International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 07, July-2015

Analysis of Denial of Services(DOS) Attacks and Prevention Techniques

Kutub Thakur
Department of Computer Science
Seidenberg School of CSIS, Pace University
New York, USA

***Abstract* - In the globalized world, Internet has out grown rapidly as a universal communication network tool, which not only allows sharing information but the entire tasks cooperatively through computing resources. However, over last few decades an illegal acts has numerously increased in the networks and moreover the devious and malicious has increased in their content and among them, especially denial of service (DoS) attacks is identified to be difficult. Thus the present paper aims to explore the DoS flooding attack problem and attempts to combat it with the classifiable countermeasures that prevent, detect, and respond to the DoS flooding attacks. The study adopted the secondary data collection method and data was collected various online and offline sources. The study proposed a cyber-security TCP-SYN is identified to be the effect method to mitigate and block the DDoS attacks and the implementation of these particular cost-effective defense mechanisms against these kinds of attack supports the business continuity to enhance their performance thoroughly.**

Keywords: Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attack, TCP-SYN Flood Attack, TCP-SYN Proxy Protection, Firewall Security

I. INTRODUCTION

In the globalized world, Internet has out grown rapidly as a universal communication network tool. This Internet infrastructure tools not only allows sharing their information but the entire tasks cooperatively through computing resources contributing [1]. However, over last few decades an illegal acts has numerously increased in the networks and moreover the devious and malicious has increased in their content and among them, especially Denial of Service (DoS) attacks is identified to be difficult. Moreover, and end host can easily join the network and communicate with any other host by exchanging packets. These are encouraging features of the Internet, openness and scalability. However, attackers can also take these advantages to prevent legitimate users of a service from using that service by flooding messages to the corresponding server, which forms a Denial of Service (DoS) attack. A Denial-of-Service (DoS) attack is considered an active attack, which attempts to make a computer or network resource unavailable to its intended users [2]. DoS attacks exhaust the computing or communication resources of the victim's computer or server.

Thus the present paper aims to explore the DoS flooding attack problem and attempts to combat it. Moreover, the study also classifies existing countermeasures based on where and when they prevent, detect, and respond to the DoS flooding attacks by adopting a review based approach. Finally, the study proposes a stimulative model creative, effective, efficient, and comprehensive prevention, detection, and response mechanisms that address the DDoS flooding problem before, during and after an actual attack.

This paper is organized as follows: Section 2 gives some background about the TCP-SYN floodingand the types of attacks are illustrated in the same section. That was used in. Section 3 provides the information about our experimental setup and the experiments presented in this paper and results and discussions. Section 4 presents the conclusion.

II. BACKGROUND OF THE STUDY

Over the years the DoS attacks have become the most insidious threats on networked computer systems. This crippling attack is found to exploit the software protocols vulnerabilities and supports in achieving phenomenal results of no resource investment. However, instead of these attacker, the internet is subjected to flooding DoS attacks, in which the attacker invest a moderate amount, and this investment is identified to create vastly superior consumption of resources on the targeted system. Protecting against flooding DoS attacks can be particularly difficult and frustrating. At the heart of this difficulty is the presence of a constant compromise or trade-offbetween providing services to legitimate users of network services, while keeping malicious users at bay.

Fig. 1. Generic Dos model

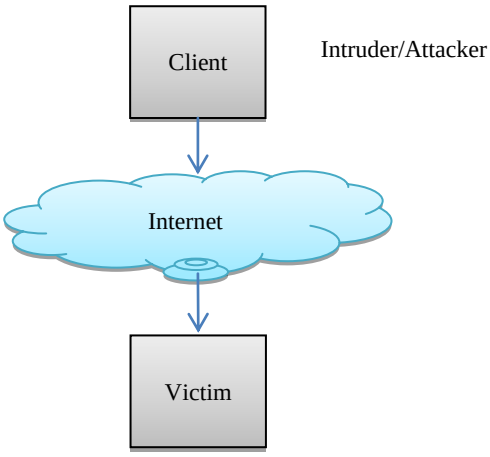
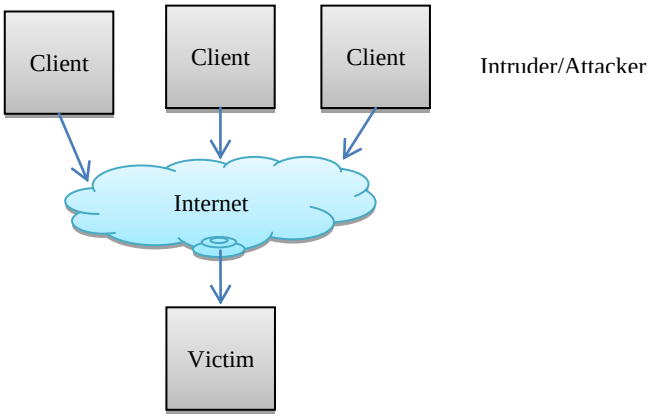


Fig. 2. Generic DDoS Model



In order to have deep understanding over the concept of DoS it is essential to know the definition and types of DoS. The below section will detail about the concept and types of DoS.

In general the term DoS is identified as an attack attempt made by the adversary who intrudes the legitimate user's service from server, butspeaking, about the attacks or threats which exhaust or saturatethe system resources, or which allows to crashes during the operation, etc are found to as a DoS attack [3]Moreover, if the hacker or attacker attacks multiple machines simultaneously then it is found to be Distributed Denial of-Service (DDoS) attack [4]. During 2000 to 2004 a high frequency of DDoS attacks faced by every orgnsiation [5].

For instance, the recent attack on 4th April 2013 at Mt. Gox an Tokyo based firm was identified as largest DDoS attack on coin exchange were the price of virtual currency was manipulated and caused an fluctuation with an unstable price. Moreover, the adversaries displayed the error pages to the traders [6]–[8].Moreover, another attack on Spamhaus caused another big chaos in the UK and Switzerland-based nonprofit organization. This is noted as the biggest DDoS cyber-attack in which 300 Gigabits per second of data was subjected to threat [9] Likewise there are several attacks such as the attacks on Webster Bank and Zions Bancorp experienced a loss of $20 billion, were as the Zions bank in Utah, had a loss of$53 billion bank [10] on 8th November 2012.Later on 14th of December 2012joined the list, which taught lesson to those who faced the threat [11]. Threat of DoS attacks has become even more severe with DDoS (Distributed Denial-of-Service) attack. These are various types of DOS and DDOS, which includes the UDP Flood Attack, were the adversary sends large number of UDP packets to a client system, and causes large network saturation. This result in available bandwidth depletion for legitimate service requests to the clients system [12].The other DoS id the Internet Control Message Protocol(ICMP) Floodthat qualifies the client or the victim to send an echo packet to a remote host in order to check the connectivity [13]. The source IP is spoofed throughoutthe ICMP flood attack the source. In addition, if a half open connections is found then the SYN Flood Attack is being flooded [11], [14].

Another commonly ICMP flooding attack is the Smurf Attack. In the "smurf" attack, attackers are using ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks. When the attackers create these packets, they do not use the IP address of their own machine as the source address. Instead, they create forged packets that contain the spoofed source address of the attacker's intended victim. The result is that when all the machines at the intermediary's site respond to the ICMP echo requests, they send replies to the victim's machine. The victim is subjected to network congestion that could potentially make the network unusable.

The Teardrop Attack is another DoS, exploits the way that the Internet Protocol (IP) requires a packet that is too large for the next router to handle be divided into fragments. The fragment packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system. In the teardrop attack, the attacker's IP puts a confusing offset value in the second or later fragment. If the receiving operating system does not have a plan for this situation, it can cause the system to crash [15]. There various other attacks like Land Attack, Mail bomb, Ping of Death, Process Table, SSH Process Table, Syslogd, etc. On the other hand, various defensive mechanisms against the attackers were developed, which is represented in the following table 1

TABLE I. VARIOUS DEFENSIVE MECHANISMS AGAINST THE ATTACKERS

Prevention Techniques	Description
Filtering routers	The packets in the network which enter and leave are filtered, through ingress and egress packet filter[16].
Disabling unused services:	The tampering and attacks are minimized through the UDP echo or through other unused services [17].
Applying security patches:	To avoid the DoS all the servers are reorganized with security techniques and patches.
IP hopping	The IP address of clients are allowed to be pre-specified with set of IPs to prevent from DDoS attacks [17].
Disabling IP broadcast:	The malicious part of this attack is that the attacker can use a low-bandwidth connection to destroy high-bandwidth connections. The amount of packets that are sent by the attacker is multiplied by a factor equal to the number of hosts behind the router that reply to the ICMP echo packets.

The prevention tools alone are not reliable, as preventing cannot eliminate IP spoofing , thus there is a need to detect for any spoofed attacks [17], [18]. Moreover, various authors [19]–[22] identified various distinct DDoS detection mechanism are available, which includes theDetection Timing, Detection activity, Signature based Anomaly based, Hybrid attack detection, Third party detection etc. These detection techniques allowed for the formulation of DDoS Attack Tolerance and Mitigation Technique, which is illustrated in the below table 3.

TABLE II. FORMULATION OF DDOS ATTACK TOLERANCE AND MITIGATION TECHNIQUE

DDoS Attack Tolerance and MitigationTechniques	Description
IntServ	It provides service classes. which closely match the different application types described earlier and their requirements
DiffServ	Scalability and flexibility is much better then IntScrv.
ClassBased Qucuing(CHOI)	Avoid bandwidth starvation problem
Proactive Scrvcr Roaming	Provide good response time in cast of attack
Resource Accounting	Each flow gets a fair amount of resources
Resource Pricing	By employing different price and purchase function. architecture can achieve QoS
Pushback Approach	Upstream routers arc not needed. Incremental deployment approach
Throttling	Helps to define an accurate and efficient packet filter
Router's Traffic Scheduling	Reduces the congestion or attack impact and manages the flow of traffic along with it but they are too expensive in terms of delays and state monitoring [23]–[25].
Target Roaming	Active servers change their location within distributed homogeneous servers proactively to eliminate or chop DDoS attacks impact [26].

There are many network-based solutions against DDoS attacks. These solutions usually use routers or overlay networks to filter malicious traffic. Thus the below section illustrates evidence based results on DDoS Attack Tolerance and Mitigation Techniques, i.e. the below section explore various DDoS mitigation techniques with previous studies.

III LITERATURE REVIEW

This section discusses the previous studies on DoS and DDoS attacks and mitigation techniques which would result in secured networkwith improved secure communication, enhancedcustomer satisfaction all industry especially service industry that increased productivity

Initially, the study Peng et al. [27]focused on application related moderation and the study by Badishi et al. [15] suggested an ack-based port-hopping protocol concentrating on the traffic between two sources, defined as sender and receiver. The receiver replies back an acceptance note for each message received from the sender, and the sender utilizes this acceptance note as signals to alter target port numbers for its messages. As the protocol is ack-based, time synchronization is not required. But consider that the acceptance message could be missed in the network, and this might make the two persons employing same port for an extended time. If any attacker can trace the port number during real time communication, then he can direct an attack at which the communication will be lost.

Abuhaiba [28] study the vulnerabilities of sensor networks, design, and implement new approaches for routing attack. As one of the cornerstones of network infrastructure, routing systems are facing more threats than ever; they are vulnerable by nature and challenging to protect. The study also examined the parameter space of many possible denial of service attacks scenarios and make excessive simulations to identify what combination of parameter settings which leads to the more damaging and thus ultimate scenarios for our attack process. The significant factor here is the swarm capacity in terms of number of injected interests into the network. These results strengthen our attack in a way that it could be done efficiently by single powerful well positioned attacker. The results indicate that increasing number of attackers has slight effect on the success of the attack.

Kumar and Gade [29] evaluated the effectiveness of a Netscreen 5GT (or NS-5GT) security device from Juniper Networks under Layer-4 flood attacks at different attack loads. The study conducted real experiments to measure the performance of this security device NS-5GT under the TCP SYN and UDP flood attacks and test the performance of these protection features. The study found that the Juniper's NS-5GT mitigated the effect of DDoS traffic to some extent especially when the attack of lower intensity. However, the device was unable to provide any protection against Layer4 flood attacks when the load exceeded 40Mbps. In order to guarantee a measured level of security, it is important for the network managers to measure the actual capabilities of a security device, using real attack traffic, before they are deployed to protect a critical information infrastructure.

Hari and Dohi [30] have presented a report on the significance of these protocol attacks. To confront with that, Badishi et al. [15] suggested a proposal that restarts the protocol. By periodical restarting, the sender and receiver can utilize new seed of pseudorandom functionality that generates various port number arrangements, in order to change the communication port number orders. Hence even if the attacker can initiate the directed attack as an event of missed acknowledgement packs, the sender and receiver can still communicate just by restarting the protocol. This restart is due to the assumption that the variation in clock times of two communicating parties assigned to determine sender and receiver to restart at the same time. In this context the variation in clock timings can be inconsistent, but the clock rate for each communicating party is stable.

Badishi et al. [15] has presented a precise model and a study about the issues of DoS to applications (ports) by an attacker who can listen in. This study apart from port-hopping protocols suggested, also consist of studying the impact of adversary's different approaches to launch blind attacks. The aim of the attacker is to reduce the feasibility that client information is obtained by the server called the delivery probability as much as possible. The researchers presented a lower bound that the attacker would not be able to reduce the delivery probability beyond that. The lower bound is based on the capability of a port for receiving messages and also attacker capacity to flood messages.The results contain important information of settings and processes as mentioned in this paper in spite of application's defense mechanism.

Lee and Thing [31]suggest another port-hopping system for the client server model. In this method, time factor is divided into distinct time slots. In this the client and server use a pseudorandom functionality to determine which port needs to be used in a specific time slot.The researcher estimates that the time offset along with delay in message is composed by the contact value of I, hence there is need for a time synchronization mechanism. Rather, the correct open time for the communication port for the time slot is delayed forward and backward by 1/2l. This mechanism shows the base idea of time-based port hopping, but yet it calculated on synchronized clock values.

Same as port-hopping, Srivatsa et al. [32]suggested client-transparent approach. This method uses JavaScript to include authentication code into the TCP/IP layer of the networking protocol stack; hence messages with unauthorized authentication code will be limited by the server's firewall. For the purpose of preventing DoS attacks, the authentication code gets altered regularly. A challenge server is enabled whose task is to produce keys that control the number of clients linked to the server and integrating the clients with the server. As this process is depending on the challenge server, security of the challenge server is quite significant. The paper denotes that a cryptographic-type of mechanism can be utilized to secure the challenge server, though this has not been discussed briefly.

Fu et al. [33] enhanced port-hopping to assist various applications, by suggesting the BIGWHEEL algorithm, in a typical application server to interact with various clients in a port-hopping system eliminating the requirement of group synchronization. Further, researchers have suggested an adaptive algorithm, HOPERAA, toenable hopping accompanied by bounded asynchrony, while commuting parties contain clock drifts. The explanations are straight forward, based on the fact that each party communicating with server is independent of other client, without any acknowledgement or time server in place. Also they do not depend on the application to have a fixed port kept open at the beginning nor do they need the clients to obtain a "first-contact" port from a third party. The analytical aspects of the algorithms have been displayed and an experimental study of their success rates, confirming the connection with the analytical values is performed. Another compelling issue to study further is to check out thevariable hopping frequencies and variable clock drifts. For instance, if the author has used TCP, then predicted RTT for TCP can be directly utilized to set the value of μ.

Tripathi et al. [34] suggested that a DDoS attack effectively by using Map Reduce programming structure. The objective was to propose a model that used SAMR Counter related algorithm that enhances the process as it inputs the information history that has been stored on each node and update the details after each execution.This way, it produces more precise Progress score and determines which process needs to be backed up. . This process has three input parameters: time interval, unbalance ratio and threshold , that are stored in HDFS using packet loader. The packet collector obtains IP packets from trace files from the disk, and writes them on HDFS. IP packets are saved in the binary format of libpcap. The unbalanced ratios and threshold for server are sent as parameters along with the timestamp. The process (Job) starts at the client end and Job Tracker running SAMR scheduler divides the job into map and limitstasks anddesignate them to a collection of nodes and at the same time it obtains the historical information which has been saved on every node and is updated after each execution. This appropriate model replaced the default scheduling through fair scheduler which uses Hadoop algorithm to determine DDoS attack. The author has compared the efficiency of two well-known operating systems, namely the Apple's Lion and Microsoft's Windows 7, in context of the DDoS attacks. The author has compared the computing performance of

both the operating systems with two ICMP based DDoS attacks. As the aspect of OS is to regulate the server or computer resources effectively as much as possible, the author has evaluated the efficiency of OS in managing computer assets. This study has evaluated by comparing the in built security of both operating systems in an iMac computer that can run both Windows 7 and Lion.Land Attack and ICMP Ping are the simulated DDoS attacks. The exhaustion of the pro-cessors, Echo Reply messages and the number of Echo Request are measured by generating under varied attack loads in both Ping and Land Attack. The results of the experiments indicate that both the operating systems could handle the attacks though they have acted differently during the attack. The Lion Operating System handled bothLand and Ping attack in the exactly the same way, but in the case ofWindows 7 the two attacks were handled differently, that result in varied processor usage by two different operating systems

Vellalacheruvu and Kumar[35] has stated that CP SYN flood is a common DDoS attack, and current operating systems shows a protection mode against this attach that can potentially reduce the web application performance and user connectivity. In this study the performance of TCP-SYN attack protectionthat comes along with Microsoft's windows server 2003 is evaluated. It is has been detected that theSYN attack protection offered by the server is only effective topreventattacks at low loads of SYN attack traffic only, and is not adequate to protect higher magnitude ofSYN attack traffic. The units of results presented in the study can assist network operators to estimate the rotection method present in millions of Windows server 2003 in protecting the most popular DDoS attacks, called the TCP SYN attack, eventually upgrade their network security by other means.

Obimbo and Ferriman[36] conducted a study on the utilization of LDAP used in the user authentication by execution of a DoS attack destroying the TCP three-way handshake requirement while initializing a connectivity to an LDAP server. The study has shown that the use of LDAP is not good enough for authentication process. In the Section 3 the suggested attack has gone through by refusal of service because of SYN floodingresulting in disruption ofLDAP service. In Section 3.2 the study argues that the authentication is an important process an eminent DoS attack has been successful. Section 4.1 has indicated two basic errors of LDAP which are securing LDAP servers from DoS attacks and securing user passwords from being traced in a network. Finally section 4.2 indicated that the use of Kerberos is a substitute to theauthentication process ofLDAP.

Zargaret al. [37] scope of the DDoS flooding attack problem and attempts to combat it. We categorize the DDoS flooding attacks and classify existing countermeasures based on where and when they prevent, detect, and respond to the DDoS flooding attacks. Moreover, we highlight the need for a comprehensive distributed and collaborative defense approach. Our primary intention for this work is to stimulate the research community into developing creative, effective, efficient, and comprehensive prevention, detection, and response mechanisms that address the DDoS flooding problem before, during and after an actual attack.

Holl [4] explored the DDoS Defense Mechanisms and identified the frequently attacked layer. In the present study various defensive mechanisms' efficiency was measured, which includes the Proactive defense mechanisms, Reactive defense mechanisms, Post attack analysis. Moreover, the study adopted the entropy comparison of consecutive packet method to achieve the Zero-Day DDoS attacks. The study results identifiedvarious challenges, which includes Size of the Botnet, Abnormal traffic detection, Long-term attacks and Large-scale testing. The study concluded that DDoS attacks are global threats, which is mitigated through selective black holing technique. However, the study stated based on the scenario the framework might vary.

Thus the research gap was identified there is no standard structure that would address and mitigate the DoS and DDos flooding attacts. In addition, various studies [29]used the SYN-TCP method but failed to provide protection against Layer4 (i.e. Transport Layer). Moreover, none of the study proved the effectiveness of SYN-TCP attempts to combat the DoS flooding attack problem.

IV CONCLUSION

Thus the study concluded that in the complexly increasing DDoS attacks, various defense mechanisms were structured, but in the modern world all the defense systems are built with various several detection techniques and mitigation algorithms. Even though the DoS attacks are handled in various structures, not all the defense mechanisms suits best for all kinds of DDoS attacks. In these cases, the TCP-SYNis identified to be the effect method to mitigate and block the DDoS attacks. However, the present study is identified to be limited to development and application, thus the future study by applies this method in real time to know the holistic approach.

REFERENCES

[1] J. H. Fowler, M. T. Heaney, D. W. Nickerson, J. Padgett, and B. Sinclair, "Causality in political networks.," *Am. Polit. Res.*, vol. 39, pp. 437–480, 2011.
[2] R. B. Junior and S. Kumar, "Apple's Lion vs Microsoft's Windows 7: Comparing Built-In Protection against ICMP Flood Attacks," *J. Inf. Secur.*, vol. 5, no. 3, pp. 123–135, 2014.
[3] P. Kulkarni, "Responsive System for DDoS Attack against Apache Web Server," National Institute Of Technology Karnadaka, 2010.
[4] P. Holl, "Exploring DDoS Defense Mechanisms," in *Network Architectures and Services*, 2015.
[5] Z. FU, "Multifaceted Defense Against Distributed Denial of Service Attacks: Prevention, Detection, Mitigation," CHALMERS UNIVERSITY OF TECHNOLOGYomputer Science and Engineering, 2012.
[6] "DDoS-for-Hire Service Is Legal and Even Lets FBI Peek in, Says a Guy with an Attorney," 2012. .
[7] "Internet Creaks Following Cyber Attack on Spamhaus," 2013. [Online]. Available: http://www.cbronline.com/news/security/internet-slows-d. [Accessed: 08-Jun-2015].
[8] T. Kitten, "2 More Banks Are DDoS Victims," 2012. [Online]. Available: http://www.bankinfosecurity.com/2-more-banks-are-ddos. [Accessed: 08-Jun-2015].

[9] "Mstream Distributed Denial of Service Tool (Zombie Detected) (DdosMstreamZombie)," 2013. [Online]. Available: http://www.iss.net/security_center/reference/vuln/ddos-m. [Accessed: 08-Jun-2015].
[10] N. McAllister, "GoDaddy Stopped by Massive DDoS Attack," 2012. [Online]. Available: http://www.theregister.co.uk/2012/09/10/godaddy_ddos_. [Accessed: 08-Jun-2015].
[11] D. Dittrich, "The 'stacheldraht' distributed denial of service attack tool," 1999. [Online]. Available: https://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt. [Accessed: 08-Jun-2015].
[12] S. Garfinkel and G. Spafford, "Practical Internet and UNIX Security," *O'Reilly Media*, 1996.
[13] CERT, *Tech Tips: Denial of Service Attacks*. Carnegie Mellon: CERT® Coordination Center Software Engineering Institute, 2010.
[14] C. Patrikakis, M. Masikos, and O. Zouraraki, "Distributed Denial of Service Attacks," *Internet Protoc. J.*, vol. 7, no. 4, p. http://www.cisco.com/web/about/ac123/ac147/archive, 2004.
[15] G. Badishi, A. Herzberg, and I. Keidar, "Keeping Denial-of-Service Attackers in the Dark," *IEEE Trans. Dependable Secur. Comput.*, vol. 4, no. 3, pp. 191–204, 2007.
[16] P. Negi, A. Mishra, and B. B. Gupta, "Enhanced CBF Packet Filtering Method to Detect DDoS Attack in Cloud Computing Environment," *Int. J. Com- Puter Sci. Issues*, vol. 10, no. 1, pp. 142–146, 2013.
[17] X. J. Geng and A. B. Whinston, "Defeating distributed denial of service attacks," *IT Prof.*, vol. 2, no. 4, pp. 36–42, 2000.
[18] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Elsevier Sci. Direct Comput. Networks*, vol. 44, no. 5, pp. 643–666, Apr. 2004.
[19] K. Hwang, M. Cai, Y. Chen, and M. Qin, "Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes," *IEEE Trans. Dependable Secur. Comput.*, vol. 4, no. 1, pp. 41–55, Jan. 2007.
[20] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, p. 39, Apr. 2004.
[21] A. Lakhina, M. Crovella, and C. Diot, "Mining anomalies using traffic feature distributions," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 4, p. 217, Oct. 2005.
[22] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical Approaches to DDoS Attack Detection and Response," in *Proceedings of DARPA Information Survivability Conference and Exposition*, 2003, pp. 303–314.
[23] A. Demers, S. Keshav, and S. Shenker, "Analysis and Simulation of a Fair Queuing Algorithm," *J. Internetworking Res. Exp.*, vol. 1, no. 1, pp. 3–26, 1990.
[24] P. Mckenny, "Stochastic Fairness Queuing," in *9th Annual Joint Conference of the IEEE Computer and Communication Societies, the Multiple Facets of Integration*, 1990, pp. 733–740.
[25] A. Mankin and K. Ramakrishnan, "Gateway Congestion Control Survey," 1991. [Online]. Available: http://www.rfc-editor.org/rfc.html. [Accessed: 08-Jun-2015].
[26] S. M. Khattab, C. Sangpachatanaruk, R. Melhem, D. Znati, and T. Mosse, "Proactive Server Roaming for Mitigating Denial of Service Attacks," in *1st International Conference on International Technology: Research and Education*, 2003, pp. 500–504.
[27] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of NetworkBased Defense Mechanisms Countering the DoS and DDoS Problems," *ACM Comput. Surv.*, vol. 39, no. 1, p. 3, 2007.
[28] H. B. Hubboub, "Denial of ServiceAttack in Wireless Sensor Networks," *A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Engineering*, 2010. [Online]. Available: http://library.iugaza.edu.ps/thesis/92125.pdf.
[29] S. Kumar and R. S. R. Gade, "Experimental Evaluation of Juniper Network's Netscreen-5GT Security Device against Layer4 Flood Attacks," *J. Inf. Secur.*, vol. 02, no. 01, pp. 50–58, 2011.
[30] K. Hari and T. Dohi, "Sensitivity Analysis of Random Port Hopping," in *2010 7th International Conference on Ubiquitous Intelligence & Computing and 7th International Conference on Autonomic & Trusted Computing*, 2010, pp. 316–321.
[31] H. Lee and V. Thing, "Port Hopping for Resilient Networks," in *Proc. IEEE 60th Vehicular Technology Conf. (VTC2004-Fall), Vol-5*, 2004, pp. 3291–3295.
[32] M. Srivatsa, A. Iyengar, J. Yin, and L. Liu, "A Client-Transparent Approach to Defend against Denial of Service Attacks," in *Proc. IEEE 25th Symp. Reliable Distributed Systems (SRDS '06)*, 2006, pp. 61–70.
[33] Z. Fu, M. Papatriantafilou, and P. Tsigas, "Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts," *IEEE Trans. Dependable Secur. Comput.*, vol. 9, no. 3, pp. 401–413, May 2012.
[34] S. Tripathi, B. Gupta, A. Almomani, A. Mishra, and S. Veluru, "Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks," *J. Inf. Secur.*, vol. 4, no. 3, pp. 150–164, 2013.
[35] H. K. Vellalacheruvu and S. Kumar, "Effectiveness of Built-in Security Protection of Microsoft's Windows Server 2003 against TCP SYN Based DDoS Attacks," *J. Inf. Secur.*, vol. 02, no. 03, pp. 131–138, 2011.
[36] C. Obimbo and B. Ferriman, "Vulnerabilities of LDAP As An Authentication Service," *J. Inf. Secur.*, vol. 2, no. 4, pp. 151–157, 2011.
[37] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, Jan. 2013.