Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.42 – 49

AN ATTACK DETECTOR BASED ON STATISTICAL APPROACH FOR DETECTION AND PREVENTION OF DDOS ATTACK

Snehal M. Pande[1] , Neha A. Borkar[2], Charul P. Nimbarte[3], Ankit R. Pohane[4], Mr. Vijendrasinh Thakur[5]

[1,2,3,4,5] Computer Science, Rajiv Gandhi College of Engineering & Research , Nagpur RTMNU, India

[1] snehal9795@gmail.com; [2] nehab4394@gmail.com; [3] charulnimbarte@gmail.com; [4] ankitpohane@gmail.com; [5] vijendrapthakur@gmail.com

Abstract— The name of the application is 'An Attack detector based on statistical approach for detection and prevention of DDoS attack'. This application provides an alternative way to detect a DDoS attack in a system. When more than one sender sends data packets to the single receiver in such a way that the capacity of a receiver exceeds beyond the limit hence an attack occurs decreasing the network performance. This attack can be prevented by using the statistical approach where the three parameters are observed i.e. Delay, throughput and energy. Depending on the analysis of parameters the DDoS attack is analyzed and the attack is prevented.

Keywords— Distributed Denial Of Service (DDoS), Intrusion Detection System, Statistical methods, Network security, Detection, Filtering

I. INTRODUCTION

Distributed Denial-of-Service (DDoS) attack is one in which the destination network elements are bombarded with high volume of fictitious attacking packets that originate from a large number of machines. A successful attack allows the attacker to gain access to the victim's machine, allowing stealing of personal internal data and possibly cause disruption and denial of service (DoS) in some cases. Out of the various categories of DoS attacks like flooding, software exploit, protocol based etc Distributed Denial of service attack is the most prominent. DDoS attack uses series of Zombies to initiate a flood attack against an unsafe single site. DDoS attack is initiated in 2 stages i.e. Recruiting phase and Action phase.

There are basically three main approaches for reducing attacks:

1) Detection 2) Prevention 3) Response.

Detection mechanisms try to detect attacks after they had happened. Preventive mechanisms try to free systems and protocols from attacks, while response process tries to detect attack sources and reduce their aftershock.

This makes DDoS command packets more untraceable. Moreover, it is easier for an attacker to hide the presence in an IRC channel as such channels tend to have large volumes of trace. Three primary methods of attacks for TCP, UDP, and HTTP and is found in two versions: binary and web-based. There are two types of anti-DDoS systems are host-based systems and network-based systems have been developed. Host-based systems are deployed on end-hosts. These systems typically use firewall and intrusion detection systems (IDS), and/or balance the load among multiple servers to defend against DDoS attacks. The host-based approach can help protect the server system; but it may not be able to protect legitimate access to the server, because high-volume attack traffic may overcrowd the incoming link to the server. On the other hand, network-based anti-DDoS systems are deployed inside networks, e.g., on routers.

Network-based anti-DDoS techniques can be divided into two categories: (1) detection /identification, and defense. A detection/ identification mechanism is responsible for detecting DDoS attacks and identifying attack packets or attack sources. The detection DDoS attacks, signal processing techniques (e.g., wavelet, statistical methods), and machine learning techniques can be used. To identify attack sources, IP traceback is typically used. The IP traceback techniques can contained the attack sources; but it requires large-scale deployment of the same IP traceback technique and needs alteration of existing IP forwarding mechanisms (i.e., IP header processing). To defend against DDoS attacks, traffic control mechanisms such as ingress filtering, route based packet filtering, and rate limiting, are usually used. Ingress filters or packet filters scan drop packets with spoofed source IP addresses that do not belong to the client to server networks; but their effectiveness rely on global deployment of these filters in the Internet; with a partial Deployment, spoofing source IP addresses is possible. Rate limit are deployed at each link of certain designated routers; in distinguishably drop some of the packets destined to a victim, when the victim is surge over by traffic. In this way, the volume of attack traffic will be less. Rate limiting is suitable for reducing attacks having high-data-rate on a link; but it is not suitable for reducing attacks having low data-rate on a link, since attacks with low-data-rate on a link will not trigger rate limiting operation. [3]

Network resources are more vulnerable to various types of attacks. Denial of service attack is one among the varied types of security threats identified as of now [1]. In general, out of the many types of attacks identified, denial of service is the one that exploits inter connectivity of the computer systems and is also the one which can be easily deployed. It purely concentrates on overloading a computer which is busy serving an essential service. By this, the targeted machine is made to do less useful things and thereby the essential service may not get CPU cycles and this may be interrupted. Thus it becomes necessary for the network administrators to safe guard their systems and to ensure that a smooth and uninterrupted service is available for its clients. This job however cannot be manually ensured, since a quick and immediate response from the victim side is required [4]. Thus the automation of detection and mitigation of such type of attacks has become essential to effectively stop the perpetrators from causing any major damage to our system environment.

II. EXISTING METHODOLOGY

A. Signature Based Detection approach

An intrusion detection system is a device or software application that monitors network or system for malicious activities or policy violations and products reports to a management stations. IDS come in a variety of flavours and approach the goal of detecting suspicious traffic in different ways. There are network based as well as host based intrusion detection system. NIDS is a network security system focusing on the attacks that comes from the inside of the network. When we classify the designing of the NIDS according to the system interactively property, there are two types: on line NIDS and offline NIDS. On line NIDS deals with the network in real time and it analyses the Ethernet packet and supplies it on the some other rules to decide if it is an attack or not. Off-line NIDS deals with a stored data and pass it on a some process to decide whether it is an attack or not.[10] Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. Organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

IDPSes typically record information related to observed events notify security administrators of important observed events and produce reports. Many IPSec can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

III.LITERATURE SURVEY

A. Techniques for detecting DDOS attack

***1) On-line detection method based on covariance analysis**:* The method could not only differentiate between the normal and attack traffic in flooding situations, but also detect the bare attacks that expose few apparent differences from normal behaviours. It is well known that 'The most difficult part for defending against DDOS attacks is that it is very hard to differentiate between normal traffic and attack traffic'[18].

2) Intrusion Detection System using Dempster Shafter Theory: The proposed technique includes Cloud Fusion Unit (CFU) which collects the alerts from different IDS (Intrusion Detection System) sensor VMs (Virtual Machines). The alerts will stored in the My SQL database of Cloud Fusion Unit. This Cloud Fusion Unit will analyze results using the Dempster-Shafer theory (DST) of evidence in 3-valued logic and it will apply the Fault-Tree Analysis for each IDS sensor VMs. The results of the sensors are fused using Dempster's combination rule [17].

3) Detection by identifying threshold value: Six Sigma and varying tolerance factor methods are used to identify threshold values correctly and dynamically for various statistical metrics [16].

***4) Misuse based intrusion detection*:** Misuse detection is an approach in detection attacks. In misuse detection approach, we define abnormal system behavior as normal behavior. It stands against unusual detection approach which utilizes the reverse approach defining normal system behavior as abnormal. [19].

***5) Anomaly based intrusion detection*:** An anomaly based intrusion detection system is a system for detecting both network and misuse by monitoring system and classifying it as either normal or anomalous. [19]

B. Techniques for preventing DDOS attack

Techniques for preventing against DDOS can be broadly divided into two types: (i) General techniques, are having some common preventive measures [13] i.e. system protection, copy of resources etc. that individual servers as well as ISPs should follow so they do not become part of DDOS attack process. (ii) Filtering techniques, which include ingress filtering, egress filtering, router based packet filtering, history based IP filtering etc.

a. General Techniques

***1) Disabling unused services*:** The less there are applications and open ports in hosts, the minimum there are chance to exploit vulnerabilities by attackers. Therefore, if network services are not required or unused, the services will be unable to prevent attacks, e.g. UDP echo, character generation services [6].

***2) Install latest security patches*:** Now, many DDOS attacks exploit vulnerabilities in target system. So removing known security holes by installing all relevant security patches prevents re-exploitation of vulnerabilities in the target system [6].

3) Disabling IP broadcast: Defence against attacks that use intermediate broadcasting nodes e.g. ICMP flood attacks, Smurf attacks etc. will successful only if host computers and all the neighbouring networks disable IP broadcast [7].

4) Firewalls: Firewalls can effectively prevent users from launching simple flooding type attacks from machines near by the firewall. Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. But some complicated attack e.g. if there is an attack on port 80 (web service), firewalls cannot prevent that attack because they can't distinguish good traffic from DoS attack traffic [8, 9].

***5) Global defense infrastructure*:** A global deployable protect infrastructure can prevent many DDOS attacks by installing filtering rules in the most important routers of the Internet. As Internet is use by various autonomous systems according their own local security policies, such type of global protecting architecture is possible only in theory [6].

b. Filtering Techniques

1) Ingress/Egress filtering: Ingress Filtering [5] is a restrictive mechanism to drop traffic with IP addresses that do not match a domain prefix connected to the entrance router. Egress filtering is an outbound filter, which ensures that only assigned or allocated IP address space leaves network. A key requirement for ingress or egress filtering is knowledge of expected IP addresses at particular port. For some networks with complicated topologies, it is not easy to obtain this knowledge

2) Router based packet filtering: Route based filtering, proposed by Park and Lee [11], extends ingress filtering and uses the route information to filter out burlesque IP packets. It is based on the principle that for each link in the core of Internet, there is only a limited set of source addresses from which traffic on the link could have originated.

3) History based IP filtering: During an attack, if the source address of a packet is not in IAD, the packet dropped. Hash based/Bloom filter techniques are used for fast searching of IP in IAD. This scheme is powerful, and does not need the contribution of the whole Internet community [12]

4) Capability based method: Source first sends request packets to its destination. Router marks (pre-capabilities) are added to request packet while passing through router. The destination may or may not grant permission to the source to send. If permission is allowed then destination returns the capabilities, if not then it does not supply the capabilities in the returned packet. DDoS attack, as packets without capabilities are treated as legacy and might get dropped at the router when congestion happens [13].

5) Secure overlay Service (SOS): All the traffic from a source point is verified by a secure overlay access point (SOAP). Authenticated traffic will be routed to a special overlay node called a beacon in an anonymous manner by consistent hash mapping. The beacon then forwards traffic to another special overlay node called a secret servlet for further authentication, and the secret servlet forwards verified traffic to the victim [14].

6) SAVE: Source Address Validity Enforcement: It enables routers to update the information of expected source IP addresses on each link and block any IP packet with an unexpected source IP address. The aim of the SAVE protocol is to provide routers with information about the range of source IP addresses that should be expected at each interface. [15].

IV.DESIGN ARCHITECTURE

Distributed denial of service attack (DDOS) is an enhanced and distributed version of denial of service attack [2]. DDoS attacks involve a large number of attacker machines which targets a single victim machine and generate a surge of traffic towards it. In this system, we used statistical approach to for detection and prevent DDOS attack.

***a) Creation of network*:** In this system, we first create a network scenario, consisting of various nodes. Each network is collaborated with each other. Typically a network will have router which will be an entry point to the network. A dedicated server has to be setup for traffic information collection.

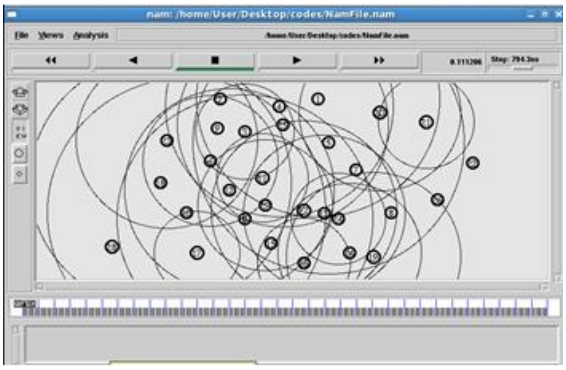

nam: /home/User/Desktop/codes/NamFile.nam
File
Views
Analysis
/home/User/Desktop/codes/NamFile.nam

Fig 1 : Network formation

***b) Demonstration of DDOS attack in network*:** As attacker send request to N zombies to attack on the target machine, the zombies started attacking toward receiver side continuously. Zombies send multiple packets to target damaging the system due to which the target system capacity exceeds the limit and it start dropping packets. This scenario states that the attack is generated in the target machine.

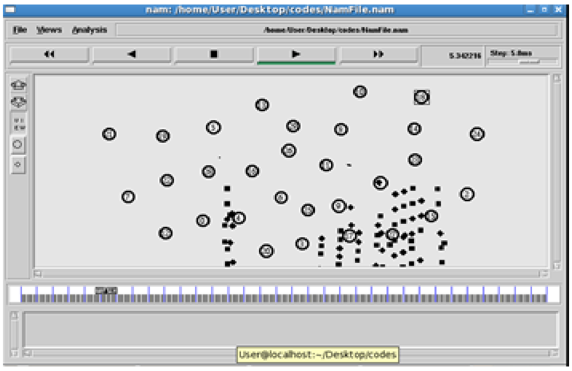

nam: /home/User/Desktop/codes/NamFile.nam
File
Views
Analysis
/home/User/Desktop/codes/NamFile.nam
5.342216
Step: 5.4ms
User@localhost:~/Desktop/codes

Fig 2 : Packet Dropping

c) Calculation of Performance Parameters**:** After attack is generated, the performance parameters are measure i.e. throughput, energy and delay. If the throughput is less and energy and delay is high then the attack is generated on the system.

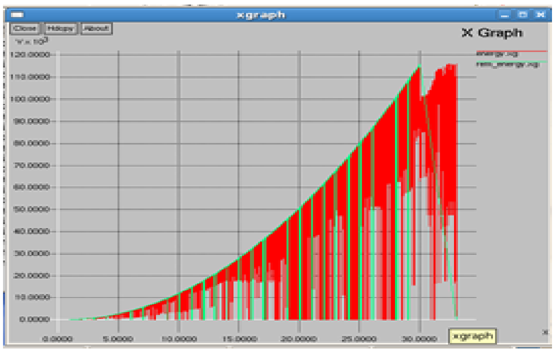
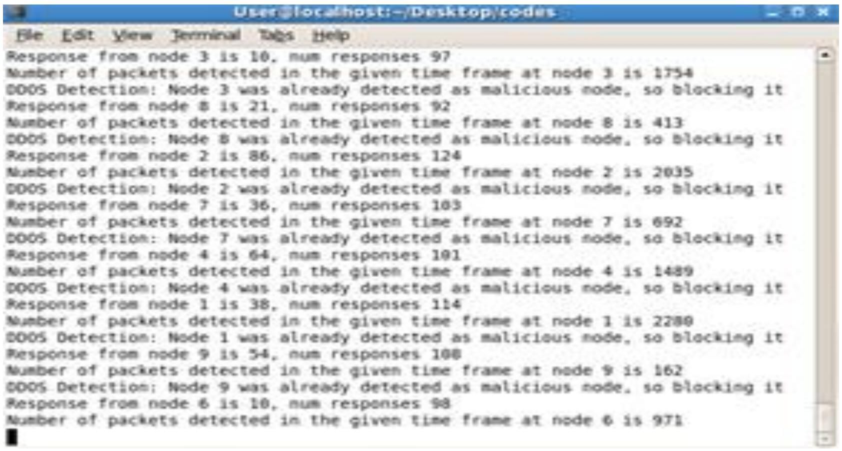


Fig 3 : Energy Graph

d) Removal of Attack: In removal of attack, if malicious nodes are found in process then it will block that node by applying level 2 so that it will not interfere in future communication. The following algorithm is used to remove the DDOS attack.



```
Response from node 3 is 10, num responses 97
Number of packets detected in the given time frame at node 3 is 1754
DDOS Detection: Node 3 was already detected as malicious node, so blocking it
Response from node 8 is 21, num responses 92
Number of packets detected in the given time frame at node 8 is 413
DDOS Detection: Node 8 was already detected as malicious node, so blocking it
Response from node 2 is 86, num responses 124
Number of packets detected in the given time frame at node 2 is 2035
DDOS Detection: Node 2 was already detected as malicious node, so blocking it
Response from node 7 is 36, num responses 103
Number of packets detected in the given time frame at node 7 is 692
DDOS Detection: Node 7 was already detected as malicious node, so blocking it
Response from node 4 is 64, num responses 101
Number of packets detected in the given time frame at node 4 is 1489
DDOS Detection: Node 4 was already detected as malicious node, so blocking it
Response from node 1 is 38, num responses 114
Number of packets detected in the given time frame at node 1 is 2280
DDOS Detection: Node 1 was already detected as malicious node, so blocking it
Response from node 9 is 54, num responses 108
Number of packets detected in the given time frame at node 9 is 162
DDOS Detection: Node 9 was already detected as malicious node, so blocking it
Response from node 6 is 10, num responses 98
Number of packets detected in the given time frame at node 6 is 971
█
```

Fig 4: Blocking of malicious node

Time Frame Based Algorithm

```
Step1:   If (APPLY_ CONTROL==1)
 Then
           If (saddr >= 0)
      Then
 PACKETS_RECEIVED=PACKETS_RECEIVED
                              + 1;
Step2:  If (APPLY_LEVEL2 == 1)
  Then
       If (MALICIOUS_NODES == saddr &&
PACKETS_RECEIVED>PACKETS_THRESHO
LD)
  Then
      Drop (p, DROP_RTR_ROUTE_LOOP);
Step3:
If(PACKETS_RECEIVED[saddr]>PACKETS_T
HRESHOLD)
          Num_dos++;
      If (APPLY_LEVEL2 == 1)
Then
      MALICIOUS_NODES = saddr;
      MALICIOUS_NODES++;
```

The removal algorithm should be relevant and robust for different scenario of attack. Generally DDOS are careful extension of highly sophisticated attack plans. It does not generally consist of careless flooding of packets, as it may turn out to be a criminal offense. So, consider two cases by which the attack may proceed. The first case is that, the attacker may have only small number of systems acting as zombies. This is because he may have had less time to gather zombies or fewer sources to do that. So generally he will try to plan an attack with this small number of systems each generating large number of packets. In this case, our algorithm detects those abnormal flows as critical and DoS and collaboratively concludes that there is an attack. We used time frame based algorithm for removal of attack. For normal communication we apply control 1, so that the sender and destinations node can perform communication without any interruption and if the sender address is greater than 0, packet received is incremented by 1.Suppose any other node interfere between the communication of two nodes then the node is consider as a malicious node and identified that node as apply level 2. If the malicious node is sender and the packet receive is exceed the capacity then it will drop the packet and detected as a DDOS attack and the node will be blocked as a malicious node. To count no. of DDOS attack we check whether these packet received by sender is greater than the packet threshold. All malicious nodes are store in a Level 2 list.

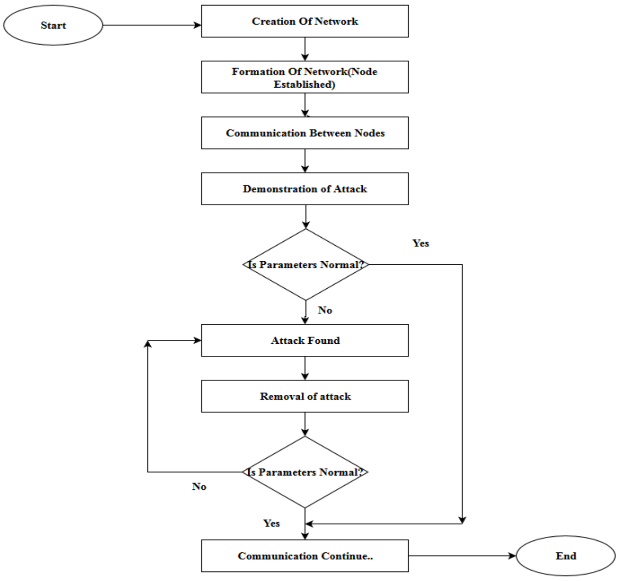


Fig 5: Flowchart

e) Parameters after attack removal and comparison**:** We then again calculate the performance parameters and compare it with previous one for verification purpose of attack removal.

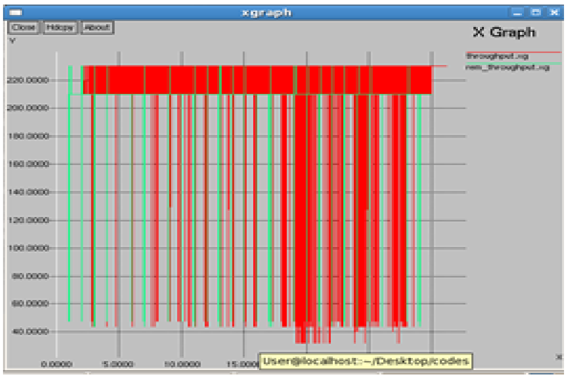


Fig 6: Graph After Attack removal

V. METHODOLOGY

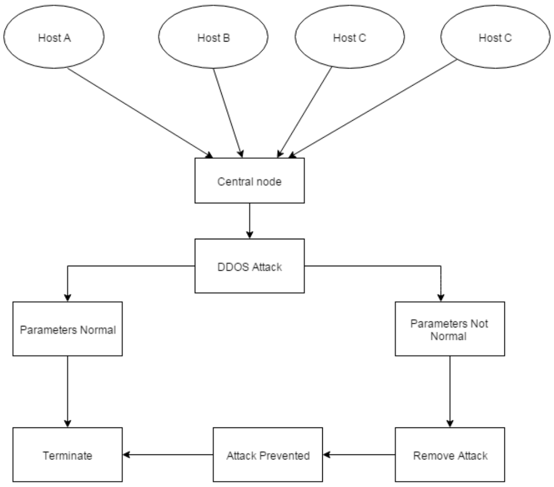


Fig 7: Activity Diagram

A**.** ***Attack generation****:* An overall view of this system architecture is provided in the fig.1.Here, multiple senders send packets to the receiver at a time. Malicious nodes are block with the help of removal algorithm. Parameter calculation is done for detection and removal of DDOS attack.

The attack generation scenario is done using TCL language. The project is implemented in NS2 platform. The front end language is TCL. The CPP code is used as a back end script on the network layer to perform protocol changes in the network. The attacking physical machines must be running UNIX type OS i.e. Fedora.

VI. CONCLUSION

The technique gives the idea of Statistical version of detection and removal of attack. The project portrays how the distributed methodology of detection provides a secure environment to the entire network domain involved rather than any particular network domain. The system involves monitoring the parameter and traffic pattern. This is an efficient technique to prevent the system from DDOS attack.

REFERENCES

[1]. S. Bellovin, J. Schiller, and C. Kaufman, "*Security Mechanism for the Internet*", RFC 3631, Internet Eng. Task Force, 2003.

[2]. H. Wang, D. Zhang, and K. Shin, "*Change-Point Monitoring for the Detection of DoS Attacks*," in the IEEE Trans. on Dependable and Secure Computing, Vol. 1, Oct.-Dec., 2004.

[3]. J. Sommers and P. Barford, "*Self-Configuring Network Traffic Generation*", in Proc. of ACM Internet Measurement Conference, Taormina, Sicily, Italy, Oct. 25-27, 2004.

[4]. K.M.Elleithy., D.Blagovic., W.Cheng. and P.Sideleau., "*Denial of Service Attack Techniques: Analysis, Implementation and Comparison"*, Systemics, Cybernetics and Informatics Vol. 3,No 1, 2006.

[5]. Yu Chen, "*Collaborative Detection of DDoS Attacks over Multiple Network Domains*", in the IEEE Transaction on Parallel and Distributed Systems, 2007.

[6] X. Geng, A.B. Whinston, "*Defeating Distributed Denial of Service attacks*", IEEE IT Professional 2 (4) (2000) 36–42.

[7] Felix Lau, Rubin H. Stuart, Smith H. Michael, and et al., "*Distributed Denial Of Service Attacks*," in Proceedings of 2000 IEEE International Conference on Systems, Man, and Cybernetics, Nashville, TN, Vol.3, pp.2275-2280, 2000.

[8] R. Oppliger,"*Internet Security: firewall and beyond*," Communications of the ACM, Volume 40, Issue 5, pp. 92-102, 1997.

[9] McAfee, "*Personal Firewall*". Available at: http://www.mcafee.com/ myapps/ firewall/ov_firewall.asp

[10] P. Ferguson, and D. Senie, "*Network ingress filtering: Defeating denial of ser-vice attacks which employ IP source address spoofing*," RFC 2267, the. Internet Engineering Task Force (IETF), 1998.

[11] K. Park, and H. Lee, "*On the effectiveness of router-based packet filtering for distributed DoS attack prevention in power-law Internets*," Proceedings of the ACM SIGCOMM Conference, 2001, pp. 15-26, 2001.

[12] T. Peng, C. Leckie, K. Ramamohanarao, "*Protection from Distributed Denial of Service attack using history-based IP filtering*," in Proceedings of IEEE International Conference on Communications (ICC 2003), Anchorage, AL, USA, Volume 1, pp. 482-486, 2003.

[13] T. Anderson, T. Roscoe, D. Wetherall, "*Preventing Internet Denial-of-Service with Capabilities*," In ACM SIGCOMM Computer Communication Review, Volume 34, issue 1, January 2004, pp. 39-44

[14] A. D. Keromytis, V. Misra, and D. Rubenstein, "*SOS: Secure Overlay Services*," in the Proceedings of. ACM SIGCOMM, pp. 61-72, 2002.

[15] J. Li, J. Mirkovic, M. Wang, and P. Reither, "*Save: Source address validity enforcement protocol*," Proceedings of IEEE INFOCOM, 2002, pp. 1557-1566.

[16] B. B. Gupta, Manoj Misra and R. C. Joshi, "*An ISP Level Solution to Combat DDoS Attacks using Combined Statistical Based Approach*".

[17] Iqra Sattar, Muhammad Shahid, Younis Abbas, "*A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment*".

[18] Shuyuan Jin, Daniel S. Yeung," *A Covariance Analysis Model for DDoS Attack Detection*".

[19] Monowar H. Bhuyan1, H. J. Kashyap1, D. K. Bhattacharyya1 and J. K. Kalita2,"*Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions*".