ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 7, July 2016

AN EFFICIENT DETECTION OF DDoS FLOODING ATTACKS : A SURVEY

A.Siva Kumar,(M.Tech)
Dept. of CSE
Sree Vidyanikethan Engineering College
Tirupati, India

M.Ganesh Karthik, M.Tech
Asst. Professor, Dept. of CSE
Sree Vidyanikethan Engineering College
Tirupati, India

***Abstract*— Now a day's flooding attacks are major threat to the distributed networks. Flooding is a Denial of Service (DoS) type of attack that can be designed to bring a network or services down by flood by large amounts of traffic packets. Flood attack occur when a network or service becomes so weighted down with packets by initiate incomplete connection requests, it can no longer process genuine link requests. By flooding a server or host with connections that cannot be processed completely, the flood attack eventually fills the host's memory buffer. Once buffer is full no further connections can be made, and the result is a DoS attack. Detection of flooding attacks can be done by using several detection techniques and they can be described in this paper.**

Keywords—flooding; DoS;

I. Introduction

Flooding is a Denial of Service (DoS) type of attack that can be designed to bring a network or services down by flood by large amounts of traffic packets. Flood attacks occur when a network or service are so weighed down with packets by initiating incomplete connection requests that it can no longer process authentic connection requests. By flooding a server or host with connections that cannot be processed completely, the flood attack eventually fills the host's memory buffer. Once buffer is full no further connections can be made, and the result known as Denial of Service (DoS) attack.

A Denial of Service is an action that prevents otherwise impairs the authorized use of networks, systems, or applications by draining resources such as CPU, memory bandwidth, and disk space.

Flood attack, Ping of Death, SYN attack, Teardrop attack, DDoS, and Smurf attack are the most general types of DoS attacks. The attackers can launch DDoS attacks typically target sites or services provided by -high-status organizations, such as government organizations, banks, credit-card payment gateways, and even root name servers.

Flooding attack: Once the DDoS network has been established and the infrastructure for

communication between the agents and the handlers established and an attacker needs to do are issue commands to the agents to start sending packets to the destination host. The agent try to send misusual data packets (repeated TCP SYN packets, Large ICMP packets) to maximize the possibility of causing disruption at the destination and the intermediate nodes. There are certain basic packet attack types which are favorites of the attack tools. All the attack tools use a combination of these packet attack types to launch a DDoS attack. The basic attack types are as follows

i) TCP flood

ii) ICMP flood

iii) UDP flood

Ping of Death attack: In Ping of Death attack, the attacker creates a packet that contains more than 65,536 bytes, which is the limit of IP protocol can be exceeded. This packet can produce different kinds of damage to the machine that receives it, that results in crashing and rebooting. The Ping of Death is a typical TCP/IP implementation attack. In this assault, the DDoS attackers create an IP packet it exceeds the IP standard's maximum 65,536-byte size. When this large packet arrives, it crashes host systems that are using a vulnerable TCP/IP stack. No modern operating system is vulnerable to the simple Ping of Death attack, but it was a long-standing problem with UNIX systems.

SYN attack: A SYN flood attack take place throughout the period of three-way handshake that marks the onset of a TCP connection. In three-way handshake protocol, a client host sends a TCP-SYN packet to a server request for a new connection. Thereby, the server sends a SYN-ACK packet to the client host and places the connection establishment request in a queue., the client acknowledge with ACK packet. When an attack situated, however, the attacker sends an abundance of TCP-SYN packets to the destination, forcing it for both to open a lot of TCP connections and to respond to them. Then the attacker does not perform this process is called three-way handshake. That follows, exposing the victim that is not able to accept any new incoming requests, because its queue is full of half- open TCP connections.

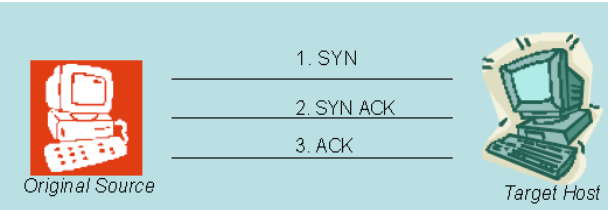

Fig 1: SYN attack

Teardrop attack: The Teardrop attack is used in olden days that rely on poor TCP/IP performance that is still around. It works by interfering with how stacks reconstruct the IP packet fragments. The trick here is that as IP packets are sometimes broken up into smaller packets called chunks, each fragment still has the original IP packet header information, and field that tells the TCP/IP protocol stack what bytes of

information it contains. When it works right, this packet header information is used to place the packet back together again. What happens with Teardrop attack even if is that your stack is hidden with IP fragments that have overlapping fields. When the stack tries to reassemble them, it cannot do it, and if it does not know to toss these trash packet fragments out, it can quickly fail. Most of the systems know how to deal with Teardrop attack now and a firewall can obstruct Teardrop packets in return for a bit more latency on network links since this makes it ignore all broken packets.

Smurf attack: In a smurf attack, the destination is filled with Internet Control Message Protocol ICMP ECHO-REPLY packets. The attacker can sends huge ICMP ECHO-REQ packets to the broadcast address of several subnets. These packets contain the source IP address field updated with destination address. Every machine that is connected with any of these subnets responds by sending ICMP ECHO-REPLY packets to the destination. Smurf attacks are very disquieting, because they are intensely distributed attacks.

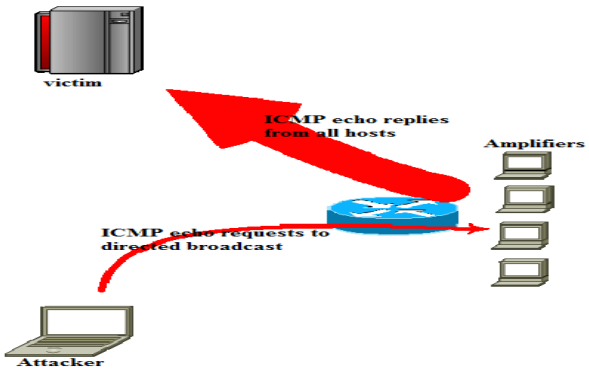

Fig 2: Smurf attack

Distributed Denial of Service

A Distributed Denial of Service(DDoS) attacks are a malicious attempt to make a server or a network resource are unavailable to end-users, usually by provisionally interrupting or freezing the services of a host system connected to the Internet. Unlike a Denial of Service (DoS) attack, in which one host system and one internet link is used to flood targeted resource with packets, a DDoS attack uses a many no of hosts and many Internet connections, often distributed worldwide in what is referred to as a botnet.

A flooding-based Distributed Denial of Service (DDoS) attack is done by the attacker by sending a large amount of unwanted traffic to the destination system and the resources of a host are unavailable, it is the very commonly used attack by the attacker. Network level congestion control can choke peak traffic to defend the network. Network monitors are used to monitor the traffic in the networks to classify them as valid traffic or attack traffic and also these monitors gives the traffic as an input to several detection algorithms for detecting DDoS attacks. However, it doesn't stop the quality of service (QoS) for valid traffic from going down because of attacks. Two features of DDoS attacks hold back the development of defense techniques. First, it is hard to distinguish between DDoS attack traffic and normal traffic. There is a lack of an effective differentiation mechanism that results in minimal

collateral damage for legitimate traffic. Second, the sources of DDoS attacks are also difficult to find in a distributed environment. Therefore, it is difficult to stop a DDoS attack effectively.

DDoS Flooding Attack Architecture:

A Distributed Denial of Service Flooding Attack is composed of four elements.

- The real attacker.
- The handlers or masters, which are compromise hosts with a special program running on them, capable of controlling multiple agents.
- The attack daemon agents or slave hosts, who are compromised hosts that are running a special program and are responsible for generating a sequence of packets towards the intended victim. Those machines are commonly external to the victim's individual network, to avoid efficient response from the victim, and external to the network of the attacker, to avoid problem if the attack is traced back.
- A victim or target host.

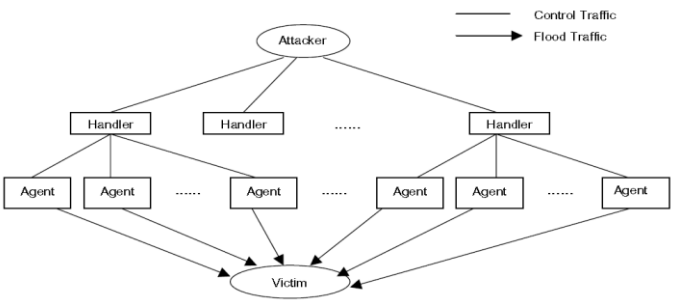

Fig 3: DDoS Flooding Attack agent-handler model

The following steps take place while prepare and conduct a DDoS attack:

1. ***Selection of agents*:** The attacker chooses the agents that will perform the attacker. These machinery need to have some vulnerability that the attacker can use to gain access to them. They should have abundant resources that will enable them to generate powerful attack streams. At the beginning this process will performed manually, but it was soon automated by scanning tools.

2. ***Compromise:*** The attacker exploit the security issues and vulnerabilities of the agent machines and plants the attack code. Additionally he tries to protect the code from detection and deactivation. Self-propagating tools such as the Ramen worm and Code Red soon computerized this phase. The owner and users of the agent systems typically have no knowledge that their system has been compromised and that they will be taking part in a DDoS attack. When participating in a DDoS attack, each agent program uses only a little amount of resources (both in memory and bandwidth), so that the users of computers experience minimal change in performance.

3. ***Communication:*** The attacker communicates with any number of handler to identify which agents are up and running, when to schedule attacks, or when to upgrade agents. Depending on how the attacker configures the DDoS attack network, agents can be instructed to communicate with a single handler or multiple

handlers. The communication between attacker and handler agents can be via TCP, UDP, or ICMP protocols.

4. ***Attack:*** At this step the attacker commands the inception of the attack. The duration of the attack as well as special features of the attack such as type, length, TTL, port numbers, etc, can be adjusted. The variety of the properties of attack packets can be precious for the attacker, in order to avoid detection.

Classification of DDoS Flooding attacks:

DDoS Flooding Attacks can be classified as follows:

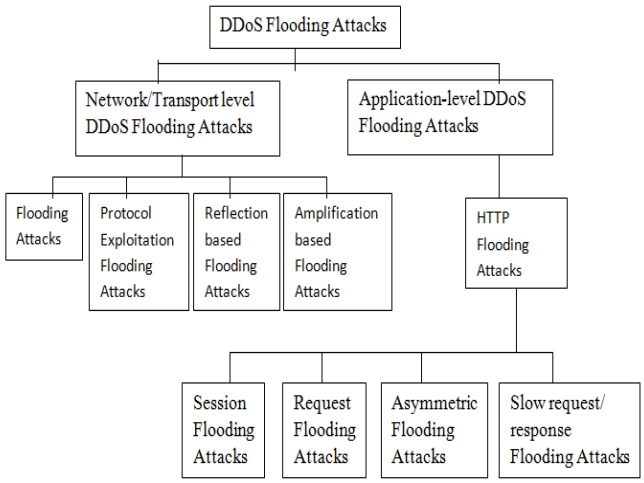

Fig 4: Classification of DDoS Flooding Attacks

II. Literature Survey

Behavior/Anomaly-based Approach:

This detection system first creates a baseline profile of the normal system, network or program activity. Subsequently any activity that deviates from the baseline is treated as a possible intrusion. This detection system is proactive and autonomous and can ensure security without any manual interference. An anomaly detection system usually consists of two phases: a training phase and testing phase. In the former, the normal traffic profile is defined; in the latter, learned profile is applied to the current traffic to look for any deviations.

A. Light weight method: To detect Flooding Attacks.

Advantage: Based on host, the rate of incoming traffic is limited.

Disadvantage: Subsequent message sent from the host will not be processed for a limited time.

B. Statistical Method: In this technique the system observes the movement of subjects and generates profile to represent their behavior. Typically two profiles are maintained for every subject: current profile and stored profile. As the system/network events are processed, the IDS update the current profile and periodically calculate an anomaly score by comparing the current profile with the stored profile using a task of abnormality of all measures within the profile. If the anomaly detection rate is higher than a certain threshold the IDS generates an alert.

Flooding Attack of messages INVITE can be detected by counting the number of messages compared with threshold.

C. DDoS Flooding Attack on VOIP networks and IMS Systems: Detection based on

change point detection using Cumulative Sum (CUSUM) algorithm.

Detection uses data mining in order to detect multiple attacks.

Signature-based Techniques:

In Signature based technique attack patterns are considered as a signature

Advantage: Detection is based on pattern matching between the current traffic and signature.

Disadvantage: Not suitable to detect flooding attacks at low rate, because the attacker can choose different strategies to produce attack traffic and thus make it difficult to produce a signature.

Low-rate-TCP/SYN-SYN/ACK protocol with considerations of packet header information:

There are a no of router buffer architectures that have smaller dropping rates for small SYN packets than for large data packets. For example, Drop-Tail technique, a queue in units of packets, where each packet takes a single slot in the buffer despite of packet size, small and large packets are equally likely to be dropped. However, for a Drop-Tail queue in units of bytes, small packets are less probable to be dropped than are large ones. Similarly, for Random Early Detection (RED) in packet mode, small and large data packets are equally likely to be dropped or noticeable, while for RED in byte mode, a packet's possibility of being dropped or marked is proportional to the packet size in bytes. For a congested router with an AQM method in byte mode, where a packet's chance of being dropped or marked is relative to the packet size in bytes, the drop or marking rate for TCP SYN/ACK data packets should generally be low. In this case, the benefit of marking SYN/ACK packets ECN-Capable should be likewise moderate. However, for a congested router with a Drop-Tail queue algorithm in units of packets or with an AQM mechanism in packet mode, and with no priority queuing for smaller packets, small and large packets should have the same chance of being dropped or marked. In such a case, making SYN/ACK packets ECN-Capable should be of significant benefit.

Advantage: Uses the counting bloom filter data structure to detect the behavior of TCP SYN-SYN/ACK and new scheme to shows a shorter time to detect low-rate attacks and high-rate attacks.

Disadvantage: All incoming packets SYN/ACK packets are classified based on Counter Bloom Filter (CBF) data structure. If there is multiple packets flow a CBF can increment and cause false results in the classification phase.

SYN Flooding:

A novel response to SYN flooding attacks. Here Network Congestion causing connections are divided into abnormal half-open and normal half-open.

Advantage: Network congestion identified using DARB (DelAy pRoBing) method.

Disadvantage: Several factors impacting the accuracy of detection and bringing potential false alerts.

i. False positive – Failure of the three-way handshake.
ii. False negatives - Difficult to distinguish the attack from network congestion.

III. OPEN ISSUES

These are the problems identified while detection of flooding attacks:

1. Subsequent messages are not processed for a limited time.
2. Difficult to produce the signature.
3. False results.
4. IPv6 headers are not handled.
5. Wide range of hardware storage and changes.
6. Bandwidth overhead.
7. Tracing of attack is not done while it is completed.
8. Memory overhead.
9. Impact on legitimate users.
10. Delay in authenticate legitimate users.3

IV. CONCLUSION

In this work primarily describes about flooding, Denial of Service (DoS) attack and it's types and Distributed Denial of Service (DDoS), Architect. In the Literature Survey describes about various detection methods and listing of their advantages and disadvantages and finally open issues under DDoS flooding attacks can be listed.

V. REFERENCES

[1] Saman Taghavi Zargar, James Joshi, and David Tipper," **A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks**", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, Feb,2013.

[2] Rajkumar, ManishaJitendra Nene," **A Survey on Latest DoS Attacks: Classification and Defense Mechanisms**", International Journal of Innovative Research in Computer and Communication Engineering,Oct,2013.

[3] Dileep Kumar G, Dr CV Guru Rao, Dr Manoj Kumar Singh, Dr Satyanarayana," **A Survey on Defense Mechanisms countering DDoS Attacks in the Network**", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 7, July 2013.

[4] Christos Douligeris, Aikaterini Mitrokotsa," **DDoS attacks and defense mechanisms: classification and state-of-the-art**", Computer Networks 44 (2004) 643–666, 2003.

[5] [6] S.Gavaskar, R.Surendiran, Dr.E.Ramaraj,"**Three Counter Mechanisms for TCP SYN Flooding Attacks**", International Journal of Computer Applications (0975-8887), Vol-6, September 2010.