A Review on Denial-of-Service Attack Detection Techniques Based on Multivariate Correlation Analysis

Santosh Khot[1]
[1]ME-PK Technical Campus, Pune University

Abstract-*Denial of Service (DoS) attacks are a critical threat to the Internet. It is very laborious to trace back the attackers for the reason that of memory less feature of the web routing mechanisms. As a result, there's no effective and economical technique to handle this issue. This paper discusses the effects of multivariate correlation analysis on the DoS detection. MCA based DoS attack detection system employs the principle of anomaly-based detection in attack recognition. This makes our resolution capable of detective work glorious and unknown DoS attacks effectively by learning the patterns of legitimate network traffic solely. DoS attacks that is based on MCA between normal and DoS attack traffic, which is fundamentally different from commonly used packet marking techniques. This technique is employed to spot the attackers with efficiency and supports an oversized quantifiability. Furthermore, a triangle-area based technique is used to enhance and to speed up the process of MCA. This technique is applied to bang the attackers in an exceedingly wide space of network that was a lot of economical and shield the info from the attackers.*

Keywords-Multivariate Correlation Analysis, Denial-of-Service attack, multivariate correlations, triangle area.

I. INTRODUCTION

Denial of Service (DoS) attack is one of the most common attacks which causes the serious impact in computing system .DoS attacks are class of attacks on targets, which aims at exhausting target resources, thereby denying service to valid users. Denial of service attack is mainly done in categorize to block a node from receiving genuine data or to block the node entirely from another genuine node. This attack is an attempt to make a machine or network resource unavailable to its intended users by either injecting a computer virus or flooding the network with useless traffic. Computer attack and network attack are the two types of dos attack .To break the server security hackers use DoS attack softening technique. The main targets of DoS attack are web server, application server, database server and communication link. It has become a major threat for current computer networks. Dos attack causes serious damages in services of network, so it is essential to develop a dos attack detection system to protect the services of network. There are two types of network based detection systems, viz. misuse based detection system [1] and anomaly based detection system [2].

In misuse based detection system attacks are detected by monitoring network activities and looking for matches with the existing attack signatures. In misuse based detection system the database should be kept updated which is a laborious task as it is a manual process. So, to overcome these drawbacks of misuse based detection system, anomaly based detection system is developed which is a novelty-tolerant detection system.

The manual attack analysis and the frequent update of the attack signature database are avoided in the case of misuse-based detection. DoS attack detection system detects known and unknown attacks respectively. To enhance and speed up the process of MCA, triangle area [3] technique is introduced to generate better discriminative features. In this system we are using normalization technique. KDD cup 99 dataset [4] is used for evaluation of DoS attack detection system.

II. LITERATURE SURVEY

Shuyuan Ji n et. al [5] The effects of multivariate correlation analysis on the DDoS detection and proposes an example, a covariance analysis model for detecting SYN flooding attacks. The simulation results show that this method is highly accurate in detecting malicious network traffic in DDoS attacks of different intensities. This method can effectively differentiate between normal and attack traffic. Indeed, this method can detect even very subtle attacks only slightly different from normal behaviors. The linear complexity of the method makes its real time detection practical. The covariance model in this paper to some extent verifies the effectiveness of multivariate correlation analysis for DDoS detection. Some open issues still exist in this model for further research.

Thivya et. Al [6] Denial of service (DoS) attacks have 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 coordinately 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.

K.Sujithra et.al [7] well organized systems such as net servers, file servers, cloud computing etc. is now under serious attack from network attackers. Denial-of-service attack is the one of the most frequent and aggressive to computing systems. In this scheme we propose a procedure called multivariate correlation analysis to detect an exact traffic flow classification by extracting the geometrical correlation between known and unknown attacks. This system includes anomaly detection method for the detection of known and unknown Dos. Additionally Triangle Area Based Technique is used to speed up the process of Multivariate Correlation Analysis (MCA). Proposed system can be evaluated by using KDD cup dataset

III. SYSTEM OVERVIEW

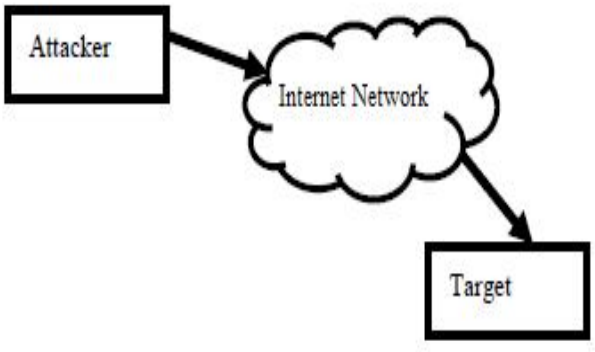

Figure 1. Overview of DOS Attack

DoS Attacks

DoS attacks see a Fig. 1, a single machine can sent a huge number of malicious packets, with the purpose of exhausting a target networking resources and computational, or crashing the target. The aim of such attacks is to despoil appropriate access of users to the target's services. In a DoS attack, one internet connection and one computer is used to flood a server with packets, with the purpose of overloading the targeted server's bandwidth and resources [8].Following are the different DoS Attack classification:

- Network Device Level: DOS attacks in the Network Device Level include attacks that might be caused either by taking the advantage of bugs in software or by trying to exhaust the hardware resources of network devices [8].
- Operating System Level: In an OS Level DOS attacks take advantage of the ways operating systems implement protocols [8].
- Application based attacks: A great number of attacks try to settle a machine or a service out of the order either by taking advantage of specific bugs in network applications that are running on the target host or by using such applications to dram a resources of their victim [8].
- Data Flooding: An attacker may attempt to use a bandwidth available to a network, host or device at its greatest extent, by sending massive quantities of data and so causing it to the process extremely large amounts of data [8].
- Attacks based on protocol features: DOS may take advantage of certain standard protocol features, for example the several attacks exploit a fact that source addresses can be spoofed [8].

IV. SYSTEM FRAMEWORK

The complete detection mechanism involves three phases. The sample by sample detection mechanism is involved in the three phases. 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. This makes our detector to give best fit protection for the targeted network because the traffic profiles used by the detectors are developed for smallnumber of network services. 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 labor 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.

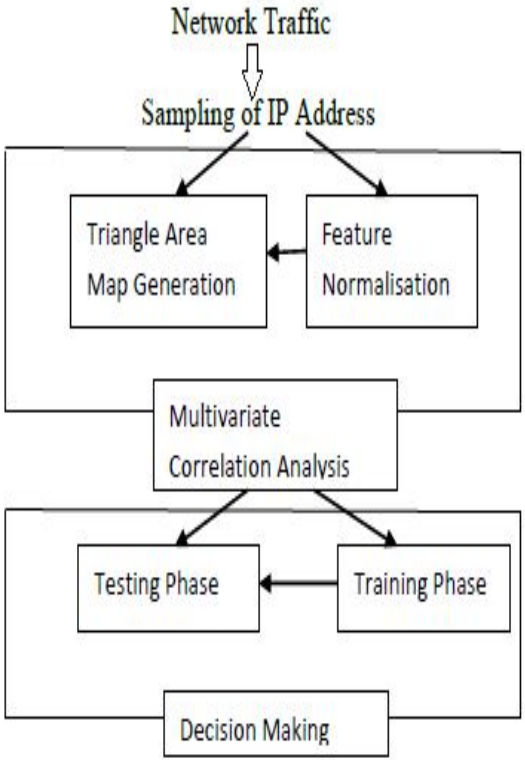

Figure 2: Denial of Service Framework

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. [9] 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.

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. 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.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.

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. [10]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.

2. Threshold Selection

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

3. Attack detection

To detect DoS attacks, the lower triangle (TAM observed lower) of the TAM of an observed record needs to be generated using the proposed triangle-area-based MCA approach[9]. Then, the MD between the TAM observed lower and the TAM normal lower stored in the respective pre-

generated normal profile Pro is computed using the detailed detection algorithm.

IV. CONCLUSION

This paper gives an brief overview about Dos attack and multiple detection mechanisms which are useful and efficient technique for the detection of DoS attack. We have extracted important features from MCA (analysis technique) and speeded it up using triangle area map method. The future work of this study will be implementation of the system and checking its efficiency in practical use and make it use practically in the real time systems for avoiding DoS attacks. In future, further optimization of this technique can also be done.

ACKNOWLEDGMENT

This is an opportunity to express my gratitude towards everyone who suggested and helped us in this Review paper. I wish devote my sincere thanks to our guide Dr. S. T. Singh for guidance and also provide gratitude to our college PK Technical Campus, Pune and my classmates for their help.

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] 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.

[4] 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.

[5] Shuyuan Jin,”A Covariance Analysis Model for DDoS Attack Detection”, Department of Computing HongKong Polytechnic University HongKong, Chinacssyjin@comp.polyu.edu.hk

[6] Thivya.,Karthika, “Efficient Detection for DOS Attacks by Multivariate Correlation Analysis and Trace Back Method for Prevention”, Department of computer science and engineering, Dhanalakshmi srinivasan engineering college,Perambalur.

[7] K.Sujithra ,”A Survey On Triangle Area Map Based Multivariate Correlation Analysis To Detect Denial-Of Service Attack”,PG Scholar, Dept of CSE, Kalingnar Karunanidhi Institute of Technology, Coimbatore, India

[8] Darshan Lal Meena Dr. R.S.Jadon , “A Survey on Different Solutions to DDoS Attacks”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, 2014.

[9] 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.

[10] V. Paxson, “Bro: A System for Detecting Network Intruders in Realtime,” Computer Networks, vol. 31, pp. 2435-2463, 1999