I J C T A, 9(11) 2016, pp. 5093-5102

A REVIEW ON DETECTION AND MITIGATION TECHNIQUE OF DISTRIBUTED DENIAL OF SERVICES ATTACK

Shymson Likmabam[*] and Rajendra Aaseri[**]

Abstract: Attacks of DDoS are common specific attempts to drain out the bandwidth of legitimate users and denied the given services. Vulnerable are found in traditional architecture which can intrude by DDoS attack. In order to attack in large number, attacker has been set up a Botnet or attacking network. These lead to various type of attack in the internet. In this paper, there are various types of attacking technique that we surveyed to study there countermeasures. And try to add some other technique regarding mitigation of DDoS attacks.

Key Words: distributed denial of service (DDoS), denial of service (DoS), Botnet, detection mechanisms andconcept of http count and CAPTCHA technique.

1. INTRODUCTION

Now a day, the most harmful attacks which are more threaten to the user and to the server are Denials of service (DoS) attacks, which denies the legitimate user to use the resources. These types of attack are extended up to large scale and which harm the large amount of data and information. This consists of number of infected systems which group together and perform the attack. There are lot of activity lead to panic in an organization and society.

Sometime websites are down due to server down but it might be attacked by DDOS. DDOS attack generally generates with the internet hackers create a virus in a huge number of computers without acquiesce of the customers. These infected computers form an attack network which controlled remotely to targeted victim.

Any electronic system running an IP, it run the malicious software in the system and infected them with bot. These allow the victim to automatic installed and the Trojan horse program are running automatically from any malicious websites. This group of infected system are under the control of a bot herder is known as a botnet. Bots are different from viruses; they do not show any sign of infection or their stay in the system, thereby keeping the user unknowingly of these malicious downloaded files and without consciously take part in the gathering of the bots to form the army of botnets. These infected clients are taking part in the DDoS attack without the consent of the user.

[*] Department of Computer Science and Engineering Lovely Professional University Jalandhar, Punjab, India
shym004@gmail.com

[**] Department of Computer Science and Engineering Lovely Professional University Jalandhar, Punjab, India
rajendra.17890@lpu.co.in

Bot-master or the bot-herder controlled the bots through the command and control server. Bot-herder sends the instruction and any updates to the bots. Through these main system or human user, they can add some new features and program-code to fill-up their defects and rupture the defense algorithm. Bots are hard to detect because of frequent updating nature.

Many web services are exploiting by the DoS attacks to specific target [1, 2, 3, 4, 5, 6]. Legitimate user are block to user their services and network resources and abnormal services are occur by sending the malicious code to compromise the targeted system and flood the network to reduces the connection bandwidth of the legitimate users. These kinds of event are leading to crash the system and harm the services

There are numerous DDoS attacks in the internet real world, they tried to pin the target system and consume the resources [7, 12].These tasks are done by those zombies system or those compromise computers under the control of bot header over the internet. And they utilize the vulnerable of these systems. By using their loophole attacker insert the malicious code and some other hacking tools to control these systems and form the "zombies". Zombies are those systems which are compromise by the attacker and they help in DDoS attacks.

First, attacker tries to confuse the victim by sending malicious code and running some application on the victim's system. (i.e., vulnerability attacks [8]).

In the Second method, flooding in application layer, network layer, and transport layer are lead to flooding attacks [8]. The attacker tries to do these events which are given below: (i) Connection bandwidths of the legitimate user are exhausting and resources of the networks or (ii) exhausting the system resources like CPU, memory, disk, database etc.

Launching of DDoS attacks are more frequent, and they are well organized to control the zombies system through remotely. These could be from different part and we called that distributed Zombies. These large number of zombies are sending large number of request packet to the targeted system and lead to slow down the services or could crash the system also.[8][9][10]. Recruiting of these zombies are done through virus, Trojan horses or worms [11]-[13], and hard to identify this type of attack [14].

Indirect communication of zombies and handlers and revealing their identities are major focusing area, these are working under the Internet Relay Chat (IRC) [9].

2. CLASSIFICATION

(a) ***Motivation of DDoS attacks:***

1. Gaining money.
2. Slowing down performance of the networks.
3. For Revenge purpose.
4. Belief of Ideological.
5. Showing their skill Challenge.
6. Unavailability's of services.
7. Cyber warfare.

(b) ***Classification base on degree of attacks:*** DDoS attacks are classifies into various category; base on the degree of automation they are automatic, semi-automatic, and manual attacks.

Automatic attack: Sophisticated tools are used to support attacker to launch the attacks and it reduces the human effort. Some parameters are configured by the attacker and others are done by the tools.

Semi-automatic: here it is almost similar with automatic attacks.

Manual attacks: in manual attacks numbers of configuration are completed by the attackers to launch the attacks like identifying the devices, port scanning, and construction of botnet and insertion of malicious code.

Zombies or agents are directly attack to the victim which is come under the direct attacks given in fig.1. But zombies are sending request packet to various compromised computer known as botnet. These botnet are used to carry the malicious packet to targeted system.

In fig. 2 shows the classification base on flooding which is used to slow down the network of the victim. Those attacks are ICMP flood, TCP flood, UDP flood.

(c) ***DDoS attacks architectures:*** There are three types of network architectures in DDoS attack: (i) the Agent-Handler architecture, (ii) Internet Relay Chat (IRC)-based architecture and (iii) the Web based architecture.

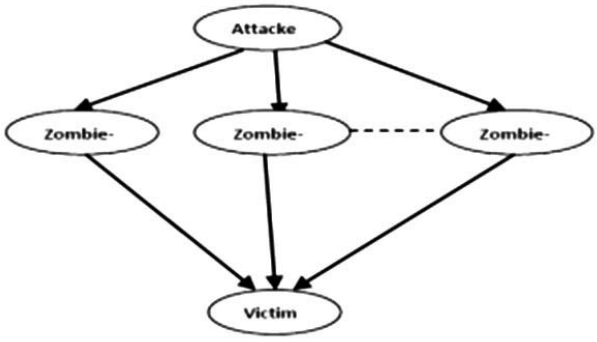

Figure 1: (a) Direct attack

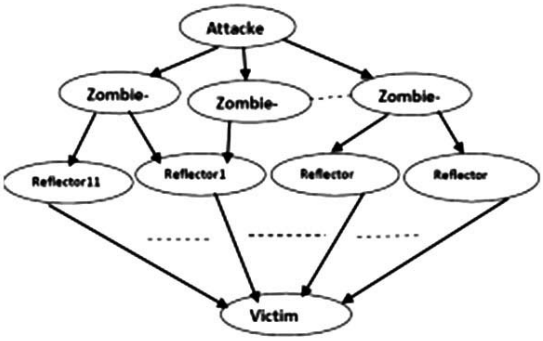

Figure 1: (b) Indirect attack

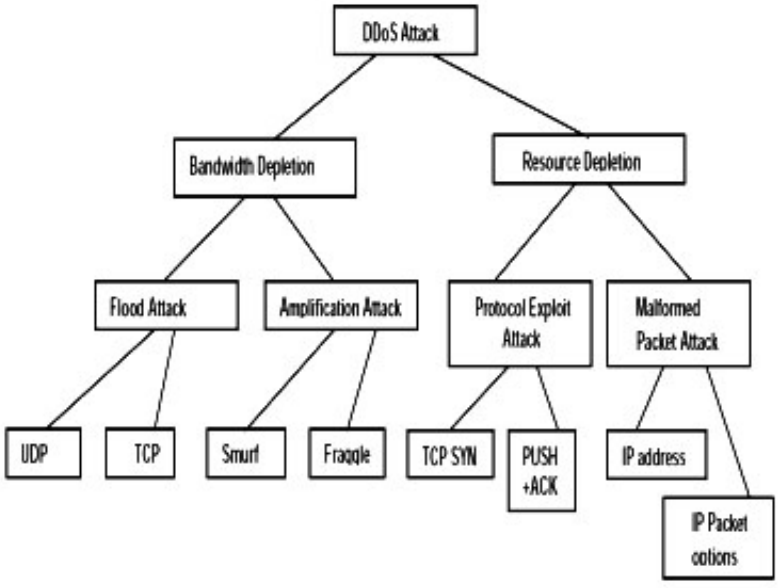

Figure 2: DDoS attacks Classifications

(i) *Agent-Handler Architecture:* The Agent-Handler architecture is also known as Botnet architecture, where the botnet are used to launch the attacks. Bot master control those zombies from botnet which include master, handler and bot. Shown in fig.3 handler are used to communicate indirectly through commands.

(ii) *IRC-based architecture:* The communication between the bot master and bot are done through Internet Relay Chat, sending command and other instructions. These hide the original address of the sources of the packet and the other information of the attackers. Text base command syntax protocols are used in IRC and they have defined their rule and regulation of the protocols. These commands are installs in the numbers of system and perform the communication. IRC are not strongly authenticated over the internet which can be used as public. IRC provide low latency, simple widely available anonymous command and controls shows in the fig.4.

(iii) *Web-based architecture:* In web-based architecture, the communication protocols used by the botnet are HTTP. They are difficult to identify the structure of their command and controls.

(d) **DDoS Strategy:** Fig.1 shows the component of DDoS attack. It consist of four steps which are shown in fig.5

1. *Identification of loophole in host:* Agents are chosen by the attacker in order to perform the attacks and those system which are no having antivirus or pirated software are vulnerable and easy to compromise it.

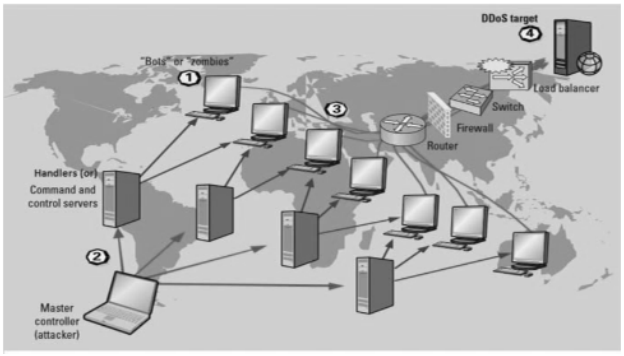

Figure 3:Agent handler Architecture Figure

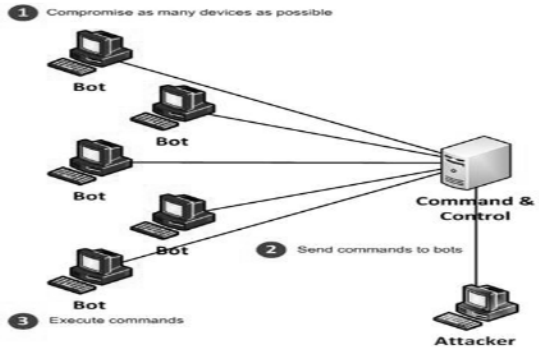

Figure 4: IRC- based Architecture

2. *Compromise:* Attacker used the security holes and vulnerabilities to install the attack code in the agent machine.

3. *Communication:* Attacker transmitted information with the handlers to identify the live agent. And various protocols are used to communicate among the attacker and handlers like TCP, ICMP, and UDP.

4. *Launching an Attack:* Before starting the attack, attackers choose the victim system. And during the attack it can adjust the feature of the attack like port number, Time to live, length, and types of attacks.

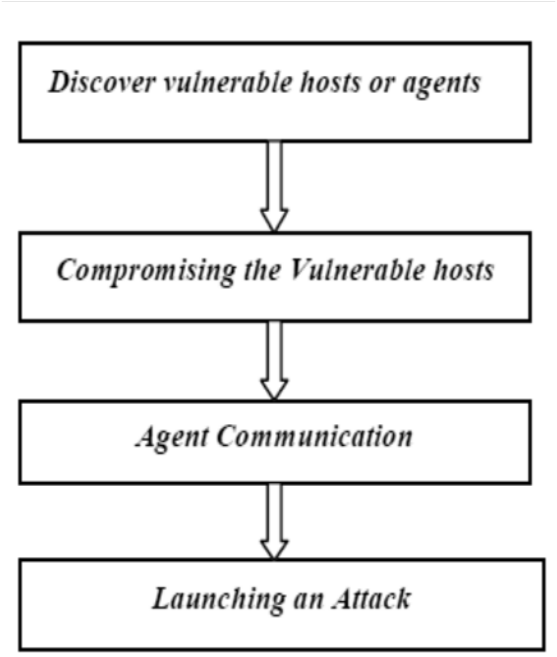

Figure 5: Steps of DDoS Attacks

3. DETECTION AND MITIGATION ARCHITECTURES

There is only one technique to fix the DDoS attack problem that is disconnecting the network otherwise it could not block the attack completely. During the DDoS attacks lots of resources are block such as bandwidth, CPU power, memory, processing time etc.

The main aim of many detection mechanisms are to DDoS attacks and stop as soon as possible.

There are four classes of DDoS schemes base on locality of deployment: (i) source-end (ii) victim-end (iii) core-end (iv) Distributed or hybrid defense mechanism. Advantages and disadvantage are discussed in the table 1.

(i) ***Source-end:*** To prevent the attack on users network sources-end defense mechanism are deployed. These filters or rate limit the malicious outgoing packet after identifies the malicious packet. This approach is best because it detects and blocks the attack at sources end and courses less damages.

(ii) ***Victim-end:*** Here the filtering and rate-limit incoming malicious traffic at the router. It provides web services by the network. It can easily classified whether its form online or offline by using misuse base detection or anomaly base detection.

(iii) ***Core-end:*** Router can identify the malicious traffic and rate limit in the network. Detection accuracy and bandwidth consumption are also balances and the traffic are aggregated both legitimate and attack packet at the router level. The rate limit of all the traffic is best.

(iv) ***Distributed-end:*** These mechanisms are deploying at multiple locations of sources, intermediate network or victim and they are co-operating each other. Detection strategy at end point can be best against DDoS attack. In the core end the rate limit are good detection rate, so the combination of these two methods could be more beneficial.

Table 1
Advantage and Disadvantage of DDoS Attack Architectures

Defense Method	*Advantages*	*Disadvantages*
Source-end	>legitimate traffic is experiences less damage	>Detecting at sources is difficult due to distributed nature.
	>less amount of traffic are check at sources and required few amount of resources are detected.	>deploying system at the source end is difficult.
Victim-end	>Due to the high rate consumption of resources, detection at router is easy.	>difficult in blocking of network bandwidth during DDoS attacks, victim resources.
	>resources are more secure in web server	
Core-end	>Collaborative operation provides more features in detection like track back.	>Deployment difficulty.
		>due to unavailability of scheme router fail to detected.
		>reconfiguration is required in all routers for implementation.
Distributed-end or Hybrid	>it sent the alarm signal while detection occurs at victim.	> required more cooperation.
	>it has more beneficial.	>Complexity and overhead are more due to distributer component.

4. HTTP COUNT AND CAPTCHA TECHNIQUE

Aim to mitigate the distributed denial of services attack base on IP blacklisting concept which will block all the blacklisted IP address. And http count technique will use inside the filter module that will determine the suspect and normal IP packet. After that the CAPTCHA technique will use to find out suspected IP packet are send by botnet or human.

Proposed mechanism is broadly divided into three folds, first we filter out the blacklisted IP address and those IP address from block IP ranges. In this experiment, take up the already available range of blacklisted IPs. IP addresses are blacklisted as they either cause IP spoofing or may have potentials of carrying out harmful activities. All the blacklisted IP addresses are updated in the bad-host file. These simple filters are unable to block IP addresses that have the capability of DDoSing. A dataset of blacklisted IP has to be maintained, every new entry of IP address are to be compare the dataset to check against it.

This type of attack is very difficult to handle as they can't be detected easily. The application layer DDoS (ALDDoS) attack uses legitimate http request and it is very difficult for the firewall and IDS system to detect. As these are considering only the ALDDoS attack, detecting mechanism and mitigate network layer DDoS attack are not considered. Proposed mechanism is broadly divided into three folds, first we filter out the blacklisted IP address and those IP address from block IP ranges. In this experiment, take up the already available range of blacklisted IPs. IP addresses are blacklisted as they either cause IP spoofing or may have potentials of carrying out harmful activities. All the blacklisted IP addresses are updated in the bad-host file. These simple filters are unable to block IP addresses that have the capability of DDoSing. A dataset of blacklisted IP has to be maintained, every new entry of IP address are to be compare the dataset to

check against it. These procedures are not effective when we have new entry having the ability of doing DDoS attack. The algorithm for blocking the known blacklisted IP addresses is given below.

BEGIN

1: Set up a default rules for accepting.

2: Observe the traffic flow through the network.

3: Consider all the ports that are monitored over the network perimeter.

4: Construct an IP tables along with ports.

5: Initialize the IP table with the default policy to accept.

6: Enable traffic to flow between the networks.

7: Check the bad-hosts file to identify the blacklisted IP addresses.

8: Update the blacklisted IP addresses to IP tables with action as block

9: Bypass the IP addresses that are not in the bad-hosts file

10: Clear all the policies and add the rules again with the newly entered IP addresses.

11: Add dropped IP addresses of the successive method of filtration to the bad-hosts file.

12: Repeat step 10 for every new entry in the bad-host file.

END

To cope up the limitations in the previous filtering mechanism, monitor the bypassed IP addresses http GET request rate. Every IP address http GET request is compared with the normal request rate. Any suspicious IP address having maximum variation in the http GET request is marked and sent for the next detection mechanism. Simple blacklisting of IP addresses are unable to filter out the malicious clients. So apply one more detection mechanism soon after the first filter.

The algorithm to count the http GET request and detect the suspected IP addresses is given below:

BEGIN

FOR each bypassed IP addresses

Monitor the IP addresses

Compute the Http count Count1 of each IP addresses

Compute the normal http count Count2

IF (Count1 $\leq$ Count2)

The request packet is coming from legitimate user hence grant permission

ELSE

Go for the next filter test

END IF

END FOR

END

The previous filtering mechanism provides the IP addresses that are suspected to be the malicious IP addresses but does not guarantee fully. Even after the previous detection mechanism the suspicious IP addresses are not updated in the bad-host file, these IP addresses undergo the next filter test known as CAPTCHA test.

The CAPTCHA test provides a mechanism that can easily differentiate the legitimate users from the automated bots. By taking the disability of the bot to pass the CAPTCHA test, these could easily find out the clients running the automated program which enable them to send http GET request. Such clients are warned, their IP address are blacklisted and updated in the blacklisted IP table.

The CAPTCHA test is divided into two modules: generation module and verification module. The objective of the generation module is to send a CAPTCHA text to the suspected addresses by modifying the web pages. The objective of the verification module is to capture the reply to the CAPTCHA test and verify whether the matching CAPTCHA text is obtained.

The algorithm for the CAPTCHA test is given below:

BEGIN

For each suspected IP address from previous filter

Generate text CAPTCHA for specific IP address by altering the request web page.

Compute a time counter Tcount limit

Tcount = Tcount - 1

IF (Tcount ≠ 0)

IF (Reply is TRUE from IP address)

The request packet is legitimate and hence forward for normal access

ELSE

Drop the IP packet to the blacklist and update in the blacklist bad-hosts file

END IF

ELSE

Update IP address in the blacklist bad-host file

END IF

END FOR

END

The CAPTCHA test rejects any mismatched in the text send and text entered by the clients. This also set up a time limit so that any delay to the reply of the CAPTCHA test is not entertained and are blocked, also set up a policy so that multiple attempts that exceeds three times are blocked. These blocked IP address are then updated in the blacklisted IP table.

The distributed denial of service attack may not be able mitigated with a single defense line. It requires something distributed in nature. Our mitigation solution is a three-step process. Firstly the process of blacklisting IP from malicious source or known malicious IP address, secondly the process of monitoring http GET request rate and marking the IP with the highest count of http GET request. Lastly the counter check of the suspect IP with CAPTCHA test to differentiate between

legitimate clients and bots. Expected results might be able to maximize the number of http count seems to be running some automated program to send http GET request.

These IP address will tested against CAPTCHA test and fail to authenticate. Further work is needed to monitor on the parameter like the content of http request and also improve the process of blacklisting malicious source. We consider only the text based CAPTCHA technique to differentiate the normal and malicious clients. It can be extended even to motion based technique and selection of image to carry out the differentiating mechanism. We consider only the slow rate attack; this can be extended even to other types of application layer DDoS attack.

5. CONCLUSION

We have done a brief discussion on different types of architecture of DDoS and their defensive mechanism, along with their merits and demerits base on their application and at what situation that they response are more effective . Finally, we presented an overview of http count and CAPTCHA technique.

References

[1] T. Peng, C. Leckie, , and RMrao, K. "Survey of network-based defense mechanisms countering the DoS and DDoS problems.", ACM Computing Survey, 39, 3:1–3:42. (2007),

[2] V. Chandola,, A. Banerjee, , and V. Kumar, ,"Anomaly detection: A survey. ACM Computing Survey," 41, 15:1–15:58. (2009)

[3] G. Loukas, and ¨G. Oke, "Protection against denial of service attacks: A survey." Computer.Journal.53, pages-1020–1037. (2010)

[4] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita "Surveying port scans and their detection methodologies." Computer.Journal.54, Pages- 1565–1581.,(2011)

[5] H. J. Kashyap, and D. K. Bhattacharyya ",A DDoS attack detection mechanism based on protocol specific traffic features.", Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, Coimbatore, India, 26-28 October, pp. 194–200. ACM. , (2012)

[6] S.Lin, and T.C.Chiueh "A survey on solutions to distributed denial of service attacks.", Technical Report TR201. Department of Computer Science, State University of New York, Stony Brook.,(2006)

[7] P. J. Criscuolo, "Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319,", Department of Energy Computer Incident Advisory Capability (CIAC), UCRL ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.

[8] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.

[9] Ranjan. S, Swaminathan. R, Uysal. M, and Knightly. E, "DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection", IEEE INFOCOM'06, 2006.

[10] Chang R. K. C., "Defending against flooding-based distributed denial of service attacks: A tutorial,", Computer Journal. IEEE Communication Magazine, Vol. 40, no. 10, pp. 42-51, 2002.

[11] Puri. R, "Bots and Botnet – an overview,", Aug. 08, 2003, [online] http://www.giac.org/practical/ GSEC/RamneekPuriGSEC.eps

[12] Todd B., "Distributed Denial of Service Attacks," Feb. 18, 2000, [online] http://www.linuxsecurity. com/resource files/intrusion detection/ ddos– whitepaper.html

[13] CERT, "Denial of Service Attacks," June 4, 2001, [online] http://www.cert.org/tech tips/denial of service.html

[14] Liu. J, Xiao. Y, Ghaboosi. K, Deng. H, and J. Zhang, "Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures,", EURASIP Journal. Wireless Communications and Networking, vol. 2009, Article ID 692654, 11 pages, 2009.

[15] K Munivara Prasad, Dr. A Rama Mohan Reddy and Dr K VenugopalRao, Discrimination of Flash crowd attacks from DDoS attacks on internet threat monitoring (ITM) using Entropy variations, IEEE African Journal of Computing & ICT , Vol 6. No. 2, pp- 53-62, June 2013.

[16] K Munivara Prasad, Dr. A Rama Mohan Reddy , IP Traceback for Flooding attacks on Internet Threat Monitors (ITM) Using Honeypots , International journal of Network Security & Its Applications (IJNSA),ISSN : 0974 - 9330, Vol.4, pp 13-27, No.1,Jan 2012.

[17] Y. Xiang., Li, K., and Zhou,, "Low-rate DDoS attack detection and traceback by using new information metrics, " IEEE Transaction on Informatio Forensics. Vol: 6, pages: 426–437, 2011.

[18] Y. C Wu,., Tseng, H. R., Yang, W., and Jan, R. H. "DDoS "detection and traceback with decision tree and grey relational analysis.,", International Journal of Ad Hoc and Ubiquitous Computing, Vol-7, 121– 136.2011.

[19] Y Chen,., K. Hwang,., and W. S. Ku, "Distributed change-point detection of DDoS attacks over multiple network domains.", Proceedings of the IEEE International Symposium on Collaborative Technologies and Systems, Las Vegas, NV, 14-17 May, pp. 543–550. IEEE CS. (2006),

[20] J. Mirkoviac,., Prier, G., and Reiher, P. "Attacking DDoS at the source.", Proceedings of the 10th IEEE International Conference on Network Protocols, Paris, France, 12-15 November, pp. 1092–1648. IEEE CS. (2002)

[21] A. M. Saifullah, ",Defending against distributed denial-of-service attacks with weight-fair router throttling." Technical Report 2009 7.Computer Science and Engineering, Washington University, St. Louis, USA. (2009)

[22] T. Peng, C.Leckie, and RM Rao, K. "Detecting distributed denial of service attacks using source IP address" monitoring. Proceedings of the 3rd International IFIP-TC6 Networking Conference, Athens, Greece, 9-14 May, pp. 771–782. Springerverlag. (2004)

[23] J. Cheng, ,Yin, J., Wu, C., Zhang, and Li, Y. "DDoS attack detection method based on linear prediction model." Proceedings of the 5th international conference on Emerging intelligent computing technology and applications, Ulsan, South Korea, 16-19 September, pp. 1004–1013. Springer- Verlag. (2009)

[24] J. Udhayan, and T. Hamsapriya, "Statistical segregation method to minimize the false detections during DDoS attacks." International Journal of Network Security, 13, pages 152–160. (2011).