AN IMPROVED SECURE ROUTER DISCOVERY MECHANISM TO PREVENT FAKE RA ATTACK IN LINK LOCAL IPV6 NETWORK

NAVANEETHAN A/L C. ARJUMAN

UNIVERSITI SAINS MALAYSIA

2021

AN IMPROVED SECURE ROUTER DISCOVERY MECHANISM TO PREVENT FAKE RA ATTACK IN LINK LOCAL IPV6 NETWORK

by

NAVANEETHAN A/L C. ARJUMAN

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

December 2021

ACKNOWLEDGEMENT

I would like to express my unlimited gratitude to God and Guru who bestowed me inner with strength, good health, a clear mind and a conducive environment to conduct my research and complete this thesis. I would like to extend my gratitude to all my family members especially my parents **late Mr Arjuman** and **Madam Suppamah**, my dearest wife **Meena Munusamy** and her parents as well as, my daughters **Poomagal** and **Koomagal** for their love, untiring support and cooperation that helped me to complete this research work. I am indebted to the **Ministry of Education (MOE) (formerly known as the Ministry of Higher Education (MOHE))** for providing me with funding through the **MyBrain Postgraduate Scholarship Programme** to complete this research work.

Furthermore, I would like to express sincere appreciation and gratitude to my **supervisor**, **Associate Professor Dr Selvakumar Manickam** for his support, guidance, valuable insight and supervision that enabled me to complete this research work. At this juncture, I would also like to thank **the Director of the National Advanced IPv6 Centre, Professor Dr Bahari Belaton** and **the Deputy Director Associate Professor Dr Wan Tat Chee** for their guidance and support. Furthermore I would like to take this opportunity to thank all the senior lecturers, my fellow researchers and all the supporting staff within the centre for their kind support in completing my research work. Finally, I would like to extend my greatest appreciation to all my well wishers and friends who have supported me both directly and indirectly throughout the course of my studies.

Navaneethan C. Arjuman

TABLE OF CONTENTS

LIST OF PUBLICATIONS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

ACL	Access Control List
ADD	Authorisation Delegation Discovery
AH	Authentication Header
AI	Artificial Intelligence
API	Application Program Interface
AP	Access Point
AR	Access Router
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
BW	Bandwidth
CA	Certificate Authority
CAR	Candidate Access Router
CIA	Confidentiality, Integrity and Availability
CGA	Cryptographically Generated Address
CPA	Certificate Path Advertisement
CPS	Certificate Path Solicitation
CPU	Central Processing Unit
DAD	Duplicate Address Detection
DES	Data Encryption System
DDOS	Distributed Denial Of Service
DHCPv4	Dynamic Host Configuration Protocol Version 4
DHCPv6	Dynamic Host Configuration Protocol Version 6
DNS	Domain Name Service
DOS	Denial Of Service
EUI	Extended Unique Identifier
ECC	Elliptic Curve Cryptography
FASR	Fake RA Attack Success Rate
HMAC	Hash-Based Message Authentication Code
HC	Host Controller
IDS	Intrusion Detection System
ICMP	Internet Control Message Protocol

ICMPv4	Internet Control Message Protocol Version 4
ICMPv6	Internet Control Message Protocol Version 6
IETF	Internet Engineering Task Force
IOT	Internet of Things
IP	Internet Protocol
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
IPSec	Internet Protocol Security
IPS	Intrusion Protection System
IT	Information Technology
SLAAC	Stateless Address Autoconfiguration
SMAC	Secure Message Authentication Code
SecMac-SRD	SecMac Secure Router Discovery
MAC Address	Media Access Control Address
MAC	Message Authentication Code
MD5	Message Digest algorithm 5
MITM	Man In Middle Attack
MN	Mobile Node
MTU	Maximum Transmission Unit
NA	Neighbour Advertisement
NAv6	National Advanced IPv6 Centre
ND	Neighbour Discovery
NDP	Neighbour Discovery Protocol
NUD	Neighbour Unreachability Detection
NIST	National Institute of Standards and Technology
NS	Neighbour Solicitation
NA	Neighbour Advertisement
NUD	Neighbour Unreachability Detection
RA	Router Advertisement
RA-Guard	Router Advertisement Guard
RAP	Router Access Passport
RC	Router Controller
RD	Router Discovery
RFC	Request For Comment

RR	Router Re-direct
RS	Router Solicitation
RA	Router Advertisement
RSA	Rivest, Shamir, and Adleman
SA	Security Association
Secure-DAD	Secure Duplicate Address Detection
SeND	Secure Neighbour Discovery
SDN	Software-defined networking
SHA-1	Secure Hash Algorithm 1
SHA-2	Secure Hash Algorithm 1
SHA-3	Secure Hash Algorithm 3
SLAAC	Stateless Address Autoconfiguration
TA	Trust Anchors
TCP/IP	Transmission Control Protocol/Internet Protocol
THC	The Hacker Choice
T-NDP	Trust Based Security Enhancement Mechanism For Neighbour Discovery Protocol (T-NDP)
TR^2PA	Trusted Router-Router Passport Advertisement
TR^2PS	Trusted Router-Router Passport Solicitation
TRDP	Trust Router Discovery Protocol
TRPA	Trusted Router Passport Advertisement
TRPS	Trusted Router Passport Solicitation
Trust-ND	Trust Neighbour Discovery
Trust-RA	Trust-ND Router Advertisement
Trust-RS	Trust-ND Router Solicitation
TSO	Trust Solicitation Option
TOA	Trust Advertisement Option
OS	Operating System
UMAC	Universal Message Authentication Code
USM	Universiti Sains Malaysia

MEKANISME PENAMBAHBAIKAN PENEMUAN PENGHALA SECARA TERSELAMAT BAGI MENGELAKKAN MASALAH PENAFIAN SERANGAN RA PALSU DALAM RANGKAIAN LINK LOCAL IPV6

ABSTRAK

Dalam rangkaian Internet Protocol Version 6 (IPv6), Neighbor Discovery Protocol (NDP) memainkan peranan penting dalam mengkonfigurasi alamat IPv6 untuk sebarang jenis hos. Hos IPv6 akan mendapatkan alamat IPv6 menggunakan "Stateless Address Auto Confuguration" (SLAAC). SLAAC telah dilaksanakan menggunakan dua jenis protokol NDP mesej iaitu "Neighbor Discovery (ND)" dan "Router Discovery (RD)" dalam rangkaian IPv6. Mesej RD terdiri daripada mesej "Router Solicitation (RS)" dan "Router Advertisement (RA)". Mesej RD standard tidak mempunyai mekanisme keselamatan untuk mengesahkan hos dan penghala yang sah. Kecacatan dalam reka bentuk protokol RD ini telah menyebabkan serangan RA Palsu. Kajian menunjukkan bahawa protokol RD standard terdedah kepada serangan RA Palsu di mana hos akan dinafikan penghala yang sah. Untuk menangani isu ini, beberapa teknik pencegahan telah dicadangkan pada masa lalu dalam proses RD. Walau bagaimanapun, teknik ini mengalami kerumitan masa yang tinggi dan juga kelemahan lain seperti serangan "hash collision" dan masalah "bootstrap". Oleh itu, tesis ini mencadangkan mekanisme RD yang lebih selamat iaitu mekanisme SecMac-Secure Router Discovery (SecMac-SRD) menggunakan masa pemprosesan yang rendah dan dapat menghalang serangan RA Palsu. Mekanisme SecMac-SRD dibina berdasarkan "UMAC hashing" dengan Sistem Kripto Pengedaran Kunci Awam ElGamal yang menyembunyikan pertukaran mesej RD dalam komunikasi tempatan di dalam rangkaian IPv6. Di bawah mekanisme ini, mesej RS dan RA standard telah

direka bentuk semula dengan pilihan tag selamat iaitu SecMac-tag untuk mengesahkan sama ada hos dan penghala adalah sah semasa proses RD. Kedua-dua hos dan penghala hanya akan menerima mesej RS dan RA yang disertakan dengan SecMac-tag. Memandangkan dalam rangkaian standard tidak dapat menguji mekanisme ini kerana semua peranti IP yang diperlukan untuk dipasang dengan pengawal mekanisme SecMac-SRD ini, rangkaian ujian tertutup IPv6 telah disediakan dengan hos dan penghala untuk mengukur prestasi dari segi masa pemprosesan, "overhead" rangkaian dan fungsi keselamatan mekanisme ini. Parameter yang sama telah diukur untuk semua mekanisme selamat yang lain dan dibandingkan dengan mekanisme SecMac-SRD. Berdasarkan keputusan eksperimen yang diperolehi menunjukkan bahawa mekanisme SecMac-SRD mencapai masa pemprosesan yang lebih singkat berbanding dengan mekanisme RD selamat yang sedia ada dan boleh mengelakkan serangan RA Palsu. Hasil daripada keputusan eksperimen jelas menunjukkan bahawa mekanisme SecMac-SRD berkesan mengatasi serangan RA Palsu semasa proses RD.

AN IMPROVED SECURE ROUTER DISCOVERY MECHANISM TO PREVENT FAKE RA ATTACK IN LINK LOCAL IPV6 NETWORK

ABSTRACT

In the Internet Protocol Version 6 (IPv6) network, Neighbour Discovery Protocol (NDP) plays a vital role in configuring the IPv6 address for any type of host. The IPv6 host will obtains the IPv6 address using Stateless Address Autoconfiguration (SLAAC). SLAAC was implemented using two types of key ICMPv6 NDP message protocol i.e Neighbour Discovery (ND) and Router Discovery (RD) in the IPv6 network. The RD messages consist of Router Solicitation (RS) and Router Advertisement (RA) messages. The standard RD by design do not have trust mechanism to authenticate the legitimate host and router. This design flaw within RD protocol has led to Fake RA attacks. Studies shows that the standard RD protocol is vulnerable to Fake RA attack where the host will be denied legitimate gateway. In order to address this issue, several prevention techniques have been proposed in the past to secure RD process. However, these techniques suffer from high time complexity and also other vulnerabilities such as hash collision attacks and bootstrapping problem. Hence, this thesis proposes an improved secure RD mechanism i.e. the SecMac-Secure Router Discovery (SecMac-SRD) mechanism consume less processing time and able to prevent the Fake RA attacks. SecMac-SRD is built based on UMAC hashing algorithm with ElGamal Public Key Distribution Cryptosystem that hide the RD message exchange in the IPv6 link local communication. Under this mechanism the standard RS and RA message has been redesigned with secure tag option ie. SecMac-tag to verify whether the host and router is legitimate during the RD process. Both the hosts and routers would only to accept

the RS and RA messages that comes with SecMac-tag. Since in the standard network it would not be feasible to test this mechanism because all the IP devices required to be installed with this SecMac-SRD mechanism controllers, a closed IPv6 network testbed has been set up with hosts and routers to measure the performance in terms processing time, network overhead and security functionality of this mechanism. The same parameters have been measured for all other existing secure mechanism and compared with SecMac-SRD mechanism. Based on the obtained experimental results show that SecMac-SRD mechanism achieved less processing time compare to the existing secure RD mechanism and can resist Fake RA attacks. The outcome of the experimental results clearly shows that SecMac-SRD mechanism effectively overcome the Fake RA attacks during RD process.

CHAPTER 1

INTRODUCTION

1.1 Background

Today's global economy largely depends on the Internet (Kogut, 2004; Rezabakhsh, Bornemann, Hansen, & Schrader, 2006). The global Internet of Things (IOT) market was USD 151 billion in the year 2018 and expected grow to USD 1,567 billion by 2025 as per the Figure 1.1 (Lueth, 2018).

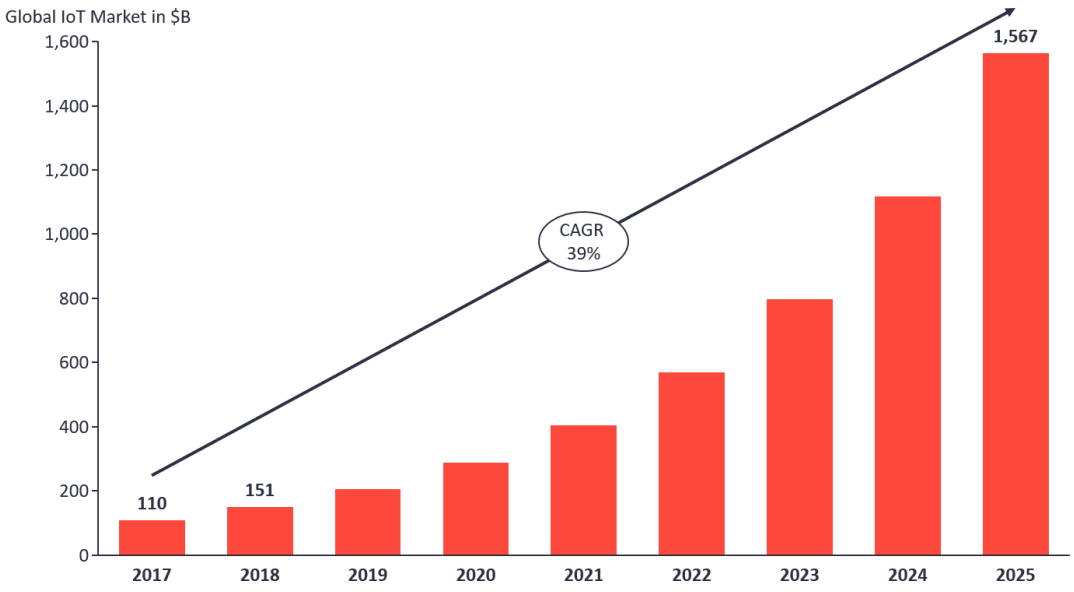

Figure 1.1 Global IoT Market Forecast

(Adapted from (Lueth, 2018))

The latest study as per Figure 1.2 shows the number of connected devices that are in use worldwide now exceeds 17 billion, with the number of IoT devices at 7 billion (that number does not include smartphones, tablets, laptops or fixed line phones) (Lueth, 2018).

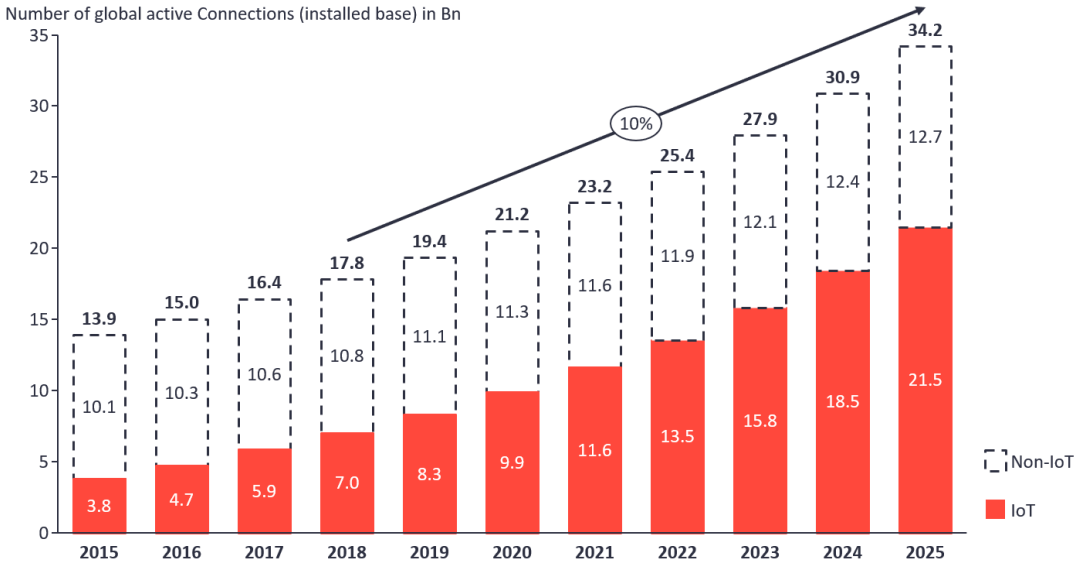

Figure 1.2 Global number of Connected Devices

(Adapted from (Lueth, 2018))

Internet of Things (IoT) now allows more and more devices such as sensors and wireless devices to be connected to Internet (Caro & Sadr, 2019). Since the transition from ARPANET to the current Internet, more and more devices are connected to the Internet (Hauben, 2007; Leiner et al., 2009). However, the growth of the Internet is now being threatened due to the depletion of current Internet addresses, i.e. Internet Protocol version 4 (IPv4) (Richter et al.,2015; Tadayoni & Henten, 2012).

In order to circumvent the shortage of IPv4 global addresses, the Internet Engineering Task Force (IETF) the body that governs the Internet community has introduced Internet Protocol version 6 (IPv6) (Bradner, 2005). The features and functions of the IPv6 are clearly explained in the RFC 2460 (Deering & Hinden, 1998).

Besides having a larger address space compared to IPv4 (Hagen, 2006), IPv6 also have several features that overcome several weaknesses in IPv4 such as better management of IP address space, elimination of addressing issues, easier TCP/IP administration, modern design of routing, better multicasting features, better support for security and improved mobility (Radhakrishnan et al., 2007) .

One of the main advantages of IPv6 compared to IPv4 is the improved security (Daya, 2013; Durdağı & Buldu, 2010). Even though IPv6 provides better security features compared to IPv4, the IPv6 protocol still faces security issues due to the weakness in the protocol design, as well as issues due to the transition mechanism and deployment (Caicedo, Joshi, & Tuladhar, 2009; Choudhary, 2009). These issues were explained in details in the RFC 4942 (Davies, Krishnan, & Savola, 2007).

Due the weakness in the IPv6 protocol and the transition mechanism, it will leads to various attacks such as reconnaissance attack, header fragmentation attacks, tunneling/Dual stack threats and Denial of Service (DoS) attacks in the IPv6 network (Barker, 2013; Zagar & Grgic, 2006; Žagar, Grgić, & Rimac-Drlje, 2007).

1.1.1 IPv6 Address Assignment and Related Security Issues

Internet Control Message Protocol (ICMP) is the integral part of any IP implementation (Kaushik & Joshi, 2010). ICMP is designed to provide query and error messages for effective communication in the IP network (Conta, Deering, & Gupta, 2006; Williams, 2018) .

Unlike in IPv4, in IPv6, ICMP for version 6 (ICMPv6) messages are also used to manage the assignment of the IPv6 address (Saad, Manickam, ALOMARI, ANBAR, & SINGH, 2014; Williams, 2018). There are several mechanisms available to assign

an IPv6 unicast address to a host in the IPv6 network (Hinden & Deering, 2003). These include the static, stateful and stateless approach. In the static scenario, a fixed IPv6 address can be assigned manually to a host by the user. In the stateful scenario, the IPv6 address is assigned by the Dynamic Host Configuration Protocol version 6 (DHCPv6) server (Bound, Volz, Perkins, Lemon, & Carney, 2003; Droms et al., 2003).

However, in the stateless scenario based on the Stateless Address Autoconfiguration (SLAAC), the host will obtain the IPv6 address using Neighbour Discovery Protocol (NDP) (Gont, 2014b; Narten, 1999; Narten, Thomson, & Jinmei, 2007). NDP protocol in IPv6 consist of five ICMPv6 message types, namely, Router Solicitation (RS), Router Advertisement (RA), Neighbour Solicitation (NS), Neighbour Advertisement (NA) and Router Redirect (Conta et al., 2006; Narten, Nordmark, & Simpson, 2007) .

However, due to the weakness that exist in IPv6 address assignment especially in the SLAAC scenario, it has weakness led to various attacks in the IPv6 networks such as Man-In The Middle Attack (MITM), DoS attack (Denial of Service) and Distributed Denial of Service (DDoS) attack etc (Groat, Dunlop, Marchany, & Tront, 2011; Kim et al., 2007; Morrell, 2016).

The vulnerabilities that exist within standard ICMPv6 NDP contribute to the DoS attacks in the IPv6 network especially in the SLAAC scenario (Anbar, Abdullah, Saad, Alomari, & Alsaleem, 2016; Nikander, Kempf, & Nordmark, 2004). NDP protocol is mainly divided into two key categories i.e. Router Discovery (RD) and Neighbour Discovery (ND) (Arkko et al., 2002).

The RD protocol consists of two message i.e. RS and RA. Since there is no security mechanism that exists in the standard RD protocol to verify the communication between the router and the host during the IP address auto-

configuration in the IPv6 network, the RD protocol will be exploited (Arkko et al., 2002), and this led to Fake RA attack (Chakraborty et al., 2014).

1.1.2 Fake RA Attack

During the standard RD process in the SLAAC scenario in the IPv6 network, the host will send out RS message to all the active routers on the link (Chakraborty et al., 2014) and all the routers on the link will reply with RA messages that contain all the relevant configurations (Arkko et al., 2002). Upon receiving all the relevant information from the gateway routers, the host will decide on the appropriate gateway router based on highest priority or the nearest next hop value of the router. All future communication to the Internet would flow through this selected router gateway.

In the standard RD process, the host is unable to check whether the gateway router is legitimate since there is no trust mechanism present in the standard protocol. This vulnerability allows bogus routers to be configured as a legitimate gateway (Tian et al.,2017). The attacker will advertise Fake RA message and allows the host to configure the bogus router parameters (Arkko et al., 2002). This eventually denies legitimate service to the host and this attack would be categorised as Fake RA attack (Arkko et al., 2002).

1.2 Research Problem

RD is an essential operation required in the address auto-configuration mechanism i.e the SLAAC mechanism to acquire the gateway router prefix for the host under the IPv6 address configuration process (Arkko et al., 2002). However, studies have shown that the standard RD operation is vulnerable to Fake RA attacks because there is no trust mechanism to verify the legitimacy of the gateway router

(Nikander et al., 2004). In order to address this, several prevention techniques such as SeND's Authorisation Delegation Discovery (ADD), Trust Router Discovery Protocol (TRDP), Router Advertisement Guard (RA-Guard), Trust Neighbour Discovery (Trust-ND) and CGA + IPSEC AH NDP mechanisms have been proposed in the past.

The SeND's ADD (Arkko et al., 2005) introduced router certificate to determine the legitimacy of the gateway router. However, the lengthy certificate process causes high computational cost and eventually leads to DoS attacks (Praptodiyono et al., 2015). The proposed TRDP (Zhang et al,2007) claimed to address the shortcoming of SeND by reducing the complexity but TRDP also face issues with high computational cost because of the lengthy router authentication process (Praptodiyono et al., 2015).

The introduction of RA-Guard (Levy-Abegnoli, Van de Velde & Mohacsi, 2011) which is a Layer 2 security solution was expected to overcome the above issues especially the high computational cost faced by SeND and TRDP but RA-Guard still faced several other issues such as unable not able to block RA messages that are communicate directly, unable to block RA messages that are channeled through tunneled traffic, only configured to support ingress RA message, unable to support on trunks ports with merge mode and unable to configure in networks that use ACL ICMPv6 optimization.

The Trust-ND mechanism which claims to be a lightweight mechanism compared to SeND and TRDP (Praptodiyono et al., 2015) because the computational cost is lower. This mechanism was built using SHA-1 hashing algorithm that is very vulnerable to hash collision attack (Bhargavan et al.,2016; Andreeva et al.2015; Polk et al,2011).

The recently introduced CGA + Internet Protocol Security (IPSec) Authentication Header (AH) NDP Mechanism (Tall et al, 2019) which claims to be a lightweight mechanism compared to SeND because the computational cost is lower. This mechanism uses the AH is part of IPSec suite (Kent, S. and R. Atkinson,1998) to authenticate the router. AH operates using Security Association (SA)s that was built based on Internet key exchange version 2 which required functional IP address. So when a new host joining the network, the host will not have functional IP address so this scenario leads to bootstrapping problem (Shah et al.,2019).

So the problems can be summarised as follows:

1. Standard RD operation is insecure by design and vulnerable to Fake RA attacks because there is no trust mechanism to verify the legitimacy of the gateway router (Nikander et al., 2004).
2. Existing latest secure RD mechanisms such as Trust ND and CGA + IPSEC AH NDP mechanism even though able to prevent Fake RA attacks but still suffers from high time complexity and inherent vulnerabilities such as hash collision attack and bootstrapping problem that can be exploited during the RD process in link local communication of IPv6 network.

1.3 **Research Questions and Objectives**

Based on the reasons mentioned in the research problem section, the standard RD process is still vulnerable to Fake RA attacks despite implementing several prevention mechanisms that have been proposed in the past. So, the research work would address the following key questions that were raised to address this research problems:

i) Why the current mechanisms that secure RD suffers from high time complexity and other vulnerabilities to prevent Fake RA attacks in the link local communication of the IPv6 network?

ii) What is the appropriate secure RD mechanism that is required to prevent the Fake RA attacks in the link local communication of the IPv6 network?

In order to achieve the research goal in answering the above-mentioned research questions, the following objectives need to be fulfilled.

1. To design a heuristic based secure RD mechanism that use less processing time to prevent Fake RA attack in the link local communication of the IPv6 network.
2. To redesign the RD message structure to prevent Fake RA attack in the link local communication of the IPv6 network.
3. To redesign the RD message exchange using public key distribution system to ensure secure key exchange between nodes in the link local communication of the IPv6 network.

1.4 Research Contribution

In the earlier sections, the role of the standard RD process in IP address assignment has been discussed briefly. To overcome issues with standard RD processes, researchers have previously proposed several security mechanisms. Although these mechanisms are able to address the RD issue, especially the Fake RA attacks, but due to the vulnerabilities in their design, these mechanisms still faced certain issues as discussed in Section 1.2. Hence, to overcome the shortcomings of these mechanisms, this research has proposed a secure mechanism to ensure secure communications of the RS and RA message in the link local communication of the

IPv6 network. The proposed mechanism will secure the RS and RA messages and protect RS and RA messages from exploitation due to Fake RA attacks in the link local communication of the IPv6 network. In order to achieve the above-mentioned research goal, a closed IPv6 network Testbed has been set up to evaluate the proposed mechanism i.e. the SecMac Secure Router Discovery (SecMac-SRD) mechanism. Below are the contributions of this research work:

1. Secure Router Discovery (SecMac-SRD) mechanism that prevents Fake RA attacks during the RD process in the link local communication of the IPv6 network.
2. Redesigned secure RS and RA messages with secure SecMac-tag options.
3. Redesigned the key exchange using public key distribution system for the secure RD message exchange.

1.5 Research Scope and Limitation

In this research study, the scope of the proposed secure RD is limited to securing the IPv6 network against the Fake RA attack in the RD process during the address auto-configuration in the IPv6 network as shown in Table 1.1. The research work involves securing the RS and RA messages during the RD process in the link local communication of the IPv6 network. This secure mechanism is designed only for the Stateless Address Auto-configuration (SLAAC) addressing scheme in the IPv6 network.

Table 1.1 Research Scope and Limitation

Items	Scope of Research
Environment	IPv6 Network

Attack Type	Fake RA Attack
NDP Message Types	RS and RA messages
DoS Target	Network Layer
Address Auto-configuration	SLAAC

1.6 **Research Steps**

To achieve the objectives of this research, the research work has been divided into various phases. Below is list of phases of the research work:

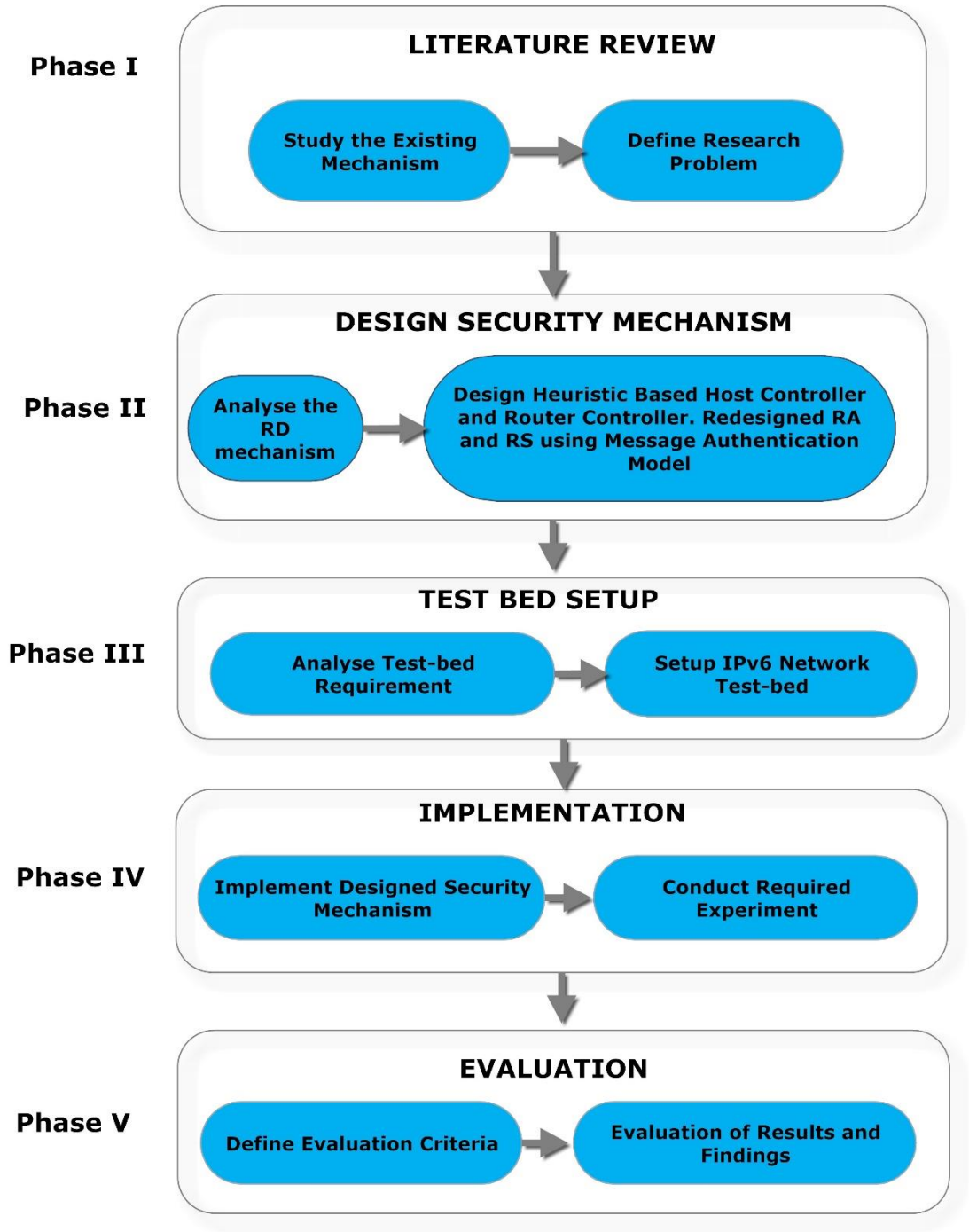

Figure 1.3 Main Phases of Research Work

In the first phase, a critical review of all the existing RD prevention mechanisms has been carried out to define the research problem. This review helps to understand in detail the existing solutions to overcome the research problem and the shortcomings of the existing solutions.

In the second phase, the solutions to the research problem have been proposed. The proposed solutions involve several layers of security to enhance the secure RD mechanism in the link local communication of the IPv6 network. A heuristic-based less processing time secure RD mechanism has been proposed in this phase to overcome Fake RA attacks during the RD message validation process in the IPv6 network.

In the third phase, a closed IPv6 network requirement has been analysed and Testbed has been set up to conduct relevant experiments to measure the performance of the newly proposed secure RD mechanism.

In the fourth phase, testing is done using the newly designed secure RD mechanism to measure the processing time and network overhead. Further test are conducted to evaluate the security feature of the RD mechanism prevent Fake RA attacks in the RD process during the IPv6 address auto-configuration in the link local communication of the IPv6 network.

The final phase would be the evaluation stage in achieving the research goal. The designed mechanism was evaluated in terms of less processing time, network overhead and effectiveness in preventing Fake RA attacks during the RD process during the address auto-configuration in the link local communication of the IPv6 network.

1.7 **Thesis Outline**

This thesis is organised into six chapters, with this chapter being an introduction to the entire thesis. This is followed by five other chapters.

Chapter Two presents the fundamental concept of IPv6 address assignment in the IPv6 network. It also provides insight to how the network prefix of the IPv6 address is obtained and the vulnerabilities involved in the standard RD process. It also provides a detailed literature review of the existing secure RD mechanisms for the RD process in the link local communication of the IPv6 network. It also discusses the issues faced by the existing mechanisms. Finally, this chapter outlines the reasons to have a new secure RD mechanism to overcome Fake RA attacks in the link local communication of the IPv6 network.

Chapter Three discusses the proposed methodology with detailed information on how the proposed mechanism would be designed. It discusses the overall architecture for newly proposed secure RD mechanism and how it components operate to generate the secure tag and function to overcomes the Fake RA attacks during the RD process.

Chapter Four illustrates the implementation details of the designed secure RD mechanism to protect the RD process during address auto-configuration in the IPv6 network.

Chapter Five discusses the evaluation of the designed mechanism and analyses the results obtained through the experimentation. In this chapter, the functionality of the proposed secure RD mechanism is evaluated and compared to standard RD, Trust-ND and CGA+IPSEC AH NDP mechanisms.

Chapter Six presents the conclusion of this thesis and possible future research work.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter provides background and discuss the related work to secure the RD process in the IPv6 address auto-configuration. First Section 2.2 will discuss the general structure of the IPv6 network communication. Section 2.3 will cover the how IPv6 address assignment done in the IPv6 network and subsections would present in detail how the Stateless IPv6 Address Auto-configuration (SLAAC) addressing scheme is implemented in the IPv6 network. The issues with RD process are discussed in Section 2.4. Section 2.5 discuss the RD vulnerabilities prevention techniques to secure the RD mechanism. Section 2.6 discusses related works on securing the RD process. This is followed by the description of the need for new security mechanisms in the RD process discussed in the Section 2.7 and its subsections. Section 2.8 discuss the trust concept in network security. The final section would be the summary of this chapter.

2.2 IPv6 Communication

In the IPv6 networks, the communication between host to host and host to router can be wired and wireless. IPv6 network uses the NDP protocol to communicate with all the devices in the IPv6 network (Narten, Thomson, et al., 2007; Zhang & Wang, 2016). In contrary IPv4 uses the Address Resolution Protocol (ARP) (Plummer, 1982). So the significance of NDP protocol in the IPv6 network communication is undeniable (Ahmed, Hassan, & Othman, 2017).

The NDP protocols primary function in the IPv6 network communication is to provide address resolution that involves Router Discovery (RD), Neighbour Discovery

(ND) and Router Re-direct (RR) (Ahmed et al., 2017; Zhang & Wang, 2016). Besides this functionality, NDP provides other services such as Neighbour Unreachability Detection (NUD) and Duplicate Address Detection (DAD) as well (Zhang & Wang, 2016).

2.3 IPv6 Address Assignment

Unlike in the IPv4, in IPv6, ICMPv6 messages are used to manage assignment of the IPv6 address (Goralski, 2017; Saad et al., 2014). Various mechanisms are available to assign IPv6 address for a host (Hinden & Deering, 2003). This includes the static, stateful and stateless approach.

In the static scenario, a fixed IPv6 address can be assignment manually by users in the IPv6 network (Blanchet, 2009). Since IPv6 address are larger (128 bits) space compared to IPv4 (32 bits), is not easy for the user to enter the hexadecimal address manually (Koskimäki, 2019). There is a high possibility that a mistake can happen when entering the large IPv6 address that is in the hexadecimal format. So, most of the users prefer to use either the SLAAC or DHCPv6 addressing scheme (Thomson, Narten, & Jinmei, 2007) .

Dynamic Host Configuration Protocol version 6 (DHCPv6) server provide IPv6 addressing based on the stateful scenario (Droms et al., 2003). The DHCPv6 addressing scheme in the IPv6 network works like the DHCPv4 in the IPv4 network but with some added new features. One of the major advantages of DHCPv6 is that it can provide both the stateful and stateless IPv6 addressing scheme whereas DHCPv4 only provides stateful IPv4 addressing. In the stateless scenario, the IPv6 address remained unchanged but the other parameters such as DNS changed when there are changes took effect. Ideally, DHCPv6 is preferred especially by administrator of enterprise networks

because it is easy to maintain the IP address and mistakes due to human error can be avoided. But, the DHCPv6 IPv6 address mechanism also suffers from other vulnerabilities such as fake DHCPv6 servers and vulnerabilities in the DHCPv6 communications (Lear, Droms, & Romascanu, 2019).

IPv6 SLAAC assigns an IPv6 address to a host based on the NDP protocols (Odom, 2016; Shah, 2019). The NDP process involves RD, ND and RR. The SLAAC plug and play feature is one of the key advantages in the IPv6 network compared to the IPv4 network that uses only a manual or DHCPv4 addressing scheme (Shah & Parvez, 2015). But the vulnerabilities in the standard NDP messages have led to various attacks in the IPv6 networks (Arjuman & Manickam, 2015; Elejla, Belaton, Anbar, Alabsi, & Al-Ani, 2019).

2.3.1 IPv6 Stateless Address Auto-configuration (SLAAC)

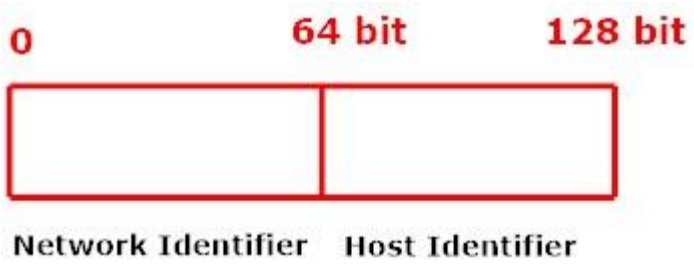

Figure 2.1 IPv6 Address

(Adapted from (Pilihanto, A. and R. Wanner (2011))

In the SLAAC scenario as per Figure 2.1, the host will obtain the lower 64 bits (Network Identifier) of the IPv6 address known as Network Prefix using RD and the upper 64 bits address known as Host Interface Identifier based on ND (Arjuman, Manickam, & Karuppayah, 2019; Deering & Hinden, 2017).

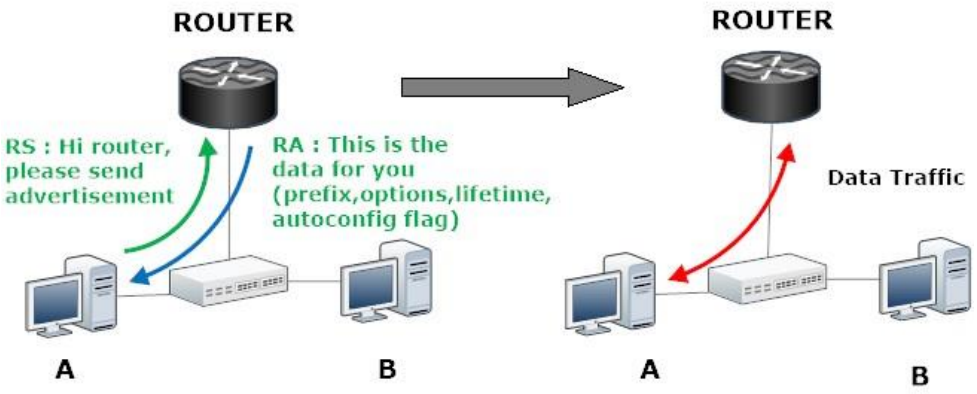

Figure 2.2 Process Flow of Router Discovery

(Adapted from (Pilihanto, A. and R. Wanner (2011))

When Host A first joins the IPv6 link, it will be perform ND followed by RD. ND will be performed using NS (ICMPv6 Message Type 135) and NA (ICMPv6 Message Type 136) messages (Al-Ani, Anbar, Manickam, Al-Ani, & Leau, 2019). Then, RD will be performed using RS (ICMPv6 Message Type 133) and RA (ICMPv6 Message Type 134) messages.

In the RD process, the host will multicast RS message to all the neighbour routers on the link to get the IPv6 Prefix and related parameters such as Maximum Transmission Unit (MTU) and Domain Name Service (DNS) details. The source address will be the IP address of the sending interface or it could be an unspecified address if there is no address on the sending interface of the host (Narten, Nordmark, et al., 2007). The typical destination address will be the all routers multicast address ff02::2.

Upon receiving the RS message from Host A; all the active routers such as Router A and Router B on the link will respond to the RS message with an RA message as depicted in the Figure 2.2. Routers usually send out RA messages periodically in the unsolicited scenario whereas in the solicited scenario they are sent out upon

receiving RS from the host (Narten, Nordmark, et al., 2007). The source address will be the link layer address of the sending router's interface. The typical destination address will be the source address of requesting host or the all-nodes multicast address ff02::1. The host will configure its default gateway based on either nearest next hop router or the highest priority as well as the following conditions.

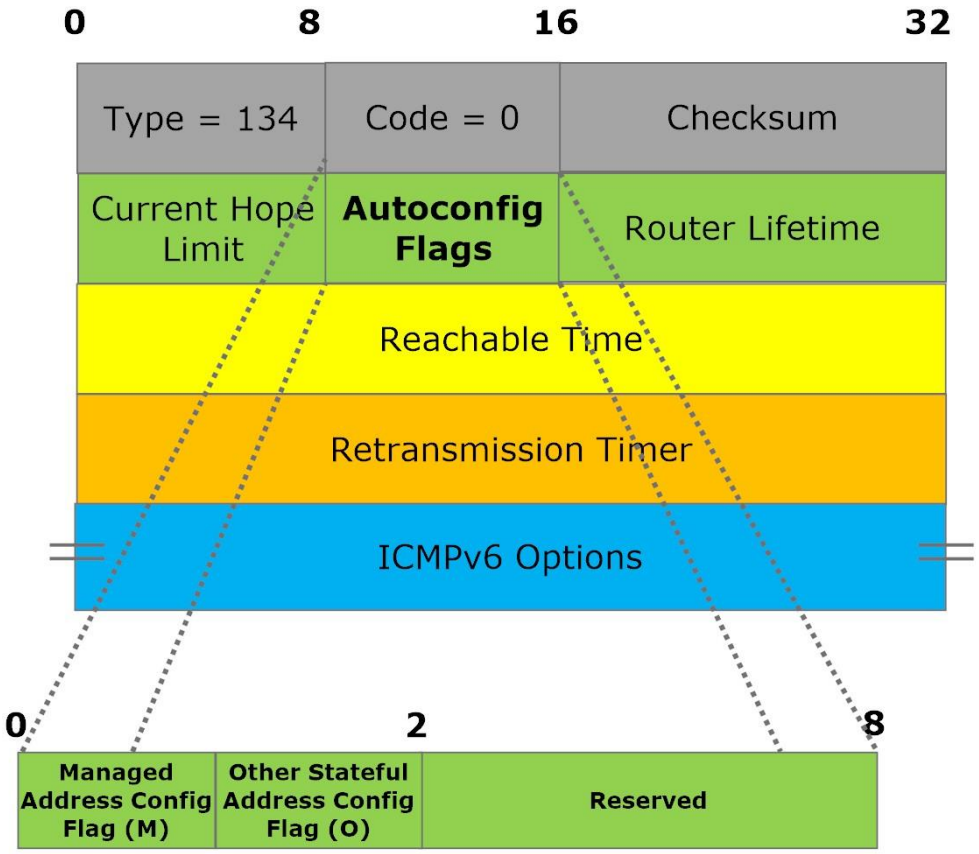

Figure 2.3 RA Message (Type 134) Format

(Adapted from(Kozierok, 2017))

Figure 2.3 depicts the RA message format (Kozierok, 2017). Table 2.1 shows the condition scenarios for Managed Address Configuration Flag (M) and Other Stateful Configuration Flag (O).

Table 2.1 RA Message Autoconfiguration Flags M and O Table

Autoconfiguration Flags: Two flags that let the router tell the host how autoconfiguration is performed on the local network.

Subfield	Size (Bytes)	Descriptions
M	1/8 (1 bit)	**Managed Address Configurations Flag** : When set, this flag tells host to use an administered or "stateful" method for address autoconfiguration, such as DHCP.
O	1/8 (1 bit)	**Other Stateful Configuration Flag** : When set, tells hosts to use an administered or "stateful" autoconfiguration method for information other than addresses.
Reserved	6/8 (6 bits)	**Reserved** : Reserved for future use: sent as zeroes.

When the Managed Address Config Flag M bit under the Autoconfig Flags is enabled, the Prefix assignment will be from the DHCPv6 server (T Chown, Loughney, & Winters, 2019). When M bit is set and the O bit is not set then O bit will be redundant and can be ignored because all the information will be provided by the DHCPv6 server (Narten, Nordmark, et al., 2007). Disabling the M bit and enabling the O bit allows the global unicast prefix assignment from RA and the ND configuration from a DHCPv6 Server. Enabling O bit means the other configuration such as the DNS related information or other server's information is from the DHCPv6 server.

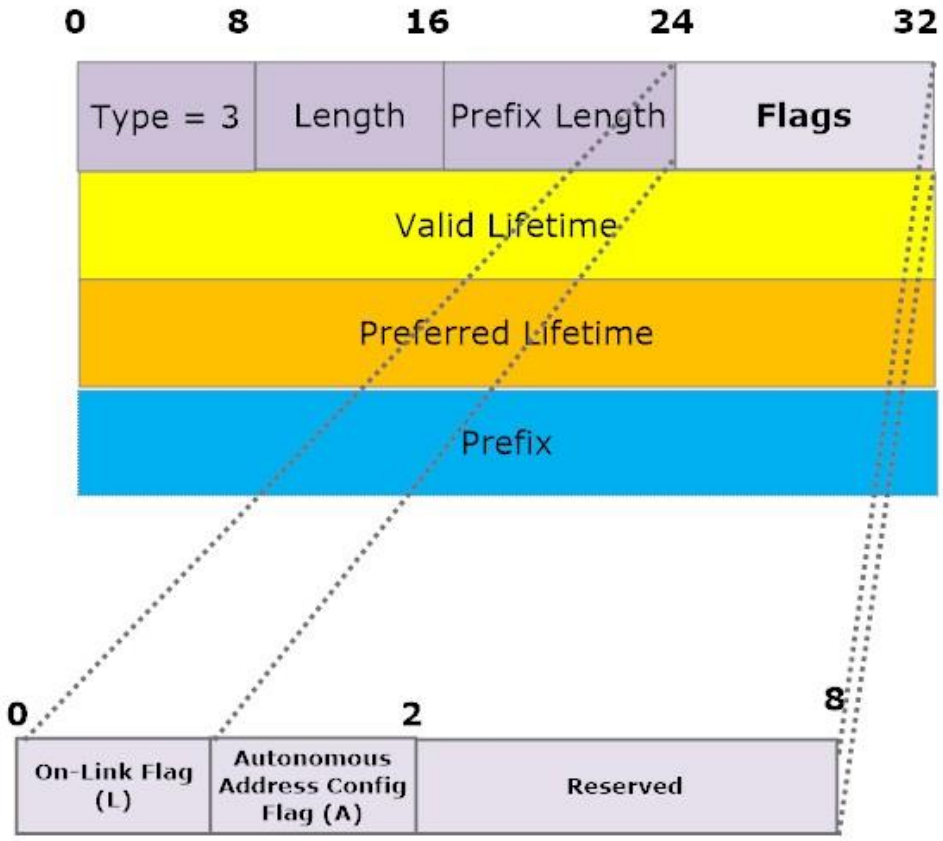

Figure 2.4 ICMPv6 Prefix Information Option Format (Type 3)

(Adapted from(Kozierok, 2017))

Another important parameter of the RA Message are the L and A flags as shown in Figure 2.4 (Kozierok, 2017). Table 2.2 shows the scenario for On-link Flag (L) and Autonomous Address Configuration Flag (A).

Table 2.2 RA Message Autoconfiguration Flags L and A Table

Flags: A pair of flags that convey information about the prefix.

Subfield	Size (Bytes)	Descriptions
L	1/8 (1 bit)	**On-Link Flag** : When set to 1, this recipient of the option that this prefix can be used for on-link determination. This means the prefix can be used for deciding whether or not an address is “on-link” (on the recipient's local network). When 0, the sender is making

		no statement regarding whether the prefix can be used for this or not.
A	1/8 (1 bit)	**Autonomous Address-Configuration Flag** : When set to 1, specifies that this prefix can be used for the IPv6 address autoconfiguration.
Reserved	6/8 (6 bits)	**Reserved** : 6 “leftover” bits reserved and set as zeroes.

If the L bit is set, then it means this router can be used for the on-link determination. If it is not set, then the sender did not commit when this router can be used to determine the on-link status. Also, when A flag is set then it means this prefix can be used for the SLAAC option.

In the SLAAC scenario, the IPv6 address of the most significant 64 will be completed using EUI-64 scheme. Upon completion of EUI-64 process, the Host Interface identifier will be obtained. Both the Network Prefix and the Host Interface Identifier will be concatenated to make the **Tentative IPv6 address**. Only upon completion of **Duplicate Address Detection (DAD)** process then only the status will change from **Tentative** to **Preferred IPv6 Address**. The completion of Duplicate Address Detection (DAD) process allows the host to have a legitimate address to communicate with the gateway router which in turn allows global communication (Narten, Nordmark, et al., 2007).

2.4 Router Discovery Vulnerabilities

The above IPv6 address assignment using the SLAAC addressing scheme is vulnerable to attacks because there is weakness in the RD process (Nizzi, Pecorella,

Esposito, Pierucci, & Fantacci, 2019; Shah, 2019). The presence of rogue routers in the network can lead to the host receiving Fake RA information.

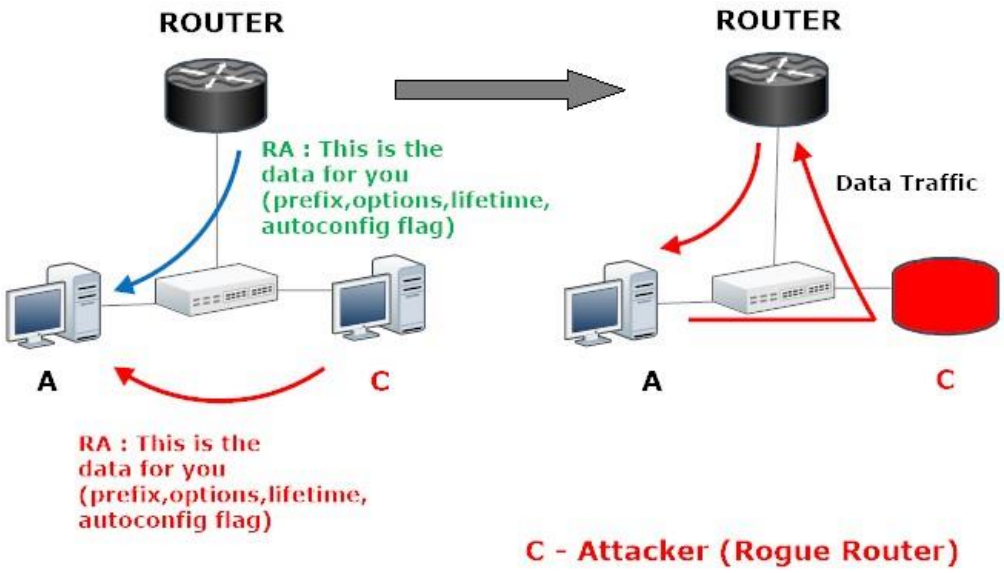

Figure 2.5 Router Advertisement Spoofing Attack

(Adapted from (Pilihanto, A. and R. Wanner (2011))

When Host A sends out RS messages to all the active routers on the link, the Attacker C will also receive the same message. The Attacker C whom acts as a rogue router will send back RA messages with higher priority so that Host A will configure its default gateway with Attacker C's rogue router prefix. The nature of selection of router is based on the nearest next hop and highest priority. The attacker can craft the RA packet with the highest priority and the nearest next hop value so that the host will be configured with the rogue router's information and it will become the as default router. Once the data transmission takes place, all the packets will be routed through the rogue router before it reaches the actual destination. The attacker will be able to eavesdrop on the information that passes through the victim host to the destination. This attack is known as Router Advertisement Spoofing (Ullrich, Krombholz, Hobel,

Dabrowski, & Weippl, 2014). Using the spoofed information from the rogue router, the attacker also can initiate various other attacks such as MITM Attack, DoS attack, DDoS attack, etc (Tim Chown & Venaas, 2011; Harshita, 2017).

The above-mentioned attacks are possible because there is no security mechanism in place to verify the legitimacy of the gateway router within the RD protocol. There are several RD security mechanisms that have been proposed to detect, mitigate and prevent the above issues. However, this research work would only focus on the prevention mechanism to overcome the RD vulnerabilities. The following sections would discuss in detail some of the secure RD mechanism that were proposed by the researchers.

2.5 **RD Vulnerabilities Prevention Mechanisms**

In order to ensure that the RD process is secure in the link local communication of the IPv6 network, over the period several researchers have proposed different trust based mechanisms to overcome the RD issues in the IPv6 link local network communication based on trust based management which will discussed in detail Section 2.8.

In the standard NDP protocol, no trust mechanism exists in the link local communication of the IPv6 network. In the IT network, there are several secure techniques used to create trust between communicating nodes ie. host and router. Below are some these secure techniques enabling trust between the nodes (Nia M. A et al.,2014)

a) Hashing Technique

b) Encryption Technique

c) Certificate Techniques

2.5.1 Hashing Security Technique

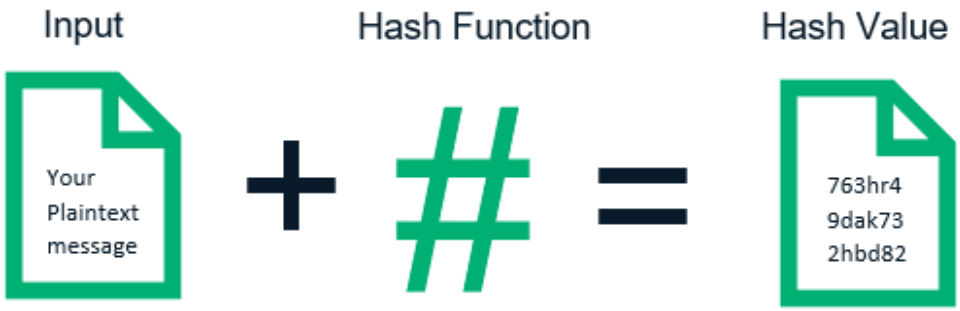

Figure 2.6 Hashing Technique

(Adapted from (N. Abdoun et. al))

The hashing technique is the process to map input of variable length of the data to a fixed-size arrays of numbers and letters using a mathematical function. The fixed-length output is called the *message digest*, or the *hash*, of the original input message. These hashes are unique and thereby provide the integrity of the message.

So the hash function (N. Abdoun et. al) defines using the following equation

$$H: \{0,1\}^* \rightarrow \{0,1\}^n \cdot n \in N \quad (2.1)$$

The hash function considered secure when meet the following meets criteria (El Ksimi, A., & Leghris, C., 2018).

- Preimage attack resistance (one-way). Finding x for given output y which make h(x)=y