International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 3, Issue 6, November-December 2014 **ISSN 2278-6856**

Design And Implementation of a System for Denial of Service Attack Detection Based on Multivariate Correlation Analysis: A Review

Priti G. Harne[1] , Prof.Ms.V.M.Deshmukh[2]

Department of Information Technology Prof Ram Meghe institute of Technology & Research
Badnera ,Amravati, India

Abstract

The reliability and availability of network services are being threatened by the growing number of Denial-of-Service (DoS) attacks. Effective mechanisms for DoS attack detection are demanded. Therefore, 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. MCA-based DoS attack detection system employs the principle of anomaly-based detection in attack recognition. This makes solution to capable of detecting known and unknown DoS attacks effectively by learning the patterns of legitimate network traffic only. in this system also detected various types of viruses. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of MCA. The effectiveness of 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.

Keywords:- Denial-of-Service attack, network traffic characterization, multivariate correlations, triangle area

1. INTRODUCTION

Denial-of-Service (DoS) attacks is an attempt to make a machine or network Resourse unavailable to its intended users.Dos attacks severely degrade the availability of a victim,which can be a host,a router,or an entire network.the availability of network services is seriously threatened by the continuosly increasing number of DoS attacks.thus effective machanisms for DoS attack detection are highly demanded. Classification of DoS attacks are as follows 1. network device level attacks 2. Operating System (OS) level attacks 3. application level attacks 4. data flood attacks,5. protocol feature attacks.In network device level attacks, the target is some hardware device on the network such as a router. The attack is launched by exploiting some software bug or hardware resource vulnerability. In Operating System (OS) level attacks, vulnerabilities of operating system in the victim machine are used to launch DoS attack. In application level attacks, vulnerabilities in the application are identified to exploit them for DoS attack. Port scanning for identifying open ports of a remote application is very common in this perspective. In data flood attacks, targets are the connection capacity of a remote host or the bandwidth of a network. Heavy traffic is generated by the attacker towards the victim to exhaust connectivity or bandwidth resources so that normal services are denied or degraded for requests of legitimate users. In protocol feature attacks, the weaknesses of some protocol features are used to exploit them for launching a DoS attack. For example, the source IP address of a data packet(which relates to Internet Protocol and is a part of TCP/IP stack) can be spoofed by an attacker to launch a DoS attack which can be harder to trace due to a fake address [1]. The DOS attack detection, mainly focuses on the development of the network-based detection mechanism.The detection system employs two approaches namely misuse detection[2] and anomaly detection[3].Misuse detection is used to identify the known attacks, using the signatures of predefined rules.[3]Anomaly detection is used to establish the usage profile of the system. During the training phase, the profiles for the legitimate traffic records are generated and the generated records are stored in the database. The trusted profile generation is build and handed over to the "attack detection" module, which compares the individual tested profile with the normal profile. To protect online service from DoS attack here present a DOS attck detection system that uses Multivariate Correlation Analysis for accurate network traffic characterization by extracting the geometrical correlations between network traffic features .the application of Multivariate Correlation Analysis(MCA) makes the intrusion detection more effective and efficient. A triangle area technique is developed to enhance and to speed up the process of MCA. Moreover benefiting from the principal of anomaly detection ,DoS attack detection approach is independent on prior knowledge of attack and is capable of detecting both known and unknown DoS attacks. in this system also detected various types of viruses.

2. RELATED WORK

In 2003, Sanguk et al.[4]- investigated the traffic rate analysis (TRA) as a traffic flow analysis mechanism and, using their TRA mechanism, analyzed TCP-based network flows under DDoS attacks. Further, they detected the DDoS network flooding attacks using the state-action rules compiled by machine learning algorithms. In 2004, Limwiwatkul et al.-Discovering the DDoS attack signature is considered to be the main point in[5] by

analyzing the TCP/IP packet header against the well defined rules and conditions, and distinguish the dinerence between normal and abnormal traffc. They developed rules that used to find the signature of DDoS stack. First they discovered the information that concluded from the traffic measurement analysis under placing rules, and then they matched, related rules using three analysis methods: volume, distributed and ratio analysis together to evaluate the possible signature of attack. In 2004, Kim et al.- In[6],proposed a combined data mining approach for the DDoS attack detection of the various types, that is composed of the automatic feature selection module by decision tree algorithm and the classifier generation module by neural network.They used the NetFlow data as the gathering data, because the analysis per flow is useful in the DDoS attack detection. In 2004, Gavrilis et al.[7]- had present and evaluate a Radial-basis-function neural network detector for Distributed-Denial-of-Service (DDoS) attacks in public networks based on statistical features estimated in short-time window analysis of the incoming data packets. A small number of statistical descriptors were used to describe the DDoS attacks behaviour, and an accurate classification is achieved using the Radial-basis-function neural networks (RBF-NN). That method is evaluated in a simulated public network and showed detection rate better than 98% of DDoS attacks using only three statistical features estimated from one window of data packets of 6 s length. In 2005, Mitrokotsa et al.[8]- By exploiting the visualization of network traffic their approach detects Denial of Service attacks by classifying malicious and normal actions. The proposed approach is extremely powerful in producing efficient results. Its main advantage lies in the fact that Emergent SOMs extend the abilities of simple KSOMs by developing high-level structures that could be invisible with simple KSOMs where only a few neurons can be used. In 2006, Sengar, Wang, et al.[9]- Proposed an online statistical detection mechanism, called vFDS, to detect DoS attacks in the context of VoIP. The core of vFDS is based on Hellinger distance method, which computes the variability between two probability measures. Using Hellinger distance, they characterized normal protocol behaviors and then detect the traffic anomalies caused by flooding attacks. In 2007 Yu Chen et al.[10]-Proposed distributed approach to detecting DDoS flooding attacks at the traffic flow level. The defence system is suitable for efficient implementation over the core networks operated by Internet service providers (ISP). they developed a distributed change-point detection (DCD) architecture using change aggregation trees (CAT). The system is built over attack-transit routers, which work together cooperatively.CAT domain servers collaborate among themselves to make the final decision. In 2007 Lu et al.[11]-explains that, a novel framework to robustly and efficiently detect DDoS attacks and identify attack packets. The key idea of their framework is to exploit spatial and temporal correlation of DDoS attack traffic. They designed a perimeter-based anti-DDoS system, in which traffic is analyzed only at the edge routers of an ISP network. In 2007 Shinde et al.[12]- Proposed a method that considers the traffic in a network as a time-series and smoothens it using exponential moving average and analyzes the smoothened wave using energy distribution based on wavelet analysis. The parameters they used to represent the traffic are number of bytes received per unit time and the proportion between incoming and outgoing bytes. By analyzing the energy distribution in the wavelet form of a smoothened time-series, growth in the traffic, which is the result of a DoS attack can be detected very early. In 2007, Yu Chen[13] - approach is to monitor the spatiotemporal pattern of the attack traffic. They had simulated the new defense system on the DETER testbed. The new scheme is proven scalable to cover hundreds of ISP-controlled network domains. With 4 network domains working collaboratively. In 2008, Shui Yu et al.[14]- They focused on detection of DDoS attacks in community networks. their motivation comes from discriminate the DDoS attacks from surge legitimate accessing, and identify attacks at the early stage, even before the attack packages reaching the target server. If the entropy rates are the same or the difference is less than a given value, then they can confirm that it is an attack, otherwise, it is a surge of legitimate accessing. In 2009, Rastegari et al.[15]**-** introduced an intrusion detection system for Denial of Service (DoS) attacks against Domain Name System (DNS). Their system architecture consists of two most important parts: a statistical pre-processor and a neural network classifier. The pre-processor extracts required statistical features in a short time frame from traffic received by the target name server. They compared three different neural networks for detecting and classifying different types of DoS attacks. In 2009, Xie et al.[16].- Creating defenses for attacks requires monitoring dynamic network activities in order to obtain timely and signification information. While most current effort focuses on detecting Net-DDoS attacks with stable background traffic, They proposed a detection architecture in this paper aiming at monitoring Web traffic in order to reveal dynamic shifts in normal burst traffic, which might signal onset of App-DDoS attacks during the flash crowd event.The proposed method is based on PCA, ICA, and HsMM. In 2009, Giseop No et al.[17].-had proposed a fast entropy scheme that can overcome the issue of false negatives and will not increase the computational time. their simulation shows that the fast entropy computing method not only reduced computational time by more than 90% compared to conventional entropy, but also increased the detection accuracy compared to conventional and compression entropy approaches. In 2009, Gupta et al.[18]- reports the design principles and evaluation results of their proposed framework that autonomously detects and accurately characterizes a wide range of flooding DDoS attacks in ISP network. Attacks are detected by the constant monitoring of propagation of abrupt traffic changes inside ISP network. For this, a newly designed flow-volume based approach (FVBA) is used to construct profile of the traffic normally seen in the

network, and identify anomalies whenever traffic goes out of profile.Six-sigma method is used to identify threshold values accurately for malicious flows characterization. In 2009, Cheng et al.[19] -proposed a IP Flow Interaction Behavior Feature (IFF) algorithm. Using IFF time series of the network flow, the network flow states are defined as Health State, Quasi Health State, and Abnormal State. Based on three network states, they propose an efficient DDoS detection method (DASA). Analysis and experiments shows that, IFF can reflect the interaction characteristics of the normal flows and the essential features of DDoS attack, and it is well general DDoS attack diagnosis feature; DASA can effectively distinguish normal flows from abnormal flows containing DDoS attack flow, and it can realize fast detection with high detection rate and low false positive rate. In 2009, Chen et al[20]- proposed a new detection method for DDoS attack traffic based on two-sample t-test. They first investigate the statistics of normal SYN arrival rate (SAR) and confirm it follows normal distribution. The proposed method identifies the attack by testing 1) the difference between incoming SAR and normal SAR, and 2) the difference between the number of SYN and ACK packets. In 2009, Tavallaee et al.21]-analyzed the entire KDD data set. The analysis showed that there are two important issues in the data set which highly affects the performance of evaluated systems, and results in a very poor evaluation of anomaly detection approaches. To solve these issues, they had proposed a new data set, NSL-KDD , which consists of selected records of the complete KDD data set. In 2010, Nguyen et al.[22]-introduced a method for proactive detection of DDoS attacks, by classifying the network status, to be utilized in the detection stage of the proposed anti-DDoS framework. Initially, they analyse the DDoS architecture and obtain details of its phases. Then, they investigate the procedures of DDoS attacks and select variables based on these features. Finally, they applied the k-nearest neighbour (k-NN) method to classify the network status into each phase of DDoS attack. The simulation result showed that each phase of the attack scenario is classified well and they are detected DDoS attack in the early stage. In 2010, Rastegari, et al.[23]- they introduced two different types of DoS attacks against DNS which are direct DoS and amplification attacks. The investigation of the impact of DoS attacks against DNS traffic led us to find the suspicious behaviours. Based on these patterns the required traffic data for analytical measurements was simulated using the most flexible network simulator, NS-2. Finally, a machine learning based system is proposed for detecting and classifying DoS attacks against DNS using several traffic statistics. The performance comparison results show that a back propagation neural network outperforms other classifiers with 99.55% detection rate for direct DoS attacks, 97.82% detection rate for amplification attacks, 99% accuracy, and 0.28% false alarm rate. In 2010, Leu et al. [24]-proposed an agent based intrusion detection architecture, which is a distributed detection system, which uses Goodness of fit test of chi-square test to detect DoS attacks. to detect DoS/DDoS attacks by invoking a statistic approach that compares source IP addresses' normal and current packet statistics to discriminate whether there is a DoS/DDoS attack. It first collects all resource IPs' packet statistics so as to create their normal packet distribution. Once some IPs' current packet distribution suddenly changes, very often it is an attack.It analyzes amount and variation of source address that send packets to us, and statistics of IP address distribution. In 2010,Lee et al.[25]- had proposed SIP-aware DDoS Attack Detection System that can monitor SIP signaling flow and detect SIP-aware DDoS attack. The proposed system collects attributes of SIP traffic, and executes anlaysing and detecting based on statistic and behavior.In 2011, Ankali et al.[26**]-** designed two independent architectures for HTTP and FTP which uses an extended hidden semi-Markov model is proposed to describe the browsing habits of web searchers. A forward algorithm is resulting for the online implementation of the model based on the M-algorithm in order to reduce the computational amount introduced by the model's large state space. In 2011,Xiang et al.[27].- Explains two effective information metrics for low-rate DDoS attacks detection: generalized entropy and information distance metric.In particular, these metrics can improve the systems' detection sensitivity by effectively adjusting the value of order alpha of the generalized entropy and information distance metrics. As the proposed metrics can increase the information distance (gap) between attack traffic and legitimate traffic, they can effectively detect low-rate DDoS attacks early and reduce the false positive rate clearly. In 2011, Huang et al.- motivated by the advancement in radio technology, They introduce a new type of jamming-DJN, which is composed of a large number of tiny, low-power jammers. They demonstrated that DJN can cause a phase transition in target network performance even when the total jamming power is held constant. They explained the phase transition using percolation theory, analyzed scaling behavior of node density and number of nodes in DJN, and they also investigated the impact of DJN topology on the jamming effectiveness.[28] In 2011, Karimazad et al.[29]- They proposed an anomaly-based DDoS detection method based on the various features of attack packets, obtained from study the incoming network traffic and using of Radial Basis Function (RBF) neural networks to analyze these features. They evaluate the proposed method using there simulated network and UCLA Dataset. In 2011, Garg et al.[30]- Explains that the various detection algorithms which are using data mining concepts & algorithms for DDoS detection & prevention. they presented various significant areas where data mining techniques seem to be a strong candidate for detecting and preventing DDoS attack. In 2011, kumarasamy et al.[31]- proposed method provides the strong defense against the malicious hosts in the network, and it easily identifies the attacker hosts by their traffic nature and blocks all the traffic from the attacker hosts. Client puzzles gives the advantage to validate the suspected hosts in order to conform whether the suspected hosts from an attacker or

from a legitimate user. Pushback helps to outsource the client puzzle work load to upstream router, which helps to decrease the processing work load on intelligent router. Using the proposed work, the attacker traffic is effectively blocked at the edge routers and hence the denial of service causing attacks can be identified in advance and offended successfully. In 2012, Renuka Devi et al.[32]- They proposed a detection scheme based on the information theory based metrics. The proposed scheme has two phases: Behaviour monitoring and Detection. In the first phase, the Web user browsing behaviour is captured from the system log during nonattack cases. Based on the observation, Entropy of requests per session and the trust score for each user is calculated. In the detection phase, the suspicious requests are identified based on the variation in entropy and a rate limiter is introduced to downgrade services to malicious users. In 2012, Bhange et al.[33]- This paper has presented idea about the DDoS Attacks and their impact on network traffic. Here paper studied a DDoS attack to analysis the distribution of network traffic to recognize the normal network traffic behavior. This Paper has also discussed flooding attacks. The EM algorism is discussed to approximate the distribution parameter of Gaussian mixture distribution model. Another time series analysis method is studied. This paper also discussed a method to recognize anomalies in network traffic, based on a non restricted α-stable model and statistical hypothesis testing. In 2012, Shiaeles at al.[34]- proposed an approach for detecting a DDoS attack using a fuzzy estimator on the mean time between network events. The proposed method is capable of detecting a DDoS and identifying the malicious IPs before the victim service suffers from exhaustion of resources due to the attack. The method can run on a mid-range PC and can provide near-real time DDoS detection. they are implementing a version of the algorithm which will be compatible to NVidia's CUDA framework and they are also considering a non-preemptive OS kernel. In 2012, Jadhav et al.[35]- With profiling of web browsing behaviour, the sequence order of web page request can be used for detecting Application layer DDoS (App_DDoS) attacks. Based on Hidden semi-Markov model (HsMM) ,a novel anomaly detector is used to describe the browsing behaviour of web users.Their method detects App- DDoS attacks with an averaged DR of 86.7% and an averaged FPR of 4.5% when the error threshold is set at $\mu + 2.5s$. These values demonstrate. In 2012, Devi et al[36]- proposed a hybrid detection scheme based on the trust information and information theory based metrics. Initial filtering is based on the trust value scored by the client. Then the information based metric, entropy, is applied for final filltering of suspicious flow. In 2012, Jeyanthi et al.[37]- analyzes the DDoS and Flash crowds characteristics and proposes a new entropy based DDoS and Flash crowds distinguishing method in VoIP network. They validate their method by simulation, and the results suggest ,their method can be used to detect Flash crowds and DDoS attacks on VoIP call processing servers. They observes the traffic condition and the purpose of dealings varies which helps in outwitting the attackers. In 2012, Akyazi et al.[38]-had proposed distributed intrusion detection methods to detect Distributed Denial of Service attacks in a special dataset and test these methods in a simulated-real time environment, in which the mobile agents are synchronized with the timestamp stated in the dataset.All of their methods use the alarms generated by SNORT, a signature-based network intrusion detection system. they used mobile agents in their methods on the Jade plat- form in order to reduce network bandwidth usage and to decrease the dependency on the central unit for a higher reliability. In 2012, Reddy et al.[39]- They proposed an effective and efficient IP Traceback scheme against DDOS attacks based on entropy variations.This paper employs by storing the information of flow entropy variations at routers. Once the DDOS attack has been identified it performs pushback tracing procedure. The Traceback algorithm first identifies its upstream router where the attack flows comes from and then submits the Traceback request to the related upstream router. In 2012. François et al.[40].-They addressed the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms of FireCol. Proposed FireCol, a scalable solution for the early detection of flooding DDoS attacks The core of FireCol is composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level.The evaluation of FireCol using extensive simulations and a real dataset is presented, showing FireCol effectiveness and low overhead, as well as its support for incremental deployment in real networks. In 2012, Alenezi et al.[41]- The key observation of this survey paper is that a CUSUM-based detection technique has many advantages over other statistical instruments in that it is nonparametric; consequently, it does not require training and is more robust to variations in the attack profile. In 2013, Javidi et al.[42]- They considered some different agents, each of which can detect one or two DOS attacks. These agents interact in a way not to interfere each other. Parallelization Technology is used to increase system speed. Since the designed agents act separately and the result of each agent has no impact on the others, you can run each system on discrete CPUs (depending on how many CPUs are used in IDS computers) to speed up the performance. In 2013, CHEN et al.[43]- they explained DOS attack detection model based on conditional random fields (CRF) . The CRF based model incorporates the signaturebased and anomaly-based detection methods to a hybrid system. The selected features include source IP entropy, destination IP entropy, source port entropy, destination port entropy, protocol number and etc. The CRF based model combines these IP flow entropies and other fingerprints into a normalize entropy as the feature vectors to depict the states of the monitoring traffic. In 2013, Kumari et al.[44]- They introduced Bottom-up approach, New Cracking algorithm,Prevention algorithm using IDS node for detecting and controlling DDoS attack in MANET.They had most of the problems of wired networks and many more due to their specific features:

dynamic topology, limited resources, lack of central management points. First, they had presented specific vulnerabilities of this new environment. Then they had surveyed the attacks that exploit these vulnerabilities and the possible proactive and reactive solutions proposed in the literature. In 2013, Balamurugan et al.[45]- They proposed an effective and efficient IPv6, UDP based DDoS attacks based on entropy variations.Here the traceback strategy is avoided, because it suffers a number of drawbacks and times. This paper employs by storing the information of flow entropy variations at routers. Once the DDoS attack has been identified it performs to delete the attacker request. The entropy variation first identifies its upstream router where the attack flows comes from and then submits the threshold level checking of the destination packets In 2014, Thwe Oo et al.[46]- presented both detecting and classifying sheme of DDoS attack using K-NN. The two proposed algorithms are developed based on various features of attack packets obtained from study the incoming and outgoing network traffic and used K-Nearest Neighbour to analyze these features. The main objectives of this paper are to analyze the DDoS attacks natures and to detect and identify types of DDoS attacks. In 2014, J.Welkin Eyes et al.[47]- neuro-fuzzy systems were proposed as subsystems of the ensemble. Sugeno type Neuro-Fuzzy Inference System has been chosen as a base classifier for their research. Single classifier makes error on different training samples. So, by creating the classifiers and combining their outputs, the total amount of error can be reduced and the detection accuracy can be increased.The experiments and the evaluations of the proposed method were performed with the KDD Cup 99 intrusion detection Dataset. In 2014, NAVALE et al.[48]- They proposed detection of DDos attack by using Counter based algorithm and Access Pattern algorithm which will implemented in Hadoop framework. Dashboard provides visual view which will help to unveil the attacker and loyal user along with statistics. the system which consists of implementation Counter based and Access pattern algorithm by using Map Reduce in Hadoop. With this they are using analytics to predict the future behaviour of attacker. The better user interface provided by means of Dashboard. Cardenas et. al.[49]- provided novel formulations for the rapid detection of these attacks in the control-theoretic framework of change detection. they presented an algorithms that effectively can detect worms from their temporal spreading characteristics. they described the effects of the network topology on the algorithms and their performance. they next present algorithms for detecting DDoS while discriminating against changes in the normal traffic.

3. SUMMARY & DISCUSSION

Many system and techniques are used to detect the Dos attack efficiently.DOS can be detected by using such as data mining , machine learning and statistical analysis. these proposed systems commonly suffer from high false positive rates because the correlations between features/attributes are intrinsically neglected or the techniques do not manage to fully exploit these correlations. Vern Paxson [2] developed a system called “Bro” a system for finding a network attacker in real time. It is a standalone system, which emphasizes high speed monitoring, real time, clear separation to achieve this Bro system. Yu chin et al. [10] explain, the idea is to detect the abrupt traffic changes across multiple networks domain. Chin developed a architecture called Distributed Change Point Detection (DCD) using Change Aggregation Tree (CAT), it is suitable for efficient implementation and it is operated by ISP. To resolve this issue, a secure infrastructure protocol is developed to establish the mutual trust or consensus. Chin – Fong Tsai et al.[50] tells a new method to detect the dos attack called “Triangle Area Based Nearest Approach”. Specifically, the k- means is used to extract the clusters centre where each one represent a one particular attack. The k-NN classifier is used to detect intrusion. By using this approach improve in terms of accuracy, detection state, and false detection rate. Theerasak et al.[51] explain about Dos attack is carried out by attack tools like worms, botnet and also the various forms of attacks packets to beat the defense system, so they propose a technique called “Behavior based Detection” that can discriminate Dos attack traffic from real method.The above method is comparable detection method; it can extracted the repeatable features of packets arrival. The Behavior Based Detection can differentiate traffic of an attack sources from legitimate traffic work with a quick response. The resulting performance so far is good enough to protect the server from crashing during a Dos attack.To deal with the above problems, an approach based on triangle area was presented to generate better discriminative features. However, this approach has dependency on prior knowledge of malicious behaviours. Tan et al. proposed a more sophisticated non-payload based DoS detection approach using Multivariate Correlation Analysis (MCA). Following this emerging idea, present a new MCA-based detection system to protect online services against DoS attacks , which is built upon previous work in [52]. In addition to the work shown in [52].

4. CONCLUSION

Denial of Service (DOS)attacks constitute one of the greatest problem in network security. The detection of DOS attack is a challenging task. This paper presents a survey on various DOS attack detection techniques that was proposed earlier by researcher. various authors view their algorithms as a best and efficient. Most of them compare their proposed work with existing work. DOS attack detection methods have been extensively studied. Each method has its own advantages and disadvantages. An attempt towards investigating a new approach is necessary to overcome the drawbacks.

REFERENCES

[1] C. Douligeris, and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art" Computer Networks 44 (2004) 643–666, October 2003

[2] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time,"The Proceedings of the 7th USENIX Security Symposium San Antonio, Texas, January 26-29, 1998

[3] P. Garcı´a-Teodoro, J. Dı´az-Verdejo, G. Macia´-Ferna´ndez, E. Va´zquez "Anomaly-based network intrusion detection:Techniques, systems and challenges," comp u t e r s & s e c u r i t y 2 8 (2 0 0 9) 1 8 – 2 8

[4] S. Noh, C. Lee, K. Choi, and G. Jung" Detecting Distributed Denial of Service (DDoS) Attacks through Inductive Learning" by the Korea Research Foundation under grant KRF-2002-041- D00465, IDEAL 2003, LNCS 2690, pp. 286–295, 2003.

[5] L. Limwiwatkul' and A. Rungsawangr "Distributed Denial of Service Detection using TCP/IP Header and Traffic Measurement Analysis" lntanational Syinposium on Communications and Information Technologes (ISCIT 2004)Sappom, Japrui. Octohcr 26- 29. 2004

[6] M. Kim, H. Na, K. Chae, H. Bang, and J. Na "A Combined Data Mining Approach for DDoS Attack Detection" ICOIN 2004, LNCS 3090, pp. 943–950, 2004.

[7] D. Gavrilis, E. Dermatas "Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features" Computer Networks 48 (2005) 235–245 . 21 December 2004

[8] A. Mitrokotsa, C. Douligeris "Detecting Denial of Service Attacks Using Emergent Self-Organizing Maps" IEEE International Symposium on Signal Processing and Information Technology 2005

[9] H. Sengar H. Wang D. Wijesekera S. Jajodia "Fast Detection of Denial-of-Service Attacks on IP Telephony" Center for Secure Information Systems Department of Computer Science George Mason University College of William and Mary Fairfax, VA 220301-4244-0476-2/06/©2006 IEEE

[10] Yu Chen, Kai Hwang, and Wei-Shinn Ku, Collaborative Detection of DDoS Attacks over Multiple Network Domains" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, TPDS-0228-0806.2007

[11] Kejie Lu a, Dapeng Wu b, Jieyan Fan b, Sinisa Todorovic c, Antonio Nucci "Robust and efficient detection of DDoS attacks for large-scale internet" Computer Networks 51 (2007) 5036–5056

[12] P. Shinde, S. Guntupalli" Early DoS Attack Detection using Smoothened Time-Series andWavelet Analysis" Third IEEE International Symposium on Information Assurance and Security0-7695-2876-7/07 © 2007.

[13] Yu Chen, Kai Hwang, Wei-Shinn Ku" Distributed Change-Point Detection of DDoS Attacks: Experimental Results on DETER Testbed" Department of Electrical and Computer Engineering SUNY – Binghamton Binghamton, NY 13902, 2007

[14] Shui Yu and Wanlei Zhou" Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks" Sixth Annual IEEE International Conference on Pervasive Computing and Communications 0-7695-3113-X/08©2008

[15] S.Rastegari, M. Iqbal Saripan and M. Fadlee A. Rasid" Detection of Denial of Service Attacks against Domain Name System Using Neural Networks" IJCSI International Journal of Computer Science Issues, Vol. 6, No. 1, 2009

[16] Yi Xie and Shun-Zheng Yu" Monitoring the Application-Layer DDoS Attacks for Popular Websites" IEEE/ACM Transactions On Networking, VOL. 17, NO. 1, FEBRUARY 2009

[17] Giseop No† and Ilkyeun Ra" An Efficient and Reliable DDoS Attack Detection Using a Fast Entropy Computation Method" Department of Computer Science and Engineering University of Colorado Denver, Campus Box 109, 1200 Larimer St., Denver, CO80204, USA 2009. 978-1-4244-4522-6/09/ ©2009 IEEE

[18] B. B. Gupta, R. C. Joshi and M. Misra" Dynamic and Auto Responsive Solution for Distributed Denial-of-Service Attacks Detection in ISP Network" International Journal of Computer Theory and Engineering, Vol. 1, No. 1, April 2009 1793-8201

[19] J. Cheng, B. Zhang, J. Yin, Yun Liu, and Z. Cai" DDoS Attack Detection Using Three-State Partition Based on Flow Interaction" School of Information Science and Engineering, Central South University, Changsha, 410083, CCIS 58, pp. 176–184, 2009

[20] Chin-Ling Chen" A New Detection Method for Distributed Denial-of-Service Attack Traffic based on Statistical Test" Journal of Universal Computer Science, vol. 15, no. 2 (2009), 488-504

[21] M. Tavallaee, E. Bagheri, Wei Lu, and Ali A. Ghorbani" A Detailed Analysis of the KDD CUP 99 Data Set"proceedings of the 2009 IEEE symposium on computational intelligence in security and defence Applications(CISDA 2009)

[22] Hoai-Vu Nguyen and Y. Choi" Proactive Detection of DDoS Attacks Utilizing k-NN Classifier in an Anti-DDos Framework" World Academy of Science, Engineering and Technology, International Science Index Vol:4, No:3, 2010

[23] S. Rastegari, M. Iqbal Saripan and Mohd Fadlee A. Rasid" Detection of Denial of Service Attacks against Domain Name System Using Machine Learning Classifiers" Proceedings of the World Congress on Engineering Vol I WCE 2010, June 30 - July 2, 2010, London, U.K

[24] Fang-Yie Leu & I-Long Lin *"A DoS/DDoS Attack Detection System Using Chi-Square Statistic Approach" ISSN: 1690-4524 Systemics, Cybernetics And Informatics VOLUME 8 - NUMBER 2 - YEAR 2010

[25] Do-Yoon Ha, Chang-Yong Lee,Hyun-Cheol Jeong, Bong-Nam Noh" Design and Implementation of SIP-aware DDoS Attack Detection System" Advances in Information Sciences and Service Sciences Volume 2, Number 4, December 2010

[26] Dr. D V Ashoka" Detection Architecture of Application Layer DDoS Attack for Internet" Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:984-990 (2011)

[27] Y. Xiang, Ke Li, and W. Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011

[28] H. Huang, *Member, IEEE*, N.Ahmed, and P. Karthik "On a New Type of Denial of Service Attack in Wireless Networks:The Distributed Jammer Network" IEEE Transactions On Wireless Communications, VOL. 10, NO. 7, JULY 2011

[29] R. Karimazad1 and A. Faraahi2" An Anomaly-Based Method for DDoS Attacks Detection using RBF Neural Networks" **2**011 International Conference on Network and Electronics Engineering IPCSIT vol.11 © (2011)

[30] K. Garg 1 , R. Chawla "Detection Of Ddos Attacks Using Data Mining" International Journal of Computing and Business Research (IJCBR) ISSN (Online) : 2229-6166 Volume 2 Issue 1 2011

[31] S. kumarasamy and Dr.R.Asokan "Distributed Denial Of Service (Ddos)Attacks Detection Mechanism" International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.5, December 2011

[32] S. Renuka Devi and P. Yogesh "DETECTION OF APPLICATION LAYER DDOS ATTACKS USING INFORMATION THEORY BASED METRICS" Department of Information Science and Technology,College of Engg. Guindy, Anna University, Chennai. India pp. 217–223, 2012.

[33] A. Bhange, A. Syad, S. Singh Thakur " DDoS Attacks Impact on Network Traffic and its Detection Approach**"** International Journal of Computer Applications (0975 – 8887) Volume 40– No.11, February 2012

[34] S. N. Shiaeles a, V. Katos a, A. S. Karakos a, Basil K. Papadopoulos" Real time DDoS detection using fuzzy estimators" computers & s e c u r i t y 3 1 (2 0 1 2) 7 8 2 -7 9 0

[35] V. Jadhav and P. Devale" Hidden Semi-Markov Model For Detecting Application Layer Ddos Attacks" International Journal of Advances in Engineering & Technology, May 2012.

[36] S. Renuka Devi and P. Yogesh" A Hybrid Approach To Counter Application Layer Ddos Attacks**"** International Journal on Cryptography and Information Security(IJCIS),Vol.2, No.2, June 2012

[37] N. Jeyanthi1 and N. Ch. Sriman Narayana Iyengar" An Entropy Based Approach to Detect and Distinguish DDoS Attacks from Flash Crowds in VoIP Networks" International Journal of Network Security, Vol.14, No.5, PP.257-269, Sept. 2012

[38] U. Akyazi & A. Sima Uyar "Distributed Detection Of Ddos Attacks During The Intermediate Phase Through Mobile Agents" Computing and Informatics, Vol. 31, 2012, 759–778

[39] V.Sus hma Reddy, 2K.Damodar Rao, 3P.Sowmya Laks hmi" Efficient Detection of Ddos Attacks by Entropy Variation" IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 7, Issue 1 (Nov-Dec. 2012), PP 13-18

[40] J. François, I. Aib and R. Boutaba "*FireCol*: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 20, NO. 6, DECEMBER 2012

[41] M. Alenezi & M. J Reed" Methodologies for detecting DoS/DDoS attacks against network servers" ICSNC 2012 : The Seventh International Conference on Systems and Networks Communications ISBN: 978-1-61208-231-8 ,2012

[42] M. Masoud Javidi, M. Hassan Nattaj" A New and Quick Method to Detect DoS Attacks by Neural Networks" Journal of mathematics and computer Science 6 (2013), 85-96

[43] Shi-wen CHEN, Jiang-xing WU, Xiao-long YE, Tong GUO" Distributed Denial of Service Attacks Detection Method Based on Conditional Random Fields" JOURNAL OF NETWORKS, VOL. 8, NO. 4, APRIL 2013

[44] Geetika, *N. Kumari* " Detection and Prevention Algorithms of DDOS Attack in MANETs" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013

[45] D. Balamurugan1, S. Chandrasekar2, D. Jaya Prakash3, M.Usha4" Analysis of Entropy Based DDoS Attack Detection to Detect UDP Based DDoS Attacks in IPv6 Networks" International Journal of Information and Computation Technology (IJICT) ISSN 0974-2239 Volume 3, Number 10 (2013)

[46] T. Thwe Oo & T. Phyu" Statistical Anomaly Detection of DDoS Attacks Using K-Nearest Neighbour" International Journal of Computer & Communication Engineering Research (IJCCER)Volume2 - Issue 1 January 2014

[47] J.Welkin Eyes, S.Karthiprem, E.Thangadurai "High Accuracy Detection Of Denial Of Service Attack Based On Triangle Map Generation**"** International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 90-96

[48] G.S. Navale, V. Kasbekar, V. Ganjepatil, S. Bugade" Detecting And Analyzing Ddos Attack Using Map Reduce In Hadoop" International Journal of Industrial Electronics and Electrical Engineering, Volume- 2, Issue- 2, Feb.-2014

[49] A. A. Cardenas, J. S. Baras and V. Ramezani" Distributed Change Detection for Worms, DDoS and other Network Attacks".

[50] 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.

[51] Theerasak T., Shui Yu, W. Zhou and G. Beliakov" Discriminating DDoS Attack traffic from Flash Crowd through Packet Arrival Patterns" The first international workshop on security in computers,networking and communications

[52] Z. Tan, A. Jamdagni, Xi, P. Nanda and R. Ping Liu, A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:25 NO:2 YEAR 2014