INTEGRATED FRAMEWORK FOR SECURE DISTRIBUTED MANAGEMENT OF DUPLICATED IPv6 ADDRESS DETECTION

SHAFIQ UL REHMAN

UNIVERSITI SAINS MALAYSIA

2017

INTEGRATED FRAMEWORK FOR SECURE DISTRIBUTED MANAGEMENT OF DUPLICATED IPv6 ADDRESS DETECTION

by

SHAFIQ UL REHMAN

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

April 2017

ACKNOWLEDGEMENT

*********In the name of Allah, the most Magnificent, the most Merciful *********

Alhamdulilah! With the blessing of Almighty Allah (swt), the Lord of the whole universe, Who bestowed me with good health, sound mind and conducive facilities to conduct and document this research work. I would like to express my gratitude to all my family members, especially to my **parents** and my brother_ **Dr. Khalid Hakeem_** for their kind cooperation, support, encouragements and love which helped me in completing this research work. I am indebted to the **Ministry of Higher Education (MOHE) Malaysia** for providing me the financial support in the form of a prestigious scholarship [**Malaysian International Scholarship (MIS)]** to pursuit this research study.

Moreover, I would like to express my sincere appreciation and thanks to my supervisor **Dr. Selvakumar Manickam,** for his support, guidance, valuable suggestions, and supervision that has helped me to focus on my research work to achieve my goal successfully and to produce this research work. I would like to extend my appreciation and thanks to the **Director of the NAv6 Center Prof. Dr. Rosni Abdullah** and to all senior lectures and my senior research scholars in the center who have given me advices since I enrolled in **USM**. I would like to thank them all for their kind support and encouragement throughout my study in the center. I would also like to thank all the administrative staffs in the center for their official and technical support. Last but not least, my special thanks to all my friends and my well-wishers for their kind support and well wishes. *May Allah (swt) bless you all!*

Shafiq Ul Rehman

TABLE OF CONTENTS

CHAPTER 2 LITERATURE REVIEW

LIST OF TABLES

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
ARP	Address Resolution Protocol
ARPANET	Advanced Research Projects Agency Network
CGA	Cryptographically Generated Addresses
CIA	Confidentiality Integrity Availability
CPA	Certificate Path Advertisement
CPS	Certificate Path Solicitation
CPU	Central Processing Unit
DAD	Duplicate Address Detection
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
ECC	Elliptic Curve Cryptographic
EUI	Extended Unique Identifier
ESM	Extended State Machine
FSM	Finite State Machine
HCM	Host Controller Model
HMAC	Hashing Message Authentication Code
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IID	Interface Identifier

IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
JDK	Java Development Kit
LLC	Link Local Communication
MAC	Media Access Control
MAC	Message Authentication Code
MD	Message Digest
MITM	Man-in-the-middle
MLD	Multicast Listener Discovery
NA	Neighbor Advertisement
NAv6	National Advanced IPv6 Centre
ND	Neighbor Discovery
NDP	Neighbor Discovery Protocol
NDPmon	Neighbor Discovery Protocol Monitor
NS	Neighbor Solicitation
RA	Router Advertisement
RFC	Request for Comment
RS	Router Solicitation
RSA	Rivest Shamir Adleman
SDN	Software Defined Networking
Secure-DAD	Secure-Duplicate Address Detection
SeND	Secure Neighbor Discovery
SHA	Secure Hash Algorithm

SLAAC	Stateless Address Auto-configuration
SPOF	Single Point of Failure
SSAS	Simple Secure Addressing Scheme
THC	The Hackers Choice
UMAC	Universal Message Authentication Code
USM	Universiti Sains Malaysia

RANGKA KERJA BERSEPADU UNTUK PENGURUSAN DIEDARKAN SELAMAT TAHUN DIULANG IPV6 ALAMAT PENGESANAN

ABSTRAK

Alamat bernegara auto-konfigurasi adalah ciri utama protokol IPv6, yang membolehkan tuan rumah untuk mengkonfigurasi alamat IP secara automatik tanpa perlu apa-apa perkhidmatan tambahan seperti; DHCPv6. Walau bagaimanapun, untuk berkomunikasi dalam rangkaian setiap tuan rumah mesti mempunyai alamat IP yang unik. Untuk tujuan itu, alamat proses pengesanan pendua digunakan untuk memastikan bahawa alamat IP yang dihasilkan sendiri adalah unik dalam rangkaian. Dalam usaha untuk melaksanakan proses DAD, tuan rumah IPv6 menggunakan jiran permintaan dan jiran iklan mesej yang berkomunikasi antara satu sama lain dalam rangkaian diedarkan IPv6. Walau bagaimanapun, reka bentuk mekanisme NDP telah menanggung kelemahan keselamatan dan terdedah kepada spoofing, menyebabkan menjadi terdedah kepada serangan DoS. Penyelidikan telah menunjukkan bahawa proses DAD terdedah kepada penafian serangan perkhidmatan, yang boleh menghalang tuan rumah IPv6(s) daripada mendapatkan alamat IP yang unik. Dalam usaha untuk menangani isu ini, beberapa mekanisme telah dicadangkan seperti; Hantar, Trust-ND, SSAS, Pull Model, dan DAD-h. Walau bagaimanapun, disebabkan oleh reka bentuk mereka, mekanisme ini telah secara tidak langsung memperkenalkan kelemahan spoofing yang boleh menyebabkan serangan DoS mengenai proses DAD. Oleh itu, tesis ini memberi satu rangka kerja bersepadu yang dipanggil "Secure-Duplicate Alamat Pengesanan (Secure-DAD)", untuk menjamin mesej NS/NA dari mana-mana exploitations yang boleh menyebabkan serangan DoS semasa proses DAD

dalam IPv6 rangkaian diedarkan. Secure-DAD, memperkenalkan pilihan NDP baru yang dipanggil "Secure-tag" untuk menjamin NS/NA mesej pertukaran antara tuan rumah semasa proses DAD. IPv6-ujian telah persediaan bagi menjalankan uji kaji, untuk mengesahkan prestasi Secure-DAD berbanding DAD standard dan mekanisme Trust-ND. Secure-DAD dinilai dari segi ringan, kerahsiaan, integriti dan ketersediaan. Analisis keputusan menunjukkan bahawa Secure-DAD ini lebih baik dengan peningkatan dari segi pengurangan masa pemprosesan 45.1% berbanding dengan Trust-ND.Selain itu, analisis keselamatan menunjukkan bahawa Secure-DAD boleh memastikan mesej kerahsiaan, integriti dan ketersediaan daripada serangan DoS semasa pengesahan alamat dalam proses IPv6 DAD. Oleh itu, dari proses penilaian, ia telah terbukti bahawa Secure-DAD boleh digunakan untuk proses DAD dalam rangkaian diedarkan IPv6.

INTEGRATED FRAMEWORK FOR SECURE DISTRIBUTED MANAGEMENT OF DUPLICATED IPv6 ADDRESS DETECTION

ABSTRACT

Stateless address auto-configuration is the primary feature of IPv6 protocol, which allows hosts to configure IP addresses automatically without the need of any additional services such as; DHCPv6. Nevertheless, to communicate in a network every host must have a unique IP address. For that purpose, duplicate address detection process is used to ensure that self-generated IP address is unique in a network. In order to perform DAD process, IPv6 hosts use neighbor solicitation and neighbor advertisement messages to communicate with each other in IPv6 distributed network. However, the design of NDP mechanism has incurred security flaws and are vulnerable to spoofing, causing to be prone to DoS attacks. Research has shown that DAD process is vulnerable to denial of service attacks, which can deprive IPv6 host(s) from obtaining a unique IP address. In order to address this issue, several mechanisms have been proposed such as; SeND, Trust-ND, SSAS, Pull Model, and DAD-h. However, due to their design, these mechanisms have indirectly introduced spoofing vulnerabilities which can cause DoS attacks on DAD process. Hence, this thesis presents an integrated framework called “Secure-Duplicate Address Detection (Secure-DAD)”, to secure NS/NA messages from any exploitations which can induce DoS attacks during DAD process in IPv6 distributed network. Secure-DAD, introduces a new NDP Option called “Secure-tag” to secure NS/NA messages exchange between the hosts during DAD process. IPv6 test-bed has been setup to

conduct the experiments, to verify the performance of Secure-DAD compared with standard DAD, and Trust-ND mechanism. Secure-DAD was evaluated in terms of lightweight, confidentiality, integrity, and availability. Analysis of the results showed that Secure-DAD is more promising with improvement in terms of processing time reduction of 45.1% compared to Trust-ND. Moreover, security analysis showed that Secure-DAD can ensure message confidentiality, integrity, and availability against DoS attacks during address verification in IPv6 DAD process. Hence, from the evaluation process, it has been proven that Secure-DAD is applicable for DAD process in IPv6 distributed network.

CHAPTER ONE

INTRODUCTION

1.1 Overview

From the days of ARPANET (Leiner et al., 2009), with slightly over two hundred connected hosts involving five organizations to a massive global, always-on network connecting hosts in the billions. According to the recent report, Internet has become as important as the need for electricity and water (Leusse, 2015). The legacy Internet protocol (Postel, 1981) i.e. Internet protocol version 4 (IPv4) has served its purpose from over the years (Ali, 2012). However, the advancement of Internet technologies with ever-expanding Internet users and a growing number of IP-enabled devices had raised various issues about its limited features set such as: IP address Pool, robustness as well as its scalability (Ali, 2012; Batiha et al., 2011).

In order to overcome these challenges, the Internet Engineering Task Force (IETF) which is the governing body of Internet community has designed a new version of Internet protocol, i.e. Internet protocol version 6 (IPv6) as defined in RFC 2460 (Deering, 1998). IPv6, in addition to providing a much larger address space, new features were introduced such as; simpler header format, extension header, mobility functions, as well as address auto-configuration (Davies, 2012; Colitti et al., 2010). Nevertheless, as with any new technology, IPv6 also suffers from security vulnerabilities and issues such as; reconnaissance attacks, header fragmentation attacks, risks of tunnels and potential holes in dual stacks approaches, and denial of service (DoS) attacks which can be carried out by misusing the ICMPv6 messages

types (Elejla et al., 2016; Saad, et al. 2013). Internet Control Message Protocol version 6 (ICMPv6) is the implementation of the Internet Control Message Protocol (ICMP) for Internet Protocol version 6 (IPv6). ICMP messages are being used to perform error reporting and diagnostic functions. ICMPv6 is an integral part of IPv6 Protocol and is defined in RFC 4443 (Conta and Gupta, 2006). ICMPv6 messages have been discussed in details in Chapter Two in Section 2.2.2. Figure 1.1 depicts the typical IPv6 attack types.

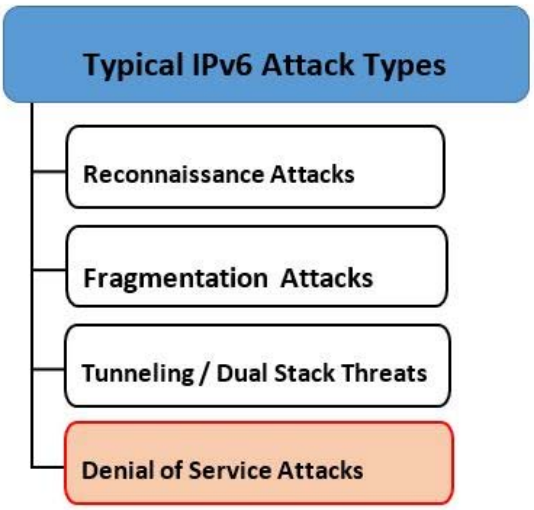

Figure 1.1:Typical IPv6 Attack Types.

1.1.1 IPv6 Features and Related Security Issues

One of the main features of IPv6 protocol, other than large address pool, is the address auto-configuration as defined in RFC 2462 (Thomson, 1998). This feature allows host joining a network to seamlessly obtain network configuration and automatically configure itself without the need for service i.e. Dynamic Host Configuration Protocol (DHCPv6). DHCP is a communications protocol which is based on client/server

model that allows network administrators to centrally manage and automate the network configuration of devices attaching to an Internet Protocol (IP) network as defined in RFC 3315 (Droms, 2003). Whereas, address auto-configuration which is meant for distributed networks i.e. peer-to-peer based allows IPv6 hosts to manage addresses configuration automatically in IPv6 network. Thus, stateless auto-configuration simplifies addressing assignment among hosts in IPv6 network as hosts can generate addresses without need for DHCPv6 services i.e. stateful auto-configuration. The centralized and distributed address management will be further elaborated in Chapter Two.

Stateless address auto-configuration has eased IP addressing assignment. Nevertheless, due to the way it was designed it raises security consequences if not configured properly (AlSa'deh et al., 2012; Groat et al., 2010; Narten et al., 2007). Therefore, in general comparison, IPv6 protocol offers better features and options than IPv4 protocol (Saad, et al. 2013; Ali 2012; Batiha et al., 2011; Durdaugi and Buldu, 2010). However, research have shown that there are certain areas in IPv6 protocol i.e. stateless address auto-configuration which is vulnerable to denial of service (DoS) attacks that prevents IPv6 host(s) to configure itself to join the network (Elejla et al., 2016; Barbhuiya et al., 2011; Caicedo et al., 2009; Yang et al., 2007; Garber, 2000). DoS attack and its impact on IPv6 network has been discussed in Section 1.1.3.

1.1.2 Denial of Service Attacks

Denial of Service (DoS) attack is one of the most significant threats in both IPv4 and IPv6 networks (Raghavan and Dawson, 2011). Furthermore, the recent study (Elejla et al., 2016) has shown that DoS attacks are the major security threats to IPv6 network.

According to this study, 68% of the IPv6 vulnerablities comes under DoS attacks category. These attacks consume the computational resources of the target host(s) and the bandwidth of the network. This leads to the service provided by the target host become unavailable to its intended users. A DoS attack generated by utilizing the vulnerabilities in the network protocols, affects the performance of the target host as well as the other hosts sharing the same network. A targeted host is unable to process such large amount of network traffic and becomes unavailable or out of service.

Moreover, when this attack is carried out on a large scale is known as Distributed Denial of Service (DDoS) attacks (Specht and Lee, 2004). A distributed denial of service (DDoS) attack only differs with DoS attack from the method. DoS attack is made from a singular system or network while DDoS attack is organized to happen simultaneously from a large number of systems or networks (Prudente et al., 2012; Peng, et al., 2007).

1.1.3 Denial of Service Attacks in IPv6 Network

DoS attacks are typically carried out at application and network layers (Li et al., 2011). In IPv6 network such attacks can further be carried out at the link local level due to the design of Neighbor Discovery Protocol (NDP) (Arkko et al., 2005). NDP is one of the main protocol in the IPv6 Internet protocol suite. It operates in the link layer of the Internet model as specified in RFC 1122 (Braden, 1989), and is responsible for communication between the hosts in IPv6 link local network. Neighbor Discovery Protocol has been further discussed in Section 1.1.5. Therefore, based on the attack level, the DoS attacks in IPv6 network can broadly be classified into two main categories i.e. application level and network level. Further, network level DoS attacks

can be sub-divided into Gateway (router) and link local level respectively as illustrated in Figure 1.2.

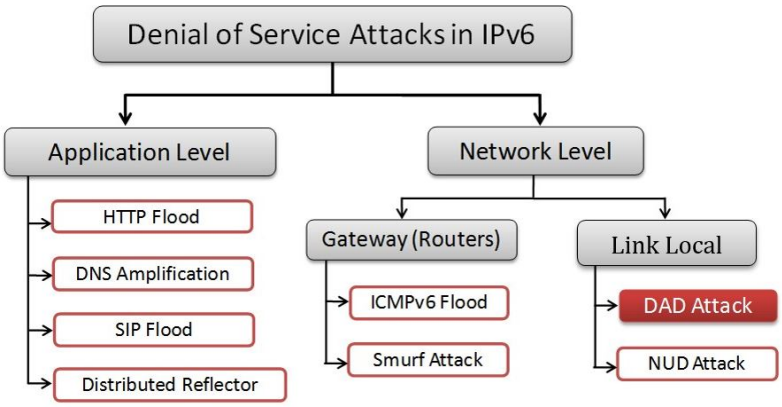

Figure 1.2: Taxonomy of Denial of Service Attacks in IPv6 Network.

During address auto-configuration in IPv6 link local communication (LLC), Internet Control Message Protocol version 6 (ICMPv6) messages are used by the hosts to communicate with neighboring hosts within a local link (Conta and Gupta, 2006). However, studies (Elejla et al., 2016; Saad et al. 2013; Caicedo et al. 2009; Nikander et al. 2004) have shown that the ICMPv6 messages are vulnerable to DoS attacks during duplicate address detection (DAD) process. Duplicate Address Detection (DAD) process is being performed by IPv6 hosts to avoid IP address conflict in the network (Krishnan and Daley, 2010; Thomson, 1998), while host(s) attempts to configure its self-generated interface identifier in the network (IID) (Carpenter and Jiang, 2014).

Therefore, any attacker host can take advantage of it and can fabricate these ICMPv6 messages. Later, attacker can exploit these modified messages to generate DoS attacks in a number of ways such as; ICMPv6 messages spoofing, Man-in-the-Middle form or simply sending excessive number of bogus ICMPv6 messages to the target host on the same link. Here, DoS attack refers to the absence of the service i.e. configuring IP addresses rather than service unavailability due to flooding attack. Thus, in this manner, attacker can disrupt the IPv6 hosts to obtain their interface identifiers (IIDs) (Elejla et al., 2016; Rafiee and Meinel, 2013). IPv6 DAD process and its related issue has been described in detail in Section 1.1.6.

1.1.4 Address Configuration

In IPv6, stateless address auto-configuration (SLAAC) mechanism allows host(s) to derive IP address automatically as the interface identifier (ID) portion of a link layer address is generated directly from the device-specific MAC i.e. media access control address due to its design, unlike in IPv4 protocol as mentioned in RFC 4291 (Hinden and Deering, 2006). Therefore, there is no need of Address Resolution Protocol (Plummer, 1982) in IPv6 protocol. This new protocol called Neighbor Discovery Protocol replaced ARP functionality in IPv6 SLAAC mechanism. SLAAC mechanism has been discussed in detail in Chapter Two in Section 2.2.

1.1.5 Neighbor Discovery Protocol

Neighbor Discovery Protocol (NDP) was defined in RFC 4861 (Narten et al. 2007). From the name itself i.e. neighbor discovery, this protocol by using ICMPv6 messages allows IPv6 hosts to discovery the neighboring hosts in IPv6 link local network. Moreover, it provides additional functionalities such as; address resolution, neighbor

unreachability detection, router discovery, redirect method for access routers to inform IPv6 hosts the most appropriate route available in the network. Also, to perform duplicate address detection process in IPv6 link local network, which has been discussed in detail in Section 1.1.6. Figure 1.3 depicts the neighbor discovery process in IPv6 link local network.

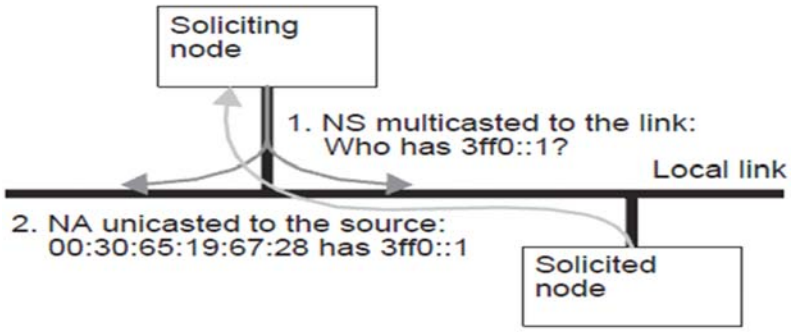

Figure 1.3: Neighbor Discovery Process in IPv6 Network.
(Adapted from (Arkko et al., 2002))

In IPv6 link local communication, NDP uses five types of Internet Control ICMPv6 messages also known as neighbor discovery protocol messages to perform these operations are as follows:

1. Router Solicitation (RS) message type 133, is used by IPv6 hosts to discover the presence of an access router(s) in IPv6 link local network.

2. Router Advertisement (RA) message type 134, is used by router(s) in response to the hosts RS message or used to periodically advertises the RA messages.

3. Neighbor Solicitation (NS) message type 135, is used by the IPv6 hosts to perform the operations like address resolution, host unreachability detection and to perform duplicate address detection process in IPv6 link local network.

4. Neighbor Advertisement (NA) message type 136, is used by the IPv6 hosts to reply back to the NS message queries in IPv6 link local networks.

5. Redirect message type 137, is used by the access routers to advertise better route to the destination for hosts in IPv6 Link local network.

1.1.6 Duplicate Address Detection Process and its Security Issues

Duplicate Address Detection (DAD) process ensures that all configured addresses by IPv6 hosts are likely to be unique on a same link local network. Hence, every IPv6 host(s) has to perform DAD process before assigning the addresses to an interface (Yao et al., 2010; Moore et al., 2006). Although it can be argued that IP conflict is extremely remote due to the immensity of the address space, this will not be the case in the coming years due to growth in mobile device and newly emerging technologies such as; Internet of Things (IoT) and Cloud computing (Botta et al., 2016, Li et al., 2015).

Therefore, when a new host joins the link local network or any existing host on the same link wants to configure a new IP address, at first IPv6 host(s) has to ensure that no neighboring host on the same link is using this self-generated IP address. Therefore, DAD process is being performed to verify the uniqueness of self-generated IP addresses among IPv6 hosts on a same network (Yao et al., 2010; Moore et al., 2006). IPv6 DAD process has been illustrated in Chapter Two in Section 2.3.

IPv6 hosts use neighbor solicitation (NS) and neighbor advertisements (NA) messages to perform DAD process in IPv6 network as aforementioned in Section 1.1.5. For unique address verification purpose, DAD mechanism assumes that all the neighboring hosts are reliable in IPv6 network. Therefore, whatever the responses a

host receives via NS/NA messages from the existing hosts during address verification process it acts accordingly regardless of being valid or invalid message (Yao et al., 2010; Moore et al., 2006).

However, if the NS message is replied by a malicious host via fake NA messages by claiming the self-generated IP address is already obtained. This will prevent IPv6 hosts to configure their unique IP addresses. As a result, IPv6 host(s) will be unable to communicate in IPv6 distributed network. This type of attack is known as DoS-on-DAD attack, which deprives host(s) from address configuration in IPv6 distributed network. Studies (Elejla et al., 2016; Rafiee and Meinel, 2013; Gont 2012; Yang et al., 2007) have shown that the IPv6 DAD process is vulnerable to DoS attacks. DoS-on-DAD attack has been explained in detail in Chapter Two in Section 2.3.2.

1.2 Research Problem

Duplicate address detection process is an essential operation in address auto-configuration mechanism (Yao et al., 2010; Moore et al., 2006), i.e. in SLAAC mechanism to verify the uniqueness of self-generated IP address in IPv6 network. However, studies (Elejla et al., 2016; Rafiee and Meinel, 2013; AlSa'deh et al., 2012; Yang et al., 2007) have also shown that the standard DAD process is vulnerable to DoS attacks during address verification process while host(s) attempts address auto-configuration. Hence, from the studies it has been found that IPv6 host(s) can be deprived from obtaining a unique IP address, which can disrupt the host's link local communication (Elejla et al., 2016; Moore et al., 2006; Yao et al., 2010). In order to address this issue, some of the security mechanisms have been proposed such as; SeND, Pull Model, SSAS, Trust-ND, and DAD-h mechanisms.

SeND mechanism was suggested to solve the security concerns of DAD process in IPv6 network (Arkko et al., 2005). However, this mechanism is not trivial due to its heavy computation and complexity issues which can induce DoS attack during DAD process due to its designed mechanism (Praptodiyono et al., 2015; Rafiee et al., 2013). In order to address this issue, Simple Secure Addressing Scheme (SSAS) was proposed (Rafiee et al., 2013). Although, this mechanism to some extent has addressed the complexity issue by introducing a new addressing scheme compared to the SeND mechanism. Nevertheless, SSAS mechanism still requires significant amount of time to process the neighbor discovery messages i.e. NS/NA which can be exploited by a malicious host to cause DoS attack on DAD process (Praptodiyono et al., 2015).

Similarly, alternative mechanisms for IPv6 DAD process was proposed known as Pull Model (Yao et al., 2010) which uses the pull concept (Duan et al., 2005). The idea behind it was instead of sending the generated target address to existing hosts for verification; rather request i.e. Pull all the existing hosts obtained IP addresses and then compute the hash value and perform the duplicate address verification by computing the hash (Yao et al., 2010). Nevertheless, this mechanism was found vulnerable to brute force attack due to its designed mechanism (Apostol, 2012; Knudsen at al., 2011). Therefore, the proposed idea was not implemented.

In the recent past, Trust-ND mechanism has been proposed that claims to be the lightweight mechanism compared to SeND and SSAS schemes (Praptodiyono et al., 2015). Trust-ND uses the concept of trust as defined in RFC 3756 (Nikander et al., 2004). Nevertheless, the issue with Trust-ND mechanism is that it is built on SHA-1 hashing algorithm (Polk et al., 2011; Wang et al., 2005) which is vulnerable to hash collision attacks (Bhargavan et al., 2016; Andreeva et al., 2015; Polk et al., 2011).

Thus, due to its designed mechanism, any malicious host can compromise Trust-ND to induce DoS attack during DAD process in IPv6 distributed network.

Recently, DAD-h mechanism was proposed (Song and Ji, 2016), this mechanism was designed based on MD5 hash algorithm. According to Song and Ji, (2016), DAD-h mechanism hides the hosts self-generated i.e. target address during address verification process and ensures only those hosts participate in DAD process that are enabled with DAD-h mechanism. However, research have shown that MD5 is vulnerable to hash collision attacks (Bhargavan et al., 2016; Andreeva et al., 2015; Polk et al., 2011). Thus, any malicious host can compromise the DAD-h to cause DoS attack during DAD process in IPv6 distributed network.

Although some of the mechanisms were introduced to secure NS and NA messages which are being used by the IPv6 hosts to perform DAD process in IPv6 network. Nevertheless, these proposed mechanisms have indirectly introduced spoofing vulnerabilities which can cause DoS attacks on DAD process. Since, there is no proper mechanism to address this problem. Therefore, preventing the spoofing of NS/NA messages which can induce DoS attacks on DAD process in IPv6 distributed network is the research problem addressed in this thesis.

Based on the research problem as above mentioned there are some reasons that are responsible for this problem as follows:

1. During DAD process IPv6 host(s) uses neighbor solicitation (NS) and neighbor advertisement (NA) messages, which are insecure by design. Therefore, any malicious host can simply modify the NA message upon receiving the NS message.

2. Existing mechanisms such as: Trust-ND, Pull Model, and DAD-h, suffer from security issues such as; hash collision, brute force attacks which can be exploited to cause NS/NA message spoofing thus, can induce DoS attack on DAD process in IPv6 distributed network.

1.3 Research Goal and Hypothesis

The goal of this research work is to secure DAD process during address auto-configuration, with reduced process overhead in IPv6 distributed network. Thus, IPv6 hosts can perform secure DAD process and the failure caused by DoS attack can be eliminated in IPv6 distributed network. In order to achieve this goal, the hypothesis of this research has been presented as follow:

> *An integrated framework for securing duplicate address detection process by preventing any exploitations of neighbor solicitation (NS) and neighbor advertisement (NA) messages which are responsible for inducing denial of service (DoS) attack during message verification process between hosts in IPv6 distributed network.*

1.4 Research Questions and Objectives

Due to the reasons as aforementioned in Section 1.2, IPv6 DAD process is still prone to DoS attacks. As a result, three research questions rise to address this research problem as follows:

1. What are the constraints of existing security mechanisms?
2. What is a suitable mechanism to prevent spoofing during DAD process?
3. What are the appropriate evaluation methods to evaluate the designed mechanism?

In order to achieve the research goal in answering the abovementioned research questions, the following objectives need to be fulfilled:

1. To design an integrated framework to secure DAD process against DoS attacks in IPv6 distributed network that is more effective in terms of resources requirement.

2. To redesign the NDP message structure to prevent spoofing attacks via replay and MITM attacks.

3. To deploy an IPv6 test-bed to evaluate the performance of the redesigned NDP messages in terms of lightweight, confidentiality, integrity, and availability during DAD process in IPv6 distributed network.

1.5 Research Contributions

The role of DAD process in IPv6 address auto-configuration and its security issues has been briefly discussed. In order to address its issue, security mechanisms have been proposed as aforementioned in Section 1.2. Nevertheless, these proposed mechanism due to their designed mechanism are vulnerable to spoofing attacks which can induce DoS attacks during DAD process in IPv6 distributed network as stated in Section 1.2. In order to resolve this issue, this research has redesigned NDP messages to secure link local communication in IPv6 distributed network. By securing the neighbor solicitation (NS) and neighbor advertisement (NA) messages via Secure-tag Option from any exploitation which can cause DoS attacks on DAD process between the hosts in IPv6 distributed network.

Moreover, address resolution and neighbor unreachability detection functionalities also use NS and NA messages to perform their operations in IPv6 link local network. Since, both of these operations are part of NDP process as stated in Section 1.1.5. Therefore, these Secured NS/NA messages are also applicable for these operations to secure address resolution and neighbor unreachability detection processes between the hosts in IPv6 distributed network. Therefore, the contributions of this research are as follows:

1. Integrated framework for secure DAD process in IPv6 distributed network.

2. Redesigned NDP messages i.e. NS/NA messages by introducing Secure-tag Option to perform secure DAD process.

3. Other sub-contributions of this research are related to two NDP processes i.e. address resolution and neighbor unreachability detection operations. By securing these operations via Secured NS/NA messages.

1.6 Research Scope

In this study, the research scope of the designed security mechanism is limited to secure DAD process during stateless address auto-configuration in IPv6 distributed network as depicted in Table 1.1. By securing NS and NA message via Secure-tag Option to ensure a secure link local communication during DAD process between the hosts in IPv6 distributed network. This Integrated framework is designed for Stateless Address Auto-configuration (SLAAC) in IPv6 distributed network. Although, DAD process is also required in stateful address auto-configuration (DHCPv6) i.e. client/server model based, used to manage the network devices and address configuration centrally. However, that is out of the scope of this thesis. Moreover,

NS/NA messages can also be exploited to cause flood attack by buffer overflow and neighbor cache poisoning. Since, this research is not focusing on flooding attacks. Therefore, NS/NA flooding is not covered in this thesis.

Table 1.1: Research Scope

Items	**Scope of Research**
Environment	IPv6 Network
Attack Type	DoS-on-DAD Attack
NDP Message Types	Neighbor Solicitation (NS) & Neighbor Advertisement (NA)
DoS Target	Network layer
Address Auto-configuration	Stateless Address Auto-configuration (SLAAC)

1.7 Research Steps

In order to achieve the objectives of this research, numerous research phases have been followed that includes: (i) Literature review, to analyze the existing studies and define the research problem, (ii) Design of an integrated framework to secure DAD process in IPv6 distributed network, (iii) Prerequisites and test-bed setup for the experimental purposes, (iv) Implementation of the redesigned NDP messages to secure DAD process for IPv6 distributed network, and (v) Evaluation of the redesigned NDP messages for IPv6 DAD process. Figure 1.4 explains the main phases of this research study.

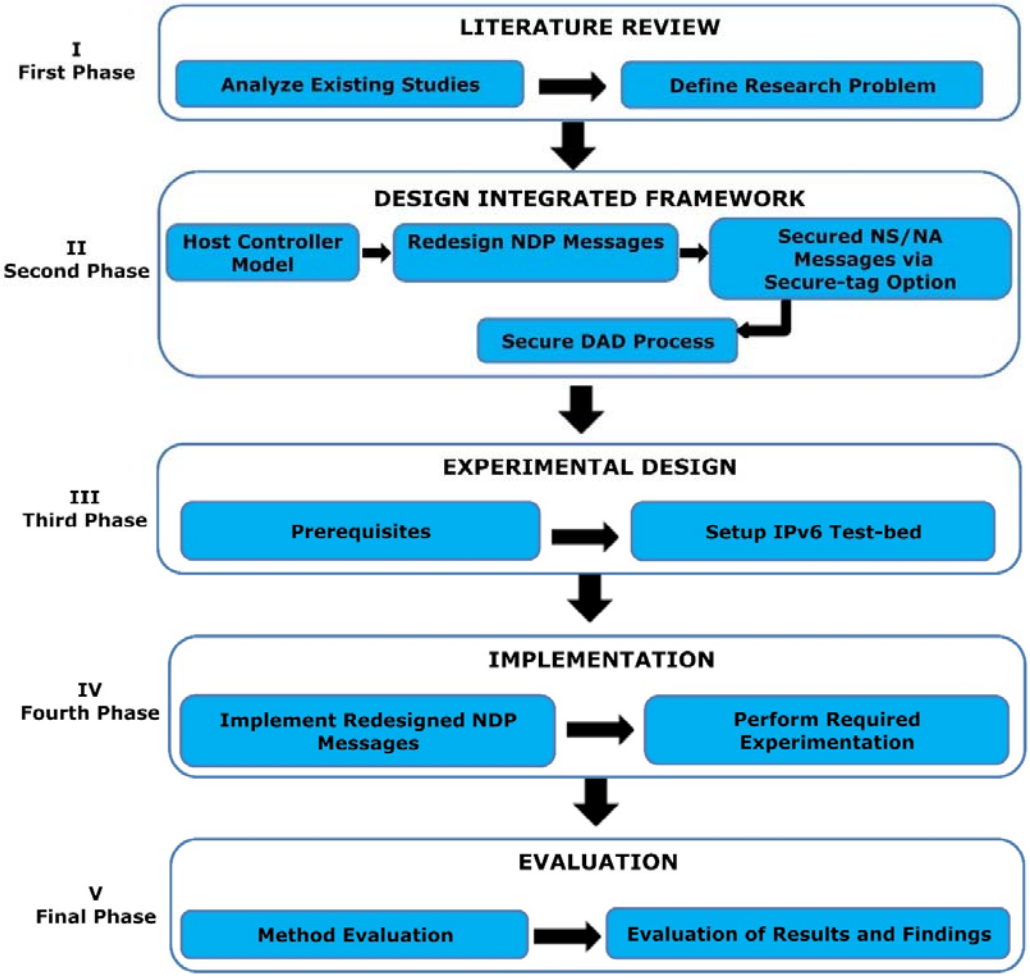

Figure 1.4: Main Phases of Research Study.

In the first phase, the research problem is defined and comprehensively analyzed through a critical review of existing mechanisms. Hence, this literature review provides an understanding of the problem, existing solution space, and future research scope.

In the second phase, the solution for the research problem is presented. The solution consists of several stages to secure DAD process in IPv6 distributed network. The designed integrated framework employs software defined network concept to

secure IPv6 hosts DAD process via Secure-tag Option from disrupting during address verification process in IPv6 distributed network.

In the third phase, prerequisites for the experimental deign such as; Java platform, experimental tools etc. are selected to setup IPv6 test-bed environment to carry out the research experiments.

The fourth phase is mainly concerned with implementation of the redesigned NDP messages i.e. Secured NS/NA messages to secure DAD process during address auto-configuration in IPv6 distributed network.

In the final phase, the evaluation stage leads to the attainment of the goal of this research. For that purpose, the redesigned NDP messages i.e. Secured NS/NA messages are evaluated to ensure a secure DAD process during address auto-configuration, with reduced process overhead in IPv6 distributed network.

1.8 Thesis Organization

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

Chapter Two describes the concepts of stateless address auto-configuration mechanism and duplicate address detection process in IPv6 distributed network. Moreover, it provides the literature review of the related works on existing security mechanism for DAD process in IPv6 distributed network. Issues with the existing security mechanisms are also discussed. Finally, this chapter provides the need of a new security mechanism for securing IPv6 DAD process against DoS attacks during address verification process in IPv6 distributed network.

Chapter Three discusses the proposed methodology by elaborating how an integrated framework was designed. Moreover, the algorithm and how it handles DoS threats on DAD process during address auto-configuration in IPv6 distributed network.

Chapter Four illustrates the implementation details of the redesigned NDP messages i.e. Secured NS/NA messages to protect DAD process during address auto-configuration in IPv6 distributed network.

Chapter Five discusses the evaluation of the redesigned NDP messages i.e. Secured NS/NA messages and analysis of the results obtained through experimentations. This chapter also discusses the performance evaluation of the Secure-DAD compared with existing mechanisms.

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

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The importance of securing IPv6 Duplicate Address Detection process was generally described in Chapter One. This chapter provides the background and some related research on securing DAD process that defines the general structure of this research. The rest of this chapter is organized as follows: At first, a general concept about IPv6 link local communication is presented. IPv6 address auto-configuration mechanism and related information is described in details in Section 2.2 and its subsections respectively. Then, this chapter explains the DAD process, its related security issue, its impact and significance of securing DAD process in IPv6 link local network are mentioned in Section 2.3 and its respective subsections.

The related works on securing duplicate address detection mechanism are provided in Section 2.4 and its respective subsections. In Section 2.5 some alternative security mechanisms are mentioned. The summary of the related works is presented in Section 2.6. This is followed by the description on the need of new security mechanism for DAD process in Section 2.7 and its subsections respectively. Section 2.8 presents the concept of Software-Defined Networking and its relevance to the design of a new security mechanism for DAD process. At last, the summary of this chapter is provided.

2.1.1 IPv6 Link Local Communication

In IPv6 link local network, IPv6 host can communicate with other neighboring hosts directly using wired as well as wireless medium. For this purpose, IPv6 hosts use new communication protocol known as Neighbor Discovery Protocol (NDP) (Narten et al., 2007) in IPv6 link local network instead of Address Resolution Protocol (ARP) (Plummer, 1982) used by IPv4 protocol as aforementioned in Chapter One.

Neighbor discovery, as the name suggests in IPv6 networks allow the hosts to find the presence and link local addresses of other hosts on the same link. Also, it provides other functionalities such as; address resolution, neighbor unreachability detection, router discovery, redirect method for routers to inform hosts about the most appropriate router available on the same link. Besides, it resolves duplicate address detection on the same link which has been discussed in details in Section 2.3.

2.2 IPv6 Address Auto-Configuration

IPv6 address auto-configuration are of two types such as; stateful address auto-configuration (DHCPv6) and stateless address auto-configuration (SLAAC). In case of stateful address auto-configuration, IPv6 hosts obtain address configuration paramenters and other network services from the DHCPv6 server. This type of address configuration is based on client-server model where IPv6 hosts as a client requests the DHCPv6 server to pass the address configuration parameters in order to be able to obtain the unique IP address as specified in RFC 3315 (Droms, 2003).

On the other hand, Stateless Address Autoconfiguration (SLAAC) mechanism as defined in RFC 4862 (Thomson et al., 2007), enables IPv6 hosts to obtain IP addresses automatically without the need for DHCPv6 server. SLAAC mechanism can

ease addressing assignments compared to the Stateful Address Auto-configuration (DHCP server), while configuring hosts as it does not require any intervention, thus provides flexibility in address configuration.

Stateful address auto-configuration (DHCPv6) is suitable for the centralized network where a central server is being deployed to provide address configuration and other network services to the hosts. Whereas, Stateless Address Autoconfiguration (SLAAC) is meant for decentralized network consisting of a collection of autonomous hosts that communicate with each other by exchanging messages (Li & Singal 2007). For instance, public area networks where the address configuration and network services are shared in a distributed manner. Since, this thesis is only focusing at securing DAD process during Stateless Address Autoconfiguration (SLAAC) for IPv6 distributed network. Therefore, Stateful address auto-configuration (DHCPv6) as mentioned in Chapter One is beyond the scope of this thesis, hence cannot be discussed further.

2.2.1 IPv6 Address Auto-configuration Process

When a new host joins an IPv6 network it goes through a number of operations to configure its own interface identifier (Cooper et al., 2016). For instance, once a host connects to an IPv6 network, it sends a Router Solicitation (RS) message to the access router to get the network prefix information. In response, access router replies with a Router Advertisement (RA) message to provide the requested information. As the host gathers required parameters which allows it to generate its own interface identifier (IID) (Hinden and Deering, 2006).

IPv6 host creates the rightmost 64 bits Interface Identifier (IID), which identifies an individual host within a local network. The IID is often configured from the Extended Unique Identifier (EUI-64) that is generated based on the interface hardware identifier usually the MAC address of the network card (Cooper et al., 2016; AlSa'deh et al., 2013; Narten et al., 2007).

Afterwards, the host combines the subnet prefix with the IID to form a complete 128 bits IPv6 address which is required for the IPv6 hosts to communicate in a network. In order to be able to communicate on the same network, IPv6 host(s) has to verify the uniqueness of its self-generated IP address which is the final stage of address auto-configuration (Yao et al., 2010; Moore et al., 2006), which is being performed by Duplicate Address Detection process as aforementioned in Chapter One and has been further explained in detail in Section 2.3.

In IPv6 link local communication, IPv6 hosts use ICMPv6 messages also known as Neighbor Discovery Protocol messages to perform address auto-configuration process (Rosen, 2014; Conta and Gupta, 2006) as stated in Chapter One in Section 1.1.5. Figure 2.1 depicts the new host address auto-configuration process in IPv6 network.

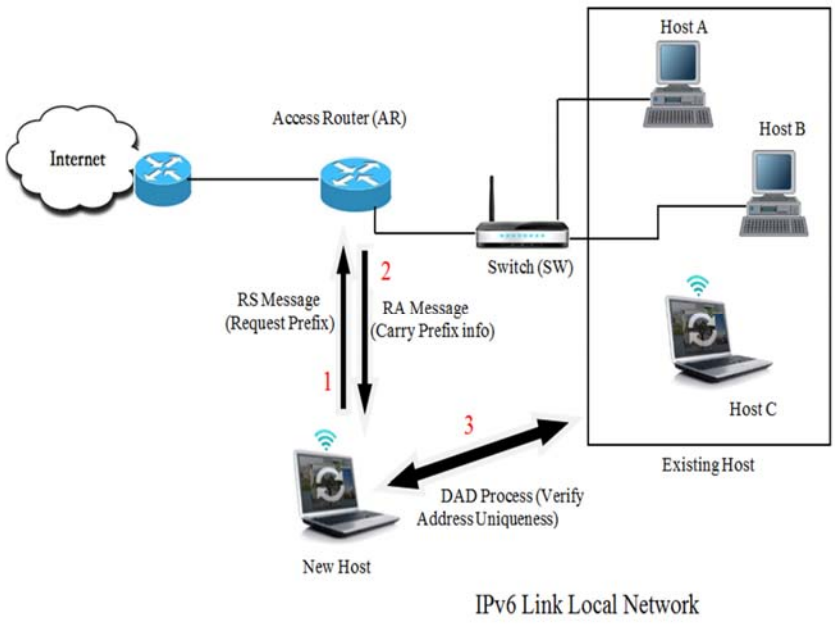

Figure 2.1: IPv6 Address Auto-configuration Process.

2.2.2 The Need of ICMPv6 Messages

ICMP is a main part of Internet protocol suite, as defined in (Postel, 1981). ICMP messages are generally used for diagnostic, testing, control purposes or generated in response to errors, and report problem conditions in IP operations which are directed to the source IP address of the originating packet (Rosen 2014). For example, IPv4 uses ICMPv4 messages for that purposes. Similarly, IPv6 protocol uses ICMPv6 messages for doing the same operations.

The differences between the two ICMP message protocols, i.e. ICMPv4 and ICMPv6, are in specific message types and formats. For instance, in ICMPv4 there is no relationship between *Type* value and message type. However, in ICMPv6 error messages have a *Type* value of 0 to 127, informational messages 128 to 255 and

ICMPv6 messages are transported by IPv6 packets in which the IPv6 Next Header value for ICMPv6 is set to 58 (Li et al., 2011; Convery and Miller, 2004). Appendix A lists the ICMPv6 message types and their functionalities.

However, studies (Saad, et al. 2013; Ali 2012; Batiha et al., 2011; Durdaugi and Buldu, 2010) have shown that ICMPv4 messages are vulnerable to security threats some of the well-known threats are: Ping of Death, Smurf attack, ICMP redirect attack, and DoS attacks. In order to counter these security threats, prevention measures can be employed by deploying the IDS's and firewalls at the edge or gateway routers to detect and drop or block such malicious ICMP messages. Similarly, ICMPv6 messages can suffer from the same issues. Nevertheless, ICMPv6 messages cannot be simply blocked or dropped due to the fact that Neighbor Discovery Protocol (NDP), address auto-configuration and other IPv6 services requires ICMPv6 messages to perform these operations (Elejla t al., 2016; Saad et al. 2013; AlSa'deh and Meinel, 2012; Caicedo et al. 2009; Nikander et al. 2004).

2.2.3 IPv6 Address Auto-configuration States

Auto-configured address can be in one or more of the following states during its valid-life timer i.e. Tentative, Valid, Preferred, Deprecated or Invalid (Thomson et al., 2007). These states can be described as follows:

1. Tentative state: Auto-configured address is considered tentative when it is in the process of being verified as unique. Verification of an address occurs during duplicate address detection process. A host(s) having tentative address cannot receive unicast traffic. However, can receive and process multicast