Anomaly Based Approach for Defending Denial of Service Attack in Web Traffic

R.Ramkumar[1], R.Rahul[2], Sri Gowtham[3]
[1,2]UG Student, [3]Asst.Professor
Department of CSE, Bharath University, Chennai.

Abstract— Distributed Denial of Service (DDOS) attacks has become a great threat for internet security. This attackis an advanced form of DOS (Denial of Service) attack. This attack changes its whole origin ID and it gives trouble to find it out and it has become a serious threat for internet security.

Almost all traditional services such as bank websites, power resources, medical, educational institutions and military are extended to World Wide Web and thus many people widely use internet services. As many users of Internet is mandatory, network security for attacks are also increasing. Current DDoS attacks are carried out by hacking tools, viruses and botnets using different packet-transmission strategies and various forms of attack packets to beat defense system networks. These problems lead to defense system network requiring various detection methods in order to identify attacks. But DDoS attacks can mix their traffics during flash crowds. By doing this, the network of defense systems cannot detect the attack traffic in time. Denial of service (DOS) attack is potential damaging attack which degrades the performance of online servers in no time. This attack performs an intensive attack on the target server by flooding it with large useless packets. Our Triangular MCA-based DoS attack detection system employs the principle of anomaly based detection in attack recognition. To cope with such damaging attacks becomes challenge for the researchers. Preventing and avoiding this attack mainly focuses on the development of network-based detection mechanisms. Detection systems based on these techniques monitor traffic transmitting over the protected networks. This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. In this paper Detection of denial of service attack is done using anamoly based approach, multivariate correlation analysis.

Key Terms: Anomaly Approach, Distributed Denial of Service Attack, DDOS Attack.

I. INTRODUCTION

Web applications are becoming increasingly popular and complex in all sorts of environments, ranging from ecommerce applications to banking. As a consequence, web applications are subject to all sort of attacks. Additionally, web applications handle large amounts of confidential and important data, which attracts malicious users to hack. The effects of many attacks may be disastrous [1], like identity supplanting, sensitive data hijacking, access to unauthorized information, web page's content modification, command execution, etc. Therefore it is fundamental to protect web applications and to adopt the suitable security methods.

Unfortunately, conventional firewalls, operating at network and transport layers, are usually less effective to protect against web-specific attacks. To be really effective, the detection is to be moved to the application layer.

Today internet has become increasingly important to current society. Almost all traditional services such as bank websites, power, medical, educational institutions and defense networks are extended to Internet now and thus many people widely use Internet. As many people of using Internet is raised, network security for attacks are also constantly increasing. All computer systems have to suffer from security vulnerabilities which are both technologically difficult and economically costly to be solved by the manufacturers. Secure communication has some desirable security aspects such as confidential, authenticated, message integrated. But more people are aware of that availability and access control are also urgent requirements of secure communication because of the notorious DDoS (Distributed Denial of Service) attack that utilizes adequate puppet computers to lunch the coordinated attack on targeted sites.

An Intrusion Detection System (IDS) analyzes information from a computer or a network to detect malicious actions and behaviors that can compromise the security of a computer system. When a malicious behavior is detected, an alarm is launched. IDS's have been classified as either signature detection systems (also called negative approach) or anomaly detection systems (positive approach). An hybrid intrusion detection system combines the technique with an couple of approaches. The signature-based approach looks for the signatures of known attacks (misuse of the system resources), which exploit weaknesses in system and application software. It uses pattern matching techniques against a frequently updated database of attack signatures. It is useful to detect already known attacks or their slight resemblance, but not the new ones or malicious variations that defeat the pattern recognition engine.

The anomaly-based approach looks for behavior or use of computer resources deviating from “normal” or “common” behavior [1]. The underlying principle of this approach is that “attack behavior” differs enough from “normal user behavior” thus it can be detected by cataloging and identifying the differences involved. First, the “normal” behavior must be well defined, which is not an easy task. Once normal behavior is fully qualified, irregular behavior will be tagged as intrusive.

Intrusion detection which classifies the attacks on the Internet from usual behavior of usage on the Internet networks. Now the intrusion detection systems are vital tool in the cluster environment fight to keep its computing resources secure .It is an unavoidable portion of the information security system. Enormous application oriented system over the Internet such as online shopping, net banking, trading stocks and foreign exchange and online auction have been improved. Moreover, open access platform of the Internet system, computer systems and data is always at risk under some security issues. Extreme growth of the Internet network has prompted network intrusion detection to create a vital component of infrastructure protection mechanisms. Network intrusion detection can be identified by a set of malicious actions which may threaten the availability of a network resource, integrity, confidentiality, security.

Intrusion detection conventionally categorized in to misuse detection and anomaly detection. Misuse detection mainly focuses for specific patterns or sequences of programs and user behaviors that match well-known intrusion scenarios. Anomaly detection develops a system of normal network functions, and attacks are detected by evaluating significant deviations from the normal behavior of the user. The advantage of intrusion detection is that it may detect rare intrusions that have not been observed yet.

In this paper, we have proposed the multi-variate correlation analysis techniques and anomaly detection based approach for efficient detection of DDOS attacks. an algorithm has been proposed to discriminate DDOS attacks from flash crowds by analyzing the flow correlation coefficient among suspicious flows. Although this approach improves detection accuracy and it is vulnerable to attacks that linearly change all monitored features. This approach can only label an entire group of observed samples as legitimate or attack traffic but not the individuals in the group. To overcome this problem, we propose nonpayload-based DoS detection approach using multivariate correlation analysis (MCA).

II. Related Work

The increased occurrences of security threats and increased damage by DDoS attacks have motivated the development of different attack detection techniques. These approaches vary depending on their goal of detection and set of rules required for operation. Many of these methods are based on identifying anomalies in network traffic.

Karimazad and Faraahi [6] proposed an anomaly based DDoS detection method based on features of attack packets, finding them using Radial Basis Function (RBF) neural networks. Vectors with seven features are used to activate an RBF neural network and classify traffic into normal and DDoS attack traffic classes. They evaluated the approach using UCLA Datasets. That system can be classified by normal or attack, but that cannot be distinguished and identified what types of attacks.

In [2], the correlation between the outgoing and incoming traffic of a network is analyzed and the changes in the correlation are used to detect DDoS attack. Fuzzy classification is used in their method in order to guarantee the accuracy. Their method is evaluated using DARPA datasets. In [5], a combined data mining approach is used to classify the traffic pattern to normal and different attacks. This approach is used decision tree to select important attributes and neural networks are exploited to analyze the selected attributes. Limwiwatkul and Rungsawang [4] proposed to discover DDoS attack signatures by analyzing the TCP/IP packet header against well-defined rules and conditions, and separating the difference between normal and abnormal traffic. The authors mainly focus on ICMP, TCP and UDP flooding attacks.

In [11], this approach is a statistical approach based on several features values. The proposed system only showed features extraction module and saved these features into database to identify normal and attack packets. In [12], the proposed system is a combined data mining approach to detect protocol anomaly against DDoS attack. In this paper, traffic features are extracted from network traffic and then it is clustered into normal and attack traffic by using a data mining classification algorithm. This paper only shows detection phrase using only proposed algorithm. Now, in current paper, the proposed system presents a hybrid method using proposed packet classification algorithm and K-NN. The results show that the accuracy comparison using K-NN only and using both proposed algorithm and K-NN.

III. Experimental analysis

The overview of proposed work is discussed here with framework and sample by sample detection.

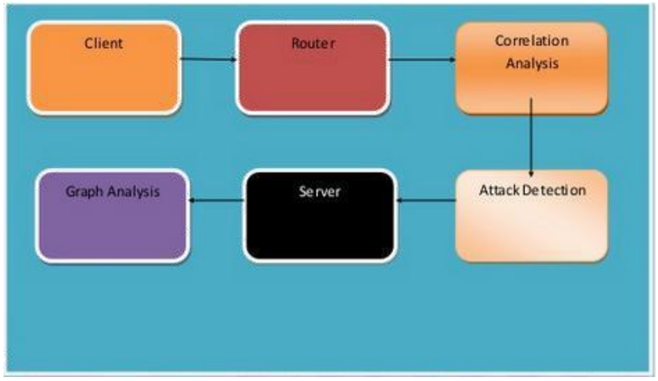


Figure3.1: Process Flow Design

Intrusion detection conventionally categorized in to misuse detection and anomaly detection. Misuse detection mainly focuses for specific patterns or sequences of programs and user behaviors that match well-known intrusion scenarios. Anomaly detection develops a system of normal network behaviors, and intrusions are detected by evaluating significant deviations from the normal functions of the user. The merit of anomaly detection is that it may detect rare intrusions that have not been observed yet.

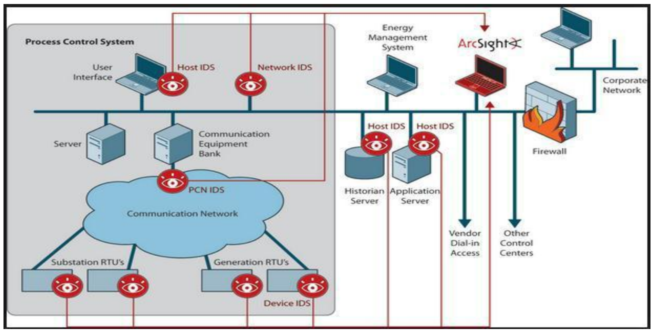


Figure 3.2: Analysis and Identification of Threads

In this paper, we have proposed the multi-variant correlation analysis techniques and anomaly detection based approach for efficient detection of DDOS attacks. an algorithm has been proposed to discriminate DDOS attacks from flash crowds by analyzing the flow correlation coefficient among suspicious flows. Although this approach improves detection accuracy and it is vulnerable to attacks that linearly change all monitored features. This approach can only label an entire group of observed samples as legitimate or attack traffic but not the individuals in the group. To overcome this problem, we propose nonpayload-based DoS detection approach using multivariate correlation analysis (MCA).

The complete detection mechanism involves three phases. The sample by sample detection mechanism is involved in the three phases.[2] In phase one basic information is created from ingress network traffic to the internal traffic where the servers and traffic records are formed in particular well defined time. The targeted network is monitored and analyzed, so that the overhead of the detection is reduced [3]. 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 networks. [2] In the second phase the multivariate correlate analysis is implemented. The triangle area map is generated which is used to extract the correlation between two distinct server within the record which is taken from the first phase. The attack activities are identified by making hem to cause changes to the correlation, with the help of these changes intrusions can be detected. All the triangle area correlations stored in triangle area maps (TAMs) are then used to replace the original basic features. This provides us with better information to sort out the legitimate and illegitimate traffic records.

In phase three the decision making is done using the anomaly based detection system. This gives information about any DoS attacks without the requirement of the required knowledge. The labour intensive attack analysis and misuse based detection are negotiated. Two techniques are involved in decision making (i.e. the training phase and test phase). The training phase consists of “Basic Profile Generation” which is used to generate profiles for various types of legitimate traffic records and these profiles are stored in the database. During the test phase the “Tested Profile Generation Module” builds profiles for individual traffic records, which are then moved over to the intrusion detection module. This does the task of comparing the individual tested profile with respective stored normal profile. In attack detection module threshold –based classifier is used to distinguish the DoS attack from legitimate traffic.

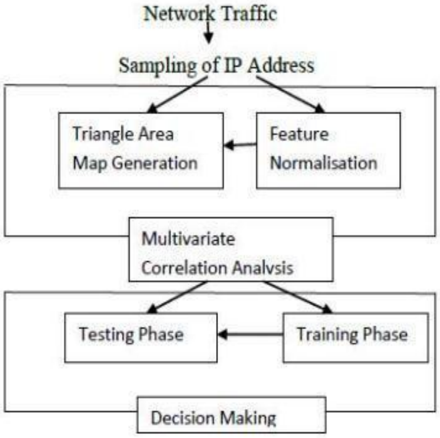


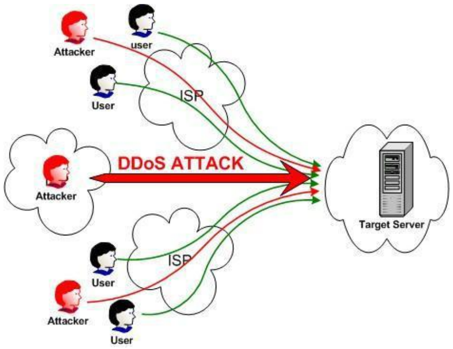
Figure: 3.3 Denial of Service Framework

It is systematically proved that the group-based detection mechanism maintained a higher probability in classifying a group of sequential network traffic samples than the sample-by sample method. The identity was based on an assumption that the samples in a tested group were all from the same distribution [3]. This restrictions in the applications of the group based detection to limited attacks, because intrusion occur unexpectedly in general and it is difficult to obtain a group of sequential samples only from the same distribution. To avoid this restriction, our system in this paper investigates traffic samples individually. This gives 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) attack 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 [3].

A. *Sample by Sample Detection*

Sample by sample detection serves as the basis for a wide range of IP network operations and engineering tasks such as problem solving, accounts and user profiles. It measures and supervising is done by capturing every packet traversing a router interface or a bond. With today's increased data transfer links, an approach is no longer feasible due to the excessive overheads it occurs. As a result, packet sampling has been suggested as alternative addressing .The rate of arrival of packets in a network. However, it has been shown [15] that system network traffic exhibits periodic cycles or bonds. The criteria [15] and other studies have been that not only does network traffic exhibit strong bond in the audit data but the trend also tend to increasing term. The least squares predictor is utilized for predicting the free time. The adopter has adopted the capability to follow .This describing the sampling algorithm.



Let us assume the vector Z hold the values of the N values, such that ZN is the most recent sum and Z1 is the oldest sample. Having fixed a window size of N, when sample occurs, the vector is right shifted such that ZN replaces ZN−1 and Z1 is discarded. The weighted prediction model therefore predicts the value of ZN given ZN−1, ...,Z1. we can express this predicted value as a function of the N past samples i.e.,

Let us assume that the vector Z holds the values of the N samples, such that ZN is the sample and Z1 is the sample. H fixing a size of N, the sampling occurs; the vector is shifted ZN replaces ZN−1 and Z1. The predictioned model therefore predicts the value. This predicted value as a function of the N past samples i.e.,

$$\hat{Z}_N = \alpha^{\mathbf{T}} \tilde{\mathbf{Z}},$$

where ˆ ZN is the new predicted value, ˜Z is the vector of past N − 1 samples, and αT is a vector of predictor coefficients distributed such that newer values have a greater impact on the predicted value ˆ ZN. A second vector, t, records the time that each sample is taken and is shifted . The objective of pridictioned algorithm is to find an appropriate coefficient vector, αT , such that the following summation is minimized.

$$S = \sum_{i=1}^{N-1} w_i \left(Z_i - \hat{Z}_i \right)^2,$$

Where $\mathbf{W} = \mathbf{w}^{\mathbf{T}}\mathbf{w}$ is a $(N-1) \times (N-1)$

$$w_i = \frac{1}{(t_N - t_i)} \left(\frac{1}{\left| Z_i - \hat{Z}_i \right|^2 + \eta} \right), 1 \le i \le N-1, \quad (4)$$

This detection mechanism maintained in a higher probability in classifying a sequential network traffic than the sample-by-sample detection mechanism .This restricts the applications of the group-based detection , The attacks occur in general and it is difficult to obtain a group of sequential samples only exists. System in this paper investigating traffic samples separately. It benefits that are not criticized in this detection mechanism.1.This attacks can be detecting in this detected mechanism.2.The intrusive traffic samples are as more than one .3.Correctly classified as a sample to its populated higher than the one achieved using the group-based detected mechanism. We illustrate them through a mathematical example which assumes traffic samples are independent and identically distributed and legitimate traffic and illegitimate traffic follow normal distributions X1 ~ Y(μ1,σ2 1) and X2 ~ Y(μ2,σ2 2) . The group-based labeling are used to identify the correct distribution for the individuals from a group of k independent samples. The threshold value for classifying a sample into one of the two distributions Y (μ1,σ21) and

Y(μ2,σ2). The sample by sample labeling can always achieve better detection precision than the group-based labeling.

IV. EXPERIMENTAL RESULTS

A. *Multivariate Correlation Analysis:*

In statistics, the coefficient of multiple correlations is a measure of how well a given variable can be predicted using a linear function of a set of other variables. It is measured by the square root of the coefficient of determination, but under the particular assumptions that an intercept is included and that the best possible linear predictors are used, whereas the coefficient of determination is defined for more general cases, including those of nonlinear prediction and those in which the predicted values have not been derived from a model-fitting procedure. The coefficient of multiple correlation takes values between zero and one; a higher value indicates a better predictability of the dependent variable from the independent variables, with a value of one indicating that the predictions are exactly correct and a value of zero indicating that no linear combination of the independent variables is a better predictor than is the fixed mean of the dependent variable.

The square of the coefficient of multiple correlation can be computed using the vector $\mathbf{c} = (r_{x_1y}, r_{x_2y}, \dots, r_{x_Ny})^\top$ f correlations r_{x_n y} between the predictor variables x_n (independent variables) and the target variable y (dependent variable), and the correlation matrix R_{xx} of inter-correlations between predictor variables. It is given by

$$R^2 = \mathbf{c}^\top R_{xx}^{-1}\,\mathbf{c}$$

Where $\mathbf{c}^\top$ is the transpose of C, and R_{xx}^{-1} is the inverse of matrix.

$$R_{xx} = \begin{pmatrix} r_{x_1x_1} & r_{x_1x_2} & \dots & r_{x_1x_N} \\ r_{x_2x_1} & \ddots & & \vdots \\ \vdots & & \ddots & \\ r_{x_Nx_1} & \dots & & r_{x_Nx_N} \end{pmatrix}$$

If all the predictor variables are related, the matrix R_{xx} is the Identity matrix and R^2 simply equals $\mathbf{c}^\top\,\mathbf{c}$ the sum of the squared correlations with the variable. The predictor variables are related, the inverse of the relation matrix R_{xx} accounts for this.

The squared coefficient of multiple relations are also be computed as the fraction of variance of the dependent variable that is explained by the variables, The fraction can be computed the sum of squared residual, the sum of the square of the errors—divided by the sum of the squared deviations of the values of the dependent variable from its expected value.

The coefficient of multiple correlations is a measure of how well a given variable can be predicted using a linear function of a set of variables. It can be measured by the root of determination, on under the accurate assumptions the best possible linear predictors are used and the intercept is included, whereas the coefficient of determination is defined for more cases, including the nonlinear prediction from the predicted values are not been given. It takes values in between one and zero; a higher value indicates a better predictability of the given variable, with a numbers indicated that the predictions are exactly correct and a value of zero indicating that no linear combination of the independent variables is a better predictor than is the fixed mean. By using this approach triangled area for extracting the correlative information between the features within an observed data object. We had applied the concept of triangle area to extract the geometrical correlation. On comparing the 2 Triangles of an area map, we can imagine this map into two images along their diagonals. The differences are identified on the triangles of the images, and can be found on their triangles. To perform a comparison of TAM, it choose to investigate both the upper triangles or the lower triangles. This produces the result as compared using the entire TAM , the correlations residing in a traffic record can be represented effectively and correctly by the upper triangle or the lower triangle of the respective.

B. *Detection Mechanism*

Threshold-based anomaly detector, was proposed in this whose normal profiles are generated using purely legitimate network traffic records for future comparisons with new incoming investigated traffic records. The Difference between a new incoming traffic record and the normal profile is examined by the proposed detector. If the Difference is greater than a pre-classified threshold, the traffic record is report as an attack. Otherwise, it is flagged as a legitimate traffic record. Clearly, normal profiles and thresholds have direct influence on the performance of a threshold-based detector. A low quality normal profile causes an inaccurate Behavior to legitimate network traffic. For this process, we first apply the proposed triangle-area-based MCA approach to analyze legitimate network traffic, and the generated TAM are then used to give quality features for normal profile generation.

C. *Normal Profile Generation*

Assume there is a set of g legitimate training records; the triangle-area based MCA approach is applied to analyze the records. [1] Mahalanobis Distance (MD) is adopted to measure the dissimilarity between traffic records. This is because MD has been a success and widely used in cluster analysis, classified and multivariable outied detection techniques. It evaluates distance between two multivariable data objects by taking the correlations between variables into account removing the dependency on the scale of measurement during the calculation. Finally, the obtained distribution of the normal training traffic records, are stored in the normal profile for attack detection.

D. Threshold Selection

The threshold is used to differentiate attack traffic from the legitimate one. For distribution, α is normally ranged from 1 to 3. That means detection decision can be made with a certain level of confidence varying from 68% to 99.7%in association with the selection of different values. Thus, if the MD between an traffic record x observed and the respective normal profile is greater than the threshold value, it will be considered as an attack.

E. Evaluation of MCA Based DOS Attack Detection System

Testing our approach on KDD Cup 99 dataset contributes a convincing evaluation and makes the comparisons with other state-of-the-art techniques. Additionally, our detection system innately withstands the negative impact introduced by the dataset because its profiles are built purely based on legitimate network traffic. During the evaluation, the 10 percent labeled data of KDD Cup 99 dataset is used, where three types of legitimate traffic (TCP, UDP and ICMP traffic) and six different types of DoS attacks (Teardrop, Smurf, Pod, Neptune, Land and Back attacks) are available in the communication path. All of these records are first filtered and then are further grouped into seven clusters according to their labels (see Table 9 in Appendix 4 in the supplemental file to this paper for details) form. The overall evaluation process is detailed as follows. First, the proposed triangle-area-based MCA approach is assessed for its capability of network traffic characterization. Second, a 10-fold cross-validation is conducted to evaluate the detection performance of the proposed MCA-based detection system, and the entire filtered data subset is used in this task. In the training phase, we employ only the Normal records in the data set. Normal profiles are built with respect to the different types of legitimate traffic using the algorithm. The corresponding thresholds are determined according to given the parameter α varying from 1 to with an increment of 0.5.

During the test phase, both the Normal records and the attack records are taken into account. the observed samples are examined against the respective normal profiles which are built based on the legitimate traffic records carried using the same type of Transport layer protocol. Third, four metrics, namely True Negative Rate (TNR), Detection Rate (DR), False Positive Rate (FPR) and Accuracy (i.e. the proportion of the overall samples which are classified correctly), are used to evaluate by the proposed MCA-based detection system. To be a good candidate, our proposed detection system is required to achieve high detection accuracy.

F. Result and Analysis in Original Data

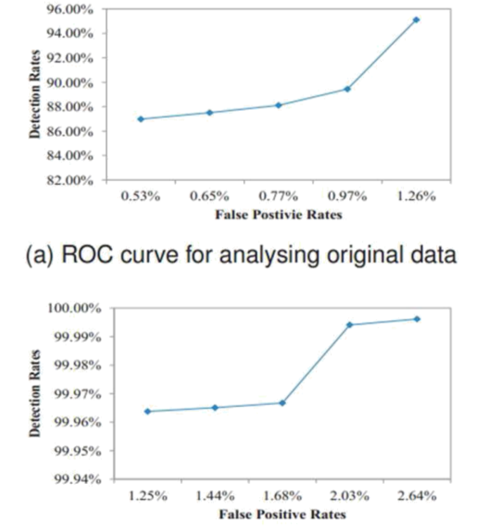
Many threshold frequencies were set in common. The final value reveals that at a certain threshold the server goes to sleep mode for long time period and crashes. And this particular threshold is set as a limit to detect the intrusive networks.

G. Result and Analysis on Normalized Data

The results shows that the data does have significant influence on our detection system, whose overall performance increases in accuracy when taking the normalized data as the inputs and now completely classified correctly by the system based the increase of the threshold value maximum 98.75% detection accuracy range without the fixed threshold value.

V. PERFORMANCE COMPARISONS

The ROC curves of the previous two evaluations are shown in the Fig. 5.1 the relationship between DR and FPR is clearly revealed in the ROC curves. The DR increases when larger numbers of false positive are tolerated. In Fig. 5a, the ROC curve for analyzing the original data using our proposed detection system shows a rising trend. The curve climbs gradually from 86.98% DR to 89.44% DR, and finally reaches to 95.11% DR the ROC curve for analyzed the normal data presents a resembling pattern but jumps dramatically from 99.97% DR to 99.99% DR after experiencing slow progress as shown in Fig our proposed MCA-based detection system (95.20% for the original data and 99.95% for the normalized data).

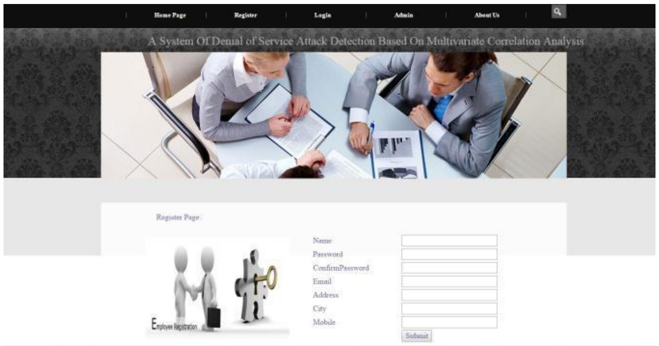


(a) ROC curve for analysing original data

(b) ROC curve for analysing normalized data

Figure 5.1 Analyzing Data comparison

VI. SCREEN SHOTS



A System Of Denial of Service Attack Detection Based On Multivariate Correlation Analysis

Register Page:

Name

Password

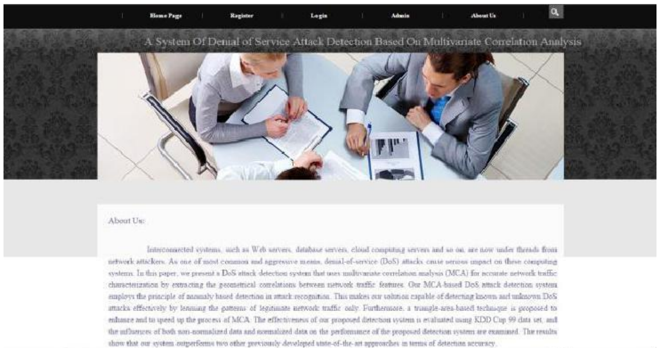
ConfirmPassword

Email

Address

City

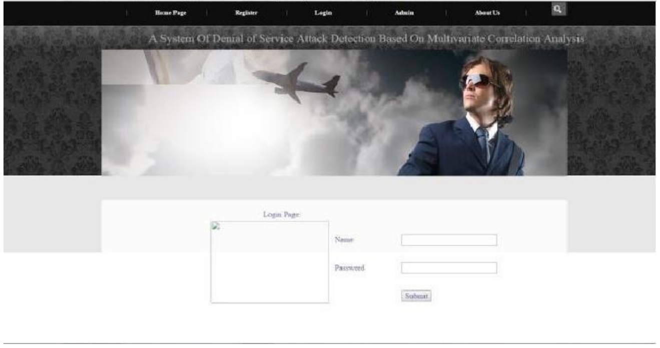
Mobile



A System Of Denial of Service Attack Detection Based On Multivariate Correlation Analysis

About Us:

Interconnected systems, such as Web servers, database servers, cloud computing servers and so on, 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. 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 employs the principle of anomaly based detection in attack recognition. This makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. 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 data set, 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.



A System Of Denial of Service Attack Detection Based On Multivariate Correlation Analysis

Login Page:

Name

Password

VII. CONCLUSION

In this paper we have presented an technique for detecting an dos attack and to and to prevent the attack by triangular MCA based detection system. The technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and gives the most accurate results for network traffic behaviors. The attack analysis and triangle area map generation technique helps our detection system to find out the attack manner and its way of attack with the system. Testing has been conducted using KDD Cup 99 dataset it contains the traffic record. In this Future work, we will further test our DoS attack detection system using real-time data and employ more sophisticated classification techniques to further alleviate the false-positive rate.

REFERENCES

[1] A. Valdes and K. Skinner, "Adaptive, Model-Based Monitoring for Cyber Attack Detection," presented at Recent Advances in Intrusion Detection, Toulouse, France, 2000.etkovic, M., Jonker, W. Preface, “Special issue on secure data management,” Journal of Computer Security, 17(1), pp.1-3 (2009)

[2] K. Park and H. Lee. On the effectiveness of route-based packet filtering for distributed dos attack prevention in power-law in-ternets. In Proceedings of ACM SIGCOMM ’2001, San Diego, CA, August 2001.

[3] Blazek, R., H. Kim, B. Rozovskii, and A. Tartakovsky, “A Novel Approach to Detection of Denial-of- Service Attacks via Adaptive Sequential and Batch-sequential Change-Point Detection Methods,” Proc. of the 2001 IEEE Workshop on Information Assurance and Security, June 2001.

[4] Eleazar Eskin, Matthew Miller, Zhi-Da Zhong, George Yi, Wei-Ang Lee, Salvatore Stolfo,” Adaptive Model Generation for Intrusion Detection Systems”,IEEE Computer Society, 2001.

[5] Y. Chen and K. Hwang, “Collaborative Change Detection of DDoS Attacks on Community and ISP Networks”, IEEE Int’l Symp. on Collaborative Technologies and Systems (CTS 2006), Las Vegas, May 15-17, 2006. Proc. of the 2nd ACM SIGCOMM Workshop on Internet Measurements, 71 - 82 (2002).

[6] Greg Vert Deb orah A. Frincke Jesse C. McConnell,” A Visual Mathematical Mo del for Intrusion Detection”, IEEE Fourth Computer Security Applications Conference , 2002.

[7] J. Ioannidis and S. M. Bellovin, “Implementing Pushback: Router-Based Defense against DDoS Attacks,” Network and Distributed System Security Symposium. (NDSS), San Diego, CA. Feb. 6-8, 2002

[8] W. Streilein, R.K. Cunningham, S.E. Webster, Improved detection of low-profile probe and novel denialof- service attacks (2002), Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, Baltimore, Maryland, June 2002, pp. 11–13.

[9] Akella, A. et al. (2003). Detecting DDoS Attacks on ISP Networks. In ACM SIGMOD/PODS Workshop on management and processing of data streams (MPDS) FCRC.

[10] Feinstein, L. et al. (2003). Statistical approach to DDoS attack detection and response. In Proceedings of the DARPA information survivability conference and exposition (pp. 303–314).

[11] C. Jin, H. Wang, and K. Shin, "Hop-count Filtering: An Effective Defense against Spoofed DDoS Traffic," Proc. of the 10th ACM Conference on Computer and Communications Security, 2003, pp. 30-41.

[12] 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. 6. 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.

[13] Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, "PacketScore: Statistics-Based Overload Control Against Distributed Denial of-Service Attacks," Proc. INFOCOM, 2004.

[14] Y. Chen, Y. K. Kwok, and K. Hwang, "MAFIC: Adaptive Packet Dropping for Cutting Malicious Flows to Pushback DDoS Attacks," IEEE International Workshop on Security in Distributed Computing Systems (SDCS-2005), 2005.

[15] Yu Chen, Yu-Kwong Kwok, and Kai Hwang, University of Southern California, Los Angeles," Filtering Shrew DDoS Attacks Using A New Frequency-Domain Approach", on June 20, 2005.

[16] D. Gavrilis and E. Dermatas, "Real-time Detection of Distributed Denial-of-service Attacks Using RBF Networks and Statistical Features," Computer Networks, vol. 48, no. 2, pp. 235-245, 2005.

[17] 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.

[18] Ahmed T., Coates M., Lakhina A.: Multivariate Online Anomaly Detection Using Kernel Recursive Least Squares. Proc. of 26th IEEE International Conference on Computer Communications (2007)

[19] 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.

[20] 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.

[21] Y.Dhanalakshmi 1 and Dr .I. Ramesh Babu," Intrusion Detection Using Data Mining Along Fuzzy Logic and Genetic Algorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.2, February 2008.

[22] Marina Thottan, Guanglei Liu, Chuanyi Ji," Anomaly Detection Approaches for Communication Networks", IEEE/ACM Tran. Networking (2009)

[23] Zhong ,R and Yue ,G. (2010) DDoS detection system based on data mining. Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan , China, 2 – 4 April , pp .062 – 065 . Academy Publisher.

[24] Barford P., Kline J., Plonka D., Ron A.: A Signal Analysis of Network Traffic Anomalies. , vol. 18, pp. 1649-1662 2008

[25] Lifang Zi, John Yearwoody, Xin-Wen Wuz," Adaptive Clustering with Feature Ranking for DDoS Attacks Detection" Fourth International Conference on Network and System Security, , Vol. 8, Issue 5, No 1, 2010.

.