

DoS detection solution for cloud platform using SNMP

Gayathri R¹ and Neelanarayanan V²

¹ ²School of Computing Science and Engineering

VIT University, Chennai, 600127, India

gayathri.r@vit.ac.in

Abstract

Internet is more prevalent in all the sectors which bring rapid changes in the computing technologies. Cloud computing is an emerging technology which replaced the existing computing techniques due to its unique dominant features and ease of use. The key design feature of the Internet creates a loophole and paves the way for attackers to exploit the vulnerabilities. Among the various cloud computing attacks, Denial of Service (DoS) attack introduces serious damage to the cloud customers in terms of availability disruption and economy of scale. This research paper aims to provide a detection mechanism for DoS attack in the cloud computing environment using the Simple Network Management Protocol (SNMP). The performance parameters play a vital role in differentiating the detection accuracy of SNMP with other existing measures. The effectiveness of SNMP is analyzed by simulating the experimental set up. **Key Words and Phrases:** DoS, SNMP, TCP-SYN.

1 Introduction

Cloud computing is a technology which comprises the existing concepts of web services, Grid computing, Network computing, Utility computing and Pervasive computing which aims to provide flexible services to users. Cloud computing is developing rapidly in

both academics and industry [5] due to its essential characteristics, which includes on-demand self-service, resource pooling, rapid elasticity, and measured service. It paves a way for the industries irrespective of their function, to increase their business capabilities on the fly without concentrating much in the new infrastructure, training of persons or licensing. Cloud is a massive collection of computer systems and servers which could be accessed through the Internet using various kinds of browsers, protocols and platforms. Cloud Platform provides a way to deliver the services to the customers. Virtualization is the key enabling technology for cloud. The applications of multiple users could be run on various virtual machines, through which the cloud monitors for the faults, viruses and other violations in the virtual environment. Hence this measure effectively eradicates the damages caused by malicious applications. Since more enterprises and persons are migrating towards cloud platform, privacy and confidentiality of data in rest, motion became a prime focus for any cloud service provider.

2 Effects of DoS and Related Survey

The applications of cloud in industries opened door for many research challenges which continues to emerge. Focused towards the security aspect of cloud environment, Distributed Denial of Service attacks play the dominant role which disrupts the availability constraint of the cloud environment. DDoS is an attack which disrupts the legitimate users [2] from accessing the cloud services by flooding the target server with bogus packets which is represented in Figure. 2. DDoS attacks should be given higher priority [3] since it leads to a drastic increase in the service demands. Among the common attack categories, we focus on TCP-SYN, UDP and HTTP floods as a preliminary work. SYN flood attack [4] is that it never responds to the server with the expected ACK value. It performs spoofing on the IP address of the legitimate client and initiates series of SYN requests which makes the server to send the SYN+ACK to falsified IP which will send back an ACK as it never sent such SYN requests. According to the survey, numerous prevention and detection measures are available for DDoS attacks which are illustrated in detail. A dynamic resource allocation mechanism is proposed [5] to elimi-

nate DDoS attacks in the cloud platform. If a cloud server is under attack, the proposed system automatically allocates additional resources from the pool. New virtual machines will be selected for cloning based on the images of existing Intrusion Prevention Systems (IPS). All the IP's work together to ensure better quality of service. As a conclusion, they are employing additional VM's from the resource pool to ensure quality of service. Actual attack mitigation measures are not addressed in the paper. Honeynet system [6] is proposed which mainly comprises honey and virtual server system. It consists of honeyfarm which is made up of honeyVM to collect the detailed attack information. Honey system controllers perform practical management for the addition or deletion of VM's and load balancing. The information collected from honeyVM will be analyzed by IDS, through which the system would cope with the new attacks. However, this measure is effective and works well only for the existing attacks. It will not cope with new attacks launched by attackers. Protocol based IDS analyze the packet information and perform the classification of the packets which flows in the honeypot by TCP, UDP, ARP and ICMP protocol. Information collected by the honeypot is composed dynamically and updated in the database. E-DoS shield is proposed which comprises the firewall, V-node and load balancer. Standard Turing tests are posed to the requesting clients to verify their legitimacy. The concepts of Software Defined Networking (SDN) which has attracted greater interest since it is used to acquire control on the network environment. SDN offers great opportunities to defeat DDoS attack in the cloud platform. In SDN, the control and data planes are combined and the underlying infrastructure is abstracted from the applications. An attacker may take advantages over the features of SDN which in turn helps to launch DDoS attacks. An EDoS shield [7] is known to be an effective technique to mitigate DDoS attacks in cloud, in which the malicious requests are detected and dropped before it reaches the service nodes.

3 Experimental evaluation of SNMP

We evaluate our detection method in the Amazon AWS console by adopting the architecture given in Figure 3. The victim server

specification is PC Intel®Xeon®2.40GHZ at 1.00 GB of RAM in which the SNMP is configured to monitor the traffic flows. The Legitimate and attack requests are simulated at different time intervals to observe its impact in the SNMP OID's. Both the traffic flows are generated using two computer systems of identical configuration. The case studies have been done to observe the impact of user legitimate/attack requests in the SNMP TCP OID's. Our preliminary work focus on detecting the TCP-SYN flood attacks in the cloud environment.

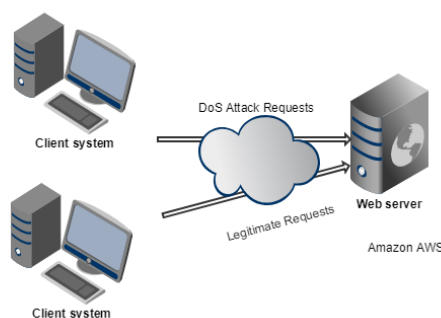


Figure 1: DoS Architecture

The Workload characteristics considered for attack traffic ranges from 10,100 and 1000 packets each sent consecutively with a time interval of 1second. The below graphs illustrates the relation between SNMP OID's chosen to differentiate the attack traffic from the legitimate one.

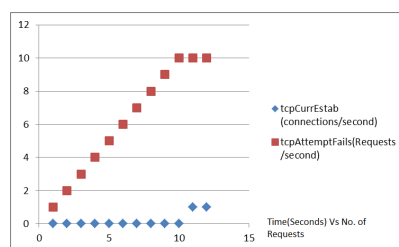


Figure 2: DoS Attack detection using SNMP

From the Figure 2, it is observed that the number of incoming attack requests which is observed through the tcpPassiveOpens

Table 1: Case study I: Impact of SNMP variables under DDoS attack.

Sl. No	SNMP Variables	Status Change	Attack parameter
1	tcpPassiveOpens	Yes	Yes
2	tcpCurrEstab	No	Yes
3	tcpRtoAlgorithm	No	No
4	tcpRtoMin	No	No
5	tcpRtoMax	No	No
6	tcpMaxConn	No	No
7	tcpAttemptFails	Yes	Yes
8	tcpEstabResets	Yes	No
9	tcpInSegs	Yes	No
10	tcpOutSegs	Yes	No
11	tcpRetransSegs	Yes	No
12	tcpConnTable	Yes	No
13	tcpInErrs	No	No
14	tcpOutRsts	No	Yes

variable is directly proportional to the tcpAttemptFails in case of DoS attack. tcpAttemptFails indicates the number of connections which have made a direct transition from either SYN-SENT or SYN-RCVD state to CLOSED state. As during DoS Attack all the received requests are SYN packets, the count of tcpCurrEstab remains constant, whereas the actual incoming request count is reflected in the tcpAttemptFails. The same variable relations are observed by varying the DoS attack rate at 100 and 1000 requests/second which are illustrated in Figure 3 and Figure 4.

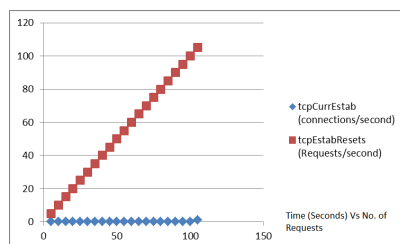


Figure 3: DoS Attack detection using SNMP (100requests)

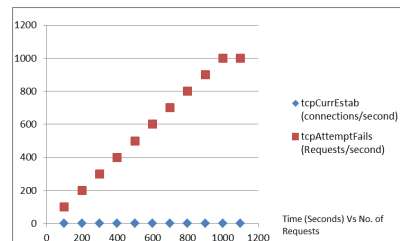


Figure 4: DoS Attack detection using SNMP (1000requests)

Table 2: Case study II: Impact of SNMP variables under Legitimate traffic

Sl. No	SNMP Variables	Status Change	Attack parameter
1	tcpPassiveOpens	Yes	Yes
2	tcpCurrEstab	Yes	Yes
3	tcpRtoAlgorithm	No	No
4	tcpRtoMin	No	No
5	tcpRtoMax	No	No
6	tcpMaxConn	No	No
7	tcpAttemptFails	Yes	Yes
8	tcpEstabResets	Yes	No
9	tcpInSegs	Yes	No
10	tcpOutSegs	Yes	No
11	tcpRetransSegs	Yes	No
12	tcpConnTable	Yes	No
13	tcpInErrs	No	No
14	tcpOutRsts	Yes	No

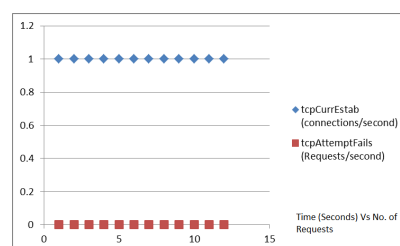


Figure 5: Status change of SNMP variables under Legitimate traffic(1 concurrent request)

From the Figure 5, it is observed that the number of incoming requests `tcpPassiveOpens` is directly proportional to the `tcpCurrEstab` as all the requests are legitimate. In this case, the `tcpAttemptFails` variable is observed as a constant. The same variable relation is observed by repeating the experiment with 10 requests by creating 9 concurrent connections as illustrated in Figure 6.

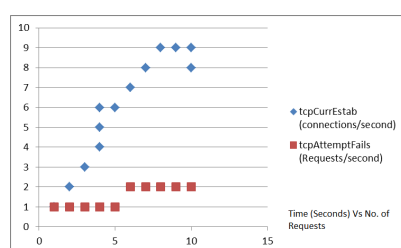


Figure 6: Status change of SNMP variables under Legitimate traffic(9 concurrent request)

4 Results and Discussion

In the case of DoS attack, `tcpAttemptFails` shows linear variation whereas in the case of legitimate traffic `tcpCurrEstab` variable shows linear variation. But due to overload conditions of web server also, `tcpCurrEstab` variable may remain constant. In that case, in order to differentiate the attack request from the legitimate one, `tcpConnTable` is referred to track the request's origin and according to the human behavioral analysis [7] a legitimate user can send only 3 requests/second. Hence it is concluded that, if more than 3 requests/second originates from the source that could be concluded as a DoS attack. SNMP variables show effective proof in defending that.

5 Conclusion and Future Work

We have presented a DoS attack detection method using the SNMP variables and demonstrated its effectiveness in real time. The identified method is tested in a real time amazon aws console. This paper discusses methods which serve as an effective measure in accurate identification and detection of DoS attack requests. The future

enhancements include proposing a prevention framework for DoS attack in the cloud platform.

References

- [1] Shui Yu, Yonghong Tian, Song Guo, Dapeng Oliver Wu, "Can We Beat DDoS Attacks in Clouds" IEEE Transactions on Parallel and Distributed Systems, Vol.25(9),p.p: 2245-2254 September 2014.
- [2] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, Rajkumar Buyya, "DoS Attacks in Cloud Computing: Issues, Taxonomy and Future Directions", ACM Computing surveys, Vol:1(1), December 2015.
- [3] Gaurav Somani, Abhinav Johri, Mohit Taneja, Utkarsh Pyne, Manoj Singh Gaur, Dheeraj Sanghi, "DARAC: DDoS Mitigation Using DDoS Aware Resource Allocation in Cloud", In the proceedings of Springer, p.p: 263-282, December 2015.
- [4] M.Armbrust,A.Fox,R.Griffith,A.D. Joseph,R.H.Katz,A.Konwinski, G.Lee,D.A.Patterson,A.Rabkin, I. Stoica,andM.Zaharia, "Above the clouds: A berkeley view of cloud computing", EECS Dept., Univ.California, Berkeley,CA, USA, Tech. Rep.UCB/EECS-2009- 28, Feb. 2009.
- [5] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing", J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1-11, Jan. 2011.
- [6] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A Survey on Security Issues in Cloud Computing", CoRR, vol. abs/1109.5388, 2011.
- [7] F. Al-Haidari,K. Salah,M. Sqalli,S. M. Buhari,"Performance Modeling and Analysis of the EDoS-Shield Mitigation",Arabian Journal of Science and Engineering, In the proceedings of Springer, 2017.

