Implementation of IPv6 Neighbor Discovery Protocol supporting CGA

Joong-Min Kim, In-Kap Park , Jae-Wook Yu
Network Lab., Dept. of Electronic Engineering,
1 Hwayang-dong, Gwangjin-gu, Seoul 143-701, Korea
Tel : +82-2-450-3495 Fax : +82-2-3437-5235
{krdio, ikpark, ulty}@konkuk.ac.kr
http://digcom.konkuk.ac.kr

Abstract: Having age of ubiquitous ahead, existing IPv4's address space insufficiency phenomenon appears because of increasing network usage as well as multimedia data transmission becomes much, necessity of new IP address system that guarantee QoS are needed. IPv6 was made to solve these problem. IPv6 solves address space insufficiency phenomenon offering by 128bit address space, and also offers hierarchical address layer that support improved QoS. IPv6 defines relation between surrounding node using Neighbor Discovery protocol. Used Neighbor Discovery messages, grasp surrounding node, include important informations about network. These network information outcrops can give rise in network attack and also service that use network will paralysis. Various kinds of security limitation was found in Present Neighbor Discovery protocol therefore security function to supplement this problem was required. In this thesis, Secure Neighbor Discovery protocol that add with security function was design and embody by CGA module and SEND module.

1 INTRODUCTION

Development of network was begun with interlink early in 60's mainframe and dumy terminal and now so call 3A(Anytime, Anywhere, Anydevice), Ubiquitous, is present in close at hand. Ubiquitous environment means that can use internet even if wherever, whenever, any appliances and also it means surrounding that connect to network without being courted in time and place freely. There is Mobile, kiosk, Telemetics, home networking etc. in Ubiquitous' beginning. Nevertheless ultimate image of Ubiquitous is puts computer chip into all things and give IP address and connect to network or wireless network. Need new internet address system that can give more addresses than current internet address system for Ubiquitous environment such as IPv6.

1.1 IPv4, IPv6, and Secure Problem

Internet Protocol version 4 (IPv4) that is present internet address system has 32-bit address space and can give 4,294,967,296 address.[1] IP address to allocate according as early was no problem in IP address assignment in structure of small scale network however communication is available in all products by growth of network scale made lack of IP address. Necessity of new IP address system is risen by IPv4's address space exhaustion, necessity of quality of service guarantee for multimedia data transmission and Routing Table's enormity, Internet Engineering Task Force (IETF) progresses research about IP Next Generation (IPng) and announced CATNIP, SIPP, TUBA etc. However announced Internet Protocol version 6 (IPv6) of new way being been short in IPng standard. IPv6 has 128-bit address space and can give address of a approximately 3.4×10^{38}address. This address is internet address system that can solve current internet address tribe problem to address space that can give address of a surface of the earth 1 square meter per approximately 6.65×10^{23} and can handle with enough forward demand.[1][2][3]

IPv6 has characteristic of Routing Table's simplification, simple address setting, IPSec (IP Security) basis offer and support improved QoS(Quality of Service) etc. except thing which offer 128-bit address space. among this address automatic setting by Neighbor Discovery made no need of directly establish by user as well as even if do not use DHCP(Dynamic Host Configuration Protocol), function that can establish address is a important function in Ubiquitous environment. When composed home networking using IPv4, if one take new appliances at the house DHCP server is need to user inputs IP directly or allocate IP to appliances however use by IPv6 establish IP address to appliances by automatically. These functions offers the convenience to user about Home network appliances easily even if one has no knowledge for network.

However, address automatic setting is having shortcoming. Security limitation has revealed and bared various kinds of network attack in Neighbor Discovery protocol which is to set address automatically. Attack that use security blind point can paralyzed part service of network and personal information leakage can occur in case of home networking. Because these problem is appear, IETF composes SEcuring Neighbor Discovery (SEND) walking group in the 2002 and is progressing connection research.

In this theses, design Secure Neighbor Discovery protocol with SEND walking group's Neighbor Discovery security regulation, and examined whether security through embodied SEND protocol has applied or not. Search Neighbor Discovery's security limitation first and examine several theories for Neighbor Discovery security regulations and security. Design and embodied SEND protocol with this.

2 IPV6 NEIGHBOR DISCOVERY PROTOCOL

Neighbor Discovery (ND) protocol includes message and process that define relation between surrounding node. Address Resolution Protocol (ARP), ICMP, ICMP router discovery, ICMP redirect function in IPv4 were included to ND comprehensively in IPv6. Address auto-configuration, router discovery, prefix discovery, address resolution, neighbor unreachability detection, MTU (Maximum Transmission Unit) discovery, next-hop detection and duplicate address detection are functions that ND offers. Because of these functions include information of network, in case information is outpoured, all network is exposed in several attacks. Examine each functions, automatic address setting unuse DHCPv6 server and is use when set IP address. Router discovery uses when find local router and when establish automatically default router. Address resolution mapping link-layer address of neighborhood node with IP address. Neighbor unreachability detection decides whether abutting Router or host can use continuously in local network. MTU discovery does to grasp size that can transmit by maximum at linker. Next-hop detection informs next-hop address to host when packet is transmitting. Duplicate address detection informs whether address is used already at neighborhood node.[3][9]

2.1 Neighbor Discovery Message

ND message uses ICMPv6 message structure. There is 5 types of ND message which is Router Solicitation (RS) message that use ICMP type 133, Router Advertisement (RA) message that use ICMP type 134, Neighbor Solicitation (NS) message that use ICMP type 135, Neighbor Advertisement (NA) message that use ICMP type 136 and Redirect message that use ICMP type 137. Figure 1 displays form of ND message.

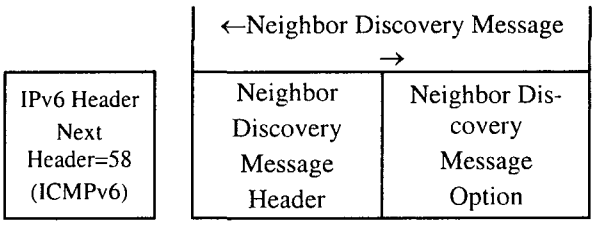

Fig.1. Neighbor Discovery message format

See that ICMPv6 is established to Next header of IPv6 header. If examine each ND message, RS message transmits in IPv6 host to search IPv6 router in link, and host sends message RA to respond immediately to IPv6 router by multicast RS without waiting regular router message. RA message is sending by response for RS message, information that need in host such as hop limit, link prefix, link MTU, router operating time here is included. NS message sends IPv6 host to searches link layer address of IPv6 node in same link, and in this message person's link layer address is included. NA message transmits at IPv6 node by response for NS message. IPv6 node sends NA message that is not required and inform in contiguity node that link layer address was changed. NA message include person's link layer address information which was sent. Redirect message is used when router informs first-hop of most suitable to host and is equal with ICMPv4's Redirect message. In redirect message address information of node send to target address of packet and succession packet that make router to send Redirect message is included.[2][9]

Information of host and Routers within same link can be discover information of link from outside if ND message is crop out. And then because of using various network attack methods can paralyzed network, ND message need security.[6]

2.2 Neighbor Discovery's security limitation

Network attack uses physical or logical security limitation of network. Multi-access link network attack method is redirect attack, Denial of Service (DoS) attack and Flooding denial of service attack. Redirect attack is that attack node redirect packet from last hop router to other node. DoS attack disturb communication between attacked node and other node. Flooding DoS attack redirect other hosts traffic to sacrifice node and then paralyze by unmeasured traffic. Three attack methods of pre shown are gotten divided by various attack method according to whether router is connected or attack from Timbuc-tu in IPv6.[5][6]

Security limitation of Neighbor Discovery function.

Purity ND function refers to function such as ND, NUD (Neighbor Unreachability Detection) and DAD (Duplicate Address Detection) that surrounding router and Rauting are not related from address automatic setting part. Security limitation that this purity ND function has can be examine through various kinds of Threats/attack. Neighbor Solicitation/Advertisement Spoofing takes advantage of connecting IP address and link-layer address using NS and NA message. Neighbor Unreachability Detection Failure uses always monitoring reachability of node that communicates with own node. Duplicate Address Detection DoS Attack uses that added and transmits address that node establishes by oneself when use stateless address automatic setting in NS message.[4][6]

Security limitation of Router Discovery function.

When purity ND function and router and Routing were involved, security limitations that appear can recognize through Threats/attack way. Malicious Last Hop Router is attack way to invent RA message so that host may establish attacker by default router. Default Router Killed attack way uses characteristic that judge there is host within link that the transmission destination is same in case default router list is empty. Good Router Goes Bad is when remain continuously without sending Redirect message only being attack such as Malicious Last Hop Router. Spoofed Redirect Message is way of attack that attacker sends Redirect message by host using link-layer address of first hop router. Bogus On-Link Prefix is way of attack to forge and sends RA message that any prefix is uniformity link. Bogus Address Configuration Prefix attack is attack that transmit mistaken Subnet prefix when host sets address automatically. Parameter Spoofing is DoS attack that transmit RA message which have forged parameter.[2][5][6]

3. SECURE NEIGHBOR DISCOVERY

ND protocol and address automatic setting are used to acquire local topology information of nodes on IPv6 network. It is hard to apply actually to AH's key administration problem although ND and address automatic setting offer security function using IPSec Authentication Header. IPSec must set by hand without using internet key exchange to form security connection (security association). IETF's SEND WG (Working Group) is studying ND extension protocol that support security function without passivity setting to solve these problem. It is studying about trust model development, protocol development that guarantee so that open key (public key) may can be shared offering certification service and key division (key distribution) protocol development and use method development of open key cipher system mainly.[6][7]

3.1 Neighbor Discovery Trust Model

IETF's SEND WG is advising to do Neighbor Discovery trust model to foundation about security solutions for IPv6 ND. ND trust model has three types which is corporate intranet model, public wireless network model who single administrator exists and ad hoc network model. According to each trust model, degree and method to require security are different.[6]

Corporate intranet model is intranet or network that all nodes belong to one administrative domain (one administrative domain)is by first rank. It is when belong to being not open to the public network that is managed by administrator mainly and all nodes trust each other in IP layer.[5][6]

Public wireless network model who single administrator exists is hotel, airport and coffee shop with administrator who manage public wireless network with wireless LAN is by second ranks.[6]

Ad hoc network model is when sicker administrator does not exist and all nodes do not trust each other is by third ranks. Usually, nodes can not use traditional certification mechanism because nodes do not exchange security connection information beforehand when they meet for the first time with companion node.[6]

In this paper, proposes and embodies ND protocol that security is applied to three trust models. Corporate intranet model, public wireless internet model who single administrator exists uses given trust model condition. However, because there is no intermediate to form relationship of mutual trust between each nodes ad hoc network model's case, it is impossible that embody ND that security is applied on given trust model condition. Therefore, some conditions must be add to given trust model's condition.

Firstly additional condition is uses trusted third party in general ad hoc network model. Secondly, each node receives authentication through third party. Thirdly, all nodes trusts quotation that is awarded in third party. ND's implementation that security is applied in ad hoc network by these addition condition is possible.

3.2 IPv6 extension header for security

IPv6 is included to basis while IPSec supported on option in IPv4. Though IPSec is included in form of extension header (extension header) in IPv6, there are AH (Authentication Header) and ESP (Encapsulating Security Payload) Header.[3] AH offers data certification to verify packet that transmit at node, data integrity (integrity) to verify that was not modified at transmission process and re-transmission prevention (anti-replay protection) that prevent transmission from captured packet. AH is consisted of Next header, Payload Length, Reserved, SPI (Security Parameter Index), Sequence Number and Authentication Data field. SPI is field to discriminate security association, and Sequence Number is field that is used for re-transmission prevention and Authentication Data is calculated value of stored by certification algorithm. AH offers authentication and integrity using MD5 - HMAC or SHA1 - HMAC algorithm. ND (Secure ND) that security of this thesis applied extends IPSec AH and provide security service.

3.3 Neighbor Discovery correction

Need correction of ND protocol to support security function.[7] Because of using coming rules, ND protocol correction and Secure ND is offer. First, address that is unspecified is not use for source address.[7] Address that is not specified is written as 0.0.0.0 in IPv4 and written as 0:0:0:0:0:0:0:0 or :: in IPv6. ND (Secure ND) that security function is applied is not using in NS, NA, RA and Redirect message. If is possible, not specified address in unuse in RS message. Do not correct neighbor cache when RS message was sent from address that did not specified.[9]

Second, Solicited-node multicast address changes to Securely-solicited-node multicast address. Securely-solicited-node multicast address is following form.

FF02:0:0:0:0:1:FEXX:XXXX
(FF02::1:FEXX:XXXX)

This multicast address is calculated by unicast and function of anycast addresses. And also form of unicast and low rank 24bit of anycast address and prefix FF02::1:FE00::/104 attaching. Extent of the result multicast address FF02::1:FE00:0000 to FF02::1:FEFF:FFFF comes out.[7] Third, temporary option (nonce option) is applied to all ND requests (solicitation) with response (solicited advertisement) of request. Temporary option is used for warranting that is response about sent request. Temporary option is consisted of Type, Length, Nonce field. Type field is identifier that specify in IANA and Length field stores temporary option of whole length by 1byte. Nonce field is minimum 6byte random number and established by side of where request message was sent. Fourth, Proxy ND does not support. Research is progressing present in present IETF's IPv6 WG that Proxy ND offers function similar to IPv4's Proxy ARP. In case unuse Proxy ND, NA's Target Address field is same with address like departure of NA message packet. Therefore, NA's Target Address field should be same with address like packet departure address in Secure ND.

3.4 Cryptographically Generated Addresses(CGA)

IPSec uses IKE (Internet Key Exchange) by basis exchange protocol to form security connection with other person.[4] In some particular case, IPSec must establish by hand without using IKE protocol. In this case, there is no problem In case of establishing from IP address by hand however problem happens when setting address by automatically through ND. For example, need security connection to use IKE in case such as system booting as well as need IP address for security connection problem such as 'Rooster is first or egg is first' happens.[6] Certification is permitted through use of open key under security connection with directly established without key administration protocol to solve these problems. Also, must use mechanism that can confirm oneself trust because do not make use of traditional certification mechanism that must form relationship of mutual trust beforehand. Cryptographically Generated Address (CGA) permits certification even if there is no relationship of mutual trust beforehand, providing service about possession of address using open key and individual key.[4][6] CGA creates IPv6's interface ID by calculating of cryptographic hash of open key.

Implementation Secure Neighbor Discovery

In this chapter, apply to substances that handled in front and also design and embody about Secure ND protocol. Important two items in Secure ND protocol design and embody is IPSec AH header and Secure ND protocol that use additional ICMPv6 message and Cryptographically Generated Addresses (CGA) that can quote in situation that can not use key exchange protocol such as IKE. In this thesis, Sorting these two items by CGA module and Secure ND (SEND) module with design and embody.

CGA module creates 128-bit IPv6 address that contains certification information in Secure ND protocol. Such created IPv6 address says it is CGA address and self certifying technique is applied. When two nodes communicate in IPv6 network, it begins communication with establishing CGA address to link local address, and to get certificate chain through Secure ND's addition message after certification ends. And communicate to own address with using certification chain that get. CGA module embodied to create and verify CGA address.

SEND module creates Delegation Chain Solicitation message and Delegation Chain Advertisement message transmit to IPv6 network and embodied to verify all Secure ND messages that is received that. Because CGA module and SEND module all act in open key base (PKI), certificate is used. Certificate uses storing basis certificate by hand when setting system in first time and use by new certificate with updated, if certification chain is obtained with using Secure ND protocol. Basis certificate, used in CGA module and SEND module, is used by certificate that is issued in Verysign which is international official recognition certification engine.

CGA module and SEND module embodied based on Windows system. Router system used Windows Server 2003 that support IPv6 to basis, and general node system installed IPv6 through Service Pack with Windows XP Professional. Microsoft Visual Studio .NET 2003 used for development tool which supports IPv6.

Implementation CGA module

CGA module is consisted greatly of CGA address creation flag, CGA address verifier and CGA Parameter Manager. CGA address creator creates CGA address, and address verifier foretells certification availability of CGA address that was received. CGA Parameter Manager store result that happen at creation process and receives included Parameter when received CGA address. CGA module, embodying form of C++ class, can use other module or application development and programmed that act in Windows consol to verify action of CGA module. If run program, result is stored to file of text form.

If examine result, necessary SecParam cost is 1 that is user inputs in CGA creation. And Subnet Prefix also use FE80::/64 which is basis value.

```
36 bc 81 c2 49 ec e1 a5 38 90 af d8 b3 e8 1b 78
```

Open key that draw in certificate is encode with A structure.

```
06 02 00 00 00 24 00 00 52 53 41 31 00 04 00 00
01 00 01 00 d5 e4 9f b0 83 f5 d2 1c ac e3 49 87
93 47 9c f2 89 e0 10 9d 44 38 0b 40 a0 fb 1a 83
35 bd 7f 34 4d bc 39 7b 50 6d ed 26 c4 fe 96 c4
a3 9f 80 9e 88 7c f4 51 f1 39 48 83 a5 87 49 a3
bd b2 70 f6 fd 36 18 aa 39 a6 ad 53 07 7f 48 0e
1f 9b 3b 8e bd 44 5d b7 7c c1 d9 57 eb 73 df b1
fa f8 1f 28 c5 22 27 d0 50 c6 a6 88 00 8e 74 e7
10 59 17 28 45 6c b6 53 69 ff 16 ad c6 f2 be f0
56 ed 6f e2
```

If find Hash1 value and Hash2 value using obtained value, Hash1 is as following.

```
34 10 64 60 b1 14 9d ee
```

Hash2 is as following.

```
00 00 7a 4b 11 8b a2 52 f6 28 04 8b ef 28
```

Created CGA address is as following using Hash1 cost.

```
fe 80 00 00 00 00 00 00 34 10 64 60 b1 14 9d ee
```

If see CGA address, it has relationship with subnet prefix FE80:: IPv6 address format.

Implementation SEND module

SEND module is design and embody with using Network Dirver Interface Specification (NDIS) of dual stack architecture of Windows. There is network adapter driver on dual stack architecture's lowest end. This driver, driver of NIC (Network Interface Card), can pass to IPv4 or IPv6 protocol part though NDIS because being fenced by NDIS. Therefore, if use NDIS packet can catch when entering NIC and created packet can transmit through NIC. SEND module inserts SEND driver to NDIS, other parts of SEND module transmit and receive packet through SEND driver can embody.

SEND module communicates using CGA address being inputted CGA address that is created in CGA module and CGA Parameter.

SEND driver part manufactured correcting NDIS driver that is used to existent pack monitoring, Secure ND message creator and verifier embodied in class form, and embodied Windows consol program for verification of SEND module.

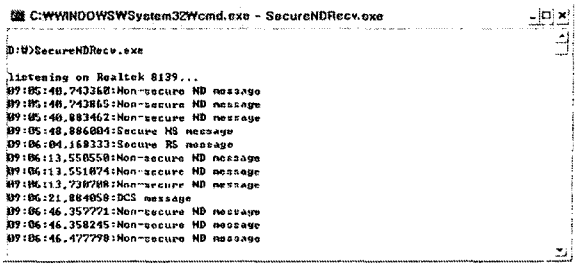

Fig.2. Verify Program of Secure ND message

4. DISCUSSION

In this thesis, Secure Neighbor Discovery protocol that add with security function was design and embody by CGA module and SEND module. CGA module creates CGA(Cryptographically Generated Address) that include certification information between node and also verify CGA address of other node. SEND module creates Secure Neighbor Discovery message that security function is added and transmits through NIC. Also, through NIC, verify received Secure Neighbor Discovery message.

References

[1] Mark A. Miller, P.E. Miller, "Implementing IPv6", *Hungry Minds*, 2000

[2] Jeff Doyle, Jennifer D. Carroll, "Routing TCP/IP volume 2", *Cisco press*, 2001

[3] Joseph Davies, "Understanding IPv6", *MS press*, 2002

[4] H. X. Mel, Doris M. Baker, "Cryptography Decrypted", *Addison Wesley*, 2000

[5] Saadat Malik, "Network Security Principles and Practices", *Cisco press*, 2002

[6] P. Nikander, J. Kempf, E. Nordmark, "IPv6 Neighbor Discovery trust models and threats", *draft-ietf-send-psreq-03.txt*, work in progress

[7] J. Arkko, J. Kempf, B. Sommerfeld, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)", *draft-ietf-send-ipsec-01.txt*, work in progress

[8] T. Aura, "Cryptographically Generated Addresses (CGA)", *draft-ietf-send-cga-01.txt*, work in progress

[9] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP version 6", *RFC2461*