ABSTRACT

Distributed Denial of Service (DDoS) attacks pose a major risk to the availability and security of modern network infrastructures. Their growing complexity and scale have outgrown traditional defense methods. Current solutions such as firewalls and standard intrusion detection systems often can't adapt to handle complex and changing intrusion patterns leading to inefficiencies in detection and mitigation. This issue majorly affects industries like finance and e-commerce where security breaches can cause huge damage. To address these problems, this study suggests a new smart Intelligent Intrusion Detection System (IDS) framework that understands complexity. This aims to detect threats with better accuracy, minimized computing power, and have few false alarms. This helps to boost security and availability against the changing world of cyber threats.

This thesis aims to create a complexity aware intelligent IDS to fix the problems with current systems. It combines cutting-edge machine learning (ML) and deep learning (DL) models with nature-inspired optimization algorithms to make DDoS attack detection more accurate faster, and stronger. Feature Engineering is the major focus in identifying the right features and making the intrusion detection model better with minimized resources. The novelty of the research lies in developing advanced, complexity-aware intrusion detection systems for DDoS attacks, leveraging innovative methods like Combined Filter for Feature Selection (CFFS), bio-inspired Dragonfly Optimization, Panthera Leo Optimization, and an Attention-Enabled Gated Recurrent Network (AEGRN) to achieve significant detection accuracy, computational efficiency, and adaptability across diverse datasets.

A significant contribution of this research is the development of four distinct methodologies. The first contribution enhances the detection of single-vector DDoS attacks using a Combined Filter for Feature Selection (CFFS) integrated with a Decision Tree (DT) classifier. This method achieved an accuracy of 97.69%, with precision and recall exceeding 99% and a false positive rate of 6.32%. However, its performance declined when applied to multiple flooding attacks, indicating the need for more robust techniques.

The second contribution introduces the Improved Dragonfly Optimization Algorithm (IDOA) alongside a Decision Tree (DT) classifier to enhance detection

accuracy for multi-vector DDoS attacks. This approach achieved 98.89% accuracy, with precision and recall above 97%, an F-score of 98%, demonstrating significant efficiency while leaving room for further improvements in accuracy and efficiency.

The third contribution involves an Integrated Intrusion Detection System (IDS) based on the Panthera Leo Optimization (PLO) technique combined with a multilayer feedforward network. This method successfully managed network traffic complexity and variability while maintaining low computational latency. Using the CICDDoS2019 dataset, it achieved a prediction accuracy of 96.8%.

The final contribution presents a novel Attention-Enabled Gated Recurrent Network (AEGRN) for detecting DDoS attacks across multiple datasets. This IDS demonstrated over 98% generalization accuracy across various datasets, with an average processing time of 17.4 seconds per epoch. Self-attention maps with BiGRU and feedforward networks proved beneficial in achieving better classification accuracy with reduced complexity and processing time.

The proposed models have been evaluated using standard performance metrics such as accuracy, precision, recall, F1-score, and computational time. Statistical validation using techniques such as ANOVA and p-tests has confirmed the reliability and significance of the improvements observed. This thesis provides a novel and effective framework for detecting DDoS attacks through the integration of advanced ML, DL, and optimization techniques. The proposed solutions demonstrate notable performance in terms of accuracy, scalability, and computational efficiency, making them suitable for deployment in real-world scenarios. Future research should focus on validating the effectiveness of the developed model on real-time datasets to better reflect real-world cyber threats. Additionally, efforts should be made to assess the model's capability in identifying and mitigating AI-enhanced and Deep DDoS threats, ensuring robustness against evolving attack strategies that leverage artificial intelligence.