XXXIII CONIC 23/24
Congresso de Iniciação Científica
Ciência em Movimento: Construindo o Futuro com Conhecimento
25 a 27 de Novembro de 2024

# Detecção de ataques maliciosos em sistemas ciberfísicos com redes MQTT

Matheus Figueiredo de Castro – *FAPEAM*
Iury Valente de Bessa - Universidade Federal do Amazonas

## RESUMO

O uso de tecnologias de Internet das Coisas (IoT) tornou-se mais prontamente disponível com o advento de sistemas ciberfísicos. Esse contexto motiva preocupações sobre segurança cibernética e a ocorrência de ataques maliciosos em redes de IoT. A proposta desta pesquisa investiga o problema da detecção automática de ataques cibernéticos em redes de IoT baseadas em *Message Queuing Telemetry Transport* (MQTT), implantando algoritmos de inteligência artificial para processar dados de tráfego e indicar se um ataque está ocorrendo ou não. Assim, este trabalho treina diferentes classificadores binários de inteligência artificial com base em aprendizado de máquina e compara seu desempenho para detecção de ataques maliciosos em sistemas ciberfísicos com redes de IoT baseadas em MQTT. Para treinar e testar os classificadores, foi empregado o conjunto de dados *MQTTset,* o qual contém muitas amostras rotuladas com tráfego legítimo e observações sob ocorrência de ataque. Ao analisar recursos de dados e pré-processamento, os algoritmos alcançaram bom desempenho na classificação do tráfego de rede, contribuindo para a segurança de sistemas ciberfísicos.

**Palavras-Chave:** Cibersegurança; Sistemas Ciberfísicos; Inteligência Artificial; Internet das Coisas; Aprendizado de Máquina.

**AGRADECIMENTOS**

Agradecemos ao Conselho Nacional de Desenvolvimento Científico e Tecnológico - Brasil (CNPq, processo 140593/2023-3) e da Fundação de Amparo à Pesquisa do Estado do Amazonas (FAPEAM, processos 01.02.016301.02763/2023-23, 01.02.016301.00673/2023-06 e Programa de Apoio à Iniciação Científica do Amazonas) pelo apoio financeiro.