iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Multivariate Correlation Analysis for Detection of Denial-Of-Service Attack

Venkatesh[1], Santhosh Kumar A[2], Mahadevaswamy[3], Suresh C[4], Asha G R[5]
[1,2,3,4] *Department of CSE, UG [BE] scholars, BMSCE, Bangalore*

Abstract- In networking systems, many Web servers, Database servers, Cloud computing servers and so on, are now under threats from network attackers. One of most common types of attack is denial-of-service (DoS) attacks which causes serious impact on these computing systems. Multivariate correlation analysis technique is used for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. In MCA-based DoS attack detection method employs the principle of anomaly based detection technique in attack recognition. This makes system capable of detecting known and unknown DoS attacks effectively by learning the characteristics of legitimate network traffic only. Furthermore, to increase the speed and effectiveness of MCA process a triangle-area-based technique is used and the effectiveness of this detection system is evaluated using KDD Cup 99 data set, and the influences of both normalized data and non-normalized data on the performance of the proposed detection system.

Keywords- Multivariate correlation, Denial of Service, KDD cup99, triangle area

I. INTRUDUCTION

Denial-Of-Service attack is one of the most common types of attack on online servers. DoS attacks, usually reduces the availability of resources to the clients. The Attackers severely impose large computation tasks by flooding it with huge rate of duplicate packets. Thus, the victim can be forced to be out of network services for few minutes to even several days. This causes serious problem to the victim. There are different types of DoS attacks are there and brief explanation is given in the fig-1[2]. In DoS attack detecting system deal with Network level, Application level and Data level attacks.

Attack	Affected Area	Example	Description
Network Level Device	Routers, IP Switches, Firewalls	Ascend Kill II, "Christmas Tree Packets"	This type of Attack attempts to exhaust hardware resources using multiple duplicate packets or a software bug.
OS Level	Equipment Vendor OS, End-User Equipment.	Ping of Death, ICMP Echo Attacks, Teardrop	Attack takes advantage of the way operating systems implement protocols.
Application Level Attacks	Finger Bomb	Finger Bomb, Windows NT RealServer G2 6.0	Attack a service or machine by using an application attack to exhaust resources.
Data Flood (Amplification, Oscillation, Simple Flooding)	Host computer or network	Smurf Attack (amplifier attack) UDP Echo (oscillation attack)	Attack in which massive quantities of data are sent to a target with the intention of using up bandwidth/processing resources.

Fig-1 Types of DOS attacks [2]

©IJRASET 2015: All Rights are Reserved

II. RELATED WORK

Effective detection of DoS attacks are mandatory for the protection of network services to avoid DoS attack. There are two types of detecting systems, They are: Network based detecting system and Host based detecting system. Network based detecting system is better to use. Generally, network-based detection systems can be classified into two main categories, namely, anomaly-based detection systems and misuse based detection systems [1]. Misuse-based detection systems detect attacks by monitoring network activities and looking for matches with the existing attack signatures, misuse-based detection systems are easily evaded by any new attacks and even variants of the existing attacks and furthermore, it is a complicated and labor intensive task to keep signature database updated because signature generation is a manual process and heavily involves network security expertise[2]. Because of this we using anomaly based detection system, which monitors and flags any network activities presenting significant deviation from legitimate traffic profiles as suspicious objects, anomaly based detection techniques detects zero-day intrusions that exploit previous unknown system vulnerabilities [3]. In this technique the profiles of legitimate users are developed based on techniques, such as machine learning [6], [7], data mining [4], [5], and statistical analysis [8], [9]. However, these systems commonly suffer from high false-positive rates because the correlations between features are neglected [10]. A covariance matrix-based approach was designed in [11] to determine the multivariate correlation for sequential samples and although the approach improves detection accuracy, it is vulnerable to attacks that linearly change all monitored features and also in addition, this approach can only label an entire group of observed samples as legitimate or attack traffic but not the individuals in the group. And to deal with the above problems, an approach is used that is based on triangle area was presented in [12] to generate better discriminative features. However, this approach has dependence on prior knowledge of malicious behaviors. In paper [13] developed a refined geometrical structure-based analysis technique, where Mahalanobis distance (MD) was used to extract the correlations between the selected packet payload features. This approach also successfully avoids the above problems, but it works with network packet payloads. In [14], author proposed a more sophisticated non pay load-based DoS detection approach using multivariate correlation analysis (MCA). Following this emerging idea, we present a new MCA-based detection system to protect online server. In paper [15] the triangle area based multivariate correlation analysis technique is referred. This DoS detection system is evaluated using KDD Cup 99 data set [16].

III. FRAMEWORK

Detection process in this system [17] consists of three major 3 steps as shown in Fig-1. The individual record detection and testing involved in the detection phase. In Step 1, normal features are generated from external network traffic to the internal network where protected servers reside in and are used to form traffic records for a well-defined time interval. By monitoring and analyzing at the destination network reduce the overhead of detecting malicious activities by concentrating only on specific network traffic attack. This makes detection system in providing 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 [18].In Step 2, multivariate correlation analysis, in which the “triangle area map generation” module is applied to extract the correlations between two distinct features within each traffic records coming from the first step. The occurrence of network intrusions cause changes to these correlations so that the changes can be used as indicators to identify the network attacks. All the detection techniques are correlated as triangle areas stored in triangle area maps (TAMs), are then used to replace the original basic features or the normalized features to indicate the records of network attacks. This provides higher to distinguish between legitimate and illegitimate traffic records. In Step 3, the anomaly based detection mechanism is adopted in decision making which enables the detection of any DoS attacks without and relevant knowledge on attack. Furthermore, the frequent update of the database that contains attackers signature in the misuse-based detection are eliminated. Meanwhile, the mechanism enhances the effectiveness of the proposed detectors and makes them harder to be evaded because attackers need to generate attacks that match the normal traffic profiles built by a specific detection algorithm. This is specifically, have two phases (i.e., the “training phase” and the “test phase”) are involved in decision making. The “normal profile generation” module is operated in the “training phase” to generate profiles for various types of legitimate traffic records, and the generated information is stored in a database. The “tested profile generation” module is used in the “test phase” to build profiles for individual observed traffic records and the tested profiles are submitted to the “attack detection” module and this compares the individual tested profiles with the already stored normal profiles[20] used in the “attack detection” module to differentiate between DoS attacks.

P

Fig-3 System architecture [19]

©IJRASET 2015: All Rights are Reserved

IV. MULTIVARIATE CORRELATION ANALYSIS

The behavior of traffic that is attacked by DoS is different from the legitimate network traffic [20]. And the behavior of any network traffic is reflected by its statistical properties. To understand these statistical properties of network traffics, A Multivariate Correlation Analysis approach is there, This MCA approach uses triangle area for extracting the correlative information between the features within an observed traffic records. MCA approach supplies with the following benefits to data analysis.

It does not require the knowledge of historic traffic in performing analysis.

Unlike the Covariance matrix approaches proposed in, which is vulnerable to linear change of all features, this triangle-area-based MCA withstands the problem.

It provides characterization for individual network traffic records rather than model network traffic behavior of a group of network traffic records. This results lower latency in decision making and enable sample-by-sample detection.

The correlations between distinct pairs of features are revealed through the geometrical structure analysis. Changes of these structures may occur when anomaly behaviors appear in the network. This provides an important signal to trigger an alert.

A. Detection by anomaly based detection technique

This section represents a threshold-based anomaly detection method, whose normal profiles are generated using purely legitimate network traffic records [21]. And then can be used for future comparisons with new incoming traffic records. The changes between a new incoming traffic record and the normal profile are examined by the detector .The traffic record is flagged as an attack, If the dissimilarity is greater than a specified threshold. Otherwise, it labeled traffic as a legitimate traffic. Normal profiles and thresholds have direct impact on the performance of a threshold-based detector. A low quality normal profile may cause an inaccurate characterization to network traffic of in which services are servicing by the servers. Therefore, first apply the proposed triangle area- based MCA approach to analyze legitimate network traffic, and the generated Triangular area map generations are then used to supply features for normal profile generation.

B. Detection by triangle area based technique

A triangle-area-based MCA approach is applied to analyze the records. Mahalanobis Distance is under concern to measure the dissimilarity between traffic records because MD has been widely used in cluster analysis, classification and multivariate detection techniques. It calculates distance between two multivariate data objects by taking the correlations between variables and removing the dependency [21].

C. Detection by threshold based technique

Threshold is specially used to differentiate attack traffic from the legitimate one. Threshold = $\mu + \sigma * \alpha$. Where α denotes normal distribution and usually ranged from 1 to 3[22]. Detection decision can be made with a certain level of confidence, varying from 68% to 99.7% by the selection of different values of α. Finally, if the MD between an observed traffic record and the respective normal profile is greater than the threshold, this will be considered as an attack.

V. CONCLUSION

Here we conclude that, the MCA-based DoS attack detection system which uses the triangle area based MCA technique and the anomaly-based detection technique is very useful to extracts the geometrical correlations in each individual pairs of two distinct features within each network traffic record and also can be used to extract the correlation between groups of network traffic records. And it gives more accurate characterization for network traffic behaviors. And this technique facilitates computing systems to be able to detect both known and unknown DoS attacks from network traffic.

VI. ACKNOWLEDGEMENT

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITYIMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

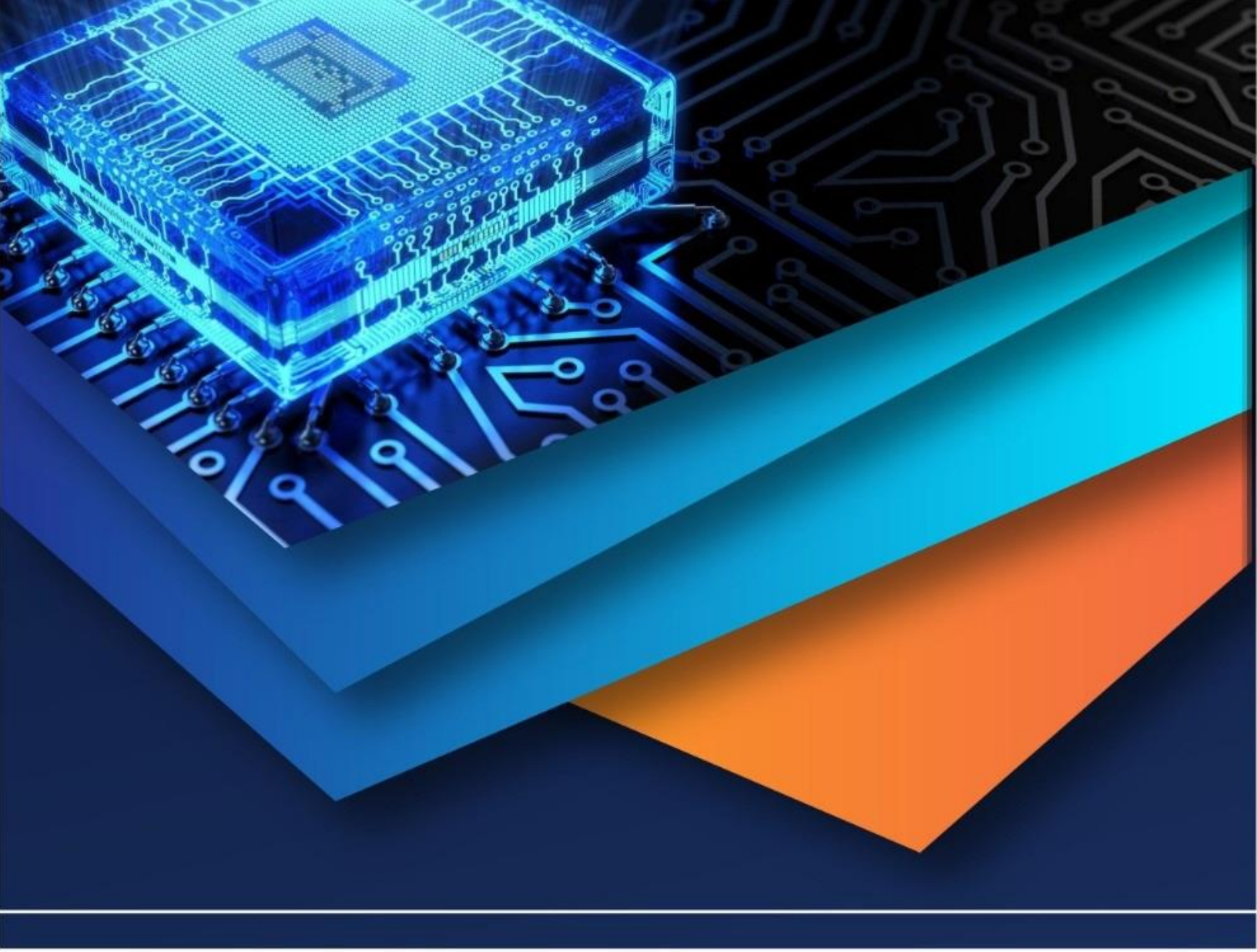
REFERENCES

[1] Karig, David and Ruby Lee. "Remote Denial of Service Attacks and Countermeasures", Princeton University Department of Electrical Engineering Technical Report CE-L2001-002, October 2001.

©IJRASET 2015: All Rights are Reserved

[2] M. Tavallaee, E. Bagheri, L. Wei, and A.A. Ghorbani, "A Detailed Analysis of the KDD Cup 99 Data Set," Proc. IEEE Second Int'l Conf. Computational Intelligence for Security and Defense Applications,pp. 1-6, 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] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic Flooding Attack Detection with SNMP MIB Using SVM," Computer Comm., vol. 31,no. 17, pp. 4212-4219, 2008.
[7] 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.
[8] 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.
[9] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," IEEE/ACM Trans. Networking, vol. 19, no. 2, pp. 512-525, Apr. 2011.
[10] 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.
[11] 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.
[12] S. Jin, D.S. Yeung, and X. Wang, "Network Intrusion Detection in Covariance Feature Space," Pattern Recognition, vol. 40, pp. 2185- 2197, 2007.
[13] 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.
[14] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R.P. Liu, "RePIDS: A Multi Tier Real-Time Payload-Based Intrusion Detection System," Computer Networks, vol. 57, pp. 811-824, 2013.
[15] 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.
[16] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R.P. Liu, "Triangle-Area-Based Multivariate Correlation Analysis for Effective Denial of- Service Attack Detection," Proc. IEEE 11th Int'l Conf. Trust, Security and Privacy in Computing and Comm., pp. 33-40, 2012.
[17] 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.
[18] 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.
[19] A.A. Cardenas, J.S. Baras, and V. Ramezani, "Distributed Change Detection for Worms, DDoS and Other Network Attacks," Proc. The Am. Control Conf., vol. 2, pp. 1008-1013, 2004.
[20] W. Wang, X. Zhang, S. Gombault, and S.J. Knapskog, "Attribute Normalization in Network Intrusion Detection," Proc. 10th Int'l Symp. Pervasive Systems, Algorithms, and Networks (ISPAN),
pp. 448-453, 2009.
[21] 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.
[22] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," Computer Networks, vol. 31, pp. 2435-2463, 1999.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)