ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Design and Implementation of a System for Denial of Service Attack Detection Based on Multivariate Correlation Analysis

Priti G. Harne[1] , Prof.V.M.Deshmukh[2]

Student of M.E., Department of Information Technology, Prof. Ram Meghe Institute of Technology & Research, Badnera, Amravati, India[1].

Head of the Dept., Department of Information Technology, Prof. Ram Meghe Institute of Technology & Research, Badnera, Amravati, India[2]

ABSTRACT: The reliability and availability of network services are being threatened by the growing number of Denial-of-Service (DoS) attacks. Effective mechanisms for DoS attack detection are demanded. Therefore, 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. the application of Multivariate Correlation Analysis(MCA) where SVM(Support Vector Machine) is used to Train the data & it classify the data/attack. Clustering is use for the alert aggregation process. Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis is a generative modelling approach using probabilistic methods.MCA-based DoS attack detection system employs the principle of anomaly detection and misuse based detection in attack recognition. This makes, solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only & also detecting various types of viruses. this system also checking for conditional privileges like packet level intruder, process level intruder etc.Furthermore, The effectiveness of propose detection system is evaluated using KDD Cup dataset.

KEYWORDS: Denial-of-Service, multivariate correlations, Misuse and Anomaly detection technique.

I. INTRODUCTION

Denial-of-Service (DoS) attacks cause serious impact on the computing systems. Denial-of-Service (DoS) attacks is an attempt to make a machine or network Resources unavailable to its intended users. Dos attacks severely degrade the availability of a victim, which can be a host, a router, or an entire network. the availability of network services is seriously threatened by the continuously increasing number of DoS attacks. thus effective mechanisms for DoS attack detection are highly demanded. Denial of service attack is basically done in order to block a node from receiving legitimate data or to block the node completely from another legitimate node. This blocking can be done either with the data sent continually or by sending radio signals.Dos attack affect on Software System ,Network Router,Server and End-User PCs.The attack aims to deny or degrade normal services for legitimate users by sending huge traffic to the victim (machines or networks) to exhaust services, connection capacity or the bandwidth. Denial of service attack severely degrades the efficiency of the online services. Therefore effective detection of dos attack is essential to the protection of the online services. The DOS attack detection, mainly focuses on the development of the network-based detection mechanism. The detection system employs two approaches namely misuse detection[1] and anomaly detection[2].

To protect online service from DoS attack here present a DOS attck detection system that uses Multivariate Correlation Analysis for accurate network traffic characterization by extracting the geometrical correlations between network traffic features .the application of Multivariate Correlation Analysis(MCA) where SVM(Support Vector Machine) is used to Train the data & it classify the data/attack.Clustering is use for the alert aggregation process. Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis is a generative modeling approach

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

using probabilistic methods. Server module is the main module for this project. This module consists of four layers viz. sensor layer (which detects the user/client etc.), Detection layer, alert processing layer and reaction layer. In addition there is also Message Log, where all the alerts and messages are stored for the references. This Message Log can also be saved as Log file for future references for any network environment. we aim at modeling these processes using approximative maximum likelihood parameter estimation techniques. Thus, the beginning as well as the completion of attack instances can be detected.and tested the system with the misuse based anomaly detection technique.Moreover benefiting from the principal of anomaly detection ,DoS attack detection approach is independent on prior knowledge of attack and is capable of detecting both known and unknown DoS attacks. in this system also detected various types of viruses. this system also checking for conditional privileges like packet level intruder, process level intruder etc.and also we extend this work by sending the Alerts as Message to the Network Administrator who governs the Network or Attack Detection System.

II. RELATED WORK

As Denial of service attack is increasing day by day and makes the availability of service to deny from actual users. Many techniques are developed to detect denial of service attack. Some methods involve misuse based detection systems and some methods involve anomaly-based detection systems.

Bro: A system for detecting network intruders in real-time [1] by *V. Paxsonis*, is an individual system for detecting network intruders in real-time by reflexively monitoring a network connection over which the intruder's traffic travels. It involves two principles. Event engine and policy script interpreter. In event engine the series of higher level events are normalized by a kernel filtered network traffic stream. And in policy script interpreter, event handlers which are written in a specialized language used to express a site's security policy are interpreted. Event handlers can update state information, synthesize new events, record information to disk, and generate real-time notifications via syslog. But this BRO technique does not monitor actively terminating misbehaving connections by sending RST packets to their end points. And it does not monitor the communication with intermediary routers

Fast entropy computation method [3] by *Giseop No and Ilkyeun Ra, Denver*, to detect dos attack tells that the compression entropy method is not suitable for validating real network attacks and creates many false negatives. But proposed fast entropy approach that can overcome the problem of false negatives and will not increase the computational time. This DoS attack detection method considerably increases detection accuracy and decreases computational time using fast entropy approach which has better performance in speed as well as accuracy. But this fast entropy computation method doesn't reduce the false positives and false negative rate much.

Collaborative detection of DoS attacks over multiple network domains [4] by *Yu Chen, Kai Hwang, and Wei-Shinn Ku*, is one more approach to detect DoS flooding attacks at the traffic flow level. In this, change aggregation tree (CAT) is developed by distributed change-point detection (DCD) architecture. The detection of unexpected traffic changes over multiple network domains at the earliest time is incorporated.

In,Xiang et al [5]had proposed using two new information metrics such as the generalized entropy metric and the information distance metric to detect low-rate DDoS attacks by measuring the difference between legitimate traffic and attack traffic. As the proposed metrics can increase the information distance (gap) between attack traffic and legitimate traffic, they can effectively detect low-rate DDoS attacks early and reduce the false positive rate clearly.

Huang et al. in[6] introduced a new type of denial of service attack to wireless networks: distributed jammer network (DJN), which is made of a large number of low-power, tiny radio jammers. Recent advancements in MEMS and NANO technologies made it possible to build nano-scale jammers that can be deployed in quantities of tens of thousands if not more. Jamming attack on wireless networks was traditionally treated from the perspective of individual jammers.

Theerasak[7] 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

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.

Garg et al.discussed various detection algorithms which are using data mining concepts & algorithms for DDoS detection & prevention.[8] author presents various significant areas where data mining techniques seem to be a strong candidate for detecting and preventing DDoSattack.DDoS attacks are quite complex methods of attacking a computer network, ISP, Individual system make it ineffectual to legitimate network users.

Tan et al. Proposed a DoS attack detection system that uses Multivariate Correlation Analysis (MCA) foraccuratenetwork traffic characterization by extracting the geometrical correlations between network traffic features[9]. Our MCA-basedDoS attack detection system employs the principle of anomaly-based detection in attack recognition. This makes our solution capableof detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. Furthermore, atriangle-area-based technique is proposed to enhance and to speed up the process of MCA.

III.PROPOSED SYSTEM ARCHITECTURE

Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis is a generative modeling approach using probabilistic methods. Server module is the main module for this project. This module consists of four layers viz. sensor layer (which detects the user/client etc.), Detection layer, alert processing layer and reaction layer. In addition there is also Message Log, where all the alerts and messages are stored for the references. This Message Log can also be saved as Log file for future references for any network environment. we aim at modeling these processes using approximative maximum likelihood parameter estimation techniques. Thus, the beginning as well as the completion of attack instances can be detected.Lets discuss about different Layers…

- Sensor Layer : Sensor Layer which gives the information about active nodes in network. Activated nodes can be displayed in sensor layer
- Detection Layer : attack is detected using MCA where SVM(Support Vector Machine) is used to Train the data & it classify the data/attack, Feature Comparison can be done by using Euclidean Distance by calculating the correlation of the parameters.
- Alert Processing Layer : Gives the alert if any attack is detected. Alert aggregation is done for different attack. So the alerts aggregated. Clustering is use for the alert aggregation process.
- Reaction Layer : Reaction Layer contains Reporting and attack Prevention mechanism.[10][11]

Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis does not degrade system performance as individual layers are independent and are trained with only a small number of features, thereby, resulting in an efficient system.Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis is easily customizable and the number of layers can be adjusted depending upon the requirements of the target network.Our framework is not restrictive in using a single method to detect attacks. Different methods can be seamlessly integrated in our framework to build effective intrusion detectors.Our framework has the advantage that the type of attack can be inferred directly from the layer at which it is detected.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

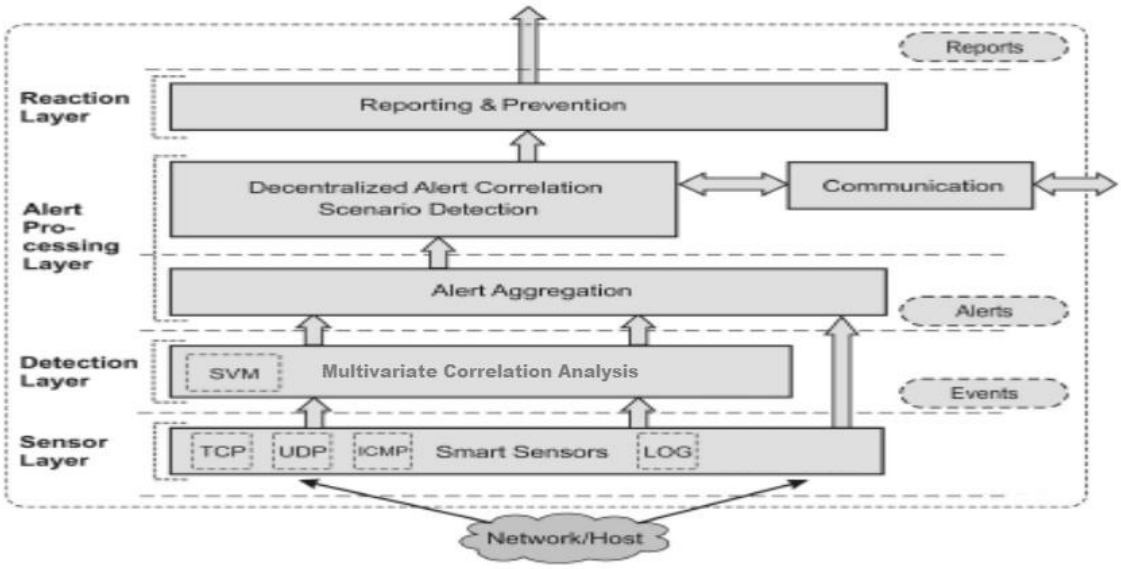

Figure1: Architecture Diagram:Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis

IV. SYSTEM COMPONENTS

A.Server

Server module is the main module for this project. This module acts as the Intrusion Detection System. This module consists of four layers viz. sensor layer (which detects the user/client etc.), Detection layer, alert processing layer and reaction layer. In addition there is also Message Log, where all the alerts and messages are stored for the references. This Message Log can also be saved as Log file for future references for any network environment.

B. Client

Client module is developed for testing the Intrusion Detection System. In this module the client can enter only with a valid user name and password. If an intruder enters with any guessing passwords then the alert is given to the Server and the intruder is also blocked. Even if the valid user enters the correct user name and password, the user can use only for minimum number of times. For example even if the valid user makes the login for repeated number of times, the client will be blocked and the alert is sent to the admin. In the process level intrusion, each client would have given a specific process only. For example, a client may have given permission only for P1process. If the client tries to make more then these processes the client will be blocked and the alert is given by the Intrusion Detection System. In this client module the client can be able to send data. Here, when ever data is sent Intrusion Detection System checks for the file. If the size of the file is large then it is restricted or else the data is sent.

C. KDD Dataset

This module is integrated in the Server module. This is an offline type of testing the intrusions. In this module, the KDD Data Set is used to check the technique of the DOS attack with Generative Data Stream Modeling. The KDD data set is downloaded and separated according to each layers. So we test the instance of KDD Dataset using the open file dialog box. Whenever the dataset is chosen based on the conditions specified the DOS Attack Detection System works.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

D. 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. This MCA approach employs triangle area for extracting the correlative information between the features within an observed data object.

E. Attack Simulation

In this module, the attack simulation is made for ourself to test the system. Attacks are classified and made to simulate here. Whenever an attack is launched the Intrusion Detection System must be capable of detecting it. So our system will also be capable of detecting such attacks. For example if an IP trace attack is launched, the Intrusion Detection System must detect it and must kill or block the process.

V. EXPERIMENTAL RESULTS

Different methods are used to demonstrate the feasibility of the proposed architecture. The first method is conditional privileges & second contains Attack simulation tests. All the experiments were conducted on an PC with 2.4 GHz and 2 GB of RAM.

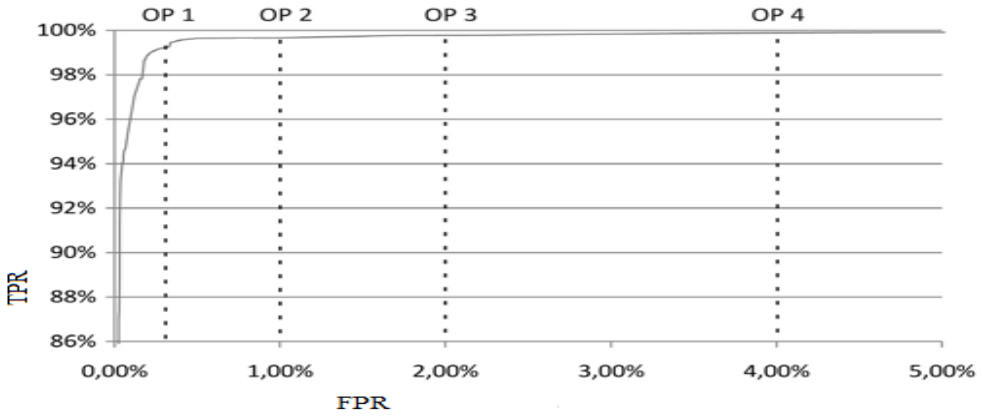

Figure 2. ROC curve for the SVM detector.

The ROC curve in Fig. 2 plots the true positive rate (TPR, number of true positives divided by the sum of true positives and false negatives) against the false positive rate (FPR, number of false positives divided by the sum of false positives and true negatives) for the trained SVM. Each point of the curve corresponds to a specific threshold. Four operating points (OP) are marked. OP 1 is the one with the smallest overall error, but as we want to realize a high recall, we also investigate three more operating points which exhibit higher TPR at the cost of an increased FPR.

A. Real time Attacks :

User level privileges *:* The system is tested with various set of username and passwords. For each pair of valid username and password the system allowed user to access the system. Also for wrong username and password the intrusion detection system detected as intruder and blocked the user.

Process level privileges*:* All legitimate user allowed to access the system and to execute certain process say P1 & P 2.If user tried to access process other than P1 & P 2; say P3,P4 etc, the IDS detected it as process level intruder and blocked the process. Also proper alert is generated at different layers.

Packet Level privileges*:* Users are allowed to transfer data with certain limitations. System is tested with various size packets. For each transfer which is within certain size limitation is allowed. The file transfer exceeding the limitation is aborted and proper alert is generated.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

B. Attack Simulation*:*

Simulation attacks are categorized as Flooding (DOS,Buffer overflow), Malware (viruses, worms, Trojan horses) attack. For each type of attack, Attack detection system responded properly and alerts are generated.

C. Alert Aggregation*:*

Alerts are generated at various levels of Attack detection system. These alerts are aggregated andstored in a database. These alerts can be easily accessed by the system admin. Log files provide useful information about attacks and the reactions by the intrusion detection system. These are stored for future reference.

For all the experiments Attack detection system responded properly and alerts are generated.

Example for alert aggregation task:

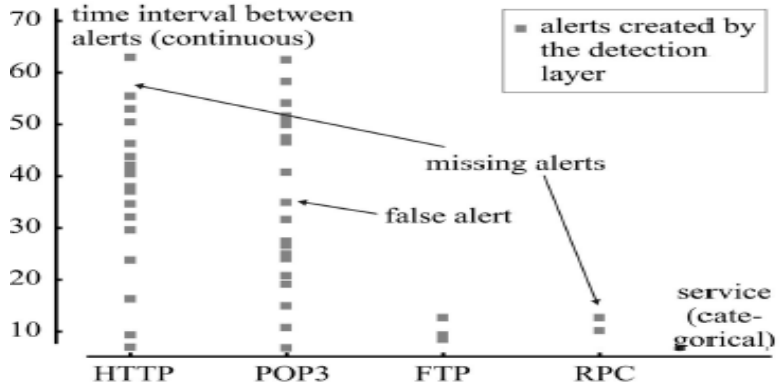

Figure 3: Actual observations: The alerts produced by a real detection layer. The task of the alert aggregation reconstruct the attacksituation by means of these observations only (including false alerts).

Table 1: Benchmark Results

OP	p[%]	tavg[ms]	r[%]
KDD DATA			
Idealized	100	0.12	99
OP1	100	0.18	98
OP2	99.02	0.97	99.46
Real-Time Attacks			
Idealized	100	0.12	99
OP1	74	0.19	99.27
OP2	60	0.29	79
Attack Simulation			
Idealized	100	0.12	99.89
OP1	100	0.12	81
OP2	99	0.19	61

*D.*Description of the Benchmark Data Sets

Percentage of detected instances (p): The percentage of detected attack instances p can thus be determined by dividing the number of instances that are detected by the total number of instances in the data set. The measure is computed with respect to the instances covered by the output of the detection layer, i.e., instances missed by the detectors are not considered.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Average runtime(Tavg): The average runtime is measured in milliseconds per alert. Assuming up to several hundred thousand alerts a day, Tavg should stay clearly below 100 ms per alert.

VI. CONCLUSION AND FUTURE WORK

Denial of Service (DOS)attacks constitute one of the greatest problem in network security. It is challenging to accurately detect denial of service(DoS) attack quickly. Here propose a new , multivariate correlation analysis based denial of service attack detection system with the misuse based anomaly detection technique.Most of the present existing Attack Detection System does not have a generalized framework. Our proposed architecture is similar to layers, so according to the network environment, the network administrator can add or remove the layers. If a new updated version of detection comes in future, then it will be very easy to add the layer with our proposed system. We also tested our system by launching various attacks to the system, and we found how the system detects and reacts according to the developed IDS. Evaluation has been conducted using KDD Cup dataset to verify the effectiveness and performance of the propose DoS attack detection system. In future, we will further evaluate the proposed technique on the task of DoS attack detection using Support Vector Data Description (SVDD) technique, which is believed to be more promising in one-class classication than SVM and NN techniques and Packet level alert agent is limited to upload small amount of data, in future this can be extended to large amount of data.

REFERENCES.

1. V. Paxson, "*Bro: A System for Detecting Network Intruders in Real-Time*,"The Proceedings of the 7th USENIX Security Symposium San Antonio, Texas, January 26-29, 1998
2. P. Garcia-Teodoro ,J. Diaz-Verdejo, G. Macia-Fernandez, E. Vazquez "*Anomaly-based network intrusion detection:Techniques, systems and challenges*," computers & security 2 8 (2009) 1 8 – 2 8
3. Giseop and Ilkyeun Ra, "*An Efficient and Reliable DDoS Attack Detection Using a Fast Entropy Computation Method*" ISCIT 2009.
4. Yu Chen, Kai Hwang and Wei-Shinn Ku*"* Collaborative Detection of DDoS Attacksover Multiple Network Domains" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, TPDS-0228-0806.2007
5. Y. Xiang, Ke Li, and W. Zhou"*Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics*" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011
6. H. Huang,N.Ahmed, and P. Karthik "*On a New Type of Denial of Service Attack in Wireless Networks:The Distributed Jammer Network*" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 10, NO. 7, JULY 2011
7. TheerasakThapngam, Shui Yu, Wanlei Zhou and GlebBeliakov," Discriminating DDoS Attack Traffic from Flash Crowd through Packet Arrival Patterns" IEEE international conference on 2009
8. K. Garg 1 , R. Chawla"*Detection Of Ddos Attacks Using Data Mining*"International Journal of Computing and Business Research (IJCBR) ISSN (Online) : 2229-6166 Volume 2 Issue 1 2011
9. Zhiyuan Tan, ArunaJamdagni, Xiangjian He, PriyadarsiNan"*A System for Denial-of-Service Attack DetectionBased on Multivariate Correlation Analysis*" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:25 NO:2 YEAR 2014
10. Alexander Hofmann and Bernhard Sick, "*Online Intrusion Alert Aggregation with Generative Data Stream Modeling*", IEEETransactions on Dependable and Secure Computing, Vol. 8, No. 2, March – April 2011.
11. Kapil Kumar Gupta, BaikunthNath and RamamohanaraoKotagiri, "*Layered Approach using Conditional Random Fields for Intrusion Detection*", IEEE Transactions on Dependable and Secure Computing, Vol.7, No.1, January-March 2010.