

Towards Eradication of SPAM: A Study on Intelligent Adaptive SPAM Filters

Tarek Hassan
(B.Sc. Computer Science, Egypt)

This thesis is presented for the degree of Master of Computer Science

Murdoch University, Western Australia

2006

*I declare that this thesis is my own
account of my research and contains as
its main content work, which has not
previously been submitted for a degree at
any tertiary educational institution.*

Tarek Hassan

ABSTRACT

As the massive increase of electronic mail (email) usage continues, SPAM (unsolicited bulk email), has continued to grow because it is a very inexpensive method of advertising. These unwanted emails can cause a serious problem by filling up the email inbox and thereby leaving no space for legitimate emails to pass through. Currently the only defense against SPAM is the use of SPAM filters. A novel SPAM filter GetEmail5 along with the design rationale, is described in this thesis. To test the efficacy of GetEmail5 SPAM filter, an experimental setup was created and a commercial bulk email program was used to send SPAM and non-SPAM emails to test the new SPAM filter.

GetEmail5's efficiency and ability to detect SPAM was compared against two highly ranked commercial SPAM filters on different sets of emails, these included all SPAM, non-SPAM, and mixed emails, also text and HTML emails.

The results showed the superiority of GetEmail5 compared to the two commercial SPAM filters in detecting SPAM emails and reducing the user's involvement in categorizing the incoming emails.

This thesis demonstrates the design rationale for GetEmail5 and also its greater effectiveness in comparison with the commercial SPAM filters tested.

TABLE OF CONTENTS

	Page No.
ABSTRACT	<i>i</i>
TABLE OF CONTENTS	<i>ii</i>
ACKNOWLEDGEMENTS	<i>v</i>
PUBLICATIONS	<i>vi</i>
CHAPTER 1. INTRODUCTION	1
1.1 Introduction	1
1.2 Definition of SPAM	2
1.3 Sources of SPAM	4
1.4 Growth of SPAM in Australia	5
1.5 Nuisance and costs of SPAM	6
1.6 Content of SPAM	6
1.7 Transmission of SPAM emails	7
1.8 Why is SPAM so common?	9
1.9 How to stop SPAM	11
1.10 Amis	12
1.11 Thesis Overview	12
CHAPTER 2. LITERATURE REVIEW	14
2.1 Introduction	14
2.2 Dealing with SPAM	15
2.3 SPAM filters	18
2.3.1 Black List Filter	20
2.3.2 White List Filter	21
2.3.3 Bayesian Filtering (Content Focus)	21
2.3.4 Fingerprints Filter	22
2.3.5 Password Filter	23
2.3.6 Challenge/Response Filter	24
2.3.7 Community-base Filter	24

2.3.8 Mobile Agent	25
2.3.9 Encryption and Trust	26
2.3.10 Copyright Tokens	26
2.4 Legal Action against SPAM	30
2.4.1 Complaining to Spammers' ISPs	31
2.4.2 The use of an Opt-in Mechanism	31
2.4.3 SPAM Litigation	32
CHAPTER 3. DESIGN OF GETEMAIL5 SPAM FILTER	36
3.1 Introduction	36
3.2 History of Bayesian Probability	37
3.3 How a Bayesian Filter Works?	39
3.4 Advantages of the Bayesian Filtering	41
3.5 Design of the Proposed Filter	42
3.5.1 Whitelist Filter	46
3.5.2 Blacklist Filter	46
3.5.3 Bayesian Filter Subject to HAM or SPAM	47
3.6 Implementation of the GetEmail5 SPAM Filter	48
3.7 Operation of the GetEmail5 Filter	52
CHAPTER 4. RESEARCH METHODOLOGY	56
4.1 Introduction	56
4.2 Preparing the Filter Requirements	56
4.2.1 Creation of a new Email Account	56
4.2.2 Obtaining a Bulk Email Sender	58
4.2.3 Collecting SPAM Emails (Data set)	58
4.3 Sending SPAM Emails	59
4.4 Receive and Analyse the Emails	63
4.5 Evaluation	63
4.5.1 First Experiment (Mixed Emails)	67
4.5.2 Second Experiment (80% SPAM and 20% non-SPAM Emails)	67

4.5.3 Third Experiment (100% Plain Text SPAM Emails)	68
4.5.4 Fourth Experiment (100% HTML SPAM Emails)	68
CHAPTER 5. RESULTS AND DISCUSSION	69
5.1 Introduction	69
5.2 Initial Evaluation of the GetEmail5 SPAM Filter	69
5.3 First Experiment	71
5.4 Second Experiment (80% SPAM and 20% non-SPAM Emails)	75
5.5 Third Experiment (100% Plain Text SPAM Emails)	79
5.6 Fourth Experiment (100% HTML SPAM Emails)	82
5.7 Analysis of the five Key Performance Indicators (KPI)	85
5.7.1 SPAM Detection	85
5.7.2 Filtering Time	86
5.7.3 False Positive	87
5.7.4 False Negative	88
5.7.5 User Involvement	89
5.8 Limitations of this Research	91
CHAPTER 6. CONCLUSIONS AND FURTHER WORK	93
6.1 Conclusions	93
6.2 Recommendations for Further Work	94
REFERENCES	95
APPENDIX	GETEMAIL5 DOCUMENTATION

ACKNOWLEDGEMENTS

The work presented in this thesis was carried out under the supervision of Mr. Peter Cole and Associate Professor Lance C.C. Fung, to whom I extend my gratitude for their valuable and friendly guidance, encouragement and helpful suggestions throughout the progress of the research and in the preparation of this thesis.

I would like to extend my special thanks and indebtedness to Kashif Saleem for his help and support.

My gratitude and heartfelt thanks to Dr. Karin Strehlow and Anthony Horton, for their support, friendship, help and encouragement, God Bless.

Finally, my thanks and gratitude go to my wife, Eman and daughter, Amira who have been understanding, patient, supportive and making *duaa(supplication)* for the success of my study. Thank you also to my parents, sisters and brother for their encouragement and support during my stay in Australia.

PUBLICATIONS

Hassan, T., Cole, P. and Fung C.C. (2006), “An Intelligent SPAM filter – GetEmail5”, Proceedings of the 2nd IEEE International Conference on Cybernetics and Intelligent Systems (CIS 2006), Bangkok Thailand, 7-9 June, 2006, (ISBN 1-4244-0023-6) pp. 86-90.

Hassan T., Cole P. and Fung C.C. (2005), “Development and evaluation of an Intelligent SPAM filter”, Proceedings of the 6th Postgraduate Electrical and Computing Symposium (PEECS 2005), (ISBN 0-7298-06090-X), Edith Cowan University, Perth, WA, pp. 142-145

Hassan T., Cole P., and Fung C.C., (2004) “Towards Eradication of Spam: A Study on Intelligent Adaptive Spam Filter”, Proceedings of the Fifth Postgraduate Electrical Engineering and Computing Symposium (PEECS 2004), 28th September 2004, Perth, Western Australia, pp 203-206.