International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

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

Avinash Devare[1] **Monika Shelake[2]** **Varsha Vahadne[3]** **Pratibha Kamble[4]** **Banu Tamboli[5]**

Department of computer Engineering, JSPM'S, JSCOE Maharashtra, India.

Department of computer Engineering, JSPM's JSCOE Maharashtra, India.

Department of computer Engineering, JSPM's JSCOE, Maharashtra, India.

Department of computer Engineering, JSPM's JSCOE Maharashtra, India.

Department of com puter Engineering. JSPM's JSCOE Maharashtra,. India

---

Abstract - In the networking systems, such as the Web servers, database servers, cloud computing servers etc are now under threads from network attackers. As one of most common and aggressive means, Denial-of-Service attacks cause serious impact on these computing systems. We are present a study on the recent approaches in handling Distributed Denial of Service attacks. DDOS attack is the fairly new type of attack to cripple the availability of Internet service and resources. During in the last decade, anomaly detection has attracted to the attention of many researchers to overcome the weakness of signature-based is IDS in the detecting novel attacks, and KDD CUP'99 is the mostly widely used data set for the evaluation of these systems. We are survey different papers describing methods of defense against DDOS attacks based on entropy variations, traffic in anomaly parameters, neural networks, device level defense, botnet flux identification and application layer DDOS defense.

***Key Words*: :** Denial of Service attack, network traffic characterization, Intrusion Detection System(IDS), Multivariate correlation, KDD cup99, DDoS attacks, DDOS Defense

1.INTRODUCTION :

DENIAL-OF-SERVICE (DoS) attacks are the one type of aggressive and menacing intrusive behavior to online servers. DoS attacks severely degrade the availability of a victim, which can be a host, a router, or an entire network. They impose intensive computation tasks to the victim by exploiting its system vulnerability or flooding it with huge amount of useless packets. Internet security has been a concern for all the users. However, a very strange kind of incident took place in 1999 . Another attack took place against Yahoo! in February 2000. Again on 20thOctober 2002, another DDoS attack took place, where 13 root servers responsible for providing Domain Name System service were affected. It caused seven of the thirteen root servers crippled. 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. Intrusion detection systems (IDSs) are monitoring devices that have been added to the wall of security in order to prevent malicious activity on a system. This work focuses on network intrusion detection systems (NIDSs) mainly because they can detect the widest range of attacks compared to other types of IDSs.

1.1MULTIVARIATE CORRELATION ANALYSIS :(MCA)

Based DoS attack detection system employs the principle of anomaly based detection in attack recognition. Makes our solution capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. Effectiveness of our proposed detection system is evaluated using KDD Cup 99 dataset, and the influences of both non-normalized data and normalized data on the performance of the proposed detection system are examine.

1.2 DENIAL-OF-SERVICE(DOS) :DoS is an attack that make available or fully consume the memory to its intend users. Denial-of-Service is one type of attacks makes some computing or a memory resources too busy or too full to handle legitimate request, or denies legitimate users access to a machine. Example Ping of

Death, Smurf etc. Short for ***Denial-Of-Service Attack***, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the *Ping of Death and Teardrop* attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks

1.3 KDD CUP 99 DATASET :

Knowledge discovery in database or KDD datasets in the largest datasets use for IDS. The KDD dataset is employed in international knowledge discovery and the data miming tools.KDD Cup 1999 dataset is consist of large number of redundant records. This data set is given as a input to proposed system to performed training and testing operations.

1.4 NETWORK INTRUSION DETECTION SYSTEM USING FUZZY LOGIC :

The anomaly- based intrusion detection makes use of effective rules identified in accordance with the designed strategy ,which is obtained by mining the data effectively. The fuzzy rules generated from the proposed strategy can be able provide better classification rate in detecting the intrusion behavior.

2. SYSTEM ARCHITECTURE :

It is a large scale attack in a co-ordinated fashion, which is typically launched indirectly with the help of other computers in internet .There are several kinds of DsDos attacks that prevents legitmate traffic from reaching the victim computer. attacks, the attack is targeted to tie up the resources of the victim computer are two main classes of such attacks: bandwidth depletion and resource depletion attacks. In case of bandwidth depletion attack, The victim network is flooded with unwanted traffic that prevents that prevents legitmate traffic from reaching the victim computer. In the order case of resource depletion attacks, the attack is targeted to tie up the resources of the victim computer.

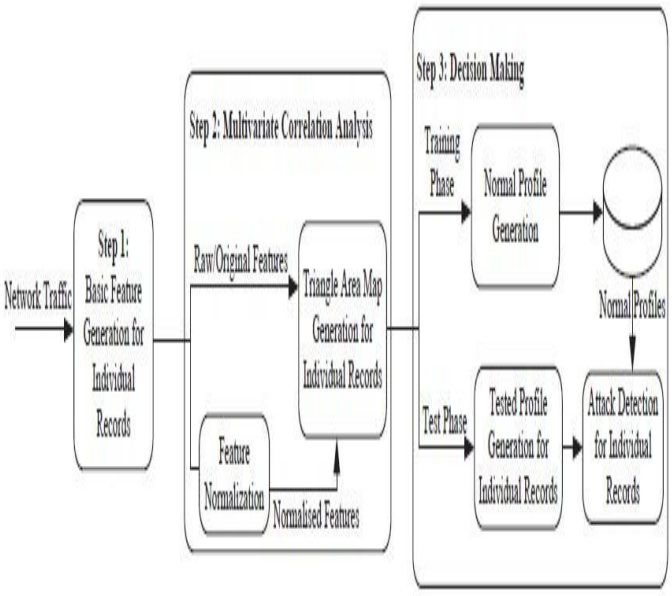


Fig 1: Framework of the proposed denial-of-service attack detection system

The whole detection process consists of three major steps As shown in fig The sample-by-sample detection mechanism is involved in the whole detection phase(i.e Steps 1,2 and 3)

Step 1: Network traffic to the internal network where protected servers reside in and are used to form traffic records for a well –defined time interval. Monitoring and analyzing at the destination network reduce The overhead of detecting malicious activities by concentrating only on relevant inbound traffic .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.

Step 2: Multivariate correlation Analysis, in which the "Triangle Area Map Generation" module is applied to extract the correlation between two distinct feathures within each traffic record coming from the first step or the traffic record normalized by the "Feature Normalization" module.

Step3: Our MCA method normalization technique are explained ,The anomaly-based detection mechanism is adopted in decision is the making.It facilitates the detection of any Dos attack without requiring any attack relevant knowledge. The labor –intensive attack

analysis and the frequent update of the attack signature is the database in the case of misuse-based detection are avoided. to the mechanism enhances the robustness of the proposed detectors and makes them harde to be evaded because attackers need to generate attacks that match the normal traffic profiles built by a specific detection algorithm.

The Normal Profile Generation is module operated in the "Training Phase" is generated profile for various types of legitmate traffic. The tested profile generation module is used for "Test phase" this builds for individual traffic records the "Attack Detection" module compares the individual tested profiles which is stored in normal profiles .A threshold-based classifier is employed in the "Attack Dection" module to distinguish Dos Attack.

Sample-by-Sample Detection: The group-based detection mechanism maintained a higher probability in classifying a group of sequential network traffic samples than the sample-by-sample detection mechanism**.** The proof was based on an assumption that the samples in a tested group were all from the same distribution(class).

3. PROPOSED SYSTEM ARCHITECTURE

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 dataset, 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.

4.WORKING OF THE SYSTEM :

In this system only one admin and two user are connected on one server. Two user are Expert user and Normal user. User to access the system so firstly register. Then you will get username and password. Normal user can post query or questions on the system. Then Multiple Expert user can send above questions answers. Expert user also firstly register on the system then post the answer to normal user. When someone normal user can post any meaningless query then rejected the query and admin can block that person. Without admin no one can unblock the system. Only admin have authority to take action on normal user activity. Once the admin can block the normal user then normal user can't post the query. When normal user are mistakenly and send this meaningless query then normal user can send request to the admin to activate or unblock. Then admin can be decides to unlock to normal user or not.

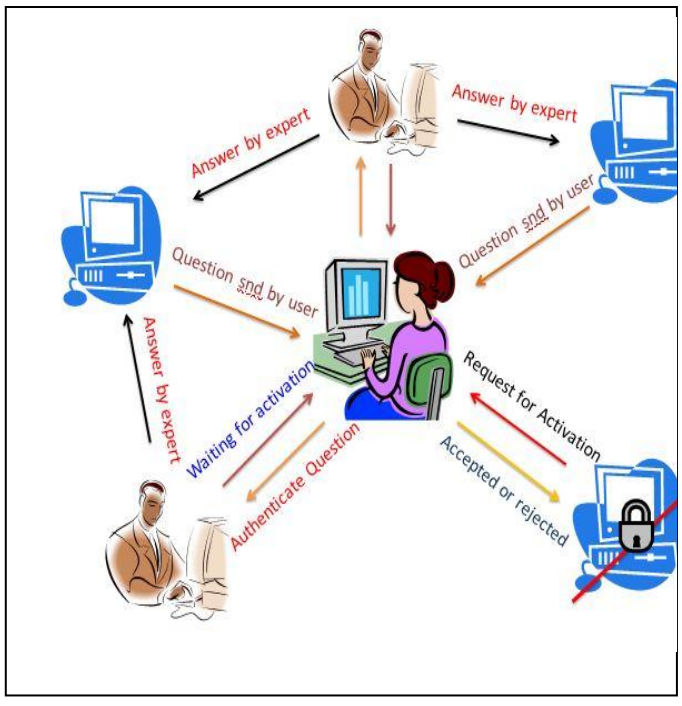
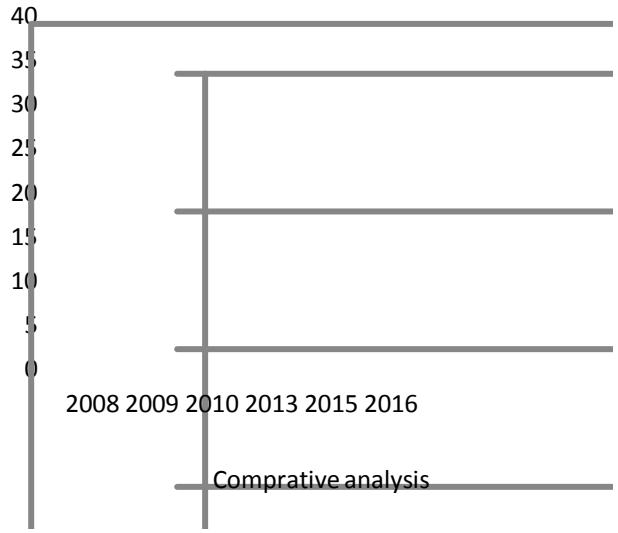


Figure 4. Working Of The System

5.COMAPARATIVE STUDY

Citation	Paper Name	Security issues covered	Year
IJCSNS International Journal of Computer Science 182 and Network Security	Trust Model for Measuring Security Strength of Cloud Computing Service	1.Authentiction 2.Data Confidentiality	2015
International Journal of Recent Scientific Research	Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA	1.DDOS	2014
Dhaval Patel,M.B.Chaudhari	Data security in cloud computing using digital signature	1.Integrity 2.Authentication	2013
Dr.V.Venkatesa Kumar, M.Nithya	Improving security issues and security attacks in cloud computing	1.DOS 2. Data integrity 3.Data loss	2008
Smita Parte, Noumita Dehariya	Cloud Computing: Issues Regarding Security, Applications and Mobile Cloud Computing	1.Dos	2007
T. Sivasakthi and Dr. N Prabakaran	Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing	Digital signature Algorithm (SHA)	2006

5.1 Comaparative Study Graph



6.ALGORITHMS USED

6.1 MULTIVARIATE CORRELATION ANALYSIS:

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 determination, but under the particular assumptions the best possible linear predictors are used and the intercept is included, whereas the coefficient of determination is defined for more general cases, including nonlinear prediction which the predicted values have not been derived from a model-fitting procedure. The 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 indicating that the predictions are exactly correct.DoS attack traffic behaves differently from the legitimate network traffic, and the behavior of network traffic is reflected by its statistical properties. When comparing two TAMs, we can imagine them as two images symmetric along their main diagonals. Any differences, identified on the upper triangles of the images, can be found on their lower triangles as well.

7.GRAPHICAL ANALYSIS OF RESULT:

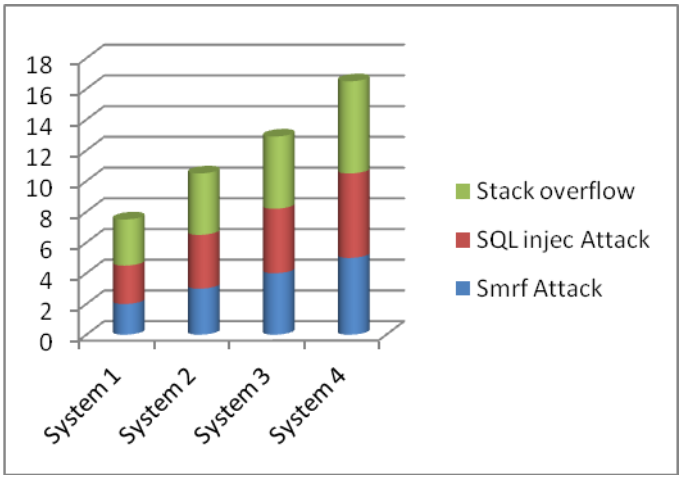


Figure: 3.Attack overcome on various system

8.RESULT

Security parameters	Admin	Normal User	Expert User
Register on System	Admin also register on sstem.then	Normal user Register on system	Expert User also Register on System
Password & username	Get the admin	Also normal user get	Also expert user get
Action Perform	Normal user & Expert user action are register	Normal user can post the query	Expert user can response to this query
Block the user	Normal user block	Meaningless query can post so admin can take action	Can't take action on normal users query

9.CONCLUSION:

We have to developed the anomaly based intrusion detection system in detecting the intrusion behavior within a network. A fuzzy decision - making module was designed to build the system more accurate for the attack detection, using the fuzzy inference approach. Intrusion detection system is one of the most important and the security policy of computer. The MCA -based DoS attack detection system which uses the triangle area based MCA technique and the anomaly - based detection technique is the very useful to extracts the geometrical correlation in each individual pairs of the two distinct features. This paper is based on the MCA-Based Dos Attack. In this paper we are using the MCA algorithm for the DoS.The Evaluation has been conducted using the KDD Cup 99 data set. To be a part of the future work the further work , test our Dos detection test using real-world-data. This paper most impact is to implement MCA algorithm.

10.ACKNOWLEDGEMENT:

This work is supported by JSPM‟s Jayawantrao Sawant College of Engineering, Pune Maharashtra. First and foremost, we would like to thank our guide Prof. A.S. Devare. Providing us with their invaluable support, motivation, suggestion and guidance throughout the course of the paper. We would like to express our gratitude towards Prof. A. S. Devare whose support and consideration has been a valuable asset during course of this paper. We convey our gratitude to our respected HEAD OF DEPARTMENT, Prof. H. A. Hingoliwala for his motivations and guidance throughout the work. And, last but not least we would like to thank Principal Dr. M. G. Jadhav for directly and indirectly help us for this work.

11.REFERENCES:

[1] Monika Shelake, Varsha Vahadne, Kamble Pratibha,Tamboli Banu,Avinash Devare" A Survey For DOS Attack Based on Multivariate Correlation Analysis", International Journal of Innovative Research in Science, Engineering and Technology(An ISO 3297: 2007 Certified Organization)Vol. 4, Issue 11, November 2015

[2] IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014

[3] Zhiyuan Tan, Member, IEEE, Aruna Jamdagni, Xiangjian He, Senior Member, IEEE, Priyadarsi Nanda, Senior Member, IEEE, Ren Ping Liu, Senior Member, IEEE, and Jiankun Hu, Member, IEEE 2015

[4] IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.12, December 2009

[5] R. Shanmugavadivu et al./ Indian Journal of Computer Science and Engineering (IJCSE)

[6] International Journal of Recent Scientific Research Research Vol. 4, Issue, 9, pp.1314- 1319, September, 2013

[7] Proceedings of the 7th USENIX Security SymposiumSan Antonio, Texas, January 26-29, 1998

[8] *ISSN (e): **2250 – 3005** || Vol, 04 || Issue, 8 || August – 2014 || International Journal of Computational Engineering Research (IJCER)*

[9] www.ijraset.com Volume 3 Issue IV, April 2015 IC Value: 13.98 ISSN: 2321-9653 International Journal for Research in Applied Science & Engineering Technology (IJRASET).

[10] Web Intelligence & Distributed Computing Research Lab Green Tower, C- 9/1, Golf Green, Calcutta 700095, India debajyoti. mukhopadhyay@gmail.com

[11] The Following Paper Was Originally Published In The Proceedings Of The 7th Usenix Security Symposium San Antonio, Texas, January 26- 29, 1998
[12] García -Teodoro P., Díaz - Verdejo J., Maciá - Fernández G., Vázquez E. Anomaly - based network intrusion detection: Techniques, systems and challenges, Computers and Security, 28, 1-2, 18-28 (2009)

[12] International Journal of Recent Scientific Research Research Vol. 4, Issue, 9, pp.1314 - 1319, September

[13] A. Mitrokotsa, and C. Douligeris, “Denial – of-Service Attacks,” Network Security: Current Status and Future Directions (Chapter 8), WileyOnline Library, pp. 117 -134, June 2006

[14] IJRET: International Journal of Research in Engineering and Technology eISSN: 2319 -11 63 | pISSN: 2321 -7308

[15] ISSN (e): 2250 –3005 || Vol, 04 || Issue, 8 || August –2014 || International Journal of Computational Engineering Research (IJCER)

[16] Thomas Dubendorfer , Matthies Bossardt,Bernhard Plattner; Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation; Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05) - Workshop 17 –Volume 18,2005.

[17] Stephen Specht, Ruby Lee; Taxonomies of Distributed Denial of Service Networks, Attacks, Tools,and countermeasures; Department of Electrical Engineering, Princeton Architecture Laboratory for Multimedia and Security, Technical Report CE-L2003-03, May 16, 2003

[18] D.E.Denning,"An Intrusion - dection Model," IEEE Transactions on Software Engineering, pp.222 - 232,1987

[19] S.Jin, D.S. Yeung, and X.Wang, "Network Intrusion Detection in covariance feature Space," Pattern Rcognition,vol.40.pp.2185 - 2197,2007

[20] 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.