A Multi-Branched Hybrid Perceptron Network for DDoS Attack Detection Using Dynamic Feature Adaptation and Multi-Instance Learning

ABSTRACT The increasing sophistication and frequency of Distributed Denial of Service (DDoS) attacks necessitate advanced detection systems. These attacks leave networks vulnerable to disruptions, resource overload, security breaches, and financial losses. Conventional detection systems suffer from high false positive rates, lower flexibility, and an inability to adapt dynamically to trending attack patterns. To address
these limitations, our proposed work introduces a novel approach to tackling these challenges by merging a
multi-branched hybrid perceptron network with dynamic feature adaptation and multi-instance learning. Our
methodology features three key innovations: 1) Multi-Branched Hybrid Perceptron architecture, 2) Dynamic
Feature Adaption, and 3) Dynamic Attention-Weighted Feature Fusion to improve feature representation and merging process. The proposed study was validated on three testing datasets: 1) UNSW-NB15, 2) CICIDS
2017, and 3) CIC-IDS 2018, and the results were compared with various state-of-the-approaches. The experimental results show that our model significantly outperforms existing methods. On UNSW-NB15, the
model achieves an accuracy of 96.02% with a precision of 0.965, a recall of 0.963, and an F1-score of 0.9645.
For CIC-IDS 2017, it reaches a near-perfect accuracy of 99.99% with all metrics at 1.00. On CIC-IDS 2018,
the model performs with an accuracy of 99.96% and perfect precision, recall, and F1-scores of 1.00. Time complexity analysis shows that while the proposed intrusion detection framework takes 21.6 seconds on CICIDS
2017, 30.0 seconds on CSE-CIC-IDS2018, and 15.5 seconds on UNSW-NB15, it remains competitive with high performance. Despite its higher time complexity on UNSW-NB15, MHHPN provides superior detection capabilities, making it practical for real-time use in complicated and extensive networks.