http://www.jctjournals.com

ISSN(ONLINE):2278 - 3814

Volume-11, Issue-6, June, 2022

JOURNAL OF COMPUTING TECHNOLOGIES (JCT)

International Journal

Page Number: 01-06

A Literature Review on D-DOS Attack Detection Using Various Approach

[1]Charulika Yadav (M.Tech Scholar),[2]Prof. Sumit Sharma
[1]M.Tech Scholar, [2]Head of department,
[1,2]Department of Computer Science and Engineering (CSE)
[1,2]Vaishnavi Institute of Technology and Science (VITS), Bhopal(M.P), INDIA
[1]charulikay@gmail.com,

***Abstract*—A distributed denial of service (DDoS) attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server. In this survey paper discuss the different previous work presented in the D-DoS attack detection. A DDoS assault may swiftly deplete the victim's computational and communication capabilities in a short period of time with little or no prior notice. Due to the seriousness of the problem, a variety of defence have been devised.**

Keywords- Distributed Denial of Service (DDoS), Cyber-attack, Confusion Matrix, feedforward neural network (FNN), Levenberg-Marquardt and Botnets.

I. Introduction

A distributed denial of service (DDoS) attack is a malicious attempt to make an online service unavailable to users, usually by temporarily interrupting or suspending the services of its hosting server.A DDoS attack is launched from numerous compromised devices, often distributed globally in what is referred to as a botnet. It is distinct from other denial of service (DoS) attacks, in that it uses a single Internet-connected device (one network connection) to flood a target with malicious traffic

DDoS attacks 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 thingan 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 overtaxed. DDoS (Distributed Denial of Service) is a relatively new kind of attack.attacking Intent with a simple 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 defenselessness 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), have 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].

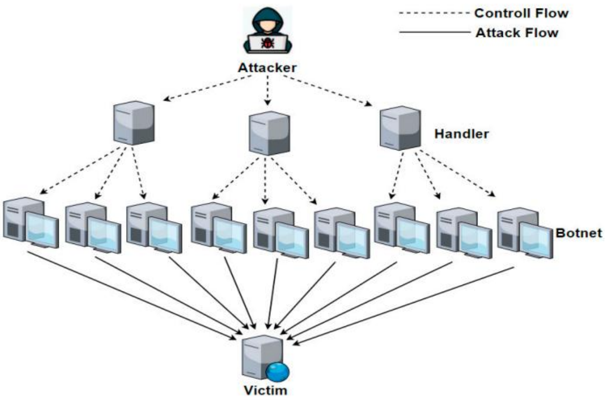

Fig. 1 Shows the D-DoS attacks using Bot Block diagram

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 literature survey. Next section III discusses the classification DDOS attacks. Section IV discusses the DDOS attacks detection techniques. Last but not least discuss the conclusion in section V.

II. LITERATURE SURVEY

Snehi_et.al,(2021), In this research work authors presented analysed the most devastating DDoS and IoT-DDoS attacks, as well as the elements of today's Cyber-Physical Device, architectural features, as well as security problems. A layer between perception as well as the cloud, Fog Computing has been suggested as a method of improving performance and performing the assigned duties on behalf of Cloud. DDoS/IoT-DDoS detection and reduction have been analysed. Next but not least, uncertainty, as well as gap evaluation, was carried, as well as the narrow down method was used to identify general gaps or vulnerabilities in the possible solutions. Using that research study, they've attempted to summarise the vulnerability analysis that can serve as a foundation for future DDoS/IoTDDoS defense solutions for future technologists and researchers. DDoS attacks are just one of several cybersecurity risks that vulnerability research examines. Provided a wide range of options [01].

Jia_et.al,(2020), In this research work investigator Virupakshar_et.al, (2020), In this research work.The researchers reviewed 70 publications from high-profile journals. Some 47% of researchers utilised data theory approaches, 42percent utilised machine learning strategies, and 20% used Artificial Neural Networks to detect DDoS attacks in SDN. Additionally, they've provided details on various security mechanisms so that other researchers can better understand the current situation. For SDN-enabled systems, operators remain a primary target for attackers [02].

Dong_et.al,(2019), In this research work DDoS attacks are becoming more prevalent in Analysts who say SDN and cloud computing environments pose the greatest risk. DDoS attacks and their detection in SDN and cloud computing are discussed at this moment by researchers. Because SDN could be a target of a DDoS attack, they look into how DDoS attacks are introduced on SDN as well as possible solutions. For DDoS attacks, researchers also discuss how to create exploratory conditions and then use simulation tools in SDN and cloud computing environments. Many unsolved issues in this area are examined, such as how to mitigate DDoS attacks in an SDN and cloud computing setting. Despite the never-ending research in this area, some issues remain unresolved. Future research should focus on this issue. They suggest the following lines of investigation for future work: Attacks against the SDN Even though SDN's unified regulation is its most attractive feature, it can also be a single point of failure when subjected to a Distributed Denial of Service (DDoS) attack. Traditional anomaly detection methods are having a hard time dealing with the growing number of DDoS attacks. As a result, SDN research is focusing on big data analysis and location advancements for DDoS attacks. SDN and NFV are mutually beneficial, but they are not dependent on each other. It is SDN's role to empower NFV. Because the logic for virtualization technology runs on a controller rather than on physical circuits, SDN helps to automate the network by allowing users to make approach-based decisions about how to coordinate system traffic flows [03].

Li_ et.al, (2018, September), This research work, presented, DDoS attack detection system based on PCA feature reduction as well as RNN prediction. Utilizing the KDD dataset, researchers compared our PCA-RNN detection method with several other methods for detecting DDoS attacks. Our PCA-RNN technique's experimental results show that it has improved detection accuracy, performance, as well as applicability[09].

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 utilising 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[10].

Buragohain, Chaitanya, et.al. (IEEE 2016), In this research work, presented and tested the proposed architecture of Flow Trapp. An SDN-based structure is provided for the detection and mitigation of both high- and low-rate DDoS attacks in data centers by this system. Incoming attack traffic can be classified using the optimization technique, which compares it to an application-specific tuple of genuine flow traffic. Remediation is used when a malicious user is discovered to transfer attack traffic regularly, rather than blocking the location at the outset. Architecture is implemented using SDN innovations such as OpenFlow and flow statistics collectors such as Flow To enhance the effectiveness of FlowTrApp, the OpenFlow controller, as well as the sFlow-RT application, can share the burden of detecting and mitigating DDoS attacks. Our method outperforms an existing QoS-based method in terms of performance[12].

Zhao, T., Lo, et.al (2015, August).In this research work, Hadoop, as well as HBase, were used to design an effective DDoS detection method that can identify threats quickly. The first step was to create a Hadoop as well as HBase cluster to process a massive unorganised set of data. Once the neural network model for DDoS detection was created as well as six training data were used to train the neural network model, it was able to identify DDoS attacks. Three parts are used to demonstrate how well-suited the skilled neural network is for the task[16].

Table 1 Comparison of Different Previous Methods

S.No.	Ref./Year	Methods	Attack	Remark
1.	[1]/ 2021	Software-Defined Cyber- Physical System (SD- CPS)	DDoS and IoT-DDoS attacks	have given the wings to Cyber- Physical System adoption
2.	[2]/2020	CNN Algorithm	Distributed denial-of-service (DDoS)	to classify the flows into benign ones or one of the four types of DDoS attacks.
3.	[03]/2019	Software-Defined Networks (SDN)	Denial of Service (DoS)	SDN decouples the network control plane from the data plane.
4.	[09]/2018	Machine Learning Algorithms	DDoS attacks	Can find out the abnormal information behind the massive data
5.	[10]/2017	Software-Defined Network(SDN)	DDoS attacks	To identify and classify various possibilities of DDoS attacks
6.	[12]/2016	Artificial Neural Network	Detection DDoS attacks	To identify and detect abnormal traffic
7.	[16]/2015	Hadoop And HBase	Denial of Service (DDoS) attack	To process huge unstructured dataset

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. 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

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.

DDoS attacks can be classified further as the primary target is to congest the network with a massive amount of the bandwidth. Utilization and it could cause the network abruption to the victim network.

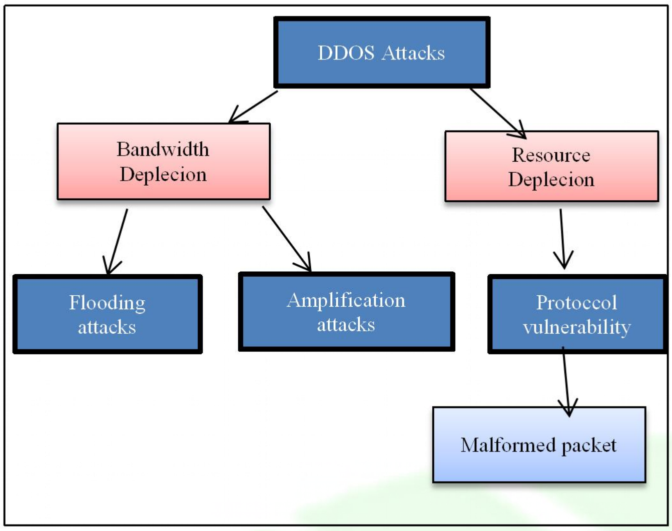

Fig. 2 Classification of DDoS attacks

DDoS attacks can be classified further as the primary target is to congest the network with a massive amount of the bandwidth Utilization and could cause the network abrupt-ion to the victim network. The secondary focus is on Network resource depletion. This means the Attacker depletes the key components such as Memory, Device CPU, and so on. The attacker's intention behind this is to consume the available resources to the point where the service can't be responded to.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. Usually, these methods can be classified as challenges associated with the SDN at each layer of the framework, application, control, and infrastructure.

1. **Volume Based Attacks**

Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack's goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).

2. **Protocol Attacks**

Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (Pps).

3. **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

4. **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.

5. **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

In this research work researcher presented different method used on DDOS attack detection a Bayesian regularization with cascaded feed forward network-based machine leaning approach for D-DoS attack detection. The presented method shows better result as compare to CNN with LSTM based deep learning methods. Table II shows the comparison between presented method and previous methods.

Reference

[1] 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.

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

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.