ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A System Denial of Service Attack Detection Based on Multivariate Correlation Analysis and Artificial Neural Network

Abhilasha B. Pawade[1], Santosh T. Waghmode[2]

[1,2]Department of Computer, Imperial College of Engineering and Research, Pune, Savitribai Phule Pune University, Pune India.

ABSTRACT: Organized systems like web Servers, database servers, cloud computing servers etc, are now under viruses from network attackers. Denial-of-Service (DoS) attacks cause serious crash on these computing systems. We present a DoS attack detection system in this paper that uses Multivariate Correlation Analysis (MCA) for exact network traffic description by extracting the geometrical correlations between network traffic features. By using principle of anomaly detection our MCA based attack detection system identifies network attacks. It makes our solution able for detecting known and unknown DoS attacks efficiently by learning the patterns of legal network traffic. Instead of Triangle Area Map we are using Genetic Algorithm for wide range of requests **.**By using self evolving system that is ANN (Artificial Neural Network) for Attack Detection. By using KDD Cup 99 dataset we are evaluating efficiency of our proposed DoS attack detection system and influences of non-normalized data and normalized data on the performance of the proposed detection system are checked. Our system outperforms than two other previously developed state of the art approaches in terms of detection exactness and avoids network intrusion which results shows.

KEYWORDS: Denial-Of-ServiceAttack,NetworkCharacterization,NetworkTraffic,Multivariate Correlation Analysis, Genetic Algorithm, Artificial Neural Network

I. INTRODUCTION

DDOS that is Distributed Denial of Service is type of DOS attack in which many compromised systems are there. These compromised systems are generally contaminated with a Trojan which are used to target a single system and it causes a Denial of Service (DoS) attack. DDoS attack suffers consist end under attack system. Also it consists of all systems which are prohibited by the hacker and unkindly used in the distributed attack. The arriving traffic flooding the sufferer originates from several different sources potentially hundreds of thousands or other in DDoS attack. It makes it unfeasible to stop the attack basically by jamming a single IP address efficiently. Additionally this is very complicated to differentiate genuine user traffic from attack traffic when widen crosswise so many points of origin.

This paper focuses on the detection of DDoS attacks which keep it away from above mentioned issues. It does not focus on their casual vectors. Generally non distributed denial-of- service attacks utilize susceptibility to disturb a service by sending few carefully untrue packets. Primarily. For flooding a particular sufferer with enormous traffic uses DDoS attacks. Because of high efficiency the status of attacks in opposition to any kind of service as there is no need to spot. In the casualty it utilizes any particular service particular fault. Because of this, this paper focuses entirely on flooding DDoS attacks. A single intrusion prevention system (IPS) or intrusion detection system (IDS) can barely identify such DDoS attacks. Though they are not situated very close to the casualty. In final case, the IDS/IPS may collide because it needs to contract with an overpowering volume of packets (some flooding attacks reach 10–100 Gb/s). By allowing such vast traffic to transfer through the Internet. It only identify or block it at the host IDS/IPS may strictly strain Internet resources. The foundation of MCA is collected of intrusion prevention systems (IPSs) situated at the Internet service providers (ISPs) level.To protect and work together by exchanging chosen traffic information the IPSs makeup implicit protection rings around the hosts. By using wide simulations the estimate of MCA and an actual dataset is offered. Also its hold up for incremental use in real networks by viewing MCA efficiency and low overhead.

DOI: 10.15680/IJIRCCE.2017. 0504307

To avoid our server from DDOS attacks we are using MCA system to identify these attacks. In such a way MCA is intended that makes it a service to which customers can subscribe. By computing and exchanging faith scores on possible attacks we participating IPSs beside the path to a subscribed customer join forces (vertical communication). The host they defend the IPSs form implicit protection rings around. When the level of a potential attack is high implicit rings utilizes horizontal communication. The threat is calculated based on the whole traffic bandwidth. This whole traffic bandwidth going to the customer compared to the maximum bandwidth it supports. MCA identifies flooding DDoS attacks and it also helps in identifying other flooding scenarios. Other scenarios of flash crowds and for botnet-based DDoS attacks. In This Paper we are using Artificial Neural Network which has self evolving system so no need to provide manual inputs or feedback for similar type of attack. We are using Genetic Algorithm instead of triangle area map. Genetic algorithms are used to identify more possible attacks.Using KDD Cup 99 dataset efficiency of our proposed system evaluated or calculated. The influences of normalized data and non-normalized data on the performance of the proposed detection system are examined. The results proves that our system is very reliable outperforms two other previously developed state of the art approaches in terms of detection correctness.

II. MOTIVATION

Organized systems likeWeb servers, Database servers, Cloud Computing servers etc. are now under viruses from network attackers. Denial-Of-Service (DOS) attacks reason for serious crash on these computing systems.The main objective of a project to identifying known and unknown DoS attacks efficiently by learning the patterns of genuine network traffic using multivariate correlatin analysis and artificial neural network. We present a DoS attack detection system that uses Multivariate Correlation Analysis (MCA) and ANN. For exact network traffic description by extracting the geometrical correlations between network traffic features we uses MCA and ANN based attack detection for decision making. Our MCA-based DoS attack detection system uses principle of anomaly based detection in attack recognition. It makes our solution able to identify known and unknown DoS attacks efficiently by learning the patterns of legal network traffic .We are using Genetic Algorithm instead of triangle area map.Genetic algorithms are used to identify more possible attacks.Using KDD Cup 99 dataset efficiency of our proposed system evaluated or calculated.The influences of normalized data and non-normalized data on the performance of the proposed detection system are examined. The results proves that our system is very reliable outperforms two other previously developed state of the art approaches in terms of detection correctness.

III. LITERATURE SURVEY

1. Title: Worldwide ISP security report
Author: Arbor, Lexington
Description:
. In help with the Internet security operations community Arbor Networks, Inc has completed this fourth edition of an ongoing series of annual operational security surveys. This survey, covering a 12-month period from August 2007 through July 2008. It is designed to supply data useful to network operators.Because of which they can make informed decisions about their use of network security technology. These decisions defend their mission critical infrastructure. This also provide as a general resource for the Internet operations and engineering community, recording information on trends and employment of various infrastructure security techniques.

The daily aspects of security in commercial networks are the main focus of survey respondents issued by Operational network securities .In this survey provides results are more exactly represent real world concerns than theoretical and emerging attack vectors which are addressed and speculated about somewhere else[22].

Key Findings

In the last three surveys the ISP Security Battle front expands. To combate distributed denial of service (DDoS) attacks most of available security resources are spent by internet service providers. ISPs explains a far more diversified security landscape and significant concerns over domain name system (DNS) spoofing, border gateway protocol (BGP) hijacking and spam this year. Now half of the surveyed ISPs consider their DNS services susceptible approximately. Associated service delivery infrastructure, including voice over IP (VoIP), session border controllers (SBCs) and load balancers are concerned over by others. In 2000, 40 Gigabits from relatively humble megabit beginnings are exceeded attacks. This year largest DDoS attacks have grown a hundred fold to break the 40 gigabit barrier now. Attack size growth continues to extensively outpace the corresponding increase in fundamental transmission speed and ISP infrastructure investment. Aslo it shows the yearly reported maximum attack size.

2. Title:Survey of network- based defense mechanisms countering the DoS and DDoS problems

Author:T. Peng, C. Leckie, and K. Ramamohanarao

Description:

Initially internet was designed for openness and scalability. Because of yardsic infrastructures certainly working as envisioned certainly. Cost or Price of this success has been poor security. For example, the Internet Protocol (IP) was designed to hold simplicity of attachment of hosts to networks. It also provides little support for verifying the contents of IP packet header fields. Because of this, it is possible to forge the source address of packets. Therefore difficult to recognize the source of traffic. There is no inherent support in the IP layer to ensure whether a source is approved to access a service. Packets are delivered to their destination, and the server at the destination must make a decision whether to accept and service these packets. Even though defenses like firewalls can be added to defend servers. How to distinguish legal requests for service from nasty access attempts is key challenge for defense. For a server to confirm the validity of those requests if is simple for sources to generate service requests, then it is hard to guard the server from nasty requests. Nasty requests waste the resources of the server. All these issues create the opportunity for a class of attack known as a denial of service attack [23].

3. Title: The zombie roundup: Understanding, detecting, and disrupting botnets

Author: E. Cooke, F. Jahanian, and D. Mcpherson

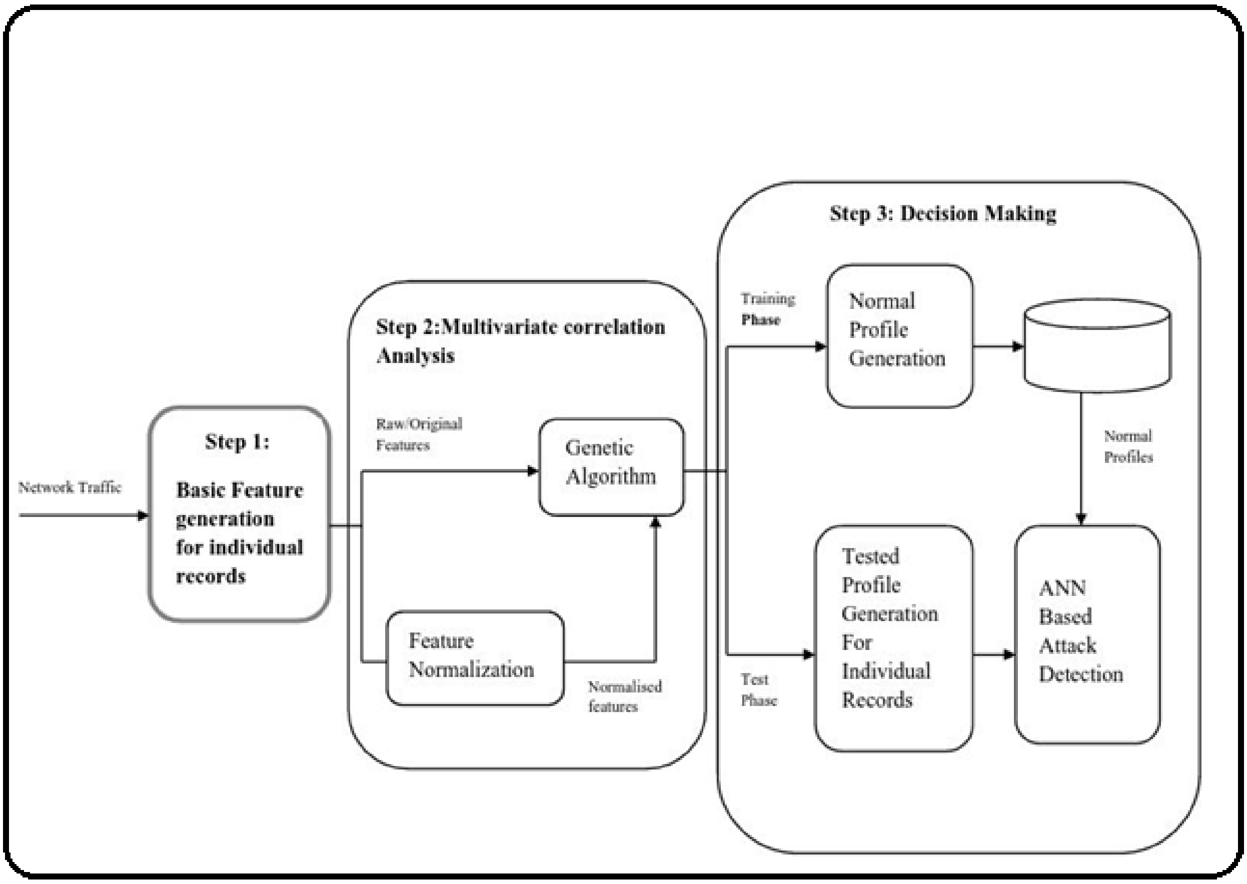
Description:

Global Internet threads are undergoing a deep transformation from attacks designed only to hold back infrastructure to those that also target people and organizations. A large pool of compromised hosts sitting in homes, schools, businesses, and governments around the world are behind these new attacks. These systems are contaminated with a bot. this bot communicates with a bot controller. Other bots forms what is generally referred to as a zombie army or botnet? Zombie army or Botnets are a very real. Botnets hurriedly evolving problem. Still this problem not well understood or studied. We outline the beginning and structure of bots and botnets which also use data from the operator community in this paper. Today to demonstrate the botnet problem experiments of the Internet Motion Sensor project and honeypot experiment are done. After that we study the usefulness of identifying botnets by frankly monitoring IRC communication or other command and control activity which prove a more broad approach which is required. Concluding by telling a system to identify botnets which use advanced command and control systems by correlating secondary detection data from many sources. It is terrifying new class of attacks which directly impacts the everyday lives of millions of people and endangers businesses around the world. New attacks steal or hacks personal information which can be used to damage reputations and it also brings about significant financial losses. The symptoms of the problem like filtering the spam, hardening web browsers, or building applications that warn in opposition to phishing tricks which are focused by current alleviation techniques. To commit attacks it is crucial to disturb and dismantle infrastructure these tools are important. A large pool of compromised hosts sitting in homes, schools, businesses, and governments around the world are core of all these threats. Impured systems with a bot communicate with a bot controller. Other bots are used to form what is generally referred to as a zombie army or botnet. A bot can be differentiated from other threats by a communication channel to a controller.

IV. SYSTEM ARCHITECTURE

Develop a complete framework for our proposed DoS attack detection system. Then propose an algorithm for normal profile generation and an algorithm for attack detection correspondingly. Then continue a detailed and complete mathematical analysis of the proposed system and inspect more on time cost.As resources of interconnected systems (like Web servers, database servers, cloud computing servers etc.) are situated in service providers' Local Area Networks(LAN).They are generally constructed using the same or alike network fundamental infrastructure and are yielding with the underlying network model. Our proposed detection system can supply effective protection to all of these systems by considering their unity.

System Flow:-


Network Traffic
Step 1:
Basic Feature generation for individual records
Step 2:Multivariate correlation Analysis
Raw/Original Features
Genetic Algorithm
Feature Normalization
Normalised features
Step 3: Decision Making
Training Phase
Normal Profile Generation
Normal Profiles
Test Phase
Tested Profile Generation For Individual Records
ANN Based Attack Detection

V. CONCLUSION

This paper presented Denial of service attack detection based on MCA which is powered by genetic algorithm and ANN. Belief scores are shared within a ring-based overlay network of IPSs. It is performed as close to attack sources as possible, providing a security to subscribed customers and saving valuable network resources. Experiments showed good performance and robustness of MCA and highlighted good practices for its configuration. Also, the analysis of MCA demonstrated its light computational as well as communication overhead. Being offered as an added value service to customers, the accounting for MCA is therefore facilitated, which represents a good incentive for its deployment by ISPs. As a future work, we plan to extend MCA to support different IPS rule structures.

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 Transactionson Software Engineering, pp. 222-232, 1987.

[4] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, “DDoS attackdetection method using cluster analysis,” Expert ystems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.

[5] A. Tajbakhsh, M. Rahmati, and A. Mirzaei, “Intrusion detectionusing 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 forNetwork 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 DDoSAttacks over Multiple Network Domains,” Parallel and DistributedSystems, IEEE Transactions on, vol. 18, pp. 1649-1662, 2007.
[9] G. Thatte, U. Mitra, and J. Heidemann, “Parametric Methods forAnomaly Detection in Aggregate Traffic,” Networking, IEEE/ACMTransactions on, vol. 19, no. 2, pp. 512-525, 2011.
[10] S. T. Sarasamma, Q. A. Zhu, and J. Huff, “Hierarchical KohonenenNet for Anomaly Detection in Network ecurity,”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 CorrelationCoefficient,” Parallel and Distributed Systems, IEEE Transactionson, vol. 23, pp. 1073-1080, 2012.
[12] S. Jin, D. S. Yeung, and X. Wang, “Network Intrusion Detection inCovariance Feature Space,”Pattern Recognition, vol. 40, pp. 2185-2197, 2007.
[13] C. F. Tsai and C. Y. Lin, “A Triangle Area Based Nearest NeighborsApproach 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: Amulti 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, “Denialof-Service Attack Detection Based on Multivariate CorrelationAnalysis,” Neural Information Processing, 2011, pp. 756-765.
[16] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, “TriangleArea-Based Multivariate Correlation Analysis for Effective Denialof-Service Attack Detection,” The 2012 IEEE 11th InternationalConference on Trust, Security and Privacy in Computing andCommunications, 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 theJAM project,” The DARPA Information Survivability Conferenceand Exposition 2000 (DISCEX ’00), Vol.2, pp. 130-144, 2000.
[18] G. V. Moustakides, “Quickest detection of abrupt changes for aclass of random processes,” Information Theory, IEEE Transactionson, vol. 44, pp. 1965-1968, 1998.
[19] A. A. Cardenas, J. S. Baras, and V. Ramezani, “Distributed changedetection 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 10thInternational Symposium on Pervasive Systems, Algorithms, andNetworks (ISPAN), 2009, pp. 448-453.
[21] M.Tavallaee, E. Bagheri, L. Wei, and A. A. Ghorbani, “A DetailedAnalysis of the KDD Cup 99 Data Set,” The The Second IEEE International Conference on Computational Intelligence for Securityand Defense Applications, 2009, pp. 1-6.
[22]A.Networks, Arbor, Lexington,MA,“WorldwideISP Security report,”Tech.Re.,2010.
[23] Peng,T.,Leckie,C., and Ramamohanrao,K.2007.Survey of network-based defense mechanisms countering the DoS and DDoS problems.ACM Comput.Surv.39,1,Article 3(April 2007),42 pages DOI=10.1145/1216370.1216373 http://doi.acm.org/10.1145/1216370.1216373.
[24]E.Coockie,F.Jahanian and D.Mcpherson, “The zombie roundup: Understanding,detecting,and disrupting botnets,” in Proc.SRUTI,Jun.2005,pp.39-44.