**International Journal of Pure and Applied Mathematics**
**Volume 120 No. 6 2018, 3423-3437**
ISSN: 1314-3395 (on-line version)
**url:** http://www.acadpubl.eu/hub/
Special Issue
http://www.acadpubl.eu/hub/

# DISTRIBUTED DENIAL OF SERVICE ATTACKS, TOOLS AND DEFENCE MECHANISMS

Mr. KISHORE BABU DASARI[1], Dr. D NAGARAJU[2],
ASST. PROFESSOR, DEPT OF CSE,
KMIT PROFESSOR
HOD,
DEPT OF IT, LBRCE
dasari2kishore@gmail.com
dnagaraj_dnr@yahoo.co.in

June 11, 2018

**Abstract**

Denial Of Service (DOS) attacks are the eminent network attacks in todays internet world. Their target is to wreck the resources of the victim machine. A DOS is assayed by a person, the DOS attack essayed by apportioned persons, is called Distributed Denial Of Service (DDOS). This paper evinces, the DDOS attack architecture, DDOS attack types, DDOS attack tools, and DDoS attack defence mechanisms. This paper, essentially unveils the DDoS attack defence, based on location posit and on activity deployment. This paper presents the boon and bane, of the different DDoS defence mechanisms. The desired objective of this paper, is to sort and properly organize the attacks and existing mechanisms, in codified order, for a better know-how and understanding, of DDOS attacks.

***Keywords*:** Denial Of Service; Distributed Denial Of Service; DDOS tools; DDOS Defence.

# 1 INTRODUCTION

Networks attacks, repudiate the access of computer network resources by using malignant node, known as availability based network attacks. Denial Of Service(DOS)[1][5][23], is sort of an active information security attack, which is an emphatic trial to squander the victim resources, like a machine or network resource provisionally or perpetually, for legitimate users by an enormous amount of pernicious packets which are sent from a single machine. There are five kinds of DOS attacks, namely, Ping of Death, TCP SYN Attack, Teardrop, Buffer Overflow and Smurf Attack. The Ping of Death, the attacker sends enormous amounts of ICMP echo ping requests, with a huge packet size to the victim machine, to trial a crash, destabilize, freeze and reboot the victim system. In a TCP SYN attack, the striker sends enormous amounts of TCP SYN requests to the victim system, so that it exhausts the victim machine resources, and make the system to gainsay services, for legitimate users. The Teardrop, the attacker sends crushed packets to the victim machine, so that it cannot reassemble them, for here, the packets overlap one another. The Buffer Overflow, the attacker sends an enormous amount of data into the buffer that exceeds the storage capacity of buffer, which leads to crash the victim system. The Smurf attack, the attacker sends the great quantums of ICMP echo(ping) requests, with a spoofed source IP address of the victim machine, to the network broadcast address such that, a lot of ping replies flooding the victim machine which sequel impact, the victim machine network severely. When DOS attack is initiated by more than one attacker, it is known as, the Distributed Denial Of Service (DDOS) attack.

Distributed Denial Of Service(DDOS) [1][5][23], is an attack assayed to degrade or completely disrupt the online service, by sending a deluge of packets, in the form of legit like requests, from diverse sources to the victim server.

# 2 DDOS ATTACK ARCHITECTURE

DDoS attack architecture[2], is categorized into two models: Agent-handler model and IRC-based model.

**Agent-Handler Model:** It [2] shown in Fig 1, consists of attacker, handler and agents or zombies. Handlers, are interfaces between the attacker and zombies. The handlers installed software packages in internet by the striker, to communicate with agents or zombies. Zombies are interfaces between handlers and victim machine. Zombies are compromised machines in the internet, which carry out the attack on the victim machine. The group of zombies are called, botnet. The botnet size is directly proportional to the severity of DDOS attack.

**IRC Based Model:** This architecture [2] (as shown in Fig 2), is the same as the Agent-Handler model, except for using handlers. Here, were using Internet Relay Chat to communicate with agents. In the IRC model attacker, we send commands to the agents through legitimate IRC ports, this halts, hinders tracking DDOS command packets. Large voluminous traffic of IRC server makes easier to the attacker, to hide his presence. An additional advantage of the attacker in this model, is he neednt maintain agents list, as he can select agents who are available on the IRC chat.

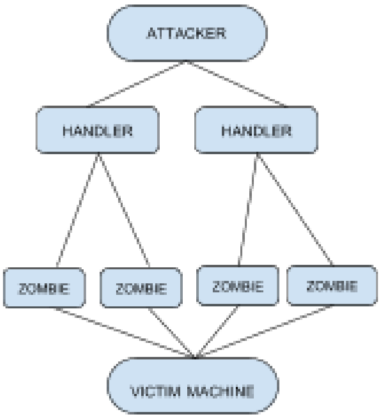

Figure 1: Agent-Handler DDOS attack architecture

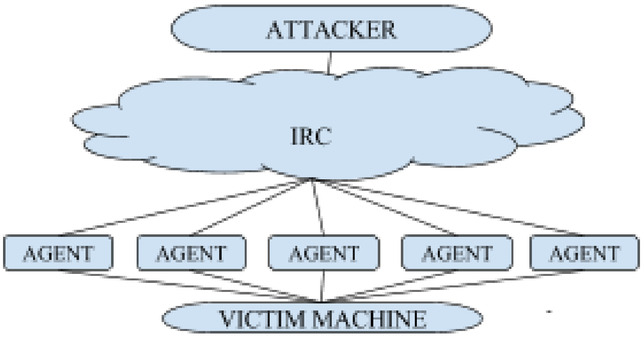

Figure 2: Internet-Relay Chat DDOS attack architecture

## 3 DDOS ATTACK TYPES

DDOS attacks[4][6] classify into three models, namely: Volume-based attacks, Protocol attacks and Application layer attacks.

**VOLUME BASED ATTACKS:** Most people are familiar with the volume based DDOS attacks[4][6]. The main goal of these attacks, is bandwidth saturation of the attacked site and making it unavailable, for legitimate traffic, by using various techniques. Attacks strength is measured in Bits Per Second (BPS). The UDP Floods[7][8][9], ICMP floods[8] and spoofed packet floods[8] are volume based attacks.

**PROTOCOL ATTACKS:** Protocol attacks[4][6], are targeted on server resources and related equipment such as firewalls and load balancers, then bandwidth. Attacks strength here, is measured in Packets Per Second (PPS). SYN floods[7], Ping of Death[8], Smurf DDOS, and fragmented packet attacks are all Protocol attacks.

**APPLICATION LAYER ATTACKS:** Application layer attacks[4][6] target the application interface of websites such as HTTP or other Web applications. The application layer or Layer 7 attacks are slow, and the furtive sending seemingly harmless requests, are meant to bring down the web server. Attacks strength here, is calculated in Requests Per Second (RPS). Slowloris, Apache killer and HTTP floods are all application layer attacks [7][8][9].

## 4 DDOS TOOLS

DDOS attack tools are divided into three categories: Agent-based, IRC-based and Web-based DDOS attack tools.

**Agent-Based DDOS Tools:** These tools[10] built on the agent-handler based DDOS attack architecture.

**Trinoo:** It is depleting bandwidth and launching UDP flood attacks.

**Tribe Flood Network (TFN):** It is depleting bandwidth, resources and launching SYN, UDP, ICMP and smurf attacks.

**TFN2K:** It is a descendant of TFN tool. TFN2K is also used for launching UDP, SYN, ICMP and smurf attacks.

**Stacheldraht:** Stacheldraht is used for launching UDP, SYN, ICMP flood and smurf attacks.

**Mstream:** It is a point-to-point flooding tool. It is also used for launching UDP, SYN, ICMP and smurf attacks.

**Shaft:** Shaft is a derivative tool of the trino tool, it can be used for launching flooding attacks. It can control attack duration and packet flooding size.

**IRC-BASED DDOS TOOLS:** These tools[10] are build on IRC based DDoS attack model.

**Trinity:** It is the best-known IRC-based tool, and is used for launching TCP SYN, TCP ACK, and TCP NULL packet floods.

**Knight:** It [20] is a frivolous powerful IRC-based tool. It can be used for launching TCP, UDP flood attacks, SYN, and PUSH+ACH attacks.

**WEB-BASED DDOS ATTACK TOOLS:** These tools[10] are lately developed for the application layer DDOS attacks. The following are the web-based tools, for ddos attacks:

**Low Orbit Ion Cannon (LOIC):** LOIC is a simple flooding based tool, that can be used to generate massive volumes of TCP, UDP, or HTTP traffic, in order to fill the server with the massive network load.

**High Orbit Ion Cannon(HOIC):** HOIC is one of the web-based DDOS attack tools, which is used to launch HTTP POST and GET requests DDOS attacks.

## 5 DDOS ATTACKS DETECTION AND DEFENCE

DDOS attack detection[3], is the first and initial step, in the DDOS defence battle. We have classified DDoS defence mechanisms into two methods, namely, DDoS defence based on location deployment, and activity deployment.

**DDOS DEFENCE BASED LOCATION DEPLOYMENT:** The first method categorizes the DDOS defence mechanisms based on location deployment. Thus, we have classified into the following four types namely:

- Source-end
- Victim-end
- Core-end
- Distributed-end

**Source-End:** A defence system located at the source-end of the network[3] works better than the remaining three points located in the network, since it is very effective in stopping attacks as near to the source as possible. It lessens the damage curb on the victim machine as the defence system is placed at the source-end which is near to the attacking point. The minimum amount of traffic at source-end minimizes network traffic congestion and defends network resources, which are required by the detection and mitigation mechanism. D-WARD is a source-end DDOS defence mechanism.

**Victim-End:** Placing a defence system at victim-end network[3] is cost effective than the rest of the three methods, as the attack has already attacked on the victim machine, so it effects severely on the victim machine degrading services. A large amount of traffic at victim-end, makes the defence system very complex. Sometimes like high rate traffic victim-end defence is not adequate to detect ddos attacks. A major setback of this method is that, the victim machine sacrifices its performance, and it resources to increase security. The victim-end defence system uses either the reactive or proactive methods, to detect ddos attacks. Core-End: Core-end router in the network, unaccompanied attempt to identify DDOS attacks. which is malicious traffic. It is a better spot to control traffic rate.

**Distributed-End:** Placing a defence system at distributed-end network[3], it performs efficiently in DDOS attacks detection, in contrast with the above methods, by cooperating among distributed multiple defence subsystems.

**DDOS DEFENCE BASED ACTIVITY DEPLOYMENT:** The second method categorizes DDOS defence mechanisms, based on the specific activity deployed. Thus, we have classified it, into the following three types:

- Preactive method
- Proactive method
- Reactive method

**PRE-ACTIVE DDoS DEFENCE METHODS:** The preactive method [3][12][13], is the best DDoS attack defence method, to prevent DDOS attacks. The major aim of the preactive method, is to stop launching DDOS attacks in the system. Preactive DDOS defence mechanisms are classified into two types:

**Filtering Techniques:** Globally coordinated(Ingress/Egress) filters: Globally coordinated filters are divided into two types namely: Ingress filters and Egress filters. These filters can stop attacking packets before they can cluster to lethal proportions on the victim machine. These two filters ensure that only valid IP address packets allow or leave the network. The ingress filtering[17] is an inbound filter proposed by Ferguson and Senie to prevent the IP address, spoofing DDOS attacks. Ingress filtering filter illegitimate source address incoming packets, put into the network. The egress filtering[17] is an outbound filter allow the valid IP address packets in the network. Ingress and egress filters have similar behaviour except inbound and outbound placement issue. Their key requisite in place, is to know the IP address of the particular port. This knowledge, can be earned by using the reverse path filtering technique. This technique is not work effective because asymmetric internet routers are not uncommon. Deploy ingress and egress filtering universally is difficult. Real IP address attacks cannot be prevented. However, ingress and egress filtering techniques drastically reduce the DDOS attack power, on the victim machine.

**Route based distributed packet filtering:** In this packet filtering[18] method, the filter is spoofed by IP packets, by using route information. When IP packet contains unexpected source address, the filter treats the address as spoofed, so the packet cannot be forwarded. This method is advance of ingress filtering. Sometimes legitimate packets may be dropped, when they change their routes. It does not work well, with the dynamic internet routing. However, the route based packet filtering works effectively, in randomly spoofed DDoS attacks.

**History based IP filtering:** This method [18], prevents DDOS attacks, by using the IP address database, which stores frequent source IP addresses. If the router finds the packet source IP address, is not in the IP address database, then it treats the packet an illegitimate, and then drops the packet. Hash based searching methods are also used to search the IP addresses in IP address database. It need not have the cooperation of the complete internet community. It requires additional database to maintain the track of IP addresses. This method is inefficient when the attacks are occurred from legitimate IP addresses.

**Capability based method**: Capability based method is proposed to prevent the DDOS attacks. In this method, the initial, first source sends request to the destination. While the source request is passed to the router, it adds pre-capability marks to request packet. Permission granted to the source to send, is decided by the destination. If it grants permission, it returns capabilities, else does not, in the returned packet. Packets without capabilities, are dropped at the router. This method requires high computational complexity and space requirement. Destination is the main lead to control its traffic by itself.

**Secure Overlay services(SOS):** Secure overlay service[19] is an architecture with distributed feature to provide security, to the victim machine from users. Secure Overlay Access points are used to verify traffic from various source points. After verification, forwarded to the beacon overlay node, here consistent mapping has been done. The traffic forwarded to secret servlet which is a special overlay node, here further authentication, the verified traffic is forwarded to the victim machine. The SOS effectiveness, is based on the distribution level of SOAPs.

**Source Address Validity Enforcement Protocol:** This method is to prevent DDoS attacks. It runs on network routers. It builds incoming tables for providing information about source address validation, to the routers. SAVE protocol builds the incoming table for each router with specification of valid source address packets by forwarding. Routers use this table information, to filter illegitimate source address packets. In addition to incoming tables, SAVE protocol contains two or more data structures: Incoming tree and SAVE update. The incoming tree, is used to derive incoming tables and SAVE update, and is used to exchange SAVE router updates.

**General Techniques:** Load balancing: Load balancing is a survival technique from DDoS attacks, to provide sufficient resources like bandwidth, memory and CPU power to elicit users, to avoid, DDoS attacks. It is a cost effective method. Honeypots: Honeypot has been proposed as DDoS attack prevention technique by Weiler. Honeypots attract the ddos attackers to attack itself, instead of the victim machine. Honeypots can also collect information of attackers, such as the activity of attack, type of attacks and software attack tools.

Other general techniques are, changing IP addresses, applying security patches, disabling IP broadcasts, disabling unused services and history based IP filtering.

**PROACTIVE DDOS DEFENCE METHODS:** The proactive method[3][12][13][25] is applied earlier than the DDOS attack, reaching the victim machine. There are three approaches to detect DDOS attacks:

- Signature based approach
- Anomaly based approach
- Entropy based approach

Signature-Based DDOS Attack Detection: It is based on traffic characteristics. However, the communication between attacker and zombie could be encrypted detection making, difficult. The main drawback of signature based detection is the difficulty to create signatures for all types of DDOS attacks. Signature-based techniques, are more generally applied, in Intrusion Detection

Systems(IDS)[15]. Signature based DDOS attack detection is very fast and reliable, but its major set back is, it does not detect new pattern attacks.

Anomaly-Based DDOS Attack Detection: It uses network traffic statistics, to calculate the observed statistical features, if an extreme deviation occurs, it triggers alarm. Two methods in Anomaly based detection: IP Attribute based and Traffic Volume based. IP Attribute-based detection is based on monitoring of the behavior of IP packet parameters such as a source IP address, a port number and Time To Live value.

Traffic Volume based detection is based on monitoring of, and behavior of network traffic and packet rate, in the network flow. The following are some anomaly based DDOS attack detection methods.

NOMAD [20] is a scalable network monitoring system. It analyzes the IP packet header information, to detect network anomalies.

D-WARD [20] is a source-end, distributed, adaptive and customizable proactive DDOS attack defence system, it has proposed Mirkovic et al. Edge routers of the network which are installed with D-WARD. D-WARD detects the illegitimate behaviour of attack.

Entropy-Based DDoS Load balancing is a survival technique from DDoS attacks, to provide sufficient resources like bandwidth, memory and CPU power to elicit users, to avoid, DDoS attacks. It is a cost effective method. Attack Detection: Entropy features are most common in present DDOS detection. Entropy based DDOS attack detection[21], is based on measurement of uncertainty, associated with a random variable. The intrusion detection system is an entropy based detection approach, to detect DDoS attacks[16]. Entropy-based technique[15], uses the statistical measure, to find the uncertainty. Its major drawback here, is large computation of data.

**REACTIVE DDOS DEFENCE METHODS:** The reactive method[3][12][13], is applied the initial stage of DDoS attack attacked on the victim machine. There are many reactive DDoS detection methods, to detect and mitigate attacks such as:

**IP traceback:** This mechanism detects the true source of fake IP packets, which are used by the attacker in the attack generation. The IP traceback[14] methods major drawback, is the high computational overhead. The victim end or intermediate routers, are used to find the source end, by using the IP traceback mechanism.

**ICMP traceback:** In this method, the router generates ICMP traceback[14] messages. These messages, contains forward packets, along with adjacent routers information. By using these ICMP traceback messages, the victim constructs attack graphs and send them back to the attacker. ICMP traceback is potential in terms of network expenses. The major limitation of this method is high computational overhead, in a large network.

**Probabilistic packet marking:** This method does not need earlier knowledge of the whole network, for an attack topology. It is a very easy method which supports incremental deployment. The main drawback of this method, is the reconstruction process of path and high computational overhead.

# 6 CONCLUSION

We here, have discussed the DDOS attack architecture, DDOS attacks types and defence mechanisms. DDOS defence schemes based on location deployment, such as source-end, intermediate and victim end defence mechanisms and activity deployment based, such as preactive, proactive and reactive DDOS defence mechanisms. We present the advantages and disadvantages of existing DDOS attacks defence mechanisms. This presentation and documentation, is useful for the readers better understanding of the DDOS attacks, their impact on victim machines and defence mechanisms, to mitigate and abate the DDOS attacks impact. Further, work in this domain is application layer DDOS[11] attacks and defence mechanisms.

# References

[1] Heshuai Li, Junhu Zhu, Qingxian Wang, Tianyang Zhou, Han Qiu, and Hang Li,"LAAEM: A Method to Enhance LDoS Attack" IEEE COMMUNICATIONS LETTERS, VOL. 20, NO. 4, APRIL 2016.

[2] Seyyed Meysam Tabatabaie Nezhad, Mahboubeh Nazari, and Ebrahim A. Gharavol "A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time" IEEE COMMUNICATIONS LETTERS, VOL. 20, NO. 4, APRIL 2016.

[3] Qiao Yan, F. Richard Yu, Senior Member, IEEE, Qingxiang Gong, and Jianqiang Li "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges" IEEE COMMUNICATIONS SURVEYS TUTORIALS, VOL. 18, NO. 1, FIRST QUARTER 2016.

[4] Nazrul Hoque, Dhruba K. Bhattacharyya, and Jugal K. Kalita "Botnet in DDoS Attacks: Trends and Challenges" IEEE COMMUNICATION SURVEYS TUTORIALS, VOL. 17, NO. 4, FOURTH QUARTER 2015.

[5] Jingtang Luo, Xiaolong Yang, Senior Member, IEEE, Jin Wang, Member, IEEE, Jie Xu, Member, IEEE, Jian Sun, Member, IEEE, and Keping Long, Senior Member, IEEE, "On a Mathematical Model for Low-Rate Shrew DDoS", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 7, JULY 2014.

[6] Zahid Anwar and Asad Waqar Malik, "Can a DDoS Attack Meltdown My Data Center? A Simulation Study and Defense Strategies", IEEE COMMUNICATIONS LETTERS, VOL. 18, NO. 7, JULY 2014

[7] L. Zhang, S. Yu, D. Wu, and P. Watters, "A Survey on Latest Botnet Attack and Defense", Proc. of 10th Intl Conference On Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, pp. 53-60, November 2011.

[8] A. Mishra, B.B. Gupta, and R.C. Joshi, "A Comparative Study of Distributed Denial of Service Attacks, Intrusion Tolerance and Mitigation Techniques", Proc. of European Intelligence and Security Informatics Conference (EISIC), IEEE, pp. 286-289, September 2011.

[9] Z. Chao-yang, “DoS Attack Analysis and Study of New Measures to Prevent”, Proc. of Intl Conference On Intelligence Science and Information Engineering (ISIE), IEEE, pp. 426-429, August 2011.

[10] (2013) Understanding Denial-of-Service Attacks. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-0 15[Online].

[11] O.Yarimtepe, G. Dalkilic, and M. H. Ozcanhan, “Distributed Denial of Service Prevention Techniques”, in 3rd International Symposium on Digital Forensics and Security (ISDFS ’15), May 2015, pp. 2428.

[12] K. Chatterjee, “Design and Development of a Framework to Mitigate DoS/DDoS Attacks Using IPtables Firewall”, International Journal of Computer Science and Telecommunications, vol. 4, no. 3, pp. 6772, 2013.

[13] (2015) Digital Attack Map. [Online]. Available: http:www.digitalattackmap.com.

[14] Opeyemi Osanaiye, Kim-Kwang Raymond Choo, Mqhele Dlodlo, “Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework” ,Journal of Network and Computer Applications, Volume 67, May 2016, Pages 147165.

[15] Abdul Serwadda, Vir V. Phoha, “When Mice devour the Elephants: A DDoS attack against size-based scheduling schemes in the internet”,Computers Security, Volume 53, September 2015, Pages 3143

[16] S.Shithartha, D.Prince Winstonb, “A Comparative Analysis between Two Countermeasure Techniques to Detect DDoS with Sniffers in a SCADA Network”, ScienceDirect, Procedia Technology 21 ( 2015 ) 179 186.

[17] Ilker Ozc elik, Richard R. Brooks “Deceiving entropy based DoS detection”, Computers Security Volume 48, February 2015, Pages 234245.

[18] Jisa David, Ciza Thomas, " DDoS Attack Detection using Fast Entropy Approach on Flow-Based Network Traffic", Procedia Computer Science 50 ( 2015 ) 30 36.

[19] Rashmi V. Deshmukha, Kailas K. Devadkarb "Understanding DDoS Attack Its Effect In Cloud Environment",Procedia Computer Science 49 ( 2015 ) 202 210.

[20] Sonia Laskara, Dhirendra Mishrab, "Qualified Vector Match and Merge Algorithm (QVMMA) for DDoS Prevention and Mitigation", Procedia Computer Science 79 ( 2016 ) 41 52.

[21] Raksha Upadhyaya, Uma Rathore Bhatta, Harendra Tripathia,"DDOS Attack Aware DSR Routing Protocol in WSN", Procedia Computer Science 78 ( 2016 ) 68 74.

[22] Christos Douligeris, Aikaterini Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art", Computer Networks 44 (2004) 643666.

[23] Boris Sieklik, Richard Macfarlane, William J. Buchanan, "Evaluation of TFTP DDoS amplification attack",computers security 57 (2016) 6792.

[24] Opeyemi Osanaiye, Kim-Kwang Raymond Choo, Mqhele Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework", Journal of Network and Computer Applications, Volume 67, May 2016, Pages 147165.

[25] Bing Wang, Yao Zheng, Wenjing Lou, Y. Thomas Hou, "DDoS attack protection in the era of cloud computing and Software-Defined Networking", Computer Networks,Volume 81, 22 April 2015, Pages 308319.