BALANCING PERFORMANCE AND SECURITY FOR IPV6 NEIGHBOUR DISCOVERY PROTOCOL

AMJED SID AHMED MOHAMED SID AHMED

UNIVERSITI KEBANGSAAN MALAYSIA

BALANCING PERFORMANCE AND SECURITY FOR IPV6 NEIGHBOUR DISCOVERY PROTOCOL

AMJED SID AHMED MOHAMED SID AHMED

THESIS SUBMITTED IN FULFILMENT FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF INFORMATION SCIENCE AND TECHNOLOGY
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2018

BALANCING PERFORMANCE AND SECURITY FOR IPV6 NEIGHBOUR DISCOVERY PROTOCOL

AMJED SID AHMED MOHAMED SID AHMED

TESIS YANG DIKEMUKAKAN UNTUK MEMPEROLEH
IJAZAH DOKTOR FALSAFAH

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2018

DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

27 July 2018

AMJED SID AHMED
MOHAMED SID AHMED
P72755

ACKNOWLEDGEMENT

First and foremost, all praise to Almighty Allah for his blessings and patience, as well as for providing me with good health during this research.

This work is dedicated to my parents, from whom I learned faith, strength, and determination. This work is also dedicated to my family, especially my beloved brothers for their continuous support, encouragement, love and care and for the joy of my life Ahmed Amjed Sid Ahmed.

I thank my supervisor, Assoc. Prof. Dr. Rosilah Hassan and my Co-supervios Dr. Nor Effendy Othman, for their ultimate guidance, patience and support during the whole journey of my studies.

Finally, I thank my research group for their help and friendship and for creating a pleasant working environment throughout my years of study in UniversitiKebangsaan Malaysia.

I am grateful to UniversitiKebangsaan Malaysia for providing me scholarship during my first two years and ministry of higher education in Malaysia for providing me scholarship during my third year, without their support I won't be able to complete my studies.

ABSTRACT

Internet Protocol version 6 (IPv6) is a protocol designed as the successor to Internet Protocol version 4 (IPv4). It is used to solve the problems faced by IPv4 in today's Internet, such as IP address space limitation, security, and scalability. The Neighbour Discovery Protocol (NDP) is an auxiliary protocol for IPv6, and it comprises two Requests for Comments (RFCs) IPv6 stateless address auto-configuration (SLAAC) and Neighbour Discovery for IPv6. The former allows the hosts to automatically configure the IPv6 address without the outside help and the latter is used for discovery of the IPv6 nodes on the same link. For the normal operations of IPv6, NDP also provides other functions including router discovery, address resolution, next-hop determination, Neighbour unreachability detection (NUD), duplicate address detection (DAD), and redirection. All of these functions are based on the transmission of NDP messages, which are encapsulated in Internet Control Message Protocol version 6 (ICMPv6) packets. NDP uses five types of ICMPv6 messages as which are Router Solicitation (RS), Router Advertisement (RA), Neighbour Solicitation (NS), Neighbour Advertisement (NA) and Redirect Message (RM). When NDP was initially developed there is an assumption that mutual hosts within a subnet will trust each other. This assumption was wrong when it turn into deployment especially in wireless environments, such as airports, coffee shops and public restaurants. NDP lack a security and is vulnerable to several Denial of Service (DoS) attacks. NDP messages are vulnerable to be attacked through spoofing, for example fake reply to address resolution may lead to man-in-the-middle attacks (MITM), and forged NAs to DAD will result in DoS attack. Therefore, malicious nodes can launch attacks through illegally using NDP messages that may lead to a total system hanging and crash. As a response, Secure Neighbour Discovery (SEND) is developed by the Internet Engineering Task Force (IETF) to specify security mechanisms for NDP. SEND proposed three mechanisms to protect NDP messages which are Authorization Delegation Discovery (ADD), Cryptographically Generated Addresses (CGA) and RSA signature. The main problem of CGA is the complexity on the address generation. In addition it is also vulnerable to several DoS attacks that could exploit the SEND messages. The aim of this research is to investigate the impacts of NDP attacks over IPv6 communication link and keep NDP protected and secure enough for its operations at the same time balance its performance to a reasonable and moderate ratio. A test bed setup was deployed and NDP attacks are implemented. Three performance metrics, throughput, RTT and resources consumption were selected to assess the impacts of these attacks over network operations using different types of operating systems. Two models were proposed, first CGA-Lighter to produce cryptographic addresses using MD5 hash function. Second Locked-CGA to secure CGA using sender's interface identifier and packets time stamp to keep CGA protected against DoS attacks. Both models were implemented using different scenarios for existing CGA and proposed one. For the address generation time CGA-Lighter showing a better performance compared to standard CGA. Similarly, Locked-CGA was significantly improved the security of CGA against DoS attacks, a malicious node has become easily to be detected and terminated from the link. Comparing the experiment scenarios results we found the proposed models is efficient enough to solve the security problem and it works with a good performance ratio.

ABSTRAK

Protokol Internet versi 6 (IPv6) adalah protokol yang dibangunkan khusus sebagai pengganti Protokol Internet versi 4 (IPv4).Tujuan utama pembangunannya adalah untuk menyelesaikan masalah-masalah penggunaan semasa IPv4 di Internet terutamanya kekurangan alamat IP, keselamatan dan kebolehan peningkatan berskala.Protokol Penemuan Tetangga (NDP) merupakan protokol tambahan IPv6 yang terdiri terkandung di dalam dokumen standard Permintaan untuk ulasan (RFC) iaitu Penemuan Tetangga untuk IPv6 (RFC 4861) dan Hos Tanpa keadaan dengan konfigurasi alamat IPv6 secara automatik (SLAAC) (RFC 4862). Fungsi standard pertama adalah untuk mencari dan menemukan semua nod IPv6 di dalam rangkaian yang sama, manakala yang kedua membolehkan peranti mendapatkan konfigurasi alamat IPv6 secara automatik tanpa bantuan alatan luaran. Di dalam operasi biasa IPv6, NDP juga berfungsi sebagai peralatan penghalaan /penyediaan awalan/penemuan parameter, resolusi alamat, penentuan lompatan berikut, pengesanan jiran yang sukar dicapai (NUD), pengesanan alamat pendua (DAD) dan penghalaan semula. Kesemua fungsi-fungsi ini adalah berdasarkan penghantaran mesej NDP, yang terkandung dalam paket Kawalan Internet Protokol Mesej versi 6 (ICMPv6). NDP menggunakan lima jenis mesej ICMPv6 iaitu Penghalaan Pengumpulan (RS), Penghalaan Pengiklanan (RA), Pengumpulan Jiran (NS), Pengiklanan Jiran (NA) dan Pengubah hala Mesej (RM). NDP dibangunkan berdasarkan andaian bahawa hos-hos berkait dalam subrangkaian yang sama akan mempercayai antara satu sama lain. Namun, andaian ini nyata tersasar apabila NDP dipasang di persekitaran tanpa wayar, seperti di lapangan terbang, kedai kopi dan restoran awam.NDP mempunyai kekangan keselamatan dan amat terdedah kepada serangan berjenis nafi khidmat (DoS). Mesej melalui NDP amat mudah terdedah kepada serangan berbentuk perdayaan, sebagai contoh balasan palsu untuk menangani resolusi alamat boleh membawa kepada serangan melalui orang tengah (MITM) dan NA yang palsu ke atas DAD akan menyebabkan serangan DoS. Berdasarkan senario tersebut, nod yang berniat jahat boleh melancarkan serangan dengan menggunakan mesej NDP secara tidak sah yang mengakibatkan kerosakan dan penggantungan operasi keseluruhan sistem.Bagi menangani isu tersebut, Pasukan Petugas Kejuruteraan Internet (IETF) membangunkan modul Penemuan Jiran Selamat (SEND) untuk menjana mekanisme keselamatan untuk NDP. SEND mencadangkan tiga mekanisme untuk melindungi mesej NDP iaitu Penemuan Delegasi dengan Keizinan (ADD), Penjanaan Alamat dengan Kriptografi (CGA) dan tandatangan RSA. Masalah utama CGA adalah kesukaran untuk menjana alamat dan ia juga terdedah kepada serangan DoS yang boleh mengeksploitasi mesej SEND. Tujuan utama penyelidikan ini adalah untuk mengkaji impak serangan ke atas NDP terhadap rangkaian komunikasi IPv6 selain memastikan agar NDP dilindungi dan beroperasi di dalam persekitaran yang selamat serta mempertingkatkan prestasi kepada nisbah yang berpatutan dan munasabah.Satu tapak uji telah disediakan bagi tujuan melaksanakan semua jenis bentuk serangan ke atas NDP.Tiga jenis pengukuran metrik prestasi iaitu daya pemprosesan (throughput), lengahan (delay), dan penggunaan sumber telah dipilih untuk menilai kesan serangan ini ke atas operasi rangkaian yang berasaskan pelbagai jenis sistem pengoperasian. Bagi kajian ini, dua model telah dicadangkan, iaitu pertama menggunakan model CGA-Lighter untuk menghasilkan alamat kriptografi menggunakan fungsi hash MD5. Model kedua menggunapakai Locked-

CGA dengan cara melampirkan pengecam antaramuka dan cop masa pada paket penghantar bertujuan melindungi CGA tersebut dari serangan DoS. Kedua-dua model telah diuji dengan senario yang berbeza menggunapakai CGA sedia ada dan kaedah yang dicadangkan.Berbanding dengan CGA standard, CGA-Lighter menunjukkan prestasi yang lebih baik terutamanya dari segi kelajuan. Hasil kajian mendapati Locked-CGA secara ketara telah meningkatkan keselamatan CGA terhadap serangan DoS, dan hasilnya nod yang berniat jahat adalah lebih mudah untuk dikesan dan ditamatkan daripada rangkaian. Berdasarkan perbandingan keputusan eksperimen melalui pelbagai senario, kajian ini menemukan bahawa kaedah yang dicadangkan amat berkesan untuk menyelesaikan masalah keselamatan dan pada masa yang sama berfungsi dengan nisbah prestasi yang baik.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS

4iR	Fourth Industry Revolution
GiB	Gigabyte
ACL	Access Control List
ADD	Authorization Delegation Discovery
AES	Advanced Encryption Standard
AH	Authentication Header
AI	Artificial Intelligence
AKD	Asynchronous Key Distributor
ARP	Address Resolution Protocol
ANN	Artificial Neural Network
BGP	Border Gateway Protocol
BU	Binding Update
CA	Certificate Authority
CGA	Cryptography Generated Address
CN	Correspondent Node
CND	Compact Neighbour Discovery
CoA	Care-Of Address
CPU	Central Processing Unit
CVE	Common Vulnerabilities And Exposures Database
DAD	Duplicate Address Detection
DAD-h	Duplicate Address Detection Hash
DARPA	Defence Advanced Research Projects Agency
DDoS	Distributed Denial Of Service
DES	Discreet Event System
DHCP	Dynamic Host Configuration Protocol

DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DST	Destination
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve DSA
ESP	Encapsulating Security Payload Header
EUI	Extended Unique Identifier
FSM	Finite State Machines
GPGPU	General-Purpose Graphical Processing Units
HA	Home Address
HAVEGE	Hardware Volatile Entropy Gathering And Expansion
HTTP	Hyper Text Transport Protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMP v4	Internet Control Message Protocol Version 4
ICMP v6	Internet Control Message Protocol Version 6
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IID	Interface Identifier
IKE	Internet Key Exchange
IOS	Internetwork Operating System
IoT	Internet of Things
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol Version 4

IPv6	Internet Protocol Version 6
ISATAP	Initiates An Intra-Site Automatic Tunnel Addressing Protocol
IS-IS	Intermediate SystemTo Intermediate System
ISO	International Organization Of Standardization
ISP	Internet Service Providers
LAN	Local Area Network
LBA	Linux Before Attack
LDA	Linux During Attack
LTA	Local Ticket Agent
MAC	Machine Address Code
MBps	Mega Byte Per Second
MCGA	Multi-Key Cryptographically Generated Addresses
MD5	Message Digest 5
MIPv6	Mobile IPv6 Protocol
MITM	Man In The Middle
MLD	Multicast Listener Discovery
MN	Mobile Node
MT6D	Moving Target IPv6 Defence
MTU	Maximum Transmission Unit
NA	Neighbour Advertisement
NAT	Network Address Translation
NC	Neighbour Controller
ND	Neighbour Discovery
NDP	Neighbour Discovery Protocol
NDPmon	Neighbour Discovery Monitor
NG	Neighbour Group

NH	Next Header
NIT	Neighbour Information Table
Nmap	Network Mapper
NS	Neighbour Solicitation
NTP	Network Time Protocol
NUD	Neighbour Unreachability Detection
OS	Operating System
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PKI	Public Key Infrastructure
PMTU	Path Maximum Transmission Unit Discovery
QoS	Quality Of Service
RA	Router Advertisement
RFC	Request For Comments
RH0	Type 0 Routing Header
RIPng	Routing Information Protocol Next-Generation
RM	Redirect Message
RPKI	Resource Public Key Infrastructure
RS	Router Solicitation
RSA	Rivest, Shamir,Adleman
RST	Rivest, Shamir,Tauman
RSVP	Resource Reservation Protocol
RTT	Round Trip Time
SA	Security Association
S-ARP	Secure Address Resolution Protocol
SAVI	Source Address Validation Improvement

SDN	Software Defined Network
SeND	Secure Neighbour Discovery
SHA-1	Secure Hash Algorithm
SLAAC	Stateless Address Auto Configuration
SNDP	Scalable Neighbourhood Discovery Protocol
SNMP	Simple Network Management Protocol
SRC	Source
SSH	Secure Socket Host
S-UARP	Upcoming Secure Unicast Protocol
SUCV	Statistically Unique And Cryptographically Verifiable Addresses
SVM	Support Vector Machine
TAO	Trust Advertisement Option
TB-CGA	Time-Based CGA
TBS	Trust Based Security
TCP	Transfer Control Protocol
TLS	Transport Layer Security
TLV	Type-Length-Value
T-NDP	Trust Based Neighbour Discovery Protocol
TR2PA	Trusted Router-To-Router Passport Advertisement
TR2PS	Trusted Router-To-Router Passport Solicitation
TRDP	Trusted Router Discovery Protocol
TRPA	Trusted Router Passport Advertisement
TRPS	Trusted Router Passport Solicitation
Trust-NA	Trust Neighbour Advertisement
Trust-NS	Trust Neighbour Solicitation
Trust-RA	Trust Router Advertisement

Trust-RS	Trust Router Solicitation
TSO	Trust Solicitation Option
UDP	Unit Datagram Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point
WBA	Windows Before Attack
WDA	Windows During Attack

CHAPTER I

INTRODUCTION

1.1 RESEARCH BACKGROUND

Due to the increasing in number of hosts in Internet, experts of networking and data communication expect that Internet Protocol Version 6 (IPv6) and its relevant protocols will soon override Internet Protocol Version 4 (IPv4) and totally replace it. One primary protocol from the IPv6 suite is the Neighbour Discovery Protocol (NDP) (Gelog et al. 2011).NDP is constituted as a replacement for the function of Address Resolution Protocol (ARP) in IPv4. Nodes use NDP service as a protocol to perform an array of functions. These functions are made up of non-router related or host specified functions, together with router definite functions. NDP perform a number of tasks including examination of the local link for the link-layer addresses of the other nodes, the discovery of routers, the detection of unreachable local nodes, resolving duplicate addresses, and redirection to more appropriate routers (redirect). In addition, it constitutes and employs nodes in an IPv6 network as a learning mechanism of the local network to identify the IP and MAC addresses and the prefixes of the routers(Nikander et al. 2004).Hosts and routers employ NDP to keep a record of all reachable neighbours while detecting all changes in link-layer addresses. This allows rapid purging of invalid cache values while also enabling packet forwarding by detecting neighbouring routers. This function is important in the event of router failure, whereby functioning alternates are actively searched for.

NDP procedures and its messages determine how close nodes communicate with each other in a link. NDP operates alongside IPv6, while interchanging link-layer addresses at the same time.Internet Control Message Protocol (ICMP) redirects data and ICMP router discovery are also carried out by NDP. Securing NDP is a necessary,

especially for open network environments wherein joining a local link requires minimal or no link-layer authentication (C. Castelluccia 2004). Protecting NDP is important as it is frequently subjected to attacks (Alsa'Deh et al. 2013)known to cause disruption in the flow of IP packets. When this protocol is disrupted, IP traffic is threatened. NDP is a particularly vulnerable protocol given that it can be accessed or manipulated via hosts and routers thereby raising several serious security threats (F. A. Barbhuiya et al. 2013).

1.2 RESEARCH MOTIVATION

The Fourth Industry Revolution (4iR) already takes its place and become a fact. Internet of Things (IoT) and Big Data are primary components that play a fundamental role toward this revolution. As the number of connected devices is in a high accelerator (more IP addresses are needed) and data transmission rates become bigger and bigger (secure communication is in demand). IPv6 became an essential and un-avoidable protocol that satisfies these technical needs for IoT and Big Data respectively.Even though IPv6 has been around for more than 16 years, most organizations are still planning to deploy IPv6 or have only deployed it partially. The migration from IPv4 to IPv6 has taken a long time due to a number of reasons including threats related to IPv6 security. When NDP was initially innovated there was a belief that nodes within the same link trust each other. When it came into implementation this assumption was wrong. Because any one within a wireless environment, such as airports and public coffee shops, can join the link easily and start threaten other joined nodes. NDP the core protocol of IPv6 vulnerable to many Denial of Service (DoS) attacks causing computers to crash. The down-time of these computers causes organizations, especially in the banking and e-commerce era, to pay a very high cost. Since its early stage of development, and up to the date of this research, IPv6 NDP still faces the problem of these vulnerabilities. Although only one industry standard solution have been proposed, secure Neighbour discovery (SeND), but still the solution itself is vulnerable to several DoS attacks. In addition the cost of using it is very high from computer resourcesperspective, which make it non-applicable for devices with limited resources and specifications.

1.3 PROBLEM STATEMENT

When IPv6 NDP defined, it was assumed that the local IPv6 link would consist of mutually trusting nodes. However, the recent developments, especially in wireless networks, have radically changed the situation (S. Praptodiyono et al. 2015). NDP lacking authorization and is vulnerable to various DoS attacks that cause IPv6 network to behave abnormally (R. M. A. Saad 2015), (O. E. Elejla et al. 2016), (Y. Lu et al. 2017). Those attacks include Router Solicitation (RS) DoS attack, Neighbour Solicitation (NS) DoS attack, Router Advertisement DoS (RA) attack, Neighbour Advertisement (NA) DoS attack, Reply attack and Duplicate Address Detection DoS (DAD) attack (G. Song & Z. Ji 2016). To address the security problems of NDP, the Internet Engineering Task Force (IETF) provided a definition for a set of improvements to the NDP that form the Secure Neighbour Discovery (SeND).SeND considered an extension of the NDP and it provides three more features; message protection, address ownership proof and a mechanism for router authorization (A. Alsadeh et al. 2013). Even though SeND has shown good potential for protecting NDP messages, SeND itself is vulnerable to several DoS attacks in addition to many other security attacks (A. Alsadeh et al. 2012). Moreover SeND is inadequate in respects to computation cost and deployment. IPv6 mapping to OSI model and NDP main functions is shown in Figure 1.1.

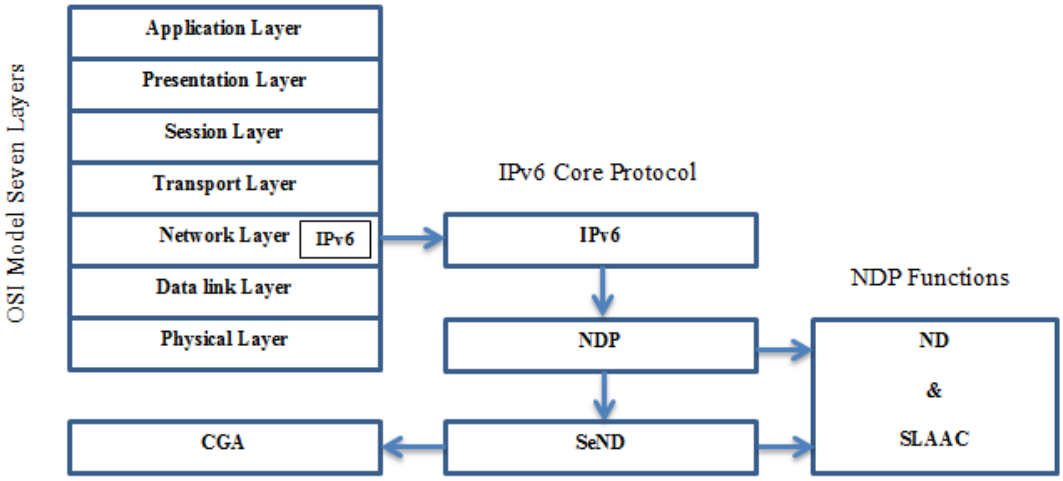

Figure 1.1 IPv6 mapping to OSI

The aim of this research is to investigate security threats that the protocol may face and improve the performance of IPv6 NDP as well as security. NDP is the core protocol of IPv6 (Y. Lu et al. 2017), consequently examination and investigation of its threats and introducing mechanisms to improve it is an important. The thesis objectives are:

1. To identify and implement security threats of IPv6 link-local communication.
2. To evaluate and analyze the impacts of Neighbour Discovery Protocol attacks on IPv6 networks operations and performance.
3. To develop a new model that overcomes DoS security threats for SeND-Based cryptographically generated address (CGA).
4. To enhance performance of SeND-based CGA in terms of generation cost by using lightweight cryptographic hash function.

1.4 RESEARCH CONTRIBUTIONS

The thesis explores mechanisms to deploy IPv6 NDP securely while keeping and maintaining low deployment cost and without modifying the standardization manner of the protocol. The detailed contributions of the thesis are as follow:

i. A complete test-bed setup has been introduced to implement and analyse behaviour of IPv6 NDP when it is under normal operations or under attacks by different types of NDP DoS attacks over multiplatform environments.

ii. Impacts of DoS attacks over IPv6 NDP has been implemented and evaluated, the behaviour of the network has been monitored and three network metrics have been selected for the evaluation purpose.

iii. A new approach to overcome DoS attacks over SeND-based CGA has been introduced. Sender's Interface Identifier (IID) and packet time stamp were incorporated in the new model to detect non-legitimated nodes within a link.

iv. The performance of the SeND protocol has been improved and enhanced using a lightweight cryptographic hash function MD5 in particular. Consequently computer resources are saved by reducing the generation costs of IPv6 address.

A mapping between research contributions and the research objectives and how we achieved these objectives is shown in Figure 1.2.

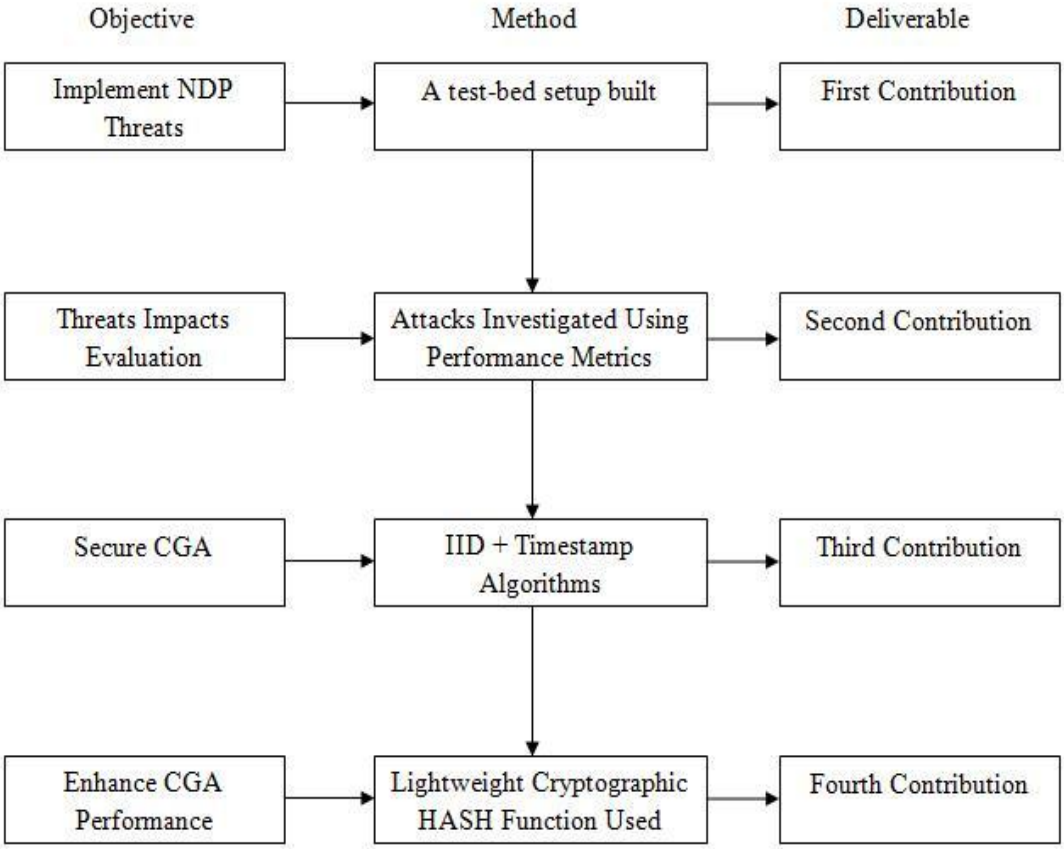

Figure 1.2 Research Objectives and Contributions Mapping

Network engineers have spent years improving IPv4 security, and vendors have continued to provide several features in devices to protect networks from IPv4 attacks. Given the vulnerability of IPv6 to many attacks, similar to the attacks used against IPv4, vendors have begun integrating similar features in IPv6 devices. However, IPv6 has new features that may be misused by attackers. In these features is where a gap exists in vendors' solutions and network engineers' understanding of IPv6 attacks. Various types of attacks, such as denial-of-service (DoS) attacks, can be used to exploit the new features in IPv6. Other threats to IPv6 include extension headers, fragmentation attacks, reconnaissance, link deterioration and smurf attack. Thisresearch investigates IPv6 NDP DoS attacks, which are classified into three types, namely, routing, non-routing and redirect attacks. A test-bed to implement NDP DoS attacks is introduced, and the influences for DoS attacks are closely monitored. Three performance metrics are used to evaluate attacks on network and computer operations. A trade-off between performance and security is performedbyintroducing two models,

namely, CGA-Lighter and Locked-CGA. SeND-based CGA DAD DoS attacks and SeND-based CGA parameters DoS attacksare defended by Locked-CGA. Meanwhile, the performance of NDP is enhanced by reducing the address generation time on the Lighter-CGA model.

1.5 RESEARCH FRAMEWORK

This research is conducted in eight phases (P1–P8) as shown in Figure 1.3. Phases1 and 2 include building a preliminary literature review from several published sources, including journal articles, proceeding papers and books related to the research area, in addition to identifying and formulating the problem statement.

Phase 3 includes building a comprehensive and intensive literature review from all types of published documents, such as papers, surveys and books related to the research scope. A gap in the research area is identified in Phase 3 as well. Phase 4 includes conducting and deploying a real test-bed setup to evaluate the impact of different NDP DoS attacks on the operations and performance of an IPv6 network.

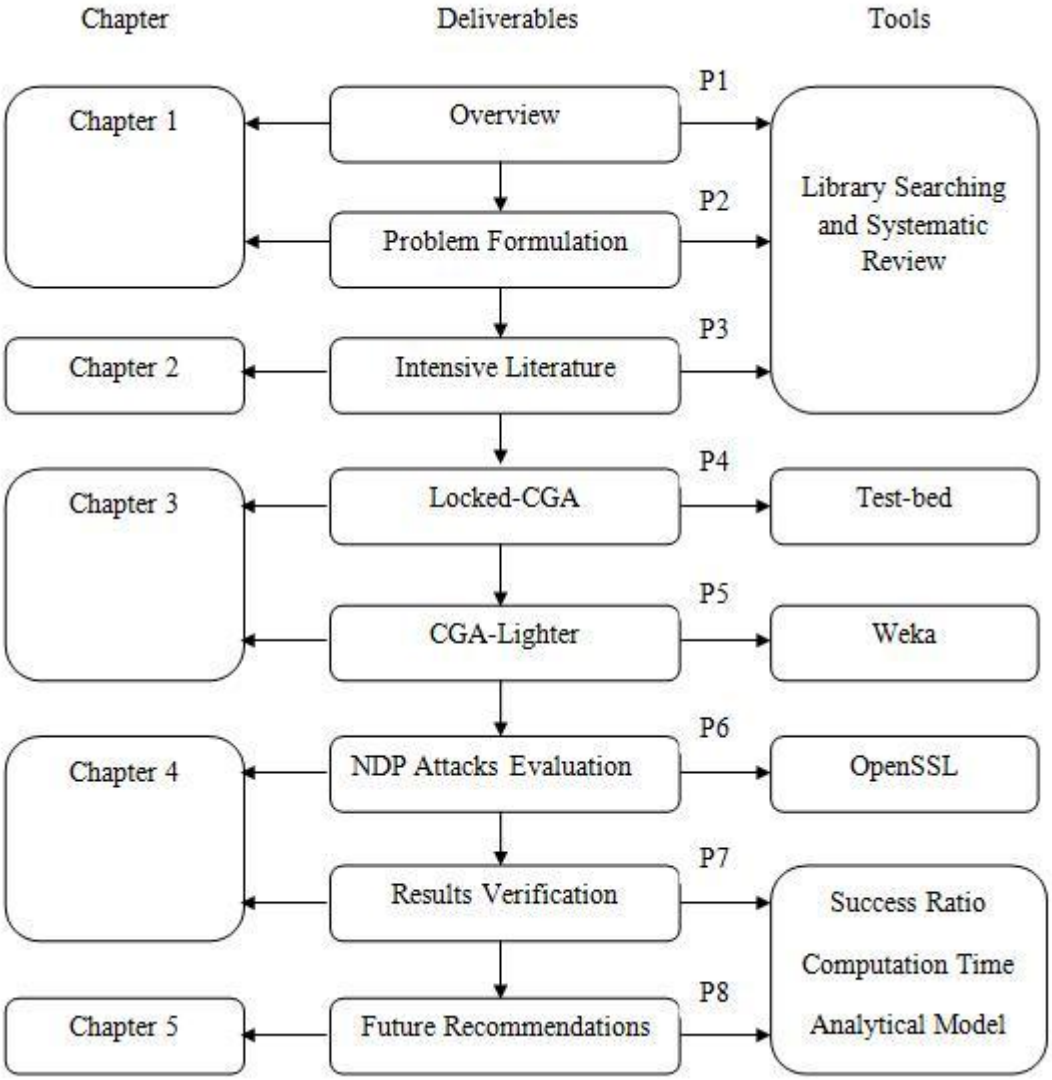

Figure 1.3 Research Framework

An analysis onthe effects of flooding-based attacks isperformed using three performance metrics, namely, throughput, round-trip time (RTT) and computer resource consumption.

In Phase 5, a lightweight cryptographically generated address, named CGA-Lighter (Model1), is developed using message digest 5 (MD5) cryptographic hash function. In a mobile environment wherethe nodes have limited resources, the usage of a heavy hash function to generate cryptographic addresses will draw back the network performance and affect it negatively. MD-5 and SHA-1 are algorithms that are considered secure because no known methods, except brute force that will

necessitate many years to break through one big message digest, can locate any collision. Should speed be of concern, then using MD-5 may be ideal because its operation will result in a faster performance than SHA-1 and will remain secure enough for numerous applications (Silva 2003).

In Phase 6, a security intrusion detection model, namely, Locked-CGA (Model2), thatusesthe packet time stamp and interface identifier (IID) of the sender is developed. Phase 7 includes verification of the twomodels proposed. Three methods are used to evaluate and validate the computational complexity, mathematical modeling and success percentage ratio of the modules. Phase 8 concludes with the attacks covered and not covered by the thesis and finally provides recommendations for future work.

1.6 THESIS STRUCTURE

This thesis comprises six chapters. Chapter I covers the introduction to the research. It contains a discussion on IPv6 and why it is neededto present the motivation for this research, followed by the research objectives and contribution. Chapter II describes the features and benefits of IPv6 andits addressing architecture and schemes. It describes NDP, which is the auxiliary protocol of IPv6,and explains its components. In this chapter,the threats related to both protocols, IPv4 and IPv6, are compared, and a detailed discussion of IPv6 attacks, how NDP messages are used and how flooding attacks can occur is also presented. The attacks of IPv6 that do not belong to NDP are discussed as well. In the last part of Chapter II, an intensive literature review in the area and the criticismson researchers' proposed approaches arepresented. The industries implement two solutions for securing NDP, namely, SeND and IPSec, whichare also covered in this chapter. Furthermore, details and weaknessesof each solution are presented.

The hypotheses and the research method are introduced in Chapter III. The steps used in conducting the research methodology are outlined,followed by the data collection process. This chapter contains details on the hardware and software used to set up the network test-bed in the computer laboratory to evaluate the impact of NDP DoS attacks on an IPv6 network. Chapter IV describes the tools used to conduct the

experiment and includes details on how data are collected and processed. At the end of this chapter, the analysis of TCP throughput, TCP RTT and CPU utilization results gathered from experiments using Windows and Linux platforms are presented.

Results gained for newly proposed models are validated in Chapter V. The results of three types, namely, programming, address generation cost and mathematical equations, are analyzed and compared with existing scenarios of current CGA to illustrate the efficiency of the research. Chapter VI contains the summary of thisthesis' achievements, contributions, scope and limitations, conclusions and future works.

CHAPTER II

LITERATURE REVIEW

2.1 INTRODUCTION

Three main parts are covered in this chapter, first IPv6 briefly introduced along with its features and benefits. In addition core protocol of IPv6 suite, NDP, covered in the part as well. Security threats for IPv6 are explained in the second part of this chapter, after which available security solutions to defend NDP are covered in details in part three. The reason behind Internet Protocol version 6 (IPv6) development is to address shortcomings of its predecessor, Internet Protocol version 4 (IPv4), mainly the size of its address space. New features needed in the modern world such as mobility and security is introduced on this occasion as shows in Figure 2.1.IPv6 has been developed for a rather long period of time. Internet Engineering Task Force (IETF) recommended IPv6 in [RFC1752], published in January 1995. Thus there have been rather big expectations from IPv6 over the years. Nevertheless, it should be always taken into account that IPv6 introduces changes at the third layer of the ISO/OSI model, outlined in Figure 2.2, while other layers are mostly unaffected. Possible drawbacks of other layers are still present and remain intact. Layer 3 of the ISO/OSI model, Network Layer, provides logical addressing which is used by routers for path determination. It is responsible for packet forwarding and data transfers among hosts on different networks. The most significant differences between IPv4 and IPv6 can be listed and briefly described in the following Section 2.1.1.

2.1.1 IPv6 Features and Benefits

There is a growing perception among communications experts that IPv6 and its associated protocols is set to soon replace the current IPv4. Because IPv4 is not capable to manage the growth of information systems, particularly the growth of

Internet technologies and services including cloud computing, mobile IP, IP telephony, and IP-capable mobile telephony, all of which necessitate the use of IPv6. Sufficient addressing space is the ultimate feature of IPv6 but it is not the only one, several other features that IPv6 had is described below.

a. AddressSpace and Addressing

Main reason for IPv6 deployment an IP address is 128 bits long, instead of 32 bits. This should provide enough addresses up to 2^{128} for foreseeable future. Addresses are usually written in hexadecimal notation. Multicast addresses designed for efficient one-to-many communication and anycast for redundant services are introduced. On the contrary, broadcasts are not implemented.

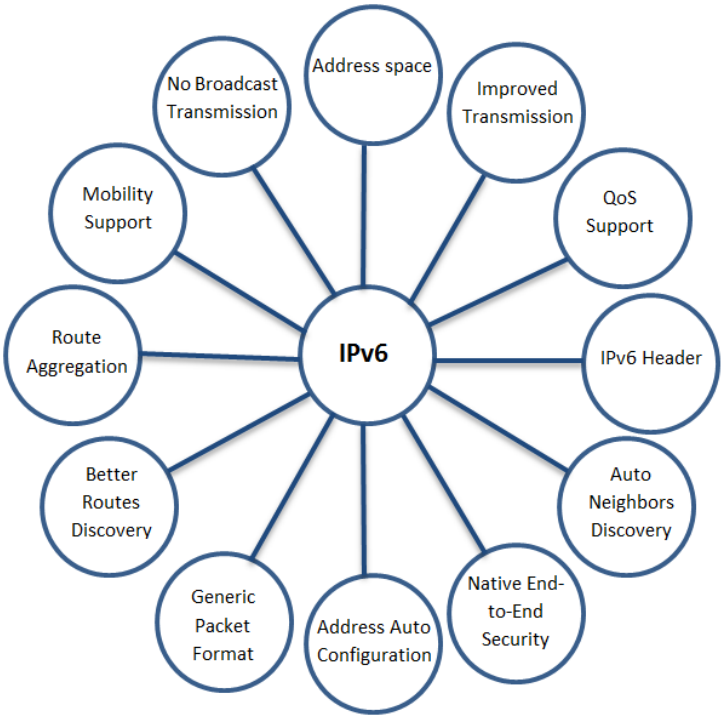

Figure 2.1 IPv6 Features and Benefits

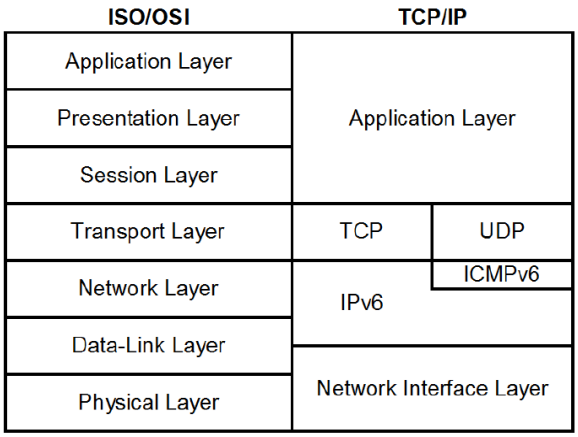

Figure 2.2 ISO/OSA Model and TCP/IP Stack

b. Route Aggregation

IPv6 addresses should be assigned hierarchically. The structure then provides for simple summarization and consequently for lighter exchange of routing information on the Internet. The large address space allows organizations to obtain continuous blocks of addresses, which should be assigned by Internet service providers.

c. IP Header

New header format is defined in [RFC4862]. In-depth description can be found therein this document. It has a fixed length of 40 bytes and is much simpler. Compared to IPv4 header, fields such as IP Header Length, Identification, Flags, Fragment Offset and Header Checksum are all removed. Figure 2.3 illustrates an IPv6 packet header format. With 40 bytes of fixed length and only 8 fields, the new header format can improve processing speeds. Every packet has this base header, which can be followed by an extension header defined in Next Header field. Such chaining is outlined in Figure 2.4.

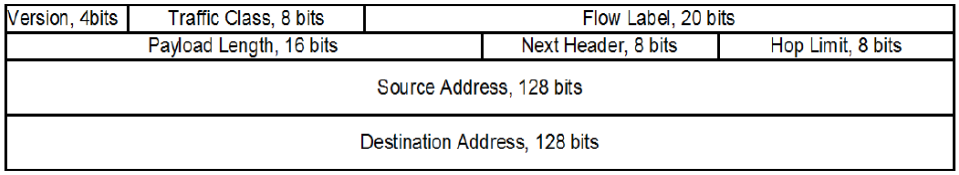

Figure 2.3 Format of IPv6 Packet Header

There can be several chained headers in one packet. [RFC2460] defines six types of extension headers: Hop-by-hop Option Header, Routing Header, Fragment Header, Destination Options Header, Authentication Header (AH) and Encapsulating Security Payload Header (ESP). The latter two will be discussed in detail in Section 2.32.

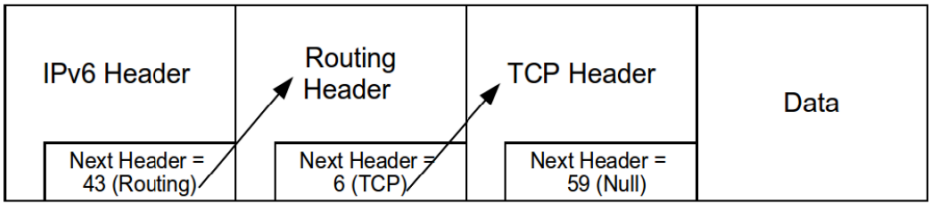

Figure 2.4 IPv6 Extension Headers Chaining Example

Fragmentation as known from IPv4 does not actually exist in IPv6. It does not happen at intermediate nodes. Packets can be fragmented at source nodes only [RFC2460]. Routers' need for fragmentation is eliminated by mechanism called Path Maximum Transmission Unit Discovery (PMTU) defined in [RFC2460]. This mechanism is used by nodes to determine a maximum transmission unit size. The source node then uses Fragment Header when packet fragmentation is needed.

d. Qos Support

Quality of Service (QoS) support is facilitated within the IPv6 packet. Flows can be labeled (using Traffic Class and Flow label header fields), enabling routers to recognize appropriate flows to which packets belong and making it possible for high priority packets to arrive to their destination in a timely manner. More information can be found in [RFC2460].

e. Mobility Support

Mobile IPv6 protocol (MIPv6) brings support for moving a node from one network to another wihtout losing connectivity. By retaining its Home Address (HoA), nodes can disconnect and reconnect at different place in Internet topology as defined in [RFC1981]. The Vast address space is essential for this mechanism.

f. Native End to End Security

Unlike IPv4, where support for Internet Protocol Security (IPsec) is optional, its implementation in IPv6 is mandated. It provides data integrity by sender authentication and optionally data confidentiality through encryption. In the IPv4 world, IPsec typically provides security between border routers , typically for Virtual Private Network (VPN) access, due to Network Address Translation (NAT) limitations. There is no need for NAT in the IPv6 world; therefore IPsec can be utilized for securing end-to-end communications. However, use of IPsec is not required. IPsec will be discussed in detail in the Section 2.3.2. Main differences between IPv4 and IPv6 can be summarized as in Table 2.1

Table 2.1 IPv4 and IPv6 Differences (J. Davies 2012)

Property	IPv4	IPv6
Address size and network size	32 bits and 8 to 30 bits	128 bits and 64 bits
Packet header size	20-60 bytes	40 bytes
Header-level extension	Limited number of small IP options	Unlimited number of IPv6 extension headers
Fragmentation	Sender or any intermediate router allowed to fragment	Only sender may fragment
Minimum allowed MTU	576 bytes	1280 bytes
Path MTU discovery	Optional, not widely used	Strongly recommended
Address assignment	Usually one address per host	Usually multiple addresses per interface
Address types	Use of unicast, multicast, and broadcast address types	Broadcast addressing no longer used, use of unicast, multicast and anycast address types
Address configuration	Devices configured manually or with host configuration protocols like DHCP	Devices configure themselves independently using Stateless Address Autoconfiguration (SLAAC) or use DHCP

g. Stateless Address Auto Configuration

A new mechanism for assigning addresses within a subnet has been implemented in IPv6 to address the greater address space. This new mechanism allows for the machine joining the subnet, limited to subnets with a 64 bit address block [RFC3697], to determine its own address and is referred to as Stateless Address Auto Configuration (SLAAC) [RFC6275]. To facilitate this process, IPv6 contains the

Neighbour Discovery Protocol (NDP) [RFC4291] which dictates the message types and sequences for determining a valid address assignment. The NDP serves many functions such as SLAAC, discovery of other nodes on the link, determining the link layer addresses of those nodes, duplicate address detection, address proxy discovery, finding available routers and Domain Name System (DNS) [RFC4862] servers, and maintaining this information. NDP replaces the Address Resolution Protocol (ARP) used in IPv4. The SLAAC process is very simple and is illustrated in Figure 2.5. We will talk in details about NDP specifications and SLAAC procedure in Section 2.3.

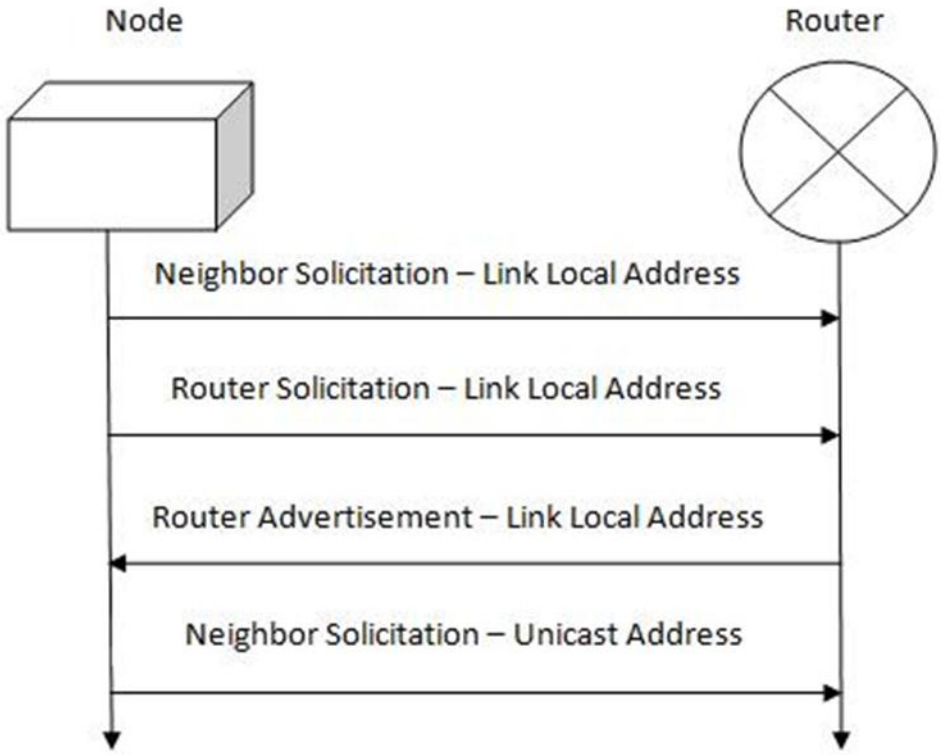

Figure 2.5 IPv6 SLAAC Message Exchange

The process starts with the node reserving its link-local address, which is an address for communication between machines on the same link. The node then sends out a NDP solicitation message to the router for a router advertisement message or waits for the periodic router advertisement message for the subnet information. The subnet information delivered includes the network portion of the IPv6 address and other optional information, including the DNS servers and Network Time Protocol

(NTP) [RFC4861] servers. To determine the second half of the node's IPv6 address, the node automatically configures an address, referred to as its interface identifier (IID) of the address. The node then combines these two pieces of information and attempts to allocate that address on the network. If the address is already allocated on the network, then the node goes through the Duplicate Address Detection (DAD) procedure and attempts the process again with a different IID.This process was designed to offload the administration of address allocation from the router to the entire subnet and is now included in the protocol. SLAAC allows for clients in a subnet to manage the available address space through mutual communication, which seen later will open up the protocol to exploitation from malicious clients.

h. Packet Format

To make the packet more generic so that it could be further extended in the future, the IPv6 standard modified the structure of the IPv4 packet format. The IPv6 header [RFC1043], consists of a fixed size block with minimal data required to detail the following payload for all packet types. This fixed size header contains the source and destination addresses, traffic classification options, the hop counter, and the type of optional extension or payload which follows the header. Designing the packet format in this manner allows for future development of options to be added to the IPv6 packet. The IPv4 packet did not have this functionality and packets had to be extended differently to accommodate features by passing them up to higher level layers. Unlike IPv4, the IPv6 protocol does not allow for packet fragmentation. It uses Path MTU Discovery (PMTUD) [RFC5908] to determine the largest maximum transmission unit (MTU) size between two hosts. The method relies on TCP to probe the path with progressively larger packets to determine the MTU [RFC2460], allowing for the entire packet to be processed at the maximum rate rather than in non-optimal pieces. These changes allow for greater extensibility of the IP and simpler processing.

2.1.2 IPv6 Addressing Schemes and Architectures

As we explain earlier, IPv6 was introduced IETF to replace IPv4. It was developed primarily due to the exhaustion of IPv4 addresses on the Internet. IPv6 provides many improvements over IPv4 including a larger address space (Sharma 2010).

Table 2.2 IPv6 Address Abbreviation

Details	Abbreviation
Full IPv6 address	2001:0db8:0000:0000:cafe:0000:1200:f1b2
Deleting leading zeros in each block	2001:0db8:0:0:cafe:0000:1200:f1b2
Double colon for consecutive zeros	2001:db8:cafe:0:1200:f1b2

Table 2.2 shows how IPv6 addresses are abbreviated. An IPv6 address is 128 bits in length and is represented in eight groups of hexadecimal values separated by colons. It is easier to read IPv6 addresses when they are abbreviated. The second abbreviation shown can only be used once (Weber 2013). In addition to the type of address shown in Table 2.2, there are some special IPv6 addresses. For example when a host joins a network, it has the unspecified address, 0:0:0:0:0:0:0:0 and is usually represented as two colons (::). Another special address is the IPv6 loopback address (::1) which is assigned to the network interface (Sanade 2014). IPv6 addressing models include unicast and multicast. Unicast addresses are used by a node to communicate with another node. On the contrary, multicast addresses are used by a node to communicate with multiple nodes. According to [RFC3513] an example of a multicast address is ff02::1. The address is known as the all-nodes multicast address. Each IPv6 interface has this address. Thus, a single packet can be sent to all interfaces within the local link using this multicast address. A node uses the unspecified address mentioned earlier as its source address before it has a configured IPv6 address. When an IPv6 node joins a network, it creates a link-local IPv6 address to establish a network connection. This usually occurs using an interface identifier for example, a Machine Address Code (MAC) address. Link-local addresses of nodes can only be used on the network link. They are not routable addresses so they cannot be used for communication between two networks (Sanade 2014).

Figure 2.6 shows examples of IPv6 addresses. Each interface has a link-local address. An interface usually uses one link-local and one or more global IPv6 addresses. Global IPv6 addresses are created by a node after it is able to configure a link-local address. A node sends a message to the all-routers multicast address, ff02::2 using its link-local address to find local routers. Routers in an IPv6 network join the all-routers multicast group (ff02::2). If a router is present, it will send prefix information to the node using the all-nodes multicast address, ff02::1 (Sanade 2014). Table 2.3 shows the address scheme used in IPv6.

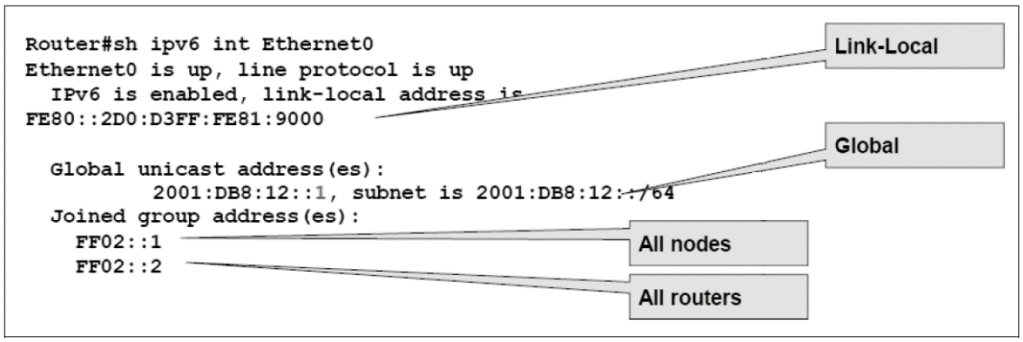

Figure 2.6 Examples of IPv6 Addresses

Table 2.3 IPv6 IPv6 Addresses Examples

Detail	Address
Global routing Prefix	2001:db8:72ed::/48
Global routing Prefix	0001
Subnet Prefix on that link	2001:db8:72ed:1::/64
MAC address from the interface	00:40:d0:8d:45:46
Interface ID with EUI-64card	0240:d0ff:fe8d:4546

The prefix identifies a network. Global addresses are generated using an interface identifier (normally a MAC address) just like link-local addresses, except that the prefix is obtained by the node from a router. Global IPv6 addresses are routable across the public Internet (Sanade 2014). Extended Unique Identifier (EUI-64) shown in Table 2.3 is the network interface identifier defined by Institute of Electrical and Electronics Engineers (IEEE) (J.Davies 2012).

2.1.3 Neighbour Discovery Protocol Specifications

The NDP summarized along with its working mechanism and technical specifications in the following section. The messages, message format processes and Neighbour Discovery's options will be covered as well.

a. Protocol Overview

RFC4861 describes a set of processes and messages featured in IPv6 NDP, which is a procedure through which the collaboration amongst Neighbouring nodes is determined. NDP was developed to overcome the limited functionality of IPv4. It also has a capacity to perform operations with IPv6 and substitutes the Internet control

Message Protocol (ICMP) Redirect message used in IPv4, ARP and ICMP router discovery [RFC4191]. Table 2.4 compares IPv4 Neighbour Messages, components, functions and their IPv6 Equivalents.NDP is employed by the nodes to perform a number of activities. These entail router specific tasks and router non-specific tasks. As far as the general tasks are concerned, the issues with the Neighbouring node regarding the link-layer address to which the IPv6 datagram is being forwarded are also settled. Moreover, the reachability of a Neighbour host or node together with its link-layer address is also determined by the NDP. Besides doing the automatic configuration of routes, addresses and prefixes along others parameters, NDP holds the potential to discover Neighbouring routers. Regarding routers, NDP looks up router alternatives for better next-hop performance to passing datagrams, to advertise router presence, perform configurations, on-link prefixes and routes.

b. Message Format

The Router Advertisement (ICMPv6 type 134), Router Solicitation (ICMPv6 type 133), Neighbour Advertisement (ICMPv6 type 136), Neighbour Solicitation (ICMPv6 type 135) and Redirect (ICMPv6 type 137) are among five different categories of NDP messages. To operate within an ICMPv6 message structure, the network experts have formatted all NDP messages in a special manner. Following components, such as a message header, an NDP message and ICMPv6 header – specific data and zero or more NDP options are part of messaging in NDP. To carry out specific functions, a number of options are available in NDP messages. Additional information is provided via these functions, for example, mobility information, redirection data, specific routes, indicating IP addresses and MAC, on-link MTU information and on-link network prefixes. Figure 2.7 shows the message format of NDP.

Table 2.4 IPv4 Equivalents to IPv6 Neighbour Messages and Functions

IPv4	**IPv6**
ARP Request	Neighbour Solicitation
ARP Reply	Neighbour Advertisement
Router Solicitation (elective)	Router Solicitation (mandatory)
Router Advertisement (elective)	Router Advertisement (mandatory)
Redirect	Redirect
ARP cache	Neighbour cache
Gratuitous ARP	DAD

c. Messages Types

The messages performing a number of functions related to IPv6 NDP were identified by [RFC2460]. These are:

i. Router Solicitation (RS)

ii. Router Advertisement (RA)

iii. Neighbour Solicitation (NS)

iv. Neighbour Advertisement (NA)

v. Redirect Message (RM)

i. Router Solicitation

The key concept behind RS messages is to allow nodes within a given subnet to explore the existence of IPv6 routers attached to this subnet. A message of multicast nature sent by hosts in the link, as immediate response a RA unicast message will be sent by the attached routers.

Figure 2.7 Neighbour Discovery Message Structure.

ii. Router Advertisement

The unsolicited RA messages are pseudo-periodically sent by the IPv6 routers—i.e., when a link contains multiple advertising routers, then the synchronization issues can be reduced by randomizing the interval between unsolicited advertisements. Upon receipt of a RS message, the solicited RA messages are also sent by the routers. The information needed by hosts is found in the Router Advertisement message so that it could determine the link Maximum Transmission Unit (MTU), the link prefixes, specific routes, the duration and validity of addresses created through auto-configuration and whether to use address auto-configuration or not.

iii. Neighbour Solicitation

To confirm a formerly established link-layer address or to discover the link-layer address of an on-link IPv6 node, the NS message is sent by the IPv6 nodes. The link-layer address of the sender is normally included in it. When the reachability of a neighbouring node is under verification, typical NS messages are unicast and they are multicast for the purpose of address resolution.

iv. NeighbourAdvertisement

In response to a NS message, the NA message is sent by an IPv6 node. The unsolicited NAs are also sent by this node so that the neighbouring nodes could be informed about changes in link-layer addresses or the node's role. The information required by nodes is kept by the NA so that the type of NA message, typically the link-layer address of the sender and the sender's role on the network could be determined.

v. Redirect

An originating host is informed about a better first-hop address for a specific destination after the RM is sent by an IPv6 router. Only routers send the RMs for unicast traffic. Moreover, only hosts process them and they are sent only to originating hosts. Table 2.5 summarize the messages types, name and ICMP number.

d. Protocol Options

NDP, as a core protocol of IPv6 came up with new options in terms of packet structure. In the following part NDP options are explained in details.

i. Source and Target Link-Layer Address Option

The link-layer address of the NDP message sender is signified by the Source Link-Layer Address option. All NDP messages except NA and RM include this option. When the source address of the NDP message is the unspecified (::), then the Source Link-Layer Address option is not included in above-said components.

Table 2.5 NDP Messages and Functions

Message Name	ICMPv6	Function
Router Solicitation	133	Router Discovery
Router Advertisement	134	Router Presence
Neighbour Solicitation	135	Neighbour Discovery
Neighbour Advertisement	136	Neighbour Presence
Redirect	137	Better Next Hop

ii. Prefix Information Option

For specifying information about address auto-configuration and address prefixes, the RA messages carry the Prefix Information option for its onward destination. A message of RA can have more than one prefix information option, thus specifying several address prefixes.

iii. Redirected Header Option

To specify the IPv6 packet through which a RM was sent by the router, the Redirected Header option is sent in RMs. Subject to the IPv6 packet that was sent in the beginning, it can contain all or part of the redirected IPv6 packet.

iv. MTUOption

To indicate the IPv6 MTU of the link, the RA messages carry the MTU option. The network analysts can use this option when the IPv6 MTU is not familiar for a link. This can be most probably due to a translational or mixed-media bridging configuration. As reported by interface hardware, the IPv6 MTU is overridden by the MTU option.

v. Route Information Option

To specify individual routes to affix to their local routing table, the RAs messages are to carry the Route Information option. The RFC4862 describes the Route Information option.

e. Protocol Functions

Given below are the numbers of objectives behind messages exchange within an NDP. these are:

i. Address resolution
ii. Duplicate Address Detection (DAD)
iii. Neighbour unreachability detection
iv. Router discovery
v. Redirect function

i. Address Resolution

As far as IPv6 nodes are concerned, an exchange of NS and NA messages are included in the address resolution process. For a given destination, resolving the link-layer address of the on-link next-hop address is the purpose of this inclusion. A multicast NS message is sent by the sending host on the appropriate interface. From the target IP address, the consequent solicited node multicast address is basically known as the multicast address of the NS message. In the Source Link-Layer Address option, the link-layer address of the sending host is included in the NS message. When the NS message is received by the target host, its own Neighbour cache is updated according to the source address of the link-layer address and the NS message. Afterwards, a unicast NA is sent by the target node to the NS sender. The Target Link-Layer Address option is included in the NA. Once the NA is received from the target, the sending host, subject to the information in the Target Link-Layer Address option, updates its Neighbour cache with an entry for the target. At this time, you can send the unicast IPv6 traffic between the target of the NS and the sending host.

ii. Duplicate Address Detection

For detection of a duplicate unicast IPv4 address on the local link, a method called gratuitous ARP and ARP Request messages is used by the IPv4 nodes. Likewise, to detect duplicate address use on the local link, the NS messages used by the IPv6 nodes

in a process known as Duplicate Address Detection (DAD), and this is explained in RFC4862. Keeping in mind the IPv4 gratuitous ARP, the ARP Request message header containing the Target Protocol Address and the Source Protocol Address fields are set to the IPv4 address for which duplication is being identified. As far as IPv6 DAD is concerned, the NS message based Target Address field is set to the IPv6 address for which duplication is being identified. Once the multicast NA is received with the Target Address field, the use of the duplicate IP address on the interface is disabled by the node. If a NA defending the use of the address is not received by the node, the address is then initialized on the interface. As far as anycast addresses are concerned, the DAD is not performed by an IPv6 node.

iii. Neighbour Unreachability Detection

Neighbouring node could be accessed only if it has been acknowledged that the neighbouring node had received and processed the IPv6 packets. It is not necessary that the end-to-end reachability of the destination is verified by the neighbour unreachability detection. Since the neighbouring node might not be the final destination of the packet, it can be a router or host. Only the reachability of the first hop to the destination is verified by the neighbour unreachability detection.

iv. Router Discovery

The process, where in, nodes trying to discover the set of routers on the local link is referred to as the “Router discovery”. In IPv6, the router discovery is analogous to the IPv4 based ICMP router discovery described in (Covenery & Miller 2004). A set of ICMP messages permitting IPv6 hosts to decide the existence of local routers is referred to as the ICMPv6 router discovery, whereby automatic configuration of local router as a default gateway is to be determined besides its auto switching to a different router as their default gateway when the current default gateway is inaccessible. An Advertisement Lifetime field is featured by the RA message in ICMPv6 router discovery. The time after which the router can be considered unobtainable is referred to as the Advertisement Lifetime. A router can become unavailable in the worst scenario and identification of a new default router would not be attempted by hosts until the RA time has passed. Since the non-availability / inaccessibility of router is

determined by the Neighbour unreachability detection, the default router list is seen to immediately choose a new router or a RS message is sent by the host to determine the availability of additional default routers.

v. Redirect Function

To inform originating hosts about a better first-hop Neighbour to which traffic should be forwarded, the redirect function is used by the routers. The redirect is used in two instances. First, an originating host on the local link "closer" to the destination is informed by a router about the IP address of a router. A routing metric function for reaching the destination network segment is referred to as the "closer". When there are multiple routers on a network segment, this condition can take place and a default router is chosen by the originating host and it is not ("closer") one to reach the destination. Second, an originating host is informed by a router that the destination is a neighbour. When the prefix of the destination is not included in the prefix list of a host, this condition can take place. The packet is forwarded to its default router by the originating host because a prefix is not matched by the destination in the list. RMs between source and destination are sent only by first router. RMs are never sent by the hosts and the routing tables subject to the receipt of a RM are never updated by the routers. RMs are rate limited in the same way as ICMPv6 error messages.

2.1.4 IPv4 and IPv6 Threats Comparison

It cannot be decided whether IPv6 is more secure than IPv4 or not. IPv6 does not introduce a significant improvement apart from IPsec protocol. The differences between these two protocols are, in most cases, double-edged. Some security threats are very similar or have slightly different considerations; some were mitigated while others were newly introduced.

a. Threats with New Considerations

It cannot be decided whether IPv6 is more secure than IPv4 or not. IPv6 does not introduce a significant improvement apart from IPsec protocol. The differences between these two protocols are, in most cases, double-edged. Some security threats

are very similar or have slightly different considerations; some were mitigated while others were newly introduced.

i. Reconnaissance

Reconnaissance is first phase of every attack (together with information gathering) and therefore accomplishing good result in this phase is an important building block for subsequent phases. As mentioned earlier, IPv6 has different address scheme. It implies need for a different approach to reconnaissance. With 128-bit long addresses and typical subnet prefix of 64 it will be significantly time-consuming to scan the subnets for live hosts. Assuming 10,000 hosts uniformly distributed in such subnet and using traditional brute-force ping sweeps scan, "even at a scan rate of 1 million probes per second (more than 400 Mbps of traffic), it would take more than 28 years of constant scanning to find the first active host" (Convery, Sean & Miller 2004). With more typical subnet with 100 hosts, the math is even more interesting, "the number jumps to more than 28 centuries of constant 1-million-packet-per-second scanning to find first host on that first subnet of the victim network" [RFC4443]. However, several techniques to speed up this process exist. It can be expected that adversary will detour network scanning and focus rather on DNS servers. The servers will be precious source of information. Because IPv6 addresses are generally not easy to remember, dynamic DNS will likely be adopted by administrators. Any patterns or sequences in nodes addressing should be avoided.

ii. Smurf Attacks

Broadcast amplification attacks, often referred to as smurf attacks, are performed by sending ICMP echo request to a broadcast address with spoofed victims address as source address, as illustrated in Figure 2.8. All nodes on the broadcast domain then respond to this request by ICMP echo replies with the formerly spoofed address. The victim becomes overwhelmed with traffic causing DoS situation as a result.

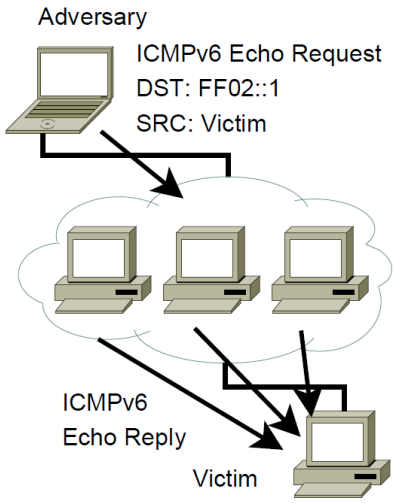

Figure 2.8 Smurf Attack Scheme

This technique is no longer possible with IPv6 because there are no broadcasts. However, multicast addresses can be used instead. Several multicast addresses are currently registered by Internet Assigned Numbers Authority (IANA).

Address FF02:0:0:0:0:0:0:1, or FF02::1 for short, represents all nodes on a segment. So it can be a great replacement for broadcast address in IPv4. This was taken into account by IETF and countermeasure is defined in RFC4443. ICMP replies should not be generated in response to ICMPv6 messages having a multicast address as a destination. Therefore smurf attack should not be an issue in IPv6 network where all nodes are compliant to RFC4443. IPv6 cannot function without ICMPv6 as its functionalities are a vital part of the protocol [RFC4890]. Consequently, it cannot be completely filtered out like it is often done in IPv4. Attention should be paid to ICMPv6 filtering. IETF defines recommendations for ICMPv6 messages filtering in RFC2827.

iii. Address Spoofing

IP address spoofing is widely utilized by adversary to hide origin of the attack and therefore their identity. The packets are crafted with a falsified source IP address, usually from completely different location. RFC2385 defines protection against spoofing of the network portion of an address. This is done by filtering on the

network's edge, where packets with source address outside the valid subnet range are dropped. However, it is not very commonly used countermeasure. IPv6 Internet should benefit from hierarchical address assignment, allocations became easily to summarize. As a result, spoofing-preventing filtering should be much easier and in effect more appealing for Internet Service Providers (ISP) to be implemented. Even without spoofing outside of customers address ranges, there is a vast range of addresses to be spoofed from within typical IPv6 subnets (264 addresses with 64 prefix).

iv. Routing Security

Corruption of routing information can lead to traffic redirection or connectivity disruption. Exchange of routing information should be well protected. In IPv4, routing protocols are commonly protected using cryptographic authentication. Being extended for IPv6 support, these protocols can be divided into two groups. First, protocols as Border Gateway Protocol (BGP) and Intermediate System-to-Intermediate System (IS-IS) did not change their security mechanism with transition to IPv6. BGP authentication uses TCP Message Digest 5 (MD5) signatures based on secret key shared by appropriate endpoints [RFC3567]. Similarly, ISIS exchanges routing information with keyed-hash message authentication code based on MD5 algorithm (HMAC-MD5), which provides integrity and authentication (Hogg &Vyncke 2011). Second, Open Shortest Path First version 3 (OSPFv3) and Routing Information Protocol Next-Generation (RIPng) have removed the means of authentication. They both rely on IPsec to provide protection to routing information exchange [RFC3315].

v. ARP and DHCP Attacks

Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) are the protocols responsible for host initialization in IPv4 networks. Host initialization via DHCP is vulnerable to spoofed responses from rogue DHCP servers. Information obtained from DHCP is IP address, DNS server address and default gateway. When replaced by adversary, it enables MITM attacks (Carnut, M & J. Gondim 2003). ARP is used for resolving MAC-IP address pairs. It can be spoofed as well, thus again enabling MITM attacks.

There is no ARP on IPv6 networks. This functionality was replaced with NDP mechanism provided by ICMPv6. Threats endangering NDP are discussed in details in Section 2.2.3. Although the function of DHCP can be partially replaced by stateless address Autoconfiguration (SLAAC), it does not provided information like DNS and NTP servers (J. L. & J. Parvez 2015). SLAAC can be complemented or completely replaced by DHCPv6. DHCPv6 is not an extension of traditional DHCP it is a new protocol defined in (Hogg &Vyncke 2011). Unfortunately, it is vulnerable to very similar threats. It can face starvation or DoS when too many addresses is requested it has no additional security for preventing rogue devices. When DHCPv6 with sequential allocation is in place, it can spare a lot of adversary's time needed for network scanning.

vi. Internet Worms

Worms are a type of malware designed to exploit a specific vulnerability in a system and then use it to propagate to other systems through the same flaws. Worms may be used to spread virus infection, Trojan horses and so on. Worms together with viruses are a significant problem of today's networking. The basic principles of worms infection does not change with IPv6. It affects ability to propagate of those worms which utilize network scanning to find new targets. The vast and sparsely populated address space of IPv6 will definitely slow down the worm propagation. Other forms of proliferation (through email, instant messaging, peer-to-peer application etc.) remain the same. It can be expected that worm developers will focus on these means of propagation or new techniques will be adopted. According to [RFC2460], these could be for example: targeting DNS lookups, sniffing NS packets and routing updates or exploit multicast addresses.

b. Newly Introduced Threats

New functionalities always broaden the attack surface available for adversary. As security becomes more and more crucial nowadays, the security aspects should be always considered when designing new feature. To avoid unnecessary risk exposure, unused features and service should be always disabled or handled properly, initialized to zero.

i. Extension Header Threats

Extension headers in IPv6 are places where all options from IPv4 packet header were moved to. Extension header is specified in Next Header (NH) field of the preceding one. Recommended order of the headers in a packet as per RFC 2460 follows:

- IPv6 Header
- Hop-by-Hop Options Header
- Destination Options Header
- Routing Header
- Fragment Header
- Authentication Header
- Encapsulating Security Payload Header
- Destination Options Header
- Upper-layer header

The headers can be chained and used multiple times almost without restrictions. RFC2460 states that IPv6 nodes must accept and attempt to process extension headers in any order and occurring any number of times in the same packet, except for the Hop-by-Hop Options Header which is restricted to appear immediately after an IPv6 header only. Sending bogus or endless combinations may lead to increased resources consumption and eventually to DoS. The headers may be also crafted in a way to bypass security systems. Additionally, there are some specific threats linked to Hop-by-Hop Options Header and Routing Header.

ii. Hop-by-Hop Options Header

It is the first extension header to appear in a packet. It contains information that must be processed on every intermediate node. Structure of the header is outlined in Figure 2.9. One of the options is the Router Alert option which indicates that a router should inspect the packet as the information it carries may be valuable for the router. Flood of

packet with this option may decrease performance or even cause DoS. According to RFC2675, the Router Alert option can be misused to bypass access list (ACL) restrictions. (Heuse 2012) describes a situation, where ICMPv6 Echo Request message with Router Alert option by pass ACL restriction. The request is allowed although it was forbidden by ACL. Another possibly problematic option is the Jumbo Payload option. IPv6 jumbograms defined in (Heuse 2012) are packets that carry payload bigger than 65 535 octets. These packets can be misused to cause DoS by consumption of resources. Proper inspection of jumbograms will very likely be challenging for security systems such as firewalls and IDS/IPS (Rash et al. 2005).

Furthermore, most of the IPsec implementations do not support jumbograms (Frankel et al. 2010).

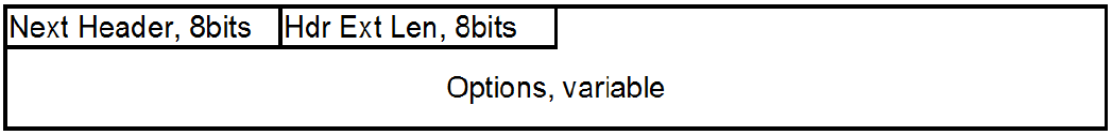

Figure 2.9 Format of Hop-by-Hop Header

iii. Routing Header

This type of header, with structure as outlined in Figure 2.10, is used to list intermediate nodes the packet should pass through on its way to the destination. Currently, there are three types of Routing Header - Type 0, 1 and 2. Type 2 is used for MIPv6 (Davies, J. 2012). Type 1 is used by a Defense Advanced Research Projects Agency (DARPA) project and Type 0 is currently deprecated by [RFC5095] due to severe security ramifications. It could be used to launch MITM or DoS attacks, bounce traffic off a host to bypass security restrictions, etc. Packets with Type 0 Routing Header (RH0) must not be processed by nodes and is no longer required to be implemented.

Next Header, 8bits	Hdr Ext Len, 8bits	Routing type, 8bits	Segments Left, 8bits
Type-specific data, variable			

Figure 2.10 Format of Routing Header

iv. Neighbour Discovery

As it has been already mentioned previously, NDP is a replacement of ARP which is based on elements of ICMPv6. ICMPv6 is inseparable part of IPv6 protocol and cannot be completely filtered out. Elements of NDP provide:

- Autoconfiguration, prefixes and other configuration
- Duplicate Address Detection
- ARP-like address resolution
- Neighbouring routers discovery
- Neighbour Unreachability Detection
- Redirection

Most of these mechanisms can be exploited for malicious activity. Formerly, no additional security to this mechanism was introduced. The NDP itself is vulnerable to different types of spoofing, redirection, reply and DoS attacks. The attacks will be described in detail in Section 2.2.3. IETF later on specified Secure NeighbourDiscovery (SEND) in RFC3971. SEND uses Cryptographically Generated Addresses (CGA) defined in RFC3972 to improve security of NDP. CGA are based on asymmetric cryptography, namely (RSA) Rivest, Shamir,Adleman algorithm. When using CGA, the lower 64 bits of their IPv6 address are generated from the network prefix, random number and public key using secure hash function (SHA-1). The parameters are then sent by NDP so it can be verified by a communication partner. The whole SEND message is digitally signed. However, CGA may also be exploited for DoS attacks. Details about SEND and CGA will be covered in details in Sections 2.3.3 and 2.3.4 respectively.

v. Quality of Services

The threats associated with IPv6 (QoS) are not of high severity. The header fields, Type of Service and Flow Label, are not protected from tampering, RFC3697 specifies them as non-alterable. An adversary can gain benefits by modifying these

fields while in transmit, leading into fraudulent use of preferred traffic streams. Firewalls, ACLs and IDS/IPS solutions should not make decisions based only on these fields. QoS can be used together with IPsec so it should be taken into account that information about upper layer protocols may not be accessible for inspection.

vi. Mobile IPv6

Although MIPv6 was designed with security as a primary concern (Frankel et al. 2010), several opportunities for malicious activity were left open. MIPv6 is susceptible to wide range of attacks such as rogue home agent, MITM threats, interception, hijacking, spoofing and DoS attacks. As nodes are moving, centralized security systems are bypassed so security of the mobile devices should be put into the spotlight.Most attacks involve modifying or forging Binding Update (BU) messages, IPv6 headers, home or Care-of Address (CoA) (Frankel et al. 2010). Attacks including DoS opportunities, taken from (Frankel et al. 2010), are as follows:

- Inducing extra BUs with bogus CNs (Correspondent Node). Although no satisfactory defence exists, route optimization is optional, and the trade-off is to risk suboptimal routing. An MN (Mobile Node) can be selective about route optimization
- Preventing a legitimate BU from completing while sending bogus BU to CN (where the attacker is on the same link as the victim)
- Reflection attacks, whereby the victim's address is forged as the source, so that the victim is flooded with replies
- Replying old route optimization BUs, especially if sequence numbers are unreliable because of crashes or rollover
- Bypassing firewall egress filtering with a forged Home Address Option

c. IPv6 Latent Threats in IPv4 Networks

Last in this section are IPv6 latent threats in IPv4 pure networks. These threats should be mentioned in this research as well, because they were introduced together with IPv6 support on network devices and operating systems. The fact that IPv6 is not in

use on particular network does not mean it should be ignored. As long as network devices understand the protocol and the features are not turned off, an attack can be performed over IPv6. The following actions can be performed by an IPv6-capable node on an IPv4 network. List is taken from (Hogg &Vyncke 2011).

- Roam to an IPv6-enabled wireless hotspot: The Router Advertisements (RA) sent by the wireless router immediately connects the host to the IPv6 Internet
- Receive a forged RA messages: The host is configured to use IPv6 (albeit with only local connectivity if the attacker does not forward the IPv6 traffic to the Internet)
- Use a routable IPv4 address: Enables IPv6to IPv4 connectivity to the Internet (assuming that there is no firewall blocking tunnelling protocol)
- Existence of the DNS name of isatap.example.org: Initiates an Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnel to this name (again assuming that there is no firewall blocking tunnelling protocol)

Teredo tunnel to connect to an IPv6-only mode: If the NAT firewall devices allow outbound Unit Datagram Protocol (UDP) packets and if the NAT function is quite open (not applicable to Internetwork Operating System (IOS) routers), a Teredo hole is punched in the firewall and allows every IPv6 Internet machine to connect to the Teredo client. Once connected to IPv6 network, all IPv6 security considerations applies to the node. It can face any of the threats mentioned in this chapter as well as dual-stack or transitions mechanisms (tunnels) related threats.

d. Indifferent Threats

Attacks which were not significantly altered by IPv6 introduction are listed and briefly discussed in this section.

i. Application and Other Layers Attacks

This section covers all attacks outside the third layer of the ISO/OSI model. These layers remain untouched by IPv6 adoption, so the same considerations applicable for IPv4 networks are applicable in IPv6 environment as well.

ii. Flooding

During this attack, a network service is flooded with more traffic that it is able to process. This leads to a DoS situation. Any IPv6 network faces the same challenges in the matter of defence against flooding attacks as an IPv4 network.

iii. Man-in-the-Middle

A MITM attack is act of eavesdropping on the network communications. It is often part of the gaining access phase of an attack. The mechanism is outlined in Figure 2.11. An adversary positions them self in the middle of communication stream (2), while the originally communicating entities still believe they communicate directly (1). The data can be modified or misused. Countermeasures for IPv6, such as IPsec or strong data encryption and mutual authentication, are the same as for IPv4. IPv6 functionalities may introduce new means to accomplish MITM attack.

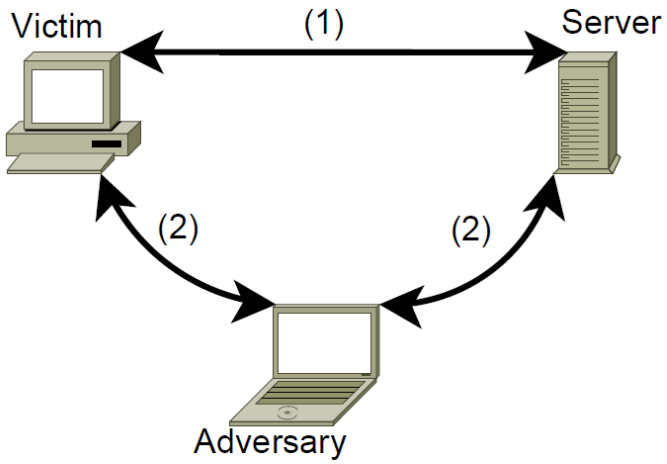

Figure 2.11 Man-in-the-middle Attack Scheme

iv. Rogue Device

Any unauthorized device on the network is called a rogue device. The most common rogue device threat, often called evil twin, is an unauthorized wireless access point (WAP) placed on a local area network (LAN). This type of threat is not changed for IPv6.

v. Sniffing

A sniffing attack occurs when an adversary tries and succeeds to capture network traffic without authorization. The captured traffic can be then used for data analysis or reply attack. Alike IPv4, the only mechanism to protect data transported over the network in IPv6 is encryption.

vi. Distributed Denial of Service

This kind of attack is very similar to abovementioned flooding attack, which is often referred to as denial of service attack. The Distributed Denial of Service (DDoS) attack leads to bandwidth or resources exhaustion as well but involves more then one attacking machine (usually hundreds to thousands). These machines were infected by malicious software which makes them "listen" to adversary's commands. When an adversary orders, the whole group of machines, called botnet, starts flooding the target. This type of attack remains present in the IPv6 world. Furthermore, IPv6 addressing makes it possible for more devices to join the Internet which can result in even more powerful DDoS attacks.

vii. Fragmentation Threats

Fragmentation in IPv4 was often used to bypass security systems and to hide attack patterns. Fragmentation as we know it does not exist in IPv6 where fragmentation by intermediary nodes is prohibited [RFC2460]. However, packets may be fragmented by the source node and therefore an adversary can use the same techniques to obfuscate attacks. Only minimum MTU differs, for IPv6 it is 1280 octets, and every fragment has to contain a Fragment Header (outlined in Figure 2.12). Packets smaller than

minimum MTU should be dropped unless it is the last fragment (More Bit, represented as M in Figure 2.12, is set to “0” value for the last fragment).

Next Header, 8bits	Reserved, 8bits	Fragment Offset, 13 bits	Res, 2bits	M, 1bit
Identification, 32bits				

Figure 2.12 Format of Fragment Header

2.2 SECURITY THREATS FOR IPV6

This section will cover the most effective currently known IPv6 attacks. It will be explained how the attacks work and how to perform them on a network so this knowledge can be based upon during the testing in Chapter 4. The attacks will be divided, quite unconventionally, not according to typology (DoS, MITM, etc.) or location of the adversary (local and remote) but into three plus one certain categories which better serve the purpose of this research. Namely Reconnaissance in Section 3.1, attacks over IPv6 in Section 3.2 and attacks over ICMPv6 in Section 3.3. In addition to one additional section which does not discuss particular attacks but implementation imperfections which are important and lively phenomenon of the new protocol, Implementation Maturity Problems - Section 3.4. Attacks of IPv4 and IPv6 and how they intersect are shown in Figure 2.13.

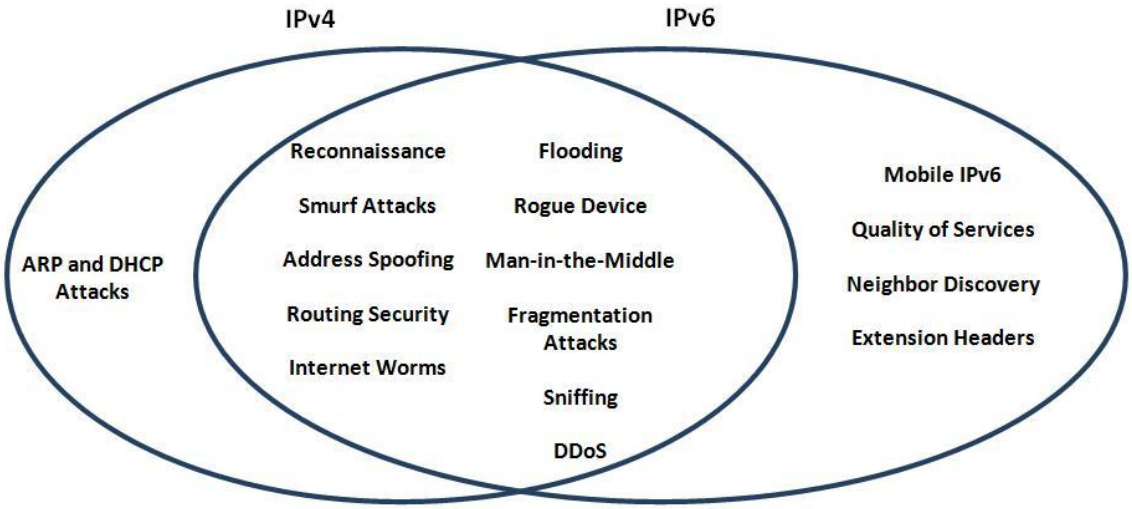

Figure 2.13 IPv4 / IPv6 Attacks Comparison

2.2.1 Reconnaissance Attacks

Only network scanning will be discussed in this section as port scanning and other kinds of information gathering was not changed for IPv6. Network Scanning is not feasible in IPv6 world, this is only partially true. Network scanning is indeed not feasible when the same techniques used for IPv4 networks are adopted. Simple brute force ping sweeps are not sufficient anymore. In IPv6 environment there are two separate areas of considerations for network scanning, namely local scanning and remote scanning. Local scans remain still rather easy. The address space is too vast and there are no broadcasts. Multicast cannot be simply pinged as per RFC4443. This is, however, true for hosts compliant to it. It can be said about only one from the two most widely used operating systems, Linux and Microsoft Windows. Surprisingly, it is Microsoft Windows but they adopted [RFC4443] with its exceptions as well and therefore the multicast can be successfully pinged. More will be discussed in Section 3.3.8. Local reconnaissance can be accomplished by other means as well. When an adversary has access to LAN, they can perform passive discovery. It is possible to listen for messages from DAD and ND mechanisms and collect IP addresses. Sometimes a few addresses would be enough to discover the numbering pattern and selectively ping the hosts. Remote scans became more complicated but several ways to speed up the scanning process exist.

IPv6 addresses in the real world deployment are mostly not random (Gont 2012). Numbering conventions often used can be listed as follows.

a. SLAAC-Based

The unknown part of these addresses is really the lower 64 bits which are based on MAC address of the node. The construction is outlined in Figure 2.14. First 24 bits are Organization Unique Identifier of the vendor manufacture network interface card. These are known (e.g. for a virtual infrastructure) or guessable using a dictionary of these values. Next 16 bits are constant and the truly unknown bits are the lowest 24 which makes the scanning much faster.

24 bits	16 bits	24 bits
IEEE OUI	FF FE	Lower bits of MAC

Figure 2.14 Lower 64 bits of SLAAC-based IPv6 Address

b. IPv4-Based

These addresses are likely used in dual-stack environment and contain IPv4 address in the IPv6 address. An example could be 2001:db8::192:168:1:1. This makes the search space same as in case of IPv4 environment.

c. Low Byte(s)

Only the lower byte or two are used for host numbering. The search space in this case is 28 or 216.

d. Wordy

Wordy addresses such as 2001:db8::b00b:babe or 2001:db8::dead:beef are easy to remember but easy to guess as well. Some kind “dictionary” scan can be utilized as well.

e. Service Port

Addresses used on machines dedicated to a single service often used easy to remember addresses such as 2001:db8::80 for web server. This addressing scheme makes the search space as small as 28.

Another kind of addresses is provided by DHCP. Once one host is found it would be easy to discover pattern of the DHCP pool but a speck of luck is needed. When scanning is not suitable, an adversary will very likely focus on DNS servers or particular types of traffic, such as e-mails, from which the addresses can be extracted. If DNS is in use on a network, a kind of dictionary attack may be utilized as there are common naming conventions for servers such as capital cities, gods from Greek mythology and so on.

2.2.2 Attacks Over IPv6

This section discusses attacks that exploit features of IPv6 itself. Embedded ICMPv6 mechanisms are discussed in the next, separate and more comprehensive Section. 3.2.1

a. Extension Headers Exploits

Extension headers seem to introduce a whole new attack domain to IPv6. Not only they may cause concern about the performance of security systems that have to process the headers correctly but security researchers have already found several ways to exploit the extension headers. Hop-by-Hop Options Header is the one and only extension header which have strictly defined position in the IPv6 packet. It has to be placed right after the IPv6 header and has to be present only once as it is the only extension header that is being inspected on every intermediate node. One of the options that can be defined within Hop-by-Hop header is Router Alert Option which informs routers on the path that they should closely examine the content as it could contain information valuable for them, such as Resource Reservation Protocol (RSVP) or Multicast Listener Discovery (MLD) message (Gont 2012). The option itself is specific Type-Length-Value (TLV) encoded number within Options field of the header. Unfortunately, this option can be exploited to cause DoS attack on a router. Router spends more time examining content of packets with Router Alert Options. Therefore, the situation when the router is flooded with large number of these packets can lead to inadequate resources consumption or deterioration of response time. Extension headers are very useful when it comes to firewall evasion. Particular techniques described in (Gont, F & Chown 2013) and (Heuse, Marc 2012). Another security solution which can be rather easily evaded using extension headers is RA Guard (RA Guard) (Heuse, Marc 2011). RA Guard is a solution intended to protect against Router Advertisement attacks which will be discussed in Section 3.3. All traffic on LAN has to pass through RA Guard in order to make the protection effective. RA Guard can be a standalone solution but it usually is additional functionality of switches. Extension header threats are closely linked to fragmentation attacks because every fragment employs Fragment Header which is extension header

as well. Attacks associated to Fragment Header will be discussed in the following section.

b. Fragmentation Attacks

Fragmentation attacks already are well known from IPv4 but IPv6 changes the fragmentation philosophy. Fragmentation can be performed exclusively by the source host and not on intermediary nodes (Gont, F & Chown 2013). This surely benefits the ease of transmission but an adversary can craft fragments more accurately. Fragments can be used to bypass IDS and IPS systems as well as firewalls. The techniques for hiding attack patterns or evading security systems are (Pivarnik&Gregr 2013):

i. Evasion

Inserting a fragment which is not processed by IDS/IPS but let through due to its transparency.

ii. Insertion

Inserting a fragment which is accepted by IDS/IPS but discarded by a target host.

iii. Overlapping fragments

Overlapping fragments can cause DoS during reassembly or misinterpretation of the data thus hiding attack pattern.

iv. Tiny fragmentation

Attempt to hide attack pattern huge amount of tiny fragments is a sign ofattack coming.

v. Disordered arrival of fragments

Disordered fragments of several packets arriving at once is a technique trying to avoid Deep Packet Inspection (DPI).

vi. Fragment flooding

Another strategy designated to avoid DPI is handling of IPv6 fragments is described in [RFC2460] and updated by (Atlasis 2012). All overlapping fragments should be silently discarded including those not yet received. However, none of the current versions of mainstream operating systems complies to these RFCs [RFC2460] [RFC5722]. IPv6 introduces Fragment Header which is used to describe fragments and carries information needed for reassembly. Together with this extension header is introduced so-called Atomic Fragment. It is a packet that contains Fragment Header although it is not fragmented offset value and More Bit is set to all zeroes. Atomic Fragments may be exploited for security systems evasion. Handling of these packet was standardized in May 2013 (Durdağı, E., & Buldu, A. 2010) and overlapping fragments were explicitly forbidden in December 2009 (Durdağı, E., & Buldu, A. 2010). Currently, there are some rumors (Durdağı, E., & Buldu, A. 2010) in the IPv6 security community that IETF is trying to work out mechanism to completely remove fragmentation from IPv6 because of its security concerns. Moreover, incomplete stream of fragments may be exploited for amplification or reflective DoS attacks. When systems are flooded with incomplete fragments stream they wait for specified amount of time for the rest of the stream to arrive. If the fragments do not arrive, host sends back ICMPv6 Time Exceeded (fragment reassembly time) message.

2.2.3 Attacks Over ICMPv6

As it has been already mentioned, ICMPv6 is a vital part of IPv6. It provides several handy features and replaces ARP utilized in IPv4. Unfortunately, it also seems to be an Achilles' heel of the whole protocol as many attacks target it. Nevertheless, it has been always taken into account that the adversary needs access to LAN to exploit these ICMPv6 vulnerabilities. In most cases, these threats have to be considered as an insider threats and public LANs as networks of much higher risk. Following sections of this chapter will discuss selected currently known ICMPv6 vulnerabilities and associated exploits.

a. Duplicate Address Detection Attack

DAD is a mechanism employed by hosts and SLAAC feature of IPv6 to prevent duplicate addresses on a network. It is susceptible to DoS attack. When a host is to join a network with address acquired, for example, through SLAAC, it sends an ICMPv6 NS message to all nodes multicast destination (DST) address, FF02::1, in order to verify that there is no host already in possession of this address. If there is no reply in specified time, the hosts assume the address is not in use and starts using it as its own IPv6 address. This mechanism is illustrated in Figure 2.15 by Steps (1), (2) and (3).

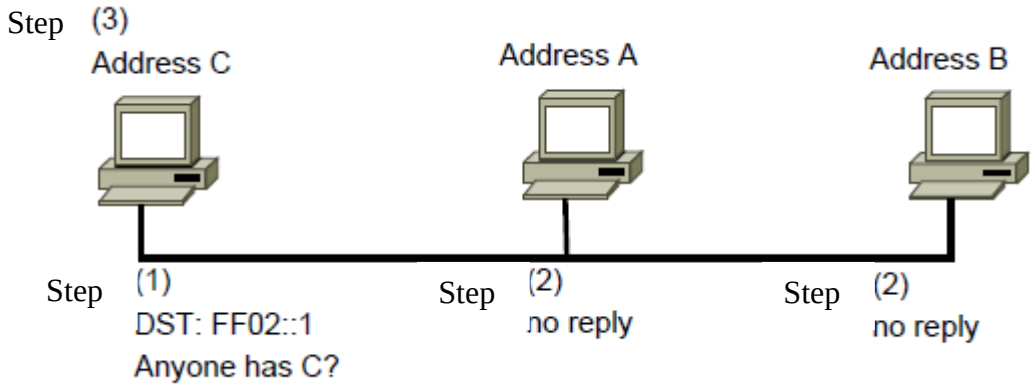

Figure 2.15 Proper Duplicate Address Detection

However, anyone can reply to NS message claiming that the particular address being solicited is their address. When an adversary has access o LAN, therefore is recipient of all-nodes multicast messages, there is nothing that could stop them from interrupting the DAD mechanism with malicious activity. The principle is very simple. Anytime a host wants to join the network and sends NS message to all nodes multicast address, adversary responds claiming the address is their thus preventing any new hosts from joining the network. The attack is summarized in Figure 2.16 by Steps (1), (2a), (2b) and (3).

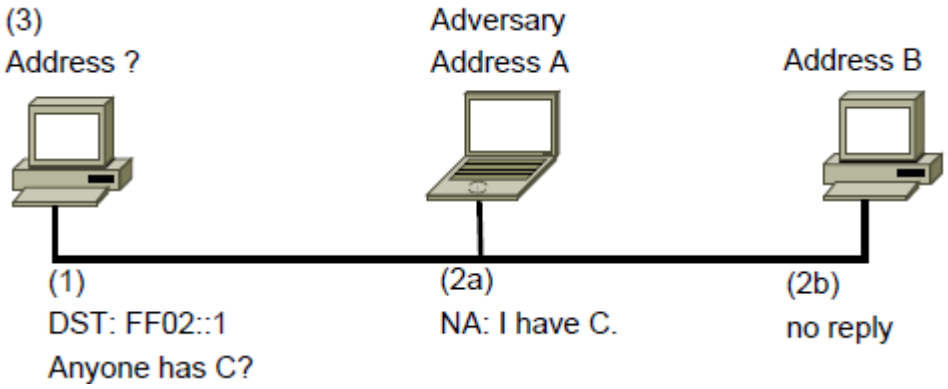

Figure 2.16 Duplicate Address Detection Attack

b. Router Advertisement Spoofing

Router Advertisement (RA) is a type of ICMPv6 message (Type 134) which is periodically sent by a router in order to advertise itself and particular subnet settings to all-nodes multicast address ff02::1. It can also be request from the router by any node on the subnet by sending Router Solicitation message to all-routers multicast address ff02::2. Structure of a RA message is outlined in Figure 2.17.

Type, 8bits	Code, 8 bits			Checksum, 16 bits
Cur Hop limit, 8bits	M bit	O bit	Reserved, 6bits	
Reachable Time, 32 bits				
Retrains timer, 32 bits				
Option, variable				

Figure 2.17 Format of Router Advertisement Message

It is obvious that RA messages can be randomly spoofed and thus an adversary can set any IP address as a default router and cause either DoS by advertising a bogus address or MITM by advertising their own, network prefixes, DNS servers and so on. Another way to cause DoS is sendinga spoofed RA message which advertise the current router but with Router Lifetime value set to zero. This will force all nodes on the subnet to discard the default router. In below section MITM attack covered in more detail.

Proper use of RS and RA messages is outlined in Figure 2.18. Host can request RA by sending RS message to all-routers multicast address Step (1). Router replies

with requested RA message Step(2). Communication then takes place directly between hosts and the router (steps (1) and (2) in the below Figure 2.18). However, anyone can send RA message and does not even have to wait for RS request. Both solicited and periodical advertisements can be overridden by a forged advertisement with higher priority. When host receives the forged RA message, it discards the previously advertised information and replaces it with the one sent by an adversary.

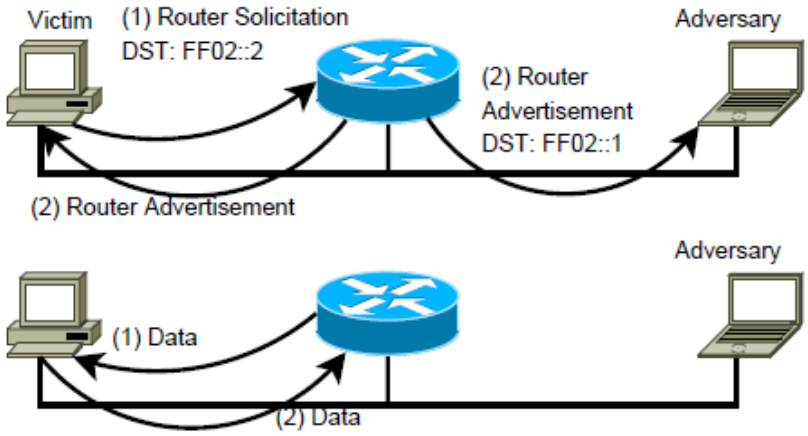

Figure 2.18 Proper Router Solicitation/Advertisement Mechanism

The attack is outlined in Figure 2.19. The above Figure 2.18 depicts attacker answering RS with its own forged RA (2). The setup then opens door for MITM attack for the adversary as all the traffic destined to router arrives directly to them ((2) on the lowerFigure 2.19) as there can be only one default gateway on the network. The adversary can modify or obtain private data, hijack sessions and much more.

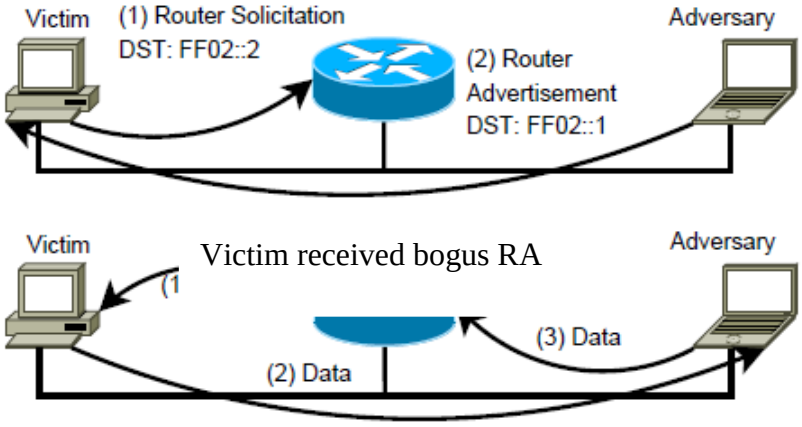

Figure 2.19 Man-in-the-Middle Attack with Spoofed Router Advertisement

c. Router Advertisement Flooding

Another ICMPv6 flooding attacks is RA flooding. The principle is simple, an adversary floods the whole network not just particular host with forged RA messages. The attack can be performed in number of slight modification. The messages can be simple advertisement messages or messages bearing data, such as announcing a new route. The victim is overwhelmed by processing the information, resources are exhausted and the situation leads to DoS. Historically, there were bugs in several operating systems which made this attack more serious. All major operating systems were vulnerable to RA flooding. Microsoft Windows 2003, 2008, XP, 7 and even Windows 8 were released with the same bug known from around year 2008. In addition Linux, Cisco IOS, Juniper Netscreen, FreeBSD and OS X (Atlasis 2012). The systems crashed, stopped responding or lost its connectivity. When the issue was fixed, just simple modification of the RA message was enough to accomplish the same results (Heuse, Marc 2012) (Heuse, Marc 2011). Currently, all the issues should be fixed by the vendors. Microsoft fixed the issue in its operating systems in updates released in April 2013. It is not necessary to reboot the system after RA attack anymore. MS Windows does not respond during the attack as its CPU utilization reaches 100% but it recovers when the flooding stops.