INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

MCA: MULTIVARIATE CORRELATION ANALYSIS FOR ATTACKS

A.SaiSakthi[1], R.VijayaLakshmi[2]

[1]B.E (CSE), Krishnaswamy College of engineering and technology, affiliated Anna university (Chennai), S.Kumarapuram, cuddalore, Tamilnadu-607109, India.
[2] M.C.A.,M.Phil,(P.hd), Krishnaswamy college of engineering and technology, affiliated Anna university(Chennai), S.Kumarapuram, cuddalore, Tamilnadu-607109, India.

Abstract

In the web servers and database servers in interconnected systems which is applied in cloud computing servers are now under threat to attack by malicious attackers. The common aggressive means for Denial of Service (DOS) attack which cause impact in the interconnected computing systems. In DOS attack for detection system that use Multivariate Correlation Analysis (MCA) which accurately determines network traffic by extracting geometrical correlations between network traffic features. In MCA based denial of service attack detection system imply principle of anomaly based detection in recognizing attack. The solution which is detecting the capability for known denial of service attack and unknown dos attack effectively learn the legitimate network traffics in different patterns only. Triangle based network technique for enhancing the proposed method to speed up process of MCA. The proposed effective detection system for evaluation of using dataset and influences both non-normalized data and normalized data on performing and examining detection system. From the resulted data performance the two other previous developed state of art approaches for detecting the accuracy.

Keywords*:* Denial Of Service (DOS) attack, Multivariate Correlation Analysis (MCA), network traffic, normalized data

1. Introduction

The major threat that affects the current computer networks in the modernized group of interconnected systems is Denial of Service Attack (DOS). In previous days local attackers use DOS attack as a technical game of attacking one particular system by stopping or denying all the messages or communication they get. The attacker wants to get control of an interrelated channel through performance of DOS attack against the person who possesses the channel. As the attacker takes control over popular websites they could not be recognized by the underground community people. As the basic DOS attack codes or tools are available from internet even normal computer users can use these codes well and become a DOS attacker.

Sometimes the employees concurrently have the view of launching of denial of service attack against any company policies to be disagreed. This kind of attack is blacklisted under illegal actions. Companies might use this kind of attacks to debar their competitors by attacking their system on important times of their growth. Past

year attackers becomes threat to online business with denial of service attacks and request their payments out of protection. Internet threats generally fight against the target by excavating its resources which will be related to any network computing and performance of services. Service having relational performance are follows bandwidth connection, TCP buffer, application services and CPU cycles.

Attacker or attacking system which individually attacks and exploits the vulnerabilities breaks the target servers and bring their services down. As it is difficult for the attackers to overload targets resources from individual computer systems there are various DOS attacks launched through number of distributed host computer attackers in the internet. This kind of attack is known as distributed denial of service attack (DDOS).

Attacking of attackers makes traffic aggregation over incomparable attacks over the victim resources where the attackers can force victim system which downgrades the system significantly system performance and stops the delivery of any kind of service. Comparing the conventional denial of service attack which could be addressed by better security service system prohibits unauthorized remote or local access to much complex and hard to prevent the attacks.

In this kind of attack it is very difficult and it is very challenging to differentiate attacking host and the real user systems to take reaction against them. Recently DDOS attacks are increased with its frequency and they are sophisticated with the severity due to its vulnerability to attack the computer that increases rapidly. This enables attackers who breaks up and installs various attacking tools in many computers.

Wireless network suffers denial of service because of mobiles laptops which share same physical signal media for transmitting computing resources with each other. They share important resources such as bandwidth, CPU even power consumption will be shared in between them. The constraints that are available in wired nodes will be a wireless network which can be forged easily by a single attacker who modify or inject packets which disrupts connections between those authenticate mobile nodes and it cause denial of service attacks. In our paper we provide overview of existing denial of service attack and have major defence system.

2. Denial of Service (DOS) Attack

In denial of service attack we have many techniques which can disable service which downgrades service performance which exhaust resources that provide services. It is impossible to enumerate each existing attack which describes representation of network based and host based attack that illustrates attack principles. The complementary information that has readers attacks for performance degradation. In network based attacks that exploits network protocols for TCP flooding because of these protocols consumes resources that maintain states. TCP flooding is one of the attacks that had wide impact on many systems.

When any attempt to client establish TCP connection to a server which first send a client SYN message to the server. The server system that acknowledges by sending the ACK message have open connection between client and server that specifies the service data which exchanges service data between them. They can be arise by the abusing half open state where the server should wait for clients ACK message after sending the synchronization message to client.

To allocate memory for server that stores information of half open connection. The memory released for server for final ACK receives for half open connection which expired in network. Hosts that attacks half open connection that easily connects with spoof service. The source IP that creates synchronizing message which ignores its synchronizing acknowledgement will have consequences for final acknowledge messages will never sent to victim client system.

The victim system that allocates limited size of space which process table that have too many half connections that fills the space rapidly. When a half open connection expires due to session timeout in which zombies that can aggressively send spoof TCP synchronize packets requests connections that have much higher rate more than its expiration rate. Finally the victim system which is unable to accept any new incoming connection can provide services for flood to be used for determining computer which responds to request computer packets.

It achieves the task for requesting any echo packet that sent to computer which receives echo reply packet. The attack that hosts forge requests for echo that have victim address as source and broadcasting

address of remote networks for destination address. Remote network for firewall or router that will not filter the special packets is cropped for delivering or broadcasting to all computers in that network. The computer that sends echo reply back to source or the termed victim carries requests packets. The victim network is congested to the network traffic.

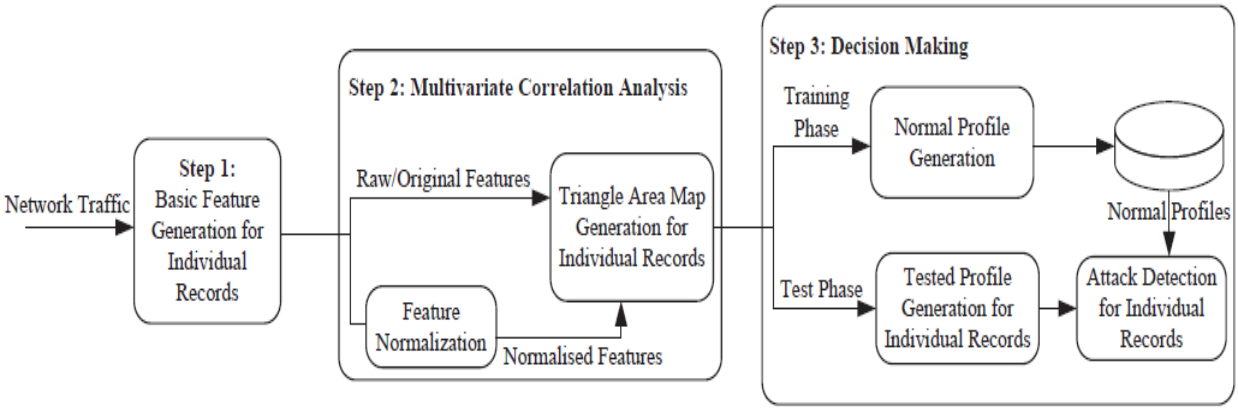

Figure 1.featuring MCA and decision making

3. Feature normalization for multivariate correlation analysis

Feature for normalizing the ingress network traffic which generates the internal network where protected servers kept and they are used for performing the traffic analysis for certain time interval. Analyzing and monitoring of network destination which reduces the overheads leads to detection of malicious activities which concentrates on relevancy for traffic inbounds. This enables the detection which provides best fit for target internal network because of legitimate traffic profiles use detectors which are developed for small number of network services.

The Multivariate Correlation Analysis for triangle area generation for maps applies the exact correlations between two different features that bounds within each and every traffic records comes from first step or the traffic records the normalization by feature normalization module from this step. The existence for network intrusion attacks which can cause changes for correlation of changes used as indicators which identifies the intrusive activities that leads to attacks. Such extracted correlations termed as triangle area maps which are used for replacing the original basic features or normalized feature that represents the traffic congestion records. This produces high discrimination information which differentiates the legitimate and illegitimate traffic records.

4. Decision making and attack evaluation

Anomaly based detection adoption in decision making facilitates detection of any denial of service attack requires without any attacks relevancy of knowledge. The intensive attack analysis for frequent update of attack keys database in case of detection which based on misuse of database attack detection will be avoided further. The enhanced mechanism for the robustness f proposed detection which makes harder evasion for attackers need to generate the new attacks makes the matches the normal traffic profile built on specific detection algorithm. The intensive task requires expertise targeted detection of algorithm.

The training or test phase involves decision making. The profile generation for normal profile operated in training for generating profiles for legitimate traffic records generates normal profile stored in database. The profile generation to be tested to be used in test phase for building profiles individual observation for traffic records. The tested profiles for individual traffic records observed for profiles tested. The tested profiles hand over the detection of attack compares the individual tested profile relevant for stored normal profiles. The classifiers based on threshold employs attack detection module distinguish denial of service attacks from authenticated traffic.

The evaluation of labelled data for dataset which have three types of legitimate traffic like TCP,UDP etc have six different types of denial of service attacks which are available for Neptune like searches. Entire records first filtered and further grouped into seven clusters according to the labels for evaluation for results of such attacks.

From the existing techniques the large amount of alerts produced is one of the drawback in which the existing IDS are optimized for detecting the attacks with high accuracy. Still they have various disadvantages outlined n number of publications that have lots of work which has been outlined in number of publications that analyze IDS in order to direction of future research.

Thus in our proposed work we represents denial of service attack detection system that uses multivariate correlation analysis for accurate network traffic characterization by extracting the geometric correlations between network traffic features. The attacks based on multivariate correlation detection system employs principle anomaly based detection in attack recognition. This denial of service attack detection presented in our paper employs principles for multivariate correlation and anomaly based detection.

Detection system had capabilities for accurate characterization of traffic irregularities and detection of known and unknown attacks. Triangle area technique developed to enhance the speed up of processing the multivariate correlation for statistical normalizing technique used for eliminating the bias from raw data.

4. Conclusion

In Multivariate correlation based denial of service attack system based on triangle area based detection technique. The former technique extracts the correlations for individual pairs of two distinct features within each network traffic records more accurate characterization for network irrelevancy of behaviours. The further techniques facilitate our system for distinguishing both known and unknown attacks. The legitimate network traffic evaluates dataset for verification for the effectiveness and performance of proposed denial of service attack detection system. The original and normalized influence for results reveals working without normalized data with our detection system achieves maximum detection accuracy. This problem solved by utilizing statistical normalization techniques for eliminating bias from data. Our proposed system achieves equal or better performance which compares two state of art approach for denial of service attack. The sophisticated classifiers of techniques for false positive rate which have computational complexity and time taken for detection system.

REFERENCES

[1] V. Paxson, “Bro: A System for Detecting Network Intruders in Realtime,” *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 & Security*, vol. 28, pp. 18-28, 2009.

[3] D. E. Denning, “An Intrusion-detection Model,” *IEEE Transactions on Software Engineering*, pp. 222-232, 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 Communications, vol. 31, no. 17, pp. 4212-4219, 2008.

[7] 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.

[8] 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.

[9] 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.

[10] 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.
[11] 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.
[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," Neural Information Processing, 2011, pp. 756-765.
[16] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Triangle-Area-Based Multivariate Correlation Analysis for Effective Denialof- Service Attack Detection," The 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, United Kingdom, 2012, pp. 33-40.
[17] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Costbased modeling for fraud and intrusion detection: results from the JAM project," The DARPA Information Survivability Conference and Exposition 2000 (DISCEX '00), Vol.2, pp. 130-144, 2000.
[18] G. V. Moustakides, "Quickest detection of abrupt changes for a class of random processes," Information Theory, IEEE Transactions on, vol. 44, pp. 1965-1968, 1998.
[19] 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.
[20] W. Wang, X. Zhang, S. Gombault, and S. J. Knapskog, "Attribute Normalization in Network Intrusion Detection," The 10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), 2009, pp. 448-453.
[21] M. Tavallaee, E. Bagheri, L. Wei, and A. A. Ghorbani, "A Detailed Analysis of the KDD Cup 99 Data Set," The The Second IEEE International Conference on Computational Intelligence for Security and Defense Applications, 2009, pp. 1-6.
[22] D. E. Knuth, The art of computer programming vol I: Fundamental Algorithms Addison-Wesley, 1973.

A Brief Author Biography

A.Saisakthi – Currently she is pursuing M.E (CSE) at Krishnaswamy College of Engineering & Technology, Cuddalore, Tamil Nadu, India. Her research areas are Cloud Computing, Data Mining, wireless network and Big Data. She had also done projects in SOA's last mile connecting smartphones to computer cloud in cloud computing domain.

R.Vijayalakshmi – had finished M.C.A., M.Phil., and now doing her(Ph.D.). She is currently working in Krishnaswamy College of Engineering and Technology. Her research area is data mining with swarm algorithms.