ijecs
open access **www.ijecs.in**

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13226-13229

An Efficient Denial-of-Service Attack Detection System Based on Multivariate Correlation Analysis

[1]Binil Anto Thampi C., [2]Syed Farook K.

[1] M-Tech Student, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India
binilanto@gmail.com

[2] Assistant Professor, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India
Syed.dimple@gmail.com

Abstract: ***Internet is increasingly being used in almost every aspect of our lives and it is becoming a critical resource whose disruption has serious implications. Attacks that aimed at blocking availability of an internet services are generally referred to as denial of service (DoS) attacks. They cause financial losses, as in the case of an attack that prevented users from having steady connectivity to major e-commerce Web sites and imply threat to public safety and national security as in the case of taking down confidential government websites. The consequences of denial of service attacks can be very damaging. Therefore, it is crucial to deter, or otherwise minimize, the damage caused by denial of service attacks. A DoS attack detection system adapted should be able to detect all variants of DoS attacks with efficient computational costs. Thus far various methods have been introduced; however most of them failed to detect new variants of DoS attack and have destitute computation cost. In Multivariate Correlation Analysis based scheme a network features based detection system is introduced. The detection is done based on a normal profile which is generated by applying statistical analysis on the network features. Even though this system has quite good detection rates, some type of DoS attacks are left undetected and have high computation costs. The problems are due to the data used in detection, where the basic features in the original data are in different scales and not optimized. So an efficient detection system is designed by applying Statistical Normalization technique and Particle Swarm Optimization on the raw data to provide efficient detection rates and immaculate computation cost.***

Keywords: Denial of Service Attack, Feature Correlation Analysis, Particle Swarm Optimization, Multivariate Correlation Analysis.

1. Introduction

DoS attacks today are part of every Internet user’s life. They are happening all the time, and all the Internet users, as a community, have some part in creating them, suffering from them or even loosing time and money because of them. DoS attacks do not have anything to do with breaking into computers, taking control over remote hosts on the Internet or stealing privileged information like credit card numbers. The sole purpose of DoS attacks is to disrupt the services offered by the victim. While the attack is in place, and no action has been taken to fix the problem, the victim would not be able to provide its services on the Internet. DoS attacks are really a form of vandalism against Internet services. DoS attacks take advantage of weaknesses in the IP protocol stack in order to disrupt Internet services. DoS attacks can take several forms and can be categorized as Normal and Distributed DoS attacks. Normal DoS attacks are being generated by a single host (or small number of hosts at the same location). The only real way for DoS attacks to impose a real threat is to exploit some software or design flaw. Such flaws can include, for example, wrong implementations of the IP stack, which crash the whole host when receiving a non-standard IP packet (for example ping-of-death). Such an attack would generally have lower volumes of data. Unless some exploits exist at the victim hosts, which have not been fixed, a DoS attack should not pose a real threat to high-end services on today's Internet. DDoS (Distributed Denial of Service) attacks would, usually, be generated by a very large number of hosts. These hosts might be amplifiers or reflectors of some kind, or even might be zombies (agent program, which connects back to a pre-defined master hosts) who were planted on remote hosts and have been waiting for the command to attack a victim. It is quite common to see attacks generated by hundreds of hosts, generating hundreds of megabits per second floods.

The main tool of DDoS is bulk flooding, where an attacker or attackers flood the victim with as many packets as they can in order to overwhelm the victim. There are various examples to DoS attacks some of them are ICMP flood, SYN flood, Teardrop attack, Smurf attack, ping to death attack, spoof attack etc. Their common denominator is that they all use weaknesses or erroneous implementations of the TCP/IP protocol, or they utilize weaknesses in the specification of the TCP/IP protocol itself.

1.1 DoS Attack Detection

Defensive responses to denial-of-service attacks typically involves the use of a combination of attack detection, traffic classification and response tools, aiming to block traffic that they identify as illegitimate and allow traffic that they identify as legitimate. There are two basic techniques for network based detection systems: (1) misuse detection, and (2) anomaly detection. Systems that use misuse detection technique generate alarms when it identifies activities that violate specific rules or when patterns of malicious activities are found. Anomaly detection is dedicated to establish normal activity profiles by computing various metrics and an attack is detected when the actual system behavior deviates from the normal profiles. To effectively detect the Dos attacks so many methods based on data clustering, machine learning, soft computing, fuzzy logic and feature correlation analysis are in practice. Out of them feature analysis methods are found more efficient in the case of computational overhead, resource consumption and false alarms. A feature is an attribute that characterize the traffic and can consider as a random variable, which is obtained from the network traffic records and session/event logs. Statistical correlations can be performed on them to discriminate between legitimate and illegitimate traffic.

2. Related works

Researchers are always been conducted to improve the Denial-of-service attack detection efficiency of anomaly based detection systems using statistical methods. Generally a statistical model for normal traffic is fitted and then a statistical inference test is applied to determine if a new instance belongs to this model. Instances that do not conform to the learnt model, based on the applied test statistics, are classified as anomalies. They select certain feature components from the traffic or packet that effectively define corresponding packet, or features can be viewed as attributes that can be extracted from network packets. Statistical modelling is performed on these features. These methods mainly focus on to increase the detection rate while keeping the false positive rate very minimum. Some of such innovative approaches are described here. M. Tavallaee et al.[1] proposed a method called Covariance Matrix Sign (CMS), uses the covariance matrix as an anomaly detection approach. In this method compared the signs in the covariance matrix of a group of sequential samples with the signs in the covariance matrix of the normal data obtained during the training process. If the number of differences exceeds a specified threshold, all the samples in that group will be labelled as attacks; otherwise they will be labelled as normal. Principal Component Analysis is performed as a pre-detection step for the dimensionality reduction. A. Jamdagni et al.[2] presented a new model, called Geometrical Structure Anomaly Detection (GSAD) based on pattern recognition technique used in image processing, which method employs geometrical structure into payload-based anomaly detection. This IDS is based on a statistical analysis of Mahalanobis Distances Map among characters appearing in network traffic and distinguishes abnormal traffic from normal ones with patterns.

Zhiyuan Tan et al.[3] introduced a method which make use of Linear Discriminant Analysis (LDA) to select significant features from a Mahalanobis Distance Map (MDM), which is generated by the Geometrical Structure Model (GSM) [2], a key component of the GSAD, for each single network packet to explore the correlations among features (ASCII characters) in a packet payload. Then, the final detection process can be fast conducted on a new low-dimensional domain. LDA is employed to select the most signification features for each normal and attack pair based on the pre-generated difference distance maps. Then All of the selected features are integrated into a new significant feature set used for normal profile development and malicious behaviour detection. J. Udhayan et al.[4] introduced a statistical segregation method (SSM) which samples the flow in consecutive intervals and then the samples are compared against the attack state condition and sorted with the mean as the parameter, then the correlation analysis is performed to segregate attack flows from the legitimate flows. Also Rate Analysis is performed to detect and categorize attacks with different rates. Shui Yu et al.[5] Proposed an method with less false alarms that effectively discriminate attacks from legitimate flow. This method uses flow correlation coefficient as a metric to measure the similarity among suspicious flows and legitimate flow (flash crowd). This method is also delay proof and effective against forthcoming flooding attacks. Recently Zhiyuan Tan et al.[6] proposed a DoS detection system that uses multivariate correlation analysis for the network characterization. It works by calculating a measure called Triangle Area Map (TAM) of the network features and based on those values corresponding normal behaviours and attack traces in a network in identified. Even though this method is efficient in many ways, it has two main problems. The computation cost in terms of system time and memory is high and some varieties of DoS attacks are undetected. The method proposed in this section 3 is effectively overcome those problems. Later in section 4 these two methods are compared on their detection capabilities and cost efficiencies.

3. Proposed work

In this section a new and efficient DoS attack detection system is introduced. The main concept of steps involved in the detection process is explained here. The framework of the proposed system is as follows. The whole detection process consists of five major steps as shown in figure 1. The steps are Feature generation, Traffic record optimization, Feature normalization, Multivariate correlation analysis and Decision making.

3.1 Feature generation

In this step, 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 analysing 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.

3.2 Traffic record optimization

The traffic record with features obtained from step 1 will be bulky. Most of the features in the data are irrelevant and not optimized. This problem can be eliminated by applying convenient optimization techniques on the data. The Particle Swarm Optimization [7] is selected for the work. The Particle Swarm Optimization (PSO) is a population based stochastic optimization technique, inspired by social behaviour of bird flocking or fish schooling. This method is selected over other optimization techniques because it is easy to implement and there are few parameters to adjust. In PSO the potential solution, called particles fly through the problem space by following the current optimum particles. Detailed working of PSO can be found in [7].

After applying the PSO on the input datasets to the system, it generates a dataset X = {x{1},x{2,}...,x{n}}, with n traffic records each containing m features. Where the traffic records are optimized and all the features selected are relevant. That is the optimized traffic records with selected features provide best result in the detection process. So, the entire data is sharpened specific to individual traffic records, thereby reducing the size of data to handle and uses less system time and memory for the processing.

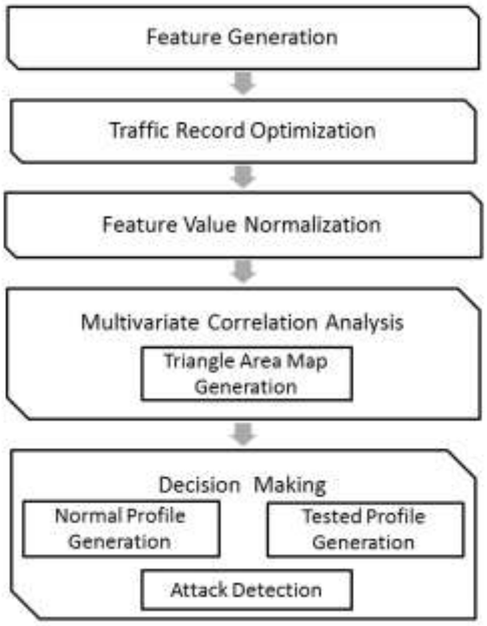
Feature Generation
Traffic Record Optimization
Feature Value Normalization
Multivariate Correlation Analysis
Triangle Area Map Generation
Decision Making
Normal Profile Generation
Tested Profile Generation
Attack Detection

Figure 1: Framework of the proposed system

3.3 Feature value normalization

Large valued features bestride in the creation of attack and normal network profiles. The small valued or zero valued features in the original data are neglected. To avoid this type of bias, an appropriate data normalization technique should be employed. The Statistical normalization technique [8] is found to be suit for the work. The statistical normalization takes both the mean scale of attribute values and their statistical distribution into deal with. It converts the output of any normal distribution into standard normal distribution, in which 99.9 % samples of the attribute are scaled into [-3, 3]. In addition, statistical normalization has been proven improving detection performance and outperforming other normalization techniques. The details can be found in [8].

The normalized feature vector x{i} is represented by the transpose of [F1{i},F2{i},..Fm{i}]. The normalization process is always done in a batch manner. The normalized feature values are then used for the TAM generation in the multivariate correlation analysis phase and later in the detection phase.

3.4 Multivariate correlation analysis

In this step 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. 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. The detailed process is described in [6].

3.5 Decision making

The anomaly-based detection mechanism is adopted in this step. It facilitates the detection of any DoS attacks without requiring any attack relevant knowledge. 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 labour 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 Making. 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.

4. Results and Analysis

For evaluating the MCA based system and the proposed system, network traffic records required in the detection process is taken from the KDD Cup99 dataset [9]. KDD Cup99 dataset is the only publicly available labeled benchmark dataset and it has been widely used in the intrusion detection systems. For the evaluation only 10 percent labeled data of KDD Cup99 dataset is used. The selected dataset contains 41 network features in each traffic record and they are from three types of legitimate traffic (TCP, UDP and ICMP traffic) and various types of DoS attacks (Land, Teardrop, Neptune, Back attacks etc.).

By evaluating these two systems based on the parameters, the detection rate and the computational cost in the terms of time and memory provides the following results. For MCA based detection system some of the DoS attack traces in the labeled dataset are found to be left undetected, failing in the detection rate. Also the system time and system memory for the overall detection process are high. Once the modified version is implemented, introducing the optimization and normalization phases, it is found that the detection rate is gradually increased and the time and memory requirements are decreased. The following graphs (figure 2-4) compare the detection rate, time requirements and memory requirements of the two systems

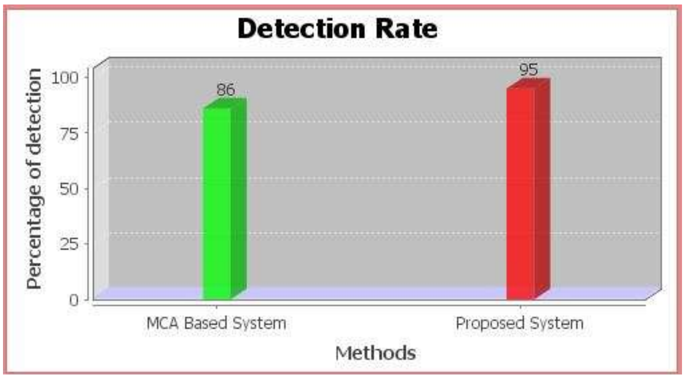

Figure 2: Detection rate comparison

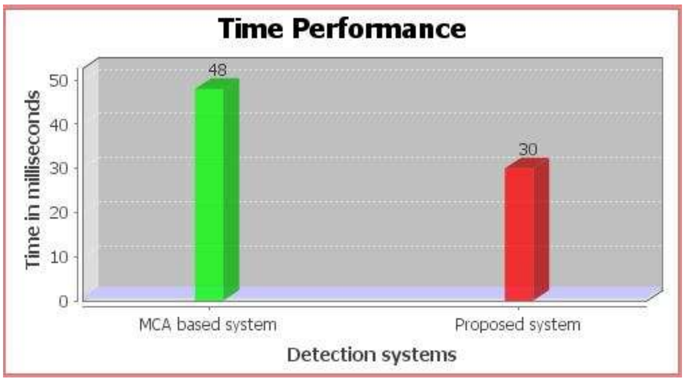

Figure 3: Time performance comparison

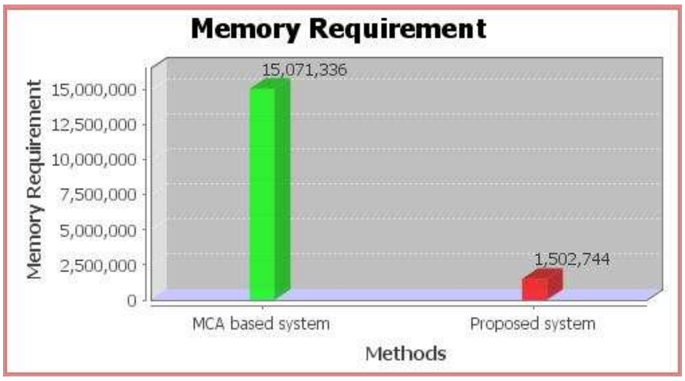

Figure 4: Memory requirement comparison

5. Conclusion

Denials of service attacks are types of intrusion that blocks the availability of an internet service. Since they cause large financial loses and threat to security, the efficient detection and prevention of DoS attacks are essential. In this work several feature correlation analysis based DoS attack detection systems are studied in detail. Out of them MCA based detection system is found more efficient. Failing in detecting some varieties of DoS attacks and large computation costs are the main drawbacks of this MCA based system. But the proposed method, which is the modified version of MCA based system overcome the problems effectively. The experimental results conclude that the proposed method reduces the computation cost and maintains high detection rates.

References

[1] Tavallaee M.,Wei Lu, Iqbal, S.A. Ghorbani, A.A., "A Novel Covariance Matrix Based Approach for Detecting Network Anomalies", Communication Networks and Services Research Conference,2008. CNSR 2008. 6th Annual, IEEE Computer Society, vol. 75, no. 81, pp. 5-8. May 2008.

[2] A. Jamdagni, Tan Zhiyuan, P. Nanda, Xiangjian He and Ren Liu., "Intrusion Detection Using Geometrical Structure", Frontier of Computer Science and Technology, 2009. FCST '09. Fourth International Conference, IEEE Computer Society, vol. no., pp.327, 333, 17-19. Dec. 2009.

[3] Tan Zhiyuan, A. Jamdagni, He Xiangjian and P. Nanda., "Network Intrusion Detection based on LDA for payload feature selection" IEEE GLOBECOM Workshops on Web and Pervasive Security ,vol., no., pp.6,10, 1545-1549, Dec. 2010.

[4] J. Udhayan and T. Hamsapriya., "Statistical segregation method to minimize the false detections during DDoS attacks." International Journal of Network Security, vol., pp. 13, 152-160. Nov. 2011.

[5] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang and F. Tang., "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient", IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 1073-1080, June 2012.

[6] S. Zhiyuan Tan, Aruna Jamdagni, X He, P Nanda and Ren Ping Liu., "A system for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 2, pp. 447-456, Feb. 2014.

[7] James Kennedy and Russel Eberhart, "Particle swarm optimization", Neural Networks, 1995. Proceedings, IEEE International Conference, vol. 4, pp. 1942-1948, Dec. 1995.

[8] W. Wang, X. Zhang, S. Gombault, and S. J. Knapskog., "Attribute Normalization in Network Intrusion Detection", The 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), pp. 448-453., 2009.

[9] 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 '00 (DISCEX 00), vol. 2, pp. 130-144, 2000.