Real-Time Detection and Mitigation of DDoS Attacks using Network Traffic Classification

Aaryan Mahadik
BE, Computer Engg
VESIT, Chembur
2021.aaryan.mahadik@ves.ac.in

Geocey Shejy
Faculty, CMPN Dept
VESIT, Chembur
geocey.shejy@ves.ac.in

Pratham Shetty
BE, Computer Engg
VESIT, Chembur
2021.pratham.shetty@ves.ac.in

Neha Lotwani
BE, Computer Engg
VESIT, Chembur
d2021.neha.lotwani@ves.ac.in

Himesh Hotwani
BE, Computer Engg
VESIT, Chembur
2021.himesh.hotwani@ves.ac.in

***Abstract* — Cybersecurity threats have become increasingly sophisticated, with Distributed Denial-of-Service (DDoS) attacks posing one of the most disruptive challenges to modern networks. These attacks overwhelm target systems with an immense volume of malicious traffic, leading to service disruptions, financial losses, and significant operational damage. Traditional DDoS detection and mitigation methods, which rely on static rule-based approaches, often fail to adapt to evolving attack patterns and zero-day threats. As a result, intelligent, adaptive, and real-time detection mechanisms have become a critical necessity for securing network infrastructures. This research introduces a real-time DDoS detection and mitigation framework using network traffic classification. By leveraging machine learning and Software-Defined Networking (SDN), the proposed system aims to improve the accuracy and efficiency of attack detection and response. The framework continuously monitors network traffic, extracts relevant flow-based features, and employs intelligent classification techniques to differentiate between legitimate and malicious traffic. Upon detecting an attack, dynamic mitigation strategies are applied to contain and neutralize the threat while ensuring minimal disruption to normal network operations. The findings demonstrate the potential of machine learning-powered SDN security mechanisms in offering faster, more reliable, and adaptive attack prevention compared to conventional detection systems. By bridging the gap between network intelligence and automated security responses, this research contributes to the advancement of next-generation cybersecurity solutions. The proposed approach enhances real-time threat detection and provides a proactive defense strategy, reinforcing network resilience against ever-evolving cyber threats.**

Keywords — DDoS detection, Machine learning, SDN, Network security, Traffic classification

I. Introduction

With the exponential growth of internet services, network security has become a critical concern. Among various cyber threats, Distributed Denial-of-Service (DDoS) attacks pose one of the most significant challenges to organizations and individuals. These attacks disrupt the availability of online services by overwhelming the target system with an enormous volume of malicious traffic, rendering it inaccessible to legitimate users. The increasing complexity of DDoS attacks, ranging from volumetric floods to sophisticated application-layer intrusions, has made traditional defense mechanisms ineffective. Conventional rule-based intrusion detection systems (IDS) struggle to keep up with rapidly evolving attack techniques, leading to high false positive rates and delayed mitigation responses. As a result, there is an urgent need for intelligent, adaptive, and real-time detection mechanisms to safeguard critical infrastructure against such threats.

Machine learning (ML) has emerged as a promising solution for network traffic classification, providing the ability to learn attack patterns from data and differentiate between legitimate and malicious traffic. Unlike static rule-based approaches, ML models can continuously evolve and adapt to new attack methods, significantly improving detection accuracy and response time. By leveraging supervised learning techniques, ML-based classifiers can analyze historical network traffic, identify anomalies, and classify potential threats in real-time. This proactive approach helps minimize service downtime, data breaches, and financial losses associated with DDoS attacks.

In this research, a real-time DDoS detection and mitigation framework is developed using network traffic classification. Several machine learning models, including XGBoost, Random Forest, CART, K-Nearest Neighbors (KNN), and different variations of Support Vector Machines (SVM - Linear, LinearSVC, and RBF kernel), are explored

for their effectiveness in identifying malicious traffic. A comparative analysis of these models is conducted based on key evaluation metrics such as accuracy, precision, recall, and F1-score. The results indicate that while multiple models achieve high classification performance, XGBoost outperforms the others, demonstrating superior accuracy and precision in distinguishing between legitimate and attack traffic.

The key contributions of this research include the development of a scalable and efficient ML-based DDoS detection system that not only classifies network traffic in real-time but also ensures rapid mitigation of identified threats. The study emphasizes feature engineering and dataset preprocessing to enhance the efficiency and accuracy of the detection system. By integrating ML-based traffic classification with automated mitigation mechanisms, the proposed framework aims to provide a robust and adaptive solution for protecting modern network infrastructures such as cloud environments, enterprise networks, and Software-Defined Networking (SDN) architectures.

The findings of this research highlight the potential of AI-driven cybersecurity solutions in combating modern DDoS attacks. By bridging the gap between machine learning advancements and practical cybersecurity needs, this study contributes to the development of intelligent, real-time defense mechanisms that can enhance network resilience, minimize attack impact, and ensure seamless service availability.

II. Related Methodology

Recent advancements in DDoS detection have leveraged Software-Defined Networking (SDN) architectures and machine learning-based classification techniques to identify and mitigate cyber threats in real-time. Traditional DDoS detection approaches have often relied on signature-based or threshold-based methods, which struggle to adapt to evolving attack patterns and zero-day threats. As a result, researchers have increasingly focused on machine learning and deep learning models to enhance detection accuracy, reduce false positives, and improve response times in real-world network environments.

One of the earliest methods for DDoS detection in SDN environments involved distributed controllers that collaborated to identify and counteract malicious traffic. Kavitha et al. [1] proposed a multi-controller SDN framework to detect anomalies in network traffic. Their method focused on analyzing packet header information to classify benign and attack traffic efficiently. Similarly, Abdulkarem et al. [2] introduced a mitigation strategy operating at the SDN data plane, ensuring minimal performance overhead while blocking attack traffic in real-time. The threshold-based approach for mitigating DDoS in cloud computing environments has also been explored. Bharot et al. [3] developed a system where predefined traffic thresholds determined the classification of legitimate and malicious traffic. This technique, while effective, suffers from a lack of adaptability to evolving attack patterns. In contrast, Dharma et al. [4] proposed a time-based detection method that evaluates packet arrival intervals, helping to distinguish between normal traffic bursts and actual DDoS events.

Recent advancements in machine learning have significantly improved DDoS detection accuracy. Alashhab et al. [5] demonstrated an ensemble-based online learning approach that dynamically adjusts to new attack patterns, achieving superior performance compared to traditional static classifiers. Similarly, Khedr et al. [6] proposed a multi-layer DDoS detection framework that combines supervised learning techniques with deep packet inspection, effectively reducing false positives in SDN-based IoT networks. Another area of research focuses on feature selection and network traffic classification for better detection accuracy. Azab et al. [7] provided a comprehensive survey on network traffic classification techniques, highlighting the advantages of statistical, flow-based, and machine learning-based classification. Hu et al. [8] further explored the integration of external attention mechanisms with convolutional neural networks to enhance real-time traffic classification accuracy.

Deep learning approaches have also been investigated for their potential in mitigating DDoS attacks. Najar et al. [9] introduced a convolutional neural network (CNN)-based model to detect DDoS patterns in SDN traffic, outperforming traditional machine learning models. Bakar et al. [10] expanded on this by incorporating a hierarchical ensemble graph neural network, which improved attack detection in large-scale distributed environments. Intrusion prevention systems (IPS) and virtual honeypots have been employed to mitigate the effects of DDoS attacks. Rahman et al. [11] proposed a honeypot-based defense mechanism in content delivery networks, effectively diverting attack traffic away from critical infrastructure. Dayal et al. [12] developed an intelligent defense scheme that detects DDoS attacks near the attack entry points, allowing proactive mitigation before the attack spreads further into the network.

Behavioral-based detection models have also been explored. Shamekhi et al. [13] introduced an adaptive time-interval-based approach that analyzes traffic behavior over time to detect anomalous patterns. Similarly, Wei et al. [14] leveraged a hybrid machine learning and deep learning framework, incorporating both statistical and behavior-based features to classify network flows accurately. Various classifiers have been evaluated for their effectiveness in DDoS detection. Najar et al. [15] compared multi-layer perceptron (MLP) and Random Forest (RF) models, concluding that MLP provides better generalization

for attack detection. Sumantra et al. [16] focused on SDN-based mitigation strategies, utilizing entropy-based measurements to differentiate between normal and attack traffic.

Despite these advancements, challenges remain in real-time detection and mitigation of DDoS attacks in SDN environments. The proposed research builds upon these prior works by integrating a real-time monitoring system with an optimized XGBoost classifier. Our approach aims to minimize false positives while ensuring rapid response to evolving attack vectors. Unlike existing solutions, our system not only detects attacks but also implements automated mitigation strategies within the SDN controller to maintain network stability.

III. Proposed Methodology

The tools being used in this project include two virtual machines running Ubuntu 22.04 LTS:

1. Target Virtual Machine (VM): Simulates a network topology using Mininet, allowing controlled traffic flow between nodes.
2. Monitoring Virtual Machine (VM): Runs the Ryu SDN Controller, which manages the packet flow in the network and collects network traffic data.

For DDoS attack generation, we use hping3, which floods the network with malicious packets. We leverage Python scripts to automate both traffic generation and collection:

- The mininet library is used to generate both benign and malicious traffic in a structured manner.
- The ryu.controller library is used to monitor network activity and collect relevant traffic data for analysis.

Machine Learning models are trained using the collected data to distinguish between legitimate and DDoS traffic, aiding in real-time mitigation strategies. Figure 1 presents a flowchart illustrating the steps involved in the proposed methodology.

To assess the effectiveness of the machine learning models in accurately distinguishing between legitimate and DDoS traffic, several standard evaluation metrics are employed. These include Accuracy, which measures the overall correctness of the model; Precision, which indicates the proportion of correctly identified DDoS instances among all predicted DDoS cases; Recall, which reflects the model's ability to detect all actual DDoS instances; and the F1-Score, which provides a balanced metric combining both precision and recall. These metrics ensure a comprehensive evaluation of the classifier's performance, especially in scenarios with class imbalance, which is common in network traffic datasets.

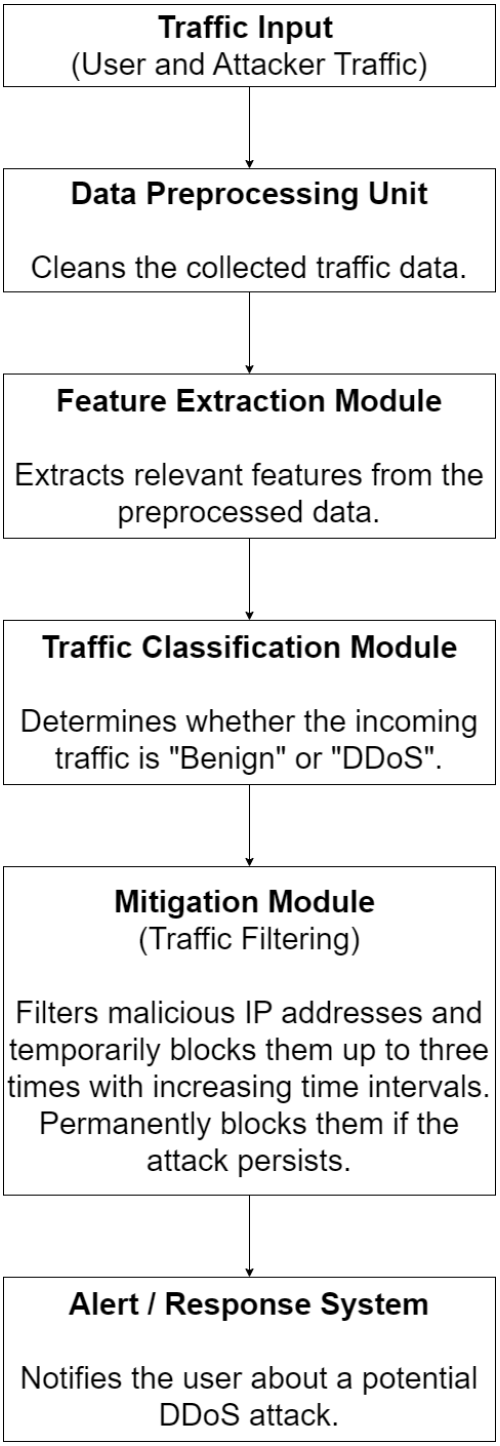

Figure 1: Overall Proposed Methodology

A. Data Generation and Collection

To build a reliable and diverse dataset for training and evaluating our DDoS detection model, we designed a controlled experimental environment using Mininet and SDN (Software Defined Networking) with Ryu as the controller framework. This environment allowed us to simulate and monitor both benign and DDoS traffic under consistent network conditions.

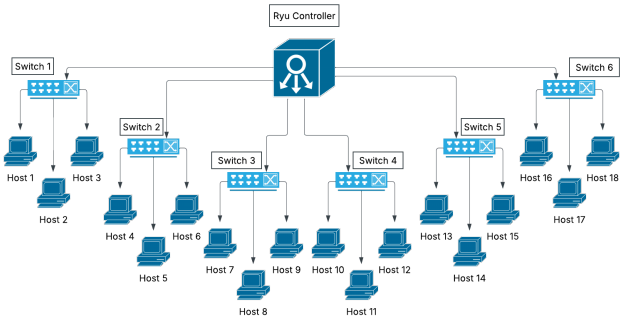

Figure 2: Custom Topology

A custom topology was constructed in Mininet consisting of six OpenFlow-enabled switches and fifteen hosts. These hosts were strategically distributed across switches to simulate real-world network segmentation and to ensure a wide variety of traffic paths. The topology supported the generation of both legitimate (benign) traffic and coordinated DDoS traffic.

For benign traffic generation, normal network communication patterns were established among various hosts. These patterns included typical TCP and UDP-based traffic flows such as pings, file transfers, and application-level interactions. On the other hand, DDoS traffic was simulated by orchestrating multiple hosts to simultaneously send a high volume of traffic to a single victim host, thus mimicking a volumetric attack scenario.

This simulated attack environment enabled us to create realistic network conditions for both normal operation and attack scenarios, giving our dataset strong representational quality.

To monitor the network and extract relevant traffic features, we implemented an SDN application that operated on the Ryu controller. The application periodically collected OpenFlow flow statistics from all registered datapaths in the network. These statistics included information such as:

- Source and destination IP addresses
- Transport layer ports (TCP/UDP)
- IP protocol types (e.g., ICMP, TCP, UDP)
- Flow duration (in seconds and nanoseconds)
- Total packet and byte counts
- ICMP-specific fields (type and code, when applicable)

From these raw values, additional derived features were computed, including:

- Packet count per second
- Packet count per nanosecond
- Byte count per second
- Byte count per nanosecond

B. Attribute Information

The dataset consists of flow-level features extracted from OpenFlow statistics, designed to capture the behavior of network flows during both benign and DDoS scenarios. Key features include:

- src_ip and dst_ip: Source and destination IP addresses identifying the endpoints of the flow.
- src_port and dst_port: Transport-layer port numbers used in the flow.
- protocol: IP protocol used (e.g., TCP, UDP, ICMP).
- duration_sec and duration_nsec: Flow duration in seconds and nanoseconds.
- packet_count and byte_count: Total number of packets and bytes transmitted in the flow.
- icmp_type and icmp_code: ICMP-specific fields present only for ICMP flows.
- pkts_per_sec and pkts_per_nsec: Derived metrics representing packet transmission rate.
- bytes_per_sec and bytes_per_nsec: Derived metrics representing byte transmission rate.

C. Model Training

Our system was trained using various machine learning algorithms, namely:

1) *XGBoost (Extreme Gradient Boosting):* XGBoost is a powerful and efficient implementation of gradient boosting that builds an ensemble of decision trees in a sequential manner. Each tree corrects the errors of the previous ones, allowing the model to learn complex patterns in the data. XGBoost uses both first and second-order gradients (hence the term "gradient boosting") to optimize its performance and prevent overfitting through regularization techniques. It is widely known for its scalability, speed, and accuracy, making it a popular choice in structured/tabular data tasks such as DDoS detection.

$$l = \sum_{i=1}^{n} l(y_i, y_i^{(t)}) + \sum_{k=1}^{t} \Omega(f_k) \quad (1.1)$$

2) *K-Nearest Neighbors (KNN):* K-Nearest Neighbors is a simple, non-parametric, instance-based learning algorithm. It works by comparing a given data point to its **k** closest neighbors in the feature space using a distance metric (typically Euclidean distance). The predicted class is determined by a majority vote among these neighbors. KNN is intuitive and effective for classification tasks where the decision boundary is non-linear. However, it can be computationally expensive for large datasets and is sensitive to feature scaling and irrelevant features, which is why preprocessing is important when using KNN.

$$d(x, x') = \sqrt{\sum_{i=1}^{n} (x_i - x'_i)^2} \quad (2.1)$$

3) *Support Vector Machine (SVM):* Support Vector Machine (SVM) is a supervised machine learning algorithm that is particularly effective for classification tasks, including network traffic analysis. In this project, SVM is employed to classify network flows as either normal or indicative of a DDoS attack. The algorithm works by finding the optimal hyperplane that separates data points of different classes with the maximum margin. In cases where the data is not linearly separable, SVM uses kernel functions to project the data into higher-dimensional space, enabling it to draw more complex decision boundaries. This ability to handle high-dimensional data makes SVM well-suited for intrusion detection systems, where subtle patterns in features like packet rates, byte flows, and source/destination addresses can help distinguish between benign and malicious activity.

$$f(x) = sign(\sum_{i=1}^{n} \alpha_i y_i K(x_i, x) + b) \quad (3.1)$$

D. Detection Module

The detection module is a critical component of the proposed system, responsible for identifying DDoS attacks in real time by monitoring network traffic, extracting relevant features, and classifying flows based on traffic behavior. Implemented within the Ryu SDN controller, this module continuously collects flow statistics from OpenFlow-enabled switches and processes them to distinguish between benign and malicious traffic. By leveraging event-driven packet monitoring, the detection module operates efficiently without introducing excessive computational overhead, ensuring rapid response to potential threats.

The process begins with continuous traffic monitoring, where the SDN controller registers active switches and maintains a list of datapaths. Whenever a new switch connects, it is added to the monitoring list, and if a switch disconnects, it is removed to optimize performance. The detection module utilizes a background monitoring thread that periodically requests flow statistics from all active switches. The FlowStatsRequest messages are sent every 10 seconds, and the switches respond with FlowStatsReply messages containing detailed traffic metrics such as source and destination IP addresses, transport protocol type (TCP, UDP, ICMP), source and destination ports, packet count, byte count, and flow duration. These statistics allow the system to analyze traffic patterns and detect anomalous behavior indicative of a DDoS attack.

After collecting flow statistics, the detection module proceeds with feature extraction and data structuring. It processes and computes key metrics such as packet count per second and byte count per second, which help characterize network behavior. A unique flow identifier is generated using a combination of IP addresses, transport protocol, and port numbers, ensuring that each flow is uniquely tracked. If the protocol is ICMP, additional parameters such as ICMP type and code are recorded. The extracted data is then formatted and stored in a csv file, where each network event is logged for real-time classification and historical analysis.

The classification logic of the detection module is based on analyzing the overall traffic distribution. Once the network flows are recorded, the system evaluates the proportion of legitimate vs. malicious traffic based on past statistics. If 80% or more of the total network traffic is classified as legitimate, the system assumes that the network is functioning normally, and no further action is taken. However, if the percentage of malicious traffic exceeds 20%, the system flags it as a potential DDoS attack. This threshold-based approach ensures low false positive rates, preventing unnecessary disruptions to legitimate users while maintaining high sensitivity to abnormal traffic surges.

The detection module operates in real time, ensuring that suspicious activity is identified before it significantly impacts the network. Unlike traditional signature-based detection methods that rely on predefined attack patterns, this module uses a dynamic classification approach that adapts to evolving attack behaviors. Future improvements could involve integrating advanced machine learning classifiers to enhance detection accuracy, allowing the system to automatically learn new attack patterns. Additionally, employing online learning techniques could enable continuous model updates, further strengthening the system's ability to detect zero-day DDoS attacks. Through real-time traffic monitoring and adaptive classification, the detection module plays a crucial role in identifying threats efficiently and enabling a proactive security response.

E. Mitigation Module

Once a potential DDoS attack is detected, the mitigation module is activated to minimize its impact and ensure service availability while preventing unnecessary disruptions to legitimate users. Implemented within the Ryu SDN controller, this module enforces dynamic flow rules in OpenFlow-enabled switches, allowing for adaptive and progressive attack mitigation. Rather than immediately blocking an IP address upon detection, the system adopts a tiered blocking strategy to differentiate between temporary traffic anomalies and persistent attackers.

When an IP address is flagged for suspicious behavior, it is temporarily blocked for 5 minutes on the first offense. This initial block acts as a warning mechanism, preventing the attacker from immediately overwhelming network resources while allowing for the possibility of false positives. If the same IP continues to exhibit malicious traffic patterns, the second detection results in a 10-minute block, followed by a 15-minute block on the third offense. If the attack persists beyond three warnings, the IP is permanently blacklisted, preventing further access to the network. This escalating timeout mechanism serves as both a preventive and corrective measure, allowing temporary anomalies to self-correct while ensuring that persistent threats are neutralized.

To implement this strategy, the mitigation module dynamically modifies OpenFlow rules in the SDN switches. When an IP is temporarily flagged, a drop rule with a time-based expiration is installed, ensuring that the block is lifted after the specified duration. If the same attacker is detected again, the system updates the rule with a longer timeout, progressively increasing the severity of the response. On the fourth detection, a permanent drop rule is enforced, preventing any further traffic from the malicious source. Additionally, the module maintains a blacklist of permanently blocked IPs, ensuring that repeat offenders cannot regain access.

The mitigation module continuously adapts to network conditions, dynamically adjusting its response based on attack severity and frequency. Unlike traditional static blocking mechanisms, which may either be too lenient or overly aggressive, this progressive blocking approach balances security and accessibility, reducing the risk of false positives while effectively stopping persistent attackers. Future enhancements could include a threat scoring system, where each IP is assigned a risk level based on the frequency and intensity of its attacks, allowing for even more refined mitigation strategies. By integrating real-time threat response, adaptive blocking, and SDN-based flow control, the proposed mitigation module ensures a resilient and intelligent defense against DDoS attacks.

IV. Result Finding And Analysis

To evaluate the performance of our proposed approach, we trained our dataset using multiple machine learning algorithms, including XGBoost, Random Forest, CART, KNN, and different variants of Support Vector Machines (SVM). The dataset was divided into training and testing subsets, with training data allocation varying across models. The classification performance of each algorithm was assessed using key metrics such as Accuracy, Precision, Recall, and F1 Score. The comparative analysis of these models is presented in Table 1, highlighting the effectiveness of each classifier in distinguishing between DDoS traffic and benign traffic. Among the tested models, XGBoost and Random Forest demonstrated superior performance, achieving near-perfect classification results.

Algorithm chosen	Accuracy %	Precision %	Recall %	F1 Score
XGBoost	99.99935664	100	99.99871192	99.99935596
Random Forest	99.99935664	100	99.99871192	99.99935596
CART	99.998713	99.998713	99.998713	99.998713
KNN	99.66	99.66	99.66	99.66
SVM (Linear)	97.32	95.04	99.84	97.38
SVM (LinearSVC)	97.17	94.84	99.78	97.24
SVM (rbf)	99.68	99.37	99.99	99.68

Table1: Comparative table of the machine learning algorithms applied to the data set

This evaluation compares machine learning models for DDoS attack detection based on training data allocation, accuracy, precision, recall, and F1 score. XGBoost, Random Forest, and CART achieve the highest accuracy (99.99%), while KNN (99.66%) and SVM models show varied results, with SVM (Linear) at 97.32%, SVM (Linear SVC) at 97.17%, and SVM (RBF) at 99.68%.

XGBoost and Random Forest also achieve perfect precision and recall (100%), while KNN and SVM models exhibit slight drops. The F1 score follows a similar trend, with tree-based models performing best. Overall, tree-based models outperform SVM models in accuracy and precision.

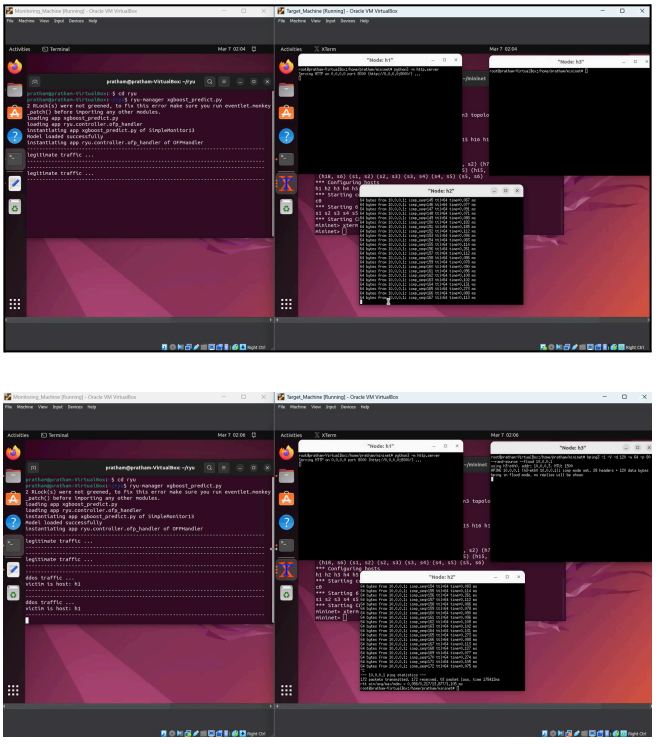

Figure 8: Using XGBoost

The XGBoost-based model classifies network traffic in real time, distinguishing between benign and malicious packets. The system continuously monitors incoming packets, accurately identifying DDoS attacks as they occur. When an attack is detected, the classifier flags it, providing instant alerts. This stage demonstrates the effectiveness of XGBoost in achieving high detection accuracy while maintaining minimal false positives.

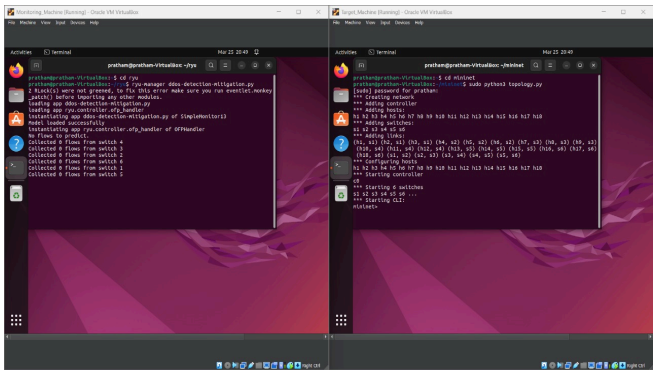

Figure 9: Connection of network topology with ryu controller

The network topology is established using Mininet, where multiple hosts and switches are interconnected. The Ryu controller is successfully launched and integrated with the topology to handle network flow management. The controller initializes and begins monitoring traffic flows from connected switches, enabling real-time flow collection for further analysis and DDoS detection.

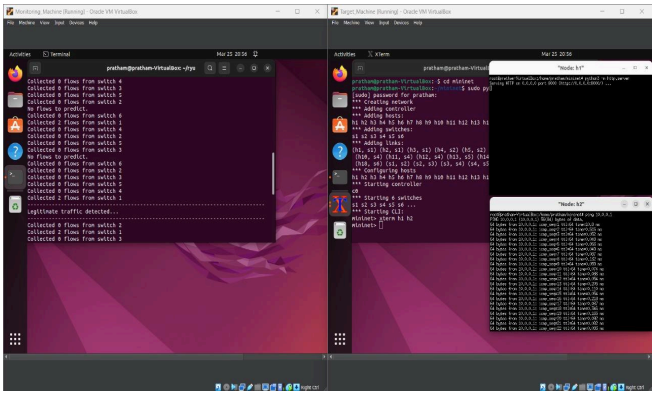

Figure 10: Legitimate traffic

The setup involves a network simulation using Mininet and the Ryu SDN controller. The controller collects flow data from multiple switches, analyzing traffic patterns. Mininet is configured with multiple hosts and switches, facilitating communication. A node runs an HTTP server while another sends ICMP ping requests, demonstrating legitimate traffic detection.

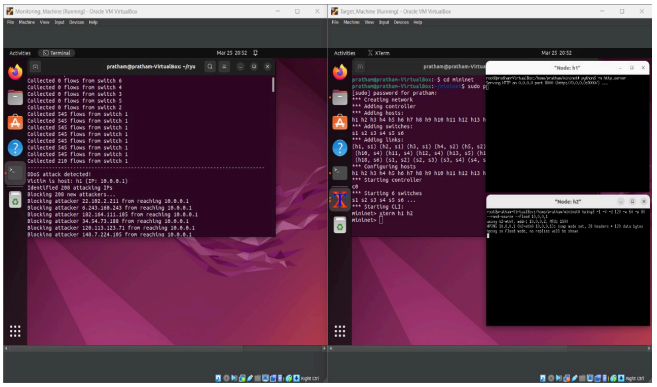

Figure 11: DDoS Traffic

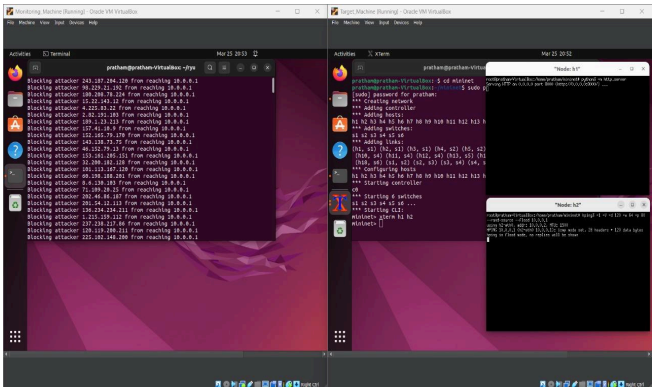

Figure 12: DDoS Attack Mitigation

A real-time DDoS attack detection and mitigation system is deployed in a virtualized network using Mininet and a monitoring mechanism. The network simulation detects and mitigates a DDoS attack targeting host h1 (10.0.0.1), where an HTTP server runs on one node while another generates high-rate ICMP flood traffic. The controller identifies 208 attacking IPs and dynamically blocks them. The monitoring component continuously logs malicious traffic and enforces mitigation by filtering attackers, ensuring network stability amid the ongoing flood attack scenario.

V. Concluding Remarks And Future Enhancements

In conclusion, the comparative analysis of machine learning models for real-time DDoS detection and mitigation in SDN environments reveals that XGBoost outperforms other classifiers in terms of accuracy, computational efficiency, and adaptability to network traffic variations. While KNN and SVM showed promising results in classifying network flows, their performance was affected by high-dimensional data and increased computational complexity. Random Forest and Decision Trees, on the other hand, provided good interpretability but lacked the speed and precision needed for real-time attack mitigation. The integration of XGBoost with an adaptive SDN-based mitigation strategy enabled faster threat response and effective mitigation of DDoS attacks while minimizing disruptions to legitimate users.

To further enhance the performance of the proposed system, advanced deep learning models, such as CNNs and LSTMs, could be explored to capture complex temporal patterns in network traffic, improving detection accuracy against evolving attack strategies. Additionally, implementing semi-supervised and online learning techniques could allow the model to adapt dynamically without requiring periodic retraining, making it more effective against zero-day attacks.

Future work could also focus on improving mitigation strategies by incorporating dynamic rerouting, rate-limiting adjustments, and deception-based techniques such as honeypots to further minimize attack impact. The integration of multi-controller SDN architectures could enhance the scalability of the system, making it suitable for large-scale enterprise and cloud-based environments. Furthermore, leveraging blockchain for trust management in SDN security policies could improve data integrity and prevent adversarial attacks on traffic classification models.

Overall, the proposed machine learning-driven DDoS detection and mitigation system demonstrates high efficiency, real-time responsiveness, and adaptability in securing SDN networks. The findings of this research serve as a foundation for future AI-driven cybersecurity advancements, ensuring robust network security against increasingly sophisticated cyber threats.

References

[1] Kavitha, D., R. Ramalakshmi, and R. Murugeswari. "The detection and mitigation of distributed denial-of-service (DDOS) attacks in software defined networks using distributed controllers." 2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES). IEEE, 2019.

[2] Abdulkarem, Huda Saleh, and Ammar Dawod. "DDoS attack detection and mitigation at SDN data plane layer." 2020 2nd Global Power, Energy and Communication Conference (GPECOM). IEEE, 2020.

[3] Bharot, Nitesh, et al. "Mitigating distributed denial of service attack in cloud computing environment using threshold based technique." Indian Journal of Science and Technology 9.38 (2016): 1-7.

[4] Dharma, NI Gde, et al. "Time-based DDoS detection and mitigation for SDN controller." 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, 2015.

[5] Alashhab, Abdussalam A., et al. "Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model." IEEE Access (2024).

[6] Khedr, Walid I., Ameer E. Gouda, and Ehab R. Mohamed. "FMDADM: A multi-layer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks." Ieee Access 11 (2023): 28934-28954.

[7] Azab, Ahmad, et al. "Network traffic classification: Techniques, datasets, and challenges." Digital Communications and Networks 10.3 (2024): 676-692.

[8] Hu, Yahui, et al. "Online network traffic classification based on external attention and convolution by IP packet header." Computer Networks 252 (2024): 110656.

[9] Najar, Ashfaq Ahmad, and S. Manohar Naik. "Cyber-secure SDN: A CNN-based approach for efficient detection and mitigation of DDoS attacks." Computers & Security 139 (2024): 103716.

[10] Bakar, Rana Abu, et al. "FTG-Net-E: A hierarchical ensemble graph neural network for DDoS attack detection." Computer Networks 250 (2024): 110508.

[11] Rahman, Md Mahmudur, Shanto Roy, and Mohammad Abu Yousuf. "DDoS mitigation and intrusion prevention in content delivery networks using distributed virtual honeypots." 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT). IEEE, 2019.

[12] Dayal, Neelam, and Shashank Srivastava. "FloodKnight: an intelligent DDoS defense scheme to combat attacks near attack entry points." Journal of Computer Virology and Hacking Techniques 20.4 (2024): 819-839.

[13] Shamekhi, Ali, Pirooz Shamsinejad Babaki, and Reza Javidan. "An intelligent behavioral-based DDOS attack detection method using adaptive time intervals." Peer-to-Peer Networking and Applications 17.4 (2024): 2185-2204.

[14] Wei, Y., and J. Liu, "DDoS Attack Detection Using Machine Learning and Deep Learning Approaches," Scientific Reports, vol. 14, 2024.

[15] Najar, Ashfaq Ahmad, and S. Manohar Naik. "DDoS attack detection using MLP and Random Forest Algorithms." International Journal of Information Technology 14.5 (2022): 2317-2327.

[16] Sumantra, I., and S. Indira Gandhi. "DDoS attack detection and mitigation in software defined networks." 2020 International Conference on System, Computation, Automation and Networking (ICSCAN). IEEE, 2020.