ICMPv6 ECHO REQUEST DDoS ATTACK DETECTION FRAMEWORK USING BACK-PROPAGATION NEURAL NETWORK

REDHWAN MOHAMMED AHMED SAAD

UNIVERSITI SAINS MALAYSIA

2016

ICMPv6 ECHO REQUEST DDoS ATTACK DETECTION FRAMEWORK USING BACK-PROPAGATION NEURAL NETWORK

By

REDHWAN MOHAMMED AHMED SAAD

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

March 2016

DEDICATION

To my appreciated father “Mohammed Ahmed Saad”,

To my dearest mother “Fatimah Mohammed Naji”,

To my dearest brother “Dr. Ali Al-Nakhlany”

To my beloved wife “Manal Al-Adahi”,

To my daughter “Malak”,

To the memory of my beloved Yemen

ACKNOWLEDGEMENT

بسم الله الرحمن الرحيم

{ نَرْفَعُ دَرَجَاتٍ مَّن نَّشَاءُ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ } (76- سورة يوسف)

All praise and thanks are due to ALLAH SUBHANH WA TAALA, the Lord of the world, for giving me the health, strength, knowledge and patience to complete this work Whom His Majesty Said (And remember! your Lord caused to be declared (publicly): "If you are grateful, I will add more (favours) unto you." (Ibrahim: 7).

Since the Prophet MOHAMMED “Peace be Upon Him” said: 'Whoever does not thank people (for their favours) has not thanked Allah (properly)', therefore, I would like to express my deep gratitude to my main supervisor Dr. Selvakumar Manickam for all his support, patience and guidance during this research. He has widened my horizon in conducting the research. His contributions were invaluable, extraordinary and his way of directing a student was unique. Furthermore, my appreciation and sincere gratitude go to the co-supervisor Dr. Mohammed Anbar for his diversified help, support and encouragement. I am privileged to be under the supervision of these supervisors during the PhD research years.

I would like to express my gratitude and thanks to all NAv6 centre members my colleagues, technicians, and administrative staff. My Acknowledgement also goes to the Institute of Postgraduate Studies, and the university library for their help and support. As well as, I would like to express my great thankful to Dr. Mohammed M. Kadhum and Dr. Kamal M. Al-Henadawi for their great help and support during this study.

My sincere thanks also go to my family those who are always in my heart; my father for his endless and continuous encouragement and constant support, my mother for her continuous prayers and inspiration. My sincere gratitude goes to my dearest brothers for their continuous supporting and encouragement. In addition to, my sisters for always keeping a smile on my face and motivating me all the time.

Moreover, I would like to express great thanks to the Ibb University, Yemen for its distinguished cooperation, support and help during the research period. Also, thanks go to my friends for their support and encouragement during the PhD research.

Redhwan Mohammed Ahmed Saad
Penang, Malaysia, March 2016

TABLE OF CONTENTS

Page

CHAPTER TWO - BACKGROUND AND LITERATURE REVIEW

CHAPTER THREE - RESEARCH METHODOLOGY FOR DETECTING ICMPv6 FLOODING ATTACKS

CHAPTER FOUR - METHODOLOGICAL DESIGN AND IMPLEMENTATION

CHAPTER FIVE - EXPERIMENTAL RESULTS, DISCUSSION, AND ANALYSIS

CHAPTER SIX - CONCLUSION AND FUTURE WORK

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviations	Meaning
AAIFD	Anomaly-based Approach for ICMPv6 Flooding Detection
ABIDS	Anomaly-based Intrusion Detection System
ANN	Artificial Neural Network technique
ARP	Address Resolution Protocol
BPNN	Back Propagation Neural Network
CGA	Cryptographically Generated Addresses
CMAC	Cerebellar Model Articulation Controller
CPU	Central Processing Unit
DAD	Duplicate Address Detection
DDoS	Distributed Denial of Service
DHCPv6	Dynamic Host Configuration Protocol version 6
DoS	Denial of Service
DTDNN	Distributed Time-Delay Artificial Neural Network
ECOS	Evolving Connectionist System
HIDS	Host-based Intrusion Detection System
IANA	Internet Assigned Numbers Authority
ICMPv6	Internet Control Message Protocol version 6
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IGR	Information Gain Ratio
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LAN	Local Area Network
MAC	Media Access Control
MiTM	Man-in-The-Middle
MLD	Multicast Listener Discovery

MLP	Multi Level Perceptron
MSE	Mean Square Error
MSOMS	Multiple Self Organizing Maps
MTU	Maximum Transmission Unit
NA	Neighbour Advertisement
NAv6	National Advanced IPv6 Centre
NDP	Neighbour Discovery Protocol
NDPmon	Neighbour Discovery Protocol Monitor
NH	Next Header
NIC	Network Interface Card
NIDS	Network-based Intrusion Detection System
NN	Neural Network
NNID	Neural Network Intrusion Detector
NNIDS	Neural Network for Intrusion Detection System
NS	Neighbour Advertisement
NSA	Network Security Admin
OC	One-way Connection
PCA	Principal Component Analysis
PMTU	Path Maximum Transmission Unit
RA	Router Advertisement
R_{ICMPv6}	Ratio of ICMPv6 Protocol
R_{io6}	Incoming and Outgoing Ratio
RMSE	Root Mean Square Error
RS	Router Solicitation
SAs	Security Associations
SBIDS	Signature-based Intrusion Detection Syatem
SeND	Secure Neighbour Discovery
SLAAC	Stateless Address Auto-Configuration
SVM	support vector machines (SVM),
TCP	Transmission Control Protocol
THC-IPV6	The Hacker Choices for IPv6 Network
v6IDSF	Intrusion Detection System for IPv6 Network Framework
v6OCD	One-way Connection Density in IPv6 Network

RANGKAKERJA PENGESANAN SERANGAN DDoS PERMINTAAN GEMA ICMPv6 MENGGUNAKAN RANGKAIAN NEURAL RAMBATAN BALIK

ABSTRAK

Pertumbuhan pesat Internet dalam beberapa tahun kebelakangan ini telah mendedahkan had ruang alamat dalam protokol Internet semasa (IP), iaitu, IPv4. Permintaan yang semakin meningkat dalam penggunaan alamat IP telah mengakibatkan kehabisan alamat IPv4 seperti yang dijangkakan. Untuk menangani kebimbangan ini, IPv6 baru telah dibangunkan untuk menyediakan ruang alamat yang mencukupi. IPv6 dimuatkan dengan protokol baru, iaitu, versi Protokol Mesej Kawalan Internet 6 (ICMPv6), dan protokol baru ini membuka pintu bagi penyerang untuk menyerang rangkaian IPv6. Salah satu jenis serangan yang paling kerap dalam rangkaian IPv6 pada lapisan rangkaian adalah satu serangan banjir ICMPv6 DoS / DDoS. Laporan Arbor Network pada tahun 2014 menunjukkan bahawa ancaman terhadap IPv6 semakin meningkat (72% merupakan kebanjiran trafik/serangan DDoS). Di samping itu, ICMPv6 adalah protokol wajib dalam rangkaian IPv6 tidak seperti dalam IPv4, iaitu ICMP boleh disekat atau diturunkan melalui get laluan lalai. Sistem pengesanan yang sedia ada terhadap gangguan trafik memainkan peranan penting dalam keselamatan rangkaian komputer. Banyak kajian telah menekankan bahawa terdapat beberapa masalah utama yang mencabar sistem pengesanan gangguan trafik sedia ada. Satu lagi masalah ialah ketepatan dalam mengesan serangan banjir ICMPv6 DoS / DDoS, yang terjejas oleh kadar penggera palsu yang tinggi. Oleh yang demikian, pengesanan perkhidmatan infrastruktur, seperti pelayan web, terhadap serangan seperti itu merupakan isu kritikal yang perlu ditangani segera. Objektif tesis ini adalah untuk mencadangkan satu rangka kerja untuk

mengesan serangan banjir ICMPv6 DoS / DDoS dalam rangkaian IPv6 dengan menggunakan Sistem Pengesanan Pencerobohan Pintar dalam Rangkaian IPv6 (v6IDS) melalui kaedah berasaskan ciri-ciri tingkah laku. Rangka kerja yang dicadangkan terdiri daripada empat peringkat untuk mencapai objektif kajian. Peringkat tersebut adalah seperti berikut. (1) Pengumpulan data dan peringkat prapemprosesan bertujuan menguasai rangkaian trafik, mengesan jenis versi IPv6, dan menapis paket ICMPv6 itu. (2) Peringkat analisis data bertujuan menentukan kedudukan dan mengekstrak ciri-ciri terbaik yang menyumbang terhadappengesanan serangan DoS/DDoS. (3) Peringkat pengesanan berasaskan anomali bertujuan mengumpulkan paket IP dan mengesan paket anomali melalui kaedah berasaskan peraturan ambang. (4) Peringkat pengesanan banjir ICMPv6 bertujuan mengesahkan pengesanan tingkah laku serangan banjir ICMPv6 menggunakan teknik rangkaian neural buatan. Hasil kajian menunjukkan keberkesanan rangka kerja v6IDS dalam mengesan serangan banjir ICMPv6 DoS / DDoS dengan menilai rangka kerja ini dengan menggunakan set data trafik sebenar, yang telah dihasilkan menggunakan ICMPv6 berasaskan DoS / DDoS sebenar menggunakanberpusat di membanjiri katil ujian serangan di NAv6. Keputusan menunjukkan bahawa rangka kerja v6IDS adalah cukup tepat dalam mengesan serangan banjir ICMPv6 DoS / DDoS, dengan ketepatan sebanyak 88.8% dari segi pengesanan anomali DoS/DDoS dan 98.3% dari segi pengesanan tingkah laku serangan banjir ICMPv6. Ketepatan rangka kerja yang dicadangkan itu dibandingkan dengan pendekatan lain yang terdapat dalam kajian literatur. Keputusannya, serta penilaian kuantitatif, jelas menunjukkan bahawa rangka kerja v6IDS yang dicadangkan dapat mengesan serangan banjir ICMPv6 DoS/DDoS.

ICMPv6 ECHO REQUEST DDoS ATTACK DETECTION FRAMEWORK USING BACK-PROPAGATION NEURAL NETWORK

ABSTRACT

The rapid growth of the Internet in the last few years have exposed the limitation of address space in the current Internet protocol (IP) namely IPv4, due to the increasing consumption of IP addresses. The IPv6 has been developed to provide sufficient address space. It ships with a new protocol. i.e., the Internet Control Message Protocol version 6 (ICMPv6), this protocol is a mandatory protocol in IPv6 networks unlike in IPv4, in which ICMP can be blocked or dropped. ICMPv6 opens the door for attackers to attack IPv6 networks. The most frequent types of attack in IPv6 networks at the network layer is an ICMPv6 DDoS flooding attack. One of the main problem in ICMPv6 DDoS flooding attacks is accuracy detection, which suffers from a high false alarm rate. Thus, protecting infrastructure service is a critical issue that urgently needs to be addressed. The aim of this thesis is to propose a framework for detecting ICMPv6 DoS/DDoS flooding attacks, which consists of four stages to achieve the research objectives, which are: (1) *Data collection and preprocessing* that aims to filter out the ICMPv6 packets and filtering dataset from any redundant data to reduce traffic volume, thus increasing the accuracy detection rate. (2) *Network traffic analysis* that contributes on selecting the most important features for detecting ICMPv6 DDoS flooding attack. (3) *Anomaly-based detection* that intends to aggregate IP packets and detect anomaly packets by proposing rules-based method with threshold technique. (4) *Verification of ICMPv6 flooding detection* that aims to verify the detection of ICMPv6 flooding attack behaviour by using artificial neural network technique. Since, this thesis consider the necessity for

detecting anomaly-based attack that can detect the malicious traffic and improve the Internet security. The major contribution of this thesis is to provide a framework that responds to detect ICMPv6 echo request flooding attack. The result as well as its quantitative evaluation, clearly shows that the proposed v6IDSF can detect ICMPv6 DDoS flooding attacks, with accuracies of 88.9% in terms of DDoS anomaly detection and 98.3% in terms of ICMPv6 flooding attacks detection respectively. The accuracy of the proposed framework is compared with the most sufficient approach available in literatures using real traffic dataset. All this would help to improve the Internet security.

CHAPTER ONE

INTRODUCTION

1.1 Overview

Internet protocol version 6 (IPv6), is designed to replace its predecessor IPv4. According to Internet Assigned Numbers Authority (IANA), after the total depletion of IPv4 addresses in February 2011, the future of computer networks and the Internet depends on IPv6. It provides address space of 128-bits compared to only 32-bits in IPv4. In addition, IPv6 also offers many advantages, such as the extensibility of the IPv6 extension header, auto-configuration, router aggregation, efficient transmission, and mobility. However, the deployment of the protocol requires time because people are still comfortable using IPv4 in their connection and security consideration. As with any new technologies, IPv6 too suffers from various undiscovered security vulnerabilities and loop-holes. Nevertheless, the protocol has definitely entered our life.

Most new networking products are now dual-stacked, providing support for both IPv4 and IPv6. In addition, many websites, such as Google, Facebook, and Yahoo!, have provided IPv6 connection (Roberts, 2011). Furthermore, IPv6 introduces new security issues that did not exist with the IPv4 address. A research on anomaly detection algorithms based on Neural Networks (NN), which has practical importance and theoretical significance, is necessary. According to the survey by the Arbor Network report in 2014, intelligent DDoS detection systems is considered to be the most important attack detection technique for IPv6 attacks, 70% are depend on these system (McPherson et al., 2014).

As with any new technology, the initial phases of IPv6 implementation are bound to be exploited by cybercriminals. From a security point of view, the IPv6 protocol represents a considerable advances in relation to the IPv4 protocol. Some examples of security threats in IPv6 networks, such as network reconnaissance, routing headers, fragment headers, denial of service, efficient bottlenecks, misuse of ICMPv6 and multicast, ICMPv6 spoofs, risks of tunnels, and potential holes in dual stacks attacks (El-Bakry and Mastorakis, 2008, Zeng, 2010) (see Chapter 2 for more details).

IPv6 and IPv4 are extremely similar only in terms of functionality (but not in terms of mechanisms). There are two auto-configuration mechanisms in IPv6; stateless using Stateless Address Auto-configuration (SLAAC), based on ICMPv6 messages (Router Solicitation and Router Advertisement) and satatefull using Dynamic Host Configuration Protocol version 6 (DHCPv6). Table 1.1 shows a comparison between IPv6 and IPv4.

Table 1.1: Comparisons between IPv6 and IPv4

	IPv4	**IPv6**
Addressing	32 bits	128 bits
Address Resolution	ARP	ICMPv6 NS/NA
Auto-configuration	DHCP&ICMP RS/RA	ICMPv6 RS/RA & DHCPv6
Fault isolation	ICMP	ICMPv6
IPsec support	Optional	Recommended
Fragmentation	Both in hosts and routers	Only in hosts

1.1.1 Internet Control Message Protocol version 6 (ICMPv6)

The Internet Control Message Protocol (ICMP) is part of the IP suite as defined in (Postel, 1981). ICMP messages are typically used for diagnostic, testing,

and control purposes. Alternatively, they are generated in response to errors and to report problem conditions in IP operations that are directed to the source IP address of the originating packet.

ICMPv6 messages (RFC 2463) contain a type and a code that relates the details of the message to the type of message, as well as a checksum and a payload with variable size. ICMPv6 error messages relay useful information back to the source of the packet regarding any error that may have occurred along the path (Convery and Miller, 2004). The header format is the same for both ICMPv4 and ICMPv6. The general packet structure of ICMPv6 is shown in Figure 1.1.

Header	8- bit ICMP Type (0-7 bit)	8- bit ICMP Code (8-15 bit)	16- bit ICMP Checksum (16-31 bit)
Protocol Payload	ICMP Contents (dependent on type and code) Message Body (32 bit)		

Figure 1.1: General ICMPv6 Packet Structure

Compared with IPv4, an ICMP specification for IPv6 exhibits the distinctive changes such as Neighbour Discovery (ND) substituting Address Resolution Protocol (ARP) and several administrative changes in IPv6 as following:

- Next Header (NH) value. For ICMPv4 (1), it is changed to ICMPv6 (58).
- ND substitutes ARP. With ICMPv6, nodes are found by ND messages similar to the ARP mechanism in IPv4.
- Increased Path Maximum Transmission Unit (PMTU). In IPv4 every node minimum capacity should carry at least 576 bytes, whereas in IPv6, 1500 bytes.
- Multicast Listener Discovery (MLD). ICMPv6 messages are used in IPv6 to replace Internet Group Management Protocol (IGMP). This protocol allows multicast listeners to obtain desirable addresses. In IPv6, there is no longer any

broadcast; instead, multicast is used. Thus, ICMPv6 services ND to autoconfigure nodes (Frankel et al., 2010).

1.1.2 ICMPv6 Security Considerations

One of the main advantages of IPv6 is its auto-configuration mechanism. If an IPv6 enable host plugs in into an IPv6 network, its IPv6 address will be generated without manual configuration. This mechanism is conducted using Neighbour Discovery Protocol (NDP) (Narten et al., 2007). According to Conta et al. (2006), NDP defines five different ICMPv6 packet types for the purpose of router solicitation, router advertisement, neighbour solicitation, neighbour advertisement, and network redirects (RFC 2461) (for more detail see Ch.2, Section 2.2.4). Therefore, ICMPv6 is the most important protocol associated with the IPv6 protocol, particularly in the auto-configuration mechanism. ICMPv6 messages have two categories, namely, error messages and informational messages.

The NDP messages belong to an informational message category. However, the design of ICMPv6 protocol has led to be vulnerable to attacks and exploitations. A possible attack vector simply sends many illegal ICMPv6 messages to a network device (Hogg and Vyncke, 2009). A network device, such as an IPv6 host, should respond to each of the ICMPv6 messages received, which will increase the load of the node. This situation may drive CPU utilization, which causes performance degradation.

Other vulnerability of ICMPv6 is it can be exploited by an attacker to carry out DoS and DDoS attacks. This research attempts to determine the best detection

method by investigating the characteristics of ICMPv6 DoS/DDoS flooding attacks in order to increase the detection accuracy.

A significant benefit of the IPv6 protocol is expected by Internet users. Thus, securing IPv6 networks is highly important. In addition, the number of DoS/DDoS attacks is increasing every day, which can affect the ICMPv6 as follows.

1.1.2.1 DoS/DDoS via ICMPv6

ICMPv6 can be used to generate a DoS/DDoS attack in several ways, including simply sending an extreme number of ICMPv6 packets echo request type 128 (any node can test connectivity to any other node over IPv6 by sending an Echo Request Message to that node, using uncast or multicast destnation) to destinations in the same site and sending error messages that disable established communications by causing sessions to drop. Moreover, if the spurious communication establishment or maintenance messages can be infiltrated onto a link, it could be possible to invalidate legitimate addresses or disable interfaces (RFC 4890). DoS/DDoS can be classified into two categories; applications level and network devices level, based on the attacked level, as shown in Figure 1.2.

One of these categories is ICMPv6 flood. In ICMPv6 flooding attacks, an attacker attempts to consume the maximum available bandwidth of a network or nodes. Such as an attacker can simply floods the targeted victim with bogus packets with spoofed source addresses (Douligeris and Mitrokotsa, 2004, Safa et al., 2008).

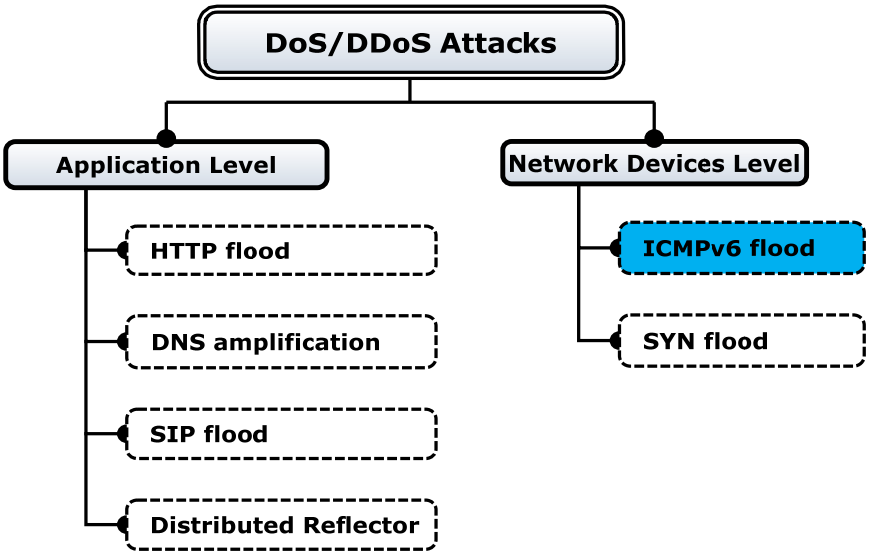

Figure 1.2: Classification of DoS/DDoS Attacks

1.1.2.2 Probing via ICMPv6

A main security consideration is detecting attackers from probing the site to determine the topology and identify hosts that might be vulnerable to attack. Frequently, malformed messages can be used to provoke ICMPv6 responses from hosts thereby informing attackers of potential targets for future attacks (Padmanabhan et al., 2015). However, other ICMPv6 features, such as the autoconfiguration of addresses, makes probing systems for weaknesses complicated for a malicious attacker. These features will not stop random scanning, but they will make it difficult to scan specific IPv6 networks. Nevertheless, IPv6 networks can be scanned effectively by using ICMPv6 messages if they are poorly designed (as in the IPv4 model) and use dense address allocations for services and routers.

1.1.2.3 Problems Resulting from ICMPv6 Transparency

Due to several ICMPv6 error packets need to be passed through a firewall in both directions, malicious users can potentially use these messages to communicate

between inside and outside, bypassing administrative inspection. For instance, it may be possible to implement a covert conversation through the payload of ICMPv6 error messages or tunnel inappropriate encapsulated IP packets in ICMPv6 error messages (Davies and Mohacsi, 2007). This problem can be mitigated by filtering ICMPv6 errors messages using a stateful packet filtration mechanism in order to ensure that the packet carried as a payload is associated with real traffic to or from the protected network.

1.1.2.4 Flooding Attack via ICMPv6

One of the most frequent types of attack in IPv4 networks is a flooding attack, which involves flooding a network device (e.g., a router or a host) with large amounts of network traffic. A targeted device cannot process such large amount of network traffic and becomes unavailable or out of service. A flooding attack can be DDoS when the targeted network device is being simultaneously flooded by network traffic from several nodes. Thus, this type of attack can also affect IPv6 networks because the basic principles of a flooding attack remain the same (Alangar and Swaminathan, 2013).

DDoS flooding attacks can be launched in two forms as shown in Figure 1.3: direct and reflector attacks. In the former, the attacker directly sends a flood of bogus packets to the victim through zombie machines. In the latter, the attacker sends request messages to reflector machines through zombie machines, while spoofing the source IP address of the victim server. Thus, reflector machines send their replies to the given address, which causes packet flooding at that site (i.e., the victim server). There are three major components constituting a reflector attack; the attacker, the amplifying reflectors, and the victim. The attacker sends ICMPv6 echo request

packets with the victim's IP address as the source address to the multicast address of an amplifying network as the destination address. So the packets appear to have been sent by the victim. Since they are sent to a multicast address of a local network, all the hosts, except those whose configuration has been specified not to respond to ICMPv6 multicast packets, in the local network will respond to each of the packets. Therefore, Smurf is a type of amplified DoS attack. Because of this amplifying effect, an individual reflector attacker can send the packets at a much lower rate compared to the packet rates created by ordinary DoS attackers who flood the victim directly. (Beitollahi and Deconinck, 2012).

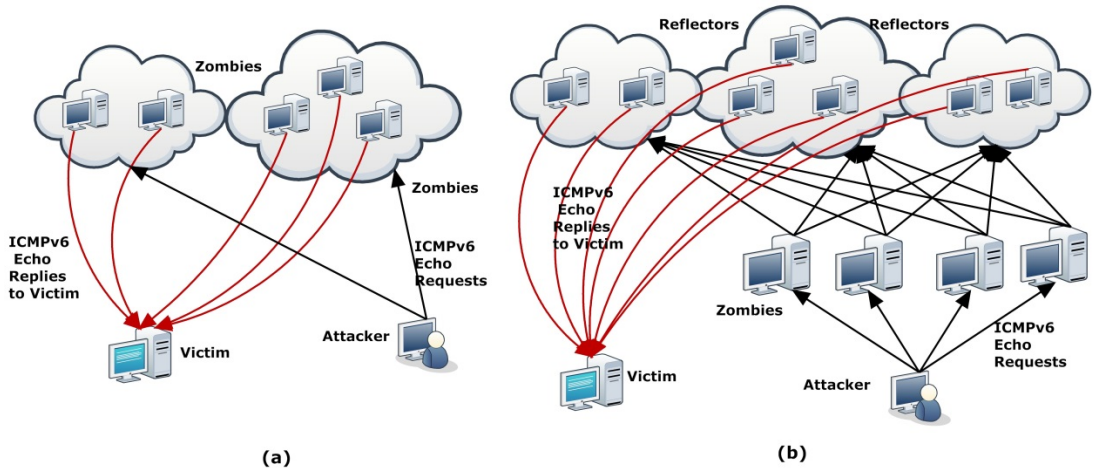

Figure 1.3: Architecture of Flooding DDoS Attacks: (a) Direct, (b) Reflector

New types of extension headers in IPv6 (such as the authentication header fields and IPv6 router header) and new types of ICMPv6 messages (such as ICMPv6 echo request type 128) that depend on multicast addresses in IPv6 (e.g., all routers must have site-specific multicast addresses) can be exploited to carry out flooding attacks (Ektefa et al., 2010). An attacker can frequently cause unamplified flooding by sending packets to its victim, either by directly addressing the victim in the packets or by guiding the packets along a specific path through an IPv6 routing header (Arkko et al., 2011).

1.2 Research Motivation

IPv6 exhibits security vulnerability that slows down IPv6 deployment. The "Ping of Death" is a famous DoS vulnerability caused by several ICMPv6 packets with echo requests in IPv6 networks (TechCenter, 2013). This situation has motivated researchers to propose techniques that can detect unknown or new ICMPv6 DoS/DDoS attacks. The following are the motivations of the research.

- ❖ According to the 2014 Cyber Security Watch Survey (McPherson et al., 2014), the amount of security incidence continues to extend more rapidly than the defences of the companies. According to this report, DoS/DDoS flooding attacks against IPv6 are the main cyber threats in general. Many of the existing security vulnerability of IPv4 are inherited by IPv6. Among all major security vulnerabilities is a DoS/DDoS attack, which has already extended in IPv6. Since the basic principles of a flooding attack remain the same (Alangar and Swaminathan, 2013, Arkko et al., 2011, Ektefa et al., 2010, Radhakrishnan et al., 2007).
- ❖ Currently, there are less security techniques available to secure IPv6 protocol as compared to the legacy IPv4 protocol, in terms of both features and performance (Gont, 2011, Gont, 2012a).
- ❖ There are many types of extension headers in IPv6, various ICMPv6 messages such as echo request message, and multicast dependency in IPv6 open doors for flooding attacks (Shanmugaraja and Chandrasekar, 2012, Oliveira et al., 2012).

1.3 Research Problem

At present, online communication has become a mandatory part of the lifestyle of many people as Internet services develops rapidly. Security researchers

have paid considerable attention to secure online services and communication against network intrusions. One of the most difficult and critical aspects in the existing Intrusion detection is ICMPv6 echo request DoS/DDoS flooding attack detection, which is explained as follows.

The difficulties in detecting flooding attacks using existing approaches are due to the fact that they use simple heuristic rules, which are configured to detect the common and well known attacks but unable to detect the new attacks such as ICMPv6 flooding attacks. In addition, the difficulties in detecting malicious packet is that packets transmitted during flooding-based attacks can exhaust the targeted host CPU resources, which can lead to the degradation of system performance. Moreover, the existing approaches do not consider the most important features to be used which selected from the dataset to detect flooding attacks.

ICMPv6 in IPv6 networks is a mandatory protocol unlike in IPv4, in which ICMP messages can be blocked or dropped by a default gateway. In addition, ICMPv6 messages are used in Neighbour Discovery process that allows IPv6 node to communicate and discover neighbouring node on the same link, finds routers for paths to other networks (Choudhary and Sekelsky, 2010), thus, introduce new security threats. One of these threats is ICMPv6 DoS/DDoS flooding attack, and several security risks are associated with uncontrolled forwarding of ICMPv6 messages (RFC4890) (Frankel et al., 2010), which will be discussed in detail in Ch.2.

The problem in existing techniques for detecting ICMPv6 DoS/DDoS flooding attacks is that they have a high false-positive rate, which leads to a low accuracy caused by the following reasons:

- Existing IPv6 security tools, such as antivirus and firewalls, are based on signature-based detection. Moreover, they are unable to detect ICMPv6 DoS/DDoS flooding attacks on targeted servers because they are designed to protect against signature-based attacks instead of the polymorphic network behaviour of the attacks launched by DoS/DDoS (Ektefa et al., 2010).

- The existing mechanism for securing the new functionality with IPv6 such as Neighbour Discovery monitoring tools (NDPMon) is inefficient for detecting ICMPv6 DoS/DDoS flooding attacks because this mechanism is targeted or designed to only detect the vulnerability of NDP-based attacks, which is a part of ICMPv6 protocol (Gont, 2012b). However, in this study we address the problem of ICMPv6 echo request.

- Existing techniques such as NIDS use nonsophisticated or simple rule-based techniques, which is not consider intelligent systems to address this problem in an IPv6 network environment (Lo and Marchand, 2004, Salah et al., 2012). That is, the difficulty in detecting novel intrusions and the increasing number of false alarms are the major drawbacks of the IDS (Gyanchandani et al., 2012).

- Existing techniques for securing ICMPv6 (such as IPsec and the SeND mechanisms) require extra encryption, which adds overhead to the process, thereby generating DoS attack. Hence, the significance of the detection system, which attempts to detect potential attacks, is a critical issue (Choudhary and Sekelsky, 2010).

In order to address the security vulnerability in ICMPv6 and also to address the drawbacks of existing techniques which heavily relies on signature, this thesis proposes an anomaly-based framework by using rule-based detection with threshold

mechanism and using artificial neural network technique such as Back-propgation algorithm (BPNN) in an IPv6 network environment in order to increase the detection accuracy for detecting DoS/DDoS attacks against the ICMPv6 protocol.

1.4 Research Objectives and Goals

With the significance of network technology and the use of IPv6 network protocols in our daily lives, security issues related to these employed protocols remain a huge concern.

The objective of this research is to propose a framework using the BPNN technique, which can accurately detect the presence of ICMPv6 echo request DoS/DDoS flooding attacks in IPv6 networks. The following objectives intend to solve the problem of low accuracy in terms of ICMPv6 DoS/DDoS flooding attack detection:

- To propose a mechanism that adapts feature ranking and extraction techniques to identify the salient features in anomaly-based detection that has the characteristics of ICMPv6 DoS/DDoS flooding attacks.
- To propose a rule-based mechanism for detecting DoS/DDoS anomalies.
- To evaluate the effectiveness of the proposed framework in terms of detection accuracy in the IPv6 environment and to compare it with existing anomaly-based approach for DoS/DDoS flooding attacks using real traffic dataset.

1.5 Research Contribution

The main contribution of this research is to propose a framework based on BPANNs, called the Intrusion Detection System in IPv6 Network Framework (v6IDSF), which is designed to detect ICMPv6 DoS/DDoS flooding attacks with a

better accuracy detection rate in the IPv6 network. The contributions of the present research are as follows.

- A framework to detect ICMPv6 DoS/DDoS flooding attacks with better accuracy using the BPANN technique in the IPv6 network.
- A feature selection mechanism to identify the features that highly contribute to detecting ICMPv6 DoS/DDoS flooding attacks based on feature ranking and extraction techniques.
- A rule-based mechanism to detect DoS/DDoS anomalies.

1.6 Research Scope and Limitation

The scope of the proposed framework in this research is limited to detect ICMPv6 DoS/DDoS flooding attacks in network layer and in the IPv6 network environment as shown in Table 1.2.

The dataset, which is used to evaluate and test anomaly-based detection, was generated with a real traffic dataset using a real ICMPv6 DoS/DDoS flooding attack test-bed via The Hacker's Choice (THC) toolkit in the IPv6 network environment.

Table 1.2: Research Scope and Limitation

Items	Scope of Research
Environment	IPv6 global network
Attack type	DoS/DDoS attack against ICMPv6 protocol (excludes other anomaly behaviour)
ICMPv6 protocol type	Echo request type 128
DoS/DDoS target	Network layer
Detection	Anomaly-based detection
Dataset	Real traffic dataset
Evaluation	Accuracy Detection

This research does not focus on DoS/DDoS flooding attacks in IPv4 networks and on other flooding attacks against Neighbour Discovery Protocol (NDP) attack in IPv6 networks, such as Spoofed ICMPv6 router advertisement (RA), Spoofed ICMPv6 neighbour advertisement (NA).

1.7 Research Steps

In this research, ANN is used to support the solution to increase the detection accuracy of ICMPv6 echo request DoS/DDoS flooding attacks in IPv6 networks by utilizing the v6IDSF.

The following methodological steps are followed to achieve the objectives of this research: (i) reviewing related literature and analysis, (ii) proposing a new framework to detect ICMPv6 echo request DoS/DDoS flooding attacks, (iii) designing and implementing the proposed framework, and (iv) testing and evaluating the result and finding. Figure 1.4 illustrates the main methodological phases of the research process.

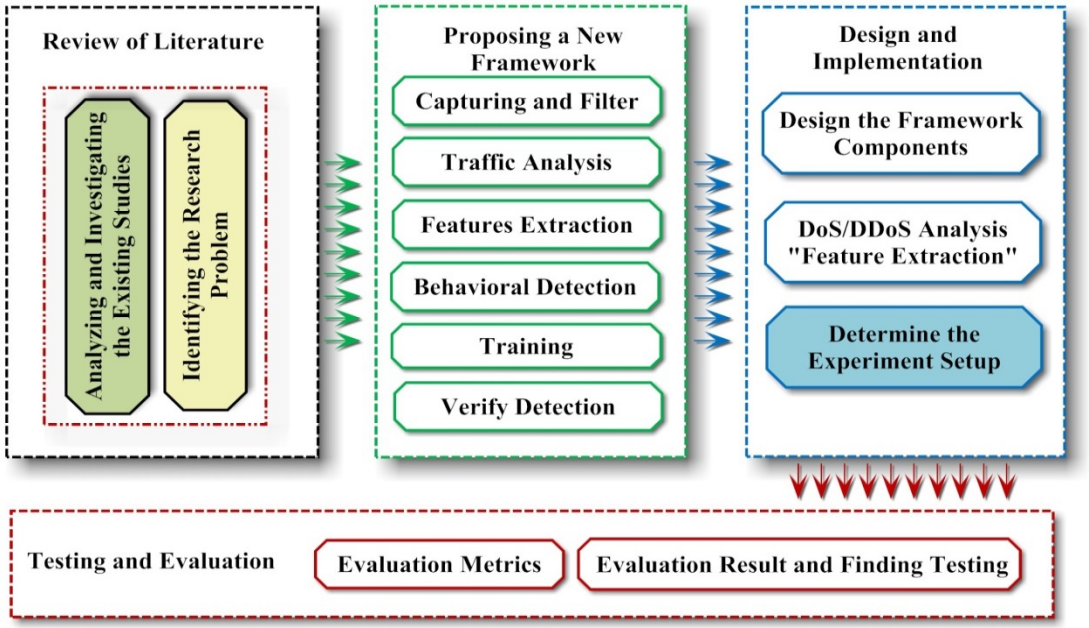

Figure 1.4: Main Stages of Research Process

In the first phase, the research problem is recognized and thoroughly investigated by a critical survey of existing studies. Hence, this phase provides an understanding of the problem, an existing solution space, and future research scope to detect ICMPv6 both DoS (from single attack host) and DDoS (from multiple attack hosts) echo request flooding attacks.

In the second phase, the solution for research problem is presented. The solution consists of several stages to detect ICMPv6 flooding attack by enhancing detection accuracy. The proposed framework employs the features of Back-propagation Neural Networks (BPNNs) that was trained suing dataset with attack traces to detect ICMPv6 flooding attacks.

The third phase is mainly concerned with the research design and implementation of the v6IDSF based on BPNN to increase detection accuracy in the IPv6 environment, which uses only five features to improve efficiency in terms of attribute construction, model training, and intrusion detection.

In the fourth phase, the test and evaluation stage also leads to the achievement of the objective. The proposed framework is tested and evaluated based on its effectiveness in increasing detection accuracy in the IPv6 environment using a real traffic dataset, which is generated with a real ICMPv6-based DoS/DDoS flooding attack test-bed. Finally, this framework is compared with existing anomaly-based approach such as Anomaly-based Approach for ICMPv6 Flooding Detection (AAIFD).

1.8 Thesis Organization

This thesis is structured into six chapters as follows:

Chapter 1 presents the objectives of this thesis. It starts by presenting an introduction discussion for the IPv6 and ICMPv6 security. The research motivation, problem statement, objectives, research steps, scope and contributions are also provided in this chapter.

Chapter 2 describes a background for understanding of the work that follows, including overview security aspects, a description of ICMPv6 flooding attack features based on security aspects, literature survey of the related work in the domain of our research, and a look at the detection model to be used as a basis frame for v6IDSF.

Chapter 3 Discusses the proposed methodology by elaborating how the proposed solution was designed. Also, it describes the integrated phases of the proposed framework and the algorithm for detecting ICMPv6 DoS/DDoS flooding.

Chapter 4 Illustrates the design and implementation of the proposed framework. Moreover, it illustrates the experimental direction and the implementation of detection. This chapter comprises the designing principles of the test-bed and dataset generation.

Chapter 5 describes the further details, evaluation of the dataset; testing and discussion of the proposed framework in the context of network IDS. In addition, the chapter elaborates the results obtained from the experiments of the detection for the ICMPv6 packets. Also, it evaluates the performance of the proposed framework comparing it with existing approach (AAIFD).

Chapter 6, the contributions, conclusion, recommendation and the possible future work for this research are presented in this chapter.

CHAPTER TWO

BACKGROUND AND LITERATURE REVIEW

2.1 Introduction

Securing IPv6 networks are essential, since IPv6 protocol is insecure by nature. Eventually, it will replace IPv4. Therefore, to make sure network communication among nodes be safe. IPv6 protocol needs to be secured. The number of DoS/DDoS attacks is increasing. These attacks attempt to disable the networking services of a target device, thus causing possible failures in the transmission of IPv6 packets and disrupt services running on IPv6 stack. In response, a number of researchers sought to find a methodology for detecting, classifying and mitigating these DoS/DDoS attacks.

This chapter surveys the related studies on the detection of ICMPv6 DoS/DDoS flooding attack and is arranged as follows. Section 2.2 explains the typical attacks on an IPv6 network and covers and reviews some of the fundamental attacks on ICMPv6. The prevention mechanisms for ICMPv6-based attacks are discussed in Section 2.3. Section 2.4 presents the approaches in DoS/DDoS attack detection. Section 2.5 formulates the features selection for DoS/DDoS flooding attack detection and the effect of extracting the most important features. Finally, Section 2.6 provides the summary of this chapter.

Figure 2.1 shows the main areas of the research background and literature review, as well as the inference between the elements of the research. Each main level is presented in a section in this chapter and provides an overview of the work with related problems.

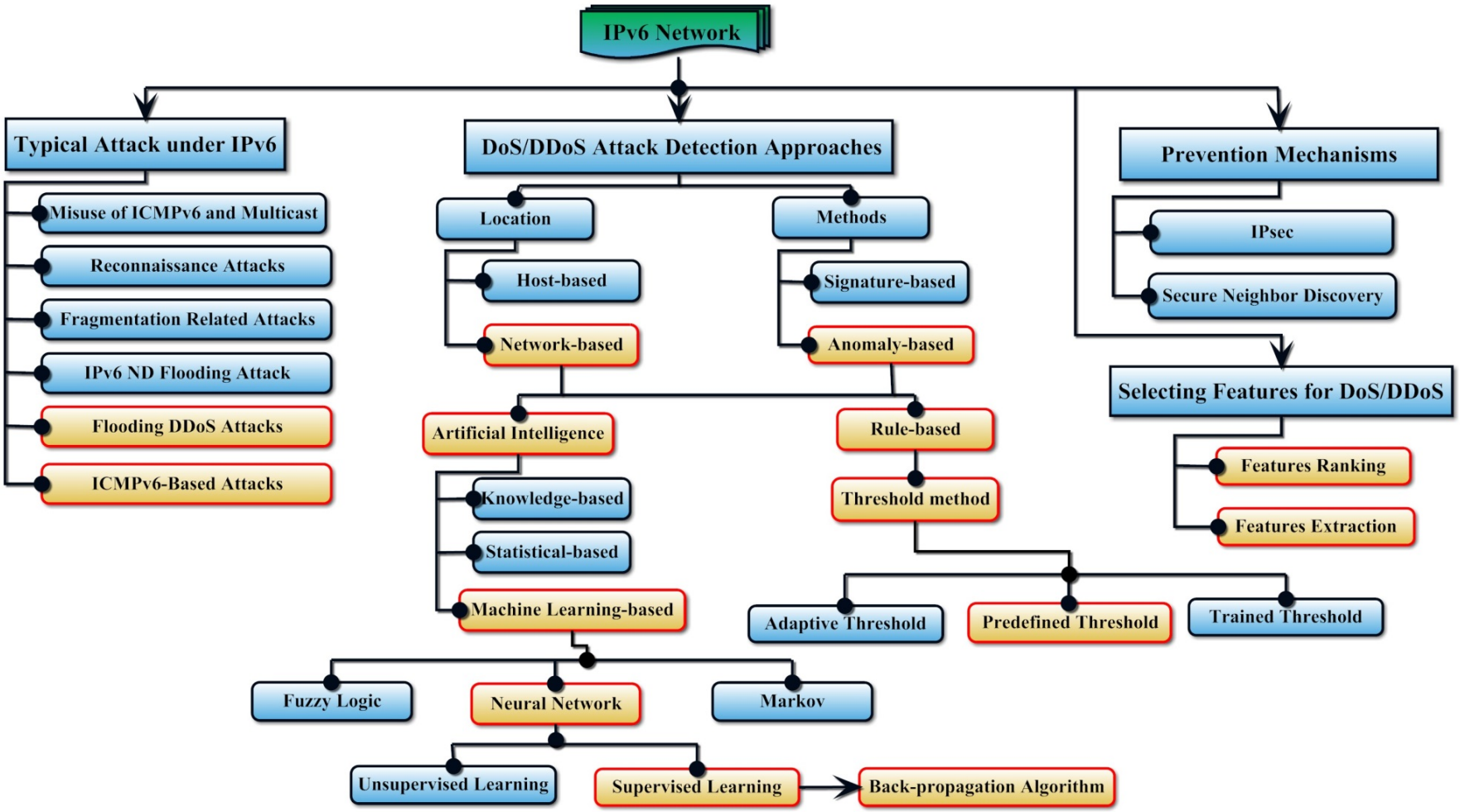

Figure 2.1: Literature Survey and Related Work

2.2 Typical Attack on IPv6

The “Ping of Death” is a famous DoS vulnerability in an IPv6 network caused by a number of ICMPv6 packets with RA requests. As announced in August 2013 via security bulletins, if an attacker sends a specially crafted ICMPv6 packet to a target system/server, the vulnerability may enable a denial of service (TechCenter, 2013).

Many changes in the specifications of the IPv6 protocol may lead to potential security problems. This subsection mainly focuses on explaining the typical attacks concerning the IPv6 protocol.

2.2.1 Misuse of ICMPv6 and Multicast

An IPv6 network has several significant mechanisms such as ND and PMTU discovery, which are dependent on several types of ICMPv6 (Conta and Gupta, 2006). The specification of ICMPv6 allows error notification responses to be sent to multicast addresses if a packet is targeted. This fact can be misused by an attacker. An attacker can cause multiple responses in a target device by sending a suitable packet to multicast addresses (the spoofed source of the multicast packet).

According to Gont and Liu (2013), a Smurf attack aims to flood the target machine with a large amount of traffic such that the target machine will be busy responding to the incoming requests. In an IPv6 network, a Smurf attack occurs when an attacker sends spoofed ICMPv6 echo request packets Type 128 to a multicast group (FF02::1), with the target machine as the source. All nodes will receive the packets and respond to the spoofed source IP address. The target machine

experiencing massive traffic will be flooded if the number of nodes on the network that receive and respond to these packets is large. This scenario can slow down the target computer to a point where it becomes impossible to work with.

Chakraborty et al. (2014), have proposed intrusion prevention system (IPS) to handle ICMPv6 threats in Smart Grid as a proper IPS for ICMPv6 misuse. This mechanism helps to efficiently prevent some attacks on the ICMPv6 protocol, such as DoS/DDoS attacks, man-in-the-middle (MiTM) attacks, and spoofing attacks. This mechanism is also light weight and does not load the system with redundant packet overhead, but it is unable to detect collaborative attacks on smart grid.

2.2.2 Reconnaissance Attacks

The first stage of the bigger attack is usually a reconnaissance attack. An intruder uses reconnaissance attacks to collect some critical data about the victim network that can be misused later in further attacks. An intruder can use active methods, such as different scanning techniques, or passive data mining in carrying out reconnaissance attack (Žagar et al., 2007).

Reconnaissance attack techniques are common for both IPv4 and IPv6. Given that they are both network layer protocols, many of their network layer vulnerabilities are similar. However, the subnet size within the IPv6 network is larger than that within the IPv4 network (the default size is 64 bits (RFC 5157)). To perform a full scan of the subnet, 264 probes should be made, thus making this task impossible. Unfortunately, several types of multicast addresses are used in IPv6. This structure helps an intruder to easily identify hosts in an IPv6 network. RFC 2375 and Hinden and Deering (1998) proposed a node, a link, and a site-specific use of

multicast addresses (e.g., all routers have a site-specific address FF02::2), which defines the initial assignment of IPv6 multicast addresses.

2.2.3 Fragmentation-Related Attacks

According to Conta and Gupta (2006), IPv6 protocol specification does not allow packet fragmentation by intermediary devices. The minimum MTU size recommended for ICMPv6 is 1280 octets. As a good security practice, fragments with less than 1280 octets should be dropped. By using fragmentation, an intruder can obtain port numbers that are not found in the first fragment, thus avoiding security monitoring devices that expect to find transport layer protocol data in the first fragment.

According to Hyuk et al. (2009), an attacker can cause a flood of reconstruction buffers in a target machine to initiate a system crash by sending a huge number of small fragments (a type of DoS attack).

2.2.4 IPv6 Neighbour Discovery Flooding Attack

NDP messages are part of ICMPv6, which provides functionalities for reporting error messages, performing network diagnostics, and handling multicast memberships (Lee and Stolfo, 2000).

NDP operates in the link layer of the Internet model (RFC 1122), and is responsible for the address auto-configuration of nodes, discovery of other nodes on the link, determining the link-layer addresses of other nodes, duplicate address detection (DAD), detecting available routers and Domain Name System (DNS) servers, address prefix discovery, and maintaining reachability information about the

paths to other active neighbour nodes (RFC 4861) (Barbhuiya et al., 2013, Conta and Gupta, 2006).

NDP defines five ICMPv6 packet types for the purpose of router solicitation (RS), Router Advertisement (RA), Neighbour Solicitation (NS), Neighbour Advertisement (NA), and network redirects (Barbhuiya et al., 2011). Table 2.1 shows the ICMPv6 messages defined for NDP.

Table 2.1: ICMPv6 Messages Defined for NDP

ICMPv6 packet type	Description
RS (Type 133)	Hosts inquire with RS messages to locate routers on an attached link. Nodes that forward packets not addressed to them generate RAs immediately upon receipt of this message, rather than at their next scheduled time.
RA (Type 134)	Routers advertise their presence together with various link and Internet parameters, either periodically or in response to an RS message.
NS (Type 135)	NSs are used by nodes to determine the link layer address of neighbour or verify that a neighbour is still reachable via cached link layer address.
NA (Type 136	NAs are used by nodes to respond to an NS message.
Redirect (Type 137)	Routers may inform hosts of a better first hop router for a destination.

By default, all IPv6 addresses are automatically part of the multicast address group FF02::1 and other groups (Figure 2.2). The MAC address look-up of the target host in an IPv6 network can be performed by sending an ICMPv6 packet to the multicast address FF02::1. The sent packet will reach all active link-local addresses on the network (RFC 3513). Exchanging ICMPv6 messages on the top of the IPv6 protocol is crucial for IPv6 communication. However, this communication can be abused by sending fake, carefully crafted response messages for DoS/DDoS attack, traffic re-routing, or other malicious purposes.

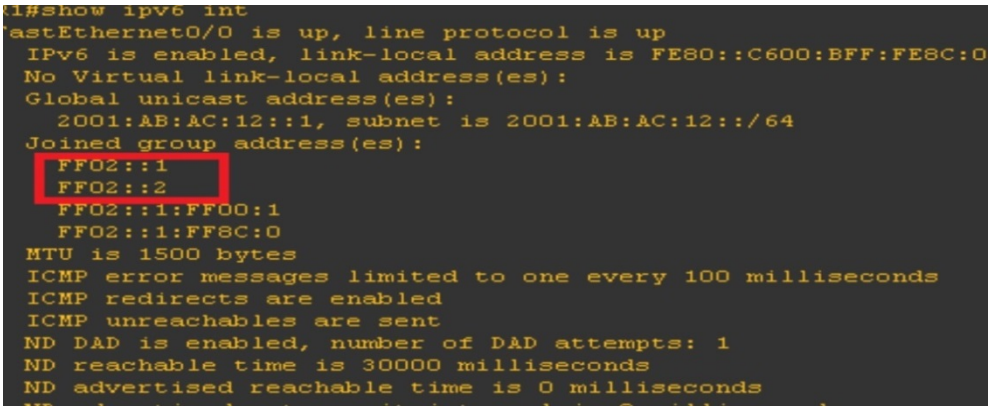

Figure 2.2: Joined Multicast Groups for IPv6 Address

2.2.5 DDoS Flooding Attacks on IPv6

A DoS/DDoS attack is one of the most significant threats in IPv4 and IPv6 networks. These attacks consume the network bandwidth and computational resources of the target and that of other users on the same network. A DoS/DDoS attack, generated by utilizing the vulnerabilities in a network protocol, affects the performance of the target and the other hosts sharing the network (Meenakshi and Srivatsa, 2007). A target device is unable to process the large amount of network traffic caused by these attacks and becomes unavailable or out of service.

Figure 2.3 illustrates the steps of a typical DDoS attack. First, an attacker selects more than one handler which has security vulnerabilities, and intrudes them by gaining access right. And the procedures for selecting agents are performed as the same way for selecting handlers, but the attacker indirectly achieves it through handlers. Second, the agents will perform DDoS attack actually by sending huge amounts of malicious traffic to a target system simultaneously. The handlers and agents are usually located in the external networks of victim's and attacker's network. Commonly, ICMPv6 is used for preform scanning to find hosts which have security vulnerabilities (There are several events that take place during the