DDoS Attack Detection using SDN Dataset

Prof. Rahul Suryawanshi[1], Pranav Hirulkar[2], Rushikesh Samudrawar[3], Ritesh Badguye[4], Prathmesh Masalkar[5]

[1,2,3,4,5] *Artificial Intelligence GH Raisoni College of Engineering and Management Nagpur, Maharashtra, India*

***Abstract*— Software Defined Networking (SDN) has recently gained significant attention in research due to its innovative design, which separates the control plane from the data plane. This separation allows for easier and more efficient network programmability compared to traditional networks. In conventional networks, any change would require reconfiguration of multiple resources, whereas in SDN, a single individual with expertise in the control plane (controller) can manage all network resources and update rules in a much shorter time. One of the most prevalent and damaging attacks today is the Distributed Denial of Service (DDoS) attack, which renders services unavailable for an extended period. In this paper, we propose a method to detect DDoS attacks targeting one or multiple victims simultaneously by combining two machine learning algorithms: entropy and Principal Component Analysis (PCA). We evaluate the effectiveness of our approach using the Mininet emulator, a POX controller, and Open vSwitch as the switch. Our results demonstrate a high detection accuracy in identifying DDoS attacks.**

***Keywords*— SDN, DDoS attack, Controller, PCA, Entropy, Machine Learning.**

I. INTRODUCTION

The rapid advancement of information technology (IT) has revolutionized industries, creating an interconnected world where digital devices and services have become indispensable. The ubiquity of these devices, from personal smartphones to large-scale industrial control systems, has enabled the generation and storage of vast amounts of data—often referred to as big data. This convergence of technology has opened up a myriad of opportunities for businesses and individuals alike, but it has also introduced significant challenges, particularly in terms of cybersecurity.

As devices and systems become increasingly interconnected, they also become more vulnerable to a range of cyber threats. The explosion of digital data and the rise of the Internet of Things (IoT) mean that more devices are connected to networks than ever before. With this interconnectedness comes a greater risk of cyberattacks, as malicious actors can exploit vulnerabilities in one part of the system to gain access to another. One of the most damaging forms of attack in this era is the Distributed Denial of Service (DDoS) attack, which targets the very infrastructure of the internet, often crippling entire websites, networks, or services.

In the face of such growing threats, traditional security measures are no longer sufficient. The need for more advanced solutions has led to the development of attack detection systems (ADS) that leverage machine learning (ML) to detect and mitigate these attacks in real-time. The fusion of big data and machine learning is creating a new frontier in cybersecurity, enabling organizations to protect the pillars of security: confidentiality, integrity, and availability.

In today's digitally interconnected world, Distributed Denial of Service (DDoS) attacks have become one of the most common and devastating forms of cyberattacks. These attacks aim to disrupt the availability of a targeted system, service, or network by overwhelming it with an excessive amount of traffic. As digital services and cloud-based systems grow, the potential damage caused by a successful DDoS attack can be severe, ranging from prolonged system downtime to loss of revenue and reputational damage. Given the increasing sophistication and scale of DDoS attacks, traditional defensive mechanisms such as firewalls and intrusion detection systems (IDS) are often inadequate. Therefore, new approaches, including machine learning (ML)-based detection systems integrated with Software-Defined Networking (SDN) environments, have gained significant attention in research and practice for their ability to provide dynamic and efficient defense mechanisms against DDoS attacks.

A Distributed Denial of Service attack involves flooding a target system with a massive volume of traffic, rendering it incapable of responding to legitimate requests. These attacks are often orchestrated using botnets—networks of compromised devices controlled by an attacker. Unlike traditional Denial of Service (DoS) attacks, DDoS attacks utilize multiple attack vectors simultaneously, making them difficult to mitigate. The attacks can be classified into several categories:

These involve overwhelming a network's bandwidth with excessive data traffic. Examples include UDP floods and ICMP floods, which aim to exhaust the target's available resources.

These exploit weaknesses in network protocols, such as SYN floods or fragmented packet attacks, which overwhelm the target's processing capacity by exploiting vulnerabilities in the underlying protocol stack.These target specific services or applications, such as HTTP or DNS servers, by overloading the server with seemingly legitimate requests, making it difficult for the system to differentiate between normal and malicious traffic.

Given the evolving nature of these threats, a static, rule-based system is often insufficient for detecting and mitigating DDoS attacks, especially in real-time. This has led to the exploration of machine learning models that can adaptively learn from network traffic patterns and detect anomalies indicative of an attack.

Machine learning offers a promising solution for enhancing DDoS attack detection because of its ability to learn from historical data, recognize patterns, and make predictions based on new traffic data. Unlike traditional rule-based systems, ML-based DDoS detection systems can continuously improve their performance by adjusting to evolving attack patterns. By analyzing various network traffic features, such as packet size, traffic volume, and connection duration, ML algorithms can classify whether a traffic flow is normal or indicative of a DDoS attack.

Several machine learning algorithms are commonly used for DDoS detection:

- Supervised learning: This involves training a model on labeled datasets where traffic is explicitly classified as normal or malicious. Common algorithms include decision trees, random forests, support vector machines (SVM), and neural networks. Once trained, the model can classify new traffic as either benign or an attack.
- Unsupervised learning: In scenarios where labeled data is not available, unsupervised learning algorithms can be used to detect anomalies in the network traffic. Techniques like clustering (e.g., k-means) or autoencoders can identify outliers, which may be indicative of DDoS attacks.
- Reinforcement learning: This approach can be applied in dynamic environments where the system continuously learns from interaction with the network environment and makes real-time decisions to mitigate attacks.

By employing these techniques, ML-based detection systems can achieve high accuracy, detect zero-day attacks, and adapt to changing attack strategies, providing a robust defense mechanism in the face of constantly evolving threats.

Software-Defined Networking (SDN) is a networking architecture that decouples the control plane from the data plane, allowing network administrators to manage network behavior programmatically using software applications. This separation enables greater flexibility and responsiveness in network management, making SDN a suitable environment for implementing DDoS detection and mitigation systems.

In a traditional network, each network device (e.g., routers, switches) operates autonomously, making it difficult to coordinate an effective response to a DDoS attack across the network. In contrast, SDN provides centralized control, enabling network administrators to monitor and manage the entire network from a single controller. This centralized view of the network allows for more efficient detection of abnormal traffic patterns and the implementation of real-time defense strategies.

II. LITERATURE SURVEY

A. Internet Attacks Enhancement

In the early days of the internet, networks were scalable and flexible, with security concerns being minimal. However, with the rapid rise in internet users over the past two decades, cyberattacks have surged significantly. [1] According to the Internet Crime Report by the Internet Crime Complaint Center (IC3) of the FBI, cyberattacks have caused a staggering $13.3 billion in losses over the past five years, with $7.7 billion of those losses occurring in just the last two years.

One of the earliest notable cybersecurity incidents was the Morris Worm attack (Rochlis & Eichin).

Since then, both the frequency and severity of cyberattacks have escalated dramatically [2]. The shift of financial and economic sectors to online platforms over the past decade has also shifted the focus of cybercriminals. For instance, the entire network infrastructure of the UK cryptocurrency exchange EXMO was crippled by a large-scale DDoS attack, with an attack volume of 30 Gbps. Similarly, the New Zealand stock exchange was taken offline for two consecutive days by another DDoS attack.

In addition to financial services, the telecommunications sector has become a major target for DDoS attacks. [3] In Q1 2021, the telecom sector rose from being the sixth most frequent DDoS target in Q4 2020 to the primary focus of such attacks (Haworth).

In 2019, the emergence of the global COVID-19 pandemic forced businesses to shift to a full-time remote work model, where many users relied on less secure home infrastructure, thereby opening the door to an increase in cyberattacks. According to the PurpleSec threat report, cybercrime surged by an alarming 600% during the pandemic. Alongside previously targeted sectors such as education and government, even coronavirus information websites became potential targets for attacker [4].

B. DDoS Attacks

The core mechanism of a Distributed Denial-of-Service (DDoS) attack is to make a target system or service unavailable to legitimate users by overwhelming it either temporarily or permanently. [5] DDoS attacks are typically executed by exploiting multiple compromised computer systems, which can range from just a few machines to as many as 100,000. One common method of launching a DDoS attack is by flooding the victim's network or web server with an excessive volume of data packets at a rapid pace. This overloads the server's resources—such as CPU capacity and memory—making it incapable of responding to legitimate users. Another approach involves sending malformed or maliciously structured packets to confuse an application or protocol, potentially causing the target system to freeze or crash.

B.1 Why are DDoS Attacks Possible?

There are numerous reasons that make a DDoS attack possible. The data packets arriving from various sources makes it tremendously difficult to identify attack source IP address. In case of slow attacks, it is hard to identify the distinction between legitimate and illegitimate traffic, which leads to bypass the majority defense mechanisms allowing attack traffic through. Apart from these, the current internet design utilizes packet-switching architecture that allows all the users to share network resources and hence bandwidth attacks cause destruction in the network. This endto-end architecture also leads to high IP Spoofing incidents, as there exists no way to authenticate a packet once it reaches the victim (Mirkovic & Reiher). Finally, the distributed nature of Internet provides the attackers with unenforceable accountability and, at the same time, making the deployment of cooperative defenses extremely difficult.

B.2 Motivation behind DDoS Attacks

Mirkovic & Reiher proposed four major reasons behind committing DDoS attack and inflicting damage onto the victim. Usually, the motivation is a personal reason [6]. It’s intended to be either fun or vengeful (or both) while at the same time demonstrating the power to disrupt a website or network, like cyberbullying and trolling. Another reason could be Hacktivism which gains respect for the hacker community by showing support or opposition regarding a certain topic like Olympic Games or due to ethical concerns like the attack on WikiLeaks. The material gains like financial or economic benefits are also a growing motivation behind DDoS attacks against corporations. The business establishments too get tempted to launch DDoS attacks against their market competitors.

C. Botnets

One common way to execute DDoS attacks is by taking advantage of many compromised machines called bots or zombies. These bots are connected to one another through the Internet, forming a group called a botnet. Every botnet has a Botmaster that communicates with all the bots, commanding them through a C&C server to carry out malicious activities. Illustrates a DDoS attack carried out by an attacker that utilize a botnet. These bots take orders from the botmaster and perform specific tasks, may be repeatedly, to destroy the target network, system or web server [7].

C.1 Botnet Communications

The botnet communications are carried out by a Command and Control (C&C) server. The C&C server is a computer that is controlled by the attacker to send commands to zombie systems to carry out an attack. Several types of C&C mechanisms are proposed in the existing literature and the C&C architectures used for communication are either centralized or decentralized:

- Centralized C&C servers: In this approach, the botmaster is connected to the C&C server to command the bots and the bots are also connected to the server to receive commands and updates. The centralized C&C servers are simple to manage on account of their single point of failure, making the response fast.
- IRC botnet: The IRC (Internet Relay Chat) is a text-based chat system that allows computer users to communicate with multiple participants in a so-called conversation channel. In a botnet, the bots connect to a specific channel in the IRC server and wait for instructions. The IRC networks are relatively easy to construct. They use simple, low bandwidth communication methods, making them widely used to host botnets. Also, they are able to continually switch channels to avoid being taken down, making them an ideal choice for coordinates. When an IRC bot connects to a specific channel, it stays in the connected state.

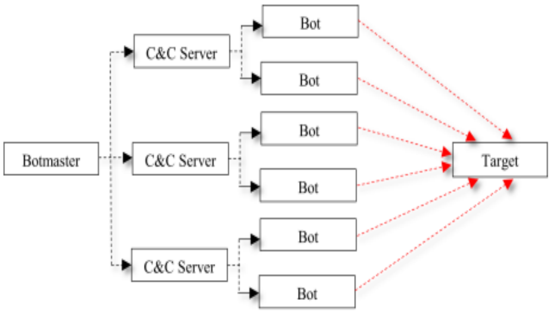

Figure 1. Botnet Employed DDoS Attack

III. METHODOLOGIES

Random forest (RF) is one of the popular machine learning techniques which is used for classification. The random forest produces different decision trees. Each tree is built by an alternate bootstrap test from the first information utilizing a tree classification algorithm.

Random Forest is a widely used machine learning algorithm for detecting DDoS (Distributed Denial of Service) attacks due to its robustness and ability to handle complex datasets. It operates by constructing multiple decision trees during the training process, where each tree is trained on a random subset of the data and features. This ensemble of decision trees makes Random Forest a highly effective classifier, as it mitigates overfitting and improves generalization by averaging the results from multiple trees.

In DDoS attack detection, the dataset typically consists of network traffic features, such as packet sizes, number of requests, source/destination IP addresses, and traffic intervals. Random Forest identifies patterns in these features that distinguish normal traffic from attack traffic. By splitting the data on different features in each tree, it can capture a wide variety of patterns that indicate potential DDoS attacks, such as a high volume of traffic coming from a small number of IP addresses in a short time period.

One of the key advantages of Random Forest in this context is its ability to handle noisy and imbalanced datasets, which are common in real-world DDoS detection scenarios. It can process large amounts of network data efficiently, providing accurate detection with low false-positive rates. Furthermore, Random Forest's inherent feature importance ranking can help identify which network traffic characteristics are most critical in distinguishing attack traffic from legitimate traffic. This makes it a powerful tool in the development of DDoS mitigation strategies.

Deep learning-based detection uses neural networks, such as recurrent neural networks (RNNs) or convolutional neural networks (CNNs), to analyze traffic data, often improving detection accuracy in complex environments. These methodologies help detect and mitigate DDoS attacks by analyzing and classifying network traffic.

It measures the frequency of the attack instances of both classes correctly identified.

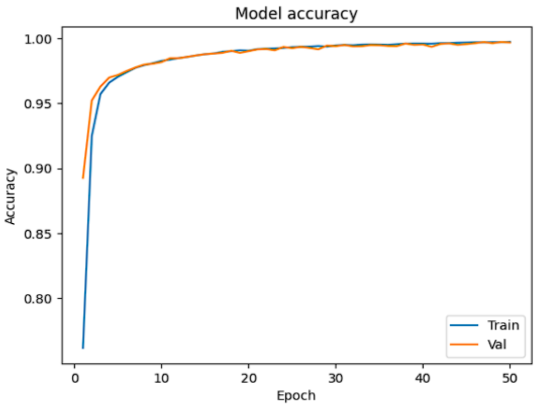

Figure 2. Model accuracy

Accuracy = TP + TN/ TP + FN + FP + TN

- Precision: It is the ratio of the number of related attacks that were identified to the total number of unrelated and related attacks that were identified. Also known as positive predictive value.

$$\text{Precision} = TP / TP + FP$$

- Recall: This is the ratio of the number of related attacks to the total number of related attacks received and also known as positive sensitive value.65

$$\text{Recall} = TP / TP + FN$$

A lower loss signifies that the model's predictions are closer to the true values, meaning it can distinguish malicious traffic patterns more accurately. Both metrics play a crucial role in tuning and improving the model's ability to detect DDoS attacks efficiently. Another challenge in DDoS detection using ML is handling imbalanced datasets, where the amount of benign traffic often far outweighs attack traffic.

Accuracy indicates how well the model distinguishes between normal and malicious traffic, which is critical in real-world DDoS detection, where false positives (misclassifying legitimate traffic as an attack) and false negatives (failing to detect an attack) can lead to serious consequences. A model with high accuracy can ensure timely detection of various DDoS attack types, such as SYN floods, UDP floods, and HTTP-based attacks.

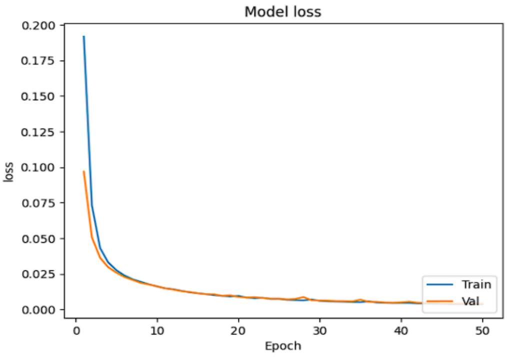

Figure 3. Model loss

Table 1 Classification summary

Correctly classified attack instances	22,490	99.7605%
Incorrectly classified attack instances	54	0.2395%

Table 2 Performance evaluation

TP rate	FP rate	Precision	Recall	Class
0.98	0.002	0.997	0.998	Normal
0.998	0.002	0.998	0.998	Attack

Table 3 Confusion matrix

a	b	Classification
9689	22	a=normal
32	12,801	b=attack

IV. RESULT AND DISCUSSION

In this study, normal and attack traffic in the dataset obtained from the SDN environment was classified using machine learning algorithms. The customized SDN-based dataset consists of TCP, UDP, and ICMP normal and attack traffics. The dataset has statistical features such as byte_count, duration_sec, packet rate, and packet per flow except for features that define source and target machines. The NCA algorithm has been used to perform an effective classification and to select the most suitable features. After analyzing 22 network features NCA algorithms, 14 effective features were selected and given as input to machine learning algorithms. More than 100 thousand network records were classified by kNN, DT, ANN, and SVM algorithms after preprocessing and feature selection. The experimental results show that DT has a better accuracy rate than the other algorithms with 100%. In future studies, it is planned to increase the diversity of attacks and compare the classification performances of machine learning models with feature selection algorithms

V. CONCLUSION

This paper presents a novel lightweight method to detect DDoS attacks over SDN architecture. By combining two important ML algorithm E-PCA to identify DDoS attacks that focus on one end-user like a server or a number of them simultaneously. We conducted experiments under two types of attacks. The experiment results show our method is highly effective with a high percentage of accuracy to detect the attack. In future work, we need to combine other ML algorithms like SVM, ANN and K-Mean. In addition, to find a method to mitigate the network after the attacks are revealed.

REFERENCES

[1] Ganorkar, S. S., Vishwakarma, S. U., & Pande, S. D. (2014). An information security scheme for cloud based environment using 3DES encryption algorithm. International Journal of Recent Development in Engineering and Technology, 2(4). J. Clerk Maxwell, A Treatise on Electricity

and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Pande, S., & Gadicha, A. B. (2015). Prevention mechanism on DDOS attacks by using multilevel filtering of distributed firewalls. International Journal on Recent and Innovation Trends in Computing and Communication, 3(3), 1005–1008. ISSN: 2321–8169.

[3] IC3. (2020). Internet crime report 2020. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/ AnnualReport/2020_IC3Report.pdf.

[4] Haworth, J. (2021a, February 16). UK cryptocurrency exchange EXMO knocked offline by 'massive' DDoS attack. The Daily Swig | Cybersecurity News and Views.

[5] Haworth, J. (2021b, April 21). Telecoms industry facing increased DDoS attacks, report warns. The Daily Swig | Cybersecurity News and Views.

[6] Haworth, J. (2020, August 26). New Zealand stock exchange hit by series of DDoS attacks. The Daily Swig | Cybersecurity News and Views.

[7] Brun, O., Yin, Y., & Gelenbe, E. (2018). Deep learning with dense random neural network for detecting attacks against IoT-connected home environments. Procedia Computer Science, 134, 458–463, Published by Elsevier Ltd.

[8] N. Meti, D. Narayan, and V. Baligar, "Detection of distributed denial of service attacks using machine learning algorithms in software defined networks," in 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017: IEEE, pp. 1366-1371.

Multi-Layer perceptron

UDP -Accuracy Score-0.9414609571788413

TCP-Accuracy Score-0.6394519306986751

ICMP-Accuracy Score-0.999919335323062

KNN

UDP-Accuracy Score-0.9621158690176322

TCP-Accuracy Score-0.7990035103612275

ICMP-Accuracy Score-0.9244978623860611

SVM

UDP-Accuracy Score-0.6605541561712847

TCP-Accuracy Score-0.6720643188766844

ICMP-Accuracy Score-0.7991449544244575

Random Forest

UDP-Accuracy Score-1.0

TCP-Accuracy Score-0.9997735250820972

ICMP-Accuracy Score-1.0

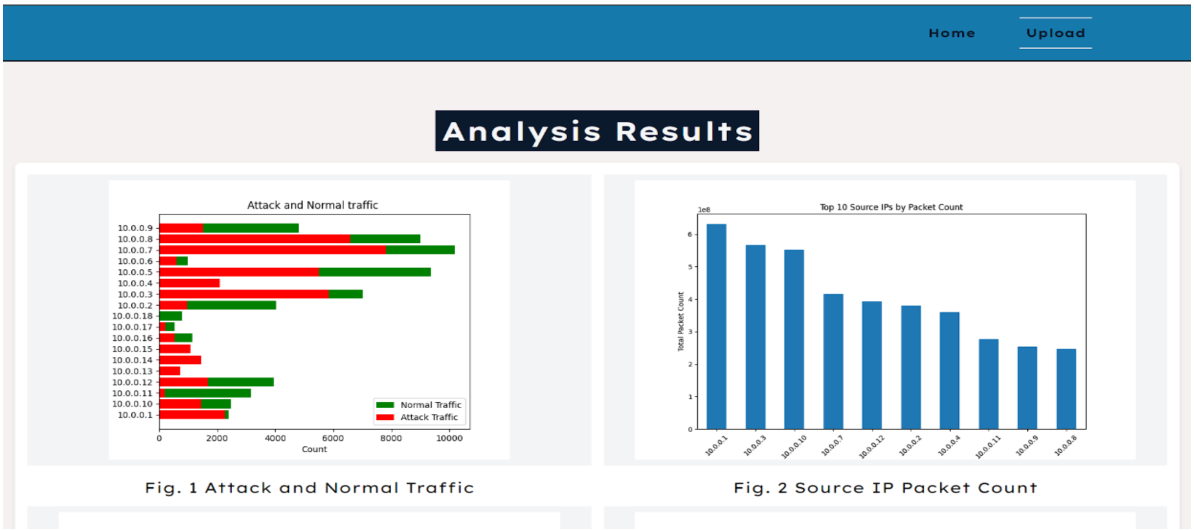

Fig. 1 Attack and Normal Traffic

Fig. 2 Source IP Packet Count

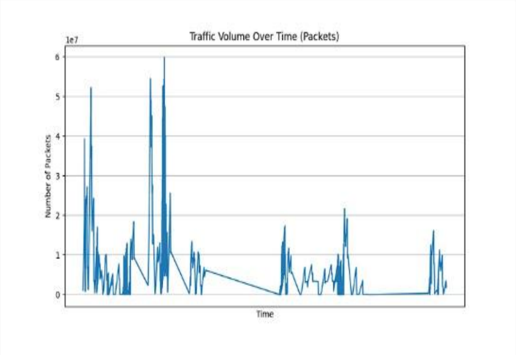

Fig. 3 Traffic Volume Over Time

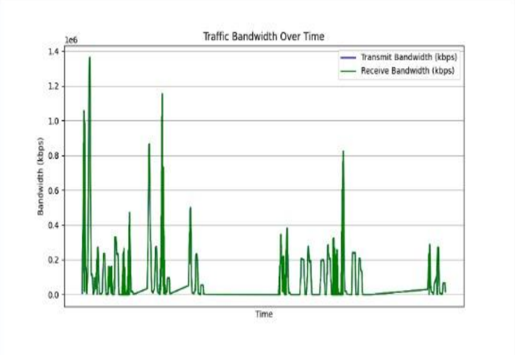

Fig. 4 Traffic Bandwidth Over Time