INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

IDENTIFICATION & AVOIDANCE OF DDOS ATTACK FOR SECURED DATA COMMUNICATION IN CLOUD

S. Sivakalai[1], Jayapriya Jayapal[2]

[1]Mailam Engineering College, Mailam, Tamil Nadu, India, E-mail address
[2]Mailam Engineering College, Mailam, Tamil Nadu, India
Author Correspondence: Address, Telephone/Fax Numbers, Email address

Abstract

Interconnected systems, such as Web servers, database servers, cloud computing servers etc, are now under threads from network attackers. As one of most common and aggressive means, Denial-of-Service (DoS) attacks cause serious impact on these computing systems. In this paper, we present a DoS attack detection system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Our MCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition. This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA. The effectiveness of our proposed detection system is evaluated using KDD Cup 99 dataset, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined. The results show that our system outperforms two other previously developed state-of-the-art approaches in terms of detection accuracy.

Keywords*:* Denial-of-Services (Dos), Multivariate Correlation Analysis (MCA), Intrusion Prevention System.

1. Introduction

IN this paper, we attempt to answer one important question: can we beat DDoS attacks in a cloud environment? The answer is positive. One essential issue of DDoS attack and defence is resource competition; if a defender has sufficient resources to counter a DDoS attack, then the attack will be unsuccessful, and vice versa. Unfortunately, the counterparts of clouds, e.g., the client server and the peer-to-peer computing platforms, do not have sufficient resources to beat DDoS attacks. However, a cloud infrastructure provider pools a large amount of resources and makes them easy access in order to handle a rapid increase in service demands [1]. Therefore, it is almost impossible for aDDoS attack to shut down a cloud. However, individual cloud customers (referred to as parties hosting their services in a cloud) cannot escape from DDoS attacks nowadays as they usually do not have the advantage. The good news is that it is highly likely for individual

cloud customers to win the battle by taking advantage of the unique features of clouds. In this paper, we explore how to overcome DDoS attacks against individual cloud customers from the resource competition perspective. Currently, cloud computing has become one of the fastest growing sectors in the IT industry all over the world.

Cloud computing features a cost-efficient, ''pay-as-you-go'' business model and flexible architectures, such as SaaS, PaaS and SaaS. A cloud platform can dynamically clone virtual machines in a very quick fashion, e.g., duplicating a gigabyte level server within one minute [2]. Despite the promising business model and hype surrounding cloud computing, security is the major concern for businesses shifting their applications to clouds [3], [4]. Distributed Denial of Service (DDoS) is a major threat to Internet based killer applications for non-cloud computing environments, such as independent news web sites, e-business and online games [5]. DDoS attacks are now carried out by botnets. Resent researches [6] have corrected a long held belief that hackers can easily compromise as many computers as they want. Due to the anti-virus and anti-malware effort and software, the number of active bots a bot master can manipulate is constrained to the hundreds or few thousands level, even though the number of bot footprints may be much larger. In the early work about DDoS defence, Yau et al. [7] treated DDoS attacks as a resource management problem. Recent researches [8], [9], [10] have further demonstrated that the essential issue of DDoS attack and defence is a competition for resources: the winner is the side who possesses more resources in the battle. Different from other computing platforms, a cloud environment usually has profound resources, full control, and dynamic allocation capability of resources. As a result, it is not possible to deny the service of a cloud with the scale of current botnets. However, an individual cloud customer does not have this advantage of surviving a brute force DDoS attack. Cloud service providers (CPS) usually offer cloud customers two resource provisioning plans: short-term on demand and long-term reservation. Major cloud providers, such as Amazon EC2 and GoGrid, provide both plans to their customers [11]. If a customer chooses the first plan, then she will be charged based on what she uses. This resource business model is vulnerable to an Economic Denial of Sustainability (EDoS) attack [12], [13]. Moreover, this kind of attack also disturbs the service of clouds who allocate resources based on spot instance [14], [15]. On the other hand, if a cloud customer takes the reservation plan, she usually makes the source reservation for the maximum usage of her business. In other words, the reserved resource for her application is limited. As a result, a threat of DDoS attack remains. As a new business model and computing platform, cloud related research has attracted a lot of attention. There has been plenty of research done on cloud, such as economical modelling [16] and resource optimization [17]. However, research on DDoS attack and defence in a cloud environment is still at an early stage. The available cloud security covers various aspects, such as attack mitigation strategies against DDoS attacks [18] or EDoS attacks [13] in a cloud environment, DDoS defence as a cloud service [19], and security architecture against DDoS attacks in cloud computing [20]. In this paper, we propose a practical dynamic resource allocation mechanism to confront DDoS attacks that target individual cloud customers. In general, there is one or several access points between a cloud data center and the Internet. Similar to firewalls, we place our Intrusion Prevention System (IPS) at these locations to monitor incoming packets. When a cloud hosted server is under a DDoS attack, the proposed mechanism will automatically and dynamically allocate extra resources from the available cloud resource pool, and new virtual machines will be cloned based on the image file of the original IPS using the existing clone technology [21], [22]. All IPSs will work together to filter attack packets out, and guarantee the quality of service (QoS) for benign users at the same time. When the volume of DDoS attack packets decreases, our mitigation system will automatically reduce the number of its IPSs, and release the extra resources back to the available cloud resource pool. As aforementioned, the essential issue to defeat a DDoS attack is to allocate sufficient resources to mitigate attacks no matter how efficient our detection and filtering algorithms are. In order to estimate our resource demands and QoS for benign users in a DDoS battle, we employ queueing theory to undertake performance evaluation due to its extensive deployment in could performance analysis, such as in [23], [24], [25]. It should be noted that our goal for this paper is to explore the possibility of defeating DDoS attacks in a cloud environment from a technical and resource competition point of view. We therefore do not involve specific DDoS detection methods, and do not involve too many business issues which may be caused by our mitigation proposal. With the proposed system in place, we believe most DDoS attacks

can be defeated, if not all attacks. This will make cloud customers more confident in shifting their businesses to cloud platforms. The contributions of this paper are summarized as follows: . We point out that DDoS attacks do threaten individual cloud customers. However, by taking advantage of the cloud platform, we can overcome DDoS attacks, which is difficult to achieve for non-cloud platforms. To the best of our knowledge, this paper is an early feasible work on defeating DDoS attacks in a cloud environment.

We propose a dynamic resource allocation mechanism to automatically coordinate the available resources of a cloud to mitigate DDoS attacks on individual cloud customers. The proposed method benefits from the dynamic resource allocation feature of cloud platforms, and is easy to implement. . We establish a queueing theory based model to estimate the resource allocation against various attack strengths. Real-world data set based analysis and experiments help us to conclude that it is possible to defeat DDoS attacks in a cloud environment with affordable costs.

2. Implementation of DDos

2.1 DDos

Denial of service (DoS) attacks has become a major threat to current computer networks. Early DoS attacks were technical games played among underground attackers. For example, an attacker might want to get control of an IRC channel via performing DoS attacks against the channel owner. Attackers could get recognition in the underground community via taking down popular web sites. Because easy-to-use DoS tools, such as Trinoo (Dittrich 1999), can be easily downloaded from the Internet, normal computer users can become DoS attackers as well. They sometime co-ordinately expressed their views via launching DoS attacks against organizations whose policies they disagreed with. DoS attacks also appeared in illegal actions. Companies might use DoS attacks to knock off their competitors in the market. Extortion via DoS attacks were on rise in the past years (Pappalardo *et al.* 2005). Attackers threatened online businesses with DoS attacks and requested payments for protection. Known DoS attacks in the Internet generally conquer the target by exhausting its resources, that can be anything related to network computing and service performance, such as link bandwidth, TCP connection buffers, application/service buffer, CPU cycles, etc. Individual attackers can also exploit vulnerability, break into target servers, and then bring down services. Because it is difficult for attackers to overload the target's resource from a single computer, many recent DoS attacks were launched via a large number of distributed attacking hosts in the Internet. These attacks are called distributed denial of service (DDoS) attacks. In a DDoS attack, because the aggregation of the attacking traffic can be tremendous compared to the victim's resource, the attack can force the victim to significantly downgrade its service performance or even stop delivering any service. Compared with conventional DoS attacks that could be addressed by better securing service systems or prohibiting unauthorized remote or local access, DDoS attacks are more complex and harder to prevent. Since many unwitting hosts are involved in DDoS attacks, it is challenging to distinguish the attacking hosts and take reaction against them. In recent years, DDoS attacks have increased in frequency, sophistication and severity due to the fact that computer vulnerabilities are increasing fast, which enable attackers to break into and install various attacking tools in many computers. Wireless networks also suffer from DoS attacks because mobile nodes (such as laptops, cell phones, etc.) share the same physical media for transmitting and receiving signals; and mobile computing resources (such as bandwidth, CPU and power) are usually more constrained than those available to wired nodes. In a wireless network, a single attacker can easily forge, modify or inject packets to disrupt connections between legitimate mobile nodes and cause DoS effects. In this article, we will provide an overview on existing DoS attacks and major defence.

In normalization module, basic features are generated from ingress network traffic to the internal network where protected servers reside in and are used to form traffic records for a well-defined time interval. Monitoring and analyzing at the destination network reduce the overhead of detecting malicious activities by concentrating only on relevant inbound traffic. This also enables our detector to provide protection which is the best fit for the targeted internal network because legitimate traffic profiles used by the detectors are developed for a smaller number of network services.

In this Multivariate Correlation Analysis, in which the "Triangle Area Map Generation" module is applied to extract the correlations between two distinct features within each traffic record coming from the first step or the traffic record normalized by the "Feature Normalization" module in this step. The occurrence of network intrusions cause changes to these correlations so that the changes can be used as indicators to identify the intrusive activities. All the extracted correlations, namely triangle areas stored in Triangle Area Maps (TAMs), are then used to replace the original basic features or the normalized features to represent the traffic records. This provides higher discriminative information to differentiate between legitimate and illegitimate traffic records.

In decision making module, the anomaly-based detection mechanism is adopted in Decision Making. It facilitates the detection of any DoS attacks without requiring any attack relevant knowledge. Furthermore, the labour-intensive attack analysis and the frequent update of the attack signature database in the case of misuse-based detection are avoided. Meanwhile, the mechanism enhances the robustness of the proposed detectors and makes them harder to be evaded because attackers need to generate attacks that match the normal traffic profiles built by a specific detection algorithm. This, however, is a labour-intensive task and requires expertise in the targeted detection algorithm. Specifically, two phases (i.e., the "Training Phase" and the "Test Phase") are involved in Decision Making. The "Normal Profile Generation" module is operated in the "Training Phase" to generate profiles for various types of legitimate traffic records, and the generated normal profiles are stored in a database. The "Tested Profile Generation" module is used in the "Test Phase" to build profiles for individual observed traffic records. Then, the tested profiles are handed over to the "Attack Detection" module, which compares the individual tested profiles with the respective stored normal profiles. A threshold-based classifier is employed in the "Attack Detection" module to distinguish DoS attacks from legitimate traffic.

During the evaluation, the 10 percent labelled data of KDD Cup 99 dataset is used, where three types of legitimate traffic (TCP, UDP and ICMP traffic) and six different types of DoS attacks (Teardrop, Smurf, Pod, Neptune, Land and Back attacks) are available. All of these records are first filtered and then are further grouped into seven clusters according to their labels. We show the evaluation results in graph.

3. Conclusions

This paper has presented a MCA-based DoS attack detection system which is powered by the triangle-area based MCA technique and the anomaly-based detection technique. The former technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and offers more accurate characterization for network traffic behaviours. The latter technique facilitates our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic. Evaluation has been conducted using KDD Cup 99 dataset to verify the effectiveness and performance of the proposed DoS attack detection system. The influence of original (non-normalized) and normalized data has been studied in the paper. The results have revealed that when working with non-normalized data, our detection system achieves maximum 95.20% detection accuracy although it does not work well in identifying Land, Neptune and Teardrop attack records. The problem, however, can be solved by utilizing statistical normalization technique to eliminate the bias from the data. The results of evaluating with the normalized data have shown a more encouraging detection accuracy of 99.95% and nearly 100.00% DRs for the various DoS attacks. Besides, the comparison result has proven that our detection system outperforms two state-of-the-art approaches in terms of detection accuracy. Moreover, the computational complexity and the time cost of the proposed detection system have been analyzed.

The proposed system achieves equal or better performance in comparison with the two state-of-the-art approaches. To be part of the future work, we will further test our DoS attack detection system using real world data and employ more sophisticated classification techniques to further alleviate the false positive rate.

REFERENCES

[1] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-time," *Computer Networks*, vol. 31, pp. 2435-2463, 1999

[2] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, "Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges," *Computers & Security*, vol. 28, pp. 18-28, 2009.
[3] D. E. Denning, "An Intrusion-detection Model," *IEEE Transactions on Software Engineering*, pp. 222-232, 1987.
[4] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using cluster analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.
[5] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, "Intrusion detection using fuzzy association rules," Applied Soft Computing, vol. 9, no. 2, pp. 462-469, 2009.
[6] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," Computer Communications, vol. 31, no. 17, pp. 4212-4219, 2008.
[7] W. Hu, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," Trans. Sys. Man Cyber. Part B, vol. 38, no. 2, pp. 577-583, 2008.
[8] C. Yu, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," Parallel and Distributed Systems, IEEE Transactions on, vol. 18, pp. 1649-1662, 2007.
[9] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011.
[10] S. T. Sarasamma, Q. A. Zhu, and J. Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 35, pp. 302-312, 2005.
[11] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, pp. 1073-1080, 2012.
[12] S. Jin, D. S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," *Pattern Recognition*, vol. 40, pp. 2185- 2197, 2007.
[13] C. F. Tsai and C. Y. Lin, "A Triangle Area Based Nearest Neighbors Approach to Intrusion Detection," *Pattern Recognition*, vol. 43, pp. 222-229, 2010.
[14] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R. P. Liu, "RePIDS: A multi tier Real-time Payload-based Intrusion Detection System," Computer Networks, vol. 57, pp. 811-824, 2013.
[15] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis," Neural Information Processing, 2011, pp. 756-765.
[16] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Triangle-Area-Based Multivariate Correlation Analysis for Effective Denialof- Service Attack Detection," The 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, United Kingdom, 2012, pp. 33-40.
[17] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Costbased modeling for fraud and intrusion detection: results from the JAM project," The DARPA Information Survivability Conference and Exposition 2000 (DISCEX '00), Vol.2, pp. 130-144, 2000.
[18] G. V. Moustakides, "Quickest detection of abrupt changes for a class of random processes," Information Theory, IEEE Transactions on, vol. 44, pp. 1965-1968, 1998.
[19] A. A. Cardenas, J. S. Baras, and V. Ramezani, "Distributed change detection for worms, DDoS and other network attacks," The American Control Conference, Vol.2, pp. 1008-1013, 2004.
[20] W. Wang, X. Zhang, S. Gombault, and S. J. Knapskog, "Attribute Normalization in Network Intrusion Detection," The 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), 2009, pp. 448-453.
[21] M. Tavallaee, E. Bagheri, L. Wei, and A. A. Ghorbani, "A Detailed Analysis of the KDD Cup 99 Data Set," The The Second IEEE International Conference on Computational Intelligence for Security and Defense Applications, 2009, pp. 1-6.
[22] D. E. Knuth, The art of computer programming vol I: Fundamental Algorithms Addison-Wesley, 1973.

Vol.2 Issue.11, Pg.: 155-160
November 2014

A Brief Author Biography

S. Sivakalai M.E. CSC – Her research interests lies in the areas of Big Data, Knowledge and Data Engineering in Data Mining, Cryptographic Security in Cloud Computing and Secure Computing.

Jayapriya Jayapal M.C.A., M.Phil., M.E., M.B.A. – Assistant Professor, Mailam Engineering College. Her research interests lies in the areas of Big Data, Knowledge and Data Engineering in Data Mining, Cryptographic Security in Cloud Computing and Secure Computing.