FLOW-REPRESENTATION APPROACH FOR ICMPV6-BASED DDOS ATTACKS DETECTION

OMAR E. O. ELEJLA

UNIVERSITI SAINS MALAYSIA

2018

FLOW-REPRESENTATION APPROACH FOR ICMPV6-BASED DDOS ATTACKS DETECTION

by

OMAR E. O. ELEJLA

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

April 2018

ACKNOWLEDGEMENT

With the name of Allah, Most Gracious, Most Merciful.

First and foremost, my sincere glorifications and adorations go to almighty Allah for his guidance, protection and strength over me to complete my research study. I would like to express sincere gratitude to my supervisors Associate Professor Bahari Belaton and Dr. Mohammed Anbar for their insightful guidance throughout the entire period of my research. I will forever remain grateful for the continued help, and wise counseling.

Indeed, without Allah then my parents' prayers, I could not have completed this research. My special thanks to my beloved parents for their continued supports, encouragements, and prayers. Thank you mum, dad, my brothers, and sisters, you are always in my mind and heart. In the same context, my deepest and special thanks go to my uncle Basem Alijla for her help, support and advises. Also, a special thanks for my best friend Mohammed Ferwana for his support and help. Your great support, efforts, and endurance is highly appreciated.

My sincere appreciations are extended to Universiti Sains Malaysia (USM) for its financial support under USM global fellowship program. I am also grateful to the School of Computer Sciences, USM which has provided all the facilities and equipments needed throughout my research. Last but not least; thank you to all my friends in Malaysia, Palestine and those who support me in any respect during my research.

TABLE OF CONTENTS

Acknowledgement ii

Table of Contents iii

List of Tables viii

List of Figures xi

List of Abbreviations xiv

Abstrak xvi

Abstract xviii

CHAPTER 1 – INTRODUCTION

1.1 Overview 1

1.2 Background 2

1.2.1 Internet Protocol version six (IPv6) 2

1.2.2 Internet Control Message Protocol version 6 (ICMPv6) 4

1.2.3 Detecting Network Intrusions 7

1.3 Research Problem 10

1.4 Research Objectives 12

1.5 Research Scope and Limitations 13

1.6 Research Contributions 14

1.7 Research Methodology 16

1.8 Thesis Structure 19

CHAPTER 2 – LITERATURE REVIEW

2.1 Introduction 21

2.2 Intrusion Detection Systems 21

2.2.1 Location-based Intrusion Detection Systems 23

2.2.1(a) Host-based Intrusion Detection System (HIDS) 23

2.2.1(b) Network-based Intrusion Detection System (NIDS) 24

2.2.2 Detection Model-based Intrusion Detection Systems 25

2.2.2(a) Signature-based Intrusion Detection System (SIDS) 26

2.2.2(b) Anomaly-based Intrusion Detection System (AIDS) 27

2.3 Related Works 29

2.3.1 Signature-based IDS for ICMPv6 Attacks 30

2.3.2 Anomaly-based IDS for ICMPv6 Attacks 34

2.3.2(a) Logic Rule-based AIDS 35

2.3.2(b) Learning-based AIDS 38

2.4 Datasets Issues and Representations 46

2.4.1 Dataset Representations 49

2.4.1(a) Packet-based Representation 49

2.4.1(b) Flow-based Representation 50

2.4.2 Existing IPv6 Datasets 53

2.4.3 Features Identification 57

2.4.4 Dataset Enrichment 58

2.5 Summary 59

CHAPTER 3 – THE PROPOSED FLOW REPRESENTATION APPROACH

3.1 Introduction 61

3.2 The Proposed Approach 62

3.2.1 Data Collection and Preprocessing Stage 64

3.2.1(a) Network Packets Capturing Step 64

3.2.1(b) ICMPv6 Packets Filtering Step........................... 65

3.2.1(c) Packets Attributes Extraction Step 67

3.2.2 Flow Construction and Basic Features Identification Stage......... 68

3.2.2(a) Flow Construction Step 70

3.2.2(b) Flow Aggregation Step 75

3.2.2(c) Flow Features Extraction Step............................ 78

3.2.3 Flow-based Dataset Validation Stage 81

3.2.3(a) Good Datasets Requirements Fulfillment Step 82

3.2.3(b) Detection Accuracy Checking Step 86

3.2.4 Data Enrichment Stage 87

3.2.4(a) Flows-based Enrichment Step 91

3.2.4(b) IP Behaviors-based Enrichment Step 92

3.2.4(c) Features Sets Combination Step 94

3.2.5 Flow-based Features Reduction Stage 96

3.2.6 ICMPv6-based DDoS Attacks Detection Stage 99

3.3 Summary.. 101

CHAPTER 4 – THE IMPLEMENTATION OF THE PROPOSED RESEARCH

4.1 Introduction 104

4.2 Tools and Programming Languages 104

4.2.1 Graphical Network Simulate 3 (GNS3)............................. 104

4.2.2 Wireshark 105

4.2.3 The Hacker Choice IPv6 (THC-IPv6) and SI6 Toolkits 106

4.2.4 WEKA 107

4.2.5 MySQL Database 108

4.2.6 NetBeans 109

4.3 Datasets Generation 110

4.3.1 Normal Traffic Generation....................................... 112

4.3.2 Malicious Traffic Generation 113

4.3.3 Datasets Preparation 116

4.3.3(a) Labeling 117

4.3.3(b) Normalization 117

4.3.3(c) Balancing 118

4.4 Design of the Proposed Approach 121

4.4.1 Data Collection and Preprocessing Stage 121

4.4.2 Flow Construction and Basic Features Identification Stage........ 126

4.4.3 Flow-based Dataset Validation Stage 131

4.4.4 Data Enrichment Stage 132

4.4.5 Flow-based Features Reduction Stage 141

4.4.6 ICMPv6-based DDoS Attacks Detection Stage 144

4.5 Summary 146

CHAPTER 5 – ANALYSIS OF RESULTS AND DISCUSSIONS

5.1 Introduction 148

5.2 Experimental Setup and Design 149

5.2.1 Hardware and Software Specifications 149

5.2.2 Hardwares 149

5.2.3 Softwares 150

5.2.4 Experimental Verifying of ICMPv6-based DDoS Attacks 151

5.3 Evaluation Metrics 153

5.4 Ground Truth Experiments 156

5.4.1 Ground Truth Experiment 1: The Impact of the Basic Flow Features 159

5.4.2 Ground Truth Experiment 2: The Impact of the Enriching Flow Features 163

5.4.3 Ground Truth Experiment 3: The Impact of the Feature Reduction 168

5.5 Comparisons with the Existing Packet-based IDSs 172

5.6 Datasets Comparison 182

5.7 Summary 185

CHAPTER 6 – CONCLUSION AND FUTURE WORK

6.1 Summary of Research Contributions 188

6.2 Achievement of Research Objectives 191

6.3 Direction of Future Work 193

REFERENCES 196

LIST OF TABLES

		Page
Table 1.1	The Scope of the Research	14
Table 2.1	Comparative Analysis of HIDS and NIDS	26
Table 2.2	Pros and Cons of SIDS and AIDS	28
Table 2.3	Summary of the Existing IDSs of ICMPv6-based DDoS Attacks	43
Table 2.4	A Comparison between Flow-based Representations and Packet-based Representations	52
Table 2.5	Comparison between the Existing IPv6 Datasets	55
Table 3.1	Examples of Stage One's Output	69
Table 3.2	Illustrative Example of an ICMPv6 Flow	74
Table 3.3	Aggregated Attributes Grouped Based on Justifications	75
Table 3.4	Examples of Flow Aggregation Step's Output	79
Table 3.5	Basic Flow Features with Their Description and Derivation	81
Table 3.6	The Extracted Enriching Features from Flows-based Enrichment Step with the Derivation Way	92
Table 3.7	The Extracted Enriching Features from IP Behaviors-based Enrichment Step with the Derivation Way	94
Table 3.8	The Set of Final Flows Features	96
Table 4.1	The ICMPv6-based DDoS attacks' commands by THC-IPv6 and SI6 Toolkits	107
Table 4.2	Scenarios of the Performed ICMPv6-based DDoS Attacks	115
Table 4.3	The Performed ICMPv6-based DDoS Attacks Scenarios	116
Table 4.4	Specifications of the Created Datasets	119
Table 5.1	Descriptions of the Evaluation Equations Terms	155

Table 5.2 The Used Classifiers With Their WEKA Names and Defaults Parameters 160

Table 5.3 The Classifiers Classification Accuracy of Flow-based Datasets with the Basic Flow Features Using Cross-Validation and Supplied Set 161

Table 5.4 The Classifiers False Positive Rates of the Flow-based Dataset with the Basic Flow Features Using Cross-Validation and Supplied Set 162

Table 5.5 The Classifiers Classification Accuracy of the Flow-based Dataset with the Final Flow Features Using Cross-Validation and Supplied Set 164

Table 5.6 The Classifiers False Positive Rates of the Flow-based Dataset with the Final Flow Features Using Cross-Validation and Supplied Set 166

Table 5.7 Results of Applying Two Feature Ranking Scheme to the Dataset with the Final Flow Features Set 169

Table 5.8 The Set of Selected Features after the Features Reduction Stage 170

Table 5.9 The Classifiers Classification Accuracy and False Positive Rates of the Flow-based Datasets with the Selected Features Using Cross-Validation and Supplied Set 171

Table 5.10 Comparison between the Classifiers Training Times before and after Features Reduction in Cross-Validation and Supplied Set 172

Table 5.11 Comparison between the Classifiers Detection Accuracy of the Packet-based IDSs and the Proposed Approach Using Cross-Validation and Supplied Set 173

Table 5.12 Comparison between the Classifiers False Positive Rates of the Packet-based IDSs and the Proposed Approach Using Cross-Validation and Supplied Set 176

Table 5.13 Comparison between the Classifiers Training Time (average) of the Packet-based Datasets and Flow-based Datasets Using Cross-Validation and Supplied Set 179

Table 5.14 Comparison between the Classifiers Training and Preprocessing Times of the Packet-based Datasets and Flow-based Datasets Using Cross-Validation and Supplied Set 180

Table 5.15 Comparison between the Proposed Approach and Previous IDSs in Term of the Included ICMPv6-based DDoS Attacks 181

Table 5.16 A Qualitative Comparison between the Proposed Flow-based Datasets and the Existing IPv6 Datasets 184

LIST OF FIGURES

Page

Figure 1.1 IPv6 Vulnerability Classes (Ard, 2004) 5

Figure 1.2 The Execution of DoS & DDoS Attacks 6

Figure 1.3 Number of Google IPv6 Users (Google, 2017) 8

Figure 1.4 The Overall Research Framework 17

Figure 2.1 The Main Areas of the Research Background and Literature Review 22

Figure 2.2 Snort Architecture (Schütte, 2014) 31

Figure 2.3 Bro Architecture (Sommer and Paxson, 2003) 32

Figure 2.4 Suricata IDS Architecture (Rietz et al., 2014) 33

Figure 3.1 The Architecture of the Proposed Flow Representation Approach 63

Figure 3.2 Flow Chart of ICMPv6 Packets Filtering 66

Figure 3.3 Flowchart of the Training and Testing a Classifier 87

Figure 3.4 Block Diagram of the Proposed Enrichment Technique 88

Figure 3.5 Block Diagram of the Applied Part of the Enrichment Technique 90

Figure 3.6 Flowchart of Features Sets Combination Stage 95

Figure 3.7 Flowchart of Stage Features Reduction 98

Figure 3.8 Detection Models Training and Testing Processes 100

Figure 4.1 The Design of the Testbed Topology 111

Figure 4.2 The Used Virtual Topology for Generating the ICMPv6-based DDoS Attacks 114

Figure 4.3 An Example of Dataset SMOTE Balancing Technique from WEKA 119

Figure 4.4 Design and Implementation of Stage One 122

Figure 4.5 The Collected and Filtered Traffic by Data Collection and Preprocessing Stage 123

Figure 4.6 Design and Implementation of Stage Two 126

Figure 4.7 Snapshot From MySQL Query of Constructing the Flows and Extracting Basic Flow Features 127

Figure 4.8 The Results of MySQL Query of Building the Flows and Extracting Basic Flow Features 128

Figure 4.9 Design and Implementation of Flow-based Datasets Validation in Stage Three 132

Figure 4.10 Design and Implementation of Stage Four 133

Figure 4.11 A Snapshot from MySQL Query of Constructing the Flows and Extracting Basic Flow Features Beside IPsrc_First_Seen Feature 134

Figure 4.12 A Snapshot from JAVA Code Used for Extracting Enriching Flow Features 135

Figure 4.13 A Snapshot of the Flow-based Datasets Traffic Represented Using the Final Flow Features 137

Figure 4.14 Design and Implementation of Stage Five 142

Figure 4.15 The Results of Features Ranking using Information Gain Ration and Chi-squared technique Rankers 143

Figure 4.16 Design and Implementation of Stage Six 144

Figure 4.17 Flow-based Dataset Represented Using the Selected Features 145

Figure 4.18 Splitting the Datasets in the Cross Validation and Supplied Set Testing Approaches 146

Figure 5.1 Flooding of RA Packets against Victim Machine Using THC-IPv6 Tool 151

Figure 5.2 The Neighbors Table of the Victim Machine 152

Figure 5.3 Resources Consumption of the Victim Machine 153

Figure 5.4 Experiments Methodology of the Conducted Evaluations Experiments 157

Figure 5.5 The Classifiers Detection Accuracies of the Flow-based Datasets with the Basic Flow Features and Final Flow Features 166

Figure 5.6 The Classifiers False Positive Rates of the Flow-based Datasets with the Basic Flow Features and the Final Flow Features 167

Figure 5.7 Comparison between the Classifiers Detection Accuracies of the Packet-based IDSs and the Proposed Approach Using Cross-Validation and Supplied Set 174

Figure 5.8 Comparison between the Classifiers False Positive Rates of the Packet-based IDSs and the Proposed Approach Using Cross-Validation and Supplied Set 177

LIST OF ABBREVIATIONS

AIDS	Anomaly-based Intrusion Detection System
BFF	Basic Flow Features
BPNN	Back-Propagation Neural Network
CHI	Chi-squared technique
CSV	Comma Separated Values
DDoS	Distributed Denial of Service
DoS	Denial of Service
EFF	Enriching Flow Features
FFF	Final Flow Features
GNS3	Graphical Network Simulate 3
HIDS	Host-based Intrusion Detection System
ICMPv4	Internet Control Message Protocol version 4
ICMPv6	Internet Control Message Protocol version 6
IDS	Intrusion Detection system
IETF	Internet Engineering Task Force
IGR	Information Gain Ration
IPSec	IP Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

KNN	K-Nearest Neighbors
MLD	Multicast Listener Discovery
NA	Neighbor Advertisement
NDP	Neighbor Discovery Protocol
NDPMon	NDP Monitoring
NIDS	Network-based Intrusion Detection System
NS	Neighbor Solicitation
OS	Operating Systems
OSI	Open Systems Interconnection
SVM	Support Vector Machine
RA	Router Advertisement
RD	Redirect
RS	Router Solicitation
SIDS	Signature-based Intrusion Detection System
SMOTE	Synthetic Minority Over-sampling Technique
STD	Standard Deviation
THC-IPv6	The Hacker's Choice IPv6
USM	Universiti Sains Malaysia

PENDEKATAN PERWAKILAN ALIRAN UNTUK PENGESANAN SERANGAN DDOS BERASASKAN ICMPV6

ABSTRAK

Selain dari peningkatan bilangan alamat protokol internet, IPv6 memperkenal beberapa fungsi baru seperti Protokol Penemuan Jiran (NDP) dan skim auto-konfigurasi alamat protokol internet yang banyak bergantung kepada Protokol Mesej Kawalan Internet versi 6 (ICMPv6). ICMPv6 diperturunkan tanggungjawab yang lebih daripada Protokol Mesej Kawalan Internet versi 4 (ICMPv4) dan ia dianggap sebagai tulang belakang serta komponen wajib dalam rangkaian IPv6. IPv6 terdedah kepada beberapa serangan yang diwarisi dari IPv4, termasuk beberapa serangan baru yang muncul bersama ciri-ciri barunya. Serangan IPv6 yang paling popular adalah Penafian Perkhidmatan (DoS) dan versi seleraknya (DDoS) yang menggunakan mesej ICMPv6. Serangan DoS & DDoS berasaskan ICMPv6 merupakan salah satu masalah besar Internet masa kini yang memberi impak kerosakan ekonomi dalam kes-kes serius. Sistem Pengesanan Anomali (AIDS) telah dicadangkan untuk menangani serangan DoS & DDoS berasaskan ICMPv6. Malangnya, sistem-sistem AIDS ini bergantung kepada perwakilan rangkaian trafik berasaskan paket sebagai input, yang mana perwakilan ini gagal untuk merekod sifat-sifat asasi serangan daripada aliran rangkaian trafik yang mengandungi unsur-unsur eksplotasi. Lebih-lebih lagi, sistem-sistem AIDS ini tidak dapat mengesan serangan secara tepat kerana kekurangan pertimbangan mereka terhadap ciri-ciri berkaitan serangan dan sifat tingkah serangan polimorfik. Di samping itu, dataset berkualiti rendah telah digunakan untuk melatih dan menguji AIDS sedia ada yang telah memberi impak kepada kejituan pengesanan mereka. Penyelidikan ini mencadangkan pendekatan yang dapat mengesan secara tepat serangan DoS & DDoS berasaskan ICMPv6. Pendekatan yang dicadangkan menggunakan perwakilan rangkaian trafik berasaskan aliran untuk mengatasi kelemahan perwakilan berasaskan paket. Perwakilan berasaskan aliran membina trafik rangkaian dengan merekodkan unsur-unsur penting dalam aliran/tingkah laku serangan DoS & DDoS berasaskan ICMPv6. Di samping itu, pendekatan yang dicadangkan mengenalpasti set ciri yang berkaitan yang akan digunakan untuk mengesan serangan serta memperkayakan ciri-ciri ini dengan ciri-ciri tingkah laku dan kontekstual untuk meningkatkan keupayaan pengesanan serangan. Perwakilan dan ciri baru ini digunakan untuk membina set data aliran ICMPv6 berlabel yang kemudiannya digunakan bagi tujuan penilaian pendekatan yang dicadangkan. Sebilangan eksperimen telah dijalankan ke atas perwakilan dan ciri yang dicadangkan dan penilian dilakukan ke atas tujuh set pengkelas. Kaedah ujian silang dan pengujian yang dibekalkan telah digunakan pada setiap eksperimen yang dijalankan. Hasil yang dicapai menunjukkan bahawa pendekatan yang dicadangkan mempunyai keupayaan pengesanan yang mantap dan tinggi dari segi ketepatan pengesanan (berkisar 97% hingga 99%) serta kadar positif palsu yang rendah (berkisar dari 0% kepada 2.7%) di kalangan pengelas. Selain itu, dataset yang dihasilkan telah ditunjukkan secara experiment mengatasi prestasi dataset sedia ada dan juga telah memenuhi keperluan dataset yang baik. Akhir sekali, kami telah terbitkan dataset berkenaan dalam talian untuk dicapai dan digunakan oleh penyelidik lain.

FLOW-REPRESENTATION APPROACH FOR ICMPV6-BASED DDOS ATTACKS DETECTION

ABSTRACT

In addition to the address expandability, IPv6 broughts new functionalities, such as Neighbor Discovery Protocol (NDP) and address auto-configuration scheme, which depends on Internet Control Message Protocol version 6 (ICMPv6) protocol. ICMPv6 is delegated with more responsibilities than Internet Control Message Protocol version 4 (ICMPv4) in IPv4, and it is considered the backbone and the mandatory part in IPv6 native networks. IPv6 is vulnerable to a number of attacks from IPv4, besides new attacks have appeared within its new features. The most popular IPv6 attacks are Denial of Service (DoS) and its distributed version (DDoS) that use ICMPv6 messages. ICMPv6-based DoS & DDoS attacks are one of the major problems of today's Internet, impacting economic damages in some serious cases. Anomaly Intrusion Detection Systems (AIDSs) have been proposed to address the problem of ICMPv6-based DoS & DDoS attacks. Unfortunately, these AIDSs rely on packet-based representations of the network traffic as their inputs, which fail to capture the nature of the attacks that consist of streams of malicious traffic. Moreover, these AIDS are unable to accurately detect the attacks due to their lack of considerations for the attacks related features and the attacks polymorphic behaviors. In addition, poor quality datasets have been used to train and test the existing AIDS which also impacting their detection accuracy. This research proposes an approach that is able to accurately detect ICMPv6-based DoS & DDoS attacks. The proposed approach uses a flow-based network traffic representation to overcome the limitations of packets-based representation. The flow-based representation constructs the traffic that capture the essential elements in the streams and behaviour of ICMPv6-based DoS & DDoS attacks. In addition, the proposed approach identifies a set of novel relevant features to be used for detecting the attacks as well as enriching these features with behaviour & contextual based features to further improve the attacks detection ability. The new representation and features are used to create labeled datasets of ICMPv6 traffic to be used for the evaluation purpose of the proposed approach. A number of experiments have been conducted on the proposed representation and features, and evaluated on a set of seven classifiers. Cross-validation and supplied set testing approaches have been applied on each of the conducted experiments. The achieved results show that the proposed approach have a robust and high detection ability in terms of the detection accuracy (ranges from 97% to 99%) while maintaining low false positive rates (ranges from 0% to 2.7%) among the classifiers. Moreover, the created datasets have been experimentally shown to outperform the existing datasets while fulfilling the good datasets' requirements. Finally, we have published the dataset online for other researchers to use.

CHAPTER 1

INTRODUCTION

1.1 Overview

Internet Protocol version 6 (IPv6) has been released to eventually replace Internet Protocol version 4 (IPv4)'s functionalities mainly due to the addresses exhaustion problem of the IPv4. IPv6 has delegated most of its core functionalities to the Internet Control Message Protocol version 6 (ICMPv6) which is considered as the main protocol for any IPv6 network to probably operate (Conta et al., 2006). However, ICMPv6 faces several implementation issues that need to be addressed including security threats. Wide-range of literature shows that ICMPv6 is vulnerable to different types of attack were exist in IPv4 such as Denial of Services (DoS) attack, besides a vector of new attacks (were not known in IPv4) that depend on the new features of IPv6 such as Duplicate Address Detection (Akamai, 2015; Barker, 2013).

One of the most serious and common attacks against ICMPv6 protocol is Distributed and Denial of Services (DoS & DDoS) attack due to their severity and disastrous impacts on IPv6 topology and infrastructure, where it consumes the bandwidth and resources of the victim in addition to its ease of performing (Satrya et al., 2015). According to Arbor Networks' 7th Annual Worldwide Infrastructure Security Report, the first DDoS attack against ICMPv6 protocol was discovered in 2011 and the percentage of these attacks are rapidly increasing year by year. Although a number of researches have been proposed to tackle this issue, it still has not been solved completely. Most of the proposed researches have low detection accuracy and do not cover all types of ICMPv6-based DoS & DDoS attacks. Therefore, these attacks are still a challenging problem for IPv6 researchers and security committees. As a result, there is a real need to propose an accurate detection mechanism for such attacks.

1.2 Background

The main focus of this research is to propose a new approach for detecting one of the serious IPv6 attacks which are ICMPv6-based DDoS attacks. This research is needed after the existing IDSs have been criticized in detecting these attacks which expose the IPv6 network to the danger. This section presents a background about the main topics of the research which are IPv6 and its security issues, ICMPv6 protocol and ICMPv6-based DDoS attacks, and the existing IDSs for ICMPv6-based DDoS attacks and their drawbacks.

1.2.1 Internet Protocol version six (IPv6)

In the 1990s, internet engineers realized that IPv4's pool of addresses is going to suffer from an exhaustion problem with the explosive increasing of internet attached devices. IPv4 address space consists of around 4 billion public IP addresses which are not enough to serve all devices in 2020 (expected to be 40.9 billion devices) (ABIresearch, 2014). As a result, Internet Engineering Task Force (IETF) started to think about a new alternative internet protocol, with a larger address space to replace IPv4. In 1998, they designed the next generation IP protocol (IPng) as a successor to IPv4 and it named later as IPv6 (Caicedo et al., 2009). IPv6 address is 128 bits, able to provide up to 3.410^{38} different addresses which are enough to serve every single atom in this world.

IPv6 is developed with a built-in security feature such as IP Security (IPSec) and end-to-end security technologies (Kent and Atkinson, 1998), therefore, it is slightly securer than IPv4. However, there are weaknesses and vulnerabilities that have been discovered in its structure/development which can be misused by attackers to achieve their goals. Moreover, attacking tools such as The Hacker Choice (THC) (Heuse, 2013) have been already published and have been successfully used to attack IPv6 networks. In addition, the security efforts provided by IPv6 over IPv4 still have several shortcomings and security issues in its implementation (Alangar and Swaminathan, 2013). The security issues exposed IPv6 to several kinds of attacks such as Denial of Services (DoS) attacks (Yang et al., 2007; Zeng, 2010). Convery and Miller (2004) reported that generally there are 13 classes of attacks, and all of them are possible in IPv6 either in the same, easier, or harder ways. In addition, there are new attacks that depend on IPv6 new features such as IPv6 Multicast Addresses which ease performing Reconnaissance attacks in IPv6 (Gehrke, 2012; Haberman and Thaler, 2002).

IETF developers included integrated security features as parts of IPv6 such as IPsec (Stockebrand, 2006) which aims to prevent some common attacks. Moreover, IPsec has been proved as an insufficient and non-trustworthy technique. Therefore, several security mechanisms have been proposed in order to provide more security to IPv6 (Barbhuiya et al., 2011). One of these mechanisms is defined in RFC 3971, named SEcure Neighbor Discovery Protocol (SEND) to protect ICMPv6 neighbor discovery messages (Arkko et al., 2005; Nikander et al., 2004). However, a number of researchers have criticized SEND mechanism as it is highly consuming resources and bandwidth (AlSa'deh and Meinel, 2012; An et al., 2007; Gelogo et al., 2011; Supriyanto et al., 2013; Weber, 2013). Therefore, IPv6 is still vulnerable to different threats and needs more security efforts to be done.

1.2.2 Internet Control Message Protocol version 6 (ICMPv6)

Internet Control Message Protocol 4 (ICMPv4) is an optional protocol for IPv4 implementation and can be blocked or dropped on the gateways unlike IPv6 implementation where ICMPv6 is a core and compulsory protocol. One of the major changes in IPv6 compared to IPv4 is its high dependency on ICMPv6 protocol (Conta et al., 2006). ICMPv6 messages have to be fully implemented in any IPv6 nodes to have the essential services of it. ICMPv6 is responsible for the same functionalities of ICMPv4 besides other new functionalities that were the responsibilities of IPv4's separate protocols such as Address Resolution Protocol and Internet Group Management Protocol. Moreover, ICMPv6 has new core functions that were shipped with IPv6 such host address Auto-configuration (Thomson et al., 2007) and Neighbor Discovery Protocol (NDP) (Narten et al., 2007). Therefore, it is considered as the backbone and the most important part of IPv6 (Weber, 2013).

ICMPv6 has two types of messages which are Informational Messages and Errors Messages. The first type is used for sharing information between nodes to implement tests, diagnostics and support critical functions. Errors Messages are generated as responses to any errors occur during the delivery of an IPv6 message (Conta et al., 2006). Although the importance of these messages for IPv6 networks, they are misused to perform several types of attacks that have been mentioned in the literature (Hogg and Vyncke, 2008; Raghavan and Dawson, 2011; Weber, 2013). For example, ICMPv6 Redirect message can be misused by attackers to perform Man In The Middle (MITM) attack as mentioned in Kim et al. (2007).

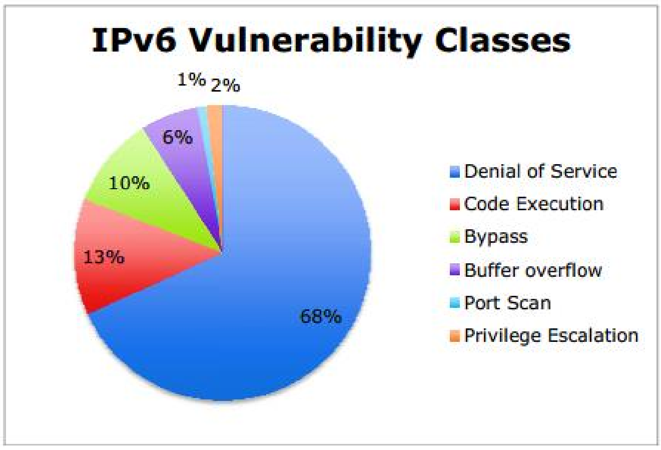

Figure 1.1: IPv6 Vulnerability Classes (Ard, 2004)

One of the most common attacks against IPv6 and ICMPv6 is Denial of Services (DoS) attacks as shown in Figure1.1. DoS attacks aim to limit the access or stop the services from legitimate users of the targeted machine by overwhelming it with many packets in a short time in order to exhaust its resources. There is another more serious form of DoS attack, named Distributed Denial of services (DDoS) attack. In DDoS attack, the attacker sends its malicious packets simultaneously from controlled (distributed) zombie devices. The diversity of the attack sources helps the attacker to avoid the detection as well as increasing the number of packets that can reach the victim. Figure1.2 illustrates the execution of both DoS and DDoS attacks. DoS & DDoS attacks are considered popular attacks because they are difficult to be eliminated by network administrators, in addition, it requires a small effort from attackers (e.g. single command) to be performed. In this thesis, ICMPv6 DoS attack is considered as a form of ICMPv6 DDoS attack that is performed from a single source. Therefor, ICMPv6-based DoS and DDoS will be referred as ICMPv6-based DDoS attacks.

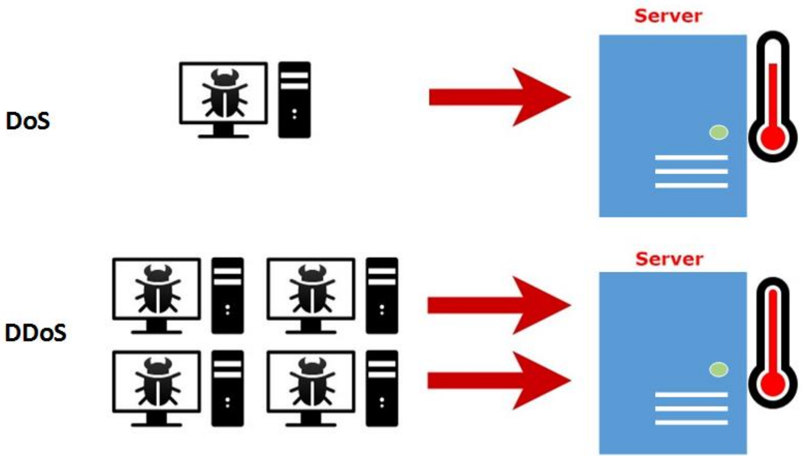

Figure 1.2: The Execution of DoS & DDoS Attacks

The deployment of IPv6 in real networks shown that many DDoS attacks are still possible in IPv6 by the same ways that were used in IPv4 such as flooding of ping request packets (Yang et al., 2007). These attacks are performed by exploiting the new characteristics of ICMPv6 protocol. For example, based on the characteristics of ICMPv6 protocol that a node has to respond for any ICMPv6 Neighbor Solicitation (NS) message received with an ICMPv6 Neighbor Advertisement (NA) message. Therefore, in the case of a big number of NS messages sent to a single node, it should reply to all these messages. That will consume a portion of the victim node's resources or may cause a complete stopping of its services while it trying to respond to the malicious messages Saad et al. (2016).

Generally, ICMP is classified as a simple protocol and lack of security awareness thus, it is vulnerable to various types of attacks. Therefore to avoid its attacks, there was a common reaction applied by IPv4 network administrators which is to block the protocol by dropping all its messages. However, administrators of IPv6 networks are not able to use such these rules (reaction) due to the ICMPv6 highly relevance for the correct functioning of IPv6 networks. In other words, IPv6 networks are not able to operate without the ICMPv6 protocol to be allowed and supported in the networks (Weber, 2013). Therefore, the only way to avoid ICMPv6 vulnerabilities is to deploy a detection system within the network to monitor and detect the abnormal behaviors of ICMPv6 that leads to detect the attacks against it.

1.2.3 Detecting Network Intrusions

According to Google's statistics, the number of its users that are using IPv6 is increasing daily as shown in Figure 1.3. In addition, IPv6 users are increasing around the world such as in Belgium, the number of IPv6 reached to 48.3% (Akamai, 2017). Moreover, several companies have enabled IPv6 for their users such as Dropbox which is serving 15% of its daily user requests in IPv6 globally (Haowei, 2017). As well as the number of IPv6 enabled users and networks is increased day by day, the number of IPv6 attacks is increased too. One of the possible ways to detect IPv6 attacks is to monitor the network traffic looking for any illegal traffics or behaviors which are called Intrusions. As well as security experts improve their IDSs, attackers are improving their attacking techniques besides new techniques to avoid being detected. Therefore, IDS should be intelligent enough to differentiate between normal and abnormal behaviors.

Intrusion Detection Systems (IDSs) can be applied to two different representation forms of input traffic which are packet-based and flow-based representations. Based on the input representation, IDSs are categorized into packet-based and flow-based IDSs. Packet-based IDS depends on the traditional analysis of the whole traffic including packets headers and payload. Flow-based IDSs transform the packets traffic into flows which are defined as sequences of packets carrying same characteristics. Each flow

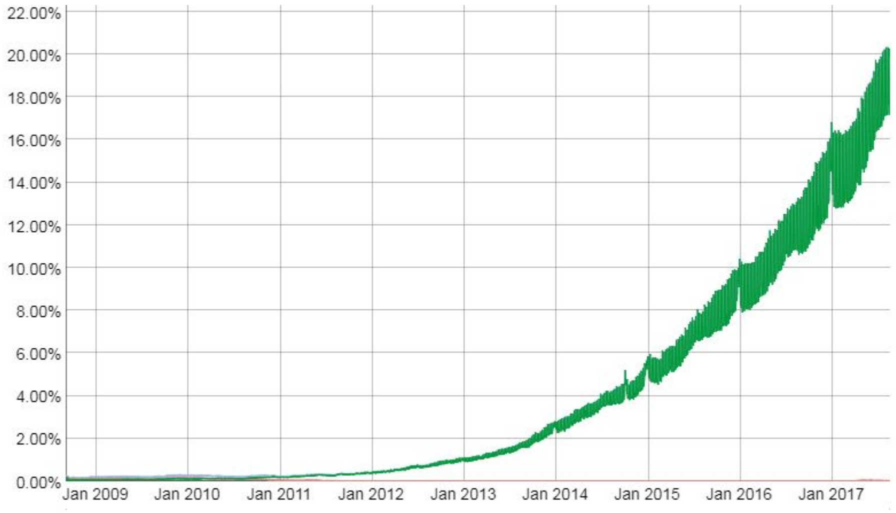

Figure 1.3: Number of Google IPv6 Users (Google, 2017)

represents information about similar packets thus it would be more useful and informative in case of attacks such as ICMPv6-based DDoS attacks. Moreover, flow-based representation helps to reduce the traffic volume especially with the current high-speed networks that are attached to an incrementing number of devices (Northcutt and Novak, 2002). In addition, flow-based representation has been applied to detect DDoS attack in different previous researches and it proved it detection efficiency with high performance (Gao et al., 2006).

Moreover, the IDSs' used detection mechanisms classifies them into two classes first, Signature-based IDSs (SIDS) and Anomaly-based IDS (AIDS). SIDSs depend on a pattern for each attack that indicates about the attack appearance. Second, AIDSs depend on the behaviors of the attacks rather than signatures. SIDS is unable to identify any unseen-before (zero-day) attacks because their signatures (pattern) are not recorded in the SIDS database. Therefore, the best choice for detecting ICMPv6-based DDoS attacks is to develop an AIDS that recognizes the behaviors of the attacks and provides the ability to detect unknown attacks on the contrast of SIDS.

Many AIDSs have been developed based on different techniques such as file system checking, statistics profiles, rules profiles and Auto learning. AIDSs work based on the assumption that intrusions generate abnormal activities indicate their existence, thus they try to differentiate between the normal and abnormal behaviors. Therefore, AIDS is considered as a classification problem that aims to train a model to learn how to differentiate between normal and malicious traffic. Learning techniques are considered as the most efficient techniques for building these models due to their ability to automate the process of building the detection model and to diminish human effort required to build these model (Shamshirband et al., 2013). Therefore, AIDSs extensively use auto learning techniques in their detection which proved their ability to accurately detect attacks on many computer networks.

The learning-based AIDS systems build a detection model by organizing (representing) the traffic behaviors based on a set of features. If these features are identified correctly the anomalies detection will have a high accuracy as well as low false positive rate of alerts. These features are used to represent the input traffic of the learning techniques in order to organize it for the techniques. To the best of the author's knowledge, there are no such published features that might be used to represent ICMPv6-based DDoS attacks' traffic. Therefore, to propose a learning-based technique for detecting such attacks, there is an initial need which is to investigate and study the behavior of these attacks traffic and identify a set of features that have different behavior in the attack traffic from the normal traffics.

1.3 Research Problem

ICMPv6 protocol is a compulsory and major part of IPv6, it is responsible for core functions (such as resolving IPv6 addresses) between IPv6 nodes (such as routers, servers, PCs, etc.). Therefore, IPv6 cannot operate without the ICMPv6's functions (Conta et al., 2006). The ICMPv6 protocol is vulnerable to several attacks including DoS & DDoS which are considered as serious and common attacks. ICMPv6-based DDoS attacks negatively impact the victim network resources which might reach to prevent its services. Moreover, these attacks are easy to perform as there are published attacking tools to perform them using a single command. Therefore, in order to support this lack of security in ICMPv6 implementation, an accurate IDS is needed for detecting these attacks to avoid their damage.

The existing IPv4 IDSs are unable to detect ICMPv6-based DDoS attacks because they are unable to filter and inspect IPv6 packets due to the structures differences. Some fields of IPv4 packets header are no longer exist in IPv6 packet header besides others fields are added in IPv6 packets header that do not exist in IPv4 packets. In addition, number of SIDSs have been proposed for IPv6 which are limited to few signatures of known attacks therefore, they cannot detect new IPv6 attack with unknown signatures (see Section 2.3.1). Moreover, few AIDSs have been exclusively proposed for IPv6 attacks using irrelevant packet-based representation (see Section 2.3.2) but they still cannot be considered as trustworthy reliable IDSs for ICMPv6-based DDoS attacks due to the following shortcomings.

- The existing AIDSs of ICMPv6-based DDoS attacks depend on a packet based representation of the traffic. Packet-based representation is irrelevant to the nature of DDoS attacks as discussed in Section 2.4.1 besides it leads to unreliable detection of the attacks as experimentally illustrated in chapter 5. Moreover, this representation increases the processing time and complexity of the approach due to the huge amount of traffic needs to be analyzed (Sperotto et al., 2010).

- The existing AIDSs of ICMPv6-based DDoS attacks have low detection accuracy because they depends on non-qualified packet-based features (represent the traffic) that do not contribute in detecting DDoS attacks robustly (see Section 2.3.2(b)). Having a good set of features for attack helps to accurately detect it besides it is used for comparisons of different detection approaches. ICMPv6-based DDoS attacks do not have a defined set of features that are related to them to be used for these aims in addition to the training and parameter tuning of any proposed IDS.

- The existing AIDSs of ICMPv6-based DDoS attacks are trained and validated using unreliable and poor quality datasets (few attack scenarios, unlabelled traffic etc.) due to the lack of benchmark datasets (see Section 2.4.2). Therefore, their achieved detection accuracies do not reflect the AIDSs ability in the case of online detection scenarios as experimentally illustrated in chapter 5.

- The existing AIDSs of ICMPv6-based DDoS attacks do not consider all the possible scenarios of ICMPv6-based DDoS attacks, therefore, they suffer from high rate of false alarm. For example, (Saad et al., 2014a)'s IDS is limited to a DDoS attack of ICMPv6 message which is performed using Echo Ping Request messages.

Moreover, as an initial need for proposing IDS systems is to have reliable datasets to be used for testing the validation of new approaches, comparison of different approaches, training, and parameter tuning. These datasets should include a normal traffic beside a malicious traffic of the targeted attacks to check the ability of the IDSs to differentiate between the two traffics. To our best of knowledge, there are no available reliable datasets for ICMPv6-based DDoS attacks for these purposes. Moreover, the datasets should have representative and informative features that are related to the targeted attack. ICMPv6-based DDoS attacks have a lack of such features to be extracted.

As such an IDS to detect ICMPv6-based DDoS attacks is a must to secure the next generation protocol IPv6. Therefore, this research aims to propose a flow-based IDS to represent the traffic in a suitable representation as well reduce the amount of input traffic. In addition, it creates flow-based datasets to be used as references by other researchers for evaluating any proposed IDSs. Furthermore, a set of representative features for ICMPv6-based DDoS attacks are extracted for accurately detecting them and to be the base for any proposed approach for such attacks.

1.4 Research Objectives

The main goal of this research is to propose a flow representation approach to accurately detect ICMPv6-based DDoS attacks. In support of this main goal, this research seeks to achieve the following objectives:

- **Research Objective 1 (RO1)**: To define a suitable formulation of ICMPv6 traffic to represent the traffic in a way that makes the attacks detectable and noticeable for any applied security approach. This objective aims to replace the existing irrelevant packet-based representation.

- **Research Objective 2 (RO2)**: To study the flows characteristics of ICMPv6-based DDoS attacks and their behaviors in real scenarios in order to identify a set of the most relevant features that can be used to differentiate between the attack flows and the normal ICMPv6 flows. These features should be qualified to overcome the issue of the used features in the existing packet-based approaches.

- **Research Objective 3 (RO3)**: To create realistic flow-based datasets that includes ICMPv6-based DDoS attacks and normal ICMPv6 traffic in order to be used for validating our approach's detection performance and to be a reference (validated) for other researchers for the same usage in addition to the comparison purposes. These objective is needed due to the unavailability of benchmark datasets.

- **Research Objective 4 (RO4)**: To propose a new enrichment technique able to extract new informative features from a network to be added in order for increasing the quality of input datasets and other purposes such as false alert reduction (see Section 3.2.4).

- **Research Objective 5 (RO5)**: To come up with a features reduction scheme to choose the best subset of flow-based features. This scheme is applied to the two sets of flow-based features that are proposed in objectives two and four (see Section 3.2.5).

1.5 Research Scope and Limitations

This research is limited to detect types of IPv6 attacks which are DoS & DDoS attacks that are using ICMPv6 messages as the medium for their traffic. ICMPv6 is a network layer protocol in the OSI model, therefore, any attack that is targeting other layers are out of this research scope. The proposed approach does not contain any database for attack signatures thus it is categorized under the anomaly-based IDSs. The generated datasets are flow-based datasets contain malicious traffic that is generated from two different attacking tools which are THC-toolkit and SI6 tools. The evaluation metrics that are used in this research are the detection accuracy and the false positive rates of detecting the targeted attacks. Table 1.1 summarizes the scope of this research.

Table 1.1: The Scope of the Research

Item	**Scope**
Environment	Internet Protocol version 6 (IPv6)
Protocol	Internet Control Message Protocol version 6 (ICMPv6)
Attacks	ICMPv6-based DDoS attacks
Targeted Layer	Network Layer
System Type	Anomaly-based Intrusion Detection (AIDS)
Datasets	Realistic flow-based datasets
Attacking Tools	THC-toolkit and SI6
Evaluation	Detection Accuracy and False Positive Rates

1.6 Research Contributions

The main contribution of this research is an approach for accurately detecting ICMPv6-based DDoS attacks based on flow representation of the traffic. The approach depends on a set of flow-based features that have been identified by studying the attacks behaviors in networks. The performance of the approach was improved by integrating an extra set of informative features that has been extracted from an enrichment technique which was also proposed in this research. The research's contributions are as follows:

1. A new flow-based representation of ICMPv6 traffic that formulates the ICMPv6

traffic in a relevant way to the attacks' nature which leads to discriminate the attacks from normal flows.

2. A set of basic flow-based features that is able to differentiate between the behaviors of attack flows and the normal flows. These features are considered as novel features as they are the first figured out features for such attacks.

3. Reference realistic datasets based on the flow-based representation and features for approach validation purposes of the detection performance of ICMPv6-based DDoS attacks. These datasets are generated to be used to achieve the main goal of this research as well as to be publicly available for IPv6 researchers to test their proposed approaches. The proposed datasets have been published on a website (Elejla et al., 2017).

4. An enrichment technique that is able to extract more relevant features from the network to improve the detection ability. The technique is used to enrich the datasets before applying the attacks detection system. Moreover, the extracted features are used to reduce the false alarm produced from the detection system. It successfully helps to improve the detection accuracy of such attacks after combining them with the previous basic features.

5. features reduction scheme using feature ranking algorithms to choose the best subset of flow-based features from the two features sets that are extracted in Contributions two and four. This subset of features has the ability to keep the detection performance as well as reduce the time needed to build the detection models compared to contribution four.

1.7 Research Methodology

This research has been conducted based on different stages of theoretical and experimental analysis to study proposing a new security approach of IPv6. In the first stage, detecting DDoS attacks of the ICMPv6 protocol is decided to be our main goal for this research due to its importance to IPv6. To achieve this objective, Several methodological steps are employed which are as follows: reviewing literature of this research, (2) study the existing representations of traffic and attacking tools, (3) generate datasets to be used by our research and other similar researches, (4) identify a set of features to be used as the base for the detection of our approach, (5) propose and apply an enrichment method to extract more informative features in order to increase the detection performance, (6) evaluate our approach and the enrichment method by applying different classification techniques then calculate and compare detection accuracies and false positive rates. Figure 1.4 depicts the overall research framework stages.

In the first stage, several studies of IPv6 standard and its attacks have been done to understand the protocol and the most vulnerable parts of it. ICMPv6 protocol has been chosen in this research due to the main functions that are under its responsibilities besides the high usage of these attacks against IPv6. After ICMPv6-based DDoS attacks were chosen as the targeted attacks, the existing researches for these attacks have been studied to explore their drawbacks and define the research gap. The outputs of this stage were to identify the problem statement and the main goal of the research.

In the second stage, this stage can be named as preparation for the third stage of datasets generation. This stage focuses on investigating the current traffic representation types to choose one to be used for building the datasets (see RO1). Also, this stage

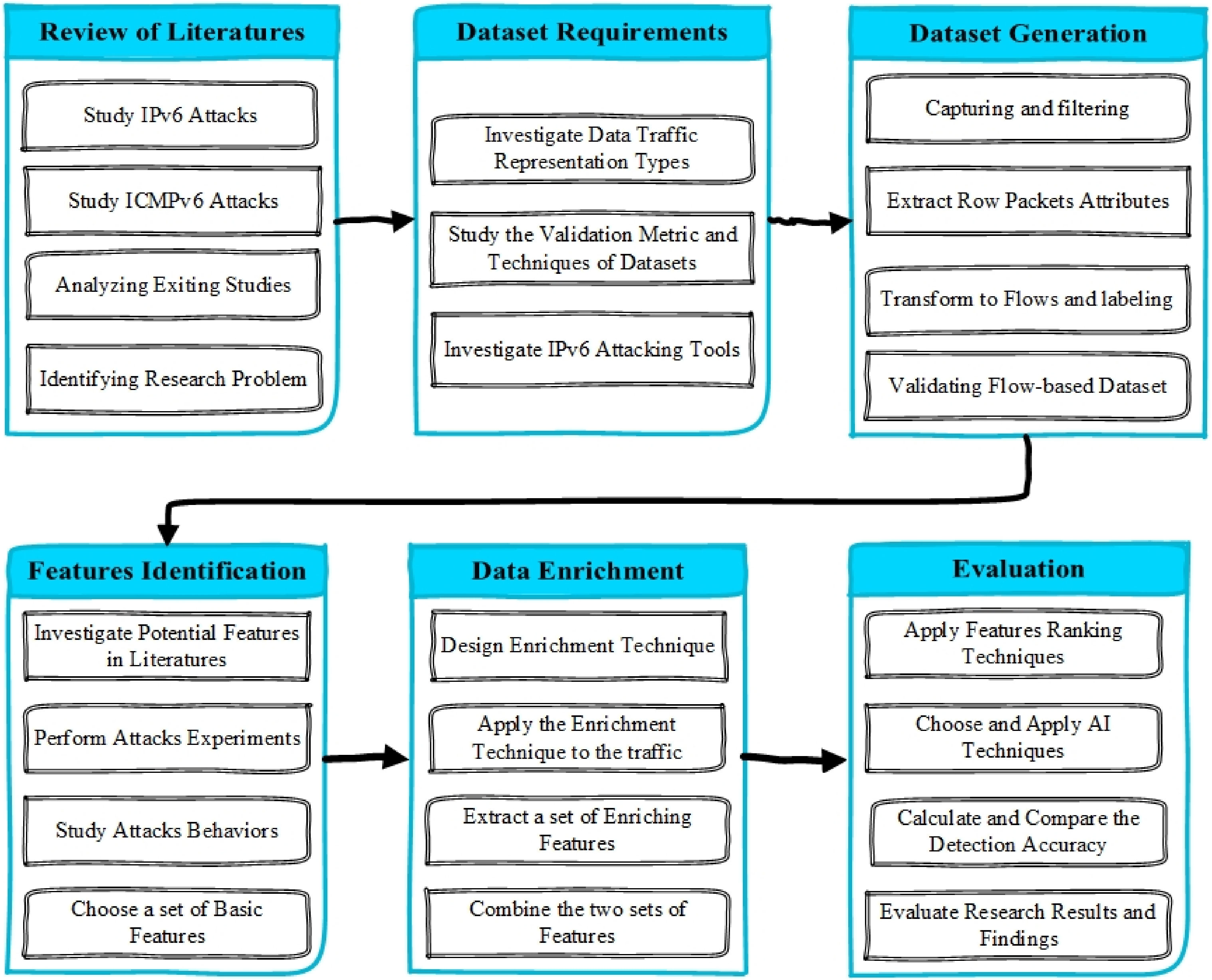
Review of Literatures
Study IPv6 Attacks
Study ICMPv6 Attacks
Analyzing Exiting Studies
Identifying Research Problem
Dataset Requirements
Investigate Data Traffic Representation Types
Study the Validation Metric and Techniques of Datasets
Investigate IPv6 Attacking Tools
Dataset Generation
Capturing and filtering
Extract Row Packets Attributes
Transform to Flows and labeling
Validating Flow-based Dataset
Features Identification
Investigate Potential Features in Literatures
Perform Attacks Experiments
Study Attacks Behaviors
Choose a set of Basic Features
Data Enrichment
Design Enrichment Technique
Apply the Enrichment Technique to the traffic
Extract a set of Enriching Features
Combine the two sets of Features
Evaluation
Apply Features Ranking Techniques
Choose and Apply AI Techniques
Calculate and Compare the Detection Accuracy
Evaluate Research Results and Findings

Figure 1.4: The Overall Research Framework

studied the requirements that should be included in the created datasets to be valid for testing our research. Tools that are used to penetrate the targeted attacks are studied also; these tools are used to generate malicious traffic in the datases (see RO3).

In the third stage, realistic datasets have been created by collecting row packets normal traffic in addition to the traffic of ICMPv6-based DDoS attacks. Moreover, these traffics are preprocessed and transformed to the flow-based datasets. These dataset are labeled based on our knowledge of the traffic characteristics such as the times and IP addresses that are used to performed the attacks. Moreover, this stage includes validating these datasets (to achieve RO3) to be considered as reference and good datasets for our research and others.

In the fourth stage, it focuses on identifying a set of features to be used for the detection of ICMPv6-based DDoS attacks. These features are mainly identified by either investigating similar literature trying to adopt their features in our research or by studying the differences between normal and ICMPv6-based DDoS attack flow behaviors by conducting attacking experiments. The output from this stage is a set of flow basic features that achieve RO2 which are used to represent the flow-based datasets.

In the fifth stage, data enrichment technique is proposed to be another source of extra informative features that can be added for several useful purposes. To achieve this research's RO4, the enrichment technique is used to extract more relevant features in order to increase the approach's detection performance of ICMPv6-based DDoS Attacks. These features are extracted either from the network about its characteristics and resources, addresses, or the flows traffic itself.

In the sixth stage, feature ranking techniques is the RO5, are applied to choose a final set of features from the two sets that have been extracted in the previous steps. Classification techniques are applied to the datasets with the selected set of features. The output of this step is a detection model to accurately detect the ICMPv6-based DDoS attacks. In order to comparatively evaluate the research, its detection accuracy, and the false positive rates are compared with other similar researches in detecting the attacks. Finally, the research findings and results are evaluated to ensure that the research objectives are completely achieved.

1.8 Thesis Structure

The remaining parts of this thesis are structured as follows:

Chapter 2 *(Literature Review)*: This chapter presents a comprehensive survey of the existing detection systems of ICMPv6-based DDoS attacks. The available datasets representations are also presented besides a survey of the existing IPv6 datasets that are used for security purposes.

Chapter 3 *(The Proposed Flow Representation Approach)*: This chapter gives detailed description of the proposed flow representation approach. In addition, it describes the integrated stages of the approach besides the used algorithm for detecting the ICMPv6-based DDoS attacks

Chapter 4 *(The Implementation of The Proposed Research)*: This chapter presents the utilized tools and software which are used to design the proposed approach. Moreover, it compromise the designing principles of the datasets besides their preparations steps. Lastly, it illustrates the design and implementation of the proposed approach's stages

Chapter 5 *(Analysis of Results and Discussions)*: This chapter describes the setup and design of the experiments which aim to evaluate the proposed approach's stages. The results of the conducted experiments are also presented in this chapter. In addition, comparisons between the proposed approach and the existing IDSs are presented. Lastly, a comparison between the proposed datasets and the available IPv6 datasets is given in this chapter.

Chapter 6 *(Conclusions)*: This chapter presents the concluding remarks and summary of the research key findings. Moreover, it discuses the futureworks the can be further studied to improve the proposed approach.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter surveys the literature and the related studies of ICMPv6-based DDoS attacks detection. In addition, it analyzes the advantages and disadvantages of the existing works and highlights the drawbacks and limitations for each of them. These drawbacks and limitations motivated the development of the proposed flow representation approach. This chapter also studies the generation and validation requirements of the proposed datasets for testing and evaluating the proposed approach. Traffic representation techniques have been discussed and criticized in this chapter as well. In addition, The chapter shows and criticizes the drawbacks of the existing IPv6 datasets and studies their ability to meet this research requirements. Figure 2.1 explains the main areas of the research background and literature review.

2.2 Intrusion Detection Systems

Definition and purpose: Intrusion detection is the process of monitoring and analyzing network's traffic looking for any indicator of intrusion existence. Intrusion Detection System (IDS) is the responsible application for automating these tasks for a network or node that it is installed on (Scarfone and Mell, 2007).

The first published study of intrusion detection was in the 1980s and the researchers continue proposing new IDSs till these days to cope with the newly discovered tech-

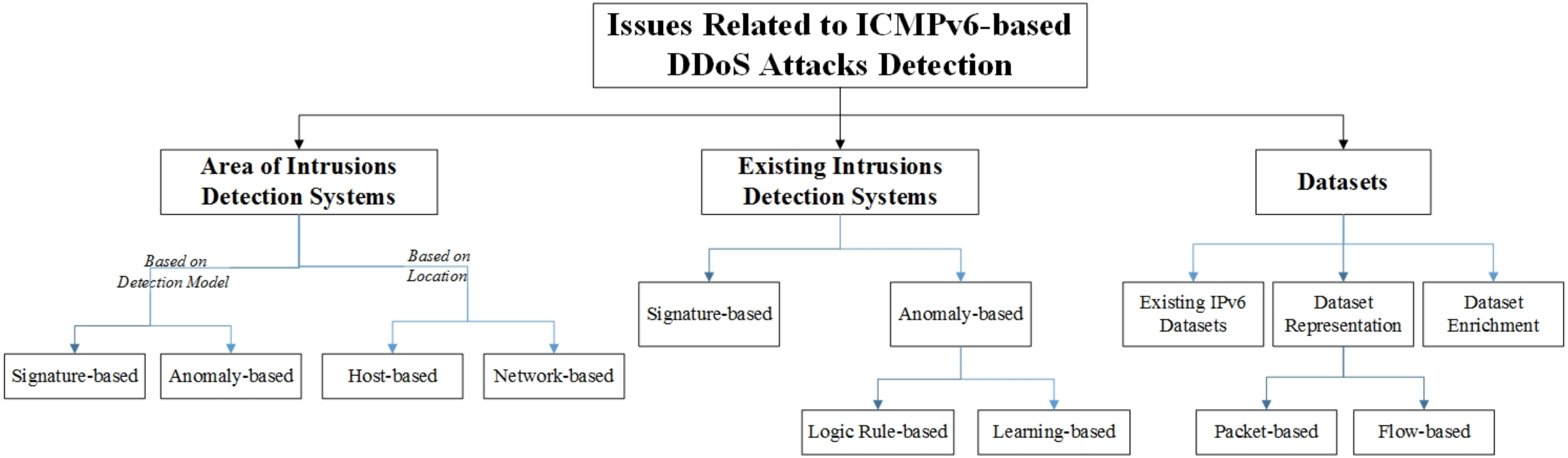

Figure 2.1: The Main Areas of the Research Background and Literature Review

niques of attack. Many different classifications of the IDSs schemes have been presented. The most common classification of IDSs is based on the installation location of the system.

2.2.1 Location-based Intrusion Detection Systems

On the light of IDS's location, the IDSs are distinguishable into two classes; Host-based Intrusion Detection System (HIDS) and Network-based Intrusion Detection System (NIDS). In addition, Amer and Hamilton (Amer and Hamilton, 2010) added one more class which is a combination of both HIDS and NIDS classes. These two classes and the differences between them are discussed in the following subsections.

2.2.1(a) Host-based Intrusion Detection System (HIDS)

The decision of the intrusion detection is affected by the place that the system is installed on. HIDS is installed in a host device to detect intrusions based on analyzing the audit data such as host log files, user activities, kernel system files, running processes, and etc., looking for any indication of abnormal activities. According to Lunt et al. (1989), HIDS has the advantage of giving the information in the form of "who access what" that gives the possibility of tracking the attackers back when needed. Moreover, the amount of information that needs to be analyzed is less and limited compared to NIDS because the operating systems and application generate less data compared to busy links in a network (Vigna and Kruegel, 2005). Also in term of attacks response, HIDS is much better due to its direct control access to the running processes so it has the ability for easily identified the attack processes and terminate them.

On the other side, HIDSs have a set of limitations that are preventing them from being the best choice of IDSs. The main limitation is that they can be disabled or falsified if the host that it is running on, is compromised (Vigna and Kruegel, 2005). This happened because of all or nothing approach that is used in most of the Operating Systems (OS). This approach allows the processes to change any kernel aspect of the OS system or the stored codes of the programmable hardware once it gains administrative privileges. Moreover, HIDS may considerably affect the OS's performance and availability by consuming the host machine resources. Last disadvantage of HIDS is that it has to be compatible with the heterogeneous platforms that it might be installed on.

2.2.1(b) Network-based Intrusion Detection System (NIDS)

NIDS is another type of IDSs that has an overall view of monitoring the incoming and outgoing traffic from a network to detect any indicator of attack or suspicious activity. In NIDS, a monitor node is set to "Promiscuous" mode to monitor the traffic of a number of hosts without affecting their connectivity or performances (Valeur et al., 2004). Therefore, it can detect the attacks that targeting more than one host even if the indicators that are collected in a single host are insufficient for recognizing the attacks. Moreover, NIDS is considered as a low-cost IDS compared to HIDS which needs to be installed in every node of the network which might be heterogeneous with various OSs with different specifications. Therefore, the deployment and maintenance of a single NIDS are less costly than for many heterogeneous HIDSs to protect one network (Vigna and Kruegel, 2005).