Redirection of Anomaly Packets towards Traffic Server in Distributed Denial of Service Attacks (RAPTTS)

Detection and Prevention Mechanisms

[1]S.Suresh
Research Scholar,
Sathyabama Institute of science and technology&
AP/CSE, Panimalar Engineering College,
Chennai, Tamilnadu, India
m.suresh.suresh@gmail.com

[2]Dr.N.Sankar Ram
Professor
Department of CSE
Sriram Engineering College
Chennai, Tamilnadu, India
nsankarram@gmail.com

[3]J.Gokul Raj, [4] S.M.Seyed Ibrahim
[3,4]Department of CSE,
Panimalar Engineering College,
Chennai, Tamilnadu, India
gokulraj221097@gmail.com, seyedhere@gmail.com

***Abstract* - Distributed Denial of Service (DDoS) is an Organised Coordinated Attack launched by an Attacker using large number of Compromised Hosts. Initially the attacker discover the vulnerability in one or more network for installation of malware programs in multiple machines to control them from a remote location. At a later stage, the attacker exploits these compromised hosts to send attack packets to the target machine, which is usually outside the original network of infected hosts, without the knowledge of these compromised hosts. Depending on the intensity of attack packets and the number of hosts used to attack, commensurate damage occurs in the victim network. When an attacker can aims to a large number of com-promised nodes, network and server may be collapsed within a short time. We have mentioned few examples of DDoS attacks are ,smurf and SYN flooding. In this paper, we studied various DDoS detection and prevention mechanisms and presented RAPTTS based DDoS Prevention Technique summarized different DDoS Attack techniques and their antidotes in a nutshell.**

Keywords – Distributed Denial of Service, Internet Security, IP Spoofing, Network Attack, Zombie, TCP SYN, CERT.,Traffic Server,Redirection and Retrieval of legitimate Packets.

INTRODUCTION

Distributed Denial of Service is a large scale coordinated organised attack whose primary motive is to deny access to web services of authorised users by overflowing the network with unwanted packets or by sending multiple requests to the server using legitimate IP's with the knowledge of IP Spoofing.DDos attacks are highly disastrous and can bring down a server or a network easily and quickly. A DDoS attacker learns the vulnerability of various networks to setup it as a compromised hosts group to launch a DDoS attack[2]. The attacker uses these compromised hosts to get Security breaches in the Victim's Network. The main causes of Security breaches are due to Poor Network Architecture, Poor Network management, Mismatch in the speeds between the core and the edge routers, Interdependencies in Internet Security. The main targets of DDos Attackers are Routers, Firewall Systems, Victim's Operating System, Victim's Entire Network Infrastructure and its corresponding Links. Once the attacker is familiar with the security breaches of the victim's network, an attack is carried out by four basic steps

*A. S*electing the Master/Zombies

Master in the sense, the compromised hosts from whom the attack is carried out. The attacker selects Master based on the high availability of resources of the machine and the ability to generate a highly powerful attack streams. The selection of the Master are made remotely by the Attacker without the knowledge of the compromised Hosts.

B. Plant the Code

In this stage, the attacker with the help of the security vulnerabilities of the Master, plants the attacking code into the zombie machine. The attacker is very clear that he /she takes necessary steps to the safeguard the planted code from being identified and destroy it in case it is found. The

attack of the victim may be direct or Indirect. In case of direct attack the compromised hosts lead the attack and attacks the legitimate users of a server from acquiring the service and flood the network with large number of request packets. The attack is initiated by the attacker. In case of indirect DDoS Attack, Servers are often used as the attacker to attack the victim's Server. The attacking server must run UDP based services to start the attack. These kind of servers are called The Reflectors. In this kind, the Master attacker sends the request to reflector server with the knowledge of the victim's IP Address as the source IP using IP Spoofing technique.As a result, these servers reply to the Victim's server and the size of the message is normally very larger than the normal message size, thus the server is flooded with more number of unwanted packets.

C. Communicate with the handlers

The attackers coordinating with the active controller to realize which Master are moved up and executing, allocating the attacks and upgrading of the Master. The Protocols involving in the communication between the attacker and the handlers are ICMP, TCP, UDP .The attacker can be able to communicate with one or more handlers based on the severity of the attack[3].

D. Attacking

The master attacker initiates the attack and specifies the victim's Network, duration of attack, type of attack, Time to Live(TTL) and the Ports. The attacker sends large amount of packets to the victim's network to flood the network resources. The Victim's Network is then overwhelmed with large amount of packets from the compromised host machines along with the legitimate requests which makes the denial of service to the Users of the network due to Device failure or Dropping the request packets.

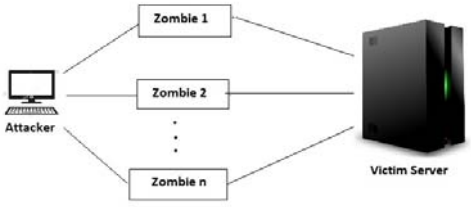


Figure 1. Flowchart of Direct DDoSAttack

The above figure represents the DDoS attack lead by the intermediate Zombies initiated by the Attacker. It is important to note that the attack lead by the attacker is carried without the awareness of the zombies. The zombies may or may not be aware that they are the part of the DDoS attack.

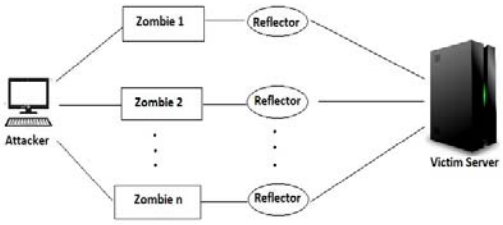


Figure 2. Flowchart of IndirectDDoS Attack

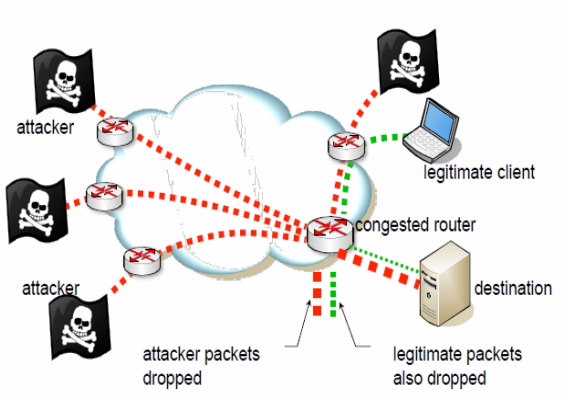


Figure 3. Pictorial Representation of DDoS Attack.

The above figure gives the complete picture of DDoS Attack Strategy carried out by an attacker to congest the Victim's Network and thus denying the legitimate user from accessing the services of the Server[1].

II. CLASSIFICATION OF DDOS ATTACKS

DDoS attacks methodology can be divided into two types. 1. The first method is to Flood the network and deplete the bandwidth of the network ,thus leads to the network breakdown 2. The second method is to squander the resources of the Server or the Pc such as CPU time. Memory etc. Thus it leads to server breakdown. The various DDoS attacks carried out using the above methodology are as follows:

A. *TCP Resets*

TCP reset attack is mainly used to abort Internet connection to the victim by resetting the (RST) flag.
In TCP connection, each packets contain the TCP header which in turn contains the RST flag , if the flag is set to 0 , there will be no harm but if the flag is set to 1 , it indicates to the receiving computer to stop using the TCP connection. Thus preventing it from using the internet.

B. *SYN FLOODING*

In this attack , the zombies send multiple SYN packets instead of single SYN packets to the server thus it consumes large server resource and deny other system to get service from the server[4].

a)UDP FLOOD

UDP is a connectionless protocol, in this the attack is carried out by sending large number of UDP packets to the Victim's server's random ports on a remote network. Thus consuming a huge amount of server's time.

b)SMURF ATTACK

It is also known as ICMP (Internet Control Messaging Protocol) Attack. Here, large number of ICMP packets are send to all the computer in the network by spoofing the Victim Server's IP. In return all the computer in that network will send the reply packets to the server and if there are large number of computers in the network , it will lead to Congestion in the network[4].

c)ARP ATTACK

ARP attack is also named as ARP Poison Routing, is a routing procedure when the attacker transmits Address Resolution Protocol (ARP) damaged messages onto a LAN. The main aim of the ARP Poison Routing is to link the MAC address of the attacker with the IP address of the host, as result of which the network traffic meant for that particular IP address to be sent to the attacker.

III. DDoS Detection Methodologies

DDoS Detection Techniques are mainly classified into two types:

1. Misuse detection
2. Anomaly-based detection

Misuse detection method tends to search for different definite patterns ,for instance it searches for formal patterns like signatures, rules, or even some activities is taken into consideration. This is done in a network traffic in order to identify the previously known DDoS intrusion types .These detection techniques show high detection rates at the same time low number of false alarms. But this detection technique fails, when it is to detect unknown DDoS intrusion types.

Anomaly-based DDoS detection technique tends to identify novel intrusion types and also detection of known types. This technique identifies network behaviour by analysing it and attempts to detect the unusual patterns[6].

A. *Misuse Detection*

The defenders at first define the abnormal system behaviour and then focus on defining other behaviour as normal. In simple words, it can be said that anything we don't know as bad is normal in the misuse detection technique. The best example for this approach is using attack signatures in IDSs. The performance of an IDS in terms of detection accuracy depends entirely on how adequate the knowledge of known attacks is and how well the detection engine can use it during detection[10].

1) Rule-Based detection

If-then rules acts as the fundamental blocks for building the rule-based detection systems. Rules are developed by analysing attacks or misuses and then transforms them into conditional rules[5] .

2) State-Transition Techniques

A state-transition technique mainly represents the misuses or attacks as a sequence of activities. The transition from one state of a monitored sensor to another state of a monitored sensor can be efficiently caused by an activity or a group of activities and this can lead to the alert state of a monitored system.

B. *Anomaly-Based DDoS Detection*

Anomaly-based detection techniques first establish the normal behaviour of a subject, which may be a user or a system. If an action is found to deviate significantly from the normal behaviour or pattern, it is recognized as anomalous or intrusive[6].
If the defender can properly establish a normal activity profile for a system, it can also flag all system states that vary from the normal profile

significantly. So, in an anomaly-based detection approach, two distinct possibilities may arise: (a) false positives, which are anomalous activities that are flagged intrusive, but are not intrusive, (2) false negatives, which are anomalous activities that are flagged as non-intrusive but are intrusive. The main advantage of anomaly detection is that it can detect unknown attacks. In the past two decades, the world has seen a good number of anomaly-based DDoS detection approaches and systems In addition to these software-based DDoS defence solutions, a large number of hardware-based network security solutions have also evolved. To counter DDoS attacks that use both low-rate and high-rate traffic, researchers use a variety of approaches such as statistical, machine learning and data mining, soft computing, and knowledge-based. We introduce some prominent solutions under each category, discuss methods used, and analyse their effectiveness.

1) Statistical Techniques

The effectiveness of statistical methods have already been established in anomaly-based intrusion detection. A statistical approach initially defines normal user behaviour based on what is acceptable within system usage policies[11]. If a monitored behaviour is found to deviate significantly from predefined normal behaviour thresholds, it is considered anomalous activity and an attack. Most methods are designed to detect network anomalies using various statistical and information theoretic measures such as deviation, cumulative sum, correlations, entropy, mutual information (MI), and covariance.

IV)DDoSPrevention Methodologies

DDos Prevention Methodology is also known as Intrusion Prevention System(IPS) which is an extended version of Intrusion Detection System (IDS). Prevention and Detection goes hand-in-hand[9]. To Prevent a Victim's Network from DDoS we have to Detect better and apply prevention Strategies. An IPS works by first Detecting the suspicious Network or Hosts and then it prevents by either Dropping the packets from those networks, generating alarms, resetting the connection and blocking the traffic. The flow of Intrusion Prevention System is given by the following diagram.

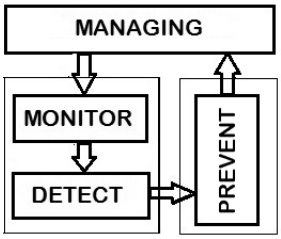


Figure 4 Overview of Intrusion Prevention System

In the Fig.4, The Managing system controls the flow of packets to and from the network.Once the packet enter into the monitoring and managing system comes into picture and detects to see any malicious packets prevailing into the system. If so, using proper prevention strategies, the malicious packets are dropped[11].

The Intrusion Prevention is done by either software or a hardware device that prevents the malicious packets moving towards the victim system. For Effective prevention, one should be able to identify the source and initiate to detect the attack sources. Since identifying the attack source is not a straight forward approach due to IP Spoofing and decentralized internet architecture, we must apply several methods to identify the Source of the attacker. Several methods to Identify Source are as follows:

A. IP TRACEBACK

As the name suggests, the IP Traceback method is used to trace the attacker, though he is using a spoofed IP. Traceback can be done either manually or automatically[7]. Since manual traceback is time consuming and tedious ,we go for Automatic IP Traceback. The IP Traceback can be explained with the help of the following diagram.

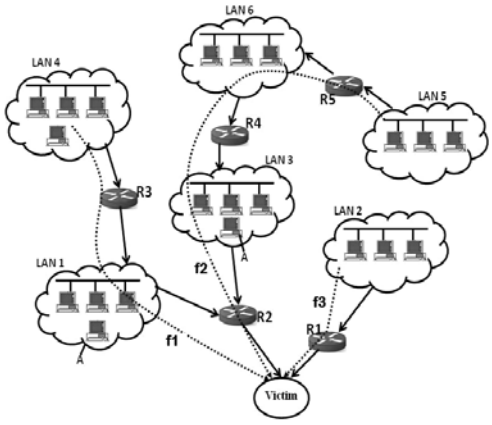


Figure 5. Network to examine Ingress and Egress filtering

In this example network, we have six LANs (viz, LAN1,LAN2,…..,LAN6) and five routers

(viz,R1,R2,..,R5). Multiple attackers from LAN1, LAN3, and LAN6 target a single victim. So in a DDoS attack, the flows destined to a victim include both legitimate flows as well as a combination of attack and legitimate flows. In Figure 5.2, a flow such as f3 is a legitimate flow,whereas f1 and f2 are combinations of attack and legitimate flows. Typically, during a DDoS attack, the volume of flow increases significantly within a short interval of time. So, one can observe a significant change in the traffic pattern at routers R2 and R4 and also at the victim. In contrast, at routers R1, R3, and R5, such changes or variations will not be visible due to the absence of attack flows. Once such variations are sensed by the victim, typically the defender attemptsto push back to the LAN(s),that are suspected to be involved in the attack. One can carry out such an exercise by using information metrics (such as entropy) to quantify the variations in the traffic at the routers and the victim. In other words, one can measure the changes in randomness of flows at the routers or at the victim for a given interval of time. Based on the discovery of significant flow variations at the victim machine in terms of entropy, the defending agent may be able to guess that high-rate attack sources are somewhere behind R2, but not behind R1, since no significant entropy variation is sensed here. Accordingly, the network defender will send a traceback request to R2 to locate the possible source ofDDoS attacks. Like the victim, based on entropy variations sensed, router R2 may identify that DDoSattacks are from two sources, one behind LAN1 and the other behind LAN3. Subsequently, the tracebackrequest can be forwarded to the edge routers of LAN4 and LAN6, i.e., R3 and R4. Similarly, at both these routers, entropy variations will be estimated and if significant change is detected in any one or at both routers, action will be taken accordingly. In the sample network, R3 can infer that attack sourcesare from LAN1. However, R4 will infer that attackers are from LAN3 and also are behind R4. Accordingly, the traceback request needs to be forwarded further to upstream routers, say R5, to locate the attack from LAN6.

B. RAPTTS MECHANISM

Redirection of Anomaly Packets Towards Traffic Server (RAPTTS) is a Extension of IP Traceback Mechanism, here instead of neglecting the Entire router from sending packets we can redirect the packets to the Traffic server where the packets are analysed based on the IP filtering technique to differentiate the legitimate and attack packets.
The inclusion of traffic server reduces the overhead of the primary server's Fucntionality and incase the primary server fails the secondary server comes into the picture and acts as a primary server and the traffic server is reconnected to the presently acting primary server.

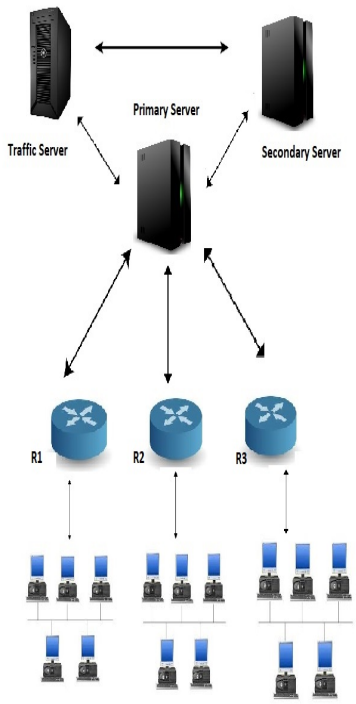


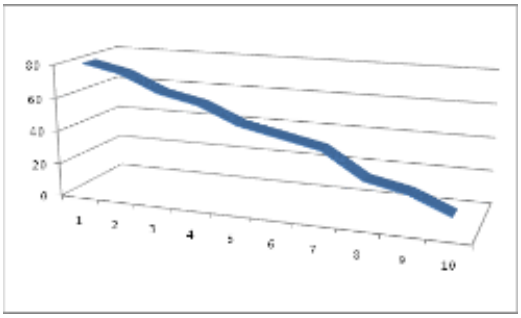
Figure 6. RAPTTS Approach

In the above figure, the main components are client system that includes both legitimate and illegitimate clients, routers that forward the data packets from clients to servers, and the end server that accepts and process the data packets from the client.

In the fig .6 , for an instance consider that the client computer under the router R1,R2 are attackers. These attacker client system consists of zombies and reflectors through which they send their data packets in huge volumes in order to create a network traffic which makes the end sever busy or to crash the server so that the legitimate client under the router R3 will be unable to send its data packets and acquire the service from server.

In Redirection of Anomaly Packets Towards Traffic Server (RAPTTS), when the primary server receives the data packets or the request for service in normal volume by the legitimate clients, the server acts on the data packets without any further delay .But when the received data packets or requests are incongruent then the packets are directed towards another individual server called Traffic Server. This server processes on the huge volume of data packets making the primary server available for the legitimate clients. In case the primary server crashes the secondary server takes the place of

primary and recives the data packet from the routers. The main advantage of this method is that, the load of the data packets from the clients are distributed among the servers and it can effectively service the legitimate clients. The disadvantages of this approach is to install and maintain an additional server[7].

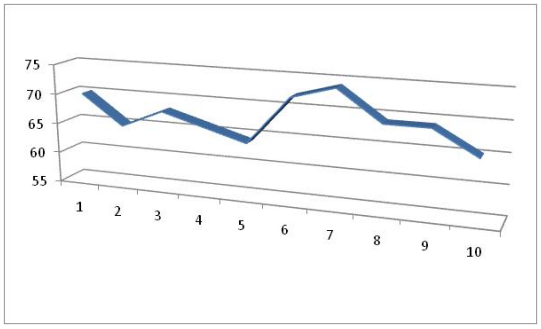


X - Load on the server
Y - Performance of the server

Figure .7 Performance to Load Graph without RAPTTS

Here, the performance of the server **decreases with the increase in load on server** by both the legitimate clients and the attackers.

Performance: It is the response time of the server to the number of incoming packets



X - Load on the server
Y - Performance of the server

Figure 8 Performance to Load Graph with RAPTTS

Here, the performance of the server **remains substantial with the increase in load on server** by both the legitimate clients and the attackers

C. LINK TESTING

In this the victim makes a test on each of its incoming links for DDoS attack traffic. If the test passes, it then links to the upstream router close to it, then the contacted router initiated the process recursively on its upstream routers until the true source of attack is found[13]. The main advantages of this method are reliability and cost effective. The limitation of this method is that is suffers from additional traffic.

D. PACKET MARKING

Packet marking is a significant method for identification of the DDoS attacker's origin. In this, routers mark forwarding packets probabilistically or deterministically with their own addresses. So, when a attack happens, the victim uses the marked information associated with the packet to traceback to the source of the attacker.[8]

E. ICMP Traceback Messages

In this, the router generates ICMP traceback messages that include content of forwarded packets along with information about the adjacent routers and sent them to the destination. When flooding occurs, using the ICMP messages the victim construct an attack graph back to the attacker.ICMP is effective interms of network overload since it requires low network management but since it uses input debugging method which is disabled in many of the routers ,it becomes tedious to establish a connection between a participating and non-participating one.

F. FILTERING TECHNIQUES

So far, we have seen how to detect the source of the attacker. Herethen, we can see various filtering techniques used to protect the network resources from DDoS attacks[14].

1) Ingress and Egress Filtering

Ingress refers to incoming packets and Egress refers to the outgoing packets of a LAN. Ingress filtering is a set of rules used to filter packets that come into the Local area Network[15]. Let us examine the ingress filtering with the help of an example.

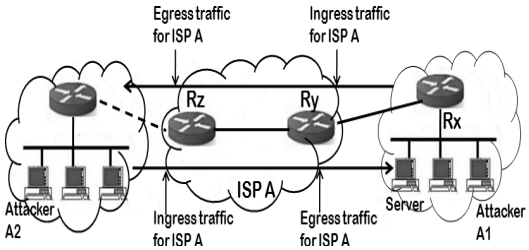


Fig.ure 9. Example to demonstrate Ingress filtering.

We see in the figure that ISP A provides access to the Internet to the network of an institution or organization, referred to as a leafnetwork. In the leaf network, router Rx is the edge router, connecting to an edge router of ISP A, i.e., router Ry. ISP A has another edge router, i.e., router Rz, through which connectivity is provided to other networks. According to the proposal, ingress and egress filters allow access to packets that come into a network or leave a network if their source addresses match a pre-defined range of source IP addresses.Let us consider a scenario. Assume that attacker A1 is inside theinstitution's network and is sending packets with spoofed IP addresses to the Server. Also assume that router Ryof ISP A is equipped with an input filter, and is connected to the institution's network. Assume also that we have set a rule that the input filter will only allow packets with source IP addresses with the prefix 202.141.129.0/24. If the attacker A1's packets with spoofed source IP addresses do not have such
a prefix, the filter will simply drop these packets at router Ry. Such a filtering facility provided by router Ryis referred to as ingress filtering. Similarly Egress filtering is used to prevent DDoS Attacks.

2) Source Address Validity Enforcement (SAVE)Protocol

It is used to enable updating of the anticipated source IP address information dynamically on each of the link. It blocks IP packets from the IP addresses which are not included in the list of the given link. It updates information about the source and the destination frequently so that Router Information table is up-to-date[16]. It assumes that the range of IP's for the router and is always stable.

3) Rate Control

It mainly focuses on the rate of arrival of packets rather than the incoming IP's. It tries to limit the arrival rate of the packets arriving a network matching a pattern.Rate control Schemes are specifically designed so that it does not affect the legitimate flow of packets and prevents the malicious overwhelmed packet flow in a network[14].
This scheme is less severe than other packet filtering methodologies.

CONCLUSION

There are several increasing types of attacks that penetrates into network which will lead to drastic degradation in security of day-to-day internet. We have concentrated on DDoS attacks detection and prevention. It is very difficult to find out the source of attack because it might spread in many sub networks. We proposed a mechanism called RAPTTS to detect the attacks as well as maintain the process of trace back without degrading the performance of network. With the help of proposed method we can detect and prevent the above mentioned DDoS attacks by maintaining the performance of network effectively..

REFERENCES

[1] **Countermeasures against Distributed Denial of Service**, A Literature Review,Manish Gupta, GayathriGopalakrishnan, and Raj Sharman, School of Management State University of New York
Buffalo, NY, USA
{mgupta3, g5, rsharman}@buffalo.edu

[2] **DDoS Attacks,Evolution, Detection, Prevention, Reaction,and Tolerance** Dhruba Kumar Bhattacharyya Jugal Kumar Kalita

[3] **DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey**
By K. Munivara Prasad, A. Rama Mohan Reddy &K.Venugopal Rao JNTUH University, India

[4] **Distributed Denial of Service :Attacks& Defences**, Fall 2011, Guest Lecture by: VamsiKambhampati

[5] International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011
DOI : 10.5121/ijcses.2011.2413 177
A Review of DDOS Attack and its Countermeasures in TCP Based Networks Akash Mittal1, Prof.Ajit Kumar Shrivastava2, Dr. Manish Manoria 3123,Department of Computer Science & Engineering, TRUBA Institute of Engineering &Information Technology, Bhopal, M.P, India,1akash_mitt87@yahoo.co.in,ajitshrivastava@rediffmail.com,manishmanoria@rediffmail.com

[6] **International Journal of Innovative Research in Computer and Communication Engineering(An ISO 3297: 2007 Certified Organization)Vol. 1, Issue 8, October 2013**
Copyright to IJIRCCE www.ijircce.com 1800 **A Survey on DDoS Attacks and DefenseApproaches**Divya Kuriakose1 V.Praveena2 PG scholar, Dept. of CSE, Dr N.G.P Institute of Technology, Coimbatore, IndiaAssociate professor, Dept. of CSE, Dr N.G.P Institute of Technology, Coimbatore, India

[7] **Denial of Service Attacks** QijunGu, PhD.Assistant ProfessorDepartment of Computer ScienceTexas State University – San MarcosSan Marcos, TX, 78666
Peng Liu, PhD. Associate Professor School of Information Sciences and Technology Pennsylvania State University
University Park, PA, 16802

[8] Yang Xiang, Member, IEEE, Ke Li, and Wanlei Zhou, Senior Member, IEEE, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011

[9] **A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks** Ruiliang Chen, Student Member, IEEE, Jung-Min Park, Member, IEEE, and Randolph Marchany, Member, IEEE

[10] **Locating Network Domain Entry and Exit point/path for DDoS Attack Traffic**
Vrizlynn L. L. Thing, Student Member, IEEE, Morris Sloman, Member, IEEE, and Naranker Dulay, Member, IEEE

[11] **Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics**
Yang Xiang, Member, IEEE, Ke Li, and Wanlei Zhou, Senior Member, IEEE

[12] **Progressive Congestion Management Based on Packet Marking and Validation Techniques**
Joan-Lluı´s Ferrer, Elvira Baydal, Antonio Robles, Member, IEEE Computer Society, Pedro Lo´pez, Member, IEEE Computer Society, and Jose´ Duato

[13] **Mitigating Routing Misbehavior in Disruption Tolerant Networks**
Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE

[14] RIHT: A Novel Hybrid IP Traceback Scheme
Ming-Hour Yang and Ming-Chien Yang

[15**] A Feasible IP Traceback Framework through Dynamic Deterministic Packet Marking**
Shui Yu, Senior Member, IEEE, Wanlei Zhou, Senior Member, IEEE, Song Guo, Senior Member, IEEE, and Minyi Guo, Senior Member, IEEE

[16] **Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing**
Qiao Yan and F. Richard Yu