ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

A SURVEY ON TRIANGLE AREA MAP BASED MULTIVARIATE CORRELATION ANALYSIS TO DETECT DENIAL-OF SERVICE ATTACK

K.Sujithra[1], V.Vinoth Kumar[2]

PG Scholar, Dept of CSE, Kalingnar Karunanidhi Institute of Technology, Coimbatore, India[1]

Assistant Professor , Dept of CSE, Kalingnar Karunanidhi Institute of Technology, Coimbatore, India[2]

Abstract: Well organized systems such as net servers, file servers, cloud computing etc… are now under serious attack from network attackers. Denial-of-service attack is the one of the most frequent and aggressive to computing systems. In this scheme we propose a procedure called multivariate correlation analysis to detect an exact traffic flow classification by extracting the geometrical correlation between known and unknown attacks. This system includes anomaly detection method for the detection of known and unknown Dos. Additionally Triangle Area Based Technique is used to speed up the process of Multivariate Correlation Analysis (MCA). Proposed system can be evaluated by using KDD cup dataset

Index terms: Denial-of-serviceattack, network characterization,multivariate correlation, triangle area

I. INTRODUCTION

A denial-of-service attack is an action that prevents or damages the authorized use of networks, system or application by exhausting resources such as CPU, memory, bandwidth and disk space. In other words, Dos attack a computer or a user is unable to access resources like email and the internet. An attack can be directed at an operating system or at the network.

At first stage they were quite "primitive" involving only one attacker exploiting maximum bandwidth from the victim, denying others to be served. This was done mostly by using Ping floods, SYN floods & UDP floods. These attacks manually synchronized by a lot of attackers in order to cause an effective damage. It is launched on internet landscapes in network form, where the attacking computer sends crafted network packets. (TCP, UDP or ICMP).

Internet based network attacker can be categorized in 2 ways

- Directed Denial of service attack model, where the specific Dos is developed and rolled out by an attacker with an aim to take down a specific network or computer.
- Indirect Denial of service attack model, where a worm or virus is at large in the wild, which causes Dos and interruption as a result of its spreading.

Normally network detection can be classified into anomaly detection and misuse based detection. Anomaly detection based on normal behavior of a system.

Misuse based detection monitoring all the network activities and looking for matches with existing attack signature. Knowledge Discovery Database(KDD) cup data set is most widely used data set for the evaluation of anomaly detection method. The data set is Prepared by Stolfo et.al. and it is built based on the data captured in DARPA'98 IDS evaluation program.

MULTIVARIATE CORRELATION ANALYSIS

Correlation between any two distinct features within each single network traffic record are through this analysis. It estimate the relationship between two variables and also play an important role in Dos attack.

It is based on two ways

- Euclidean Distance Map
- Triangle Area Map

II. RELATED TECHNIQUES

There are number of techniques to overcome the Dos attack. The list are followed

A. A Covariance Matrix method

To find the correlation between sequential samples we go for this approach. This approach improve detection accuracy , and it is in danger to attacks that linearly change all monitored features. This approach can only label a group of observed samples or traffics but not individual in the group.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

B. *Euclidean Distance Map*

The Euclidean Distance Map releases the analysis of correlation from the dependency on prior knowledge of historic network traffic. This EDM solves the issues of linear changes of all observed featured. These MCA based EDM can be high quality potential features for Dos attack detection.

C. *Emergent Self Organizing Map*

It classify "normal" traffic against "abnormal" traffic in the sense of Dos attack. Its main advantage lies in the fact that the emergent SOM's extend the abilities of simple Self Organizing Map (KSOM's) by developing high- level structures.

III. RELATED WORKS

Many system and techniques are used to detect the Dos attack efficiently. Garcia describes by using Gaussian mixture model, they find the irregular packets in the network to identify the intrusion discovery in the system.

Vern Paxson 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.

Yu chin 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.

Chin – Fong Tsai & Chi – Ting Lin tells a new method to detect the dos attack called "Triangle Area Based Nearest Approach". Specifically, the k- means is used to extract the clusters center where each one represent a one particular attack. The k-NN classifier is used to detect intrusion. By using this approach we improve in terms of accuracy, detection state, and false detection rate.

Theerasak explain about Dos attack is carried out by attack tools like worms, botnet 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 method is comparable detection method; it can extracted 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.

IV. SYSTEM ARCHITECTURE

The proposed Dos detection system architecture is given in this section,. In this we discussed about framework and sample – by- sample detection.

A. Framework

The framework consists of three steps

Step 1: Monitoring and analyzing network to reduce the malicious activities only on relevant inbound traffic. To provide a best protection for a targeted internal network.

Step 2: In this step to extract the correlation between two distinct features within each traffic record. The distinct features are come from step 1 or "feature normalization module".

All the extracted correlation are stored in a place called "Triangle area Map"(TAM), are then used to replace the original records or normalized feature record to represent the traffic record. Its differentiate between legitimate and illegitimate traffic records.

In Step 3: The anomaly based detection mechanism is adopted in decision making.

Decision making involves two phases

- Training phase
- Test phase

Normal profile generation is work in "Training phase" to generate a profile for individual traffic record and the generated normal profile are stored in a database. In test phase "tested profile generation " are used to built profiles for individual observed traffic records. Then at last the tested profiles are handed over to "Attack Detection" it compares tested profile with stored normal profiles. This module distinguishes the Dos attack from legitimate traffic.

B. Sample-by-Sample Detection

The group based detection technique maintained a high probability in classifying a group of sequential network traffic samples than the sample-by-sample detection mechanism. This proof was based on assumption that the samples in a tested groups are belongs to same distribution. It is difficult to predicate the traffic, which are belongs to same group.To overcome the above problem we can classifying the group individually .This benefits are not found in group based mechanisms.

V. DETECTION MECHANISM

Detection Mechanism include threshold based anomaly detector, their normal profiles are generated using purely legitimate network traffic records and it is used for future comparisons with new incoming investigated traffic record.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

A. Normal profile Generation

The triangle area based MCA approach is applied to analyze the record. Assume that there is a set of ***g*** the training records are

$$X^{normal}=\{x_{1}\ normal, x_{2}\ normal, \ldots x_{g}\ normal\}$$

Mahalanobis Distance

Measuring the distance between a point P and distribution D. it is a multi dimensional generalization of the idea of measuring many standard variation away P is from the mean D. This is zero if P is at the mean of D, and grows as p moves away from the mean

$$D(x) = \sqrt{(x-\mu)}tS - 1(x-\mu)$$

Threshold selection

It is used to separate attack traffic from the legitimate one

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

Attack Detection

To detect Dos attacks, the lower triangle of TAM of an observed record needs to be generated using the future triangle- area-based MCA approach.

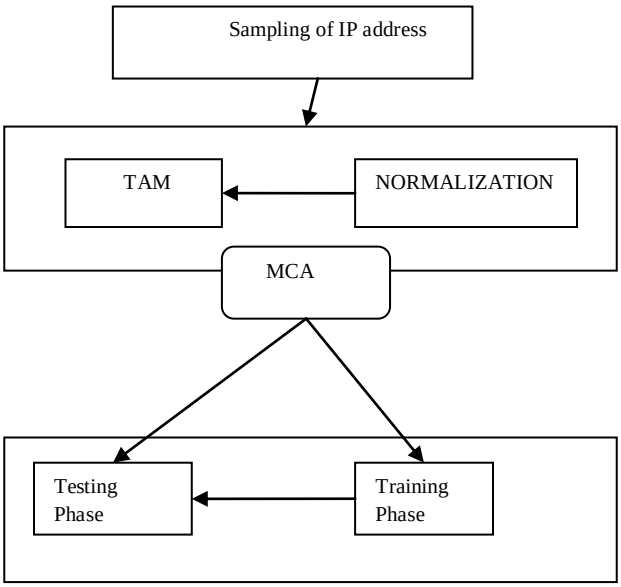

Fig 1. System arch of MCA technique

VI. PROBLEM DEFINITION

Problem with our system its commonly suffer from high false positive rate because the correlation between attributes and features are intrically neglected or techniques do not manage to fully exploit to these correlation. Normally, the Land, Teardrop and Neptune attack cannot achieve high positive rate between these attack and the respective normal profiles is close to that between the legitimate traffic networks.

VII. CONCLUSION AND FUTURE WORK

The problem in our paper however, can be solved by utilizing statistical normalization technique to eliminate the bias from the data. This technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record, and offer extra true characterization for network traffic behaviors. Evaluation can be conducted using KDD data set to give a effective performance. The results have discovered that when working with non-normalized data, our detection system achieves maximum 95.20 percent detection accuracy although it does not work well in identifying Land, Neptune, and Teardrop attack records. The proposed system achieves equal or better performance.

To be part of the future work, we will further test our DoS attack detection system using real-world data and employ more sophisticated classification techniques to further alleviate the false-positive rate

REFERENCES

[1] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," Computer Networks, vol. 31, pp. 2435-2463, 1999.
[2] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, "Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges," Computers and Security, vol. 28, pp. 18-28, 2009.
[3] D.E. Denning, "An Intrusion-Detection Model," IEEE Trans.Software Eng., vol. TSE-13, no. 2, pp. 222-232, Feb. 1987.
[4] 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.
[5] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, "Intrusion Detection Using Fuzzy Association Rules," Applied Soft Computing, vol. 9, no. 2, pp. 462-469, 2009.
[6] W. Hu, W. Hu, and S. Maybank, "AdaBoost-Based Algorithm for Network Intrusion Detection," IEEE Trans. Systems, Man, and Cybernetics Part B, vol. 38, no. 2, pp. 577-583, Apr. 2008.
[7] C. Yu, H. Kai, and K. Wei-Shinn, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649-1662, Dec. 2007.
[8] S.T. Sarasamma, Q.A. Zhu, and J. Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," IEEE Trans. Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 35, no. 2, pp. 302-312, Apr. 2005.
[9] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang,"Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 1073-1080, June 2012.
[10] S. Jin, D.S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," Pattern Recognition, vol. 40, pp. 2185-2197, 2007.
[11] 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.
[12] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R.P. Liu, "RePIDS: AMulti Tier Real-Time Payload- Based Intrusion Detection System," Computer Networks, vol. 57, pp. 811-824, 2013.
[13] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R.P. Liu, "Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis," Proc. Conf. Neural Information Processing, pp. 756-765, 2011.
[14] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R.P. Liu, "Triangle-Area-Based Multivariate Correlation Analysis for Effective

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Denialof- Service Attack Detection," Proc. IEEE 11th Int'l Conf. Trust, Security and Privacy in Computing and Comm., pp. 33-40, 2012.

[15] S.J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P.K. Chan, "Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project," Proc. DARPA Information Survivability Conf. and Exposition (DISCEX '00), vol. 2, pp. 130-144, 2000.

[16] G.V. Moustakides, "Quickest Detection of Abrupt Changes for a Class of Random Processes," IEEE Trans. Information Theory, vol. 44, no. 5, pp. 1965-1968, Sept. 1998.