IPv6 네트워크에서 SEND 프로토콜의 구현

정회원 안 개 일*, 나 재 훈*

Implementation of SEND Protocol in IPv6 Networks

Gae-Il An*, Jae-Hoon Nah* *Regular Members*

요 약

IPv6 유무선 로컬 네트워크에서 이웃하는 호스트와 라우터를 발견하기 위한 목적으로 ND (Neighbor Discovery) 프로토콜이 제안되었다. 그러나 ND 프로토콜은 악의 있는 사용자가 프로토콜 메시지를 위조하여 정상적인 호스트나 라우터로 위장하는 것이 가능하기 때문에 네트워크 공격에 취약한 문제를 가지고 있다. ND 프로토콜을 보호하기 위한 목적으로 SEND (SEcure Neighbor Discovery) 프로토콜이 제안되었다. SEND 프로토콜은 주소 소유권 증명, 메시지 보호, 재현 공격 방지, 그리고 라우터 인증 메커니즘을 제공한다. 본 논문에서는 IPv6 네트워크상에서 핵심적으로 운용될 프로토콜중의 하나인 SEND 프로토콜을 설계 및 구현하다. 또한 본 논문에서 구현한 SEND 프로토콜을 IPv6 네트워크상에서 실험함으로써 SEND 프로토콜의 공격 방어 능력과 프로토콜의 성능을 평가하고 분석한다.

Key Words : SEND Protocol, ND Protocol, IPv6, Security, Network Attack

ABSTRACT

Neighbor Discovery (ND) protocol was proposed to discover neighboring hosts and routers in IPv6 wire/wireless local networks. ND protocol, however, has a problem that it is vulnerable to network attacks because ND protocol allows malicious users to impersonate other legitimate hosts or routers by forging ND protocol messages. To address the security problem, SEcure Neighbor Discovery (SEND) protocol was proposed. SEND protocol provides address ownership proof mechanism, ND protocol message protection mechanism, reply attack prevention mechanism, and router authentication mechanism to protect ND protocol. In this paper, we design and implement SEND protocol in IPv6 local networks. And also, we evaluate and analyze the security vulnerability and performance of SEND protocol by experimenting the implemented SEND protocol on IPv6 networks.

Ⅰ. 서 론

IPv6 유무선 네트워크에서 이웃하는 호스트와 라우터를 발견하기 위한 목적으로 ND (Neighbor Discovery) 프로토콜[1]이 제안되었다. ND 프로토콜은 IPv4 네트워크에서 ARP (Address Resolution Protocol)와 ICMPv4 (Internet Control Message Protocol version 4) 프로토콜이 담당했던 주소 변환 기능과 네트워크 관리 기능을 제공할 뿐만 아니라, IP 자동 구성 (IP auto-configuration)이라는 새로운 기능도 정의하고 있다[2,3]. IP 자동 구성은 새로운 노드가 IPv6 네트워크에 접속할 때, 다른 노드와 통신하기 위하여 기본적으로 요구되는 파라미터 (예, 자신의 IPv6 주소, 디폴트 게이트웨이 주소,

* 한국전자통신연구원 정보보호연구단 (fogone@etri.re.kr, jhnah@etri.re.kr)
논문번호 : KICS2007-05-214, 접수일자 : 2007년 5월 16일, 최종논문접수일자 : 2007년 6월 25일

DNS 서버 주소, IP 헤더에서 디폴트 홉 수 등)를 네트워크 노드 스스로가 자동 구성하는 기능이다[4]. DHCP (Dynamic Host Configuration Protocol) 프로토콜[5]의 동적 IP 주소 할당 방식에서는 DHCP 서버가 필요한 반면에, ND 프로토콜 기반의 IP 자동 구성 방식은 어떠한 IP 관리 서버도 필요 없다는 점에서 큰 매력을 갖는다[2,3]. ND 프로토콜은 고정 IP 주소를 사용하는 네트워크 환경에서보다는, 모발 네트워크에서와 같이 유동 IP 주소를 사용하는 환경을 목표로 설계되었다.

이와 같이, ND 프로토콜은 IPv6 네트워크 서비스를 제공할 때 없어서는 안될 매우 중요한 기본 프로토콜중의 하나이지만, 보안에 매우 취약한 문제가 있다. IETF (Internet Engineering Task Force) 표준 기구에서는 ND 프로토콜의 보안 취약성 문제를 해결하기 위하여 SEND (SEcure Neighbor Discovery) 프로토콜[6,7]을 제안하였다. SEND 프로토콜은 CGA (Cryptographically Generated Address) 기반의 주소 소유권 증명, 시그니처 기반의 이웃 발견 프로토콜 메시지 보호, 타임스탬프 (Timestamp)와 넌스 (Nonce) 기반의 재현 공격 방지, 그리고 인증서 기반의 라우터 인증 메커니즘을 통하여 ND 프로토콜을 보호한다. 본 논문에서는 IPv6 네트워크 상에서 핵심적으로 운용될 프로토콜중의 하나인 SEND 프로토콜을 설계 및 구현하고 또한 실험을 통하여 SEND 프로토콜의 보안 취약성과 이웃 발견 프로토콜의 성능을 평가하고 분석하는 것을 목적으로 한다.

본 논문의 차례는 다음과 같다. 먼저 Ⅱ장에서는 ND 프로토콜을 간단히 살펴보고 Ⅲ장에서는 SEND 프로토콜의 설계 및 구현에 대해 설명한다. Ⅳ장에서는 실험을 통하여 SEND 프로토콜의 성능을 분석하고, 마지막으로 Ⅴ장에서 결론을 맺는다.

Ⅱ. ND 프로토콜의 분석

2.1. ND 프로토콜의 개요

ND 프로토콜[1]의 가장 중요한 기능중의 하나는 IPv6 호스트가 인터넷이나 로컬링크상에 있는 다른 호스트와 통신하는 데 필요한 파라미터들을 스스로 설정할 수 있는 IP 자동 구성을 제공하는 것이다. ND 프로토콜이 제공하는 주요 기능은 다음과 같다.

- 라우터 탐색 기능: IPv6 호스트가 인접하는 라우터를 탐색할 수 있는 기능.
- IP 주소 자동 구성 기능: IPv6 호스트가 네트워크 접속에 필요한 IP 구성정보를 자동구성하는 기능.
- 중복 주소 탐지 기능: IPv6 호스트에서 생성한 임시 IPv6 주소가 다른 노드에 의해 이미 사용되고 있는 중복된 주소인지를 탐지하는 기능.
- 프로토콜 주소 변환 기능: IPv6 주소에 대응하는 링크 계층 주소를 제공하는 기능.
- 이웃 도달성 탐지: 특정 IPv6 호스트 및 라우터에 대한 도달성 여부를 탐지하는 기능.
- 리다이렉션 기능: IPv6 라우터가 호스트에게 더 좋은 라우팅 경로가 있다는 것을 알려주는 기능.

IP 주소 자동 구성 기능은 State-full 및 Stateless 메커니즘으로 구현될 수 있다. State-full 메커니즘에서는 IPv6 호스트가 IPv6 주소를 관리하는 DHCPv6 서버에 직접 접속하여 IPv6 주소를 할당받지만, Stateless 메커니즘은 어떠한 서버의 도움 없이 호스트 스스로가 IPv6 주소를 설정하는 방식이다. Stateless 메커니즘을 따르는 호스트는 먼저 임시 IPv6 주소를 생성하고, 그 주소가 다른 노드에 의해 사용되고 있지 않다는 것을 확인한 후에 그 주소를 사용한다. ND 프로토콜은 Stateless 메커니즘을 지원하는 프로토콜이다.

ND 프로토콜은 IPv6 패킷의 "Next Header" (ND=58)에 의하여 식별되며, ND 프로토콜의 모든 기능은 NS (Neighbor Solicitation), NA (Neighbor Advertisement), RS (Router Solicitation), RA (Router Advertisement), Redirect 메시지를 통하여 제공된다. NS 메시지는 이웃하는 노드들에게 특정 IP 주소에 대한 링크 계층 주소를 질의할 때 사용되며, NA 메시지는 NS 메시지를 응답할 때 사용된다. NS 와 NA 메시지는 IP 주소 자동 구성, 중복 주소 탐지, 프로토콜 주소 변환, 그리고 이웃 도달성 탐지 기능을 제공한다. RS 메시지는 이웃하는 라우터에게 로컬 네트워크에 대한 정보(예, DNS 서버의 IP 주소 등)를 질의할 때 사용되고, RA 메시지는 RS 메시지를 응답할 때 사용된다. RS와 RA 메시지는 라우터 탐색과 IP 주소 자동 구성 기능을 제공한다. Redirect 메시지는 리다이렉션 기능을 제공하기 위하여 정의되었다.

ND 프로토콜에서, 새로운 네트워크 노드가 IPv6 네트워크에 접속할 때 자신의 IP를 자동 구성하는 전형적인 시나리오는 다음과 같다.

(1) 임시 IPv6 링크 로컬 주소 생성: IPv6 노드는 자신의 네트워크 인터페이스 식별자를 사용하여 임시 IPv6 링크 로컬 주소를 생성한다.
(2) 중복 주소 탐지 기능 실행: 다른 노드들이 그 임시 IPv6 주소를 이미 사용하고 있는지를 확인하는 과정이다. 임시 IPv6 주소를 포함하는 NS 메시지를 네트워크상에 브로드캐스트하고, 만약 다른 노드들로부터 응답이 없으면 그 임시 IPv6 주소를 자신의 IPv6 링크 로컬 주소로 사용한다.
(3) 디폴트 라우터 탐지: IPv6 노드는 자신의 디폴트 라우터를 찾기 위하여 RS 메시지를 네트워크상에 브로드캐스트한다. RS 메시지를 받은 라우터는 로컬 네트워크에 대한 IP 구성 정보를 응답하다.
(4) IP 구성 정보 설정: IPv6 노드는 수신한 IP 구성 정보를 자신의 노드에 설정한다.

2.2. ND 프로토콜의 보안 취약성

악의 있는 사용자는 ND 프로토콜 메시지를 위조하고 합법적인 호스트 또는 라우터로 위장할 수 있기 때문에, ND 프로토콜은 보안에 매우 취약한 문제를 가지고 있다[8][9][10].

그림 1은 ND 프로토콜이 가지고 있는 보안 취약성의 예를 보여주고 있다. ND 프로토콜 공격자는 그림 1-(a)에서 도시된 바와 같이 NA 메시지를 위조함으로써 정상 호스트인 Host A로 위장할 수 있으며, 따라서 victim 노드가 Host A와 통신할 수 없도록 하는 서비스 거부 공격[11]이나 또는 victim 노드가 공격자 노드와 통신하게 함으로써 victim 노드를 해킹하는 공격이 가능하다. 공격자는 또한 그림 1-(b)에서와 같이 RA 메시지를 위조함으로써 라우터로 위장할 수 있으며, 따라서 victim 노드에게 잘못된 IP 구성정보를 제공함으로써 다른 시스템과의

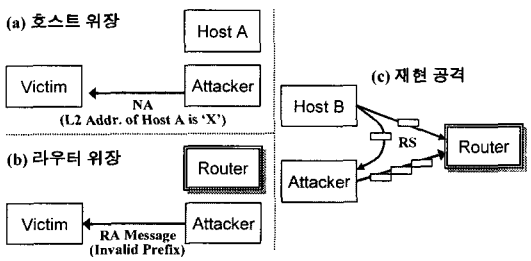


그림 1. ND 프로토콜에서 보안 취약성
Fig. 1. Security vulnerability in ND protocol

네트워크 통신을 방해할 수도 있다. 또 다른 보안 취약성 예로써, 공격자는 정상 호스트의 ND 프로토콜 메시지를 가로채 그 메시지를 목적지 시스템에게 계속 전송하는 재현 공격을 실행함으로써 서비스 거부 공격을 일으킬 수 있다. 그림 1-(C)는 재현 공격의 한 예로써, 공격자는 Host B가 전송한 RS 메시지를 복사한 후 라우터에게 그 메시지를 계속 전송함으로써 라우터에 대한 서비스 거부 공격을 일으키고 있다.

Ⅲ. SEND 프로토콜의 설계 및 구현

3.1. SEND 프로토콜

SEND (SEcure Neighbor Discovery) 프로토콜[6][7]은 ND 프로토콜을 보호하기 위하여 제안되었다. SEND 프로토콜은 ND 프로토콜 메시지와는 별도로 2개의 메시지와 몇 개의 메시지 옵션을 추가로 정의하고 있다. SEND 프로토콜은 주소 소유권 증명 메커니즘, ND 프로토콜 메시지 보호 메커니즘, 재현 공격 방지 메커니즘, 그리고 라우터의 권한 인증 메커니즘을 제공한다. 주소 소유권 증명 메커니즘과 ND 프로토콜 메시지 보호 메커니즘은 이전 장에서 소개한 호스트 위장 공격을 막기 위하여 제안되었고, 재현 공격 방지 메커니즘과 라우터 권한 인증 메커니즘은 각각 재현 공격과 라우터 위장 공격을 방지하기 위하여 제안되었다.

먼저, 주소 소유권 증명 메커니즘은 송신 노드가 ND 메시지의 IP 주소가 자신의 IP 주소라는 것을 수신 노드에게 증명하는 메커니즘으로써, 공격 노드가 다른 노드의 IP 주소를 가장하여 ND 프로토콜 메시지를 위조하는 것을 방지한다. 이를 위하여 SEND 프로토콜은 CGA (Cryptographically Generated Address)란 IPv6 주소를 정의하며, SEND 프로토콜을 지원하는 노드는 자신의 공개키와 개인키를 가지고 있어야 한다. CGA 주소는 IPv6 주소 체계와 마찬가지로 64비트의 Subnet Prefix와 64비트의 Interface ID로 구성되지만, Interface ID 부분은 다음과 같이 공개키와 여러 개의 파라미터(즉, Modifier, Subnet Prefix, Collision Count)들을 해쉬한 결과 값으로 생성된다.

CGA= ***concatenation*** (SubnetPrefix, InterfaceID)
IntefaceID= ***hash*** (PublicKey, Parameters)

송신 노드는 주소 소유권 증명에 필요한 자신의

공개키와 파라미터들을 송신 메시지의 CGA 메시지 옵션 부분에 포함시키고, 수신 노드는 그 CGA 메시지 옵션에 포함된 공개키와 파라미터들을 사용하여 송신 노드의 CGA 주소를 계산한다. 계산된 CGA 주소가 SEND 메시지의 송신 IPv6 주소와 서로 일치하지 않으면, 수신 노드는 SEND 메시지의 송신자 IP 주소가 위조되었다고 결정한다. 공격 노드가 다른 노드의 IP 주소를 도용하기 위해서는 그 노드의 공개키를 알아야 하는데, IP 주소로부터 공개키를 유추하는 것은 사실상 거의 불가능하다. 따라서 CGA 기법은 IP 주소 도용 문제를 효과적으로 해결할 수 있다.

공격 노드는 네트워크상에서 전송되고 있는 SEND 프로토콜 메시지를 캡쳐하고 수정함으로써 다른 노드의 공개키를 도용하거나 또는 SEND 메시지를 위조할 수도 있다. 이러한 문제를 해결하기 위하여, SEND 프로토콜은 ND 프로토콜 메시지 보호 메커니즘을 제공한다. 이 메커니즘은 ND 프로토콜 메시지 무결성과 송신자의 인증을 제공하기 위하여 공개키 기반의 디지털서명 기법인 RSA 시그니처를 사용한다. 송신 노드는 메시지의 송신 IP, 수신 IP, 그리고 ND 메시지를 자신의 개인키로 암호화하여 디지털 시그니처를 생성한 후 이것을 메시지에 포함시켜 전송한다. 수신 노드는 CGA 메시지 옵션에 있는 송신 노드의 공개키를 사용하여 전달된 디지털 시그니처를 복호함으로써 ND 프로토콜 메시지 무결성과 송신자 인증을 확인한다. SEND 프로토콜은 디지털 시그니처를 전송하기 위한 메시지 형식으로써 RSA 시그니처 옵션을 정의하고 있다.

세 번째로, SEND 프로토콜에서는 재현 공격 방지 메커니즘으로써 타임스탬프(Timestamp)와 난스(Nonce) 옵션을 정의하고 있다. 타임스탬프는 Redirect 메시지와 같은 광고형 메시지에 사용되며, 난스는 무작위로 생성된 값으로써 요구/응답형 메시지에 사용된다. SEND 송신 노드는 광고형 메시지를 전송할 때마다 현재의 타임스탬프 값을 그 메시지에 포함시킨다. 수신 노드는 수신한 메시지에 포함된 타임스탬프 값과 현재 시간과의 차이가 임계치 값 이상이면 재현 공격으로 판단하여 그 메시지를 폐기한다. 난스를 포함하는 요구 메시지를 받은 노드는 응답 메시지에 그 난스를 복사하여 응답해야 한다. 그 응답 메시지를 받은 노드는 자신이 보낸 요구 메시지의 난스값과 수신한 응답 메시지의 난스값이 서로 일치하지 않으면 그 응답 메시지를 재현 공격에 사용된 메시지로 간주한다.

마지막으로, 라우터의 권한 인증 메커니즘은 라우터라고 주장하는 노드가 정말로 라우터 권한을 가지고 있는지를 확인하는 메커니즘이다. 라우터는 자신이 권한이 있음을 증명하기 위해서 신뢰 앵커(Trust Anchor)로부터 권한을 위임 받았음을 증명하는 인증서(Certificate)와 그 신뢰 앵커로부터의 인증 경로(Certification Path) 정보를 호스트들에게 제공한다. 호스트는 자신이 신뢰하는 신뢰 앵커와 라우터로부터 받은 인증서 및 인증 경로를 검사함으로써 라우터의 권한 유무를 확인할 수 있다. SEND 프로토콜은 호스트가 라우터에게 인증서와 인증 경로를 요구하기 위한 메시지로써 CPS (Certification Path Solicitation) 메시지를, 그리고 라우터가 그 요구를 응답할 때 사용하는 메시지로써 CPA (Certification Path Advertisement) 메시지를 정의하고 있다.

3.2. SEND 프로토콜을 위한 구조 설계

본 논문에서는 SEND 프로토콜을 구현하기 위하여 그림 2에서 도시된 IPv6 시스템 구조를 제안한다. 그림 2에서 IPv6 모듈은 ICMPv6와 ND 프로토콜을 포함하고 있으며, 기존 커널에 이미 구현되어 있는 모듈이다.

본 논문에서 제안하는 구조는 SEND 프로토콜 기능을 직접 수행하는 SEND 모듈과 SEND 모듈이 동작하는데 필요한 정보를 설정하고 SEND 모듈의 상태정보를 관리하는 SEND GUI로 구성된다. SEND 모듈은 커널 공간에서, SEND GUI는 응용 공간에서 각각 동작한다. SEND GUI와 SEND 모듈은 문자 디바이스를 사용하여 서로 통신한다. 사용자는 SEND GUI 통하여 IPv6 시스템을 ND 프로토콜만을 사용하는 ND 모드로 설정할지 또는 SEND 프로토콜을 사용하는 SEND 모드로 설정할지를 결정

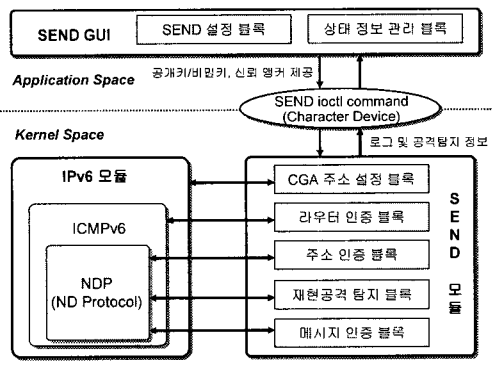


그림 2. SEND 프로토콜을 위한 IPv6 시스템의 구조
Fig. 2. Architecture of IPv6 system for SEND protocol

할 수 있다. 본 논문에서 제안하는 구조는 SEND 프로토콜의 기능을 하나의 독립적인 SEND 모듈로 설계함으로써 이식성이 뛰어나고 수정과 확장이 용이한 장점을 가지고 있다. 또한 SEND GUI를 제공함으로써, 사용자는 쉽게 SEND 프로토콜을 제어하고 현재의 보안 상태를 확인할 수 있다.

SEND 모듈은 모두 5개의 블록으로 구성되며 다음과 같은 기능을 제공한다.

- CGA 주소 설정 블록: SEND 모드로 동작할 시에 IPv6 모듈의 호출을 받아 CGA 주소 기반의 IPv6 링크 로컬 주소를 생성하는 기능을 담당함.
- 라우터 인증 블록: 라우터를 인증하기 위하여 CPS와 CPA 메시지를 생성하고 검증하는 블록임. CPS와 CPA 메시지는 ICMPv6 메시지에 해당하기 때문에 IPv6/ICMPv6 모듈과 상호 동작함.
- 주소 인증 블록: SEND 프로토콜 메시지의 CGA 메시지 옵션을 생성하고 처리하는 블록으로써 IPv6/ICMPv6/NDP 모듈과 상호 동작함.
- 재현공격 탐지 블록: 타임스탬프와 넌스 메시지 옵션을 생성하고 검증함. IPv6/ICMPv6/NDP 모듈과 상호 동작함.
- 메시지 인증 블록: RSA 시그니처 메시지 옵션을 생성하고 검증함. IPv6/ICMPv6/NDP 모듈과 상호 동작함.

SEND GUI는 모두 2개의 블록으로 구성되며 다음과 같은 기능을 담당한다.

- SEND 설정 블록: SEND 모듈이 동작하는데 필요한 공개키/비밀키 및 신뢰앵커를 설정하는 GUI.
- 상태정보관리 블록: SEND 모듈의 로그 정보 및 공격 탐지 정보를 출력하는 GUI.

SEND 모듈에서 SEND 송신 메시지를 생성하는 알고리즘은 그림 3에 도시되어 있다. SEND 모듈은 초기에 공개키/개인키를 생성하고, 그 공개키를 기반으로 하여 CGA 주소를 생성한다. 생성된 CGA 주소는 임시 IPv6 링크로컬 주소로 사용된다. IPv6 모듈은 새로운 ND 프로토콜 메시지가 생성될 때마다 SEND 모듈을 호출한다. SEND 모듈은 CGA 옵션, 타임스탬프와 넌스 옵션, 그리고 RSA 시그니처 옵션 메시지를 생성하여 ND 프로토콜 메시지에 추가한 후 IPv6 모듈로 실행 제어권을 넘긴다.

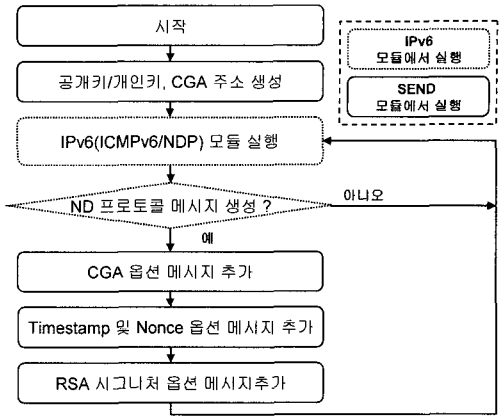


그림 3. SEND 메시지 생성 알고리즘
Fig. 3. Algorithm for SEND message generation in a sender system

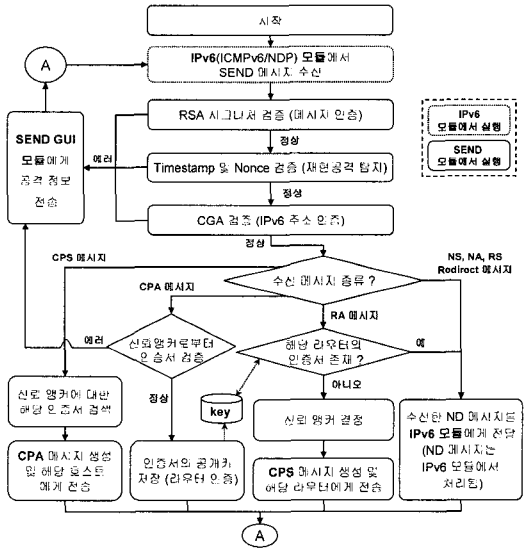


그림 4. 수신한 SEND 메시지의 처리 알고리즘
Fig. 4. Algorithm for SEND message processing in a receiver system

SEND 모듈에서의 SEND 수신 메시지 처리 알고리즘은 그림 4에 도시되어 있다. IPv6 모듈은 ND 프로토콜 메시지를 수신할 때마다 SEND 모듈을 호출한다. SEND 모듈은 수신한 SEND 메시지의 RSA 시그니처, 타임스탬프, 넌스, 그리고 CGA 주소를 각각 검증하며, 그 과정에서 에러가 발견되면 SEND GUI 모듈에게 그 에러 정보 (즉, 공격 정보)를 전송한다. 만약 수신한 메시지가 CPS 면, SEND 모듈은 그 메시지에 담긴 신뢰 앵커에 해당하는 인증서를 검색하여 CPA 메시지를 생성한 후

응답한다. CPS 메시지는 라우터에서 처리된다. 만약 CPA 메시지를 수신하면, SEND 모듈은 자신의 신뢰앵커를 사용하여 CPA 메시지에 포함된 라우터의 인증서를 검증하고 그 인증서의 공개키를 저장소에 저장한다. 만약 RA 메시지를 수신하면, 송신 라우터의 인증서(공개키)를 사용하여 메시지를 검증한다. 만약 송신 라우터에 대한 인증서가 존재하지 않으면, 호스트가 신뢰하는 신뢰앵커를 담은 CPS 메시지를 생성하여 송신 라우터에게 전송한다. 마지막으로, 수신한 메시지가 ND 프로토콜 메시지(즉, NS, NA, RS, RA, Redirect)이면, IPv6 모듈이 그 메시지를 처리할 수 있도록 IPv6 모듈에게 전달한다.

3.3. 구현 환경

본 논문에서는 리눅스 커널 2.4.20 버전에서 컴파일 버전 GCC 3.2.2를 사용하여 SEND 프로토콜을 구현하였다. SEND 모듈과 SEND GUI는 모두 C 언어로 구현되었다. SEND 모듈은 SEND 프로토콜에서 정의된 네 가지 보안 메커니즘 모두를 제공한다. SEND 모듈에서 RSA 시그니처 생성 및 검증은 공개 라이브러리인 OpenSSL을 사용하였고, SEND GUI는 GTK+2.0을 사용하여 그래픽 사용자 인터페이스를 구현하였다.

Ⅳ. SEND 프로토콜의 성능 분석

4.1. IP 자동구성 방해공격의 방어능력 실험

본 논문에서는 그림 5에서 도시된 IPv6 실험 네트워크상에서 IP 자동구성 방해공격을 실험함으로써 SEND 프로토콜의 성능을 분석한다.

그림 5에서 호스트 A는 IP 자동 구성을 실행하며, 공격 시스템은 IP 자동 구성을 방해하는 공격을 수행한다. 호스트 A의 IP 자동 구성 시나리오는 다음과 같다. 먼저, 호스트 A는 CGA 기반의 임시 IPv6 링크로컬주소 (즉, fe80::92e:90dc:93c7:e21)를 생성한다 (그림 5의 1번). 그리고 그 임시 주소가 다른 시스템에 의하여 이미 사용되고 있는지를 확인하기 위하여, 그 임시 주소를 포함하는 NS 메시지를 IPv6 랜상에 브로드캐스트한다 (그림 5의 2번). 주어진 시간 동안 송신한 NS 메시지에 대한 응답이 없으면, 그 임시 주소를 IPv6 링크로컬주소로 사용한다. 그리고, IPv6 호스트 A는 IPv6의 네트워크 프리픽스 주소 등 IP 구성 정보를 라우터로부터 얻기 위하여 RS 메시지를 브로드캐스트한다 (그림 5의 3번). RS 메시지에 대응하는 RA 메시지

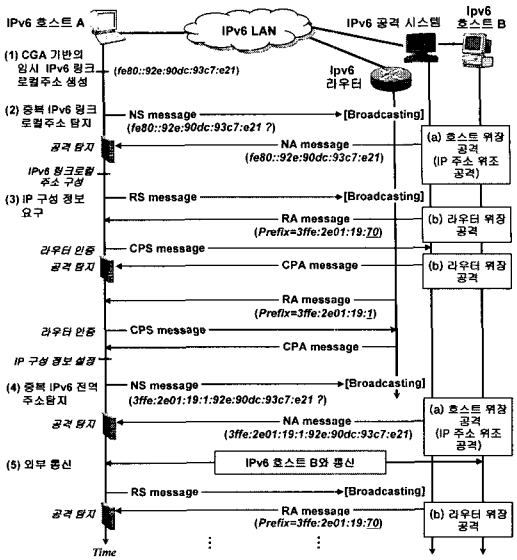


그림 5. IPv6 실험 네트워크와 IP 자동구성 공격 시나리오
Fig. 5. IPv6 experimental networks and attack scenario against IP auto-configuration

를 라우터로부터 수신하면, 호스트 A는 RA 메시지에 담겨있는 네트워크 프리픽스 주소 (즉, 3ffe:2e01:19:1)를 사용하여 임시 IPv6 전역 주소 (즉, 3ffe:2e01:19:1:92e:90dc:93c7:e21)를 생성한다. 그리고 그 주소가 다른 시스템에 의하여 이미 사용되고 있는지를 확인하기 위하여, 중복 주소 탐지(그림 5의 4번)를 실행한다. 다른 노드가 그 주소를 사용하고 있지 않으면, 그 임시 주소를 IPv6 전역주소로 사용한다. 마지막으로, 호스트 A는 IP 자동 구성이 성공적인지를 확인하기 위하여 다른 네트워크에 있는 IPV6 호스트 B와 통신한다 (그림 5의 5번).

그림 6은 공격 시스템에 구현된 ND 프로토콜 공격을 위한 GUI이다. 본 논문에서 구현된 공격 시스템은 중복 주소 탐지를 방해하는 DAD (Duplicate Address Detection) 방해 공격과 라우터 위장 공격을 실행할 수 있다. DAD 방해 공격은 네트워크상의 모든 NS 메시지를 캡처한 후, 그 NS 메시지에 담긴 IPv6 주소를 사용하여 위조된 NA 메시지를 생성하고 그 NS 메시지를 생성한 호스트에게 응답함으로써 정상 IPv6 호스트가 임시 링크로컬 주소 및 전역 주소를 사용하지 못하게 하는 공격이다. 라우터 위장 공격은 IPv6 호스트들에게 위조된 RA 메시지를 전송함으로써 IPv6 호스트들에게 잘못된 IP 구성 정보를 제공하는 공격이다. 본 실험에서 공격 시스템은 5초 마다 위조된 RA 메시지(거짓 프리픽스= 3ffe:2e01:19:70)를 브로드캐스팅한다.

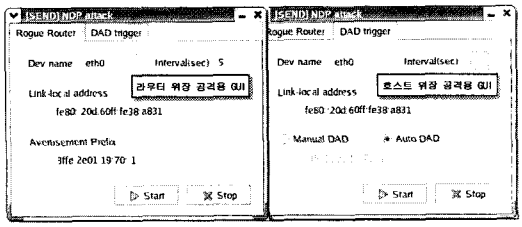


그림 6. IPv6 공격시스템에 구현된 GUI
Fig. 6. GUI implemented in IPv6 attack systems

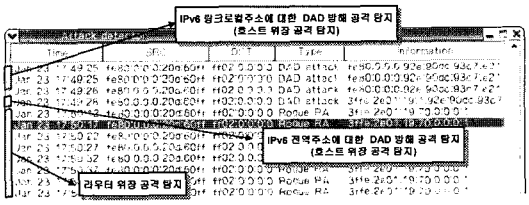


그림 7. IP 자동구성 방해공격의 탐지
Fig. 7. Detection of attacks against IP auto-configuration

본 논문에서는 ND와 SEND, 각 두 프로토콜에 대하여 IP 자동구성 방해공격을 실행하였다. ND 프로토콜은 DAD 방해 공격 및 라우터 위장 공격에 매우 취약하여 정상적인 IPv6 주소를 생성하지 못하였다. 그러나 SEND 프로토콜은 CGA 주소 검증과 RSA 시그니처 검증을 통하여 DAD 방해 공격 및 라우터 위장 공격을 정확하게 탐지하고 방어하는 것을 실험을 통하여 확인하였다. 그림 7은 공격 시스템의 IP 자동 구성 방해 공격을 호스트 A가 탐지한 결과를 도시한 SEND GUI 이다.

4.2. 이웃 발견 처리 성능 분석 실험

SEND 프로토콜의 처리 성능에 대한 실험 결과는 그림 8에 도시되어있다. 본 실험의 목적은 이웃 발견 수행 시 SEND 프로토콜이 어느 정도의 부하를 유발하는지를 알아보기 위함이다. 이웃 발견 메시지를 처리하는 평균 시간에서 ICMPv4와 ND 프로토콜은 각각 0.29, 0.34 (ms)로써 서로 성능에서 큰 차이가 없었다. 그러나 SEND 프로토콜은 75.97 (ms)로써 이웃 발견 메시지를 처리하는 데에 많은 시간이 걸리는 문제가 있음을 확인하였다. SEND 프로토콜의 성능이 좋지 않은 이유는 RSA 시그니처의 처리 시간 때문이었다. 그림 9-(b)에 도시된 바와 같이, SEND 프로토콜 중에서 CGA, 타임스탬프, 넌스 메시지를 처리하는 시간은 총 SEND 메시지 처리 시간의 0.6 % 정도로 매우 작았다. 그러나 RSA 시그니처는 99.4%로써 SEND 메시지 처리 부하의 대부분을 차지하였다.

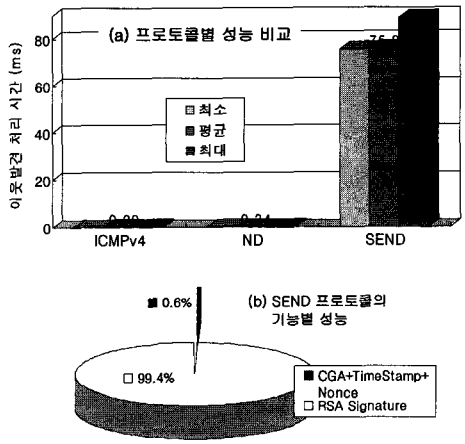


그림 8. SEND 프로토콜의 성능
Fig. 8. Performance of SEND protocol

4.3. SEND 프로토콜의 운용상 문제점 분석

SEND 프로토콜은 ND 프로토콜의 보안 취약성 문제를 해결할 수 있었지만, 다음과 같은 몇 가지 문제점을 가지고 있다.

(1) 시간 동기화 문제 -- SEND 프로토콜의 실험에서 정상 SEND 메시지가 종종 공격 메시지로 오인되는 경우가 발생했었다. 그 원인은 타임스탬프 에러였다. 즉, SEND 프로토콜을 사용하는 IPv6 시스템들간 시간 동기가 정확히 일치하지 않아서, 수신 노드가 전송 받은 정상적인 타임스탬프 값을 임계치 값을 넘긴 타임스탬프로 잘못 해석했기 때문이다. 이 문제에 대한 해결 방안은 쉽지 않을 것 같다. 새로운 호스트는 처음에 합법적인 IPv6 주소를 갖고 있지 않기 때문에 네트워크 시간을 제공하는 NTP (Network Time Protocol) 서버와 접속할 수 없기 때문이다.

(2) 서비스 거부 공격에 취약 – 본 논문에서 수행한 성능 분석 실험을 통해서 확인했듯이, SEND 프로토콜은 ND 메시지 보다 약 200 배 이상의 메시지 처리 시간을 요구한다. 이것은 SEND 프로토콜이 ND 프로토콜보다 서비스 거부 공격에 오히려 더 취약할 수 있다는 것을 의미한다.

(3) 출발지 IP 속임 공격 탐지의 한계 – SEND 프로토콜은 정상 호스트의 IP를 도용하는 공격은 탐지할 수 있지만, 일반적인 IP 주소 속임 공격은 탐지할 수 없는 한계를 갖는다. 이것은 CGA 주소기반의 IP 주소를 생성하는데 필요한 공개키와 개인키를 공격자가 인위적으로 생성하는 것이 가능하기 때문이다.

V. 결 론

본 논문에서는 ND 프로토콜을 보호하기 위하여 제안된 SEND 프로토콜을 설계하고 구현하였다. 본 논문에서는 SEND 프로토콜의 기능을 하나의 독립적인 SEND 모듈로 설계하였기 때문에 이식성이 뛰어나고 수정과 확장이 용이하다. 또한 SEND GUI를 제공함으로써 사용자는 쉽게 SEND 프로토콜을 제어하고 현재의 보안 상태를 확인할 수 있다. 아울러, 본 논문에서는 SEND 프로토콜의 공격 탐지 능력과 프로토콜 성능을 실험하였다. SEND 프로토콜은 ND 프로토콜에서 취약한 네트워크 공격을 효과적으로 방어할 수 있는 능력은 가졌지만, SEND 프로토콜 메시지의 처리 성능이 RSA 시그니처 처리 부하로 인해 ND 프로토콜의 성능을 크게 떨어지는 문제가 있음을 확인하였다. SEND 프로토콜은 비록 ND 프로토콜에서 나타나는 보안 취약성 문제를 어느 정도 해결은 하였지만, SEND 프로토콜이 실 세계에서 안전하게 사용되기 위해서는 시간 동기화 문제와 더불어 서비스 거부 공격과 출발지 IP 속임 공격을 완화시킬 수 있는 메커니즘을 좀 더 보완하고 연구할 필요가 있다고 사료된다. 본 논문에서 제기한 이슈들을 연구하는 것은 향후 과제로써 남긴다.

참 고 문 헌

[1] T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," IETF, RFC 2461, 1998

[2] S. Hagen, "IPv6 Essentials," O'Reilly, the second edition, 2006

[3] A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," IETF, RFC 2463, 1998

[4] Y. Tseng, J. Jiang, J. Lee, "Secure Bootstrapping and Routing in an IPv6-Based Ad Hoc Network.," Proc. of ICPP Workshops, pp. 375-383, 2003

[5] R. Droms, J. Bound, B. Volz, T. Lemon, C. E. Perkins, "Dynamic Host Configuration Protocol for IPv6 (DHCPV6)", IETF, RFC 3315, 2003.

[6] J. Arkko, J. Kempf, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)," IETF, RFC 3971, 2005

[7] J. Arkko, T. Aura, J. Kempf, V. Mantyla, P. Nikander, M. Roe, "Securing IPv6 Neighbor and Router Discovery," Proc. of the 3rd ACM workshop on Wireless security, pp. 77-86, 2002

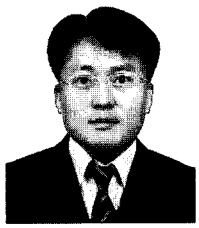
[8] P. Nikander, J. Kempf, E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats," IETF, RFC 3756, 2004

[9] P. Mutaf, C. Castelluccia, "Compact Neighbor Discovery: a Bandwidth Defense through Bandwidth Optimization," Proc. of INFOCOM, Vol. 4, pp. 2711-2719, 2005

[10] 김지홍, 나재훈, "IP 스푸핑 방지를 위한 수정된 IPv6 NDP 메커니즘," 정보보호학회논문지, 16권, 2호, pp. 95-103, 2006

[11] X. Geng, A. B. Whinston, "Defeating Distributed Denial of Service Attacks," IT Pro, pp. 36-41, 2000

안 개 일 (Gae-Il An) 정회원



1993년 2월 충남대학교 컴퓨터공학과 졸업

1995년 2월 충남대학교 컴퓨터공학과 석사

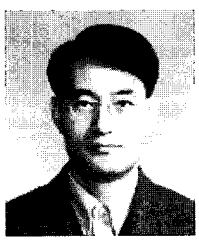
2001년 8월 충남대학교 컴퓨터공학과 박사

2006년 7월~2007년 6월 미국 시라큐스대학교 포닥연구원

2001년 8월~현재 한국전자통신연구원 선임연구원

<관심분야> 컴퓨터 네트워크, 네트워크 보안, 트래픽 엔지니어링, 네트워크 시뮬레이션

나 재 훈 (Jae-Hoon Nah) 정회원



1985년 2월 중앙대학교 컴퓨터공학과 졸업

1987년 2월 중앙대학교 컴퓨터공학과 석사

2005년 2월 한국외국어대학교 전자정보공학과 박사

1987년 2월~현재 한국전자통신연구원 P2P 보안연구팀 팀장

<관심분야> 네트워크 보안, IPv6/MIPv6 보안, P2P 보안