A SURVEY ON DDoS ATTACK DETECTION USING VARIOUS APPROACHES

Rupali Jain[1], Chinmay Bhatt[2]
CSE, SRK University, Bhopal, India[1, 2]

Abstract: **In the realm of internet technology, denial of service attacks (also known as DoS attacks) represent a significant risk and one of the most challenging types of security concerns. Because of the potential severity of these attacks, particularly DDoS attacks, there is cause for concern. An attack using a distributed denial of service can quickly and with little or no advanced warning drain the victim's computational and communication resources in a short amount of time. As a result of the gravity of the situation, a number of different countermeasures have been developed.**

Keywords: **Cyber Security, Dos Attack,**

I. INTRODUCTION

The DDoS assaults are a serious issue on the Internet. The effect of DDoS attacks has been thoroughly documented in the computer network. Literature. Disruption is the primary goal of the DOS. Security services by restricting a computer or a network in instead of attacking the service itself. This kind of thing an attack that seeks to make a network unusable normal service may be provided by focusing on either the network's the ability to transmit data at high speeds. These assaults are successful. Achieve their by the transmission of packets to a victim that the network or processing resources he has available are over taxed DDoS (Distributed Denial of Service) is a relatively new kind of attack. Attacking Intermit with simple is yet effective strategy resources. The many-to-one dimension is added by DDoS assaults.to the solution of the DOS issue D-DoS attacks often happen in stages, starting with hackers surveying or scanning for defencelessness or access points, First gaining access to a system and then carrying out the assault in its entirety, whether the goal is to steal important data or to disable the computer systems. Automated instruction (ML), as well as deep learning (DL), has both been found to be completely effective in detecting DDoS attacks. Algorithms are, however, taught to detect only examples selected from the training set's distribution models [8]. As a result, individuals may perform in situations where they have never learned. The Open Set Recognition (OSR) challenge is about figuring out what one doesn't know. Because DDoS intrusion technologies develop, resulting in shifting traffic parameters, this issue has a significant influence on DDoS attack detection [9]. Malicious node attacks could not only prevent access to network resources but also result in major risks and harm. A Denial of Service (DoS) attack, for example, prevents genuine end-users from using network resources by overflowing the target system by propagating widely and finally paralyzing it [10]. TCP/SYN Flood, Ping Flood, UDP Flood, and Distributed Denial of Service are all examples of DoS assaults (DDoS A distributed denial of service (DDoS) assault occurs when a number of compromised malicious activities attack a single target. [25].

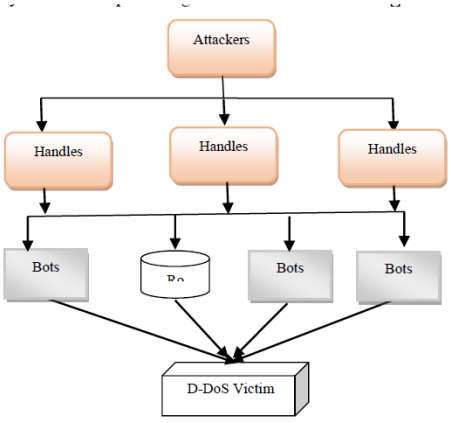

Fig. 1 Shows the D-DoS attacks using Bot Block diagram

In the above section I discuss the introduction part of proposed research work, discuss the cyber-attack and D-DoS attacks. In the section II discuss DoS attack and its types. Next section III discusses the previous works these were presented by different researchers. Finally, describe the DDoS assault detection mechanism that was presented. Section V discusses the simulation and result of the proposed method. Last but not least discuss the conclusion in section VI

II. LITERATURE SURVEY

Afsaneh Banitalebi Dehkordi, et.al. (2021), In this research work According to the researchers, SDNs are the recent in network improvements because they are flexible, reduce operational costs, as well as provide protection against DDoS attacks. DDoS attacks of high and low volume can be detected using suggested here is a blend of statistics and machine learning. An entropy-based as well as classification-based collection method is used. Experimental tests on various datasets show that the entropy-based sections with static threshold do not produce accurate findings when using the developed model that has been evaluated and analyzed. Good outcomes for dynamic threshold come at the expense of a large false positive rate (FPR). To address this issue, a variety of classification techniques are run and so more accurate results are generated [1].

Jia_et.al,(2020), In this research work investigator Flow Guard, a book IoT DDoS defence strategy, as well as two novel machine learning models for DDoS identification and classification were presented. There are 2 parts to flow guard, the filter as well as the controller, which are explained. Following the filtration rules established by the Flow Controller, the Flow Filter identifies and removes potentially harmful flows. Flow Controller uses LSTM as well as CNN machine learning techniques to identify and classify malicious flows. The CICDDoS2019 dataset as well as a calculated dataset were extensively studied by the researchers of these two approaches [5].

Agrawal Neha_et.al, (2019), in this research work a cloud computing security discussion was presented by the researchers. This on-demand capability cannot function without having ready access to cloud computing facilities and benefits. Many of these services might be rendered unavailable by DDoS assaults. After that, the report discusses how DDoS attacks are carried out by exploiting the cloud computing's important characteristics. They take into account both high-rate and low-rate DDoS attacks in a cloud computing environment in their research study. DDoS assaults and their defenses have been reclassified according to a novel taxonomy. There are a variety of strategies that may be used to identify, prevent, and reduce DDoS assaults.

Various DDoS attack release methods and their impact on cloud infrastructure are discussed by the researchers. The protection techniques and their cloud-based behavior are also contrasted. There is also a discussion of the most important metrics for evaluating the performance of any defense mechanism. According to our understanding, previous surveys do not adequately examine low-rate DDoS assaults as well as associated response methods. The novelty of a new classification of DDoS attacks as well as countermeasures is offered. There are many different forms of DDoS assaults, and how to prevent, identify, and react to them is all covered in this article. It's important to understand how DDoS attacks are launched and how that affects the cloud services. There's also a cloud-based comparison of the various defense strategies [10].

Wang_et.al, (2018), in this research work researchers made their case to the audience. DDoS assaults are commonplace in today's online world. Large-scale Internet DDoS assaults have seldom been quantified and examined in prior research, despite the importance of understanding the forms of DDoS attacks. In this research, researchers were able to describe today's Internet DDoS attacks from a variety of angles because we had access to a large dataset. These DDoS attacks reveal a number of interesting research results about today's botnet-based DDoS attacks after a thorough examination of the attacks. As a result of these findings, we now know more about present DDoS attacks and how to properly protect ourselves against them (e.g., organization and country). Even though the focus of this study is on DDoS categorization, researchers intend to use the outcomes to develop more effective defense strategies in the future [11].

Dayal, _ et. al (2017, January), in this research work, Researchers presented an attack model to identify and classify various DDoS attack scenarios in SDN. The hyenae attack tool was used to carry out a variety of DDoS attacks in an SDN environment utilizing a few of the most popular

conventional DDoS attack methods. Despite the fact that volumetric attacks have a significant effect on the research plane, they do not have a significant impact on the controller. During the attack phase, the effect is clearly visible. Protocol exploitation threats, on the other hand, have little impact on network traffic. They focus on consuming other device resources, such as the TCAM, logical port, etc. Immediately after the attack, and immediately after the attack, controllers might be seriously impacted. TCP SYN flood as well as HTTP flood attacks can in reality bring down the control system [16].

Chang-Jung, et.al. (IEEE 2016), In this research work Many sorts of network assaults are being targeted by DDoS attacks, according to Akamai statistics, which show that the attacks are getting more widespread and more hazardous. The number of strikes rose by more than double in the first quarter of 2015 compared to the same period in 2014. Detecting DDoS assaults that employ low traffic volumes for a long period of time gets increasingly challenging as the attack types improve. In the past, attackers have used brief bursts of excessive traffic to make target servers unavailable. In the first quarter of 2015, there were eight DDoS assaults of over 100 Gbps, making it difficult to notice the attacks, which have a significant amount of traffic and are very changeable, making it difficult to detect the attacks. We used neural network models to train and test our DDoS detection algorithm using the 2000 DARPA LLDOS 1.0 dataset, and the findings reveal that our detection method can identify assaults in real time with an average recognition rate of over 94%. [17]

Wang, R., et.al (2. (2015, August).In this research work, extended the OpenFlow table has a counter copy of the flflow entry. For the flflow statistics process in the switch, researchers used this value to define input flflow quickly. As part of our effort to keep tabs on the incoming traffic, researchers developed an entropy-based DDoS flood detection method as well as design. The transmitted anomaly detection mechanism was achieved by running this algorithm in the edge device of SDN. It is easy to implement this technique in SDN application or on a reconfigurable switch because the calculation of entropy value has a minimal overflow. It is possible to reduce the frequency with which information is collected as well as alleviate the communication overload between the OF switches as well as the regulator by using our system. When a DDoS attack makes use of wildcard flflow rules, our detection system can still work effectively thanks to the flflow aggregation process. It was found that our methodology can detect the attack in the early monitoring intervals when the attack begins and achieve high detection accuracy with low false positive rate [21].

Table 2.1 Comparison of Different Previous Methods

S. No.	Ref./Year	Methods	Attack	Remark
1.	[1]/ 2021	Artificial Neural Network	Distributed denial of-service (DDoS)	To identify the low-volume DDoS and high-volume DDoS attacks in their separate sense.
2.	[5]/2020	Feature selection and feedback Algorithm	Distributed denial-of-service (DDoS)	to classify the flows into benign ones or one of the four types of DDoS attacks.
3.	[10]/2020	Intrusion Detection System (IDS)	Distributed Denial of Service (DDoS)	IDS filter the attack packets, and subsequently mitigates the effect of the attack.
4.	[11]/2019	Domain Generation Algorithms (DGAs)	Internet distributed denial of service (DDoS) attacks	Malware families and variants use DGAs
5.	[16]/2018	RBF-PSO Based method	DDoS attacks	To identify and classify various possibilities of DDoS attacks
6.	[17]/2018	Machine Learning Algorithms	Detection DDoS attacks	To identify and detect abnormal traffic
7.	[21]/2016	Stacked Auto Encoder Based Method	Distributed DDoS Detection	To detect AL-DDoS attacks

			Mechanism	

III. DDOS ATTACK CLASSIFICATION

DDoS assaults may be divided into two categories: bandwidth depletion attacks and resource depletion attacks (Figure 3). An order to overwhelm the target, a bandwidth depletion attack is used. Traffic on a network that impedes the flow of lawful traffic the victim's system from receiving any unwanted traffic Bandwidth Flood attacks and amplification assaults are two types of attacks. Depleting a person or organization's resources to stifle a victim system's ability to respond. This Protocol exploit attacks are a subcategory of kind of attack. In addition to erroneous packet assaults

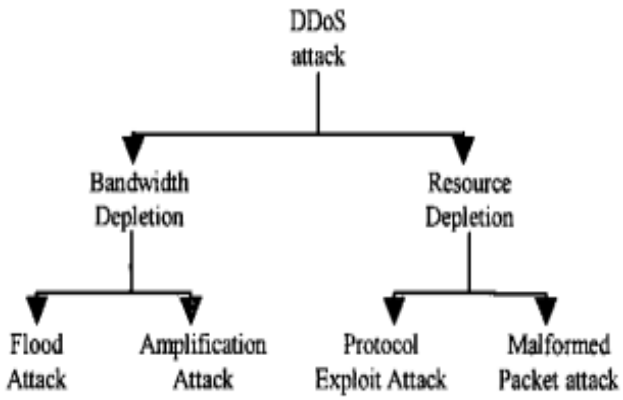

Fig. 1 Classification of DDoS attacks

Direct assaults and reflection attacks are the two main types of DDoS attacks. In the last part, we discussed direct assaults. A reflector is a kind of indirect attack that takes advantage of intermediate nodes to launch attacks. Any IP host that will return a packet if one is sent to it is a reflector.We've broken down DDoS defenses into two categories based on two separate sets of standards. There are two ways to classify the DDoS defensive mechanisms: one based on the kind of activity deployed and one based on the place where they are deployed. In the first classification, we go into great depth about the DDoS defenses, whereas in the second classification, we just mention the DDoS defenses and how they are classed.

Distributed Denial of Service (DDoS) attacks have been a real threat in many aspects of computer networks and distributed applications. The main objective of a DDoS attack is to bring down the services of a target using multiple sources that are distributed. For example, attackers can transfer thousands of packets to a victim to overwhelm its access bandwidth with illegitimate traffic, making online services unavailable. There are numerous denials of service (DoS) attack methods being used to degrade the performance or availability of targeted services on the Internet.5 Usually, these methods can be classified as challenges associated with the SDN at each layer of the framework, application, control, and infrastructure.

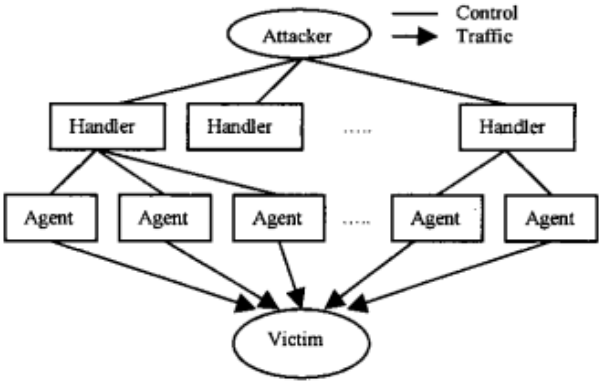

Fig. 2 Architecture of DDoS attacks

1. Application layer DDoS attacks Application layer attacks use the software in a malicious way, aiming to exhaust resources to process any further requests. These attacks are generally harder to detect on the network level as they show no clear deviation from legitimate traffic.5 since the isolation of applications or resources in SDN is not well solved, DDoS attacks on one application can also affect other applications. A common example is the HTTP flooding attacks.21

2. Control layer DDoS attacks Controllers of SDN and their communications can be subjected to different types of attacks.2 among the threats that can cause significant damages are the following: attacks on the control plane and communication between the controller and other networks components, eg, northbound API, southbound API, westbound API, or eastbound API. In addition, the

controller can be considered a single point of failure and scalability that raises potential performance problems and unavailability of the control plane.

3. Infrastructure layer DDoS attacks Infrastructure layer DDoS attacks could potentially overload through two points: switches or by attacking the southbound API.22 For example, huge traffic may be sent by an attacker to execute a DoS attack on the node by setting up a number of new and unknown flows infrastructure layer

IV. DDOS ATTACK DETECTION TECHNIQUES

DDoS attacks have been studied for a long time and the types of threats to them are mostly known.5 However, SDN is a new architecture and the studies are at an early stage. In addition, SDN networks have distinct detection methods for different types of DDoS attacks.23 These methods include entropy-based,7,24-26 machine learning–based,10-13 traffic pattern analysis,27 connection rate,27,28 and techniques that combine the use of the IDS and OpenFlow.29-31

1. Entropy The ability to measure randomness in packets arriving on a network makes entropy-based methods good candidates for the DDoS detection. The greater the randomness, the greater the entropy, and vice versa. Entropy-based methods depend on network feature distributions to detect anomalous network activities.24 the presence of anomalies in an SDN network can be identified by adopting the use of predefined thresholds. In addition, probability distributions of various network features such as source IP address, destination IP address, and port numbers are used to calculate the entropy.32

2. Machine learning Machine learning–based methods employ techniques to detect anomalies in a network environment, these can be based on models, based on statistic and math, based on unsupervised machine learning algorithms, and based on supervised machine learning algorithms.33 These algorithms take into account various network features and traffic characteristics to detect the presence of anomalies. In fact, any system that is built to detect any anomalies in the network catch the traffic on it and extract some kind of information from them, and the approach that uses machine learning is trying to catch the pattern of normal and abnormal traffic on the network, without the need to know the pattern itself

3. Traffic pattern analysis these techniques work on the assumptions that the infected hosts exhibit similar behavioral patterns that are different from benign hosts.34 Therefore, it analyzes the traffic relating to the metrics of the attack pattern networks in order to identify the attacker or the target under attack. Patterns are observed as a result of a command that is sent to many members of the same botnet causing a similar behavior (eg, sending illegitimate packets, starting to scan).

4. Connection rate Bawany et al32 define connection rate techniques as ‘‘the probability of a connection attempt being successful should be much higher for a benign host than a malicious host.’’ Whenever the likelihood ratio for a host to exceed a certain threshold, it is declared as infected. These techniques are classified into two types: connection success ratio and connection rate, which refers to the number of connections instantiated within a certain window of time.

V. CONCLUSION

A Bayesian regularization with cascaded feed forward network-based machine learning strategy for D-DoS attack detection was presented as part of this body of research work by the researchers that conducted it. This method was used to detect DDOS attacks. The results obtained using the presented method is superior than those obtained using CNN or LSTM-based deep learning algorithms. The comparison of the method that is being provided with ways that have been used in the past is shown in Table II. The presented strategy produces better results in the CISIDS2017 data set when accuracy is taken into consideration. The method that is shown shows a 99.96% accuracy. As a result of a distributed denial of service (DDoS) assault, a targeted system is unable to offer its legitimate users with the consistent services they have come to expect from it. In this work, a

modified feature selected-based neural network for effective DDoS attack detection is described.

Reference:

[1] Afsaneh Banitalebi, MohammadReza Soltanaghaei, and Farsad Zamani Boroujeni. "The DDoS attacks detection through machine learning and statistical methods in SDN." The Journal of Supercomputing 77.3 (2021): 2383-2415.

[2] Liu, Xinqian, et al. "Low-rate DDoS attacks detection method using data compression and behavior divergence measurement." Computers & Security 100 (2021): 102107.

[3] Kushwah, Gopal Singh, and Virender Ranga. "Optimized extreme learning machine for detecting DDoS attacks in cloud computing." Computers & Security 105 (2021): 102260.

[4] Snehi, Manish, and Abhinav Bhandari. "Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks." Computer Science Review 40 (2021): 100371.

[5] Jia, Yizhen, et al. "Flowguard: An intelligent edge defense mechanism against IoT DDoS attacks." IEEE Internet of Things Journal 7.10 (2020): 9552-9562.

[6] Singh, Jagdeep, and Sunny Behal. "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions." Computer Science Review 37 (2020): 100279.

[7] Virupakshar, Karan B., et al. "Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud." Procedia Computer Science 167 (2020): 2297-2307.

[8] Singh, Maninder Pal, and Abhinav Bhandari. "New-flow based DDoS attacks in SDN: Taxonomy, rationales, and research challenges." Computer Communications 154 (2020): 509-527.

[9] Dong, Shi, Khushnood Abbas, and Raj Jain. "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments." IEEE Access 7 (2019): 80813-80828.

[10] Agrawal, Neha, and Shashikala Tapaswi. "Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges." IEEE Communications Surveys & Tutorials 21.4 (2019): 3769-3795.

[11] Wang, An, et al. "Delving into internet DDoS attacks by botnets: characterization and analysis." IEEE/ACM Transactions on Networking 26.6 (2018): 2843-2855.

[12] Yang, Kun, Junjie Zhang, Yang Xu, and Jonathan Chao. "Ddos attacks detection with autoencoder." In NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, pp. 1-9. IEEE, 2020.

[13] Singh, Jagdeep, and Sunny Behal. "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions." Computer Science Review 37 (2020): 100279.

[14] Wani, Abdul Raoof, Q. P. Rana, U. Saxena, and Nitin Pandey. "Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques." In 2019 Amity International conference on artificial intelligence (AICAI), pp. 870-875. IEEE, 2019.

[15] Li, Qian, Linhai Meng, Yuan Zhang, and Jinyao Yan. "DDoS attacks detection using machine learning algorithms." In International Forum on Digital TV and Wireless Multimedia Communications, pp. 205-216. Springer, Singapore, 2018.

[16] Dayal, Neelam, and Shashank Srivastava. "Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN." In 2017 9th International Conference on Communication Systems and Networks (COMSNETS), pp. 274-281. IEEE, 2017.

[17] Hsieh, Chang-Jung, and Ting-Yuan Chan. "Detection DDoS attacks based on neural-network using Apache Spark." In 2016 international conference on applied system innovation (ICASI), pp. 1-4. IEEE, 2016.

[18] Buragohain, Chaitanya, and Nabajyoti Medhi. "FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers." In 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), pp. 519-524. IEEE, 2016.

[19] Xiao, Peng, Zhiyang Li, Heng Qi, Wenyu Qu, and Haisheng Yu. "An efficient ddos detection with bloom filter in sdn." In 2016 IEEE Trustcom/BigDataSE/ISPA, pp. 1-6. IEEE, 2016.

[20] Yadav, Satyajit, and Selvakumar Subramanian. "Detection of Application Layer DDoS attack by feature learning using Stacked AutoEncoder." In 2016 international conference on computational techniques in information and communication technologies (icctict), pp. 361-366. IEEE, 2016.

[21] Wang, Rui, Zhiping Jia, and Lei Ju. "An entropy-based distributed DDoS detection mechanism in software-defined networking." In 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1, pp. 310-317. IEEE, 2015.

[22] Zhao, Teng, Dan Chia-Tien Lo, and Kai Qian. "A neural-network based DDoS detection system using hadoop and HBase." In 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, pp. 1326-1331. IEEE, 2015.

[23] Yadav, Satyajit, and S. Selvakumar. "Detection of application layer DDoS attack by modeling user behavior using logistic regression." In 2015 4th International Conference on Reliability, Infocom

Technologies and Optimization (ICRITO)(Trends and Future Directions), pp. 1-6. IEEE, 2015.

[24] Balkanli, Eray, A. Nur Zincir-Heywood, and Malcolm I. Heywood. "Feature selection for robust backscatter DDoS detection." In 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), pp. 611-618. IEEE, 2015.

[25] Badve, Omkar P., Brij B. Gupta, Shingo Yamaguchi, and Zhaolong Gou. "DDoS detection and filtering technique in cloud environment using GARCH model." In 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), pp. 584-586. IEEE, 2015.

[26] Kokila, R. T., S. Thamarai Selvi, and Kannan Govindarajan. "DDoS detection and analysis in SDN-based environment using support vector machine classifier." In 2014 Sixth International Conference on Advanced Computing (ICoAC), pp. 205-210. IEEE, 2014.

[27] Kokila, R. T., S. Thamarai Selvi, and Kannan Govindarajan. "DDoS detection and analysis in SDN-based environment using support vector machine classifier." In 2014 Sixth International Conference on Advanced Computing (ICoAC), pp. 205-210. IEEE, 2014.

[28] Choi, Junho, Chang Choi, Byeongkyu Ko, and Pankoo Kim. "A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment." Soft Computing 18, no. 9 (2014): 1697-1703.

[29] Barati, Mehdi, Azizol Abdullah, Nur Izura Udzir, Ramlan Mahmod, and Norwati Mustapha. "Distributed Denial of Service detection using hybrid machine learning technique." In 2014 International Symposium on Biometrics and Security Technologies (ISBAST), pp. 268-273. IEEE, 2014.

[30] Kumar, Naresh, and Shalini Sharma. "Study of intrusion detection system for DDoS attacks in cloud computing." In 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp. 1-5. IEEE, 2013.

[31] https://www.researchgate.net/

[32] http://ieee-dataport.org/documents/iot-dos-and-ddos-attack-dataset

[33] https://staff.itee.uq.edu.au/marius/NIDS_datasets/