ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (993-997), Month: April - June 2015, Available at: www.researchpublish.com

MALICIOUS PACKET FILTERING USING HC-PACKET SCORE METHOD: A CONCEPT IN CLOUD

[1]Ritu Maheshwari Bansal, [2]Jyoti Dhingra

[1]Assistant Professor (CSE), Faculty of Engineering & Technology Engineering, MRIU, Faridabad, Haryana, India
[2]Research Scholar, M.Tech (CSE), MRIU, Faridabad, Haryana, India

Abstract: **Cloud computing is a distinct environment that is designed for sharing computing resources and services. It allows costumers and organizations to use its services without installing any software. It allows them to use cloud resources without investing in infrastructure and training personnel. But this technology suffers from the problem of different kinds of attacks. DDoS attacks are a critical threat to the cloud environment. Various traditional methods had been applied to mitigate them but due to their low efficiency and low storage capacity made these traditional approaches less useful and popular. So, in this paper we propose a dual mechanism in which packets are first filtered using their hop counts and then packets those are filtered are passed through the second phase of the mechanism in which packets are discarded on the basis of score calculated using the score also known as the conditional legitimate probability(CLP). The idea is to prioritize the packet based on this score which estimates the legitimacy of the given packet. Once the score is computed the packets will be selectively discarded on the basis of the static threshold.**

Keywords: **Conditional legitimate probability(CLP),Hop Count Filtering (HCF), Packet Filtering, Denial of Service (DoS), Time-To-Live (TTL).**

I. INTRODUCTION

Distributed Denial of service(DDoS) attacks are a major threat to the cyber security in which the victim networks are bombarded with a large volume of malicious packets which overloads the victim and makes it incapable of performing its normal transactions to the legitimate users. There are still various ISPs that rely on manual detection of these attacks. But human intervention results in poor response time and fails to protect the victim. So we need various mechanisms to protect the cloud environment from these attacks. There are mainly three branches of study in DDoS, namely, 1) attack detection, 2)attack traceback, and 3) attack traffic filtering. The packet score mechanism belongs to the attack traffic filtering. Research in attack filtering is also categorised into 3 areas on the basis of the point of protection, they are: source initiated, path based and victim initiated. The key notion of this scheme is "Conditional Legitimate Probability" (CLP) based on Bayesian theorem. In this research we introduce dual mechanism to fight against these type of attacks.

II. RELATED WORK

PacketScore [7] generates value distributions of some attributes in the TCP and IP headers, and then uses Bayes' Theorem to score packets. PacketScore has a pretty high filtering accuracy and it is also easy to be deployed. But since its scoring and discarding are related to attack intensity, it is not suitable for handling large amount of attack traffic. Also it has some costly operations in scoring, which leads to low process efficiency in real-time filtering.

ALPi [8] is an improvement of PacketScore. Two schemes LB and AV which uses leaky buckets and value variances of attributes respectively are proposed and are evaluated by comparison with PacketScore. Hop-Count Filtering (HCF) [9] uses the relationship of source IP address and TTL value to carry out filtering. After building an IP to hop-count mapping,

it can detect and discard spoofed IP packets with about 90% accuracy. It is effective and easy to be deployed but it is vulnerable to distributed attacks because of its assumption about spoofed IP traffic. Our method aims at mining the correlation patterns, which refer to some simultaneously-appeared characteristics in the legitimate packets. [16] [17] use the document popularity and user browsing behaviours to detect attack packets, which reflect some correlation patterns between packets in a flow. But these patterns are mainly in application layer, making these methods mostly effective for application layer DDoS.

Ayman Mukaddam et al. has proposed for victim side and conventional method of HCF has been used which is time consuming and not effective. Xia Wang et al. are not trying to improve the packet filtering technique which is needed for elimination of random IP spoofing. The algorithm of Krishna ndkjkar et al. requires a shared key between every pair of adjacent routers which requires lot of computational time and more than usual memory space [18].

III. HOP COUNT FILTERING

DDoS attacks are a serious threat to the internet resources and services. To conceal identity attackers usually forge the IP header field in the packets but he cannot falsify the number of hops the packet takes to reach its destination. This is the basis of hop count filtering. A hop is one portion of the path between source and destination. Each time packets are passed to the next device, a hop occurs. And thus hop count i.e., to filter the IP spoofed packets near the victim. The hop-count information is indirectly reflected in the TTL field of the IP header, since each intermediate router decrements the TTL value by one before forwarding it to the next hop. The difference between the initial TTL (at the source) and the final TTL value (at the destination) is the hop-count between the source and the destination. By examining the TTL field of each arriving packet, the destination can infer its initial TTL value, and hence the hop-count from the source. Here we assume that attackers cannot sabotage routers to alter TTL values of IP packets that traverse them. *Hop-Count Filtering* (HCF) builds an accurate IP2HC (IP to hop-count) mapping table. Assuming that an accurate IP2HC mapping table is present, The inspection algorithm extracts the source IP address and the final TTL value from each IP packet. The algorithm infers the initial TTL value and subtracts it from the final TTL value to obtain the hop-count. Then, the source IP address serves as the index into the table to retrieve the correct hop-count for this IP address. If the computed hop-count matches the stored hop-count, the packet has been "authenticated;" otherwise, the packet is classified as spoofed. In this way hop count filtering works and detects and discards the spoofed packets.

IV. THE PACKET SCORE MECHANISM

The most challenging issue in blocking a DDoS attack is to distinguish the legitimate packet from the malicious one. To resolve this issue, packet score scheme has been proposed. In this we utilize the concept of Conditional legitimate probability(CLP), which is based on Bayesian theorem. CLP indicates the likelihood of a packet being legitimate by comparing its attribute values with the values in the baseline profile. CLP is produced by comparing traffic characteristics during the attack with previously measured traffic characteristics. The viability of this approach is based on the fact that the there are some traffic characteristics that are inherently stable during normal network operations of a target network. This scheme has been named packet score because packet score can be viewed as a score which will estimate the legitimacy of a suspicious packet.

The conditional legitimate probability(CLP) is defined as the probability of a packet being legitimate given its attributes:

CLP(packet P)=P(packet P is legitimate| P's attributes A=ap, attribute B=bp….).

Now according to Bayes theorem the conditional legitimate probability of an event E to occur given an event F is defined as:

$$P(E|F)= \frac{P(E\cap F)}{P(F)}$$

Therefore, CLP can be rewritten as follows:

$$CLP(P) = \frac{P((P=\text{legitimate})\cap(A=ap,B=bp,....))}{P(A=ap,B=bp,....)}$$

$$= Nn*\frac{Pn(A=ap,B=bp,\ldots)/Nn}{Nm*Pm(A=ap, B=bp\ldots.)/Nm} \qquad (1)$$

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (993-997), Month: April - June 2015, Available at: www.researchpublish.com

$$= Nn*\frac{Pn(A=ap,B=bp,\ldots)}{Nm*Pm(A=ap, B=bp\ldots.)}$$

If the attributes are independent,

$P(A=ap, B=bp,\ldots\ldots)= P(A=ap)*P(B=bp)*\ldots\ldots,$

Hence CLP can be rewritten as:

$$CLP(P)=Nn*\frac{Pn(A=ap)*Pn(B=bp)*\ldots.}{Nm*Pm(A=ap)*Pm(B=bp)\ldots.} \quad (2)$$

Where A,B,C… are the discrete-value attributes for the packet P. {a1,a2,a3,…} are the possible values for attribute A, {b1,b2,b3…) are the possible values for the attribute B and so on. A might be protocol type, B might be packet size, C might be the TTL values and so on.

Nm are the total packets during an attack and Nn are the legitimate packets arriving in T seconds. Na are the attack packets.

$$Nm= Nn+ Na.$$

It is known that some IP header fields are not evenly distributed over all the possible values; rather a unique distribution pattern exists for every site[12],[21],[23]. The main benefit of this is that the attacker do not know the attribute value distribution in the legitimate traffic, they are likely to generate random or wrongly guessed pattern, which makes most of the attack packets to have smaller scores than the legitimate packet scores.

The (2) equation shows that we can calculate the legitimacy of the packet by observing the probabilities of the attribute values in the legitimate traffic (Pn) and in the total traffic (Pm). Since it is not possible to know that how many packets are legitimate during the attack period, therefore we let alone the number of legitimate packets bearing a particular value. Therefore, we take an estimate P'n in place of true Pn. This estimate is known as *nominal profile* and is collected in advance. A nominal profile traffic consists of single and joint distributions of various packet attributes. Candidate packet attributes from IP headers are:

1. Packet size
2. Time to live field(TTL)
3. Protocol type values
4. Source IP prefixes

Joint attribute distributions are considered more reliable as they represent uniqueness of traffic distributions and thus are harder for the attacker to guess. Joint attribute distributions may be

1. <packet size and protocol type>,
2. <server port number and protocol type>, and
3. < source IP address, packet size>, etc.

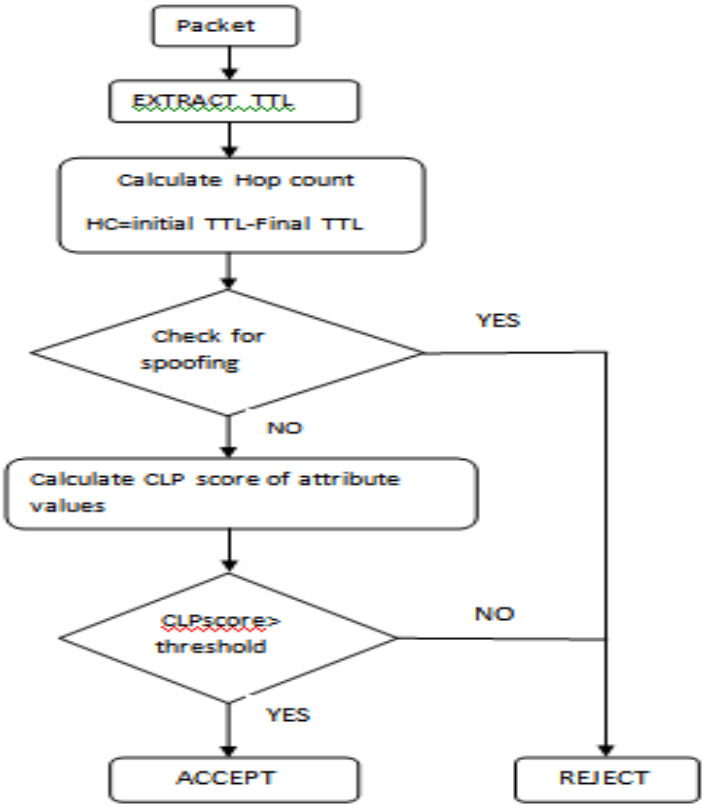
These attribute distributions are stored in the nominal profile and these are help in packet discarding during the scheme.

V. PROPOSED METHODOLOGY

The above mentioned two approaches i.e., hop count filtering and packet score scheme can be combined to produce better results. We propose this dual mechanism for packet discarding and hope to produce better results and reliable approach. The dual mechanism here means that the packet before discarding will pass through the two phases. The first phase will be the hop count filtering mechanism , the packets will be discarded on the basis of hop count according to the method explained above. The packets which pass this first phase will only be allowed to pass to the next phase and rest will be discarded. The introduction of this first phase with the packet score scheme will be more efficient and reliable as the discarding of packets from the first phase will make less load on the second phase of this dual mechanism. In the second

phase of this mechanism we calculate the score of the incoming packets first and the calculated score will be compared with the stored static threshold and if the score is more than the threshold value than only the packet will be accepted otherwise it will be discarded. In this way this dual mechanism works.

The flowchart for the above dual mechanism is described below:



VI. CONCLUSION

The most serious threat to cloud computing is DDOS attack. It caused a lot of damage to many organizations. Attacker shut down the servers for a period of time. The site became non functional for some time. Dual mechanism approach is used to prevent attack. This method is about to improve the existed packet score method. So HC-packet score technique may be provided as a tool to prevent from attack by using IP Spoofing and correlation pattern among attributes of packet in cloud environment. DDOS attack is mainly associated with spoofed packets. The spoofed packets are dropped in the initial phase so reducing the overhead in calculating score of the all packets.

REFERENCES

[1] M. Armbrust et al., "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp.50-58, 2010.

[2] L. Zhang, and Q. Zhou, "CCOA: Cloud Computing Open Architecture," Proceedings of the IEEE International Conference on Web Services, pp.607-616, 2009.

[3] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems," ACM Computing Surveys, vol. 39, no. 1, p.3, 2007.

[4] Cisco IOS Security Configuration Guide, Release 12.2, "Configur- ing Unicast Reverse Path Forwarding," pp. SC-431-SC-446, http:// www .ci s co.com/uni v ercd/c c/td/doc/ p rodu ct/ s oftware/ ios122/122cgcr/ fsecur_c/fothersf/ scfrpf.pdf, 2006.

[5] C. Estan, S. Savage, and G. Varghese, "AutomaticallyInferring Patterns of Resource Consumption in Network Traffic,"Proc. 2003 ACM SIGCOMM, pp 137-148, 2003.

[6] CSI/FBI Survey, http://www.gocsi.com/forms/fbi/csi_fbi_ survey.jhtml, 2006.

[7] FBI Fugitive, http://www.fbi.gov/wanted/fugitives/cyber/ echouafni_s.htm, 2006.

[8] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing," RFC 2827, 2000.

[9] L. Garber, "Denial-of-Service Attacks Rip the Internet," Computer, pp. 12-17, Apr. 2000.

[10] J. Ioannidis and S.M. Bellovin, "Implementing Pushback: Router- Based Defense against DDoS Attacks," Proc. Network and Distributed System Security Symp., Feb. 2002.

[11] C. Jin, H. Wang, and K.G. Shin, "Hop-Count Filtering: An Effective Defense against Spoofed Traffic," Proc. ACM Conf. Computer and Comm. Security (CCS '03), Oct. 2003.

[12] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites," Proc. Int'l World Wide Web Conf., May 2002.

[13] S. Kasera et al., "Fast and Robust Signaling OverloadControl," Proc. Int'l Conf. Network Protocols, Nov. 2001.

[14] A.D. Keromytis, V. Misra, and D. Rubenstein, "SOS: An Architecture for Mitigating DDoS Attacks," IEEE J. Selected Areas in Comm., vol. 22, no. 1, pp. 176-188, Jan. 2004.

[15] Ddd A. Kuzmanovic and E.W. Knightly, "Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants)," Proc. ACM SIGCOMM 2003, Aug. 2003.

[16] H. Kim and I. Kang, "On the Effectiveness of Martian Address Filtering and Its Extensions," Proc. IEEE GLOBECOM, Dec. 2003.

[17] Y. Kim, J.Y. Jo, H.J. Chao, and F. Merat, "High-Speed Router Filter for Blocking TCP Flooding under Distributed Denial-of-Service Attack," Proc. IEEE Int'l Performance, Computing, and Comm. Conf., Apr. 2003.

[18] Y. Kim, J.Y. Jo, and F. Merat, "Defeating Distributed Denial-of- Service Attack with Deterministic Bit Marking," Proc. IEEE GLOBECOM, Dec. 2003.

[19] Y. Kim, W.C. Lau, M.C. Chuah, and H.J. Chao, "PacketScore: Statistics-Based Overload Control against Distributed Denial-of- Service Attacks," Proc. IEEE INFOCOM, Mar. 2004.

[20] Q. Li, E.C. Chang, and M.C. Chan, "On the Effectiveness of DDoS Attacks on Statistical Filtering," Proc. 2005 IEEE INFOCOM, 2005.

[21] D. Liu and F. Huebner, "Application Profiling of IP Traffic," Proc. 27th Ann. IEEE Conf. Local Computer Networks (LCN), 2002.

[22] M. Mahoney and P.K. Chan, "Learning Nonstationary Models of Normal Network Traffic for Detecting Novel Attacks," Proc. ACM 2002 SIGKDD, pp. 376-385, 2002.