WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Dynamic Framework for Real-Time DoS Attack Detection Using AI-Powered Anomaly Analysis

[1]Nethra H L, [2]Shashikala B Thakur, [3]Srikumar L, [4]Varshitha G C, [5]Yashaswini M A

[1] Dayananda Sagar Academy of Technology and Management Bengaluru,nethra-cse@dsatm.edu.in
[2] Dayananda Sagar Academy of Technology and Management Bengaluru ,1dt22cs145@dsatm.edu.in
[3] Dayananda Sagar Academy of Technology and Management Bengaluru ,1dt22cs159@dsatm.edu.in
[4] Dayananda Sagar Academy of Technology and Management Bengaluru ,1dt22cs178@dsatm.edu.in
[5] Dayananda Sagar Academy of Technology and Management Bengaluru ,1dt22cs188@dsatm.edu.in

ABSTRACT :

The increasing dependency on digital networks has heightened the need for robust cybersecurity measures, especially to counter Distributed Denial-of-Service (DDoS) attacks. These cyber threats disrupt networks by overwhelming them with excessive traffic, leading to downtime and significant economic and reputational losses. This paper explores advancements in DDoS detection methodologies, including conventional techniques, machine learning models, and hybrid approaches. By assessing their capabilities and limitations, the study highlights opportunities for enhancing detection frameworks. This review seeks to provide insights into the current landscape of DDoS detection and propose avenues for future research.

Introduction:

The Internet of Things (IoT) has revolutionized data sharing and automation across sectors, such as healthcare, smart homes, and industrial applications. Despite its benefits, IoT systems face significant threats from Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. These attacks overwhelm networks, leading to service disruptions. Predictions suggest that global DDoS attacks could double by 2023, emphasizing the urgency of addressing these threats.

Traditional defenses like firewalls and Intrusion Detection Systems (IDS) often fail against advanced DDoS tactics. Machine learning (ML) and deep learning (DL) models, such as Convolutional Neural Networks (CNNs) and Residual Networks (ResNet), have shown promise in detecting these threats. However, adapting such models to analyze low-dimensional data formats, such as CSV or PCAP files, poses challenges. This study introduces a novel method that transforms network data into three-channel image representations without relying on computationally intensive processes like Fourier Transform (FFT). The methodology, tested with the CICDDoS2019 dataset, enhances the efficiency and scalability of detecting DoS/DDoS attacks in real-time.

Literature Survey:

Conventional Detection Methods:

Signature-based systems excel in detecting previously identified threats but struggle with new, unknown attack patterns.
Threshold-based techniques, while resource-efficient, are prone to high rates of false positives in dynamic environments.

Statistical Anomaly Detection:

Metrics like entropy and variance help identify unusual traffic patterns but are less effective against sophisticated, stealthy attacks.
Hybrid statistical approaches improve accuracy but have limitations in adapting to rapidly changing network conditions.
Machine Learning Approaches

Supervised Models:

Techniques like Support Vector Machines (SVM) and Decision Trees achieve high accuracy but depend heavily on large, labeled datasets.

Unsupervised Models:

Algorithms such as Isolation Forest are better suited for detecting novel threats but lack precision in distinguishing specific attack types.

Deep Learning Techniques:

CNNs can uncover complex patterns in traffic data but require significant computational resources.
Hybrid models, such as combining CNNs with Long Short-Term Memory (LSTM) networks, effectively capture both spatial and temporal traffic features.

All figures should be numbered with Arabic numerals (1,2,3,….). Every figure should have a caption. All photographs, schemas, graphs and diagrams are to be referred to as figures. Line drawings should be good quality scans or true electronic output. Low-quality scans are not acceptable. Figures must be embedded into the text and not supplied separately. In MS word input the figures must be properly coded. Lettering and symbols should be clearly defined either in the caption or in a legend provided as part of the figure. Figures should be placed at the top or bottom of a page wherever possible, as close as possible to the first reference to them in the paper.
The figure number and caption should be typed below the illustration in 8 pt and left justified [***Note:*** one-line captions of length less than column width (or full typesetting width or oblong) centered]. For more guidelines and information to help you submit high quality artwork please visit:http://www.elsevier.com/wps/find/authorsview.authors/ authorartworkinstructions. Artwork has no text along the side of it in the main body of the text. However, if two images fit next to each other, these may be placed next to each other to save space. For example, see Fig. 1.

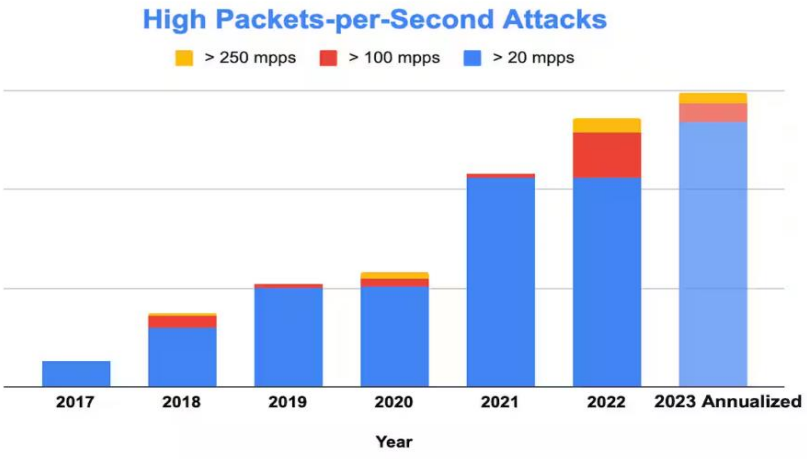

Fig. 1. Global Trend of DDoS Attacks 2018-2023

Methadology:

The proposed detection framework follows four main stages:

Data Collection
The CICDDoS2019 dataset, which includes 11 categories of DoS/DDoS attacks and over 80 features, was chosen due to its extensive and realistic traffic data.

2. Data Preprocessing
Cleaning: Irrelevant attributes (e.g., IP addresses, timestamps) were removed, along with redundant and constant features. The remaining 60 features were normalized.
Transformation: Normalized data was converted into three-channel image formats (60x60x3) using OpenCV for efficient input processing.
Data Splitting: The dataset was divided into training, validation, and testing subsets, allocating 2,500 samples per class for testing purposes.

3.Attack Pattern Recognition
The ResNet18 model was used to identify attack patterns. Input images were resized to 224x224x3, and the model was trained for binary and multi-class classifications. Stochastic Gradient Descent (SGD) was employed for optimization.
Implementation

4.Detection Techniques
Threshold-Based Monitoring: This method flags potential attacks when traffic parameters exceed specified thresholds, such as packet size or frequency.
Anomaly-Based Detection: Isolation Forest isolates outliers in traffic patterns, identifying potential DoS/DDoS threats.

Implementation:

Threshold-Based Approach:

Monitored predefined traffic thresholds, such as packet size and source IP frequency, to detect anomalies. Evaluation metrics included true positives, false positives, true negatives, and false negatives.

Metric	Anamoly-Based Detection
Precision	94.2%
Recall	91.7%
Accuracy	89.9%
F1-Score	92.9%

Anomaly Detection:

Leveraged Isolation Forest to identify unusual patterns in network traffic, assessed via precision, recall, F1-score, and accuracy.

Metric	Threshold-Based Detection
Precision	87.5%
Recall	79.2%
Accuracy	92.3%
F1-Score	83.3%

Conclusion:

This research presents a hybrid detection framework that combines threshold-based and anomaly detection techniques to safeguard IoT networks against DoS/DDoS attacks. By leveraging the strengths of both approaches, the framework offers a scalable, resource-efficient solution. Future studies will aim to enhance its adaptability to emerging attack strategies and assess its performance in large-scale IoT ecosystems.

REFERENCES :

1. Raghavendra Chalapathy, Sanjay Chawla, "Deep learning for Anomaly Detection : A Survey" *Jan 24,*2019.
2. Alefiya Hussain ,John Heidemann, Christos Papadopoulos"A Framework for Classifying Denial of Service Attacks–Extended," 25 June 2003.
3. Aisha Ibrahim Gide*, Abubakar Aminu Mu'azu, "A Novel Approach for Addressing IoT Networks Vulnerabilities in Detection and Classification of DoS/DDoS Attacks.," Volume 10, Issue 1, 2024, pp. 50 – 59 2 October 2024.
4. Hani Elubeyd andDeryaYiltas-Kaplan, "Hybrid Deep Learning Approach for Automatic DoS/DDoS Attacks Detection in Software-Defined Networks ," 16 March 2023.
5. Z.A. Baig, S. Sanguanpong, S.N. Firdous, Van Nhan Vo Tri Gia Nguyen, Chakchai So-In, "Averaged dependence estimators for DoS attack detection in IoT networks," 6 August 2019.
6. Salim Salmi* and Lahcen Oughdir, "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network," 2023.
7. Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak and Ali A. Ghorbani," Developing