International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Denial-Of-Service Attack Detection Based On Multivariate Correlation Analysis and Triangle Area Map Generation

Heena Salim Shaikh, Parag Ramesh Kadam, N Pratik Pramod Shinde, Prathamesh Ravindra Patil, Prof Amruta Hingmire

Alard College of Engineering and Management, Pune, Maharashtra, India

Abstract: ***In computing, a denial-of-service (DoS) is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. Systems like Web servers, database servers, cloud computing servers etc. are very vulnerable to be attacked by network hackers. Denial-of-Service (DoS) attacks cause disastrous effects on these computing systems. In this paper, a detection system is proposed that detects DoS attacks by using the technique of Multivariate Correlation Analysis (MCA). The technique of MCA is used for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. For attack recognition, proposed system uses the principle of anomaly-based detection. The use of this principle makes it easier for detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only.***

Keywords: Anomaly-based Detection, Denial-of-Service Attack, Detection and Protection, Multivariate Correlation Analysis (MCA), Network Traffic Characterization

1. Introduction

Amongst various online attacks hampering IT security, Denial of Service (DoS) has the most devastating effects. It has also put tremendous pressure over the security experts lately, in bringing out effective defense solutions. These attacks could be implemented diversely with a variety of tools and codes. Since there is not a single solution for DoS, this attack has managed to prevail on internet for nearly a decade. Therefore there is need to develop detection systems which will effectively detect the DoS attacks and will prevent the IT security from getting hampered. These systems will detect the attacks and prevent the system from the adverse effects.

Unlike most other “hacks”, a Denial of Service (DoS) does not require the attacker to gain access or entry into the targeted server. The primary goal of a DoS attack is instead to deny legitimate users access to the service provided by that server. Attackers achieve their DoS objective by flooding the target until it crashes, becomes unreachable from the outside network, or can no longer handle legitimate traffic. The actual volume of the attack traffic involved depends on the type of attack traffic payload used. With crafted payload such as malformed IP fragments, several such packets may be sufficient to crash a vulnerable TCP/IP stack; on the other hand, it may take a very large volume of perfectly conforming IP fragments to overwhelm the defragmentation processing in the same TCP/IP stack. Sophisticated attackers may choose to use a mixture of normal and malformed payloads for a DoS attack. DoS attacks can vary in impact from consuming the bandwidth of an entire network, to preventing service use of a single targeted host, or crashing of a single service on the target host. Most DoS attacks are flood attacks; that is, attacks aimed at flooding a network with TCP connection packets that are normally legitimate, but consume network bandwidth when sent in heavy volume The headers of malicious packets are typically forged, or spoofed, to fool the victim into accepting the packets as if they are originating from a trusted source. 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 amount 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.

In this paper, the DoS attack detection system is proposed which uses the principles of MCA and anomaly-based detection. These principles make the proposed system more efficient because of their capabilities like 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. In the following paper, existing detection systems are discussed and architecture of the proposed system is explained.

2. Proposed System

Existing System

Interconnected systems, such as Web servers, database servers, cloud computing servers etc, are now under threads from network attackers. As one of most common and aggressive means, Denial-of-Service (DoS) attacks cause serious impact on these computing systems.

Disadvantages

This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only.

Proposed System

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 employs the principle of anomaly-based detection in attack recognition[1]. This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only[2]. Furthermore, a triangle-area-based technique is proposed to enhance and to 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. The results show that our system outperforms two other previously developed state-of-the-art approaches in terms of detection accuracy.

Advantages

The results show that our system outperforms two other previously developed state-of-the-art approaches in terms of detection accuracy. Also to find various attacks from the user to avoid Network Intrusion.

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts. True Type 1 or Open Type fonts are required. Please embed all fonts, in particular symbol fonts, as well, for math, etc.

3. System Implementation

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Main Modules:

1. User Module :

In this module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first[5].

2. Multivariate Correlation Analysis :

DoS attack traffic behaves differently from the legitimate network traffic, and the behavior of network traffic is reflected by its statistical properties. To well describe these statistical properties, we present a novel Multivariate Correlation Analysis (MCA) approach in this section. This MCA approach employs triangle area for extracting the correlative information between the features within an observed data object[4].

3. Detection Mechanisms:

We present a threshold-based anomaly detector, whose normal profiles are generated using purely legitimate network traffic records and utilized for future comparisons with new incoming investigated traffic records. The dissimilarity between a new incoming traffic record and the respective normal profile is examined by the proposed detector. If the dissimilarity is greater than a pre-determined threshold, the traffic record is flagged as an attack. Otherwise, it is labeled as a legitimate traffic record[5]. Clearly, normal profiles and thresholds have direct influence on the performance of a threshold-based detector. A low quality normal profile causes an inaccurate characterization to legitimate network traffic. Thus, we first apply the proposed triangle area- based MCA approach to analyze legitimate network traffic, and the generated TAMs are then used to supply quality features for normal profile generation[4].

4. Computational complexity And Time Cost Analysis:

We conduct an analysis on the computational complexity and the time cost of our proposed MCA-based detection system. On one hand, as discussed in, triangle areas of all possible combinations of any two distinct features in a traffic record need to be computed when processing our proposed MCA. The former technique extracts the 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 legitimate network traffic. our system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic.

4. Methodology and Algorithm

The Three Steps used in our project is as below:

Step1: In first phase, the basic information is generated from ingress network traffic to the internal traffic where the servers and traffic records are formed in particular well defined time interval. The destination network is monitored and analyzed, so that the overhead of the detection is reduced. This makes our detector to give best fit protection for the targeted network because the traffic

profiles used by the detectors are developed for small number of network services.

Step 2: In the second phase the multivariate correlate analysis is implemented. The triangle area map is generated which is used to generate the correlation between two distinct server within the record which is taken from the first phase. The illegal entry activities are identified by making hem to cause changes to the correlation. All the triangle area relations stored in triangle area maps (TAMs) are then used to replace the original basic features[4].

Step 3: In phase three the decision making is performed which uses the anomaly based detection system. This gives information about any DoS attacks without the requirement of the relevant knowledge. The lengthy and time consuming attack analysis and misuse based detection are avoided[6].

Multivariate correlation analysis: DoS attack traffic behaves differently from the valid network traffic, and the behavior of network traffic can be found out by its statistical properties. To well describe these statistical properties, we present a novel Multivariate Correlation Analysis (MCA) approach. This MCA approach applies triangle area for generating the correlative information between the features within an observed data object A Triangle Area Map (TAM) is constructed and all the triangle areas are arranged on the map with respect to their indexes. Hence, the TAMi is a symmetric matrix having elements of zero on the main diagonal[7].

5. System Results

Following figures are the output/result of our system.

Figure 1: Home: The first page is the login window. The user can sign in by entering respective email id and password.

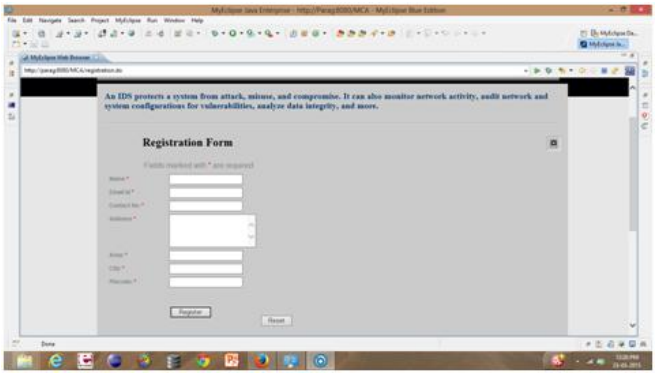

Figure 2: Register- User can register themselves with MCA by filling the details required in registration form .

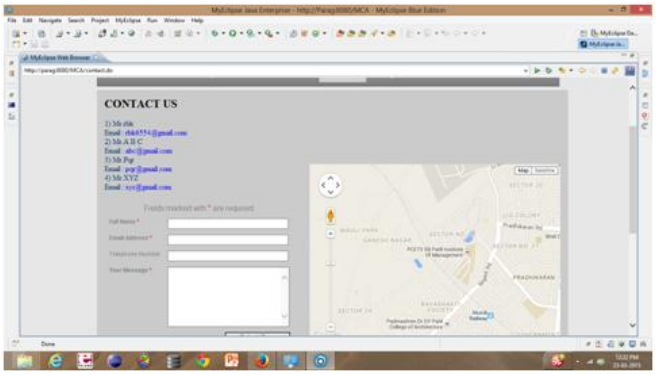

Figure 3: Contact us: – Here email ids are provided for any help & queries. Also user can report problem by just providing name, email address and message regarding error.

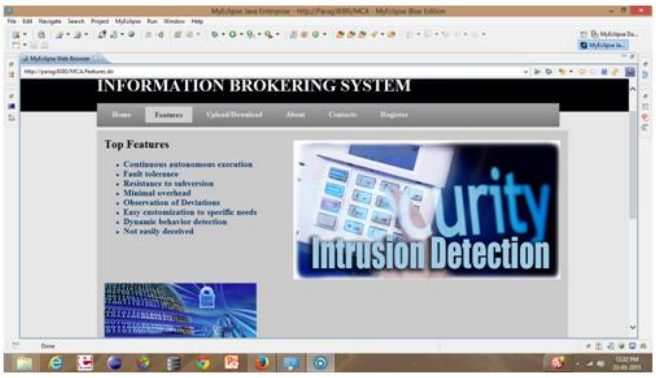

Figure 4: Features - features shows specialty of our MCA.

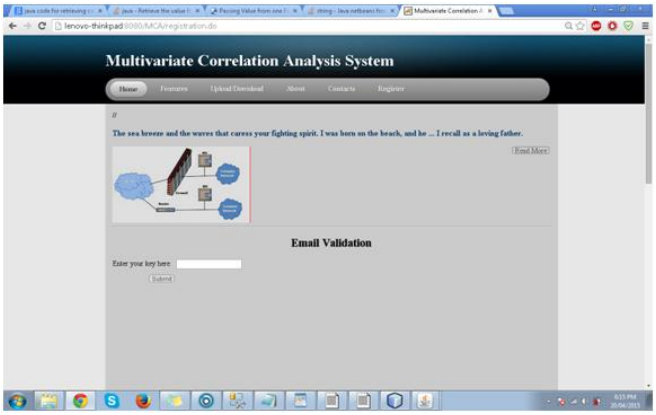

Figure 5: Email validation - After registering ourselves with MCA email validation is carried out. Here we have to enter key which is provided to the user by email. Key is generated automatically and registered user can get key

from their email only. If email does not exist then it will automatically report an error at the same time.

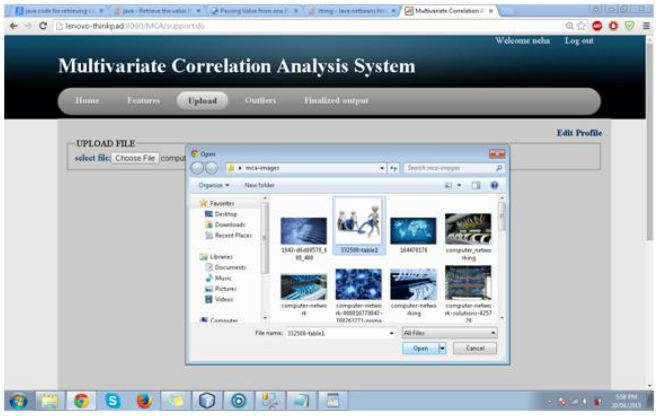

Figure 6: Upload: - User can select the file which he wants to upload by browsing it. After the selection the upload button is used to upload it on the web.

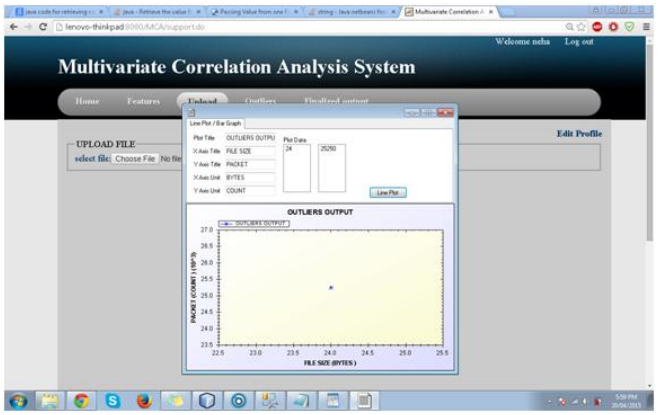

Figure 7: Our system will check the uploaded file by analyzing the report.

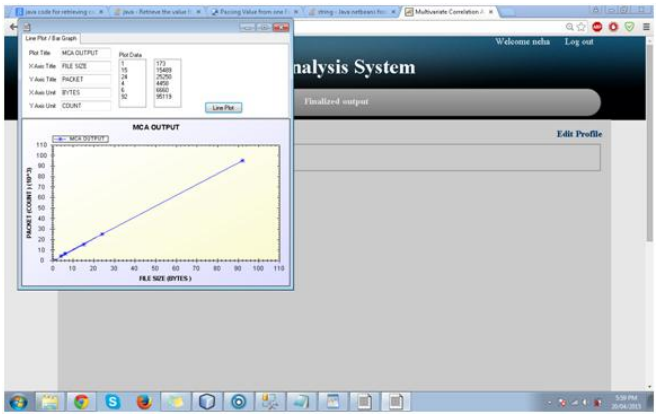

Figure 8: If file does not contain any malicious content it will be uploaded successfully else error can occur & will not be processed any more.

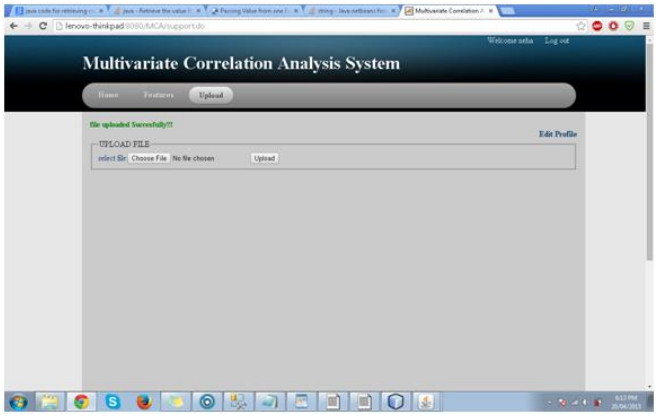

Figure 9

6. Conclusion

With the number of DoS attacks increasing over the past years and many online services are becoming victims of these attacks, it is important that network engineers, designers, and operators build services in the context of defending against DoS attacks. The main intention of DoS attacks is to consume resources, such as memory, CPU processing space, or network bandwidth, in an attempt to make them unreachable to end users by blocking network communication or denying access to services. Thus in this paper a MCA-based DoS attack detection system is developed which is powered by the triangle-area based MCA technique and the anomaly-based detection technique. The MCA technique extracts the 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 Anomaly-based detection technique facilitates the system to be able to distinguish both known and unknown DoS attacks from legitimate network traffic.

References

[1] 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.

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

[3] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Cost based modelling 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.

[4] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Triangle- Area-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.

[5] 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.

[6] 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.

[7] 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