International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 2 Issue: 1 08-Feb-2014,ISSN_NO: 2321-3337

Detecting Denial of Service attack using Multivariate Correlation Analysis

P.Chitra[1], Assistant Professor

P.Pooja [2], V .Vijayalakshmi [3], S.Divya [3]

Dept of Computer Science and Engineering

Velammal Institute of Technology

vvijivenkatesh@yahoo.co.in, prathushipooja@gmail.com, divya.sundaresan26@yahoo.com

ABSTRACT− *In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. DOS attack reduces the efficiency of the server, inorder to increase the efficiency of the server it is necessary to detect the dos attacks. Hence MULTIVARIATE CORRELATION ANALYSIS is used, this approach employs triangle area for extracting the correlation information between the ip addresses. Based on the extracted information the denial of service attack is detected and the response to the particular ip address is blocked, thus increasing the efficiency. Our proposed system is evaluated using KDD Cup 99 data set, and the influence of data on the performance of the proposed system is examined.*

1 Introduction

Denial of service attack severely degrades the efficiency of the online services. Therefore effective detection of dos attack is essential to the protection of the online services. The DOS attack detection, mainly focuses on the development of the network based detection mechanism[3]. The detection system employs two approaches namely misuse detection[1] and anomaly detection[2]. Misuse detection is used to identify the known attacks, using the signatures of predefined rules.[2]Anomaly detection is used to establish the usage profile of the system. During the training phase, the profiles for the legitimate traffic records are generated and the generated records are stored in the database. The trusted profile generation is build and handed over to the “attack detection” module, which compares the individual tested profile with the normal profile.

2 SYSTEM ARCHITECTURE

In the following section our proposed DOS, attack detection system architecture, where the system framework and the sample by sample detection mechanism are discussed.

2.1 Framework

The complete detection mechanism involves three phases. The sample by sample detection mechanism is involved in the three phases.[2] In phase one basic information is generated from ingress network traffic to the internal traffic where the servers and traffic records are formed in particular well defined time interval. The destination network is monitored and analyzed, so that the overhead of the detection is reduced[3]. This makes our detector to give best fit protection for the targeted network because the traffic profiles used by the detectors are developed for small number of network services. [2]In the second phase the multivariate correlate analysis is implemented. The triangle area map is generated which is used to extract the correlation between two distinct server within the record which is taken from the first phase. The intrusive activities are identified by making hem to cause changes to the correlation, with the help of these changes intrusions can be identified. All the triangle area correlations stored in triangle area maps (TAMs) are then used to replace the original basic features. This provides us with better information to sort out the legitimate and illegitimate traffic records. In phase three the decision making is done using the anomaly based detection system. This gives information about any DoS attacks without the requirement of the relevant knowledge. The labour intensive attack analysis and misuse based detection are avoided. Two steps are involved in decision making(i.e.the training phase and test phase). The training phase consists of "Normal Profile Generation" which is used to generate profiles for various types of legitimate traffic records and these profiles are stored in the database. During the test phase the "Tested Profile Generation Module" builds profiles for individual traffic records, which are then handed over to the attack detection module. This does the task of comparing the individual tested profile with respective stored normal profile. In attack detection module threshold –based classifier is used to distinguish the DoS attack from legitimate traffic.

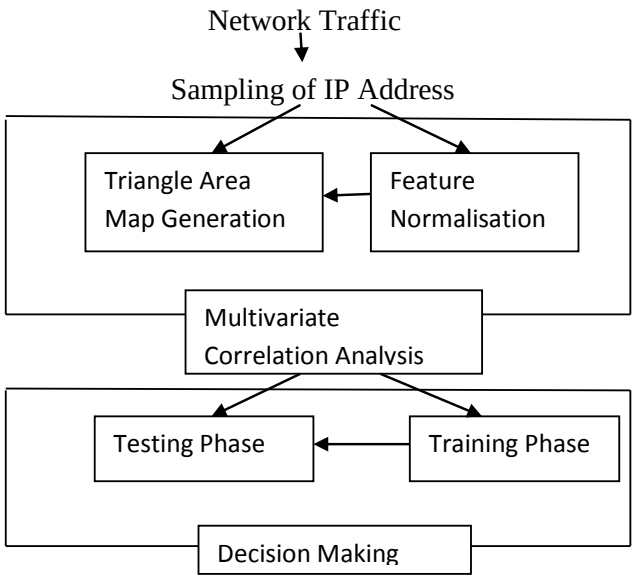

Fig – Denial Of Service Framework

2.2 Sample by sample detection

It is systematically proved that the group-based detection mechanism maintained a higher probability in classifying a group of sequential network traffic samples than the sample-by-sample mechanism. Whereas, the proof was based on an assumption that the samples in a tested group were all from the same distribution (class)[3]. This restricts the applications of the group-based detection to limited scenarios, because attack occur unpredictably in general and it is difficult to obtain a group of sequential samples only from the same distribution. To remove this restriction, our system in this paper investigates traffic samples individually. This offers benefits that are not found in the group-based detection mechanism. For example, (a) attacks can be detected in a prompt manner in comparison with the group-based detection mechanism, (b) intrusive traffic samples can be labeled individually, and (c) the probability of correctly classifying a sample into its population is higher than the one achieved using the group-based detection mechanism in a general network scenario[3].

3 Multivariate correlation analysis

DoS attack traffic behaves differently from the legitimate network traffic, and the behavior of network traffic is reflected by its statistical properties. [4]To well describe these statistical properties, we present a novel Multivariate Correlation Analysis (MCA) approach in this section. This MCA approach employs triangle area for extracting the correlative information between the features within an observed data object.[6]A Triangle Area Map (TAM) is constructed and all the triangle areas are arranged on the map with respect to their indexes. Hence, the *TAMi* is a symmetric matrix having elements of zero on the main diagonal.

4 DETECTION MECHANISM

In this section, we present a threshold-based anomaly detector, whose normal profiles are generated using purely legitimate network traffic records and utilized for future comparisons with new incoming investigated traffic records. The dissimilarity between a new incoming traffic record and the respective normal profile is examined by the proposed detector[5]. If the dissimilarity is greater than a pre-determined threshold, the traffic record is flagged as an attack. Otherwise, it is labeled as a legitimate traffic record. Clearly, normal profiles and thresholds have direct influence on the performance of a threshold-based detector.[1] A low quality normal profile causes an inaccurate characterization to legitimate network traffic. Thus, we first apply the proposed triangle area- based MCA approach to analyze legitimate network traffic, and the generated TAMs are then used to supply quality features for normal profile generation.

4.1 Normal profile generation

Assume there is a set of *g* legitimate training traffic records, The triangle-area based MCA approach is applied to analyze the records. [1]Mahalanobis Distance (MD) is adopted to measure the dissimilarity between traffic records. This is because MD has been successfully and widely used in cluster analysis, classification and multivariate outlier detection techniques. Unlike Euclidean distance and Manhattan distance, it evaluates distance between two multivariate data

objects by taking the correlations between variables into account removing the dependency on the scale of measurement during the calculation. Finally, the obtained distribution of the normal training traffic records, are stored in the normal profile for attack detection.

4.2 Threshold Selection

[6]The threshold given is used to differentiate attack traffic from the legitimate one.

4.3 Attack detection

To detect DoS attacks, the lower triangle (*TAMobserved lower*) of the TAM of an observed record needs to be generated using the proposed triangle-area-based MCA approach[6]. Then, the MD between the *TAMobserved lower* and the *TAMnormal lower* stored in the respective pre-generated normal profile *Pro* is computed using the detailed detection algorithm.

5 RESULT ANALYSIS

Many threshold frequence were set in camparison. The result reveals that at a certain threshold the server goes to sleep mode for long time period and crashes. Now this particular threshold is set as a limit to detect the intrusive networks.

CONCLUSION AND FUTURE WORK

[6]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 behaviors. 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 [2]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 Realtime," 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]. AdaBoost-Based Algorithm for Network Intrusion Detection
Weiming Hu, Senior Member, IEEE, Wei Hu, and Steve Maybank, Senior Member, IEEE.

[4]. Traffic flooding attack detection with SNMP MIB using SVMq
Jaehak Yu, Hansung Lee, Myung-Sup Kim *, Daihee Park
Department of Computer and Information Science, Korea University, Yeongi-Gun, Republic of Korea

[5]. Parametric Methods for Anomaly Detection in Aggregate Traffic
Gautam Thatte, Student Member, IEEE, Urbashi Mitra, Fellow, IEEE, and John Heidemann, Senior Member, IEEE.

[6]. A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis Zhiyuan Tan, Aruna Jamdagni, Xiangjian He‡, Senior Member, IEEE, Priyadarsi Nanda, Member, IEEE, and Ren Ping Liu, Member, IEEE.