Denial of Service Attack Detection System Using Multivariate Correlation Analysis

CHAMAKURI MADHURIMA[1], CHINTHAKRINDI GEAYA SRI[2], BITRA SRILATHA[3,] JONNADULA RAJASRI[4]

[1,2,3,4] *Student, Department of Computer Science and Engineering, Vasireddy Venkatadri Institute of Technology, Guntur, India.*

Abstract- ***There are many interconnected systems which we are working in our daily life i.e., cloud computing servers, web servers. These systems are now under the threat of various network attacks. Out of those, Denial of Service (DoS) causes serious impact to these interconnected systems. 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 it is important to detect and prevent DoS attacks. In this paper, we present a DoS attack detection system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. Our MCA based DoS attack detection system uses anomaly-based detection technique to recognize the attack. This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. Moreover, our system uses Triangle Area Map which is capable of speed up the process of MCA. The effectiveness of our proposed detection system is evaluated using KDD Cup 99 dataset, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examined.***

Index Terms: Denial of Service (DOS) attack, Multivariate Correlation Analysis (MCA), network traffic, normalized data, Triangle Area Map.

I. INTRODUCTION

A denial-of-service attack is a security event that occurs when an attacker takes action that prevents legitimate users from accessing targeted computer systems, devices or other network resources. Denial-of-service (DoS) attacks typically flood servers, systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them. While an attack that crashes a server can often be dealt with successfully by simply rebooting the system, flodding attacks can be more difficult to recover from. The United States Computer Emergency Readiness Team (US-CERT) provides some guidelines for determining when a DoS attack may be underway. US-CERT suggests the following may indicate such an attack:

- Degradation in network performance, especially when attempting to open files stored on the network or accessing websites;
- Inability to reach a particular website;
- Difficulty in accessing any website; and
- A higher than usual volume of spam email.

DoS attacks severely degrade the availability of a victim, which can be a host, a router, or an entire network. They impose intensive computation tasks to the victim by exploiting its system vulnerability or flooding it with huge number of useless packets. The victim can be forced out of service from a few minutes to even several days. This causes serious damages to the services running on the victim. Therefore, effective detection of DoS attacks is essential to the protection of online services. Work on DoS attack detection mainly focuses on the development of network-based detection mechanisms. Detection systems based on these mechanisms monitor traffic transmitting over the protected networks. These mechanisms release the protected online servers from monitoring attacks and ensure that the servers can dedicate themselves to provide quality services with minimum delay in response. Moreover, network-based detection systems are loosely coupled with operating systems running on the host machines which they are protecting. As a result, the configurations of network-based detection systems are less complicated than that of host-based detection systems.

Generally, network-based detection systems can be classified into two main categories, namely misuse based detection systems and anomaly-based detection systems. Misuse-based detection systems detect attacks by monitoring network activities and looking for matches with the existing attack signatures. Despite 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. 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. Owing to the principle of anomaly-based 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. 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. A statistical normalization technique is used to eliminate the bias from the raw data. Our proposed DoS detection system is evaluated using KDD Cup 99 dataset and outperforms the state-of the-art systems.

II. LITERATURE SURVEY

Many system and techniques are used to detect the Dos attack efficiently. Garcia describes by using Gaussian mixture model, they find the irregular packets in the network to identify the intrusion discovery in the system.

Vern Paxson developed a system called "Bro" a system for finding a network attacker in real time. It is a standalone system, which emphasizes high speed monitoring, real time, clear separation to achieve this Bro system.

Yu chin explain, the idea is to detect the abrupt traffic changes across multiple networks domain. Chin developed a architecture called Distributed Change Point Detection (DCD) using Change Aggregation Tree (CAT), it is suitable for efficient implementation and it is operated by ISP. To resolve this issue, a secure infrastructure protocol is developed to establish the mutual trust or consensus.

Chin – Fong Tsai & Chi – Ting Lin tells a new method to detect the dos attack called "Triangle Area Based Nearest Approach". Specifically, the k- means is used to extract the clusters center where each one represents a one attack. The k-NN classifier is used to detect intrusion. By using this approach, we improve in terms of accuracy, detection state, and false detection rate.

Theerasak explain about Dos attack is carried out by attack tools like worms, botnet and the various forms of attacks packets to beat the defense system, so they propose a technique called "Behavior based Detection" that can discriminate Dos attack traffic from real method.

The above method is comparable detection method; it can extract the repeatable features of packets arrival. The Behavior Based Detection can differentiate traffic of an attack sources from legitimate traffic work with a quick response. The resulting performance so far is good enough to protect the server from crashing during a Dos attack.

III. PROPOSED SYSTEM ARCHITECTURE

The overview of proposed DoS attack detection system architecture is given in this portion, where the system framework and detection mechanism are discussed. The whole detection process consists of three levels as shown in Fig.1. Step 1. Multivariate correlation analysis Step 2. Normal profile generation. Step 3. Attack Detection.

A: Proposed Architecture

The framework consists of three Steps:

Step 1: In this level the basic features are generated from network traffic ingress to internal network where proposed servers resides in and are used to form the network traffic records for well-defined time. Monitoring and analyzing network to reduce the malicious activities only on relevant inbound traffic.

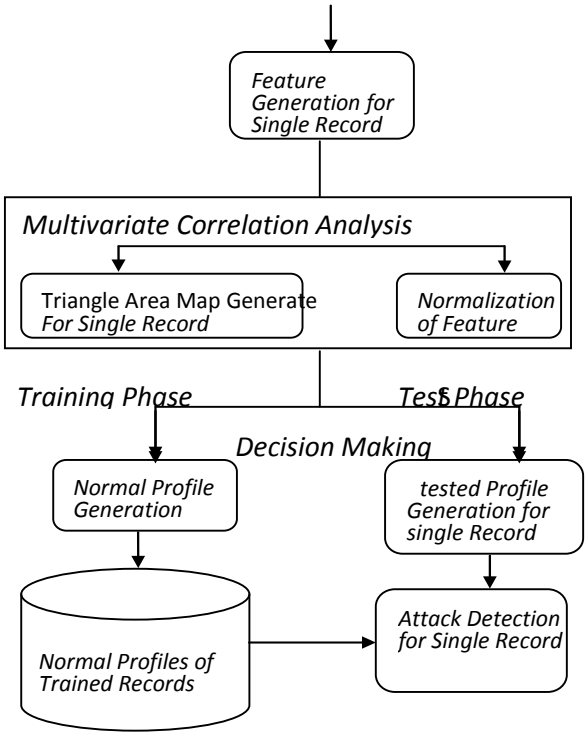

Fig. 1 Framework of DoS attack detection system

To provide a best protection for a targeted internal network. 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.

Step 2: In this step the Multivariate Correlational Analysis is applied in which the Triangle Area Map Generation module is applied to extract the correlation between two separate features within individual traffic record.
The distinct features are come from level 1 or "feature normalization module" in this step. All the extracted correlations are stored in a place called Triangle Area Map(TAM), are then used to replace the original records or normalized feature record to represent the traffic record. It's differentiating between legitimate and illegitimate traffic records.

Step 3: The anomaly-based finding mechanism is adopted in decision making. Decision making involves two phases as

- Training phase.
- Test phase

Normal profile generation module is work in "Training phase" to generate profiles for several types of 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 at last the tested profiles are handed over to "Attack Detection" module it compares tested profile with stored normal profiles. This distinguishes the Dos attack from legitimate traffic.

This needs the expertise in the targeted detection algorithm and it is manual task. Particularly, two levels (i.e., the Training Phase and the Test Phase) are included in Decision Making. The Normal Profile Generation module is operated in a Training Phase to generate profiles for several types of legal records of traffic, and the normal profiles generated are stored in the database. The tested profile generation module is used in a Test Phase to build profiles for each observed traffic documentation. Next, the profiles of tested are passed over to an attack detection part, which calculates the tested profiles for individual with the self-stored profiles of normal. A threshold-based classifier is employed in the attack detection portion module to differentiate DoS attacks from appropriate traffic.

B. Multivariate Correlation Analysis

DoS attack traffic treat differently from the appropriate traffic of network and the behavior of network traffic is reflected by its geometric means. To well describe these statistical properties, here a novel multivariate correlation analysis (MCA) moves toward in this part. This multivariate correlation analysis approach uses triangle area for remove the correlative data between features within a data object of observed (i.e. a traffic record).

C. Detection Mechanism

In this section, we present a threshold based on anomaly finder whose regular profiles are produced using purely legal records of network traffic and utilized for the future distinguish with new incoming investigated traffic report. The difference between an

individual normal outline and a fresh arriving traffic record is examined by the planned detector. If the variation is large than a pre-determined threshold, then a record is treated as anomaly record otherwise it is marked as the legal traffic record.

IV. CONCLUSION

This paper has presented a MCA-based DoS attack detection system which is powered by a triangle-area based MCA technique and an anomaly-based detection technique. The former technique extracts 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 proper network traffic. In this technique Time complexity is reduced, also Results are taken on real time dataset and false positive rate is reduced.

ACKNOWLEDGMENT

We would like to thank all the authors of different research papers referred during writing this paper and our project guide Mr.Ch. Vijayananda Ratnam for his help and encouragement for the completion of our project.

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] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] S. Jin, D. S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," Pattern Recognition, vol. 40, pp. 21852197, 2007.

[13] 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.

[14] 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.

[15] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Denialof-Service Attack Detection Based on Multivariate Correlation Analysis," Neural Information Processing, 2011, pp. 756-765.

[16] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "TriangleArea-Based Multivariate Correlation Analysis for Effective Denialof-Service Attack Detection," The 2012 IEEE 11th International

Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, United Kingdom, 2012, pp. 33-40.