Detecção de Intrusões na Internet das Coisas (IoT): Um Ambiente de Experimentação para Obtenção de Dados Reais sobre Protocolos Emergentes

Isadora F. Spohr[1], Douglas R. Fideles[2], Silvio E. Quincozes[2,3], Juliano F. Kazienko[1], Vagner E. Quincozes[4]

[1]CT/CTISM – Universidade Federal de Santa Maria (UFSM) – Santa Maria, Brasil.

[2]FACOM — Universidade Federal de Uberlândia (UFU) – Uberlândia, Brasil.

[3]LEA, PPGES — Universidade Federal do Pampa (UNIPAMPA) – Alegrete, Brasil.

[4]IC – Universidade Federal Fluminense (UFF) – Niterói, Brasil.

ifspohr@inf.ufsm.br, x1douglas1x@gmail.com

silvioquincozes@unipampa.edu.br, kazienko@redes.ufsm.br

vequincozes@midiacom.uff.br

Abstract. *Efficient communication between Internet of Things (IoT) devices, especially in environments with limited computational resources, is a constant challenge. New protocols, such as Zenoh and the Data Distribution Service (DDS), have emerged to meet these demands, offering high performance and advanced features for large-scale distributed systems. However, the literature lacks public datasets for protocols like Zenoh and XRCE-DDS (eXtremely Resource Constrained Environments), limiting research in performance and security. This work presents the development of a detailed dataset on the performance of these protocols in various communication scenarios, providing a valuable resource for future research in real-time communication in IoT systems.*

Resumo. *A comunicação eficiente entre dispositivos da Internet das Coisas (IoT), especialmente em ambientes com recursos computacionais limitados, é um desafio constante. Novos protocolos, como o Zenoh e o Data Distribution Service (DDS), têm surgido para atender a essas demandas, oferecendo alto desempenho e recursos avançados para sistemas distribuídos e em larga escala. No entanto, a literatura carece de datasets públicos para protocolos como Zenoh e XRCE-DDS (eXtremely Resource Constrained Environments), limitando as pesquisas em desempenho e segurança. Este trabalho apresenta o desenvolvimento de um dataset detalhado sobre a performance desses protocolos em diversos cenários de comunicação, fornecendo um recurso valioso para futuras pesquisas em comunicação em tempo real em sistemas IoT.*

1. Introdução

Nos últimos anos, o paradigma da Internet das Coisas (IoT) vem crescendo exponencialmente, impulsionado principalmente por indústrias como saúde, agricultura e cidades inteligentes. A comunicação entre dispositivos representa um desafio significativo, especialmente em ambientes com recursos computacionais limitados.

Para atender à demanda de aplicações IoT, novos protocolos têm surgido, como o Zenoh, um protocolo Publish/Subscribe que se propõe a oferecer alto desempenho e recursos avançados para sistemas distribuídos e em larga escala. Em paralelo, o Data Distribution Service (DDS), um padrão de middleware para comunicação em tempo real e de baixo atraso, vem se destacando em sistemas embarcados, principalmente no campo da robótica [Zhang et al. 2023]. O DDS permite que as aplicações determinem variados aspectos da transferência de dados, como os requisitos de latência e taxa de transferência, através de suas políticas de Qualidade de Serviço (QoS) [Quincozes et al. 2024]. A implementação XRCE-DDS (eXtremely Resource Constrained Environments) foi criada especificamente para dispositivos com recursos limitados, como os utilizados em muitos sistemas IoT. O XRCE-DDS, quando comparado ao DDS, possui um número menor de objetos e operações, ao mesmo tempo que apresenta recursos adicionais para clientes remotos, tornando-o ideal para tais sistemas.

A disponibilidade de datasets é crucial para pesquisas acadêmicas, desenvolvimento industrial e aplicações em IoT. No entanto, a literatura carece de datasets públicos para protocolos como Zenoh e XRCE-DDS. Embora existam trabalhos onde uma rede experimental é construída para fins de comparação de desempenho envolvendo os protocolos XRCE-DDS, DDS, entre outros [Maggi et al. 2022, Liang et al. 2023], não se conhece um ambiente de experimentação destinado à produção de conjuntos de dados para detecção de intrusão através do protocolo XRCE-DDS ou Zenoh.

Este trabalho visa demonstrar o progresso na construção de um dataset detalhado sobre o desempenho de XRCE-DDS e Zenoh em diferentes cenários de comunicação. O dataset será um recurso valioso para pesquisas que buscam analisar o desempenho e a segurança de protocolos de comunicação em tempo real em sistemas IoT.

2. Referencial Teórico

O DDS é um protocolo de *middleware* focado em dados que permite comunicação em tempo real e de baixa latência, ideal para sistemas distribuídos e heterogêneos. Suas principais características incluem a garantia de baixa latência, essencial para aplicações IoT, e escalabilidade, capaz de suportar desde dispositivos limitados até sistemas conectados à nuvem, com potencial para escalar até milhões de participantes. Além disso, o DDS oferece diferentes níveis de Qualidade de Serviço (QoS), permitindo aos desenvolvedores definir parâmetros que assegurem a confiabilidade e o tempo de resposta conforme necessário [Foundation 2016, Quincozes et al. 2024].

O XRCE-DDS é uma implementação do DDS para dispositivos com recursos limitados. Suas vantagens incluem otimização para dispositivos com recursos reduzidos, comunicação eficiente em tempo real, proporcionando baixa latência, e suporte a vários protocolos de comunicação, incluindo TCP, UDP, Ethernet e Wi-Fi [Maggi et al. 2022].

O estudo de protocolos IoT, seu desempenho em variados ambientes e suas possíveis falhas de segurança e vulnerabilidades são de crescente interesse para a comunidade acadêmica [Abdulghani et al. 2020]. Certos protocolos, como o MQTT, possuem uma extensa literatura e diversos datasets desenvolvidos [Alatram et al. 2023, Hindy et al. 2020, Vaccari et al. 2020], possibilitando análises baseadas em diferentes métricas. Entretanto, protocolos mais recentes e menos populares, como o Zenoh, sofrem de lacunas na literatura, agravadas por múltiplas implementações, como o XRCE-DDS.

Não se conhece, até então, nenhum dataset público baseado nestes protocolos, fato que motivou o desenvolvimento do presente trabalho. Os principais trabalhos relacionados são resumidos na Tabela 1.

Tabela 1. Sumário de trabalhos relacionados.

Referência	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
[Abdulghani et al. 2020]	×	✓	✓	×	×	✓	×	×	×	×
[Maggi et al. 2022]	×	×	✓	β	×	✓	×	×	✓	✓
[Ferraz Junior et al. 2022]	×	✓	✓	β	×	×	×	✓	×	✓
[Dehnavi et al. 2021]	×	×	✓	✓	×	×	×	✓	×	✓
[Silva Cotta et al. 2023]	×	×	✓	✓	×	×	×	✓	×	✓
[Liang et al. 2023]	×	✓	✓	×	✓	×	×	✓	✓	×
[Alatram et al. 2023]	✓	✓	×	×	×	✓	✓	×	×	✓
[Hindy et al. 2020]	✓	✓	×	×	×	✓	✓	×	✓	×
[Vaccari et al. 2020]	✓	✓	×	×	×	✓	✓	×	✓	×
[Zhang et al. 2023]	×	✓	✓	×	✓	×	×	✓	✓	✓
[López Escobar et al. 2024]	×	×	×	×	✓	×	×	✓	×	✓
Este trabalho	✓	×	✓	✓	✓	α	α	✓	×	✓

Legenda para células: (β) Mencionado brevemente; (✓) Tratado no texto; (×) Não mencionado; (α) Versões futuras.

Legenda para Colunas: (1) Dataset, (2) MQTT, (3) DDS, (4) XRCE-DDS, (5) Zenoh, (6) Cenários de ataque, (7) Detecção de intrusão, (8) Análise de performance, (9) Simulação, (10) *Testbed*.

Em relação à implementação XRCE-DDS, [Maggi et al. 2022] analisam vulnerabilidades em serviços DDS, incluindo XRCE-DDS, recomendando práticas de mitigação. [Dehnavi et al. 2021] propõem um modelo XRCE-DDS bare-metal para sistemas embarcados distribuídos, avaliando desempenho em redes CompSOC e com modelagem SADF. [Silva Cotta et al. 2023] apresentam um método para avaliar a latência do XRCE-DDS, comparando-o com métodos de comunicação em veículos autônomos. Apesar de analisarem fatores de segurança e desempenho do XRCE-DDS, os trabalhos citados não disponibilizam datasets públicos baseados em seus ambientes de experimentação.

Outras pesquisas tratam do protocolo DDS, mas não da distribuição XRCE-DDS. [Ferraz Junior et al. 2022] avaliam o desempenho de sistemas *Publish-Subscribe* (AMQP, MQTT e OpenDDS) na comunicação entre dispositivos heterogêneos e a nuvem, focando em eficiência energética e segurança. [Liang et al. 2023] comparam o desempenho de Zenoh, MQTT, Kafka e DDS em termos de taxa de transferência e latência, testando em máquinas Ubuntu conectadas por Ethernet. Ambos os trabalhos são focados no desempenho dos protocolos, não tratando de cenários de ataque ou intrusão, além de não apresentarem datasets.

Para o protocolo Zenoh, [Zhang et al. 2023] comparam a taxa de transferência e latência de DDS, Zenoh e MQTT em comunicações *Edge-to-Edge* e *Edge-to-Cloud* em sistemas robóticos, avaliando também a precisão em um robô real. [López Escobar et al. 2024] propõem uma arquitetura IoT e comparam Zenoh e MQTT

na transmissão de mensagens via WiFi e 4G em *Cloud-to-Edge Continuum*. Nesses trabalhos tratando do Zenoh há, também, uma lacuna quanto à disponibilidade de datasets e à análises sobre a segurança do protocolo.

Em suma, enquanto diversos trabalhos abordam o desempenho dos protocolos DDS e Zenoh, há uma falta de datasets públicos para pesquisas. Este trabalho foca nos protocolos Zenoh e DDS, especialmente XRCE-DDS, gerando um dataset para análise de desempenho e funcionamento via *testbed*, porém, se tratando de um trabalho em andamento, nessa primeira versão apenas o XRCE-DDS é considerado na geração do dataset. Nas próximas versões, o protocolo Zenoh será adicionado às análises, permitindo que em trabalhos futuros sejam implementados cenários de intrusão para estudos de detecção de interações maliciosas.

3. Desenvolvimento

Este trabalho se propõe a mostrar o andamento da construção de um *dataset* detalhado sobre o desempenho do XRCE-DDS e do Zenoh em diferentes cenários de comunicação. No estado atual, o presente trabalho trata-se de um *dataset* parcial considerando o protocolo XRCE-DDS, a ser expandido e melhorado em versões futuras, incluindo o protocolo Zenoh na avaliação. Para obtenção do *dataset*, foi definido um *testbed* composto por diversos dispositivos, cada um com características específicas e funções distintas para realizar o experimento. Para simular um ambiente típico de comunicação em IoT, o *testbed* inclui três tipos diferentes de microcontroladores, referenciados na Tabela 2, cada um com suas próprias vantagens e desvantagens:

Característica	**NodeMCU V3**	**STM32F103C8T6**	**DOIT ESP32**
Arquitetura	32 bits	32 bits	32 bits
Clock	80MHz	72MHz	80 à 240 MHz
WiFi	Sim	Não	Sim
Bluetooth	Não	Não	Sim
RAM	160KB	20KB	512KB
FLASH	16MB	256KB	4MB
GPIOs	17	36	36
Interface	SPI/I2C/UART/I2S/SDIO	SPI/I2C/UART	SPI/I2C/UART/I2S/CAN/SDIO/IR/PWM

Tabela 2. Comparativo de microcontroladores para implementação de XRCE-DDS em sistemas IoT.

3.1. Descrição do Cenário

O cenário proposto para a análise do desempenho do XRCE-DDS envolve a utilização de diferentes microcontroladores e dispositivos agentes para criar um ambiente de comunicação distribuído e eficiente. O cenário completo contempla a configuração de nós sensores utilizando microcontroladores como DOIT ESP32 Bluetooth e WiFi, NodeMCU V3 e STM32F103C8T6, que enviam dados simulados de tempo, temperatura e umidade. Estes dados são gerados por um código específico e enviados a uma frequência parametrizável para um agente através do protocolo XRCE-DDS. Os agentes, implementados em dispositivos como Raspberry Pi 4, Banana Pi M2 Zero e um notebook Windows, recebem esses dados e os publicam em tópicos DDS, permitindo que assinantes na rede DDS leiam os dados. A coleta e análise dos dados são realizadas por um computador de

monitoramento equipado com o Wireshark, que captura os pacotes de dados transmitidos, fornecendo informações detalhadas sobre o tráfego de rede, como tamanho do pacote, tempo de envio, tempo de chegada, endereço de origem e destino, e detalhes do protocolo. O software utilizado inclui o Micro XRCE-DDS Client, Micro XRCE-DDS Agent, Fast DDS e Wireshark.

O cenário atualmente implementado para a prova de conceito consiste em um teste com três nós sensores NodeMCU V3, um agente (notebook Windows) e um notebook adicional para monitoramento e captura dos dados. Nesse teste, três ESP8266 atuam como nós sensores, enviando dados simulados de data/hora, temperatura e umidade para um agente que executa o Micro XRCE-DDS, publicando esses dados no tópico DDS "SensorData". A monitorização e coleta de dados são realizadas utilizando o Wireshark e scripts personalizados, bem como o *middleware Fast DDS*, para observar e analisar o desempenho do XRCE-DDS no ambiente proposto.

Para cada um dos cenários de teste (com e sem acesso à Internet), foram realizados experimentos com diferentes configurações de envio de dados. Em um cenário, os nós sensores enviaram pacotes de dados em intervalos fixos de um segundo, simulando uma taxa de atualização controlada. No outro cenário, não foi imposto nenhum limite na frequência de envio, permitindo que os sensores transmitam dados livremente, o que pode gerar um volume maior de tráfego na rede, tentando simular um ataque. Esta variação de padrões de envio de dados visa avaliar o desempenho do protocolo DDS XRCE sob diferentes condições de carga e tráfego de rede, contribuindo para uma análise mais abrangente de sua aplicabilidade em cenários reais de IoT.

3.2. Dataset Parcial Resultante

Os dados coletados do cenário proposto foram utilizados como entrada para a ferramenta CICFlowMeter[1]. O CICFlowMeter, desenvolvido pelo *Canadian Institute for Cybersecurity* (CIC), é uma ferramenta robusta para a extração de fluxos de rede e a criação de conjuntos de dados que são amplamente utilizados para pesquisas em segurança cibernética. Entre as principais características do CICFlowMeter, destacam-se a capacidade de calcular mais de 80 atributos de fluxo, como duração, bytes enviados e recebidos, número de pacotes, largura de banda, tempo entre pacotes, e medidas estatísticas, que são essenciais para a análise detalhada do tráfego de rede.

São disponibilizadas duas versões do *dataset*[2], um com acesso à internet e com dispositivos residenciais (*smartphones*, computadores, TVs, etc.) e outro com o tráfego isolado da internet e livre de tais interferências[3].

Referências

Abdulghani, R. M., Alrehili, M. M., Almuhanna, A. A., and Alhazmi, O. H. (2020). Vulnerabilities and security issues in iot protocols. In *2020 First international conference of smart systems and emerging technologies (SMARTTECH)*, pages 7–12. IEEE.

[1]Disponível em: `https://github.com/ahlashkari/CICFlowMeter`

[2]O conjunto de dados encontra-se disponível em `https://www.kaggle.com/datasets/submissaoanonima/xrce-dds-dataset-sbseg-2024/data`.

[3]O código-fonte e a descrição detalhada do dataset obtido, incluindo os atributos coletados e suas descrições, está disponível no GitHub `https://github.com/drsbg/XRCEDDSDatasetSBseg2024`

Alatram, A., Sikos, L. F., Johnstone, M., Szewczyk, P., and Kang, J. J. (2023). DoS/DDoS-MQTT-IoT: A dataset for evaluating intrusions in IoT networks using the MQTT protocol. *Computer Networks*, 231:109809.

Dehnavi, S., Goswami, D., Koedam, M., Nelson, A., and Goossens, K. (2021). Modeling, implementation, and analysis of XRCE-DDS applications in distributed multiprocessor real-time embedded systems. In *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1148–1151. IEEE.

Ferraz Junior, N., Silva, A. A., Guelfi, A. E., and Kofuji, S. T. (2022). Performance evaluation of publish-subscribe systems in IoT using energy-efficient and context-aware secure messages. *Journal of Cloud Computing*, 11(1):6.

Foundation, O. (2016). Scenario-aware dataflow. `https://opendds.org/`. Accessed: 19 jun. 2024.

Hindy, H., Bayne, E., Bures, M., Atkinson, R., Tachtatzis, C., and Bellekens, X. (2020). Machine learning based IoT intrusion detection system: An MQTT case study (MQTT-IoT-IDS2020 dataset). In *International networking conference*, pages 73–84. Springer.

Liang, W.-Y., Yuan, Y., and Lin, H.-J. (2023). A performance study on the throughput and latency of Zenoh, MQTT, Kafka, and DDS. *arXiv preprint arXiv:2303.09419*.

López Escobar, J. J., Díaz-Redondo, R. P., and Gil-Castiñeira, F. (2024). Unleashing the power of decentralized serverless IoT dataflow architecture for the Cloud-to-Edge Continuum: a performance comparison. *Annals of Telecommunications*, 79(3):135–148.

Maggi, F., Vosseler, R., Cheng, M., Kuo, P., Toyama, C., Yen, T., and Vilches, E. B. V. (2022). A Security Analysis of the Data Distribution Service (DDS) Protocol. *Trend Micro Research, Inc., Japan*, pages 15–20.

Quincozes, V. E., Quincozes, S. E., Kazienko, J. F., Gama, S., Cheikhrouhou, O., and Koubaa, A. (2024). A survey on IoT application layer protocols, security challenges, and the role of explainable AI in IoT (XAIoT). *International Journal of Information Security*, 23(3):1975–2002.

Silva Cotta, J. L., Agar, D., Bertaska, I. R., Inness, J. P., and Gutierrez, H. (2023). Latency Reduction and Packet Synchronization in Low-Resource Devices Connected by DDS Networks in Autonomous UAVs. *Sensors*, 23(22):9269.

Vaccari, I., Chiola, G., Aiello, M., Mongelli, M., and Cambiaso, E. (2020). MQTTset, a new dataset for machine learning techniques on MQTT. *Sensors*, 20(22):6578.

Zhang, J., Yu, X., Ha, S., Pena Queralta, J., and Westerlund, T. (2023). Comparison of DDS, MQTT, and Zenoh in Edge-to-Edge and Edge-to-Cloud Communication for Distributed ROS 2 Systems. *arXiv e-prints*, pages arXiv–2309.