Enhanced Attack Resistance Scheme for App-Ddos Attacks using Bayes Optimal Filter Strategy

A.Vince Paual
Research Scholor,Singhania University,Rajasthan,India.

Anuranj P
Asst. Professor, Dept. of CSE, FISAT, Angamaly.

K. Prasadh
Principal, Valiakoonambaikulathamma College of Engineeering, Kerala

ABSTRACT

Countering distributed denial of service (DDoS) attacks is becoming ever more challenging with the vast resources and techniques increasingly available to attackers. Derived from the low layers, new application-layer-based DDoS attacks utilizing legitimate HTTP requests to overwhelm victim resources are more undetectable. The case may be more serious when such attacks mimic or occur during the flash crowd event of a popular Website. The problem concerned in this project is sophisticated attacks that are protocol compliant, non-intrusive, and utilize legitimate application-layer requests to overwhelm system resources. It characterizes application-layer resource attacks as either request flooding, asymmetric, or repeated one-shot, on the basis of the application workload parameters that they exploit.

The traffic characteristics of low layers are not enough to distinguish the App-DDoS attacks from the normal flash crowd event. In this paper, the proposal work presents Gaussian distribution factor to enhance the attack resistance scheme for having better detection rate even for stationary object in the application DDoS attacks. The attack detection is identified with the Gaussian distribution of the traffic data of flash crowds surrounding the respective web sites. In this paper, the proposed mechanisms used to thwart the application DDoS attacks using bayes optimal filter strategy. The simulation using Network Simulator results proves that the attack resistance rate and delay is minimized and hence the proposed scheme outperforms the existing scheme.

Keywords

Application DDoS attacks, Bayes optimal filter strategy, Gaussian distribution.

1. INTRODUCTION

Distributed Denial of Service (DDoS) attack has caused serious damage to the server with more resources in the hands of the attackers and makes bullying even more for the development of new Internet services. Traditionally, DDoS attacks are carried out in the network layer, such as ICMP flood, SYN flood, UDP floods, which are called networks of DDoS attacks in this paper. The purpose of these attacks is to consume the bandwidth of the network and deny service to legitimate users of the victim's system. since many studies have observed this type of attack and have proposed various schemes to protect the network and equipment of the attacks of bandwidth is not as easy as in the past by hackers to launch DDoS attacks based on network level.

During the past several years, flash crowd is one of the important mechanisms of network traffic that has been observed by researchers., Flash crowd means the situation when a large amount of users simultaneously access a popular Website on the Web, which generates a surge in traffic to the website and might cause the site to be virtually unreachable. Because traffic explosion and large volume are the common characteristics of App-DDoS attacks and flash crowds. This is not easy for current techniques to distinguish them initially by statistical characteristics of traffic.

Therefore, the App-DDoS attacks stealthy and can be more dangerous for popular websites that the general Net-DDoS attacks when they imitate (or hide) the normal flash crowd. Some of the previous papers focus on the detection of App-DDoS attacks to the flash crowd event. In this paper proposal work presents a plan to catch the spatial and temporal trends of normal event flash crowds and to develop the detection of App-DDoS attacks. Since the lower layer traffic characteristics are not sufficient to distinguish the App-DDoS attacks in the normal flash crowd event, the purpose of this work is to identify a way to determine whether the increased traffic caused by attackers App DDoS, or by normal web users.

2. LITERATURE WORK

Our review of the literature indicated that researchers are trying to detect DDoS attacks from three different layers: the IP layer, the TCP layer and application layer [1], [2], [3]. To differ from all these points of view, researchers are exploring different approaches to the normal traffic from one of these attacks. Here we review the research community, from every perspective [4], [5]. Most DDoS attacks at the IP level research focused. These mechanisms try to detect attacks by analyzing the specific properties, such as the arrival rate, or header information. For example, [6], [8] use the Management Information Base (MIB) data, the parameters that show the different packages and routing statistics from the router to reach the initial count.

In [7] used cross-correlation analysis in order to capture the market trends and decide where and when a DDoS attack possibly arises. A DDoS attack can be a simultaneous attack on the network of the victim (eg a web server or router) from a large number [9] of compromised hosts that can spread between different networks are characterized independently [11], [13]. Simply exploiting the huge asymmetry between the entire network of resources and capabilities of a victim, a DDoS flooding attack on congestion can quickly target of attack [8].

In [14], asymmetry of the packets in two ways is used to find attacks [10], [12] in border routers. A flash crowd is a large increase in traffic on a particular site that the site virtually inaccessible as causes. The proposal in this paper presents a model of flash crowd events suddenly and assesses the performance of different techniques of multi-level cache instead of to handle these events. Our results indicate that a significant reduction in reaction time of the client and server and network loads can be carried out from the crowd during the flash using the techniques of database cache, and save even more can be achieved with appropriate replacement algorithms the choice and placement of proxies.

Then a method is to provide proactive detection of DDoS attacks by classifying the state of the network for use in the detection phase of the general anti- DDoS frame. More specifically, to describe the two phases of DDoS architecture, control phase and the attack phase. Then the procedures of DDoS attacks to examine the variables that the major role in the detection of DDoS attacks are, how they should be changed in an unusual way, if the attack is chosen. Finally the Bayesian classifier method is to apply to the State network packet for every stage of DDoS attack to be classified.

3. ENHANCED ATTACK RESISTANCE SCHEME FOR APP-DDOS ATTACKS

A distributed denial of service attack (DDoS) occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods. Malware can carry DDoS attack mechanisms; one of the better-known examples of this was My Doom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hard coding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent (or the Trojan may contain one). Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web. Stacheldraht is a classic example of a DDoS tool. It utilizes a layered structure where the attacker uses a client program to connect to handlers, which are compromised systems that issue commands to the zombie agents, which in turn facilitate the DDoS attack. Agents are compromised via the handlers by the attacker, using automated routines to exploit vulnerabilities in programs that accept remote connections running on the targeted remote hosts. Each handler can control up to a thousand agents. These collections of systems compromisers are known as botnets. DDoS tools like stacheldraht still use classic DoS attack methods centered on IP spoofing and amplification like smurf attacks and fraggle attacks (these are also known as bandwidth consumption attacks). SYN floods (also known as resource starvation attacks) may also be used. Newer tools can use DNS servers for DoS purposes. Simple attacks such as SYN floods may appear with a wide range of source IP addresses, giving the appearance of a well distributed DDoS. These flood attacks do not require completion of the TCP three way handshakes and attempt to exhaust the destination SYN queue or the server bandwidth. Because the source IP addresses can be trivially spoofed, an attack could come from a limited set of sources, or may even originate from a single host. Stack enhancements such as syn cookies may be effective mitigation against SYN queue flooding, however complete bandwidth exhaustion may require involvement

Bayes optimal packet classifier

Bayes classifier a probabilistic classifier based on applying Bayes' theorem with strong independence assumptions. Independent feature model for the anonym packets. Bayes classifier assumes that the presence (or absence) of a anonym packet feature of a class is unrelated to the presence (or absence) of any other packet feature. Depending on the precise nature of the probability model, Bayes optimal classifiers can be trained very efficiently in a supervised learning setting. In our case, parameter estimation for Bayes models uses the method of maximum likelihood

The attacks can be easily discovered from the normal flash crowd workload by the entropy. The fact that the entropy series is stable shows that the document popularity is stable. Although the attackers can inject vicious requests into the flash crowd traffic, the original popularity distribution of documents is changed, which causes the entropy series lower than the normal level. Therefore detect the potential App-DDoS attacks by the entropy of document popularity fitting to the proposed model.

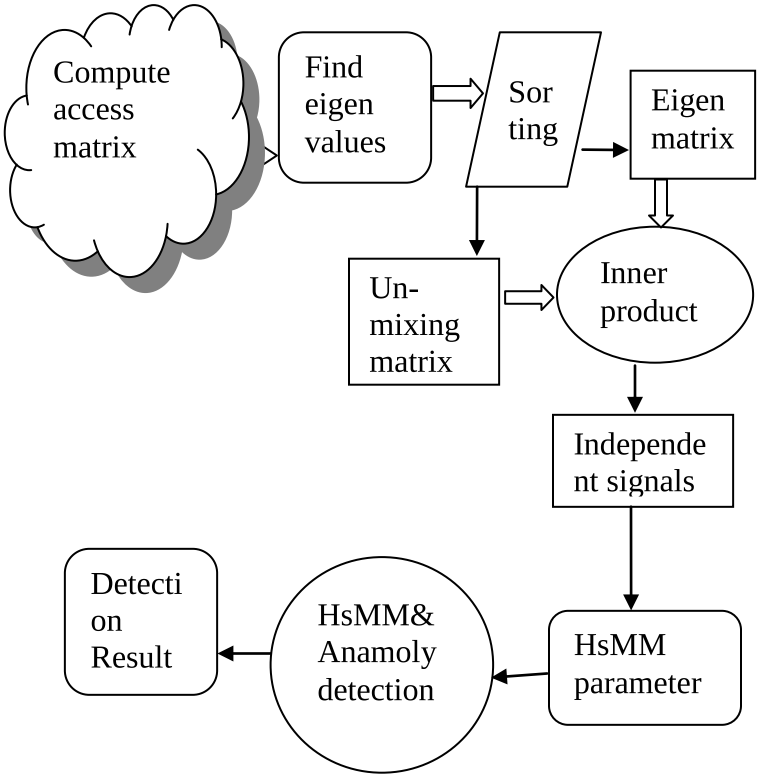

Figure1: App DoS Attack detection Using HsMM

Before the Gaussian scheme is applied to detection, some parameters have to be preset, which includes the time unit of observed data, the length of the observed vector sequence, the number of the remaining principal components, and the detection threshold of entropy for anomaly detection in HsMM. discuss each of them as follows. The time unit and the length of the observed vector sequence can be set according to the computation ability and memory of the detection system. In this paper, set the time unit to be 5 s and the length of one observed sequence to be 1 min. Although the small scale of the time unit may bring us high precision, the length of sequence can not be set too short because it may not contain sufficient attack signals for reliable detection.

4. EXPERIMENTATION OF GAUSSIAN DISTRIBUTION FACTOR FOR RESISTING APPLICATION DDOS ATTACKS

The experimental evaluation was carried to implement the proposed algorithm in the NS2 simulator. The network topology is generated by NS2. In our simulation initially 30 clients were taken. Each nodes replay one user’s trace collected from synthetic data sources. The ratio of randomly selected attack nodes to whole nodes is 10%. In addition, assume the attackers can intercept some of the request segment of normal surfers and replay this segment or hot pages to launch the App-DDoS attacks to the victim Web server. When the attack begins, every potential attack node replays a snippet of another historical flash crowd trace.

The interval between two consecutive attack requests is decided depends on three patterns including constant rate attacks, increasing rate attacks and random pulsing attacks. The size of requested document is used to estimate the victim node’s processing time (delay) of each request, i.e., if the requested document is larger, the corresponding processing time will be longer. By this way, simulate the victim’s resource (e.g., CPU) cost by client’s requests.

During the simulation, 30 nodes were participated in the process. There were six nodes named as server nodes and remaining nodes were named as client nodes. Each server has four client nodes. Attacker nodes were found when Server checked client randomly one by one. From this experimentation, we calculated Attack resistance rate and delay rate in terms of number of nodes and mobility.

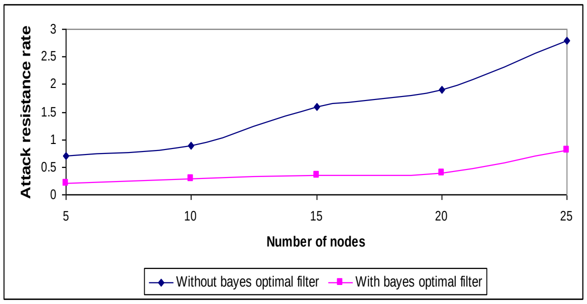

Figure 2: Number of nodes vs. attack resistance rate

As shown in figure 2, Attack resistance rate was measured in terms of number of nodes. As the number of nodes increased, Attack resistance rate also gets increased. Comparison of without Bayes optimal filter and with Bayes optimal filter were shown. Using Bayes optimal filter was showing Better attack resistance rate.

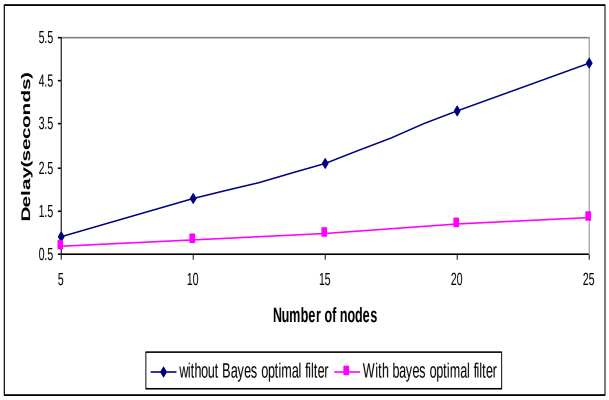

Figure 3: Number of nodes vs. Delay

Figure 3 depicts the Number of nodes Vs Delay rate. The delay rate was noted in every five nodes were processed. The delay rate was linear in our proposed strategy. By using Bayes optimal filter the delay rate controlled. As number of nodes increased delay also increased.

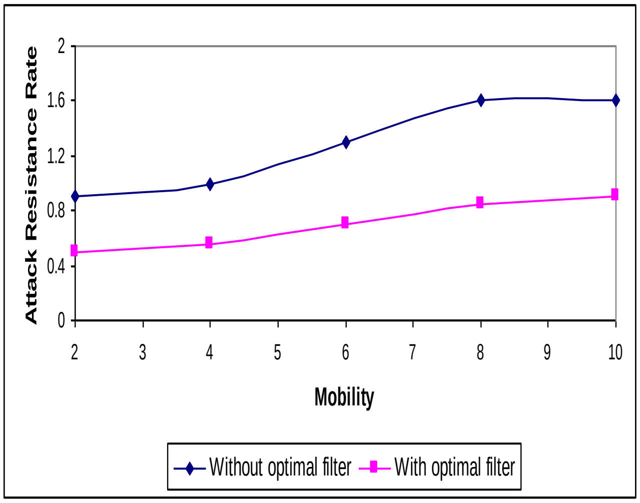

Figure 4: Mobility vs. attack resistance rate

As shown in figure 4, Attack resistance rate was measured in terms of Mobility. As mobility increased, Attack resistance rate also gets increased. Attack resistance rate was reduced by using the Bayes optimal filter strategy. Our proposed scheme showed better performance.

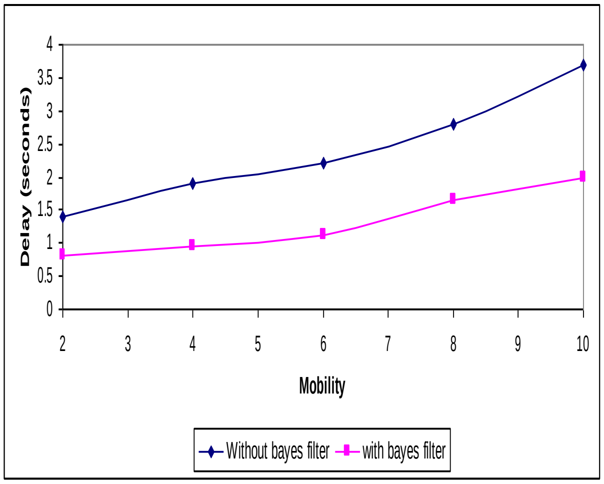

Figure 5: Mobility vs. Delay

The delay rate is calculated in terms of seconds. As mobility increases delay rate also increases. Mobility is measured in terms of meter per second. Our scheme is having better efficiency.

5. CONCLUSION

Creating defenses for attacks requires monitoring dynamic network activities in order to obtain timely and signification information. In traffic detection to control the web architecture, Gaussian distribution factor introduced, in order to reveal the dynamic changes in the explosion of normal traffic. It shows the start of App-DDoS attacks during the flash crowd event. Bayesian factor reveals the early attacks only in the popularity of the documents obtained in the server log.

The simulation experiment with different modes of attack-App (DDoS attacks that constantly increasing rate of attacks and raids stochastic pulse) flash crowd event gathered in a demonstration carried out from data network traffic traces to an ISP. Our results show that the simulation system is the movement of the web traffic through flash crowd attacks and the entropy of the observed data fit the distribution of the Bayes factor as a measure of the disturbance is caused capture. The simulation results proved that the attack resistance rate and delay is minimized.

6. REFERENCES

[1] Yi Xie and Shun-Zheng Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites" IEEE/ACM Transactions on networking, vol. 17, no. 1, February 2009 .

[2] S. Kandula, D. Katabi, M. Jacob, and A. W. Berger, "Botz-4-Sale: Surviving Organized DDoS Attacks that Mimic Flash Crowds,"MIT, Tech. Rep. TR-969, 2004.

[3] I. Ari, B. Hong, E. L. Miller, S. A. Brandt, and D. D. E. Long, "Modeling, Analysis and Simulation of Flash Crowds on the Internet,"Storage Systems Research Center Jack Baskin School of Engineering University of California, Santa Cruz Santa Cruz, CA, ech. Rep. UCSC-CRL-03-15, Feb.28, 2004 http://ssrc.cse.ucsc.edu/, 95064.

[4] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites," in Proc. 11th IEEE Int. World Wide Web Conf., May 2002,pp. 252–262.

[5] Y. Xie and S. Yu, "A detection approach of user behaviors based on HsMM," in Proc. 19th Int. Teletraffic Congress (ITC19), Beijing, China, Aug. 29–Sep. 2 2005, pp. 451–460

[6] Y. Xie and S. Yu, "A novel model for detecting application layer DDoS attacks," in Proc. 1st IEEE Int. Multi-Symp. Comput. Computat. Sci. (IMSCCS|06), Hangzhou, China, Jun. 20–24, 2006, vol. 2, pp. 56–63.

[7] T. Peng and K. R. M. C. Leckie, "Protection from distributed denial of service attacks using history-based IP filtering," in Proc. IEEE Int. Conf. Commun., May 2003, vol. 1, pp. 482–486

[8] S.-Z. Yu and H. Kobayashi, "An efficient forward-backward algorithm for an explicit duration hidden Markov model," IEEE Signal Process. Lett., vol. 10, no. 1, pp. 11–14, Jan. 2003.

[9] L. I. Smith, A Tutorial on Principal Components Analysis [EB/OL], 2003 [Online]. Available: http://www.snl.salk.edu/~shlens/pub/ notes/ pca.pdf

[10] A. Hyvärinen, “Survey on independent component analysis,” Neural Comput. Surveys, vol. 2, pp. 94–128, 1999

[11] A. Hyvärinen, “Fast and robust fixed-point algorithms for independent component analysis,” IEEE Trans. Neural Netw., vol. 10, no. 3, pp. 626–634, Jun. 1999 .

[12] J. B. D. Cabrera, L. Lewis, X. Qin, W. Lee, R. K. Prasanth, B. Ravichandran, and R. K. Mehra, “Proactive detection of distributed denial of service attacks using MIB traffic variables a feasibility study,” in Proc. IEEE/IFIP Int. Symp. Integr. Netw. Manag., May 2001, pp. 609–622.

[13] J. Yuan and K. Mills, “Monitoring the macroscopic effect of DDoS flooding attacks,” IEEE Trans. Dependable and Secure Computing, vol. 2, no. 4, pp. 324–335, Oct.-Dec. 2005.

[14] J. Mirkovic, G. Prier, and P. Reiher, “Attacking DDoS at the source,” in Proc. Int. Conf. Network Protocols, 2002, pp. 312–321.