ISSN: 2348-2079

International Journal of Intellectual Advancements and Research in Engineering Computations (IJIAREC)

IJIAREC |Vol.11 | Issue 4 | Oct - Dec -2023

www.ijiarec.com

DOI : https://doi.org/10.61096/ijiarec.v11.iss4.2023.13-17

Review

Distributed Detection And Prevention For The Distributed Denial Of Service Attacks

M. DivyaBharathi[1], B. BeaulaPinky. M.E[2]

[1]*PG Student, Dept. of C.S.E, Sri Shanmugha College Of Engineering And Technology, [Salem], Tamilnadu, India*
[2]*Assistant Professor, Dept. of C.S.E, Sri Shanmugha College Of Engineering And Technology, [Salem],Tamilnadu, India*

*Author for Correspondence: M. DivyaBharathi
Email: yokeshshanmuga@gmail.com

Published on: 30 Dec 2023

Published by:
DrSriram Publications

Abstract

Distributed Denial of Service (DDOS) attacks continue to escalate in size and impact despite efforts to control and limit exposures that enable them to be successful. The combining separate existing information technologies in a collaborative system. Devices used to gather evidence on attack methods and provide for reverse engineering malware are 'honey pots'.Intrusion prevention systems (IPS) can take action to alert administrators to potential misuse of computing assets and in many cases execute predetermined response to malicious activity Denial of Service (DDOS) attack, which aims to make a service unavailable to legitimate clients, has become a severe threat to the Internet security. Traditional DDOS attacks mainly abuse the network bandwidth around the Internet subsystems and degrade the quality of service by generating congestions at the network. Consequently, several network-based defense methods have tried to detect these attacks by controlling traffic volume or differentiating traffic patterns at the intermediate routers .However, with the boost in network bandwidth and application service types, recently, the target of DDOS attacks has shifted from network to server resources and application procedures themselves, forming a new application DDOS attack.

Keywords: Distributed Denial of Service (DDOS), Intrusion prevention systems (IPS).

INTRODUCTION

Denial Of Service (DDOS) attack, which aims to make a service unavailable to legitimate clients, has become a severe threat to the Internet security. Traditional DDOS attacks mainly abuse the network

bandwidth around the Internet subsystems and degrade the quality of service by generating congestions at the network. Consequently, several network-based defense methods have tried to detect these attacks by controlling traffic volume or differentiating traffic patterns at the intermediate routers .However, with the boost in network bandwidth and application service types, recently, the target of DDOS attacks has shifted from network to server resources and application procedures themselves, forming a new application DDOS attack.

PROBLEM DESCRIPTION

By exploiting flaws in application design and implementation, application DDOS attacks exhibit three advantages over traditional DDOS attacks which help evade normal detections: malicious traffic is always indistinguishable from normal traffic, adopting automated script to avoid the need for a large amount of "zombie" machines or bandwidth to launch the attack, much harder to be traced due to multiple redirections at proxies. According to these characteristics, the malicious traffic can be classified into legitimate-like requests cases:

1) At a high inter arrival rate and
2) Consuming more service resources.

PROJECT OVERVIEW

The identification of attackers can be much faster if we can find them out by testing the clients in group instead of one by one. Thus, the key problem is how to group clients and assign them to different server machines in a sophisticated way, so that if any server is found under attack, we can immediately identify and filter the attackers out of its client set. Apparently, this problem resembles the group testing (GT) theory which aims to discover defective items in a large population with the minimum number of tests where each test is applied to a subset of items, called pools, instead of testing them one by one.Therefore, we apply GT theory to this network security issue and propose specific algorithms and protocols to achieve high detection performance in terms of short detection latency and low false positive/negative rate. Since the detections are me rely based on the status of service resources usage of the victim servers, no individually signature-based authentications or data classifications are required; thus, it may overcome the limitations of the current solutions.

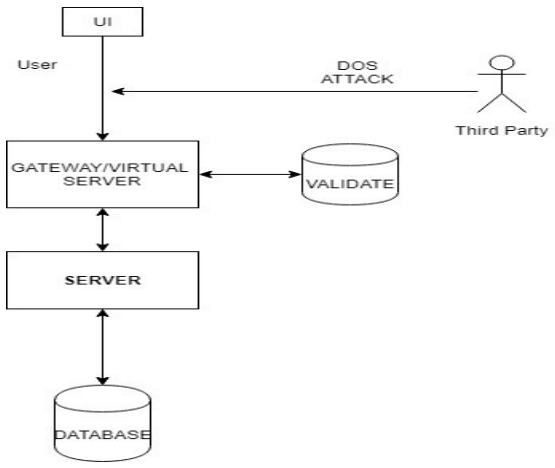
EXISTING SYSTEM

Application DDOS attack, which aims at disrupting application service rather than depleting the network resource, has emerged as a larger threat to network services, compared to the classic DDOS attack. Owing to its high similarity to legitimate traffic and much lower launching overhead than classic DDOS attack, this new assault type cannot be efficiently detected or prevented by existing detection solutions.

DISADVANTAGES

- Each request is verified for DDOS, once it is posted to server.Sometimes continues verification or checking of some request or every request in sequence manner can increase the server work load.
- Due to this existing system leads to failure randomly.

PROPOSED SYSTEM



To identify application DDOS attack, we propose a novel group testing (GT)-based approach deployed on back-end servers, which not only offers a theoretical method to obtain short detection delay and low false positive/negative rate, but also provides an Underlying framework against general network attacks. More specifically, we first extend classic GT model with size constraints for practice purposes, then redistribute the client service requests to multiple virtual servers embedded within each back-end server machine, according to specific testing matrices.

Based on this framework, we propose a machine learning detection mechanism and modern cracking algorithm using some dynamic thresholds to efficiently identify the attackers. The focus of this work lies in the detection algorithms proposed and the corresponding theoretical complexity analysis. We also provide preliminary simulation results regarding the efficiency and practicability of this new Scheme.

*Profile Mode:*The application first allowed to run in profile mode to capture the threshold time for each kind if request.

*Secure Mode:*The application is then changed to secure mode where DDOS attacker is identified and blocked to reduce the load the actual server.

Advantage

- Applying machine learning aspect to identify the threshold improves the quality of DDOS detection
- Every request or all the requests to the server are parallel checked for DDOS by using GT.

Due to this server performance is not affected and reduces the workload of Server.

METHODOLOGY

ALGORITHM: MODERN CRACKING ALGORITHM

PACKET FILTER

Packet filters act by inspecting the "packets" which transfer between computers on the Internet. If a packet matches the packet filter's set of rules, the packet filter will drop (silently discard) the packet, or reject it (discard it, and send "error responses" to the source). It is observed that a web transaction typically consists of hundreds or even thousands of packets sent from a client to a server. During a DDOS attack, since the packets will be randomly dropped at high probability, each of these packets will go through a long delay due to TCP timeouts and retransmissions. Consequently, that total page download time in a transaction can take hours. Such service quality is of little or no use to clients. In contrast, our defense system ensures that, throughout a web transaction, only very first packet from a client may get delayed. All later packets will be protected and served.

MAC GENERATOR

MAC Generator distinguishes the packets that contain genuine source IP addresses from those that contain spoofed address. Once the very first TCP SYN packet of a client gets through, the proposed system immediately redirects the client to a pseudo-IP address (still belonging to the website) and port number pair, through a standard HTTP URL redirect message. Certain bits from this IP address and the port number pair will serve as the Message Authentication code (MAC) for the client's IP address.

MAC is a symmetric authentication scheme that allows a party A, which shares a secret key k with another party A, which shares a secret key k with another party B, to authenticate a message M sent to B with a signature MAC (M, k) has the property that, with overwhelming probability, no one can forge it without knowing the secret key k. Next we are verifying the secret key to prevent attackers who are using genuine address or spoofed address. Since a legitimate client uses its real IP address to communicate with the server, it will receive the HTTP redirect message (hence the MAC). So, all its future packets will have the correct MACs inside their destination IP addresses and thus be protected. The DDOS traffic with spoofed IP addresses, on the other hand, will be filtered because the attackers will not receive the MAC sent to them.

So, this technique effectively separates legitimate traffic from DDOS traffic with spoofed IP addresses.

IP HANDLER

When an attackers using genuine address, the proxy server uses the Deficit Round Robin algorithm to collect the address of the client request. if an attacker sends packets much faster than its fair share, the scheduling policy will drop its excess traffic. More Over, for each genuine IP address, the system will perform accounting on the number of packets that reach the firewall but are dropped by the scheduler; its IP address will be blacklisted.

SYSTEM IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of Methods to achieve changeover and evaluation of changeover methods.

CONCLUSION

A novel technique for detecting application DDOS attack by means of a new constraint-based group testing model. Motivated by classic GT methods, three detection algorithms were proposed and a system based on these algorithms was introduced. Theoretical analysis and preliminary simulation results demonstrated the outstanding performance of this system in terms of low detection latency and false positive/negative rate.

Our focus of this Project is to apply group testing principles to application DDOS attacks, and provide an underlying framework for the detection against a general case of network assaults, where malicious requests are indistinguishable from normal ones. For the future work, we will continue to investigate the potentials of this scheme and improve this proposed system to enhance the detection efficiency. Some possible directions for this can be:

- The sequential algorithm can be adjusted to avoid the requirement of isolating attackers
- More efficient d-disjunct matrix could dramatically decrease the detection latency, as we showed in the theoretical analysis. A new construction method for this is to be proposed and can be a major theoretical work for another Project.
- The overhead of maintaining the state transfer among virtual servers can be further decreased by more sophisticated techniques.
- Even that we already have quite low false positive/ negative rate from the algorithms,

REFERENCES

1. Francois J, Aib I, Boutaba R.Firecol: a collaborativeprotectionnetwork for the detection of floodingDDOSattacks.IEEEACM Trans Netw.2012;20(6, Dec):1828-41. doi: 10.1109/TNET.2012.2194508.
2. Zargar ST, Joshi J, Tipper D.A survey of defensemechanismsagainstdistributeddenialofService (DDOS)floodingattacks.IEEE CommunSurv Tutorials.Nov2013;15(4):2046-69. doi: 10.1109/SURV.2013.031413.00127.
3. Yaar A, Perrig A, Song D.StackPi: newpacketmarking and filteringmechanisms for DDOS and IPspoofingdefense.IEEE J Sel AreasCommun.Oct2006;24(10):1853-63. doi: 10.1109/JSAC.2006.877138.
4. Wang H, Jin C, Shin KG.Defense againstspoofedIPtrafficusinghop-countfiltering.IEEEACM Trans Netw.Feb2007;15(1):40-53. doi: 10.1109/TNET.2006.890133.
5. Duan Z, Yuan X, Chandrashekar J.Controlling IPspoofing through interdomainpacketfilters.IEEE Trans Depend SecComput. Feb2008;5(1):22-36. doi: 10.1109/TDSC.2007.70224.
6. Sung M, Xu J.IPtraceback-based intelligent packet filtering: a novel technique for defending against Internet DDOS attacksIEEE, translatorOn Parall.and Distr. Sys.Sep2003;14(9):861-72.
7. Sung M, Xu J, Li J, Li L.Large-scaleIPtraceback in high-speed Internet: practicaltechniques and information-theoreticfoundation.IEEEACM Trans Netw.Dec2008;16(6):1253-66.
8. Xiang Y, Li K, Zhou W.Low-rateDDOSattacksdetection and traceback by usingnewinformationmetrics. IEEE Trans.Inform.ForensicSecurIEEE, translator.May2011;6(2):426-37. doi: 10.1109/TIFS.2011.2107320.
9. Ballani H, Chawathe Y, Ratnasamy S, Roscoe T, Shenker S.Off by default! In:Proceedings of theHotNets-IV, Nov2005, College Park, MD, USA.
10. Luo H, Chen Z, Cui J, Zhang H, Zukerman M, Qiao C, "CoLo.R: an information-centric internet architecture for innovations.IEEE Netw. May2014;28(3):4-10.
11. Antikainen M, Aura T, Sarela M.Denial ofService attacks in bloomfilter- based forwarding.IEEEACM Trans Netw.Oct2014;22(5):1463-76. doi: 10.1109/TNET.2013.2281614.
12. Luo H, Chen Z, Cui J, Zhang H.An approach for efficient, accurate, and timelyestimation of trafficmatrices. In:Proceedings of the IEEE globalinternetsymposium (GI'14), May2014, Toronto, Canada. p. 67-72. doi: 10.1109/INFCOMW.2014.6849170.

13. Luo H, Cui J, Chen Z, Jin M, Zhang H.Efficient integration of software defined networking and information-centric networking with Color. In:Proceedings of theIEEE GLOBECOM. Vol. ’14(Dec).TX: Austin; 2014. p. 1962-7. doi: 10.1109/GLOCOM.2014.7037095.
14. Chen Z, Luo H, Cui J, Jin M.Security analysis of a future Internet architecture. In:Proceedings of theIEEE ICNP. Vol. ’13(Oct).Göttingen, Germany; 2013:1-6. doi: 10.1109/ICNP.2013.6733675.
15. Yaar A, Perrig A, Song D.SIFF: a stateless internet flow filter to mitigate DDOS flooding attacks. In:Proceedings of the IEEE symposium on security and privacy, May2004, Oakland, CA, USA:130-43. doi: 10.1109/SECPRI.2004.1301320.