ISSN: 2348-2079

Volume-11 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Detection and Prevention of DDOS Attacks Using Tri-Layer Modern Cracking Algoritham

Y.Sathish Kanna[*1], Dr.S.Pathur Nisha M.E.,Ph.D[2]

[1]*Scholar, Nehru Institute of Technology, Coimbatore 641105, Tamilnadu, India.*
[2]*Professor and Head, Nehru Institute of Technology, Coimbatore 641105, Tamilnadu, India.*

Corresponding Author: Y.Sathish Kanna
Published on: 30.03.2023

ABSTRACT

Distributed 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.
As stated in, 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 of two cases: 1) at a high inter arrival rate and 2) consuming more service resources.
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 Therefore; we apply GT theory to this network security issue and propose Modern Cracking 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.

Keywords: Algoritham

INTRODUCTION

Distributed Denial of Service (DDoS) attacks using computationally intensive HTTP requests have emerged as a serious threat to web applications in recent years. These attacks are called asymmetric Application Layer DDoS(AL-DDoS) attacks and are capable of exhausting server resources using considerably fewer attack requests than other application layer DDoS attacks.
In addition to their potency, Asymmetric DDoS attacks possess certain features which make them extremely difficult to detect. First, they are executed using legitimate HTTP requests, which makes it impossible to detect these attacks by inspecting individual requests. Second, they exhibit a very low attack bandwidth and thus, cannot be detected by existing volumetric DDoS detection mechanisms. Third, they resemble legitimate user traffic such as flash crowds, which are sudden spikes in legitimate user traffic to a web server due to a noteworthy event or sale.
Our contributions in this work are as follows:

- We propose the use of an annotated Probabilistic Timed Automata (PTA) to capture the behavioral dynamics of legitimate users accessing a web application.
- We propose a mechanism to detect asymmetric AL-DDoS attacks by using cumulative suspicion score assignment based on the annotated PTA.
- We demonstrate that the proposed detection mechanism performs considerably well in detecting asymmetrical-DDoS attacks, and can be used effectively at real time.

EXISTING SYSTEM

The demonstrate how lack of strong location authentication allows creation of software-based Sybil devices that expose crowd sourced map systems to a variety of security and privacy attacks. This experiments show that a single Sybil device with limited resources can cause havoc on Waze, reporting false congestion and accidents and automatically rerouting user traffic. More importantly, the describe techniques to generate Sybil devices at scale, creating armies of virtual vehicles capable of remotely tracking precise movements for large user populations while avoiding detection.

DIS ADVANTAGES

- ✓ Less security and privacy
- ✓ Highly impact of the attacks

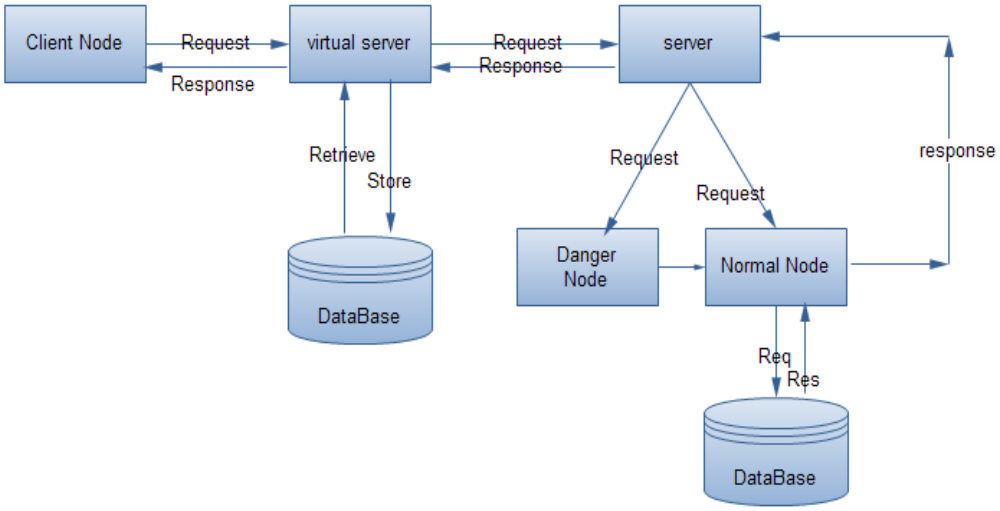
PROPOSED SYSTEM

The propose a new approach based on co-location edges, authenticated records that attest to the one-time physical co location of a pair of devices. Over time, co-location edges combine to form large proximity graphs that attest to physical interactions between devices, allowing scalable detection of virtual vehicles. The demonstrate the efficacy of this approach using large-scale simulations, and how they can be used to dramatically reduce the impact of the attacks. They have informed Waze/Google team of our research findings. Currently, they are in active collaboration with Waze team to improve the security and privacy of their system.

ADVANTAGES

- ✓ Improve security and privacy
- ✓ Reduce impact of the attacks
- ✓ Large proximity graphs
- ✓ This approach using large-scale simulations

SYSTEM ARCHITECTURE



SYSTEM DEVELOPMENT MODULES

- Login Process Denial of Services.
- Group attacker modules.
- Group testing modules.
- Victim/Detection modules

MODULE DESCRIPTION

LOGIN PROCESS DENIAL OF SERVICES

It may be possible to overwhelm the login process by continually sending login-requests that require the presentation tier to access the authentication mechanism, rendering it unavailable or unreasonably slow to respond.

When a user enters an incorrect username and/or password, the application should respond with a generic error message stating that the information entered was incorrect. If the application explicitly states which component of the username/password pair was incorrect then an attacker can automate the process of trying common usernames from a dictionary file in an attempt to enumerate the users of the application. Whilst applications may handle authentication failure messages correctly, many still allow attackers to enumerate users through the forgotten password feature.

GROUP ATTACKER MODULES

The maximum destruction caused by the attacks includes the depletion of the application service resource at the server side, the unavailability of service access to legitimate user, and possible fatal system errors which require rebooting the server for recovery. We assume that any malicious behaviors can be discovered by monitoring the service resource usage, based on dynamic value thresholds over the monitored objects. Data manipulation and system intrusion are out of this scope. That application interface presented by the servers can be readily discovered and clients communicate with the servers using HTTP/1.1 sessions on TCP connections.

We consider a case that each client provides a non spoofed ID, which is utilized to identify the client during our detection period. Despite that the application DDoS attack is difficult to be traced; by identifying the IDs of attackers the firewall can block the subsequent malicious requests. The attackers are assumed to launch application service requests either at high inter arrival rate or high workload, or even both. The term “request” refers to either main request or embedded request for HTTP page. Since the detection scheme proposed

will be orthogonal to the session affinity, we do not consider the repeated one-shot attack mentioned in. We further assume that the number of attackers d << n where n is the total client amount. This arises from the characteristics of this attack. Due to the benefits of virtual server s we employee, this constraint can be relaxed, but we keep it for the theoretical analysis in the current work.

GROUP TESTING MODULES

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.

A detection model based on GT can be assume that there are t virtual servers and n clients, among which d clients are Binary testing matrix M and testing outcome vector V. Attackers. Consider the matrix M t*n in Fig. 1, the clients can be mapped into the columns and virtual servers into rows in M, where M[I, j]= 1 if and only if the requests from client j are distributed to virtual server i. With regard to the test outcome column V, we have V[i]= 1 if and only if virtual server i has received malicious requests from at least one attacker, but we cannot identify the attackers at once unless this virtual server is handling only one client. Otherwise, if V ½i_ ¼ 0, all the clients assigned to server I are legitimate. The d attackers can then be captured by decoding the test outcome vector V and the matrix M.

VICTIM/DETECTION MODULES

The victim model in our general framework consists of multiple back-end servers, which can be Web/application servers, database servers, and distributed file systems. We do not take classic multitier Web servers as the model, since our detection scheme is deployed directly on the victim tier and identifies the attacks targeting at the same victim tier; thus, multitier attacks should be separated into several classes to utilize this detection scheme. We assume that all the back-end servers provide multiple types of application services to clients using HTTP/1.1 protocol on TCP connections.

Each back-end server is assumed to have the same amount of resource. Moreover, the application services to clients are provided by K virtual private servers (K is an input parameter), which are embedded in the physical back-end server machine and operating in parallel. Each virtual server is assigned with equal amount of static service resources, e.g., CPU, storage, memory, and network bandwidth. The operation of any virtual server will not affect the other virtual servers in the same physical machine. There a sons for utilizing virtual servers are twofold: first, each virtual server can reboot independently, thus is feasible for recovery from possible fatal destruction; second, the state transfer overhead for moving clients among different virtual servers is much smaller than the transfer among physical server machines.

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:

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 Project.
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. This error-tolerant matrix has great potentials to improve the performance of the PND algorithm and handle application DDOS attacks more efficiently.

FUTURE ENHANCEMENT

We will continue to investigate the potentials of this scheme and improve this proposed system to enhance the detection efficiency.

- 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, we can still improve it via false-tolerant group testing methods.

REFERENCES

1. Francois J, Aib I, Boutaba R. Firecol: a Collaborative Protection Network for the Detection of Flooding ddos Attacks. IEEE ACM Trans Netw. 2012;20(6, Dec):1828-41. Available from: https://hal.science/hal-00959439/document

2. Zargar ST, Joshi J, Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun Surv Tutor. Nov 2013;15(4):2046-69. Available from: https://ieeexplore.ieee.org/abstract/document/6489876/
3. Yaar A, Perrig A, Song D. StackPi: new packet marking and filtering mechanisms for DDoS and IP spoofing defense. IEEE J Sel Areas Commun. Oct 2006;24(10):1853-63. Available from: https://ieeexplore.ieee.org/abstract/document/1705617/
4. Wang H, Jin C, Shin KG. Defense against spoofed IP traffic using hop-count filtering. IEEE ACM Trans Netw. Feb 2007;15(1):40-53. Available from: https://ieeexplore.ieee.org/abstract/document/4100726/
5. Duan Z, Yuan X, Chandrashekar J. Controlling IP spoofing through interdomain packet filters. IEEE Trans Depend Sec Comput. Feb 2008;5(1):22-36. https://ieeexplore.ieee.org/abstract/document/4358709/
6. Sung M, Xu J. IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks IEEE, translator On Parall. and Distr. Sys. Sep 2003;14(9):861-72. https://ieeexplore.ieee.org/abstract/document/1233709/
7. Sung M, Xu J, Li J, Li L. Large-scale IP traceback in high-speed Internet: practical techniques and information-theoretic foundation. IEEE ACM Trans Netw. Dec 2008;16(6):1253-66. https://ieeexplore.ieee.org/abstract/document/1301319/
8. Xiang Y, Li K, Zhou W. Low-rate DDoS attacks detection and traceback by using new information metrics IEEE, translator on Inf. Foren. and Sec. Vol. 6(2); May 2011. p. 426-37. https://ieeexplore.ieee.org/abstract/document/5696753/
9. Ballani H, Chawathe Y, Ratnasamy S, Roscoe T, Shenker S. In: Proceedings of the HotNets-IV, Nov 2005, College Park, MD, USA.
10. 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, May 2004, Oakland, CA, USA. https://ieeexplore.ieee.org/abstract/document/1301320/
11. Luo H, Chen Z, Cui J, Zhang H, Zukerman M, Qiao C, "CoLo. R: An information-centric internet architecture for innovations. IEEE Netw. May 2014;28(3):4-10. https://ieeexplore.ieee.org/abstract/document/6843226/