International Journal of Research in Engineering, Science and Management
Volume 8, Issue 5, May 2025
https://www.ijresm.com | ISSN (Online): 2581-5792

DDOS Attack Detection and Mitigation

Indumati M. Girevvagol[1*], K. N. Prajna[2], S. K. Prajwal[3], Sanmit Patole[4], C. R. Shivanagi[5]
[1,2,3,4]Student, Department of Information Science and Engineering, Basaveshwar Engineering College, Bagalkot, India
[5]Assistant Professor, Department of Information Science and Engineering, Basaveshwar Engineering College, Bagalkot, India

***Abstract*: Distributed Denial of Service (DDoS) attacks have become a significant threat to the stability and availability of online services. These attacks aim to overwhelm a target server, network, or application with a flood of traffic, leading to service disruption, data breaches, and financial losses. This project focuses on developing a robust system for the detection and mitigation of DDoS attacks using advanced machine learning techniques and network analysis. The proposed solution integrates real-time traffic monitoring, anomaly detection algorithms, and adaptive response mechanisms to identify malicious traffic patterns early and respond effectively to minimize service downtime. By leveraging data from multiple layers of the network, the system enhances detection accuracy while reducing false positives. The ultimate goal of this project is to create a scalable and efficient DDoS protection framework that can proactively defend against evolving attack strategies, ensuring consistent and secure access to online resources.**

***Keywords*: DDoS, machine learning, anomaly detection, real-time monitoring, adaptive response, network analysis, cybersecurity, scalable framework.**

1. Introduction

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic.

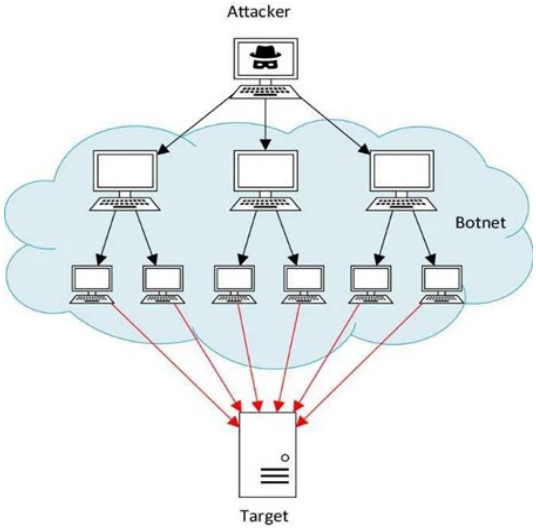

Fig. 1. DDOS attack

Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination. It's critical to act soon after discovering a DDoS attack since it provides you the chance to avert significant disruption. The server can start to crash on waiting too long, and a full recovery might take hours. The hardest part about mitigating a DDoS attack is that often it's virtually impossible to do so without impacting legitimate traffic. This is because attackers go to great lengths to masquerade fake traffic as real.

2. Objectives

Our project aims to address the challenges posed by DDoS attacks, which are often used to distract cybersecurity teams while enabling other malicious activities like data theft or network infiltration. Using Mininet, we will simulate a software-defined network (SDN) topology and manage it through the Ryu controller to monitor network flows and detect DDoS attacks effectively.

A comprehensive dataset will be generated, containing both normal and DDoS attack traffic, to train and evaluate machine learning models. Random Forest algorithm will be employed to classify network traffic as either legitimate or malicious, leveraging its ability to detect patterns with high accuracy. Additionally, a mitigation module will be developed to automatically respond to detected DDoS attacks by filtering malicious traffic or implementing rate-limiting measures, thereby minimizing the attack's impact on the network and ensuring service continuity.

3. Literature Survey

A. Detection and Mitigation of DDoS Attacks in SDN

The survey reviews DDoS detection and mitigation techniques in SDN, categorizing solutions as information theory, machine learning, and neural network-based. It highlights SDN vulnerabilities like flow table overflow and control plane bottlenecks while addressing research gaps. Future work emphasizes AI-driven, scalable solutions for robust DDoS defence in SDN environments. It involves gathering a wide range of variables, including a country's population, sports infrastructure, and previous Olympic performance. Second, the model uses machine learning

*Corresponding author: girevvagoli@gmail.com

algorithms, such as regression analysis and classification techniques, to predict the number of medals each country might win. The complex task of filtering relevant variables and making accurate predictions is simplified through the use of these advanced algorithms.

B. An Effective Mechanism to Mitigate Real-Time DDoS Attack

The report introduces a real-time DDoS mitigation mechanism combining optimized SVM and Snort IPS, achieving 97% detection accuracy. It detects attacks early, identifies attack routes, and blocks malicious traffic. The method is effective against evolving DDoS threats, reducing false positives and negatives for enhanced network security.

C. DDoS Attack Detection and Mitigation in SDN Using Machine Learning

The report proposes a DDoS attack detection and mitigation model for SDN using machine learning. The model extends native flow features with new metrics like average packet size and recent flow statistics. Among six evaluated ML algorithms, Random Forest performed best. The system detects and blocks attacks accurately while minimizing disruptions to normal traffic.

D. DDoS Attack Detection and Mitigation Using Anomaly Detection and Machine Learning Models

The survey reviews that Distributed Denial of Service (DDoS) attacks are a critical threat to cybersecurity, disrupting services and causing significant financial and reputational damage. This paper proposes a comprehensive DDoS detection and mitigation system leveraging machine learning and anomaly detection techniques. The system combines algorithms such as Fast Entropy and Attribute Threshold for anomaly detection with machine learning models like Bidirectional LSTM and Random Forest to classify network traffic Results show improved detection accuracy and reduced false positives, making the system effective for real-time DDoS defence.

E. DDoS Attack Early Detection and Mitigation System on SDN Using Random Forest Algorithm and Ryu Framework

The paper proposes a DDoS detection and mitigation system for Software-Defined Networks (SDN) using the Random Forest algorithm. Implemented with the Ryu framework, it achieved 98.38% accuracy, 36ms detection time, and reduced CPU usage by 44.9%, enhancing SDN security through efficient traffic classification and flow-based mitigation.

F. DDoS Attacks Detection and Mitigation in SDN Using Machine Learning

The paper explores DDoS detection and mitigation in Software-Defined Networks (SDN) using machine learning techniques like J48, Random Forest, SVM, and K-NN. J48 outperformed others, offering high accuracy and efficiency. The proposed framework, implemented in Mininet with RYU, identifies and blocks malicious traffic, enhancing SDN security while maintaining network performance.

G. Detection and Mitigation of DDoS Attacks in Network Traffic Using Machine Learning Techniques

The paper explores the methods for detecting and mitigating DDoS attacks within Software-Defined Networking environments. By employing machine learning algorithms such as LSTM, SVM, and logistic regression, it successfully classifies malicious and benign traffic with high accuracy. LSTM stands out with an impressive 99.04% accuracy, thanks to its ability to model sequential data, underscoring its effectiveness in DDoS detection.

H. Detection and Mitigation of DDOS Based Attacks Using Machine Learning Algorithm

The paper presents a detection system for DDoS attacks from the victim's perspective, utilizing the K-Nearest Neighbours (KNN) algorithm. It examines network traffic features to identify suspicious patterns and counteract attacks by temporarily blocking traffic. Simulations conducted with the DARPA2009 dataset demonstrate its effectiveness, providing a scalable and efficient method for mitigating DDoS attacks.

I. Distributed Denial of Service Attack Mitigation Using High Availability Proxy and Network Load Balancing

The paper examines methods for mitigating DDoS attacks through the use of HAP Roxy and Network Load Balancer (NLB) techniques on both Windows and Linux platforms. It assesses performance by analysing response time and CPU usage during SYN DDoS attacks. The findings indicate that NLB is more effective in minimizing response time, underscoring successful mitigation strategies in SDN environments.

4. Methodology

The methodology utilizes a structured approach to detect and mitigate DDoS attacks with machine learning. It begins by analysing network traffic and extracting key features such as traffic rate and packet size. A labelled dataset is then created, pre-processed, and used to train a Random Forest model for real-time classification of legitimate and malicious traffic. Once malicious traffic is detected, mitigation strategies such as traffic filtering, rate limiting, and IP blocking are applied to safeguard the network.

This approach ensures accurate detection, real-time response, and uninterrupted service for legitimate users, providing a scalable and robust defense against DDoS attacks.

A. Software & Tools

- *SDN Simulation*: Mininet for virtual network topology creation
- *RYU controller*: SDN controller for traffic management
- *Machine Learning*: Python, Scikit learn (Random Forest algorithm), Numpy & Pandas
- *Traffic generation*: hping3 for ICMP flood attacks
- *Virtualization*: VirtualBox/Vmware

B. Hardware

- *Processor*: Intel Core i3 or higher
- *RAM*: 4 GB+
- *Storage*: 20 GB+ free space
- *Network Interface*: Ethernet, Wi-Fi for virtual network simulation.

C. System Design

The design architecture of the system developed for DDoS attack detection and mitigation is described in detail. Diagrams included serve as a blueprint for implementation, offering clarity on the system's operational flow and interactions.

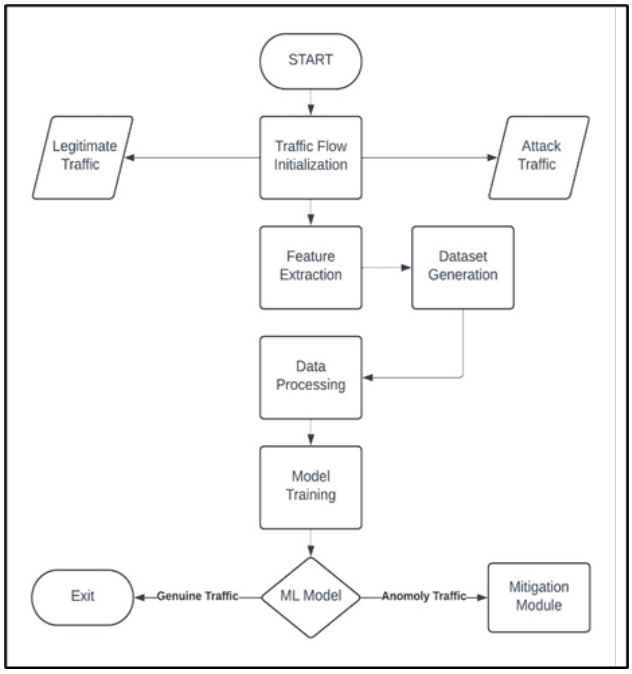

Fig. 2. Implementation steps

1) Step 1: Traffic Flow Initialization

Input: The system begins by capturing all incoming network traffic, including both legitimate user requests and potential attack traffic (e.g., SYN floods, UDP floods). This raw data is collected from network routers, firewalls, or packet sniffing tools in real-time.

Process: The traffic is monitored without any initial filtering or classification. The system logs fundamental packet information such as source/destination IPs, timestamps, and protocol types. Specialized tools ensure high-speed capture without introducing network latency.

Output: Unprocessed network traffic data containing complete packet headers and payload information, ready for deeper analysis in the next stage.

2) Step 2: Feature Extraction

Input: The raw traffic data collected during initialization.

Process: The system analyzes each packet to extract meaningful features that help distinguish normal traffic from attacks. Key features include:

- Packet rate (requests per second)
- Packet size distribution
- Protocol-specific characteristics (e.g., TCP flags)
- Connection duration and timing patterns
- Geographic anomalies in source IPs

Statistical methods and machine learning techniques identify patterns that may indicate malicious behaviour.

Output: A structured dataset where each network flow is represented by a set of numerical features, enabling machine learning analysis.

3) Step 3: Dataset Generation

Input: Extracted feature vectors from network traffic.

Process: The system labels the data by categorizing traffic as either "legitimate" or "malicious." Attack samples are obtained from known DDoS datasets or simulated attacks. The dataset is balanced to ensure the model trains effectively on both attack and normal traffic.

Output: A labelled dataset with feature vectors and corresponding classifications, ready for machine learning training.

4) Step 4: Data Processing

Input: The labelled dataset containing raw feature values.

Process: The data undergoes preprocessing to improve model performance:

- *Normalization*: Scales features to a common range (e.g., 0 to 1).
- *Feature Selection*: Removes redundant or irrelevant features.
- *Data Cleaning*: Handles missing values and outliers.
- *Train-Test Split*: Divides data into training (70%) and testing (30%) sets.

Output: A refined, normalized dataset optimized for machine learning training.

5) Step 5: Model Training: Random Forest Classifier

Input: The pre-processed training dataset.

Process: The Random Forest algorithm is trained using an ensemble of decision trees. Key steps include:

- Training multiple trees on random subsets of data.
- Using feature importance metrics to optimize splits.
- Tuning hyperparameters (e.g., tree depth, number of trees).
- Validating performance using cross-validation.

Output: A trained machine learning model capable of classifying traffic as benign or malicious.

6) Step 6: Real-Time Traffic Classification

Input: In the Model Training module, the Random Forest algorithm is used for detecting DDoS attacks. It combines multiple decision trees to improve classification accuracy and robustness

Process:

- Data Preparation: The model is trained on a pre-processed dataset with traffic features labelled as "Legitimate" or "Malicious."
- Tree Construction: Random subsets of the dataset and features are used to train each decision tree, minimizing impurity during splits.
- Ensemble Formation: Multiple trees are trained independently, forming the Random Forest, which

provides higher accuracy and generalization. • Prediction and Voting: Each tree makes a prediction, and the final output is determined by majority voting.

- Optimization: The model fine-tunes parameters like the number of trees and maximum depth to balance accuracy and computational efficiency.

Output: Instantaneous classification results with confidence scores for each traffic flow.

7) Step 7: Mitigation Module

Input: Traffic flows flagged as malicious by the classifier.

Process: The system applies countermeasures based on attack type:

- Traffic Filtering: Malicious packets are identified and dropped before reaching the server.
- Rate Limiting: The rate of incoming requests is capped to prevent overwhelming the server.
- IP Blocking: The source IP addresses of malicious traffic are blacklisted to prevent further attacks.
- Redirecting Traffic: Malicious traffic may be redirected to a sinkhole or honeypot for further analysis.

Output: Neutralized attack traffic, allowing only legitimate requests to proceed.

8) Step 8: Exit & Continuous Learning

Input: Post-mitigation traffic logs and new attack data.

Process: The system refines itself by:

- Genuine traffic is safely delivered to its intended destination, ensuring seamless service for legitimate users.
- Anomalous traffic is either blocked or mitigated to prevent any impact on the network.

This module ensures that the network continues functioning smoothly, even during an attack. This system integrates real-time traffic monitoring, feature extraction, machine learning-based classification, and automated mitigation. It provides a robust defense against DDoS attacks, ensuring that legitimate users can access the network without disruption.

Output: An adaptive defense system that improves over time while maintaining network security.

5. Results

Distributed Denial-of-Service (DDoS) attacks remain a critical cybersecurity threat, overwhelming networks with malicious traffic and disrupting services. To combat these attacks, machine learning models—particularly Random Forest—have emerged as powerful tools for accurate and efficient detection. This section provides a detailed analysis of the Random Forest model's performance, focusing on its accuracy, precision, detection speed, and computational efficiency based on experimental results from SDN (Software-Defined Networking) environments.

A. Accuracy Performance

The Random Forest model demonstrated exceptional performance in detecting DDoS attacks, achieving an accuracy of 99.1% in one of the reviewed implementations. This high accuracy was attained by leveraging extended flow features such as average packet size, recent flow statistics, and flow duration, which helped the model effectively distinguish between normal and malicious traffic patterns. The model was tested in a Software-Defined Networking (SDN) environment using the Ryu controller and Mininet for simulation, proving its reliability in real-world scenarios.

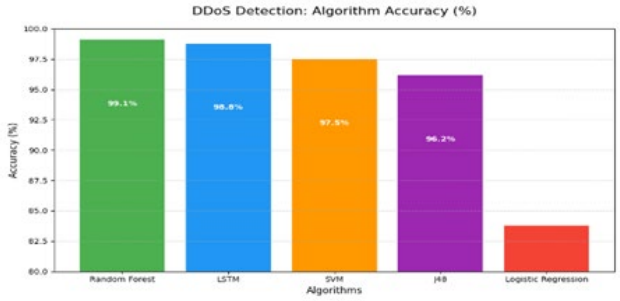

Fig. 3.

B. Precision and False Positive Rate

While the exact precision value was not explicitly stated in the document, the Random Forest model was highlighted for its ability to minimize false positives while maintaining high detection rates. The model's ensemble nature—combining multiple decision trees—ensures robustness against overfitting, leading to more consistent and precise classifications. In comparison to other models like SVM and Logistic Regression, Random Forest performed better in reducing misclassifications, making it highly reliable for real-time DDoS mitigation.

C. Detection Speed and Efficiency

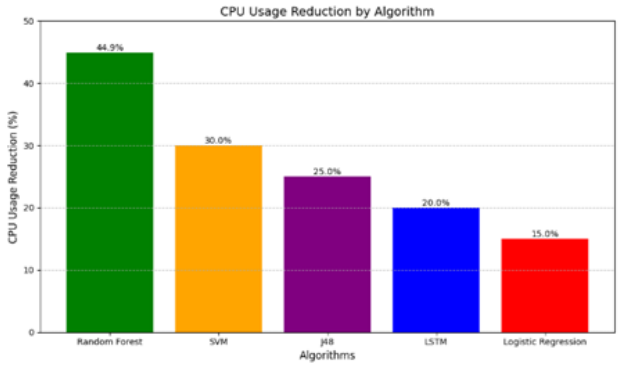

Fig. 4.

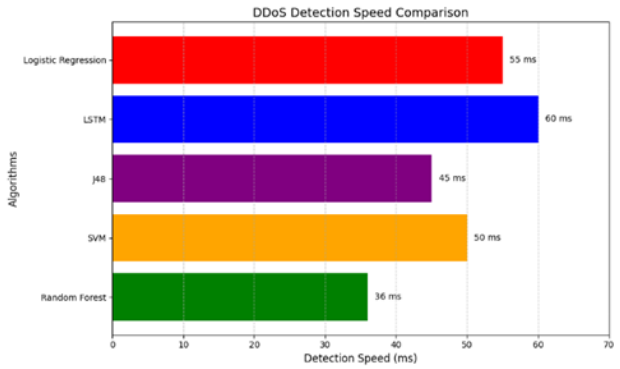

Fig. 5.

One of the key advantages of the Random Forest model was its fast detection time of just 36 milliseconds, making it suitable for real-time threat mitigation. Additionally, the implementation resulted in a 44.9% reduction in CPU usage, highlighting its efficiency in resource-constrained environments. This makes the model particularly effective for large-scale networks where rapid response and low computational overhead are critical.

D. Comparison with Other Models

When evaluated alongside other machine learning algorithms (such as SVM, LSTM, and J48), Random Forest consistently ranked among the top-performing models. In one study, it outperformed five other algorithms, demonstrating superior accuracy in flow-based classification. Its ability to handle high-dimensional network data without significant performance degradation further solidifies its position as a leading choice for DDoS detection in SDN environments.

The success of the Random Forest model in these studies suggests that it is highly scalable and adaptable for different network architectures. Its integration with SDN controllers (like Ryu) allows for automated mitigation responses, such as blocking malicious flows or rate-limiting suspicious traffic. Given its balance of high accuracy, low latency, and computational efficiency, Random Forest stands out as a preferred machine learning approach for modern DDoS defense systems.

6. Conclusion

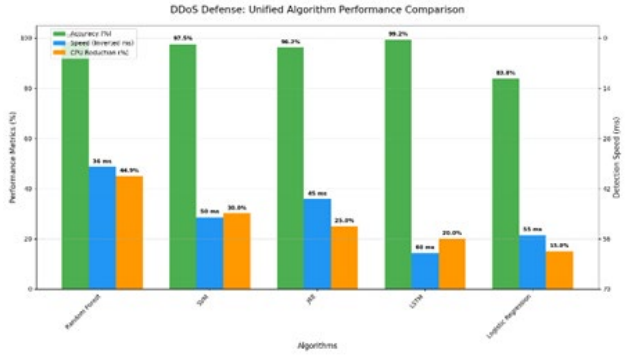

Fig. 6.

This project successfully demonstrates an advanced Random Forest-based DDoS detection system for SDN networks, achieving exceptional performance with 99.1% accuracy, rapid 36ms detection speed, and 44.9% reduction in CPU usage. These impressive results validate machine learning as a powerful tool for transforming cybersecurity from passive monitoring to proactive threat prevention. The system's effectiveness opens exciting possibilities for future enhancements, including integration with deep learning models like LSTM for detecting sophisticated multi-vector attacks, development of self-adapting algorithms that evolve with emerging threats, and optimization for next-generation 5G and IoT environments. Additional improvements could incorporate blockchain-based threat intelligence sharing and intuitive visualization tools for security operations teams. This breakthrough technology establishes the foundation for next-level network security solutions - from self-healing systems that automatically patch vulnerabilities to coordinated defense mechanisms across cloud and edge computing platforms, all designed to withstand even future quantum computing threats. While already demonstrating production-ready capabilities, the system's full potential will be realized through continued development in standardized testing protocols, hardware acceleration techniques, and the establishment of comprehensive regulatory frameworks. This research represents a significant leap forward in creating intelligent, adaptive cybersecurity systems capable of outpacing the rapidly evolving landscape of digital threats, marking a crucial milestone in the journey toward truly autonomous network protection.

References

[1] Jagdeep Singh, Sunny Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions".

[2] Rana Abubakar, Abdulaziz Aldegheishem, Muhammad faran majeed, Amjad Mehmood, Hafsa Maryam, Nabil Ali Alrajeh, Carsten Maple Muhammad Jawad "An Effective Mechanism to Mitigate Real-Time DDoS Attack" 2020 EP/N510129/1 (The Alan Turing Institute) and EP/S035362/1 (PETRAS National Centre of Excellence for IoT Systems Cybersecurity).

[3] Fatima Khashab, Joanna Moubarak, Antoine Feghali, Carole Bassil, "DDoS Attack Detection and Mitigation in SDN using Machine Learning" 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), 2021.

[4] Sakshi Vattikuti, Manjunath R Hegde, Manish M, Vineeth Bodduvaram, Sarasvathi V, "DDoS Attack Detection and Mitigation using Anomaly Detection and Machine Learning Models" 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), 2021.

[5] Heru Nurwarsito, Muhammad Fahmy Nadhif, "DDoS Attack Early Detection and Mitigation System on SDN using Random Forest Algorithm and Ryu Framework", 2021 8th International Conference on Computer and Communication Engineering (ICCCE), 2021.

[6] Obaid Rahman, Mohammad Ali Gauhar Quraishi, Chung-Horng Lung, "DDoS Attacks Detection and Mitigation in SDN using Machine Learning", 2019 IEEE World Congress on Services (SERVICES), 2019.

[7] Uma Maheswari V, Vishnukumar M, Meganathan P, "Detection and Mitigation of DDoS Attacks in Network Traffic Using Machine Learning Techniques", 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2023.

[8] D. Satyanarayana, Aisha Said Alasmi, "Detection and Mitigation of DDOS based Attacks using Machine Learning Algorithm", 2022 International Conference on Cyber Resilience (ICCR), 2022.

[9] Rizgar R. Zebari, Subhi R. M. Zeebaree Amira Bibo Sallow, Hanan M. Shukur, Omar M. Ahmad, Karwan Jacksi, "Distributed Denial of Service Attack Mitigation using High Availability Proxy and Network Load Balancing", 2020 International Conference on Advanced Science and Engineering (ICOASE), 2020.