Review on DDOS Detection using Machine Learning

Jeswin Johnson
M.Tech student, CSE Dept.
Mangalam College of Engineering,
Ettumannor,Kottayam India

Dr. Sabu George
Associate .Professor, CSE Dept.
Mangalam College of Engineering,
Ettumannor,Kottayam India

Abstract:- **In today's world, technology has become an unavoidable element of human life. In fact, during the Covid-19 epidemic, everything from the business sector to educational organizations has transitioned from offline to online. It leads to exponential growth in intrusions and assaults across the Internet-based technologies. One of the fatal danger rising is the Distributed Denial of Service (DDoS) assault that may shut down Internet-based systems and applications in no time. The attackers are changing their skill techniques frequently and consequently avoid the existing detecting mechanisms. Since the number of data created and stored has expanded manifolds, the standard detection systems are not suited for identifying modern DDoS attacks. This work systematically evaluates the prominent literature specifically in deep learning to identify DDoS using machine learning techniques.**

Index Terms— DDoS, , Network Intrusion Detection System, Machine Learning, Deep Learning.

I. INTRODUCTION

A distributed denial of service (DDoS) assault sends floods of attack packets to the target resources, rendering them inaccessible to normal users on the network and on the victim host. A DoS attack radiates from a single source and floods resources that serve genuine traffic.. Currently, one of the most prevalent network assaults is distributed denial-of-service. The damage caused by a DDoS assault is getting worse as computer and communication technology advance so quickly. Therefore, it is more crucial than ever to do research on DDoS attack detection. DDOS is a server attack where the main goal is to deny authorized users access to the source. In this case, it completely disables one user source. Multiple digital device which are connected is more vulnerableHackers may also aim for personal information and data that protects them from unauthorized additions [4]. Nowadays some related research has been conducted and certain advancements have been made. However, there is yet no detection system with a detection accuracy that is sufficient, due to the diversity of DDoS attack tactics and the fluctuating amount of attack traffic.

1.1 Working of DDOS attack

DDoS attacks are done by using networks of machines linked to the Internet. These networks are made up of computers and other devices (such as IoT devices) that have been infected with malware, allowing an attacker to manage them remotely. Individual devices are known as bots (or zombies), while a network of bots is known as a botnet. After establishing a botnet, the attacker may conduct an attack by sending remote commands to each bot. When the botnet targets a victim's server or network, each bot sends requests to the target's IP address, possibly overloading the server or network and triggering a denial of service to regular traffic. Because each bot is a genuine Internet device, distinguishing between attack and normal traffic can be challenging.

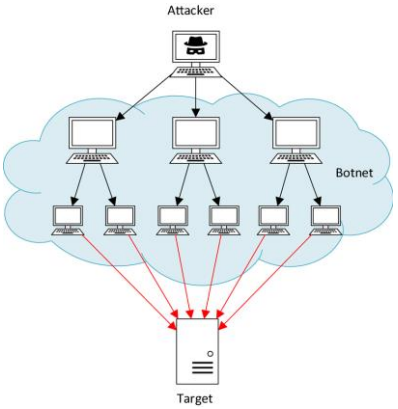

Figure 1:DDOS attack with Botnet

1.2 Identification of DDOS attack

One of the most visible indication of a DDoS attack is a site or service being abruptly sluggish or unavailable. However, because a valid rise in traffic might result in identical performance concerns, more analysis is typically necessary. Some of these warning signals of a DDoS attack can be detected using traffic analytics tools:

- Excessive amounts of traffic coming from a single IP address or IP range
- A surge of traffic from users who have a common behavioral profile, such as device type, geography, or web browser version.
- An unusual increase in requests to a single page or endpoint.
- Unusual traffic patterns, such as spikes at unexpected times of day or patterns that appear to be artificial (e.g. a spike every 10 minutes).Other, more precise indicators of a DDoS attack differ depending on the type of attacks.

1.3 Various types of DDOS attack

A. UDP Flood:

A denial-of-service (DDoS) attack that floods a target using

User Datagram Protocol (UDP) packets. The attack's purpose is to flood random ports on a remote computer. This causes the host to look for the application listening on that port frequently and, if none is discovered, to respond with an ICMP 'Destination Unreachable' packet.

B. ICMP (Ping) Flood:

An ICMP flood attack, like a UDP flood attack, overwhelms the target resource with ICMP Echo Request (ping) packets, often delivering packets as quickly as possible without waiting for answers. Because the victim's servers frequently attempt to react with ICMP Echo Reply packets, this form of attack can use both outgoing and incoming bandwidth, resulting in a large overall system delay.

C. SYN Flood:

A SYN flood DDoS attack takes use of a known vulnerability in the TCP connection process (the "three-way handshake"), in which a SYN request to establish a TCP connection with a host must be matched with a SYN-ACK response from that host, followed by an ACK response from the requester.

D. Ping of Death:

The attacker conducts a ping of death ("POD") assault by delivering repeated faulty or malicious pings to a machine. A huge IP packet is divided into many IP packets (known as fragments) in this situation, and the destination host reassembles the IP fragments into the whole packet. This can cause memory buffers assigned to the packet to overflow, resulting in denial of service for genuine packets.

E. Slowloris:

Slowloris is a highly focused attack that allows one web server to bring down another without disrupting other services or ports on the target network. Slowloris does this by keeping as many connections to the target web server open as feasible. It does this by connecting to the target server but transmitting only a portion of the request.

F. HTTP Flood:

The attacker uses seemingly valid HTTP GET or POST requests to attack a web server or application in an HTTP flood DDoS attack. HTTP floods utilize less bandwidth than other attacks to bring down the targeted site or server since they do not involve faulty packets, spoofing, or reflection methods. The attack is most successful when it pushes the server or application to dedicate the greatest amount of resources to each and every request.

G. NTP Amplification:

The perpetrator of an NTP amplification attack uses publicly accessible Network Time Protocol (NTP) servers to flood a targeted server with UDP traffic. Because the query-to-response ratio in such cases ranges between 1:20 and 1:200 or more, the attack is classified as an amplification assault. This implies that anyone with access to a list of accessible NTP servers may simply launch a catastrophic high-bandwidth, high-volume DDoS attack.

II LITERATURE REVIEW

Various researchers have devised measures to avoid DDOS attacks [1][5][8]. Some key approaches are discussed further below.

Jiangtao Pei et al. [5] employed a DDoS attack tool to execute local attacks in their study. The packet capture tool compares the capture attack to normal packets, discovers the laws of data attack, and then converts it into data attack characteristics. The random forest approach was employed in machine learning to detect the DDoS assault. It begins by extracting the feature and format conversion, which is then utilized to conduct the characteristics on a big scale. These collected characteristics are sent into the random forest algorithm, which detects the DDoS assault.

Ancy Sherin Jose et al. [2] hypothesized that OpenFlow enable SDN to capture flow data from which derived features may be obtained. They also said that DDoS categorization was performed using a dataset containing simulated networks. To research and identify DDoS more precisely, experimental characteristics are employed for assessment. They used 7 characteristics from Group 3 and achieved an overall accuracy of 99.99 percent. They discovered the finest two attributes that assist us in detecting DDoS attacks. The attributes employed can be used to create a lightweight model for multistage classification. When numerous attacks are performed at the same time, the protocol entropy might drop.

Sara Abdalelah Abbas[10] , They used dimensionality reduction techniques known as principal component analysis in their study (PCA). They have decreased the amount of characteristics utilized in training. They also trained the model using multiple machine learning models. Using the best-trained machine-learning system, they achieved an accuracy of 99.97%.

F. Nisha Ahuja and colleagues [7] Software Defined Networking [SDN] is defined by software in which traffic is managed , centralized and directed between hosts. The SDN dataset is used to train the model and generate the mininet emulator. The author used Random Forest and Support Vector Machine [SVM] in these research articles to categorize traffic using SVC results and filtering across the Random Forest. The model's accuracy is 98.8 percent and its precision is 98.27 percent, indicating that the class is right in many circumstances. The accuracy indicated that detection was performed in the absence of traffic management.

III COMPARATIVE ANALYSIS

Table 1: Accuracy of DDOS detection using various machine-learning algorithms

Sl.No	Topic	Author Name	Algorithm	Accuracy
1	Detecting Flooding DDOS Attacks Over Software Defined Networks using Machine Learning Techniques	Ancy Sherin Jose, Latha R Nair,Varghese Paul	Support Vector Machine	99.99%.
2	Distributed Denial Of Service Attacks Detection System By Machine Learning Based On Dimensionality Reduction	Sara Abdalelah Abbas, Mahdi S.Almhanna	PCA	99.97%
3	A DDoS Attack Detection Method Based on Machine Learning	Jiangtao Pei, Yunli Chen, Wei Ji	Random Forest Algorithm	99.49%
4	Feature selection and comparison of classification algorithms for wireless sensor networks	Pande S, Kamparia A., Gupta D	SVM, Perceptron, K-nearest neighbor	98.87%
5	Automated DDOS attack detection in software-defined networking.	Nisha Ahuja, Gaurav Singal,Debajyoti Mukhopadhyay,Neeraj Kumar	Random Forest and Support Vector machine	98.8%

IV CONCLUSION

A DDoS attack happens when numerous hacked computers are utilized to conduct an attack on a single target, overloading it with unwanted traffic and taking it down or drastically degrading its performance. Either situation may also confuse IT workers, allowing black hat hackers to exploit additional weaknesses, steal data, or infect a network with other types of malware. DDOs attacks will continue to be a major danger to many large and small enterprises since they cause a wide range of harm to internet users. Areas that may rely on human operators, high computing times, and a lack of freely available data Still, several areas must be prioritized in order to identify DDoS attacks. DDoS attacks are detected using a variety of algorithms, including Linear Regression, Random Forest, selection. Their dataset component analysis, recursive The study also discusses the future of analyzing and performing DDoS attacks using a deep learning model, as well as topological attack detection.

K. Pande S. et al. [3] proposed that they employed univariate feature selection, principal component analysis, recursive feature removal, and univariate feature characteristics. They decreased the number of features to 11 after completing feature selection, and then trained the machine learning algorithms. For training the model, they employed five distinct machine learning algorithms: SVM, perceptron, K-nearest neighbor, stochastic gradient descent, and XGboost. They achieved the highest accuracy of 98.87 percent.

Deep learning is particularly important for detecting DDoS attacks that employ Convolution neural networks. So, we've gone through numerous techniques for detecting DDoS attacks. DDoS attacks have reached a tipping point, with the low cost and accessibility of initiating an attack implying that their frequency will only rise. We saw something similar happen with spam a few years ago, when the cost of sending bulk email reduced, compute power, bandwidth, and email software improved, and the number of SPAM grew. Similarly, trends in the cost, performance, and availability of current DDoS attacks indicate that these will proliferate in future.

V REFERENCES

[1] Dutta Sai Eswari1, P.V.Lakshmi, A Survey On Detection Of Ddos Attacks Using Machine Learning Approaches, Turkish Journal of Computer and Mathematics Education,2021.
[2] Ancy Sherin Jose, Latha R Nair2, Varghese Paul. Towards Detecting Flooding DDOS Attacks Over Software Defined Networks Using Machine Learning Techniques published in Genetic 2021
[3] Pande, S., Khamparia, A. & Gupta, D. Feature selection and comparison of classification algorithms for wireless sensor networks. J Ambient Intell Human Compute (2021).
[4] Parvinder Singh Saini, Sajal Bhatia, Sunny Behal. Detection of DDos attack using machine learning algorithms published in research gate in March 2020.
[5] Jiangtao Pei, Yunli Chen, Wei Ji." A DDoS Attack Detection Method Based on Machine Learning" published in ICSP 2019.
[6] Chin-Shiuh Shieh, Wan-Wei Lin, Thanh-Tuan Nguyen, Chi-Hong Chen, Mong-Fong Horng and Denis Miu. Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model , IEEE ICICT 2021.

[7] Nisha Ahuja, Gaurav Singal, Debajyoti Mukhopadhyay, Neeraj Kumar. Automated DDOS attack detection in software defined networking published in Science Direct 2021.
[8] Alzahrani, R.J.; Alzahrani, A. Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic. Electronics 2021, 10, 2919. https://doi.org/10.3390/electronics10232919.
[9] Pheeha Machaka, Olasupo Ajayi, Hloniphani Maluleke, Ferdinand Kahenga, Antoine Bagula, Kyandoghere Kyamakya,Modelling DDoS Attacks in IoT Networks using Machine Learning,2021.
[10] Sara Abdalelah Abbas , Mahdi S. Almhanna ,Distributed Denial Of Service AttacksDetection System By Machine Learning Based On Dimensionality Reduction, Icmaict 2020.
[11] Swathi Sambangi and Lakshmeeswari Gondi."A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression" published in 25 December 2020.
[12] Alzahrani, R.J.; Alzahrani, A. Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic. Electronics 2021, 10, 2919.https://doi.org/10.3390/electronics10232919.