# RESEARCH OVER DIFFERENT TECHNIQUES IN IMPLEMENTATION TO DETECT DOS ATTACKS IN CURRENTINTERNET ERA

**Swarooparani[1]*, Dr. Sridevi[2]**

**Abstract—** The Inreasing Frequency Of Denial-Of-Service (Dos) Assaults Puts The Dependability And Accessibility Of Network Services At Danger. It Is Necessary To Have Efficient Dos Attack Detection Mechanisms. By Using The Suggested Analysis Method, Significant Correlated Data Can Be Provided. Among The Features, Blending In Utilizing This Undiscovered Data, The Accuracy Of Detection Can Be Greatly Improved.

**Keywords—**Dos, DDos, Denial-of-Service Attack, Euclidean Distance Map, Multivariate Correlations, Anomaly Detection.

[1]*Dept. Of Computer Science Engineering (Faculty of Engineering & technology(Exclusive for Women)) Sharnbasva University, Kalaburagi, India
2Dept. Of Computer Science Engineering (Faculty of Engineering & technology(Exclusive for Women)) Sharnbasva University, Kalaburagi, India

***Corresponding Author:** Swarooparani
*Dept. Of Computer Science Engineering (Faculty of Engineering & technology(Exclusive for Women)) Sharnbasva University, Kalaburagi, India

**DOI**: 10.53555/ecb/2024.13.02.09

## I. INTRODUCTION (*HEADING 1*)

This template, modified in MS Word 2007 and saved as a–Word 97-2003 Document‖ for the PC, provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

## II. RESEARCH OVER DIFFERENT AUTHORS ON DOSDETECTION

Fei Wang, Xiaofeng Hu, Xiaofeng Wang, Jinshu Su,Xicheng Lu has published with title –UNFAIR RATE LIMITING ON TRAFFIC AGGREGATES FOR DDOS ATTACKS MITIGATION‖ and they propose Distributed Denial of Service (DDoS) attacks pose a threat to network applications. Many countermeasures have been proposed to tackle such attacks. This paper focuses on DDoS mitigation techniques, the practical way to filter attack traffic and keep victims alive. To rate limit attack traffic with as little normaltraffic affected as possible, not just the amount of increased volume, but also how increased traffic is propagated in the network, denoted by traffic increasing patterns, is considered. Here they have propose unfair rate limiting (URL), in which traffic aggregates are given different priority by extracting increasing patterns and analyzing their relationship with DDoS attacks. Aggregates more likely to include attacks traffic are punished harder during mitigation. Basic and fine-grained unfair rate limiting mechanisms (BURL and FURL) are presented upon port-flows andbitwise-flows, respectively. Simulation results show that both two mechanisms can effectively mitigate DDoS attacks.But FURL outperforms BURL in filtering attack traffic without dropping normal packets. And they also conclude that their paper proposes an unfair rate limiting mechanism to tackle DDoS attacks. Instead of treating all traffic aggregates fairly during DDoS mitigation, we also consider the traffic increasing patterns, and in this way, divide traffic aggregates into three subsets with different mitigation priorities. As a result, traffic aggregates that most likely include DDoS attack traffic are suppressed most. We apply URL two-level traffic aggregates, port-flow and bitwise-flow, thus presenting BURL and FURL, respectively. Through experiments, they prove outstanding performances of proposed mechanisms. Fine-grained FURL works better in filtering attack traffic while dropping as few normal packets as possible.

Jiahui Jiao1, Benjun Ye1, Yue Zhao1, Rebecca J. Stones1,Gang Wang1, Xiaoguang Liu1*, Shaoyan Wang2, Guangjun Xie2 has published a paper regarding –Detecting TCP-based DDoS Attacks in Baidu Cloud Computing Data Centers‖ these authors abstracts Cloud computing data centers have become one of the most important infrastructures in the big-data era. When considering thesecurity of data centers, distributed denial of service (DDoS) attacks are one of the most serious problems. Here considering DDoS attacks leveraging TCP traffic, which are increasingly rampant but are difficult to detect. To detect DDoS attacks, we identify two attack modes: fixed source IP attacks (FSIA) and random source IP attacks (RSIA), based on the source IP address used by attackers. We also propose a real-time TCP-based DDoS detection approach, which extracts effective features of TCP traffic and distinguishes malicious traffic from normal traffic by two decision tree classifiers. We evaluate the proposed approach using a simulated dataset and real datasets, including the ISCX IDS dataset, the CAIDA DDoS Attack 2007 dataset, and a Baidu Cloud Computing Platform dataset. Experimental results show that the proposed approach can achieve attack detection rate higher than 99% with a false alarm rate less than 1%. This approach will be deployed to the victim-end DDoS defense system in Baidu cloud computing data center. And their research describe and test a TCP-based DDoS attack detection method. It focuses on two identified attack modes (fixed source IP attacks and random source IP attacks) and provides a different detectionstrategy for each. We examine the proposed method with four datasets: one simulated dataset, one ISP dataset and twopublic datasets. The experimental results demonstrate it can identify the different attack modes and distinguish benign network traffic from main TCP-based attacks with high attack detection rates and low false alarm rates. We test the proposed method in Baidu data centers, and it will be deployed to the

Baidu Cloud Computing Platform to detect TCP-based DDoS attacks.

Xiaoyu Liang, Taieb Znati has published an paper on An empirical study of intelligent approaches to DDoS detection in large scale networks, and has explained their research work as Distributed Denial of Services (DDoS)attacks continue to be one of the most challenging threats to the Internet. The intensity and frequency of these attacks are increasing at an alarming rate. Numerous schemes have been proposed to mitigate the impact of DDoS attacks. This paper presents a comprehensive empirical evaluation of Machine Learning (ML)-based DDoS detection techniques, to gain better understanding of their performance indifferent types of environments. To this end, a framework is developed, focusing on different attack scenarios, to investigate the performance of a class of ML-based techniques. The evaluation uses different performancemetrics, including the impact of the ―Class Imbalance Problem‖ on MLbased DDoS detection. The results of the comparative analysis show that no one technique outperforms all others in all test cases. Furthermore, the results underscore the need for a method oriented feature selection model to enhance the capabilities of ML-based detection techniques. Finally, the results show that the class imbalance problem significantly impacts performance, Underscoring the need to address this problem in order to enhance ML-based DDoS detection capabilities. And given the conclusive report as they conduct a series of experimentsto explore the advantages, limitations and influential factors for ML-based DDoS detection techniques. Instead of studying specific solutions, our work focus on empirically evaluating the ―building blocks‖, which are commonly shared among intelligent DDoS detection schemes. A comparative analysis of the overall performance of these techniques is carried out, to provide a better understanding of the techniques‘ capabilities to detect DDoS attacks. Although the comparative results show that no single technique that outperforms all others in all test cases, the detection capabilities exhibited by ML-based techniques are evident. Additionally, different techniques exhibit different preferences over feature types, emphasizing the significance of feature selection and suggesting that feature selectionshould be model oriented. A sensitivity analysis illustrates the influence of the observed traffic proportions on the performance of these techniques. As expected, the observed traffic proportions severely impact the performance of traditional detection methods that rely on monitoring the two-way traffic, while ML-based techniques display weak correlation with the proportion of the observed traffic.

Lastly, we explored the impact of the class imbalance problem on the performance of ML-based techniques. The results show that the impact of the class imbalance problem should not be underestimated, especially with respect to the dynamically evolving nature of DDoS attacks. Future work can be focused on investigating an ensemble of intelligent schemes, strategically distributed across the network, using an appropriate feature selection model for an adaptive and efficient DDoS detection.

Anteneh Girma, Moses Garuba, Jiang Li, Chunmei Liu has also published an paper on ―Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment‖ and has explained their research work as Cloud service availability has been one of the major concerns of cloud service providers (CSP), while hosting different cloud based information technology services by managing different resources on the internet. The vulnerability of internet, the distribute nature of cloud computing, various security issues related to cloud computing service models, and cloud‘s main attributes contribute to its susceptibility of security threats associated with cloud service availability. One of the major sophisticated threats that happen to be very difficult and challenging to counter due to its distributed nature and resulted in cloud service disruption is Distributed Denial of Service (DDoS) attacks. Even though there are number of intrusion detection solutions proposed by different research groups, and cloud service providers (CSP) are currently using different detection solutions by promising that their product is well secured, there is no such a perfect solution that prevents the DDoS attack. The characteristics of DDoS attack, i.e., having different appearance with different scenarios, make it difficult to detect. This paper will review and analyze different existing DDoS detecting techniques against different parameters, discusses their advantage and disadvantages, and propose a hybrid statistical model that could significantly mitigate these attacks and be a better alternative solution for current detection problems. And alsoproposed an effective alternative hybrid scheme against DDoS attacks based on Entropy and Covariance Matrices. We are looking forward to apply a different approach with a comprehensive hybrid detection scheme at both the network and host level. Because, many of the available DDoS detection schemes performance found to be below the par and DDoS attacks are growing exponentially, it prompts the real need of having a comprehensive solution. We believe that this proposed scheme with double check points is expected to be a better alternative solution in mitigating the risk significantly by producing a better result.

Akashdeep Bhardwaj, Gvb Subrahmanyam, Vinay Avasthi, Hanumat Sastry, Sam Goundar has published an paper on

–DDoS Attacks, New DDoS Taxonomy and Mitigation Solutions – A Survey‖ their research explains as Cloud computing has started to gain acceptance for adoption and implementation among organizations, however, this new technology area has already started to deal with security, performance and availability challenges. Within Cloud Security issues being paramount for the corporates, private enterprises, the denial of service attacks are rated as the highest priority threat to the cloud environments. This study presents a review on the academic literature research work on the DDoS attack on Cloud, introduces a new DDoS

Classification taxonomy and proposes parameters for determining an effective DDoS solution. And has provided and report survey of the academic literature on DDoS attacks against cloud computing from 2009 to 2015. New cloud attack taxonomy and parameters to determine effective DDoS solution is presented. A comprehensive DDoS mitigation solution involves detection, blocking and mitigation in real time as well as be positioned at the DDoS attack source. For this the DDoS detection nodes need to be spread across the internet globally. These nodes are used for the DDoS attack detection, response and prevention. Apart from this feature, the following factors need to be considered for the proposed DDoS mitigation solution as x Functionality – be able to reduce if not block the impact of the DDoS attack, no matter how large or powerful the DDoSflood attack is. x Ease of implementation – does not require any network design modification or infrastructure data flow reconfiguration. Low overhead – should not pose additional overhead on the existing data center systems and processing power. x Recognize Legitimate traffic – should not be reporting large number of false positives where in legitimate traffic is getting dropped during a DDoS blocking process. xFindings - With the new taxonomy classifying DDoS attacks becomes clear and simple since it is based on detailed technical action items which can easily be obtained and measured. Then the impact as well as priority can be ascertained. For an effective DDoS solution, the paper proposed four parameters like mitigation functionality that would help reduce if not block DDoS attack impact, irrespective of the capacity of DDoS flood, then with implementation ease implying no network redesign or modification in the infrastructure, plus not have anyadditional overhead on data center infrastructure and finally be able to recognize the real user legitimate traffic and have as low false positives as possible.

An paper on –Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Trace back Mechanisms‖ has been published by authors Arun Raj Kumar, P. and S. Selvakumar and their research work explains Collaborative applications are feasible nowadays and are becoming more popular due to the advancement in internetworking technology. The typical collaborative applications, in India include the Space research, Military applications, Higher learning in Universities and Satellite campuses, State and Central government sponsored projects, e- governance, e- healthcare systems, etc. In such applications, computing resources for a particular institution/organization spread across districts and states and communication is achieved through internetworking. Therefore the computing and communication resources must be protected against security attacks as any compromise on these resources would jeopardize the entire application/mission. Collaborativeenvironment is prone for various threats, of which Distributed Denial of Service (DDoS) attacks are of major concern. DDoS attack prevents legitimate access to critical resources. A survey by Arbor networks reveals that approximately 1,200 DDoS attacks occur per day. As the DDoS attack is coordinated, the defense for the same has to be a collaborative one. To counter DDoS attacks in a collaborative environment, all the routers need to work collaboratively by exchanging their caveat messages with their neighbors. This paper analyses the security measures ina collaborative environment, identifies the popular DDoS attack tools, and surveys the existing trace back mechanismsto trace the real attacker. And reports the security as Critical information and infrastructure protection is an ongoing process rather than providing a onetime solution. Because yesterday‘s solutions that were implemented become irrelevant today as it has become obsolete. Nowadays DDoS attack happens with legitimate traffic. So with the help of stored attack signatures, it is tedious to detect and trace back. Possible attacks in a collaborative environment and their impacts are identified of which denial of service is a serious threat. There are many DDoS attack tools available to attackers. These tools do not require much technical knowledge in order to launch an attack as these are all automated and can have disastrous effects.

One approach on ―A Real Time System for Denial of service Attack Detection Based on Multivariate Correlation Analysis Approach‖ by Miss Komal K. More, Prof. Pramod B. Gosavi explains how Now-a-days, Denial of Service (DOS) attacks are emerging as most dangerous threat for variety of inter-connected web servers. Internet users require internet for performing different task such as online activities like general information surfing, online banking etc. DOS attack averts the users from using these amenities hence, it is essential to detect DOS attack. This paper demonstrates a novel approach named as Multivariate correlation analysis based denial of service attack detection system in real time. Our MCA approach makes use theprinciples of anomaly based detection system and to speed the process of MCA triangle area approach is implemented over the complete system. MCA calculates the geometrical co-relations between network traffic structures. The efficiency of the system is checked by three different datasets KDD cup 99 dataset, second is the advanced and improved NSL dataset and any real time dataset. And provide an provides an innovative approach dependent uponmultiversity co-relational investigation for finding Denial of service attacks which separates both known/unknown DOS attacks from lawful network traffic records. Essential geometrical co-relational features are pulled out from singular pairs of two dissimilar features, the triangle area map tactic aids to boost up the process speed. We successfully implemented and tested the proposed system over offline and real world datasets with almost 100% detection accuracy which significantly decreased falsepositive rate to almost 0.1 % and more accurate attack detection with increased threshold value ranging between 1ı to 4ı. We have not considered time constraint during implementation of real time approach, thus we can definethe future scope of this approach as implementation of the system over real world data with considering time constraint(time complexity) and finding more enhanced and refined traffic categorization method to reduce the false-positive recognition rate.

An paper on ―Modern Machine Learning for Cyber-defense and Distributed Denial of Service Attacks‖ In computer networks, Denial-of-Service (DoS) attacks attempt to make computers or network resources unavailable for their intended use. DoS attacks are difficult to detect and mitigate since they normally do not attempt to access the private data of their intended victim, but rather intend to disrupt the publicly available resources their victims provide. This paper discusses methods for detecting and mitigating DoS attacks with a focus on techniques that leverage machine learning algorithms. Such algorithms promise to: (a) detect when computer services are being used in an adversarial fashion, (b) separate network traffic into nominal and anomalous components, and (c) provide opportunities for mitigating the attacks while maintaining the integrity of the effected services. The key ingredient of the ideas presented here is the use of correlations and dependencies in computer access patterns, and the larger context in which they exist, to separate the ―wheat‖ -- the real users of the services -- from the ―chaff‖ --the perpetrators who are attempting to disrupt the services has been researched and published by Randy C. Paffenroth, Chong Zhou and reports Denial-of-Service (DoS) attacks can make computers or network resources unavailable for their intended use and they are hard to detect and mitigate since they, in large measure, use the affected services as intended. DoS attacks do not attempt to access the private data of their intended victim, but instead disrupt publicly available resources, such as Internet commerce sites, byoverwhelming them with service requests. Since, by their very nature, such attacks can be difficult to distinguish from nominal traffic, this paper discussed several machine learning methods for detecting and mitigating DoS attacks. Of particular importance for DDoS mitigation are modern methods that leverage deep learning and neural networks. Such methods have been used successfully in many problemdomains, and herein we provided several examples of their use in DDoS mitigation.

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, we propose amultivariate correlation analysis approach to investigate and extract second-order statistics from the observed network traffic records. These second-order statistics extracted by the proposed analysis approach can provide important correlative information hiding among the features. By making use of this hidden information, the detection accuracy can be significantly enhanced. The effectiveness of the proposed multivariate correlation analysis approach is evaluated on the KDD CUP 99 dataset. The evaluation shows encouraging results with average 99.96% detection rate and 2.08% false positive rate. Comparisons also show that our multivariate correlation analysis based detectionapproach outperforms some other current researches in detecting DoS attacks has been researched and published by Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, PriyadarsiNanda, and Ren Ping Liu with paper title as ―Denial-of- Service Attack Detection Based on Multivariate Correlation Analysis‖ and This paper has proposed a Euclidean distance based multivariate correlation analysis approach to extract the inner correlations (second-order statistics) of network traffic records, which can better exhibit the network traffic behaviours. We have evaluated the analysis approach using the KDD CUP 99 dataset. The results show that these second-order statistics can clearly reveal the changes of network behavior caused by DoS attack. The multivariate correlation analysis based DoS attack detection approachachieves 99.96% detection rate and 2.08% false positiverate. The detection accuracy is improved by involving the second-order statistics instead of the original first-order statistics into the classification. However, our approach still suffers from a high false negative rate in detecting Back attack. This may be caused by the non-normalized data or the redundant features in the dataset. Therefore, we will employ data normalization methods and optimal feature selection in our future work in order to improve the detection accuracy. Also, temporal information will be considered in the successive research.

―Low volume viruses: new tools for criminals‖ by author James Kay explains Low volume viruses are a new threat on the corporate horizon. The time between a virus being detected and signatures being issued by the anti-virus software vendors – the virus writer‗s ‗window of exposure‗– can be as little as a few hours and Analysis for a craftier enemy: Analysis like this is becoming more and more important as virus writers up their game with sophisticated techniques to fool reactive virus filters, either developing viruses that won‗t be detected, refining propagation techniques, such a low volume viruses or issuing so many vary ants of a mass distributed virus that patches need to be updated constantly (in 2004 alone, signatures for over 10,000 new viruses or variants of existing viruses were generated, a 30 percent increase on 2003. That‗s more than one every hour). Heuristics analysis should not be used in isolation but it is an important part of the anti-virus mix. Heuristic detection technology is used alongside traditional signature-based anti-virus engines. These filter out known viruses and heuristic detection goes one step further to identify additional potential threats before they are named. The low volume virus is just one example of the innovations that virus writers are employing to circumvent traditional anti-virus defenses. As virus writers get more cunning and threats more specific, the role of heuristics in protecting networks can only increase. Consequently, any company without protection from a heuristics service has a serious exposure to the risk of virus infection

―DDoS attack detection method using cluster analysis‖ by authors Keunsoo Lee, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, Sehun Kim has proposed Distributed Denial of Service (DDoS) attacks generate enormous packets by a large number of agents and can easily exhaust the computing and communication resources of a victim within a short period of time. Here they have a method for proactive detection of DDoS attack by exploitingits architecture which consists of the selection of handlers and agents, the communication and compromise, and attack. We look into the procedures of DDoS attack and then select variables based on these features. After that, we perform cluster analysis for proactive detection of the attack. We experiment with 2000 DARPA Intrusion Detection ScenarioSpecific Data Set in order to evaluate our method. The results show that each phase of the attack scenario is partitioned well and we can detect precursors of DDoS attack as well as the attack itself. And they have an efficient method to detect and control DDoS attacks proactively using cluster analysis. Although there have been lots ofstudies for the detection of DDoS attacks, they mostly focused on the traffic generated during the attack period. To find precursors of a DDoS attack, we look into the feature of the DDoS attack and select nine parameters which show abnormal changes in traffic according to the phases of the attack. After the parameter selection, cluster analysis is applied to form groups into which normal traffic and each phase of the DDoS attack are partitioned. In order to evaluate this detection method, we experiment with 2000 DARPA Intrusion Detection Scenario Specific Data Set. As a result, we can divide data set into normal groups, phase 1, phase 2, attack, and post-attack group, respectively. Among the five phases of the DDoS attack, we can detect three phases and our proposed meth ods show that each phase of the attack scenario is partitioned well. We can detect precursors of the DDoS attack at early phases by using this method, so we can handle the DDoS attack proactively.Moreover, our method is easy to implement since it uses only normalized distance. These features can help construct a defense mechanism against DDoS attacks. There are some issues worthy of future research. In the future work, we expect to analyze network traffic more effectively by extracting more variables and develop an advanced detection algorithm. We analyzed our algorithm for DDoS attack included in 2000 DARPA data set only. It may be desirable to apply the proposed method to different types of DDoS attacks and data sets.

–Evaluation on Multivariate Correlation Analysis Based Denial-of-Service Attack Detection System‖ by authors Zhiyuan Tan, Aruna Jamdagni, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu has proposed a Denial-of- Service (DoS) attack detection system is explored, where a multivariate correlation analysis technique based on Euclidean distance is applied for network traffic characterization and the principal of anomaly-based detection is employed in attack recognition. The effectiveness of the detection system is evaluated on the KDD Cup 99 dataset and the influence of data normalizationon the performance of attack detection is analyzed here as well. The evaluation results and comparisons prove that the detection system is effective in distinguishing DoS attack network traffic from legitimate network traffic and outperforms two state-of-the-art systems. And also briefly recapped our proposed Euclidean based MCA technique andMCA based DoS attack detection system. A comprehensive evaluation of the proposed MCA based DoS attack detectionsystem was conducted on the KDD CUP 99 dataset. The results show that our detection system achieves encouragingperformances when cooperating with either non-normalized original data (99.96% detection rate and 2.08% false positive rate.) or normalized data (). It is illustrated that our detection system clearly outperforms the two state-of-the-artsystems in terms of detection rate and false positive rate. However, the false positive rate of our detection systemneeds to be further reduced in order to release network administrators from being disrupted by frequent shown falsealarms. Thus, we will employ more sophisticatedclassification techniques in our future work to alleviate the false positive rate. Furthermore, manifold will be consideredin the successive research to bring in more valuable information for attack detection.

## CONCLUSION

In this survey research article, we outline the authors' approach to dealing with DDoS attacks across numerous networks, including the internet, the Internet of Things, the cloud, etc. We need to develop a reliable technique to identify DDos attacks in networks, and while many researchers have come close, there is still a needfor a more potent approach. Some concerns merit more investigation. In the future, we hope to develop a sophisticated detection system and analyze network data more effectively by extracting additional factors.

## REFERENCES

1. Arun Raj Kumar, P. and S. Selvakumar, –Distributed Denial-of- Service (DDoS) Threat in Collaborative Environment— A Survey on DDoS Attack Tools and Traceback Mechanisms” , 2009 IEEE International Advance C‹›niputing Conference (I.ACC 2009)
2. Patial‹i, India, 6—7 Nl‹irch 2009
3. Akashdeep Bhardwaj Gvb Subrahmanyam Vinay Avasthi Hanumat Sastry Sam Goundar –DDoS Attacks, New DDoS Taxonomy and Mitigation Solutions – A Survey‖, International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016
4. Fei Wang, Xiaofeng Hu, Xiaofeng Wang, Jinshu Su, Xicheng Lu
5. ,–Unfair Rate Limiting On Traffic Aggregates For Ddos Attacks Mitigation‖
6. Anteneh Girma Moses Garuba Jiang Li Chunmei Liu, –Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment‖, 2015 12th International Conference on Information Technology-New Generations
7. Jiahui Jiao, Benjun Ye, Yue Zhao, Rebecca J. Stones, Gang Wang, Xiaoguang Liu, Shaoyan Wang, Guangjun Xie,–Detecting TCP-based DDoS Attacks in Baidu Cloud Computing Data Centers.‖, 2017 IEEE 36th Symposium on Reliable Distributed Systems
8. James Kay, Article in Network Security, june 2005.
9. Keunsoo Lee , Juhyun Kim, Ki Hoon Kwon, Younggoo Han, Sehun Kim ,–DDoS attack detection method using cluster analysis‖, Expert Systems with Applications 34 (2008) 1659–1665.
10. Miss Komal K. More, Prof. Pramod B. Gosavi –A Real Time System for Denial of service Attack Detection Based on Multivariate Correlation Analysis Approach‖, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016
11. Randy C. Paffenroth, Worcester Polytechnic Institute, Worcester, MA Chong Zhou, Worcester Polytechnic Institute, Worcester,

MA,–Modern Machine Learning for Cyber-defense and Distributed Denial of Service Attacks‖, : DOI 10.1109/EMR.2019.2950183, IEEE.

12. Zhiyuan Tan1, Aruna Jamdagni1, Xiangjian He1, Priyadarsi Nanda, and Ren Ping Liu,–Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis‖, Centre for Innovation in IT Services and Applications (iNEXT), University of Technology, Sydney, Australia CSIRO Marsfield, Australia.
13. Zhiyuan Tan1, Aruna Jamdagni, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu,–Evaluation on Multivariate Correlation Analysis Based Denial-of-Service Attack Detection System‖, Centre for Innovation in IT Services and Applications (iNEXT), University of Technology, Sydney, Australia CSIRO Marsfield, Australia.
14. Xiaoyu Liang, Taieb Znati,–An empirical study of intelligent approaches to DDoS detection in large scale networks‖, 2019 international conference on computing, networking and communication (ICNC): Network algorithms and performance Evaluation