A Review Of Detection of DDOS Attack Using Entropy Based Approach
1Surender Singh, 2Sandeep Jain
1,2Dept. of CSE, Kurukshetra University, DIET, Karnal, Haryana, India

Abstract
Web-sites acts as the best platforms for attacks like DDOS attack worm propagation and many other attacks which are related to application layer. To detect application layer DDOS attack is a cumbersome task. It is basically originated from the lower layer i.e. network layer and transport layer. Whereas this new application layer based DDOS attacks utilizes genuine HTTP request to make victim resources busy somewhere else which are undetectable. Various tools like hyenae, strut, LOIC, HOIC etc have been used to see the scenario of DDOS attack on various websites. Distributed framework helps to increase the quality of response for genuine traffic under DDOS attacks. A distributed solution is required for the distributed nature of DDOS attack. Hence we will propose architecture for the defense which can efficiently detect these attacks. The behaviors of packet flows will be analyzed. Entropy based detection and trace back algorithm will be used, which efficiently distinguish the malicious flows from the legitimate flows. This work includes simulation and their performance analysis of our proposed framework.

Keywords
Entropy, DDOS, Hyenae, LOIC, HOIC, Transmission Delay.

I. Introduction
Denial of service is an intentional attempt to completely disrupt or degrade availability of service/resources to authorized/genuine user by attackers. Exploiting of weakness in internet protocol, application, and operating system is done by these attacks. Some well known DOS attacks are sync flood, tear drop, smurf, ping of death, land, finger, bom, black holes, octopus, shork, ARP cache poisoning.
DDOS attacks are advanced/huge form of DOS attack where attackers hire hundreds or even thousands of compromised host called zombies against a single target.

It can be divided into two categories:
1. Bandwidth attack
2. Resource attack
Now App-DDOS attacks are those which focus on exhausting the server resources such as sockets, CPU, memory, disk/database bandwidth and input/output bandwidth. The app-DDOS uses the weakness enabled by the standard practice of opening services such as HTTP and HTTPS (TCP Port 80 and 443).

II. DDOS Attacks
A Denial-Of-Service attack (DOS attack) or distributed denial-of-service attack (DDoS attack) is a way which denies giving services to its intended users. Various attackers do all these with different modes, intention and target. But it generally consists of the concerted efforts of a person, or multiple people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Saturating the target machine with external communications requests is one of the common methods, such that it cannot respond to legitimate traffic, or responds slowly. Such attacks usually lead to a server overload. In general terms, DOS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

III. Symptoms of Denial-of-Service Attacks
1. Network performance becomes very slow (opening _les or accessing web sites)
2. Unavailability of a particular web site.
3. Dramatic increase in the number of spam emails received (this type of DOS attack is considered an e-mail bomb)

IV. Methods of Attack
1. Consumption of computational resources, such as bandwidth, disk space, or processor time.
2. Disruption of state information, such as unsolicited resetting of TCP sessions.
3. Disruption of physical network components.
4. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

V. Related Works
M. Glenn, [1], in “A summary of DOS/DDOS prevention, monitoring and mitigation techniques in a service provider environment”, describes that the frequency and sophistication of Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) on the Internet are rapidly increasing. Service providers are under mounting pressure to prevent, monitor and mitigate DoS/DDoS attacks directed toward their customers and their infrastructure.
The Internet is part of the critical national infrastructure but is unique in that it has no customary borders to safeguard it from attacks. Attacks that are seen every day on the Internet include direct attacks, remote controlled attacks, reflective attacks, worms, and viruses.

Specific attacks directed at a service provider’s infrastructure can be very damaging and cause wide spread outages. This paper covers these attacks and discusses techniques to prevent attacks including good security policies, new/updated product security testing, and patch management, spoofed packet dropping (uRPF) and firewall/IDS/IPS deployment in a service provider environment. Protection of the provider’s infrastructure is another key aspect and is addressed in this paper.

Attack monitoring and mitigation is a crucial part of a service provider’s operation. DoS/DDoS and DRDoS monitoring techniques are reviewed and practical mitigation techniques are discussed. Widespread deployment of remotely triggered black hole filtering is a quick and effective way of mitigating many of these attacks. New techniques that combine uRPF, rate limiting and granular filtering lists with black hole filtering are providing service providers with a new arsenal of tools to keep up with the ever escalating arms race on the Internet.

Fasheng Yi, et al. [2], in “Source-Based Filtering Scheme against DDoS Attacks”, describes that IP address spoofing is employed by a lot of DDoS attack tools. Most of the current research on DDoS attack packet filtering depends on cooperation among routers, which is hard to achieve in real campaigns. Therefore, in this paper, the author propose a novel filtering scheme based on source information in this paper to defend against various source IP address spoofing. The proposed method works independently at the potential victim side, and accumulates the source information of its clients, for instance, source IP addresses, hops from the server during attacks free period. When a DDoS attack alarm is raised, we can filter out the attack packets based on the accumulated knowledge of the legitimate clients. We divide the source IP addresses into (uRPF) and firewall/IDS/IPS deployment in a service provider network.

C. Lin, et al [3], in “An Effective Priority Queue-Based Scheme to Alleviate Malicious Packet Flows from Distributed DoS Attacks”, describes that A Distributed Denial-of-Service attack affects the bandwidth or resources of a targeted system. By flooding networks and disrupting access to services, it may cause damage on multimedia network services and Internet Service Providers. In this paper, the authors propose to analyze the behavior of packet flows and adopt a priority queue-based algorithm that assign packets from normal users to a high priority queue and packets from suspected attackers to a low priority queue. Simulations in network simulator, NS2, prove our proposed priority queue-based scheme is effective in blocking attacking traffic while maintaining constant flows for legitimate users.

Yi Xie, et al [4], in “Monitoring the Application-Layer DDoS Attacks for Popular Websites”, describes that Distributed denial of service (DDoS) attack is a continuous critical threat to the Internet. Derived from the low layers, new application-layer-based DDoS attacks utilizing legitimate HTTP requests to overwhelm victim resources are more undetectable.

The case may be more serious when such attacks mimic or occur during the flash crowd event of a popular Website. Focusing on the detection for such new DDoS attacks, a scheme based on document popularity is introduced. An Access Matrix is defined to capture the spatial-temporal patterns of a normal flash crowd. Principal component analysis and independent component analysis are applied to abstract the multidimensional Access Matrix. A novel anomaly detector based on hidden semi-Markov model is proposed to describe the dynamics of Access Matrix and to detect the attacks. The entropy of document popularity fitting to the model is used to detect the potential application-layer DDoS attacks. Numerical results based on real Web traffic data are presented to demonstrate the effectiveness of the proposed method.

T. Peng, et al. [5], “Protection from distributed denial of service attacks using history-based IP filtering” describes that In this paper, the authors introduce a practical scheme to defend against distributed denial of service (DDoS) attacks based on IP source address filtering. The edge router keeps a history of all the legitimate IP addresses which have previously appeared in the network. When the edge router is overloaded, this history is used to decide whether to admit an incoming Ip packet. Unlike other proposals to defend against DDoS attacks, our scheme works well during highly-distributed DDoS attacks, i.e., from a large number of sources. The author present several heuristic methods to make the IP address database accurate and robust, and the author present experimental results that demonstrate the effectiveness of our scheme in defending against highly-distributed DDoS attacks.

S. Tanachaiwiwat, et al [6], “Differential packet filtering against DDoS flood attacks”, describes that the authors present a new packet filtering scheme, which is traffic-smart to defend against network worms and flood attacks. The scheme prevents malicious hackers from orchestrating DDoS flooding attacks on any IP-based public network. All packets from each IP source are counted and timed during their life cycles. Special IP counters and timers are used to support the filtering process. This new approach mitigates flood attacks through adaptive filtering with differential quality of services provided to good and bad packets. The authors show the implementation requirements of the schemes on network routers or firewalls. Through an example traffic and filter setting, the authors demonstrate the advantages of the differential packet filtering. An improvement factor of 45 % was achieved, compared with the static routing without discrimination between good and bad packets. Index Terms: DDoS attacks, IP address spoofing, packet filtering, network routers, stateful firewalls, quality of service, and intrusion detection system

VI. Conclusion
As DDoS attacks become an increasingly frequent disturbance of the global internet, proper attention is being given to these area. After analyzing many existing DDoS detection and response techniques and defense framework, we found many major criteria of DDoS defence.

They are to detect attacks quickly and with high effectiveness and to control attack traffic so as to sustain quality of detection and response for legitimate traffic. To solve these challenges entropy based defense framework have been proposed. Basically the defense framework can be divided into three phases. Entropy-based detection technique can detect the attack if there are anomalous variation of en-tropy in the packet own.
We have included the clustering algorithm which keeps out all those clusters/objects which have the higher number of hits. This is done recursively. As our defence strategy has simple calculation, high sensitivity, low false positive rate, and lastly no need of additional network traffic device. There have been a large growth of social networks for example twitter, facebook, MySpace in recent years. Attractive means of interactions and communication are offered by these social networks, at the same time they also have issues of security and privacy. So our proposed framework can secure those sites.

VII. Future Scope

In future, evaluation of framework for more internet topologies can be done. In particular, it can be planned to investigate the following issues in more detail.
1. The future enhancement which is required is the rate limiting technique can be added to this framework.
2. Also another important point is the recovery of the traffic. As in our framework we have not considered so the legitimate users are unable to utilize the resource quickly and effectively during recovery.

References