A Survey on Deep Learning by Hybrid Approach for DDOS Attack and Prevention

Voseen [1], Ghanshyam Sahu [2], Lalit Kumar P Bhaiya [3]

[1]*M. Tech Scholar, Department of CSE, Bharti College of Engineering and Technology, Durg, Chhattisgarh, India.*

[2]*Associate Professor, Department of Computer Science & Engineering, Bharti College of Engineering and Technology, Durg, Chhattisgarh, India.*

[3]*Associate Professor, Bharti University, Durg, Chhattisgarh, India.*

Corresponding Author: voseen5@gmail.com

Abstract: - DDoS is one of the most dangerous threats on the Internet today which prevents access to vital services. The variety of attack methods and the amount of real-time traffic that needs to be analyzed make DDoS detection difficult. On the Internet, there are a sizable variety of network security tools that may be used to both create and defend against network assaults [1]. With the aid of advanced assaulting tools, attackers can produce attack traffic that resembles regular network traffic. Several defense strategies fall short in this context of real-time DDoS assault detection. In this paper we reviewed and studied different techniques for solving DDOS (Distributed Denial of Service) attacks and in future implement we will develop a hybrid approach that combines deep learning models which provides an effective feature extraction and finds most of relevant features that sets automatically without any human interpretation. We performed a thorough analysis of the DDoS issue in this research and suggested a straightforward taxonomy to classify the assault extent and potential mitigation options. This taxonomy helps assist software developers and security experts in comprehending the typical flaws that motivate attackers to initiate DDoS attacks.

Key Words— DDOS, Auto-encoder, Software Defined Network, Categorization of Attacks and Defense.

I. INTRODUCTION

DDOS (Distributed Denial of Service) is type of malicious cyber-attack which was used by cyber criminals to block access on a host system, online service or network resource by its intended users. In tandem with the Internet's and related computer networks' rapid expansion, DDoS attacks are becoming more complicated and common. On the Internet, there are numerous network security technologies that may be used to both create and protect against network assaults. With advanced assaulting tools, attackers can produce attack traffic that resembles regular network traffic.

Manuscript revised April 18, 2023; accepted April 19, 2023. Date of publication April 22, 2023.

This paper available online at www.ijprse.com

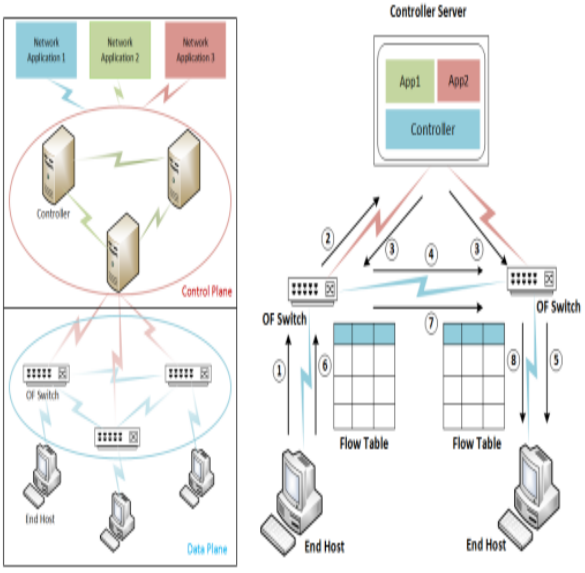
ISSN (Online): 2582-7898; SJIF: 5.59

Several defense strategies fall short in this context of real-time DDoS assault detection. When it comes to traffic characteristics, DDoS attack traffic often acts differently from legitimate network traffic.

AE(AutoEncoder) is a feed-forward neural network that is unsupervised. It is made up of numerous hidden layers, an output layer, and an input layer. The layout is symmetrical, with any hidden layers typically having fewer neurons than the input and output layers while the output layer shares the same number of neurons as the input layer. One of the hidden layers with the fewest neurons is the bottleneck layer, also known as a latent space.

The SDN architecture reduces network devices, sometimes known as "switches," to basic packet-forwarding components by decoupling the control plane and data plane from them. Compared to the current network architecture,[2] which strongly integrates both planes, the decoupling of control logic and its centralised controller offers a number of benefits. The ability to apply policies from a single location, a controller, and monitor their impacts throughout the whole network makes management easy, reduces the likelihood of error, and improves

security. Switches become universal and vendor independent. By leveraging the API that a controller provides to them, applications that operate inside of a controller can program these switches for various purposes, such as layer 2/3 switch, firewall, IDS, and load balancer.



(a) Different planes and network applications in SDN (b) Reactive traffic flow set-up in SDN [27]

Fig, 1 An SDN architecture and basic traffic flow in SDN

II. RELATED WORK

2.1 Classification of DDOS attacks:

The classification of DDoS threats based on aberrant application layer behavior, which also offers a summary of the different DDoS tools. Additionally, it divides DDoS attack handling methods into categories based on concepts for monitoring, avoiding, detecting, and mitigating. So, the goal of this work is to address DDoS attack difficulties at the application layer and to provide information regarding handling techniques' flaws in order to improve future developments in this field.

Knowing how attacks are classified is very advised in order to mount a successful defense. We discussed the attacks and categorized them into the subsequent domains. Domains: Attack networks, repressed vulnerabilities, DDoS assault influence, attack intensity dynamics, and level of computerization methods [3].

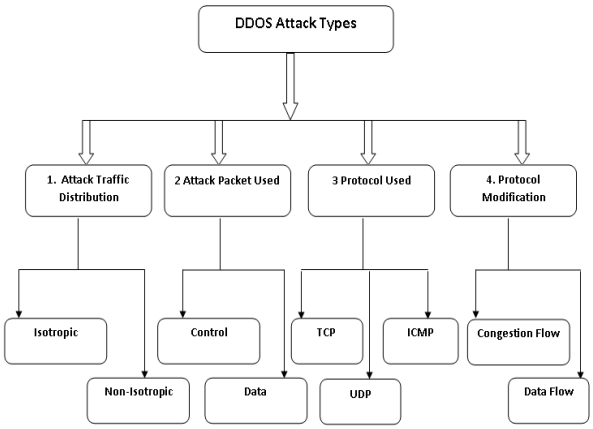


Fig.2. Types of DDOS Attacks

Under level of computerization DDoS attacks based on instructions attacker must use scanning to discover a weakness in the anticipated slave system, then break into it to install and control malicious programmers. In semi-preset DDoS attacks, the slave computer receives malicious malware from the master computer, which then scans the vulnerable device. Which kind of attack a later attacker wishes to establish must be specified. The two additional branches of semi preset assaults are direct and indirect communication.

In DDOS attack network there are two types (i) Agent handler which is composed of clients, agent and handler. Software programmers known as handlers are dispersed around the internet and are used for covert communication between agents. The slave machine where the agent is situated is the one that will really launch the DDoS attack. Using the TCP, UDP, or ICMP protocols, client and handler or handler and agent can communicate with one another.

The oppressed vulnerability, in a flood attack, the slave machine floods the target with a lot of IP packets to use up its bandwidth. This flood has the potential to either slow down or fully deplete the system. UDP and ICMP assaults are famous for flooding attacks.[3] In an intensification attack, the attacker or agent sends packets to broadcast IP addresses by taking use of the router's IP address broadcast functionality. The malicious attack traffic reduces the victim's bandwidth.

In DDOS influence attack the entire bandwidth is completely cut off at the destination end, this DDoS attack is known as a disorderly attack. A DDoS assault is considered a degrading attack if it results in a partial bandwidth usage. Degrading attacks are challenging to spot since they gradually cut off valid bandwidth. By s, the same number of IP packets that cause collateral damage are continuously sent to the victim during a

continuous attack intensity, without any breaks. With the label "variable attack intensity" [4], it is obvious that the density of attack changes over the course of the attack. Due to this characteristic, network defence measures cannot see the attack itself. Attack density affects how such attacks turn out.

2.2 DDoS Defense Categorizations

In this paper we present classification of DDOS defense mechanism according to different criteria, the classification categorizes the DDOS defense mechanism according to their deployment of location, so we are describing in the below figure as a categorization of DDOS defense Submissive defense mechanisms are those that start working only after a DDoS attack has been noticed. By monitoring inbound network traffic, passive defensive mechanisms carry out traffic restriction, blocking, and filtering.

DDOS Attack Categorization			
Level of computerization	Instruction Based Attack		
	Semi-Preset Attack	Direct Attack	
		Indirect Attack	
	Preset Attack		
Attack Network	Agent Handler	Client-Handler Communication	TCP
			UDP
			ICMP
	IRC Handler	Agent-Handler Communication	TCP
			UDP
			ICMP
Oppressed Vulnerabilities	Flood Attack	UDP Flood	Random Port
			Same Port
		ICMP Flood	
	Intensification Attack	Smurf Attack	
		Fragile Attack	Direct Attack
			Loop Attack
		TCP SYN	
		Protocol Exploitation Attack	PUSH+ACK
		Address Spoofing	Routable Address Spoofing
			Non-Routable Address Spoofing
		Malicious Formed Packet Analysis	IP Address
			IP Packet Option
Influence	Disorderly		
	Degrading		
Attack Intensity Dynamics	Continuous Attack Intensity		
	Variable Attack Intensity		

There are two types of submissive defense systems: identifying mechanisms and counter mechanisms. Identification Techniques include traffic Degree monitoring, source IP address monitoring and Packet characteristics analysis. The detecting defense transforms into the counter defence after seeing a DDoS attack. One well-known DDoS defence method is the filtering of erroneous IP packets from the flow.

Counter defense mechanism, in order to lessen the harm, the counter defense system seeks to stop the attack as quickly as feasible. Since counter defensive strategies frequently exchange attacking data like attack signatures, the defence deployment should be extensive. Base end defence, mapping trace back, packet marking trace back, and protocol-based defence are the active protection techniques at the moment.

Defense Deployment Position The sudden increase in traffic is one of the signs of a DDoS attack because high Degree IP traffic characterizes DDoS attacks. Since communication always happens between the source and the destination, a transitory node is required to make that connection. According to logic, the source end network, the transitional network, and the destination end network are the three different places where DDoS protection systems can be deployed.

III. LITERATURE REVIEW

J. Mirkovic and P. Reiher [5] –The author describes the categorises of attacks to highlight commonalities and significant aspects of attack tactics that will help produce a better response. Defenses are categorized based on the currently available defence technologies, the fundamental justification, and the unique mitigation strategy for each tool against DDoS attacks. The authors of this paper also outline various defense-related difficulties and make the case that, if these difficulties can be resolved, the DDoS issue will be resolved entirely and based on network traffic, exploited vulnerabilities, measures for preventing assaults, and positions for defence deployment.

Rohan Doshi, Noah Apthorpe and Nick Feamster [6], Insecure consumer IoT devices have been leveraged by botnets like Mirai to launch distributed denial of service (DDoS) assaults against vital Internet infrastructure. This drives the creation of novel methods to swiftly identify consumer IoT attack traffic. Using a range of machine learning algorithms, including neural networks, we show in this study that IoT-specific network behaviours (such as a small number of endpoints and regular packet intervals) can help with feature selection and produce highly accurate DDoS detection in IoT network traffic. These findings suggest that low-cost machine learning techniques and flow-based, protocol-independent traffic data could be used by home gateway routers or other network middleboxes to automatically identify local Internet of Things device sources of DDoS attacks.

Q. Liao, H. Li, S. Kang, and C. Liu [7] developed a method of detecting DDoS assaults at the application layer based on user access frequencies, particularly focused on request time interval and frequency. E time interval is the span between the current and following HTTP GET requests. The time period for a typical user may be longer than that of an attacker since a typical user will take more time to browse engaging pages. For instance, it takes about 572 seconds to access the next page after the first page loads in a normal browsing session. The latency between the current request and the future requests is shorter during DDoS attacks.

L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred[8] developed a DDoS detection method based on Chi-square distribution and source IP address entropy calculation. The scientists found that compared to the deviations brought on by DDoS assaults, the variation in source IP address entropy and chi-square statistics induced by variations in genuine traffic was rather minimal.

M. Ghanbari and W. Kinsner,[9] proposed to increase the sensitivity of the CNN in identifying DDoS attacks, a feature extraction approach based on the discrete wavelet transform and the variance fractal dimension trajectory was developed. The evaluation results demonstrate that the suggested approach recognizes DDoS assaults on the CAIDA DDoS attack dataset with 87.35% accuracy No performance data are presented to back up the authors' claim that their technique enables real-time detection of DDoS attacks in a variety of situations.

Satyajit Yadav and Selvakumar Subramanian[10] proposed a strategy based on pattern learning is proposed to identify AL-DDoS assaults. To create an AL-DDoS attack dataset, the features from the web server log (Attack and Normal) are extracted. The retrieved features are pre-processed in order to convert them all to numbers. The feature learning module is then fed the preprocessed features as input. In the feature learning process, deeper learning techniques like Stacked AutoEncoder are used to learn more abstract features, and a deep architecture is built.
Mr.Jay Gholap[11] have attempted to implement the data mining development process, particularly with regard to agricultural soil datasets they worked on in parallel research areas by achieving and maintaining appropriate levels of soil productivity, is of ultimate use for enhancing crop production in agricultural land. This essay seeks to study the time of land production using a decision-tree process. Additionally, it focuses on changing the behaviour of the DT algorithm (Decision Tree) for J48 utilising various techniques including boosting and aspect selection. That research discussed how J48 provides 92% accuracy, making it suitable for use by home learners.

P. S. Samom and A. Taggu[12] SYN, NET, Portmap, and UDPLag are 4 different forms of DDoS attacks that may be detected using an MLP model, and the model's performance is compared against other machine learning techniques. The Chi-Squared Function is used in their work as a feature extractor to choose 20 features, and the PCA approach is used for dimension reduction. For the CICDDoS2019 dataset, their submission demonstrated that their model had a 99.92% accuracy rate. Despite the fact that some of these existing works seem to offer good performance close to 99%, they frequently just offer binary classification, i.e., they simply identify

whether network traffic contains a DDoS attack or not, but they don't offer to categorise what type of DDoS attack it is.

Yuanyuan Wei, Julian Jang-Jaccard, Fariza Sabrina[13] in their proposed model, the Multi-layer Perceptron Network (MLP) component classifies the attacks into several DDoS attack categories using the compressed and reduced feature sets generated by the AE as inputs. Processing big feature sets with noise (i.e., extraneous feature values) results in bias and performance overhead. Our experimental results show a very high and robust accuracy rate and an F1-score that exceeds 98%, which also beat the performance of many similar approaches. These results were acquired by thorough and extensive trials on various performance aspects on the CICDDoS2019 dataset. This demonstrates that our suggested model can be used to defend against the increasing amount of DDoS attacks.

IV. CONCLUSION

In this paper, we reviewed different techniques for preventing the DDOS attacks by different algorithm which was proposed from different authors. Like as a brand-new, complete DDoS attack defensive architecture, together with its specifications for various stages and roles. In essence, all of the aforementioned needs must be created and implemented in the current information technology environment. In the absence of this, DDoS attacks will continue to be the biggest risks to the information technology ecosystem. Also, attackers disguise their identities by using the spoofed packets. The hacked machines are permanently concealed thanks to this feature. Moreover, the TCP protocol is weak, which enables attackers to mimic normal communication patterns in order to carry out a successful DDoS attack. We offer the defence requirements for each stage of the attack process, such as the production stage of the attack agent, the dissemination stage of the attack agent, the attack stage, and the after-attack stage. For each assault defence position, we have also suggested the defence requirements at the host, edge, and backbone network levels.

REFERENCES

[1]. N. Hoque and M. H. Bhuyan and R. C. Baishya and D. K. Bhattacharyya and J. K. Kalia, Network attacks: Taxonomy, tools and systems, Journal of Network and Computer Applications, vol 40, pp:307–324, Elsevier, 2014.

[2]. Kreutz, D., Ramos, F.M.V., Verssimo, P.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S.: Software-Defined Networking: A Comprehensive Survey. Proceedings of the IEEE 103(1), 14–76 (2015).

[3]. Usman Tariq, ManPyo Hong, and Kyung-suk Lhee, "A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques", Springer-Verlag Berlin Heidelberg 2006, ADMA 2006, LNAI 4093, pp. 1025 – 1036, 2006.

[4]. HCJ Lee, VLL Thing, Y Xu, M Ma: ICMP Traceback with Cumulative Path, an Efficient Solution for IP Traceback: in Proceedings of the international conference on Information and Communication Security, Oct. 2003.

[5]. J. Mirkovic, J. Martin, P. Reiher, A taxonomy of DDoS attacks and DDoS defense mechanisms, UCLA CSD Technical Report no. 020018.

[6]. Rohan Doshi, Noah Apthorpe and Nick Feamster,' Machine Learning DDoS Detection for Consumer Internet of Things Device", IEEE Symposium on Security and Privacy Workshops,2018.

[7]. Q. Liao, H. Li, S. Kang, and C. Liu, "Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching," Security and Communication Networks, vol. 8, no. 17, pp. 3111–3120, 2015.

[8]. L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical Approaches to DDoS Attack Detection and Response," in Proceedings DARPA Information Survivability Conference and Exposition, 2003.

[9]. M. Ghanbari and W. Kinsner, "Extracting Features from Both the Input and the Output of a Convolutional Neural Network to Detect Distributed Denial of Service Attacks," in Proc. of ICCI*CC, 2018.

[10]. Satyajit Yadav and Selvakumar Subramanian, "Detection of Application Layer DDoS Attack by Feature Learning Using Stacked Autoencoder", International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016.

[11]. Mr.Jay Gholap "Performance of j48 algorithm for prediction of soil fertility" Dept. of Computer Engineering, College of Engineering, Pune, Maharashtra, Indi, 2012.

[12]. P. S. Samom and A. Taggu, ''Distributed denial of service (DDoS) attacks detection: A machine learning approach,'' in Applied Soft Computing and Communication Networks. Singapore: Springer, 2021, pp. 75–87.

[13]. Yuanyuan Wei, Julian Jang-Jaccard, Fariza Sabrina, "AE-MLP: A hybrid deep learning approach for DDOS detection and classification" in IEEE access 2021, vol. 9, pp. 146810-146821.