情報保護學會論文誌
第16卷 第2號, 2006. 4

IP 스푸핑 방지를 위한 수정된 IPv6 NDP 메커니즘

김 지 홍[1†‡], 나 재 훈[2]
세명대학교[1], 한국전자통신연구원[2]

The Modified IPv6 NDP Mechanism for Preventing IP Spoofing

Ji Hong Kim[1†‡], Jae Hoon Nah[2]
Semyung University[1], Electronics and Telecommunications Research Institute[2]

요 약

IPv6는 IPv4의 문제점을 해결하기 위해 설계된 새로운 인터넷 프로토콜이다. IPv4에서 IPv6로 새롭게 변경된 부분 중, 주소자동설정기능에 대해 살펴본다. IPv6에서는 NDP 메커니즘을 이용하여 네트워크 정보를 수집하여 주소를 설정한다. 현재의 표준안에는 NDP 프로토콜에 대한 보안방안으로 IPsec AH 메시지를 사용할 것으로 정의되어있으나, 초기 주소설정과정에서는 주소가 없는 상태이므로 어떠한 보안연계도 적용할 수 없다. 이외에도 현재 NDP 프로토콜에서의 많은 보안문제점이 지적되고 있으며, 이러한 문제를 해결하기 위하여 SEND 프로토콜이 제안되었다.

본 논문에서는 NDP와 SEND 프로토콜상의 보안문제점을 분석하고, 이러한 공격에 대한 근본적인 문제점에 해당되는 IP 스푸핑 공격을 방지하기 위한 방안으로서, PKC와 AC 방식을 이용한 수정된 NDP 프로토콜을 제안한다.

ABSTRACT

IPv6 is a new version of the Internet protocol, designed as the successor to IPv4. Among the changes from IPv4 to IPv6, we focused on the stateless address auto-configuration mechanism. The address auto-configuration mechanism is used by nodes in an IPv6 network to learn the local topology. The current specifications suggest that IPsec AH may be used to secure the mechanism, but there is no security association during address auto-configuration process because it has no initial IP address. As there are so many security threats, SEND protocol was designed to counter these threats.

In this paper we analyzed the security problems in NDP and SEND protocol. So we proposed the Modified NDP mechanism using PKC and AC in order to solve these problems.

Keywords : *IPv6, NDP, CGA, SEND, PKC, AC*

Ⅰ. 서 론

IPv6[1] 는 기존의 IPv4의 주소 고갈문제와 보안문제를 해결하기 위하여 제안된 네트워크계층의 프로토콜이다. IPv6의 보안문제점은 노드의 이동성을 지원하기 위한 Mobile IPv6 분야로 확장되면서, 많은 문제점이 제기되고 있다.

현재 이러한 IPv6 분야의 전반적인 보안상의 문제를 해결하기 위한 방안으로는 크게 인프라기반(infrastructure)의 문제 해결방안과 비인프라기반(infrastructureless)의 문제 해결방안의 두 가지 연구 흐름으로 구분된다. 인프라기반의 문제 해결방안으로는 부트스트랩시에 사용자의 credential과 EAP 프로토콜을 적용하는 diameter 방식의 AAA (Authentication, Authorization, and Accounting) 서버 방식에 대한 연구가 활발히 진행되고

접수일: 2005년 12월 13일; 채택일: 2006년 3월 31일
† ‡ 주저자, 교신저자 : jhkim@semyung.ac.kr

있다. 비인프라기반의 문제 해결방안으로 NDP (Neighbor Discovery Protocol)의 문제점을 보완하기 위하여, CGA(Cryptographic Generated Address) 주소와 RSA 디지털 서명문 및 라우터 인증서 검증에 기반을 둔 SEND (Secure Neighbor Discovery) 방식을 제안하고 있다. 또한 이와는 별도로 IP 주소에 대한 이동성과 멀티호밍을 지원하기 위하여 ID(Identifier) 정보와 위치(locator) 정보를 분리하기 위한 연구로서, HIP(Host Identity Protocol)를 연구하는 작업자 그룹[11]과 L3Shim 방식[12]을 연구하는 Multi6 작업자 그룹이 있다.

IPv6 노드들은 IPv4와는 달리 주소자동설정기능(address auto-configuration)[2]을 가지고 있다. 주소자동설정기능이란 노드가 네트워크에 접속하면, 자신의 MAC 주소를 이용하여 link local 주소를 생성하고, 이에 대한 중복성(DAD : Duplicate Address Detection) 여부를 체크한 후, 해당 네트워크에서 제공되는 subnet prefix 정보를 라우터로부터 전달받아 global unicast IP 주소로 설정하는 방법이다. 이러한 주소자동설정을 위해서 IPv6에서는 NDP 프로토콜[3]을 제시하고 있다. 그러나 NDP 프로토콜은 보안상의 많은 문제점[4]을 가지고 있기 때문에, 이에 대한 보완방안으로 SEND 프로토콜[8]이 제안되었다. 본 논문에서는 이러한 NDP 방식과 SEND 방식의 문제점을 분석하고, 이러한 문제점을 해결하기 위한 노드 PKC와 AC를 이용한 방식을 제안한다.

본 논문은 다음과 같이 구성된다. 2장에서는 기본적인 NDP를 이용한 주소자동설정기능과 이에 대한 보안문제점을 다루고, 3장에서는 CGA를 이용한 SEND 프로토콜에 대한 설명과 이에 대한 보안문제점을 다룬다. 4장에서는 이러한 문제점에 대한 해결방안으로서, Identity 정보에 해당되는 MAC 주소에 대한 공개키 인증서, location 정보에 해당되는 IP 주소에 대한 속성인증서(공개키 인증서와의 바인딩 정보 포함)를 이용한 방법을 제안하고, 마지막 5장 결론으로 마무리한다.

II. NDP 프로토콜

2.1 주소자동설정기능

IPv4 에서의 주소설정기능은 고정주소 지정방법과 자동주소 설정방법이 있다. 고정주소 지정방법은 관리자에 의해 주어진 주소로 설정하는 방법이며, 자동주소 설정방법은 DHCP(Dynamic Host Configuration Protocol) 서버에 의해 주소를 할당받는 방법이다. 이에 반하여 IPv6에서는 노드가 스스로 주소를 설정하는 방법(stateless address auto-configuration)[2]과 DHCP 서버에 의해 지정되는 주소로 설정하는 방법(stateful address auto-configuration)[13]이 있다. 본 절에서는 노드가 스스로 주소를 설정하는 stateless address auto-configuration 방식을 지원하기 위해 사용되는 NDP 프로토콜을 다룬다. 그림 1은 IPv6에서 정의된 NDP 프로토콜을 이용한 자동 주소설정 방법[2,3]의 절차를 보인다.

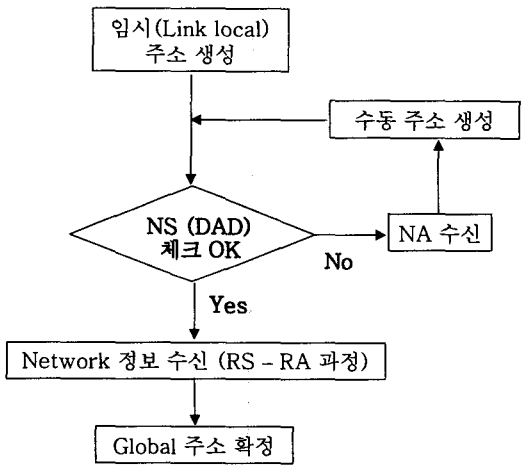


그림 1. 자동주소설정과정

먼저 노드는 MAC 주소를 기반으로한 임시주소를 생성하고, 이에 대한 중복성을 체크하기 위한 NS(Neighbor Solicitation) 메시지를 발송한다. 인근으로부터 NA(Neighbor Advertisement) 메시지가 수신되지 않으면, 중복성이 없는 것으로 보고, 인근의 라우터에게 subnet prefix 정보를 요청하는 RS(Router Solicitation) 메시지를 보내고, 라우터로부터 RA(Router Advertisement) 메세지를 수신하여 IP 주소를 확정한다. 그림 1의 과정은 다음과 같이 단계별로 구분된다.

단계 1 : 임시 주소 생성
단계 2 : DAD 체크 (NS-NA 과정)
단계 3 : 네트워크 정보 수신 (RS-RA 과정)

단계 4 : 글로벌 주소 생성
단계 5 : NDP 데이터 송수신 및 인터넷 통신

2.2 NDP 프로토콜에서의 문제점

NDP 프로토콜에 대한 보안공격은 표 1[4]과 같다. 표 1에서 N/R이란 Neighbor/Router를 의미하며, ND(Neighbor Discovery)는 Neighbor와의 통신과정인 NS/NA 패킷에 대한 보안공격이며, RD(Router Discovery)란 라우터와의 통신과정인 RS/RA 패킷에 대한 보안공격을 의미한다. R/D는 Redirect 공격인지 혹은 DoS 공격인지를 구분한다. 마지막으로 Mesgs. 는 해당 공격과 관련되는 NDP 메시지를 의미한다. 보안공격에 대한 상세한 내용은 참고문헌 [4]에 설명되어있다.

표 1. NDP 에 대한 보안공격

Attack name	N/R	R/D	Msgs.
NS/NA Spoofing	ND	Redir	NA, NS
NUD failure	ND	DoS	NA, NS
DAD DoS	ND	DoS	NA, NS
Malicious router	RD	Redir	RA, RS
Default router killed	RD	Redir	RA
Good router goes bad	RD	Redir	RA, RS
Spoofed redirect	RD	Redir	Redir
Bogus on-link prefix	RD	DoS	RA
Bogus address config	RD	DoS	RA
Parameter spoofing	RD	DoS	RA
Replay attack	All	Redir	All
Remote ND DoS	ND	DoS	NS

MIPv6[5]에서는 NDP 메시지의 무결성을 제공하기 위하여 IPsec 프로토콜의 AH 확장헤더를 사용하도록 정의하고 있으나, 실제로 초기의 주소자동생성과정에서는 IPsec을 위한 어떠한 보안연계(SA : Security Association)도 생성되어 있지 않기 때문에 사용될 수 없다.

표 1에서의 NDP 프로토콜과 관련된 보안공격을 살펴보면, 대부분 위조된 발신지 주소를 사용한 공격으로서, 발신자 및 발신지 IP 주소에 대한 인증문제로 귀착될 수 있다. 그러므로 발신자가 허위주소를 사용하는 IP 스푸핑 공격을 방지할 수 있도록 함으로서 대부분의 공격은 방지될 수 있다.

Ⅲ. SEND 프로토콜

SEND 프로토콜[8]은 NDP 프로토콜의 보안문제점을 보완하기 위하여 2005년 4월에 제안된 프로토콜이다. SEND 프로토콜에는 NDP 메시지에 대한 옵션들과 ADD (Authorization Delegation Discovery)관련 메시지들과 또한 CGA 옵션과 RSA 디지털서명 옵션이 추가로 정의되어있다. 본 논문에서는 주소자동설정과정에서의 문제점을 다루기 위해서 CGA 생성과정만을 간단히 설명한다.

3.1 CGA

NDP 방식의 보안 문제점을 보완하기 위해 제시된 CGA생성 방법[2]는 그림 2와 같다. 주소설정절차는 그림에서 1번부터 8번으로 표시되며, 5번 과정에서 생성된 Hash 값의 초기 16*sp(security parameter) 비트의 값이 0이 아니면 modifier 값을 1 증가시키고 4번 과정을 반복한다. 이때 생성된 주소를 CGA 1단계 주소라고 한다. 마찬가지로 8번 과정에서 생성된 주소가 충돌이 발생된다면, collision bit 값을 1 증가시키고 6번 과정을 반복한다. 이와 같은 과정을 거쳐 최종 생성된 값을 CGA라 하며, 이를 노드 주소로 사용한다.

CGA 생성을 위한 준비단계에 해당되는 1-3의 과정과 함께, 4번부터의 생성과정은 그림 2와 같다.

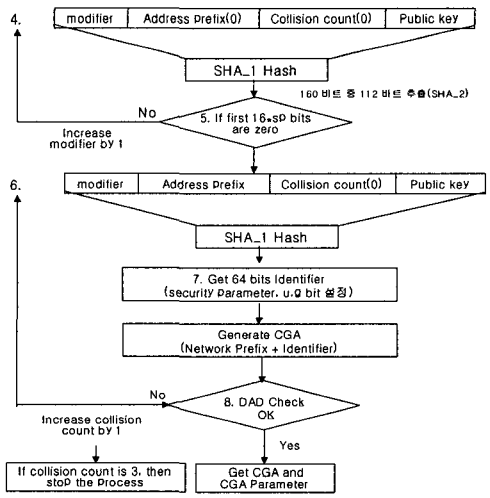


그림 2. CGA 생성절차

1. Public/Private key 생성
2. 16 octet modifier 선택
3. 3 bit security parameter(0-7) 선택

그림 5번 과정에서 생성된 주소를 1단계 CGA 주소라 부른다. 노드는 1 단계 CGA 주소를 오프라인 상에서 노드가 미리 생성하여 저장해 두었다가, subnet prefix 정보를 받은 후에, 이후 과정을 진행하고 최종 IP 주소를 확정한다.

3.2 CGA 주소의 장점

노드에서 임의로 공개키와 개인키 쌍을 생성하고, 공개키와 라우터의 RA 메시지를 통하여 수신된 subnet prefix를 이용하여 CGA 주소를 생성한다. 송신 노드는 CGA 주소와 RSA 디지털 서명문을 생성하여 보내고, 수신 노드는 수신된 CGA 파라메터를 이용하여 CGA를 재생성하고, 첨부된 RSA 디지털 서명문을 검증하는 방법으로 발신지 주소를 인증한다. 이러한 CGA는 다음과 같은 장점을 가진다.

① 노드는 필요에 따라 오프라인 상태에서 CGA 1 단계 주소를 미리 생성하여 저장해 둔다. 이는 NDP 통신과정에서 실시간으로 CGA 주소를 생성해야 한다는 부담을 덜어줄 수 있다. 특히 이동 환경에서는 1단계에서 계산된 해쉬값 결과를 보관하고 있다가, RA 메시지에 포함된 subnet prefix 정보를 이용하여 2단계 해쉬함수를 거쳐여 CGA 주소를 생성할 수 있다. 따라서 이동 환경에서 새로운 주소(CoA)를 생성하는 시간이 비교적 짧다.

② 링크의 안전성에 따라, 해쉬함수에서 제공되고 있는 sp 값을 0에서 7까지로 증가시킴으로서 안전성을 높힐 수 있다. 이는 복잡도를 $O(2^{59})$에서 $O(2^{59+(16*sp)})$로 증가시키는 역할을 한다.

③ 키가 누출되거나 훼손된 경우에도, 별도의 절차없이 공개키와 개인키쌍을 새로 생성하여 사용하면 된다. 또한 384 비트의 키 길이로 안전성에 문제가 있다면, 더 큰 길이의 키를 사용하면 된다.

④ 노드는 동일한 도메인내에서 여러 개의 CGA 주소를 미리 생성하여, CGA 주소를 바꾸어 가면서 사용할 수도 있다. 이는 주소에 대한 비예측성과 난수성을 제공하기 때문에 프라이버시 보호 역할을 한다.

3.3 SEND 프로토콜의 문제점

SEND 프로토콜은 NDP의 많은 문제점을 개선시킬 수 있는 방법이다. 다음은 SEND에 관한 주요 보안문제점은 다음과 같다.

① 기밀성을 제공하지 않는다.
SEND 프로토콜은 송신자의 subnet prefix 정보와 공개키 정보 등을 이용하여 CGA 주소를 생성하여 IP 주소로 사용하고, RSA 디지털 서명문을 사용함으로서, 송신자에 대한 인증기능과 서명기능을 제공한다. 그러나 전송되는 메시지에 대한 기밀성을 보장하지 않는다.

② 계산량이 너무 많다.
SEND 프로토콜에서는 RD 과정뿐 아니라, ND 과정의 NS, NA 메시지에도 각각 CGA 메시지 옵션과 RSA 서명문 옵션을 사용하도록 규정하고 있다. 이와 더불어 재전송(Replay) 공격을 방지하기 위하여 nonce 옵션과 timestamp 옵션을 권장하고 있다. 그러나 실제로 노드마다 송신 시에 CGA 와 RSA 서명문을 생성하고, 수신 시에 CGA 재생성 및 RSA 서명문 검증과 같은 작업은 노드에 많은 부하를 야기하게 된다. 결국 다량의 NDP 패킷을 특정 노드로 보냄으로서 DoS 공격을 야기할 수 있다.

③ CPS/CPA 메시지에 대한 DoS 공격
SEND 프로토콜에서는 라우터 인증을 위하여 신뢰점(trust anchor)으로부터 위임된 공개키 인증서를 사용한다. 라우터로부터 네트워크 정보를 담은 RA 메시지를 수신한 노드는 라우터의 진위 여부를 체크하기 위하여, 라우터에게 노드가 알고 있는 신뢰점으로 부터 CPS (Certification Path Solicitation) 메시지를 전송하고, 라우터로부터 CPA(Certification Path Advertisement) 메시지를 이용하여 인증서를 하나씩 전송받게 된다. 그러나 이와 같은 방식은 DoS 공격에 매우 취약하다. 예를 들면, 공격자가 임의로 생성한 CGA 주소를 이용하여, 합법적인 노드로 가장하여 라우터에게 신뢰점으로 부터 인증서 체인의 전송을 요청하는 메시지들을 다량으로 보낼 수 있다. 이

와 같은 공격이 계속되면 라우터는 부하를 감당하기 어려울 것이며, 이로 인해 정상적인 서비스를 제공할 수 없을 것이다. 마찬가지로 공격자는 라우터로 가장하여 특정 노드에게 많은 인증서들을 전송하면, 노드에서는 인증서 검증을 위하여 많은 시간을 허비하게 될 것이다.

CGA 방식이 PKI 기반구조에 대한 관리상의 문제점을 피하기 위하여, 임의로 생성된 공개키 쌍과 IP 주소를 바인딩 시키는 방법으로 노드를 인증하기 위해 제안되었지만, SEND 프로토콜은 CGA 재생성과정 및 RSA 서명문 검증과정에서 부하를 발생시킬 수 있으며, 또한 라우터의 인증서 검증과정에서 DoS 공격 대상이 될 수 있다.

또한 일단 설정된 CGA 주소에 대해서는 지속적인 인증기능을 제공할 수 있으나, 세션 도중에 키손상 등으로 인하여 공개키 쌍을 새로 생성하여 CGA 주소가 변경되는 경우에는, 이전 CGA 주소와 새로 생성된 CGA 주소간의 연계성을 가질 수 없다.

Ⅳ. 제안 방식

본 논문에서는 라우터 뿐 만아니라, 노드들도 초기에 자신의 Identity를 나타낼 수 있는 MAC 주소에 대한 디바이스 공개키 인증서(이하 PKC라 함)를 발급받고 사용하는 것으로 가정한다. 이러한 가정은 차세대 유비쿼터스 환경에서의 지능형 디바이스에 대한 각종 보안위협에 대한 대책으로도 적용될 수 있다. 본 논문에서는 이와 더불어 이동환경에서 수시로 발급되는 locator에 해당되는 IP 주소에 대하여 속성인증서(이하 AC라 함)를 사용하도록 제안한다.

(1) MAC 주소에 대한 PKC :

일반적으로 MAC 주소는 유일한 특성을 가지고 있으며, 고유한 값을 가진다. 네트워크상의 모든 노드들은 초기에 CA로부터 MAC 주소에 대한 PKC를 발급받는다. 이러한 PKC는 IP 주소와 무관하기 때문에 이동 환경에서도 Identity 정보로서 지속적으로 사용될 수 있다. 이때 발급된 PKC는 장기적으로 서명문 뿐 아니라 세션키 생성 등을 통하여 암호문 통신에 사용될 수 있다. 응용에 따라서는 PKC에 저장된 MAC 주소와 패킷에 기록된 MAC 주소가 일치하는 지 여부를 체크함으로서, 약식으로 PKC를 검증할 수도 있다.

(2) IP 주소에 대한 AC :

로컬 네트워크 상의 라우터들은 AC(Attribute Certificates)를 발급하기 위한 ACA(AC Authority) 기능을 수행한다. 라우터는 AC 발급을 요청하는 노드들이 제시한 PKC를 검증하고, 해당 네트워크를 사용하기 위한 IP 정보 등을 포함한 AC를 발급하는 기능을 한다. 발급된 AC에는 해당 PKC와의 바인딩 정보가 포함된다.

각 노드들은 홈 네트워크 내에서 뿐 만 아니라, 외부 네트워크로 이동하는 경우에도, 해당 네트워크 내의 ACA 기능을 가진 라우터로 자신의 PKC를 제시하고, AC 발급을 요청하며 라우터는 노드의 PKC를 검증하고, 해당 네트워크를 사용할 수 있도록 AC를 발급한다.

노드 및 라우터들은 AC를 첨부한 NDP 패킷을 전송하며, 수신측에서는 AC에 서명된 라우터의 서명문을 확인하고, AC에 기록된 주소와 IP 주소를 비교함으로서 노드를 검증할 수 있다.

이후, 노드가 이동하는 경우에, 홈 에이전트 혹은 상대노드(CN : Corresponding Node)에게 바인딩 정보를 전송할 필요가 있는 경우에는 주소의 변경을 알리기 위해 AC 를 사용할 수 있다.

본 논문에서는 이와 같은 NDP 방식과 SEND 방식의 문제점을 해결하기 위하여 PKC와 AC를 이용한 방법을 제안한다. 또한 PKC와 AC의 용도 및 발급방법은 표 2와 같이 구분될 수 있다.

표 2. PKC와 AC를 이용한 방안

인증서	주체	용도	발급 방법	비고
PKC	MAC 주소	1. 암호문생성 2. 서명문생성	초기에 CA로부터 발급	Identity 정보
AC	IP 주소	1. IP 주소인증 2. PKC와의 바인딩정보	인근 라우터로부터 발급	location 정보

4.1 제안된 방식의 동작

제안 방식을 이용한 주소설정방법은 다음과 같은 단계를 적용한다.

단계 0 : 준비단계

자신의 MAC 주소를 이용하여 CA로부터 PKC를 발급받는다. CA는 가급적이면 네트워크 관리자로부터 도메인내의 라우터 인증서를 발급하는 CA를 이용하는 것이 인증서 검증에 효율적이다.

단계 1 : 임시 주소 생성

RFC 2462[2]에 정의된 대로 MAC 주소를 이용한 link local 주소를 생성한다. 만일 프라이버시를 보장하기 위해서는 별도의 암호학적 주소를 사용할 수 있다.

단계 2 : DAD 체크 (NS-NA 과정)

RFC 2462[2]에 정의된 바와 동일한 방법으로 NS 패킷을 발송하여 주소의 중복성을 체크한다.

단계 3 : 네트워크 정보 수신 (RS-RA 과정)

노드는 RS 패킷에 "AC 발급요청" 옵션을 첨부하고, 자신의 PKC와 함께 인근의 라우터로 보낸다. 라우터에서는 노드의 PKC를 검증하고, 이상이 없는 경우에는 주체의 PKC 일련번호(주체 PKC 검증용)와 발급자의 PKC 일련번호(AC 서명문 검증용)와 노드의 IP 주소를 포함한 AC를 생성하고, 서명문을 추가하여 RA 메시지에 "AC 발급" 옵션을 포함하여 노드에게 발급한다.

단계 4 : 글로벌 IP 주소 생성

노드는 인근의 라우터로부터 수신된 AC를 이용하여 자신의 글로벌 IP 주소를 확정한다. 이후, NDP와 관련된 통신 메시지를 보낼 때에는 라우터로부터 발급된 AC를 첨부한다. 수신 측에서는 AC의 서명문을 검증하고, AC에 기록된 발신자의 주소와 패킷에 기록된 발신지 주소와의 동일함을 검증한다.

단계 5 : 기타 NDP 데이터 송수신 및 인터넷 통신

단계 4에서 설정된 글로벌 IP 주소를 이용하여 외부 인터넷과의 통신에서는 AC를 첨부하지 않는다. 다만 노드가 이동함으로서, 홈 에이전트 및 상대노드에게 주소의 변경을 알려야 하는 바인딩 정보를 전송할 경우에도 AC가 사용된다.

단계 5에서 AC에 저장된 발급자에 대한 정보는 AC 서명문 검증에 사용될 수 있고, 주체에 대한 정보로 PKC 일련번호를 이용하여 AC 주체에 대한 PKC를 검증할 수 있다. 그러나 인근 도메인의 경우에는 응용에 따라 PKC 검증 및 AC 검증작업을 일부 생략할 수 있다.

4.2 제안된 방식의 장점

제안된 방식은 다음과 같은 장점이 있다.

① 발신지 노드인증 절차가 간단하다.

노드들은 사전에 PKC를 발급받고, RS 메시지(AC 발급요청 옵션 첨부)와 자신의 PKC를 함께 인근 라우터에 전송하여 AC 발급을 요청한다. 또한 라우터에서는 RA 메시지(AC 발급 옵션 첨부)를 이용하여 노드에게 AC를 전달할 수 있다. 발급된 이후에는, 모든 NDP 패킷에 AC 옵션을 첨부하여 전송하고, 수신측에서는 인근의 ACA 기능을 가진 라우터의 공개키를 이용하여 AC에 첨부된 서명문을 검증하고, AC에 기록된 주소와 패킷에서 사용된 발신지 주소와의 동일성을 검증할 수 있다. 이와 같이 제안 방식은 NDP 방식에서의 허위주소를 이용한 보안위협을 제거할 수 있을 뿐 아니라, SEND 방식과 같이 CGA 주소와 RSA 서명문을 처리하기 위한 부하를 줄일 수 있다.

NDP, SEND, AC를 이용한 세 가지 방식에 대한 검증방법을 비교하면, 그림 3에서와 같다. NDP 방식은 주소설정이후에 사용될 수 있는 IPsec AH 메시지를 이용한다. SEND 방식의 경우에는 CGA와 RSA 서명문을 사용하기 때문에 수신측에서 CGA를 재생성하고, RSA 서명문을 생성하여 검증하는 방법을 사용한다. 반면 AC 방식은 첨부된 AC에 대한 서명문을 검증하여, AC의 무결성을 입증한 후, AC에 기록된 IP 주소가 실제 사용된 주소와 동일한 지를 비교하는 형식으로 검증된다.

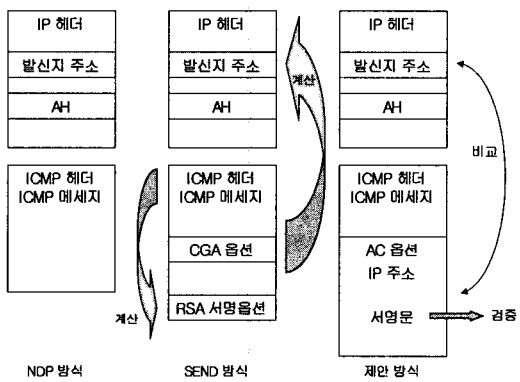


그림 3 세 가지 방식의 비교

② 이동 환경에서 동일하게 적용될 수 있다.

이동 환경에서 CoA 주소를 발급받기 위한 과정도 홈 네트워크 환경에서와 동일하다. 다만 라우터에서는 초기의 AC 발급을 요청한 노드에 대하여 노드의 PKC를 검증하기 위한 메커니즘이 적용되어야 하지만, 필요에 따라 생략될 수 있다. PKC에 기재된 주체인 MAC 주소와 현재 수신된 패킷의 MAC 주소를 비교하는 방법이 이용될 수도 있다. 이에 대한 적용은 응용에 따라 선택할 수 있도록 한다.

실제로 NDP 메커니즘과 SEND 프로토콜의 경우에는 주소설정과정에서는 노드인증기능이 없다. 이러한 노드인증 기능은 제안된 알고리즘에서 추가적으로 제공되는 기능이므로, PKC의 주체인 MAC 주소와 해당 노드와의 확인 과정으로 간략히 행할 수 있으며, 필요에 따라 공개키 기반구조의 인증서 검증과정을 준용할 수 있다.

③ 바인딩 업데이트 과정이 간략화 된다.

노드가 이동하는 과정에서 CoA 주소를 홈네트워크의 홈에이전트에 등록하는 과정은 간단하게 된다. 노드는 이미 홈네트워크에서 MAC 주소를 기반으로 한 PKC를 발급받았기 때문에, 초기의 PKC 검증과정을 수행한 이후로는 노드가 이동할 때마다, CoA 주소를 담은 AC 서명문에 대한 검증과정만이 필요하다. 또한 노드가 이동하는 경우, 상대노드와의 주소 바인딩을 위한 RR(Return Routability) 과정[14]도 CoA 주소를 담은 AC와 PKC를 이용할 수 있다. 만일 노드가 초기에 상대노드와의 통신과정에서 PKC를 제공하고, 이를 검증한 이후에는, 노드가 이동할 때마다, 상대노드에게 PKC를 제공할 필요는 없으며, CoA 주소를 담은 AC 서명문 만을 검증함으로서, 이러한 절차는 간략히 될 수 있다.

④ 디바이스 인증서로서의 PKC 기능

AC를 이용한 방법은 NDP 과정에서 뿐 아니라, 일반적인 통신에서도 적용될 수 있다. 노드가 사용하는 IP 주소에 대한 인증서에 해당되는 AC를 첨부하여 전송함으로서, 발신지 주소에 대한 신뢰를 높힐 수 있다.

또한 제안 방법에서 사용된 MAC 주소에 대한 PKC는 로컬네트워크 내의 NDP 과정에서 AC와 함께 주소 위조를 방지하기 위한 목적으로 제안하였지만, MCA 주소를 포함한 PKC는 노드의 디바이스 인증서로서 노드가 이동 상태에서 홈에이전트 혹은 상대노드와의 바인딩정보를 전달하기 위해 사용될 수 있을 뿐 만 아니라, 이러한 디바이스인증서는 유비쿼터스 환경하에서 디바이스간의 인증을 위한 도구로서 사용될 수 있을 것이다.

이와 같은 기능에 대하여 세 가지 방법(NDP, SEND 방식과 제안 방식)을 비교하면 표 3과 같다.

표 3. NDP, SEND, 제안 방식 간의 비교

	NDP	SEND	제안 방식
기밀성	X	X	O
무결성	IPsec	CGA, RSA 서명문 검증	AC 검증
라우터 인증서	X	O	O
노드 인증서	X	X	O

표 3에서 기밀성의 경우에는 제안방식에서는 라우터 및 노드들이 모두 공개키 인증서를 가지고 있기 때문에, 필요한 경우에는 세션키를 공유하고, 암호알고리즘을 적용할 수 있다. 무결성은, NDP 방식의 경우에는 IPsec의 AH를 적용할 수 없으며, SEND 방식의 경우에도, 주소가 확정되지 않은 상태에서는 CGA 검증과 RSA 디지털 서명옵션을 사용할 수 없다. 그러나 제안방식에서는 RS 패킷에 대하여 AC 발급요청문과 함께, 자신의 MAC 주소를 포함한 PKC를 제시함으로서 제공된다.

주소설정이후의 데이터 통신과정에서 제안방식에서는 IP 주소 뿐 아니라, PKC와의 바인딩 정보를 가진 AC를 사용함으로서 검증절차를 간략화 하였다. 만일 노드인증이 반드시 필요한 응용에서는 노드의 인증서를 확인하는 절차를 필요로 하지만, 초기 주소설정과 같은 대부분의 응용에서는 제안된 검증방법으로 구현될 수 있다.

4.3 제안 방식에서 사용되는 추가 옵션

이와 같은 PKC 및 AC 방식을 이용한 NDP 과정에서는 다음과 같이 추가적인 옵션을 필요로 한다.

① AC 발급요청 옵션

노드는 자신의 PKC와 함께, 노드의 link-layer 주소를 이용한 임시주소 등을 포함한 AC 요청문을 RS 메시지를 이용하여 라우터로 보낸다.

② AC 발급 옵션

①의 AC 발급요청 패킷을 수신한 라우터는 노드

의 PKC를 검증하고, 합당한 경우에는 RA 메시지를 이용하여 PKC 일련번호, IP 주소를 포함한 AC를 발급한다. 발급된 AC에는 발급자의 서명문이 첨부된다.

③ AC 옵션

초기 자동주소설정을 위한 NS, RS 패킷을 제외한 모든 NDP 패킷에는 라우터로부터 발급받은 AC를 포함하는 옵션을 사용한다. 수신측에서는 먼저 AC 발급자(인근 라우터)의 서명문을 검증하고, 패킷에서 사용된 주소와 AC에 기록된 주소를 비교하는 방법으로 검증할 수 있다.

기타 노드 PKC 및 라우터 PKC를 검증하기 위한 옵션 메시지가 추가될 수 있으며, 인근 지역간의 PKC 검증 방법에 대해서는 추가적인 연구사항으로 남겨둔다.

V. 결 론

최근 IPv6가 제안된 이후로, 이동 환경에서 가장 문제가 되고 있는 것이 주소설정과 이와 관련된 부스트래핑 문제이다. 노드가 이동하여도 응용계층의 프로세서에게 세션동안 지속적인 서비스를 제공하기 위해서는 IP 주소에 대한 정당성을 제공하여야 한다. 또한 NDP 메커니즘에 대한 보안문제점에서 지적되었듯이, 대부분의 보안공격이 허위주소를 사용하고 있다. 그러므로 발신지 주소를 허위주소로 사용하는 것을 방지하기 위하여, 발신지 주소 인증방법으로 AC를 이용하였다.

본 논문에서는 NDP 및 CGA를 이용한 SEND 프로토콜 방식의 문제점을 지적하고, 이를 보완하기 위한 방안으로서 PKC와 AC를 이용한 수정된 NDP 방식을 제안하였다. 제안된 방식은 노드의 Identity 정보를 나타내는 MAC 주소를 가진 PKC, 네트워크 이동상황을 고려한 locator 정보인 IP 정보와 PKC와의 바인딩 정보를 포함한 AC를 적용하였다. 현실적으로 노드마다 PKC를 부여한다는 것이 논쟁의 소지가 될 수 있으나, 유비쿼터스 환경하에서는 모든 지능형 노드들에 대하여 보다 신뢰성있는 통신을 위하여 PKC를 부여할 것으로 기대되며, 이는 디바이스 인증서로서 사용될 수 있을 것으로 기대된다.

또한 본 제안은 노드의 유일한 주소인 MAC 주소를 가진 PKC와 link local 주소를 이용한 IP 주소를 가진 AC로 제안하였지만, IP 주소의 익명성이 필요하거나 혹은 여러 개의 주소를 필요로 하는 노드의 경우에는 다른 암호학적 IP 주소도 고려될 수 있다. 일반적으로 사용자에게 다중인증서를 제공하듯이, 필요에 따라 노드들에게도 IP 주소 뿐 아니라, 기타 암호학적 주소를 발급하고, 이를 노드만의 유일 이름인 MAC 주소와 함께 PKC 일련번호로 바인딩되는 AC를 발급받을 수 있다.

본 논문에서는 RS 메시지와 함께 송신된 노드의 PKC에 기록된 MAC 주소와 실제 패킷의 MAC 주소를 비교하는 방법으로 PKC 검증 방법을 제안하였지만, 노드에 대한 확실한 인증을 위해서는 PKC에 대한 검증과정이 필요하다. 그러므로 노드 및 라우터의 PKC에 대한 검증방법에 대해서는 추가적인 연구가 필요하다. 노드가 인근지역으로 이동한다는 특성을 PKI 기반구조와 접목하여, 보다 효율적이고 간단한 PKC 검증방법이 연구되어야 할 것으로 사료된다.

마지막으로 본 제안은 MAC 주소를 이용하여 노드의 Identity를 표현하는 PKC와 이동에 따른 노드의 locator를 표현하는 AC를 이용함으로서, 현재 IETF에서 진행 중인 IP 주소의 Identifier와 Locator 분리를 위한 또 다른 방법으로 볼 수 있다. 현재로서는 IPv6 주소 구성과 관련된 많은 현안문제를 해결할 수 있는 완벽한 방법은 없으나, 본 논문에서 제안된 방식도 나름대로 IPv6의 보안문제점을 해결하는데 많은 도움이 될 것으로 사료된다. 그러나 본 논문은 이론적인 비교와 분석에 의해 제시된 방법이다. 따라서 제안된 방식을 실제로 적용하기 위해서는 보다 많은 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] Deering, S.; and R. Hinden, "Internet Protocol, Version 6 Specification", RFC 2460, December 1998

[2] Thomspn, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

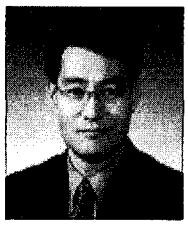
[3] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IPv6", RFC 2461, December 1998

[4] Pekka Nikander, James Kempf, Erik

Nordmark, "Ipv6 ND Trust Models and Threats", RFC 3756, May 2004.
[5] David B. Johnson, Charles E. Perkins, Jari Arkko, "Mobility Support in IPv6", RFC 3775, June 2004
[6] Jari Arkko, Vijay Devarapalli, Francis Dupont, "Using Ipsec to protect Mobile Ipv6 Signaling between MN and HA", RFC 3776, June 2004.
[7] Tuomas Aura, "Cryptographic Generated Address(CGA)", RFC 3972, March 2005.
[8] Jari Arkko, James Kempf, Brian Zill, Pekka Nikander, "SEcure Neighbor Discovery", RFC 3971, March 2005
[9] Charles Lynn, Stephen Kent, Karen Seo, "X.509 Extensions for IP Addresses and AS Identifier" RFC 3779, June 2004.
[10] Stephen Farrell, Russell Housley, "An Internet Attributes Certificate Profile for Authorization", RFC 3281, April 2002.
[11] Robert Moskowitz, Pekka Nikander, Petri Jokela, "Host Identity Protocol" Internet Draft draft-ietf-hip-base-03, June 2005,
[12] Geoff Huston, "Architectural Commentary on Site Multihoming Using Level 3Shim", Draft draft-shim6-arch-00.txt, February 2005.
[13] Relph Droms, Jim Bound, Bernie Volz, Ted Lemon, Charles E. Perkins, "Dynamic Host Configuration Protocol for IPv6 (DHCPV6)", RFC 3315, July 2003.
[14] 강현선, 박창섭, "Redirect 공격과 DoS 공격에 안전한 MIPv6 바인딩 업데이트 프로토콜", 정보보호학회 논문지, 제 15권, 5호,10, 20005.

〈著者紹介〉

김 지 홍 (Ji Hong Kim) 종신회원
1982년 : 한양대학교 전자공학과 졸업,
1984년 : 한양대학교 전자통신공학 석사,
1996년 : 한양대학교 전자통신공학 박사
1995.2 ~현재 : 정보통신기술사
1991.3 ~현재 : 세명대학교 정보보호학과 교수
〈관심분야〉 공개키기반구조, 접근제어, 네트워크보안,



나 재 훈 (Jae Hoon Nah) 정회원
1985년 : 중앙대학교 컴퓨터공학과 졸
1987년 : 중앙대학교 컴퓨터공학과 석사
2005년 : 한국외국어대학교 전자정보공학과 박사
1987년 ~현재 : 한국전자통신연구원 P2P보안연구팀 팀장
〈관심분야〉 IPv6/MIPv6 보안, P2P 보안