논문 2004-41TC-12-5

보안기능을 지원하는 IPv6 ND Protocol 구현에 관한 연구

(A Study on Implementation of IPv6 Neighbor Discovery Protocol supporting Security Function)

유 재 욱*, 박 인 갑*, 김 중 민*

(Jae-Wook Yu, In-Kap Park, and Joong-Min Kim)

요 약

IPv6는 Neighbor Discovery(ND) 프로토콜을 사용하여 주변 노드간의 관계를 정의한다. 주변 노드를 파악하기 위해 사용되는 ND 메시지들은 네트워크에 관한 중요한 정보들을 포함한다. 이러한 네트워크 정보가 유출될 경우 네트워크 공격에 노출되어 네트워크를 이용한 서비스가 마비될 수 있다. 현재 ND 프로토콜은 여러 가지 보안 취약점이 발견되었으며 이를 보완하기 위한 보안기능이 요구되었다.

본 논문에서는 ND 프로토콜에 보안기능을 추가한 Secure ND 프로토콜을 CGA 모듈과 SEND 모듈로 구현하였다.

Abstract

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.

Keywords : Network, IPv6, Security

I. 서 론

네트워크의 발달은 60년대 초 메인프레임과 더미 터미널을 연결하는 것으로 시작되어 현재 3A(Anytime, Anywhere, Anydevice) 산업이라고도 하는 유비쿼터스(ubiquitous) 시대를 눈앞에 두고 있다. 유비쿼터스 환경은 언제, 어디서나, 어느 기기로나 인터넷을 이용할 수 있다는 것을 의미하고 시간과 장소에 구애받지 않고 자유롭게 네트워크에 접속하는 환경을 의미하기도 한다. 유비쿼터스의 초기 단계로 모바일, 키오스크, 텔레매틱스, 홈네트워킹 등이 있으나 유비쿼터스의 궁극적인 모습은 모든 사물에 컴퓨터 칩을 심고 주소를 부여해 유무선 네트워크로 연결하는 것이다. 이러한 유비쿼터스 환경을 위해서는 현재의 인터넷 주소체계보다 더 많은 주소를 부여할 수 있는 새로운 인터넷 주소체계가 필요하게 되었다.

IPv6는 128비트 주소공간을 제공하는 것 이외에 Routing Table의 간소화, 단순한 주소설정, IPSec (IP Sercurity) 기본제공 그리고 나아진 QoS (Quality of Service) 지원 등의 특징을 가지고 있다[1]. 이중 Neigh-bor Discovery에 의한 주소 자동설정은 사용자가 직접 주소를 설정할 필요가 없고, DHCP (Dynamic Host Configuration Protocol)을 이용하지 않아도 주소를 설정할 수 있는 기능으로 유비쿼터스 환경에서는 꼭 필요한 기능이다. 그러나 주소 자동설정은 단점도 지니고 있다. 주소 자동설정을 하는데 이용되는 Neighbor Discovery 프로토콜에는 보안 취약점이 있어서 여러 가지 네트워크 공격에 노출되어 있다. 보안 허점을 이용한 공격은 네트워크의 일부 서비스를 마비시킬 수도 있

* 정회원, 건국대학교 전자정보통신공학부
(Dept. of Electronic Engr., KonKuk University)
접수일자: 2004년4월14일, 수정완료일: 2004년12월10일

으며 홈 네트워킹의 경우 개인정보유출이 일어날 수도 있다.

본 논문에서는 SEND 워킹그룹의 보안 규정을 바탕으로 Secure Neighbor Discovery 프로토콜을 설계하고, 보안 알고리즘을 적용하여 구현하고, 구현된 SEND 프로토콜을 통해 보안이 적용 되었는지를 살펴보았다. 먼저 Neighbor Discovery의 보안 취약점을 알아보고 Neighbor Discovery 보안 규정들과 보안을 위한 여러 이론들을 살펴본다. 이를 바탕으로 SEND 프로토콜을 설계하고 구현하였다.

II. Secure Neighbor Discovery Protocol

1. Neighbor Discovery 보안모델

IETF의 SEND WG에서는 IPv6 ND를 위한 보안 솔루션들에 대해 Neighbor Discovery 보안모델을 기초로 할 것을 권고하고 있다. ND 보안 모델은 세 가지로 사내 인트라넷(corporate intranet) 모델, 단일 관리자가 존재 하는 공중 무선(public wireless) 네트워크 모델 그리고 ad hoc 네트워크 모델이 있다. 각 보안 모델에 따라서 보안을 요구하는 정도와 방법이 다르다.[3]

첫째로 사내 인트라넷 모델은 모든 노드가 하나의 관리 도메인(one administrative domain)에 속해있는 인트라넷이나 네트워크이다.

둘째로 단일 관리자가 존재하는 공중 무선네트워크 모델은 호텔, 공항, 커피숍 내에서의 무선 LAN과 같이 공중 무선네트워크를 관리하는 관리자가 있는 모델이다.

셋째로 ad hoc 네트워크 모델은 신뢰할 수 있는 관리자도 존재하지 않고 모든 노드들이 서로를 신뢰하지 못하는 경우이다. 일반적으로 노드들은 상대 노드와 처음으로 만나게 되므로 사전에 보안관련 정보를 교환하지 못하기 때문에 전통적인 인증메커니즘을 사용할 수 없다.

2. 보안을 위한 IPv6 Extension Header

IPv6에는 IPv4에서 옵션으로 지원되던 IPSec이 기본으로 포함되어 있다. IPv6에서 IPSec은 확장 헤더(extension header)의 형태로 포함되어 있는데 AH (Authentication Header)와 ESP(Encapsulating Secu-rity Payload) Header가 있다.[6][7][8]

AH는 노드에서 전송한 패킷을 검증하기 위한 데이터 인증, 전송과정에서 수정되지 않았음을 검증하기 위한 데이터 무결성(integrity) 그리고 캡쳐된 패킷을 재전송하는 것을 막는 재전송 방지를 제공한다. AH는 Next header, Payload Length, Reserved, SPI(Security Parameter Index), Sequence Number 그리고 Authenti-cation Data 필드로 구성된다.

SPI는 보안 연관(security association)을 식별하기 위한 필드이고, Sequence Number는 재전송 방지를 위해 사용되는 필드이며 Authentication Data는 인증 알고리즘에 의해 계산된 값이 저장되는 필드이다[6]. AH는 MD5-HMAC 또는 SHA1-HMAC 알고리즘을 이용하여 인증과 무결성을 제공한다.

ESP는 데이터의 기밀성, 인증, 무결성 그리고 재전송 방지를 제공한다. ESP는 SPI, Sequence Number, Payload Data, Padding, Padding Length, Next header 그리고 Authentication Data 필드로 구성된다. Payload Data 필드는 보안 연관에 의해 암호화된 데이터가 저장되며 길이를 맞추기 위한 값이 Padding 필드에 추가 된다. 추가된 Padding의 길이가 Padding Length 필드에 저장되고 Authentication Data 필드는 SPI 필드부터 Next header 필드까지를 인증한 결과 값이 저장된다[7]. ESP는 DES-MD5 알고리즘을 사용하여 보안 서비스를 제공한다.

3. ND Protocol 수정

보안 기능을 지원하기 위해서는 ND 프로토콜의 수정이 필요하다[4]. 다음 규칙들을 이용하여 ND 프로토콜을 수정하고 Secure ND를 제공한다.

첫째, 지정되지 않은 주소(unspecified address)는 출발지 주소(source address)로 사용하지 않는다[4]. 지정되지 않은 주소는 IPv4에서 0.0.0.0으로 표기되고 IPv6에서 0:0:0:0:0:0:0:0 또는 ::으로 표기되는 주소를 말한다. 보안이 기능이 적용된 ND(Secure ND)에서는 NS, NA, RA 그리고 Redirect 메시지에 대해서 지정되지 않은 주소를 사용하지 않는다. 가능하면 RS 메시지에 대해서도 지정되지 않은 주소를 사용하지 않는다. 지정하지 않은 주소로부터 RS 메시지가 보내졌을 때 neighbor cache를 수정하면 안된다[9].

둘째, Solicited node 멀티캐스트 주소는 Securely solicited node 멀티캐스트 주소로 변경한다. Securely solicited node 멀티캐스트 주소는 다음과 같은 형식으로 되어 있다.

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

이 멀티캐스트 주소는 unicast와 anycast 주소들의

함수로서 계산된다. unicast와 anycast 주소의 하위 24 비트와 prefix FF02::1:FE00::/104를 붙임으로써 형성된다. 그 결과 주소의 범위가 FF02::1:FE00:0000에서 FF02::1:FEFF:FFFF까지 나온다.[4]

셋째, 임시옵션(nonce option)은 모든 ND 요청과 요청에 대한 응답에 적용된다. 임시옵션은 보내진 요청에 대한 응답임을 보증하는데 사용된다. 임시옵션은 Type, Length, Nonce 필드로 구성된다. Type 필드는 IANA에서 지정하는 식별자이고 Length 필드는 1바이트로 임시옵션 전체길이를 저장한다. Nonce 필드는 최소 6바이트의 랜덤 넘버(random number)로 요청메시지를 보내는 측에서 설정한다.

넷째, Proxy ND는 지원하지 않는다. Proxy ND는 IPv4의 Proxy ARP와 유사한 기능을 제공하는 것으로 현재 IETF의 IPv6 WG에서 현재 연구가 진행 중이다[4]. Proxy ND를 사용하지 않은 경우에 NA의 Target Address 필드는 NA 메시지 패킷의 출발지 주소와 같게 된다. 따라서 Secure ND에서는 NA의 Target Address 필드가 패킷 출발지 주소와 같아야한다.

4. Authorization Delegation Discovery

IPv6 ND를 포함한 몇 가지 프로토콜들은 노드가 새로운 링크에 접속했을 때 망으로부터 받은 정보를 이용해서 자동설정을 할 수 있도록 한다. 이 경우 침입 라우터(rogue router)가 설정될 수도 있고, 받은 정보의 정확도를 판단할 방법이 없다. Secure ND에서는 새로운 ICMPv6 메시지를 추가하여 라우터의 도움을 받아 클라이언트가 인증 사슬(certificate chain)을 얻을 수 있도록 한다. 새로운 ICMPv6메시지는 Delegation Chain Solicitation 메시지와 Delegation Chain Advertisement 메시지이다. 이 두 가지 메시지를 이용하여 인증 사슬을 얻는 과정을 Authorization Delegation Discovery라 한다.[4]

호스트가 라우터에 Delegation Chain Solicitation 메시지를 전송하면 라우터는 Delegation Chain Adver-tisement 메시지를 생성하여 전송한다. Secure ND는 새로운 메시지와 옵션를 추가하여 SEND 모듈을 구현한다.

5. Cryptographically Generated Addresses

IPSec은 상대방과 보안연관을 맺기 위해 IKE (Internet Key Exchange)를 기본키 교환 프로토콜로 사용한다. IPSec은 특정한 경우에 IKE 프로토콜을 사용하지 못하고 수동으로 설정해야 한다. 이러한 경우 IP 주소를 수동으로 설정하는 경우에는 문제가 없지만 ND를 통해서 주소 자동설정을 하는 경우는 문제가 발생한다. 예를 들어 시스템 부팅과 같은 경우에 IKE를 사용하기 위해서는 보안연관이 필요하고, 보안연관을 위해서는 IP 주소가 필요하게 되어'닭이 먼저냐 달걀이 먼저냐'와 같은 문제가 발생하게 된다[3]. 이러한 문제를 해결하기 위해 키관리 프로토콜 없이 직접적으로 설정된 보안연관 하에서 공개키 사용을 통한 인증을 허용한다. 또한 사전에 신뢰관계를 형성해야 하는 전통적인 인증메커니즘을 사용하지 못하므로 스스로 신뢰를 확인해 줄 수 있는 메커니즘을 이용해야한다. CGA는 공개키와 개인키 쌍을 이용하여 주소의 소유권에 대한 서비스를 제공하여 사전에 신뢰관계가 없어도 인증을 가능하게 한다.[3][5]

CGA는 공개키의 암호화 해쉬(cryptographic hash)의 계산에 의해 IPv6의 인터페이스 식별자(interface ID)를 생성하는 것이다.

6. Secure ND에 적용되는 보안알고리즘

Secure ND에 적용되는 보안 알고리즘은 ND 확장 프로토콜에서 사용하는 X.509 공개키 시스템 그리고 IPSec과 CGA에서 사용하는 SHA-1 알고리즘이다.

X.509 공개키 시스템은 공개키 시스템(PKI)이라 불리는 전자 인증의 관리 방식 중 하나이며 Secure Hash Algorithm(SHA)는 일반적으로 SHA-1이라고 부른다. 이 알고리즘은 최대 길이가 264비트 보다 작은 메시지의 입력을 가지고 160비트의 메시지 다이제스트를 출력으로 생성한다. 본 논문에서는 X.509 공개키 시스템을 이용하여 SEND 모듈을 설계 및 구현하였으며, CGA 모듈과 SEND 모듈에 SHA-1 알고리즘을 적용하였다.

III. Secure Neighbor Discovery 구현

1. CGA 모듈 구현

CGA 모듈은 크게 CGA 주소 생성기, CGA 주소 검증기 그리고 CGA Parameter Manager로 구성되어있다. CGA 주소 생성기는 CGA 주소를 생성하고, 주소 검증기는 받은 CGA 주소의 인증 여부를 판단한다. CGA Parameter Manager는 생성과정에서 발생한 결과를 저장하고, CGA 주소를 받았을 때 함께 포함된 Parameter를 받아들인다. CGA 모듈의 전체 구성은 그림 1과 같다. Subnet Prefix는 64비트의 subnet prefix

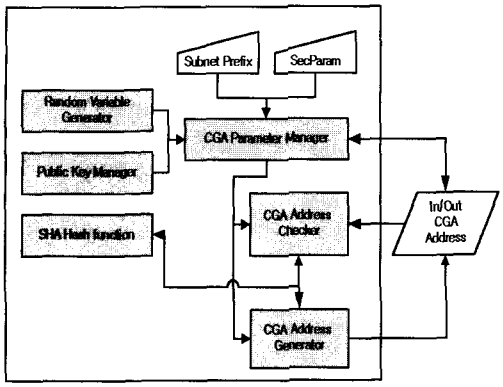

그림 1. CGA 모듈 블럭다이어그램
Fig. 1. CGA Module Block Diagram.

주소를 설정하는 것으로 사용자가 지정하며 link local 주소인 FE80::이 기본값이다. SecParam은 0에서 7사이의 Security Parameter 값을 설정하는 것으로 사용자가 지정하며 기본값을 0으로 설정한다. Random Variable Generator는 128비트의 modifier값을 출력하도록 구현하였다. modifier값은 랜덤 값으로 구성되며 Random Variable Generator는 랜덤 함수를 이용하여 값을 생성하고 바이너리 형태로 저장한다. Public Key Manager는 인증서로부터 공개키를 추출하여 저장한다. 인증서마다 크기가 다른 공개키를 추출하기 위해서 가변크기의 저장 공간을 사용하도록 설계하였다. SHA Hash function은 가변크기의 입력을 이용하여 해쉬 알고리즘 수행한다. 수행 결과는 160비트의 고정크기 출력으로 만들어 진다. CGA 주소 생성기와 검증기는 160비트의 출력을 Hash1값과 Hash2값으로 만든다.

CGA 모듈은 C++의 클래스 형태로 구현하여 다른 모듈이나 어플리케이션 개발에 이용할 수 있도록 하였으며 CGA 모듈의 동작을 검증하기 위해 Windows consol에서 동작하는 프로그램을 구현하였다. 프로그램을 실행하면 결과는 텍스트 형태의 파일로 저장된다.

2. SEND 모듈 구현

SEND 모듈은 Windows의 dual stack architecture의 Network Dirver Interface Specification(NDIS)를 이용하여 설계 및 구현하였다. dual stack architecture의 최하단부에 network adapter driver가 있다. 이 driver는 NIC (Network Interface Card)의 driver로 NDIS에 의해 보호되고 있어 NDIS를 통해야만 IPv4 또는 IPv6 프로토콜 부분으로 전달된다. 따라서 NDIS를 이용하면 NIC로 들어오는 패킷을 얻을 수 있고, 생성한 패킷을 NIC를 통해 전송할 수 있다. SEND 모듈은 그림 2와

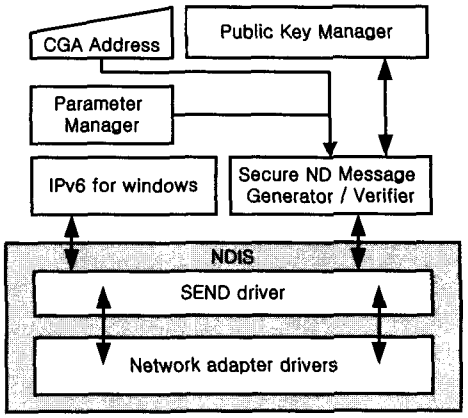

그림 2. SEND 모듈 블럭다이어그램
Fig. 2. SEND Module Block Diagram.

같이 SEND driver를 NDIS에 삽입하여 SEND 모듈의 다른 부분들이 SEND driver를 통해 패킷을 송·수신할 수 있도록 구현하였다.

SEND 모듈은 CGA 모듈에서 생성된 CGA 주소와 CGA Parameter를 입력받아 CGA 주소를 이용한 통신을 한다. Secure ND 메시지 생성기는 Secure ND 메시지들 중 Delegation Chain Solicitation와 Advertisement 메시지를 생성하여 네트워크로 전송하고, Secure ND 메시지 검증기는 모든 Secure ND 메시지를 검증할 수 있도록 구현하였다. ND 메시지들은 ICMPv6 헤더를 사용하여 통신할 수 있도록 ICMPv6의 Type이 지정되어 있다. Secuere ND 메시지 중 새로 추가된 Delegation Chain Solicitation와 Advertisement 메시지는 type이 지정되어 있지 않아 새로 지정하였다. ICMPv6가 정보 메시지로 사용될 때 type 필드의 최상위 비트를 1로 세팅해야 한다는 규칙에 맞게 Delegation Chain Solici-tation 메시지는 ICMPv6 Type을 241로 지정하고, Advertisement 메시지는 242로 지정하였다. Secure ND 메시지 검증기는 ICMPv6 헤더와 AH 헤더를 분석하여 Secure ND 메시지를 구분한다.

SEND driver 부분은 기존의 packet monitoring에 사용되는 NDIS driver를 수정하여 제작하였고, Secure ND 메시지 생성기와 검증기는 클래스 형태로 구현하였으며 SEND 모듈의 검증을 위해 Windows consol 용 프로그램을 구현하였다. Secure ND 메시지 전송 프로그램은 전송하고자 하는 메시지를 선택하면 해당 메시지를 Secure ND 메시지 형식으로 전송한다. Secure

ND 메시지 검증 프로그램은 NIC로부터 받은 메시지를 분석하여 화면에 표시한다. 검증 프로그램의 경우 전송 프로그램에서 보내는 데이터 이외에 네트워크에서 발생하는 데이터도 받게 된다. 이 경우 검증 프로그램은 보안이 적용되지 않은 ND 메시지로 판단한다.

Ⅳ. 실 험

본 논문에서는 보안모델 중 하나인 사내 인트라넷(corporate intranet) 모델을 기초로 IPv6 link local 네트워크를 구성하여 CGA 모듈과 SEND 모듈을 실험하였다[3]. 실험을 위한 네트워크 환경은 그림 3과 같다. 허브를 이용하여 게이트웨이, 라우터 시스템, 일반노드 시스템1 그리고 일반노드 시스템2를 연결하고, 게이트웨이는 인터넷에 연결하였다. 인터넷과 게이트웨이는 IPv4로 연결 되어 있고, 허브를 중심으로 라우터, 일반노드1 그리고 일반노드2는 IPv4와 IPv6를 동시에 지원하는 Windows dual stack architecture를 이용하여 구성하였다.

CGA 모듈은 라우터 시스템과 일반 노드 시스템에서 다수의 CGA 주소를 생성시켜 Security Parameter에 따른 알고리즘 반복횟수와 생성 소요시간을 비교해 보고, SEND 모듈은 ICMPv6의 Type과 AH 헤더의 유무에 따라 Secure ND 메시지 검증이 정확하게 일어나는지 확인한다.

1. CGA 모듈 시뮬레이션 및 고찰

CGA 모듈은 Secure ND 프로토콜에서 사용할 보안이 적용되어 있는 IPv6 주소(CGA)를 생성하는 모듈이다. CGA 주소는 설정된 SecParam에 따라 보안 알고리즘을 반복수행하는 횟수가 바뀌어 CGA 주소생성 시간에 영향을 준다. CGA 모듈 시뮬레이션은 라우터 시스템과 일반노드 시스템에서 수행하여 SecParam의 값에 따른 CGA 주소생성 시간을 측정해 보고, 라우터 시스템과 일반노드 시스템에서 어떠한 차이가 있는지 비교하여 CGA 모듈의 적용방법과 개선점을 생각해 본다. 표 1은 라우터 시스템과 일반노드 시스템에서 Security Parameter값을 바꾸어가며 1만개의 CGA를 생성하는데 소요된 평균시간을 나타낸다.

CGA 주소 생성과정에서 SecParam값이 0인 경우는 Hash2를 구하는 SHA-1 Hash 알고리즘을 한번만 실행시키고, 값이 1이상인 경우는 Hash2의 상위 16 비트가

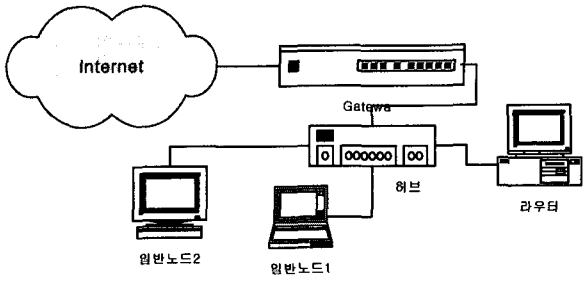

그림 3. 테스트를 위한 link local 네트워크
Fig. 3. Link local network for testing modules.

표 1. CGA 생성시간
Table 1. Generation times of CGA.

시스템 / SecParam	라우터 시스템 (P3-870MHz)	일반노드 시스템1 (P3-696MHz)
0	0.000094 sec	0.00014 sec
1	1.0443 sec	1.7964 sec

SecParam과의 조건을 만족할 때 까지 알고리즘을 반복한다. 조건을 만족하는 Hash2의 수를 예상하면 SHA-1 Hash 알고리즘의 출력은 160비트로 고정되어 있어 2^{160}개의 Hash2를 예상할 수 있다. 이때 SecParam을 n이라 하면, 상위 16n비트가 0인 경우이므로 $2^{(160-16n)}$개의 Hash2를 예상할 수 있어 SecParam의 값이 커질수록 해당되는 Hash2의 수는 적게 된다. 따라서 SecParam이 커질수록 CGA 주소생성 시간이 증가하게 되며, SecParam이 2이상인 경우는 장시간 알고리즘을 수행해도 결과값을 얻는다는 보장이 없으므로 네트워크에서 사용할 수는 없다.

SecParam이 0인 경우는 Hash2를 생성하기 위해 알고리즘을 한번만 수행하므로 생성시간의 차이는 시스템의 성능차이에 의해 생긴 것이다. 따라서 시스템 성능에 따라 SecParam을 조정하고 CGA 모듈을 사용해야 한다. Secure ND는 IPv6를 사용하는 PC, 서버 등의 컴퓨터이외에 네트워크기능을 탑재하고 있는 다양한 기기에서 사용될 수 있다. 이때 CGA 모듈을 실제 네트워크에 적용하기 위해서는 시스템 사양이 낮은 모바일 기기의 경우 SecParam 값을 0으로 설정해서 사용하고, 시스템 사양이 높은 PC나 서버 컴퓨터는 SecParam 값을 0이나 1로 설정해서 사용해야 한다. 만약 SecParam 값을 2이상 사용하기 위해서는 고속으로 CGA 주소생성 알고리즘을 수행할 수 있는 하드웨어를 구현하거나, CGA 주소생성 알고리즘의 수정이 필요하다.

2. SEND 모듈 시뮬레이션 및 고찰

SEND 모듈은 CGA 모듈에서 생성된 CGA 주소를

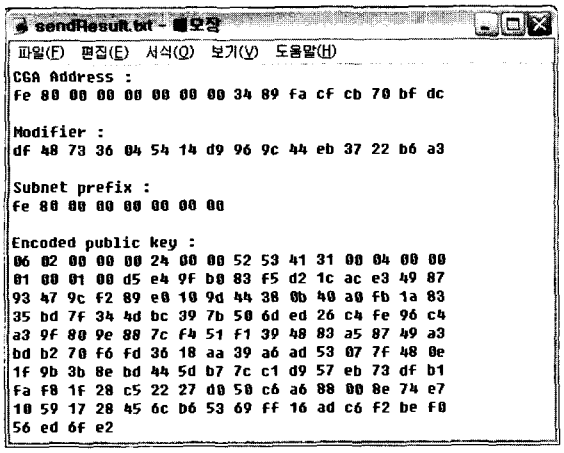

그림 4. Secure ND 메시지 전송정보
Fig. 4. Sent information of Secure ND message.

이용하여 Secure ND 메시지를 전송하는 모듈이다. CGA 주소는 SecParam을 1로 설정하여 주소를 생성하였고, Secuer ND 메시지는 모두 AH(Authentication Header)를 가지고 있어 일반 ND 메시지와 구별된다. SEND 모듈 시뮬레이션은 Secure ND 메시지를 생성하여 전송하고, CGA 주소와 CGA Parameter를 이용하여 Secure ND 메시지를 검증한다. 또한 IPv6 패킷을 모니터링 할 수 있는 Ethereal 네트워크 분석기를 이용하여 전송된 Secure ND 메시지를 캡쳐하여 정확한 IPv6 패킷인지 분석해 본다.

SEND 모듈 실험은 일반노드 시스템1에서 Secure ND 메시지 중 Router Solicitation 메시지를 전송하고, 라우터 시스템에서 Secure ND 메시지 검증 프로그램을 통해 메시지를 검증하고 Ethereal 네트워크 분석기를 통해 메시지를 캡쳐하여 패킷을 분석하였다.

그림 4는 Secure ND 메시지 전송 프로그램의 전송 정보를 저장한 파일이다. Router Solicitation 메시지를 전송할 때 생성된 CGA 주소와 CGA Parameter로 사용된 modifier, subnet prefix 그리고 공개키가 저장되어 있다. 그림 5는 Secure ND 메시지 검증 프로그램의 검증 정보를 저장한 파일이다. 패킷을 전송받은 시간과 link-layer (layer 2)의 헤더 정보가 나타나 있고, IP (layer 3)의 헤더 정보가 나타나 있다. IP 헤더는 version이 0x06으로 IPv6를 나타내고, Next header가 0x33으로 AH를 나타낸다. 목적지 주소(source address)는 그림 4의 CGA 주소와 같은 것을 확인할 수 있다. AH를 보면 Next header가 0x3A로 ICMPv6를 나타내고, SPI (Security Parameters Index)와 SN(Sequence Number)가 설정되어 있다. 또한 Authentication Data 필드에는 CGA Parameter 정보와 인증 정보가 저장된

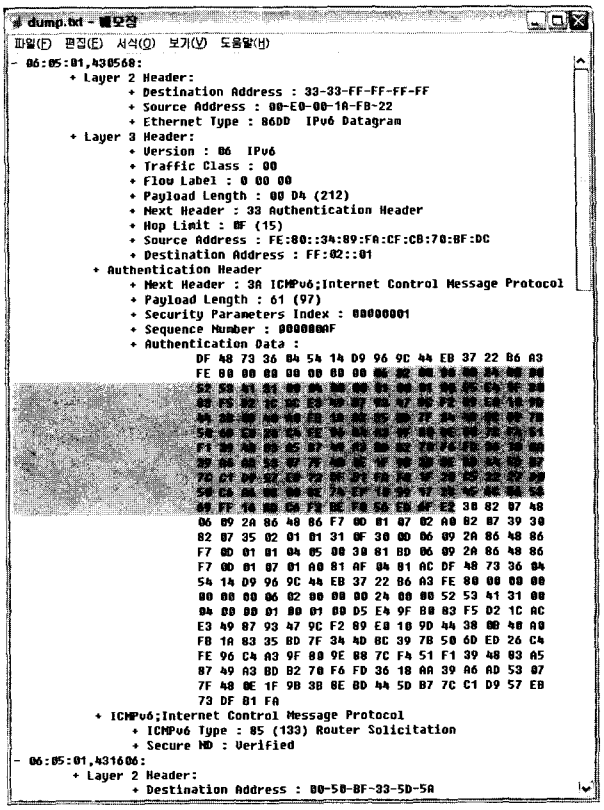

그림 5. Secure ND 메시지 검증정보
Fig. 5. Verified information of Secure ND message.

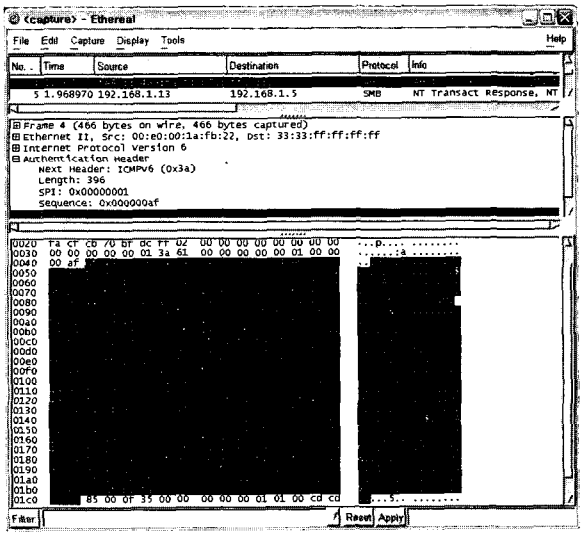

그림 6. Ethereal 모니터링 프로그램의 패킷정보
Fig. 6. Packet Infomation by Ethereal monitoring program.

다. CGA Parameter 정보를 이용해서 Secure ND 메시지를 검증하고 결과를 출력한다. AH 다음으로 ICMPv6의 정보가 나타나고, Type 필드를 통해 RS 메시지임을 확인 할 수 있다. Verified는 메시지가 보안 알고리즘에 의해 검증되었음을 나타낸다.

그림 6은 Ethereal 네트워크 모니터링 프로그램을 이

용하여 Secure ND 메시지를 캡쳐하여 분석한 것이다. 그림 5의 메시지 검증정보와 비교해 보면 동일한 내용을 담고 있다. 그림 6에서 ICV 필드는 Authentication Data 필드와 동일한 내용을 담고 있는 필드로 그림 5의 CGA Parameter와 인증 정보를 저장하고 있다. ICV 필드 다음 데이터가 0x85이므로 이는 ICMPv6의 Type을 나타내며 RS를 나타낸다. 따라서 SEND 모듈에서 생성하는 메시지는 AH와 ICMPv6를 Next Header로 갖는 IPv6 메시지의 형식과 동일하다. Secure ND 메시지는 CGA 주소와 AH의 Authentication Data 필드의 정보를 이용하여 인증을 받는다. 만약 공격자가 패킷 모니터링을 통해 CGA Parameter를 알아내더라도 암호알고리즘에 의해 서명된 인증 정보를 생성할 수 없기 때문에 공격이 불가능하게 된다.

V. 결 론

IPv6는 Neighbor Discovery(ND) 프로토콜을 사용하여 주변 노드간의 관계를 정의한다. 주변 노드를 파악하기 위해 사용되는 ND 메시지에는 네트워크에 관한 중요한 정보들이 포함되어 있다. 이러한 네트워크 정보가 유출될 경우 네트워크 공격에 노출되어 네트워크를 이용한 서비스가 마비될 수 있으며 해킹을 통해 개인의 정보가 유출될 수도 있다. 현재 ND 프로토콜은 여러 가지 보안 취약점이 발견되었으며 이를 보완하기 위한 보안기능이 요구되었다.

본 논문에서는 ND 프로토콜에 보안기능을 추가한 Secure ND 프로토콜을 CGA 모듈과 SEND 모듈로 나누어 설계 및 구현하였다. CGA 모듈은 시뮬레이션을 통해 Security parameter(SecParam) 값에 따라 CGA 주소 생성시간이 바뀌는 것을 확인하였고 시스템에 따라서 CGA 주소 생성시간이 달라지는 것을 확인하였다. 시뮬레이션 결과에 따라 CGA 모듈을 네트워크에 적용하기 위해서는 노드의 특성에 따라 SecParam 값을 조정하여 사용해야 한다. 또한 높은 보안을 적용하기 위해서는 2 이상의 SecParam 값에서 CGA 주소를 빠르게 생성할 수 있는 새로운 알고리즘이 요구된다. SEND 모듈 시뮬레이션에서 SEND 모듈이 생성하는 Secure ND 메시지가 IPv6 표준에 맞는 확장 헤더를 이용하는 것을 확인하였다. 이는 일반 ND 메시지와 Secure ND 메시지를 하나의 네트워크에서 공존시키는 것이 가능하고 AH 헤더와 인증 정보의 유무로 서로를 구분 할 수 있음을 뜻한다. SEND 모듈은 네트워크에 메시지 패킷을 송수신하기 위한 SEND driver 부분이 운영체제에 종속적으로 제작되어 Windows 계열의 운영체제에서만 동작한다. SEND 모듈을 네트워크에 적용하기 위해서는 Unix나 Linux용 SEND driver의 구현이 요구된다.

본 논문에서는 Secure ND 프로토콜을 가상의 네트워크를 구성하여 수동적인 메시지 전송방식으로 실험하였다. 앞으로 실제 네트워크에서 Secure ND 프로토콜을 사용하기 위해서는 CGA 생성 알고리즘이 보완된 CGA 모듈과 능동적인 메시지 전송이 가능한 SEND 모듈을 설계 및 구현해야 한다.

참 고 문 헌

[1] Jeff Doyle, Jennifer D. Carroll, "Routing TCP/IP volume 2", Cisco press, 2001.
[2] Joseph Davies, "Understanding IPv6", MS press, 2002.
[3] P. Nikander, J. Kempf, E. Nordmark, "IPv6 Neighbor Discovery trust models and threats", draft-ietf-send-psreq-03.txt, work in progress
[4] J. Arkko, J. Kempf, B. Sommerfeld, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)", draft-ietf-send-ipsec-01.txt, work in progress
[5] T. Aura, "Cryptographically Generated Addresses (CGA)", draft-ietf-send-cga-01.txt, work in progress
[6] S. Kent, R. Atkinson, "IP Authentication Header", RFC2402
[7] S. Kent, R. Atkinson, "IP Encapsulating Security Payload", RFC2406
[8] S. Deering, R. Hinden, "Internet Protocol, Version 6", RFC2460
[9] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP version 6", RFC2461
[10] A. Conta, S. Deering, "Internet Control Message Protocol for the Internet Protocol Version 6", RFC2463

저 자 소 개

유 재 욱(정회원)
2002년 건국대학교 전자정보통신공학과 학사 졸업.
2004년 건국대학교 전자정보통신공학과 석사 졸업.
<주관심분야: Network, 멀티미디어>

김 중 민(정회원)
2000년 경기대학교 전자공학과 학사 졸업.
2002년 건국대학교 전자정보통신공학과 석사 졸업.
2004년 건국대학교 전자정보통신공학과 박사 수료.
<주관심분야: Network, 통신>

박 인 갑(정회원)
1973년 고려대학교 전자공학과 학사 졸업.
1976년 고려대학교 전자공학과 석사 졸업.
1986년 고려대학교 전자공학과 박사 졸업.
현재 건국대학교 전자정보통신공학과 교수
<주관심분야: Network, 마이크로프로세서>