Impacto da criptografia de dados na eficiência energética em dispositivos IoT que utilizam o protocolo MQTT

Emanuel de Franceschi Vieira[1], **Tiago Antônio Rizzetti**[1]

[1]Curso Superior de Tecnologia em Redes De Computadores
Universidade Federal de Santa Maria (UFSM)
Av. Roraima nº 1000. Cidade Universitária. Camobi. Santa Maria - RS

emanuel.vieira@redes.ufsm.br, rizzetti@ctism.ufsm.br

Resumo. *Este artigo apresenta uma análise comparativa do protocolo MQTT (Message Queuing Telemetry Transport) no contexto da Internet das Coisas (IoT), com foco na influência da criptografia de dados. Para isso, foram realizados testes em um ambiente controlado, utilizando microcontroladores ESP32 DevKit v1 como clientes e configurando um broker MQTT em uma máquina virtual dedicada. Durante os testes, foram coletados dados relevantes relacionados ao consumo de energia dos clientes nas comunicações MQTT, comparando cenários com e sem a implementação de criptografia de dados. Os resultados obtidos revelam os impactos da criptografia no consumo energético, proporcionando informações valiosas para a eficiência energética em aplicações IoT.*

Abstract. *This article presents a comparative analysis of the MQTT (Message Queuing Telemetry Transport) protocol in the context of the Internet of Things (IoT), with a focus on the influence of data encryption. Tests were conducted in a controlled environment, using ESP32 microcontrollers as clients and configuring an MQTT broker on a dedicated virtual machine. During the tests, relevant data related to the energy consumption of clients in MQTT communications were collected, comparing scenarios with and without data encryption implementation. The results obtained reveal the impacts of encryption on energy consumption, providing valuable information for energy efficiency in IoT applications.*

1. Introdução

A Internet das Coisas (IoT) tem revolucionado a forma como os usuários interagem com o mundo ao seu redor, conectando dispositivos e possibilitando o compartilhamento de informações em tempo real [Paulo Spaccaquerche 2023]. Com isso, percebe-se que o uso de protocolos de comunicação adequados é essencial para garantir a eficiência e o bom funcionamento das aplicações IoT. Entre os diversos protocolos existentes, o MQTT é uma opção amplamente utilizada e reconhecida por sua eficiência e confiabilidade.

Em IoT, a segurança dos dados torna-se uma prioridade fundamental, uma vez que uma grande quantidade de informações sensíveis e pessoais é compartilhada entre os diversos dispositivos interconectados. A implementação da criptografia de dados desempenha um papel fundamental na proteção dessas informações, garantindo a confidencialidade das mensagens transmitidas.

Considerando a ampla adoção de dispositivos IoT em diversos setores e a importância da segurança da informação, é fundamental que os protocolos de comunicação sejam cuidadosamente avaliados para que possam atender aos requisitos específicos de cada aplicação. A análise comparativa acerca dos impactos causados pela implementação da criptografia de dados irá permitir identificar e avaliar alguns pontos importantes, como a capacidade de gerenciar grande volumes de dados, tempo de resposta e consumo energético.

Durante o desenvolvimento deste trabalho, foram realizados testes em um ambiente controlado, utilizando microcontroladores *ESP32 DevKit v1* como clientes e um *broker* MQTT configurado em uma máquina virtual. Através dos testes, busca-se coletar dados relevantes relacionados ao consumo de energia das diferentes aplicações. Isso nos permitirá fornecer uma comparação entre as comunicações realizadas com e sem o uso de criptografia de dados, com o objetivo de apresentar informações valiosas sobre os impactos no consumo de energia dessas aplicações.

2. Trabalhos Relacionados

O artigo escrito por [Bayılmış et al. 2022] oferece uma visão geral de protocolos de comunicação e analisa suas vantagens e limitações. Ele também realiza testes comparativos entre os protocolos MQTT, CoAP e WebSocket, medindo a taxa de transferência, consumo de energia e latência média. Os testes ocorreram em um ambiente controlado com um dispositivo IoT, um servidor em um notebook, um medidor de energia USB e uma rede sem fio utilizando a infraestrutura 4.5G.

O estudo de [Quincozes et al. 2021] avalia vários mecanismos de criptografia simétrica para garantir a confidencialidade das mensagens nos protocolos MQTT e CoAP, analisando o consumo de energia, tempo de resposta, uso de memória, tempo de CPU e dados transmitidos. Os mecanismos incluem AES128, AES256, TEA e DES, testados em uma aplicação Android com clientes CoAP e MQTT.

3. Protocolo MQTT

MQTT é um protocolo de comunicação para IoT, projetado com o objetivo de proporcionar um transporte leve e eficiente, ideal para conectar dispositivos remotos com limitações de recursos. Atualmente, este protocolo é amplamente utilizado em diversos setores, como automotivo, manufatura, telecomunicações, entre outros [MQTT 2022]. O MQTT também permite a comunicação assíncrona entre os dispositivos, desse modo o emissor e o receptor não precisam saber a existência um do outro. Isso é possível graças ao modelo de publicação e assinatura (*publish/subscribe*), que é adotado pelo protocolo.

No modelo *publish/subscribe* existem dois sujeitos na rede: os clientes e o *broker*. Os clientes são dispositivos que podem atuar tanto como publicadores, enviando mensagens para tópicos específicos, quanto como assinantes, recebendo mensagens publicadas por outros dispositivos nos tópicos aos quais estão inscritos. O *broker*, por sua vez, é o ponto central, responsável por receber todas as mensagens enviadas pelos publicadores, filtra-las e encaminha-las para os assinantes interessados em receber essas informações [Manandhar 2017].

Para implementar o protocolo MQTT e facilitar a realização dos testes, optou-se por utilizar o *broker* Mosquitto como componente central responsável pela gestão das

mensagens. O Mosquitto é uma escolha popular e confiável na comunidade de IoT, por conta de sua robustez e eficiência. Ele oferece um ambiente de código aberto, que permite configurar e gerenciar a troca de mensagens entre os clientes IoT. Além disso, o Mosquitto é capaz de suportar conexões seguras por meio do protocolo SSL/TLS.

4. Criptografia de dados

Em ambientes IoT, a criptografia de dados desempenha um papel fundamental para garantir a segurança e privacidade das trocas de informações. Com o aumento do número de dispositivos conectados e a diversidade de tecnologias envolvidas, torna-se essencial proteger os dados transmitidos. A encriptação permite a codificação dos dados, tornado-os ilegíveis para qualquer pessoa, exceto autorizados, assegurando a confidencialidade das informações [Kim and Solomon 2014].

Existem várias abordagens para implementar a criptografia em IoT, sendo as mais comuns a criptografia simétrica e a criptografia assimétrica. Neste trabalho, optou-se por utilizar a criptografia assimétrica, que usa certificados digitais para realizar autenticação mútua entre os clientes e o *broker* MQTT. O algoritmo SHA-256 é empregado para garantir a integridade das mensagens, enquanto a cifração é realizada por meio do protocolo TLS (*Transport Layer Security*) versão 1.2, utilizando o algoritmo AES-256. A abordagem de criptografia assimétrica permite que as partes envolvidas se comuniquem utilizando apenas um canal público, eliminando a necessidade de trocar chaves antes da comunicação, tornando-a altamente conveniente em ambientes IoT onde a simplicidade e a eficiência são pontos cruciais [Kim and Solomon 2014].

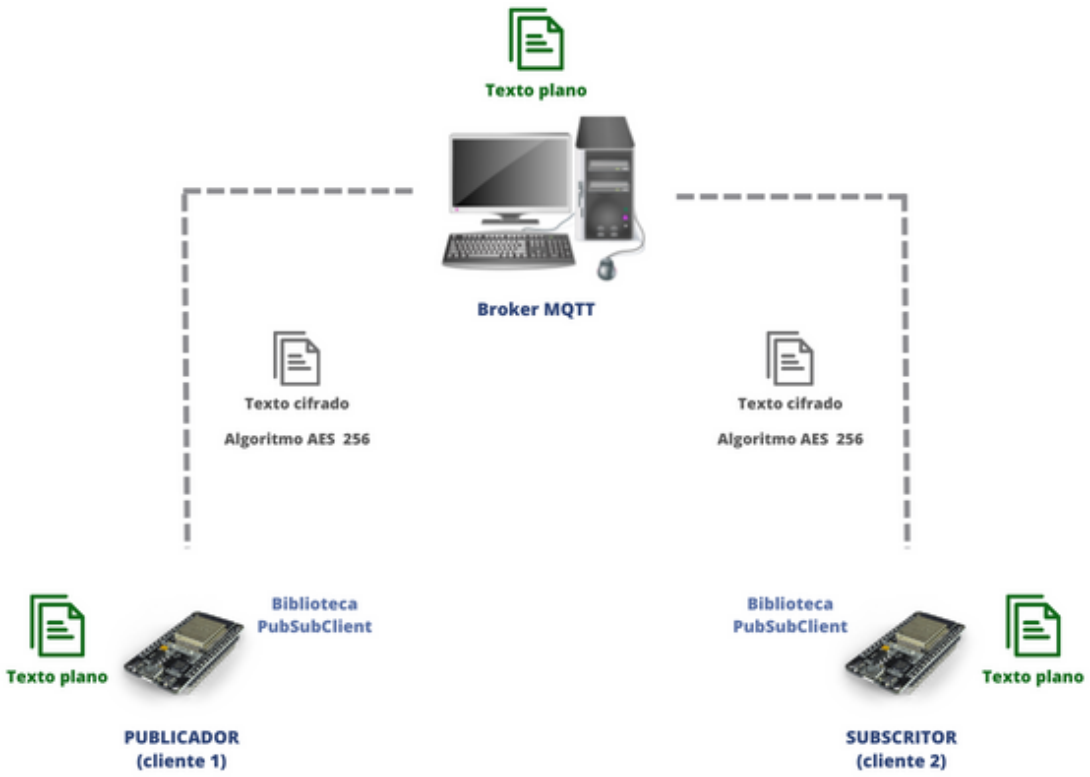

Figura 1. Funcionamento da criptografia nos testes realizados

5. Cenário de Testes

Durante os testes, foram usados microcontroladores *ESP32 DevKit v1* que atuam como clientes responsáveis por enviar e receber mensagens através do protocolo MQTT, utilizando a biblioteca *PubSubClient*. Esses microcontroladores são plataformas de desenvolvimento com suporte a Wi-Fi e *Bluetooth*, ideais para aplicações IoT. Além dos microcontroladores ESP32, também foi utilizado um *Access Point* dedicado, com a finalidade de fornecer a conectividade necessária aos dispositivos. A escolha de uma rede Wi-Fi dedicada busca reduzir possíveis interferências externas que possam afetar os resultados dos testes, como congestionamento de rede e conflitos de sinal.

A configuração do *broker* MQTT foi realizada em uma máquina virtual com 8 GB de memória RAM e 20 GB de armazenamento, executando o sistema operacional Ubuntu Server 22.04 LTS. A máquina hospedeira possui um processador Intel© Core™ i7-3770 CPU @ 3.40GHz x 4. A principal vantagem de usar uma máquina virtual é evitar que configurações anteriores interfiram nos testes realizados.

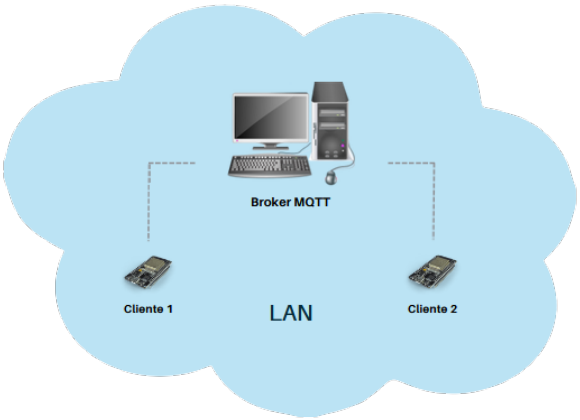

Figura 2. Ambiente de testes

5.1. Parâmetros dos testes

Para avaliar o impacto da criptografia assimétrica no consumo de energia nas comunicações MQTT, foram estabelecidos os parâmetros de teste a seguir, que foram aplicados em ambos os cenários, ou seja, com e sem a utilização de criptografia de dados:

- **Tamanhos das mensagens:** Foram implementadas diversas versões de código no dispositivo publicador, permitindo o envio de diferentes tamanhos de mensagens. Os tamanhos definidos foram 1024, 2048 e 4096 bytes. Essa abordagem permite representar diferentes cargas de dados em nossos testes.
- **Intervalo entre mensagens:** Foi configurado um envio contínuo de mensagens na frequência máxima, sem a utilização de atrasos programados entre as mensagens. Isso permitiu avaliar o consumo de energia sob condições de transmissão constante e na taxa máxima de envio de mensagens.
- **Análise com osciloscópio:** Foi utilizado um osciloscópio para monitorar a média da corrente em cada um dos dispositivo ESP32. A análise foi realizada em uma janela de 40 segundos, utilizando a ferramenta de ampliação (*zoom*) para focar apenas no pico da onda ou seja, quando ocorre o envio ou recebimento de mensagens.

6. Resultados obtidos

Nesta seção, serão apresentados os resultados obtidos ao analisar o consumo de energia dos dispositivos ESP32 durante a realização dos testes. Para medir esse consumo, foi utilizado um método simples e eficaz, conectando o ESP32 a uma fonte de alimentação de 5V através de um resistor de 1 Ohm. O osciloscópio forneceu a média da corrente elétrica durante um determinado período de tempo. Com base na corrente média obtida, é possível calcular a potência consumida, multiplicando-a pelo valor de tensão (em média, 4,98 V). Por fim, multiplica-se essa potência pelo período de tempo observado, para determinar o consumo de energia, em joules.

Ao analisar a taxa de envio das mensagens no cenário de testes utilizado, nota-se que são transmitidas aproximadamente 100 mensagens por segundo. Essa alta frequência de transmissão de dados é relevante para a análise do consumo de energia, uma vez que representa um cenário de carga elevada e constante nos dispositivos ESP32. Essa abordagem foi definida para causar um estresse na comunicação, pois em situações onde uma quantidade menor de mensagens é transmitida há uma maior dificuldade em analisar os impactos causados no consumo de energia dos dispositivos.

Os gráficos a seguir ilustram, de maneira comparativa, os valores referentes ao consumo energético das diferentes implementações, permitindo uma análise mais aprofundada do consumo de energia de cada dispositivo. Além disso, também é apresentado o consumo basal, que representa o consumo energético quando os dispositivos não estão publicando nem recebendo mensagens.

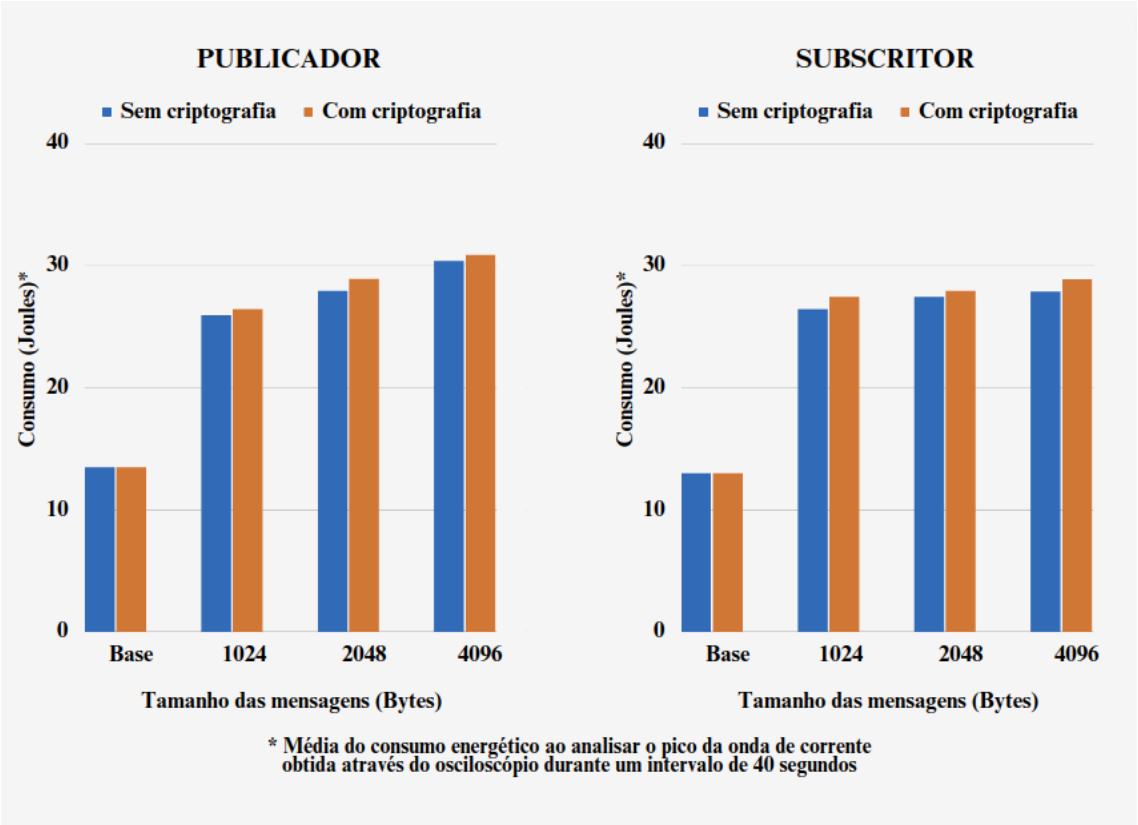

Figura 3. Gráficos comparativos do consumo energético nos dispositivos ESP32

Com base na análise dos dados coletados, fica evidente que o uso de mecanismos de criptografia assimétrica exerce uma influência sobre o consumo de energia, embora esse impacto seja observado de forma moderada e não represente uma alteração significativa nos recursos energéticos dos dispositivos presentes no cenário de testes durante a realização deste estudo. Diferente dos trabalhos relacionados, este trabalho utilizou microcontroladores ESP32 atuando como clientes, e os valores obtidos demonstraram uma notável proximidade entre o consumo de energia com e sem criptografia.

7. Conclusão

Este estudo investigou o impacto do uso de mecanismos de criptografia assimétrica no consumo de energia de dispositivos ESP32 em cenários de comunicação MQTT. Através da coleta e análise de dados, foi observado que a implementação de criptografia exerce uma influência moderada, mas não significativa, sobre o consumo de energia dos dispositivos. Os resultados revelam que, embora haja um aumento no consumo de energia à medida que o tamanho das mensagens aumenta, a diferença entre as configurações com e sem criptografia permanece relativamente estável.

É importante ressaltar que a segurança dos dispositivos IoT desempenha um papel fundamental no cenário atual, onde a conectividade está cada vez mais presente. A crescente proliferação de dispositivos IoT em várias áreas, desde ambientes residenciais até aplicações industriais, destaca a importância crítica da criptografia de dados. As descobertas indicam que a implementação da criptografia assimétrica, não compromete significativamente a eficiência energética dos dispositivos, tornando-a uma escolha viável e prudente para garantir a integridade e a privacidade dos dados em sistemas IoT.

Conforme a Internet das Coisas continua a crescer, a segurança permanece como um pilar fundamental. Este estudo fornece uma base sólida para a tomada de decisões no desenvolvimento de soluções IoT seguras e eficientes em termos energéticos. Porém, também sinaliza a necessidade de pesquisas adicionais para explorar os efeitos de diferentes métodos criptografia em dispositivos e contextos IoT variados, com o objetivo de otimizar os recursos energéticos e garantir a segurança nas comunicações.

Referências

Bayılmış, C., Ebleme, M. A., Ünal Çavuşoğlu, 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.

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

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

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

Paulo Spaccaquerche (2023). Aplicações de iot que se tornaram viáveis com o 5g. Acesso em 02 jun. 2023.

Quincozes, V., Quincozes, S., and Kazienko, J. (2021). Avaliando a sobrecarga de mecanismos criptográficos 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, Porto Alegre, RS, Brasil. SBC.