

**AUTHENTICATION FOR STATELESS ADDRESS
ALLOCATION IN IPv6 NETWORKS**

BY

ADENIYE, SULI CHARLES

A Thesis Presented to the
DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DAHHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE
In
COMPUTER ENGINEERING

FEBRUARY 2012

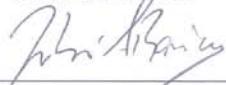
KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

This thesis, written by Adeniye, Suli Charles under the direction of his thesis advisor and approved by his thesis committee, has been presented to and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN COMPUTER ENGINEERING.**

Thesis Committee



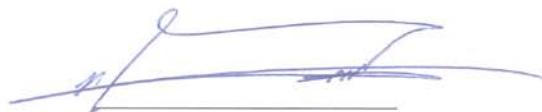
Dr. Zubair A. Baig (Advisor)



Dr. Sadiq M. Sait (Member)



Dr. Ahmad Al-Mulhem (Member)



Dr. Basem Al-Madani
Department Chairman



Dr. Salam A. Zummo
Dean of Graduate Studies

12/3/12

Date

DEDICATION

TO MY PARENTS

ACKNOWLEDGEMENTS

First of all, I am grateful to Almighty Allah for endowing me with strength, zeal and knowledge to accomplish this work.

I would also want to express my profound appreciation to Dr. Zubair Ahmed Baig, my thesis advisor, for his regular excellent feedback and comments at every stage of this work. He was always available to receive me, know my progress and allay my fears on some issues even outside of his office hours.

I would also like to thank Dr. Sadiq Mohamed Sait and Dr. Ahmad Al-Muhem for their invaluable suggestions and constructive criticisms. I am equally grateful to the Computer Engineering Department's Chairman, Dr. Basem Al-Madani and other faculty members and staff of the department for their support.

Also worthy of mention is the warm and motivating atmosphere provided by members of Nigerian community in KFUPM, especially the ones in the College of Computer Sciences and Engineering. I thank them for their advices and fruitful discussions.

I am most grateful to my parents for their support right from day one. They brought me up to value learning and hard work, have regards for sincerity and also to appreciate people.

Finally, I thank my wife 'Deola and my little son, Abdallah for their support and for having to cope with my long period of absence for most part of this thesis work.

TABLE OF CONTENTS

List of Tables.....	vii
List of Figures.....	viii
Thesis Abstract (English).....	xi
Thesis Abstract (Arabic).....	xiii
CHAPTER 1: INTRODUCTION.....	1
1.1 The Internet Protocols.....	1
1.2 The IPv6 Protocol.....	2
1.3 IPv6 Features.....	2
1.4 Configuration of Nodes Addresses in IPv6 Networks.....	9
1.5 Stateless Address Auto-configuration and Neighbour Discovery Protocol.....	13
1.6 Address Formation Using Stateless Auto-configuration.....	13
1.7 Duplicate Address Detection (DAD).....	15
1.8 Motivation and Objectives of the Thesis.....	17
1.9 Thesis Methodology.....	18
1.10 Contributions of the Thesis.....	18
CHAPTER 2: BACKGROUND, TERMINOLOGIES AND LITERATURE SURVEY.....	20
2.1 Security Issues Common to IPv4 and IPv6.....	20
2.2 Security Vulnerabilities Specific to IPv6 Protocol.....	22
2.3 Concept of Trust and Reputation in Peer-to-Peer Networks.....	26
2.4 Survey on Trust-based Schemes.....	29

CHAPTER 3: TRUST-BASED MECHANISM FOR PROTECTING IPV6 NETWORKS AGAINST STATELESS ADDRESS AUTO-CONFIGURATION ATTACKS.....	33
3.1 Proposed Trust Algorithm.....	36
3.2 Simulation and Analysis.....	37
3.3 Conclusion.....	42
3.4 Accomplishment.....	42
 CHAPTER 4: MSB / LSB SCHEME.....	43
4.1 Terminology.....	43
4.2 EUI-64 and Neighbour Discovery Protocol.....	44
4.3 Stateless Address Auto-configuration Attack Detection: MSB / LSB Technique.....	43
4.4 The Proposed MSB / LSB Algorithm.....	48
4.5 Experimental Setup.....	49
4.6 Performance Analysis.....	50
4.7 Analysis of Results.....	53
4.8 Strengths of the MSB / LSB Scheme.....	60
 CHAPTER 5: CONCLUSIONS AND FUTURE WORK.....	61
5.1 Conclusions.....	61
5.2 Future Work.....	62
 REFERENCES.....	63
VITA.....	70

LIST OF TABLES

Table 1.1: Scope bits in a multicast address.....	6
---	---

LIST OF FIGURES

Figure 1.1: Structure of an IPv4 Packet.....	1
Figure 1.2: Structure of an IPv6 Address.....	4
Figure 1.3: Format of a link-local Address.....	4
Figure 1.4: Format of an IPv6 Multicast Address.....	5
Figure 1.5: IPv6 Packet header structure.....	6
Figure 1.6: DHCP Server and Client.....	12
Figure 1.7: DHCP Server, Client and a Relay.....	12
Figure 1.8: Formation of a link-local address.....	14
Figure 1.9: Formation of a global site address with router solicitation and router advertisement messages.....	16
Figure 1.10: Auto-configuration process–formation of a link-local and globally-unique address.....	16
Figure 2.1: Host Initialization Attack.....	24
Figure 3.1: The effect of increasing the number of good nodes y on the value of τ	36
Figure 3.2: G_{ij} values against varying k for a diverse number of good nodes y , $N = 20$	39

Figure 3.3: Gij values against varying k for a diverse number of good nodes y, N = 50.....	39
Figure 3.4: Gij values against varying k for a diverse number of good nodes y, N = 100.....	39
Figure 3.5: Gij values against varying k for a diverse number of good nodes y, N = 200.....	40
Figure 3.6: Gij values against varying k for a diverse number of good nodes y, N = 500.....	40
Figure 3.7: Gij values against varying k for a diverse number of good nodes y, N = 800.....	40
Figure 3.8: The effect of increasing network size on the delay incurred by the address verification scheme for varying values of α	41
Figure 4.1: Format of MSB / LSB neighbour solicitation message.....	46
Figure 4.2: Format of MSB / LSB neighbour advertisement message.....	47
Figure 4.3: Plot of time window vs number of neighbour advertisement response, N = 100.....	54
Figure 4.4: Figure 4.3: Plot of time window vs number of neighbour advertisement response, N = 200.....	55
Figure 4.5: Plot of time window vs number of neighbour advertisement response, N = 300	55
Figure 4.6: Plot of time window vs number of neighbour advertisement response, N = 400	56
Figure 4.7: Plot of time window vs number of neighbour advertisement response, N = 500	56
Figure 4.8: Plot of time window vs number of neighbour advertisement response, N = 800	57
Figure 4.9: Plot of time window vs number of neighbour advertisement response, N = 100, L = 3	58

Figure 4.10: Plot of time window vs number of neighbour advertisement response, N = 200, L = 3 59

Figure 4.11: Plot of time window vs number of neighbour advertisement response, N = 800, L = 3 59

THESIS ABSTRACT (ENGLISH)

NAME: ADENIYE, SULI CHARLES
TITLE: AUTHENTICATION FOR STATELESS ADDRESS ALLOCATION IN IPv6 NETWORKS
MAJOR: COMPUTER ENGINEERING
DATE: 20 FEBRUARY 2012

The IPv6 protocol is the next-generation IP protocol that addresses many of the shortcomings in the present IPv4 protocol. Some of the enhancements in the IPv6 over IPv4 are increased address space, mandatory security and provision of stateless auto-configuration, a technique by which a new node forms its own address without the assistance of DHCP server or manual configuration by a network administrator. While the stateless auto-configuration approach allows instant plugging in of a node, guarantees immediate communication with other nodes and eliminates the costs of procuring and maintaining DHCP servers, it however opens up ways for malicious nodes in the network to disallow many upcoming nodes from initialising their network interfaces, a form of denial of service. In this thesis, we propose two techniques to allow upcoming nodes in an IPv6 network to ascertain, in distributed fashion, the uniqueness of their respective network identifiers. The first scheme uses a P2P trust-verification approach for identifying a rogue node. The second scheme is based on information hiding. Our proposed schemes do not rely on centralized verification servers, and they prove to provide high assurance to new nodes intending to join the network, with minimal overhead, as illustrated through our simulations and analysis.

MASTER OF SCIENCE DEGREE
KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
Dhahran, Saudi Arabia

THESIS ABSTRACT (ARABIC)

الاسم: سولي شارليس ادينبيه

العنوان: مصادقة لعملية تخصيص العنوان المهمel في شبكات الاصدار السادس لبروتوكول الانترنت

التخصص: هندسة الحاسوب الالي

التاريخ: 28 ربيع الأول، 1433 هجري

الاصدار السادس من بروتوكول الانترنت هو بروتوكول الجيل الجديد من بروتوكولات الانترنت التي تحل العديد من اوجه القصور في الاصدار الرابع من بروتوكول الانترنت الحالي. هنالك بعض التحسينات في الاصدار السادس بالمقارنة مع الاصدار الرابع من حيث حجم العنوان، والأمن، وتوفير الاعدادات التلقائية للعناوين المهمة بحيث أن العقد الجديدة تقوم بتشكيل العنوان الخاص بها من دون مساعدة خادم بروتوكول الاعدادات التلقائية للمضيف، ومن دون الاعدادات اليدوية لمسؤول الشبكة. في حين أن نهج الاعدادات التلقائية المهمة يسمح بالتوصيل التلقائي للعقدة، ويضمن التوصيل التلقائي مع العقد الأخرى ويلغي تكلفة شراء وتصليح خادم بروتوكول الاعدادات التلقائية للمضيف. وكذلك يفتح فرص للعقد المشبوهة بعدم السماح للعقد الجديدة من الاتصال بالشبكة والذي هو شكل من أشكال الحرمان من الخدمة. في هذه الأطروحة، إننا نقترح اثنين من التقنيات تسمح للعقد الجديدة في الاصدار السادس من بروتوكول الانترنت من التأكد من حصولها على عنوان فريد، بحيث يتم ذلك بطريقة لامركزية. التقنية الأولى تستخدم طريقة تأكيد الثقة المستخدمة في النظير إلى النظير للتعرف على العقد المشبوهة. بينما التقنية الثانية تعتمد على إخفاء المعلومات. التقنيات المقترحة لا تعتمد على خوادم تأكيد مركبة، وقد أثبتت فعالية عالية بالنسبة للعقد الجديدة التي تحاول الانضمام الى الشبكة، مع الحد الأدنى من الزمن اللازم لإتمام العملية. وهذا ما سوف يتم بيانه من خلال المحاكاة والتحليل.

درجة الماجستير في العلوم

جامعة الملك فهد للبترول و المعادن

الظهران المملكة العربية السعودية

CHAPTER 1

INTRODUCTION

1.1 The Internet Protocols

The idea of Internet Protocols was conceived in the mid-1970s at the Defence Advanced Research Projects Agency (DARPA) when there was a need in building a packet-switched network that would enable communication between dissimilar computer systems at research institutions. The Internet Protocol version 4 (IPv4) which had hitherto served as the core of the present Internet was specified in [RFC791] and mainly functions to provide connectionless, best-effort delivery of datagram through an internetwork [27]. It also provides fragmentation and reassembly of datagram to support data links having different maximum transmission unit (MTU) sizes. The IPv4 which is based on 32-bit address format, has a packet structure illustrated in Figure 1.1

Version	IHL	Type of Service	Total length
Identification		Flags	Fragment offset
Time-to-live	Protocol	Header checksum	
Source Address			
Destination Address			
Options (+ padding)			
Data (variable)			

Fig. 1.1 Structure of an IPv4 Packet

1.2 The IPv6 Protocol

Specified in the [RFC2460] [1] and designed to address the shortcomings in IPv4, the Internet Protocol version 6, so-called “the next-generation internet protocol” or IPng provides a more flexible and powerful framework upon which next generation network applications and services would be deployed [2]. One of the main drivers for designing the new protocol was the shrinking of address space in IPv4, which was designed in the early 80’s and had laid the foundation for the Internet. However, the IPv4 protocol was based on 32 bits and could only provide 2^{32} (or 4.3 billion) IP addresses, which were projected to be used up by Internet hosts in the next few years. While IP address conserving techniques such as Network address translation (NAT) and Classless Inter-domain Routing (CIDR) have served the internet community in prolonging the time when the whole address space would be fully consumed, analysts have argued that NAT operation is antithetical to the end-to-end principle of data transfer in the internet. In addition, the NAT’s philosophy does not encourage the proliferation of applications (such as P2P) that require that communication nodes are fully transparent to one another.

1.3 IPv6 Features

1.3.1 Increased Address Space

The IPv6 protocol design, on the other hand, is based on 128 bits and provides up to 2^{128} (or 3.4×10^{38}) addresses, a huge address space that is more than adequate for both today’s and future’s hosts and application needs. The avalanche of IPv6 addresses eliminates the need for NAT, maintains the end-to-end data transfer principle [3], as well as supports at

low cost, P2P, VoIP and videoconferencing applications all of which do not fare well with NAT.

IPv6 Address Format

While IPv4 addresses are represented in four fields of decimal numbers, in the range 0 to 255, each number representing 8 bits (e.g. 192.168.0.10, 10.1.9.242 etc), addresses in IPv6 are represented using hexadecimal notation to allow for larger number of IP address representation. In addition, the hexadecimal scheme compresses the representation of addresses better - It uses 8 fields of hexadecimal numbers (0-F), each field delineated with a colon symbol, and represents 16 bits using 4 hexadecimal digits [29]. For example, 2002:1234:0000:ACBD:2054:0000:0000:0B15 is a valid IPv6 address.

IPv6 addressing is also guided with some rules which are – (i) hexadecimal letters are not case-sensitive, for instance, ‘ACBD’ denotes ‘acbd’ (ii) leading zeros in a field are optional, for example, ‘0B15’ denotes ‘b15’ (iii) successive fields of zeros are represented as ‘::’, but this appears only once in an address, for example, the full IPv6 address above can also be written as 2002:1234:0:acbd:2054::b15.

[RFC4291] specifies three forms of addresses in IPv6 protocol – Unicast, Anycast and Multicast:

- i. Unicast Address** – A unicast address refers to a single interface of a node and packet sent to this address is only received by this interface. An important example of unicast address is the global unicast address which all nodes use in communicating on the Internet. The global unicast address use the address range

of 2000:: to 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. All of these addresses have 001 as the leftmost bits.

The basic structure of an IPv6 address is depicted as shown in Figure 1.2 below:

Prefix from provider (48 bits)	Site subnets (16 bits)	Host part: Interface Identifier (64 bits)
-----------------------------------	---------------------------	--

Fig. 1.2 Structure of an IPv6 address

As shown, the 48-bit leftmost part of the address represents the prefix allocated by the provider to a site. The middle 16 bits represents the number of subnets in a site – this means that an IPv6 network site can have a maximum of 2^{16} subnets. The 64-bit rightmost part is the length of the interface identifier, which identifies a host in a subnet. An IPv6 subnet can have up to 2^{64} addresses.

A Scoped address is another form of unicast address and it is of two types – Link-local scope and site-local scope. The link-local addresses can only be used between nodes connected on the same link and are never forwarded by a router. A link-local address is represented by fe80:0:0:0:<interface identifier> as shown in Figure 1.3

Fe80 (16 bits)	0 (48 bits)	Interface Identifier (64 bits)
-------------------	----------------	-----------------------------------

Fig. 1.3 Format of a link-local address

An IPv6-enabled interface has a link-local address automatically configured. This enables it to communicate with other nodes on the same link.

ii. Anycast Address – An anycast address refers to a group of interfaces. Packets sent to an anycast address are received by one of the interfaces in the group (usually the nearest one). An anycast address can only be used as a destination address and starts with the prefix of the target network, followed by the host part that identifies the anycast group.

iii. Multicast Address – A multicast address also refers to a group of addresses. However, packets sent to a multicast address would be delivered to all the interfaces in the group [28]. The format of a multicast address is ff<L><S>>::/16 is illustrated in Figure 1.4. L bit is the lifetime of the multicast group and the S bit denotes the scope. The lifetime field enables us to specify a multicast address as temporary such as one-hour videoconference, or permanent use like an address identifying all routers on a link.

FF (8)	L (4)	S (4)	Multicast group identifier (112 bits)
-----------	----------	----------	--

Fig. 1.4 Format of a IPv6 multicast address

A value of 0 (0000) in the ‘L’ field indicates ‘permanent’ group while a value 1 (0001) denotes ‘temporary’ multicast group. The different values allowed in the scope field and what they represent is illustrated in Table 1.1.

Table 1.1 Scope bits in a multicast address

Value of S (binary)	Value of S (hex)	Scope
0001	1	Interface
0010	2	Link
0100	4	Admin
0101	5	Site
1000	8	Organisation
1110	E	Global
Others		Reserved

Broadcast address is extensively used in IPv4 for many things. IPv6 discontinues the use of broadcast and uses multicast instead. This is to encourage the efficient use of network bandwidth since datagram sent to nodes in a multicast group is received and processed by all nodes, unlike in a broadcast where some or many nodes may not be intended recipients of the datagram. Figure 1.5 shows the packet header of an IPv6 packet

Version (4 bits)	Traffic class (8 bits)	Flow label (20 bits)		
Payload length (16 bits)		Next header (8 bits)	Hop limit (8 bits)	
Source address (128 bits)				
Destination address (128 bits)				
Data payload				

Fig. 1.5 – IPv6 Packet header structure

1.3.2 Address Auto-Configuration & Host Discovery

IPv6 provides a means for network devices to initialise their interfaces and start communicating with peer nodes without the need for a server or static configuration. In addition, IPv6 comes with a very crucial protocol - the neighbour discovery protocol (NDP) which allows a node to discover neighbouring nodes and routers [51]. Besides host discovery function, the NDP also performs a number of functions such as address resolution, redirection, and neighbour unreachability detection.

1.3.3 Mandatory Security

The IPv4 was initially designed with no security consideration in mind. The provision of security is therefore the responsibility of higher layer protocols (i.e. transport and application layers). Although this design worked well some years after the initial introduction of the IPv4, however today's security threats that exist in the Internet such as denial-of-service attacks, man-in-the-middle attacks, malicious code distribution, reconnaissance attacks etc have proved this IPv4 security model inadequate. The IPSec is a suite of cryptographic protocols whose use is mandatory in IPv6, but not in IPv4.

The IPSec protocol suite comprises:

- i. Authentication Header (AH) protocol, which allows for authentication and integrity of data.
- ii. Encapsulating Security Payload (ESP) protocol, which enables authentication, integrity as well as privacy of data.
- iii. Internet Key Exchange (IKE) protocol, which helps in initially setting up and negotiating security parameters between two end points. It also keeps

track of this information so that communication stays secure till the end.

1.3.4 Optimized Header

A number of factors account for why the header structure of an IPv6 datagram is much simpler and efficient than that of IPv4. First, the number of fields in the header is less than that of IPv4 which reduces the processing time intermediate routers would have to spend on headers. Second, the option field appears after the base header which means that routers would not need spending time to compute the checksum needed to verify packet integrity. And third, the extension header allows for more flexible inclusion of protocols than what IPv4 can offer.

1.3.5 Quality of Service

The 8-bit Traffic Class and 20-bit Flow Label headers provide the quality of service requirements in IPv6. While the Traffic Class header is used originating nodes and / or forwarding routers in identifying and distinguishing IPv6 packets from different classes or priorities (doing essentially the same function as a Type of Service header in IPv4, the Flow Label field defines the packets of the flow. The main benefit of the Flow Label is that intermediate routers do not have to open the inner packet to identify the flow, but only check the flow identification fields, source address and flow label, to direct traffic as required [30].

1.4 Configuration of Nodes' Addresses in IPv6 Network

A host in an IPv6 network can have an IP Address in one of three ways –

- i. static address configuration
- ii. stateless address auto-configuration, and
- iii. stateful (server-based) address auto-configuration [1][2].

In static address configuration, the information used in configuring an IPv6 host is either obtained from a command line or from a static file. This information typically comprise the IP address, prefix length, and DNS servers. Similar to IPv4, this configuration method is used in giving addresses to routers and servers, which rarely change their addresses in the network.

The stateful address auto-configuration technique uses a DHCP server, which provides a mechanism of passing reusable IPv6 addresses and other configuration parameters to network nodes [3].

The following list of terms are imperative to be able to have get a clear picture of how a node gets configured with an IPv6 address and other configuration parameters using the DHCPv6 server / client protocol.

SOLICIT: a Solicit message is typically sent by a client to locate DHCP servers.

ADVERTISE: an Advertise message is sent by a server to indicate that it is available for a DHCP service, and it is sent by a server in response to a Solicit message received from a client.

REQUEST: a Request message is sent by a client to request configuration parameters, including IP addresses from a specific client.

CONFIRM: a Confirm message is sent to any available server by a client to verify that the addresses assigned to the client is still appropriate to the link to which the client is connected.

RENEW: a Renew message is sent to the server that originally provided the client's addresses and configuration parameters in order to extend the lifetime on the client's address and to also update other configuration parameters.

REBIND: a Rebind message is sent to any available server in order to extend the lifetime on the addresses assigned to the client and also update other configuration parameters. A Rebind is sent after a client receives no response to a Renew message.

REPLY: A Reply message including assigned addresses and configuration parameters is sent by a server to a Solicit, Request, Renew, Rebind message received from a client. A Reply message is sent in response to an Information-request message. In Confirming / Denying that the addresses assigned to the client are appropriate to the client's link. The server also sends a reply message to the client.

RELEASE: a Release message is sent by a client to the server to indicate that the address assigned to it will no longer be used

DECLINE: If a client has determined that one or more addresses assigned to it by DHCP server is already in use on the client's link, it sends a Decline message to the server.

RECONFIGURE: The Reconfigure message is sent by the server to inform the client that the server has new or updated configuration parameters in order that the client can start a Renew / Reply or Information-request / Reply transaction to be able to receive updated information.

INFORMATION-REQUEST: This message is sent to a server by a client to request configuration parameters without the assignment of any IP addresses

RELAY-FORW: a Relay-forward message is sent by a relay agent to servers either directly or through another relay agent. The received client message / relay-forward message is encapsulated in an option field in the relay-forward message

RELAY-REPL: a Relay-reply message containing a message that a relay-agent delivers to a client is sent to it by the DHCP server. The message could be relayed by other relay agents for delivery to the destination relay agent

The relay agent extracts client message encapsulated by the server as an option in the Relay-reply and relays it to the client

A DHCP client may be configured using a DHCPv6 server in two network configurations – a network scenario in which the client shares the same link with the DHCP server and a scenario where the server and the client do not share the same link, which necessitates the use of a DHCP relay. These scenarios are shown Figures 1.6 and 1.7 respectively.

Typically, a client boots up in an IPv6 network generating its link-local address and sends a Network Discovery – Router Solicitation (ND RS) message to all-router multicast address FF02::2 to request for router advertisement (RA). If the ‘Managed Configuration

Flag' in the Router Advertisement packet is set or there is no router advertisement after several router solicit, the client proceeds to send a DHCP Solicit message to all-DHCP-agents multicast address FF02::1:2 to locate the available DHCP servers.

If a DHCP server is on the same link as the requesting client, the server responds with a DHCP Advertise message. Else, a DHCP Relay forwards the Solicit message to any available DHCP server on the network site multicast address FF05::1::3. A DHCP server responds to the client via the relay [4].

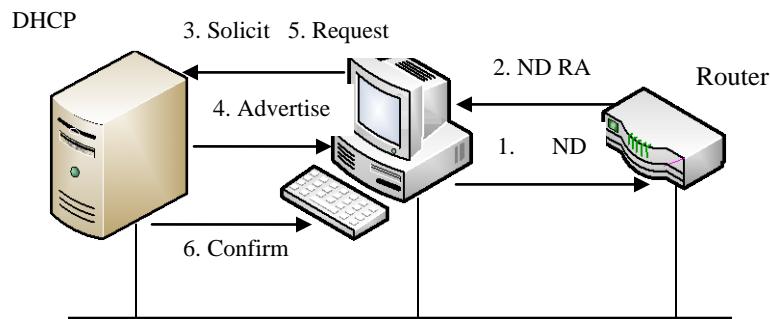


Fig. 1.6 DHCP Server and Client

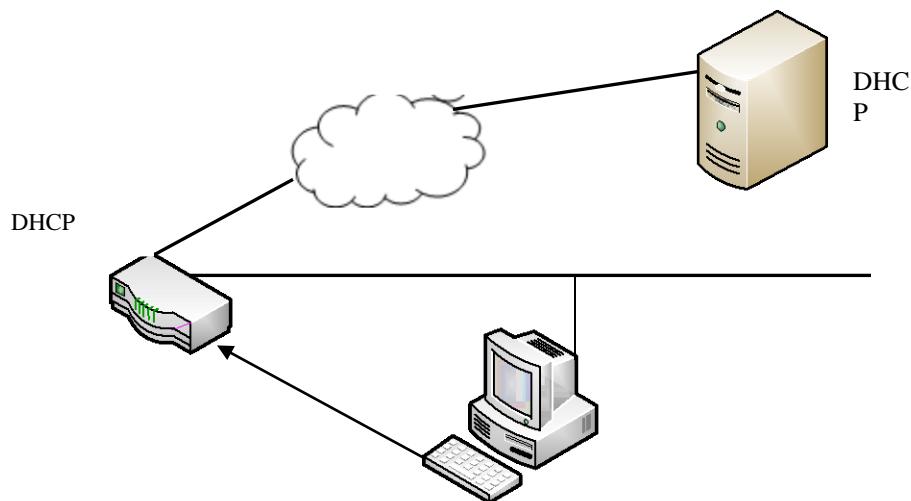


Fig. 1.7 DHCP Client, Server and a Relay

1.5 Stateless Auto-configuration and Neighbour Discovery protocol

Eliminating the need for a DHCPv6 client / server algorithm as employed in the stateful address auto-configuration described earlier, the stateless address auto-configuration is a technique in which IPv6 network nodes form their addresses from a combination of information they get from their interface address, and the subnet prefix of the link to which they are attached [5].

A crucial component of the stateless auto-configuration algorithm is the Neighbour Discovery (ND) protocol. Implemented within the Internet Control Message protocol, the Neighbour Discovery protocol provides an enhanced functionality of IPv4's Address Resolution Protocol (ARP), as well as allowing hosts to discover the neighbouring routers and a means of getting configuration information from them. In addition, the ND protocol defines Neighbour Unreachability Detection mechanism, an algorithm that helps to determine when a neighbor becomes unreachable [6].

Two pairs of messages are the key part of the Neighbour Discovery protocol. One is neighbor solicitation (NS) and neighbor advertisement (NA) which helps in determining the link-layer address of neighbours, as well as verifying that a neighbor is reachable. The other pair is router solicitation (RS) and router advertisement (RA) both of which are employed in obtaining information from routers.

1.6 Address formation using the Stateless Auto-configuration

A node's interface is assigned an address using the stateless auto-configuration approach, in the following sequence:

- i. A node forms the link-local address

- ii. The node ascertains the uniqueness of its link-local address by performing duplicate address detection (DAD) check.
- iii. The node obtains a network-prefix value from the neighboring routers
- iv. The node forms its global-site local address from the network-prefix information obtained from router advertisements.

The node generates its link-local address by concatenating its link-local prefix FE80::/64 bits with its 64 bits interface ID. The 64-bit interface ID is generated from the node's 48-bit MAC address by inserting a 16-bit 'FF-FE' string in between the third byte and the fourth byte and then setting the uniqueness bit (the uniqueness bit is the second bit of the leftmost octet and it identifies the distinctiveness of the MAC address – it is typically set to 1 if the MAC address is unique). For instance, an IPv6 node with a MAC address 00-12-6B-3A-9E-9A would create a temporary link-local address by inserting FF-FE in the middle of the 48-bit MAC address, setting the uniqueness bit to give an interface ID of 0212:6BFF:FE3A:9E9A, and concatenating the link-local prefix with the interface ID which results in link-local address of FE80::0212:6BFF:FE3A:9E9A. This is illustrated in Figure 1.8.

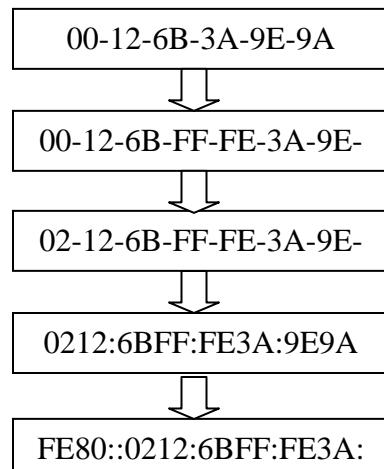


Fig. 1.8 Formation of link-local address

1.7 Duplicate Address Detection (DAD)

In order to confirm that the assigned link-local address is unique, and hence the usability of the address on the local link, the node undergoes a duplicate address detection process by sending a message to the corresponding solicited-node multicast address. This solicited-node multicast address is formed by concatenating a fixed leftmost of 104 bits with 24 bits that is taken from the rightmost part of the link-address. Thus, the solicited-node multicast address for FE80::0212:6BFF:FE3A:9E9A is FF02::1:FF3A:9E9A. If there is a neighbor advertisement (NA) response to this neighbor solicitation message, this indicates that the link-local address is already in use by another node and cannot be used by the soliciting node. Duplicate addresses should not be experienced very often during the auto-configuration process since the interface identifier, which forms part of the address, is obtained from a unique MAC address.

However, if the IPv6 node does not get a neighbor advertisement message in response to its neighbor solicitation message, it proceeds to obtain network-prefix information by sending a router solicitation (RS) message to all the routers on its link on the destination multicast address FF02::2. The router advertisement (RA) containing the network prefix is sent by the routers (for example, with a prefix 3FFE:A00:1:/64 in the source address) to the all-nodes multicast FF02::1 (all-nodes multicast address). Thus, the new node can form its globally-unique address by appending the network-prefix information to its interface identifier. The globally-unique address can be used by the node to communicate on the internet. This is illustrated in Figures 1.9 and 1.10.

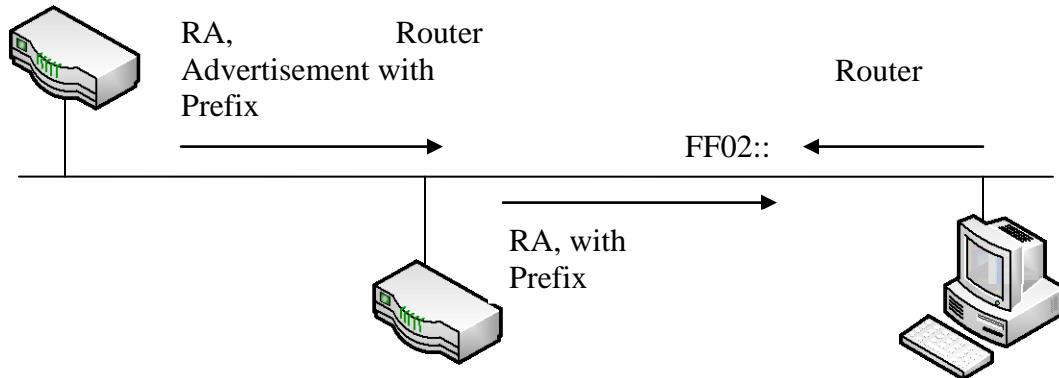


Fig. 1.9: Formation of global site address with Router Solicitation and Advertisement messages

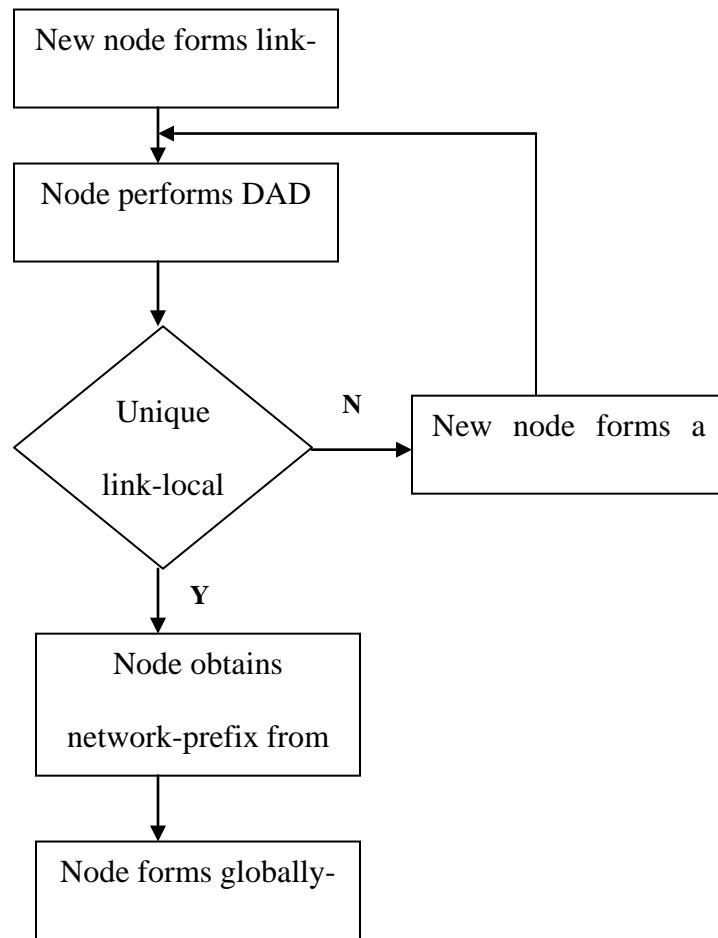


Fig. 1.10 Auto-configuration process - formation of link-local & globally unique address

Many reasons have contributed to the success of stateless auto-configuration in the IPv6 protocol. Besides the fact that it is a means of reducing the operational and deployment cost of the overall network because many nodes can be self-configured, it is also making the network user-friendly for inexperienced users [7][8].

Despite the success of the stateless auto-configuration technique, it has some security implications when used in an IPv6 network. These are duplicate address detection attack Denial of Service attack, Man-in-the-middle attack, Sniffing, bogus-on-link prefix attack and parameter spoofing attack [9-11].

1.8 Motivation and Objectives of the Thesis

The motivation for this thesis is to identify the security vulnerabilities that impact the availability of services using IPv6 protocol suite. In particular, we develop and implement algorithms for preventing denial of service (DoS) that a node booting up in an IPv6 network might experience during the process of stateless address auto-configuration. We achieve this by defining a simulation model to test the scalability and effectiveness of the proposed algorithm. Finally, we collect and analyze the results from the simulations. We outline the objectives of this work as follows:

- i. To identify vulnerabilities that will affect the availability of services using the IPv6 protocol suite,
- ii. To formulate mechanisms / algorithms for preventing loss of services / Denial of Service based on node identification and verification,

- iii. Define a simulation model to test the scalability and effectiveness of the proposed solutions, and
- iv. Analyze results from the simulations.

1.9 Thesis Methodology

The whole thesis is broken down to phases, each of which has to be accomplished in order to achieve the above objectives. These phases are:

- i. To conduct a literature survey on IPv6
- ii. To conduct a literature survey on peer-to-peer node verification protocol
- iii. To conduct a literature survey on attack model for IPv6
- iv. Proposal / formulation of a mechanism for preventing DoS attacks in IPv6
- v. Simulation test-bed setup using appropriate tools such as MATLAB, OPNET etc
- vi. Analysis of simulation results

1.10 Contributions of the Thesis

The thesis contributions are as follows:

- i. Literature survey on the IPv6 protocol including the features, addressing architecture, stateless address auto-configuration and duplicate address detection.
- ii. Security vulnerabilities common to IPv4 and IPv6 protocols
- iii. Security vulnerabilities specific to IPv6 protocol.
- iv. Stateless address auto-configuration attack model in IPv6
- v. Literature survey on Trust and Reputation

- vi. Trust algorithm proposal for solving stateless address auto-configuration attack in IPv6 networks
- vii. MSB / LSB (Information hiding) algorithm proposal for solving stateless address auto-configuration

CHAPTER 2

BACKGROUND, TERMINOLOGY AND LITERATURE SURVEY

2.1 SECURITY ISSUES COMMON TO IPv4 AND IPv6

2.1.1 Sniffing Attacks

This class of threat entails capturing of data being transmitted in a network [42]. Packets being conveyed in plain texts are susceptible and can be examined by an adversary in order to obtain very sensitive information such as login credentials [43]. TCPdump, a tool which comes with UNIX and most UNIX-like operating systems is often used in carrying out this kind of attack. While the use of IPSec may be promising in alleviating sniffing in networks, simplification of key management for IPSec still remains challenge.

2.1.2 Application-layer Attacks

Application layer attack is carried out by exploiting the weaknesses in the application layer and as such it accounts for the bulk of threats existing on the Internet today [44]. Some of the common examples in this attack category are web server attacks, malicious (including viruses, and Trojans), SQL injection attacks, buffer overflows, cross-site scripting, etc. Even with transition to IPv6, there may be a very little change in application layer threats. This is because an attack initiated at this layer can still traverse an encrypted link and still cause damage in the same manner as when the link were in the

clear [45]. Moreover, layer 3 devices such as firewalls and IDS may not guarantee security when they see encrypted traffic.

2.1.3 Rogue Devices

These are devices such as wireless access point; DHCP or DNS server, router or switch introduced into the network and are not authorized [17][46]. If IPSec is used, it could help in reducing the level of attack by a rogue device since every device introduced into the network would need to be authenticated.

2.1.4 Man-in-the-Middle Attacks

The absence of proper authentication mechanism in IPv4 and IPv6 headers gives room for man-in-the middle attacks. By staying in the middle between a customer and a web-based transaction, an adversary can act as proxy, intercept all communications, observe and modify transactions [47].

Single-factor authentication such as the usage of username and password have proved inadequate in avoiding this kind of threat in the Internet and as such multifactor authentication such as the use of hardware tokens, challenge-response, machine fingerprinting and tagging etc are being used to eliminate man-in-the-middle attacks.

2.1.5 Flooding Attacks

In flooding attack, network devices such as routers or nodes (PCs and servers) and network services are bombarded with large amount of illegitimate requests so as to make

the targeted device or service unable to process such large amount of network traffic and therefore becoming unavailable to legitimate users or requests – a situation often termed denial of service (DOS). One of the most prominent examples of network-based DOS attacks is TCP SYN flooding in which an adversary sends a huge amount of special TCP packets to a victim in order to exhaust its processing resources [48][49]. Other forms of DOS employ huge HTTP requests initiated from large number hosts (referred to as bots) to a targeted host or server in the Internet. A number of approaches have been proposed to alleviate the problem of flooding in the Internet. One of these proposals is in [50] in which clients making requests to a server are filtered and authenticated based on their requests, and authenticated clients are issued tickets depending on which services the client can receive. This way, only legitimate requests are accepted to be processed by the targeted host.

2.2 SECURITY VULNERABILITIES SPECIFIC TO IPV6

As we alluded to earlier, IPv6 is not a superset of IPv4. Rather, it is a new suite of protocols within which the support of IPSec for security at the network layer is mandatory. And, in spite of the great number of features which allow it to simplify and enhance IPv4, some of its features and issues related to its deployment have raised some genuine security concerns.

First of all, the fact that the support for IPSec is compulsory in IPv6 but its use is not [12], may create avenues that can predispose an IPv6 network infrastructure to malicious activities of hackers, if the IPSec feature is not used. Second, the current Internet is still largely running on IPv4 and it would probably take some time before there can be a

complete shift to IPv6. During the period of IPv4-IPv6 migration, both networks would coexist, and some of the approaches used during this transition such as Dual-stack backbones, IPv6-over-IPv4, protocol translation etc. [13-15] might probably be exploited by attackers.

Some of the attacks that IPv6 network can experience are:

2.2.1 Reconnaissance

In this form of threat, an attacker first gathers some vital information about the network and then uses the information collected to launch an attack. Ping probes may be employed to determine what range of IP addresses are being used in the victim's network. Having identified the hosts connected to the victim's network via probing, the attacker may proceed to do a port scanning in order to exploit vulnerabilities in the application and / or services running on each host. Because of the huge number of hosts present in an IPv6 network subnet, host probing should present a very difficult task for an attacker [16]. However, the multicast addressing structure in IPv6 networks could make key devices such as DHCP servers, routers, and nodes etc easy targets of an attacker's diabolical activities

2.2.2 Host Initialization

A host trying to generate an IP address for itself using the stateless auto-configuration technique may be barred from forming such address in the presence of an attacker in the network. After creating its link-local address by appending the link-local prefix (FE80::/64) to its interface identifier, the host checks the uniqueness of the address by undergoing the duplicate address detection (DAD) via sending a neighbor solicitation

(NS) message to all the nodes on the local link. The absence of neighbor advertisement (NA) message as a response to the node's NS message guarantees that the link-local address generated by the upcoming node is distinctive and as such the host can use it. However, the presence of an attacker on the node's local link would frustrate the address formation process - The attacker, as shown in Figure 2.1, sends an NA message in response to the NS message coming from the upcoming host which makes the host to form another link-local address and undergo the DAD process again. In the end, the upcoming node may give up and would not initialize its interface [5][17].

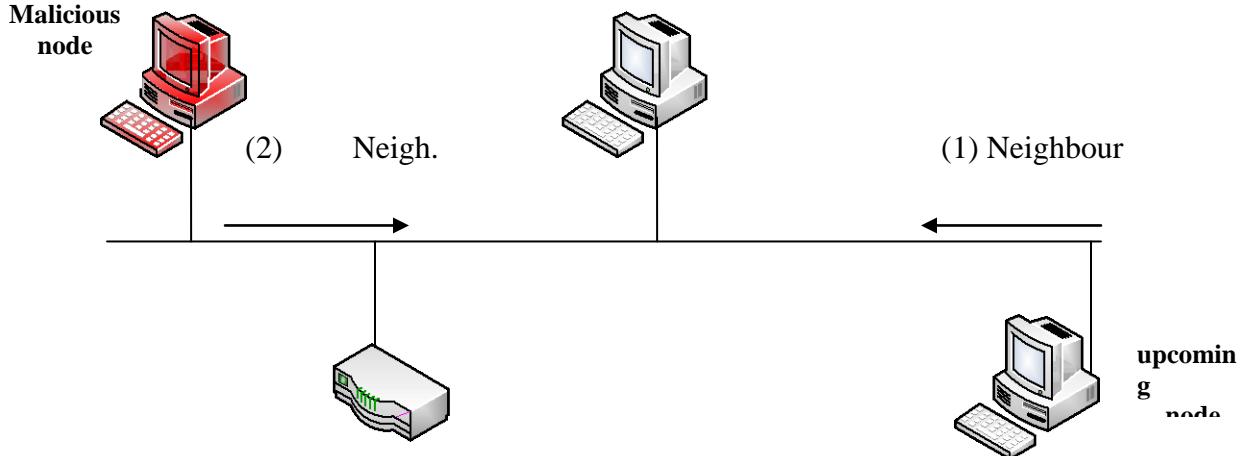


Fig. 2.1: Host Initialization Attack

2.2.3 Routing Headers

Routing headers are a means for an IPv6 node to list the addresses of intermediate nodes that its packets need to pass through when the node is sending message to a destination [18]. Normal hosts in an IPv6 could accept packets from an attacker because if the hosts are listed in the attacker's routing header. These malicious packets could further be

forwarded to other trusted nodes and the process continues. This scenario may eventually cause resources to be used up quickly at the routers, hence leading to a DoS attack.

2.2.4 Multicast-based Attacks

The use of broadcast address in IPv4 has been discontinued in IPv6. Instead, IPv6 uses the multicast-addressing scheme a lot. Messages are sent to a group of nodes, routers, DHCP servers etc using their respective multicast addresses.

In an IPv6 network having a malicious node, messages that are being sent to a multicast address could be intercepted and modified by the malicious node so as to enable it gather information that could enable it to know important systems on the network which could be the target of attacks [5][24].

2.2.5 Transition Issues

The transition to IPv6 from the present IPv4 would be gradual. Some of the approaches being proposed for this migration are Dual-Stack approach whereby nodes incorporate the two protocols and use the appropriate one for communication, for example, most PCs' operating systems today have both IPv4 and IPv6 protocol stacks; Translation approach, by which a protocol can be converted to another protocol; and Tunneling approach, by which IPv6 protocol is overlaid over a legacy IPv4. The IPv6 datagram is typically encapsulated inside the payload of the IPv4 datagram, whereby the IPv4 source and destination addresses of the IPv4 datagram are the addresses of the encapsulation and de-capsulation node [7].

These migration approaches, however, are prone to security challenges. For example, in dual-stack technique, there is a need for parallel infrastructure with the added security problems of both protocols. Managing two separate protocols may provide an opportunity for attack [37].

2.2.6 Other Security Issues

There are other security challenges in IPv6 network such as Application layer attacks, which are a broad category of threats at layer 7 of TCP/IP protocol stack. Unfortunately, IPSec as mandatory as it is in IPv6 would do nothing to protect against this kind of attack since IPSec is a security protocol at layer 3. Other security concerns are lack of overall understanding of IPv6 by security staff which may allow attackers to exploit IPv6 assets. Moreover, since IPv6 systems are not yet widely deployed in production environments, the possibility exists that the number of vulnerabilities in implementing IPv6 protocol can still increase as IPv6 networks are being massively deployed in the near future.

2.3 CONCEPT OF TRUST AND REPUTATION IN PEER-TO-PEER NETWORKS

2.3.1 Peer-to-Peer Network

Peer-to-peer network is a type of network architecture in which a peer can act as a server and a client, as the peer can provide service as well as request for service from other peers. In addition, there is no central authority or infrastructure that could coordinate the behaviour of peers. Further, each peer makes autonomous decisions based on information received from its neighbours, and peer can join or leave the network as it

pleases. Because of this dynamic and autonomous nature of P2P model, it is a great success in the Internet community, as Internet applications such as instant messaging, distributed processing and file sharing are built on top of peer-to-peer communication model.

Stateless address auto-configuration technique of forming addresses in IPv6 networks also supports this communication paradigm, since new nodes intending to initialize their interfaces do not need to contact a server for address information. A new peer forms a temporary address (i.e., link-local address) and goes through the duplicate address detection process to ascertain the usability of this address. The platform of our work is therefore peer-to-peer.

Despite all these great features of the peer-to-peer communication model, there are a number of security concerns that threaten its success. First, since no peer has the power or duty of monitoring and restraining other peers' behavior and second, each peer is anonymous, all of which means that interactions in a P2P takes place between stranger peers, some peers may decide to render malicious services such as sending unreal or fake information, and colluding with other peers to provide bad service.

A malicious node or set of malicious nodes in an IPv6 networks may also frustrate the stateless address auto-configuration process if they always respond with a network advertisement message to a network solicitation message of an upcoming node. The new may give up initializing its interface after a few other attempts at forming new link-local addresses and going the duplicate address detection.

One technique that we propose to deal with stateless auto-configuration threat in IPv6 network is Trust and Reputation.

2.3.2 Trust

Jiang and Ye [40] define Trust for peer X to peer Y as an evaluation based on X's history of interactions with Y, either directly with personal experience i.e. direct feedback, or as reported recommendations from other peers i.e. indirect feedbacks. Josang et al [41] defines trust as a firm belief than an entity has about another entity from past experiences, knowledge about the entity's nature and / or recommendations from trusted entities. This belief is typically an expectation about the entity's behavior.

Some of the features of trust are – transitivity, composability, personalization, asymmetry, dynamism, context sensitivity [40].

Transitivity – When a peer A trusts in peer B, A should also trust B to make recommendations about other peers C, D and so on.

Composability – a peer A receiving a number of recommendations about peer B from other peers should be able to combine all of the trust values in the received recommendations into a single belief (trust value) about B's trustworthiness. For instance, if peer A receives recommendations about peer B from other peers 1, 2, 3 ... k, then the combined trust value of B in A is:

$$Trust\ degree_{AB} = \frac{1}{k} \sum_i^k Trust\ degree_{iB}$$

And if each of peers i has different weights in A, then the trust value can be:

$Trust\ degree_{AB} = \frac{1}{k} \sum_i^k w_i \cdot Trust\ degree_{iB}$, where $w_i \geq 0$ ($\sum w_i = 1$) is the weight that peer A attaches to each of the recommendation trust values from peer i .

Asymmetry – The fact that peer A trusts another peer B does not mean peer B would trust peer A with the same trust value in both directions.

Context Sensitive – Trust is a function of a specific context. Peer A may trust peer B on very good file quality but may not trust recommendations from B about another peer C.

2.4 SURVEY ON TRUST-BASED SCHEMES

Grifith [25] presents a technique called M_{DT-R} that allows peers to delegate and manage the risks of cooperating in a P2P network by using trust and recommendation of other peers. The agents (peers) perceive the trustworthiness of fellow peers using the dimensions of Success, Cost, Timeliness and Quality. The trust value is computed as a value in the interval $[0, 1]$ and is regularly updated using an $Update_{success}$ or $Update_{fail}$ function.

In [26], Chu et al presented a reputation model which allows a peer to determine the reputation value of another peer, a scheme that enables the first peer in distinguishing peers providing good QoS from those providing poor QoS. In determining the reputation value, the first peer uses the recommendations from its neighbour peers to hasten up the calculation for another peer, and also uses a trust mechanism to overcome the problem of malicious recommendation.

The work done in [31] highlights a distributed node authentication scheme in wireless sensor networks which relies on public information and the majority rules. In this scheme, which does not require certified servers, every sensor node stores its neighbor's identity and location information, such that a node A trying to determine the authenticity

of node B would only have to obtain this information from B's neighbours. They were able to achieve a satisfying detection rates while keeping the false positive rates low despite the location inaccuracies in their localization algorithms.

Ren et al [32] presents an improved trust model based on Bayesian trust model. Their technique uses a logarithm approach to compute and update the trust for peers and a number of services, while preventing malicious peers from attacking legitimate peers. Their technique also prevents malicious peers from increasing their trust.

Wu et al. [33] presented a trust model based on reputation in which they incorporated both trust and distrust using a polling algorithm. Their proposal, which is a modified form of SupP2Prep [34], a protocol for management via polling in P2P networks, uses two amendments on the SupP2Prep protocol. The first amendment is that peers in a P2P network are apportioned to different groups based on their interests and only members in the same group are permitted to vote. And second, distrust is taken into account – the model considers voting of peers from the perspective of both trust and distrust. In evaluating the trustworthiness of peers and to effectively deal with malicious behavior in P2P network, their model identified seven factors which are satisfaction or dissatisfaction degree in interactions, number of interactions, size of interactions, time, vote accuracy, punishment function, and risk.

In [35] Chen et al proposed a reputation system to verify the trustworthiness of users and shared files. Their work highlights several trust models such as Trust Model on Direct

Feedback, which determines the direct trust of peer X to peer Y using total transaction numbers between X and Y and good feedback numbers that X receives from Y at i^{th} transaction; Trust Metric with Aging Factor, which uses a decay function that assigns more weights to recent transaction and less weight to past transactions; and locally final trust model by combining the reputation and direct feedback.

“NeighborTrust” is proposed by Gupta et al in [36]. As opposed to many schemes which attempt to calculate global trust and reputation value for each peer by keeping these values in a global trust matrix from which the values are communicated to all participating peers, NeighborTrust maintains trust for only neighbor peers thereby reducing communication and computational overhead for each peer. In this protocol, the trust rating of a peer is linked with its privilege of establishing with establishing with existing peer and the rate at which the peer inject traffic into the network. This idea gives an incentive to peers to maintain good behavior, hence, limiting the rate at which DDoS is experienced inside the network. The trust ratings for peers are also encrypted and transmitted using a middleware which prevents malicious nodes to manipulate their trust ratings.

Jiang and Ye [37] also proposed a reputation-based scheme which has both direct and indirect feedback to prevent peers from distributing malicious contents into the network. In coming up with their scheme, they identified some of the common pitfalls made by researchers of reputation-based systems such as using direct feedback only without using recommendation from other peers, not differentiating the transaction period in computing

the trust value, and not including other factors such as number of transactions and credibility of direct feedback.

CHAPTER 3

A TRUST-BASED MECHANISM FOR PROTECTING IPV6 NETWORKS AGAINST STATELESS ADDRESS AUTO- CONFIGURATION ATTACKS

3.1 PROPOSED TRUST SCHEME

In this chapter, we present our trust-based technique for countering the effect of a node auto-configuration attack. The proposed technique is based on distributed definition and confirmation of address uniqueness, and does not affect the flexibility provided by the address auto-configuration property of the IPv6 protocol.

In our scheme, a new node joining an IPv6 network forms its link-local address from the concatenation of its interface identifier and link-prefix and attempts to confirm the usability of the link-local address by sending a multicast neighbour solicitation (NS) message (the NS message contains the link-local address) to all the nodes on the local link. If there is no neighbour advertisement (NA) response to the new node's NS message, this implies that its link-local address is unique and it can proceed to form a global address using its link-local address.

However, if there is neighbour advertisement response from a node inside the network, the new node first extracts the IP address of the responding node from the neighbour advertisement message and then proceeds to verify the claim of the responding node by

finding out its trust value from its neighbours. This new node does this by sending a second neighbour solicitation message containing the IP address of the claiming node (responding node) to all the neighbours of the responding node, requesting for its trust value in the network. The new node establishes the trustworthiness of the claiming node by extracting the claiming node's trust value from each of the neighbour advertisement responses and computing the aggregate trust value, which compares to a certain trust threshold.

For our trust scheme, each node i in the network is assumed to have a list of k neighbours, where the value k and the exact neighbour list is randomly selected and defined at network initialization time. The neighbour list for a given node i consists of all nodes which can confirm the existence of a link-local address in the network, if an advertised LLA request by an upcoming node (say w) is considered in use, based on an incorrect response received from a malicious node operating network.

The following is a list of parameters used by the proposed scheme:

- i. k_i is the number of trusted neighbours of an existing IPv6 node i , where i is the node ID.
- ii. Θ is the threshold on the minimum number of neighbour responses needed for node address verification.
- iii. $T_{i \rightarrow j}^e$ is the trust value between a node pair $\{i, j\}$ during a given time epoch e.
- iv. N is the total number of nodes in the network.
- v. y is the number of legitimate nodes in the network.
- vi. $N - y$ is the expected number of rogue nodes.

- vii. α is the trust factor
- viii. τ is the optimal time window length

The trust factor α is derived from the number of responses (network advertisement messages) received from k neighbours of a given node i , when a network solicitation message is sent. The value of α is dependent on the window of time (which in turn is a function of the network size, number of hops and approximate round-trip delay), where $\alpha \in \{0, 1\}$.

Based on the dependencies defined, the decision factor, given by $G_{i \rightarrow j}$, enables a requesting node to determine whether to trust a response (NA) coming from a node j , or not, and is provided by Equation 3.1.

$$G_{i \rightarrow j} = \alpha \cdot T_{i \rightarrow j}^e + \frac{\alpha}{(N - y) \cdot \tau} \quad (3.1)$$

If $G_{i \rightarrow j} > \theta$, node i trusts j , else it does not trust node j and starts afresh forming a new link-local address and sends another network solicitation message.

In order to find the optimal window of time within which the k trustable responses (NA) need to be received by the sender i , the differential of equation is equated to zero. Equation 3.2 best provides the maximized value of τ , to attain the maximum trust within a window of time of length $T_{i \rightarrow j}^e$.

$$\tau = \frac{1}{\sqrt{y \cdot (N - y) \cdot T_{i \rightarrow j}^e}} \quad (3.2)$$

As shown in Figure 3.1, the time window (τ) within which an upcoming node i can expect a valid and verified response to its network advertisement (NA) message decreases with increasing number of good nodes y in the network.

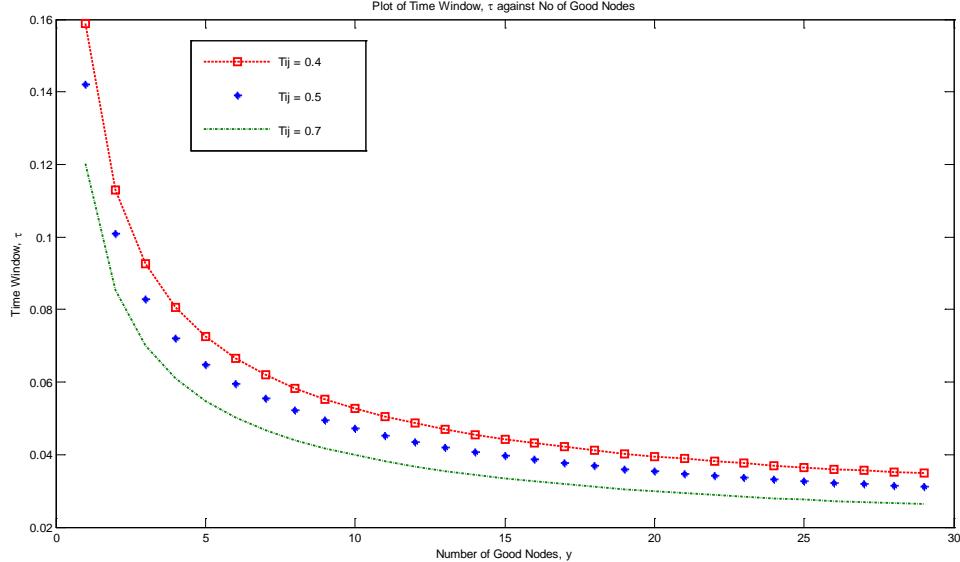


Fig. 3.1 The effect of increasing number of good nodes y on the value of τ

In algorithm 3.1, we illustrate the steps of execution of the trust-based address verification scheme. The steps of the algorithm are executed based on a response received to a new node address uniqueness request in the network.

Basically, a new attempting to join a network forms its link-local address via stateless address auto-configuration and tries to verify its address uniqueness by multicasting a NewNodeLLARequest (corresponding to neighbour solicitation message) to all nodes on the local link. If there is no response, the new node goes ahead to use its address. If there is a response, the new node sends another NewNodeLLARequest message to all the k neighbours of the responding node. The new node uses τ as the time window

within which it expects a response to the NewNodeLLARequest message. From the response to the second NewNodeLLARequest message, the new node extracts the trust information of the claiming node from its k neighbours, computes the aggregate trust value and then compares it with a certain threshold. With this, the new node can ascertain if claim of the responding is genuine or not.

1. Determine the optimal value of τ
2. **foreach** NewNodeLLARequest **do**

Address multicast: $n \rightarrow N$

foreach $Neighbour_k^n$ **do**

Determine $Trust_k^n$

end

foreach $Neighbour_k^n$ **do**

If $G_{i \rightarrow j} > \theta$, **then**

$T_{i \rightarrow j}^e = 1$

end

else

$T_{i \rightarrow j}^e = 0$

end

end

end

Algorithm 3.1: Proposed Trust Algorithm

3.2 SIMULATION AND ANALYSIS

The simulator for testing the effectiveness of our proposed trust-based attack detection mechanism was written in MATLAB. The parameters defined for the

scheme above were varied and their corresponding effects on the outcome of the simulations were analyzed.

Figures 3.2 – 3.7 provide an insight of the effect of increasing number of trusted neighbours in the network, on the trust factor $G_{i \rightarrow j}$, for varying numbers of trusted nodes in the network, i.e. values of y . Each graph represents a network of a different value of N , namely, 20, 50, 100, 200, 500 and 800. A new node in an IPv6 network goes ahead with using its LLA if there is no neighbour advertisement response to its neighbour advertisement request containing the temporary address.

However, if there is a response, the node depends on the trust value $G_{i \rightarrow j}$ generated by any node i in the network, willing to perform address verification on behalf of the new node. With increasing numbers of legitimate nodes in the network, there is a lesser chance for a malicious node to influence the trust value in the network advertisement message exchanged in the network and thus the requesting node could reliably accept the trust value issued by the resolving node i .

As observed from the graphs, the effect of increasing network size on the scheme is negligible, thus attesting to the scalability of the proposed scheme.

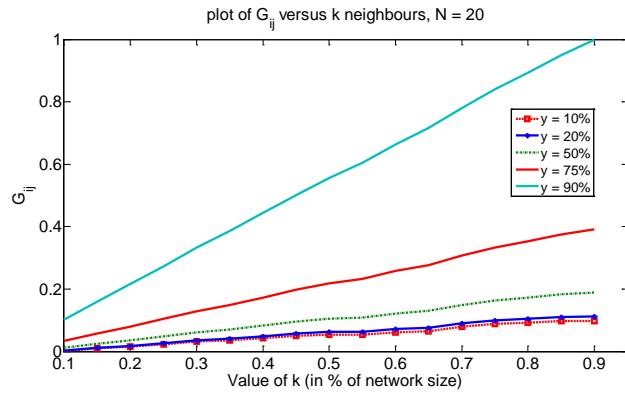


Fig. 3.2 G_{ij} values against varying k for a diverse range of good nodes (y), $N = 20$

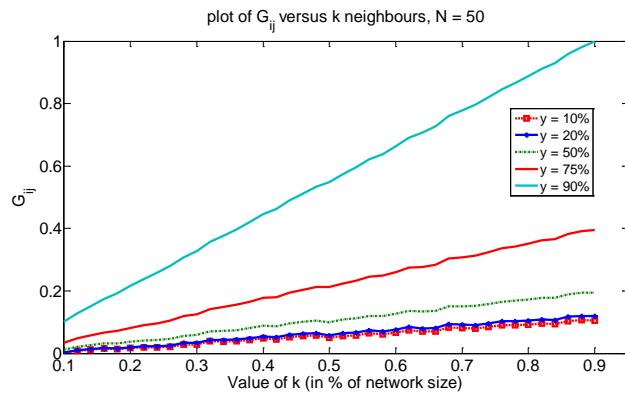


Fig. 3.3 G_{ij} values against varying k for a diverse range of good nodes (y), $N = 50$

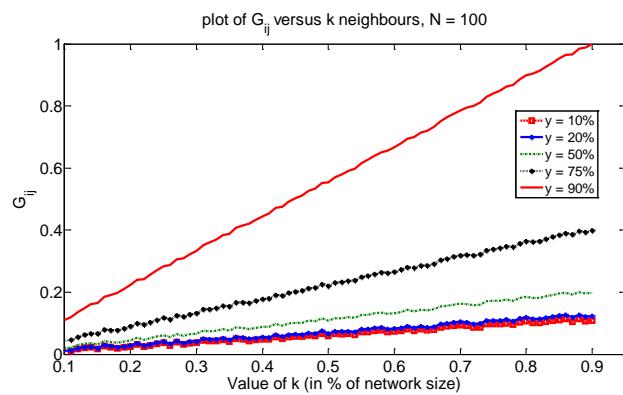


Fig. 3.4 G_{ij} values against varying k for a diverse range of good nodes (y), $N = 100$

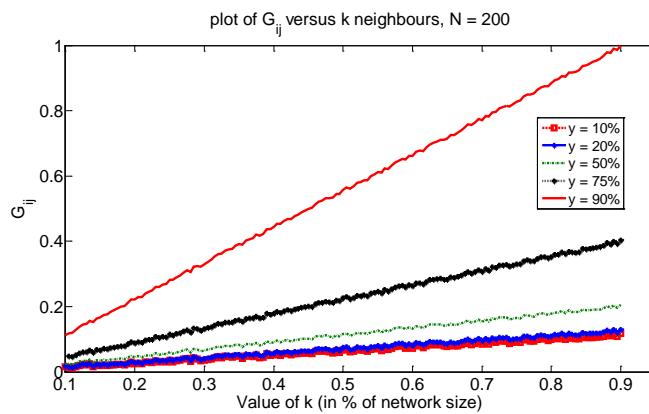


Fig. 3.5 G_{ij} values against varying k for a diverse range of good nodes (y), $N = 200$

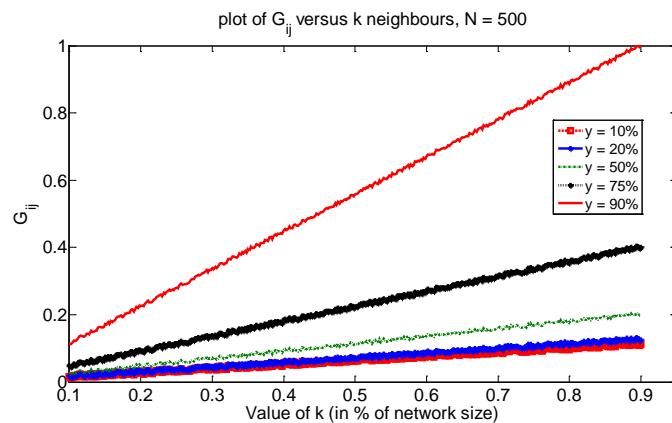


Fig. 3.6 G_{ij} values against varying k for a diverse range of good nodes (y), $N = 500$

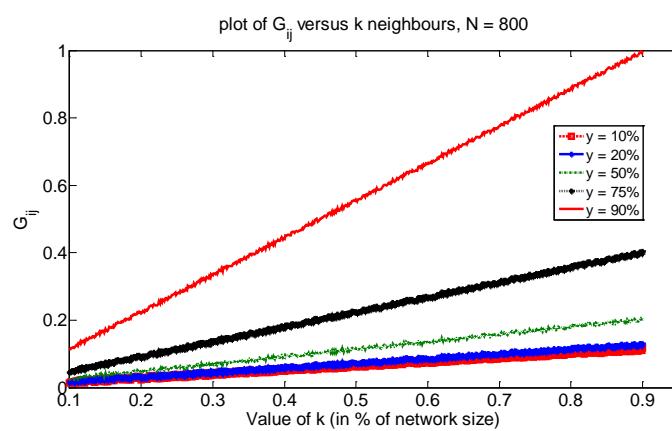


Fig. 3.7 G_{ij} values against varying k for a diverse range of good nodes (y), $N = 800$

In Figure 3.8, we illustrate the delay experienced by the network advertisement messages, based on the network size. The general trend in the plots is that as the number of nodes in the network increases, so does the delay. This occurs because of the increasing number of messages exchanged in the network, with increasing number of nodes, for a fixed value of $k = 10\%.N$. Similarly, the size of the network has a direct relationship with the number of hops and as such delays are higher in 500-node and 800-node networks when compared with smaller networks. However, as the trust values in the messages exchanged in the network increase (i.e. caused by the higher proportion of good nodes), the delay experienced by the messages is less. Therefore, increasing value of α , has a corresponding effect on the incurred delay.

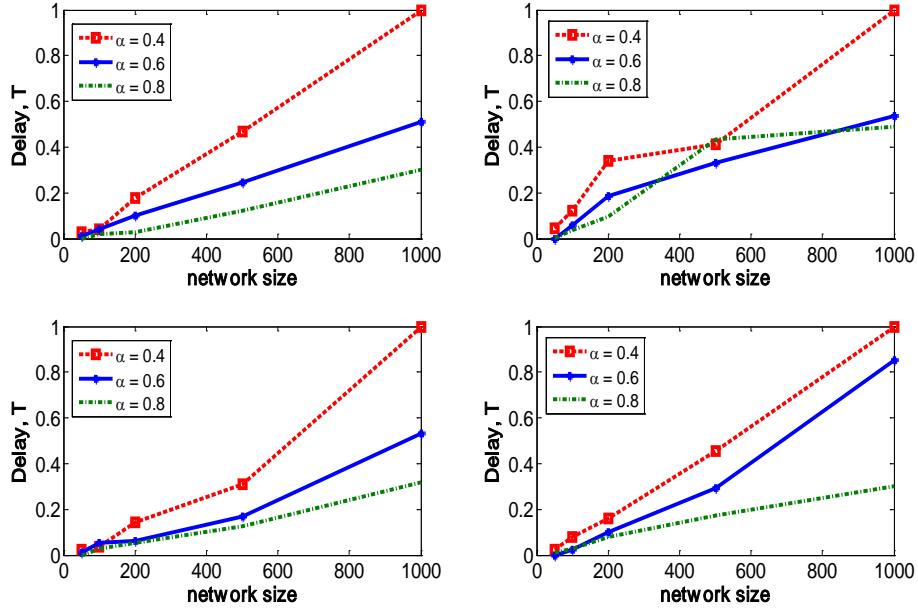


Fig. 3.8 The effect of increasing network size on the delay incurred by the address verification scheme, for varying values of α

This occurs because with higher number of legitimate nodes in the network, the neighbour list consisting of k neighbours for each node i , will include nodes in close proximity to i . As a result, the performance of the scheme is seen to improve with increasing values of α . It may be noted that the values of α is directly proportional to the number of legitimate nodes y in the network.

3.3 CONCLUSION

We present in this chapter a trust-based approach that enables a new node with stateless auto-configured address attempting to join a network to detect a malicious claim by a rogue node which tries to claim ownership of the new node's address. The new node achieves this by getting the trust information of the rogue node from its neighbours and then computes the aggregate trust information of the rogue node.

The scheme assumes that every k neighbour a node i in the network is trustworthy and as a result, the new node can assume that the trust information it is getting from the neighbour advertisement message for a node is true. However, in the presence of several colluding nodes i.e. when the some or all of the k neighbours of a node are malicious, the scheme could fail, since malicious node would never be detected by the new node is trying to verify the claim of the malicious node.

3.4 ACCOMPLISHMENT

This chapter of the thesis was published in the proceedings of the 17th IEEE International Conference of Networks that held during 14th – 16th December, 2011 in Singapore.

CHAPTER 4

MSB / LSB SCHEME

IPv6 protocol introduces a new auto-configuration technique by which nodes could initiate their interfaces in a network without the need of a static configuration by an administrator or by using a DHCP server. The node forms an address combining information from routers inside a network and that from its physical address. In the process of ascertaining the usability of this address, malicious nodes inside the network could subvert this auto-configuration mechanism if they continue to respond with a network advertisement message portraying that the address formed by the new node is in use.

In this chapter, we design and implement an MSB / LSB scheme which uses the last 24 bits of a new node LLA, to ease the process of node address verification and to contain any malicious node that may attempt to frustrate the auto-configuration technique.

4.1 TERMINOLOGY

- ♦ **Unspecified Address:** a reserved address value that indicates the lack of an address (i.e. the address is unknown). It is never used as a destination address, but may be used as a source address if the sender does not (yet) know its own address (for instance, when verifying an address is unused during stateless address auto-configuration).

The unspecified address has a value of 0:0:0:0:0:0 or ::

- ◆ **Link-local Address:** a unicast address having link-only scope that can be used to reach neighbours. All interfaces on routers must have link-local address. Interfaces on hosts are also required to have link-local address.
- ◆ **Address Auto-configuration and Address Resolution:** Address auto-configuration introduces the mechanisms needed in order to allow nodes to configure an address for an interface in a stateless manner while Address Resolution is used by a node to determine the link-layer address of an on-link destination (e.g. neighbour) given only the destination's IP address.
- ◆ **Duplicate Address Detection (DAD):** Duplicate address detection is a mechanism which allows a node to determine whether or not an address it wishes to use is already in use by another node.

4.2 EUI-64 AND THE NEIGHBOUR DISCOVERY PROTOCOL

When sending a packet from a node A to another node B and given that the host part of an address embeds the MAC address, a node A might just extract the MAC address from the IPv6 address of the destination B and then use the MAC address as the destination layer 2 frame address. This would avoid the need for the neighbour solicitation and advertisement process, the duplicate address detection and it would be faster. However, for the reasons below, a source node may not want to do this:

- The fact that a node has an address that looks like an EUI-64 does not necessarily mean that the MAC address is there.
- Some link-layers do not have unique MAC address addresses.
- There is not necessarily a one-to-one relationship between the MAC and the IPv6 address.
- Nodes are also using manually assigned addresses or temporary addresses, which have no EUI-64 part. These addresses must use neighbour discovery
- It is safer to implement this mechanism for all addresses to avoid duplicate addresses on the same link
- The cost of initial neighbour solicitation / advertisement exchange is low compared to the safety guard it provides.
- If multiple addresses on the same interface use the EUI-64 from the same MAC addresses, implementation can choose to make the neighbour solicitation only on the first one and skip for others, increasing the efficiency of the neighbour solicitation and advertisement process.

4.3 STATELESS ADDRESS AUTO-CONFIGURATION ATTACK DETECTION:

MSB / LSB TECHNIQUE

This scheme uses only the last 24 bits corresponding to the last 6 hex letters of a link-local address for verification. In this scheme, the new node does not send its newly formed link-local address inside the payload of a network solicitation message during the duplicate address detection stage. Rather, it only sends a part of its link-local address string and tries to find out which of its neighbour peer nodes shares this string in their

link-local address. The ending 24 bit string of the new node's address is however divided into two parts – the most significant bit (MSB) and the least significant bit (LSB). The new node inserts the LSB into the payload of the neighbour solicitation message and multicasts the NS message to all the nodes on the link, during the duplicate address detection stage, asking any of these nodes whose last part of its LLA address tallies with the LSB to send their full IP address when responding with their neighbour advertisement messages.

The main idea behind this scheme is that a receiving peer of the NS message should not have access to the link-local address of the new node. With this, a responding neighbour peer, if malicious, would not be able to act as if it is the owner of the LLA. So, a neighbour peer whose link-local address shares the LSB string with the new node, would respond including its link-local address and MAC address inside its neighbour advertisement message.

The format of the neighbour solicitation message sent by the new node therefore is illustrated in Figure 4.1:

Neighbour Solicitation message

Source MAC	Source IP	Destination MAC	Destination IP	Payload
-	:: (unspecified address)	-	All-nodes multicast address	LSB of the last 24 bits of its LLA

Fig. 4.1 Format of MSB / LSB Neighbour Solicitation message

In the NS message, both the Source MAC and the destination MAC fields are empty.

The destination MAC field is empty since the message is being sent to all the existing nodes in the network, so no specific IPv6 node is targeted – the target is all the nodes on the local link. The Source MAC field is empty because the new node does not want any existing node to guess its IP since the link-local address is typically derived from the MAC address. Source IP address field is unspecified (::) as the new node has not validated its newly formed address.

The format of neighbour advertisement is as shown in Figure 4.2:

Neighbour Advertisement message

Source MAC	Source IP	Destination MAC	Destination IP	Payload
Link layer address of responding node	Link-local address of responding node	-	All-node multicast address (ff02::1)	Its LLA

Fig. 4.2 Format of MSB / LSB Neighbour Advertisement message

In the NA message, the destination MAC field is empty of the NA message is also being sent to all the nodes on the local link.

Upon receipt of an NA or a number of NAs to its NS message, the new node checks the source IP fields of the NAs to see if any of them matches with its own. If there is no match, the new node goes ahead to use its address. Otherwise, it sends another NS message with different payload information.

The number of bits inside the LSB string, m , is varied by the new node from 1 bit to 13 (just a bit more than half of the total string) while the MSB takes the remaining part. During duplicate address detection stage, the new node inserts the LSB into the payload field of the NS message and multicasts it to the all-node multicast address which would be received by all nodes on the local link. All nodes whose last part of their LLAs matches with the LSB respond with NAs including their LLAs.

The new node constructs a list of the respondent nodes alongside their IPv6 addresses (LLAs) and tries to see if its IP address is in the list. If not, the new node considers its address unique and goes on using its address. If the new node's address is found in this list however, the new node forms another address by first randomly picking any MSB string from the possible 2^{24-m} MSB string combinations (m is the number of bits in the LSB) and then concatenating the chosen MSB string with the used LSB. This combination guarantees that a different link-local address is formed. The new node goes through the duplicate address detection again with the new address. For our work, we considered cases where m , the number of bits in the LSB string is varied from 1 to 13. However, if there is a match between the LLA of the new node and that of a responding node, the new node proceeds to generate another address choosing any one of the remaining 2^{24-m} potential addresses (m is number of bits in the LSB), concatenating it with its LSB. This new combination would be the last 24 bits of its LLA, and should be unique. So the new node goes through the Duplicate Address Detection process again.

4.4 THE PROPOSED MSB / LSB ALGORITHM

Input: {new node's LLA, a set of random IPv6 neighbour peers, LSBs of the last 24 bits of peers' LLAs}

Output: {list of LLAs of responding nodes, new node's decision to use address}

1. New node forms an LLA
2. The new node extracts the last 24 bits of its LLA and divides it into MSB and LSB
3. The new node constructs an NS and multicasts it to all the nodes on the link, encapsulating the LSB inside the payload of the NS
4. All existing nodes with a match with the LSB of the new node will respond with an NA message including their LLAs within their respective NA payloads.
5. New node searches from list of respondent addresses to check for a match with its LLA.
6. If no match

Address is considered unique and new node joins the network with this LLA

END

7. Else

- a. Selects a new LSB from the pool of remainder addresses (i.e., from the remaining $2^{24} - m$ addresses), where m = Number of intended LSB bits, defined at network initialization time.
- b. Constructs a new LLA based on the new LSB.
- c. Go to Step 3.

8. end

Algorithm 4.1 Proposed MSB / LSB Scheme

4.5 EXPERIMENTAL SETUP

We illustrate the MSB / LSB scheme with a simple IPv6 network of random peer nodes in which a new node with a link-local address of fe80::0212:6bff:fe3a:9e9a attempts to join the network. The last 6 hex letters of the new node '3a9e9a' corresponding to '00111010100111010011010' divided into binary strings of MSB and LSB. The number of bits inside the LSB sting is varied by the new node from 1 bit to 13 (just a bit

more than half of the total string) while the MSB takes the remaining part. During duplicate address detection stage, the new node inserts the LSB into the payload field of the NS message and multicasts it to the all-node multicast address which would be received by all nodes on the local link. All nodes whose last part of their LLAs matches with the LSB respond with NAs including their LLAs.

The new node constructs a list of the respondent peers alongside their IPv6 addresses (LLAs) and tries to see if its IP address is in the list. If not, the new node considers its address unique and goes on using its address. If the new node's address is found in this list however, the new node forms another address by first randomly picking any MSB string from the possible 2^{24-m} MSB string combinations (m is the number of bits in the LSB) and then concatenating the chosen MSB string with the used LSB. This combination guarantees that a different link-local address is formed. The new node goes through the duplicate address detection again with the new address.

For our work, we considered cases where m , the number of bits in the LSB string is varied from 1 to 13, and equally perform a simulation with random set of IPv6 neighbour peers on the local link with the new nodes.

4.6 PERFORMANCE ANALYSIS

To test the performance of the proposed scheme for detection of duplicate addresses, and to verify the correctness of all NA responses received by a new node, the scheme needs to be analyzed in the context of varying network and application parameters. Following is a list of parameters that will affect the performance of the scheme:

y = number of legitimate nodes

N = total network size

$K = N - y$ = number of rogue nodes

L = number of LSB bits used

α = number of responses

τ = time window (duration) between neighbour solicitation and neighbour advertisement

The number of legitimate nodes in the network, y , is a system parameter that is varied for analysis of the scheme under the presence of diverse adversarial classes. For instance, a network which has witnessed a large number of recent malicious attacks, in particular, duplicate address attacks, will have a lower value of y , as opposed to networks with infrequent attack instances. The size of the network is defined as the total number of nodes operational in the network at any point in time. The analysis of the scheme may generate outcomes that are directly affected by the size of the network. We do not consider the topological aspects of the network, but rather assume that the IPv6 network is constituted of nodes that are reachable by any new node intending to join the network.

K is defined as the number of rogue nodes in the network. This value is simply a difference between the total number of nodes in the network and the number of legitimate nodes.

L is the number of LSB bits employed by the new node in the payload of the NS message. This has an impact on the number of NA responses α , from the existing nodes inside the network

The total number of responses received i.e., total number of NAs, to an NS of a new node is represented through α .

This TTD is the delay that the system can tolerate for the convergence of the entire detection scheme. If the delay exceeds W then the advantage of detecting is overshadowed by the overhead that the scheme will incur. If the delay is less than W then the scheme is efficient enough to perform the detection so as to be of any value to the purpose i.e. attack detection.

The total tolerable delay for the MSB / LSB scheme is given as:

$$W = (N-y).L / \tau + \tau \alpha N \quad (4.1)$$

If the total number of rogue nodes (hypothetically) is large, then the delay will be high, as it is anticipated that in the duplicate address attack, most if not all rogue nodes will respond to the NS with an NA. On the contrary, if K is small, then the effective delay will be low. Second, for large values of L the expected number of responses will be low, since fewer numbers of nodes will be having an overlapping address with that of the new node in this case. If the value of L is small, then more number of nodes will be having overlapping bit sequences in their respective addresses with the new nodes' address. In such a scenario, the total number of responses to the NS will be high. Therefore, the overall delay will be high. The length of the time window (τ) is inversely proportional to the number of rogue nodes in the network as well as to the length of the LSB. Increasing

number of responses to the NS will incur higher delays as opposed to receiving fewer responses. Therefore, increasing value of α will have a non-decreasing effect on the overall delay of the scheme. Larger the network more will be the expected number of NA responses to a given NS. The length of the time window is directly proportional to the values of both N and α .

When Equation (4.1) is differentiated with respect to τ , Equation (4.2) best describes an expression for the minimum time window within which a neighbour advertisement response is expected to a neighbour solicitation is sent:

$$\tau = \sqrt{\frac{N \alpha}{K L}} \quad (4.2)$$

4.7 ANALYSIS OF RESULTS

Results in Figure 4.3 depict a network configuration of 100 nodes with several compositions of malicious nodes. In this scenario, percentages of malicious nodes to total network size were varied from 10% to 25%.

A new node joining the network with a neighbour solicitation message multicast on the local link experiences some time delays of the order of τ (in microsecond) before it receives neighbour advertisement messages from the nodes claiming the ownership of the new node's link-local address. With a number of malicious nodes inside the network, the amount of neighbour advertisement messages received by the new nodes are measured as a percentage of the total network size.

The impact of the increasing proportion of malicious nodes is felt on the time window length. If the whole network is constituted of 10% malicious nodes as in Figure 4.3, the time window length experienced by a new node between its neighbour solicitation and

neighbour advertisement response(s) is about $3 \mu\text{s}$. The new node collects all the neighbour advertisement message responses and compares its address with those of claiming nodes. If the network contains 25% malicious nodes, the time window experienced by the new node is $8 \mu\text{s}$.

Figure 4.4 shows a 200-node network. Since it is a larger network than that of figure 4.3 and consequently with more number of malicious nodes, a new node joining this network experiences a delay of $8.5 \mu\text{s}$ when there are only 10% of the neighbour advertisement responses are coming from the malicious nodes. With more percentages of the total network size being constituted by malicious nodes and hence greater responses coming from malicious nodes, the delays increase. In addition, it took a longer time for the network to converge.

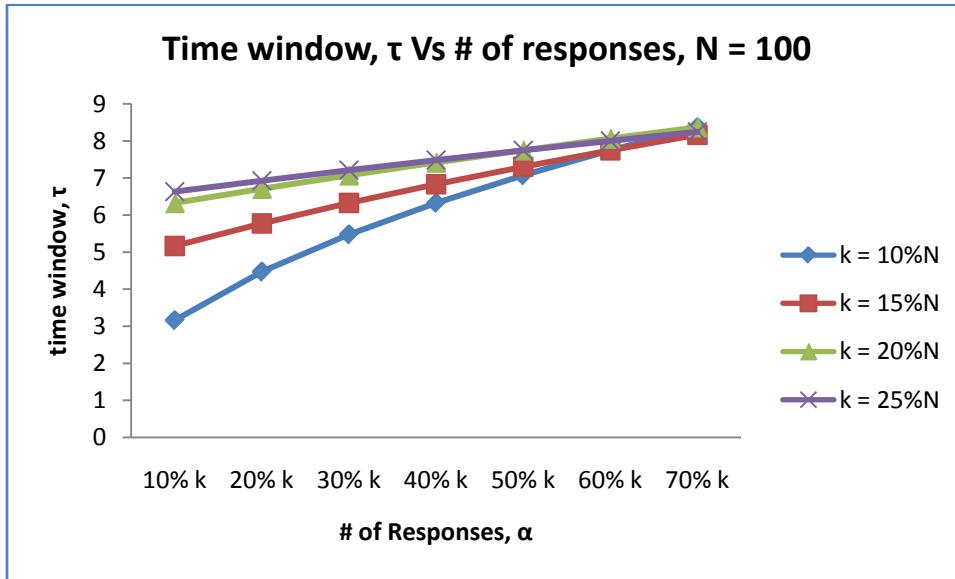


Figure 4.3 Plot of time window vs number of neighbour advertisement messages, $N = 100$

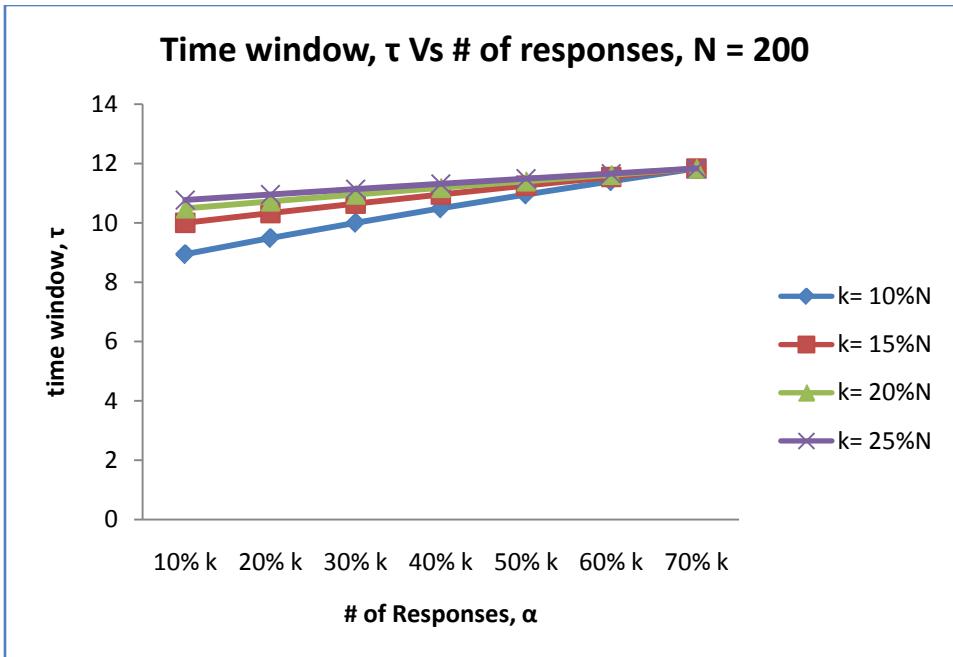


Fig. 4.4 Plot of time window vs number of neighbour advertisement messages, $N = 200$

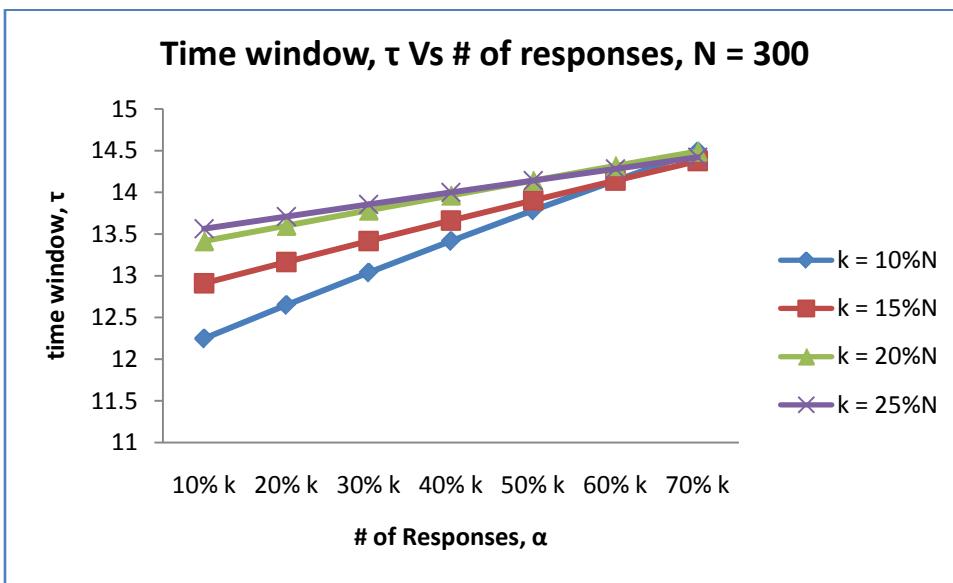


Fig. 4.5 Plot of time window vs number of neighbour advertisement messages, $N = 300$

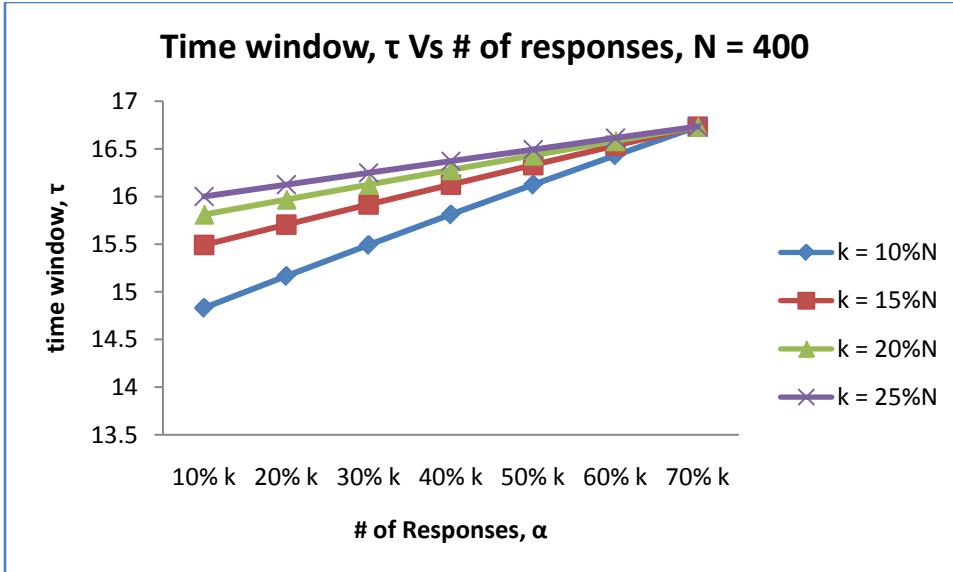


Fig. 4.6 Plot of time window vs number of neighbour advertisement messages, $N = 400$

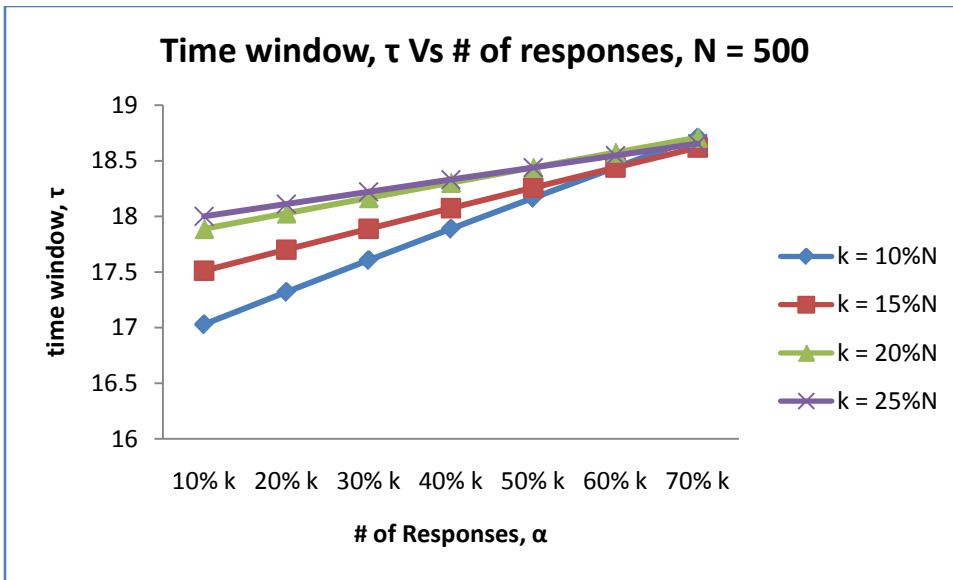


Fig. 4.7 Plot of time window vs number of neighbour advertisement messages, $N = 500$

Similar pattern is observed for network sizes of 300-, 400- up till 800-node network.

With more number of nodes in the network, the new node has a corresponding number of

neighbour advertisement messages to process from both legitimate nodes and malicious nodes after sending its neighbour solicitation request on the local link.

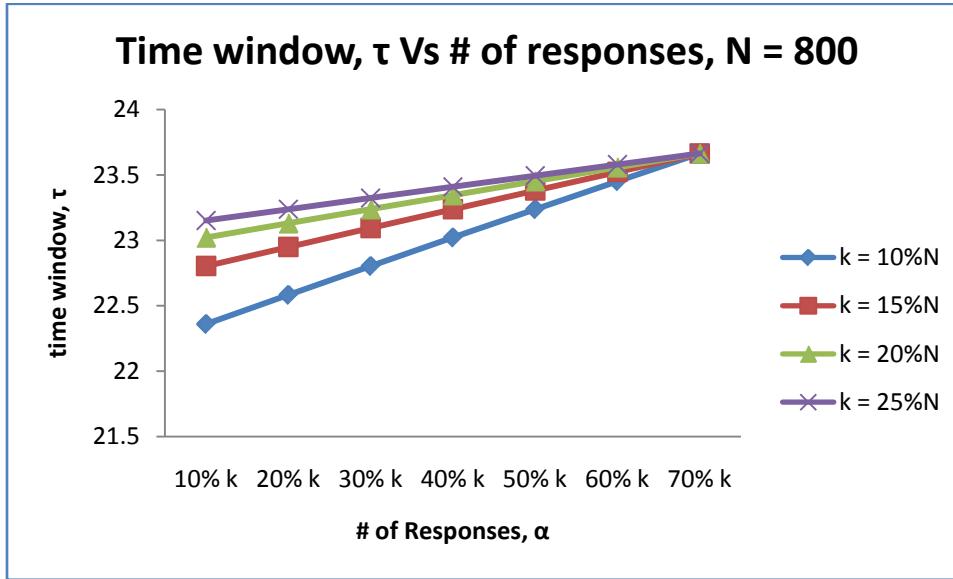


Fig. 4.8 Plot of time window vs number of neighbour advertisement messages, $N = 800$

However, when the new node uses a higher number of LSB bits in the neighbour solicitation message, this impacts on the time window and the time it takes for the scheme to converge. For example, when the LSB bits used in the neighbour solicitation request message is increased to 3 and the network size is 100, there is a great reduction in the time window to about $1.8\mu s$ as opposed to $3 \mu s$ in figure 4.3, when 10% of the total network is constituted by a malicious node.

Similar trend is also obtained in other network configurations. If the new node uses 3 LSB bits in an 800-node size network as depicted in figure 4.10, the minimum delay experienced by the new node when 25% of total network nodes are malicious is about $13.4\mu s$. Compared to $23.1 \mu s$ in figure 4.7, the delay is much more reduced.

With more number of LSB bits, the number of IP address matches of the new node with those of existing nodes is far less. This also leads to less number of neighbour advertisement responses from existing nodes which translates to less overhead on the network.

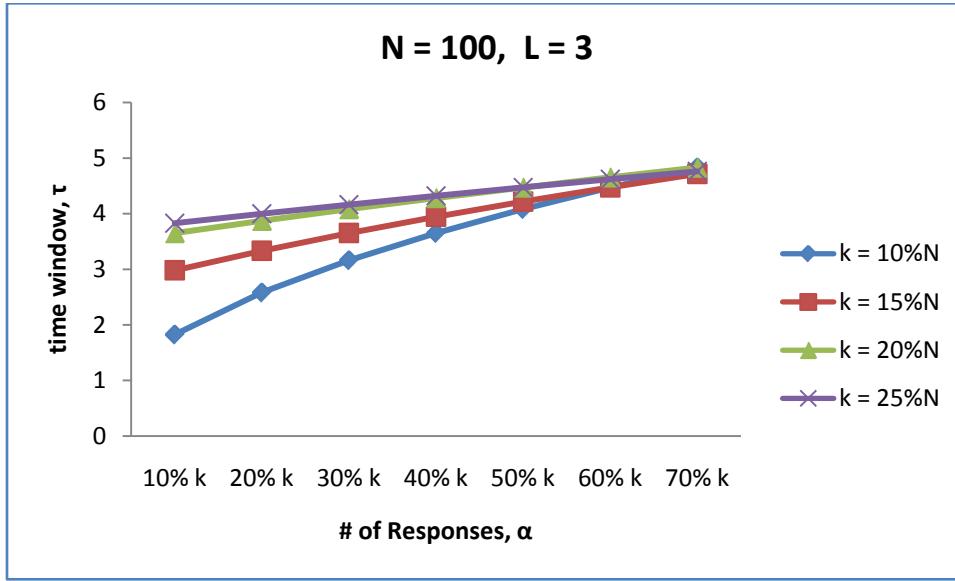


Fig. 4.9 Plot of time window vs number of neighbour advertisement messages, $N = 100$, $L = 3$

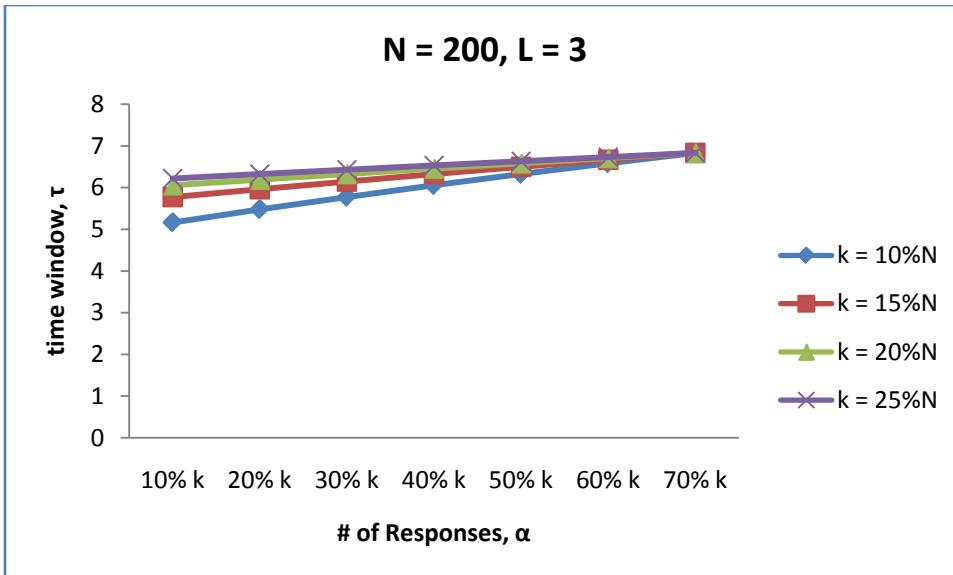


Fig. 4.10 Plot of time window vs number of neighbour advertisement messages, $N = 200$, $L = 3$

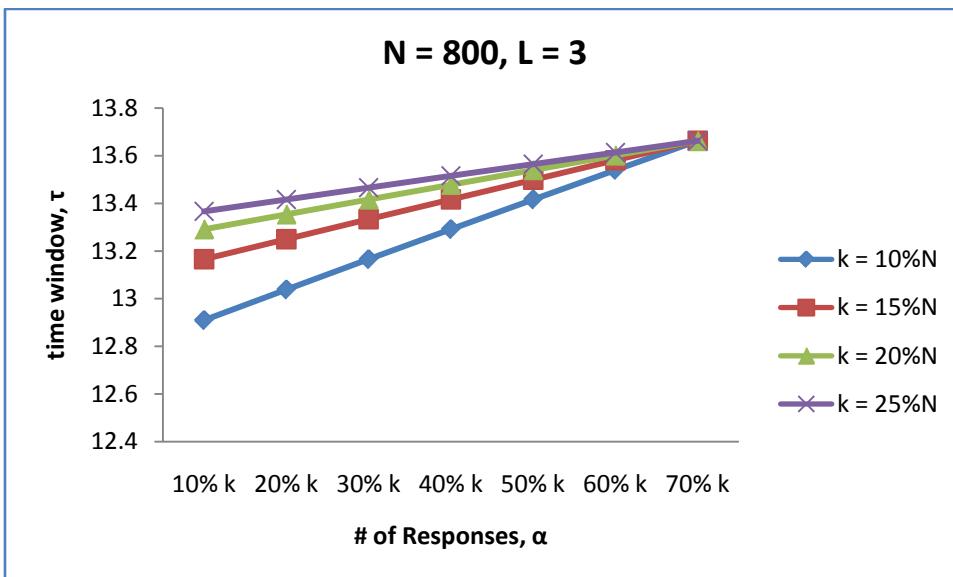


Fig. 4.11 Plot of time window vs number of neighbour advertisement messages, $N = 800$, $L = 3$

4.8 CONCLUSION

Besides the fact that the proposed MSB / LSB scheme is effective in verifying the claim of responding peers when a new node in an IPv6 network is undergoing the duplicate address detection and helps prevents a denial of service, the benefit of this technique also lies in the fact that:

- i. It helps reduce the overhead as the number of responses keeps decreasing to zero when a higher number of LSB bits is employed.
- ii. It is a powerful means by which a new node can authenticate the claims of other peer nodes without revealing the information it is attempting to verify.

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

5.1 CONCLUSION

The main focus of this thesis is to propose and implement techniques that would prevent malicious nodes from denying a legitimate node in initializing its interface when joining an IPv6 network.

Two approaches were proposed. The first approach is a reputation-based technique which involves the determination of aggregate trust of nodes inside a network. The aggregate trust is calculated from the neighbours of every node inside the network, and it is included inside the neighbour advertisement a joining node receives in response to its neighbour solicitation message sent to the k neighbours of the malicious node.

This scheme, however, assumes that each node inside the network is surrounded by some random trustworthy k neighbours from which the aggregate trust of a node is determined.

The second approach is the MSB / LSB scheme which uses information hiding concept to verify the claim of a malicious node. In this scheme, the joining node only discloses some of its features as the LSB inside the payload of its neighbour solicitation message and requests any nodes that have the LSB match to send their full IPv6 addresses inside their neighbour advertisement messages.

While the reputation scheme may fail based on the assumption that every node is has some k trustworthy random neighbours, an assumption that may not hold all the time, especially if some of the neighbour nodes later become malicious, the second scheme, however, is not constrained by this shortcoming.

In all simulation scenarios in the MSB / LSB scheme, no node inside the network is aware of the link-local address of the joining node and for this reason, it is difficult for any malicious node to spoof the joining node's address.

In addition, simulation results also showed that there were no responses to a joining node's neighbour solicitation message request before some 30% of the LSB bit are used for authentication.

And even in a very rare case of any response, the joining node can still choose any MSB bit stream out of 2^{24-m} space (m is the number of LSB bits), concatenating it with the LSB bit stream and goes through the duplicate address detection process again.

5.2 FUTURE WORK

In this work, different IPv6 network configurations were simulated with only one node attempting to join the network. As part of our future work, we intend to study scenarios where more than one node is joining the network at the same time.

REFERENCES

- [1] S. Deering and R. Hinden, “Internet Protocol Version 6 Specification,” Internet Engineering Task Force RFC 2460, 1998.
- [2] L. Ladid, “The Next Big Bail-Out: Will IPv6 save the Internet?” in proceedings of CompSysTech International Conference on Computer Systems, Technologies and Workshop for PhD students in computing, 2009.
- [3] J. Govil, J. Govil, N. Kaur, and H. Kaur, “An Examination of IPv4 and IPv6 Networks: Constraints and Various Transition Mechanisms,” in proceedings of Southeastcon conference, 2008, pp. 178-185.
- [4] R. Kaur and R. Maini, “Study of various issues of Internet Protocol Version 6,” in International Journal of Computer Applications, Vol. 12, No. 1, 2010, pp. 19-23.
- [5] “IPv6 Security Issues,” URL: www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf, Accessed on 20 February, 2012.
- [6] C. Partridge, A. W. Arsenault, and S.T. Kent, “Information Assurance and the Transition to IP Version 6 (IPv6),” in proceedings of IEEE Military Communication Conference, 2007, pp. 1-8.
- [7] M. Blanchet, “Migrating to IPv6 – a practical guide to implementing IPv6 in mobile and fixed networks”, John Wiley and Sons, 2006.

- [8] X. Yang, T. Ma, and Y. Shi, “Typical DoS/DDoS threats under IPv6,” in proceedings of the International Multi-Conference on Computing in the Global Information Technology, 2007, pp. 55-60.
- [9] R. Droms, J. Bound, B. Voltz, T. Lemon, C. Perkins and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” Internet Engineering Task Force (IETF) RFC 3315, July 2003.
- [10] C. E. Perkins, and J. Bound, “DHCP for IPv6”, in proceedings of the IEEE Symposium on Computers and Communications, 2002, pp. 493-497.
- [11] C. E. Caicedo, J. B. D. Joshi, and S. R. Tuladha, “IPv6 Security Challenges,” in Journal of Computer, Vol. 42, Issue 2, 2009, pp. 36-42.
- [12] T. Narten, “Neighbour Discovery and Stateless Auto-configuration in IPv6,” in Journal of IEEE Internet Computing, Vol. 3, Issue 4, 1999, pp. 54-62.
- [13] J. J. Silva Tobella, M. Stiemerling, and M. Bruner, “Towards Self-Configuration of IPv6 Networks,” in Networks Operations and Management Symposium, 2004, pp. 895-896.
- [14] D. J. Wilson and R. Dragnea, “IPv6 in Fixed and Mobile Networks,” Alcatel Telecommunication Review, 2004, pp. 1-7.
- [15] M. Kim and D. Seo, “The study of secure auto-configuration Technology in IPv6,” in proceedings of 7th International Conference on Advanced Communication Technology, 2005, pp. 85-88.

- [16] R. Radhakrishnan, M. Jamil, S. Mehfuz, and M. Moinudin, “Security issues in IPv6,” in proceedings of 3rd International Conference on Networking and Services, 2007, pp. 110-115.
- [17] E. Durdagi and A. Buldu, “IPv4 / IPv6 security and threat comparisons,” in Procedia Social and Behavioural Sciences, Vol. 2, Issue 2, 2010, pp. 5285-5291.
- [18] D. Yang, X. Song, and Q. Guo, “Security on IPv6,” in 2nd International Conference on Advanced Computer Control, 2010, pp. 323-326.
- [19] J. Bi, J. Wu, and X. Leng, “IPv4 / IPv6 Transition Technologies and Univers6 Architecture,” International Journal of Computer Science and Network Security, Vol. 7, No. 1, 2007, pp. 232-343.
- [20] M. Cooper and D. C. Yen, “IPv6: business applications and implementation concerns,” in Journal of Computers and Electrical Engineering, Vol. 33, Issue 5-6, 2007, pp. 425-437.
- [21] P. Hunter, “IPv6: Security Issues,” Network Security, 2004, pp. 17-19.
- [22] J. Mohacsi, “IPv6 Security: Threats and Solutions,” Information Society Technologies, 2005.
- [23] S. Szigeti and P. Risztics, “Will IPv6 Bring Better Security,” in the proceedings of the 30th EUROMICRO Conference, 2004, pp. 532-537.
- [24] D. Zagar and K. Grgic, “IPv6 Security threats and Possible Solutions,” in proceedings of World Automation Congress, 2006, pp. 1-7.

- [25] N. Griffiths, “Enhancing Peer-to-Peer Collaboration using Trust,” in Journal of Expert Systems and Applications, Vol. 31, Issue 4, 2006, pp. 849-858.
- [26] X. Chu, X. Chen, K. Zhao and J. Liu, “Reputation and Trust Management in Heterogeneous Peer-toPeer networks,” in Journal of Telecommunication Systems, Vol. 31, No. 3-4, 2010, pp. 191-203.
- [27] The Internet Protocol Specification, Internet Engineering Task Force RFC 791, 1981.
- [28] B. J. Nickels, “An Introduction to Investigating IPv6 Networks,” in Journal of Digital Investigation, Vol. 4, Issue 2, 2007, pp. 59 – 67.
- [29] R. Hinden and S. Deering, “IPv6 Addressing Architecture,” Internet Engineering Task Force RFC 4291, 2006.
- [30] E. Fgee, J. Kenney, W. J. Phillips, W. Robertson and S. Sivakumar, “Implementing an IPv6 QoS management scheme using flow label and class of service fields,” in proceedings of Canadian Conference of Electrical and Computer Engineering CCEC, 2004, pp. 1049-1052.
- [31] Q. Zang, X. Zhou and F. Yang, “Distributed Node Authentication in Wireless Sensor Networks,” in proceedings of 2nd International Conference on Future Computer and Communication, 2010, pp. 72-76.
- [32] X. Ren, K. Li, R. Li and L. Yang, “An Improved Trust Model in P2P,” in proceedings of Asia-Pacific Conference on Services Computing, 2006, pp. 76-81.

- [33] X. Wu, J. He and F. Xu, “An enhanced trust model based on reputation for P2P networks,” in proceedings of International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, Taichung, China, June 2008, pp. 67-73.
- [34] S. Chhabra, E. Damiani, S. Paraboschi and P. Samarati, “A protocol for reputation management in super-peer networks,” in proceedings of 15th International Workshop on Database and Expert Systems and Applications, Zaragoza, Spain, August 2004, pp. 973-983.
- [35] J. Chen, X. Xu and S. Bruda, “Combining Data Trust in Reputation Systems to Boost P2P Security,” in proceedings of 2nd International Conference on Future Computer and Communication (ICFCC), Wuhan, May 2010, pp. 194 –199
- [36] A. Gupta, D. Malhotra, and L.K. Awasthi, “NeighborTrust: A Trust-based scheme for Countering Distributed Denial-Of-Service Attacks in P2P Networks,” in proceedings of 16th IEEE International Conference on Networks, New Delhi, India, Dec. 2008, pp. 1-6.
- [37] X. Jiang and L. Ye, “Reputation-based Trust Model and Anti-Attack Mechanism in P2P Networks,” in proceedings of 2nd International Conference on Network Security, Wireless Communications, and Trusted Computing, 2010, pp. 498-501.
- [38] M.A. Badamchizadeh, A.A. Chianeh, “Security in IPv6,” in proceedings of the 5th WSEAS International Conference on Signal Processing, Istanbul, Turkey, May 2006, pp. 249-254.

- [39] S. Frankel, R. Graveman, J. Pearce, and M. Rooks, “Guidelines for secure deployment of IPv6 – Recommendations of the National Institute of Standards and Technology,” United States Department of Commerce, National Institute of Standards and Technology, Dec. 2010.
- [40] X. Jiang, L. Ye, “Attack-Resistant Techniques in P2P Reputation Systems,” in proceedings of 2nd International Conference on Networking and Digital Society, China, June 2010, pp. 390-393.
- [41] A. Josang, R. Ismail and C. Boyd, “A Survey of Trust and Reputation systems for online service provision,” in International Journal of Decision Support Systems, Vol. 43, Issue 2, March 2007, pp. 618-644.
- [42] D. Zagar, K. Grgic and S. Rimac-Drlje, “Security Aspects in IPv6 networks – implementation and testing,” in Journal of Computers and Electrical Engineering, Vol. 33, Issue 5-6, 2007, pp. 425-437.
- [43] IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0), URL: http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf, Accessed on 20 February, 2012.
- [44] C. Douligeris and D. N. Serpanos, “Network Security – Current Status and Future Directions,” IEEE Press, A. John Wiley and Sons, NJ, 2007.
- [45] S. Hogg and E. Vyncke, “IPv6 Security – Protection measures for the next Internet Protocol,” Cisco Press, Indianapolis, 2009.

- [46] S. Convery and D. Miller, “IPv6 and IPv4 Threat Comparison and Best Practice Evaluation (v1.0),”
Url:http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf, Accessed on 20 February, 2012
- [47] “Man-in-the-middle Attacks – Helping to eliminate the threat without impacting the business,” Url: <http://www.techrepublic.com/whitepapers/man-in-the-middle-attacks-helping-to-eliminate-the-threat-without-impacting-the-business/975615>, Accessed on 20 February 2012
- [48] M. Jensen, N. Gruschka and N. Luttenberger, “The Impact of Flooding Attacks on Networked Services,” in International Conference on Availability, Reliability and Security, 2008, pp. 509-513.
- [49] G. Carl, G. Kesimal, R.R. Brooks and S. Rai, “Denial-of-Service Attacks Detection Techniques,” in Journal of IEEE Internet Computing, Vol. 10, Issue 1, 2006, pp. 82-89.
- [50] M. Alhabeeb, X. Wu, A. Almuhaideb, P. D. Le and B. Srinivasan, “Holistic Approach for Critical System Security: Flooding Prevention,” in the 6th International Conference on Networked Computing, South Korea, 2010, pp. 1-8.
- [51] G. An, K. Kim, J. Jang, and Y. Jean, “Analysis of SEND Protocol through implementation and Simulation,” in proceedings of IEEE Conference on Convergence Information Technology, 2007, pp. 670-676.

VITA

Suli Adeniye had his Bachelor's degree in Computer Engineering at the Obafemi Awolowo University, Ile-Ife, Nigeria. After the mandatory one-year national service program in 2005, he worked as a Telecom Engineer in Telnet Nigeria Limited where he resigned to join the Master's program in Computer Engineering at the King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, which he completed in 2012.

Please address correspondence to:

Name: Suli Adeniye

Present Address: 2nd Street, By Crown Plaza Hotel, Thukbah, Eastern Region, Kingdom of Saudi Arabia

Nationality: Nigerian

Permanent Address: 5, Alhaji Saka Street, Behind Union Bank Plc, Ogere Remo, Ogun State, Nigeria.

Mobile Numbers: +966552339150, +2348028434090

Email: suliadeniye@gmail.com