ANALYSIS OF "DPHCF-RTT" PACKET FILTERING TECHNIQUE AGAINST DPHCF and DCHCF TECHNIQUES

Dr. Anil Rajput[1], Ritu Maheshwari Bansal [2]

[1]Professor (CS), Department of Computer Science, CSA Govt. PG Nodal College, Sehore, M.P., (India)

[2]Assistant Professor (CSE), Faculty of Engineering & Technology Engineering, MRIU, Faridabad, Haryana, (India)

ABSTRACT

IP spoofing based DDoS attack is a DoS attack that relies on multiple compromised hosts in the network to attack the victim. IP spoofing makes the task of filtering illegitimate packets from the legitimate traffic of packets very difficult as IP addresses can be forged very easily. A number of mitigation techniques have been proposed related to higher computational time and low detection rate of illegitimate packets. In this paper, DPHCF-RTT has been analysed against other existing Probabilistc and Conventional Hop Count Filtering techniques. Goal is to improve the limitations of Conventional HCF or Probabilistic HCF techniques by maximizing the detection rate of illegitimate packets and reducing the computation time through DPHCF-RTT. It is based on distributed probabilistic HCF using RTT. It has been used in an intermediate system. Round Trip Time (RTT) provides valuable information that would help improve the efficiency of probabilistic DHCF technique which solely relies on Hop Count. DPHCF-RTT has shown a maximum detection rate up to 99% of malicious packets.

***Keywords*: DDoS, Distributed Conventional Hop Count Filtering (DCHCF), Hop Count Filtering (HCF), Distributed Probabilistic HCF (DPHCF), Intermediate System, Packet Filtering, Round Trip Time (RTT), TTL**

I INTRODUCTION

A Denial of Service (DoS) is an attack with the purpose of preventing legitimate users from using a victim server or network resources. Attacker fills the networks bandwidth with large amount of request packets that consumes the bandwidth and makes it difficult for the legitimate user to access the service in this attack. DDoS attack is a big threat to availability of services on the Internet. The attackers are not going to thieve, modify or remove the information exchanged on networks, but they attempt to impair a network service.

Without being authenticated on the Internet, any packet can be sent to anyone. 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 [9].

In this paper, section II presents Packet Filtering Techniques, section III presents DPHCF-RTT technique, section IV presents Results and Discussion, and lastly, section V presents Conclusions.

II PACKET FILTERING

Packet filtering is a process of controlling access to a network by analyzing 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 basic building block of network security [10].

In Hop Count Filtering, hop count is the number of hops a packet traverses when it moves from the sender to the receiver destination that can be used to check the authenticity of packet [3]. IP TTL field helps preventing packets from looping forever. TTL is introduced to specify the maximum lifetime of each packet in the Internet which is an 8-bit field in the IP header. Each intermediate router decreases the TTL value of IP packet by one before sending it to the next-hop. When a packet reaches its destination, the final TTL value is the initial TTL decreased by the number of intermediate hop counts.

When the TTL reaches zero or when the major difference occurs in the number of hops in the table in case of attack, the packet is discarded. No. of Hops cannot be falsified, although any field in the IP header can be forged by an attacker. An attacker cannot randomly spoof IP addresses while maintaining consistent hop-counts as the hop-count values are diverse [4]. The server can distinguish spoofed IP packets from legitimate ones using a mapping between IP address and hop counts. Source IP address spoofing means lying about the return address of a packet. Attackers can easily gain unauthorized access to a computer or a network by spoofing the IP address of that machine. It is important to examine hop-count distributions at various locations in the Internet as HCF cannot recognize forged packets whose source IP addresses have the same hop-count value as that of an attacker [5].

Ayman Mukaddam et al. [6] has proposed for victim side and conventional method of HCF has been used which is time consuming and not effective. Xia Wang et al. [7] are not trying to improve the packet filtering technique which is needed for elimination of random IP spoofing. The algorithm of Krishna Kumar et al. [1] requires a shared key between every pair of adjacent routers which requires lot of computational time and more than usual memory space. The probability based hop count filtering (PHCF) technique of B.R. Swain et al. [2] does not guarantee that the remaining unchecked packets will be legitimate only. Hence, this technique lacks in maximizing up to 100% detection of illegitimate packets from total packets. In the technique of Haining Wang et al. [5] attacker may also find the effective way by creating an effective IP2HC table to overcome HCF. Hence, this is also ineffective as legitimacy of packets is not sure [8].

Hence, after reviewing the literature, it is found that CHCF and PHCF techniques at distributed nodes, which are used to filter the malicious packets from the total packets, possess some limitations related to computational time, detection rate of illegitimate packets. Hence, there exists lot of scope to maximize the detection rate of illegitimate packets and reducing the computational time.

III DPHCF-RTT

DPHCF-RTT drops almost 100% of malicious packets which is not in conventional HCF where 90% of malicious packets are dropped and in probabilistic HCF where 80% to 85% of packets will be dropped. In DPHCF-RTT, Probability based distributed HCF along with RTT, every packet has been checked once for its legitimacy at the routers and then packet are transferred to the victim side [10].

At intermediate routers, malicious packets have been efficiently detected through DPHCF-RTT. The malicious packets, so discarded, do not contain any legitimate packets. The number of packets, definitely, remains unchecked considering some threshold value of packets to be malicious in total number of packets. The checked packets are passed to the victim server and the unchecked packets are passed on to the next router for further application of DPHCF-RTT technique on them. This process is carried out till no unchecked packet remains.

The effectiveness of DPHCF-RTT has been examined over PHCF and CHCF technique in respect of detection rate of malicious or illegitimate packets and computation time for filtering malicious packets [9]. In this paper, DPHCF-RTT technique has been analysed against DPHCF and DCHCF i.e. Distributed Conventional Hop Count Filtering to observe the effectiveness and efficiency of DPHCF-RTT over these two existing techniques.

IV RESULTS AND DISCUSSION

4.1 Detection Rate

DPHCF-RTT technique has been examined on different hops from 1 to 4 and for 30. It is found more efficient when larger numbers of intermediate nodes are considered. It gives high detection rate of malicious packets when compared with lesser number of hops below 4. Efficient results have been shown in getting detection rate of malicious packets up to 99.33%. Its detection rate consistently swings around the optimum value of 99% which is a good indication of packet filtering.

The comparison of effectiveness and efficiency of DPHCF-RTT technique has been shown in Fig. 1 in between DPHCF and DCHCF techniques. If maximum number of hops will be considered, it will definitely increase the detection rate of malicious packets up to approximately 100%.

Tab. 1 Detection rate Percent of DPHCF-RTT Vs DPHCF and DCHCF

40000 pkts / sec on no. of Hops	Detection Rate Percent of DPHCF-RTT against DPHCF & DCHCF Technique		
	RTT+DPHCF	DPHCF	DCHCF
Hop nos. = 1	84.6643	87.2821	87.2821
Hop nos. = 2	93.7286	95.2643	95.2643
Hop nos. = 3	97.5786	82.5429	82.5429
Hop nos.= 4	98.1929	97.0286	87.8893
Hop nos. =30	99.5321	91.3143	91.3143

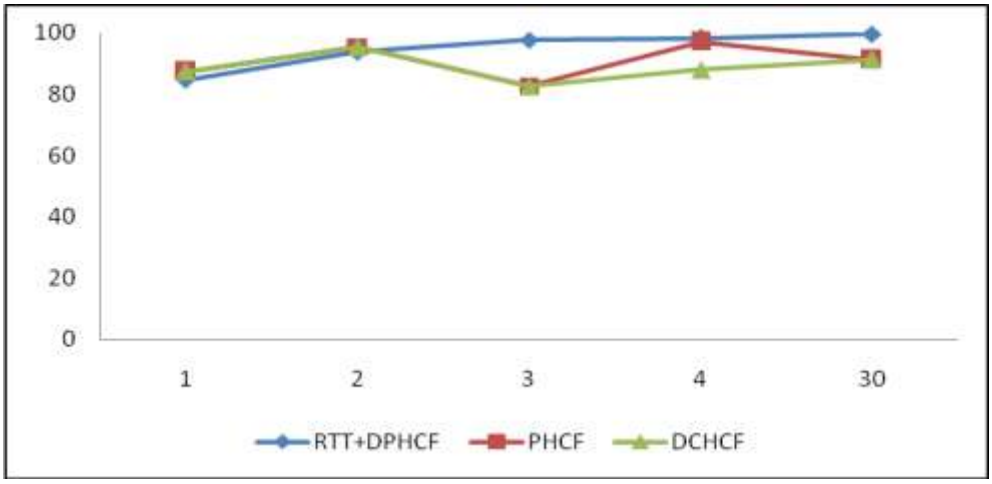

Fig. 1 DPHCF-RTT Vs PHCF and CHCF at Distributed Nodes

4.2 Computation Time

DPHCF-RTT filters malicious packets with minimum computation time as compared to DPHCF and DCHCF techniques as well as PHCF and CHCF techniques at the victim server for different number of hops at different arrival rate of packets. Hops = 1 in DPHCF-RTT takes very less computation time in contrast to more number of hops. This is due to high packet flooding and faster detection rate for a single hop. But, the accuracy of detection is not sure in contrast to more number of hops. In Fig. 2 comparison has been done between the DPHCF-RTT and DPHCF and DCHCF for 30 no. of hops. In Fig. 3, comparison has been done between DPHCF-RTT for number of hops = 4 with PHCF and CHCF techniques at victim server.

Tab. 1 Computation Time of DPHCF-RTT Vs DPHCF and DCHCF

Computation Time of DPHCF-RTT against DPHCF & DHCF Technique (in milliseconds)							
DPHCF-RTT(Hop =30)	0.1	0.15	0.2	0.25	0.3	0.35	0.4
DPHCF (Hop = 30)	0.1	0.15	0.2	0.25	0.3	0.35	0.4
DCHCF (victim Server)	0.4	0.6	0.8	1	1.2	1.4	1.6

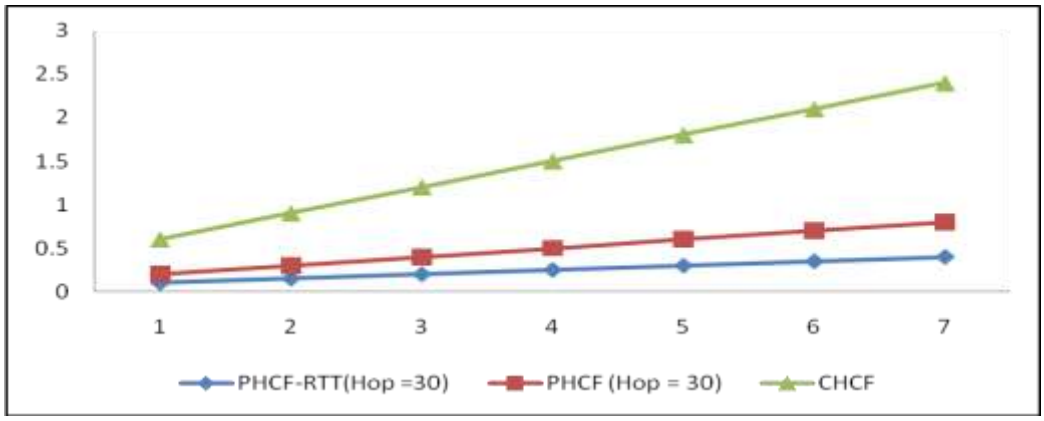

Fig. 2 DPHCF-RTT vs. PHCF and CHCF (Hops = 30)

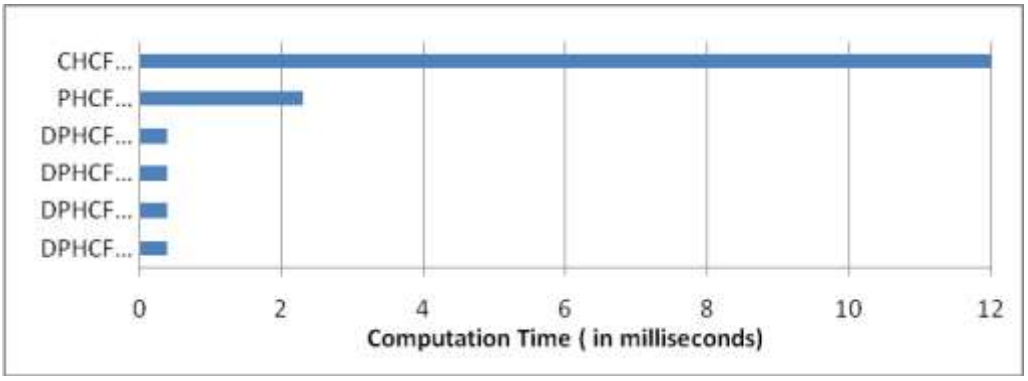

Fig. 3 DPHCF-RTT vs. PHCF and CHCF for maximum Packets Arrival Rate = 400000

V CONCLUSION

Performance of DPHCF-RTT has been analysed and compared with PHCF and CHCF techniques at intermediate nodes as well as at the victim server. Basis of comparison are Detection rate of malicious packets and the computation time Detection rate of malicious packets of DPHCF-RTT have been found up to 99% as compared to PHCF and CHCF techniques. Also, the computation time for filtering illegitimate packets has been found to be reduced for DPHCF-RTT drastically and found effective as compared to PHCF CHCF techniques at intermediate nodes as well as at the victim server. DPHCF-RTT can be implemented on real-time environment or on the cloud platform for maximum number of intermediate nodes up to 30 in the future.

REFERENCES

[1] 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.

[2] B. R. Swain, B. Saboo, "Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method," IEEE International Conference on Advance Computing, NIT, Rourkela, pp. 1170-1172, 6-7, March 2009.

[3] A. Mukaddam, I. 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.

[4] F. Zhang, J. eng, Z. Qin, M. Zhou, "Detecting the DDoS Attacks Based on SYN proxy and Hop-Count Filter," IEEE International Conference on Communications, Circuits and Systems, University of Electronic Science and Technology, China, pp. 457-461, 11-13, July, 2007.

[5] 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

[6] A. Mukaddam, I. 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.

[7] A Wang, Xia, Li Ming, Li Muhai, "A scheme of distributed hop-count filtering of traffic," International Communication Conference on Wireless Mobile and Computing, pp. 516-521, 7-9 Dec.2009.

[8] R. Maheshwari, C. Rama Krishna, M. Sridhar Brahma "Distributed Denial of Service (DDoS) Attacks Mitigation and Packet Filtering Techniques: A Comprehensive Review," PTU National Conference on Innovations & Knowledge Discovery in Computing Technologies, IET Bhaddal, Punjab, India, pp. 9-15, 13th-14th August, 2013.

[9] R. Maheshwari, C. Rama Krishna, "Mitigation of DDoS Attacks using Probability based Distributed Hop Count Filtering and Round Trip Time," International Journal of Engineering Research & Technology, vol. 2(7), pp. 1135-1140, July, 2013.

[10] R. Maheshwari, C. Rama Krishna, "Defending Network System against IP Spoofing based Distributed DoS attacks using DPHCF-RTT Packet Filtering Technique," IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques, pp. 211-214, 2014.