International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in; editorijoer@gmail.com

Vol.4., Issue.6., 2016
Nov-Dec.

RESEARCH ARTICLE

ISSN: 2321-7758

DRDoS ATTACK DETECTION MODEL USING CORRELATION MATRIX

VIKAS MORE[1], DEOKATE GAJANAN[2]

[1]Student, [2]Assistant Professor

Department of Computer Engineering, Savitribai Phule University of Pune, Maharastra, India

[1]vikas.chevron@gmail.com;[2]deokate.gd@gmail.com

ABSTRACT

Distributed Reflection Denial of Service is the recent iteration in the series of Denial of Service attacks. Since the increasing popularity of web-based applications has led to several critical services being provided over the Internet, it is important to prevent malicious attackers from launching such attacks that causes disruption of service. This paper first presents a brief discussion on some of the important types of DDoS attacks that currently exist and some existing mechanisms to combat these attacks. We use Correlation Matrix based Detection algorithm which helps to find whether the network is experiencing a channel failure or is under attack. The detection algorithm is based on a statistical analysis of network flow. Once the attack is detected, the attack path and source are multicast to all nodes, so that the nodes in the network can avoid any traffic from them, thus reducing the effect of DRDoS attack for a specified period of time. This type of model have good detection accuracy, evaluation carried out demonstrate effectiveness of the proposed defence mechanism against DDoS attacks.

INTRODUCTION

A DRDoS is modified version of DDoS attack that is more dangerous than earlier of its predecers. This type of attack uses normal hosts called “reflectors” to flood the victim. Ingenious variation on the traditional SYN attack to actually trick innocent servers is the main strong point in the success of these attacks and core infrastructure routers into unknowingly executing a DDoS attack.

There exists detection mechanisms for DDoS attack, but they are not applicable to DRDoS as attack traffic is further diluted by the reflectors and these type of attacks has the ability to amplify the attack traffic. The result of DRDoS attack results in no general access to the remote server or possibly crashing of server [3]. Packet content, protocol inspection may be helpful, but it needs lots of computational resources which is infeasible solution for most small business companies to setup such costly infrastructure [6, 7]. This issue given boost to research community to develop cost effective, protocol independent methods of detecting most kinds of DRDoS attacks. The evaluation of this type of system is carried out using KDD 99 dataset. This paper uses correlation matrix based method for DDoS detection and based on the evaluation result those are captured it is found that this model is able to detect nearly 84% of DDoS attacks with only 4% of false positive rate. The rest of the paper is organized as follows, section 2 provides an overview of existing countermeasures against DRDoS attacks, Section 3 gives a detailed definition of the attack detection steps and algorithms used in proposed system and finally conclusion is drawn in Section 4.

Literature Survey

A Network ingress filtering is a mechanism proposed to prevent attacks that use spoofed source addresses [13]. This involves configuring the routers to drop packets that have illegitimate

source IP addresses. One of the serious pitfalls of this method is its inability to curtail a flood attack that originates with a spoofed IP address from within the network. ICMP traceback messages are useful to identify the path taken by packets through the Internet [14]. This requires a router to use a very low probability with which traceback messages are sent along with the traffic. Hence, with sufficiently large number of messages, it is possible to determine the route taken by the traffic during an attack. This enables localization of the attacking host. An approach to overcome the problems associated with ascertaining the validity of IP addresses in ingress filtering is to use the routing information instead of just the source address. IP traceback proposes a reliable way to perform hop by hop tracing of a packet to the attacking source from where it originated [15][16]. However, this requires coordinated effort from all the routers in the network along with the path from the victim to the attacker, and examination of the packet logs. Deterministic packet marking (DPM) is another mechanism to detect DoS attacks [12]. It relies on routing information inscribed in the packet header by the routers as the packet traverses the network. This approach leads to an increase in the size of the IP packet header as the size of IP header increases linearly with the number of hops traversed. The resultant variable header size increases the complexity of processing. Intrusion prevention Technique which can be efficiently used to detect the DR-DoS attack [3]. Hiroshi Tsunoda, Kohei et.al [10] proposed work on detecting DRDoS attacks by a simple response packet confirmation mechanism Response packet confirmation mechanism. His proposed model was simple to deploy and computational cost is also low. Basheer Al-Duwairi et.al [11] proposed distributed packet pairing for reflector based DDoS attack mitigation. Rank Correlation based Detection Efficiently differentiate attack packets from the malicious packets. The Protocol Independent Detection and Classification (PIDC) Response rate = good. Xiao, Bin et.al [9] proposed a novel approach to detecting DDoS Attacks at an early stage Cooperative based detection method warning will be sent to the protected server, if packet drop occurs.

PROPOSED System

This system uses correlation based approach for characterizing network flows. It works in two stages as per given in figure 1. The two phases are given as follows, training and detection phase which is also called as testing phase, Before training there is additional phase included which is essential for any data mining or machine learning model that is data pre-processing and normalization. This important step is carried out before passing the data to the training state, with removed labels from each sample. In the training phase, the system applies statistical transformation techniques to determine the correlation between various networks flows by which we can carry out flow characterization. Once overall training completed the collected statistical measures such as standard deviation, mean, mean correlational matrix is stored into database so that in future detection phase it can be used as reference point. In the detection phase, mixture of normal and DoS attack samples were given and Detection Rate and False Positive Rate is measured. The statistical method used in this system reveals the correlation between various attributes in the packet samples and we use them with network flow rate to characterize the network samples.

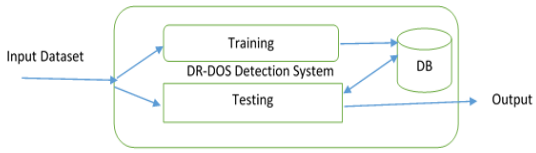

Fig. 1 System Architecture

The correlation between any two samples can be obtained using equation given below, where Tr2,1 is the correlation between attribute number 2 to attribute 1. Once we have flow correlation between normal samples, we can put a threshold to detect DRDoS attacks [15]. Correlation between any two samples can be obtained using statistical analysis. Once we have flow correlation between normal samples, we can put a threshold to detect DRDoS attacks [15].

$$Cov = \begin{bmatrix} \sigma(Tr_{2,1}^{normal}, Tr_{2,1}^{normal}) & \sigma(Tr_{2,1}^{normal}, Tr_{3,1}^{normal}) & \cdots & \sigma(Tr_{2,1}^{normal}, Tr_{m,m-1}^{normal}) \\ \sigma(Tr_{3,1}^{normal}, Tr_{2,1}^{normal}) & \sigma(Tr_{3,1}^{normal}, Tr_{3,1}^{normal}) & \cdots & \sigma(Tr_{3,1}^{normal}, Tr_{m,m-1}^{normal}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma(Tr_{m,m-1}^{normal}, Tr_{2,1}^{normal}) & \sigma(Tr_{m,m-1}^{normal}, Tr_{3,1}^{normal}) & \cdots & \sigma(Tr_{m,m-1}^{normal}, Tr_{m,m-1}^{normal}) \end{bmatrix}.$$

Standard deviation between any two samples can be calculated as,

$$\sigma(Tr_{j,k}^{normal}, Tr_{l,v}^{normal}) = \frac{1}{g-1}\sum_{i=1}^{g}(Tr_{j,k}^{normal,i} - \mu_{Tr_{j,k}^{normal}})(Tr_{l,v}^{normal,i} - \mu_{Tr_{l,v}^{normal}}).$$

A packet sample in KDD 99 dataset consist of 42 attributes, we consider only those attribute whose distance between mean and standard deviation is large. A packet sample in KDD 99 dataset consist of 42 attributes, we consider only those attribute whose distance between mean and standard deviation is large.

RESULTS AND DISCUSSION

This system evaluation is conducted using KDD Cup 99 dataset [7] that is developed for researchers at DARPA and it is available at their website. The data has been recorded for 7 weeks it contains normal as well as attack samples consisting of various attacks and overall samples collected consist of million. Each sample consist of 42 attributes and each of these samples are labeled so that individual researchers can train their models and carry out evaluation [12]. A smaller set out of 5 million samples is separated that is free from duplicates and it is recommended for the young researchers. During the evaluation, the 10 percent labeled data of KDD Cup 99 dataset is worn, here we have 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. We normalized the dataset before applying to this system. First, the proposed correlation based approach is evaluated for its accuracy of network traffic characterization. To evaluate the detection performance of the proposed correlation matrix-based detection system, and the entire filtered data subset is used in this assignment. The training is carried out on normal dataset and the network flow characteristics are extracted such as standard deviation between various attributes from their mean. Once training is over, we supplied mixture of normal as well as DoS attack samples and carried out evaluation. Various evaluation measures used in any intrusion detection system are Detection Rate, False Positive Rate and Accuracy. At different threshold levels we get changing values of FPR and DR. Finally the best detection rate we can achieve is 84% and corresponding FPR determined is 4%.

TABLE I: RESULTS

Sr. No	Threshold Level	False Positive Rate	Detection Rate
1	0.4	21%	100
2	0.5	18%	97
3	0.6	10%	92
4	0.8	4%	82

Conclusions

The steady evolution of DDoS attacks as a means for achieving political, economic, and commercial gains, and the relative ease, low costs, and limited accountability in launching such attacks, have rendered them one of the top threats to today's Internet services. Although various independent DDoS attack prevention, mitigation, and traceback techniques have been proposed by researchers over the last decades, their relative uptake has been minimal at beast, due to the lack of a robust, fool-proof, and universal DDoS attack defense mechanism. This paper uses correlation based approach for detecting DRDoS attack. This method is able to detect unknown attacks as well. The evaluation is carried out on KDD Cup 99 dataset and results are good. It has been verified that extracting correlation between various attributes in traffic flows is useful for differentiating network flows. Even if training time require by this system is high, once training is carried out everything works fine.

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.

A. Tajbakhsh, M. Rahmati, and A. Mirzaei, "Intrusion detection using fuzzy association rules," Applied Soft Computing, vol. 9, no. 2, pp. 462-469, 2009.

[5]. 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.

[6]. W. Hu, W. Hu, and S. Maybank, "Ada Boost-Based Algorithm for Network Intrusion Detection," Trans. Sys. Man Cyber. Part B, vol. 38, no. 2, pp. 577-583, 2008.

[7]. 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.

[8]. 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.

[9]. S. T. Sarasamma, Q. A. Zhu, and J. Huff, "Hierarchical Kohonenenet for Anomaly Detection in Network Security," Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on, vol. 35, pp. 302-312, 2005.

[10]. 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.

[11]. S. Jin, D. S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," Pattern Recognition, vol. 40, pp. 2185- 2197, 2007.

[12]. 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.

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.

[13]. 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.

[14]. S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Cost based 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.