International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Efficient Detection for DOS Attacks by Multivariate Correlation Analysis

Animol T Joseph[1], Athira Raj[2]

[1]Final Year M. Tech. (Cyber Security), KMP College of Engineering, Perumbavoor, Kerala, India

[2]Assistant Professor, Department of Computer Science and Engineering, KMP College of Engineering, Perumbavoor, Kerala, India

Abstract: ***The interconnected systems are under the threads from the network attack. Denial of service attack is the most common thread. DoS attack attempt to prevent a computer or service from being available. In the proposed system, we present a DoS attack detection system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by analyzing network traffic pattern. Anomaly based detection is used to detect the attack in Multivariate correlation analysis. This help to detect the known an unknown DoS attacks effectively by learning the patterns of legitimate network traffic. Our model is capable of detecting a intrusion whenever an end host performs any of the DOS attack.***

Keywords: Denial-of-Service attack, Network Traffic characterization, Multivariate correlations, Anomaly based detection, Network traffic pattern**.**

1. Introduction

Denial of service [1] attack is one type of attack that attempt to make a machine or network resource unavailable to its user. A DoS attack consists of effort to temporarily suspend the services of a host connected to the internet. DoS attacks degrade the availability of a victim that can be a host, a router, or an entire network. They enforce intensive computation tasks to the victim by exploiting its system vulnerability or flooding it with huge amount of useless packets. The victim can be forceful the service from a few minutes to even several days. This creates serious damages to the services running on the victim system. So, effective detection of DoS attacks is essential to the protection of online services. DoS attack detection mainly focuses on the development of network-based detection mechanisms. Detection systems based on the monitor traffic transmitting over the protected networks.

There are mainly two type of detection system that are host based intrusion detection[4] and network based intrusion detection system. Network-based detection systems are loosely coupled and configuration configurations of network based detection systems are less complicated than that of host-based detection systems. Network-based detection systems can be classified into two main categories, namely misuse based detection systems [2] and anomaly-based detection systems [3].In misuse-based detection systems[6] detect attacks by monitoring network activities and looking for matches with the existing attack signatures. So, misuse-based detection systems are easily evaded by any new attacks and even variants of the existing attacks.

Anomaly based detection, which monitors and flags any network activities presenting significant deviation from legitimate traffic profiles as suspicious objects. Anomaly based detection help to detect the zero day attack. The DoS attack detection system employs the principles of MCA and anomaly-based detection[5]. The proposed system has the capabilities of accurate characterization for traffic behaviors and detection of known and unknown attacks respectively.

2. Related Work

Many system and techniques are used to detect the Dos attack efficiently. Different methods are used to detect the DoS attack. Vern Paxson[2] 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.

Carmen Torrano-Gimenez[3] presented a simple and efficient web attack detection system or Web Application Firewall (WAF). The system is based on the anomaly-based methodology it proved to be able to protect web applications from both known and unknown attacks. The system analyzes input requests and then decides whether they are anomalous or not

D. E. Denning[4] presents powerful real-time intrusion detection capable of detecting a wide range of intrusions related to attempted break-ins, masquerading (successful break-ins), system penetrations, Trojan horses, viruses, leakage and other abuses by legitimate users, and certain covert channels. Yu chin[5] 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.

Theerasak[6] explain about Dos attack is carried out by attack tools like worms, bot net and also 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 mentioned method are used to detect the attack. 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.

3. Proposed System

The overview of our proposed DoS attack detection system architecture is given where the system framework and the sample-by-sample detection mechanism are discussed.

3.1. Framework

There are three phases involved in the detection mechanism. The whole detection phases contain the sample by sample detection.

Firstly basic features of the network traffic are generated from the each individual record. Here the traffic record is generated in a particular time interval. Monitoring and analyzing network at the destination network so the network overhead will reduces in inbound network.

The second step is multivariate correlation analysis. This 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". If there any intrusion occurs then it causes the changes to these correlations so that the changes can be used as indicators to identify the intrusive activities. All the extracted correlations used to replace the original basic features or the normalized features to represent the traffic records. This help to distinguish between the legitimate profile and illegitimate profile.

The step3 consist of anomaly based detection mechanism which is used to perform the decision making. It provides the detection of any DoS attacks without requiring any attack relevant knowledge. There are two phases are involved in the decision making that are training phase and tested phase. "Normal Profile Generation" module is operated under the "Training Phase" to generate profiles for various types of legitimate traffic records. And the generated profiles are stored in the database. The "Tested Profile Generation" module is under the "Test Phase" to build profiles for individual observed traffic records. Then, the tested profiles are transfer to the "Attack Detection" module, which contain normal profiles to compare the result. A threshold-based classifier is employed in the "Attack Detection" module to distinguish the DoS attacks from legitimate traffic.

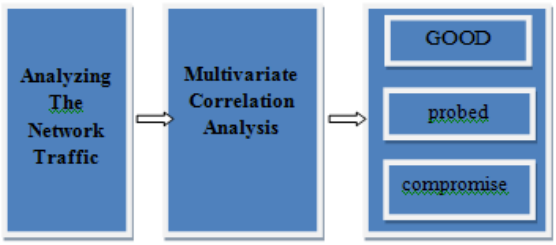

Figure 1: Framework

3.2. Sample by Sample detection

Our system in this paper investigates traffic samples individually. By evaluating the traffic sample individually this offers benefits that are not found in the group-based detection mechanism. For example, (a) attacks can be detected in a prompt manner in comparison with the group-based detection mechanism, (b) intrusive traffic samples can be labeled individually, and (c) the probability of correctly classifying a sample into its population is higher than the one achieved using the group-based detection mechanism in a general network scenario.

4. Multivariate Correlation Analysis

DoS attack traffic behaves differently from the legitimate network traffic, and the character of network traffic is reflected by its statistical properties. To describe these statistical properties, we present a new Multivariate Correlation Analysis (MCA). This MCA approach employs for extracting the correlative information between the features within an observed data object i.e., a traffic record.

MCA approach has following benefits

1. It does not require the knowledge of historic traffic in performing analysis.
2. It provides characterization for individual network traffic records and this enable sample by sample detection.

5. Detection Mechanism

Detection mechanism consist of threshold based anomaly detection whose normal profiles are generated by purely legitimate network traffic records and utilized for future comparisons with new incoming investigated traffic records. The difference between a new incoming traffic record and the corresponding normal profile is examined by the proposed detector. If this dissimilarity is greater than the threshold value then it is considered as attack.

5.1. Normal Profile Generation

MCA approach is applied to analyze the record. Normal profile is used to compare the new incoming traffic pattern. Firstly identify the legitimate traffic pattern. The normal profile is completely based on the legitimate traffic. Certain threshold is sets to identify the legitimate traffic pattern.

5.2. Threshold selection

The threshold given in (16) is used to differentiate attack traffic from the legitimate one.

Threshold = $\mu + \sigma * \alpha$.

The legitimate traffic pattern is set in between the certain threshold. If the traffic is exceed the threshold value then it is considered as an DoS attack.

5.3 Attack Detection

To detect the attack compare the traffic record with the legitimate traffic. There is a large deviation from the legitimate traffic then it is attack.

For the attack detection we are using the threshold analysis. The following algorithm used to identify the attack.
1) Generate the traffic record
2) Analysis the traffic pattern
3) IF (threshold<traffic record) Then
4) return Normal
5) else
6) return Attack.
7) END IF

6. Conclusion

This paper has presented a MCA-based DoS attack detection system and anomaly based detection technique. Our system able to distinguish between both known and unknown DoS attacks from legitimate network traffic. Detection accuracy can be detected in each access point. If any system contains DoS attack it can be accurately identified and reported.

References

[1] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He," A system for denial-of-service attack detection based on multivariate correlation analysis" IEEE transactions on parallel and distributed systems vol:25 no:2 year 2014
[2] V. Paxson, "Bro: A system for detecting network intruders in realtime," Computer Networks, vol. 31, pp. 2435-2463, 1999
[3] Carmen Torrano-Gimenez, Alejandro Perez-Villegas1, and Gonzalo Alvarez, "An anomaly-based approach for intrusion detection in web traffic,"
[4] D. E. Denning, "An intrusion-detection model," IEEE Transactions on Software Engineering, pp. 222-232, 1987.
[5] Yu Chen and Wei-Shinn Ku "Collaborative detection of ddos attacks over multiple network domains," IEEE transactions on parallel and distributed systems, on june 2007
[6] Theerasak Thapngam, Shui Yu, Wanlei Zhou and Gleb Beliakov," Discriminating DDoS Attack Traffic from Flash Crowd through Packet Arrival Patterns" IEEE international conference on 2009

Author Profile

Animol T Joseph received the B.Tech degree in Information Technology from Anna University Chennai in 2012 and currently pursuing final year M. Tech degree in Computer Science and Engineering with specialization in Cyber Security from KMP College of Engineering, Perumbavoor.

Athira Raj received B.Tech in computer Science and M.Tech in Computer Science from Mahatma Gandhi University Kottayam in 2009 and 2012 respectively and currently working as assistant professor in KMP College of Engineering Perumbavoor in Computer Science and Engineering Department