International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

Efficient Detection for DOS Attacks by Multivariate Correlation Analysis and Trace Back Method for Prevention

Thivya. T[1], Karthika.M[2]

Student, Department of computer science and engineering, Dhanalakshmi srinivasan engineering college,Perambalur.

Asst Prof, Department of computer science and engineering, Dhanalakshmi srinivasan engineering college,Perambalur

1 thivya.techno@gmail.com,

2 karthismile89@gmail.com,

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. In this project, traces back of the attackers are efficiently identified and also to protect the data from the attackers using Multivariate Correlation Analysis (MCA) by estimate accurate network traffic characterization. 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. Proposed system use a novel trace back method for 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—Denial-of-Service attack,multivariate correlations, network traffic characterization, triangle area, trace back Scheme.

I INTRODUCTION

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.

Generally, network-based detection systems can be classified into two main categories, namely misusebased detection systems [1] and anomaly-based detection systems [2]. Misuse-based detection systems detect attacks by monitoring network activities and looking for matches with the existing attack signatures. In spite of having high detection rates to known attacks and low false positive rates, misuse-based detection systems are easily evaded by any new attacks and even variants of the existing attacks.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

Furthermore, it is a complicated and labor intensive task to keep signature database updated because signature generation is a manual process and heavily involves network security expertise. Research community, therefore, started to explore a way to achieve novelty-tolerant detection systems and developed a more advanced concept, namely anomaly based detection. Owing to the principle of detection, which monitors and flags any network activities presenting significant deviation from legitimate traffic profiles as suspicious objects, anomaly-based detection techniques show more promising in detecting zero-day intrusions that exploit previous unknown system vulnerabilities [3]. Moreover, it is not constrained by the expertise in network security, due to the fact that the profiles of legitimate behaviors are developed based on techniques, such as data mining [4], [5], machine learning [6], [7] and statistical analysis [8], [9]. However, these proposed systems commonly suffer from high false positive rates because the correlations between features/attributes are intrinsically neglected [10] or the techniques do not manage to fully exploit these correlations. Recent studies have focused on feature correlation analysis. Yu et al. [11] proposed an algorithm to discriminate DDoS attacks from flash crowds by analyzing the flow correlation coefficient among suspicious flows.

A covariance matrix based approach was designed in [12] to mine the multivariate correlation for sequential samples. Although the approach improves detection accuracy, it is vulnerable to attacks that linearly change all monitored features. In addition, this approach can only label an entire group of observed samples as legitimate or attack traffic but not the individuals in the group.

To deal with the above problems, an approach based on triangle area was presented in [13] to generate better discriminative features. The DoS attack detection system presented in this paper employs the principles of MCA and anomaly-based detection. They equip our detection system with capabilities of accurate characterization for traffic behaviors and detection of known and unknown attacks respectively. A triangle area technique is developed to enhance and to speed up the process of MCA.

Proposed system use a novel trace back method for DoS attacks that is based on MCA between normal and DoS attack traffic, which is fundamentally different from commonly used packet marking techniques.

This method is used to identify the attackers efficiently and supports a large scalability. Furthermore, a triangle-area-based technique is used to enhance and to speed up the process of MCA. This method is applied to block the attackers in a wide area of network which was much efficient and protect the data from the attackers.

II Related Works

The whole detection process consists of three major steps as shown in Fig. 1. The sample-by-sample detection mechanism is involved in the whole detection phase (i.e., Steps 1, 2 and 3) and is detailed in Section 2.2. In Step 1, 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.

The detailed process can be found in [17]. Step 2 is 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 (Step 2). 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. Our MCA method and the feature normalization technique are explained in Sections 3 and 5.2 respectively. In Step 3, the anomaly-based detection mechanism [3] is adopted in Decision Making.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

The facilitates the detection of any DoS attacks without requiring any attack relevant knowledge. Furthermore, the labor-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 labor-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 Marking.

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.

III THE PROPOSED APPROACH

An approach based on triangle area was presented in this project to generate better discriminative features. However, this approach has dependency on prior knowledge of malicious behaviors. Here distance was used to extract the correlations between the selected packet payload features. We proposed a more sophisticated non-payload based DoS detection approach using Multivariate Correlation Analysis (MCA). Following this emerging idea, A new MCA-based detection system to protect online services against DoS attacks in this work.

Proposed work facilitates the detection of any DoS attacks without requiring any attack relevant knowledge. Furthermore, the labor-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.

The Steps Involved are

- Denial of Service Attack Detection
- MCA Technique
- Denial of Service Attack Prevention
- IP Trace Bach Scheme

Advantages

- An Efficient Detection system
- New Prevention Technique
- Anomaly Based Detection Method
- Able to Detect Known and Unknown Attacks
- Hence security level is increased.

4.1 Architecture

IV ARCHITECTURE

In Figure 4.1, The admin will have permission to view the entire processes done by the user. The user can only view the authenticated process after getting registered to the approach.

User can view their personal information and the data which sent by him. In the server module have the static and secure login to enter and starts the server to receive the data.

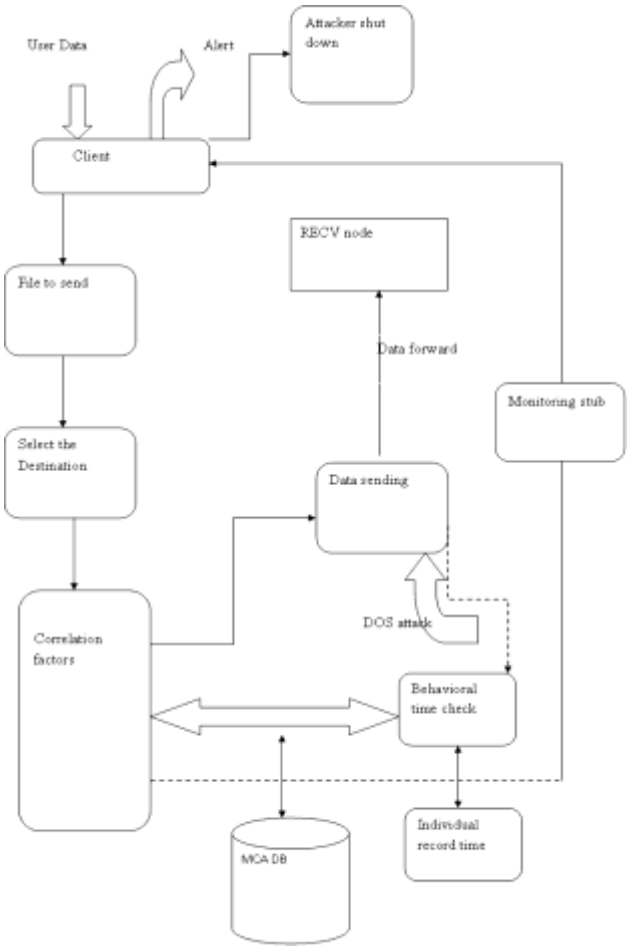
Once the user registered , they have to analyze their position in network and keep track about the time and distance among other nodes within the network.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

The network has divided by workgroups. After getting login to our process, this module will get the connected systems and shows to the users. The user can select the system to deliver their data by file transfer.

The disconnected and the shutdown systems are not visible in the list. After that users can compare the path info by using correlation factors among nodes. Every node update their own table about correlation factors and that will circulate entire network.

The user has to select the system to transfer the data and the file to be transferred. The selected file will be encrypted for secured transfer. When the data received by the desired path of destination, the key automatically enabled and decrypted.



In our process, we have to monitor the client data, which are sent to the receiver with a certain path. After the intruder affects the current data, there is no use of reports. So here, we trace back the path of every data. Tracing the path of the data from one end to another end helps to find path deviations.

All the data transactions and intruder information are forward to the administrator. The administrator can able to make the denial of service of the intruder from the reports module. Proposed work facilitates the detection of any DoS attacks without requiring any attack relevant knowledge. Furthermore, the labor-intensive attack analysis and the frequent update of the attack signature database in the case of misuse-based detection are avoided.

V CONCLUSION

An approach based on triangle area was presented in this project to generate better discriminative features. However, this approach has dependency on prior knowledge of malicious behaviors. Here distance was used to extract the correlations between the selected packet payload features. A triangle-area-based technique is used to enhance and to speed up the process of MCA. The labor-intensive attack analysis and the frequent update of the attack signature database in the case of misuse-based detection are avoided.

The mechanism enhances the robustness. This method is applied to block the attackers in a wide area of network which was much efficient and protect the data from the attackers. To provide the detection of any DoS attacks without requiring any attack relevant knowledge. A new MCA-based detection system to protect online services against DoS attacks in this work. IP Trace Back Scheme can Performs the Prevention Process.

VI. REFERENCES

[1] Baras J.S., A. A. Cardenas, , and V. Ramezani, "Distributed change detection for worms, DoS and other network attacks," The American Control Conference, Vol.2, pp. 1008-1013, 2004..

[2]Daz-Verdejo.J ,P. Garca-Teodoro, G. Maci-Fernndez, and E.Vzquez,"Anomaly-based Network Intrusion Detection: Techniques,Systems and Challenges,"Computers & Security, vol. 28,pp. 18-28, 2009.

[3] Denning D.E., "An Intrusion-detection Model," IEEE Transactions on Software Engineering, pp. 222-232, 1987.

[4] Guo.S, W. Jia, F. Tang, S. Yu, and W. Zhou, "Discriminating DoS Attacks from Flash Crowds Using Flow Correlation Coefficient," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, pp. 1073-1080, 2012.

[5] Heidemann.J, U. Mitra and,G. Thatte, , "Parametric Methods for Anomaly Detection in Aggregate Traffic," Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011.

[6] Jamdagni,.A, P. Liu P. Nanda , and Z. Tan, "RePIDS: A multi tier Real-time Payload-based Intrusion Detection System,"Computer Networks, vol. 57, pp. 811-824, 2013.

[7] Jin.S, D. X. Wang and S. Yeung,, "A DetailedAnalysis of the KDD Cup 99 Data Set," The The Second IEEE InternationalConference on Computational Intelligence for Securityand Defense Applications, 2009, pp. 1-6.

[8] Kai.H, C. Yu 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] Kim.S, H. Lee , D. Park and J. Yu, "Traffic flooding attack detection with SNMP MIB using SVM," Computer Communications,vol. 31, no. 17, pp. 4212-4219, 2008.

[10] 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.

[11] Moustakides G. V., "Quickest detection of abrupt changes for a class of random processes," Information Theory, IEEE Transactionson, vol. 44, pp. 1965-1968, 1998.

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