Sniff, Learn, detect: A Lightweight ML-Based Intrusion Detection Method Using Packet Features

Kushagra Gupta[a], Harshita Kumawat[a], Devika Kataria[a]

[a]*Department of Computer Science and Engineering, JK Lakshmipat University, Jaipur, Rajasthan, India*

Keywords: Malware Detection, Machine Learning, Naïve Bayes Classifier, Network Traffic Analysis

Abstract: Network sniffing is a technique used to monitor and analyze network traffic by identifying the types of packets, their source and destination IP addresses, ports, and the protocols in use. The effectiveness of packet sniffers can be significantly enhanced by incorporating machine learning algorithms to detect potential cyber-attacks targeting specific hosts. In this study, live network traffic was captured using sniffer developed using raw socket and packets of a DHCP starvation attack—generated through the Yersinia tool were captured. The captured packets were stored in PCAP format and converted into structured CSV datasets for analysis of attack. Through feature extraction and preprocessing, key attributes such as IP addresses, port numbers, protocol types (e.g., TCP, UDP, DHCP DISCOVER, ICMP), and packet sizes were derived and transformed into suitable inputs for machine learning models.

A Naive Bayes classifier was employed to categorize the packets as either normal or malicious. The study emphasizes enhancing detection accuracy, reducing false positive rates, and improving the adaptability and efficiency of the model. Techniques such as Laplace smoothing, feature binning, and scalable training were used to address the zero-probability problem and ensure model robustness.

To extend the detection capabilities beyond simple malicious/benign classification, the model incorporates a temporal analysis component. The attacks were further classified using a Decision Tree based on entropy or information gain per feature, in order to identify whether the attack had “Just Started,” was “Under Progress,” or had reached a “Critical” stage. The use of Decision Trees also provides transparency and interpretability, making it easier to audit the classification process and understand the contribution of each feature toward the final decision.

This paper proposes a computationally efficient and effective approach for real-time network threat detection. The integration of machine learning into packet sniffing holds significant promise for strengthening network security, particularly in Intrusion Detection Systems (IDS) and broader cybersecurity infrastructures.