# DETECTION OF DENIAL OF SERVICE (DoS) ATTACKS IN LOCAL AREA NETWORKS BASED ON OUTGOING PACKETS

**MEHDI EBADY MANAA**

**UNIVERSITY UTARA MALAYSIA**

**2012**

# Detection of Denial of Service (Dos) Attacks in Local Area Networks Based on Outgoing Packets

**A project submitted to Dean of Awang Had Salleh Graduate School**

**in partial fulfillment of the requirement for the degree**

**Master of Science of Information Technology**

**Universiti Utara Malaysia**

**By**

**MEHDI EBADY MANAA**

# PERMISSION TO USE

In presenting this project of the requirements for a Master of Science in Information Technology (MSc. IT) from Universiti Utara Malaysia, I agree that the University library may make it freely available for inspection. I further agree that permission for copying of this project paper in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or in their absence, by the Dean Awang Had Salleh Graduate School. It is understood that any copying or publication or use of this project or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my project paper.

Request for permission to copy or make other use of materials in this project, in whole or in part, should be addressed to:

Dean Awang Had Salleh Graduate School
College of Arts And Sciences
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman
Malaysia

# ABSTRACT

Denial of Service (DoS) is a security threat which compromises the confidentiality of information stored in Local Area Networks (LANs) due to unauthorized access by spoofed IP addresses. DoS is harmful to LANs as the flooding of packets may delay other users from accessing the server and in severe cases, the server may need to be shut down, wasting valuable resources, especially in critical real-time services such as in e-commerce and the medical field. The objective of this project is to propose a new DoS detection system to protect organizations from unauthenticated access to important information which may jeopardize the confidentiality, privacy and integrity of information in Local Area Networks. The new DoS detection system monitors the traffic flow of packets and filters the packets based on their IP addresses to determine whether they are genuine requests for network services or DoS attacks.

Results obtained demonstrate that the detection accuracy of the new DoS detection system was in good agreement with the detection accuracy from the network protocol analyzer, Wireshark. For high-rate DoS attacks, the accuracy was 100% whereas for low-rate DoS attacks, the accuracy was 67%.

# ACKNOWLEDGEMENTS

First and foremost, I would like to thank our GOD “Allah”, the most gracious and the most merciful, for having made everything possible by giving me strength, confidence, and courage to accomplish this work.

I wish to express my sincere gratitude to Dr. Angela Amphawan for her guidance and direction in this work. She gave me many interesting, valuable and sincere feedbacks throughout her supervision. I greatly benefited from her detailed comments and insights that helped me clarify ideas in “Detection of Denial of Service Attacks in Local Area Networks based on Outgoing Packets”.

I sincerely thank to my evaluator Dr. Ahmad Suki Che Mohamad Arif, and other committee members, for graciously reviewing this work and giving valuable suggestion and comments on my work.

I would also like to say a big thanks all UUM lecturers and staff members at the School of Computing who were kind enough to give me their precious time and assistance, without which I would not have been able to complete this Masters Project.

I am indebted and thankful to the Chancellor of University Utara Malaysia who referred me to valuable e-recourses at the Sultanah Bahiyah Library.

I wish to thank the Ministry of Higher Education of Iraq for the financial support awarded to me.

Last but not least, extreme thanks are reserved for the last. Words cannot express my gratitude to my family, especially my sympathetic, compassionate and beloved parents, my dear brothers Ahmed, Ali, Hassan, Hussain, Mohammed and Mohmoud, my sister, my faithful wife, and my four daughters, Benin, Khawther, Fatima and Abrar. Words cannot describe their constant love, care, concern, patience, and direction in every aspect of my life throughout the two years of my study abroad. I’m forever thankful, grateful, and indebted to them. May Allah bless them! I dedicate the accomplishment of this project to my beloved father, my affectionate mother, and to the twin of my spirit, my wife.

**Thank you UUM.**

MEHDI EBADY MANAA

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

**Chapter Five:**

# LIST OF APPENDIXES

# LIST OF ABBREVIATION

| | |
|---|---|
| **DoS** | Denial of Service |
| **DDoS** | Distributed Denial of Service |
| **LAN** | Local Area Network |
| **DBMS** | Database Management System |
| **DNS** | Domain Name System |
| **DHCP** | Dynamic Host Configuration Protocol |
| **PoD** | Ping of Death |
| **CBF** | Counting Bloom Filter |
| **TTL** | Time to Live |
| **TP** | True Positive |
| **TN** | True Negative |
| **FP** | False Positive |
| **FN** | False Negative |
| **UML** | Unified Modelling Language |
| **XP** | Extreme Programming |
| **JPcap** | Java Packet Capture |

# CHAPTER ONE

# INTRODUCTION

This chapter briefly provides the research landscape and elaborates the main concepts leading to the conception of a novel detection system for Denial of Service attacks.

Section 1.1 describes the top-bottom research landscape and hierarchical architecture while providing important concepts pertaining to the network architecture and service related to the research undertaken. This is crucial in laying the foundation for understanding the intricacies of the research undertaken and paves the way for elucidating the impetus of the research work involved. This leads to Section 1.2 on the motivation of the research, followed by the problem statement, in Section 1.3, the corresponding research questions in Section 1.4, the objectives of the study in Section 1.5, the scope of the study in Section 1.6 and the significance of the study in Section 1.7. Finally, Section 1.8 provides the organization of the remaining chapters of the report.

## 1. Introduction

Information has become an organization's most precious asset. Organizations have become increasingly dependent on information. The widespread use of e-commerce has increased the necessity of protecting the system to a very high extent (Botha, Von Solms, Perry, Loubser, & Yamoyany, 2002), (P. Kiran Sree, 2008).

Within an organization, information is typically located on servers that are shared by the entire organization or by individual units. Alternatively, information

The contents of the thesis is for internal user only

## References


Abdelsayed, S., Glimsholt, D., Leckie, C., Ryan, S., & Shami, S. (2003). *An efficient filter for denial-of-service bandwidth attacks.* Paper presented at the Global Telecommunications Conference (GLOBECOM), Australia:IEEE.

Aken, J. E. (2004). Management research based on the paradigm of the design sciences: The quest for field tested and grounded technological rules. *Journal of management studies, 41(2),* 219-246.

Ardakan, M. A., & Mohajeri, K. (2009). Applying Design Research Method to IT Performance Management: Forming a New Solution. *Journal of Applied Sciences, 9*(7), 1227-1237.

Beck, K. (2005). *Extreme Programming Explained: Embrace Change*. Boston: Addison-Wesley.

Bellaïche, M., & Gregoire, J. C. (2009). *SYN flooding attack detection based on entropy computing.* Paper presented at the Global Telecommunications Conference (GLOBECOM), Honolulu, HI: IEEE .

BoonPing Lim, M., & Uddin, S. (2005). Statistical-based SYN-flooding detection using programmable network processor. *IEEE, 3 (2 ),* 465 - 470 .

Botha, M., Von Solms, R., Perry, K., Loubser, E., & Yamoyany, G. (2002). The utilization of artificial intelligence in a hybrid intrusion detection system. *ACM*, 149-155.

Cabrera, J. B. D., Popyack Jr, L. J., Lewis, L., Ravichandran, B., & Mehra, R. K. (2001). The monitoring, detection, interpretation and response paradigm for the security of battlespace networks. *IEEE,* 102-106.

Carl, G., Kesidis, G., Brooks, R. R., & Rai, S. (2006). Denial-of-service attack-detection techniques. *Internet Computing, IEEE, 10*(1), 82-89.

Chang, R. K. C. (2002). Defending against flooding-based distributed denial-of-service attacks: A tutorial. *Communications Magazine, IEEE, 40*(10), 42-51.

Chen, C. L. (2008). *Detecting distributed denial-of-service attack traffic by statistical test.* Paper presented at the Third International Conference on Communications and Networking, Hangzhou , China: IEEE.

Cho, Y., Navab, S., & Mangione-Smith, W. (2002). Specialized hardware for deep network packet filtering. *Field-Programmable Logic and Applications: Reconfigurable Computing Is Going Mainstream,* 337-357.

Connolly, T. M., & Begg, C. E. (2003). *Database systems*. Boston : Addison-Wesley.

Coulouris, G., Dollimore, J., & Kindberg, T. (2005). *Distribuited Systems: Concepts and Design*. London & Palo Alto: Addison-Wesley.

Farrow, R. (2000). *Distribuited Denial of Service Attacks - how Amazon, Yahoo , eBay and others were brought down.* Retrieved Sep 25, 2011, from technet.microsoft.com:http://technet.microsoft.com/en-us/library/cc722942.aspx

Génova, G., & Llorens, J. (2005). The emperor's new use case. *Journal of Object Technology, 4*(6), 81-94.

Guilbert, L., & Toner, A. (2010). *Protect your organization's sensitive information and reputation with high-risk data discovery.* Retrieved Sep 1, 2011, from www.pwc.com: http://www.pwc.com/us/en/it-risk-security/assets/high-risk-data-discovery.pdf

Hellerstein, J. M., Stonebraker, M., & Hamilton, J. (2007). Architecture of a database system. *Foundations and Trends in Databases, 1*(2), 141-259.

Huget, M. P. (2002). Extending agent UML protocol diagrams. *Agent Oriented Software Engineering (AOSE-02), Bologna, Italy.*

Ibrahim, L. M. (2010). Anomly Network Intrusion Detection System Based On Distributed Time-Delay Neural Network (DTDNN). *Journal of Engineering Science and Technology, 5(4*), 457-471.

James, C., & Murthy, H. A. (2011). *Time Series Models and its Relevance to Modeling TCP SYN Based DoS Attacks. Next Generation Internet.* India: Indian Institute of Technology Madras.

Kawahara, R., Ishibashi, K., Mori, T., Kamiyama, N., Harada, S., Hasegawa, H., et al. (2007). Detection accuracy of network anomalies using sampled flow statistics. *International Journal of Network Management*, 1959-1964.

Khosrow-Pour, M. (2006). *Emerging trends and challenges in information technology management* . Washington, DC, USA: IGI Global.

Kuechler, B., & Vaishnavi, V. (2008). development in design science research anatomy of a research project. *European Journal of Information Systems, 17(5)*, 489-504.

Kurose, J., & Ross, K. (2005). *Computer networks: A top down approach featuring the Internet*. London: Addison- Wesley.

Lee, W., Stolfo, S. J., & Mok, K. W. (1999). *A data mining framework for building intrusion detection models*. Paper presented at the Symposium on Secuirty and Privacy, Oakland, California, USA: IEEE.

Li, J., Liu, Y., & Gu, L. (2010). DDoS Attack Detection Based On Neural Network. Paper presented at the 2nd International Symposium on Aware Computing (ISAC). Tainan, Taiwan: IEEE.

Lifang Zi, J. Y.-W. (2011). *Adaptive Clustering with Feature Ranking for DDoS Attacks Detection*. Paper presented at the 7th EURO-NGI on Next Generation Internet (NGI),Germany: IEEE.

Limwiwatkul, L., & Rungsawang, A. (2004). *Distributed denial of service detection using TCP/IP header and traffic measurement analysis.* Paper presented at the lntanational Syinposium on Communications and Information Technologes (ISCIT), Japan: IEEE.

Liu, P., Yu, M., & Jing, J. (2005). *Information Assurance*:. John Wiley & Sons.

Manusankar, C., Karthik, S., & Rajendran, T. (2010). *Intrusion Detection System with Packet Filtering for IP Spoofing.* Paper presented at the the International Conference on Communication and Computational Intelligence (INCOCCI), India:IEEE.

Martin, R. C. (2003). *Agile Software Development: Principles, Patterns, and Practices*: New Jersey, USA: Prentice Hall.

Mell, P., Bergeron, T., & Henning, D. (2005). *Creating a patch and vulnerability management program.* USA: National Institute of Standards and Technology (NIST).

Mikko Sarela, C. E., Zahemszky, A., Nikander, P., & Ott, J. (2010). BloomCasting: Security in Bloom filter based multicast. *Aalto University, Espoo, Finland.* Finland: Springer.

Moore, D., Voelker, G. M., & Savage, S. (2001). *Inferring Internet denial-of-service activity*. Paper presented at the in Usenix Security Symposium, Washington, D.C: CAIDA.

Nandivada, V. K., & Palsberg, J. (2005). *Timing analysis of TCP servers for surviving denial-of-service attacks*. Paper presented at the Real-Time and Embedded Technology and Applications Symposium (RTAS), San Francisco, California: IEEE.

Nashat, D., & Jiang, X. (2008). *Detecting syn flooding agents under any type of ip spoofing.* Paper presented at the International Conference on e-Business Engineering (ICEBC), Xi'an, China: IEEE.

Nashat, D., Jiang, X., & Horiguchi, S. (2008). *Router based detection for low-rate agents of DDoS attack.* Paper presented at the International Conference on High Performance Switching and Routing (HSPR): IEEE.

Neda Hantehzadeh, A. M., & Wilathgamuwa, G. (2010). *Statistical analysis of self-similar Session Initiation Protocol (SIP) messages for anomaly detection*. Paper Presented at the Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP) ,Germany: IEEE.

Nyame-Asiamah, F., & Patel, N. (2009). *Research methods and methodologies for studying organisational learning*. Paper presented at the European and Mediterranean Conference on Information Systems (EMCIS), Izmir.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research, 2*(1), 1-28.

P. Kiran Sree, P. K. S. (2008). Exploring a Novel Approach for providing Software Security Using Soft Computing Systems. *International Journal of Security and Its Applications (IJSIA), 2*(2), 51-58.

Palmieri, F., & Fiore, U. (2010). Network anomaly detection through nonlinear analysis. *Computers & Security, 29*(7), 737-755.

Parziale, L., Britt, D. T., Davis, C., Forrester, J., Liu, W., Matthews, C., et al. (2006). *TCP/IP Tutorial and Technical Overview.* U.S.A.: IBM.

Pfleeger, C. P., & Pfleeger, S. L. (2007). *Security in computing*: Prentice Hall, USA.

Rothenberg, C. E., & Petri Jokela, P. N. (2010). *Self-routing Denial-of-Service Resistant Capabilities using In-packet Bloom Filters*. Paper presented at the European Conference on Computer Network Defense (EC2ND), Milano, Italy: IEEE.

Schuba, C. L., Krsul, I. V., Kuhn, M. G., Spafford, E. H., Sundaram, A., & Zamboni, D. (1997). *Analysis of a denial of service attack on TCP.* Paper presented at the Proceedings Symposium on Security and Privacy, Washington, DC, USA: IEEE.

Sengar, H., Wang, H., Wijesekera, D., & Jajodia, S. (2006). *Fast detection of denial-of-service attacks on IP telephony.* Paper presented at the 14th International Workshop on Quality of Service (IWQoS), New Haven, CT, USA : IEEE.

Shaikh, R. A., Iqbal, A. A., & Samad, K. (2005). *Review Over Anomaly Detection Algorithms for Detecting SYN Flooding Attacks.* Paper presented at the Student Conference on Engineering Sciences and Technology(SCONEST), Karachi, Pakistan: IEEE .

Snoeren, A. C. (2001). *Hash-based IP traceback.* Paper presented at the conference on the Special Interest Group on Data Communication (SIGCOMM), San Diego, California, USA: ACM.

Tabataba, F. S., & Hashemi, M. R. (2011). *Improving False Positive In Bloom Filter*. Paper presented at the conference on 19th Iranian Conference on Electrical Engineering (ICEE), Tehran, Iran:IEEE

Tang, H., Xu, C., Luo, X., & OuYang, J. (2009). *Traceback-based Bloomfilter IPS in defending SYN flooding attack.* Paper presented at the 5th International

Conference on Wireless Communications, Networking and Mobile Computing, USA: IEEE.

Tuncer, T., & Tatar, Y. (2008). *Detection SYN Flooding Attacks Using Fuzzy Logic.* Paper Presented at the International Conference on Information Security and Assurance, (ISA), Busan, South Korea: IEEE

Tsai, C.-L., Chang, A. Y., & Ming-Szu, H. (2010). *Early Warning System for DDoS Attacking Based on Multilayer Deployment of Time Delay Neural Network.* Paper Presented at the Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP),Germany: IEEE.

Viana, M. M., & Neuman de Souza, J. (2007). *A complex analysis approach to the modelling for the tracing and identification of Denial-of-Service attackers.* Paper presented at the International Conference on Telecommunications and Malaysia International Conference on Communications, Penang, Malaysia: IEEE.

Wang, H., Zhang, D., & Shin, K. G. (2002). Detecting SYN flooding attacks. *IEEE, 3*(23-27), 1530 - 1539.

Yanchun, M. (2010). System for attack recognition based on mining fuzzy association rules. Paper present at the International Conforence On Computer Design And Appliations (ICCDA). Qinhuangdao, China: IEEE.

Zadeh, L. A. (1965). Fuzzy sets. *Information and control, 8*(3), 338-353.

Zhang, J., Chen, Y., Liu, G., & Li, H. (2009). *Using Sequence Diagram to Support Aspect-Oriented Programming in MDA.* Paper present at the International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC), Hangzhou, Zhejiang , China: IEEE

Zhang, Y., Liu, Q., & Zhao, G. (2010). *A real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis.* Paper presented at the International Conference on Computer Science and Information Technology (ICCSIT), Chengdu, China: IEEE.