Assessing the Impact of Machine Learning-Based DDoS Attack Detection on SDN Network Performance

[1]$SmritiArora$,[2] $HariBabuK$,[3] $ShrinivasChoudhary$
CSIS
BITS Pilani, Rajasthan , India
[1]$p20210101@pilani.bits-pilani.ac.in$,[2] $khari@pilani.bits-pilani.ac.in$,
[3]$h20230088@pilani.bits-pilani.ac.in$

***Abstract*—In recent years, the field of network security has seen significant progress. Researchers and developers have focused their efforts on designing innovative techniques to detect and counter various security threats and malicious activities. These advancements have strengthened the resilience of networks against potential attacks and have provided organizations with more effective tools to safeguard their digital assets.Within these groundbreaking developments, the application of AI technologies, notably machine learning (ML) and deep learning (DL), has proven to be remarkably successful in safeguarding software-defined networks (SDN) and bolstering the comprehensive internet security framework to defend against distributed denial-of-service (DDoS) attacks.**

This research paper focuses on evaluating the performance of an SDN-based DDoS detection system, with a specific emphasis on measuring the time required to identify an ongoing attack. By conducting a thorough analysis of the system's efficiency and responsiveness, this study aims to highlight the advantages of leveraging SDN and data plane programming in overcoming the shortcomings of traditional DDoS mitigation techniques. This study's results are expected to support current initiatives aimed at strengthening cybersecurity measures and safeguarding essential systems against emerging digital threats. The research outcomes will provide valuable insights to help organizations and policymakers adapt their defense strategies in response to the constantly changing nature of cyber risks.

***Index Terms*—DDoS attack, SDN, Decision Tree Classifier, SVM**

I. Introduction

In today's fast-paced digital landscape, safeguarding the robustness and protection of network systems has become a paramount objective for businesses and institutions globally. The growing frequency and sophistication of Distributed Denial of Service (DDoS) attacks have surfaced as a significant challenge, jeopardizing the accessibility and reliability of vital network operations. These destructive assaults strive to inundate network assets with an enormous influx of fraudulent data packets, effectively crippling their ability to serve authorized clients and users. Distributed denial-of-service (DDoS) attacks are characterized by intentional attempts to impair the standard operations of a network through the inundation of an overwhelming volume of data traffic, thereby rendering the targeted system unable to process legitimate requests effectively.

Conventional methods for combating such attacks often relied on dedicated hardware and software solutions that operated externally to the network. However, these approaches suffered from several limitations, including delayed detection, reliance on third-party services, and poor scalability.

To address these challenges, researchers have turned to cutting-edge technologies such as SDN and data plane programming, which can be integrated directly into the network infrastructure. The emergence of SDN, along with the OpenFlow protocol, has revolutionized the way DDoS attacks are detected and prevented.

Traditional network architectures, with their rigid and static nature, often struggle to adapt and respond effectively to the ever-evolving landscape of DDoS threats. The absence of adaptability and fine-grained command over network assets impedes the capacity to identify and counter these offensive actions in a timely manner. This is precisely where the advent of Software-Defined Networking (SDN) becomes instrumental, ushering in a transformative approach to network administration and protection.

Software-Defined Networking (SDN) transforms traditional network structures by separating network control functions from data forwarding operations. This innovative approach allows for centralized oversight and flexible programming of network assets, fundamentally changing how networks are managed and operated.

By decoupling the control and data planes, network administrators can achieve a level of insight into network traffic flows that was previously unattainable. This architectural shift enables the dynamic adaptation of security measures and policies in response to up-to-the-minute threat information, empowering organizations to proactively defend their networks against emerging dangers. With SDN, network operators can swiftly adapt to emerging threats and implement targeted countermeasures to protect against DDoS attacks.

The programmable nature of SDN empowers network administrators to design and deploy sophisticated DDoS detection mechanisms that surpass the capabilities of traditional methods. These cutting-edge SDN-driven detection methods employ sophisticated algorithms and machine learning frame-

works to scrutinize network data flows in real-time, recognizing irregularities and telltale signs that point towards the presence of ongoing DDoS assaults.By continuously monitoring network flows and detecting deviations from normal behavior, SDN-enabled security systems can trigger automated mitigation strategies.

This research paper explores the utilization of Software-Defined Networking (SDN) principles in the context of identifying Distributed Denial of Service (DDoS) attacks. The primary objective is to conduct an in-depth examination of the effectiveness and efficiency of a particular DDoS detection approach that leverages the capabilities offered by SDN architecture.We present a comprehensive overview of the detection mechanism, outlining its architecture, algorithms, and operational principles. Furthermore, we discuss the methodology employed to measure the performance of the detection system, including the metrics and experimental setup used.

Through rigorous experimentation and data analysis, we evaluate the effectiveness and efficiency of the SDN-based DDoS detection mechanism. The performance results obtained from our experiments provide valuable insights into the system's ability to accurately identify DDoS attacks, the response time in triggering mitigation actions, and the overall impact on network performance. These findings contribute to the growing body of knowledge on SDN-based security solutions and highlight the potential of SDN in enhancing network resilience against DDoS threats.

A. Literature Review

In the past few years many studies have been carried out by the researchers for the DDoS detection and their mitigation techniques and the accuracy and precision of the same and the comparison of multiple techniques helped us understand the better results over the time. The summary of such studies is as follows:

The proposed framework [1] distinguishes between different categories of DDoS attacks by applying classification algorithms to the CIC-DDoS 2019 dataset. This dataset, which comprises packets captured within an SDN environment, undergoes preprocessing followed by analysis using various classification methods to identify DDoS incidents. The SDN dataset was generated through the use of the Mininet emulator and RYU controller, utilizing a range of DDoS tools. The results demonstrate that the decision tree algorithm exhibits superior performance compared to both Support Vector Machines (SVM) and Naïve Bayes classifiers in terms of its effectiveness in detecting these malicious activities.

The study [2] introduces an innovative approach to identify and counter Distributed Denial of Service (DDoS) attacks within the context of Software-Defined Networking (SDN). The proposed solution leverages a Ryu controller and integrates a Decision Tree classifier, employing machine learning algorithms to recognize intricate traffic patterns that are indicative of ongoing DDoS assaults.

The effectiveness of the suggested technique in [3] is verified through the use of a newly generated dataset that encompasses a diverse range of contemporary attack types, including HTTP flood, SID DoS, and normal traffic patterns. The categorization of these various attack categories is carried out using WEKA, a powerful machine learning software suite.

This research in [4] introduces a computationally efficient approach for detecting DDoS attacks, leveraging the principles of deep transfer learning. The study assesses the transfer performance of different network architectures by employing transferability metrics to enable a comparative analysis.

The suggested framework in [5] consists of an Online Monitoring System (OMS), a module for detecting spoofed traffic, and an Interface-Based Rate Limiting (IBRL) algorithm. The OMS facilitates the real-time evaluation of DDoS attack impact by continuously monitoring the deterioration of host and network performance indicators.

The research presented in [6] is a versatile and modular framework engineered to identify and counter Low-Rate Distributed Denial of Service (LR-DDoS) attacks in Software-Defined Networking (SDN) settings. The Intrusion Detection and Response (IDR) system undergoes training using a diverse array of machine learning models to achieve improved precision in detecting these malicious activities.

The research in [7] employs Support Vector Machine (SVM) and Decision Tree classifiers to conduct real-time examination of network data flows, efficiently detecting and neutralizing prospective threats before they can inflict any harm on the system.

The proposed framework in [8] utilized artificial intelligence algorithms to identify Distributed Denial of Service (DDoS) assaults in the context of Software-Defined Networking (SDN) architectures.

II. MACHINE LEARNING APPROACH TO ENHANCE DDOS ATTACK DETECTION IN SDN ENVIRONMENTS

Distributed Denial of Service (DDoS) attacks have become more frequent and sophisticated in recent years, posing significant challenges to organizations striving to maintain the availability and security of their online services. These malicious activities pose serious threats to the stability and security of network services, making it increasingly challenging for organizations to maintain uninterrupted operations and protect their digital infrastructure from harm. Conventional safeguards frequently find it difficult to counter these evolving threats effectively.

However, the emergence of cutting-edge technologies, has paved the way for the development of innovative approaches to identifying and countering DDoS attacks. These advanced techniques have significantly improved the effectiveness and efficiency of DDoS mitigation strategies, providing organizations with more robust defenses against these malicious activities.These cutting-edge tools present promising avenues to tackle the shortcomings of conventional defense tactics when confronted with progressively complex cyber threats.

Software-Defined Networking (SDN) is an innovative approach to network architecture that separates the control plane,

which makes decisions about network traffic flow, from the data plane, which handles the actual forwarding of data packets. This separation allows for a more flexible, programmable, and centralized approach to network management. By decoupling these two critical aspects of networking, SDN enables a more flexible, programmable, and centralized approach to network control and configuration.This separation allows for unified oversight and flexible configuration of network resources, fundamentally altering how networks are designed and managed. This architectural shift allows for greater flexibility, scalability, and control over network resources. By leveraging the capabilities of SDN, we can develop intelligent and adaptive DDoS detection systems that can dynamically respond to attack patterns and optimize network performance.

In contrast, Machine Learning techniques have emerged as highly effective methods for processing and interpreting large volumes of network traffic information. These advanced algorithms excel at recognizing unusual patterns and behaviors that often signal the presence of DDoS attacks, providing a valuable asset in the field of network security. By training ML models on historical network traffic data, we can develop algorithms that can accurately classify and detect DDoS attacks in real-time. These models can learn from past attack patterns, adapt to new attack vectors, and continuously improve their detection accuracy over time.

The combination of SDN and ML techniques offers a promising approach to combat DDoS attacks effectively. By integrating ML-based detection algorithms into the SDN control plane, we can enable intelligent and automated DDoS defense mechanisms.

A. Decision Tree Algorithm

The decision tree is a type of guided machine learning technique commonly employed for categorization purposes. This method operates by dividing the input data into smaller groups based on the characteristics of various features. These divisions form a tree-like structure with branches, ultimately leading to final classifications or outcomes at the terminal points, known as leaves.

Basic Structure:

The Decision Tree algorithm comprises three distinct node categories:

Root node - Symbolizes the complete dataset, which is subsequently partitioned into smaller subsets during the tree-building process.

Decision nodes - These nodes represent a feature or attribute on which the data is split.

Leaf nodes - These nodes represent the final predicted class of the input.

Once the tree is built on the dataset, making a prediction involves traversing the tree from root to the leaf and making decisions on each decision node based on input value. The value of the leaf node is the prediction.

B. Decision Tree Training

Dataset: For the experiment we have used the CIC-DDoS 2019 dataset [9]. This is a widely used DDoS attack dataset containing data of various kinds of attacks [10]. The dataset contains benign as well as malicious flows. We have used the dataset for TCP Syn Attack. We have used features such as Destination IP, Source IP, Destination Port, Flow Duration,Flow Bytes/s, Protocol, Source Port, Flow ID,Flow Packets/s,Timestamp, Packet Count and Byte Count for training the algorithm. These features were selected because these are the flow stat values the controller receives from the switch upon request.

C. Detection System Architecture

In our SDN-based detection system, we have employed Ryu as the SDN controller, which is set up and run on a remote Azure virtual machine (VM). To simulate our experiments, we have utilized Mininet, a powerful network emulation tool.

Once the Mininet topology is established and the controller is running, the controller initiates a continuous process of sending flow stats requests to the switch within the Mininet topology at predetermined intervals. Upon receiving the request, the switch responds by sending a flow stats reply back to the controller.

The flow stats reply contains crucial information about each source and destination ports,packet count,the flow ID,flow, including source and destination IP addresses, protocol, and byte count. These statistics are then recorded by the controller and stored in a CSV file for further analysis.

After the flow stats are successfully written to the CSV file, the controller reads the data and feeds it into a machine learning (ML) prediction algorithm. This algorithm serves as the core component of our DDoS detection mechanism.

The ML algorithm takes the flow stats as input and performs a comprehensive analysis to determine whether each flow exhibits characteristics indicative of a DDoS attack. By leveraging advanced machine learning techniques, such as anomaly detection and pattern recognition, the algorithm can effectively distinguish between legitimate traffic and malicious DDoS traffic.

Based on the analysis, the ML algorithm generates a prediction for each flow, classifying it as either a potential DDoS attack or normal traffic. This prediction is then communicated back to the controller, enabling it to take appropriate actions based on the results.

By continuously monitoring the network traffic and applying the ML-based prediction algorithm, our SDN-based detection system can promptly identify and flag suspicious flows that may be part of a DDoS attack.

The integration of SDN and machine learning in our detection system provides a powerful and adaptive approach to combating DDoS attacks. By harnessing the flexibility and centralized management provided by SDN, coupled with the smart decision-making abilities of machine learning algorithms, we can efficiently identify and counter DDoS threats as they occur, thereby bolstering the comprehensive security and

robustness of the network infrastructure.Every few seconds following algorithm is executed:

```
DetectDDoS():
 Send_Flow_Stat_Request()
 flow_stats = Receive_Flow_Stat_Reply()

 model = DecisionTreeClassifier()
 result = model.predict(flow_stats)
        // 1 if ddos, 0 if safe

 return result
```

Following is a figure depicting the system architecture.

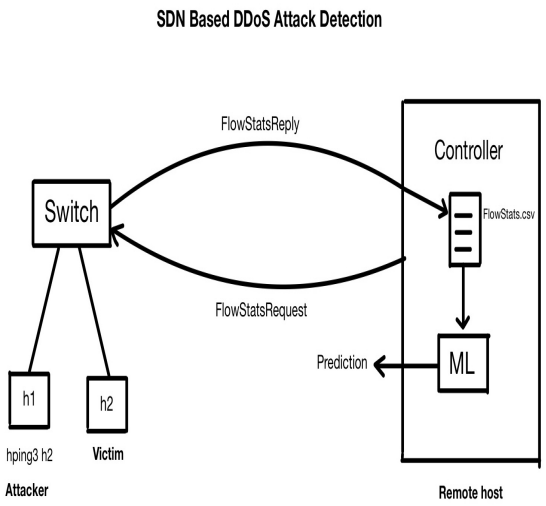

Fig. 1. DDoS Detection System

D. Topology

In our experiment, we employed a straightforward Mininet topology consisting of two hosts, h1 and h2, connected to a single switch. Host h1 was designated as the attacker, while host h2 served as the victim.

To execute the TCP SYN attack, we utilized the hping3 utility, which was configured in two distinct ways:

1. Fast mode: In this configuration, hping3 sends packets at an interval of approximately 10 milliseconds. While this option generates a significant amount of traffic, it does not completely overwhelm the network.

2. Flood mode: Under this setting, hping3 unleashes packets without any rate limiting or intervals between them. This relentless barrage of packets aims to inundate the network and exhaust its resources.

By employing these two hping3 configurations, we were able to simulate different intensities of TCP SYN attacks within our Mininet environment. The Fast mode allowed us to observe the impact of a sustained, yet manageable attack, while the Flood mode represented a more severe and potentially devastating assault on the network.

Through this controlled experiment, we aimed to assess the effectiveness of our SDN-based detection system in identifying and responding to TCP SYN attacks of varying magnitudes, ultimately showcasing its ability to safeguard the network against such threats.

E. Measuring Time

In our study, we aim to quantify the total time required to identify DDoS attacks using our SDN-based system. To achieve this, we employ a precise timing mechanism that captures the duration of key processes within the detection workflow.

The initial step in the data collection procedure involves the controller initiating a flow statistics query, which is then transmitted to the targeted network switch. At this moment, the current time is recorded. Once the switch responds to the flow statistics request by sending back the relevant data, the controller records the time elapsed between the initial query and the receipt of the reply. This time difference represents the communication delay between the switch and the controller, which is a crucial component of the overall detection time.

Once the flow stats are obtained, they are fed into our machine learning-based prediction algorithm. The algorithm analyzes the data and determines whether the flow exhibits characteristics indicative of a DDoS attack. After the prediction is completed, we calculate the time difference between the start of the prediction process and its conclusion. This time difference signifies the total prediction time.

By combining the communication delay and the prediction time, we obtain the total time required for detecting a potential DDoS attack using our SDN-based system. This comprehensive measurement provides valuable insights into the efficiency and responsiveness of our detection mechanism, enabling us to assess its effectiveness in real-time DDoS attack mitigation.

III. Results

To thoroughly evaluate the performance of our SDN-based DDoS attack detection system, we conducted a series of rigorous experiments using the hping3 utility. We employed two distinct configuration options: fast and flood, to simulate different intensities of DDoS attacks.

In the fast option, we executed the attack a total of 5 times, ensuring a consistent and reliable assessment of the system's response under this specific attack scenario. On the other hand, for the flood option, which represents a more severe and resource-intensive attack, we performed the attack a total of 10 times. This increased number of iterations allowed us to gather a larger dataset and obtain a more comprehensive understanding of the system's behavior under extreme conditions.

The measured times for each attack scenario were meticulously recorded and presented in a well-structured table. This table serves as a central repository for the results obtained from our experiments, providing a clear and concise overview of the detection system's performance.

A thorough examination of the information presented in the table can provide us with crucial insights regarding the performance and efficacy of our SDN-powered detection system in recognizing and countering DDoS threats. The results enable us to assess the system's response times, accuracy, and overall robustness when confronted with varying attack intensities.

Moreover, the data collected from these experiments forms a solid foundation for further analysis and optimization of the detection system. By leveraging this information, we can identify potential areas for improvement, fine-tune the system's parameters, and enhance its ability to safeguard the network against DDoS threats in real-world scenarios.

Through these comprehensive experiments and the resulting data, we aim to validate the effectiveness of our SDN-based DDoS attack detection system and contribute to the ongoing efforts in developing robust and reliable security solutions in the face of evolving cyber threats.

TABLE I
PREDICTION TIMES

Attack Type	**Prediction Times in seconds**		
	Minimum	***Maximum***	***Average***
fast	0.1	0.32	0.22
flood	2.05	8.9	4.75

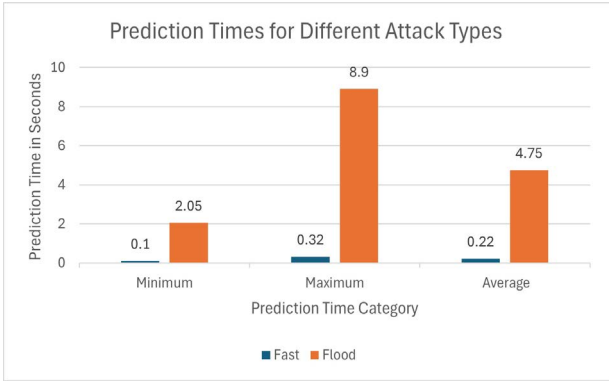

Fig. 2. Prediction Times

A. Observations

In our analysis of the SDN-based DDoS attack detection system, we have identified two primary components that contribute to the total time required for detection: the communication latency between the switch and the controller, and the time taken to make the prediction. Our findings reveal that the communication latency is the dominant factor, while the prediction latency is comparatively negligible.

The results of our experiments, as presented in the table, provide valuable insights into the relationship between the attack intensity and the communication latency. When we performed the attack using the 'fast' option, which does not completely overwhelm the switch, we observed an average prediction time of 0.22 seconds. This indicates that under moderate attack conditions, the switch is still able to respond to the controller's requests within a reasonable timeframe.

However, when we employed the 'flood' option, which unleashes a relentless barrage of packets, the switch becomes totally overwhelmed. This is evident from the significantly higher average prediction time of 4.75 seconds. The flood attack generates a tremendous amount of traffic, causing the switch to struggle in processing and responding to the controller's requests. As a result, the communication latency increases dramatically, leading to a longer overall detection time.

These findings underscore the critical role of the communication delay between the switch and the controller in determining the effectiveness and responsiveness of the DDoS attack detection system. The attack intensity directly impacts the switch's ability to handle the incoming traffic and communicate with the controller in a timely manner.

To mitigate the impact of communication latency on the detection time, it is essential to optimize the network infrastructure and ensure that the switch has sufficient resources to handle high-volume attacks. This may involve implementing load balancing techniques, upgrading hardware capabilities, or employing additional security measures to prevent the switch from being overwhelmed.

Furthermore, our analysis highlights the importance of considering the communication latency when designing and deploying SDN-based DDoS attack detection systems. By understanding the factors that influence the communication delay and its impact on the overall detection time, network administrators and security professionals can make informed decisions to enhance the system's performance and minimize the detection latency.

In conclusion, our study emphasizes the significance of the communication latency between the switch and the controller in the context of SDN-based DDoS attack detection.

IV. Conclusion

In this study, we have undertaken a comprehensive evaluation of the performance characteristics exhibited by a DDoS attack detection system that integrates Software-Defined Networking (SDN) principles with machine learning algorithms for predictive analysis. The results of our investigation highlight that the prediction latency, defined as the time required by the machine learning model to categorize a network flow as either legitimate or malicious, constitutes a relatively minor component of the overall prediction process. This suggests that the SDN-based DDoS detection approach, coupled with machine learning techniques, can provide efficient and timely identification of potential threats without introducing significant delays in the system's response time.

The major component of the overall detection time is the communication delay between the switch and the controller. This delay encompasses the time required for the controller to send flow stats requests to the switch, and for the switch to respond with the corresponding flow stats replies.

Our analysis highlights the importance of optimizing the communication between the switch and the controller to minimize the detection time and enhance the responsiveness of the SDN-based DDoS attack detection system. By reducing this communication delay, we can significantly improve the system's ability to identify and mitigate DDoS attacks in real-time.

REFERENCES

[1] H. Kousar, M. M. Mulla, P. Shettar, and D. G. Narayan, "Detection of ddos attacks in software defined network using decision tree," in *2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)*, 2021, pp. 783–788.

[2] A. M. Mankawade, P. D. Kolpe, A. M. Pote, S. D. Patil, and S. S. Patil, "A dynamic framework for ddos attack detection and mitigation in software defined network using machine learning," in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, 2024, pp. 1–7.

[3] P. S. Saini, S. Behal, and S. Bhatia, "Detection of ddos attacks using machine learning algorithms," in *2020 7th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2020, pp. 16–21.

[4] J. He, Y. Tan, W. Guo, and M. Xian, "A small sample ddos attack detection method based on deep transfer learning," in *2020 International Conference on Computer Communication and Network Security (CCNS)*, 2020, pp. 47–50.

[5] B. Kiruthika Devi, G. Preetha, G. Selvaram, and S. Mercy Shalinie, "An impact analysis: Real time ddos attack detection and mitigation using machine learning," in *2014 International Conference on Recent Trends in Information Technology*, 2014, pp. 1–7.

[6] J. A. Pérez-Díaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, "A flexible sdn-based architecture for identifying and mitigating low-rate ddos attacks using machine learning," *IEEE Access*, vol. 8, pp. 155 859–155 872, 2020.

[7] S. Sanapala, D. D. Reddy, G. L. Chowdary, and K. Vikyath, "Machine learning based ddos attack detection in software defined networks (sdn)," in *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, 2023, pp. 1124–1126.

[8] H. Polat, O. Polat, and A. Cetin, "Detecting ddos attacks in software-defined networks through feature selection methods and machine learning models," *Sustainability*, vol. 12, no. 3, 2020. [Online]. Available: https://www.mdpi.com/2071-1050/12/3/1035

[9] "Dataset-cic-ddos2019," https://www.kaggle.com/datasets/dhoogla/cicddos2019.

[10] M. C. P. Saheb, M. S. Yadav, S. Babu, J. J. Pujari, and J. B. Maddala, "A review of ddos evaluation dataset: Cicddos2019 dataset," in *Energy Systems, Drives and Automations*, J. R. Szymanski, C. K. Chanda, P. K. Mondal, and K. A. Khan, Eds. Singapore: Springer Nature Singapore, 2023, pp. 389–397.