IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

Survey on Malicious Packet Classification Techniques

Pratibha Tambewagh
Lecturer, Department of Information Technology
Bharati Vidyapeeth Institute of Technology, Kharghar, Navi Mumbai, Maharashtra, India

Abstract: *Malicious packet classification is a critical component in safeguarding network infrastructures against evolving cyber threats. Traditional methods, such as port-based and payload-based inspections, have become less effective due to the increasing use of encryption and sophisticated evasion techniques by attackers. Consequently, there has been a significant shift towards leveraging machine learning (ML) and deep learning (DL) approaches to enhance detection capabilities. Recent advancements highlight the efficacy of transformer-based models in analyzing raw payload data for identifying malicious traffic. For instance, a novel approach utilizing transformers demonstrated notable accuracy in distinguishing between benign and malicious packets, even when relying solely on payload bytes . Similarly, the adaptation of natural language processing techniques, such as Word2Vec, to network packet data has shown promise in automatic feature extraction, facilitating improved classification performance .The integration of convolutional neural networks (CNNs) and gated recurrent units (GRUs) has also been explored, particularly in the context of Internet of Things (IoT) networks, achieving high accuracy in both binary and multiclass classification tasks. Furthermore, the application of variational autoencoders (VAEs) has been investigated for detecting anomalies in network traffic, offering potential in identifying denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. In addition to these methods, the emergence of self-supervised learning and contrastive learning techniques has opened new avenues for enhancing the robustness of malicious traffic classification systems. These approaches aim to improve the generalization capabilities of models, particularly in scenarios involving encrypted or obfuscated traffic. Despite these advancements, challenges persist, including the need for large, labeled datasets, the handling of encrypted traffic, and the development of models resilient to adversarial attacks. Future research directions may focus on addressing these issues, as well as exploring hybrid models that combine multiple learning paradigms to bolster detection efficacy.*

Keywords: Packet classification,DD0S attacks, Cyber security

DOI: 10.48175/568