SPECIMEN FORMAT FOR THESES OF MONTH

Faculty	:	School of Physical and Computational Sciences
Department	:	Computer Science
Branch/ Area:	:	Cyber Security
Sub Subject Heading:	:	Intelligent Intrusion Detection Systems, Network Security, Deep Learning, Machine Learning, Optimization Techniques
Candidate's Name	:	M. Kalaivani
Candidate's Address with email	:	30, Udaiyar Street, Nathegounden Pudur, Alandurai, Coimbatore – 641101 Kalaivaniprathap23@gmail.com
Title of the thesis	:	Complexity Aware Intelligent Intrusion Detection for DDoS Attacks
(i) In Roman Script	:	-
(ii) In roman Script	:	-
Nomenclature of Degree:	:	Ph.D
Month & Year of Enrolment:	:	July 2018
Month & Year of Registration:	:	July 2018
Month &Year of Submission:	:	January 2025
Month &Year of Award	:	July 2025
Name of Supervisor	:	Dr G. Padmavathi
Designation of Supervisor	:	Professor, Department of Computer Science, Avinashilingam Institute for HomeScience and Higher Education for Women, Coimbatore – 641043
Centre/department/school in which research was conducted	:	Department on Computer Science
University's Name & Address	:	Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore – 641043

Abstract within 300 words:

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 an Intelligent Intrusion Detection System (IDS) framework that understands complexity. This aims to detect threats with high 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. 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 high 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 high 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 an 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. Although other models such as Op-LSTM, GRU, and LSTM were comparatively performing well, the integration of self-attention maps with BiGRU and feedforward networks proved beneficial in achieving improved 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 significant 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.

i) Major objectives :

- **Primary Objective**

  To design a complexity-aware, intelligent intrusion detection system (IDS) for DDoS attack detection using advanced feature engineering ensuring improved accuracy, adaptability, and efficiency across multiple datasets.

- **Secondary Objectives**
    1. To accurately detect single-vector DDoS flooding attacks with improved detection accuracy and reduced computational time.
    2. To detect multi-vector DDoS flooding attacks with high performance and a low false alarm rate.
    3. To detect multiple DDoS attacks with scalability, low false positives, and efficient execution.
    4. To effectively identify DDoS attacks across multiple datasets with reduced computational complexity and enhanced performance.

ii) Hypothesis:

H1: Integrating optimized feature selection and classification techniques will significantly improve detection accuracy and reduce computational time for single-vector DDoS attacks.

H2: Hybridization of bio-inspired optimization algorithms with machine learning classifiers will enhance detection performance and reduce false alarms in multi-vector DDoS scenarios.

H3: Employing deep learning models optimized for complexity and scalability will result in robust detection of multiple DDoS attack types across datasets with improved precision and execution time.

H4: A progressive, multi-phase IDS framework can adaptively respond to varying DDoS complexities, offering superior detection capability over traditional methods.

iii) Methodology :

The research is structured in four progressive phases:

- Phase I: Detection of single-vector DDoS flooding attacks using
    - Ensemble-Based Combined Filter (CFFS) for feature selection
    - Decision Tree (DT) classifier

      → Achieved high detection accuracy with reduced computational time.
- Phase II: Identification of multi-vector DDoS flooding attacks by
    - Hybridizing Improved Dragonfly Optimization Algorithm (IDOA) with DT

- Using enhanced feature engineering

  → Lower false alarm rate and improved performance.

- Phase III: Detection of multiple DDoS attacks using
  - Panthera Leo Optimized Multilayer Feed Forward Neural Network (PLO-MLFFN)

    → Achieved high accuracy and scalability across training/testing splits.
- Phase IV: Detection across multiple datasets using
  - Attention-Enabled Gated Recurrent Networks (AEGRN)
  - Deep Feed Forward Networks

  → Addressed scalability, reduced complexity, and ensured robustness.

Cross-validation, comparative evaluation, and rigorous experimentation were used in each phase to ensure robustness and reliability.

iv) Findings:

Phase I:

- The proposed CFFS-DT approach in Phase I significantly outperformed other models by achieving 97.69% accuracy, 99.13% precision, and 98.50% recall, with the lowest error rate of 2.40% and fastest execution time of 1.2 seconds. This demonstrates the effectiveness of the Correlation-based Feature Selection (CFFS) method in improving both the performance and efficiency of the Decision Tree classifier for DDoS detection.

Phase II:

- In Phase II, the proposed Improved Dragonfly Optimization Algorithm with Decision Tree (IDOA-DT) classifier delivered superior performance compared to other classifier combinations. It achieved the highest accuracy (98.89%), precision (98.00%), recall (97.00%), and F-score (98.00%), while maintaining the lowest false positive rate (6.71%), lowest error rate (4.99%), and shortest execution time (0.69 seconds).

- These results clearly demonstrate the effectiveness of the IDOA-DT combination in providing a fast, accurate, and reliable solution for intrusion detection in DDoS

scenarios. The cross-validation results further validate its robustness and generalizability across different data splits.

.Phase III:

- The proposed PLO-MLFFN model achieved consistently high performance across metrics: Accuracy – 96.8%, Precision – 96.75%, Recall – 96.73%, Specificity – 96.5%, and F1-score – 96.89%.
- It demonstrated the fastest detection time of 7.5–7.6 seconds per epoch, maintaining low latency even with increasing proportions of test data.
- The model showed robust and reliable classification across multiple DDoS attack types, with over 96% correct classification for each category in the confusion matrix.
- It outperformed existing models (SVM, CART, ELM, BAT-ELM) in both detection time and metric-based evaluation, indicating strong generalization.
- While highly effective, scalability remains limited, suggesting the need for further optimization in large-scale deployments.

Phase IV:

- The AEGRN and Deep Feedforward Neural Network (FFN) models demonstrated robust performance across multiple benchmark datasets (CICDDoS2019, UNSW, NSL-KDD Train/Test).
- The proposed model consistently outperformed LSTM, GRU, and Op-LSTM in terms of model building time (MBT), averaging just 17.4 seconds per epoch, indicating faster training and reduced computational cost.
- Validation curves across all datasets showed minimal gap between training and testing accuracy, with an extremely low RMSE of 0.001, proving strong generalization ability.
- The architecture maintained high detection precision and scalability, effectively handling complex DDoS patterns while optimizing runtime performance.
- Overall, the model balances efficiency, accuracy, and scalability, aligning well with the goal of a complexity-aware intelligent intrusion detection system.

Overall, the proposed framework significantly enhanced detection performance, reduced false alarms, and minimized computational complexity, making it a strong candidate for real-time DDoS detection in modern networks.

Examiners

Internal Examiner :

Dr. Manjaiah D.H

Senior Professor & Chairman, Dean, Faculty of Science and Technology

Department of PG Studies and Research in Computer Science, Mangalore University, Mangalore – 574199, Karnataka, India

External Examiner :

Professor Dharmendra Sharma AM

Professor of AI, University of Canberra, Australia

175 William Webb Drive, McKellar ACT 2617, Australia