An automatic IP Falsifying Attacks detection using Hop Count Filtering and Round-Trip Time

Dr Raghavender K V Assoc Prof CSE department G NARAYANAMMA INSTITUTE OF TECHNOLOGY AND SCIENCE SHAIKPET HYDERABAD, drkvraghavender@gmail.com

ABSTRACT

A DDoS attack is a DoS attack which relies on multiple compromised hosts in the network to attack the victim, thereby, bringing down its performance. Majority of DDoS attack tools utilize IP spoofing technology that makes it very difficult to filter illegitimate packets from aggregated traffic as IP addresses can be forged easily. The existing research work contains the problems related to higher computational time and low detection rate of illegitimate packets. In this paper, we have proposed Distributed Probability based Hop Count Filtering using RTT (DPHCF-RTT) technique to improve the above said limitations by maximizing the detection rate of illegitimate packets and reducing the computation time. It has the advantage for resolving the problems of network bandwidth jam and host resources exhaustion. Round Trip Time (RTT) provides valuable information that would help improve the efficiency of probabilistic DHCF technique which solely relies on Hop Count. Proposed technique DPHCF-RTT has shown maximum detection rate up to 99% of malicious packets with maximum 4 numbers of hops with minimum Computation time.

INTRODUCTION

A Denial of Service (DoS) is an attack with the purpose of preventing legitimate users from using a victim server or network resources. The attackers are not going to thieve, modify or remove the information exchanged on networks, but they attempt to impair a network service. A Distributed Denial of Service (DDoS) attack is exemplified as a comprehensive, large-scale, and coordinated attack that deploys many computers to launch attack indirectly through many compromised computers on the Internet to achieve its goal.

In DDoS attack, attacker fills the network bandwidth with large amount of request packets, thus consuming the bandwidth. It can be performed at network level, operating system level, and application level. Even the most popular websites like Twitter, Facebook, Google etc couldn't escape from being hit by it, which caused millions of their users affected [14]. The most eye opener case was the DDoS incident that targeted White house, Federal Trade Commission and the Department of the Treasury. A Botnet, comprised of 30,000–60,000 infected computers, had been

used. The attack traffic consumed 20-40 gigabytes of bandwidth per second. It was the largest attack traffic observed. Such attack caused target outage for 4-5 days which was the longest outage duration ever [4] [24][25][26][27][28][29].

DDOS ATTACKS AND DEFENSEMECHANISMS

DoS attacks is considered when a computer or a network is incapable of providing the desired services. These types of attack doesn't cause damage to the data but make the resources unavailable to the users [5]. Attack patterns are descriptions of common methods for exploiting software [1]. Attack Pattern is a process of identifying attackers view, give the information about the type of attack, prerequisites of an attack, weakness of attack, the knowledge required to perform an attack and all the information about the attack that had been occurred in the network.

Two main classes of DDoS attacks are: bandwidthand resource depletion attacks [8] as shown in Fig. 1. In bandwidth depletion attack, victim network is flooded with unwanted traffic that prevents legitimate traffic from reaching the victim system. It can be defined as any activity that aims to disable the services provided by the victim by sending an excessive volume of useless traffic. A resource depletion ties up the resources of a victim system. This type of attack targets a server or process at the victim making it unable to legitimate requests for service [2]. There are two major impacts of bandwidth attacks. The first is the consumption of the host's resources. The second impact is consumption of the network bandwidth, which is more threatening than the first [11].

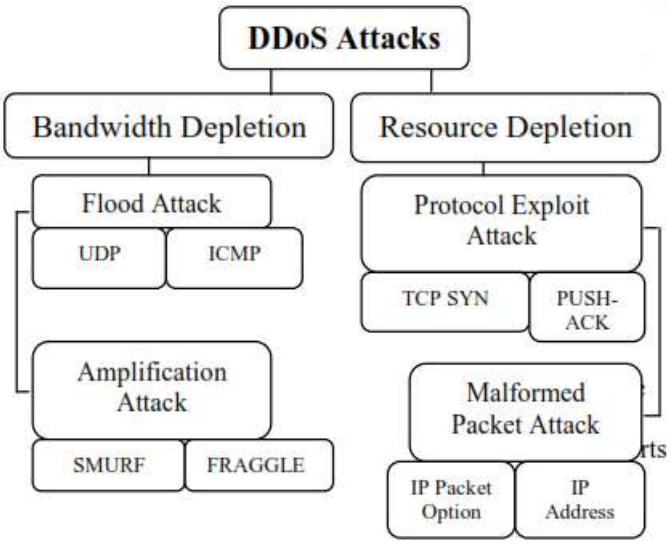

Fig. 1 Taxonomy of DDoS Attacks

Bandwidth Depletion attacks A flood attack involves the zombies to send large volumes of traffic to a victim system, thus congesting the victim system's bandwidth [2][8][9][12]. An amplification attack involves either the attacker or the zombies to send messages to a broadcast IP address, to cause all systems in the subnet reached by the broadcast address so as to send a message to thevictim system.

This method amplifies malicious traffic that reduces the victim system's bandwidth. Resource Depletion Attacks DDoS resource depletion attacks involve the attacker sending malformed packets that tie up network resources so that none are left for legitimate users [2][8]. There are two types of DDoS attack networks as shown in Fig. 2. These are the Agent-Handler model and the Internet Relay Chat (IRC) model.

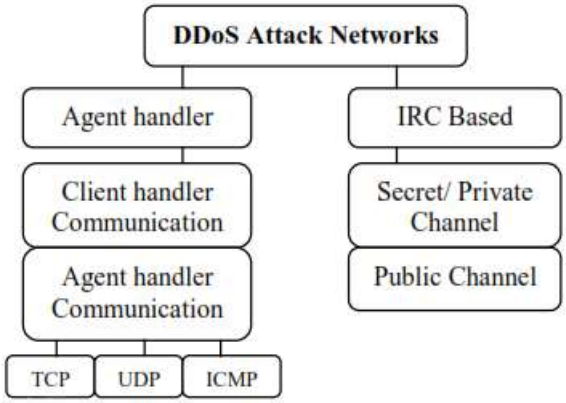

Fig. 2: A Typical Scenario of DDoS Attacks

DDoS Agent Handler Attack Model: DDoS Agent- Handler attack network consists of clients, handlers, and agents. The client is where the attacker communicates with the rest of the DDoS attack system. The handlers are software packages located throughout the Internet that the attacker's client uses to communicate with the agents [15]. In descriptions of DDoS tools, the terms handler and agents are sometimes replaced with ―master‖ and ―daemons‖, respectively [6].

DDoS IRC-based Attack Model: It is similar to the Agent-Handler model except that IRC communication channel is used to connect the client to the agents. An IRC channel provides an attacker with additional benefits such as the use of legitimate IRCports to send commands to the agents. IRC is a multi- user, on-line chatting system. It allows computer users to create two-party or multi-party interconnections and type messages in real time to each other [15]. There are three essential components to DDoS countermeasures [3]. Component for preventing the DDoS attack that includes preventing secondary victims and detecting and neutralizing

handlers, component for dealing with a DDoS attack while it is in progress and lastly, post-attack component which involves network forensics. So, current DDoS detection and defense approaches can be categorizedinto three mechanisms: Proactive Mechanisms, Reactive Mechanisms and Post Attack Analysis [10].

Pro-Active or Preventive defense mechanisms: Preventive mechanisms refer to the actions performed prior to an attack either to eliminate the possibility of being a target of attacks or to aid the target to endure the effects of attacks sufficiently.

Reactive defense mechanisms: Reactive mechanisms refer to the actions performed to mitigate the effects of one or more ongoing attacks and they consist of detection and response procedures.

Post attack analysis or Post-Active methods: Post-active methods refer to the actions performed after an attack has occurred attempting to mitigate the threat of DDoS in the future. Most commonly post active methods are about tracing the attacker as well as analysing the vulnerabilities the attack exploited and engaging into repairs accordingly.

RELATED WORK

Packet filtering is a process of controlling access to a network byanalyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination. Packet filtering is both a tool and a technique that is a basic building block of network security [7]. A packet filtering device is a very appropriate measure for providing isolation of one subnet from another. The packet filter examines the header a packet and makes a decision of whether to pass or reject the packet based upon the contents of the header. Probabilistic approach is the most widely used technique for uncertainty analysis of mathematical models [23]. In the probabilistic approach, uncertainties are characterized by the probabilities associated with events.

Hop Count Filtering (HCF): Hop Count (HC) is defined as the number of hops a packet traverses as it moves from the sender to the receiver [21]. HC is not usually sent in the IP packet but is rather inferred from the IP Time-to-Live (TTL) Field. The main function of IP TTL field is to prevent packets from looping forever. The sender sets the initial value of TTL. Each node on the path decrements the TTL value by one. If the TTL reaches zero, the packet is discarded. The receiver can estimate the HC by subtracting the received TTL value from the closest initial TTL value bigger than the received packet's TTL. Usually, these initial TTL values are operating system dependent and are limited to few possibilities which include 30, 32, 60, 64, 128, and 255

[16]. Therefore, guessing the initial TTL set by the OS is possible without explicitly knowing what the OS is. It can even be used to prevent DDoS attacks [16][13][19][18].

Principle working of this method is that number of hops between the source and destination can be used to assess the authenticity of packet [20]. Although an attacker can forge any field in the IP header, he cannot falsify the number of hops an IP packet takes to reach its destination. More importantly, since the hop-count values are diverse, an attacker cannot randomly spoof IP addresses while maintaining consistent hop-counts. On the other hand, an Internet server can easily infer the hop-count information from the TTL field of the IP header [17]. Using a mapping between IP address and their hop-counts, the server can distinguish spoofed IP packets from legitimate ones.

Since HC values have a limited range, typically between 1 and 30, multiple IP addresses may have the same hop-count values. Consequently, HCF cannot recognize forged packets whose source IP addresses has the same hop-count value to a destination as that of a zombie. A good hop-count distribution should have two properties: being symmetric around the mean value, and being reasonably diverse over the entire range. Symmetry is needed to take advantage of the full range of hop-count values, and diversity helps maximize the effectiveness of HCF.

Ayman Mukaddam et al. [22] proposed the utilization of both RTT and Hop Count to detect IP Spoofing. This is a cumbersome technique when packets transmitted are lost in the network and are to be re- transmitted. RTT is influenced by the distance between the sender and the receiver, link bandwidth and the queuing behaviour of the nodes. Xia Wang et al. [13] focussed on the elimination of the execution caused by the DDoS attack and tracking its attack source. They have used filters at the intermediate node on the basis of some fixed hop count threshold. But, they have not tried to improve on packet filtering technique which is needed for elimination of random IP spoofing.

Krishna Kumar et al. [19] proposed to detect IP spoofing by checking both the Hop Count and the Path Identification (PID) at every router. The PID is inserted in each IP Packet in the identification field. If both the hop count and the PID match, then the packet is considered legitimate otherwise, the routers start attack detection process. The algorithm requires a shared key between every pair of adjacent routers. It requires lot of computational time and more than usual memory space.

B.R. Swain et al. [23] proposed a probability based HCF technique over conventional HCF technique resulting in the saving of computational time. Their packet analysis is based on

probability of packet arrival p, number of malicious packets n and number of legitimate packets m. This technique does notguarantee that the remaining unchecked packets will be legitimate only.

Haining Wang et al. [16] proposed HCF to remove IP packets at the very start of network processing. They considered two HCF states which are learning state and filtering state. HCF works in learning state under normal conditions and watch for abnormal TTL behaviours without discarding any packets. After detecting an attack, mechanism switches to filtering state to discard IP packets with mismatched Hop Counts. This HCF technique has been used at the victim side. HCF is an important technique to remove the randomly spoofed IP traffic or random IP Spoofing. But, attacker may also find an effective way by creating an effective IP2HC table to overcome HCF.

So, there exists lot of scope to improve these limitations by maximizing the detection rate of illegitimate packets and reducing the computational time.

PROPOSED TECHNIQUE AND ITSIMPLEMENTATION

We have proposed Distributed Probability based Hop Count Filtering using Round Trip Time (DPHCF- RTT) technique. Proposed DPHCF-RTT has been implemented in Matlab 9. We have taken a set of arrival rate of pack s per second and the probability values of packets being malicious as follows:

= {10000, 15000, 20000, 25000, 30000, 35000, 40000). p = {0.7, 0.6, 0.5, 0.4, 0.5, 0.6, 0.7}.

The total number of malicious and non-malicious packets M i.e. (m+n) will be * 10). The Poisson distribution is then calculated for all these seven values as product of arrival rate of packets and probability values p which will be used to calculate the Total Cumulative Distribution Function (TCDF). The maximum value of TCDF value will give the calculation of total number of probability based expected malicious packets n in total packets sent. The number of malicious packets detected is given by Count. The value of Count is approaching towards the probability based total malicious packets given by n. Total malicious packets m, so introduced, are lesser than n. The flood_length value is given by * p).

Algorithm: DPHCF-RTT

For given $\lambda, p, m + n$:
Set ***total_packets*** for λ;
Calculate ***flood_length*** of malicious packets;
Calculate n of malicious packets;
Set RTT value;
Initialize the ***Count*** to 0 for intermediate hops;

Set no. of hops = ***hop***;
For no. of hops = 1: ***hop***:
For Each Packet ***i***:
If (Count ≠ n)
Extract the final TTL T and IP Address ***I***;
Infer the initial TTL T_o;
Compute the Hop Count $H_c = T - T_o$;
Index ***I*** to get the stored Hop-Count H_s;
If (($h_c = h_s$) and RTT value is ***valid***)
Packet is ***Legitimate***;
Else If (($h_c \neq h_s$) or RTT value is ***invalid***)
Packet is ***Spoofed***;
End if;
If (Packet = ***Spoofed***)
Count++;
Drop the Packet;
Else
Allow the Packet;
End If;
End If;
End For;
total_packets = (total_packets – n);
If (total_packets ≠ 0)
next_hop ***Count***=Count + next_hop Count;
Set ***total_packets*** to ***n;***
End For;
Compute final ***Count***;
Calculate ***detection_rate*** for malicious packets;
Calculate ***computation_time*** for malicious packets;
End For;

RTT is the difference in time between the time a packet is sent and the times is corresponding reply is received. RTT is influenced by the distance between the sender and the receiver, link bandwidth and the queuing behaviour of the nodes. The utilization of both RTT and probability based distributed HCF to detect IP Spoofing will eliminate the weakness of the HCF technique. Now the attackers have to guess both RTT and the Hop Count values at all the intermediate nodes for the spoofed packet to be considered legitimate. Since, these variables are independent; the probability of guessing both the parameters correctly is lower than the probability of guessing only Hop Count correctly.

In DPHCF-RTT technique, the probable numbers of malicious or spoofed IP packets have been calculated using Poisson distribution. Probability based hop count filtering technique has been applied at the intermediate nodes sequentially in combination with RTT. DHCF filtered legitimate packets have been sent to the server and the illegitimate packets are discarded. Remaining unchecked packets due to probability are tagged and sent to the next intermediate noderepeatedly, until all packets get checked for illegitimacy.

RESULTS AND DISCUSSION

a. DETECTION RATE

DPHCF-RTT technique has utilized maximum 4 numbers of hops. Proposed technique has been compared with the Probabilistic HCF (PHCF) technique at the victim server as shown in Fig. 3. DPHCF-RTT technique has shown efficient results in getting Detection Rate of malicious packets up to 99.33%.

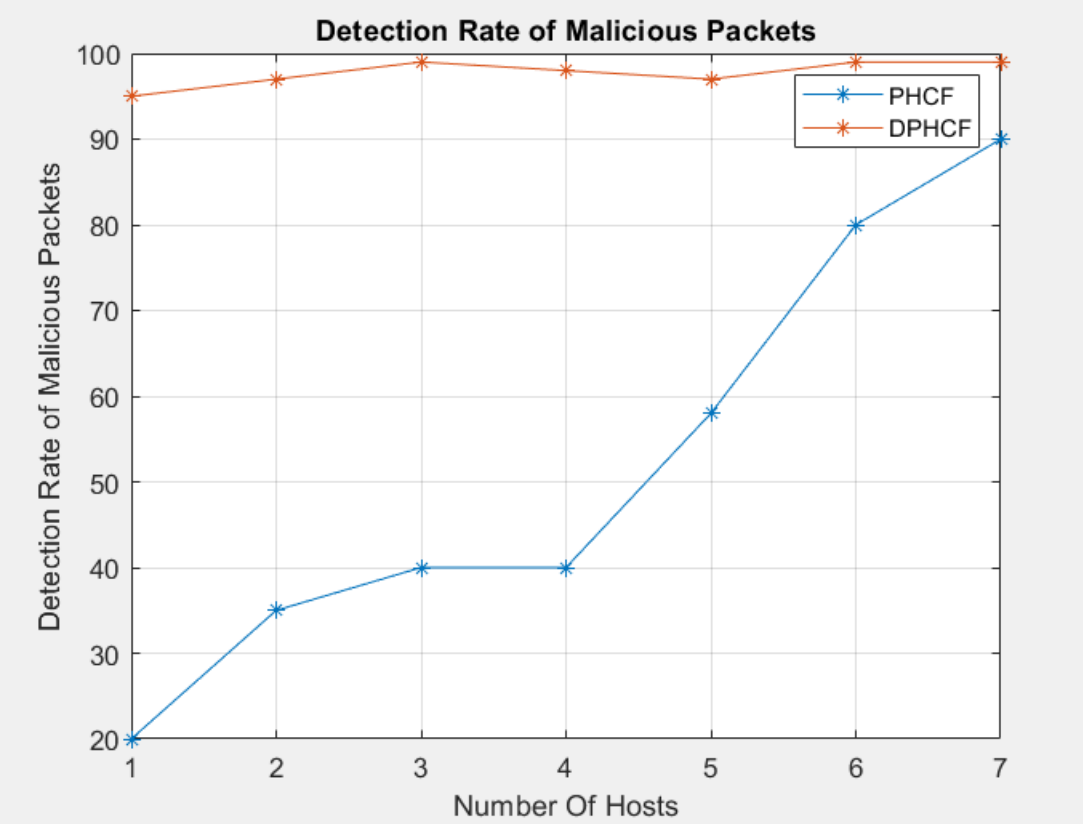

Fig. 3: Comparison of DPHCF-RTT (Hops = 4)vs. PHCF at victim server

1. The detection rate of DPHCF-RTTconsistently swings around the optimum value of 99% which is a good sign of packet filtering technique. This result is the outcome of the combination of DHCF and RTT which has prevented IP spoofing attacks up to the maximum.
2. Victim server cannot be overloaded with large number of packet flooding as it may lead to network jam and server bog down. But, DPHCF-RTT technique can handle packet flooding, as the implementation can be done in a distributive manner using up to 30 numbers of intermediate Hops.
3. Not all packets have been checked at the victim server in the PHCF technique. But, in proposed DPHCF-RTT technique all packets have been checked on numbers of intermediate hops probabilistically.

b. COMPUTATION TIME

In DPHCF-RTT technique, maximum 4 numbers of hops have been considered to increase the efficiency and effectiveness of PHCF technique using RTT. Proposed technique filters malicious packets more effectively. In Fig.4, comparison has been done in terms of computation time for DPHCF-RTT technique with PHCF technique.

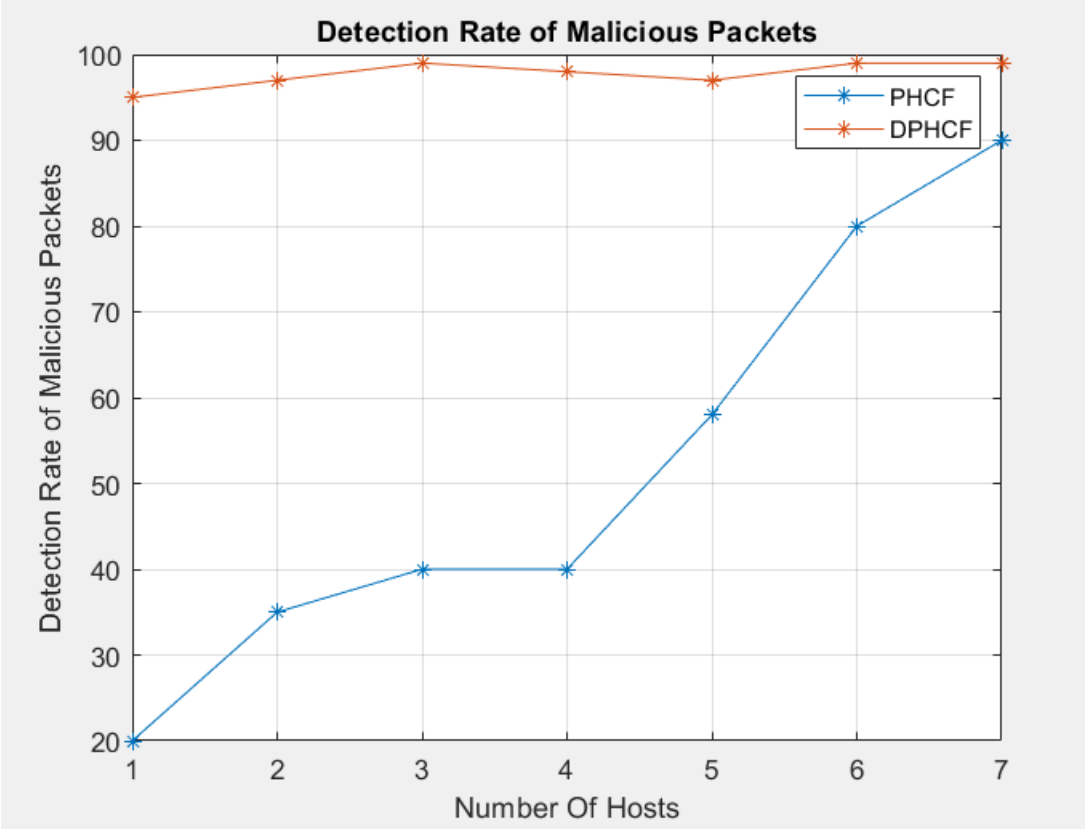

Fig. 4:

Computation Time of DPHCF-RTT (Hops = 4) vs. PHCF at Victim Server

DPHF-RTT technique shows minimum computation time as compared to PHCF technique. This is due to the fact that the time consumption at the victim server is more due to overload. When, this load of packet filtering gets distributed at the intermediate routers then, the total computation time reduced. Hence, this phenomena result in efficiency and effectiveness of flooded packet filtering.

CONCLUSIONS

A number of DDoS attack mitigation techniqueshave been proposed in the literatures which have certain limitations in terms of computational time, detection rate of illegitimate packets while processing. Distributed Probability based Hop Count Filtering using Round Trip Time algorithm has been proposed and implemented. Comparison has been done with the Probabilistic and Conventional Hop Count Filtering techniques as well as with some other Research-Oriented techniques. Results have been gathered at victim server side as well at the intermediate nodes or Hops. Detection rate of malicious packets and the computation time have been considered as the basis of comparison.

DPHCF-RTT technique has reduced the chance of random IP spoofing of packets correctly and effectively to prevent the victim server from such attacks. It has improved the detection rate of the malicious or illegitimate packets up to 99% which is 80-85% for Probability based HCF approach and 90% for Conventional HCF approach.

It has also shown the reduction in the computation time for illegitimate packet filtering through DPHCF-RTT at intermediate routers. Hence, our proposed technique DPHCF-RTT can be considered as one of the robust and unique technique.

REFERENCES

[1] A.Madhuri, A.Ramana Lakshmi, ―Attack Patterns for Detecting and Preventing DDoS and Replay Attacks,‖ International Journal of Engineering and Technology, vol. 2 (9), pp. 4850-4859, 2010.

[2] G. Zhang and M. Parashar, ―Cooperative Defence against DDoS Attacks,‖ Journal of Research and Practices in IT, vol. 38 (1), pp. 69-84, February 2006.

[3] R. Kumar, R. Karanam, R. Bobba, S. Raghunath, ―DDoS Defense Mechanism,‖ IEEE International Conference on Future Networks, VIT University, Vellore, India, pp. 254- 257, 2009.

[4] M. Sachdeva, G.Singh, K.Kumar, K.Singh, ―DDoS incidents and their Impact: A Review,‖ The International Arab Journal of Information Technology, vol. 7 (1), pp. 14-

22, January, 2010.

[5] Dhwani Garg, ―DDOS Mitigation Techniques-A Survey,‖ International Conference on Advance Computing in Communication and Networks, pp. 1302-1309, 2011

[6] S. Specht, R. Lee, ―Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures,‖ Technical Report CE-L2003-03, pp.164, May 2003.

[7] Dan Strom, ―The Packet Filter: A Basic Network SecurityTool,‖ Global Information Assurance Certification Paper,2002.

[8] Simon Liu, ―Surviving Distributed Denial-of-ServiceAttacks,‖ IEEE Journal on IT Professional, vol. 11 (5), pp.51-53, 2009.

[9] R. K. Chang, ―Defending against flooding-based DDoSattacks: A tutorial‖, IEEE Communications Magazine, vol.40 (10), pp. 42-51, October 2002.

[10] L. Garber, ―Denial-of-Service attack rip the Internet,‖IEEE Journal on Computer, vol. 33 (4), pp. 12-17, 2000.

[11] J. Molsa, ―Mitigating denial of service attacks: A tutorial,‖Journal on Computer Security, vol. 13, pp. 807-837, 2005.

[12] Misha Singhal, ―Design and Development of Anti-DoS/ DDoS Attacks Framework using IP/tables,‖ Thapar university, Patiala, Master's Thesis, June 2011.

[13] A Wang, Xia, Li Ming, Li Muhai, "A scheme of distributed hop-count filtering of traffic," International

[14] K.Arora, K.Kumar, M.Sachdeva, ―Impact Analysis of Recent DDoS Attacks,‖ International Journal on Computer Science and Engineering, vol. 3 (2), pp. 877-884, February 2011.

[15] S. M. Specht, R. B. Lee, ―Distributed denial of service:taxonomies of attacks, tools and countermeasures," ACM17th International Conference on Parallel and DistributedComputing Systems, pp. 543-550, September, 2004.

[16] H. Wang, C.Jin and K. Shang, ―Defense Against Spoofed IP Traffic Using Hop-Count Filtering,‖ IEEE Transaction on Networking, vol. 15 (1), pp. 40-53, February, 2007.

[17] Fengli Zhang, Jig eng, Zinguang Qin, Mingtian Zhou,―Detecting the DDoS Attacks Based on SYN proxy and Hop-Count Filter,‖ IEEE International Conference on Communications, Circuits and Systems, University ofElectronic Science and Technology, China, pp. 457-461,11-13, July, 2007.

[18] I. B. Mopari, S.G.Pukale, M.L.Dhore, "Detection and defense against DDoS attack with IP spoofing," IEEE International Conference on Computing, Communication and Networking, Vishwakarma Institute of Technology, Pune, India, pp. 1-5, 18-20, December, 2008.

[19] B. Krishna Kumar, P.K. Kumar, R. Sukanesh, "Hop Count Based Packet Processing Approach to Counter DDoS Attacks," International Conference on Recent Trends in Information, Telecommunication and Computing, PET Engineering College, Thirunelvelli, India, pp. 271-273, 12-13, March, 2010.

[20] Cheng Jin, Haining Wang, Kang G. Shin, ―Hop-countfiltering: an effective defense against spoofed traffic,‖

[21] AymanMukaddam, Imad H. Elhajj, ―Hop count variability,‖ 6th IEEE International Conference on Internet Technology and Secured Transactions, American University of Beirut, Lebanon, pp. 240-244, 11-14, December , 2011.

[22] AymanMukaddam, Imad H. Elhajj, ―Round Trip Time to Improve Hop Count Filtering,‖ IEEE Symposium on Broadband Networks and Fast Internet, American University of Beirut, Lebanon, pp. 66-72, 28-29, May, 2012.

[23] Biswa Ranjan Swain, Bibhudatta Sahoo, ―Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method,‖ IEEE International Conference on Advance Computing, NIT, Rourkela, India, pp. 1170-1172, 6-7, March 2009.

[24] P. S. Mann, D. Kumar, ―Improving Network Performance and mitigate DDoS attacks using Analytical Approach under Collaborative Software as a Service (SaaS) Cloud Computing Environment,‖ International Journal of Computer Science and Technology, vol. 2(1), pp. 119-122, March, 2011.

[25] D. Moore, C. Shannon, D. Brown, G. Voelker, S. Savage,―Inferring Internet Denial of Service Activity,‖ ACM Transaction on Computer Systems, New York, USA, vol.

24 (2), pp. 115-139, 2006.

[26] D. Dittrich, ―The Tribe Flood Network Distributed Denial of Service Attack Tool,‖ 2007, [Online]. Available: http:// staff.washington.edu/dittrich/misc/trinoo.analysis.txt.

[27] C. Douligeris, A. Mitrokotsa, ―DDoS Attacks and Defense Mechanisms: Classification and State of the Art,‖ Journal on Computer Networks, vol. 44 (5), pp. 643-666, 2004.

[28] D. Moore, G.Voelker, S.Savage, ―Inferring Internet Denial of Service Activity,‖ 10th USENIX Symposium on Security, pp. 20-25, 2001.

[29] S. Gibson, ―The Strange Tale of the Denial of ServiceAttacks against GRC.COM,‖ 2007, [Online]. Available: