

RISK CONCENTRATION FOR CONTEXT ASSESSMENT
(RiCCA) OF SMS MESSAGES USING DANGER THEORY

Kamahazira binti Zainal

Thesis submitted in partial fulfilment for the degree of
DOCTOR OF PHILOSOPHY
SCIENCE AND TECHNOLOGY

UNIVERSITI SAINS ISLAM MALAYSIA
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

August 2018

BIODATA OF AUTHOR

Kamahazira Zainal (4120261) was born on 29th March 1978. She previously was a student at Universiti Putra Malaysia (UPM) and obtained Bachelor of Engineering (Computer and Communication) in 2000. Then, she obtained her Master in Information Security from Universiti Teknologi Malaysia (UTM) in 2008. At this moment she is pursuing her Ph.D. from Universiti Sains Islam Malaysia (USIM), also specifically in information security and assurance.



ACKNOWLEDGEMENTS

وَاللَّهُ الرَّحْمَنُ الرَّحِيمُ

Praise to Almighty Allah SWT for blessing me with good health, strength and determinations. The completion of this journey has not been possible without His will.

My greatest appreciation goes to my parents, especially my mom who always pray the best and keep the good thoughts. I also would like to express my deepest gratitude to my supervisor, Associate Professor Dr Mohd Zalisham bin Jali for his valuable guidance, trust, motivation and comments. The same wish goes to my co-supervisor, Ir. Dr Abu Bakar bin Hasan for his support and interest of my research. Without their continuous support, this thesis would not have been the same as presented here.

While working on this thesis, my research was supported by the Ministry of Higher Education of Malaysia and Research Management Centre of USIM under grant number USIM/FRGS/FST/32/50315. Thank you very much for the generous financial support.

To my beloved siblings and 'true' friends, thank you for your persistent support and understanding. I am very grateful to have all of you by my side especially during my difficulties and hard, tough time. To my teachers, this journey has begun because of you. For my darling nieces, Double MH (Marissa Humaira and Mardhiya El-Hannah binti Shahrul Azmizi), this wonderful journey is treasured cheerfully and accompanied with you two.

و ما أوفيقى إلى بالله

And my success is from Allah.

ABSTRAK

Susulan daripada perkembangan teknologi telefon mudah alih dan Internet, *spam* merupakan satu isu serius yang telah timbul dengan banyak sekali. Rekod kerugian yang tidak pernah berakhir disebabkan oleh *spam* ini telah menggerakkan kajian ini. Kajian ini bertujuan untuk menjadi sebahagian pelengkap kepada penyelesaian sedia ada dan membantu pengguna mengenal pasti mesej *spam* yang berpotensi berbahaya. Tumpuan kajian ini adalah mesej *spam* berbahasa Inggeris dalam format teks Perkhidmatan Pesanan Ringkas atau SMS yang kebiasaannya tanpa disedari mengandungi unsur penipuan. Dengan kandungan SMS yang begitu meyakinkan dan keadaan para pengguna yang mudah tertipu dan tidak berwaspada merupakan salah satu faktor yang menyumbang kepada pelbagai kes berbentuk penipuan dan kecurian identiti. Kajian ini telah mengaplikasikan salah satu daripada teori *Artificial Immune Systems* (AIS), iaitu *Danger Theory*. Peranan *dendritic cells* yang berupaya untuk mengesan risiko kerosakan yang disebabkan oleh bahan berbahaya dalam tubuh manusia telah menjadi idea bagi teori ini. *Danger Theory* ini digunakan bagi menafsirkan kandungan mesej *spam* untuk mengesan sebarang kemungkinan risiko yang disebabkan oleh kandungan *spam* dengan mengilustrasikan elemen biologi dari teori ini di dalam konteks isu *spam*. Kombinasi teori biologi ini dengan teknik lain seperti penilaian risiko dan perlombongan teks telah menghasilkan model, *Risk Concentration for Context Assessment* atau RiCCA. RiCCA ini dibangunkan daripada algoritma *Danger Theory* iaitu *Dendritic Cell Algorithm* (DCA) dan *Deterministic Dendritic Cell Algorithm* (dDCA). Melalui beberapa siri ujian dengan menggunakan gabungan set data daripada *UCI Machine Learning* dan mesej *spam* yang dikumpulkan sendiri, telah menunjukkan RiCCA sebagai alat yang boleh mengukur tahap risiko *spam*. Kedua-dua algoritma ini berjaya menunjukkan bahawa *Danger Theory* mampu diaplikasikan dalam pengukuran risiko dengan kadar ketepatan adalah 90% dengan prestasi dDCA adalah lebih baik daripada DCA, kadar ketepatan 94.16%. Prototaip yang dibangunkan dapat dipertingkatkan lagi sebagai salah satu aplikasi mudah alih. Di samping itu, kajian ini boleh dilaksanakan dengan lebih lanjut untuk saiz mesej yang lebih besar (selain daripada SMS yang hanya terhad kepada 160 aksara) dan juga turut boleh diuji dalam bahasa selain daripada bahasa Inggeris.

ABSTRACT

Unified with the booming of mobile and Internet technology, spam is one of the serious issues that have been emerged tremendously. The never ending records of loss that caused by spam have initiated and motivated this study. With the purpose to produce a complementary solution for the current safeguards, this study aims to assist users in identifying potential harmful messages. The focus of the study is deploying an English text spam in Short Messages Services (SMS) format that usually consists of fraud intention in disguise. Due to the convincing but deceptive contents, users easily get enticed and their lack of awareness about implicit spam's impact loss is one of the most vulnerable factors that lead to numerous cases of fraud, scam and identity theft. This study applied one of the prominent theories from Artificial Immune Systems (AIS), Danger Theory. The behaviour of dendritic cells to sniff danger that caused by a harmful substance in the human body has become the fundamental idea of this theory. Danger Theory is employed in deciphering the risky content of spam message via mapping its' biological properties in spam environment. Consolidation of this theory with other procedures such as risk assessment and text mining has produced a model namely as Risk Concentration for Context Assessment or RiCCA. This RiCCA prototype is developed from Danger Theory algorithms that is Dendritic Cell Algorithm (DCA) and Deterministic Dendritic Cell Algorithm (dDCA). Through a series of simulation with the deployment of merged dataset from UCI Machine Learning and self-collected spam messages, has indicated RiCCA as a reliable medium for measuring the risk concentration. Both algorithms demonstrated that Danger Theory is feasible in measuring risk of SMS content with more than 90% of accuracy rate, which dDCA outperformed DCA with distinctive result of 94.16% accuracy rate. For future work, the prototype can be further enhanced as one of the mobile application. Moreover, this study can be further applied for a larger size of message context (instead of SMS that is limited to 160 characters) and also tested in other languages.

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

المخلص AL-MULAKHKHAS

بعد تطوير تكنولوجيا الهاتف المحمول والإنترنت ، تعتبر الرسائل الاقترامية مشكلة خطيرة نشأت إلى حد كبير إن السجل غير المنته من الخسارة بسبب الرسائل الاقترامية قد نقل هذه الدراسة. تهدف الدراسة إلى أن تكون جزءًا مكملًا للحلول الحالية وتساعد المستخدمين على تحديد رسائل البريد العشوائي الخطيرة. التركيز على هذه الدراسة هو رسالة بريد إلكتروني غير مرغوبة باللغة الإنجليزية في تنسيق النص لخدمة الرسائل القصيرة أو وحالة SMS الرسائل النصية القصيرة التي عادة ما تحتوي على عناصر من الاحتيال. مع ما يسمى محتوى المستخدمين الساذجين والمخفضين هي واحدة من العوامل التي تسهم في مختلف حالات العث وسرقة الهوية نظرية الخطر. لقد أصبح دور الخلايا ، (AIS) طبقت هذه الدراسة واحدة من نظريات نظم المناعة الاصطناعية. التغصنية القادرة على اكتشاف خطر الأضرار الناجمة عن المواد الضارة في جسم الإنسان فكرة لهذه النظرية يتم استخدام نظرية الخطر هذه لتفسير محتويات رسائل البريد العشوائي للكشف عن أي خطر محتمل ناجم عن محتوى البريد العشوائي من خلال توضيح العناصر البيولوجية لهذه النظرية في سياق قضايا البريد العشوائي ، هذا المزيج من النظريات البيولوجية مع تقنيات أخرى مثل تقييم المخاطر وتعدين النص قد أسفر عن نموذج من خوارزمية نظرية الخطر وهي خوارزمية RiCCA تم تطوير هذا RiCCA تركيز المخاطر لتقييم السياق أو من خلال سلسلة من الاختبارات. (dDCA) وخوارزمية الخلية الشجرية الديترتيكية (DCA) الخلية التغصنية ورسائل الرسائل غير المرغوب UCI Machine Learning باستخدام مجموعة من مجموعات البيانات من كأداة يمكن أن تقيس مستوى مخاطر الرسائل غير المرغوب فيها RiCCA فيها المجموعة نفسها ، فقد أظهرت وقد أظهرت كلتا الخوارزميتين أنه يمكن تطبيق نظرية الخطر في قياس المخاطر مع دقة معدل 90% مع أداء ومعدل دقة 94.16%. يمكن زيادة تحسين النماذج الأولية كواحد من تطبيقات ، DCA أفضل من dDCA الجوال. بالإضافة إلى ذلك ، يمكن تنفيذ هذه الدراسة بشكل أكبر لأحجام الرسائل الكبيرة (إلى جانب الرسائل النصية القصيرة التي لا تتعدى 160 حرفًا) ويمكن اختبارها بلغات أخرى غير الإنجليزية.

TABLE OF CONTENTS

AUTHOR DECLARATION AND COPYRIGHT	ii
BIODATA OF AUTHOR	iii
ACKNOWLEDGEMENTS	iv
ABSTRAK	v
ABSTRACT	vi
<i>AL-MULAKHKHAS</i>	vii
TABLE OF CONTENTS	viii
LIST OF TABLES	xiii
LIST OF FIGURES	xvi
LIST OF ALGORITHMS	xix
LIST OF APPENDICES	xx
LIST OF PUBLICATIONS	xxi
GLOSSARY	xxii
LIST OF ABBREVIATIONS	xxv
CHAPTER 1: INTRODUCTION	1
1.1 Motivation Of The Research	1
1.2 Problem Statement	4
1.3 Research Questions	6
1.4 Research Objectives	6
1.5 Scope Of Research Works	7
1.6 Framework Of Research Methodology	7
1.7 Thesis Outline	11
CHAPTER 2: LITERATURE REVIEW	12
2.1 Introduction	12
2.2 The Issue Of Spam	13
2.2.1 Spam History	13
2.2.2 Spam Characteristics And Its Adverse Effects	14
2.2.3 Why Focus On SMS Spam	19
2.3 Human Perception And Behaviour Towards Online Threat	21
2.3.1 The Necessity Of Users' Assistance	24
2.4 Mechanism Of Controlling Spam And Its Impact - Policy, Technical And Industry Approaches	25
2.4.1 Organizations – Governments And Private Sectors	25

2.4.2 Individuals – Users, Consumers, And Researchers	28
2.5 Danger Theory	32
2.5.1 Abstraction View Of Danger Theory	33
2.5.2 DCA As An Information Data Fusion, Signal Processing, And Correlation Algorithm	37
2.5.3 Characteristic Of Danger Theory Applied In Computational Intelligence	40
2.5.4 The Conceptual Framework Or <i>In Silico</i> Processes For Danger Theory Application In The Field Of Computational Intelligence	44
2.6 Danger Theory Variants	49
2.7 Spam Treated As A Threat With Risk	52
2.7.1 Risk Management	53
2.7.2. Risk Level Matrix	55
2.7.3 Description Of Risk Level	56
2.8 Text Mining	57
2.8.1 Pre-processing Of Text	57
2.8.2 Effects Of Pre-processing	58
2.8.3 Statistical Analysis For Weight Derivation	59
2.8.4 Term Weighting Schemes In Spam Classification And Risk Assessment	60
2.9 Dataset	61
2.9.1 Type Of Dataset Sources	63
2.9.2 Available SMS Dataset	64
2.10 Summary	65

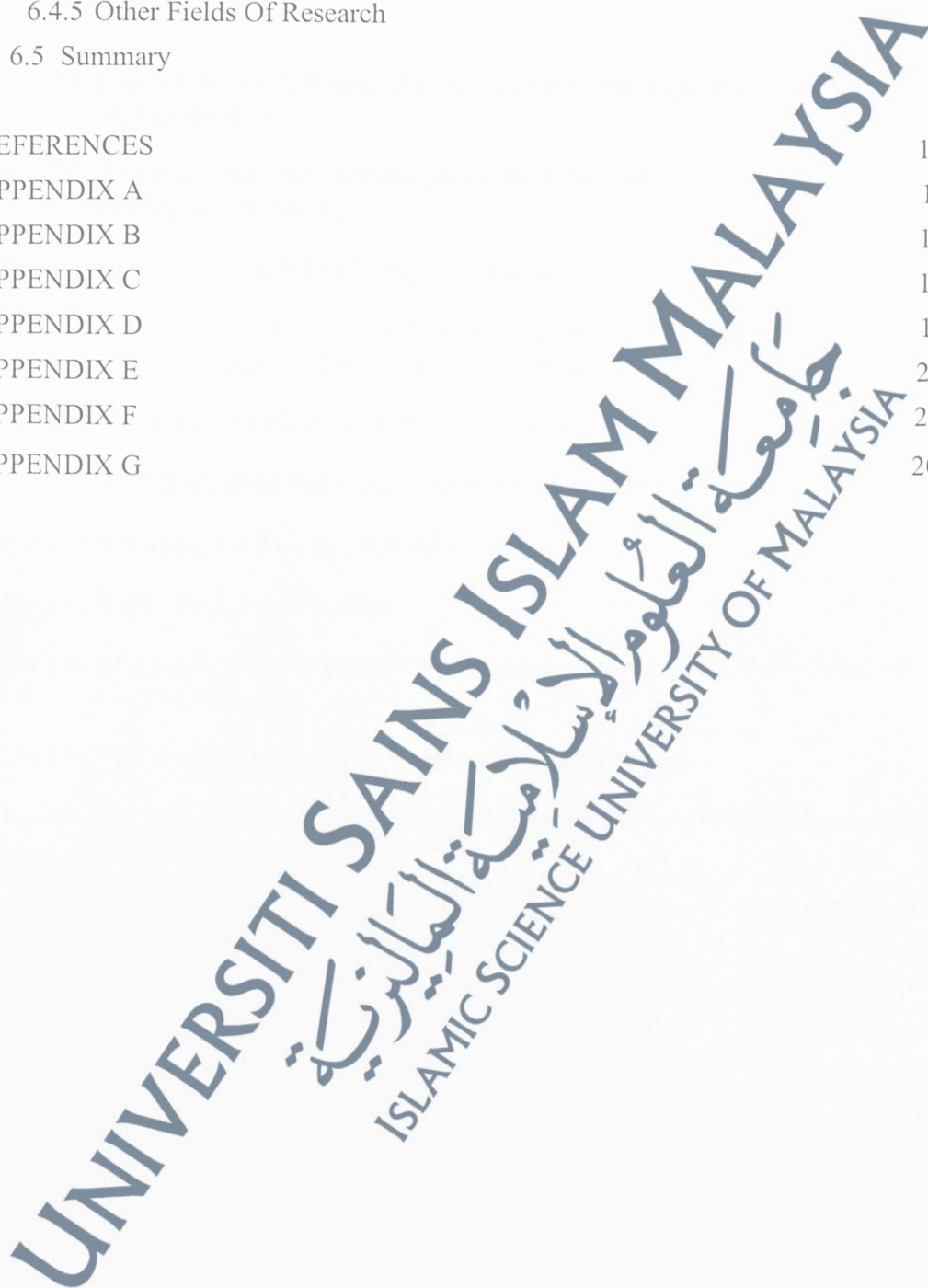
CHAPTER 3: RISK CONCENTRATION FOR CONTEXT ASSESSMENT (RiCCA)

	66
3.1 Introduction	66
3.2 Immunology-based System's Design And Development: The Life Cycle	69
3.3 Algorithms In Spam Management	72
3.4 Treating Spam As Part Of Risk Management	76
3.5 Mapping Biological Facets Of Danger Theory And Spam Management	78
3.5.1 Theoretical Versus Conceptual Consideration Of The Proposed Model, RiCCA	81
3.6 Potential Influence Factors For Spam Classification	87
3.6.1 Dataset Of SMS Spam	88
3.6.2 Data Pre-processing	90
3.6.3 Signals And Antigen: Identification Of The Reliable Term Weighting Schemes With Various Range Of Risk Value And Weights For Signal Transformation	93

3.6.3.1	Input Signals Calculation With Term Weighting Schemes	93
3.6.3.2	Weight For Input And Output Signals	96
3.6.3.2.1	Risk Scale Value Range, S	96
3.6.3.2.2	Weights For Signal Transformation, WM	97
3.6.3.2.3	Anomaly Threshold, t_m And T_k	98
3.7	The Classifier: Empirical Differences Between DCA And dDCA	98
3.7.1	Dendritic Cell Algorithm (DCA) And Deterministic Dendritic Cell Algorithm (dDCA)	98
3.7.2	Antigen Multiplication	99
3.8	Experimental Setup For Testing The DCA And dDCA	100
3.9	Results And Findings Of Initial Simulation	101
3.10	Summary	107
CHAPTER 4: THE DESIGN AND DEVELOPMENT OF THE PROTOTYPE		110
4.1	Introduction	110
4.2	The Design And Development Of The RiCCA Prototype	112
4.2.1	General Process	119
4.2.1.1	Diagram And Process Flow	119
4.2.1.2	Algorithm	120
4.2.2	Pre-processing Of The Corpus/Message	121
4.2.2.1	Diagram And Process Flow	121
4.2.2.2	Algorithm	122
4.2.3	Term Weighting Schemes As Feature Selection Methods	123
4.2.3.1	Diagram And Process Flow	123
4.2.3.2	Algorithm	124
4.2.4	Dendritic Cell Algorithm (DCA) Process	125
4.2.4.1	Diagram And Process Flow	125
4.2.4.2	Algorithm	128
4.2.5	Deterministic Dendritic Cell Algorithm (dDCA) Process	129
4.2.5.1	Diagram And Process Flow	129
4.2.5.2	Algorithm	132
4.3	Summary	132
CHAPTER 5: THE IMPLEMENTATION, RESULT AND ANALYSIS		133
5.1	Introduction	133
5.2	Experimental Setup: Validating The Algorithm Via RiCCA	133
5.2.1	Dataset Deployment	134

5.3 Series Of Experiments	136
5.3.1 Experiment 1 – Influential Parameters With Effective Values	136
5.3.2 Experiment 2 – DCA Versus dDCA	139
5.3.3 Experiment 3 – Various Proportions Of Initial Population	139
5.3.4 Experiment 4 – Antigen Multiplication	140
5.3.5 Experiment 5 – Non-immune Classifiers	141
5.4 Performance Measurement	141
5.4.1 End-Users’ Judgment As Baseline Comparison	143
5.5 Results And Analysis	146
5.5.1 Experiment 1– Influential Parameters With Effective Values	146
5.5.1.1 TF With Pre-processing	146
5.5.1.2 TF Without Pre-processing	148
5.5.1.3 IG Ratio And CHI^2 With Pre-processing	150
5.5.2 Experiment 2 – DCA Versus dDCA	154
5.5.3 Experiment 3 – Various Proportions Of Initial Population	159
5.5.4 Experiment 4 – Antigen Multiplication	162
5.5.5 Experiment 5 – Non-immune Classifiers	164
5.6 Discussion	165
5.6.1 Text Mining	165
5.6.1.1 Term Weighting Schemes	165
5.6.1.2 Pre-processing	165
5.6.1.3 Dictionary List For Stop Word And Root Word	166
5.6.2 Weight Sensitivity	166
5.6.3 DCA Versus dDCA	166
5.6.4 Non-immune Classifiers	168
5.7 Summary	170
CHAPTER 6: CONCLUSIONS	171
6.1 Introduction	171
6.2 Contribution	171
6.2.1 Application Of Danger Theory In Risk Measurement	173
6.2.2 Significant Role Of Text Mining	174
6.2.3 Full Cycle Of Spam Management	174
6.2.4 Implicit Risk Reader For Users	175
6.3 Limitations	175
6.4 Future Research	175

6.4.1 Automate As Mobile Application	175
6.4.2 Extended Scope Of Spam For Testing	176
6.4.3 Enhancing The Data Availability	176
6.4.4 Comparative Analysis With Other Technique	177
6.4.5 Other Fields Of Research	177
6.5 Summary	177
REFERENCES	178
APPENDIX A	192
APPENDIX B	193
APPENDIX C	194
APPENDIX D	195
APPENDIX E	203
APPENDIX F	204
APPENDIX G	205

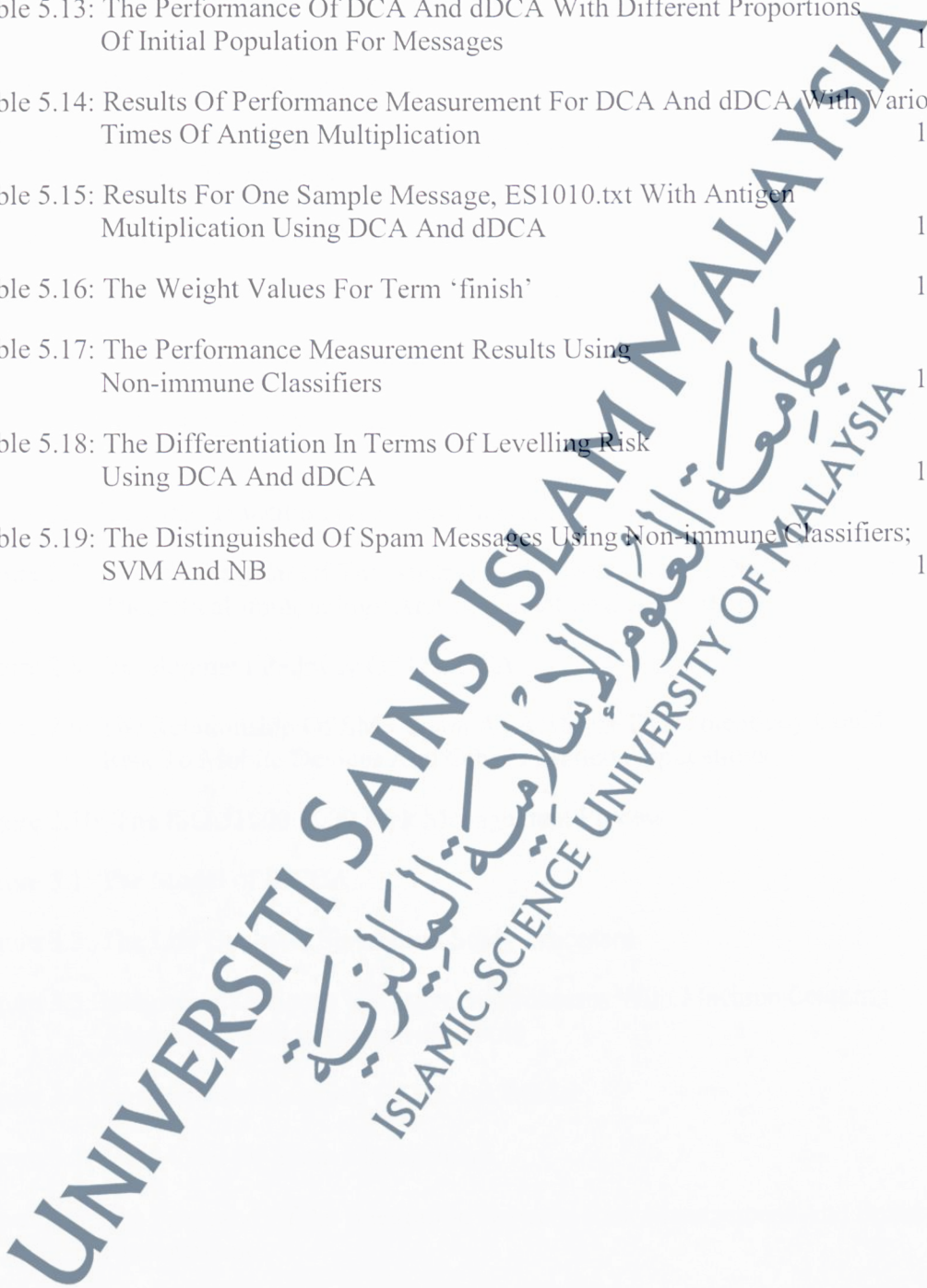


LIST OF TABLES

Tables	Page
Table 1.1: Interrelationship Between Research Questions, Objectives, And Outcomes	10
Table 2.1: Related Works In Spam Filtering For Previous Applied Feature Extractions And Classifiers	29
Table 2.2: The Derivation And Interrelationship Of Weights In The Signal Processing	36
Table 2.3: Application Of DT In Computational Intelligence	42
Table 2.4: The Properties Of Danger Theory Applied In Text Messages Spam Filtering For Email and SMS Format	47
Table 2.5: Theoretical Differences Between DCA And TLR	49
Table 2.6: The Theoretical Differences Between DCA And dDCA	51
Table 2.7: A Sample Of Risk Level Matrix	56
Table 2.8: Term Weighting Schemes	61
Table 3.1: The Application Of Simulation Study Processes In RiCCA Designation And Development	71
Table 3.2: Description Of Phases In Spam Management Model	78
Table 3.3: The Conceptual Mapping Between Immune System Model, Danger Theory And SMS Spam	79
Table 3.4: The Integration Of Danger Theory, Risk Assessment And Text Mining In The Mechanism Of RiCCA Model	86
Table 3.5: Origin Sources For SMS Spam Collection V.1	88
Table 3.6: Statistics Of Instances In SMS Spam Collection V.1	89
Table 3.7: The Dataset Used For Initialization And Testing Phase	89
Table 3.8: Part Of Speech	91
Table 3.9: The Wordlist Created Using RapidMiner	91
Table 3.10: The Top 10 Spam Terms, With The Pre-processing	94
Table 3.11: The Top 10 Spam Terms, Without The Pre-processing	95
Table 3.12: Two (2) Different Ranges Of Risk Scale	97

Table 3.13: Two (2) Different Matrices For Transforming Weights	97
Table 3.14: Four (4) Series Of Simulated Experiments	100
Table 3.15: TP Rate For Matured Cell Consists Of High And Medium Tokens	101
Table 3.16: TP Rate For Matured Cell Consists Of High Tokens	102
Table 3.17: Comparison Of TP Rate Between DCA And dDCA	103
Table 3.18: Comparison Of TP Rate Between DCA And dDCA With Antigen Multiplication Of 10, 40 And 100 Times	105
Table 3.19: Outcome Of Risk Concentration Calculation Using DCA And dDCA	106
Table 4.1: Risk Assessment In Text Spam Messages	115
Table 4.2: The Relationship Portrayed For Integration Of DCA Algorithm In RiCCA Model	117
Table 4.3: Proposed Scale Of Risk Level Value, In Between 0 To 1	126
Table 4.4: Proposed Weight Matrix For Signal Correlation Value	127
Table 4.5: Proposed Scale Of Risk Level Value, In Between 0 To 1	130
Table 5.1: Series Of Experiments	134
Table 5.2: Source Of Dataset	134
Table 5.3: Three (3) Different Ranges Of Risk Scale	137
Table 5.4: Three (3) Different Transforming Weights	138
Table 5.5: The Proportion Of Spam And Ham Messages For Initial Population Sampling	139
Table 5.6: The Number Of Messages Deployed To Construct The Initial Population Database Library According To Times Of Antigen Multiplication	140
Table 5.7: Confusion Matrix	142
Table 5.8: The Performance Measurement Results Using DCA With TF And Pre-processing	147
Table 5.9: The Performance Measurement Results Using DCA With TF And Without Pre-processing	149
Table 5.10: The Performance Measurement Results Using DCA With IG Ratio And With Pre-processing	151

Table 5.11: The Performance Measurement Results Using DCA With CHI^2 And With Pre-processing	153
Table 5.12: The Performance Measurement Results Using dDCA With All Term Weighting Schemes	155
Table 5.13: The Performance Of DCA And dDCA With Different Proportions Of Initial Population For Messages	160
Table 5.14: Results Of Performance Measurement For DCA And dDCA With Various Times Of Antigen Multiplication	162
Table 5.15: Results For One Sample Message, ES1010.txt With Antigen Multiplication Using DCA And dDCA	163
Table 5.16: The Weight Values For Term 'finish'	163
Table 5.17: The Performance Measurement Results Using Non-immune Classifiers	164
Table 5.18: The Differentiation In Terms Of Levelling Risk Using DCA And dDCA	167
Table 5.19: The Distinguished Of Spam Messages Using Non-immune Classifiers; SVM And NB	169



LIST OF FIGURES

Figures	Page
Figure 1.1: The Geography Of Mobile Threats By A Number Of Attacked Users In 2016	2
Figure 1.2: Methodological Framework	9
Figure 2.1: The Integration Of Mobile (Smartphone) And Internet Technology	18
Figure 2.2: Sample Of An Alert Notifications From Bank's Website	28
Figure 2.3: Simplification Of SMS Spam Filtering Methodology	31
Figure 2.4: The Transformation Of Immature DCs	35
Figure 2.5: The Transforming Weight From Input To Output Signals Applied In DCA	36
Figure 2.6: DC State Transition Overview Diagram	38
Figure 2.7: A Flow Diagram Of The Abstraction Process Used In Designation Of Theoretical Immunology And Computational Algorithms	45
Figure 2.8: Development Pathway Of The DCA	50
Figure 2.9: The Relationship Of SMS Spam As A Threat That Potentially Could Bring Risk To Mobile Devices And Other Installed Applications	53
Figure 2.10: The ISO 31000:2009 Risk Management Process	55
Figure 3.1: The Model of RiCCA	68
Figure 3.2: The Life Cycle Of Simulation Study Processes	70
Figure 3.3: Integration Of Spam Management Processes With Machine Learning Algorithms And Experimental Tools	74
Figure 3.4: Unsupervised Learning Of RiCCA Model	75
Figure 3.5: The Model Of Spam Management	76
Figure 3.6: The Proposed Of An Integration Between Risk Management And Spam Management	77
Figure 3.7: Mapping Of The Danger Theory With The Proposed Model Of RiCCA	80

Figure 3.8: Theoretical Understanding In Contrast With The Conceptual Consideration	81
Figure 3.9: The Transformation Between Signals In Dendritic Cells (DCs)	82
Figure 3.10: Induction Of An Immune Response	85
Figure 3.11: The Scatter Plot For Top 10 Spam Terms, With The Pre-processing	95
Figure 3.12: The Scatter Plot For Top 10 Spam Terms, Without The Pre-processing	96
Figure 3.13: The Process Flow Of Simulated Experiment	100
Figure 3.14: TP Rate With Different Weighting Schemes, Multiple Values For Risk Scale And Transforming Weights. These Figures (a) And (b) Corresponds To Table 3.15	102
Figure 3.15: TP Rate With Different Weighting Schemes, Multiple Values For Risk Scale And Transforming Weights. These Figures (a) And (b) Corresponds To Table 3.16	103
Figure 3.16: The TP Rate Value For DCA And dDCA With SF And WM1. These Figures (a) And (b) Corresponds To Table 3.17	104
Figure 3.17: The Taxonomy Of Research Direction	109
Figure 4.1: The Connection Of Biological Studies With RiCCA	110
Figure 4.2: A Concept Mapping Between Biological (Theoretical) And The Developed Model	111
Figure 4.3: Processes Of Design And Development Of A Prototype	113
Figure 4.4: An Overview Of RiCCA Model	114
Figure 4.5: An Overview Diagram For The Entire Process Of RiCCA	118
Figure 4.6: Diagram And Flow For General Process	119
Figure 4.7: Diagram And Flow For Pre-processing Phase	121
Figure 4.8: Diagram And Flow For Term Frequency, TF Process	123
Figure 4.9: Diagram And Flow For DCA Classifier Process	125
Figure 4.10: Diagram And Flow For dDCA Classifier Process	129
Figure 5.1: The Screenshot Of SMS Backup & Restore Mobile Application	135

Figure 5.2: The Process Flow Of Simulated Experiment Using RiCCA	136
Figure 5.3: The Screenshot Of IG Ratio Process Using RapidMiner	137
Figure 5.4: The Screenshot Of Spam Detection Process For SVM And NB Using RapidMiner	141
Figure 5.5: The Demographic Details For Participants	145
Figure 5.6: Various Anomaly Thresholds, t_m Tested For DCA Using TF, With Pre-processing	147
Figure 5.7: Various Anomaly Thresholds, t_m Tested For DCA Using TF, Without Pre-processing	149
Figure 5.8: Various Anomaly Thresholds, t_m Tested For DCA Using IG Ratio, With Pre-processing	151
Figure 5.9: Various Anomaly Thresholds, t_m Tested For DCA Using CHI^2 , With Pre-processing	153
Figure 5.10: Various Anomaly Thresholds, T_k Tested For dDCA Using TF, With Pre-processing	156
Figure 5.11: Various Anomaly Thresholds, T_k Tested For dDCA Using IG Ratio, With Pre-processing	157
Figure 5.12: Various Anomaly Thresholds, T_k Tested For dDCA Using CHI^2 , With Pre-processing	158
Figure 5.13: DCA And dDCA Performance With Various Proportions Rate Of Messages In Initial Population	161
Figure 5.14: Levelling Risk In DCA And dDCA By Retrieving The Value Of Output Signals From The Risk Scale	168

LIST OF ALGORITHMS

Algorithms	Page
Algorithm 2.1: Generic DCA Algorithm That Depicts The Entire Process Of Danger Measurement	40
Algorithm 2.2: Generic dDCA Algorithm That Depicts The Entire Process Of Danger Measurement	52
Algorithm 3.1: Pseudo-code Of Spam Risk-labelled Algorithm Based On Generic DCA	83
Algorithm 4.1: General Process of RiCCA	120
Algorithm 4.2: Process For Pre-processing Phase	122
Algorithm 4.3: Process For Term Frequency, TF	124
Algorithm 4.4: Process For DCA Classifier	128
Algorithm 4.5: Process For dDCA Classifier	132

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

LIST OF APPENDICES

Appendices	Page
Appendix A: Copy Of Full-text Published Papers	192
Appendix B: Research Operational Template (ROT)	193
Appendix C: Research Milestone	194
Appendix D: Source Code For The RiCCA Prototype	195
Appendix E: Questionnaire: Implicit Risk Of Spam Messages	203
Appendix F: Validation Form: The Influence Of Risk Concentration For Context Assessment (RiCCA) Of SMS Messages In Daily Use	204
Appendix G: Interface Of RiCCA Prototype	205

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

LIST OF PUBLICATIONS

1. **Zainal, K.,** Sulaiman, N. F., & Jali, M. Z. 2015. "An Analysis of Various Algorithms For Text Spam Classification and Clustering Using RapidMiner and Weka". *International Journal of Computer Science and Information Security (IJCSIS)*, 13(3), 66–74. Retrieved from <http://sites.google.com/site/ijcsis/>
2. **Zainal, K.,** & Jali, M. Z. 2015. "A Perception Model of Spam Risk Assessment Inspired by Danger Theory of Artificial Immune Systems". In *International Conference on Computer Science and Computational Intelligence (ICCSCI)* (Vol. 59, pp. 152–161). Elsevier Masson SAS. <http://doi.org/10.1016/j.procs.2015.07.530>
3. **Zainal, K.,** & Jali, M. Z. 2016. "A Review of Feature Extraction Optimization in SMS spam Messages Classification". In *International Conference on Soft Computing in Data Science (SCDS)* (Vol. 652, pp. 158–170). http://doi.org/10.1007/978-981-10-2777-2_14
4. **Zainal, K.,** & Jali, M. Z. 2017a. "The Design and Development of Spam Risk Assessment Prototype: In Silico of Danger Theory Variants". *International Journal of Advanced Computer Science and Applications (IJACSA)*, 8(4), 401–410. Retrieved from www.ijacsa.thesai.org
5. **Zainal, K.,** & Jali, M. Z. 2017b. "The Significant Effect of Feature Selection Methods in Spam Risk Assessment using Dendritic Cell Algorithm". In *International Conference on Information and Communication Technology (ICoICT 2017)* (pp. 277–284).
6. **Zainal, K.,** Jali, M. Z., & Hasan, A. B. 2018. "Comparative Analysis of Danger Theory Variants in Measuring Risk Level for Text Spam Messages." In *International Symposium on Data Mining Applications (SDMA)* (pp. 133–152). http://doi.org/10.1007/978-3-319-78753-4_1
7. **Zainal, K.,** & Jali, M. Z. 2018. "An Immunological-based Simulation: A Case Study of Risk Concentration for Mobile Spam Context Assessment". In *International Journal of Advanced Science, Engineering and Information Technology (IJASEIT)* (pp. 732-742). Retrieved from <http://dx.doi.org/10.18517/ijaseit.8.3.2719>

GLOSSARY

Adaptive immunity	a secondary response when the pathogen encountered for the second time which the concentration of relevant antibodies increases rapidly. Also known as specific response
Anomaly threshold (t_m for DCA; T_k for dDCA)	the signature of malicious in numerical value that separates normal and abnormal antigen. The measured output signal that is greater than this value is considered as malignant substance
Antigen	specific molecules present on surface of pathogen and recognized by immune system. The term antigen is an abbreviation from the word antibody generator
Apoptotic	signal alert released by normal cell death (semi-mature), indicate safe context
B-cells	develop in the bone marrow and involve in humoral immunity
Co-Stimulation (CSM)	a signal that act as co-stimulator in T-cells and B-cells activation
CD 4-Helper	commander of the immune response and it detects infection and sounds the alarm for initiating both T-cell and B-cell responses
CD 8-Cytotoxic	detects and kills infected or damaged body cells
Cell mediated immunity	involves mostly T-cells and responds to any cell that displays aberrant MHC markers, including cells invaded by pathogens, tumour cells, or transplanted cells
Context Assessment	measurement of cumulative output signals and the greater of semi-mature or mature of these signals become the cell context for antigen assessment. This cell context is used to label all antigen collected by the DCs with the derived context value in between 0 to 1
Danger Model	a theory of how the immune system works. It is based on the idea that the immune system does not distinguish between self and non-self, but rather between things that might cause damage and things that will not
Danger signal	signify abnormal behaviour which is indicates of an anomaly that is less than PAMPs

Danger Theory (DT)	takes care of 'non-self but harmless' and of 'self but harmful' invaders into human body systems. The central idea is that the immune system does not respond to non-self but to danger
Dendritic Cell (DC)	responsible to digest antigen material and forward it to the T-cells of the immune system. Also acting as messengers between the innate and adaptive immune systems
Ham	a valid or non-spam substance (such as SMS message)
Humoral immunity	involves B-cells or antibodies that recognize antigens or pathogens that are circulating in the lymph or blood
Immature DC (iDC)	Initial state of dendritic cell is immature and at this stage the cell is collecting debris and exposing to some signals will determine its next stage, either mature or semi-mature. Also known as naïve DC.
Immunity	refers to the situation in which an organism can defy a contagious illness
Inflammation	the signal amplify the effects of the other categories of signals; PAMPs, Danger and Safe signals
Innate immunity	primary response, occurs when any type of pathogen appears in the body for the first time. Also known as non-specific response
<i>In Silico</i>	refers to characterize biological experiments carried out entirely in a computer or via computer simulation
<i>In Vitro</i>	refers to the technique of performing a given procedure in a controlled environment outside of a living organism (within the glass)
<i>In Vivo</i>	refers to examination using a whole, living organism as opposed to a partial or dead organism (within the living)
Libtissue	prototype software system for constructing second generation AIS and applying them to real-world problems especially in intrusion detection study
Lightweight Intrusion detection SYStem (LISYS)	other prototype of AIS version for computational purposes, besides libtissue
Mature DC (mDC)	The immature dendritic cell that exposed to a greater quantity of either PAMPs or Danger signals than Safe

	signals will be transformed to mature state. At this stage, dendritic cells have the ability to present antigen and activate T-cells
Mature Context Antigen Value (MCAV)	determine the intensity or degree of the detected danger with the mean value of context per antigen type
Major Histocompatibility Complex (MHC)	a set of cell surface proteins essential for the acquired immune system to recognize foreign molecules
Necrotic	signal alert released by abnormal cell death (mature), indicate danger context
Pathogens Associated Molecular Patterns (PAMPs)	signify abnormal behaviour which highly indicates of an anomaly
Pathogen	an organism that can cause disease
Risk	is a measure of the extent to which an entity is threatened by a potential circumstance or event
Risk Concentration	translated as the severity of a spam text message. In this study, the malignant level referring to the risk density based on three (3) levels of categorical data (high, medium, low level of risk) that comes together with a numerical value (in between 0 to 1). The closer the calculated value to 1, the higher the potential risk is anticipated
Safe signal	signify a safe or normal context
Semi-mature DC (smDC)	The immature dendritic cell that exposed to a greater quantity of Safe signals will be transformed to semi-mature state. At this stage, dendritic cells do not have the ability activate T-cells but still able to present antigen
Spam	irrelevant or unsolicited messages, commonly sent over the Internet, typically to a large number of users, for the purpose such as advertising, phishing, and spreading malware.
T-cells	develop in the thymus and in charge for response in cell mediated immunity

LIST OF ABBREVIATIONS

Acc	Accuracy
AIS	Artificial Immune Systems
APC	Antigen Presenting Cell
A2P	Application to Person
BIS	Biological Immune Systems
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
CSM	Co-Stimulation
CHI ²	Chi-square
DAD	Disclosure, Alteration, Denial
DC / DCs	Dendritic Cell / Dendritic Cells
DCA	Dendritic Cell Algorithm
dDCA	Deterministic Dendritic Cell Algorithm
DT	Danger Theory
FEMA	Federal Emergency Management Agency
FN	False Negative
FP	False Positive
GSMA	Groupe Speciale Mobile Association or GSM Association
iDC	Immature Dendritic Cell / Naïve DC
IG Ratio	Information Gain Ratio
IGF	Internet Government Forum
ISO	International Organization for Standardization
IT	Information Technology
LISYS	Lightweight Intrusion detection System
MCAV	Mature Context Antigen Value
MCMC	Malaysian Communications and Multimedia Commission or Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) in Malay
mDC	Mature Dendritic Cell
MHC	Major Histocompatibility Complex
NB	Naïve Bayesian
NIST	National Institute of Standards and Technology
PAMPs	Pathogens Associated Molecular Patterns
PDCA	Plan, Do, Check, Action
RiCCA	Risk Concentration for Context Assessment
RM	Risk Management
S	Risk Scale
smDC	Semi-mature Dendritic Cell
SMS	Short Messaging Services
S _p	Spam probability
SPIM	SPam over Instant Messaging
SVM	Support Vector Machine
TF	Term Frequency
TLR	Toll-Like Receptor
T _k	Anomaly Threshold (dDCA)
t _m / t(m)	Anomaly Threshold (DCA)

TN	True Negative
TP	True Positive
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol
WM	Weight Matrix
Wi-Fi	Wireless Fidelity

