

# TBDA-Traceback Based Defence Against DDoS Attack

Akash Naykude<sup>1</sup>, Sagar Jadhav<sup>2</sup>, Krushna Kudale<sup>3</sup>, Sumaiyya Shaikh<sup>4</sup>, Yogendra Patil<sup>5</sup>

<sup>12345</sup>S.B.P.C.O.E. Indapur,

\*\*\*

**Abstract** - Now a day internet use is increased rapidly, and business, organizations, industrial and many more data and information needs to be secure in real. In networking field communication and transmission of data from one side to another side is very common thing. But Distributed Denial-of-Service (DDoS) attacks are very harmful in network and security. A DDoS attack is responsible for unavailable a machine or network resource to its connected users or clients. DDoS attack also able to do reduction in the efficiency or capability of the server for performing its work. That's why DDOS attacks are very challenging issues in today's world. The problem is increases when spoofed IP addresses are present in the attack packets. In order to solve this critical situation of problem, we developed a new mechanism to reduce the impact created by DDoS attacks. Sometimes, even if the attacking traffic can be filtered by the victim side, here also the attacker may block the access of the victim by consuming the computing resources. It consumes a large amount portion of the bandwidth of the victim Network or machine. This research paper is proposes a Traceback-based Defense against DDoS Attacks (TBDA) approach to resolve this problem very goodly. In this paper, we designed one technique that is impressively filtered out the majority of DDoS attack traffic. So, our main objective or intention for this work is to improving the overall performance and quality of the appropriate traffic and also minimise the attack traffic to maintain the connection of service for better communication. **Key Words:** DDoS Attack, IP Spoofing, IP Traceback, Packet Filtering, Traffic Control.

busy long time. This is example simply called a *denial of service* attack.

We see some attacks happened in previous years one by one. In February of 2000, one of the first major DDoS attacks was done against Yahoo.com website. In this attack what happened is that the Internet was getting off for about 2 hours continually [10]. Simple strategy of Distributed Denial of Service (DDoS) attack is that it uses many computers or machines IP'S to launch a large scale coordinated DoS attack against one or more targets PC'S. DDoS attack has the capability to slow down or break down victim's computing and communication resources within a short period of time. The Distributed Denial of Service (DDoS) attack is also a bandwidth attack, where attack traffic is directed from multiple distributed sources, that's why the attacking power of a DDoS attack is based on the huge number of multiple sources [11]. Hence, the DDoS attack is more powerful and it can be consist of all types of traffic to the victim or that particular user's network connection and communication.

In this study, we propose a distributed system to detect and avoid to a large DDoS attacks. Actually the most common DDoS attacks target is the computer networks bandwidth or connectivity and our goal is to recover or avoid these types of situations or conditions very simply. In Section II we described related work, in which we describes what type of work and solution is implemented in this paper. In Section III we present DDoS Defence System overview. In Section IV we present Image Processing which is for more deep study in sending simple request to a server. In Section V we described Classification in DDoS. In Section VI we described Experimental Results.

## 1. INTRODUCTION

First of all, DDoS is nothing but Distributed Denial of Service, which is type of attack that utilizes multiple distributed attack sources. Basically, the attacker uses a large number of controlled agents or slaves also sometimes referred to as zombies, distributed in different locations to launch a large number of DoS attacks against a single target or multiple targets. For more clarification, consider one example related to DoS attack. Suppose we want to make a telephone call, but sometimes we are not able to connect. It will happen on major special holydays or in crowd. Actual reason behind it is that telephone system is designed to handle a limited number of call requests at a particular time. Suppose that an attacker wanted to make the telephone system unusable by customers or users. Making this repeatedly (call after call) is an attempt to make all circuits

## 2. RELETED WORK

We don't have more ideas and solutions against the DDoS attacks problem but in this paper we present some structure and solutions to avoid the DDoS attacks and analyze and classify the solutions to the DDoS attacks easily. Using total concept of each solution, we understand about the effectiveness of the solutions and our main purpose is to clearly describe the existing problems. So that why, a better way for understanding of DDoS attacks can be achieved or obtained from more efficient defense mechanisms systems.

The DDoS defense mechanism is divided into major three parts [14]. These three parts are nothing but: Survival

Mechanisms from DDoS, Proactive techniques against DDoS and Reactive Mechanisms against DDoS [6]. The distributed behaviour and working of DDoS attacks makes them extremely difficult to detect or traceback and defend. Attackers normally use spoofed or we also called as fake IP addresses in order to hide their own true identity and information, which makes the traceback or detection of DDoS attacks even more and more difficult.

There are lots of attacks had been launched in different-different organizations since summer of 1999 [1]. See, in February 2000, most famous site Yahoo.com is in under attack of DDoS for near about 2 hours. Also in [1]-[9] stated that in October 2002, several root servers are get shut downed for an hour. The region behind is that DDoS Attacks [1]-[10]. Another big DDoS flooding attack was happened in February 2004, on SCO group website [1]-[11].

So that's why it's important to defence against this type of attacks in real activity. When an attack is detected and recorded, the next thing is that to find out who is the originator behind this attack. This turns out to be a really hard problem in the Internet. But no need to worry about that because the solution is given in this research and also it is helpful for us to defeat DDOS.

### 3. DDoS DEFENCE SYSTEM

At the time of launching an attack, the attacker can include spoof IP addresses in the attack packets to hide their own identity for being traced and blocked from anyone, so as to continue its attack one victim. The source address being distributed along the large amount of different spoofed addresses and it uses some detection tools to identify the traffic problems [12].

We developed one system which is very strong and faster to detect a DDoS attack very easily. Attacker uses various IP addresses to do attack and jam the server or slowing down the server. But Our DDoS detection and defence system is able to prevent and avoid attack. So, by using previous paper and our research we implemented this project or system successfully. Now it's time to know more about DDoS Attack and DDoS detection and defence System.

One figure include in this section which is DDoS defence system, it is a main working and architectural flow diagram which we have implemented. Look, In order to design a strong and effective DDoS defense mechanism, we done an intensive survey has been proposed on the DDoS attack as well as its existing solutions. Throughout the study, we discover that by activating this block system into our machine we can able to avoid it.

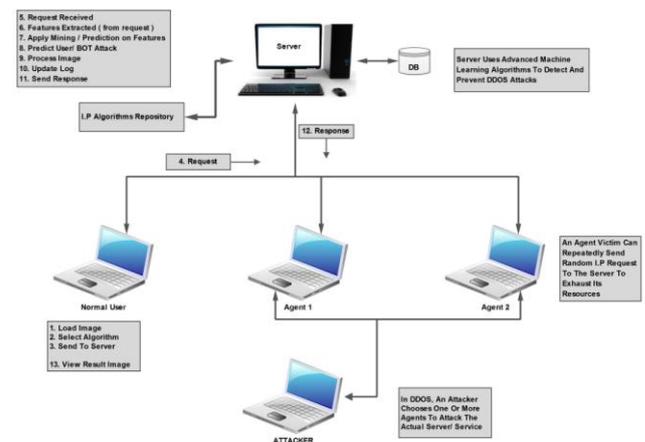


Fig -1: DDoS Defence System

See, the attacker communicates with many numbers of masters to recognise which agents are running on that time, when to schedule attacks for completing the target, and when to upgrade particular agents. Usually, attackers will try to place the master software agent on a specific router or network server which can be able to handles large amount of traffic. That's why they make it more complicated to identify messages between the master and agents. These users of the agent systems are typically have no knowledge that their system has been compromised and considering that they are now part of DDoS attack. When involving in a DDoS attack, each and every agent program uses only a small amount of resources like both memory and bandwidth also [2].

In the figure 1, see there is one client or normal user, one server and many agents with one attacker. Now, this attacker is going to make a feck requests by using these agents and going to slow down and mix with normal client and servers connection. But in our developed system server in more powerful to identify that which is normal client and who is attacker. After that it blocks IP address of that attacker and it's done.

The client under attack is defined as *primary victim (Masters)*, while the hosts used to launch this attack are often called *secondary victims (Agents)*. The use of secondary victims in performing a DDoS attack provides the attacker with the ability to create and perform a much larger and more disruptive attack, while making it more difficult to track down the original attack source.[9].

### 4. IMAGE PROCESSING SYSTEM

In this section we described about image processing algorithms or functions which we are used in this system for just forwarding simple request to the server. Need of this technique in our project or system is that just sending image as request to server for processing it. That's why we are not

implemented as well as required more image processing algorithms for our project. Those algorithms are following:

#### 4.1 GreyScale

This is simple image processing algorithm which is commonly used for image without apparent color. The darkest and more possible color is black, which is total absence of transmitted or reflected light. RGB means RED, GREEN and BLUE colors. By using this RGB all colors get creates. This GrayScale image is also called as black-and-white image. Conversion of Colored image into GrayScale image is a task of server in this project.

#### 4.2 Thresholding

Thresholding is a one of the simplest method for image segmentation. From a GrayScale image, thresholding is used to create binary images. It replaces each pixel in an image with a black pixel if image intensity is less than some fixed constant or white pixel if the image intensity is greater than that constant. Color image can also able to convert into a threshold. The HLS and HSV color models are mostly used.

#### 4.3 Blur

This one is used for creating an image that image does not represents single instance of time. Fast moving object etc. comes under this type of image conversion. Means image get created in this shade is blur or motion blur. Because of the effect is caused by the relative motion between objects, motion blur can be used for creating these types of images.

These types of image conversion algorithms applied in our system for making system more useful also. By using these techniques we can also do image blur, threshold and GrayScale with security.

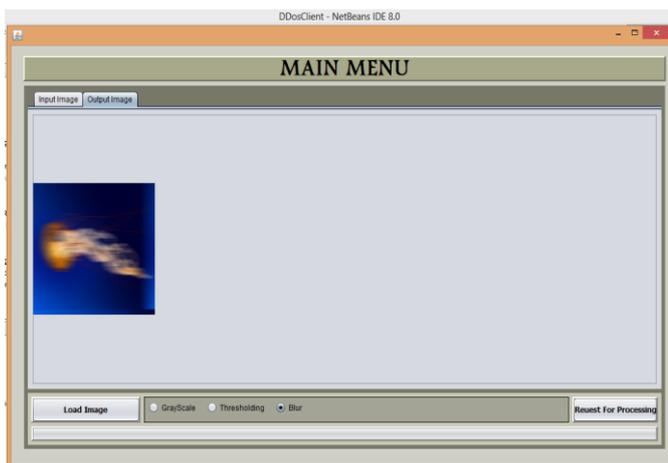


Fig -2: Image Processing Methods

See the figure 2, it shows that the DDoS defence system's image processing and actually what will be the way or process is happened in image request in project. It also shows that how a request is going to send by client to server by using necessary button. Working is also simple, we need to just load image, select method and request for processing,

after that server get on work and process image and send back to the client if it is normal client or user only.

### 5. DDoS ATTACK TAXONOMY

In this section we described DDoS attack taxonomy or classification of DDoS attack. There are a many DDoS attack techniques and types [6][10]. We present taxonomy (classification) of the DDoS attack in figure 3. There are two main categories of DDoS attacks: Those are nothing but the *Bandwidth Depletion* and *Resource Depletion*. Here we see both categories one by one.

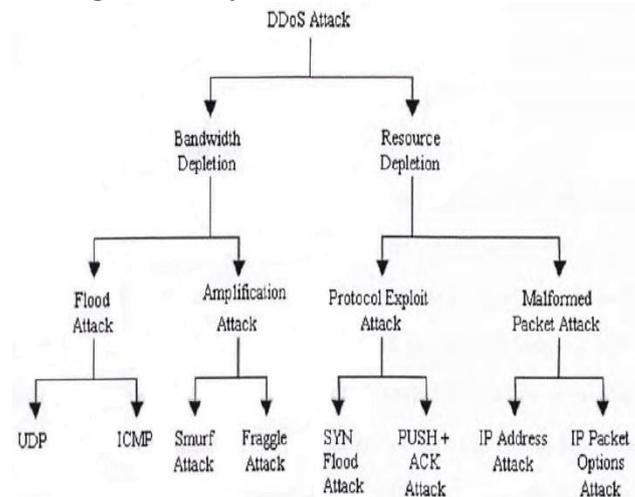


Fig -3: Taxonomy of DDoS attack.

#### 5.1 Bandwidth Depletion Attacks:

This mechanism is designed to mix out unwanted traffic into the victim network rapidly. This includes two more main classes of DDoS bandwidth depletion attacks. One of them is flood attack and it is more commonly applied. In this flood attack, it involves the agents or zombies for sending large amount of traffic into a victim system, for purpose of accessing large area of the victim system's bandwidth. Another attack is amplification attack for DDoS. In this attack, attacker or the agents (zombies) sending messages to a broadcast IP address and a reason behind it is that to amplifies malicious traffic that reduces the victim system's bandwidth [4]. The DDoS uses these both attack for access the connected network of user for attacking.

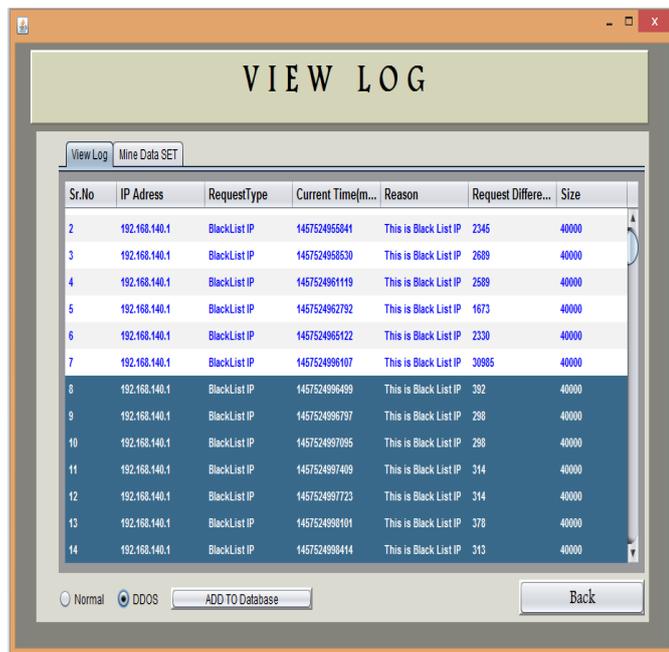
#### 5.2 Resource Depletion Attacks:

A DDoS resource depletion attacks having capability of access a network resources of appropriate user or victims machine [14]. That means automatically server is get slow down. Sometimes the attacker sending packets to server for purpose of get misuse of network protocol for communications and sending bad packets that accessed well in network resources.

## 6. EXPERIMENTAL RESULT

In the experimental result, first of all we need to send a request from client to server. For that purpose we used some image processing algorithms. Client sends request for processing it from server. So client sends one image for Grayscale, thresholding or blur. We are implementing just DDoS attack detection system that's why we are not going to require more image processing algorithms because few algorithms are sufficient to run the system and detect attack.

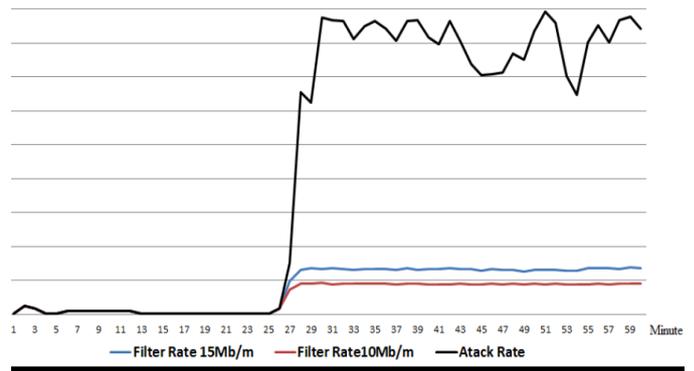
Now client is going to send request which we considered as image. Client loads image and sends it to the server by using one of the image processing function. Now server gets on work like analysing the requests and its time difference. Normal user can send 3-5 requests in one second [17]. But if more than 5-10 request are obviously attacker's requests.



Sr.No	IP Address	RequestType	Current Time(m...)	Reason	Request Differe...	Size
2	192.168.140.1	BlackList IP	145752495841	This is Black List IP	2345	40000
3	192.168.140.1	BlackList IP	1457524958530	This is Black List IP	2689	40000
4	192.168.140.1	BlackList IP	1457524991119	This is Black List IP	2589	40000
5	192.168.140.1	BlackList IP	1457524962792	This is Black List IP	1673	40000
6	192.168.140.1	BlackList IP	1457524965122	This is Black List IP	2330	40000
7	192.168.140.1	BlackList IP	1457524996107	This is Black List IP	30985	40000
8	192.168.140.1	BlackList IP	1457524996499	This is Black List IP	392	40000
9	192.168.140.1	BlackList IP	1457524996797	This is Black List IP	290	40000
10	192.168.140.1	BlackList IP	1457524997095	This is Black List IP	290	40000
11	192.168.140.1	BlackList IP	1457524997409	This is Black List IP	314	40000
12	192.168.140.1	BlackList IP	1457524997723	This is Black List IP	314	40000
13	192.168.140.1	BlackList IP	1457524998101	This is Black List IP	378	40000
14	192.168.140.1	BlackList IP	1457524998414	This is Black List IP	313	40000

**Fig -4: DDoS Attack**

See the fig. 4. Time difference is in millisecond [17]. Normal request is in between thousands milliseconds but other side, attackers time difference is in bellow five hundred milliseconds. Like this way detection process is work.



**Fig -5: DDoS traffic rate with and without using TBDA System.**

Our system is able to maintain view log for analysing requests and data sets. Also self-security and protection system for a admin to secure itself by using log in functionality. Various image processing activities implemented in system like Blur, Thresholding and GrayScale techniques.

This project is able to run on single laptop or computer. Also its able to run on two machines or three machines. But in that case these machines are in network like hotspot or in LAN connection [17]. One machine can hold client and admin module and another machine holds attacker to do attack. If requests are coming in large strength then server identifies attacker by using view log and declare it as an attacker. But image is not processed sent by attacker, server send same image to the attacker as it is without processing. And if it is a normal user request then server processes it as per requirement and send output to the client very faster way.

## 7. CONCLUSION

This paper describes deep information about Distributed Denial of Service attack. And for security purpose we developed one awesome system to traceback and defence against DDoS attack. The main this is that attackers request of processing is captured and does not processed. That means it is blocked without knowing them. For future work, we need to implement and evaluate the securing of the TDDA system itself.

In this paper, we have presented taxonomies or classification of DDoS attacks, an overview of DDoS attacks, DDoS attacks detection and defense schemes, and overall architectural view, Image processing with Experimental results and related terms. DDoS attack creates various types of issues related to our network communication and data transfer. Because of this, a possible solution is needs to be

developed to detect DDoS attacks. The key behind it is that, we improved the quality, for network servers and help to solve the DDoS problem and to facilitate more comprehensive solutions.

## ACKNOWLEDGEMENT

Distributed Denial of Service attacks can cause several problems like, disable server, access network resources and bandwidth, etc. DDoS attacks are not only a serious problem for the wired networks but also for the wireless connection. DDoS attack affects on both side, victim and network link. For these purposes we need to survive from DDoS attack for better work and effective communication between users and servers. For more security purposes we developed one faster system called as TDDA System.

## 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] Ho-Yu Lam, Chi-Pan Li, Samuel T. Chanson and Dit-Yan Yeung Department of Computer Science Hong Kong University of Science and Technology Clear Water Bay, Kowloon, Hong Kong "A Coordinated Detection and Response Scheme for Distributed Denial-of-Service Attacks".
- [3] Zhenhai Duan, Member, IEEE, Xin Yuan, Member, IEEE, and Jaideep Chandrashekar, Member, IEEE "Controlling IP Spoofing Through Inter-Domain Packet Filters".
- [4] Yulong Wang and Rui Sun State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China "An IP-Traceback-based Packet Filtering Scheme for Eliminating DDoS Attacks".
- [5] Robert Stone, UUNET Technologies, Inc. robert@uu.net, "CenterTrack: An IP Overlay Network for Tracking DoS Floods".
- [6] Christos Douligieris and Aikaterini Mitrokotsa, department of informatics, university of piraeus, piraeus, greece, "DDoS attacks and defense mechanisms: a classification".
- [7] Christos Douligieris \*, Aikaterini Mitrokotsa, Department of Informatics, University of Piraeus, 80 Karaoli and Dimitriou Str, Piraeus 18534, Greece, Received 9 October 2003; accepted 13 October 2003, Responsible Editor: I.F. Akyildiz, "DDoS attacks and defense mechanisms: classification and state-of-the-art".
- [8] Valentin Razmov, (valentin@cs.washington.edu), Computer Science and Engineering Department, University of Washington, May 10, 2000, "Denial of Service Attacks and How to Defend Against Them".
- [9] Monowar H. Bhuyan, 1Department of Computer Science & Engineering, Tezpur University, Napaam, Tezpur-784028, Assam, India, "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions".
- [10] Stephen M. Specht, Ruby B. Lee, Electrical Engineering, Princeton University Princeton, NJ 08544, "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures".
- [11] John Ioannidis, Steven M. Bellovin, smb@research.att.com, AT&T Labs Research, "Implementing Pushback: Router-Based Defense Against DDoS Attacks".
- [12] Vahid Aghaei-Foroushani\* and A Nur Zincir-Heywood, "IP traceback through (authenticated) deterministic flow marking: an empirical evaluation".
- [13] Vahid Aghaei Foroushani, A. Nur Zincir-Heywood, Faculty of Computer Science, Dalhousie University, Halifax, NS, Canada, vahid@cs.dal.ca, "TDFA: Traceback-based Defense against DDoS Flooding Attacks".
- [14] Darshan Lal Meena, (Ph.D Scholar) Department of Computer Science, MP, Bhoj Open University, Bhopal (MP) -462016 IND. "A Survey on Different Solutions to DDoS Attacks".
- [15] Divya Bhavasar, Master of computer engineering, parul institute of engineering and technology, india, "A survey on distributed denial of service attack and defence".
- [16] A.John1, T Sivakumar.2, Department of Computer Science, Ramanujam School of Mathematics and Computer Science Pondicherry University, Puducherry, India, "DDoS: Survey of Traceback Methods".
- [17] Andrey Belenky and Nirwan Ansari, Senior Member, IEEE, "IP Traceback with Deterministic Packet Marking".