ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.7, 5105–5113
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.7.76 Spec. Iss. on AMABDA-2020

WEB-ACL BASED DOS MITIGATION SOLUTION FOR CLOUD

GAYATHRI R.[1], RAJIV VINCENT, M. RAJESH, ARUN KUMAR SIVARAMAN,
AND A. MURALIDHAR

ABSTRACT. TodayâĂŹs internet community is vulnerable to wide range of attacks due to its interconnected nature. Denial of Service poses a serious threat due to prevalence of hacking tools which makes such attacks more common. DoS is more disruptive as it completely compromises the availability constraint of a web service or online service. Mitigation solutions are numerous based on several researches but none stands to be efficient in overwhelming or countering such attacks. Hence a detailed analysis about the existing technologies in cloud platform along with the mitigation measures are essential, which helps in yielding most prominent and promising solution. This study focuses those aspects and as an outcome web based ACL is proposed which helps in filtering the DoS attacks before it reaches the application itself. Web-based ACLâĂŹs are effective in filtering and differentiating the incoming traffic based on the rules defined. The rules for DoS detection are defined based on the dataset analysis of KDD for analysing the patterns and arrived at an efficient solution. The efficiency of web ACL is tested in Amazon Web Services (AWS) console and effectiveness in filtering is formulated.

1. INTRODUCTION

Internet is a wide scale of networked systems which operates together for offering numerous service categories. The World Wide Web acts as a major driving force as it attracts more than one million new users in a day. The rapid

[1] *corresponding author*

2010 *Mathematics Subject Classification.* 65Y20.
Key words and phrases. DDoS, KDD, AWS, ACL.

development of information technology with increased storage, computing capabilities, and decreased costs makes it more affordable and pervasive. The current technological advancements with a tremendous increase in the computing power pave way for the rise of numerous security violations. The cyberspace is the interconnected ecosystem that poses inherent vulnerabilities that cannot be removed as the entry points are innumerable.

The current scenario monitors and controls the critical infrastructure which in turn is exposed to risk factors such as the interconnectedness of sectors, proliferation of exposure points and concentration of assets. Ensuring integrity and availability in such cases are essential for the economy, public safety, and national security. Attacks on online services are growing in both quantity and sophistication. A successful attack creates a major impact on internet-connected services and makes it irreparable. The consequences in security breach affect all common categories of financial, legal and reputation sectors. The massive attractive features and pay-as-you-go model of cloud computing draws the attention among 70% of the organizations to migrate their services to cloud. Denial of Service (DoS) is the widely prevalent security attack which disrupts the online services. The same DoS arriving from multiple sources are termed as Distributed Denial of Service (DDoS) attacks. According to the annual cybersecurity report of cisco [1], 42 % of the organizations experienced DoS attacks in 2017. Second Life reported the prevalent DoS attack in the year 2018 where the complete portal is down for 24 hours. In 2018, security researches detected a new botnet named chalubo [2], which is mainly designed for launching the TCP-SYN attack.

Early detection of DoS is essential as it completely disrupts the availability constraint of online services. Cloud computing is the current technology which is uniquely adopted in almost all organizations for various scenarioâĂŹs due to its simplicity, elasticity and rapid scaling capabilities.

2. Background and Impact of DoS

The power of current technologies indirectly contributes to the launch of large scale DoS attacks. These attacks exponentially increase the number of requests at the target by increasing the attack power. This, in turn, increases the difficulty of attribution as the true attack source is harder to identify. DoS affect organizations in terms of both cost and time while the resources, services are inaccessible. If the critical infrastructure of an organization goes inaccessible, it leads to a severe business loss where it is the loss of customers in terms of e-commerce. According to the recent report of Amazon Web Services (AWS), even a 100-millisecond delay in response time causes a 1 % drop in the overall sales. Any company losing its reputation due to DoS, witnesses the switching of its customers to an alternate option as they canâĂŹt afford to have an unavailable service.

Detection and Mitigation of DoS attacks yield topmost priority as it disrupts the CIA (Confidentiality, Integrity, Availability) triad which is the backbone for internet services. If any online services failed to address the concerns related to CIA, heavy financial loss and loss of reputation occurs which even includes the loss of customerâĂŹs trust. According to the DoS attack statistics represented in Fig. 1, the frequency of DoS attacks is increasing every year. The volume of DoS attacks is growing abruptly as it begins with 0.4 GB in the year of 2000 and reaches approximately 500 GB in the current year. It is impossible to handle such a large volume of incoming attack traffic by the traditional defense mechanisms which in turn creates a way for the emergence of advanced methodologies.

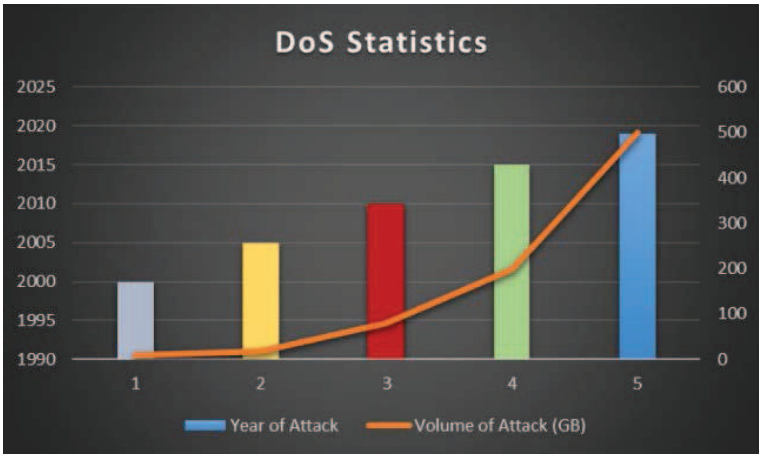

FIGURE 1. DoS Statistics

- Monetary profit
- Disruption of execution framework
- Retribution
- Ideological conviction

- Scholarly challenge
- Administration inaccessibility
- Cyberwarfare

3. Role of MTD in DoS Detection

In spite of the advancements, the DoS attacks are launched by exploiting the loopholes in the protection methodologies. Hence an effective DoS defence strategy is still an open challenge. In addition to the traditional defence measures firewall and intrusion detection systems, the updated techniques such as dynamic packet marking, packet filtering, header inspection and Simple Network Management Protocol (SNMP), Moving Target Defence (MTD) also joins hand in the process of detecting TCP-SYN based DoS attacks. The MTD based techniques for shuffling the incoming requests, additional capacity for instantiating server nodes, attack isolation using head proxy [6], authentication through Proof-Of-Work (POW) [7], MOTAG for proxy relocation [8], proxy harvesting attack [9] [10] are the more common strategies adopted in the current techniques. Each technique addresses the DoS mitigation in an efficient way but the drawbacks incurred should be given more priority as the effectiveness of the solution is merely based on those constraints.

In the detection procedure of SNMP, the MIBs tcpAttemptFails and tcpOutRsts [3][4][5] are utilized which verifies how many numbers of incoming requests are getting mapped to failed and reset requests. Based on such observations, traffic differentiation between normal and attack ones are achieved. The MTD techniques attempt to yield better results to avoid DoS by continuously changing either the location or defence procedure of the resources through the advanced measures as listed below:

- increased uncertainty
- limited exposure to vulnerability
- reversed asymmetric situation
- frequent target change, and
- Increased resiliency

4. MTD Based DoS Architecture

Diversity and Redundancy are the identified Moving Target Defence strategies in order to create uncertainty and randomness in the attack paths directed to the webserver. Such measures increase the uncertainty, cost, and complexity for attackers, limits the exposure to vulnerabilities and increases overall resiliency by decreasing the attack probability. Current MTD techniques lack in terms of quantitative measures for evaluating the effectiveness of MTD techniques. Attack probability and cost measures are considered to demonstrate the effectiveness of MTD system.

Mitigation of DoS attacks is a critical concern in the current computing scenario as it disrupts the baseline of an organizationâĂŹs function by degrading its service and performance. The role of mitigation is to provide complete protection of the targeted resources from DoS attacks. In general, such protection is achieved through the specially designed network equipment or any other cloud-based protection service. The traditional mitigation approaches failed to prove its effectiveness due to the advanced attacking tools. Complete mitigation of DoS is an open challenge as achieving it will increase the complexity of protection methods. Hence there is a need for an efficient strategy that is satisfied by the Moving Target Defence technique.

A dynamic moving target attack surface creates numerous difficulties against attackers. This equalizes the playing field between defenders and attackers. MTD belongs to the proactive category which attempts to nullify the attacks by introducing uncertainty during the attack reconnaissance and planning phases. Such uncertainty could be achieved by frequent, random changes in the system configuration to make it unpredictable by the attackers. In general, the various MTD methods can be grouped in one among the three main categories as listed below:

(1) Network-level MTD
(2) Host-level MTD
(3) Application-level MTD

The network-level MTD refers to changes that are made in the shape and structure of the network graph which includes uncertainty in terms of IP-hopping, randomizing port numbers, dynamic port mapping and fake listing hosts. The host-level MTD focuses on changes concerning the host and operating system by changing its naming and configuration. The application-level MTD includes version and randomly arranging memory layout.

4.1. **Components of MTD.** To have a clear understanding of MTD systems, the components needs to be explored as it plays a major role. Through the MTD components, complete detection architecture of MTD could be drawn as depicted below:

(1) **MTD technique (What-to-Move):** This MTD technique identifies the component to be modified to introduce complexity to the attackers. These components can vary from identities within the network to physical devices.

(2) **MTD approach (When-to-Move):** It describes the logic used when and how often to modify the configuration to protect it from attackers. Various methods are available to carry out this including pseudo-random and game-theoretic approaches.

(3) **Applications of MTD:** It identifies the area of the MTD system which is applicable to hinder reconnaissance efforts or to protect against unwanted modification and analysis.

(4) **Evaluation methods:** It defines methods to evaluate whether the chosen MTD methodology is effective or not. There are numerous definitions to assess the same.

5. Access Control List (ACL) for DoS Avoidance

Based on the initial analysis about the patterns of DoS from KDD dataset and from SNMP experimental set up the metrics count of incoming requests, arrival rate, request size, IP address, established connections are considered and ACL rules are formulated based on the inferences.

» DoSFilterACL1: (Mode: count)
Contains rule to validate HTTP methods in incoming requests

» DoSFilterACL2: (Mode: count)
This contains rule to validate the pattern of URI in the incoming requests.

» DoSFilterACL3: (Mode: count)
Contains rule to check the pattern of Request Size in incoming requests extracted from the HTTP Body

» DoSFilterACL4: (Mode: count)

Contains rule to check the type of User-Agent extracted from the HTTP Body

» DoSFilterACL5: (Mode: Block)

Contains rule to check the pattern of known vulnerabilities in Windows

» DoSFilterACL6: (Mode: Block)

Contains rule to check the pattern of known vulnerabilities in Linux

» DoSFilterACL7: (Mode: Block)

Rate limits maximum number of requests permitted from a single IP address in a 5-minute period. It considers the request that match the criteria in rule statement.

The effectiveness of ACL is evaluated based on the attack probability success rate which is depicted in Figure 2.

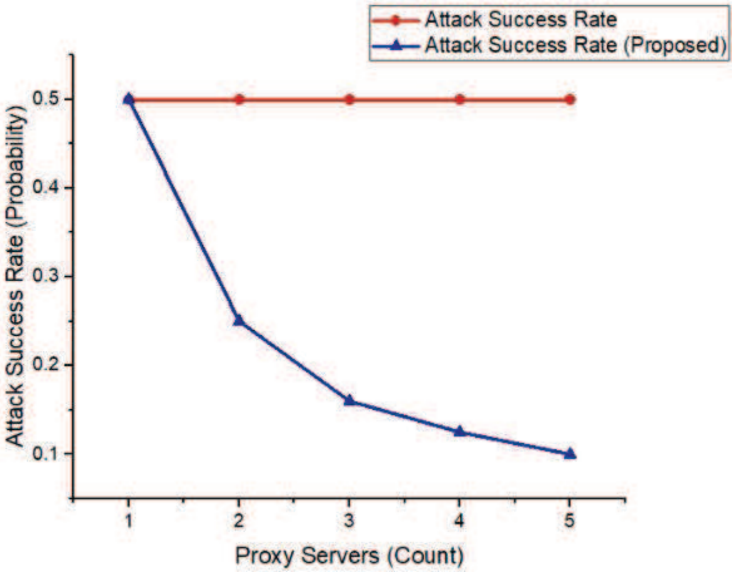

FIGURE 2. Probability of Attack Success Rate

In MTD, attack uncertainty could be achieved. Hence on analysing the technological importance and prevalence of both methods, we have proposed and implemented web based ACLâĂŹs for blocking the DoS attack traffic based on the metrics derived from the existing literature and results are formulated with respect to the attack success rate. Even if number of users is increasing, the attack probability remains the same as less than 0.1. Hence this type of measure is efficient in mitigation DoS attack.

Conclusion and Future Work

This work demonstrates the adoption of MTD strategies in order to avoid DoS attacks in the cloud environment. Though the proposed SNMP MIBs early DoS detection is achieved in the current computing scenario. The reconnaissance and attack planning phases are eliminated through the MTD concepts. Introducing uncertainty in such phases forces the attacker to use advanced exploiting tools and consumes more time, cost. The attackers usually adapt to known exploitable tools and attacking methods to launch an attack in a shorter duration with reduced costs. If the cost aspect of attackers is disturbed, the time taken to launch attacks will be more, and the same has been evident based on our probability of attack success rate value. Increase in the ACLâĂŹs specific to the pattern of DoS in the incoming traffic reduces the attack success rate.

The current work failed to ensure the performance of DoS detection under complex real-time scenarios. Thus, the integration of a scalable algorithm with less complexity for the current computing scenario can be employed in the future. Thus, in turn, it helps to enhance the DoS mitigation process.

References

[1] N. Hawkins: *Why communication is vital during a cyber-attack*, Network Security, 2017, 12âĂŞ14.

[2] P. Geenens: *IoT botnet traits and techniques*, Botnets: Architectures, Countermeasures, and Challenges, 2019, pp. 101.

[3] R. Gayathri, V. Neelanarayanan: *Denial of Service Attack prediction using Gradient Descent Algorithm*, Advances in Internet Research and Engineering (Springer Nature), **1**(45) (2020), 1-8.

[4] R. Gayathri, V. Neelanarayanan: *Identification of Regression function and distribution model for Denial of Service attack in Second Life online community using Simple Network Management Protocol*, International Journal of Web Based Online Communities , Inderscience, **15**(3) (2019), 225-237.

[5] R. Gayathri, V. Neelanarayanan: *DoS detection solution for cloud platform using SNMP*, International Journal of Pure and Applied Mathematics, **119**(11) (2018), 175-183.

[6] K. Munivara, A Prasad, Rama Mohan Reddy, K. Venugopal Rao: *DoS and DDoS Attacks: Defence, Detection and Traceback Mechanisms - A Survey*, Global Journal of Computer Science And Technology, **14**(7) (2014).

[7] H. Wang, L. Xu, G. Gu: *FloodGuard: a DOS attack prevention extension in software defined networks*, 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Rio de Janeiro, 2015, 239-250. doi: 10.1109/DSN.2015.27

[8] G.-L. Cai, B.-S. Wang, W. Hu, T.-Z. Wang: *Moving target defense: state of the art and characteristics*, Frontiers of Information Technology and Electronic Engineering **17** (2016), 1122âĂŞ1153.

[9] A. Clark, K. Sun, R. Poovendran: *Effectiveness of ip address randomization in decoy-based moving target defense*, 52nd IEEE Conference on Decision and Control, Florence, 2013, 678-685. doi: 10.1109/CDC.2013.6759960

[10] M. Darwish, A. Ouda, L.F. Capretz: *A cloud-based secure authentication (csa) protocol suite for defense against denial of service (dos) attacks*, Journal of Information Security and Applications, **20** (2015), 90âĂŞ98.

School of Computer Science and Engineering,
Vellore Institute of Technology,
Chennai, India.
E-mail address: `gayathri.r@vit.ac.in`

School of Computer Science and Engineering,
Vellore Institute of Technology,
Chennai, India.
E-mail address: `rajiv.vincent@vit.ac.in`

School of Computer Science and Engineering,
Vellore Institute of Technology,
Chennai, India.
E-mail address: `rajesh.m@vit.ac.in`

School of Computer Science and Engineering,
Vellore Institute of Technology,
Chennai, India.
E-mail address: `arunkumar.sivaraman@vit.ac.in`

School of Computer Science and Engineering,
Vellore Institute of Technology,
Chennai, India.
E-mail address: `muralidhar.a@vit.ac.in`