SURVEY ON DDOS FLODDING ATTACKS AND DEFENSE MECHANISM

[1]Krina Patel
[1]Assistant Professor
[1]Department of Information Technology,
[1]Silver Oak College of Engineering and Technology[1]Ahmedabad, India

Abstract : DDoS attacks are a dreadful problem with the internet services and the network. DDoS attacks are the massive attacks launched by distributing malicious computers. The hard problem against the defense of the DDoS attack is to distinguish the legitimate traffic from the attack traffic. Different strategy used to a detect this attack. This paper introduces about the major problem occur in the security which is known as DDoS attacks. The objective of this paper is to provide a survey of various mechanisms of distributed denial flooding attacks, its detection and various approaches to handle these attacks. Detection of DDOS flooding attack can be on source side as well as on the victim side. Based on the surveyed work it provides the reader to work in the research by using these approaches and featuresofDDOSattacks.

IndexTerms **- DDoS attack, DDos Flooding Attack, Defense techniques, Security.**

I. INTRODUCTION

Distributed Denial of service attack is a defined an attack launched by many attacker's host to one or more victim host, such that victim host is not further capable of providing its services or resources. This is done by sending a large amount of requests simultaneously by attacker's host called flooding to forbid the services to its legitimate users. The target host is either respond poorly or it crashes. DDoS is a propagation of DoS. In Dos attack there is one attacker host to launch the attack to one victim host. But DDoS has the very destructive power to harm the sever than DoS. Handling of DoS is easier than DDoS. An arsenal of computers called botnets are used to perform a DDoS attack. These computers of botnets are employed through the use of viruses,etc.

According to the CERT/CC, the primary DDoS attacks occurred in 1999. In February 2000, one of the first major DDoS attacks was waged against yahoo.com, eCommerce, EBay and Amazon. This attack kept these off the web for about 2 hours and caused damage of 1.7 billion dollars. Another DDoS attack occurred in October 2002 against the 13 root servers that provide the DNS service to internet users around the world. If all 13 servers were to go down, there would be unfortunate problems accessing the web. Although the attack only lasted for an hour and the effects were hardly noticeable to the typical Internet user, it caused seven of the thirteen root servers to stop working. If unchecked, more powerful DDoS attacks might probably disable essential internet services in minutes [6].

It is very difficult to find the original attacker because of sending spoofed IP addresses by botnets which are under control of attacker. The main target of the DDoS attacks are credit card, banks, websites, social sites. The incentives of the attacker includes financial gain, economical gain, revenge, competition. The purpose the attacker is to consume the bandwidth and services. DDOS attacks can be launched in two different ways. These are direct ddos attack and indirect ddos attack. In direct DDoS attack the traffic is send directly to the botnets to launch an attack against victim. In indirect DDoS attack the traffic is send indirectly to the botnets to launch an attack .DDoS attacks are very dangerous for the network security.

Two type of DDoS attack based on bandwidth and resource depletion. In this different type like, Flooding attack, UDP attack, ICMP attack, Smurf attack, TCP SYN attack, IP Address etc.

II. Literature Survey

Rizqi, Gandeva, Fazmah et al [1] develop a prototype to detect DDos attack using source addresses analytical method and analysis of network flow to given security of IPv6 network. Hong, Shuqiao, Hongchao, Mingming et al [2] provide a two-stage detection strategy by combining superpoint and flow similarity measurement to used sliding-detection algorithm. This detection approach can detect efficiently and Total Variation Distance. S. Chopade, K. Pandey, D. Bhade et al [3] presented a simple distance estimation based technique to detect the cloud from flooding attack and protect other server. Syed Hussain, Ghulam Beigh et al [4] is detect a UDP flooding attack used different queuing model like us DT, RED, DDR, FQ, SFQ. Vahid Aghaei, A. nur Zincir et al [5] develops a Traceback-based defence

against DDoS flooding attacks (TDFA) approach to counter this problem. The goal is to place the packet filtering as close to the attack source and control the traffic from network.

III. RESEARCH GAP ANALYSIS

no	Paper Title	Publications	Research Gap
1	The Detection of DDoS Flodding Attack using Hybrid Analysis in IPv6 Network.	IEEE-2015	IPv6 detection process used low or high traffic reduced. But improved the speed of detection.
2	Superpoint-Based Detection Against Distributed Denial of Service (DDoS) Flodding Attacks.	IEEE-2015	Detection of flash crowds with lots of accuracy But maintain the superpoint record is difficult.
3	Security Cloud Servers against Flooding Based DDoS Attacks.	IEEE-2013	Simple and effective technique used only real time mesurement.
4	Impact of DDoS Attack (UDP Flooding) on Queuing Models.	IEEE-2013	UDP detection process give good throughput but improve end to end delay.
5	TDFA: Traceback-based Defense against DDoS Flooding Attacks.	IEEE-2014	Detection of normal traffic but evaluate the security.

VI COMPARATIVE ANALYSIS

no	Paper Title	Method Used	Advantages	Disadvantages
1	The Detection of DDoS Flodding Attack using Hybrid Analysis in IPv6 Network.	Hybrid method	Detection prototype can be a variety of conditions.	Improve the average speed of detection.
2	Superpoint-Based Detection Against Distributed Denial of Service (DDoS) Flodding Attacks	Source address distribution based detection	Random legitimate flash crowds with lots of accuracy. Real time detection on high speed.	Designing algorithms for maintaining destination superpoint records. Not work for application level.
3	Security Cloud Servers against Flooding Based DDoS Attacks	Average Distance Estimation.	Simple but effective exponential smoothing technique. High detection rate.	It can only use real time measure ment.
4	Impact of DDoS Attack (UDP Flooding) on Queuing Models.	Queuing Techniques.	Good perfor mance. Better UDP throughput.	Improve throughput, packet loss, end to end delay.
5	TDFA: Traceback-based Defense against DDoS Flooding Attacks	TDFA.	TDMA against the real word DDoS and normal traffic.	Implement and evaluate the security of the TDFA system.

IV Problem Statement

DDoS attack detect to different algorithm and mechanism. Now current system detect the DDoS attack 90% to 95% accuracy in detection algorithm. In Future to implement and evaluate the system securing to itself. In the absence of an appropriate security mechanism. And that implement to authentication mechanism is very strong. Now Hybrid algorithm is best of above other algorithm but it's average speed is improve to in future.

V Conclusion

DDoS attacks are a dreadful problem with the internet services and the network. DDoS attack is a malicious attempt to suspending or interrupting services to target node. Various schemes are developed defence against to this attack. And to detect DDOS attack using source addresses analytical methods and analysis of network flow it gives the better accuracy in IPv6. DDoS attack is one advanced method to attacking network system it prevent legitimate user from using network resources. Trash back is the process of tracing back the forged IP packet to legitimate source rather than Spoofed IP address that was used by attacker and detect the normal traffic. MMSE (Minimum Mean Square Error) linear predictor to estimate the traffic rates from different distances is very simple and efficient technique.

References

[1]Rizqi L.Chandra, Gandeva B.Satrya, Fazmah A.Yulianto. "The Detection of DDoS Flodding Attack using Hybrid Analysis in IPv6 Network."2015 IEEE 3rd International Conference on information and communication Technology (ICoICT): 978-1-4799-7752-9/2015.

[2]Hong Jiang, Shuqiao Chen, Hongchao Hu, Mingming Zhang. "Superpoint-Based Detection Against Distributed Denial of Service (DDoS) Flodding Attacks." 2015 IEEE: 978-1-4673-6762-2/2015.

[3]S.S. Chopade, K.U. Pandey, D.S. Bhade. "Security Cloud Servers against Flooding Based DDoS Attacks." 2013 IEEE International conference on Communication Systems and Network Technologies (CSNT): 978-0-7695-4958-3. doi:10.1109/CSNT.2013.114.

[4]Syed Mujtiba Hussain, Ghulam Rasool Beigh. "Impact of DDoS Attack (UDP Flooding) on Queuing Models." 2013 4th International Conference on Computer and Communication Technology(ICCCT): 978-1-4799-1572-9/2013.

[5]Vahid Aghaei Foroushani , A. Nur Zincir-Heywood. "TDFA: Traceback-based Defense against DDoS Flooding Attacks." 2014 IEEE International Conference on Advanced Information Networking and Application (AINA): 1550-445X. doi:10.1109/AINA.2014.73.