Current Trends in Detection and Mitigation of Denial of Service Attacks-A Survey

Shishira S R
Dept. of Information Science
NMAMIT
Nitte, India

Vasudeva Pai
Dept. of Information Science
NMAMIT
Nitte, India

Manamohan K
Dept. of Computer Science
MIT
Manipal, India

ABSTRACT

Denial of Service (DoS) attack is a threat in today’s network because DoS attacks are easy to launch, while defending a network resource against them is very difficult. DoS attack is an attempt to make a machine or network resource unavailable to its legitimate users. It has put tremendous pressure over security experts in bringing out effective defense solutions. These attacks could be implemented with variety of tools and codes. Large number of countermeasure techniques tries to detect the attack and filter it out. In this paper a study is made on recent techniques on Denial of Service protection. Our discussion aims to identify the current methods in detection and mitigation of DoS attacks in the network.

General Terms

Denial of Service (DoS), Distributed Denial of Service (DDoS).

Keywords

Traffic Feature Conditional Entropy (TFCE), Genetic Algorithm (GA), Cumulative Sum (CUSUM).

1. INTRODUCTION

From the day the Internet has originated, the problems faced by the client and the server are existing in the wireless scenario. One of the most prominent attacks that still revolve around is Denial of Service (DoS) attacks [1]. DoS and Distributed Denial of Service (DDoS) are growing concerns as more people use on-line services for e-commerce, banking, and social networking. DoS attacks prevent authorized users to access the available resources and services. The attacker attempts to prevent legitimate users from accessing the information or services by sending large number of fake requests, whereas in a DDoS attack, the master owns millions of insecure machines called zombies which act according to the master command to overload the victim with huge volume of packets. Figure.1 shows DDoS consists of a real attacker, zombies and a victim host.

There are two general forms of DoS attacks: those that crash services and those that flood services. In most cases DDoS attacks involve forging of IP sender address so that the location of the attacking machines can’t easily be identified. The Key feature of DDoS includes distributing the attack across hundreds or thousands of compromised hosts (often residing on different network) and coordinating the attack among the hosts. In the summer of 1999, the Computer Incident Advisory Capability (CIAC) reported the first DDoS attack incident and most of the DoS attacks since then have been distributed in nature [2]. Most of the DDoS flooding attacks launched have tried to make the victim’s service unavailable. For instance, in February 2000, Yahoo experienced one of the first major DDoS flooding attacks that kept the company’s services off the Internet for about 2 hours incurring a significant loss in advertising revenue. This attack was launched by using system that had previously been infected by the Mydoom virus. In a recent survey commissioned by VeriSign, it has been found that 75 % of respondents had experienced one or more attacks between July 2008 and July 2009 [3]. Most recently since September 2012, online banking sites of 9 major U.S banks have been continuously the targets of series of powerful DDoS flooding attacks launched by a foreign hacker group called “Izz ad-Din al-Qassam cyber Fighters”[4]. Therefore protecting resources from these frequent and large DDoS attacks make the research community to focus on developing a comprehensive DDoS defense mechanism that can appropriately respond to attacks. This paper is organized as follows: Section 2 and 3 discuss the motivation and the main objective of the survey. Section 4 briefly discusses the types of DoS attacks and its detection and mitigation techniques.

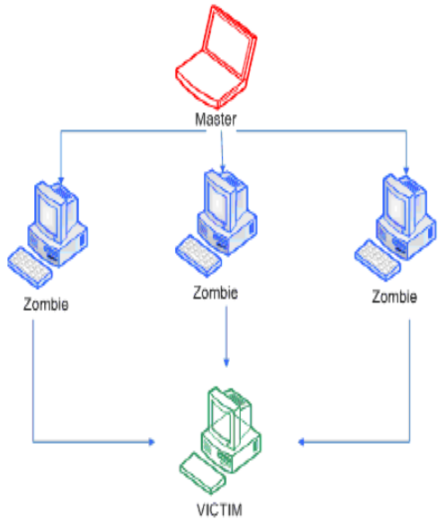

Fig1: DDoS attack

2. MOTIVATION

The increasing number of attacks and unresolved issues are actively present in the IT world for nearly a decade and there has never been an ultimate solution for this. These attacks have got business down, crippled the economy of nation. Allocating extra bandwidth, tracing back the attacks, identifying and stopping the packets are few of general suggestions from experts. But the exact solution varies with the severity of the attack. The factors that motivated to do a survey are revenue loss, invariably slow network performance and service unavailability. Thus the ultimate motivation arose with a desire of stopping these attacks that could lead to safe and secure IT world.

3. OBJECTIVE

The main objective of this survey is to understand the subject in detail by taking into consideration the previous incidents and attacks that happened in the past.

4. LITERATURE REVIEW

DoS attacks are generally carried out with large number of systems attacking a specific victim. There are several types of DoS that could interrupt a normal service. The attacking methods can be classified into two methods according to Erikson Jon. First method is to flood the network and not allowing legitimate packets to get through it. Second method is to crash a hardware or software and make it inoperable.

4.1 Types of DoS attacks

Different types of Dos attacks are as follows

4.1.1 Smurf Attack

This attack floods the victim's bandwidth. In this method, the attacker sends a large number of ICMP echo requests. Hence all the ICMP messages have spoofed source address as that of victim's IP address. This attack floods the victim's bandwidth.

4.1.2 Syn Flood

SYN Flood attack is the most popular and effective brute-force DoS attack. SYN Flood attack sends TCP connect request with SYN flag to the victim server. Then the victim server returns ACK acknowledgement to the attacker, but the attacker doesn't acknowledge, so the connection is not established fully, and this kind of connection is called half-connection. The victim server maintains a huge number of half-connections which will cost a mass of resources.

4.1.3 Router HTTP Attack

The router HTTP attack is a kind of semantic attack. If the Cisco router has not set the "not HTTP server" rule, the attacker may lock the router until the administrator reboot the router by sending the HTTP request like "GET /000 HTTP/1.0" to the router. At the beginning of the attack, the attacker needs to probe the router's web service port and status. If the web server is running, the attack can continue. Then the attack data need to be constructed, and socket need to be open. These two steps are both the precondition of sending the request, and they can be executed in parallel.

4.1.4 Reflected/Spoofed Attack

A Distributed Reflected Denial of Service attack (DRDoS) involves sending forged requests of some type to a very large number of computers that will reply to the requests. Using IP address spoofing, the source address is set to that of the targeted victim, which means all the replies will go and flood the target. ICMP Echo Request attacks (Smurf Attack) can be considered one form of reflected attack, as the flooding host sends Echo Requests to the broadcast addresses of the misconfigured networks; thereby many hosts send Echo Reply packets to the victim.

4.1.5 Slow Read Attack

Slow Read attack sends legitimate application layer requests but reads responses very slowly, trying to exhaust the server's connection pool. Slow reading is achieved by setting a very small number for the TCP Receive Window size and at the same time by emptying clients TCP receive buffer slowly. With this action we have a very low data flow rate.

4.1.6 Distributed Attack

A Distributed Denial of Service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. When a server is overloaded with connections, new connections can no longer be accepted. Simple attacks such as SYN floods may appear with a wide range of source IP addresses, giving the appearance of a well Distributed DoS. Because the source IP addresses is spoofed, an attack could come from a limited set of sources. Advantages to an attacker of using a distributed denial-of-service attack is that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, thus making it harder to track and shut down.

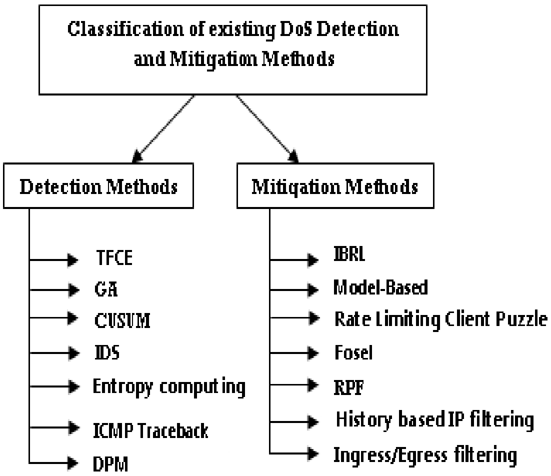

Fig 2: Classification of DoS Detection and Mitigation methods

4.2 Detection Methods

There are various different methods to detect and mitigate Denial of Service attacks. In this paper we studied detection methods such as TFCE, GA, CUSUM, and IDS.

4.2.1 Traffic Feature Conditional Entropy

Yun Liu et al., [5] proposed a method to detect DoS attack using Conditional Entropy. This Conditional Entropy is used to characterize the DDoS attacks. Further SVM (Support Vector Machine) classifier is used to detect the attack. Conditional Entropy is calculated for three features i.e. sip|dip, sip|dport, dport|dip in which sip represents source ip address, dip represents destination ip address, dport represents destination port. If sip|dip value is greater than others then it represents the attack. Further, detection and false alarm ratio is calculated to check the ratio of detection. Using this method when time T is kept below 2s the detection ratio decreases. Thus this method used received time T above 3s to detect the attack.

4.2.2 GA based Optimized Traffic Matrix

Je Hak Lee et al., [6] proposed a Genetic Algorithm which improves the traffic matrix building operation and optimize the parameters. The method is as follows, the traffic matrix for one window size is constructed and used as testing data set while using genetic algorithm the training data sets are developed. Genetic algorithm includes matrix size, packet based window size and threshold value. Compute the variance using traffic matrix. If the variance is less than Threshold refers that there exists DoS attack.

4.2.3 Cumulative Sum (CUSUM)

CaLynna Sorrells et al., [7] proposed Quickest detection of Denial-of-Service Attacks in Cognitive Wireless Network. Cumulative Sum (CUSUM) algorithm is used to minimize the detection delay so that a network manager may react to the event as soon as possible to mitigate the effect of attacks. The nodes are put into 'bins' based on the percentage of node appearing in the resulting paths. CUSUM value is noted for every entry. Decision rule is employed here i.e. if CUSUM Value is less than zero results in DoS attack else it is a normal traffic. Placing within a cross-layer framework, CUSUM Algorithm is capable of detecting DOS attacks with minimum delay. But the tests of the cross-layer examination procedures are not performed using this method.

4.2.4 Intrusion Detection System (IDS)

Divya Bansal et al., [8] proposed a Cross Layer Interactions for Detecting Denial of Service Attacks in Wireless Mesh Network (WMN). This system uses cross layer Intrusion Detection System to gather information from different layers to recognize the DoS attacks. This architecture provides high bandwidth, spectral efficiency. First level of detection triggers selecting a monitor for analyzing the trace files for intruders. Second level collects information from multiple layers. All these information are gathered and combined which gives a high chance of discovering attack in multi hop network. Monitoring system starts if sender cannot receive ACK. Sender randomly selects monitor node, applies the algorithm and creates the HITLIST which has nodes that can be malicious. This list is later sent to Level2. In level 2 the cause of the attack is found. Decision module decides whether the DoS attack is from malicious node or not. Depending on the decision, the generator sets the appropriate alarm.

4.3 Mitigation Methods

4.3.1 Interface based Rate Limiting Algorithm (IBRL)

B.S. Kiruthika Devi et al., [9] proposed a DDoS detection using host-network based metrics. This method finds the network anomalies, deploy the system at distributed routers, then identify the attack packets and filter them. Legitimate traffic throughput is improved and attack traffic throughput is reduced and IBRL (Interface based Rate Limiting) is used in mitigating DDoS traffic effectively. Initially all traffic traces are collected from the network. Impact of traffic is measured with performance metrics (CPU usage, memory, packet loss, latency, and throughput). Thus during DDoS attack this metrics are measured and the attack traffic is mitigated using IBRL algorithm. Initially throughput of SerialInterface1 of edge router is checked against SerialInterface2 and SerialInterface3 of same router. If the SertialInterface1 is found greater than those, then link utilization of SerialInterface1 is checked. If the link utilization exceeds 95% of bandwidth capacity then Rate limit rules are applied on SerialInterface1 to mitigate the attack. The weight based performance metrics to combine the impact of DDoS attacks and quantify at different attack strengths aren't achieved.

4.3.2 Model-based Adaptive Method

Cornel Barna et al., [10] proposed a Model-based Adaptive DoS attack for DoS Mitigation where DoS attacks are detected and mitigated at web application levels. Arriving HTTP requests are filtered based on set of rules. To mitigate DoS attacks, two new components are used which includes Dynamic Firewall and Analyzer. Dynamic Firewall is responsible for identifying requests which overloads the server. The incoming requests which are filtered are passed to the Analyzer for further analysis. To identify the legitimate requests CAPTCHAs are used and those requests which are part of DoS attacks are dropped. The incoming traffic is fed into Dynamic firewall as shown in the figure, which is responsible for redirecting all requests which overloads the server. It includes two components: Reverse Proxy and Decision engine. Reverse Proxy is a simple HTTP request router which redirects legitimate requests to web Application and suspicious request to analyzer while Decision engine constructs routing rules for reverse proxy and identifies HTTP requests which overloads the web application. Suspicious requests are not dropped, they are forwarded to analyzer. Analyzer presents a CAPTCHA test that must be passed before the request is identified as legitimate. The requests are considered malicious when a request from the same source has failed or not answered the CAPTCHA within a time period. Performance goals (throughput, response time, and utilization values) are fed into Decision Controller which constructs the filters used by reverse proxy. At each iteration it predicts whether incoming requests would overload the web application. It collects the information on the workload. Error correction of the collected data is not examined by the author.

4.3.3 Rate Limiting Client Puzzle Scheme

Jing Yang Koh et al., [11] proposed a method for DoS mitigation using Rate limiting client puzzle schemes. A leaky bucket rate limiting queue mechanism is proposed in their work. This mechanism will limit the incoming request which overloads the server. Client puzzle defense mechanism is deployed at application server and acts as a gate keeper to prevent DoS attacks and avoid server overloading. An incoming request is fed into the bucket and client puzzle is issued with difficulty parameter Q .In practice, the client can finish solving a puzzle earlier or later the expected delay. Counters are used to count the total number of issued, submitted and expected puzzle solutions which is used to prevent the attack.

4.3.4 Filtering Method using Fosel Architecture

Hakem Beitollahi et al., [12] proposed a technique to mitigate DoS attack by filtering with a help of an Overlay Security Layer called as FOSel. FOSel reduces processing time noticeably and also the attackers cannot use spoofed IP addresses. The simulation results shows that FOSel filter has shown really good results when it comes to DoS attacks. It reduces the chance of successful attacks and it is almost as twice faster than SOS (Secure Overlay Services). The application site is protected by a filter that discards any packet whose source addresses is not approved. Set of approved source addresses are secretly kept from the attackers so that they cannot use them. An overlay layer is designed, the attackers know the IP addresses of the nodes of the layer and of the sites, but there are some nodes whose addresses are secret (green nodes). If the identity of a green node is revealed and it is targeted then it is removed from overlay and the site chooses another node randomly as a new green node. To choose a green node, site sends a message to the overlay node, and tells the node about the task. Every site has several green nodes. Overlay network with the green nodes provide to the site very effectively and fast filter against the attacks. The filter just needs to compare the IP addresses. But Fosel filter processes only one part of received packets and discards all rest without processing, and the secret green nodes send multiple copies of the messages to the target application site which can overload the system.

4.3.5 Router based Approach

David L Meenakshi et al., [13] proposed a Router based approach to mitigate DoS attacks on the wireless networks. Router base approach uses router's significant feature called as Access Control List (ACL). This method drops the packet of non-legitimate users. First step is to differentiate the packets using types of attacks. Hence to do that, author considered a router with two interfaces, where Ethernet is connected to an internal LAN. Router is configured using commands with applying access list. Each list is assigned a number 169. These lists are limited to assigned range of numbers and will not filter out any traffic, but it is categorizes packets in useful way. These list can be used to diagnose all two types of attacks i.e. Smurf, SYN floods. Most of the traffic which arrives on Serial interface consists of ICMP echo reply packets .This is the sign of a Smurf attack. Now instead of blocking these ICMP requests, WRED packet dropping mechanism is implemented to drop these packets. Source of an attack is identified by tracing back hop by hop and applying ACL filters. Host addresses which end in .0 or .255 are very uncommon in Internet. Hence with this list, many "noise" packets can be eliminated from the log. To drop the packet Network congestion Avoidance is adopted with ACL i.e. weighted RED algorithm is adopted for dropping the attacker's packet. ACL will detect the requests which are repeated and gives its results to WRED dropping parameter of the router. So, based on this information bulky TCP, ICMP non-legitimate packet has more priority. Packets with high IP precedence are non-legitimate and are dropped. Thus for implementing the idea of WRED with ACL, router's IOS are modified.

5. CONCLUSION

In this paper, we presented a survey on recent techniques of detecting and mitigating of Denial of Service attacks. With the spread of DoS attacks on the Internet, the DoS attack resistance ability of the network systems and facilities draws more and more attention. Because of the variety of DoS attacks, it is almost impossible to find a decent way to defend against such kind of attacks. There have been several solutions that slightly progressed in that field, but they have just delayed the attacks. Above mentioned Traffic feature conditional entropy method offers a better performance in terms of efficiency.

6. REFERENCES

[1] Saman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE,"A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks"

[2] SANS Institute. Subramani rao Sridhar rao ,"Denial of Service attacks and mitigation techniques: Real time implementation with detailed analyis" The SANS Institute,2011.

[3] Forrester Consulting, The trends and changing landscape of DDoS threats and protection, a commissioned study conducted by Forrester Consulting on behalf of VeriSign, Inc., July 2009.

[4] Erikson, Jon (2008). HACKING the art of exploitation (2nd edition Ed.). San Francisco:No Starch Press. p. 251. ISBN 1-59327-144-1.

[5] Yun Liu et al.,'Detecting DDoS Attacks Using Conditional Entropy', IEEE 2010.

[6] Je Hak Lee ,Dong Seong Kim ,Sang Min Lee ,Jong Sou Park, 'DDoS Attacks Detection Using GA based Optimized Traffic Matrix',2011 IEEE Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.

[7] CaLynna Sorrells and Lijun Qian Husheng Li,"Quickest detection of denial-of-service attacks in cognitive wireless networks" ACM, 2012.

[8] Divya Bansal, Sanjeev Sofat, "Use of cross layer interactions for detecting denial of service attacks in WMN",2010.

[9] B.S. Kiruthika Devi, G. Preetha, S. Mercy Shalinie,"DDoS detection using host-network based metrics and mitigation in experimental testbed", IEEE, 2012.

[10] Cornel Barna, Mark Shtern, Michael Smit, Vassilios Tzerpos, Marin Litoiu York University,"Model-based adaptive DoS attack mitigation", ACM, 2012.

[11] Jing Yang Koh, Joseph Teo Chee Ming, and Dusit Niyato ,"Rate limiting client puzzle schemes for Denial-of-Service mitigation", IEEE 2013.

[12] Hakem Beitollahi, Geert Deconinck, Katholieke Universiteit Leuven, Belgium "FOSeL: Filtering by helping an overlay security layer to mitigate DoS attacks", IEEE, 2008.

[13] David L,Meenakshi Sood,Mahesh Kumar Kajla,"Router based approach to mitigate DoS attacks on the wireless networks,IEEE,2011.