



UNIVERSITI PUTRA MALAYSIA

**ENHANCED IP SPOOFING DEFENSE THROUGH CLUSTERED
INTERDOMAIN PACKET FILTERING STRATEGY**

LEE SOON

FSKTM 2011 18

**ENHANCED IP SPOOFING DEFENSE THROUGH
CLUSTERED INTERDOMAIN PACKET
FILTERING STRATEGY**



LEE SOON

**MASTER OF SCIENCE
UNIVERSITI PUTRA MALAYSIA**

2011



© COP YRIGHT UPM

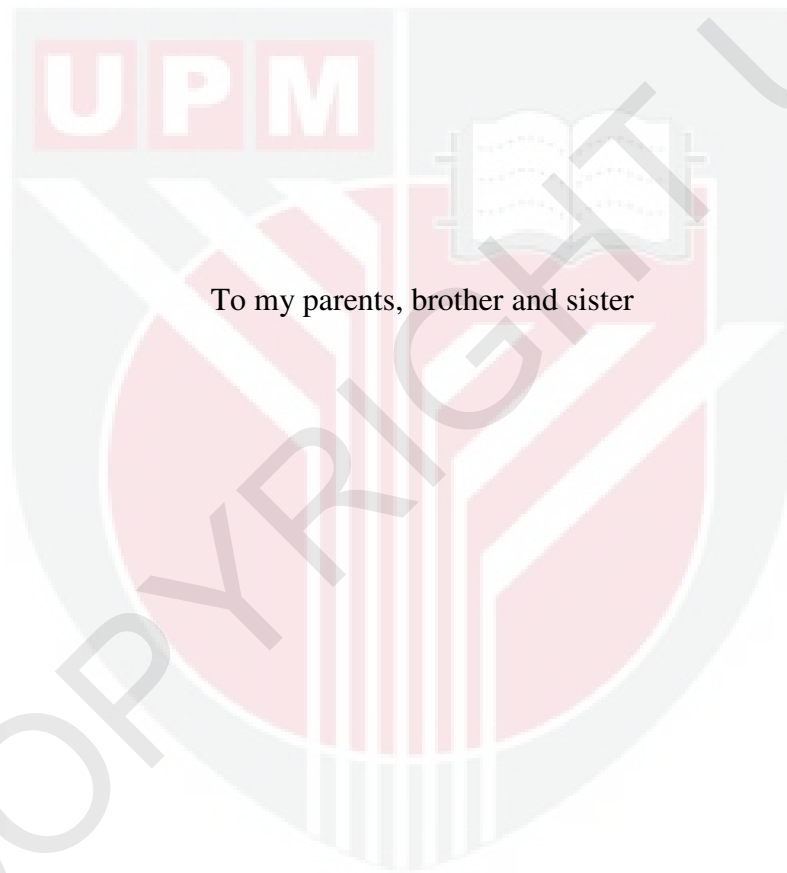
**ENHANCED IP SPOOFING DEFENSE THROUGH CLUSTERED
INTERDOMAIN PACKET FILTERING STRATEGY**



**BY
LEE SOON**

**Thesis Submitted to the School of Graduate Studies, Universiti Putra
Malaysia, in Fulfillment of the Requirements for the Degree of Master of Science**

September 2011



To my parents, brother and sister

© COPYRIGHT UPM

Abstract of thesis presented to the Senate of Universiti Putra Malaysia
in fulfillment of the requirement for the degree of Master of Science

**ENHANCED IP SPOOFING DEFENSE THROUGH CLUSTERED
INTERDOMAIN PACKET FILTERING STRATEGY**

By

LEE SOON

September 2011

Chair : Professor Mohamed Othman, PhD
Faculty : Computer Science and Information Technology

In current Internet communication world, validity of the source of Internet Protocol packet is an important issue. The problems of IP spoofing alarm legitimate users of the Internet. Various spoofing defenses techniques and mechanisms are proposed by researchers, among which, Interdomain Packet Filter (IDPF) architecture proposed by Duan, et al. is promising. Based on the information from Border Gateway Protocol (BGP), IDPF is constructed. Filtering nodes are chosen based on vertex cover of the graph. This thesis presents a clustered strategy for selection of filtering nodes for IDPF architecture. Clusters of filtering nodes are chosen from the Autonomous System with highest number degree. Through analysis and simulation, the effectiveness of IDPF with Clustered Filtering was measured. The work presented here has profound implications for future studies of IP spoofing defense under IDPF.

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

**PENINGKATAN PERTAHANAN PERMALSUAN PROTOKOL INTERNET
MELALUI STRATEGI PENAPISAN PAKET KLASTER ANTARA DOMAIN**

Oleh

LEE SOON

September 2011

Pengerusi : Profesor Mohamed Othman, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Dalam dunia komunikasi Internet saat ini, kesahihan sumber paket Internet merupakan isu penting. Masalah pemalsuan paket Internet telah menggera pengguna sah lain dari Internet. Pelbagai teknik dan mekanisme pertahanan terhadap pemalsuan paket Internet telah diajukan oleh para penyelidik, di antaranya, senibina penapis paket antara domain (IDPF) dicadangkan oleh Duan, dll amat memberangsangkan. IDPF dibina berdasarkan maklumat dari protokol batas pintu gerbang. Nod penapisan dipilih berdasarkan penutup mercu graf. Tesis ini menunjukkan pemilihan nod penapis senibina IDPF berdasarkan strategi berkelompok. Nod kluster penapis dipilih daripada sistem autonomi dengan sambungan nod tertinggi. Melalui analisis dan simulasi, keberkesanan IDPF dengan penapisan berkelompok diukur. Kerja yang disampaikan dalam tesis ini mempunyai implikasi besar untuk kajian masa depan dalam pertahanan pemalsuan paket Internet di bawah IDPF.

ACKNOWLEDGEMENTS

I would like to thank every one that helps me to accomplish my master research in University Putra Malaysia. Firstly I would like to thank Prof. Dr. Mohamed Othman for his patient and advices guiding me throughout this research. I would also like to take this opportunity to convey my highest appreciation to thank my parents for giving me courage and support. I really appreciate all the guidance and advices given by them throughout the research. I would like to thank my friends Tareq Rasul and Nazmin, and all those I've not mentioned. Thank you for all you supports and helping hands.

I certify that an Examination Committee has met on date of viva voce to conduct the final examination of name of student on his (or her) degree thesis entitled "Title of thesis" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the student be awarded the (Name of relevant degree).

Members of the Examination Committee were as follows:

Abdul Azim Abd Ghani, PhD

Professor

Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Name of Examiner 1, PhD

Title (e.g. Professor/Associate Professor/Ir) – omit if irrelevant.
Name of Faculty
Universiti Putra Malaysia
(Internal Examiner)

Name of Examiner 2, PhD

Title (e.g. Professor/Associate Professor/Ir) – omit if irrelevant
Name of Faculty
Universiti Putra Malaysia
(Internal Examiner)

Name of External Examiner, PhD

Title (e.g. Professor/Associate Professor/Ir) – omit if irrelevant
Name of Department and/or Faculty
Name of Organisation (University/Institute)
(External Examiner)

BUJANG KIM HUAT, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of type of degree. The members of the Supervisory Committee were as follows:

Mohamed Othman, PhD

Professor

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Chairman)

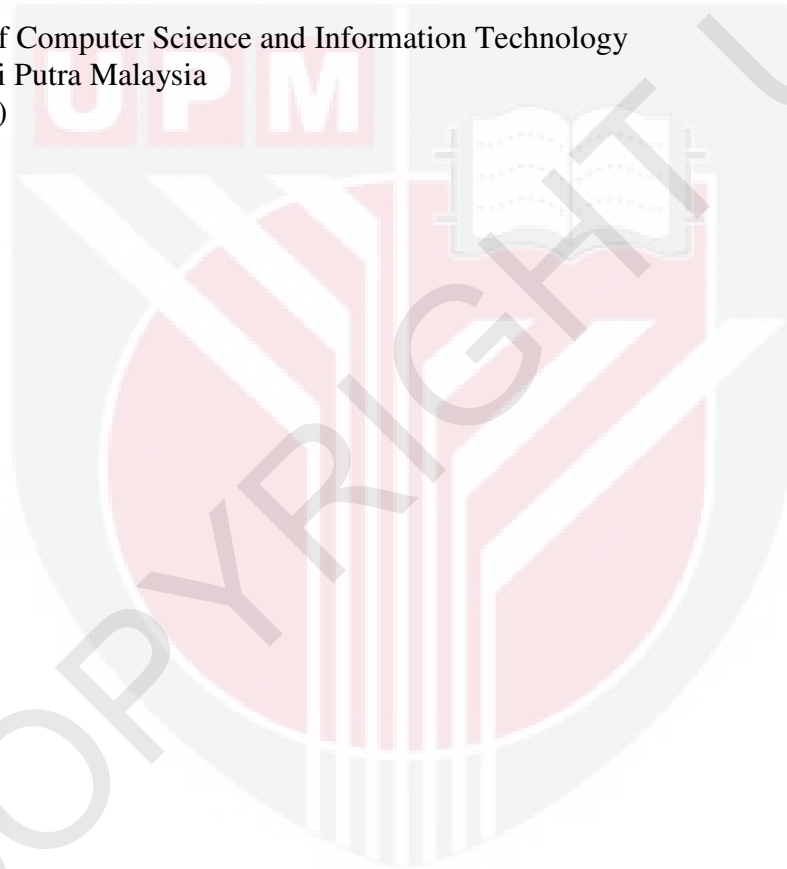
Nur Izura Udzir, PhD

Lecturer

Faculty of Computer Science and Information Technology

Universiti Putra Malaysia

(Member)



BUJANG BIN KIM HUAT, PhD

Professor and Dean

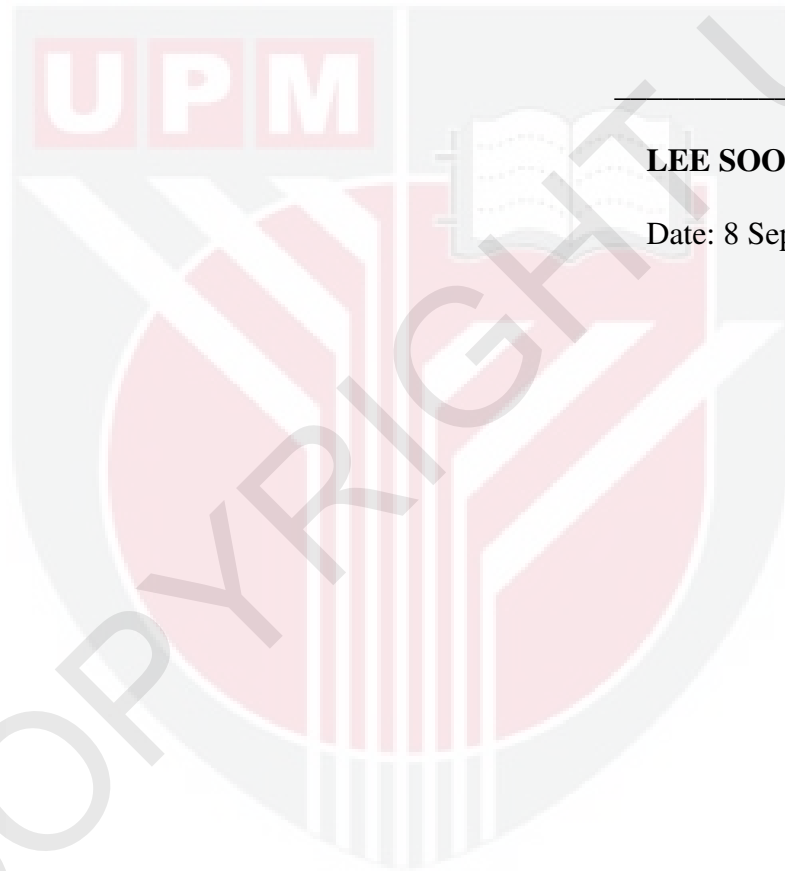
School of Graduate Studies

Universiti Putra Malaysia

Date:

DECLARATION

I declare that the 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 is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.



LEE SOON

Date: 8 September 2011



TABLE OF CONTENTS

	PAGE
ABSTRACT	iii
ABSTRAK	iv
ACKNOWLEDGEMENT	v
APPROVAL	vi
DECLARATION	viii
LIST OF TABLES	xi
LIST OF FIGURES	xii
LIST OF ABBREVIATIONS	xiii
CHAPTERS	
1 INTRODUCTION	1
1.1 Background and Motivation	1
1.2 Problem Statement	2
1.3 Research Objective	3
1.4 Research Scope	3
1.5 Thesis Organization	4
2 LITERATURE REVIEW	6
2.1 Introduction	6
2.2 IP Spoofing Attacks	6
2.2.1 ICMP Ping Flood	6
2.2.2 SYN Flood	7
2.2.3 Man-in-the-middle Attack	8
2.3 Related Works	8
2.3.1 Spoofing Prevention Before Transmission	8
2.3.2 Spoofing Detection During Transmission	8
2.3.3 Spoofing Detection At Destination	16
2.4 Summary	26
3 RESEARCH METHODOLOGY	27
3.1 Introduction	27
3.2 Research Framework	27
3.3 Research Assumptions	28
3.4 System Requirements	31
3.4.1 Hardware	31
3.4.2 Simulation Data Extraction	31
3.4.3 Simulation Tool	32
3.5 IDPF Simulation Environment and Parameters	32
3.6 Simulation Data Sets	33
3.7 Performance Metrics	34
3.8 Performance Simulations	36
3.9 Summary	36

4	INTERDOMAIN PACKET FILTERING	37
4.1	Introduction	37
4.2	Route Based Distributed Packet Filtering	37
4.2.1	DPF Spoofed Packet Detection and Filtering	38
4.2.2	Placement of DPF Filtering Nodes	39
4.3	Inter-domain Packet Filtering	40
4.3.1	BGP Path Selection	40
4.3.2	IDPF Spoofed Packet Detection and Filtering	41
4.3.3	Placement of IDPF Filtering Nodes	42
4.4	Summary	42
5	CLUSTERED FILTERING STRATEGY ON IDPF	43
5.1	Introduction	43
5.2	Vertex Cover Filtering Strategy	44
5.3	Clustered Filtering Strategy	46
5.4	Performance Evaluation	49
5.4.1	Benchmarking result of year 2004 between VC and CF	50
5.4.2	Benchmarking result of year 2005 between VC and CF	55
5.4.3	Benchmarking result of year 2006 between VC and CF	59
5.4.4	Benchmarking result of year 2007 between VC and CF	64
5.4.5	Benchmarking result of year 2008 between VC and CF	68
5.5	Comparison of number of nodes for each cluster	73
6	CONCLUSION AND FUTURE WORK	75
6.1	Conclusion	75
6.2	Future Work	76
	REFERENCES	77
	BIODATA OF STUDENT	81
	LIST OF PUBLICATIONS / AWARDS	82