CSEC640 IA1: Method(s) for Detecting, Preventing or Mitigating Denial of Service (DoS) attacks

Megan Bell

University of Maryland University College

March 5, 2017

Author**'s** Note

This paper was prepared for CSEC 640 Monitoring, Auditing, Intrusion Detection, Intrusion Prevention, and Penetration Testing, taught by Professor Steven Rigby.

Table of Contents

CSEC640 IA1: Method(s) for Detecting, Preventing or Mitigating DoS Attacks

Introduction

Any issue that reduces or denies access to computing resources is considered denial of service (DoS) (Goodrich & Tamassia, 2011). DoS may stem from mistakes, but any DoS poses significant business risk, cost, and reputational harm (Hersher, 2017; Continelli, n.d.). Sadly, the economic impact of DoS attacks can be extraordinary, costing an organization more than $400,000 for a single attack (Somani, Gaur, Sanghi, Conti, and Buyya, 2015). With the evolution of cloud computing, organizations should be highly motivated to reduce the risk of DoS through a combination of defensive, preventative, or mitigating measures.

This paper provides a survey of four important research papers that highlight the trends in successful DoS protection and prevention. The first paper reviews DoS needs for cloud environments. The second paper discusses possible approaches to address DNS amplification attacks given the potential risks stemming from such attacks. The third paper reviews the importance of dual defensive security practices. Finally, the fourth paper reviews a novel traffic management approach for DoS attacks. DoS is used to describe all types of DoS attack types.

Paper 1: DoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions.

The architecture behind cloud computing differs from traditional information systems infrastructures in that resources reside in data centers with centralized computing and are derived from virtualization technologies (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, & Zaharia, 2010). Cloud computing providers enact security requirements to support virtualization and to

address a range of threats such as DoS attacks. Somani, Gaur, Sanghi, Conti, and Buyya (2015) performed a comprehensive examination research literature concerning security for cloud environments and developed a framework to address security design needs of attack prevention, detection, and mitigation solutions. One of the most notable points in addressing DoS attacks is defining DoS attacks as Economic Denial of Sustainability (EDoS) attacks. With more than half of U.S. businesses using cloud computing, DoS could adversely impair several businesses within a single attack (Cohen, 2014).

Detection, Mitigation, or Prevention Techniques

Prevent: Architect a Layered Defense

As observed in Appendix A Table A1, a sophisticated DoS attack may exhibit a diversity of attack methods and characteristics. DoS may employ one of several networking or application protocols and take place at differing attack intensities. Preventing an attack begins with defining layered security architectural requirements. Security must exist at the network backbone service provider, the virtual infrastructure components, and the application layers, which can be reviewed in Appendix A Figure A2. A comprehensive framework redresses major security concerns as presented in Appendix A Figure A3. The major challenge in this study is the need for a case study example to describe an attack scenario with implemented security defenses.

Prevent: Challenge Response Protocols (CRP)

Somani, Gaur, Sanghi, Conti, and Buyya (2015) discuss the need for human verification and various challenge response options. CRP is presented in light of Turing tests, which could

distinguish computer versus human actions. Turing test options such as Captcha enable delineation of whether certain computer activities originate from humans or systems (Huang, Huang, & Chiang, 2013). While CRP requires evolution as computing capabilities advance, CRP is an important component to interrupting certain DoS attacks. Requiring confirmation of human activity could provide a simple solution for control of human-interactive hosts.

Mitigate: Scalability Attacks

Cloud computing carries the unique risk of computing resources that scale on-demand in response for increased capacity. Attackers could use scalability to amplify the magnitude of attack with some knowledge of a scaling algorithm and timing of scaling. The authors define this topic as *Effective Resource Allocation Time*, and its importance is that an organization could plan defensive strategies around the scaling of cloud resources to protect the systems integrity. Controlling scalability could thwart attacks by removing vulnerable resources. Specifically, cloud computing has the inherent capacity to rapidly shift and redeploy computing resources wile halting resources under attack.

Paper 2: Fingerprinting Internet DNS Amplification DoS Activities

DoS attacks are often discussed in terms of TCP protocol attacks such as SYN floods. However, DoS attacks may employ any number of protocols or traffic interruption techniques to achieve denial of service. One common and dangerous attack type is known as an amplification attack where a number of requests are sent to publically accessible hosts using a protocol such as Domain Name Service (DNS) to flood targeted victims with an onslaught of network traffic (Vacca, 2013). DNS amplification attacks manipulate what is known as DNS open resolver in

which a DNS server is left broadly accessible to any source of DNS request rather than authorized DNS requests. Malicious network traffic is sent to these DNS servers, and the servers are tricked into serving requests where smaller-sized input DNS data packets yield larger-sized outbound DNS response traffic, where the increased data size is an amplification factor. The targeted host system can become overwhelmed with high levels of network traffic.

DNS amplification attacks are difficult to address due to the need to protect valid network traffic. Further, the ease of execution makes DNS amplification a widely used exploit that has been implemented in about 34% of DoS attacks (MacFarland, Shue, & Kalafut, 2015). Few organizations have the network infrastructure and resources to deal with such attacks (CERT, 2013). However, Fachkha, Bou-Harb, and Debbabi (2014) developed a method to characterize DNS amplification attacks associated with suspect network sources and reduce related risks.

Detection, Mitigation, or Prevention Techniques

Detection: Define the Scope of Suspicious Activity

Fachkha, Bou-Harb, and Debbabi (2014) approach the threat of DNS amplification attacks from the perspective of targeting suspect network traffic sources. Since DNS is fundamental to all network traffic, focusing on suspect sources provided a means to distinguish legitimate and suspect network traffic. With this context, the authors evaluate sources of suspect traffic to profile DNS amplification attack characteristics that could be used for defense and mitigation. DNS requests from these sources are collected for a period of three month, and bad actors are identified as originating from "darknet" sources. In total, about 720 GB of network traffic is collected. Post-collection, different traffic profiles such as low activity stealth DNS requests and flash DNS

request attacks are developed based DNS traffic patterns.

Detection: Practice Profiling to Quantify Risk

MacFarland, Shue, & Kalafut (2015) identify methods such as remote hosting of DNS servers to alleviate DNS amplification attacks. This method channels DNS traffic to an alternative vector, but did not address the underlying attack type. Rather than switching traffic burden, Fachkha, Bou-Harb, and Debbabi (2014) systematically profiles DNS amplification attacks to proactively locate a range of attack patterns. As observed in in Appendix B Table B1, a base pattern is developed to characterize an attack versus normal DNS traffic. An attack is defined as having at least 25 DNS query data packets from the same host with an information request of ANY which results in telling a DNS server to send the maximum amount of information to a target.

Based on profiling collected DNS data flows, the authors successfully detect attack patterns. A summary of attack categories are listed in Appendix B Table B2. The most significant is a flash attack where the DNS server is bombarded with a high rate of DNS queries. Another interesting attack type is the stealth attack where few packets were sent, indicating reconnaissance. In both the flash attack and stealth attack, the authors identify specific parameters that could be used in a network intrusion detection system (NIDS) for suspicious DNS activity.

Prevention: Fine-tuning NIDS

Active security research can lead to gap identification in network traffic filtering and detection capabilities. In this study, the authors evaluate their results against a NIDS system. The NIDS analyzes collected data and corroborates some attack patterns observed by the authors. For

example, the NIDS detects high velocity DNS amplification attacks, but not low velocity stealth attacks. This type of gap may be important to potentially fine-tuning NIDS rules and alerts. An organization may find that stealth attacks fall outside risk identification parameters and not worth tracking. However, knowledge of stealth attacks may contribute to better threat modeling.

Paper 3: Design and Development of Proactive Models for Mitigating Denial-of-Service and Distributed Denial-of-Service Attacks

H.R. and Sekaran (2007) evaluate two defense models of *Secure Overlay Services (*SOS) Model and the *Server Hopping* Model and their role in detecting and mitigating DoS attacks. The first method of Secure Overlay Services (SOS) refers to an architecture developed to protect communications (Keromytis, Misra, & Rubenstein, 2004). The goal of SOS is to protect communications channels during an attack by distinguishing against authorized and unauthorized users. The second method is the Server Hoping Model (SHM) with distributed firewalls where a proxy server controlled flexible resource availability for approved clients. In the event of DoS, the Server Hoping Model can switch servers to provide continuous availability—circumventing attacks. This paper signifies the importance of evaluating a multi-pronged defense approach.

Detection, Mitigation, or Prevention Techniques

Prevent: Secure communications

SOS evolved in the aftermath of 9/11 where it was realized that communications lines required protection (Keromytis, Misra, & Rubenstein, 2004). SOS is an end-to-end architecture that combines, encrypted communication channels, and software level verification nodes to secure

and to direct communications. When network traffic is impeded, SOS protects its communications channels and forwards protected communications. Without SOS, a DoS attack can quickly escalate network traffic to potentially dangerous levels with an example of rate escalation presented in Appendix C Figure C1. When under attack, SOS achieves consistent delivery of communications traffic as observed in Appendix C Figure C2.

Mitigate: Bypass Attacks

SHM with distributed firewalls is designed to protect active connected systems while bypassing attacks. It is a framework that relies on pre-established and controllable networking relationships between a host client and target server. In order for this model to work, network connections must be monitored for connectivity and then automatically updated for server location changes. The model must accommodate a method of transitioning active server connectivity and the current state of application activity.

In experiments, SHM maintains availability of computing resources. This could be an important advancement to address loss of systems access to legitimate users and to maintain organizational computing operations under attack. SHM is achieved through proxy servers for dynamic server connection management. The proxy server's location changes dynamically as a function of time, and a cryptographic key is shared between a server and its connected clients. SHM systems adjust connectivity based on firewall response.

Detect: Use Active and Flexible Firewalls

Firewalls were originally developed as hardware appliances that filtered network traffic. As

security needs evolved, firewalls took on additional roles such as a network intrusion prevention system (NIPS). SHM has further evolved the role of the firewall into a secure and flexible server connection management tool. With a firewall delivering frontline commands in telling the system to adjust for traffic control conditions, SHM achieves the delivery of self-adjusting defense. As observed in Appendix C Table C3, SHM halts an attack even while DoS attack traffic escalates.

Paper 4: Defending against DoS attacks with max-min fair server-centric router throttles

It has been proposed that DoS can be treated as a network congestion problem. In this context, Ioannidis and Bellovin (2002) propose using routers to manage DoS attacks through a pushback mechanism where a router identifies a malicious packet and then adjusts traffic accordingly to let good traffic pass while halting bad traffic. This option left control to the router, which could potentially be overwhelmed in high-volume DoS attacks. Yau et al (2005) quantitatively propose a network traffic response solution that enacted collective router traffic control. Central tenants are that routers in the same network have trust and traffic can be selectively throttled when resource demands achieve certain thresholds.

Detection, Mitigation, or Prevention Techniques

Prevent: Collaborative Network Traffic Control

Yau et al (2005) indicate that network traffic could be systemically managed through resource throttling. Resource throttling engages multiple routers in a connected network to collaborate on overall control of network traffic. Throttling works through communication of a throttle signal between routers where coordinated congestion permits routers to maintain

appropriate bandwidth for respective network traffic management while sharing increased network traffic burden. A router with heavier traffic flow is able to share its burden with other networked routers. Deploying routing controls within a networked environment achieves automation that balance traffic load and reduce the severity of sudden network traffic congestion, which is a significant benefit in delivering consistent availability of resources.

Deployment and maintenance of this system are important early investments. First, routers must have reasonable capabilities to participate in throttled traffic management. Two, an organization must have the technical capabilities to build and to deploy a customized network of interconnected routers. Third, deployment of a custom traffic management system requires occasional reassessment for updates and performance tuning.

Detect: Algorithms Provide Baselines for Action

Yau et al (2005) quantify traffic control as a measurable event where the set of interconnected routers use thresholds to monitor and adjust network traffic among connected routers. Normal traffic levels are set based on typical host activity within a network. When network traffic reaches a certain threshold, the set of routers coordinate to ensure access to network resources. A minimum-maximum algorithm facilitates adjusting traffic loads to distribute traffic. The baseline algorithm also incorporates the abilities of individual routers to tolerate certain levels of traffic. Fairness among routers is established by throttling software to assist in deployment of the baseline algorithm. It is important to achieve convergence with a sustainable mathematical baseline, which may be the most difficult aspect of this traffic control system.

Mitigate: Routers Can Coordinate Traffic To Alleviate Attack Burden

A subset of traffic control management is the ability to alleviate traffic congestion in response to DoS mitigation. A series of experiments conducted by Yau et al (2005) acknowledged that throttling traffic control did not completely balance attack network traffic while maintaining good network traffic. Successful deterrence depended of several factors—some of which could be measured in light of percentage of good traffic permitted by the network and the number of router involved in protection. Study authors indicated that network traffic complexity could result in false positives that penalize legitimate traffic. However, a system of known good pre-authorized users and systems could establish definitive and efficient network access while restricting suspicious activity. This paper would benefit from further elaboration on its potential mitigation benefits.

Conclusion

Four important theme papers were surveyed for the detection, prevention, and mitigation of DoS attacks. First, cloud environments were reviewed for the need to prevent attacks with layered security and use of human interaction. Scaling risks were also discussed for use in DoS attack mitigation. Second, detection and prevention of amplification DoS attacks were evaluated relative to the DNS protocol. Focusing on suspect traffic and profiling offers the opportunity to limit such attacks with better prevention and detection. Third, dual defense mechanisms to protect communications and bypass DoS attacks were considered. Denial to resources in DoS attacks eliminates target detection and reach for attack. Finally, a layered network response based on self-adjusting traffic management identified methods to address the need for more intelligent network systems that can defend themselves from attack and mitigate attack burden.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & Zaharia, M. (2010). A view of cloud computing. *Communications Of The ACM*, *53*(4), 50-58.

Cohen, R. (2014, June 11). The cloud hits the mainstream: More than half of U.S. businesses now use cloud computing. *Forbes*. Retrieved from https://www.forbes.com/sites/reuvencohen/2013/04/16/the-cloud-hits-the-mainstream-more-than-half-of-u-s-businesses-now-use-cloud-computing/#3a8adec010be

Continelli, A. (n.d.). How to identify and prevent software failure risks. Retrieved from https://www.business.com/articles/aaron-continelli-identify-and-prevent-software-failure/

Fachkha, C., Bou-Harb, E., & Debbabi, M. (2014, March). Fingerprinting internet DNS amplification DDoS activities. In *New Technologies, Mobility and Security (NTMS), 2014 6th International Conference on* (pp. 1-5). IEEE.

Goodrich, M. T., & Tamassia, R. (2011). Introduction to computer security. Boston: Pearson.

HR, N., & Sekaran, K. C. (2007). Design and development of proactive models for mitigating denial-of-service and distributed denial-of-service attacks. *IJCSNS*, *7*(7), 167.

Hersher, R. (2017, March 03). Amazon and the $150 million typo. NPR. Retrieved from http://www.npr.org/sections/thetwo-way/2017/03/03/518322734/amazon-and-the-150-million-typo

Huang, V. S. M., Huang, R., & Chiang, M. (2013, March). A DDoS mitigation system with multi-stage detection and text-based turing testing in cloud computing. In Advanced

Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on (pp. 655-662). IEEE.

Ioannidis, J., & Bellovin, S. M. (2002, February). Implementing pushback: Router-based defense against DDoS attacks. In *NDSS*. Retrieved from http://www.cs.columbia.edu/~locasto/projects/candidacy/papers/ioannidis2002pushback.pdf

Keromytis, A. D., Misra, V., & Rubenstein, D. (2004). SOS: An architecture for mitigating DDoS attacks. *IEEE Journal on selected areas in communications*, *22*(1), 176-188.

MacFarland, D. C., Shue, C. A., & Kalafut, A. J. (2015, March). Characterizing optimal DNS amplification attacks and effective mitigation. In *International Conference on Passive and Active Network Measurement* (pp. 15-27). Springer International Publishing.

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2015). DDoS Attacks in cloud computing: issues, taxonomy, and future directions. Retrieved from https://arxiv.org/pdf/1512.08187.pdf

US-CERT. (n.d.). Alert (TA13-088A). Retrieved from https://www.us-

Vacca, J. R. (2013). Computer and information security handbook (Second ed.). Amsterdam: Elsevier.

Yau, D. K., Lui, J., Liang, F., & Yam, Y. (2005). Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles. *IEEE/ACM Transactions on Networking (TON)*, *13*(1), 29-42.

Appendix A

Diagrams: DoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions

Table A1

DDoS Attack Example with Delineated Characteristics

Features	**Details**
Attack Packets	HTTP GET, POST, TCP SYN, ICMP and amplification by DNS, NTP and TFTP
Attack Frequency	Typical minimum frequency is >500 requests/s, depends upon resources at bot the ends [Moore et al. 2006]
Attack Bandwidth	Gbps to 300 Gbps [Burt 2014]
Attackers	A single source, a network or botnet. Cloud servers (BotClouds) may also be used to utilize profound resources to win the “arms race”.
Attack Methods	Low rate, flood, flash mimic, amplification and massive
Attack Repetition	In many cases repetition is done from different sources after few minutes/hours
Attack Duration	Minutes to hours (average 72 minutes in [Burt 2014]) and some lasts a few days.
Attack Targets	Multimedia, government, e-commerce, cloud services and many other targets

Table A1

DDoS Attack Example with Delineated Characteristics

Features	Details
Attack Motives	Competition, Rivalry, Extortion, Smoke-screening and cyber war between countries
Attack Timings	Important days for the enterprises including product launch, sale launch, important days for countries etc.

Table A1. Example DDoS attack model. Reprinted from "DoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions", by Somani, Gaur, Sanghi, Conti, & Buyya, 2015, retrieved from https://arxiv.org/pdf/1512.08187.pdf. Copyright 2015 by Somani & Conti.

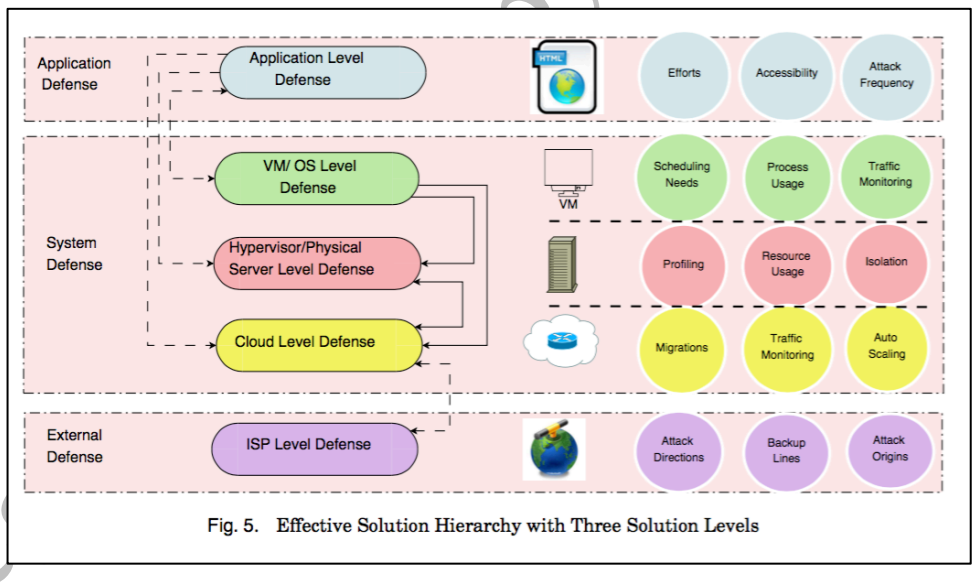

Fig. 5. Effective Solution Hierarchy with Three Solution Levels

Figure A1. Cloud DDoS attack security framework illustration. Reprinted from "DoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions", by Somani, Gaur, Sanghi, Conti, & Buyya, 2015, retrieved from https://arxiv.org/pdf/1512.08187.pdf. Copyright 2015 by Somani & Conti.

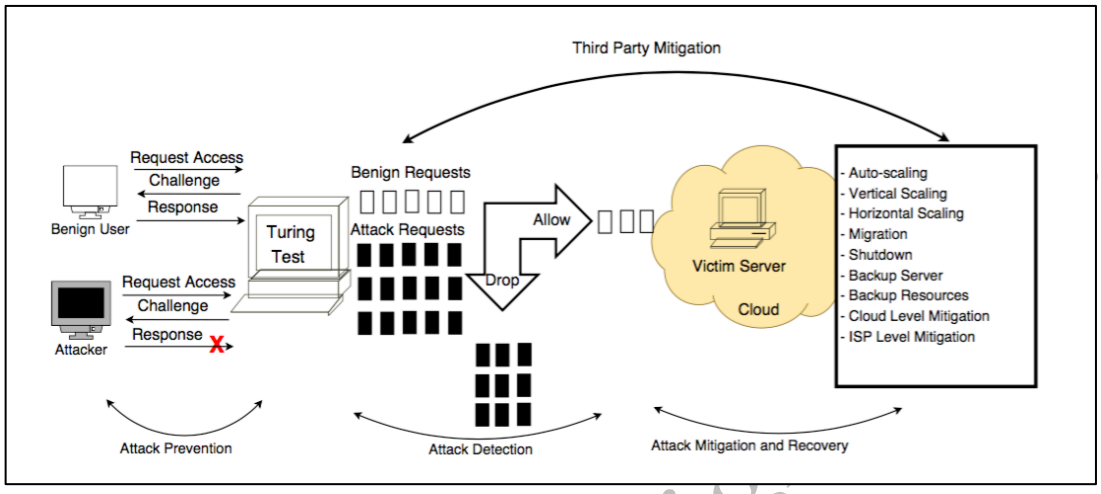

Figure A2. Cloud DDoS security mitigation illustration. Reprinted from "DoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions", by Somani, Gaur, Sanghi, Conti, & Buyya, 2015, retrieved from https://arxiv.org/pdf/1512.08187.pdf. Copyright 2015 by Somani & Conti.

Appendix B

Diagrams: Fingerprinting Internet DNS amplification DDoS activities

Table B1

Defined Criteria to Identify DNS Attack

Parameter	Value
Packet Count	> 25
Scanned Hosts	> 25
DNS Query Type	ANY
Requested Domain	Root_DNS_DB

Table B1. Defined criteria to identify DNS attack. Reprinted from "Fingerprinting Internet DNS Amplification DDoS Activities", by Fachkha, Bou-Harb, & Debbabi, 2014, In New Technologies, Mobility and Security (NTMS), IEEE 6th International Conference on (pp. 1-5). Copyright 2017 by IEEE.

Table B2

Attack Profile Characterization for DNS Amplification

Attack Category Rate	Value (pps)
Packet Count	Rate <= 0.5

Table B2 Attack Profile Characterization for DNS Amplification	
Scanned Hosts	0.5 < rate < 4700
DNS Query Type	rate >= 4700

Table B2. Attack profile characterization for DNS amplification. Reprinted from "DoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions", by Somani, Gaur, Sanghi, Conti, & Buyya, 2015, retrieved from https://arxiv.org/pdf/1512.08187.pdf. Copyright 2015 by Somani & Conti.

Appendix C

Diagrams: DoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions

The following Fig. 8. represents analysis of DoS /DDoS attack without any defense models.

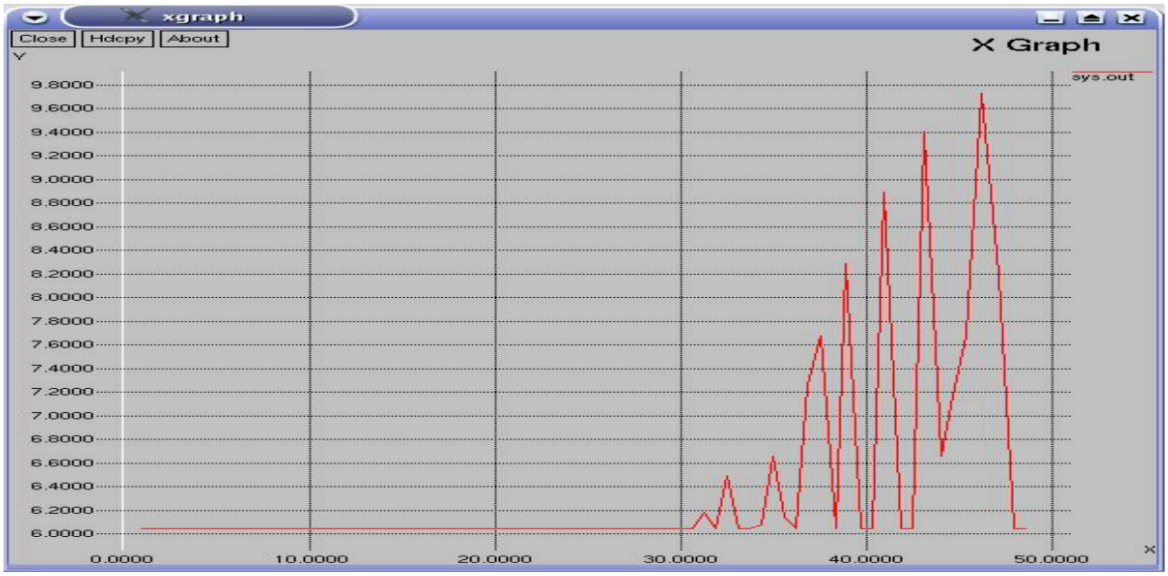

Fig. 8 Analysis of DoS

Figure C1. Illustration of DoS attack without defensive measures. Reprinted from "Design and Development of Proactive Models for Mitigating Denial-of-Service and Distributed Denial-of-Service Attacks", by HR & Sekaran, 2007, IJCSNS, 7(7), 167. Copyright 2017 by IJCSNS.

The following Fig. 9. represents packet delivery time without DoS defense and with DoS defense for SOS architecture.

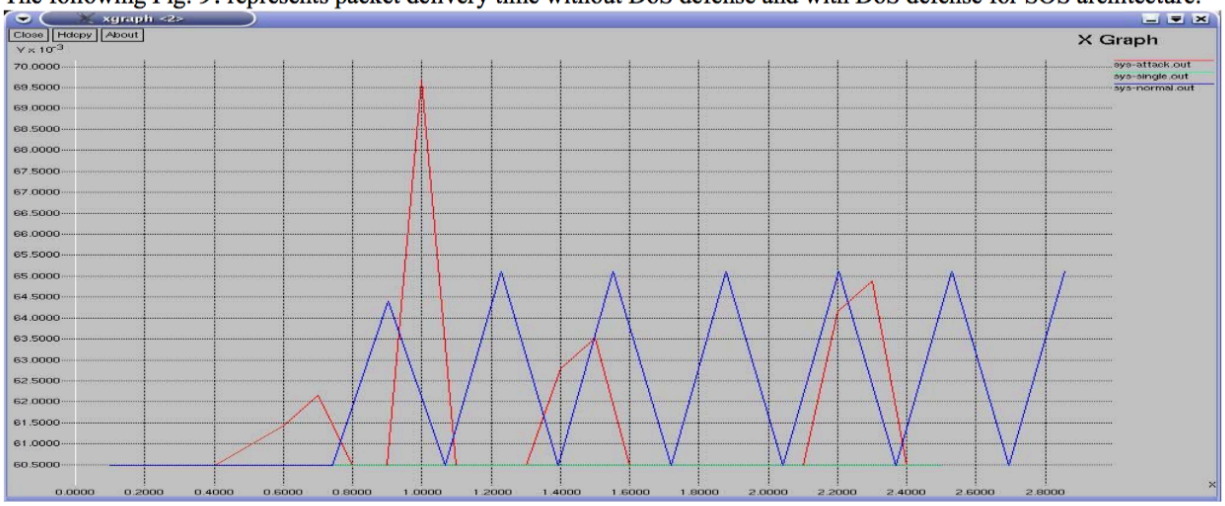

Fig. 9 Packet delivery time without DoS defense and with DoS defense for SOS

Figure C2. Illustration of DoS attack with SOS defense. Reprinted from "Design and Development of Proactive Models for Mitigating Denial-of-Service and Distributed Denial-of-Service Attacks", by HR & Sekaran, 2007, IJCSNS, 7(7), 167. Copyright 2017 by IJCSNS.

The following Fig. 10. represents packet delivery time without DoS defense and with DoS defense for server hopping with distributed firewall architecture.

Fig. 10 Packet delivery time without DoS defense and with DoS defense for Server Hopping

Figure C3. Illustration of DoS attack with server hop defense. Reprinted from "Design and Development of Proactive Models for Mitigating Denial-of-Service and Distributed Denial-of-Service Attacks", by HR & Sekaran, 2007, IJCSNS, 7(7), 167. Copyright 2017 by IJCSNS.