MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

A SYSTEM FOR DENIAL OF SERVICE ATTACK DETECTION BASED ON MULTIVARIATE CORRELATION ANALYSIS

P.V.Sawant[1], M.P.Sable[2], P.V.Kore[3], S.R.Bhosale[4]

Department of Computer Engineering, University of Pune Imperial College of Engineering and Research, Pune, India

[1]prtksawant09@gmail.com, [2]minalsable121@gmail.com, [3]pooja.kore10@gmail.com,[4]shitu.bhosale@gmail.com

Abstract- *Over the internet, in our day to day life we are working with interconnect systems such as web servers, database servers, cloud computing servers. These are the systems which are dealing with so many requests and responds them as legitimate requests. But the systems can be targeted by the attackers using Denial-of-Service(DoS) attack for temporary or permanent failure of the system. Denial-of-Service attack causes serious impact on the performance of the server with many a times the server gets down and stops processing the requests especially the genuine or legitimate requests. It happened so, because the server remains busy with the fake requests sent from the attackers by serving those fake requests. So, to increase the efficiency and the performance of the server, we must need to detect and avoid the DoS attacks. In this paper, we present a DoS attack detection system using features normalization and triangle area map techniques under Multivariate Correlation Analysis(MCA) which are useful for accurate traffic characterization. Traffic Characterization is done by extracting geometric correlation between network traffic features. Our DoS attack detection system can detect both known and unknown DoS attacks since it implements the principle of anomaly based detection for attack reorganization. Effectiveness of the system is increased because of its capability to learn the new patterns of legitimate network traffic. Triangle-area-based technique is used to speed up the process. Detection of SQL injection is also introduced in the system for security purpose of the stored legitimate profiles. The system designed to carry out attack detection is a question-answer portal i.e. a web*

application and hence the system is using HTTP protocol unlike previous systems which were using TCP.

Keywords: *Denial-of-Service attack, Features Normalization, Triangle Area Map, Multivariate Correlation, anomaly based detection, SQL injection, HTTP, and TCP*

1. 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 [8] and anomaly based detection system[9].

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. In this paper, Our proposed system is for protecting services of network against DoS attacks.. This detection system can provide an effective protection to interconnected systems like web servers, database servers, cloud computing servers etc. by considering their commonality. This system is anomaly based detection system and it employs principles of multivariate correlation analysis (MCA)[1]. DoS attack detection system detects known and unknown attacks respectively. To enhance and speed up the process of MCA, triangle area [10] technique is introduced to generate better discriminative features. In this system we are using normalization technique. KDD cup 99 dataset [11] is used for evaluation of DoS attack detection system.

2. PROPOSED SYSTEM ARCHITECTURE

As shown in the system architecture, the detection mechanism has three steps. In first step generation of basic feature takes place for an individual record from ingress network traffic. To reduce the overhead of the detection, the destination network is monitored and analyzed, which help detector to protect targeted network

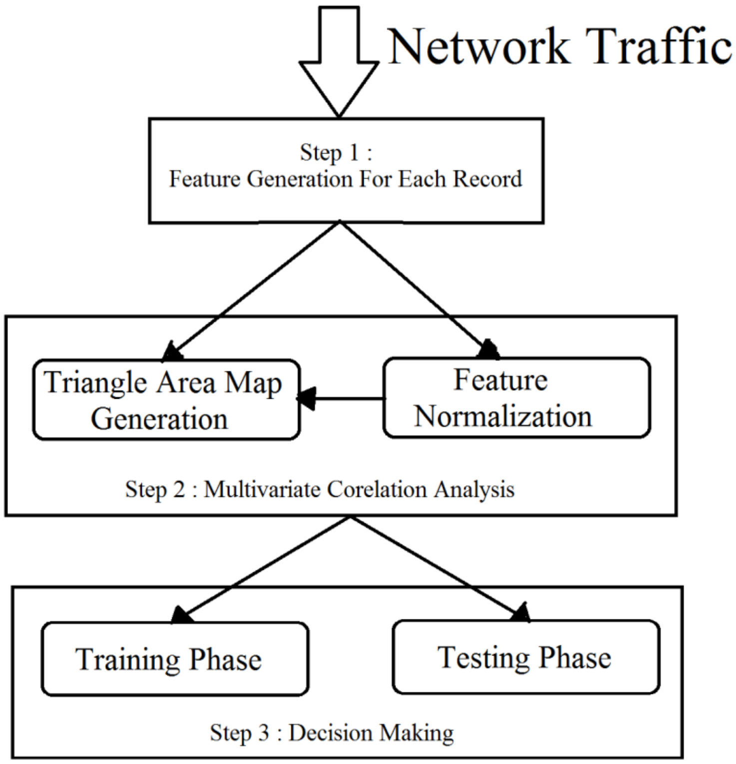

Fig. 1 Framework of DoS attack detection system

In second step, multivariate correlation analysis is implemented in which includes "Triangle Area Map (TAM) generation" and "Feature Normalization". To extract the correlation between two distinct features within each traffic record coming from the first step, we applied the Triangle area Map generation technique. In feature normalization module, traffic records get normalized which is given as input to the TAM. To replace the original basic features, all the triangle area correlations stored in triangle area maps (TAMs) are then used. This helps to differentiate between legitimate traffic records. In decision making step, anomaly base detection mechanism is adopted because of which we can detect the attack without requiring any attack relevant knowledge.

In third step called "Decision Making" includes two phases namely training phase and test phase. In training phase "Normal profile generation" is operated in which generation of profiles takes place for various type of legitimate records and are stored in database. In test phase, "Tested profile generation" module is used to build profiles for individual traffic records then tested profile is given to the module called "Attack Detection". The comparison of individual tested profiles with the respective stored normal profiles takes place in the attack detection module.

3. RESULT

The system will end up with blocking the user who is trying to attack (DoS or SQL injection) on the system. The blocking will be of two types, permanent blocking and temporary blocking. The threshold value has beed decided depending on impact of the attack. If the current attack value is more than threshold then user will be blocked permanently and if it is less than threshold then he will be notified about his behaviour on the network and will be able to request the admin to unblock his services. Admin has the privilege to remove temporary blocking.

4. CONCLUSION AND FUTURE SCOPE

The research proposed here is 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 study also lead us to introduce SQL injection attack detection in the system since preserving the data needed for the analysis was also a challenge. 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

We would like to sincerely thank Mrs. Darshika Lothe, our guide, for her support and encouragement.

REFERENCES

[1] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He‡, Senior Member, IEEE, Priyadarsi Nanda, Member, IEEE, and Ren Ping Liu, Member, IEEE, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. , NO. , 2013.

[2] www.ijetae.com/files/ICMACE14/IJETAE_ICMACE_14_32.pdf

[3] 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.

[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] 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.

[6] Mirzaei. A ,M. Rahmati ,and A. Tajbakhsh, ,Intrusion Detection System using Hybrid differential evolution and group method of data handling approach Pattern Recognition, vol. 43, pp.222-229, 2010.

[7] http://www.slideshare.net/skothari22/a-system-for-denial-ofservice-attack-detection-based-on-multivariate-correlation-analysis-2

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

[9] 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.

[10] 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.

[11] 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.