IOT-TSO: UNSUPERVISED TENSOR-BASED CLASSIFICATION OF MALICIOUS IOT TRAFFIC

Author's: S. Divya[1], R. Surendiran[2], K. Sujith[3], N. Vanjulavalli[4]

Abstract

The rapid expansion of the Internet of Things (IoT) ecosystem has revolutionized connectivity across smart homes, healthcare systems, industrial automation, and smart cities. However, the increasing number of interconnected devices has significantly expanded the cybersecurity attack surface, making IoT networks highly vulnerable to sophisticated and large-scale cyber threats such as Distributed Denial of Service (DDoS), botnet propagation, port scanning, spoofing, and data exfiltration. Traditional intrusion detection systems (IDS) primarily rely on signature-based or supervised machine learning approaches that require labeled datasets. In dynamic IoT environments, obtaining comprehensive labeled traffic data is challenging, and supervised models often struggle to generalize to zero-day or evolving attack patterns. proposes a novel unsupervised framework for malicious traffic detection that models IoT network behavior using multi-dimensional tensor representations. Instead of analyzing flat feature vectors, the proposed system constructs a three-dimensional traffic tensor structured as Device × Time Window × Network Features. This tensor-based modeling preserves temporal correlations, device-level behavioral patterns, and inter-feature dependencies, enabling richer representation learning compared to traditional approaches.