DDoS attack: A Review on Network Security

Chaudhari Nivrutti Janardhan[1], Dr.Shailesh Kumar[2], Dr. Mangesh D. Salunke[3]
[1] *Department of Computer Engineering, Research Scholar, Shri JJT University, Rajasthan*
[2] *Department of Computer Engineering, Associate Professor, Shri JJT University, Rajasthan*
[3] *Department of Computer Engineering, Asst. Professor, JSPM NTC, Pune*

***Abstract*— A DDoS (Distributed Denial of Service) attack as name indicates is simply an attempt by an attacker to exhaust the resources available to a network, application or service so that authorize users cannot gain access in distributed manner. The Denial of Service (DOS) attacks are one of the most widely spread problems faced by most of the Internet Service Providers (ISP's) today. Denial-of-Service (DoS) attacks cause serious impact on the computer network systems and DDoS is kind of DoS attack which attacker spread with distributed form with the help of malicious Botnet computers or system. DDoS attacks carry six figure price tag for businesses, costs large businesses an average of $444,000 in lost revenue. Overall, nearly 1 in 5 businesses experienced a DoS attack during the year-long study period, so it is necessary to counter DDoS attack.**

Index Terms: **Computer and Network security, DoS, DDoS attack, Cyber-attack.**

1.INTRODUCTION

Smurf DDoS that is Smurf Distributed Denial of Service attack is type of network attack that is used by attacker to digitally render victims in order to access the data, files on network or server itself. Smurf DDoS are real treat to network that attacker can inject to user's system and uses packet flooding mechanism or approach like Ping Flood, IP Flood, TCP flood, UDP Flood for making network or server or any system inaccessible to the authenticate user. [2]. Smurf DDoS attacker changes their targets from individuals to organizations such as banking, government offices, and hospitals and may more. [3] Attacker uses different ways to penetrate the user system with Smurf DDoS attack that is known as deployment location of attack like spam mails, compromised web sites, Downloading/Opening any malicious file, Log-into any already infected PC, Installing Pirated software are some Examples. A Smurf DDoS attack relies on mis-configured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine[4].SmurfDDoS is network layer distributed denial of service (DDoS) attack, named after the DDoS. Smurf malware that enable its execution. Smurf attacks are somewhat similar to ping floods, as both are carried out by sending a slews of ICMP Echo request packets [4].

1.1 Phases of Attack:

As every network attack follows some steps or phases of execution so as the Smurf DDoS attack also have some phases of execution for successfully produce attack on victim's machine, Smurf DDoS attack phases describe the detail working of attack.

The following steps lead to a Smurf DDoS attack:

1: Huge numbers of ICMP requests are sent to the victim's IP address

2: The source destination IP address is spoofed

3: The hosts on the victims network respond to the ICMP requests

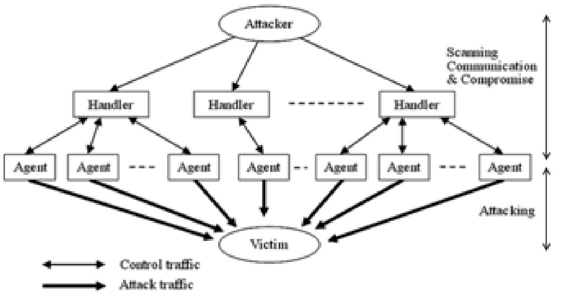

Fig 1 : DDoS attack scenario [3]

This creates a significant amount of traffic on the victim's network, resulting in consumption of bandwidth and ultimately causing the victim's server to crash. [5]

Most of the serious attacks in cloud computing comes from distributed denial of service (DDoS), Due to vulnerabilities in the system interface, DDoS attacks are easier to implement and very difficult for security experts to countermeasure. DDoS attacks carry six figure price tag for businesses, costs large businesses an average of $444,000 in lost revenue. Overall, nearly 1 in 5 businesses experienced a DoS attack during the year-long study period. DDoS attack becomes on of the most threatening attack to security of computer networks. Also the use of Internet today is increasing, the study shows that DDoS attack has highest ranking among other attacks, so there is need to counter such type of attack [4]

2. TYPES OF DDOS ATTACK

DDoS assaults are likewise productive while being reasonable, driving more individuals to exploit this sort of assault. The obstruction to section of DDoS assaults as far as cost has to a great extent gone. That implies anybody can dispatch an assault: coordinated wrongdoing, a gathering of blackmailers, or simply a disappointed ex-worker or a contender. Also anybody can be the person in question. One of our clients is a tiny organization that does preparing for individuals in the development business, yet they went under assault for a very long time.

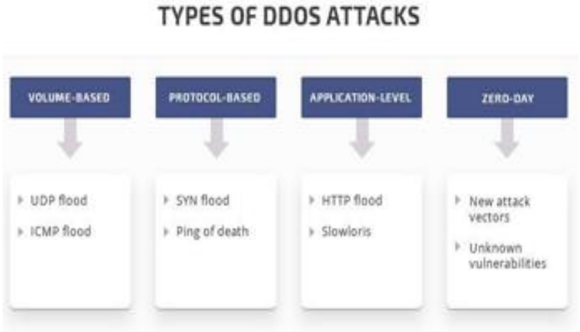

Fig 2: Types of DDoS attack. [3]

While DDoS offer a less muddled assault mode than different types of cyber-attacks, they are developing further and more refined.[5]

There are three fundamental classifications of assault.

(i) Volume-based attacks, which utilize high traffic to immerse the organization transmission capacity.

(ii) Protocol attacks, which center around taking advantage of server assets.

(iii) Application attacks, which center around web applications and are viewed as the most modern and genuine sort of assaults.

There are two normal methods of dispatching a DDoS attack:

Take advantage of programming weaknesses – Programmers can target both known and obscure programming weaknesses and send twisted parcels trying to squash the casualty's framework.

Burn-through computational or correspondence assets – Programmers can send monstrous volumes of authentic looking parcels, in this manner devouring the casualty's organization transmission capacity, central processor, or memory until the designated. Framework can presently don't deal with any solicitations from real clients.[5]

3. COUNTERMEASURE TECHNIQUES FOR DDOS

For any cyber or network attack prevention, detection and mitigation countermeasure can be applied for securing the network from malicious activity or attack. The scope is to give preventive measures such as keeping system and network up-to date, Anti-virus and other third-party applications such as java, adobe reader updated for applying against Smurf DDoS attack. If still attack is happening then first step is to detect the attack by selecting the features and comparing it with database for detecting Smurf DDoS attack to make your network secure.[5]

1. Attack prevention system:

DDoS prevention technique before the attack happens. This enables the authorize user to reduce attack attempts without denying the services by providing backup services available on demand. This technique can be preferred approach to DDoS attack but may be impractical with all types of flooding attacks.[5]

2. Detection system:

DDoS detection system is used them during attack. This enables to detect attack as it begins and respond immediately by minimizing the impact of attack. Detection system involves detection of suspicious pattern or suspicious behavior of that packet. DDoS detection system can be divided into two types such as signature based detection and anomaly based detection. Anomaly based detection is based on traffic deviation from normal and signature based detection are mostly of packets and protocols attacks based on some pattern.[5]

4. LITERATURE REVIEW

Saikat Das et. al. propose a NIDS which can detect existing as well as new types of DDoS attacks. The key feature of our NIDS is that it combines different classifiers using ensemble models, with the idea that each classifier can target specific aspects/types of intrusions, and in doing so provides a more robust defense mechanism against new intrusions. Further, we perform a detailed analysis of DDoS attacks, and based on this domain-knowledge verify the reduced feature set [27, 28] to significantly improve accuracy. We experiment with and analyze NSL-KDD dataset with reduced feature set and our proposed NIDS can detect 99.1% of DDoS attacks successfully. We compare our results with other existing approaches. Our NIDS approach has the learning capability to keep up with new and emerging DDoS attack patterns.[6]

P. J. Beslin Pajila and E. Golden Julie reviewed in there article about Internet of Things is a developing technique, it is the system of vehicles, home apparatuses, physical gadgets, and different things installed with hardware, programming, sensors, actuators, and system availability which empower these items to associate and trade data. IOT is made out of vast number of various end frameworks associated with web. Physical gadgets installed with RFID, sensor, etc. which enables item to communicate with one another. Security is a serious issue because all the heterogeneous end systems are communicated with each other through internet.[7]

A. Maslan et.al, author proposes and discuss about DDoS attacks are attacks carried out by an attacker by sending many packets to the server. Packages sent can contain malware so that the network that is attacked can experience out of bandwidth because the attacks run continuously. Security of a system is a factor that needs to be considered in the operation of information systems, which are intended to prevent threats to the system and detect and correct due to any system damage. The types of attacks can be Ping of Death, flooding, Remote controlled attacks, UDP floods, and Smurf Attack. This study aims to develop a new approach to detect DDoS attacks, based on packet data capture in network log forms and feature extract optimization that is statistically analyzed with neural network functions as a detection method. The method is done by adjusting the weight value of each connectivity from the input, neuron, and output. This method shows the journey of data that is on the network when exposed to a DDOS attack, so this method can help identify DDoS attacks with an accuracy of 88%. [8]

Jeremy Charlier et. al. present SynGAN, a framework that generates adversarial network attacks using the Generative Adversial Networks (GAN). SynGAN generates malicious packet flow mutations using real attack traffic, which can improve NIDS attack detection rates. As a first step, we compare two public datasets, NSL-KDD and CICIDS2017, for generating synthetic Distributed Denial of Service (DDoS) network attacks. We evaluate the attack quality (real vs. synthetic) using a gradient boosting classifier. The rapid digital transformation without security considerations has resulted in the rise of global-scale cyber-attacks. The first line of defense against these attacks is Network Intrusion Detection Systems (NIDS). Once deployed, however, these systems work as black boxes with a high rate of false positives with no measurable effectiveness. There is a need to continuously test and improve these systems by emulating real-world network attack mutations. [9]

Catak et. al., In this author focused primarily on the classification of network traffics based on the deep learning methods and technologies for network flow models. In order to increase the classification performance of a model that is based on the deep neural networks has been used. The model used in this research for the classification of network traffics evaluated and the related metrics showing the classification performance have been depicted in the figures and tables. As the results indicate, the proposed model can perform well enough for detecting DDoS attacks through deep learning technologies. [10]

R. S. Chaudhari and G. R. Talmale, they reviewed in there paper about DDoS attack is the most common attack with main disturbing effect. DDoS is the serious security threat, it challenge the accessibility of resources to legitimate clients. This attack causes the denial of service to genuine user due to flooding of traffic from unauthorized user. Various kind of DDoS attack are identified which include tcp, syn flood, ping flood attack, udp flood, smurf attack. Researchers have used various defense mechanisms for detection of DDoS attack, various data mining algorithm is also used for detection approach Clustering, classification, regression, neural network, Bayesian are few of the algorithm which previously used for attack detection. From research analysis, clustering and classification algorithm of data mining gives best result in terms of accuracy, time, true positive, true negative, false positive and false negative rate and detection rate. When clustering algorithm combines with classification algorithm give high accuracy. [11]

E. A. Ahmed and H. A. Ahmed, Authors are basically focusing on denial of service (DOS) in their research paper which is one of the popular attacks. It is a major reason of the inaccessibility of services and resources to the users by flooding the network and generating a lot of requests with invalid return addresses. They are going to propose a model to control DOS attack so the users will get an environment where their data is available over the cloud. Cloud computing is another innovation among many other latest technologies that enables the customers to get access to the services as per their demand. Cloud computing is getting success due to its self-service nature and on demand services. It provides great flexibility to its customers as they have to pay only for those services which they are in need to use without getting worried to pay the cost of hardware and software maintenance. Most of the users share their data by using cloud services so the major concern in cloud computing is the availability of data but it is observed that due to certain attacks data is not readily available when it is needed by the users.[12]

Naiji Zhang et. al., authors proposed in their research about The Distributed Denial of Service attack is one of the most common attacks and it is hard to mitigate, however, it has become more difficult while dealing with the Low-rate DoS (LDoS) attacks. The LDoS exploits the vulnerability of TCP congestion-control mechanism by sending malicious traffic at the low constant rate and influence the victim machine. Recently, machine learning approaches are applied to detect the complex DDoS attacks and improve the efficiency and robustness of the intrusion detection system. In this research, the algorithm is designed to balance the detection rate and its efficiency. The detection algorithm combines the Power Spectral Density (PSD) entropy function and Support Vector Machine to detect LDoS traffic from normal traffic. In our solution, the detection rate and efficiency are adjustable based on the parameter in the decision algorithm. To have high efficiency, the detection method will always detect the attacks by calculating PSD-entropy first and compare it with the two adaptive thresholds. The experimental results show that the proposed approach can detect 99.19% of the LDoS attacks and has an O (n log n) time complexity in the best case. [13]

T. Roempluk and O. Surinta, authors present the method for identifying distributed denial of service (DDoS) attacks. Two benchmark dataset, including KDD CUP 1999 and NSL-KDD, were used. The dataset were checked and deleted duplicate data. After the process, the amount of records of KDD Cup 1999 dataset were decreased from 4,898,431 records to 529,655 records, and the amount of records of NSL- KDD dataset were decreased from 125,373 to only 12,354 records. The reduction of the records always happened because of the characteristics of DDoS attacks which send repeated data to the victim's server. The researchers converted alphabet data to numeric data, then training by K- nearest neighbor (KNN), multi-layer perceptron and support vector machine. The result showed that KNN was the best method to identify the DDoS attacks. [14]

Myint Oo et. al., authors propose a detection method of DDoS attacks by using SDN based technique that will disturb the legitimate user's activities at the minimum and to propose Advanced Support Vector Machine (ASVM) technique as an enhancement of existing Support Vector Machine (SVM) algorithm to detect DDoS attacks. ASVM technique is a multiclass classification method consisting of three classes. In this paper, we can successfully detect two types of flooding-based DDoS attacks. Our detection technique can reduce the training time as well as the testing time by using two key features, namely, the volumetric and the asymmetric features. We evaluate the results by measuring a false alarm rate, a detection rate, and accuracy. The detection accuracy of our detection technique is approximately 97% with the fastest training time and testing time. [15]

Bashar Ahmed Khalaf et. al., authors review classifies and illustrates the attack types, the testing properties, the evaluation methods and the testing datasets that are utilized in the methodology of the proposed defense methods. Finally, this review provides a guideline and possible points of encampments for developing improved solution models of defense methods against DDoS attacks. Most of the proposed DDoS defense methods have different types of drawbacks and limitations. Some of these methods have signature-based defense mechanisms that fail to identify new attacks and others have anomaly-based defense mechanisms that are limited to specific types of DDoS attacks and yet to be applied in open environments. Subsequently, extensive research on applying artificial intelligence and statistical techniques in the defense methods has been conducted in order to identify, mitigate, and prevent these attacks. However, the most appropriate and effective defense features, mechanisms, techniques, and methods for handling such attacks remain to be an open question. This review paper focuses on the most common defense methods against DDoS attacks that adopt artificial intelligence and statistical approaches. [16]

Arshi M et al. performed in their research the DDoS attacks are the most destructive attacks that interrupt the safe operation of essential services delivered by the internet community's different organizations. DDOS stands for Distributed Denial Of Service attacks. These attacks are becoming more complex and expected to expand in number day after day, rendering detecting and combating these threats challenging. Hence, an advanced intrusion detection system (IDS) is required to identify and recognize anomalous internet traffic behavior. Within this article the process is supported on the latest dataset containing the current form of DDoS attacks including (HTTP flood, SI DDoS). This study combines well-known grouping methods such as Naïve Bayes, Multilayer Perception (MLP), and SVM, Decision trees. [17]

Benamar Bouyeddou et al. created A monitoring mechanism is vital for detecting malicious attacks against cyber systems. Detecting denial of service (DOS) and distributed DOS (DDOS) is one of the most important security challenges facing network technologies. This paper introduces a reliable detection mechanism based on the continuous ranked probability score (CRPS) statistical metric and exponentially smoothing (ES) scheme for enabling efficient detection of DOS and DDOS attacks. In this regard, the CRPS is used to quantify the dissimilarity between a new observation and the distribution of normal traffic. The ES scheme, which is sensitive in detecting small changes, is applied to CRPS measurements for anomaly detection. Moreover, in CRPS-ES approach, a nonparametric decision threshold computed via kernel density estimation is used to suitably detect anomalies. Tests on three publically available datasets proclaim the efficiency of the proposed mechanism in detecting cyber-attacks.[18]

5. CONCLUSION

In this paper, we have highlighted and discuss about DDoS that is Distributed Denial service of Attack the cyber-attack on computer network from review point of view with some security aspects of countermeasure the DDoS attack. Also now a day, Smurf DDoS attack are real threats to Computer and network Security, therefore to prevent from Smurf DDoS is necessary step to avoid such king of attack, also to detect such attacks to make your network and system protected from such malicious attack And also computer and computer network and increase the security in computer networks there is need to build a system for counter Smurf DDoS attack.

REFERENCE

[1] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai,Denial-of-service attack detection techniques, Internet Computing, IEEE, vol.

[2] Gang Wang, Jian Ma, Lihua Huang and Jinxing Hao, In the A new approach to Intrusion Detection using ANN and fuzzy clustering, in the Elsevier 2010

[3] S.Chavan, K.Shah, S.Sanyal, S.Mukherjee, A.Abraham, and N.Dave, In the &quot; Adaptive neuro-fuzzy Intrusion detection systems, in ITCC-Vol. 1 of 2004.

[4] Swathi Sambangi and Lakshmeeswari Gondi , A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression, 14th International Conference INTER-ENG 2020 Interdisciplinarity in Engineering, Mures, Romania, 8–9 October 2020.

[5] Bouyeddou B, Harrou F, Sun Y, Kadri B (2018) Detection of smurf flooding attacks using Kullback-Leibler-based scheme. 2018 4th International Conference on Computer and

Technology Applications (ICCTA). Available: http://dx.doi.org/10.1109/ cata.2018.8398647

[6] Yi Zhang, Qiang Liu and Guofeng Zhao, &quot; A real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis, &quot; 2010 3rd International Conference on Computer Science and Information Technology, 2010, pp.163-167,doi: 10.1109/ ICCSIT.2010.5563549.

[7] S. Das, A. M. Mahfouz, D. Venugopal and S. Shiva, "DDoS Intrusion Detection Through Machine Learning Ensemble, 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2019, pp. 471-477, doi: 10.1109/QRS-C.2019.00090.

[8] A. Maslan, K. M. Mohammad, F. Binti Mohd Foozy and S. N. Rizki, "DDoS Detection on Network Protocol Using Neural Network with Feature Extract Optimization", 2019 2nd International Conference on Applied Information Technology and Innovation (ICAITI), 2019, pp. 60-65, doi: 10.1109/ICAITI48442.2019.898 21 36.

[9] Jeremy Charlier, Aman Singh, Gaston Ormazabal, Radu State, Henning Schulzrinne, "SynGAN: Towards Generating Synthetic Network Attacks using GANs", CoRR abs/1908.09899 (2019)

[10] Catak, Ferhat Ozgur and Mustacoglu, Ahmet Fatih. "Distributed Denial of Service Attack Detection Using Autoencoder and Deep Neural Networks'. 1 Jan. 2019 : 3969 – 3979.

[11] R. S. Chaudhari and G. R. Talmale, &quot;A Review on Detection Approaches for Distributed Denial of Service Attacks, & quot; 2019 International Conference on Intelligent Sustainable Systems (ICISS), 2019, pp. 323-327, doi: 10.1109/ISS1.2019.8908125.

[12] E. A. Ahmed and H. A. Ahmed, ";A Proposed Model for Controlling Distributed Denial of Service Attack on Cloud Computing", 2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST), 2019, pp. 1-4, doi: 10.1109/ICEEST48626.2019.8981709.

[13] N. Zhang, F. Jaafar and Y. Malik, "Low-Rate DoS Attack Detection Using PSD Based Entropy and Machine Learning", 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2019, pp. 59-62, doi: 10.1109/CSCloud/EdgeCom.2019.00020.

[14] T. Roempluk and O. Surinta, "A Machine Learning Approach for Detecting Distributed Denial of Service Attacks" 2019 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT-NCON),2019,pp.146149,doi:10.1109 /ECTINCON.2019.8692243.

[15] Myint Oo, Myo, Kamolphiwong, Sinchai, Kamolphiwong, Thossaporn, Vasupongayya, Sangsuree, "Advanced Support Vector Machine-(ASVM-) Based Detection for Distributed Denial of Service (DDoS) Attack on Software Defined Networking (SDN)", https://doi.org /10.1155/2019/8012568,DOI- 10.1155/2019/ 8012568, Journal of Computer Networks and Communications, Hindawi.

[16] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed and W. M. Abduallah, "Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods" , in IEEE Access, vol. 7, pp. 51691-51713, 2019, doi: 10.1109/ACCESS.2019.2908998.

[17] Arshi M, Nasreen MD, and Karanam Madhavi," A Survey of DDOS Attacks Using Machine Learning Techniques", E3S Web of Conferences 184, 01052 (2020) https://doi.org/10.1051/ e3sconf/202018401052 ICMED 2020

[18] Mangesh D. Salunke, Ruhi Kabra, "Denial-of-Service Attack Detection", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 11

[19] Mangesh D. Salunke, Ruhi Kabra, Ashish Kumar, "Layered architecture for DoS attack detection system by combine approach of Naive bayes and Improved K-means Clustering Algorithm", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 02 Issue: 03 | June-2015

[20] Salunke M.D, Kumbharkar P.B., Y K Sharma, "A Proposed Methodology to Prevent a

Ransomware Attack", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9 Issue-1, May 2020