View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Universiti Teknikal Malaysia Melaka (UTeM) Repository

SIGNIFICANT FEATURE IDENTIFICATION MECHANISM FOR IPv6 IN ENHANCING INTRUSION DETECTION SYSTEM

ZULKIFLEE BIN MUSLIM

DOCTOR OF PHILOSOPHY

2017

© Universiti Teknikal Malaysia Melaka

Faculty of Information and Communication Technology

SIGNIFICANT FEATURE IDENTIFICATION MECHANISM FOR IPv6 IN ENHANCING INTRUSION DETECTION SYSTEM

Zulkiflee bin Muslim

Doctor of Philosophy

2017

© Universiti Teknikal Malaysia Melaka

SIGNIFICANT FEATURE IDENTIFICATION MECHANISM FOR IPv6 IN ENHANCING INTRUSION DETECTION SYSTEM

ZULKIFLEE BIN MUSLIM

A thesis submitted
in fulfillment of the requirements for the degree of Doctor of Philosophy

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

© Universiti Teknikal Malaysia Melaka

DECLARATION

I declared that this thesis entitled, “Significant Feature Identification Mechanism For IPv6 In Enhancing Intrusion Detection System” is the result of my own research work except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature	: ………………………………
Name	: ZULKIFLEE BIN MUSLIM
Date	: ………………………………

© Universiti Teknikal Malaysia Melaka

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of Doctor of Philosophy.

Signature : ……………………………………………..
Supervisor Name : PROF. DR. SHAHRIN B. SAHIB
Date : ……………………..

© Universiti Teknikal Malaysia Melaka

ABSTRACT

An *Intrusion Detection System* (IDS) is a security mechanism used to detect attack patterns that occur in a network. IDS has been adapted from an Internet Protocol version 4 (IPv4) onto an Internet Protocol version 6 (IPv6) environment for the same purpose. IPv6 security issue requires IDS that has the capability to ease new threats. However, the ineffectiveness of the existing native IPv6 detection techniques cause the network attack detection in IPv6 is unconvincing. This problem has emerged due to lack of feature analysis to identify the most significant features before the chosen features used in detection technique construction. Therefore, this study has propose a technique called *Significant Feature Identification Mechanism for IPv6* (SIMv6) as a solution for feature selection issue in IPv6 domain. The *SIMv6* model has a capability of self-learning and flexible to fit with any type of data which requires feature selection solution. In this study, *SIMv6* is applied on the IPv6 dataset to identify the most significant features which is named as *Significant Features in IPv6* (SigFeatv6). Then, *SigFeatv6* is tested and evaluated its performance to differentiate between normal and attack packets accurately. The performance of *SigFeatv6* then has been compared with the performance of other features used by existing native IPv6 detection techniques. *ANOVA* and *T-Test* are the statistical tests used to evaluate the significant difference for the accuracy score between different features. Next, as time feature is an important feature for future detection technique a derived feature called *TimeInterval* was introduced to enhance the *timestamp* feature. *SIMv6* again is applied on a new set of IPv6 dataset which includes *TimeInterval* as one of its feature. The result indicates that features proposed by *SIMv6* obtained 99.87% accuracy score in average to differentiate between normal and various IPv6 network attacks packet. From the findings, *SIMv6* is capable of determining the most significant features to distinguish IPv6 packet status more effective compares to other features used by prior studies. Furthermore, the introduction of *TimeInterval* feature has improved the *SigFeatv6* performance. A testbed based on IPv6 network environment was deployed to produce a reliable IPv6 dataset. In the future, a new detection technique can be formulated based on the features proposed in *SigFeatv6* while *SIMv6* can also be applied in other domains which require feature selection solution.

© Universiti Teknikal Malaysia Melaka

ABSTRAK

Sistem Pengesanan Pencerobohan (IDS) merupakan sebuah mekanisme keselamatan untuk mengesan corak serangan yang berlaku di dalam rangkaian. Sistem ini telah diadaptasikan daripada persekitaran IPv4 ke IPv6 untuk tujuan yang sama. Isu keselamatan IPv6 memerlukan IDS yang mampu mengekang ancaman baru. Walaubagaimanapun, ketidakberkesanan teknik pengesanan IPv6 asli menyebabkan pengesan serangan rangkaian di persekitaran IPv6 tidak meyakinkan. Masalah ini timbul berpunca dari kekurangan analisa ciri-ciri untuk mengenalpasti ciri yang paling penting sebelum ciri-ciri terpilih digunakan untuk membangunkan teknik pengesanan. Oleh itu, kajian ini mencadangkan sebuah teknik bernama Significant Feature Identification Mechanism for IPv6 (SIMv6) sebagai penyelesaian untuk isu pemilihan ciri-ciri dalam domain IPv6. SIMv6 mempunyai kemampuan untuk belajar sendiri dan fleksibel untuk sesuai dengan sebarang jenis data yang memerlukan solusi pemilihan ciri-ciri. Dalam kajian ini, SIMv6 telah diaplikasikan ke atas set data IPv6 untuk mengenalpasti ciri-ciri terpenting yang dinamakan sebagai Significant Features in IPv6 (SigFeatv6). Kemudian, SigFeatv6 diuji dan dinilai prestasinya untuk membezakan antara paket normal dan serangan secara tepat. Prestasi SigFeatv6 kemudiannya dibandingkan dengan prestasi ciri-ciri yang gunakan dalam teknik pengesanan IPv6 asli sedia ada. ANOVA dan T-Test merupakan pengujian statistic yang digunakan untuk menilai perbezaan ketara untuk markah ketepatan antara ciri-ciri berbeza. Selepas itu, memandangkan ciri masa merupakan ciri utama untuk teknik pengesanan akan datang sebuah ciri dipanggil TimeInterval telah diperkenalkan untuk meningkatkan ciri timestamp. SIMv6 sekali lagi diaplikasikan ke atas set data IPv6 baru termasuk TimeInterval sebagai salah satu ciri-cirinya. Keputusan menunjukkan ciri-ciri yang dipilih of SIMv6 mendapat 99*.87% markah ketepatan secara purata untuk membezakan antara paket normal and pelbagai jenis serangan rangkaian IPv6. Dari hasil dapatan, SIMv6 mampu menentukan ciri-ciri paling penting untuk membezakan status paket IPv6 dengan lebih efektif berbanding dengan ciri-ciri yang digunakan oleh kajian-kajian sebelum ini. Tambahan lagi, pengenalan ciri TimeInterval telah meningkatkan prestasi SigFeatv6. Sebuah lapangan kajian berdasarkan persekitaran rangkaian IPv6 telah dibangunkan untuk menghasilkan set data IPv6 yang boleh dipercayai. Untuk masa depan, sebuah teknik pengesanan baru boleh dirumuskan dengan menggunakan ciri-ciri yang disarankan dalam SigFeatv6 sementara SIMv6 boleh diaplikasikan ke domain lain yang memerlukan penyelesaian pemilihan ciri-ciri.*

© Universiti Teknikal Malaysia Melaka

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and the Most Merciful

Alhamdulillah, all praises to Allah for His strength and blessing in completing this thesis. I would like to express my gratitude to my respectful supervisor as well as my mentor, Professor Dr. Shahrin Sahib, whose expertise, understanding, and patience significantly enhanced my graduate experience. I appreciate his vast knowledge, skill, and genuine empathy throughout my study.

I would like to express my appreciation to my co-supervisor and all my colleagues and staff members of FTMK for their cooperation in making this study a success. Not to forget Universiti Teknikal Malaysia Melaka (UTeM) and Ministry of Higher Education Malaysia for sponsoring this study.

Last but not least, my deepest gratitude goes to my beloved parents: Hjh Halimah Md Isa and Hj Muslim B. Hussain, and also to my sisters, Noor Aishah, Noraini, Noor Azizah, and Noor Ashikin, for their endless love, prayers, and encouragement. Heartfelt thanks to my beloved wife, Haniza Nahar, and my precious children, Afiq, Wani, Anis, Wafi, Aniq, Ahmad and Warda, for their love, care, memories, and endless support of me.

To those who indirectly contributed to this research, your kindness means a lot to me. Thank you very much.

Zulkiflee Bin Muslim, 2017.

© Universiti Teknikal Malaysia Melaka

TABLE OF CONTENTS

	PAGE
DECLARATION	
APPROVAL	
ABSTRACT	**i**
ABSTRAK	**ii**
ACKNOWLEDGEMENT	**iii**
TABLE OF CONTENTS	**iv**
LIST OF TABLES	**viii**
LIST OF FIGURES	**x**
LIST OF APPENDICES	**xii**
LIST OF ABBREVIATIONS	**xiii**
LIST OF PUBLICATIONS	**xiv**

CHAPTER

1. INTRODUCTION	**1**
1.1 Introduction	1
1.2 Research Overview	1
1.3 Research Problem	4
1.4 Research Question	7
1.4.1 Main Research Question	7
1.4.2 Sub Research Questions	8
1.5 Research Objectives	9
1.6 Research Methods	10
1.7 Research Contributions	11
1.8 Research Scope	12
1.8.1 Scope of the Dataset	12
1.8.2 Scope of the Testbed	12
1.9 Thesis Organization	13
1.10 Summary	16

© Universiti Teknikal Malaysia Melaka

2. LITERATURE REVIEW **17**

2.1 Introduction 17

2.2 Overview of an Intrusion Detection System 17

2.2.1 IDS Definition 18

2.2.2 IDS Framework 18

2.2.3 IDS Taxonomy 20

2.2.4 IDS Implementation 25

2.3 IPv6 Current Challenges 28

2.3.1 IPv6 Security Issues 29

2.3.2 IPv6 Dataset for Research Purposes 30

2.3.3 IPv6 IDS Detection Technique Issues 33

2.4 Analysis of Current IPv6 IDS Detection Technique 34

2.4.1 Analysis Based on Technique Construction Process 35

2.4.2 Analysis Based on Feature Used 39

2.4.3 Analysis Based on Data Collection Environment 42

2.4.4 Analysis Based on Evaluation Parameters 44

2.4.5 Current Detection Technique Summary 45

2.5 Feature Selection Technique 47

2.5.1 Feature Selection Process 48

2.6 Summary 60

3. METHODOLOGY **63**

3.1 Introduction 63

3.2 Research Methodology 63

3.3 Research Approach 65

3.3.1 Quantitative Method 65

3.4 Research Framework 66

3.4.1 Literature Review 67

3.4.2 Testbed Deployment 68

3.4.3 Feature Formulation 69

3.4.4 Feature Formulation 70

3.4.5 Documentation 72

© Universiti Teknikal Malaysia Melaka

	3.5	Research Process	72
		3.5.1 Theoretical Study	73
		3.5.2 Exploratory Study	78
	3.6	Summary	81
4.	**FEATURE FORMULATION**		**82**
	4.1	Introduction	82
	4.2	Testbed Deployment	83
		4.2.1 Testbed Network Layout Design	83
		4.2.2 Testbed Scenario Design	89
		4.2.3 Data Collection Procedure	91
		4.2.4 Data Reliability Verification	93
	4.3	Feature Formulation Procedure	97
		4.3.1 Common Feature	98
		4.3.2 Justified Feature	100
		4.3.3 Finalized Feature	101
		4.3.4 Data Smoothing	102
	4.4	Prepared Dataset	109
	4.5	Summary	110
5.	**IMPLEMENTATION OF FEATURE ASSESSMENT**		**111**
	5.1	Introduction	111
	5.2	Feature Evaluation	111
		5.2.1 Significant Feature Identification Mechanism for IPv6 (SIMv6)	113
		5.2.2 SIMv6 Feature Selection	116
	5.3	Feature Evaluation Process Flow	118
		5.3.1 Author Selection	120
		5.3.2 Data Preparation for Feature Evaluation	122
		5.3.3 Procedure for Feature Evaluation	125
		5.3.4 Feature Evaluation Result	127
	5.4	The Impact of the Time Feature	129
	5.5	Summary	130

© Universiti Teknikal Malaysia Melaka

6. DETERMINATION OF SIGNIFICANT FEATURE FOR IPV6 IDS 131

6.1 Introduction 131

6.2 TimeInterval Feature 132

6.3 The Effectiveness of *TimeInterval* 133

6.4 The Feature Selection with *TimeInterval* 136

6.5 *SigFeatTIv6* Performance Evaluation 138

6.6 Summary 141

7. DISCUSSION AND CONCLUSION 144

7.1 Introduction 144

7.2 Research Process 145

7.3 Research Conclusion 146

7.4 Research Objectives Summarization 149

7.4.1 RO1: Propose a Feature Formulation Process 149

7.4.2 RO2: Effective Mechanism to Determine the Significant Features 150

7.4.3 RO3: Significant Feature Identification 151

7.5 Research Contributions 151

7.5.1 RC1: Feature Formulation Process 152

7.5.2 RC2: A Comprehensive and Reliable IPv6 Dataset 152

7.5.3 RC3: A New Process Flow of Schematic Dataset Construction 154

7.5.4 RC4: Significant Feature Identification Mechanism for IPv6 (SIMv6) 154

7.5.5 RC5: A Novel Features Evaluation Procedure 155

7.5.6 RC6: Introduction of *TimeInterval* Feature 155

7.6 Research Limitations 156

7.6.1 The Dataset Limitation 156

7.6.2 The Feature Selection Limitation 157

7.7 Future Research 158

7.7.1 New Detection Technique 158

7.7.2 Advanced Features Construction 158

7.7.3 Apply SIMv6 to Other Domain 159

REFERENCES 160

APPENDICES 184

© Universiti Teknikal Malaysia Melaka

LIST OF TABLES

TABLE	TITLE	PAGE
1.1	The Impact of Intrusion Activities	3
1.2	Summary of the Research Problem	7
1.3	Main Research Question	8
1.4	Summary of Research Questions	8
1.5	Summary of Research Objectives	9
1.6	Summary of the (RP), (RQs), (ROs), and (RMs)	10
1.7	Summary of the Research Contribution	11
2.1	List of Papers Used for IPv6 Detection Technique Review	34
2.2	IPv6 Detection Technique Outcomes Review	36
2.3	List of Feature Used by Previous Researchers	39
2.4	Data Collection Environment Review	42
2.5	List of Evaluation Parameters Review	44
2.6	PSO SVM Feature Selection Technique Application	57
2.7	Test Data Criteria	59
3.1	Comparison between Nimda and Sasser Infection Scenarios	77
3.2	IPv4 Detection Techniques Using Three Selected Features	77
4.1	Testbed Device Information	85
4.2	IPv6 Packet Generated Traffic Pattern Scheme	87
4.3	The Coverage of the Selected Attacks	90
4.4	Summary of the Data Collection Schedule	92
4.5	Connectivity Test (Ping)	93
4.6	Packet Distribution Summary	94
4.7	ANOVA with Single Factor	97
4.8	Selected Features for Feature Analysis	101

© Universiti Teknikal Malaysia Melaka

TABLE	TITLE	PAGE
4.9	Number of Random One Minute Samples	103
4.10	List of Features Stored in Each Dataset	106
4.11	Dataset Generated by Elejla (2016)	108
4.12	List of Datasets	109
5.1	Datasets Used for Feature Analysis	112
5.2	Feature Analysis by using SIMv6	117
5.3	Features Selected for SigFeatv6	118
5.4	Authors Who Conducted a Study on an IDS Detection Technique in IPv6	120
5.5	Selected Authors for Feature Evaluation	121
5.6	Authors for Feature Evaluation	122
5.7	Dataset Prepared for Feature Evaluation	123
5.8	Feature Evaluation Results	128
6.1	Selected Authors for Feature Validation	134
6.2	t Test: Two Sample Assuming Equal Variances	135
6.3	The Most Significant Features for Different Attacks	137
6.4	Selected Authors for Feature Validation	138
6.5	Data Classification Result on SigFeatTIv6	139
6.6	Anova with Single Factor Result	140
7.1	Research Objectives Summarization	149
7.2	Research Contributions Summarization	152

© Universiti Teknikal Malaysia Melaka

LIST OF FIGURES

FIGURE	TITLE	PAGE
1.1	IPv6 Security Concerns Survey Results (Cerveny 2012)	6
1.2	Thesis Organization	13
2.1	General Intrusion Detection System Framework	19
2.2	Focus Area within Data Analysis Module	20
2.3	IDS Taxonomy or Classification (Amer and Hamilton Jr 2010)	21
2.4	Taxonomy for IDS Detection Technique	23
2.5	Network Based Intrusion Detection System	25
2.6	IDS Architecture	26
2.7	Pattern Analysis Module	27
2.8	New Pattern Construction Procedure	28
2.9	Most Concerning Threats in IPv6 (Jackson 2008)	30
2.10	Model of Generic Network Traffic	31
2.11	Feature Selection Process (Dash and Liu 1997)	47
2.12	Enhanced Feature Selection Process	49
2.13	PSO with SVM	53
2.14	Hyperplane through Two Different Classes	55
3.1	Research Methodology Used	64
3.2	Research Framework	66
3.3	Darpa Dataset Construction Benchmark	68
3.4	Feature Formulation Phase	69
3.5	An Analogy of Data Evaluation Process	71
3.6	The Research Process Flow	73
3.7	Network Layout for the Proof of Concept Testbed	76

© Universiti Teknikal Malaysia Melaka

FIGURE	TITLE	PAGE
4.1	Testbed Network Design	84
4.2	Time Interval Packet Distribution	96
4.3	Feature Formulation Process Flow	98
4.4	Common Features of IPv6 Packets	99
4.5	Data Smoothing Flowchart	104
4.6	Data Smoothing Procedure	107
5.1	SIMv6 Process Flow	114
5.2	The Process Flow of Feature Evaluation	119
5.3	Procedure of the Sub Data Preparation Process	124
5.4	Feature Implementation and Evaluation	125
5.5	Feature Evaluation Procedure	126
7.1	Research Process Flow	145

© Universiti Teknikal Malaysia Melaka

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	*SIMv6* Result For Data1 (Alive6)	184
B	*SIMv6* Result For Data1 (FloodRouter)	186
C	*SIMv6* Result For Data1 (Smurf6)	188
D	*SIMv6* Result For Data1 (CombineAttack)	190
E	*SIMv6* Result For Data2 (Alive6)	192
F	*SIMv6* Result For Data2 (FloodRouter)	194
G	*SIMv6* Result For Data2 (Smurf6)	196
H	*SIMv6* Result For Data2 (CombineAttack)	198

© Universiti Teknikal Malaysia Melaka

LIST OF ABBREVIATIONS

IDS	Intrusion Detection System
Timestamp	The original *time* value extracted from a captured packet
TimeInterval	Duration between arrival *times* of two consecutive *timestamp*
SrcIP	Source of IP address
SrcPort	Source of Port address
DstIP	Destination of IP address
DstPort	Destination of Port address
Protocol	The protocol value extracted from a captured packet
Hlim	Hop Limit
Nlength	Next length
Npayload	Next payload
TN	True Negative
TP	True Positive
FN	False Negative
FP	False Positive
FPR	False Positive Rate
Recall	Credibility measurement
Precision	Correct identification measurement
SVM	Support Vector Machine
PSO	Particle Swarm Optimization
SigFeatv6	The Significant Features in IPv6 (Proposed in this study)
SigFeatTIv6	The Significant Features in IPv6 with TimeInterval feature
SIMv6	Significant Feature Identification Mechanism for IPv6
TNR	True Negative Rate
TPR	True Positive Rate
TA	Total Accuracy

© Universiti Teknikal Malaysia Melaka

LIST OF PUBLICATIONS

A. Publications

Zulkiflee Muslim, Mohd Faizal Abdollah, Mohd Fairuz Iskandar Othman, Nur Azman Abu, and Shahrin Sahib. (2011). Behavioral Analysis on IPv4 Malware in both IPv4 and IPv6 Network Environment. *International Journal of Computer Science and Information Security (IJCSIS),* 9 (2).

Zulkiflee Muslim, Siti Azirah Asmai, Haniza Nahar, Zakiah Ayop, and Shahrin Sahib. (2011). Behavioral analysis on IPv4 malware on different platforms in IPv6 network environment. In: *IEEE International Conference Open Systems*. IEEE.

Zulkiflee Muslim, Robiah Yusof, Nur Azman Abu, and Shahrin Sahib. (2012). Improvising Intrusion Detection for Malware Activities on Dual Stack Network Environment. *World Academy of Science, Engineering and Technology (WASET),* 67 (International Science Index 67, 2012), pp. 536 544.

Zulkiflee Muslim, Haniza Nahar, Shahrin Sahib, and Mohd Khanapi Abd. Ghani. (2014). A Framework of IPv6 Network Attack Dataset Construction by Using Testbed Environment. *International Review on Computers and Software (IRECOS),* 9 (8), pp. 1434 1441.

Zulkiflee Muslim, Mohd Sanusi Azmi, Sharifah Sakinah Syed Ahmad, Shahrin Sahib, Mohd Khanapi Abd Ghani. (2015). A Framework of Features Selection for IPv6 Network Attacks Detection. *World Scientific and Engineering Academy Society (WSEAS) Transactions on Communications*.

© Universiti Teknikal Malaysia Melaka

CHAPTER 1

INTRODUCTION

1.1 Introduction

The objective of this chapter is to provide an overall view of this study. In this chapter, there will be a detailed discussion about the research problem, which will be solved toward the end of this study. Then, the research problem will be elaborated into the main research question. From the research question, the objectives of this study will be identified. After that, various limitations of this study will be underlined in the research scope. Next, the research design of this study will be explicitly explained. Subsequently, the research contribution of this study will be elaborated. Finally, a chapter summary is presented.

1.2 Research Overview

Internet Protocol version 6 (IPv6) was invented in 1998, as stated in the RFC (Request for Comments) 2460 (Deering and Hinden 1998). IPv6 is a new technology that is considered a successor to IPv4 technology. IPv6 was invented to overcome certain issues that were present in the previous technology. The main issue taken into serious consideration was the fact that IPv4 addresses are facing total depletion. Although a technique called Network Address Translation (NAT) has been proposed in the IPv4

© Universiti Teknikal Malaysia Melaka

network to overcome the address depletion issue, the solution is only a temporary one. Users are still demanding unique IP (Internet Protocol) addresses to be assigned to their nodes. The emergence of new technologies, such as the Internet of Things (IOT) (Xia et al. 2012), cloud computing (Zissis and Lekkas 2012), and wireless technology applications (Al Ameen et al. 2012), makes the need for IP addresses even more severe. Due to this issue, the Internet Engineering Task Force (IETF) drafted the first specification for IPv6 technology in RFC 2460 in 1998.

As the number of Internet users continues to increase, IANA is rarely able to allocate IP addresses to new users. As an alternative, the new IPv6 technology has been introduced to overcome the IP address space allocation issues. June 8, 2011 was World IPv6 Day, which was intended to encourage IPv4 Internet users to migrate to IPv6 Internet. There are some new features offered in IPv6 that are better than IPv4 (Reddy et al. 2012). Unfortunately, IPv6 is not backward compatible to IPv4. The IPv4 Internet and the IPv6 Internet are considered two different worlds. Users have to decide whether they want to use IPv4 or IPv6 to connect to the Internet.

Although IPv6 was officially launched in June 2011, many IPv4 users have been reluctant to migrate because they feel comfortable with the existing IPv4 protocol (Huston 2013). Based on a survey, only large companies participated in World IPv6 Day. Many other companies still lack adequate resources to adopt IPv6. Some of the limitations faced by these companies in 2011 included not having enough of a budget to purchase new devices that support IPv6. Furthermore, some companies did not have enough awareness of IPv6 technology to drive its adoption; they did not have the required knowledge or skills to implement IPv6 (Alhassoun and Alghunaim 2016). Finally, and most importantly, most of these companies remained unconvinced by the lure of IPv6 technology since it was still

© Universiti Teknikal Malaysia Melaka

new and might have had unexpected hiccups. IPv6 had not been fully tested on a large network scale prior to its launch (Trinh et al. 2010; Caicedo et al. 2009).

After both the IPv4 and IPv6 networks had been implemented, many users felt that the IPv6 services were not as good as those services offered in IPv4 (Han et al. 2014). Many researchers have invested a great deal of effort to enhance IPv6 implementation in order to offer better services. The main goal is to offer IPv6 services that are at least on par with the IPv4 network. Hence, research topics in the IPv6 domain are heavily focused on IPv6 services (Bagnulo et al. 2012; Gu et al. 2013; Mrugalski et al. 2013). Unfortunately, researchers may have focused too much on IPv6 services and implementations; consequently, security issues are currently overlooked or neglected. What is more, the new threats emerge for IPv6 network are need to be focused and the current security solution for IPv6 is needed to be improved (Hendriks et al. 2015).

Table 1.1: The Impact of Intrusion Activities

Company (Intrusion Activity)	**Year**	**Affected Items**	**Lost Information**	**Type of Loss**
CheckFree Corp. (Hacked Web Server)	2009	Personal information was stolen.	5,000,000 users	Intangible
Google.com (Stolen Documents)	2009	Documents were stolen.	< 0.05% of documents	Tangible
New York Mellon Corp. (Employee Theft)	2009	Company money was stolen by an employee.	> 1 million USD	Tangible
Spain (Plane Crash)	2008	The maintenance system malfunctioned.	Human lives	Intangible

Table 1.1 above shows some of the impacts from intrusion attacks based on several reports. According to Patel et al. (2010), the intrusion activities caused tangible losses by affecting millions of database records as well as by creating millions of victims from

© Universiti Teknikal Malaysia Melaka

different organizations and companies. These intrusion attacks also generated financial losses that amounted to more than 1.5 million USD from several affected organizations in 2009. Meanwhile, some of the intangible losses incurred from the intrusion activity that came in the form of people dying. Based on a claim made by Bellovin (2010), an intrusion attack caused a plane crash back in 2008. The plane crashed as a result of a maintenance system malfunctioning after it had been compromised by malware attacks. In yet another example, more than five million users were affected when a personal information data server was hacked. A study found that more than twenty new vulnerabilities are detected in computer networking products every month (Patcha and Park 2007). In 2005, a survey completed by several companies indicated that total financial losses due to intrusion attacks amounted to around 130 million USD (C.S. Institute and F.B.O. Investigation 2005). What is more, without proper monitoring mechanism some sensitive data for companies and employees also can be misused for bad purposes (Gupta et al. 2017). It is clear from all these facts that intrusion activities cannot be treated carelessly, as their impact might not only involve money but also human lives. Hence, an IDS should be implemented as one countermeasure mechanism that can be used to deal with intrusion activities.

1.3 Research Problem

The impact of an intrusion attack can be quite severe if the launched attacks are not treated seriously (CyberSecurity Malaysia 2013). Cyber Security Malaysia, in a joint venture with the Information Telecommunications Authority of Oman (ITA), organized a conference to discuss emerging threats with regard to the cyber world. This demonstrates the fact that cyber threats cannot be treated locally; instead, they need to be addressed on a global level. What is more, intrusion activities tend to gradually increase alongside the

© Universiti Teknikal Malaysia Melaka

rapid development of the information society (Zhang 2009). Unfortunately, current control mechanisms proved insufficient to content intrusive activities (Levitt and Dias 2017).

IPv6 has been designed to overcome several issues that occurred in IPv4, especially in terms of security. However, IPv6 per se is not a panacea for all the security issues that transpired with IPv4 (Alangar and Swaminathan 2013). Other aspects, such as network design, application design, and users' policies, also contributed to the network security issues as a whole. Some of the knowledge discovered in IPv4 can still be applied in the IPv6 network environment. However, some of the knowledge is considered inappropriate for use in IPv6 due to its new features. In these cases, the use of an Intrusion Detection System (IDS) as a detection mechanism in IPv4 is still an alternative solution that can be implemented in an IPv6 environment. Nevertheless, the detection techniques used in IPv4 do need to be verified before being deployed in the IPv6 network environment.

The process of implementing IDS in IPv6 is almost identical to the process for IPv4. The detection techniques used in IPv4 can be applied in IPv6, but the detection techniques constructed in the IPv4 environment cannot be transposed directly to the IDS in the IPv6 network environment. This is simply because the data pattern discovered was based on the IPv4 network environment and the network pattern in IPv6 differs from that of its predecessor (Peng et al. 2013). What is more, the detection techniques invented for IPv6 network were never being tested in full scale of real network (Barbhuiya et al. 2013). As a result, the detection techniques are insufficient to ease threats in the IPv6 network environment.

© Universiti Teknikal Malaysia Melaka