Detection and Mitigation of DDOS Attack against Web Server

Dhruv A. Patel[2], Prof. Hasmukh Patel[2]

[1]GTU,Ahmedabad, India
[2]HOD, LCIT Bhandu, Mehsana, India

***Abstract*-- In the modern computer world, use of the internet is increasing day by day. However, the increasing use of the internet creates some security issues. These days, such new types of sophisticated security attacks occurred and it is not easy to detect and prevent those attacks effectively. One common method of attack involves sending large amount of request to site or server and server will be unable to handle such huge requests and site will be offline for many days depends upon the attack. This is major security threat to internet services and most critical attack for cyber security world is called distributed denial of service (DDOS) attack. How to detect and prevent against a DDOS attack is currently a hot topic in both industry and academia. Traditionally, DDOS attacks are carried out at the network layer. Since many studies have noticed this type of attacks and have proposed different schemes and solutions (e.g., network measure or anomaly detection) to protect the network. It is not as easy as in the past for attackers to launch the DDOS attacks based on network layer. So, attackers shift their offensive strategies to application layered attacks and establish a more sophisticated type of application layer DDOS attacks such as HTTP flooding. The significance of the application layer DDOS attack and increased occurrence and strength of attack led my work to use creative, effective and efficient mechanism that address the DDOS flooding problem. Here, I am looking forward to detect and mitigate the effect of DDOS attack against web server. I will propose such a mechanism that will detect DDOS attack, differentiate the attack traffic from normal traffic, and mitigate the effect of DDOS attack. My main goal is to increase the availability of web server for legal users.**

***Key Words* – DDOS, Availability, Web server, HTTP flooding, zombie machines, Botnet**

I. INTRODUCTION

The world has seen rapid advances in science and technology in the last two decades, which has enabled dealing with a wide range of human needs effectively. These needs vary from simple day-to-day needs like paying electricity bills, booking train-tickets, information gathering etc. In modern era, use of internet is also increasing by human. These technologies have taken human life into much higher levels of sophistication and ease. But in the middle of this phenomenon, the rise and growth of a parallel technology is startling – that of compromising security. This includes attacks on information, such as stealing of private information, hacking, and outage of services. These attacks effect on CIA (confidentiality, integrity, availability) triad. Such a type of attack which compromises the availability of information or service to legal user is called DDOS attack.

Problem Description

A Distributed Denial of Service (DDOS) Attack is most common and dangerous attack on internet today. It attacks on organization's infrastructure. It is becoming more and more danger everyday as attacker are using widely spanned army of bots spread around the world, and to becomes very difficult to detect and diminish this attack. The issue is the ease with which serious DOS and DDOS attacks can be possibly carried out today. Software tools available for free download on the Internet have ability to carry out low volume to high volume DOS and DDOS attacks. In the OSI model, the DDOS attacks may be targeted at different layers, many concentrate on the network layer, such as ICMP flooding, SYN floods and UDP flooding are called Net-DDOS attacks. Attacks aimed at the application layers are called App-DDOS attacks such as HTTP flooding. Application layer is vulnerable to a wide range of threats, including relatively unsophisticated attacks. So, it's a challenge to completely protect against application layer DDOS attack. It is a type of attack in which a network of compromised computer attacks a single target which is generally a server and it results in stopping of service on that server or system.

In DDOS attack, malicious attacker installs malware on compromises system without user's knowledge. The group of such compromised systems is known as Botnet or Zombie Army. Attacker gets command of many of such „Bots" to use for sending ping requests, forge request for the target server. As the number of such fake requests will equal the network bandwidth, it takes available network resources at the target end as well.

This not only effects network bandwidth but may also results server into services or service crashing and so genuine user may get slow or no response from the target server. i.e. Genuine users are denied to use the service for which they have requested, thus the term „Denial of Service".

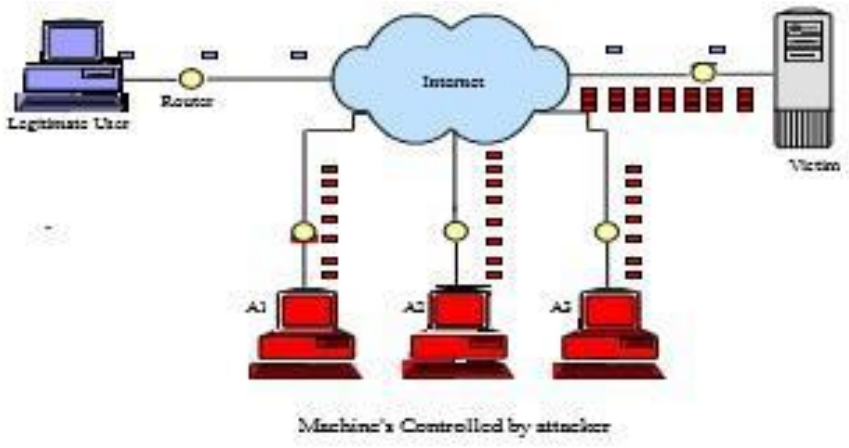


Fig I DDOS attack scenario [**1]**

Still 2014, there is not such an effective mechanism that can prevent DDOS attack and attack is increasing every year. Here, i will present such an effective solution to increase the availability of web server for legal users.

II. LITERATURE REVIEW

Background

DDOS Attack is most dangerous attack on the internet in today's era. In the summer of 1999, the Computer Incident Advisory Capability (CIAC) reported the first Distributed DOS attack incident and since then most of the Dos attacks have been distributed in nature [3]. Many DDOS flooding attacks had been launched against many different organizations since the summer of 1999[3].Most of the DDOS attacks launched to date have tried to make the victim services unavailable leading to revenue losses and increased costs of mitigating the attacks and restoring the services.

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 significant loss in advertising revenue[4]. In October 2002, 9of the 13 root servers2 that provides the Domain Name Server (DNS) service to Internet users around the world shutdown for an hour because of a DDOS flooding attack [5].

After that, these attacks have been increased dramatically such that now it has become the most dangerous and powerful threat of the internet in such a way that it is really very hard to identify and mitigate such attacks. Till now, major of the Internet sites including Yahoo, eBay, Google etc. have been attacked and recently Worldpress.com [2]. Even in 2013 and 2014 DDOS attack happened and it was running over 300gbps.

Why do such attacks occur?

The main aim of a DDOS attack is to harm on victim, either for personal reasons like against home computer or for revenge purpose, for secret information Theft by damaging victim's resources. Some attacker also experiment this attack to gain popularity by making successful attack on popular web servers which give them fame in the hacker community. Sometimes attackers are usually belongs to the military or terrorist organizations of a country [6] and they are politically motivated [2] to attack a wide range of critical sections of another country.

So, we can categorize DDOS attack based on motivation of the attackers into following categories.

1. Financial/Economical gain
2. Revenge
3. Ideological belief
4. Intellectual challenge
5. Cyber warfare

Understanding of attack

DDOS attack normally is of mainly three phases [9].

1. **Target Acquisition -** It is the first phase of DDOS attack. An attacker first study network and gets a victim IP address. Victim can be any like Web server, DNS server, Internet gateway, etc. The reason behind attack could be economic or for fun.
2. **Groundwork -** This is the subsequent phase of DDOS attack. An attacker develop a large network with compromised agent machines and then install malware software without user's knowledge on each machine and later used to flood the network traffic.
3. **Actual Attack -** In the final phase named actual attack, the attacker controls whole network of bots or zombies and command them to flood the network with packets to produce high traffic which then slowdown the service or destruct the service.

Effects on an Organization

Almost all of the organizations dependent on internet based systems require building up more secure defences techniques against distributed denial of service attacks. These attacks can disturb online applications and services and it is a number one security problem that service providers are facing today. Organizations experienced more than 350,000 DDOS attacks which affecting business with crucial online applications across the market.

Recently, Attacks are becoming larger with attack size increasing significantly from 400 Mbps in 2001 to 49 Gbps in 2009. Botnet is available for rent at £80 per day or less, with that anybody can get computational power to launch DDOS attack. DDOS attacks on organizations result in tangible losses and it doesn't matter whether it has been attacked or whether it is just providing resources to stop the attack. Moreover, once the attack is over, the interruption to an organization's service can cause long lasting effects on its reputations, and it also creates negative impact on its customer's satisfaction and trust.

Related Work

In today's internet world, there are two main methods to launch DDOS attacks. The first method is for the attacker to send some malformed packets to the victim to confuse a proto color an application running on it. The other method, currently which is the most common one, involves an attacker trying to do one or both of the following:

1. Disrupt a legitimate user's connectivity by exhausting bandwidth, router processing capacity or network resources; these are network/transport-level flooding attacks [10].
2. Disrupt a legitimate user's services by exhausting the server resources (e.g. CPU, memory, disk/database bandwidth, and I/O bandwidth); these are application-level flooding attacks.[11]

There are different types of DDOS attack. They are mainly divided into two categories.

1. Network layer attacks
2. Application layer attacks

Here, my research topic is about to increase the availability of web server so I will discuss the defense mechanisms against application layer DDOS attack. In below table, I have summarized all existing defense mechanisms against application layer DDOS attacks.[2][12]

Defence Mechanism	**Functionality**	**Limitations**
Hidden semi Markov model	Xie et al.propose an anomaly detector based on hidden semi Markov model to describe the dynamics of access matrix and to detect the attack.	Main disadvantage of this method is the high complexity of algorithm.
DDOS shield	This mechanism use statistical approach to detect characteristics of HTTP session and use rate-limiting as the primary defence mechanism. It consists of suspicious assignment mechanism and a DDOS resilient scheduler.	It is not clear if a legitimate session is given another chance to receive the service if it is dropped by the DDOS resilient scheduler.
DAT(Defence against tilt DDOS attack)	This approach monitors user's features like traffic volume, session behaviour etc. throughout connection session to determine whether users is malicious or not.	For different users' behaviours DAT provides different services that may sometime prevent legal user for appropriate service.
Speak up	The goal of this mechanism is that good client crowd out the bad ones there by capturing a much larger fraction of server resources. This mechanism encourages all clients to send high volume of traffic.	In this approach, it is assumed that server will somehow detect whether or not it is under attack.
DOW(Defence and Offense wall)	This approach uses to speak up mechanism with anomaly detection method based on k means clustering. Their detection model drops suspicious sessions while speak up encourages more	This mechanism is too resource consuming to be implemented.

	legitimate sessions.	
CAPTCHA	This approach divides attack traffic from normal by authenticate them using different questions images etc.	Requiring users to solve puzzles to authenticate themselves introduce more delays to legitimate users.
Admission control and Congestion control	In this approach, admission control is used to limit the number of concurrent client served by the online services by port hiding. Then they perform congestion control to allocate more resources to good client by setting client priority level.	This mechanism requires challenge server which may be the target of attacker.

Table I Comparison of Different Mechanisms

III. RESERCH PROBLEM FORMULATION AND PROPOSED WORK

Problem formulation

There are different types of DDOS attack as discussed above.

1. Layer 3: IP attacks on the network bandwidth
2. Layer 4: TCP attacks on server sockets
3. Layer 7: HTTP attacks on web server threads
4. Layer 7+: Web application attacks on CPU resources

While examining DDOS attack, we all refer the various layer of OSI model;especially focus is on the seventh layer, the application layer. This layer provides an interface to end user tasks and facilitates different applications and programs.
As per survey, total application layer attacks increased from 2011 to 2012 is 42.97%.

Fig II Trend of Application Layer Attack [13]

In application layer DDOS attacks particular HTTP flooding attacks are mostly used by attacker as per survey.

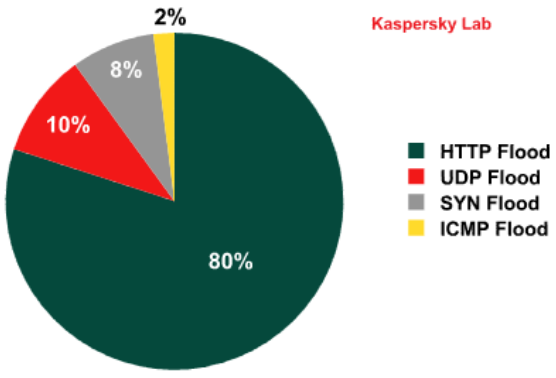


Fig III Trend of different kind of DDOS attacks [13]

Because of increasing trend of HTTP flooding attacks it is necessary to defend against such attack. HTTP flooding attacks are generally on web server. Web server provides various kinds of services to the users. So it is necessary that these services are available for legal users.

Current situation and Scope of my Research

Current situation: There are many defense mechanisms against application layer DDOS attack. Some mechanisms only detect attacks, some mitigate the effect of the attack some mechanisms did both detect and mitigate DDOS attack [7][8] but still 2014, DDOS attack is increasing day by day and there is no such effective mechanism against DDOS attack.

Scope: Web server is used to provide services to users. However, if web server is down then users are denied to get services or information. Scope of my work is to increase availability for legal users using effective detection and mitigation mechanism against DDOS attack. Most of attackers use tools to generate massive traffic. So, here I provide such a mechanism that can detect DDOS attack, differentiate attack traffic against normal traffic and mitigate the effect of DDOS attack.

Proposed Solution

There are many approaches used to detect and mitigate the effect of DDOS attack. Different approaches have different limitations like legal users have to wait more time for service, high false positives, high false negatives, more time consuming and complex, require more memory usage etc. Here, I propose one light weight mechanism to detect and mitigate the DDOS attack against web server. My proposed solution divided into three phase.

1. Identify DDOS attack.
2. Differentiate DDOS attack traffic from normal traffic.
3. Mitigate the effect of DDOS attack.

First phase is to identify DDOS attack. It is a very important stage to defend against any attack. Attack should be identifying as early as possible before it could lead noticeable damage. If we identify attack after its damage then it is need less. So, my focus is to identify DDOS attack as early as possible before further steps.

Second phase is to differentiate DDOS attack traffic from normal traffic. In today's days, attackers use BOTNET machines for attack. This zombie machines (compromised systems)are available easily on internet in few dollars. So attackers use thousands of such machines for attack against victim (web server). So, my focus is to differentiate that traffic from normal Traffic.

Third phase is to mitigate the effect of DDOS attack. After identifying and detecting the attack, next step is to mitigate the effect of this attack. So, my focus is to increase the availability of web server for legal users by mitigate the effect of DDOS attack.

Proposed Flow Diagram

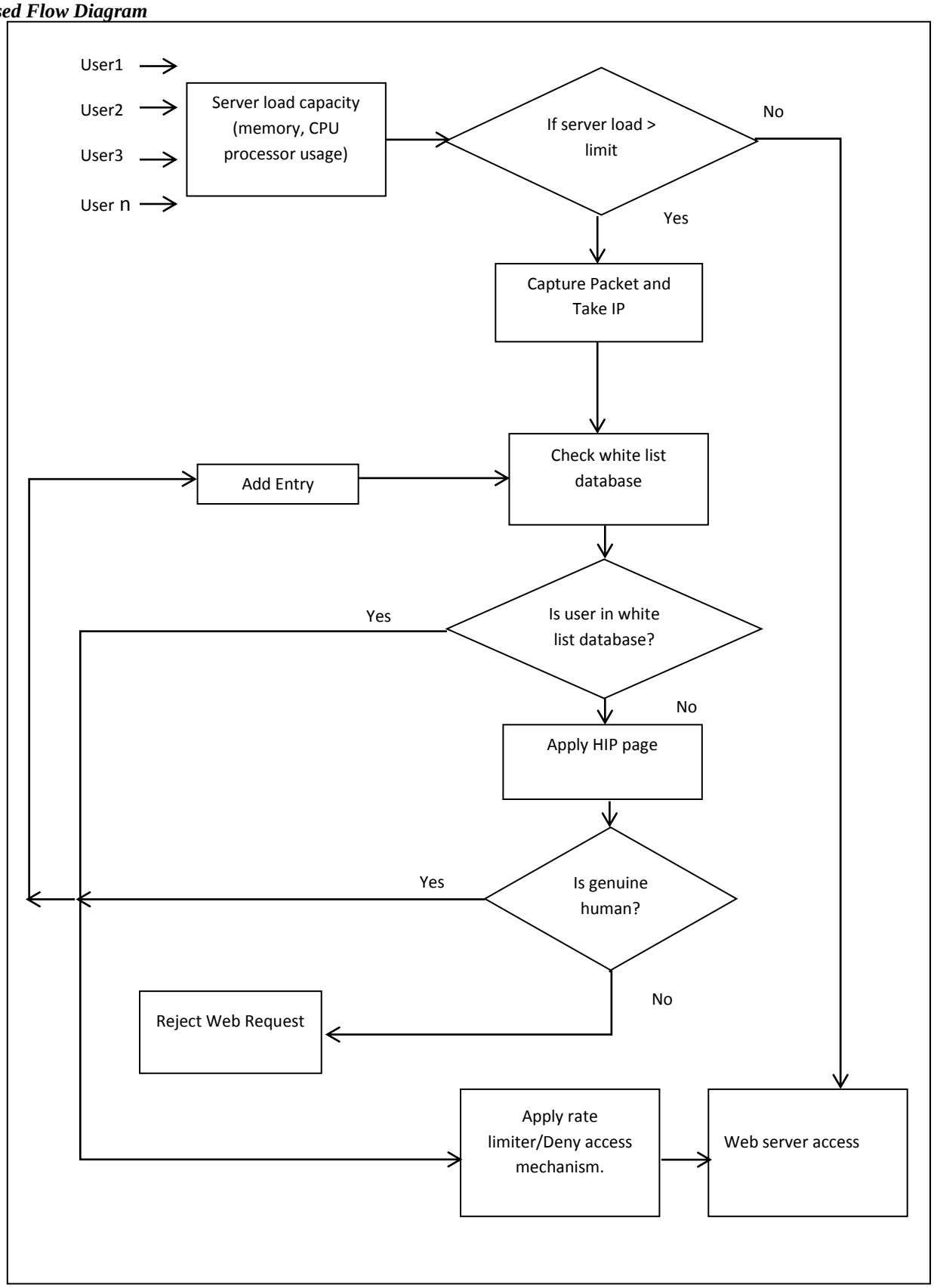


Fig IV Flow Diagram

Functional Description

- First of all when web request come to web server, my proposed mechanism will check if server-load is high or not. Server load is compared with predefined limit. This limit is depends on different kind of servers its capacity and applications running on it. Memory and CPU processor usage parameters will used to measure server load.

- If server load is not high and below the limit then it is not necessary to detect DDOS attack and resolve it. However, if server load is high then packet will captured and looking for IP addresses.
- These IP addresses will be checked in White list database. If IP address is available in white list database then it will go to the next phase. However, if IP address is not available then it will go to HIP (Human Interaction Page).Initially white list database will empty.
- My mechanism will use HIP (Human Interaction Page) to differentiate attack traffic from normal traffic. This is a main step of my mechanism because attackers in this days use zombie machines for attack. In this page, user has to interact and give answers of image question etc. If user can't give answer successfully than web request of that user will be rejected. However, if user give answer successfully than that user's entry will be added in white list database so next time that user does not need to pass through HIP.
- Users which are available in white list database and users who passed successfully through HIP will not directly get access of webpage because worst case possibility that white list database IP may be used as zombie machine or as a spoofed address. So my mechanism will use rate limiter or deny access mechanism which will check requests from particular IP in particular time. So, if that request rate are higher than this mechanism will deny access to that user for some time. After that time if user will still available than it can get access of web server.
- In this way my proposed mechanism will work and try to improve availability of webserver for legal users.

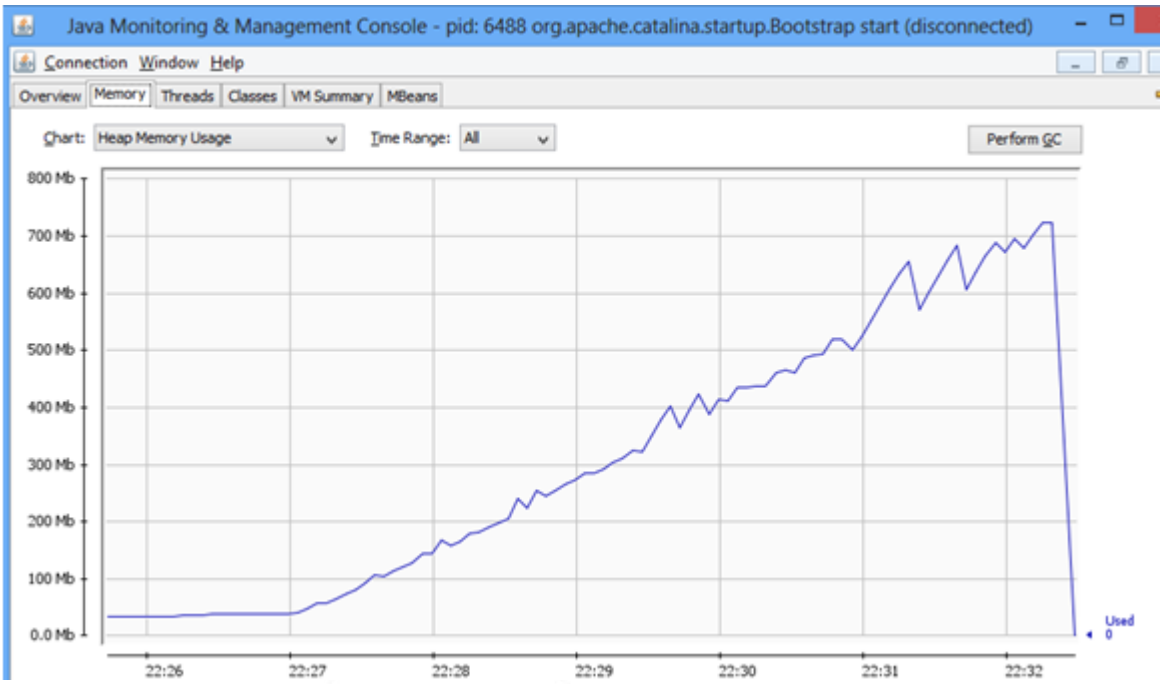
How can be my approach is different from other mechanisms?

- There are many existing mechanisms to defend against DDOS attack. To protect webserver, most of existing mechanisms focus on either to detect DDOS attack or to prevent DDOS attack. Here I am proposing light weight hybrid mechanism that can identify, detect and mitigate the effect of DDOS attack.
- Most of existing mechanisms use system logs, or signature based mechanism, or behavior based mechanism, or traffic based mechanism, or creates normal user profile and compare it with real time user profile to detect DDOS attack. Whereas, my mechanism will measure server load capacity and limit the capacity for normal webserver access. Server load is automatically continuously observed using Linux crone job.
- In modern internet world, attackers use zombie machines instead of spoof IP. So it is necessary to identify those machines traffic. Existing mechanisms tried to solve this issue but it sometime compromise the legal user time. In our proposed approach, we are using HIP to differentiate attack traffic from normal traffic. Attack packets generated with different tools using zombie machines can't give answers and successfully interact. So my mechanism can differentiate attack traffic from normal traffic in this way. Legal users don't have to wait to access to server because if particular user entry in white list database than that users have no need to pass through HIP.
- For more security, my proposed approach use rate limiter/deny access mechanism to control the access of web server of particular user so web server can't be overwhelmed and become unavailable.
- In this way, I have proposed hybrid mechanism that work differently than existing mechanisms to increase availability of web server for legal users.

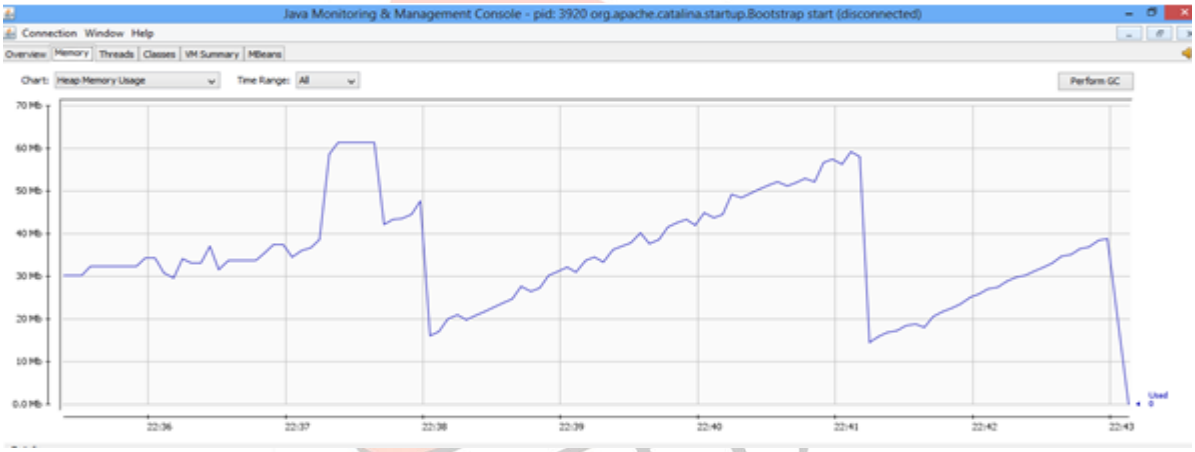
IV. RESULTS AND PERFORMANCE

I have used java Monitoring and Management console (JConsole) for results and performance. JConsole is a graphical tool for monitoring java virtual machine. JConsole is a part of jdk and it can provide the information about performance and resource consumption of application running on java platform.

Load without applying my mechanism vs Load with applying my mechanism(single attacker)

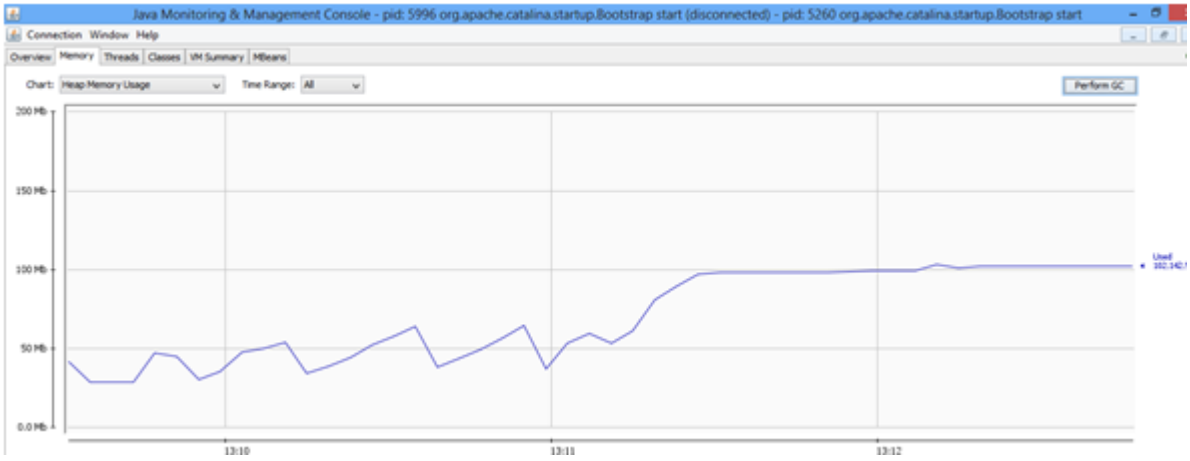


Server load after applying my mechanism (Using single attacker)



Load without applying my mechanism vs Load with applying my mechanism(multiple attacker)

Server load after applying my mechanism (Using single attacker)



- Above two results shows the effect of my mechanism. In this way, The availability of web server increased.

V. CONCLUSION

As discussed in this PAPER, application layer DDOS flooding attack is still biggest concerns for security professionals and internet world. DDOS flooding attacks are made possible by inherent flaws in the internet design and the lack of proper security mechanisms in numerous computer systems. There are millions of computers being added to internet every year. We can be sure that there are not going to be adding millions of new system administrators for these new hosts. This is an already highly target reach environment for attackers to scout for system that can be used as DDOS attack agent. So, this problem is only going to be increase more severe in future. In this report I have proposed light weight hybrid approach to detect and mitigate the effect of DDOS attack against web server. This mechanism identify HIP for differentiate DDOS attack traffic from normal traffic and rate limiter/deny access mechanism to restrict the access of legal user so web server can't be overwhelmed and increase the availability of web server. My results shows server load will decreased from 2gb to around 100mb for mutilple attacker.

VI. ACKNOWLEDJMENT

Apart from the efforts of me, the success of any task depends largely on the encouragement and guidelines of many others. I take this opportunity to express my gratitude to the people who have been instrumental in the successful completion of this work. I would like to express my deepest gratitude to ShriAdityaSinha Sir, Team coordinator, C-DAC Pune, without his encouragement and guidance this work would not have materialized. I would like to show my greatest appreciation to my external guide Prof. Hasmukh Patel, HOD CE, LCIT, Bhandu. I can't say thank you enough for his tremendous support and help. I feel motivated and encouraged every time. I take immense pleasure in thanking Mr.Naresh Kumar Gardas, Course Coordinator, C-DAC, Mr.Jiggyasu Sharma, Project Engineer C-DAC and Mr.AshwinKevat, Coordinator, GTU for having permitted me to carry out this work and for all valuable assistance in this work. Finally, yet importantly, I would like to express my heartfelt thanks to my beloved parents for their blessings, my friends/classmates for their help and wishes for the successful completion of this work.

REFERENCES

[1] B.B.Gupta,R.C.Joshi, Manoj Misra. Distributed Denial of Service Prevention Techniques. IEEE Journal Article -2010, 268-276.

[2] Saman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE Paper-2013. A Survey of Defence Mechanisms Against Distributed Denial of Service (DDOS) Flooding Attacks, 1–24.

[3] P.J.Criscuolo, Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), Lawrence Livermore National Laboratory, February 14, 2000.

[4] Yang-Seo Choi, Jin-Tae Oh, Jong-Soo Jang. Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention. Information Technology Convergence and Services ITCS 2010 2nd International Conference on, 1–6.

[5] Sujatha Shivabalan, Dr P J Redcliffe. A novel framework to Detect and block DDOS at Application layer. IEEE Journal Article-2013, 578-582.

[6] A.Ramamoorthi, T. Subbulakshmi, Dr. S. Mercy Shalinie. Real time detection and classification of DDoS attacks using enhanced SVM with string kernels. 2011 International Conference on Recent Trends in Information Technology ICRTIT, 91–96.

[7] S. Renuka Devi, P. Yogesh.An Effective Approach to Counter Application Layer DDoS Attacks.IEEE Journal Article - 2012(July), 0–3.

[8] Subramani rao Sridhar rao. Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis.2011- SANS Institute InfoSec Reading Room.

[9] Qijun Gu, Peng Liu. Denial of Service Attacks. Department of Computer Science Texas State University – San Marcos School of Information Sciences and Technology Pennsylvania State University Denial of Service Attacks Outline, 1–28.

[10] Yi Xie, Shun-Zheng Yu. A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors. IEEE/ACM Transaction on Networking, FEBRUARY-2009.
[11] J. Mirkovic and P. Reiher. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communications Review, April 2004, 39-53.
[12] T. Peng, C. Leckie, and K. Ramamohanarao, Survey of network-based defense mechanisms countering the DOS and DDOS problems, ACM Comput. Surv, Article 3, April, 2007
[13] RioRey, Inc. 2009-2012, RioRey Taxonomy of DDoS Attacks, RioRey Taxonomy Rev, 2012. http://www.riorey.com/x-resources/2012/RioRey Taxonomy DDoS Attacks 2012.
[14] http://www.sans.org/reading-room/whitepapers/detection/denial-service-attacksmitigation-techniques-real-time-implementation-detailed-analysi-33764, 12th Dec, 2013
[15] http://resources.infosecinstitute.com/layer-seven-ddos-attacks, 12th Dec, 2013.