International Journal of Advanced Technology in Engineering and Science www.ijates.com
Volume No 03, Special Issue No. 01, March 2015 ISSN (online): 2348 – 7550

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

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

[1]*Assistant Professor (CSE), Faculty of Engineering & Technology Engineering,*

[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 major 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 confidence based filtering method. The method is deployed using two periods, i.e. attack and non attack period.

Keywords*: Confidence Based Filtering (CBF), Hop Count Filtering (HCF), Packet Filtering, Denial of Service (DoS), Time-To-Live (TTL)

I INTRODUCTION

DDos attacker is one of the most common attack in cloud computing. Services become unavailable to the legitimate users for some interval of time by sending connection requests to the server. It was reported that 94 % of data center operators security attacks, 76 % had suffered distributed denial of service. Many researchers had founded many measures to prevent such attack such as Intrusion detection, Hop Count method, CBF etc. These all methods have some advantages over others.

In recent years, many researches on DDoS defense have been carried out and many successful schemes have been put forward. There are approximately three major branches of the research: attack detection [4] [5] [6], attack filtering[7] [8] [9] [10] [11] [12], and attack traceback [13] [14] [15]. As mentioned in [7], the branch of attack filtering can be roughly categorized into three areas based on the point of protection: source-initiated, path-based and victim-initiated. The method proposed in this paper is in victim-initiated area, which filters incoming attack packets from victim side. In this area of research, a number of brilliant approaches have already been proposed.

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 behaviors 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 Kumar 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 HC-CBF PACKET FILTERING TECHNIQUE

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. One of such attack is DDOS attack. Attack in which attacker continuously sends bogus packets to the cloud servers. Cloud will waste its bandwidth in serving these requests. As a result legitimate users will not get any services of the cloud provider. So, to handle these attacks we need methods that are effective enough and can be proved to a great use. So, in this paper the above problem is being handled and HC-CBF technique is proposed.

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. 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.

The main goal of HC-CBF is to filter the packets received from various source on the basis of the IP spoofing by using TTL field in the packet and then allowing these filtered packets to go through CBF method. CBF is based upon the correlation pattern stored in the packets. These patterns are mainly in network and transport layer.DDOS attack is accompanied by IP spoofing. Attackers conceal their identity by changing the Source IP

address field of the packet to make it as packet is coming from the legitimate user. But attacker cannot forge the Hop Count of the packet i.e. numbers of hops it require to reach destination from the source. This idea is used in here to filter the packets.

Hop count and SYN flag of the packets detects whether the packet is spoofed one or legitimate. If the source IP address is not in the table then SYN flag is checked. If it is set then hop count is calculated and entry is added in the table else discard the packet. The case when the source IP address is in the table already. We extract the value of SYN flag from the incoming packet. If it is set then computed hop count is compared with the saved Hop count. The packet will be allowed if both have same values else the entry in the table for that IP address is updated. But if the SYN flag is not set in the packet, we again compare hop counts values. If same we allow the packet but instead of updating entry in table, here packet is dropped. Hence the spoofed packet is rejected and rest the packets which passed this test are collected under filtered list for further test. This filtering has reduced the numbers of packets on which further tests will be applied. Hence it reduced the overhead of applying CBF on all the packets.

CBF consist of two concepts- Confidence and Score. Each packet from the filtered list is collected and the frequency of appearance of single attribute is calculated. This is the confidence of that attribute value. More the confidence value, more will be legitimacy of the packet. If the confidence of single attribute is greater than the minconf which is decided earlier are selected to generate attribute value pairs. This step is essential because if the confidence of one attribute value in an attribute value pair is not greater than minconf, the confidence of the combination of this value pair will still not be greater than minconf. All the packets in the filtered list are again scanned to count the frequency of appearances of attribute value pairs and count their confidence. Attribute values pairs whose confidence is greater than minconf will update the nominal profile.

Nominal profile is a 3 dimensional array. The first dimension is for first attribute pair and the second dimension is for second attribute pair. The third dimension is the confidence value dimension. There is no need to update nominal profile if the confidence of attribute pairs less than predefined confidence value. This step again reduces overhead of updating profile for each attribute pair. This is all done in non attack phase. Attack and non attack phase can be distinguished either on timing basis or on the number of packet basis or any other function. In attack phase we calculate score of packets. Score is the weighted average of the confidence of the attribute value pairs in it.

$$\text{score} = \sum_{i=0}^{n}(\text{weight} * \text{confidence [attribute value pairs]}) / \sum_{i=0}^{n}(\text{weight})$$

where , n= number of packets

Weights of the attributes are adjusted on the basis of operating system, network structure and other elements. The patterns which are less copied by attackers are generally are given higher weight. Weight of the protocol type is usually given less weightage because it could be easily guessed by the attacker. Score calculation requires looking in the nominal profile for the confidence of the attribute pairs and applying some arithmetic operations. Attributes pairs whose confidence is not on the nominal profile, minconf value is used instead when confidence values are used in calculating score. Score of the packets is generated by the above method. After calculating CBF scores of the packets, attack packets are distinguished from the legitimate ones. Method will only accept the packets with scores greater than discarding threshold. Discarding Threshold can be fixed

depending upon the score distribution or dynamic like load shedding algorithm. Fixed discarding threshold is used in this approach. So, in this proposed methodology every incoming packet is passing through the two stages and thus is more confident and we can have more trust on the packet.

IV 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 CBF method which is based on the correlation patterns. So HC-CBF 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 confidence and 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] A. Chonka, J. Singh, and W. Zhou, "Chaos Theory Based Detection against Network Mimicking DDoS Attacks," IEEE Comm. Letters, vol. 13, no. 9, pp.717-719, 2009.

[5] Y. Xiang, K. Li, and W. Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," IEEE Trans. Information Forensics and Security, vol. 6, no. 2, pp.426-437, 2011

[6] H. Liu, and M.S. Kim, "Real-Time Detection of Stealthy DDoS Attacks Using Time-Series Decomposition," Communications (ICC), 2010 IEEE International Conference, 2010.

[7] Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, "PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial of Service Attacks," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 2, pp.141-155, 2006.

[8] P.E. Ayres, H. Sun, H. J. Chao, and W. C. Lau, "ALPi: A DDoS Defense System for High-Speed Networks," IEEE J. Selected Areas Comm., vol. 24, no. 10, pp.1864-1876, 2006.

[9] H. Wang, C. Jin, and K.G. Shin, "Defense against Spoofed IP Traffic Using Hop-Count Filtering," IEEE/ACM Trans. Networking, vol. 15, no. 1, pp.40-53, 2007.

[10] P. Du, and A. Nakao, "DDoS Defense Deployment with Network Egress and Ingress Filtering," Communications (ICC), 2010 IEEE International Conference, 2010.

[11] Z. Duan, X. Yuan, and J. Chandrashekar, "Controlling IP Spoofing through Interdomain Packet Filters," IEEE Trans. Dependable and Secure Computing, vol. 5, no. 1, pp. 22-36, 2007.

[12] F. Soldo, A. Markopoulou, and K. Argyraki, "Optimal Filtering of Source Address Prefixes: Models and Algorithms," Proc. IEEE INFOCOM, 2009.

[13] M.T. Goodrich, "Probabilistic Packet Marking for Large-Scale IP Traceback," IEEE/ACM Trans. Networking, vol. 16, no. 1, pp.15-24, 2008.

[14] Y. Xiang, W. Zhou, and M. Guo, "Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks," IEEE Trans. Parallel and Distributed Systems, vol. 20, no. 4, pp.567-580, 2009.

[15] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS Attacks Using Entropy Variations," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 3, pp.412-425, 2011.

[16] Y. Xie, and S. Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," IEEE/ACM Trans. Networking, vol. 17, no. 1, pp.15-25, 2009.

[17] Y. Xie, and S. Yu, "A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors," IEEE/ACM Trans. Networking, vol. 17, no. 1, pp.54-65, 2009.

[18] 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.