ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Detection and Mitigation of DDOS Attacks By Circular IPS Protection Network

S. Shanthini Priyanka[1], S. Hasan Hussain[2]

Department of Computer Science and Engineering, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India[1, 2]

ABSTRACT— One of the major threat in most of the networks is the distributed denial of service and its mitigation is another important concern, This paper addresses this problem by using the firecol whose core is composed of a ring of Intrusion prevention systems(IPS) defends by exchanging only a selected traffic. In this paper, we address the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms of the circular protection network. The coreis composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information. The firecol can protect the system even if more than 100GB of messages are sending by the same attacker to the victim. It is a more effective and efficient way to protect the system from the DDOS attack.

KEYWORDS— IPS, Mitigation, flooding, Distributed denial-of-service (DDoS), Detection.

I.INTRODUCTION

The distributed denial of service (DDoS) attack is a serious threat to the security of Internet. Distributed DOS (DDoS) is a large-scale, coordinated attack on a victim system or network resource. Launched indirectly through many compromised computers on the Internet DDoS attack countermeasures can be categorized into four classes: prevention, detection, mitigation, and traceback, of which detecting and mitigating these kind of attack is a real challenge. Defending against DDoS attacks is challenging for two reasons. First, the number of attackers1 involved in a DDoS attack is very large. Even if the volume of traffic sent by a single attacker might be small, the volume of aggregated traffic arriving at the victim host is overwhelming. Second, attackers usually spoof their IP addresses, which make it very difficult to trace the attack traffic back to its sources. Unfortunately, detecting a botnet is also hard, and efficient solutions may require to participate actively to the botnet itself [2], which raises important ethical issues, or to first detect botnet-related malicious activities (attacks, infections, etc.), which may delay the mitigation. To avoid these issues, this paper focuses on the detection of DDoS attacks. Although non distributed denial-of-service attacks usually exploit vulnerability by sending few carefully forged packets to disrupt a service, DDoS attacks are mainly used for flooding a particular victim with massive traffic as highlighted in [1]. In fact, the popularity of these attacks is due to their high effectiveness against any kind of service since there is no need to identify and exploit any particular service-specific flaw in the victim. Hence, this paper focuses exclusively on flooding DDoS attacks. A single intrusion Prevention System is capable of detecting such attacks only if it is close to the victim hence to overcome this problem a circular network that comprises of multiple intrusion prevention system is used that forms a collaborative protection network around the node to be protected detecting the DDoS attacks, this circular protection network uses some of the metrics like maximum bandwidth it allows, entropy rate, score lists it maintains based on the previous observations to detect the attack. In addition to detecting the DDos attacks it also detects attacks caused by Botnets. This paper proceeds as follows. Section II describes the related work and the global operation of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

the circular protection network. This paper proceeds as follows. Section III describes the architecture and the global operation of system. The different leveraged metrics and components of the system are presented in Section III. Section IV presents components. Section V explains the conclusion and future works

II.RELATED WORK

Botnets are prevailing mechanisms for the facilitation of the distributed denial of service (DDoS) attacks on computer networks or applications. Currently, Botnet-based DDoS attacks on the application layer are latest and most problematic trends in network security threats. Botnet-based DDoS attacks on the application layer limits resources, curtails revenue, and yields customer dissatisfaction, among others. DDoS attacks are among the most difficult problems to resolve online, especially, when the target is the Web server[3].

The goal of a Botnet based DDoS attack is to entail damage at the victim side. In general, the ulterior motive behind this attack is personal which means block the available resources or degrade the performance of the service which is required by the target machine. Therefore, DDoS attack is committed for the revenge purpose. Another aim to perform these attacks can be to gain popularity in the hacker community. In addition to this, these attacks can also perform for the material gain, which means to break the confidentiality and use data for their use.

A. Botnet Based DDoS Attack Architecture

Botnet based DDoS attack networks fall under three categories, namely, the agent-handler, IRC-based, and Web-based models.

1)Agent-Handler Model

The agent-handler model of a DDoS attack comprises clients, handlers, and agents as shown in Figure 2. The client is one with whom the attacker communicates in the DDoS attack system. The handlers are software packages located throughout the Internet. The client uses these packages to communicate with the agents. The agent software thrives in compromised systems, eventually conducting the attack at the appropriate time. The attacker communicates with any of the handlers to identify operational agents and to determine when to attack or to upgrade agents. Owners and users of agent systems are typically unaware that their system has been compromised and is under a DDoS attack. Depending on the configuration of the DDoS attack network, agents can be instructed to communicate with one handler or with multiple handlers. Attackers often attempt to install the handler software on a compromised router or network server. The target typically handles large volumes of traffic, making message identification difficult between the client and the handler and between the handler and the agents. The terms —handler and —agents are sometimes replaced with —master and —demons, respectively, in descriptions of DDoS tools [4].

2)Internet Relay Chat (IRC) Model

An IRC channel benefits an attacker with the use of —legitimate IRC ports to send commands to agents. The use of legitimate ports hinders the tracking DDoS command packets. Additionally, IRC servers tend to have large volumes of traffic, enabling an attacker to conceal its presence easily. The attacker does not necessarily maintain a list of the agents because it can immediately enter the IRC server and view all available agents [5]. The agent software in the IRC network sends and receives messages through the IRC channel and informs the attacker when an agent becomes operational.

3) Web-based Model

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Although the most preferred method for Botnet command and control (C&C) is the IRC-based model, Web-based reporting and command has emerged over the past few years. A number of bots in the Web-based model simply report statistics to a Web site, whereas others are intended to be fully configured and controlled through complex PHP scripts and encrypted communications over the 80/443 port and the HTTP/HTTPS protocol.

B. Classification Of Botnet Based DDoS Attacks

The wide variety of DDoS attacks indicates the various conducted taxonomies of such attacks [4, 6-9]. New kinds of attacks are identified daily, and some remain undiscovered. In this work, we focus on Botnet based DDoS attacks that affect the application layer, especially the Web server [28]. The type of DDoS attack depends on the vulnerability of exploitation. The first type of attack is characterized by the consumption of the resources of the host. The victim can generally be a Web server or a proxy connected to the Internet. When the traffic load is high, packets are sent out to inform senders, who can either be legitimate users or attack sources, to reduce their sending rates. Legitimate users respond by decreasing their sending rates, whereas attack sources maintain or even increase their sending rates. Consequently, resources of the host, such as the CPU or memory capacity, become depleted, and the host is hindered from servicing legitimate traffic. The second type of attack involves the consumption of network bandwidth. If malicious traffic in the network dominates the communication links, traffic from legitimate sources is obstructed. In effect, bandwidth DDoS attacks are more disruptive than attacks resulting in resource consumption [7]. Detail discussion of these attacks is given below:

1)Net DDoS-based Bandwidth Attacks

Net DDoS-based bandwidth attacks are normally introduced effectively from a single attack source that takes advantage of specific IP weaknesses. Examples of such attacks are SYN and ICMP flood attacks.

A SYN flood attack utilizes a vulnerability of the TCP three-way handshake, such that a server must contain a large data structure for incoming SYN packets regardless of authenticity. During SYN flood attacks, SYN packets are sent by the attacker with unknown or non-existent source IP addresses. The three-way handshake occurs when the server stores the request information from the client into the memory stack and then waits for client confirmation. Given that the source IP addresses in SYN flood attacks are unknown or non-existent, confirmation packets for the requests created by the SYN flood attack are not received. Each half-open connection accumulates in the memory stack until it times out. Hence, the memory stack becomes full. Consequently, no requests can be processed, and the services of the system are disabled. Thus, SYN flood attacks are considered one of the most powerful flooding methods [13]. ICMP is based on the IP protocol that can diagnose the status of the network. An ICMP flood attack is a bandwidth attack that uses ICMP packets that can be directed to an individual machine or to an entire network. When a packet is sent from a machine to an IP broadcast address in the local network, all machines in the network receive the packet. When a packet is sent from a machine to the IP broadcast address outside the local network, the packet is delivered to all machines in the target network. Other types of ICMP flood attack are the SMURF and the Ping-of-Death attacks [31].

2) App-DDoS Attacks

Attack power can be amplified by forcing the target to execute expensive operations. These attacks can consume all available corporate bandwidth and fill the pipes with illegitimate traffic. Routing protocols can also be affected and services are disrupted by either resetting the routing protocols or offering data that harm server operation [29].

C . DDoS Attack Detection And Mitigation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

As DDoS attackers pursue monetary profit, critical Internet sites (CISs) become a good target. These attacks will be more difficult to defend because the botnet size continuously increases, and the attackers spare no pains in preparing the attacks. We observe that CISs can continue their main businesses if most important clients can access the services. This motivates us to build a whitelist[15], called a VIP list in this article, and the source addresses in the list are given higher priority when the CIS is under attack. The VIP list is built from the previous login logs of authentication processes at the application layer. The experimental results showed that the proposed scheme effectively mitigates DDoS attacks[3].The next is about application-layer resource attacks as either request flooding, asymmetric, or repeated one-shot, on the basis of the application workload parameters that they exploit. To protect servers from these attacks, a counter-mechanism namely *DDoS Shield[13]* that consists of a suspicion assignment mechanism and a DDoS-resilient scheduler is used. This suspicion mechanism assigns a continuous value as opposed to a binary measure to each client session, and the scheduler utilizes these values to determine if and when to schedule a session's requests. Using test bed experiments on a web application, the potency of these resource attacks and the efficacy of our counter-mechanism is evaluated[4].Defending against Distributed Denial of Service (DDoS) attacks based on IP source address filtering [14]uses the edge router that 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, this scheme worked well during highly-distributed DDoS attacks, i.e., from a large number of sources, several heuristic methods were proposed to make the IP address database accurate and robust[5].When compared with higher-rate distributed denial of service attacks, allow-rate distributed denial of service (DDoS) attack has significant ability of concealing its traffic because it is very much like normal traffic. It has the capacity to elude the current anomaly-based detection schemes. Information metric can quantify the differences of network traffic with various probability distributions. Which was detected using two new information metrics such as the generalized entropy metric and the information distance metric to detect low-rate DDoS attacks by measuring the difference between legitimate traffic and attack traffic. The entropy metric [6] that were proposed detect attacks several hops earlier than the traditional Shannon metric.

III.ARCHIETECTURE

A. Circular Protection System

The circular system (Fig. 1) maintains virtual rings or shield of protection around registered customers. A ring is composed of a set of IPSs that are at the same distance (number of hops) from the customer (Fig. 2). As depicted in Fig. 1, each IPS instance analyzes aggregated traffic within a configurable *detection window*. The *metrics manager* computes the frequencies and the entropies of each rule. A rule describes a specific traffic instance to monitor and is essentially a traffic filter, which can be based on IP addresses or ports. Following each detection window, the *selection manager* measures the deviation of the current traffic profile from the stored ones, selects out of profile rules, and then forwards them to the *score manager*. Using a decision table, the *score manager* assigns a score to each selected rule based on the frequencies, the entropies, and the scores received from upstream IPSs Using a threshold, a quite low score is marked as a *low potential attack* and is communicated to the downstream IPS that will use to compute its own score. A quite high score on the other hand is marked as *high potential attack*. However, since the entire traffic cannot be possibly monitored, we promote the usage of multiple levels and collaborative filtering described previously for an efficient selection of rules, and so traffic, along the process. In brief, to save resources, the *collaboration manager* is only invoked for the few selected candidate rules based on resource-friendly metrics.

B. Subscription Protocol

The circular system protects subscribers (i.e., potential victims) based on defined rules. A *system* rule matches a pattern of IP packets. Generally, this corresponds to an IP sub network or a single IP address. However, the rule definition can include any other monitor able information that can be monitored, such as the protocols or the ports used. It is an added value service to which customers subscribe using the protocol depicted in Fig. 3. The protocol uses a trusted server of the ISP that

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

issues tokens. When a customer subscribes for the *FireCol* protection service, the trusted server adds an entry with the subscribing rule along with its subscription period (TTL) and the supported capacity. The server then issues periodically a corresponding token to the customer with TTL and a unique ID signed using its private key. All communications between subscribers and the server are secured a using private/public key encryption scheme.

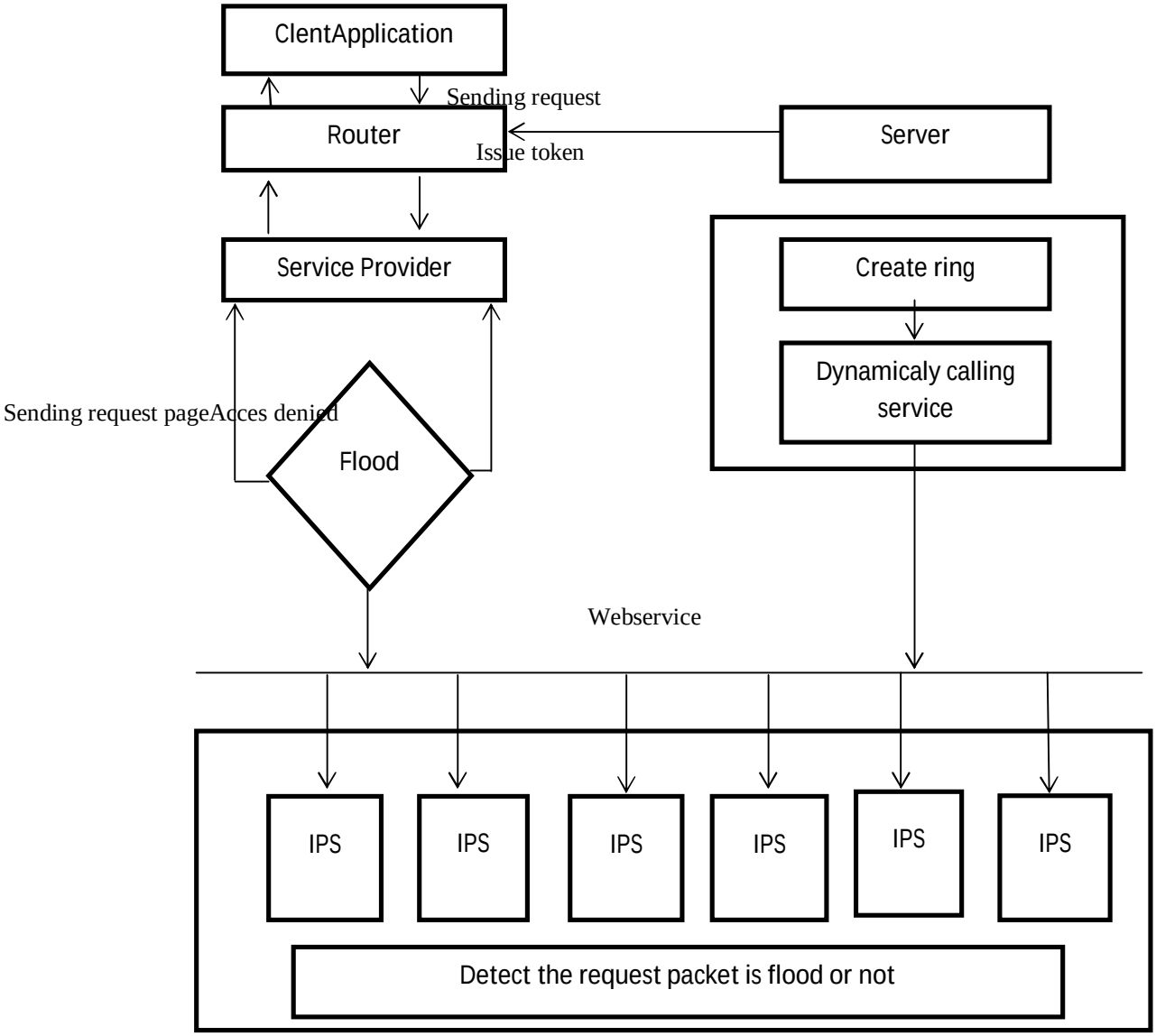

Fig.1. Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

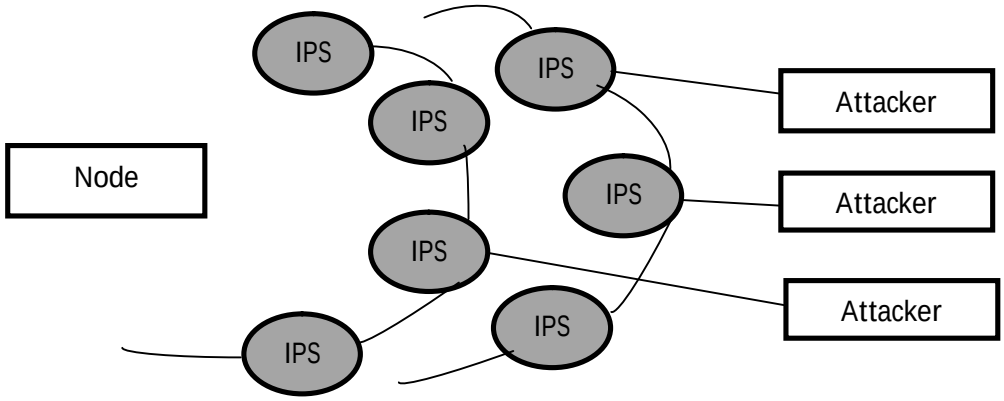

Fig. 2. IPS Protection from flooders.

IV.SYSTEM METRICS

With set of rules R=$\{r_i | i \epsilon [0,n]\}$, *FireCol* maintains the following frequency and entropy-based metrics.

1)Frequency: The frequency f_i is the proportion of packets matching rule r_i within a detection window

$$f_i = \frac{F_i}{\Sigma_{j=1}^{n} F_j} \qquad (1)$$

where F_i is the number of packets matched by rule r_i during the detection window.

2) Entropy: The entropy [(2)] measures the uniformity of distribution of rule frequencies. If all frequencies are equal (uniform distribution), the entropyis maximal, and the more skewed the frequencies are, the lower the entropy is.

$$H = -E[log_n f_i] = -\Sigma_{i=1}^{n} f_i log_n(f_i) \qquad (2)$$

V.COMPONENTS

The *FireCol* system is composed of several collaborating IPSs each enriched with the following components

1) Packet Processor: The packet processor examines traffic and updates elementary metrics (counters and frequencies) whenever a rule is matched.

2) Metrics Manager: The metrics manager computes entropies and relative entropies.

3) Selection Manager: The *detection_window_ended* event (Fig. 1) is processed by the *selection manager*, which checks whether the traffic during the elapsed detection window was within profile. It does so by checking whether the traffic distribution represented by frequencies follows the profile. This corresponds to check if the frequencies and the entropy

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

rates (2) are less than the threshold values if it exceeds the threshold value then they are marked as abnormal entries and their access is denied.

4) Score Manager: The *score manager* assigns a score to each of the selected rules depending on their frequencies and the entropy. The entropy and the frequency are considered high if they are respectively greater than a threshold and the different cases:

1) *High entropy and High rule frequency:* In this case, the traffic is well distributed, meaning that most rules have about the same frequency (they cannot be all high as the sum is one). Hence, having one rule that is quite different from the others is a good sign that it is a potential attack.

2) *Low entropy and High rule frequency:* In this case, the attack is only potential, but not as much as when the entropy is high. In Fig. 6, the black distribution has several high and low frequencies, and it is not clear if the high frequencies represent direct threats as they can be only due to the low values of other frequencies.

3) *High entropy and Low rule frequency:* This case represents a potential threat. Here, all frequencies are about the same, making it not a threat as the frequency is low. However, since it is increasing and deviates from the profile (first selection by the *selection manager*), it may surpass other frequencies later on in time.

4) *Low entropy and Low rule frequency:* This case includes both high and low frequencies because of the low entropy. Thus, it is not possible to conclude about any threat.

5) Collaboration Manager: The *collaboration manager* is the last component in charge of confirming potential attacks. We claim that detecting a flooding attack can be confirmed only if the traffic it generates is higher than the customer's capacity. Hence, the IPS where the alert is triggered has to initiate a ring level communication to calculate the average traffic throughput for subsequent comparison with the subscriber's capacity.

VI.CONCLUSION AND FUTURE WORKS

Thus the Circular Protection Network system could effectively detect and mitigate DDoS attacks by means of detection and mitigation algorithms based on the history based filtering methods and other filtering parameters. The future work includes the filtering by increasing the ring numbers and the parameters considered for filtering.

VII.REFERENCES

[1] A. Networks, Arbor, Lexington,MA, "Worldwide ISP security report,"Tech. Rep., 2010.

[2] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling, "Measurementsand mitigation of peer-to-peer-based botnets: A case study on storm worm," in Proc. USENIX LEET, 2008, Article no. 9.

[3] S. Byers, et al., "Defending against an Internet-based attack on the physical world," ACM Transactions on Internet Technology (TOIT), vol. 4, pp. 239-254, 2004.

[4] S. M. Specht and R. B. Lee, "Distributed denial of service: Taxonomies of attacks, tools, and countermeasures," in the Proceedings of the International Workshop on Security in Parallel and Distributed Systems, 2004, pp. 543-550.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[5] V. Company, "Distributed Denial of Service (DDoS) and Botnet Attacks," An iDefense Security Report, 2006.

[6] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, vol. 34, pp. 39-53, 2004.

[7] B. B. Gupta, R. C. Joshi, M. Misra, ―An ISP level solution to combat DDoS attacks using combined statistical based approach, International Journal of Information Assurance and Security (JIAS), 3 (2), pp. 102-110, 2008.

[8] U. Tariq, et al., "A comprehensive categorization of DDoS attack and DDoS defense techniques," Advanced Data Mining and Applications, pp. 1025-1036, 2006.

[9] A. Asosheh Dr and N. Ramezani, "A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification," WSEAS Transactions on Computers, vol. 7, pp. 281-290, 2008.

[10] B. B. Gupta, R. C. Joshi, M. Misra, ―Defending against Distributed Denial of Service Attacks: Issues and Challenges, Information Security Journal: A Global Perspective, vol. 18, issue 5, Taylor & Francis, UK, pp. 224-247, 2009. DOI: 10.1080/19393550903317070

[11] Debasish Das, Utpal Sharma, D. K. Bhattacharyya., "Detection of HTTP flooding attacks in multiple scenarios," in the proc. of ICCCS-2011, 2011, pp.517-522.

[12] A Mishra, BB Gupta, RC Joshi, ―A Comparative Study of Distributed Denial of Service Attacks, Intrusion Tolerance and Mitigation Techniques," In the proc. of European Intelligence and Security Informatics Conference (EISIC-2011), , pp. 286-289, 2011. [13] D. C. Wyld, et al., "Trends in Network and Communications," International Conferences, NeCOM, 197: Springer, 2011.

[14]. DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks Supranamaya Ranjan, Member, IEEE, Ram Swaminathan, Mustafa Uysal, Antonio Nucci, Senior Member, IEEE,and Edward Knightly, Senior Member, IEEE

[15]Using Whitelisting to Mitigate DDoS Attacks on Critical Internet Sites

[16]T. Peng, C. Leckie, and K. Ramamohanarao, "Protection from distributed denial of service attacks using history-based IP filtering," in Proc. IEEE ICC, May 2003, vol. 1, pp. 482–486.

[17]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