A System for Distributed Denial-of-Service Attacks Detection Based on Multivariate Correlation Analysis

C. Shivanya[1], D. Elizabeth Paulsyah[2]
[1,2]Students
Department of Computer Science and Engineering,
Francis Xavier Engineering College,
Tirunelveli.

Abstract
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, Distributed Denial-of-Service (DDoS) attacks cause serious impact on these computing systems. A DDoS attacks detection system that uses Multivariate Correlation Analysis (MCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features.The MCA based DDoS attacks detection system employs the principle of anomaly-based detection in attack recognition. This makes our solution capable of detecting known and unknown DDoS attacks effectively by learning the patterns of legitimate network traffic only. A triangle-area-based technique is proposed to enhance and to speed up the process of MCA. 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.

1. INTRODUCTION

Denial of Service (DoS) attack is one of the most common attacks which causes the serious impact in computing system .DoS attacks are class of attacks on targets, which aims at exhausting target resources, thereby denying service to valid users. Denial of service attack is mainly done in categorize to block a node from receiving genuine data or to block the node entirely from another genuine node. This attack is an attempt to make a machine or network resource unavailable to its intended users by either injecting a computer virus or flooding the network with useless traffic. Computer attack and network attack are the two types of dos attack .To break the server security hackers use DoS attack softening technique. The main targets of DoS attack are web server, application server, database server and communication link. It has become a major threat for current computer networks. Dos attack causes serious damages in services of network, so it is essential to develop a dos attack detection system to protect the services of network. There are two types of network based detection systems, viz. misuse based detection system and anomaly based detection system .

In misuse based detection system attacks are detected by monitoring network activities and looking for matches with the existing attack signatures. In misuse based detection system the database should be kept updated which is a laborious task as it is a manual process. So, to overcome these drawbacks of misuse based detection system, anomaly based detection system is developed which is a novelty-tolerant detection system. The manual attack analysis and the frequent update of the attack signature database are avoided in the case of misuse-based detection. In this paper, Our proposed system is for protecting services of network against DoS attacks.. This detection system can provide an effective protection to interconnected systems like web servers, database servers, cloud computing servers etc. by considering their commonality. This

system is anomaly based detection system and it employs principles of multivariate correlation analysis (MCA). DoS attack detection system detects known and unknown attacks respectively. To enhance and speed up the process of MCA, triangle area technique is introduced to generate better discriminative features. In this system we are using normalization technique. KDD cup 99 dataset is used for evaluation of DoS attack detection system.

2. RELATED WORK

There are different Denial Of service Attack detection techniques proposed by the researchers over time to time which have some advantages over and vice-versa. There are many techniques used like K-map, combination of stateful and stateless signature with trace back technique, game-theoretic, Multivariate Correlation Analysis (MCA). Suseela T. Sarasamma, Qiuming A. Zhu, and Julie Huff [2] put a new K-Map (Kohonen Net) multilevel hierarchical structure for an intrusion finding system is presented. Each step of the hierarchical map is organized as the simple winner takes all K-Map. One important advantage of this K-Map multilevel hierarchical is its calculation capability. Apart from other statistical inconsistency detection techniques such as K-means clustering or probabilistic analysis, nearest neighbour approach that engage distance measurement in a feature interval to recognize the outlines our request does not carry costly point to point calculations in organizing a data into clusters. One more advantage is network size reduced. It uses the grouping efficiency of the K-Map for detecting anomalies on selected dimensions of data set. Randomly selected data subsets that contain both the attacks and normal records from a KDD Cup data are used to train the hierarchical net. The paper [2] illustrate the multilevel hierarchical Kohonen Net or Kohonen self-ordering map (K-Map) to implement an inconsistency based intrusion detection system (IDS sensor). We did our testing and training using the pre -processed KDD Cup data set. Main objective was to detect different types of attacks as possible. The experiment was done in two levels. Firstly we used a single level winner takes all K-Map to do a development of IDS. John Haggerty, Qi Shi and MadjidMerabti [3], can combines both stateless and stateful signatures to provide early finding of the DoS attacks due to this enterprise network is protect. This paper is mostly focuses on how domain based way response to an attacks is used by mechanism to block traffic attack. This new solution is enables the blockage of the attack to be gradually propagated only through affected domains toward the attack sources. Albert Banchs, JoergWidmer, Andres Garcia Saavedra and Pablo Serrano [6], put game theory we address the problem of selfishness from a game-theoretic standpoint in DoS . They propose algorithm that satisfies the following properties: a) Wireless network is driven to the optimal point of operation when all the stations implement the algorithm and b) one or more selfish stations cannot obtain any gain by deviating from an algorithm. Ruiliang Chen, Jung-Min Park and Randolph Marchany [4], put mitigation of attack plan actively strangle traffic attack produced attacks in Distributed Denial of Service (DDoS). In such paper presents Attack Diagnosis (AD), a new mitigation of attack scheme that adopts a divide and conquer technique. Packet marking and pushing concepts are combined in AD, and its architecture is in chain with the ideal DDoS attack countermeasure pattern for finding attack is performed near the packet filtering and sufferer node is executed close to the attack of sources. GautamThatte, UrbashiMitra, Fellow, and John Heidemann [7] , develops parametric technique to find network anomalies using contrast to other works requiring flow separation in only aggregate traffic statistics, even when the anomaly of total traffic is a small fraction . By adoptingsimple statistical models for

background traffic and anomalous in the domain of time. One can forecast standard parameters in the real time, thus to avoid the need for manual parameter tuning or long training phase. Additionally, it uses both traffic-rate yielding a bivariate standards and packet-size statistics that ignore most false positives. Wanlei Zhou, WeijiaJia, Feilong Tang ,Song Guo, and Yong Xiang [5] , describe denial of service attack in distributed is a complex threat to the botnets and net are usually the engines behind them. By mimicking the patterns of traffic of flash crowds the sophisticated bot masters try to disable finders this poses a complicated challenge to those who justify against distributed denial of service attacks. According to deep study of organization of current botnets and size, we found that as compared to the flows of flash attack the current attack flows are usually more same to each other. Based on this [5] it propose the algorithm of discretion using the flow correlation coefficient as a similarity metric among doubtful flows. We formulated the problem and represent theoretical proofs for the applicability of the proposed technique of discrimination in theory. Our extensive experiments confirmed the demonstrated effectiveness and theoretical analysis of the proposed technique in practice.

3.PROPOSED SYSTEM

The overview of proposed DoS attack detection system architecture is given in this portion, where the system framework and detection mechanism are discussed. The whole detection process consists of three levels

Level 1. Multivariate correlation analysis

Level 2. Normal profile generation.

Level 3. Attack Detection.

A. Proposed Architecture

The framework consists of three Levels

Level 1: In this level the basic features are generated from network traffic ingress to internal network where proposed servers resides in and are used to form the network traffic records for well-defined time period. Monitoring and analysing network to reduce the malicious activities only on relevant inbound traffic. To provide a best protection for a targeted internal network. This also enables our detector to provide protection which is the best fit for the targeted internal network because legitimate traffic profiles used by the detectors are developed for a smaller number of network services.

Level 2: In this step the Multivariate Correlational Analysis is applied in which the Triangle Area Map Generation module is applied to extract the correlation between two separate features within individual traffic record. The distinct features are come from level 1 or “feature normalization module” in this step. 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. It?s differentiating between legitimate and illegitimate traffic records.

Level 3: The anomaly based finding mechanism is adopted in decision making. Decision making involves two phases as Training phase. Test phase Normal profile generation module is work in “Training phase” to generate a profiles for various types of traffic records and the generated normal profiles are stored in a database. The “Tested Profile Generation” module is used in the “test phase” to build profiles for individual observed traffic records. Then at last the tested profiles are handed over to “Attack Detection” module it compares tested profile with stored normal profiles. This distinguishes the Dos attack from legitimate traffic.This needs the

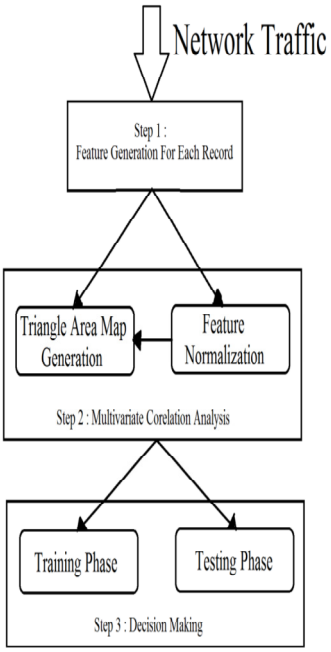
expertise in the targeted detection algorithm and it is
manual task. Particularly, two levels (i.e., the Training Phase and the Test Phase) are included in Decision Making. The Normal Profile Generation module is operated in a Training Phase [1] to generate profiles for various types of legal records of traffic, and the normal profiles generated are stored in the database. The tested profile generation module is used in a Test Phase to build profiles for the each observed traffic documentation. Next, the profiles of tested are passed over to an attack detection part, which calculates the tested profiles for individual with the self-stored profiles of normal. A threshold based classifier is employed in the attack detection portion module to
differentiate DoS attacks from appropriate traffic [8].

B. Multivariate Correlation Analysis

DoS attack traffic treat differently from the appropriate traffic of network and the behaviour of network traffic is reflected by its geometric means. To well describe these statistical properties, here a novel multivariate correlation analysis (MCA) moves toward in this part. This multivariate correlation analysis approach use triangle area for remove the correlative data between features within a data object of observed (i.e. a traffic record).

C. Detection Mechanism

In this section, we present a threshold based on anomaly finder whose regular profiles are produced using purely legal records of network traffic and utilized for the future distinguish with new incoming investigated traffic report. The difference between an individual normal outline and a fresh arriving traffic record is examined by the planned detector. If the variation is large than a pre-determined threshold, then a record of traffic is coloured as an attack otherwise it is marked as the legal traffic record.



D. Algorithm for Normal Profile Generation

In this algorithm [1] the normal profile Pro is built through the density estimation of the MDs between individual legitimate training traffic records (TAM normal, i, lower) and the expectation (TAM normal, lower) of the g legitimate training traffic records.

Step 1: Input network traffic records.

Step 2: Extract original features of individual records.

Step 3: Apply the concept of triangle area to extract the geometrical correlation between the jth and kth features in the

vector xi.

Step 4: Normal profile generation

i. Generate triangle area map of each record.

ii. Generate covariance matrix.

iii. Calculate MD between legitimate record‟s TAM and input records TAM

iv. Calculate mean

v. Calculate standard deviation.

vi. Return pro.

Step 5: Attack Detection.

i. Input: observed traffic, normal profile and alpha.

ii. Generate TAM for i/p traffic

iii. Calculate MD between normal profile and i/p traffic

iv. If MD < threshold

Detect Normal

Else

Detect attack.

In the training phase, we employ only the normal records. Normal profiles are built with respect to the various types of appropriate traffic using the algorithm describe below. Clearly, normal profiles and threshold points have the direct power on the performance of the threshold based detector. An underlying quality usual shape origins a mistaken characterization to correct traffic of network.

E. Naïve Bayes Algorithm for Attack Detection

This algorithm is used for classification purpose.

Step1: Task is to classify new packets as they arrive, i.e., decide to which class label they belong, based on the currently existing traffic record.

Step2: Formulated our prior probability, so ready to classify a new Packet.

Step 3: Then we calculate the number of points in the packet belonging to each traffic record.

Step 4: Final classification is produced by combining both sources of information, i.e., the prior and to form a posterior probability.

F. Mathematical Modeling

Let S be the system which we use to find the DoS attack detection system.

They equip proposed detection system with capabilities of accurate characterization for traffic behaviors and detection of known and unknown attacks respectively.

 Input: Given an arbitrary dataset $X = \{x1, x2, \cdots, xn\}$

 Output: DP (Detected Packets) :

DP={n,m}

Where n is normal packets and M is the malicious packets.

Process: S= {D, mvc, NP, AD, DP}

Where, S= System.

D= Dataset

mvc = Multivariate correlation analysis.

NP = Normal profile generation.

AD =Attack detection.

DP= Detected packets.

VI. CONCLUSION

This paper has presented a MCA-based DoS attack detection system which is powered by a triangle-area based MCA technique and an anomaly-based detection technique. The former technique extracts geometrical correlations hidden in individual pairs of two distinct features within the 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 proper network traffic. In this techniques are Time complexity is reduced, also Results are taken on real time dataset and false positive rate is reduced.

ACKNOWLEDGMENT

We would like to thank all the authors of different research papers referred during writing this paper. It was very knowledge gaining and helpful for the further research to be done in future.

REFERENCES

[1] Zhiyuan Tan, ArunaJamdagni, Xiangjian He, Senior Member, Priyadarsi Nanda, and Ren Ping Liu, “A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2013

[2] S. T. Sarasamma, Q. A. Zhu, and J. Huff, “Hierarchical Kohonenen Net for Anomaly Detection in Network Security,” Systems, Man and Cybernetics, Part B: Cybernetics, IEEE Transactions on, vol. 35, pp. 302-312, 2005.

[3] J. Haggerty, Qi Shi, “Early Detection and Prevention of Denial-of-Service Attacks: A Novel Mechanism with

Propagated Traced-Back Attack Blocking" IEEE Transaction on, Vol. 23, 2005.

[4] R. Chen, Jung-Min Park, R. Marchany, "A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service attacks", IEEE Transactions, Vol. 18, 2007

[5] R Nagadevi, P NageswaraRao, RameswaraAnand, "A New Way of Identifying DOS Attack Using Multivariate Correlation Analysis", International Journal of Computational Engineering Research (IJCER), Vol.04, 2014.

[6] A. G. Saavedra, P. Serrano, J. Widmer, "A Game-Theoretic Approach to Distributed Opportunistic Scheduling Banch", IEEE Transactions on, vol. 21, 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.

[8] S. Gomathi, "An Efficient Way of Detecting Denial-Of-Service Attack Using Multivariate Correlation Analysis", International Journal of Innovative Research in Computer and Communication Engineering (IJRCCE) Vol.2, 2014.

[9] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," Parallel and Distributed Systems", IEEE Transactions on, vol. 23, pp. 1073 -1080, 2012.

[10] DarshanLalMeenaDr.R.S.Jadon , "A Survey on Different Solutions to DDoS Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, 2014.

[11] V. Jyothsna, V. V. Rama Prasad, " A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, Vol.28,2011