Asian Journal of Engineering and Applied Technology (AJEAT)
Vol1.No.1 2013 pp 35-38.
available at: www.goniv.com
Paper Received:11-06-2013.
Paper Accepted:28-06-2013
Paper Reviewed by: 1. John Arhter 2. Dr.K.Ramkumar
Editor : Prof. P.Muthukumar

A GROUP BASED TESTING APPROACH TO DETECT DOS ATTACK

[1]*S.Selvakumaran.*, [2]*K.Manikandan*
[1,2] *Faculty of Engineering and Technology*
[1,2]*PRIST UNIVERSITY, Kumbakonam.*
[1] *sysadmmrkt@yahoo.com* ,[2] *mkmanikandan.mca@gmail.com*

ABSTRACT

Application DoS 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 DoS 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. To identify application DoS 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 two-mode detection mechanism 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. Further discussions over implementation issues and performance enhancements are also appended to show its great potentials.

Keywords: DoS, Attack, Class Group Testing, Dtection Algorithm

1. INTRODUCTION

DENIAL-OF-SERVICE (DoS) attack, which aims to make a service unavailable to legitimate clients, has become a severe threat to the Internet security. Traditional DoS attacks mainly abuse the network bandwidth around the Internet subsystems and degrade the quality of service by generating congestions at the network [2]. Consequently,
several network-based defense methods have tried to detect these attacks by controlling traffic volume or differentiating traffic patterns at the intermediate routers [10], [13].However, with the boost in network bandwidth and application service types, recently, the target of DoS attacks has shifted from network to server resources and application procedures themselves, forming a new application DoS attack [1], [2].
As stated in [2], by exploiting flaws in application design and implementation, application DoS attacks exhibit three advantages over traditional DoS 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 of two cases: 1) at a high interarrival rate and 2) consuming more service resources. We call these two cases “high-rate” and “high-workload” attacks, respectively,in this paper.
Since these attacks usually do not cause congestion at the network level; thus, bypass the network-based monitoring system [21], detection, and mitigation at the end system of the victim servers have been proposed [1], [3], [19]. Among them,the DDoS shield [1] and CAPTCHA-based defense [3] are the representatives of the two major techniques of system-based approaches: session validation based on legitimate behavior profile and authentication using human-solvable puzzles. By enhancing the

Asian Journal of Engineering and Applied Technology (AJEAT)
Vol1.No.1 2013 pp 35-38.
available at: www.goniv.com
Paper Received :11-06-2013.
Paper Accepted:28-06-2013
Paper Reviewed by: 1. John Arhter 2. Dr.K.Ramkumar
Editor : Prof. P.Muthukumar

accuracy of the suspicion assignment for each client session, DDoS shield can provide efficient session schedulers for defending possible DDoS attacks. However,the overhead for per-session validation is not negligible,especially for services with dense traffic. CAPTCHA-based defenses introduce additional service delays for legitimate clients and are also restricted to human interaction services.

A kernel observation and brief summary of our method is: 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 [14] 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 merely 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.

2.RELATED WORKS

2.1 Existing system

Since these attacks usually do not cause congestion at the network level; thus, bypass the network-based monitoring system , detection, and mitigation at the end system of the victim servers have been proposed [1], [3]. Among them, the DDoS shield [1] and CAPTCHA-based defense [3] are the representatives of the two major techniques of system-based approaches: session validation based on legitimate behavior profile and authentication using human-solvable puzzles. By enhancing the accuracy of the suspicion assignment for each client session, DDoS shield can provide efficient session schedulers for defending possible DDoS attacks. However, the overhead for per-session validation is not negligible, especially for services with dense traffic. CAPTCHA-based defenses introduce additional service delays for legitimate clients and are also restricted to human interaction services.

In a system viewpoint, our defense scheme is to embed multiple virtual servers within each physical back-end server and map these virtual servers to the testing pools in GT, then assign clients into these pools by distributing their service requests to different virtual servers. By periodically monitoring some indicators (e.g., average responding time) for resource usage in each server and comparing them with some dynamic thresholds, all the virtual servers can be judged as “safe” or “under attack.” By means of the decoding algorithm of GT, all the attackers can be identified. Therefore, the biggest challenges of this method are threefold:

1) How to construct a testing matrix to enable prompt and accurate detection.
2) How to regulate the service requests to match the matrix in practical system.
3) How to establish proper thresholds for server source usage indicator, to generate accurate test outcomes.

2.2 Proposed System

Similar to all the earlier applications of GT, this new application to network security requires modifications of the classical GT model and algorithms, so as to overcome the obstacle of applying the theoretical models to practical scenarios. Specifically, the classical GT theory assumes that each pool can have as many items as needed and the number of pools for testing is unrestricted. However, in order to provide real application services, virtual servers cannot have infinite quantity or capacity, i.e., constraints on these two parameters are required to complete our testing model. Our main contributions in this paper are as follows:

1. Propose a new size-constrained GT model for practical DoS detection scenarios.
2. Provide an end-to-end underlying system for GT based schemes, without introducing complexity at the network core.
3. Provide multiple dynamic thresholds for resource

Asian Journal of Engineering and Applied Technology (AJEAT)
Vol1.No.1 2013 pp 35-38.
available at: www.goniv.com
Paper Received:11-06-2013.
Paper Accepted:28-06-2013
Paper Reviewed by: 1. John Arhter 2. Dr.K.Ramkumar
Editor : Prof. P.Muthukumar

usage indicators, which help avoid error test from legitimate bursts and diagnose servers handling various amount of clients.
4. Present three novel detection algorithms based on the proposed system, and show their high efficiencies in terms of detection delay and false positive/negative rate via theoretical analysis and simulations.

3. CLASSIC GROUP TESTING

3.1. Basic Idea

The classic GT model consists of t pools and n items (Including at most d positive ones). This model can be represented by a t × n binary matrix M where rows represent the pools and columns represent the items. An entry M[i,j] 1 if and only if the i^{th} pool contains the j^{th} item; otherwise, M[i,j]= 0. The t-dimensional binary column vector V denotes the test outcomes of these t pools, where 1-entry represents a positive outcome and 0-entry represents a negative one. Note that a positive outcome indicates that at least one positive item exists within this pool, whereas negative one means that all the items in the current pool are negative.
Due to the benefits of virtual servers we employ, this constraint can be relaxed, but we keep it for the theoretical analysis in the current work.

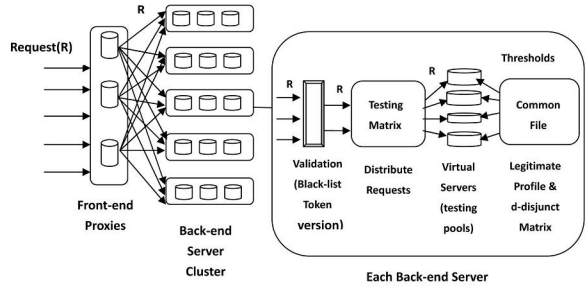

Fig Victim/detection model.

4 DETECTION ALGORITHMS

4.1 Sequential Detection with Packing

This algorithm investigates the benefit of classic sequential group testing, i.e., optimizing the grouping of the subsequent tests by analyzing existing outcomes. Similar to traditional sequential testing, each client (column) only appears in one testing pool (server) at a time. However, to make full use of the available K servers, we have all servers conduct test in parallel.

4.2 Sequential Detection without Packing

Considering the potential overload problem arises from the "packing" scheme adopted in SDP, we propose another algorithm where legitimate clients do not shift to other servers after they are identified. This emerges from the observation that legitimate clients cannot affect the test outcomes since they are negative. Algorithm 2 includes the abstract pseudocode of this SDoP scheme. Notice that in this algorithm for the DANGER mode, requests from one client are still handled by one server, as SDP did.

4.3 Partial Nonadaptive Detection

Considering the fact that in the two sequential algorithms mentioned, we cannot identify any attackers until we isolate each of them to a virtual server with negative outcome, which may bring up the detection latency. Therefore, we propose a hybrid of sequential and non adaptive method in this section. In this scenario, the requests from the same client will be received and responded by different servers in a round-robin manner. Different from SDP and SDoP, a d-disjunct matrix is used as the testing matrix in this scheme and attackers can be identified without the need of isolating them into servers

5. CONCLUSIONS

We proposed a novel technique for detecting application DoS 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 paper is to apply group testing principles to application DoS attacks, and provide an underlying framework for the detection against a general case of network assaults, where malicious requests are indistinguishable from normal ones

Asian Journal of Engineering and Applied Technology (AJEAT)
Vol1.No.1 2013 pp 35-38.
available at: www.goniv.com
Paper Received :11-06-2013.
Paper Accepted:28-06-2013
Paper Reviewed by: 1. John Arhter 2. Dr.K.Ramkumar
Editor : Prof. P.Muthukumar

.

5.3 FUTURE ENHANCEMENT

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:

1. The sequential algorithm can be adjusted to avoid the requirement of isolating attackers;
2. 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 paper;
3. The overhead of maintaining the state transfer among virtual servers can be further decreased by more sophisticated techniques;
4. Even that we already have quite low false positive/ negative rate from the algorithms, we can still improve it via false-tolerant group testing methods, as discussed next.

REFERENCES

[1] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, "DDos-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection," Proc. IEEE INFOCOM, Apr. 2006.

[2] S. Vries, "A Corsaire White Paper: Application Denial of Service (DoS) Attacks," application-level-dos-attacks.pdf, 2010.

[3] S. Kandula, D. Katabi, M. Jacob, and A.W. Berger, "Botz-4-Sale:Surviving Organized DDoS Attacks That Mimic Flash Crowds,"Proc. Second Symp. Networked Systems Design and Implementation (NSDI), May 2005.

[4] S. Khattab, S. Gobriel, R. Melhem, and D. Mosse, "Live Baiting for Service-Level DoS Attackers," Proc. IEEE INFOCOM, 2008.[5] M.T. Thai, Y. Xuan, I. Shin, and T. Znati, "On Detection of Malicious Users Using Group Testing Techniques," Proc. Int'l Conf. Distributed Computing Systems (ICDCS), 2008.

[6] M.T. Thai, P. Deng, W. Wu, and T. Znati, "Approximation Algorithms of Nonunique Probes Selection for Biological Target Identification," Proc. Conf. Data Mining, Systems Analysis and Optimization in Biomedicine, 2007.

[7] J. Mirkovic, J. Martin, and P. Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," Technical Report 020018, Computer Science Dept., UCLA, 2002.

[8] M.J. Atallah, M.T. Goodrich, and R. Tamassia, "Indexing Information for Data Forensics," Proc. Int'l Conf. Applied Cryptography and Network Security (ACNS), pp. 206-221, 2005.

[9] J. Lemon, "Resisting SYN Flood DoS Attacks with a SYN Cache,"Proc. BSDCON, 2002.

[10] Service Provider Infrastructure Security, "Detecting, Tracing,and Mitigating Network-Wide 2005.

[11] Y. Kim, W.C. Lau, M.C. Chuah, and H.J. Chao, "Packetscore:Statisticsbased Overload Control against Distributed Denial-of-Service Attacks," Proc. IEEE INFOCOM, 2004.

[12] F. Kargl, J. Maier, and M. Weber, "Protecting Web Servers from Distributed Denial of Service Attacks," Proc. 10th Int'l Conf. World Wide Web (WWW '01), pp. 514-524, 2001.

[13] L. Ricciulli, P. Lincoln, and P. Kakkar, "TCP SYN Flooding Defense," Proc. Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS), 1999.

[14] D.Z. Du and F.K. Hwang, Pooling Designs: Group Testing in Molecular Biology. World Scientific, 2006.

[15] M.T. Thai, D. MacCallum, P. Deng, and W. Wu, "Decoding Algorithms in Pooling Designs with Inhibitors and Fault Tolerance," Int'l J. Bioinformatics Research and Applications, vol. 3,no. 2, pp. 145-152, 2007.