AN ALGORITHM FOR MODERATING DOS ATTACK IN WEB BASED APPLICATION

D. Sophia Navis Mary , A.Thasleema Begum
thasleemafila@gmail.com
First Assistant Professor, MCA Department, Ethiraj College for Women, Chennai, Tamil Nadu
Second M.Phil Research Scholar, MCA Department, Ethiraj College for Women, Chennai, Tamil Nadu

Abstract- **The denial of service attack is the most powerful damaging attacks used by hackers to harm a business or organization. This attack is one of most dangerous cyber-attacks. It causes service outages and the loss of millions, depending on the time of attack. In past few years, the use of the attack has enlarged due to the accessibility of free tools. This tool can be blocked simply by having a good firewall, but an extensive and clever DoS attack can avoid most of the restrictions. A Denial of Service attacks against web sites occur when a hacker attempts to make the web server, or servers, unavailable for legitimate users and finally, to take the service slowing them down. This is attained by flooding the server's request queue with fake requests. After this, server will not be capable to handle the requests of genuine users. For some time, it was thought that these types of attacks were generally used against large companies, government sites, and activist sites as a form of protest to interrupt their web presence. In general, there are two forms of the DoS attack. The first form is on that can crash a server. The second form of DoS attack only floods a service. Online Vulnerability Scanner is a tool which is capable to detect DoS Attack in web application and compare its performance. We proposed an aegis algorithm which can be used to moderate DoS attack in web application Vulnerability.**

Index Terms- **Aegis Algorithm, DoS Attack, Hackers, Online Vulnerability Scanner, Web Application.**

I. INTRODUCTION

DoS are the acronym for Denial of Service. It is an attack that is intended at either cutting off network access to a resource such as a web site/app/service etc. or making it extremely slow. This type of attack is usually active by thrashing the target resource such as a web server with too many requests at the same time. This results in the server failing to respond to all the requests. The effect of this attack can either be crashing the servers or slowing them down. Denial of Service attacks is used to deny legitimate users access to a resource such as accessing a website. In this paper, we will introduce you to what denial of service attack is, how it is achieved and how you can defend against such attacks.

II. PROBLEM STATEMENT

Denial-of-service attacks are a real-and growing-threat to businesses worldwide. DoS attacks are weapons of mass disruption. Unlike access attacks that penetrate security perimeters to steal information, DoS attacks paralyze Internet systems by irresistible servers, network links, and network devices (routers, firewalls, etc.) with fake traffic. DoS is emerging as the weapon of choice for hackers and easily launched against limited defenses. DoS attacks not only target individual Websites or other servers at the edge of the network- they subdue the network itself. Attacks have initiated to explicitly intent the network infrastructure, such as aggregation or core routers and switches, or Domain Name System servers in a provider's network. The growing dependence on the Internet makes the impact of successful DoS attacks-financial and otherwise-progressively sore for service providers, enterprises, and government agencies. And newer, more powerful DoS tools promise to unleash even more destructive attacks in the months and years to come. Because DoS attacks are among the most difficult to defend against, responding to them appropriately and effectively poses a great challenge for all Internet-dependent organizations. Network devices and ancient perimeter security technologies such as firewalls and intrusion detection systems; although significant components of an overall security strategy do not by themselves provide complete DoS protection. Instead, defending against the current DoS attack threatening Internet availability needs a purpose-built architecture that includes the ability to exactly detect and defeat increasingly sophisticated, complex, and deceptive attacks. Taking on DoS attacks requires an our new approach in the Aegis algorithm that not only detects increasingly complex and deceptive attacks but also moderates the effects of the attack to safeguard business continuity and resource availability.

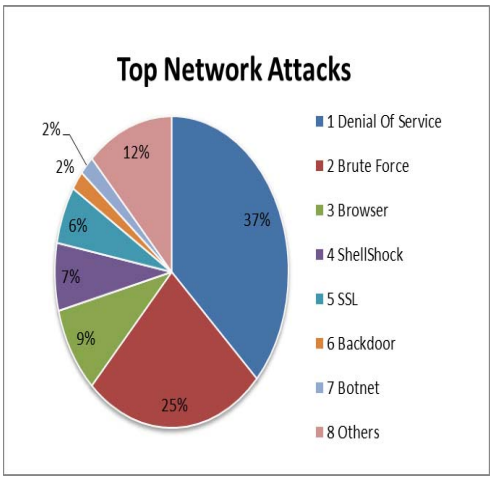


Fig 1. Top Network Attacks

978-1-5090-4797-0/17 $31.00 © 2017 IEEE
DOI 10.1109/ICTACC.2017.17

III. LITERATURE REVIEW

S.NO.	TITLE OF THE PAPER	TECHNIQUE NAME	MECHANISM
1	Flood Guard: A DoS Attack Prevention Extension in Software-Defined Networks [1].	Flood Guard	This paper reports one severe SDN-specific attack, i.e., data-to-control plane saturation attack, which excesses the infrastructure of SDN networks. In this attack, an attacker can make a large amount of table-miss packet in messages to devour resources in both control plane and data plane. To moderate this security threat, we introduce an effective, lightweight and protocol-independent defense framework for SDN networks.
2	Prevention of DDOS Attacks using New Cracking Algorithm [2].	New Cracking Algorithm	DDOS defense system that can protect the accessibility of web services during severe DDOS attacks. The proposed system identifies whether the number of accesses of client exceeds more than five times to the same sever, then the client will be kept as an attacker in blocked list and the facility could not be provided. So our algorithm defends legitimate traffic from a huge volume of DDOS traffic when an attack occurs.
3	Detection and Mitigation of Denial of Service Attacks Using Stratified Architecture [3].	Puzzle, Mac Filtration and Cryptography Based Authentication	To prevent or protect a machine from being affected from these attacks. This article contains sequences of Denial of Service attacks on a target machine and proposed an algorithm which prevents DoS attacks. This algorithm has three layers through which the requesting client goes through for efficient authentication.
4	Simulation of DDoS Attack & Real Time Prevention Algorithm [4].	Limiting number of Users and Packet size	DoS attacks are implemented by either forcing the targeted computer to reset, or consuming its resources so that it can no longer provide its intended service or blocking the communication media among the envisioned users and the victim so that they can no prolonged communicate adequately.
5	DDoS Attacks Detection of Application Layer for Web Services using Information based Metrics [5].	FAÇADE layer	Based on first phase, in detection phase, variation in entropy will be perceived and malicious users will be detected. Rate limiter is also introduced to stop or reduce serving the malicious users. This paper aids the FAÇADE layer for detection and blocking the illegal user from attacking the system.
6	Comparative Study Of Preventive Algorithms Of DDoS Attack [6].	Modified cracking algorithm and Hop count filtration	This paper presents a complete overview of DDoS attacks, types of DDoS attacks, attacks on various OSI levels. Moreover the algorithms for DDoS prevention is similar to cracking algorithm and hop count filtration are defined and their comparative analysis is made.
7	Mitigating Distributed Denial of Service Attack in Cloud Computing Environment using Threshold based Technique [7].	Artificial Immune System(AIS) algorithm	The proposed work can be implemented in any cloud network to save it from killing the resources for malicious requests. For more enhancement client based protection can also be implemented such that the attacker will not be able to form its crowd for the purpose of DDoS attack.
8	A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks[8].	Intrusion detection systems, intrusion prevention systems, distributed DDoS defense, collaborative DDoS defense.	In this paper, we explore the scope of the DDoS flooding attack problem and attempts to battle it. We categorize the DDoS flooding attacks and categorize current countermeasures built on where and when they prevent, detect, and respond to the DDoS flooding attacks.

IV. Types of DDoS Attack

There are two types of Dos attacks namely,

1) *DoS*– this type of attack is executed by a single host.
2) *Distributed DoS*– this type of attack is executed by a number of cooperated machines that all target the same victim. It floods the network with data packets.

DoS attacks can be generated in two different ways: direct attack and reflector attack.

A. Direct attack

In a direct attack, a huge number of attack packets are directed to the victim machine directly. In this attack, the attacker takeoffs the source IP address so that the response is misdirected and goes away.

B. Reflector attack

In case of a reflector attack, many innocent intermediate nodes known as reflectors (Botnets or Zombies) are used to generate an attack. An attacker sends packets that essential response to the reflectors with the packets' emblazoned source address usual to the victim's address. The attack packets can be constructed using TCP, UDP, ICMP or IGMP protocols.

V. How DoS Attack Works

Two Ways of launching Denial of Service attacks against web applications are:

1) Attempts to "flood" web applications, thereby preventing legitimate user traffic.
2) Attempts to disturb service to a specific system or person, e.g., blocking user access by repeated invalid login attempts resulting in the account's suspension.

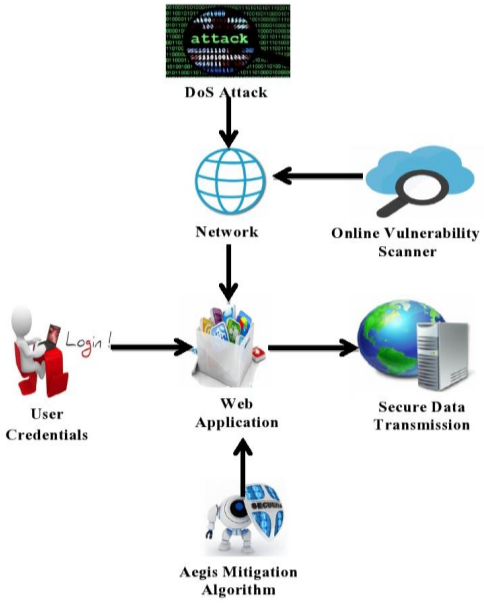


Fig 2. DoS Attack System Architecture

VI. DoS Attack on Network and Transport Layer

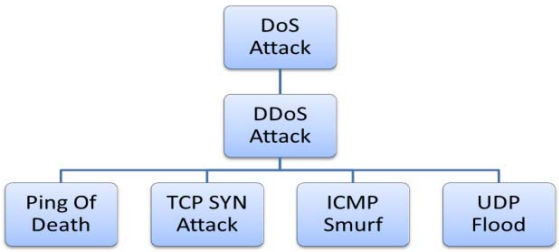
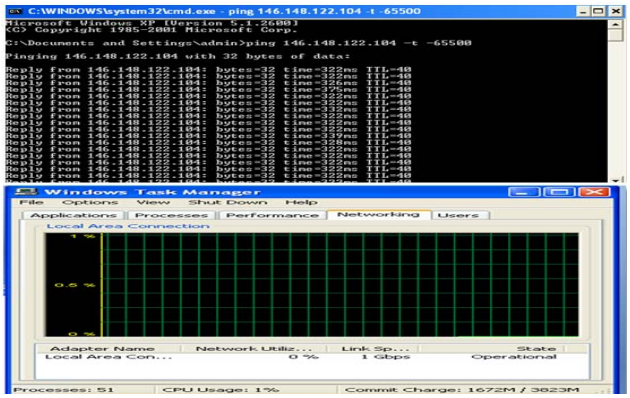


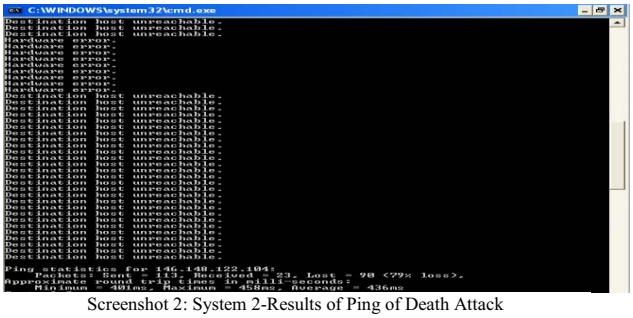
Fig 3. DoS Attack on Network and Transport Layer

A. Ping of Death

The ping command is usually used to check the availability of a network resource. It works by transfer small data packets to the network resource. The ping of death proceeds advantage of this and sends data packets beyond the maximum limit (65,536 bytes) that TCP/IP allows. TCP/IP fragmentation halts the packets into small hunks that are sent to the server. Since the sent data packages are larger than what the server can handle, the server can halt, reboot, or crash. Flooding the target computer with data packets doesn't have much effect on the victim. In order for the attack to be more effective, you should attack the target system with pings from more than one system.



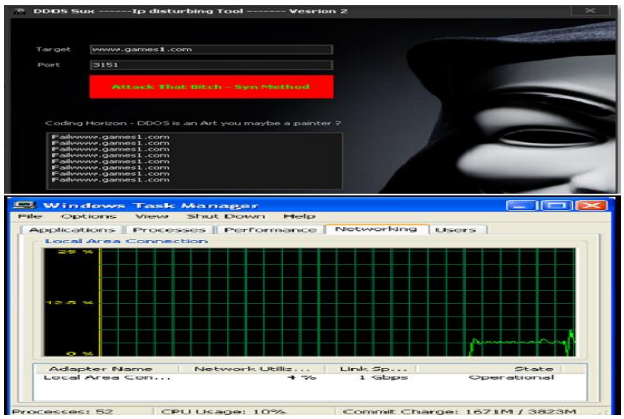
Screenshot 1 : System 1- Results of Ping of Death Attack



Screenshot 2: System 2-Results of Ping of Death Attack

B. TCP SYN Attack

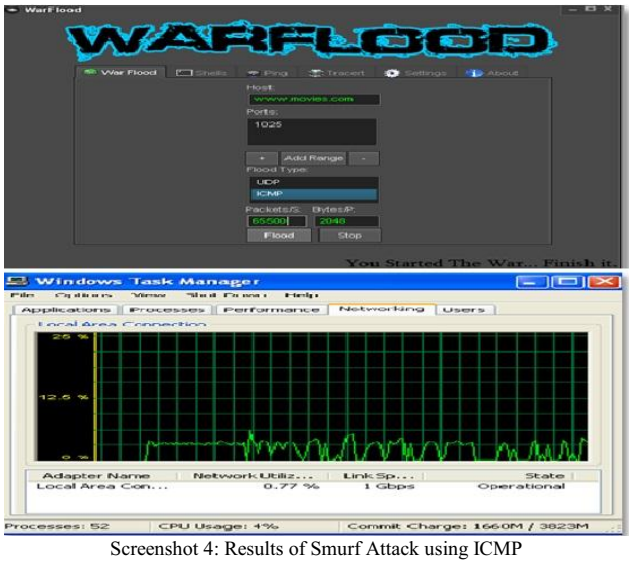
SYN is an acronym for Synchronize. This kind of attack takes advantage of the three-way handshake to establish communication using TCP. SYN attack works by flooding the victim with faulty SYN messages. This reasons the victim machine to allocate memory resources that are never used and deny access to genuine users.



Screenshot 3: Results of TCP SYN Attack

C. Smurf Attack

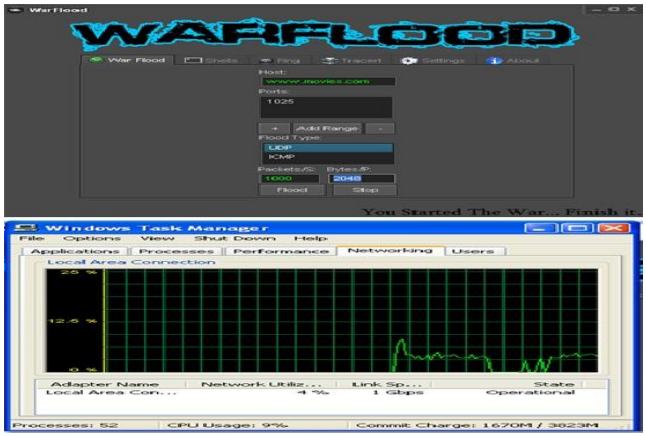
This type of attack uses huge amounts of Internet Control Message Protocol (ICMP) ping traffic aim at an Internet Broadcast Address. The reply IP address is spoofed to that of the planned victim. All the replies are sent to the victim in its place of the IP used for the pings. Since a single Internet Broadcast Address can support a maximum of 255 hosts, a smurf attack intensifies a single ping 255 times. The effect of this is reducing down the network to a point where it is impossible to use it.



Screenshot 4: Results of Smurf Attack using ICMP

D. UDP Flood Attack

UDP flooding is like to ping flood. Here instead of ping packets, UDP packets are blasted against the server. UDP could be a lot more effective than ICMP in smaller networks as the size of the UDP packets are vast. The packet size could be fixed up to 65000 bytes which could easily flood an assumed Ethernet network when multiple zombies are set up.



Screenshot 5: Results of UDP Flood Attack

VII. Proposed Aegis Algorithm

There are basically three basic steps in the algorithm. It comprises of monitoring, detection and mitigation. In the proposed solution a list of faulty IP addresses has been identified based on their performance and named as the block list. So if the request with IP address made by the sender in the block list, the system will not allow access the resources and drop its request. If the request will be passed through the first stage then at second stage it is checked whether the number of requests are less than the threshold or not.

At the third stage requesting an amount of resources are compared with a threshold value “Th”. “Th” is the threshold value of the request that can be done maximum at time T. “Th” can be calculated by watching the behavior of a maximum number of requests made when there is no attack. If the request for the web application is less than “Th” then the web application will be allocated to the request otherwise this request will be dropped and suspected as the malicious request. Fig.4 shows the flow chart for the proposed Aegis algorithm.

A. Behavior pattern Recognition

It is effectively protects against malicious behavior such as Denial of Service. Use an Effective tool to identify a wide array of application-level attacks.

B. Traffic flow Table

It offers comprehensive information about traffic accounting, bandwidth monitoring used to identify the traffic anomaly.

C. Signature Knowledgebase

It maintains a signature profile of an attack. Detection of specific attacks is possible through signatures.

1) Flow Chart

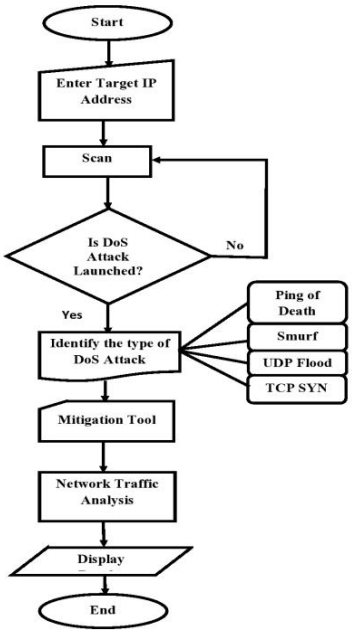


Fig 4. Simulation Design

2) Aegis Algorithm

The following sequence of steps gives the detailed description of the proposed algorithm

Step I: Start and Enter the Target IP Address of the web Application/Website.

Step II: Scan and maintain the history of the IP Address.

Step III: Store the Network traffic of the targeted victim and detect a DoS Attack has launched.

Step IV: If DoS Attack has launched then go to mitigation component

Step V: else verify the legitimate request by verify the IP address. Whenever the number of requests arrives at time 'T', the IP address of this request falls into the block list or not. IF the request from a particular IP address falls into the block list it will be suspected as malicious request and dropped.

Step VI: Use the mitigation tool of DoS attack and display the results.

VIII. .How To Avoid Dos Attack

An organization can adopt the following policies to protect itself against Denial of Service attacks.

1) Attacks such as SYN flooding take advantage of bugs in the operating system. Installing security patches can help to moderate the chances of such attacks.
2) Intrusion detection systems can also be used to identify and even stop illegal activities.
3) Firewalls can be used to stop modest DoS attacks by authorize/blocking all traffic coming from an attacker by identifying IP.
4) Routers can be configured via the Access Control List to limit access to the network and drop suspected illegal traffic.

IX. Conclusion

This paper presents the concept of DoS attack and tests it in a simulated environment and the results are studying during the early phase of the research. We plan to refine an algorithm based on the investigation and able to identify the various types of DoS attack pattern. Time taken to detect the attack is another area that needs more investigation. We studied the DoS attack on network and transport layer at the first simulation phase. We expect these results to remain consistent and likely to improve as we progress the development of the system.

Acknowledgment

The authors are thankful to the anonymous referees for their careful reading and valuable comments that have improved the quality of the paper.

REFERENCES

[1] H. Wang, L. Xu and G. Gu, "FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks," *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, Rio de Janeiro, 2015, pp. 239-250. doi: 10.1109/DSN.2015.27

[2] V.Priyadharshini , Dr.K.Kuppusamy, "Prevention of DDOS Attacks using New Cracking Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2263-2267.

[3] A.Prakasha, M.Satisha,T.Sri Sai Bhargava, Dr. N. Bhalajia, "Detection and Mitigation of Denial of Service Attacks Using Stratified Architecture" 4th International Conference on Recent Trends in Computer Science & Engineering (ICRTCSE) 2016.

[4] Silica Kole, Deepak Kumar Gupta, Pulkit Goel, "Simulation of DDoS Attack & Real Time Prevention Algorithm", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013 1536 ISSN 2229-5518.

[5] Nilesh A. Suryawanshi, S.R.Todmal, “DDoS Attacks Detection of Application Layer for Web Services using Information based Metrics, “International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 9, May 2015.

[6] Divyashree Chavan, Colleen Francis, Elbin Mary Thomas, Prathama Moraye, “Comparative Study Of Preventive Algorithms Of Ddos Attack “International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February-2016 ISSN 2229-5518.

[7] Nitesh Bharot, Priyanka Verma , Veenadhari Suraparaju and Sanjeev GuptaC. ,” Mitigating Distributed Denial of Service Attack in Cloud Computing Environment using Threshold based Technique” , Indian Journal of Science and Technology, Vol 9(38), October 2016.

[8] Saman Taghavi Zargar, James Joshi and David Tipper,“A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks” in *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046-2069, Fourth Quarter 2013.

[9] L. Dridi and M. F. Zhani, "SDN-Guard: DoS Attacks Mitigation in SDN Networks," *2016 5th IEEE International Conference on Cloud Networking (Cloudnet)*, Pisa, 2016, pp. 212-217. doi: 10.1109/CloudNet.2016.9

[10] SANS Institute. Subramani rao Sridhar rao ,“Denial of Service attacks and mitigation techniques: Real time implementation with detailed analyis” The SANS Institute,2011.

[11] Barna, M. Shtern, M. Smit, V. Tzerpos and M. Litoiu, "Model-based adaptive DoS attack mitigation," *2012 7th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)*, Zurich, 2012.

[12] M. Zolotukhin, T. Hämäläinen, T. Kokkonen and J. Siltanen, "Increasing web service availability by detecting application-layer DDoS attacks in encrypted traffic," *2016 23rd International Conference on Telecommunications (ICT)*, Thessaloniki, 2016.

[13] M. Kuerban, Y. Tian, Q. Yang, Y. Jia, B. Huebert and D. Poss, "FlowSec: DOS Attack Mitigation Strategy on SDN Controller," *2016 IEEE International Conference on Networking, Architecture and Storage (NAS)*, Long Beach, CA, 2016, pp. 1-2. doi: 10.1109/NAS.2016.7549402

[14] www.CheckPoint -2016 Security Report.com

[15] Sonia Laskara , Dhirendra Mishrab, “Qualified Vector Match and Merge Algorithm (QVMMA) for DDoS Prevention and Mitigation” 7th International Conference on Communication, Computing and Virtualization 2016.

[16] Dong Lin, University of Pennsylvania Department of Computer and Information Science Technical Report "Network Intrusion Detection and Mitigation Against Denial of Service Attack", . January 2013.

[17] B.S. Kiruthika Devi, G. Preetha, S. Mercy Shalinie,“DDoS detection using host-network based metrics and mitigation in experimental testbed”, IEEE, 2012.

[18] Cornel Barna, Mark Shtern, Michael Smit, Vassilios Tzerpos, Marin Litoiu York University,“Model-based adaptive DoS attack mitigation”, ACM, 2012.

[19] Shishira S R, Vasudeva Pai and Manamohan K, “Current Trends in Detection and Mitigation of Denial of Service Attacks-A Survey” International Journal of Computer Applications (0975 – 8887) International Conference on Information and Communication Technologies (ICICT-2014).

[20] S. Chithra, Dr. E. George Dharma Prakash Raj, “OVERVIEW OF DDOS ALGORITHMS: A SURVEY” , International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 2, Issue. 7, July 2013, pg.207 – 213

[21] Deepika Mahajan Monika Sachdeva, “DDoS Attack Prevention and Mitigation Techniques - A Review”, International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.

[22] K.R.W.V.Bandara, T.S.Abeysinghe, A.J.M.Hijaz, D.G.T.Darshana, H.Aneez, S.J.Kaluarachchi,K.V.D.L.Sulochana and Mr.DhishanDhammearatchi , “Preventing DDoS attack using Data Mining Algorithms”, International Journal of Scientific and Research Publications, Volume 6, Issue 10, October 2016 392 ISSN 2250-3153.

• D. Sophia Navis Mary is currently working as an Assistant professor and a Research guide at Ethiraj College for women, Chennai. Her research interest includes; Information security, network security and cryptography. E-mail : sophianavis@gmail.com

• A.Thasleema Begum is currently pursuing the Masters of Philosophy in Computer Science and specializing in the field of cryptography and network security at Ethiraj College for Women, Chennai in the year of 2016-17.Ph.: +918508431211, E-mail : thasleemafila@gmail.com