

FORMULATING GENERALIZE MALWARE ATTACK PATTERN USING FEATURES  
SELECTION

RUDY FADHLEE BIN MOHD DOLLAH

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

**FORMULATING GENERALIZE MALWARE ATTACK PATTERN USING  
FEATURES SELECTION**

RUDY FADHLEE BIN MOHD DOLLAH

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY  
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2014

## BORANG PENGESAHAN STATUS TESIS

JUDUL:

FORMULATING GENERALIZE MALWARE ATTACK PATTERN USING FEATURES SELECTION

SESI PENGAJIAN: SESI 2013/2014

Saya RUDY FADHLEE BIN MOHD DOLLAH mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. \*\* Sila tandakan (/)

\_\_\_\_\_ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

\_\_\_\_\_ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

\_\_\_\_\_/\_\_\_\_\_ TIDAK TERHAD

\_\_\_\_\_  
(TANDATANGAN PENULIS)

Alamat tetap : No 14 Lot 19830  
Kg Banggol Tok Jiring, 21060  
Kuala Terengganu  
Terengganu Darul Iman.

Tarikh : \_\_\_\_\_

\_\_\_\_\_  
(TANDATANGAN PENYELIA)

Nama Penyelia:  
(Dr. Robiah Binti Yusof)

Tarikh: \_\_\_\_\_

**FORMULATING GENERALIZE MALWARE ATTACK PATTERN USING  
FEATURES SELECTION**

RUDY FADHLEE BIN MOHD DOLLAH

This report is submitted in partial fulfillment of the requirement for the Bachelor of  
Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY  
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2014

## DECLARATION

I hereby declare that this project report entitled

### **FORMULATING GENERALIZE MALWARE ATTACK PATTERN USING FEATURES SELECTION**

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : \_\_\_\_\_ Date: \_\_\_\_\_

(RUDY FADHLEE BIN MOHD DOLLAH)

SUPERVISOR : \_\_\_\_\_ Date: \_\_\_\_\_

(DR. ROBIAH BINTI YUSOF)

## DEDICATION

*Dear Allah*

*May my life is within your guidance.*

*Dear Beloved Parents*

*Thank you for your never ending love, support, patience and encouragement. May*

*Allah bless always with you*

*Dear Lecturers and Supervisor*

*Thank you for all the knowledge and support.*

*Dear Friends*

*Thank you for all the knowledge, support and encouragement...*

## ACKNOWLEDGEMENTS

I would like to thank Dr.Robiah binti Yusof for her excellent support, guidance, motivation, constant patience, and continuous understanding throughout the semester of my Final Year Project in Universiti Teknikal Malaysia Melaka (UTeM).

I would also like to express my deepest appreciation to my beloved mother (Maimun), beloved father (Mohd Dollah) and my siblings (Murni Hayati and Murni Hayana) for their endless love, constant encouragement, support, motivation, patience and understanding throughout the year of my studies in UTeM.

To my friends, thank you for listening, offering me advice, and supporting me through this entire process. Special thanks to Amir Hamdi, Adibah Razali, Safarina, Hidayah Ibrahim, Al-Hafiz, Zhafri, Hafiz Gapar and all members of FTMK 3 BITC 2013/2014 which made my final years at UTeM a moment to remember.

## ABSTRACT

Number of malware is growing dramatically. Malicious codes can be easily obtained and use as one of weapon to gain illegal objectives. Hence, in this project, network traffic are explored to identify the traces left on the victim and attacker to reveal the true victim and attacker. For the purpose of this project, it focused on malware intrusion and traditional worms namely Blaster and Sasser worm variants. This project is operated based on victim's and attacker's perspective. Thus, the objective of this project is to identify the features/attributes of malware in perspective of victim and attacker, to generate attack pattern of malware in perspective of victim and attacker, and to generalize the attack pattern in perspective of victim and attacker. Based on generating the attack pattern, the attack pattern for malware is generalized in algorithm script to verify it accuracy.



## ABSTRAK

Bilangan *malware* semakin meningkat secara mendadak. Kod *malicious* mudah diperolehi dan digunakan sebagai salah satu senjata untuk mencapai objektif yang tidak baik. Oleh itu, dalam projek ini, rangkaian trafik diteroka untuk mengenalpasti kesan – kesan yang ditinggalkan oleh mangsa dan penyerang untuk menentukan corak surih *worm* untuk mendedahkan mangsa atau penyerang yang sebenar. Bagi tujuan itu, ia tertumpu kepada pencerobohan *malware* dan *traditional worm* iaitu variasi Blaster dan Sasser *worm*. Projek ini dikendalikan berdasarkan perspektif mangsa dan penyerang. Oleh itu, objektif projek ini adalah untuk mengenalpasti ciri – ciri atau sifat *malware*, untuk menjana corak serangan *malware*, dan untuk menjana corak menyerang secara umum dalam perspektif mangsa dan penyerang. Corak menyerang *malware* dijadikan umum dalam bentuk skrip algoritma untuk memastikan ketepatannya

## TABLE OF CONTENTS

<b>CHAPTER</b>	<b>SUBJECT</b>	<b>PAGE</b>
	<b>DECLARATION</b>	
	<b>DEDICATION</b>	<b>ii</b>
	<b>ACKNOWLEDGMENT</b>	<b>iii</b>
	<b>ABSTRACT</b>	<b>iv</b>
	<b>ABSTRAK</b>	<b>v</b>
	<b>TABLE OF CONTENTS</b>	<b>vi</b>
	<b>LIST OF TABLES</b>	<b>ix</b>
	<b>LIST OF FIGURES</b>	<b>x</b>
<b>CHAPTER I</b>	<b>INTRODUCTION</b>	
	1.1 Project Background	1
	1.2 Problem Statement	3
	1.3 Research Question	4
	1.4 Objectives	4
	1.5 Scopes	5
	1.6 Project Significance	5
	1.7 Conclusion	5
<b>CHAPTER II</b>	<b>LITERATURE REVIEW</b>	
	2.1 Introduction	6
	2.2 Types of Malware	8
	2.2.1 Malware Definition	8
	2.2.2 Malware Classification	9
	2.2.3 Worm Definition	10
	2.2.4 Worm Classification	10
	2.2.5 Type of Worm	12
	2.2.6 Blaster.A Worm	13

2.2.7	Blaster.A Characteristic	13
2.2.8	Blaster.T Worm	14
2.2.9	Blaster.T Characteristic	15
2.2.10	Sasser.B Worm	15
2.3	Attack Pattern	16
2.3.1	Attack Pattern Definition	16
2.3.2	Importance of Attack Pattern	17
2.4	Technique of Identifying Malware Attack Pattern	19
2.4.1	Malware Detection Technique Definition	19
2.4.2	Types of Identifying Technique	20
2.4.3	Features Selection Definition	20
2.4.4	Selected Features	21
2.5	Network Tool	21
2.5.1	Wireshark	21
2.6	Network Traffic	23
2.6.1	Packet Detail	23
2.7	Programming Language	26
2.7.1	Scripting	26
2.8	Overall Discussion on Chapter 2	26
2.9	Conclusion	28
<b>CHAPTER III METHODOLOGY</b>		
3.1	Project Methodology	29
3.1.1	Phase I: Literature Review	30
3.1.2	Phase II: Analysis	30
3.1.3	Phase III: Design and Development	30
3.1.4	Phase IV: Implementation	30
3.1.5	Phase V: Testing and Evaluation	30
3.2	Project Requirement	31
3.2.1	Software Requirement	31
3.2.2	Hardware Requirement	31
3.3	Project Schedule and Milestone	32
3.4	Conclusion	32
<b>CHAPTER IV DESIGN AND IMPLEMENTATION</b>		
4.1	Introduction	33

	4.2	Analysis Design	33
	4.3	Analysis and Finding Data	44
	4.4	Implementation	87
	4.5	Conclusion	89
<b>CHAPTER V</b>		<b>TESTING AND ANALYSIS</b>	
	5.1	Introduction	90
	5.2	Test Plan	91
	5.3	Test Strategy	92
	5.4	Test Design	93
	5.5	Test Result and Analysis	94
	5.6	Conclusion	97
<b>CHAPTER VI</b>		<b>CONCLUSION</b>	
	6.1	Observation on Weaknesses and Strengths	98
	6.2	Proposition for Improvement	99
	6.3	Contribution	100
	6.4	Conclusion	101
		<b>REFERENCES</b>	
		<b>APPENDICES A</b>	
		<b>APPENDICES B</b>	
		<b>APPENDICES C</b>	
		<b>APPENDICES D</b>	
		<b>APPENDICES E</b>	

## LIST OF TABLES

<b>TABLE</b>	<b>TITLE</b>	<b>PAGE</b>
1.1	Summary of problem statement	3
1.2	Summary of research question	4
1.3	Summary of research objectives	5
2.1	Malware Descriptions	9
2.2	Type of worm	12
2.3	Blaster.A worm naming	13
2.4	Blaster.T worm naming	14
2.5	Summary of Sasser Variants	15
2.6	Packet list pane	22
2.7	Description of each field in IP Header	24
2.8	Description of each field in TCP Header	25
2.9	Summary of the attack pattern	27
2.10	Features that selected and with it description	28
3.1	Software requirements	31
3.2	Hardware specification	31
4.1	Summary of Features's Percentage for 3 Scenarios	58
4.2	Features that selected and with it description	58
4.3	Features that selected and with it description	76
4.4	Percentage of features	82
4.5	Selected features for generalize malware attack pattern	82
4.6	Selected features for the project	85
5.1	Data to be tested	93
5.2	Comparison of Testing Output of Blaster. A - 8Mac2010_0100pm	94
5.3	Comparison of Testing Output of BlasterT_5.00pm	96
5.4	Comparison of Testing Output of SasserB-230410	97

## LIST OF FIGURES

<b>FIGURE</b>	<b>TITLE</b>	<b>PAGE</b>
1.1	Incidents received in Q3 2013 classified according to the type of incidents handled by MyCERT.	2
1.2	The incident handled by MyCERT in third quarter 2013 compared with previous quarter.	3
1.3	Malicious code incidents received in 2013 handled by MyCERT	3
2.1	Literature review phase part 1	7
2.2	Literature review phase part 2	8
2.3	General malware taxonomy by Karresand	9
2.4	Classification of worm	11
2.5	Proposed generic taxonomy of malware detection technique.	20
2.6	Packet List Panel in Wireshark	22
2.7	Packet Detail Pane in Wireshark	22
2.8	Packet Byte Pane in Wireshark	23
2.9	IP Header version 4	24
2.10	TCP Header	25
3.1	Project Methodology	29
4.1	Scenario 1 of Blaster.A - 8Mac2010_0100pm	35
4.2	Scenario 2 of Blaster.A - 9Mac2010_1220am	36
4.3	Scenario 3 of Blaster.A - 9Mac2010_1730pm	37
4.4	Blaster.T attack in scenario A	38
4.5	Blaster.T attack in scenario B	39
4.6	Blaster.T attack in scenario C	40
4.7	Sasser.B intrusions Scenario D	41
4.8	Sasser.B intrusions Scenario E	42
4.9	Sasser.B intrusions Scenario F	43
4.10	General process of selecting malware features	44
4.11	Connection establishment on port 135, protocol TCP	45
4.12	Connection on port 135, protocol DCERPC	45

4.13	Connection on port 135, TCP protocol	46
4.14	Connection on port 4444 with TCP protocol (1)	46
4.15	Connection on port 4444 with TCP protocol (2)	47
4.16	Connection on port 4444 with TCP protocol (3)	47
4.17	Connection on port 4444 with TCP protocol (4)	48
4.18	Connection on port 69 with TFTP protocol	48
4.19	Connection of port 4444 with TCP protocol (5)	49
4.20	Data packet of msblast.exe	49
4.21	Connection of port 4444 with TCP protocol (6)	50
4.22	Connection of port 4444 with TCP protocol (7)	50
4.23	Connection of port 4444 with TCP protocol (8)	51
4.24	Percentages of Features on Scenario 1 of Blaster. A 8Mac2010_0100pm	52
4.25	Percentages of Features on Scenario 1 of Blaster. A 8Mac2010_0100pm	53
4.26	Percentages of Features on Scenario 2 of Blaster. A 9Mac2010_1220am	54
4.27	Percentages of Features on Scenario 2 of Blaster. A 9Mac2010_1220am	55
4.28	Percentages of Features on Scenario 3 of BlasterA - 9Mac2010_1730pm	56
4.29	Percentage of Features on Scenario 3 of BlasterA - 9Mac2010_1730pm	57
4.30	Blaster.A attack pattern design on attacker perspective	59
4.31	Blaster.A attack pattern design on victim perspective	60
4.32	Blaster.T first flow of attacker	60
4.33	Connection on port 135 using DCERPC protocol	61
4.34	Connection on port 135 with TCP protocol	61
4.35	Connection on port 4444 with TCP protocol (1)	62
4.36	Connection on port 4444 with service krb524 using TCP protocol (2)	62
4.37	Connection on port 4444 with service krb524 using TCP protocol (3)	63
4.38	Connection on port 4444 with service krb524 using TCP protocol	

	(4)	63
4.39	Connection on port 4444 with service krb524 using TCP protocol	
	(5)	64
4.40	Connection on port 4444 with service krb524 using TCP protocol	
	(6)	64
4.41	Connection on port 4444 with service krb524 using TCP protocol	
	(7)	65
4.42	Connection on port 69 with tftp protocol	65
4.43	Connection on port 3xxx with tftp protocol	65
4.44	Continue Connection on port 4444 with TCP protocol (8)	66
4.45	Continue Connection on port 4444 with TCP protocol (9)	66
4.46	Continue Connection on port 4444 with TCP protocol (10)	67
4.47	Continue Connection on port 4444 with TCP protocol (11)	67
4.48	Continue Connection on port 4444 with TCP protocol (12)	68
4.49	Continue Connection on port 4444 with TCP protocol (13)	68
4.50	Continue Connection on port 4444 with TCP protocol (14)	69
4.51	Continue Connection on port 4444 with TCP protocol (15)	69
4.52	Continue Connection on port 4444 with TCP protocol (16)	70
4.53	Continue Connection on port 4444 with TCP protocol (17)	70
4.54	Continue Connection on port 4444 with TCP protocol (18)	71
4.55	Continue Connection on port 4444 with TCP protocol (19)	71
4.56	Connection Finish	71
4.57	Percentages of first data set	73
4.58	Percentage of second data	74
4.59	Percentage of third data	75
4.60	Blaster.T attack pattern design on attacker perspective	77
4.61	Blaster.T attack pattern design on victim perspective	78
4.62	Sasser.B uses port 445 and sent SMB packets	79
4.63	Opens port 9996 to run remote shell	79
4.64	Sasser.B opens port 5554	80
4.65	Statistic of IP address (Scenario D)	81
4.66	Statistic of IP address (Scenario E)	81
4.67	Statistic of IP address (Scenario F)	81
4.68	Sasser.B attack pattern on attacker perspective	83



4.69	Sasser.B attack pattern on victim perspective	84
4.70	Generalize worm attack pattern design on attacker perspective	86
4.71	Generalize worm attack pattern design on victim perspective	86
4.72	Flowchart of generalize attack pattern process	88
5.1	Testing Phase life cycle	91
5.2	Classes of Test	92
5.3	Testing output of Blaster. A - 8Mac2010_0100pm	94
5.4	Testing Output of BlasterT_5.00pm	95
5.5	Testing Output of BlasterT_5.00pm (2)	95
5.6	Testing Output of SasserB-230410	96

## CHAPTER I

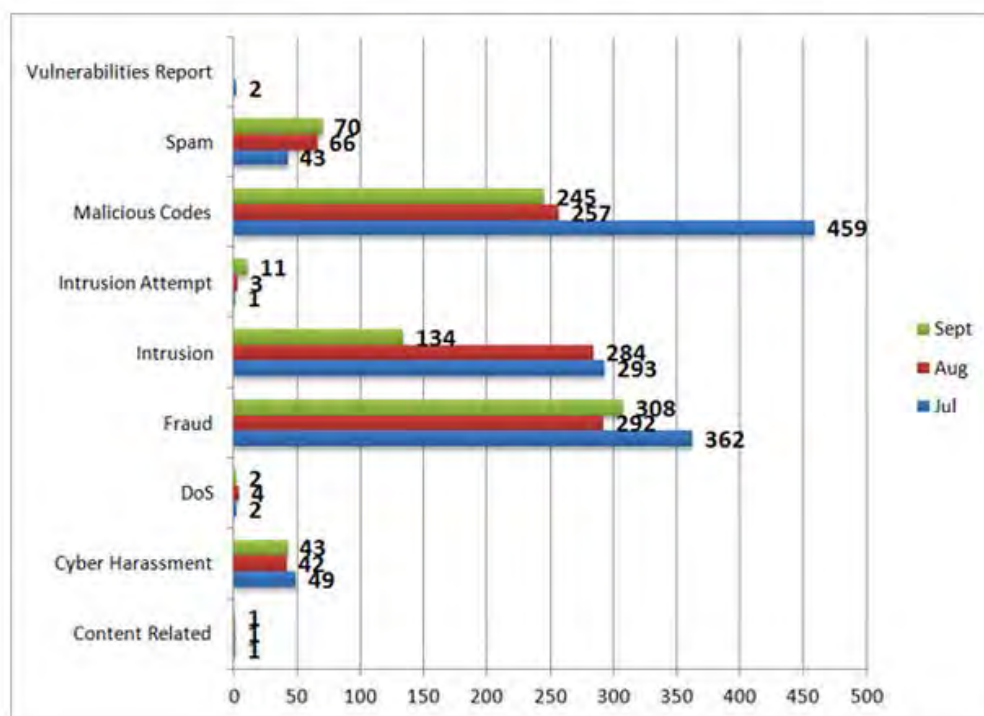
### INTRODUCTION

#### 1.1 Project Background

Malware, a word that stands for “malicious software” is a software or program that designed to penetrate or damaged a computer system which the victim not know their machine is being attacked. It can be grouped into two categories; independents and dependents. Independents malware does not need a host or program to spread the threats. Meanwhile, dependents need host or program to spread the attacks and require human intervention to launch the threat. The malware includes Trojan, virus and worm.

This project purpose is to analyze the malware ability on the view of victim and attacker. It is also to give outcome of generalize attack pattern of three malwares (Sasser.B, Blaster.A and Blaster.T).The generalize attack pattern is important to computer security researcher to enhance the security measure of the computer system.

Figure 1.1 shows a graph of incident received by Malaysian Computer Emergency Response Team(MyCERT) and is stated in the third quarter 2013 report. The incidents are vulnerabilities, spam, malicious code, intrusion attempt, intrusion, fraud, denial of service, cyber harassment, and content related. According to the Figure 1.1 below, malicious code shows a high number of cases handled by MyCERT.



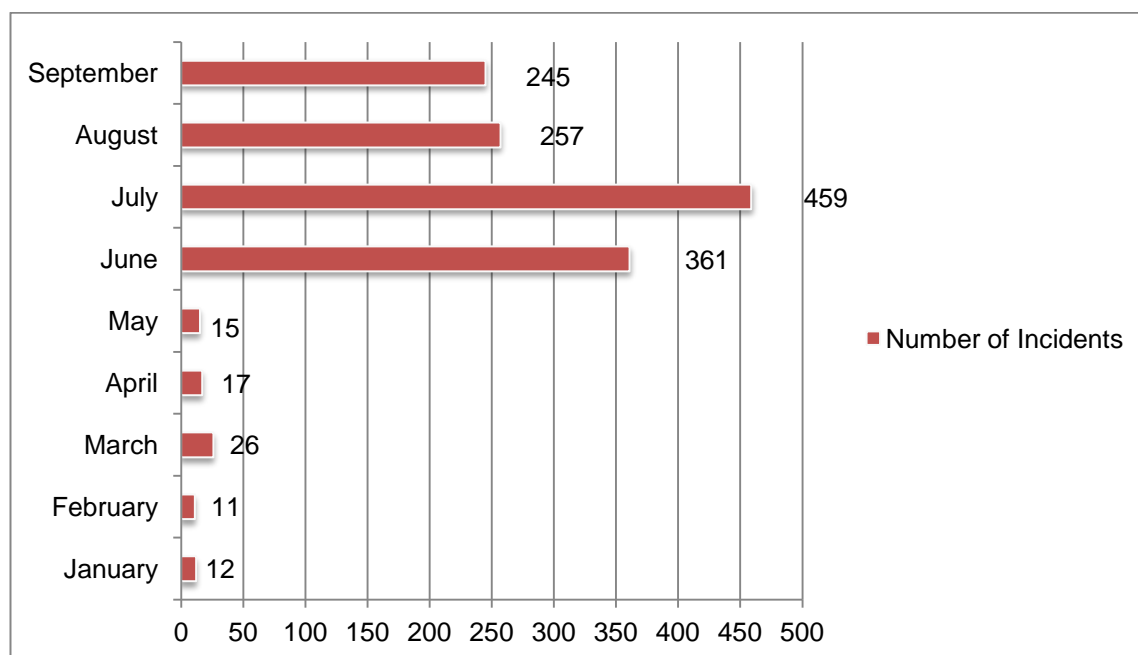
**Figure 1.1 : Incidents received in Q3 2013 classified according to the type of incidents handled by MyCERT.**

In addition, Figure 1.2 illustrates the incident handled by MyCERT of third quarter of 2013 compared to previous quarter. The data shows that Malicious Code have the highest increase compared to other categories of incident.

Categories of Incidents	Quarters		%
	Q2 2013	Q3 2013	
Content Related	26	3	88.46
Cyber Harassment	133	134	0.75
DoS	8	8	0.00
Fraud	1374	962	29.99
Intrusion	864	711	17.71
Intrusion Attempt	8	15	87.50
Malicious Codes	393	961	144.53
Spam	283	179	36.75
Vulnerabilities Report	4	2	50.00

**Figure 1.2 : The incident handled by MyCERT in third quarter 2013 compared with previous quarter.**

The summarized number of incidents about malicious code is created throughout the year 2013 is illustrated in Figure 1.3.



**Figure 1.3 : Malicious code incidents received in 2013 handled by MyCERT.**

Based on the both Figures 1.1, Figure 1.2 and Figure 1.3, we cannot take lightly of malicious code as it is a weapon that can be use by cybercriminal to do crime. Hence, it is very important to study and analyze the trace of the malware attack. The attack pattern provides information of their attack goals and we can use it to defend against the attack.

## 1.2 Problem Statement

**Table 1.1 : Summary of problem statement**

No	Problem Statement
RP1	With thousands of different malware on the Net, it is difficult to handling this malicious code based on it pattern individually.

## 1.2 Research Question

Only one Research Question (RQ) is generated to identify the research problem. From Research Problem 1 (RP1), Research Question 1 (RQ1) is produced. Table 1.2 is the summary of research question.

**Table 1.2 : Summary of research question**

RP	RQ	Research Question
RP1	RQ1	How can we generalize malware attack pattern of Sasser.B, Blaster.T and Blaster.A?

## 1.4 Objectives

Based on the research question in previous section, suitable Research Objective (RO) is produced to achieve aim of the research. There are three research objectives identified for this research.

**RO1: To identify the general feature or attribute of malwares (Sasser.B, Blaster.T and Blaster.A).**

Investigate the features or attributes of Sasser.B, Blaster.T and Blaster.A by analysing the network traffic of existing data.

**RO2: To generate attack pattern in perspective of victim and attacker.**

Based on identifying the features of malware, attack pattern of malware (Sasser.B, Blaster.T and Blaster.A) is generated for victim and attacker.

**RO3: To verify the accuracy of the algorithm script.**

Based on generating the attack pattern, the attack pattern for malware is generalized in algorithm script to verify its accuracy.

**Table 1.3 : Summary of research objectives**

RP	RQ	RO	Research Objective
RP1	RQ1	RO1	To identify the general feature or attribute of malwares (Sasser.B, Blaster.T and Blaster.A).
RP1	RQ1	RO2	To generate attack pattern in perspective of victim and attacker.
RP1	RQ1	RO3	To verify the accuracy of the algorithm script.

## 1.5 Scopes

The scope of this research will focus on certain matters as specified below:

1. This research is using only three specific type of traditional worm - Sasser.B, Blaster.T and Blaster.A.
2. Focusing on attack pattern of victim and attacker perspective.
3. Using network traffic data (tcpdump).

## 1.6 Project significance

Based on the research objectives, this research will contribute in identify the appropriate attributes / features in respective network traffic of malwares (Sasser.B, Blaster.T and Blaster.A) in perspective of victim and attacker. Besides, this research will propose the malware's (Sasser.B, Blaster.T and Blaster.A) attack pattern in perspective of victim and attacker. Furthermore, this research will propose the general malware's attack pattern in perspective of victim and attacker.

## 1.7 Conclusion

In conclusion, the generalize attack pattern help researcher to identify the objective of the attack and can expand it to strategize the defend mechanism of the computer network system. The next chapter will discuss on literature review, project methodology, software requirement, hardware requirement, and other requirement.

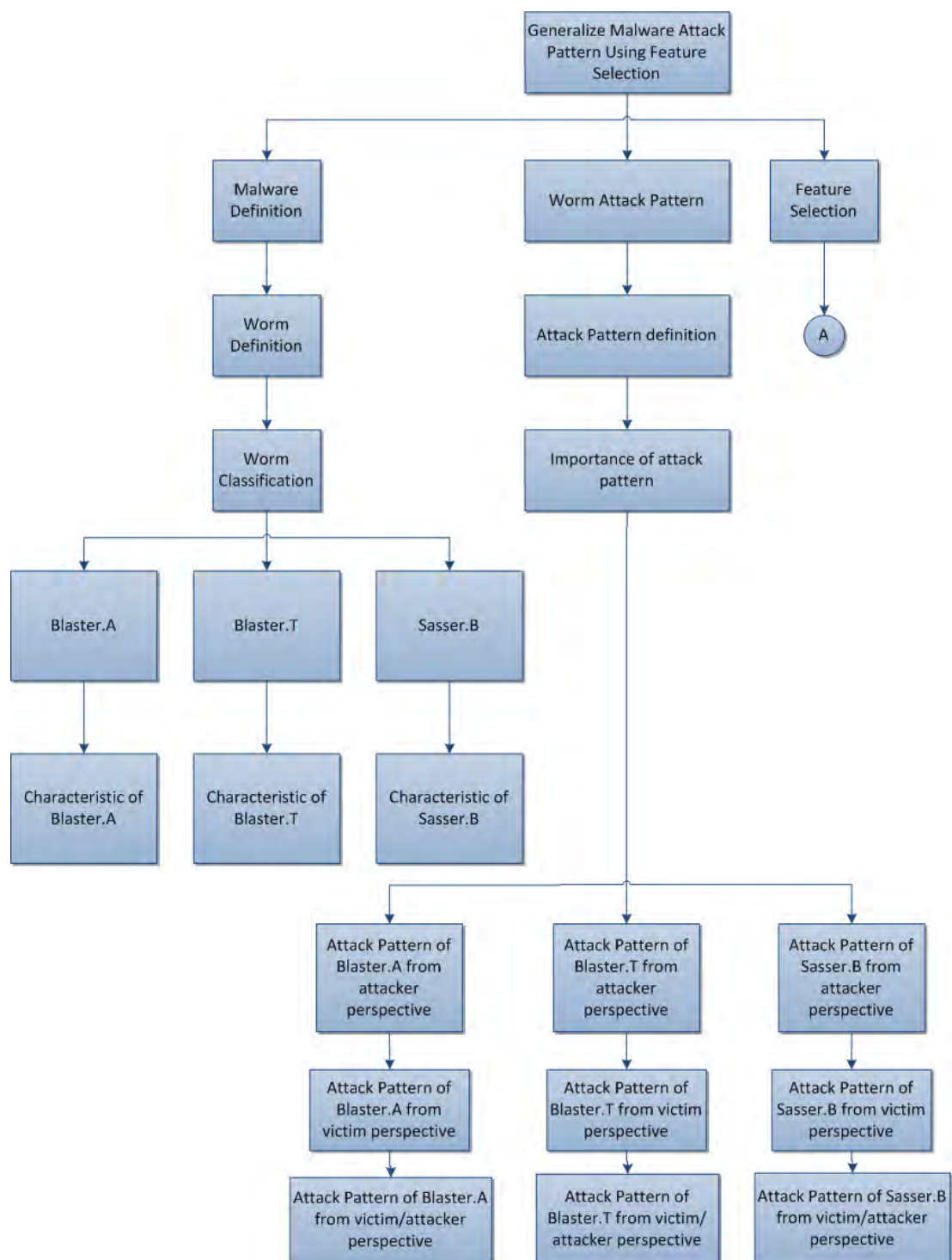
## **CHAPTER II**

### **LITERATURE REVIEW**

#### **2.1 Introduction**

In this chapter, there are two main topics that will be discussed, the literature review and project methodology. The literature review will be based on reading phase framework design to ensure the literature is related to research title and will help to answer research question (RQ1) and achieve research objectives (RO1), (RO2) and (RO3). The project methodology will also be discussed later in this chapter.

Figure 2.1 and Figure 2.2 are reading frameworks for the literature review phase. This framework will be used as a guide in this chapter. The project title is broken down into several items consisting of malware definition, worm attack pattern and feature selection. The malware definition focuses on literature of worm definition and the scopes are about three worms which are Blaster.A, Blaster.T and Sasser.B. The worm attack pattern framework part is about defining the attack pattern term and identifying the role perspective of attacker, victim and victim/attacker scenario. In addition, the feature selection part focuses on network tools, network traffic and programming language for scripting at a later phase of the project.



**Figure 2.1 : Literature review phase part 1**