UNIVERSITI PUTRA MALAYSIA

DDOS AVOIDANCE STRATEGY FOR SERVICE AVALIBILTY

BEDOUR FAHHAD HAMED ALRASHIDI

FSKTM 2015 40

DDOS AVOIDANCE STRATEGY FOR SERVICE AVALIBILTY

BY

BEDOUR FAHHAD HAMED ALRASHIDI

Thesis Submitted to the Faculty of Computer Science and Information Technology, University Putra Malaysia, in Fulfillment of the Requirements for the Degree of Master of Computer Science

June 2015

A abstract of thesis presented to the Senate of University Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

DDOS AVOIDANCE STRATEGY FOR SERVICE AVALIBILTY

BY

BEDOUR FAHHAD HAMED ALRASHIDI

June 2015

Chairman: Lecturer Mrs Hjh Zaiton Muda.
Faculty: Computer Science and Information Technology

A Distributed Denial of Service (DDoS) attack is widely regarded as a major threat for the current Internet because of its ability to create a huge volume of unwanted traffic and avoid the service for the users. It is hard to detect and respond to DDoS attacks due to the large and complex network environments. When the DDoS attack is being executed, in most of the cases, the target cannot provide its services normally. This is not a significant problem for non-critical application, but for availability critical services such as stock financial, stock market, or governmental, the effect of the attack may involve huge damage. In this thesis, the distance-based DDoS detection technique was introduced by developing prototype as a real simulation for different protocols flood in vb.net. The technique was tested by using the CAIDA DDoS Attack 2007 Dataset. The method for discreet event simulation (DES) was applied to get the result after applying DDoS attack protection. The attacks are detected by analyzing distance values and traffic rates. The distance information of a packet can be inferred from the Time to- Live (TTL) value of the IP header.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
Sebagai memenuhi keperluan untuk ijazah Master Sains.

DDOS AVOIDANCE STRATEGY FOR SERVICE AVALIBILTY

BY

BEDOUR FAHHAD HAMED ALRASHIDI

June 2015

Pengerusi: Lecturer Mrs Hjh Zaiton Muda
Fakulti: Computer Science and Information Technology

Serangan *Distributed Denial of Service (DDoS)* dianggap secara meluasnya sebagai ancaman yang utama terhadap Internet terkini kerana kebolehannya untuk mencipta trafik yang tidak diperlukan dalam jumlah yang besar dan menghalang servis kepada pengguna. Adalah sukar untuk mengecam dan memberi maklum balas kepada serangan DDoS disebabkan persekitaran rangkaian yang terlalu besar dan kompleks. Dalam kebanyakan kes, apabila serangan DDoS sedang dilaksanakan, target tidak dapat memberikan servis yang normal. Perkara ini tidak menjadi masalah yang ketara kepada aplikasi bukan-kritikal tetapi bagi servis yang kritikal seperti kewangan stok, pasaran stok, atau pihak swasta, kesan kepada serangan ini akan melibatkan kerosakan yang besar. Dalam tesis ini, teknik pengesanan DDoS berasaskan jarak diperkenalkan dengan membangunkan satu prototaip sebagai simulasi sebenar untuk beberapa protokol *flood* yang berbeza dalam vb.net. Teknik ini telah diuji menggunakan dataset CAIDA DDoS Attack 2007. Kaedah untuk simulasi kejadian secara diskret (DES) diaplikasikan untuk mendapat keputusan selepas memasukkan kawalan serangan DDoS. Serangan dikesan dengan menganalisa nilai jarak dan kadar trafik. Maklumat jarak bagi paket boleh disimpulkan daripada *Time-To-Live* (TTL) bagi kepala IP.

ACKNOWLEDGEMENTS

I would like to thank all people who support me along by all means for my master's Research journey and make this study achieved. Foremost, I would like to express my sincere gratitude to my Associate Professor Mrs Hjh Zaiton Muda for the continuous support of my Master study, for her patience, motivation and immense knowledge. Her guidance support me in all the time of Research. Besides my supervisor , I would like to thank my assessor Dr. Zuriati for the stimulating discussions and enlightening me for improving my research. My deep appreciation to all my friends for their precious support ,courage and their positive advices which made me continue with this journey . Special thanks to my mother Turkya, father Fahaad , sisters, brother and brother in law for their endless love and support , I would not have finish my study and any overcome any challenges in my life without their prayers and advices. Lastly , without the care and mercy of Allah in my life , I would not able to make and achieve anything .

APPROVAL

A thesis prepared by Bedour Fahaad Alrashidi with the title "**DDOS AVOIDANCE STRATEGY FOR SERVICE AVALIBILTY**" submitted in partial to fulfilment of requirement of the master of Computer Science and Information Technology Universiti Putra Malaysia.

Approved By:

_____

Zaiton Muda

Senior Lecturer

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Supervisor)

_____

Zuriati Ahmad Zukarnain , PhD

Associated Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Assessor)

DECLARATION

I declare that this thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously and it is not concurrently submitted to other institutions.

_____

BEDOUR FAHHAD HAMED ALRASHIDI

Date:

TABLE OF CONTENTS

LIST OF TABLES

Page

Tables

LIST OF FIGURES

Figure **Page**

LIST OF ABBRIVAITION

DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
NIDS	Network Intrusion Detection System
SDN	Software Defined Networks
TCP	Transmission Control Protocol
TTL	Time To Live
TLS	Transport Layer Security
UDP	User Datagram Protocol
DES	Discreet Event Simulation

CHAPTER 1

INTRODUCTION

1.1 Background

Today, Distributed Denial of Service (DDoS) attacks have become a common threat to online businesses. With over 50,000 distinct attacks per week, DDoS attacks have become highly visible and costly form of cyber-crime, and are increasingly being proactively addressed by online businesses to avoid devastating costs of DDoS related downtime. Recent trends in the Internet show that the total amount of the DDoS attacks reached over 100 gigabit per second barrier. It also shows that the amount of DDoS attack traffic has been increasing in size year by year. A study conducted by Arbor networks shows the year-by-year increase of the DDoS attack traffic on the Internet, from the year 2001 to 2011 as shown in Figure 1. Denials of service attacks (DoS) deny services to legitimate users offered by the server or target machine. With time, DoS attack evolved to distributed denial of service attack where attacker compromises some other vulnerable machines on the Internet to coordinate attack at a single instant of time on the victim machine thus multiplying the effect of denial of service.

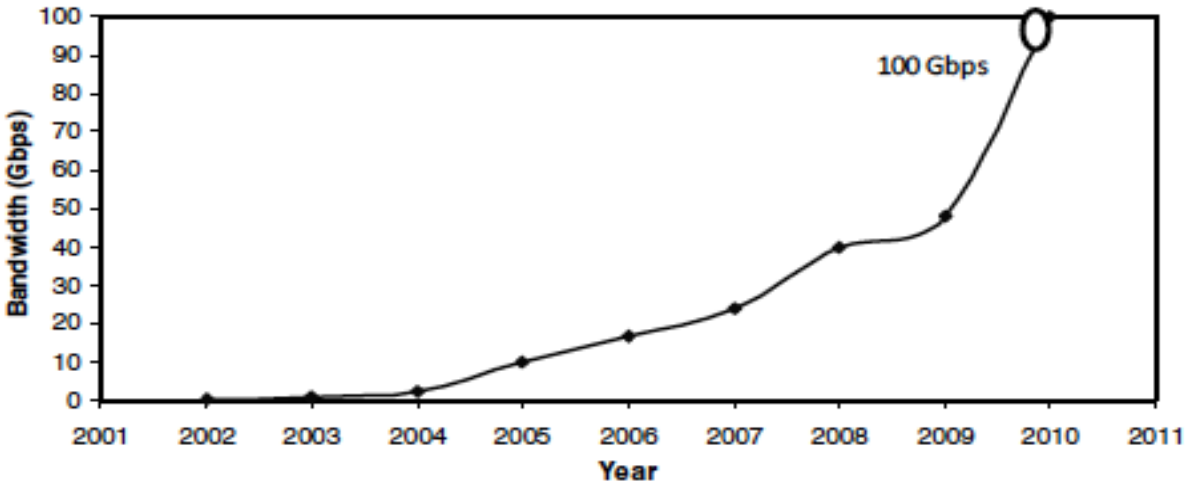

Figure 1: DDoS Attack Traffic on the Internet

As the time is going on, the impact of DDoS assaults on Internet security is becoming colossally. Inside of an almost no compass there is a gigantic increment in the size a recurrence of DDoS assaults. With the new advances and new procedures, the aggressors are discovering more refined approaches to assault the servers. In this circumstance it is important to concoct different components to identify and guard these DDoS assaults and shield the servers from the aggressors. Numerous investigates have be done to identify the DDoS assault activity in transport layer, which is more powerless against DDoS assaults. DDoS assaults are more regular in transport layer. Coming to application layer, they acquire enormous misfortune and it is exceptionally hard to relieve DDoS assaults even under the vicinity of solid firewalls and Intrusion Prevention Security. Inquires about are being led to alleviate application layer DDoS assaults. Figure 2 shows the top 10 attack techniques in (2013) and the most percentage goes to DDoS attack by 23% so it is clear that this issue have to be addressed and solved by doing many research.

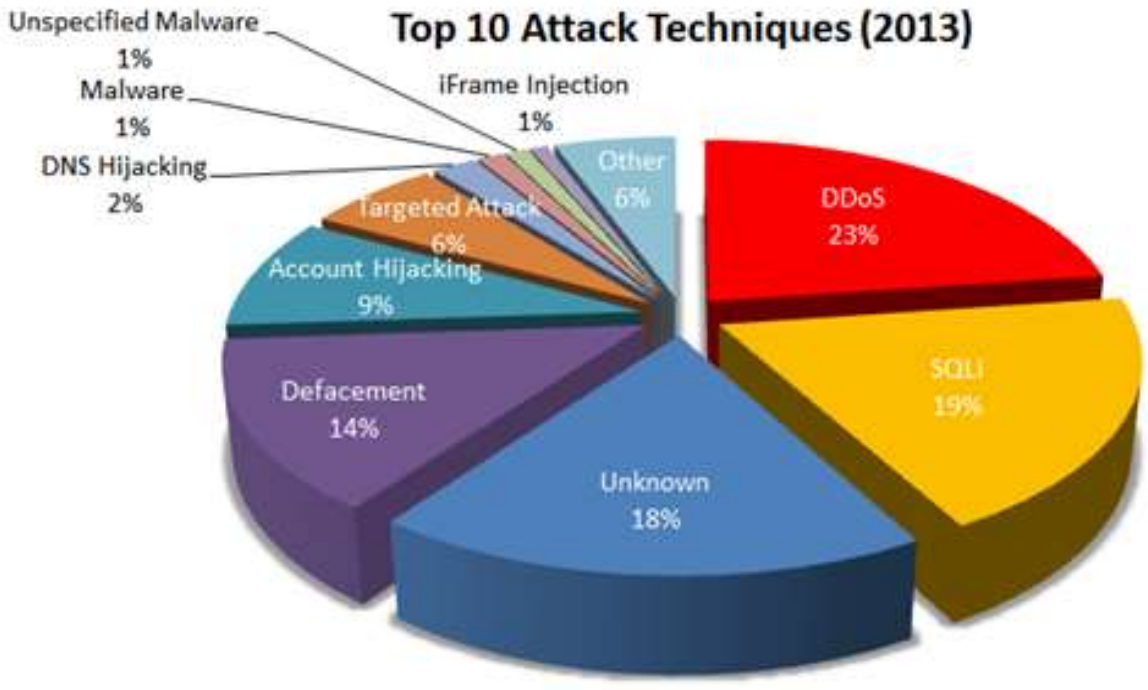

Figure 1.2: The Top 10 Attack Techniques in (2013)

As a rule, system bundles use TCP/IP for transmission. The bundles themselves are innocuous, however in the event that there are an excess of unusual parcels, it will bring about the system gadgets or servers to over-burden. This can rapidly devour the framework assets. Another case is if the parcels exploit certain conventions' creating the disappointment of system gadgets or servers. Both cases will bring about refusal of administration. These are the fundamental standards of DDoS assaults.

1.2 Problem statement

- The main problem need to be discussed in this study, is based on the paper work from (Seung-Hoon Kang et al. ,2013). The work they achieved solution for DDoS protection system in previous work is to provide the service to predigested users by using the DDoS avoidance strategy for service availability by divide the attack scenario in different time points and provide alternative access channels to already authenticated and other valid users but they did not focused in in the increase of the level of protection by improving the Internet infrastructure and some mechanism and features to avoid the attacker and eliminating the vulnerabilities that could be target of attack, and installing security patches. These security measures provide safeguard mechanism to reduce the possibility of DDoS attacks by provide effective mechanism to eliminate or avoid attacks and deliver continuous service availability.
- DDoS Attack response should employ intelligent packet discard mechanisms to reduce the downstream impact of the flood while preserving and routing the non-attack packets, by reducing the traffic when it overpasses a threshold value and it tries to cover the issue of how to recognize the malicious traffic from the receiving traffic, meanwhile the discovery of the real source where the attack is being executed.

- The number of devices that has been attacked has increased due to the lack of well defined patterns.
- Choosing suitable detection method is playing the major role to detect DDoS attack in different scenarios.
- There is therefore the need for an effective and efficient techniques to make protection of normal traffic from the DDoS attack .

1.3 Objectives

The objective of this work can be split into two folds; this will help to find the best Output and embed it to be used for future DDosS avoidance system.

- Find a suitable method and techniques to make the service available and the normal packet is executing in the network without DDoS attack.
- Develop a prototype for DDoS avoidance system using a suitable monitoring for the packets in the selected network.

1.4 Scope

This study has different scopes need to be followed in order to meet the objectives Planned:

- To re-implement DDoS avoidance strategy for availability by using discrete event simulation (DES).
- Propose a prediction System by monitoring and analyzing the packet before and after DDoS attack .

1.5 Organization of thesis

The remainder of this thesis is organized as follows:

Chapter 2 will discuss the existing DDoS and DoS techniques, algorithms and their applications in addition to the advantages and disadvantages. Chapter 3, is considering data preprocessing in general the analysis and preparations in order to have a good methodology for DDoS when apply the detection and protection techniques.

In Chapter 4, we apply the detecting classification techniques such as TCP, UDP floods and used the evaluation measurements to measure the model built performance by using time and capacity of the packet metrics. In Chapter 5, the System will be implemented based on the rules generated from the best model in Chapter 4 and will develop a system prototype to be used by end user .

In Chapter 6, will conclude the study and its effect and what is the future work that can improve the result of current study.

REFERENCES

S. H. Kang, K. Y. Park, S. G. Yoo, and J. Kim, "DDoS avoidance strategy for service availability," Cluster Computing, Online First,Springer, DOI: 10.1007/s10586-011-0185-4, October 2011.

Yim, H.B., Kim, T.W.: Probabilistic route selection algorithm to trace DDoS attack traffic source. In: IEEE International Conference on Information Science and Application (ICISA2011), Apr.2011, pp. 1–8 (2011).

Zhang, C., Cai, Z., Chen, W., Luo, X., and Yin, J. (2012) Flow level detection and filtering of low-rate DDoS. Computer Networks, 56, 3417–3431.

Mirkoviac, J., Prier, G., and Reiher, P. (2002) Attacking DDoS atthe source. Proceedings of the 10th IEEE International Conference on Network Protocols, Paris, France, 12-15 November, pp. 1092–1648. IEEECS.

Chen, C. L. (2009) A new detection method for distributed denial of- service attack traffic based on statistical test. Journal of Universal Computer Science, 15, 488–504.

Thomas, R., Mark, B., Johnson, T., and Croall, J. (2003)NetBouncer: Client-legitimacy-based high performance DDoS filtering. Proceedings of the 3rd DARPA Information Survivability Conference and Exposition, Washington, DC, 22-24 April, pp. 111–113. IEEE CS, USA.

Zhang, G. and Parashar, M. (2006) Cooperative defence against DDoS attacks. Journal of Research and Practice in Information Technology,38, 1–14.

Lu, K., Wu, D., Fan, J., Todorovic, S., and Nucci, A. (2007)Robust and efficient detection of DDoS attacks for large-scale internet. Computer Networks.

Dongwon Seo, Heejo Lee and Adrian Perrig, "PFS: Probabilistic Filter Scheduling Against Distributed Denial-of-Service Attacks", 36th Annual IEEE Conference on Local Computer Networks(LCN 2011), pages9-17.

Shiaeles, S. N., Katos, V., Karakos, A. S., and Papadopoulos, B. K.(2012) Real time DDoS detection using fuzzy estimators. Computers & Security, 31, 782–790.

Kumar, P. A. R. and Selvakumar, S. (2011) Distributed denial of service attack detection using an ensemble of neural classifier. Computer Communication, 34, 1328–1341.

Douligeris C. Mitrokosta, A. (2004) DDoS Attacks and Defense Mechanisms: Classification and State-of- the-Art. Computer Networks,44,643-666 .

Muraleedharan N, Arun Parmar, Manish Kumar: A Flow Based Anomaly Detection using Chi-square technique.978-1-4244-4791-6/10©2010 IEEE.

Yonghua You, Mohammad Zulkernine, and Anwar Haque, "Detecting Flooding- Based DDoS Attacks", IEEE Proceedings on International Conference on Communications (ICC) 2007.

B. Krishnamurthy and J. Wang. On Network-aware Clustering of Web Clients. In Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer

Communication, pages 97–110. ACM, 2000. ISBN 1581132239.

B. Krishnamurthy, S. Sen, Y. Zhang, and Y. Chen. Sketch-based ChangeDetection: Methods, Evaluation, and Applications. In Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement, pages 234–247. ACM, 2003.

A. Kuzmanovic and E.W. Knightly. Low-rate TCP-targeted Denial of Service Attacks: The Shrew vs. The Mice and Elephants. In Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, page 86. ACM, 2003. ISBN 1581137354.

C. Labovitz. The Internet Goes to War. http://asert.arbornetworks.com/2010/12/the-internet-goes-to-war/, 14 Dec 2010. [Online; accessed23-Sep-2012].

Q. Le, M. Zhanikeev, and Y. Tanaka. Methods of Distinguishing Flash Crowds from Spoofed DoS Attacks. In Proceedings of 3rd EuroNGI Conference on Next Generation Internet Networks, pages 167–173. IEEE, 2007. ISBN 1424408571.

A. Leach. Mr Sulu causes DDoS panic after posting link on Facebook. http://www.theregister.co.uk/2012/06/08/takei_ddos_ facebook_fans/, 2012. [Online; accessed 22-Nov-2012].

C. Lévy-Leduc. Detection of Network Anomalies Using Rank Tests.

J. Li, Y. Liu, and L. Gu. DDoS Attack Detection Based on Neural Network.In Aware Computing (ISAC), 2010 2nd International Symposium on, pages 196–199. IEEE, 2010.

G. Linden. Make Data Useful. Presentation, Amazon, November, 2006.

W.Z. Lu and S.Z. Yu. An HTTP Flooding Detection Method Based on Browser Behavior. In Computational Intelligence and Security, 2006 International Conference on, volume 2, pages 1151–1154. IEEE, 2006. //www.theage.com.au/technology/technology-news/

G. Münz and G. Carle. Application of Forecasting Techniques and Control Charts for Traffic Anomaly Detection. In Proc. 19th ITC Specialist Seminar on Network Usage and Traffic, Berlin, Germany, 2008.

J. Nazario. Political DDoS: Estonia and Beyond (Invited Talk). In USENIX Security, volume 8, 2008.

H. Niksic. GNU wget. Available from the master GNU archive siteprep.ai.mit.edu, and its mirrors, 1998.

H. Park, P. Li, D. Gao, H. Lee, and R. Deng. Distinguishing between FE and DDoS Using Randomness Check. Information Security, pages 131–145,
2008.

J.S. Park and M.S. Kim. Design and Implementation of an SNMP-basedTraffic Flooding Attack Detection System. Challenges for Next Generation Network Operations and Service Management, pages 380–389, 2008.

O. Paul. Improving Web Servers Focused DoS Attacks Detection. In Proceedingsof the

IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation (MonAM 2006), Tuebingen, Germany, 2006.

V. Paxson. Bro: A System for Detecting Network Intruders in Real-time Computer networks, 31(23):2435–2463, 1999.

V. Paxson. An Analysis of Using Reflectors for Distributed Denial-ofservice Attacks. ACM SIGCOMM Computer Communication Review, 31
(3):38–47, 2001.

S. Sanfilippo. Hping–Active Network Security Tool. http://www.hping.org/, 2008. [Online; accessed 22-Nov-2012].

C.E. Shannon. A Mathematical Theory of Communication. ACM SIGMOBILE Mobile Computing and Communications Review, 5(1):3–55, 2001.

R. Singel. Operation Payback Cripples MasterCard Site in Revenge for WikiLeaks Ban. http://www.wired.com/threatlevel/2010/12/ web20-attack-anonymous/, Dec 2010. [Online; accessed 24-Sep-2012].

V.A. Siris and F. Papagalou. Application of Anomaly Detection Algorithms or Detecting SYN Flooding Attacks. Computer Communications, 29(9):
1433–1442, 2006.

J. Sommers, H. Kim, and P. Barford. Harpoon: a flow-level traffic generator for router and network tests. In ACM SIGMETRICS Performance Evaluation Review, volume 32, pages 392–392. ACM, 2004.

R. Stapleton-Gray and W. Woodcock. National Internet Defense—Small States on the Skirmish Line. Communications of the ACM, 54(3):50–55,
2011.

Packet Storm. Tribe Flood Network 2000 (TFN2K) DDoS Tool, available on-line: http://packetstormsecurity. org/distributed. TFN2k_Analysis-
1.3. txt, 2000.

W.W. Streilein, D.J. Fried, and R.K. Cunningham. Detecting Flood-based Denial-of-service Attacks with SNMP/RMON. In Workshop on Statisticaland Machine Learning Techniques in Computer Intrusion Detection,
Fairfax, Virginia, USA, 2003.

S. Suriadi, A.J. Clark, andD. Schmidt. Validating Denial of Service Vulnerabilities in Web Services. In IEEE Computer Society Proceedings of the Fourth International Conference on Network and System Security. IEEE Computer Society, 2010.