios analisaram os protocolos IoT. Cosmi e Mota (2019) exploraram suas características e vulnerabilidades. Thangavel et al. (2014) compararam o desempenho, notando que o MQTT (TCP) apresenta maior *overhead* de comunicação, enquanto o CoAP (UDP) demonstra menor latência em redes estáveis. Especificamente sobre segurança, Al-Masri e Al-Qutayri (2021) conduziram uma análise comparativa do desempenho de ambos sob ataques DoS, simulando *floods* e avaliando a latência. Seus resultados corroboram que ambos são vulneráveis, mas os impactos variam significativamente com base no vetor de ataque (ex: *flood* de conexão vs. *flood* de *payload*), alinhando-se aos objetivos desta pesquisa.

4. MATERIAIS E MÉTODOS

Nesta seção estão descritos os recursos de *hardware* e *software* utilizados e a configuração dos testes. Está explicitada também a interpretação empregada sobre a relação do tamanho dos pacotes com ataques bem-sucedidos de negação de serviço.

4.1 Dispositivos Utilizados

Este estudo utiliza um ambiente de teste com três dispositivos principais:

- **Servidor/Broker:** Um Raspberry Pi 4, escolhido por sua capacidade de processamento para executar os serviços MQTT e CoAP.
- **Cliente de Teste:** Um Raspberry Pi Zero W, representando dispositivos IoT típicos com recursos limitados, responsável por medir o tempo de resposta.
- **Cliente Atacante:** Um MacBook Pro, simulando os ataques gerando tráfego malicioso.

4.2 Configuração dos Testes

A análise foca no impacto do tamanho dos pacotes, que influencia diretamente o desempenho. Pacotes maiores podem aumentar o tempo de transmissão e latência, especialmente em redes limitadas, além de exigir fragmentação, o que adiciona sobrecarga de processamento [Al-Kashoash e Kemp 2017; Thangavel et al. 2014].

O ambiente de teste foi implementado utilizando bibliotecas Node.js. O **Servidor (Broker)** foi configurado no Raspberry Pi 4; o **Cliente Atacante** (MacBook Pro) foi configurado para injetar pacotes maliciosos e sobrecarregar o servidor com tamanhos variados; e o **Cliente de Teste** (Raspberry Pi Zero W) coletou os dados de desempenho.

O servidor e os clientes operaram sem qualquer mecanismo adicional de segurança para avaliar o desempenho isolado dos protocolos. Foram simulados 1000 dispositivos enviando 1000 mensagens a cada 10 milissegundos, um ataque de inundação de pacotes e conexões. Os testes foram repetidos para diferentes tamanhos de cargas úteis: 1 byte, 100 bytes e 1000 bytes.

5. RESULTADOS E DISCUSSÃO

Os testes avaliaram o tempo de resposta dos protocolos MQTT e CoAP com pacotes de 1 byte, 100 bytes e 1000 bytes, em três momentos: antes do ataque, durante o ataque e após o ataque. Os resultados são apresentados nas Figuras 3 e 4.

Na Figura 3, o tempo de resposta do protocolo MQTT é mostrado. Antes do ataque, o tempo de resposta foi baixo (17 ms) para todos os tamanhos de pacotes. Durante o ataque, houve um aumento significativo, especialmente para pacotes maiores. O tempo de resposta para pacotes de 1000 bytes alcançou 637 ms, enquanto para pacotes de 100 bytes foi de 539 ms, e para pacotes de 1 byte foi de 330 ms . Após o ataque, os tempos de resposta retornaram a níveis baixos, mas ligeiramente mais altos que os iniciais, especialmente para pacotes de 1000 bytes (34 ms).

A Figura 4 apresenta o tempo de resposta do protocolo CoAP. Semelhante ao MQTT, o tempo de resposta antes do ataque foi baixo (10 ms). Durante o ataque, os tempos de resposta aumentaram drasticamente. O tempo de resposta para pacotes de 1000 bytes chegou a 1148 ms, enquanto para pacotes de 100 bytes foi de 457 ms e para pacotes de 1 byte foi de 225 ms . Após o ataque, os tempos de resposta diminuíram, mas ainda levemente aumentados (21 ms para 1000 bytes).

O aumento de latência drasticamente maior no CoAP (1148 ms) com pacotes de 1000 bytes, em comparação ao MQTT (637 ms), sugere que o processamento de pacotes UDP maiores (potencialmente fragmentados) impõe uma sobrecarga no servidor que é mais explorável por um ataque de *flood* volumétrico.

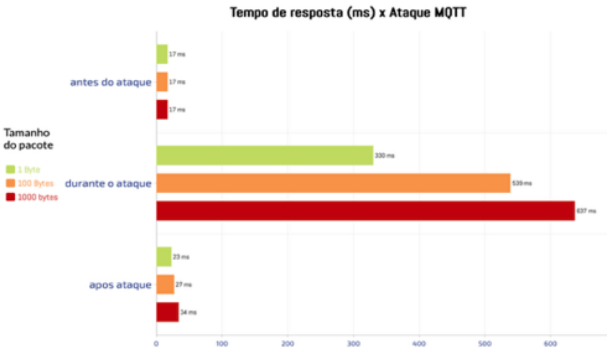

Figura 3 - Ataque MQTT

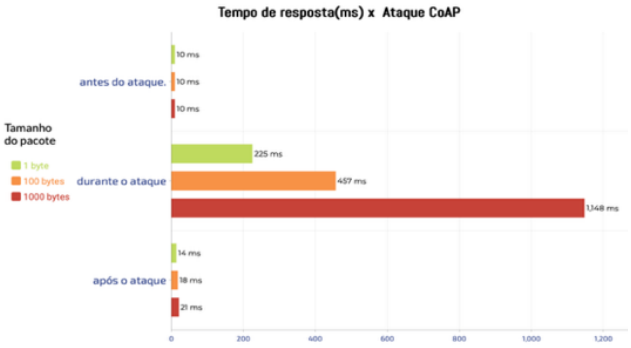

Figura 4 - Ataque CoAP

Os testes demonstram que o tempo de restabilização do servidor após um ataque é maior para pacotes de tamanhos maiores. Isso foi evidente tanto no protocolo MQTT quanto no CoAP, onde pacotes de 1000 bytes mostraram tempos de resposta ainda elevados logo após o ataque.

6. CONCLUSÃO E TRABALHOS FUTUROS

Este estudo analisa os impactos de diferentes tamanhos de pacotes nos protocolos MQTT e CoAP em um ambiente IoT. Os resultados mostram que pacotes maiores aumentam o tempo de resposta e de restabilização do servidor, especialmente em cenários de ataques DoS.

Para trabalhos futuros, pretende-se explorar mais detalhadamente os aspectos de segurança dos protocolos, incluindo métricas para mitigação contra ataques, ampliar a gama de dispositivos nos testes, testar os protocolos em diferentes condições de rede e desenvolver técnicas de otimização. O trabalho está em andamento, com próximos passos incluindo a implementação de testes para obter uma compreensão mais abrangente do desempenho e segurança dos protocolos de comunicação em IoT.

7. REFERÊNCIAS

AL-KASHOASH, H. A.; KEMP, A. H. Comparison of 6LoWPAN and LPWAN for the Internet of Things. Australian Journal of Electrical and Electronics Engineering, v. 13, n. 4, p. 268–274, 2017.

AL-MASRI, E.; AL-QUTAYRI, M. A comparative analysis of MQTT and CoAP performance under DoS and DDoS attacks. In: IEEE GLOBAL CONFERENCE ON ARTIFICIAL INTELLIGENCE AND INTERNET OF THINGS (GCAIoT), 2021. Proceedings... [S.l.]: IEEE, 2021. p. 136-141.

BANKS, A.; GUPTA, R. MQTT Version 3.1.1. OASIS Standard. 2014. Disponível em: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html. Acesso em: 03 dez. 2025.

COSMI, A.; MOTA, F. Uma análise dos protocolos de comunicação para Internet das Coisas. In: WORKSHOP DE COMPUTAÇÃO URBANA (COURB), 3., 2019, Belém. Anais... Porto Alegre: Sociedade Brasileira de Computação, 2019.

LOCKE, D. MQTT For Sensor Networks (MQTT-SN) Protocol Specification. Version 1.2. [S.l.]: International Business Machines (IBM) Corporation, 2010.

MBURINE, Q. F. et al. Análise de Desempenho dos Protocolos de Aplicação CoAP, MQTT e Radnet Protocol para Internet das Coisas. 2024. Tese/Dissertação/Trabalho de Conclusão de Curso – [Nome da Instituição], [Cidade], 2024.

SEITZ, J. A.; SCHÜTTE, J.; TILLMANNS, S. CoAP-based amplification attacks. In: IEEE/ACM INTERNATIONAL CONFERENCE ON INTERNET-OF-THINGS DESIGN AND IMPLEMENTATION (IoTDI), 3., 2018. Proceedings... [S.l.]: IEEE, 2018. p. 248-253.

SHELBY, Z.; HARTKE, K.; BORMANN, C. The Constrained Application Protocol (CoAP). RFC 7252. [S.l.]: Internet Engineering Task Force (IETF), 2014.

SINGH, J. et al. Twenty security considerations for cloud-supported Internet of Things. IEEE Internet of Things Journal, v. 3, n. 3, p. 269–284, 2015.

THANGAVEL, D. et al. Performance evaluation of MQTT and CoAP via a common middleware. In: IEEE INTERNATIONAL CONFERENCE ON INTELLIGENT SENSORS, SENSOR NETWORKS AND INFORMATION PROCESSING (ISSNIP), 9., 2014, Singapore. Proceedings... Singapore: IEEE, 2014. p. 1–6.

VUCINIC, M. et al. Security analysis of the MQTT protocol. In: INTERNATIONAL CONFERENCE ON IDENTIFICATION, INFORMATION AND KNOWLEDGE IN THE INTERNET OF THINGS (IIKI), 2016. Proceedings... [S.l.]: IEEE, 2016. p. 73-78.