International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Detection and Classification of Distributed Denial of Service (DDoS) Attack

Rida Anwar[1], Shruti Gorasia[2]
[1,2]M.Tech Student, DIMAT, CSVTU, Bhilai

Abstract*— On line services are on a rapid upward push in today's internet global. Web servers, which host these online services, are the prime targets for the hackers to perform Distributed Denial of Service (DDoS) attacks. Attackers release DDoS assaults on net servers in order to disrupt the offerings or to eat the network bandwidth. This makes legitimate users unable to access the web resources at times. DDoS attack compromise the availability of the service by means of utilizing the energy of thousands and thousands of zombies (compromised computers) below the manipulate of the bot masters. DDoS attacks existed since mid 1980's and they are still the top most web security threat. Hence, mitigation of DDoS attacks is becoming very important. The distributed and dynamic nature of the DDoS attacks makes it more difficult to mitigate. In order to mitigate the DDoS attacks, several techniques have been proposed in the past by various researchers. However, most of the project research were focusing either on Application Layer or Network Layer and are mostly providing single layer of defense. In such scenario, hackers and attacker are taking advantage of the weakness of these mitigation techniques to launch the DDoS attack. In this research work, I will focus to implement Enhanced Support Vector Machine as well as to improve the accuracy of it.

Keywords: **DDoS, Enhanced Support Vector Machine, ICMP UDP, Internet Protocol, DNS**

I. INTRODUCTION

A. Distributed Denial Of Service(DDoS)

The internet owes plenty of its historical success and increase to its openness to new programs. New applications may be designed, applied and come into sizeable use a good deal more speedy, if they do not need to wait for key features to be added to the underlying network. Perversely, this has took place as a rational response of network and machine administrators needing to address the effects of the net's openness. The net architecture is prone to Denial-of-provider (DoS) assaults, wherein any series of hosts with sufficient bandwidth can disrupt valid verbal exchange between any pair of different parties, truely by way of flooding one quit or the alternative with undesirable site visitors. Those attacks are giant, growing, and have tested proof against all attempts to forestall them. Thus, in order to defend against these Distributed Denial-of-Service (DDoS) attacks that plague websites today; it is proposed to mitigate the DDoS attacks.

B. Comman DDoS Attacks

CERT Coordination Center defines three basic types of Denial of Service attacks:-
Consumption of scarce, restrained, or non renewable sources.
Destruction or alteration of configuration statistics.
Bodily destruction or alteration of network components.
Some common DDoS attack types are discussed below

1) *SYN Flood*: In the SYN Flood attack, the attacker compromises the three-way-handshake for a TCP connection. In normal scenario between client and server communication, the TCP client sends a SYN packet to the TCP server. Upon receiving the SYN packet, the TCP server opens a session and sends back a SYN/ACK packet to the TCP client and waits for ACK packet for the three way handshake to be established. If the server does not receive the ACK, the server waits for a timeout and closes the session and releases the resources. The attacker continually sends SYN packets to the server without sending the final ACK packet, thereby making the server to open multiple half open sessions, which in turn depletes the server resource.

2) *HTTP Flood*: In HTTP flood attacks, the attacker floods numerous HTTP request to access a web resource from the target web server. The requested resource is a large file, making the web server to spend its CPU resources to load the file. Mostly the attacker employs zombies, which mimics the normal web browsing behaviors.

3) *ICMP Flood (SMURF attack):* In ICMP Flood attack, the attacker floods ICMP echo request packets that have the victim server's IP address, to a broadcast address. The ICMP echo reply comes from all the hosts in the network to the victim server IP address, thereby exhausting the bandwidth of the victim server network. DNS, ICMP protocols are commonly used

these kinds of attacks.

4) UDP Flood: In UDP flood attack, the victim server network is overwhelmed by the large volume of UDP packets. These UDP packets are forwarded with random port numbers. If the application is not running on a specified port, the victim server will respond with an ICMP packet of "Destination unreachable to the sender". As plenty of UDP packets with random ports are generated, massive UDP packets exhaust the resources on the victim server network.

5) DNS Flood: DNS servers enable the clients to find the servers they are looking for the client requests the IP address of a server by issuing the domain name. The DNS Server resolve the domain name to IP address and vice versa. Attackers make use of this capability of the clients,by involving network of zombies to target a single DNS server with flood of valid request. It becomes very difficult for the DNS servers to distinguish from normally heavy traffic.

C. Botnet DDoS Attacks

A "bot" is a sort of malware that allows an attacker to take manage over an affected laptop. additionally referred to as a "botnet", which is typically made from sufferer machines that stretch throughout the globe. A botnet is a set of computers, linked to the internet, that engage to perform some dispensed task.

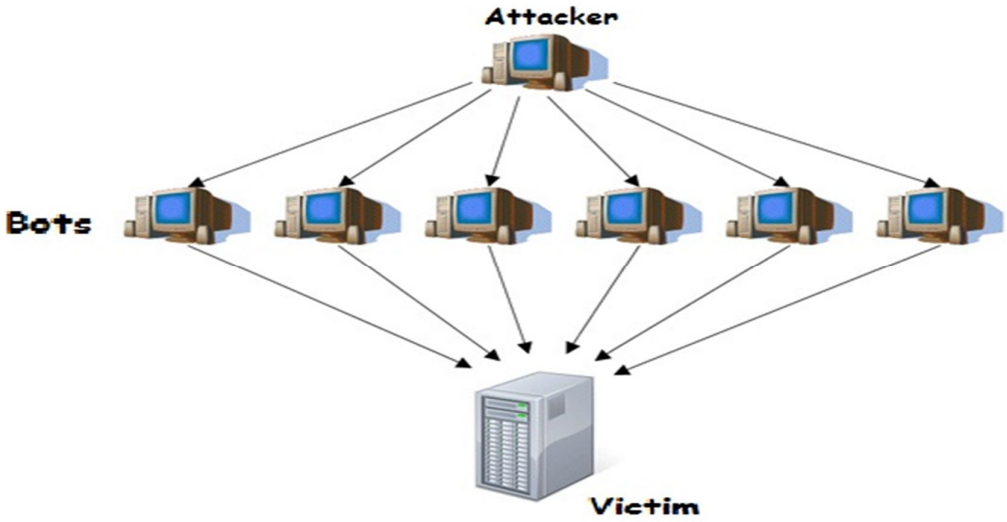

Fig.1: DDoS Attack

Botnets have turn out to be the biggest threats on the internet and are used for launching assaults and committing fraud. A have a look at suggests that, on a typical day, approximately 40% of the 800 million computers connected to the net in a botnet. those infected machines interact in many illegitimate activities which includes distributing junk mail, stealing touchy statistics, launching denial-of-provider attacks, and spreading new infections.

II. DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK TOOLS

Distributed Denial of service attacks are under existence since mid 1980's and are still the topmost web security threat. The vital reason behind this attack is the availability and sophistication of the attack tools. Examples of attack tools are : Trinoo, TFN2K, Shaft etc., The attack tools generate UDP Flooding ,ICMP Flooding ,TCP Flooding, Smurf attack etc.
The below table gives details of DDoS attack tool and the type of attacks generated.

Table 2.1 Attack tools vs. attack type generated

DDoS attack tool	Attack type generated by the tool
TFN2K	UDP Flooding, TCP Flooding, Smurf, ICMP Flooding
Shaft	UDP Flooding, TCP Flooding, ICMP Flooding
Stacheldraht	UDP Flooding, TCP Flooding, ICMP Flooding
Knight	UDP Flooding, TCP Flooding
Mstream	TCP Flooding
Trinity	UDP Flooding, TCP Flooding
Trinoo	UDP Flooding

III. SURVEY OF DIFFERENT TECHNIQUES FOR THE DETECTION OF DDOS ATTACK

Several studies and researches have been reported in the last few years for the detection and classification of DDoS attack by extracting different features mentioned in the above section. The work is as follows:

In year 2004, Stephen M. Specht and Ruby B. Lee described approximately DDoS attacks make a networked gadget or service unavailable to legitimate customers. those assaults are an annoyance at a minimum, or may be critically adverse if a crucial system is the number one sufferer. loss of community sources causes economic loss, work delays, and loss of verbal exchange between community users. answers should be advanced to save you those DDoS attacks.

In year 2006,Yang Xiang, Wanlei Zhou, and Zhongwen Li proposed an analytical model that can describe the interactions between the DDoS attack party and the defense party according to experiments.

In year 2009, Arun Raj Kumar, P. and S. Selvakumar proposed the most popular tools are identified, studied, and compared. DDoS attack happens not only for wired networks but also for wireless environments (where laptops are used as workstations in each site).

In year 2009,Ashley Chonka, Jaipal Singh, and Wanlei Zhou proposed the introduced a new algorithm that can predict the nature of network traffic in a dynamic system.

In year 2012,Poongothai, M and Sathyakala, M they do not proposed solutions for the issues discussed in this paper, it's miles vital to recognize and understand trends in attack technology with a view to efficiently and accurately evolve protection and reaction techniques to help examine how protection regulations, processes, and technologies may need to trade to cope with the present day traits in DDoS attack technology.

In year 2012,Alex Doyal, Justin Zhan and Huiming Anna Yu proposed Triple Dos is a DDoS defense method that makes use of clustering at the side of an overhead relay network to protect in opposition to dispensed denial of service assaults.

In year 2013,Yuan Tao, and Shui Yu proposed experiments and simulations demonstrate that the proposed detection algorithms are effective and independent of attack features.

In year 2015, I Gde Dharma N., M. Fiqri Muthohar, Alvin Prayuda J. D., Priagung K. and Deokjai Choi described experiment scenario and also how to evaluate the performance of method.

In year 2015,Amey Shevtekar and Nirwan Ansari proposed a new DDoS attack model by using botnets that is evadable and can be easily mistaken as real congestion.

In year 2015,Bharti Nagpal, Pratima Sharma, Naresh Chauhan and Angel Panesar decribed the various vulnerable systems on the Internet that can be used for launching DDoS attacks and, DDoS attacks are very difficult to defend against in spite of using defense mechanisms and will be an effective form of attack.

IV. DDOS DEFENSE TECHNIQUES

Several solutions are proposed by various researchers to overcome DDoS attacks in order to secure the networking environment from malicious attackers. The categories of defense mechanisms are:

Firewall based protection
Active Monitoring
Overlay Networks
Filtering mechanism
Capability based approaches
Trace back and Pushback mechanism
Filtering and Capability based mechanism
Identification and Classification of Botnets
CAPTCHA mechanism

A. Firewall Based Protection

Until the year 1996, the firewall was the basic means of protection for all sorts of network based attacks. Firewalls have simple rules, including to allow or deny protocols, ports or IP addresses. Firewalls were also used to mitigate DDoS threats. Bailey et al (1996) proposed a methodology SYN Defender, which protects against the TCP SYN flood assaults by means of intercepting all SYN packets and mediating the relationship attempts earlier than they reach the operating machine.

B. Active Monitoring

This category of solutions includes using software program marketers to continuously tracking TCP/IP visitors in a network at a given vicinity. It can watch for certain conditions to arise and react appropriately. Schuba et al (1997) proposed an active anomaly detection tool that can detect the condition of SYN flooding attack and react appropriately to defeat, or at least lessen

the impact of, an attack. The researcher introduces, "synkill " that gives safety towards SYN flooding for all hosts linked to the identical neighborhood region network, impartial in their running gadget or networking stack implementation.

C. Overlay Networks

Here an overlay network is used to mitigate DDoS threat, where an overlay is a computer network which built on top of another network. Stone (2000) proposed an IP overlay Network for tracking DoS floods called Center Track. It consists of IP tunnels or other connections that is used to selectively routine interesting datagram's directly from edge routers to special tracking routers.

D. Filtering Mechanism

These methods employ a method of filtering of the packet based on some filtering rules. If an ISP is aggregating routing announcements for more than one downstream networks, strict site visitors filtering should be used to limit site visitors, which claims to have originated from out of doors these aggregated announcements.

E. Capability Based Approaches

Capabilities or tokens are used in this mechanism for authentication purposes and also to classify between a legitimate and an attacker.

F. Traceback And Pushback Mechansim

Traceback mechanism concentrates on identifying the hosts liable for an attack and like supply filtering, does little to save you source from sending Pushback however employs dynamic site visitors filters. Dynamic pushback is used to prevent resource exhaustion. With pushback, node or link characterizes the types of packets causing the flood, and sends request upstream to rate limit them closer to the source.

G. Filtering Capability Approaches

Capabilities or tokens are used in this mechanism for authentication purpose and also to classify between a legitimate and an attacker.

H. Identification And Classification Of Botnet

Seewald & Gansterer (2009) proposed a passive approach to detect and identify the botnets. A passive botnet defense approach is proposed at three identify the botnets. A passive botnet defense approach is proposed at three hierarchical levels, namely the level of a single packet, network access and TCP conversations.

I. Captcha Based Mechansim

Several works are in the literature that provides an application level defense mechanism. Google, Yahoo and Hotmail uses text based CAPTCHA (Computer Aided Public Turing Test to tell Computer Human Apart) as an application level defense mechanism.

V. CONCLUSION

From the review of the above papers and different features, it can be concluded that many different techniques can be used to detect Distributed Denial of Service(DDoS) using different features.DDoS is a kind of DOS assault in which multiple compromised systems, which are frequently infected with a Trojan, are used to goal a single machine inflicting a Denial of service (DoS) attack.Hence, the detection has to be done in its earlier stages. There is a constant research happening in this field.right here, an strive is done to research and apprehend a number of the strategies used until now for the detection and classification of DDoS assault through the usage of some algorithms and the methods proposed within the reasearch papers.

VI. ACKNOWLEDGMENT

For this paper, a large amount of credit must go to our guide Reader and Head, Dept of C.S.E, Mrs Preeti Tuli. The author expresses sincere thanks to her for her continuous assistance, patience and support in the preparation of this paper.

REFERENCES

[1] YiXie and Shun-Zheng YU,"A large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviours" IEEE 2009.
[2] YiXie and Shun-Zheng, "Monitoring the Application layer DDoS Attacks for Popular Websites", IEEE/ACM Trans. On networking, Vol.17, No.1, pp, 15-25, 2009.
[3] Yoohwan Kim, Wing Cheong Lau, Mooi Choo Chuah and Jonatan Chao "Packet Score: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks", IEEE Trans. On dependable and secure computing, Vol.3, No. 2, PP. 2594-2604, 2006.

[4] Amey Shevtekar and Nirwan Ansari, “Is It Congestion or a DDoS Attack?” transaction IEEE communications letters, VOL.13, No. 7, Jul 2009, pp. 546-548.
[5] Thing, V.L.L. Sloman, M.Dulay, N. “Locating network domain entry and exit point/path for DDoS attack traffic” IEEE Trans. On Networking and Service Management, Vol. 6, No.3, pp. 163-170, 2009.
[6] Chonka, A.singh, J.Wanlei Zhou, “Chaos theory based detection against network mimicking DDoS attacks”, IEEE Trans. On Communications Letters, Vol.13, No. 9, pp. 717-721, 2009.
[7] Arun Raj Kumar, P. and S. Selvakumar, “Distributed Denial of Service (DDoS) Threat in Collaborative Environment-A survey on DDoS Attack Tools and Traceback Mechanisms”, International Advance Computing Conference (IACC 2009), pp 1275-1280, March 2009.
[8] Poongothai and Sathyakala, “Simulation and Analysis of DDoS Attacks”, International Conference on Emerging Trends in Science, Engineering and Technology, pp 78-85, 2012.
[9] B. Hancock, “Trinity v3, a DDoS tool”, Computer Security, 2000.
[10] Saman Taghavi Zargar, James joshi and David Tipper, “A Survey of Defense Mechanism Against Distributed Denial of Service (DDoS) Flooding Attacks”, IEEE communications Surveys & Tutorials, Vol. 15, No. 4, pp. 2046-2068, 2013.
[11] Alex Doyal, Justin Zhan and Huiming Anna Yu, “Towards Defeating DDoS Attacks”, International Conference on Cyber Security, pp. 209-211, 2012 IEEE.
[12] Yang Xiang, Wan lei Zhou and Zhongwen Li, “An Analytical Model for DDoS Attacks and Defense”, IEEE 2006.
[13] Soon Hin Khor and Akihiro Nakao, “DaaS: DDoS Mitigation- as – a-Service”, IEEE 2011
[14] Yuan Tao and Shui Yu, “DDoS Attack Detection at Local Area Networks Using Information Theoretical Metrics”, IEEE 2013.
[15] Bharat Rawal, Anthony Tsetse and Harold Ramcharan, “Emergence of DDoS Resistant Augmented Split Architecture”, IEEE 2013.
[16] Bharti Nagpal, Pratima Sharma, Naresh Chauhan and Angel Panesar, “DDoS Tools: Classification, Analysis and Comparison” IEEE 2015.
[17] I Gde Dharma N.,M. Fiqri Muthohar, Alvin Prayuda J. D., Priagung K., Deokjai Choi, “Time-based DDoS Detection and Mitigation for SDN Controller”, IEEE 2015.
[18] Qiao Yan, F. Richard Yu, Qingxiang Gong and Jianqiang Li, “Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges” IEEE 2015.