情報保護學會論文誌
第18卷 第6(A)號, 2008. 12

보안 이웃 탐색 프로토콜 성능 향상 기법에 관한 연구*

박 진 호†, 임 을 규‡
한양대학교

A Study on the Performance Improvement in SEcure Neighbor Discovery (SEND) Protocol*

Jin-Ho Park†, Eul-Gyu Im‡
Hanyang University

요 약

이웃 탐색(Neighbor Discovery) 프로토콜은 IPv6 프로토콜 사용 환경에서 동일 링크에 연결된 노드 사이에 이웃 노드에 관한 정보를 교환하는데 사용되는 프로토콜이다. 처음으로 제안되었던 IPsec 프로토콜의 인증 헤더(Authentication Header)를 이용한 이웃 탐색 프로토콜 보호 방법은 키 교환 프로토콜을 사용할 수 없고 수동적 키 분배의 어려움이 있는 문제점이 있었다. 그 후 모든 이웃 탐색 메시지를 디지털 서명(Digital Signature)으로 보호하는 보안 이웃 탐색(SEND) 프로토콜이 제안되었다. 그렇지만 공개키 암호화 시스템을 기반으로 한 디지털 서명 기술은 일반적으로 고비용이 드는 것으로 알려져 있어 가용성 측면에서 상당한 성능 저하가 있을 것으로 예상된다. 본 논문에서는 보안 이웃 탐색 프로토콜의 가용성을 개선시키기 위해 CGA(Cryptographically Generated Addresses) 주소 생성 과정에서 해시 함수 입력에 MAC(Media Access Control) 주소를 추가하는 Modified CGA 기법과 캐시를 활용하는 방법을 제안하였으며, 실험을 통해 기존 방법과의 성능 차이를 비교하였다.

ABSTRACT

Neighbor Discovery(ND) protocol is used to exchange an information of the neighboring nodes on the same link in the IPv6 protocol environment. For protecting the ND protocol, firstly utilizing Authentication Header(AH) of the IPsec protocol was proposed. But the method has some problems-uses of key exchange protocol is not available and it is hard to distribute manual keys. And then secondly the SEcure Neighbor Discovery(SEND) protocol which protects all of the ND message with digital signature was proposed. However, the digital signature technology on the basis of public key cryptography system is commonly known as requiring high cost, therefore it is expected that there is performance degradation in terms of the availability. In the paper, to improve performance of the SEND protocol, we proposed a modified CGA(Cryptographically Generated Address) which is made by additionally adding MAC(Media Access Control) address to the input of the hash function. Also, we proposed cache mechanism. We compared performance of the methods by experimentation.

Keywords : SEcure Neighbor Discovery

Ⅰ. 서 론

IT기술의 발전으로 인터넷 규모가 끊임없이 성장하고 있다. 최근에는 일반 개인용 컴퓨터뿐만 아니라 인터넷 접속 기능을 갖춘 핸드폰, 가전제품 등과 같은 단말들이 늘어나면서 인터넷 주소 공간 부족 문제가 점차 현실화되어가고 있다. 따라서 현재 사용되고 있는 32bit 주소 체계의 IPv4 프로토콜을 대체할 새로운 128bit 주소 체계의 IPv6(Internet Protocol Version 6) 프로토콜이 연구되어 온지 약 15년이 훌쩍 넘어들고 있다[1,2]. 하지만 현재까지는 상업적인 서비스를 제공하기에 앞서 시범망을 구축하여 기술 검증과 성능 개선 그리고 기존 IPv4 프로토콜기술과의 호환성 등 IPv6 기술이 현실적으로 사용되기에 앞서 풀어야할 다양한 관련 기술들에 대하여 연구가 진행 중이다.

이러한 IPv6 프로토콜에서는 IPv4 프로토콜에서 사용되었던 ARP(Address Resolution Protocol) 기능이 이웃 탐색 프로토콜(Neighbor Discovery Protocol)에 편입되었다. 또한 이웃 탐색 프로토콜은 라우터 탐색 기능과 비상태형 주소 자동 설정(Stateless address auto-configuration) 기능 등을 제공하여 링크 상에서 DHCP(Dynamic Host Configuration Protocol) 서버의 도움 없이 스스로 주소를 설정할 수 있는 편리한 기능을 제공한다.

이웃 탐색 프로토콜에는 자체적인 보안 메커니즘 부재로 인해 악의적인 사용자가 쉽게 프로토콜의 취약점을 이용하여 공격이 가능하기 때문에 최초의 보호 방법으로서 IPsec 프로토콜의 인증 헤더(Authentication Header)를 이용한 보호 방법이 제안되었다. 하지만 키 교환 프로토콜을 사용할 수 없고, 수동적 키 분배의 어려움 등과 같은 단점으로 인해서 현실적으로 사용이 매우 제한적이다.

다음으로 제안된 보호 방법은 CGA(Cryptographically Generated Address) 기술과 디지털 서명(Digital Signature) 기술을 이용한 보안 이웃 탐색 프로토콜(SEND; SEcure Neighbor Discovery)이다. CGA(Cryptographically Generated Addresses) 주소를 사용하여 IP 주소와 공개키를 결합시키며, 이 결합된 공개키를 이용하여 디지털 서명을 검증함으로써 이웃 탐색 메시지의 내용을 보호하는 이 기술은 강력한 보안 수준을 제공할 수 있다. 그렇지만 디지털 서명 기술은 고비용이 드는 공개키 암호화 시스템 기술을 바탕으로 하고 있어 상당한 에너지 자원을 요구하기 때문에 특히 PDA나 휴대폰과 같이 컴퓨팅 성능 및 배터리 자원의 제약이 있는 환경에서 보안 이웃 탐색 프로토콜 적용은 디바이스에 큰 부담을 줄 수 있다.

본 논문에서는 모든 이웃 탐색 메시지를 디지털 서명을 이용하여 보호하는 보안 이웃 탐색 프로토콜을 가용성 측면에서 개선시켜 에너지 효율적인 보안 이웃 탐색 프로토콜을 제안하였으며, 실험을 통해 기존 보안 이웃 탐색 프로토콜과의 성능 차이를 예측 비교 분석 하였다.

다음의 제II장에서는 기본적인 이웃 탐색 프로토콜 설명과 기존에 제안된 보호 기술들을 소개 분석하고, 제III장에서는 본 논문에서 제안하는 에너지 효율적인 보안 이웃 탐색 프로토콜을 소개하고, 제 Ⅳ장에서는 성능 비교 실험 내용을 소개하며, 제 Ⅴ장에서는 결론을 맺는다.

Ⅱ. 관련 연구

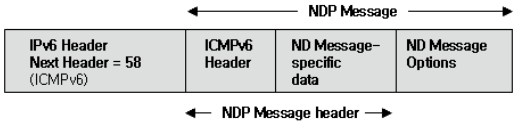
2.1 이웃 탐색 프로토콜

이웃 탐색 프로토콜(Neighbor Discovery Protocol)은 IPv6 프로토콜을 사용하는 네트워크 환경에서 동일 링크에 연결된 노드(호스트 혹은 라우터) 사이에 이웃 노드에 관한 정보를 교환하는 프로토콜이다. 몇 가지 편리한 기능들을 제공하는데, 그 기능에는 목적지 노드의 IP 주소에 대한 하위 계층의 링크 레이어 주소를 결정하는 주소 해석(Address resolution)기능, 호스트가 연결되어있는 링크에서 로컬 라우터를 찾는 라우터 탐색(Router discovery) 기능, 인터페이스에 대한 주소를 자동으로 설정하는 주소 자동 설정(Address auto-configuration) 기능, 이웃 노드에 더 이상 접근할 수 없는지 탐지하는 이웃 노드 접근불가 탐지(NUD; Neighbor Unreachability Detection) 기능, 노드가 사용하려고 하는 주소를 다른 노드에서 이미 사용 중인지 탐지하는 중복 주소 탐지(DAD; Duplicate Address Detection) 기능, 더 좋은 첫 번째 홉 노드를 알려주는 리다이렉트(Redirect) 기능 그리고 그 외에 프리픽스 탐색(Prefix

접수일: 2008년 7월 7일; 채택일: 2008년 10월 7일
* 본 연구는 한국과학재단 특정기초연구 (R01-2006-000-11196-02008) 지원으로 수행되었음
† 주저자, pjh0347@hanyang.ac.kr
‡ 교신저자, imeg@hanyang.ac.kr

discovery) 기능, 파라미터 탐색(Parameter discovery) 기능, 다음 홉 결정(Next-hop determination) 기능 등이 있다[3,4].

위와 같은 이웃 탐색 기능은 ICMPv6(Internet Control Message Protocol version 6) 프로토콜에 RS(Router Solicitation), RA(Router Advertisement), NS(Neighbor Solicitation), NA(Neighbor Advertisement) 그리고 Redirect 이렇게 다섯 가지 메시지 타입을 정의하여 구현되어 있다[5]. 이웃 탐색 프로토콜 패킷의 구조는 [그림 1]과 같다.



[그림 1] 이웃 탐색 프로토콜 패킷 구조

2.2 IPsec Authentication Header(AH)

가장 먼저 제안되었던 이웃 탐색 보호 방법은 IPsec 프로토콜의 인증 헤더(AH; Authentication Header)를 이용한 방법이다.

IPsec은 네트워크 계층에서 IP 통신을 안전하게 보호하기 위해 개발된 기술로서 패킷의 무결성과 기밀성을 보호하기 위해 강한 인증과 암호화 알고리즘을 사용한다. IPsec은 인증 헤더와 캡슐화 보안 페이로드(ESP; Encapsulating Security Payload)의 두 가지 트래픽 보호 프로토콜과 보안 연계(SA; Security Association) 그리고 키 관리 프로토콜로 구성되어 있다. 인증 헤더는 패킷에 대한 무결성(Integrity), 인증(Authentication) 그리고 부인방지(non-repudiation) 기능을 제공하며, ESP는 기밀성(Confidentiality)을 기본적으로 제공하며 선택 알고리즘에 따라서 추가적으로 인증과 무결성을 제공한다[6,7]. SA는 상대측 노드와의 통신을 보호하는데 사용되는 트래픽 보호 프로토콜, 프로토콜 운용 모드, 암호 알고리즘, 암호 키, 키의 수명 등 몇 가지 파라미터에 대한 약속을 의미하며 보안 연계 데이터베이스(SAD; Security Association Database)에 저장한다[8]. IKE(Internet Key Exchange)와 같은 키 관리 프로토콜을 이용하여 상대측과 SA 설정 및 유지를 관리한다[9].

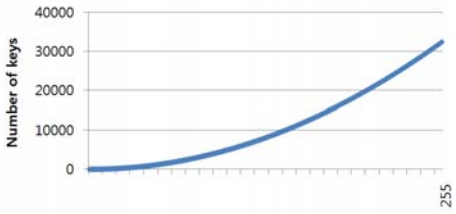
IPsec을 실제로 사용하기 위해서는 한 가지 전제 조건이 있다. IP 패킷 보호에 사용되는 암호 키를 두 노드 사이에 교환하기위해 사용되는 키 관리 프로토콜은 이미 통신이 가능한 상태에서 동작할 수 있다. 즉 다시 말하면, 인터페이스에 주소를 설정하여 통신이 가능한 상태가 되어 있어야 한다는 것이 전제 조건이라고 할 수 있다.

이웃 탐색 프로토콜의 비상태형 주소 자동 설정 기능은 스스로 주소를 생성하여 설정하는 과정에서 이웃 탐색 메시지를 주고받게 되는데, 아직 이 패킷들을 보호하기 위해 필요한 암호 키 교환이 수행되지 않은 상태이므로 보호할 수 없기 때문에 Chicken-and-Egg 문제가 있다[10].

위 문제의 해결 방법은 사전에 수동적으로 두 노드 사이에 공유하는 암호 키를 설정하여 보호하도록 하는 것이다. 하지만 단순히 모든 노드가 공유하는 그룹 키를 분배하는 것이 아니라 두 노드 사이에만 공유하는 비밀키를 수동적으로 분배해야하기 때문에 실질적으로 노드 수가 많아지면 거의 적용하기 힘들다. 수동적으로 분배해야할 암호 키의 수는 모든 노드들 사이에 간선이 존재하는 완전 그래프(Complete Graph)의 총 간선 수와 같다.

$$number\ of\ keys = \frac{n(n-1)}{2}$$

따라서 관리자나 사용자가 수동적으로 설정하여 사용하기에는 부적합하다는 것을 알 수 있다. 다음 [그림 2]는 하나의 C 클래스 네트워크에서 필요한 키의 수를 그래프로 나타내었다.



[그림 2] 수동적 키 분배의 어려움

2.3 SEcure Neighbor Discovery (SEND)

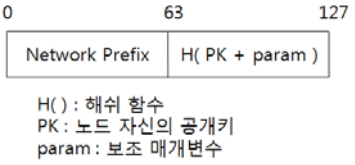
IPsec 인증 헤더를 이용한 보호 방법은 위에서 언급한 바와 같이 수동적 키 분배의 어려움이 있어 새로운 방식의 보호 기술인 보안 이웃 탐색 프로토콜(SEND;

SEcure Neighbor Discovery Protocol)이 제안되었다[11].

주요 기능으로는 이웃 탐색 메시지의 송신지 주소가 메시지를 전송한 노드의 주소임을 증명하는 주소 소유권 증명 기능, 공개키 암호화 시스템을 기반으로 한 디지털 서명을 통해 송신자를 인증하고 메시지의 무결성을 제공하는 인증과 무결성 기능, Redirect 메시지와 같은 단방향 메시지는 타임 스템프(Time stamp)값을 이용하고 Solicitation-Advertisement와 같은 양방향 메시지는 임의의 수 Nonce를 이용하여 이전에 전송된 메시지를 다시 사용하는 재연 공격(Replay Attack)을 방지하는 재연 공격 방지 기능 그리고 라우터 탐색과정에서 라우터의 신뢰성을 제공하는 권한 위임 탐색 기능 등이 있다.

보안 이웃 탐색 프로토콜은 CGA(Cryptograp hically Generated Addresses) 기술과 디지털 서명(Digital Signature) 기술을 기반으로 하고 있다[10,12].

암호학적인 연산을 통해 생성한 주소를 CGA (Cryptographically Generated Address) 주소라고 하며, CGA 주소의 형식은 [그림 3]과 같다. CGA 주소의 처음 64bit는 네트워크 프리픽스 값을 설정하고, 그 뒤의 나머지 64bit는 기존의 비상태형 주소 자동 설정에서 사용되었던 인터페이스 ID 대신에 노드에서 공개키와 보조 파라미터를 해시 입력 값으로 하여 얻은 해시 값을 설정하여 생성한다.



[그림 3] CGA 주소 형식

CGA 주소는 수신 받은 이웃 탐색 메시지의 CGA 옵션에서 CGA 주소를 생성할 때 사용했던 공개키와 보조 파라미터를 취하여 해시 값을 재계산하고 이 값을 송신지 CGA 주소의 인터페이스 ID 부분과 비교하여 검증한다. CGA 주소의 검증은 CGA 주소와 공개키 사이의 결합을 확인하여 CGA 주소를 사용하는 노드는 그 주소 생성에 사용된 공개키를 소유하고 있다는 것을 증명한다.

CGA 주소 검증 후에는 이웃 탐색 메시지의 RSA signature 옵션에 포함된 디지털 서명과 CGA 옵션에 포함된 공개키를 취하여 디지털 서명 검증을 수행한다. 이로서 이웃 탐색 메시지의 인증과 무결성에 대한 증명과 함께 통신하는 노드의 주체를 인증할 수 있게 된다.

보안 이웃 탐색 프로토콜은 ICMPv6 프로토콜에 새로운 메시지 타입을 정의하고 이웃 탐색 메시지에 추가적으로 옵션을 정의하여 구현되어 있다. [표 1]에 각 기능에 대한 구현 형태를 정리하였다.

디지털 서명 기술은 고비용이 드는 공개키 암호화 시스템 기술을 바탕으로 하고 있어 강력한 보안 수준을 제공할 수 있지만 상당한 에너지 자원을 요구하기 때문에 특히 PDA나 휴대폰과 같이 컴퓨팅 성능 및 배터리 자원의 제약이 있는 환경에서 보안 이웃 탐색 프로토콜 적용은 디바이스에 큰 부담을 줄 수 있다.

[표 1] 보안 이웃 탐색을 위한 메시지와 옵션

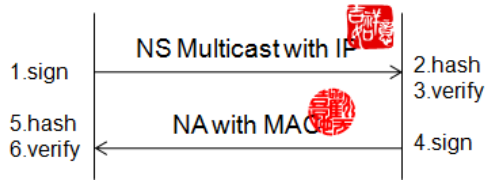
기 능	구 현 형 태
주소 소유권 증명	CGA Option
인증과 무결성	RSA Signature Option
재연 공격 방지	Timestamp, Nonce Option
권한 위임 탐색	CPS, CPA message Trust Anchor, Certificate Option

Ⅲ. 에너지 효율적인 보안 이웃 탐색

이웃 탐색 프로토콜은 주소 해석, 라우터 탐색, 중복 주소 탐지, 이웃 도달 불가 탐지, 리다이렉트 등 크게 다섯 가지 기능으로 요약된다. 각 기능에 따라서 메시지에 담긴 정보의 종류와 그 특성이 다르기 때문에 보호 방법도 상황에 맞게 효율적인 방법으로 해결할 수 있을 것이다. 따라서 본 논문에서는 주소 해석, 라우터 탐색, 중복 주소 탐지 기능에 대해서 보안 이웃 탐색 프로토콜의 보안 수준을 현실적으로 허용 가능한 수준으로 낮추는 대신 응답성과 에너지 효율성을 개선시키는 방법을 제안하였다.

3.1 주소 해석

주소 해석 기능은 상대측 호스트의 IP 주소를 알고 있는 상태에서 이에 대응되는 MAC 주소를 얻기 위해 수행하는 기능으로, 요청하는 노드는 NS 메시지의 Target Address 필드에 IP 주소를 설정하여 전송하고

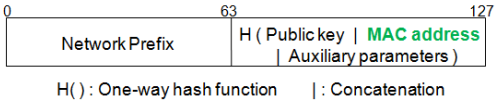


[그림 4] 보안 이웃 탐색의 주소 해석 과정

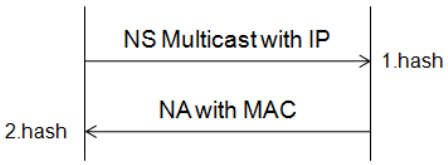
응답하는 노드는 NA 메시지의 Target link-layer address 옵션에 MAC 주소를 설정하여 전송한다.

기존의 보안 이웃 탐색에서는 이웃 탐색 메시지를 서명하여 디지털 서명을 포함시켜 보내면, 수신측에서는 일차적으로 공개키와 IP 주소 사이의 결합을 검증하여 CGA 주소를 검증한 후, 이차적으로 검증된 공개키를 이용하여 디지털 서명을 검증하여 메시지에서 각 이웃 탐색 기능별로 보호가 필요한 데이터를 보호했다.

본 논문에서 제안하는 방법은 먼저, CGA 주소를 생성할 때 추가적으로 MAC 주소를 해시 입력 값으로 넣어 생성하여 사전에 MAC 주소와 IP 주소 사이에 결합시켜 놓는다. 그런 후, 주소 해석 과정에서는 CGA 주소 검증 과정에서 MAC 주소도 함께 검증되므로 디지털 서명이 필요 없다. 단지 해시를 이용하여 MAC 주소와 IP 주소 사이에 결합 상태를 검증하여 보호할 수 있다.



[그림 5] Modified CGA 주소 형식



[그림 6] 제안하는 기법의 주소 해석 과정

주소 해석 과정에서는 NA 메시지에 포함된 Router flag 정보 또한 보호해야 한다. 노드의 역할이 라우터라는 것을 알리기 위해서는 RA 메시지를 이용하며, 라우터에서 호스트로 변경되었음을 알리기 위해서는 NA 메시지의 Router flag가 이용된다. Router flag값이 1로 설정되어 있으면 라우터를, 0으로 설정되어 있으면 일반 호스트를 의미한다. NA 메시지 수신 측에서는 캐시 되어있는 정보와 비교하여 Router flag값이 1에서 0으로 변경될 시 해당 이웃 노드 주소를 디폴트 라우터 목록에서 제거하도록 되어 있다. 악의적인 노드는 NA 메시지의 Router flag 값을 0으로 변조하여 전송함으로써 NA 메시지 수신 측 노드에서 해당 라우터의 주소를 디폴트 라우터 목록에서 제거 시켜 통신을 불가능하게 만들 수 있을 것이다.

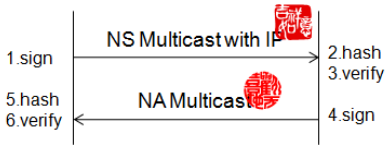
위와 같은 문제 해결을 위해 “제 3절 라우터 탐색”에서 제시한 방법과 같이 서명을 이용하여 초기 라우터 탐색 과정에서 노드의 역할이 라우터라는 것을 캐시 해두고, Router flag 값이 바뀐 NA 메시지를 수신 받을 경우 디지털 서명을 이용하여 보호하도록 했다. 노드의 역할 변경은 거의 발생하지 않기 때문에 서명을 이용한 보호는 거의 일어나지 않는다.

제안하는 방법의 보안 수준은 CGA 주소와 MAC 주소 사이의 결합 강도에 기반하며, 결합 강도는 결국 단방향 해시 함수의 충돌 율에 의해 결정된다. 기존의 보안 이웃 탐색 프로토콜에서의 보안 수준은 일차적으로 CGA 주소와 공개키 사이의 결합 강도에 기반 하여 단방향 해시 함수의 충돌 율에 의해 결정되며, 이차적으로는 디지털 서명 즉, 공개키 암호화 기술의 보안 강도를 갖는다. 해시 충돌이 발생하여 공격자의 공개키로 동일한 CGA 주소를 생성한 경우 이차적 보안 수단인 디지털 서명 기술은 무용지물이 되므로, 제안하는 방법의 보안 수준은 기존의 보안 이웃 탐색 프로토콜과 동일한 보안 수준을 갖는다.

3.2 중복 주소 탐지

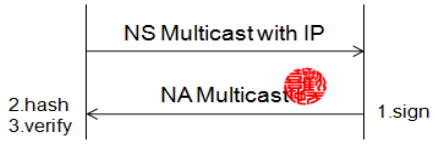
중복 주소 탐지 기능은 비상태형 주소를 스스로 생성한 후 사용하기 전에 네트워크에서 이미 사용 중인 노드가 있는지 확인 검증하기 위해 수행하는 기능으로, 요청하는 노드는 NS 메시지의 Target Address 필드에 tentative 주소를 설정하여 전송하며 만일 그 주소를 사용하는 노드가 있다면 NA 메시지로 응답한다.

기존의 보안 이웃 탐색에서는 중복 주소 탐지 과정 또한 앞에서 살펴본 주소 해석 과정에서 설명한바와 같이 동일한 방법으로 보호한다.

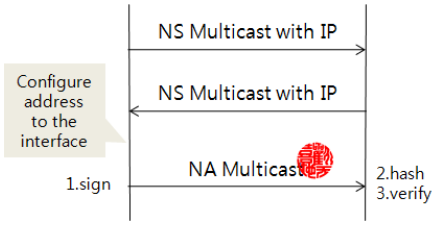


[그림 7] 보안 이웃 탐색의 중복 주소 탐지 과정

본 논문에서 제안하는 방법은 NS 메시지를 서명하지 않고 평문으로 전송하도록 하며, NS 메시지를 전송하고 일정 시간동안 NA 메시지를 기다리는 중에 다른 노드로부터 동일한 IP 주소에 대한 중복 주소 탐지 과정의 NS 메시지를 받았을 경우 IP 주소를 인터페이스에 설정하고 NA 메시지를 전송하도록 한다.



[그림 8] 제안하는 기법의 중복 주소 탐지 과정 (1)



[그림 9] 제안하는 기법의 중복 주소 탐지 과정 (2)

제안하는 방법은 평문으로 NS 메시지를 전송하도록 동작을 변경시켜 가용성을 개선시키면서도 기존의 보안 이웃 탐색 프로토콜이 제공하는 보안 수준에 크게 영향을 주지 않고 현실적으로 허용 가능한 수준의 보안을 제공하는데, 그 이유를 분석해 보면 다음과 같다.

중복 주소 탐지 과정에서 NS 메시지 내용 중 보호를 필요로 하는 정보는 Target Address 정보 하나뿐이다. 이 값을 서명을 통해 보호하지 않아 발생할 수 있는 공격에는 Target Address 값을 변경하여 메시지 변조 공격을 통한 DoS 공격을 예상해 볼 수 있다. 즉, Target Address 필드를 희생자 노드의 주소로 설정하여 대량의 NS 메시지를 전송하면 상대측 노드에서는 현재 자신이 그 주소를 사용 중임을 알리기 위해 NA 메시지에 디지털 서명하여 응답하게 되므로 DoS 공격이 가능하다.

하지만 기존의 보안 이웃 탐색 프로토콜에서도 DoS 공격은 가능하다. 중복 주소 탐지 과정에서 IP 헤더의 목적지 주소(Destination address)를 특정 노드의 IP 주소에 대한 solicited-node multicast address로 설정하고 NS 메시지를 서명하여 전송하면, 보안 이웃 탐색 프로토콜이 적용된 수신측 노드에서는 Target Address를 확인하기 이전에(이웃 탐색 메시지 처리 과정을 거치기 전에) 디지털 서명 검증을 수행하여 이 메시지를 받아들일지 무시할지 결정하게 된다. 따라서 NS 메시지의 Target Address 필드 값이 자신의 IP 주소가 아니더라도 디지털 서명 검증과정을 거쳐야 되기 때문에 DoS 공격이 가능하다. 제 Ⅳ장에서의 실험 결과에 의하면 서명 생성이 서명 검증 보다 약 50배 정도의 비용이 더 들기 때문에 DoS 공격이 상대적으로 어려워 질 수도 있지만, 사전에 디지털 서명을 미리 생성해 두고 일시에 전송한다면 또 그렇지만은 않다고 볼 수 있다. 이와 같은 중복 주소 탐지 과정 외에 라우터 탐색 과정에서도 서명한 RS 메시지를 대량으로 라우터에 전송하는 방식으로 DoS공격이 가능하다[11].

이러한 DoS 공격의 피해를 최소화시키기 위해 이웃 탐색 프로토콜에 내장된 rate limit과 restricted state 메커니즘을 이용하도록 되어 있다[3,11,3]. 결과적으로 이웃 탐색 메시지의 전송 주기 및 캐시 상태를 조절하여 DoS 공격으로부터 보호하도록 되어 있기 때문에 제안하는 방법의 보안 수준이 크게 떨어지지 않는다는 것을 알 수 있다. 보안 이웃 탐색 프로토콜에서는 공격자가 DoS 공격전에 미리 디지털 서명을 생성해 두어야 하지만 제안한 방법은 사전 준비 없이 공격이 가능하기 때문에 기존의 보안 이웃 탐색 프로토콜에서의 보안 수준보다 약간 떨어진다고 볼 수 있을 것이다.

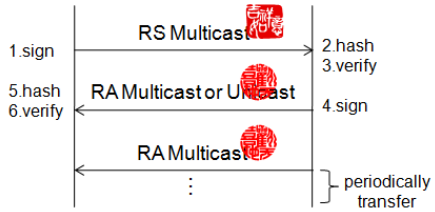
중복 주소 탐지과정에서 자신이 보낸 NS 메시지와 동일한 Target Address 값이 설정된 NS 메시지를 다른 노드로부터 받았을 경우 이를 중복 주소 탐지 충돌이라고 하는데, 기존의 방법과 제안하는 방법은 그 처리방법이 다르다. 기존 보안 이웃 탐색에서는 두 노드 모두 그 주소를 사용하지 않고, CGA 주소 생성에 사용되었던 보조 파라미터에 포함된 collision count를 1 증가 시켜 새로운 CGA 주소 생성 및 중복 주소 탐지 과정을 다시 수행하도록 하고 있다[10]. 본 논문에서 제안하는 방법은 악의적인 노드가 계속적으로 재연 공격(Replay Attack)하여 상대방 노드가 주소를 설정하지 못하도록 DoS 공격을 수행하는 것으로부터 보호하기 위해 선점형 주소 할당 방법을 제안했다. 즉, 중복 주소 탐지 충돌을 감지했을 때, NA 메시지를 전송하여 사용 중이라고 응답함으로써 자신이 그 주소를 사용하도록 하였다. 인터페이스에 주소 설정하는 과정과 NA 메시지를 전송하는 과정은 구현에 따라서 순서를 바꿀 수도 있다. [그

림 9]에 그 과정을 나타내었다.

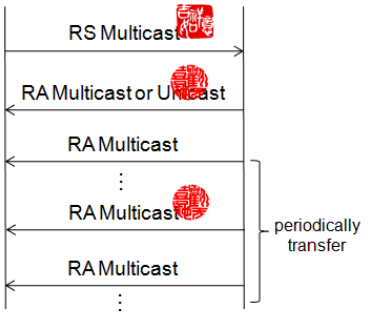
3.3 라우터 탐색

라우터 탐색 기능은 호스트 측에서 RS 메시지를 전송하여 라우터로부터 RA 메시지를 수신 받아 네트워크 프리픽스와 같은 정보를 얻을 때 사용하는 기능으로, 라우터는 호스트의 빠른 주소 자동 설정 또는 주소 재지정(Address Renumbering)과 같은 편리함을 제공하기 위해 주기적으로 RA 메시지를 전송하기도 한다.

기존 보안 이웃 탐색의 라우터 탐색 과정에서도 모든 RS/RA 메시지를 디지털 서명을 이용하여 보호한다. [그림 10]에 그 동작 과정을 나타내었다.



[그림 10] 보안 이웃 탐색의 라우터 탐색 과정



[그림 11] 제안하는 기법의 라우터 탐색 과정

제안하는 방법에서 라우터 측에서는 서명된 RS 메시지를 수신하여 이에 응답할 때, 그리고 캐시 기법을 사용하여 주기적으로 전송하는 라우터 광고 메시지의 내용이 이전에 광고했던 내용과 달라진 것을 감지했을 때 서명된 RA 메시지를 송신한다. 주기적으로 전송하는 광고의 내용이 이전과 같을 경우에는 평문 RA 메시지를 전송한다. 노드 측에서는 라우터로부터 서명된 RA 메시지를 수신했을 때 캐시에 저장해 두고 라우터가 주기적으로 전송하는 평문 RA 메시지를 수신했을 때 캐시 데이터와 비교하여 다를 경우 서명된 라우터 탐색 메시지를 이용하여 캐시를 업데이트 한다. 이 경우는 노드가 잠시 네트워크 연결이 원만하지 못하여 라우터가 전송한 변경된 내용의 서명된 라우터 광고 메시지를 수신하지 못한 경우 또는 악의적인 노드가 메시지 위조 공격을 시도한 경우이며 이를 정상적으로 처리할 수 있다. 노드 측에서 서명된 RS 메시지를 전송하는 경우는 주소 자동 설정 과정에서의 초기 라우터 탐색과 캐시 데이터의 손상 등과 같은 상황에서 발생한다.

위와 같은 차이점 외에 또 한 가지 기존 방법과의 차이점으로, 이웃 탐색 표준 문서에서는 RS 메시지에 대한 응답으로 RA 메시지를 모든 노드 멀티캐스트(all nodes multicast) 혹은 유니캐스트로 전송하도록 권고하고 있지만 현재 대부분의 IPv6 프로토콜 스택을 탑재한 운영체제에서는 항상 모든 노드 멀티캐스트로 전송하는 방식을 채택하고 있었다. 제안하는 방법은 RS 메시지의 송신지 주소가 할당되지 않은 주소(Unspecified Address)가 아닌 한 유니캐스트 방식으로 응답하도록 동작을 변경하여 한 노드가 요청한 쿼리로 인하여 모든 노드가 RA 메시지의 디지털 서명을 검증해야 되는 비효율적인 자원 소모 현상을 해결하였다.

제안하는 방법의 보안 수준은 제 2절 중복 주소 탐지에서 제안한 방법의 보안 수준과 동일하다.

Ⅳ. 성능 비교 분석

본 논문에서 제안하는 방법과 기존의 보안 이웃 탐색 프로토콜과의 성능 차이를 실험을 통해 예측해 보기 위해서 먼저 각 이웃 탐색 기능별로 보호에 필요한 비용을 수식으로 정리하고, 수식에 사용된 암호학적 알고리즘 및 캐시 데이터 비교 성능을 구현을 통해 측정하였으며, 실제 IPv6 네트워크를 구축하여 각 이웃 탐색 기능별 사용 빈도를 조사한 후, 네트워크에서 이웃 탐색 프로토콜을 보호하는데 드는 총 비용을 구하는 공식을 만들어 계산하여 비교하였다.

4.1 이웃 탐색 보호 비용

이웃 탐색 보호에 비용 차이가 발생하는 주소 해석, 중복 주소 탐지, 라우터 탐색 등 세 가지 이웃 탐색 기능에 대해서 그 처리 비용을 수식으로 정리하여 [표 2]에 나타내었다.

[표 2] 보안 이웃 탐색과 제안기법의 처리 비용 비교

이웃 탐색 기능		보안 이웃 탐색		제안 기법	
주소 해석	SOL/ ADV	SND	C_{RSA_SIGN}	SND	0
		RCV	$2C_{SHA-1} + C_{RSA\_VERIFY}$	RCV	$2C_{SHA-1} + C_{CMP\_RFLAG}$ + [retry]***
중복 주소 탐지	SOL	SND	C_{RSA_SIGN}	SND/ RCV	0
		RCV	$2C_{SHA-1} + C_{RSA\_VERIFY}$		
	ADV	SND	C_{RSA_SIGN}		
		RCV	$2C_{SHA-1} + C_{RSA\_VERIFY}$		
라우터 탐색	SOL	SND	C_{RSA_SIGN}		
		RCV	$2C_{SHA-1} + C_{RSA\_VERIFY}$		
	ADV	SND	C_{RSA_SIGN}	SND	(C_{RSA_SIGN})* or 0**
		RCV	$2C_{SHA-1} + C_{RSA\_VERIFY}$	RCV	($2C_{SHA-1} + C_{RSA\_VERIFY}$)* or ($2C_{SHA-1} + C_{CMP\_RA}$ + [retry]***)**

C_{RSA_SIGN} : RSA 디지털 서명 생성 비용
C_{RSA_VERIFY} : RSA 디지털 서명 검증 비용
C_{CMP_RFLAG} : 캐시된 Router flag와 비교 비용
C_{SHA-1} : SHA-1 해시 함수 처리 비용
C_{CMP_RA} : 캐시된 RA 메시지와 비교 비용
* 디지털 서명이 포함된 RA 메시지 처리 비용
** 디지털 서명이 포함되지 않은 RA 메시지 처리 비용
[retry]*** 디지털 서명을 포함한 메시지로 다시 수행

보안 이웃 탐색에서는 모든 이웃 탐색 메시지를 송신할 때 C_{RSA_SIGN}의 비용이 들며, 수신할 때에는 $2C_{SHA-1}$+ C_{RSA_VERIFY}의 비용이 든다. 반면에 제안하는 방법은 이웃 탐색 기능별로 다른 보호 메커니즘을 적용하였기 때문에 그 처리 비용도 각각 다르다. 라우터의 공개키 신뢰성 검증을 위한 Certificate path 처리와 같이 기존 보안 이웃 탐색의 기능을 변형하지 않은 내용에 대해서는 성능이 동일하다고 볼 수 있으므로 생략하였으며, 참고적으로 주소 생성 비용은 $2C_{SHA-1}$으로 두 방법이 동일하다.

4.2 암호학적 알고리즘과 캐시 비교 성능 측정 실험

앞 절에서 언급한 디지털 서명 생성과 검증, 해시 함수 그리고 캐시 데이터 비교 등의 성능을 측정하였다. 측정 방법은 CPU 타임스탬프카운터(Time stamp Counter) 값을 이용하여 알고리즘 수행 시 계산에 사용된 계산량(clock cycle)과 시간(microsecond)을 50회씩 반복하여 측정하였다[14]. 실험 환경은 [표 3]과 같다.

[표 3] 실험 환경

하드웨어	
CPU	Pentium 3 800 Mhz
RAM	256 MB
소프트웨어	
운영체제	Linux kernel 2.6.24
암호화 알고리즘	OpenSSL cryptographic library[16]
프로그래밍 언어	C, ASM

암호학적 알고리즘의 성능 측정을 위한 구체적 방법으로, 해시 알고리즘은 CGA 기법에서 사용하는 SHA-1을 기준으로 했으며, 해시 함수 입력 값으로 Hash2 값은 modifier, 9 zero octets, public key를 그리고 Hash1 값은 final modifier, subnet prefix, collision count, public key를 사용하였다. CGA 주소 생성 및 검증 시에는 Hash2와 Hash1 두 번의 해시를 사용한다[10].

디지털 서명 알고리즘은 보안 이웃 탐색에서 사용하는 RSA 알고리즘을 기준으로 했으며, 1024bit 키를 사용했다. 디지털 서명으로 보호한 데이터의 크기는 사전 실험을 통해 얻은 평균 크기인 240byte로 했다.

50회에 걸친 실험에서 얻은 결과의 상위, 하위 10% 씩을 제외한 나머지의 평균값은 [표 4]와 같았다. 본 실

[표 4] 암호학적 알고리즘 성능 비교

	RSA Sign	RSA Verify	SHA-1 Hash (x2)
Computational Clock (clock)	9,784,428	170,266	17,143
Computing Time (us)	12,185	214	23

험에 의하면 디지털 서명 생성에 약 12ms 정도의 시간이 소요 되었다. 일반적인 유선 랜에서 ping 응답속도가 0.3ms 정도하는 것과 비교해볼 때 상당히 응답성이 느릴 것이라는 것을 예측해볼 수 있었다.

다음으로 RA 메시지나 NA 메시지의 Router flag 비교와 같은 단순 메모리 데이터 비교, 즉 캐시 비교 성능 측정을 위한 구체적 방법으로, RA 메시지의 크기는 prefix 옵션과 Source link layer address 옵션을 포함한 크기인 56byte로, Router flag는 4byte로 가정하여 실험했으며, 50회에 걸친 실험 결과에서 상위, 하위 10%씩을 제외한 나머지의 평균값을 구한 결과는 [표 5]와 같았다. 이 실험 결과를 통해 56byte를 비교하나 4byte를 비교하나 성능 상 차이는 없었다. 그 이유는 RDTSC 인스트럭션 명령어를 이용하여 CPU 타임스탬프카운터 값을 기준으로 측정하는 방법은 1000 clock 이하에서 정밀도가 떨어지기 때문이었다[15].

[표 5] 단순 데이터 비교 성능

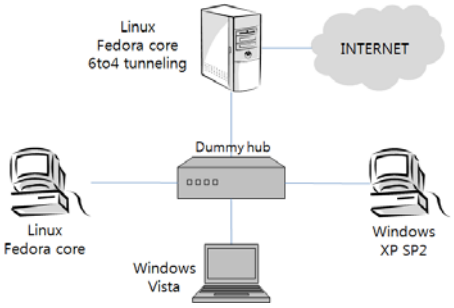
	Router flag	RA message
Computational Clock (clock)	44	44
Computing Time (us)	1.5	1.5

4.3 이웃 탐색 기능별 사용 빈도 측정 실험

제안하는 방법은 세 가지 이웃 탐색 기능에 대해 그 처리 비용이 기존 보안 이웃 탐색과 다르다. 따라서 각 이웃 탐색 기능이 어느 정도의 빈도로 사용되는지 알아야 전체 비용을 알 수 있기 때문에 IPv6 네트워크에서 사용되는 이웃 탐색 기능별 사용 빈도를 먼저 실험을 통해 측정해 보았다.

이웃 탐색 기능별 사용 빈도를 측정하기 위해 먼저 일반적인 IPv6 네트워크를 구성하였다. 듀얼 스택을 지원하는 윈도우 데스크탑 컴퓨터, 리눅스 데스크탑 컴퓨터, 윈도우 노트북 컴퓨터 그리고 리눅스 게이트웨이 서버로 이루어진 IPv4/IPv6 공존 네트워크를 더미 허브를 이용하여 구성하고 게이트웨이 서버에 6to4 터널링을 설정하여 IPv4 네트워크를 통해서 외부 IPv6 네트워크에 연결되도록 설정했다. 네트워크 구성은 [그림 12]와 같다.

게이트웨이 서버에서는 호스트의 비상태형 주소 자동 설정 기능을 지원하기 위해 라우터 광고 데몬(radvd)을 수행하며 광고주기 설정 값은 MinRtrAdvInterval는 10, MaxRtrAdvInterval는 30으로 설정하였다. IPv6 트래픽을 발생시키기 위해서 SAMBA, HTTP, FTP, SSH, DNS, Ping과 같은 일반적인 여러 네트워크 응용 서비스 기능들과 비상태형 주소 자동 설정 기능을 다음 시나리오를 바탕으로 수행하며 30분 동안 패킷을 수집하였다.

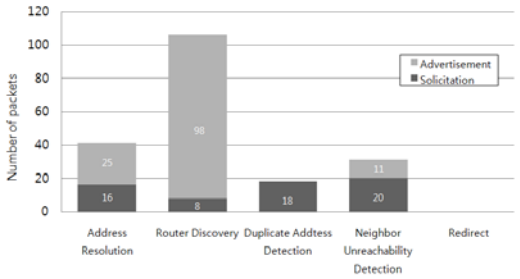


[그림 12] 실험 네트워크 구성도

- 게이트웨이 서버에 각종 응용 서비스 서버 기능 활성화
- 게이트웨이 서버에서 패킷 수집 시작
- 세 호스트에서 비상태형 주소 자동 설정 기능 수행
- 4대의 컴퓨터 사이에 ping 테스트 수행
- 노트북 컴퓨터 주소 자동 설정 수행
- 게이트웨이 서버와 리눅스 데스크탑 사이에 SAMBA로 공유 파일 전송
- 게이트웨이 서버에서 리눅스 데스크탑으로 SSH 접속
- 윈도우 데스크탑에서 외부 웹서버 www.kame.net 접속
- 노트북에서 게이트웨이 웹서버에 접속
- 두 데스크탑 컴퓨터 주소 자동 설정 수행
- 리눅스 데스크탑에서 게이트웨이 서버에 FTP 접속
- 4대의 컴퓨터 사이에 ping 테스트 수행
- 게이트웨이 서버에서 패킷 수집 종료

수집한 패킷에서 이웃 탐색 메시지만 별도로 추출하여 각 이웃 탐색 기능별 사용 빈도를 통계 낸 데이터를 [그림 13]에 나타내었다.

중복 주소 탐지 과정에서의 NA 메시지와 리다이렉트 메시지는 발생하지 않았고, 4개의 노드로 실험했을



[그림 13] 이웃 탐색 기능별 사용 빈도 통계

경우 라우터 탐색 메시지가 다른 이웃 탐색 기능의 메시지보다 상대적으로 높은 비율을 차지하고 있었으며, 이는 노드의 수가 많아질 경우 상대적으로 라우터 탐색 메시지의 비중은 낮아질 것이다.

4.4. 성능 비교 실험 결과

앞 실험에서 이웃 탐색 보호에 사용된 몇 가지 메커니즘들의 처리 비용을 구현을 통해 측정했고, 각 이웃 탐색 기능별 보호에 필요한 비용을 공식화했으며, 실제 네트워크를 구성하여 이웃 탐색 메시지의 발생 빈도를 측정하였다. 이런 실험 결과들을 바탕으로 제안하는 방법과 기존 방법을 각각 실제 네트워크에 적용했을 때 예상되는 에너지 절감 효과를 계산하여 두 방법의 성능을 예측 비교해 보았다.

[표 2]에서 정리한 보호 비용 공식을 이용하여 동일

[표 6] 파라미터 정의

파라미터	의 미
N_{NODES}	노드 수
$N_{ROUTERS}$	라우터 수
N_{AR_PKTS}	주소 해석 메시지 수
$N_{DAD\_PKTS}(N_{DAD\_SOL\_PKTS}+N_{DAD\_ADV\_PKTS})$	중복 주소 탐지 메시지 수
$N_{RD\_PKTS}(N_{RD\_SOL\_PKTS}+N_{RD\_ADV\_PKTS})$	라우터 탐색 메시지 수
$N_{RD\_SOL\_UNSPECIFIED\_PKTS}$	IP 헤더의 송신지 주소가 unspecified address인 RS메시지 수
$N_{NUD\_PKTS}(N_{NUD\_SOL\_PKTS}+N_{NUD\_ADV\_PKTS})$	이웃 도달 불가 탐지 메시지 수
$N_{REDIRECT\_PKTS}$	리다이렉트 메시지 수

[표 7] 계산에 사용된 파라미터 실험값

파라미터	실험값	파라미터	실험값
C_{RSA_SIGN}	9,784,428	$N_{DAD\_SOL\_PKTS}$	18
C_{RSA_VERIFY}	170,266	$N_{DAD\_ADV\_PKTS}$	0
C_{SHA-1}	17,143	$N_{RD\_SOL\_PKTS}$	8
C_{CMP_RA}	44	$N_{RD\_SOL\_UNSPECIFIED\_PKTS}$	2
C_{CMP_RFLAG}	44	$N_{RD\_ADV\_PKTS}$	98
N_{NODES}	4	N_{NUD_PKTS}	31
$N_{ROUTERS}$	1	$N_{REDIRECT\_PKTS}$	0
N_{AR_PKTS}	41		

링크 상에 있는 모든 호스트와 라우터에서 이웃 탐색 메시지를 보호하는데 소모하는 총 비용을 각 이웃 탐색 기능별로 공식화 했다. 공식에 사용된 파라미터 정의는 다음 [표 6]과 같다.

먼저, 기존의 보안 이웃 탐색에서 각 이웃 탐색 기능별로 [표 9]과 같은 비용이 소모된다.

그리고 제안하는 방법에서 각 이웃 탐색 기능별로 [표 10]와 같은 비용이 소모된다.

위의 공식에 대입한 파라미터 값은 앞서 실험을 통해 얻은 데이터를 이용하였으며 [표 7]과 같다.

공식에 파라미터를 대입하여 계산한 결과 예상되는 성능 차이는 [표 8] 그리고 [그림 14]와 같았다.

[표 8] 이웃 탐색 기능별 소모비용 정량적 비교

	기존 SEND	제안한 방법
주소 해석	409,548,180	1,407,530
중복 주소 탐지	179,801,640	0
라우터 탐색	1,098,992,208	152,070,056
이웃 도달 불가 탐지	309,658,380	309,658,380
리다이렉트	0	0

[그림 14] 예상되는 이웃 탐색 전체 성능 비교

[표 9] 네트워크의 모든 노드에서 소모되는 비용 합산식 - 제안한 방식

이웃 탐색 기 능	소모비용 합산식
주소 해석	$N_{AR\_PKTS}{}^{*}(2C_{SHA-1}+C_{CMP\_RFLAG})$
중복 주소 탐지	$(N_{DAD\_ADV\_PKTS}{}^{*}C_{RSA\_SIGN})+(N_{DAD\_ADV\_PKTS}{}^{*}N_{NODES}{}^{*}(2C_{SHA-1}+C_{RSA\_VERIFY}))$
라우터 탐색	$((N_{RD\_SOL\_PKTS}-N_{RD\_SOL\_UNSPECIFIED\_PKTS})*C_{RSA\_SIGN})+$ $((N_{RD\_SOL\_PKTS}-N_{RD\_SOL\_UNSPECIFIED\_PKTS})*N_{ROUTERS}{}^{*}(2C_{SHA-1}+C_{RSA\_VERIFY}))+$ $(N_{RD\_SOL\_PKTS}{}^{*}C_{RSA\_SIGN})+$ $((N_{RD\_SOL\_PKTS}-N_{RD\_SOL\_UNSPECIFIED\_PKTS})*(2C_{SHA-1}+C_{RSA\_VERIFY}))+$ $(N_{RD\_ADV\_PKTS}-(N_{RD\_SOL\_PKTS}-N_{RD\_SOL\_UNSPECIFIED\_PKTS})*N_{NODES}{}^{*}$ $(2C_{SHA-1}+C_{CMP\_RA}))$
이웃 도달 불가 탐지	$N_{NUD\_PKTS}{}^{*}(C_{RSA\_SIGN}+(2C_{SHA-1}+C_{RSA\_VERIFY}))$
리다이렉트	$N_{REDIRECT\_PKTS}{}^{*}(C_{RSA\_SIGN}+(2C_{SHA-1}+C_{RSA\_VERIFY}))$

[표 10] 네트워크의 모든 노드에서 소모되는 비용 합산식 - 기존 보안 이웃 탐색

이웃 탐색 기 능	소모비용 합산식
주소 해석	$N_{AR\_PKTS}{}^{*}(C_{RSA\_SIGN}+(2C_{SHA-1}+C_{RSA\_VERIFY}))$
중복 주소 탐지	$N_{DAD\_SOL\_PKTS}{}^{*}(C_{RSA\_SIGN}+(2C_{SHA-1}+C_{RSA\_VERIFY}))+$ $(N_{DAD\_ADV\_PKTS}{}^{*}C_{RSA\_SIGN})+(N_{DAD\_ADV\_PKTS}{}^{*}N_{NODES}{}^{*}(2C_{SHA-1}+C_{RSA\_VERIFY}))$
라우터 탐색	$((N_{RD\_SOL\_PKTS}-N_{RD\_SOL\_UNSPECIFIED\_PKTS})*C_{RSA\_SIGN})+$ $((N_{RD\_SOL\_PKTS}-N_{RD\_SOL\_UNSPECIFIED\_PKTS})*N_{ROUTERS}{}^{*}(2C_{SHA-1}+C_{RSA\_VERIFY}))+$ $(N_{RD\_ADV\_PKTS}{}^{*}C_{RSA\_SIGN})+(N_{RD\_ADV\_PKTS}{}^{*}N_{NODES}{}^{*}(2C_{SHA-1}+C_{RSA\_VERIFY}))$
이웃 도달 불가 탐지	$N_{NUD\_PKTS}{}^{*}(C_{RSA\_SIGN}+(2C_{SHA-1}+C_{RSA\_VERIFY}))$
리다이렉트	$N_{REDIRECT\_PKTS}{}^{*}(C_{RSA\_SIGN}+(2C_{SHA-1}+C_{RSA\_VERIFY}))$

실험적으로 구성한 네트워크에서 약 77%의 에너지 효율 향상을 기대할 수 있었다. 그리고 해시 알고리즘과 캐시 비교 기법을 통해 부분적으로 이웃 탐색 기능의 응답성을 높일 수 있었다. 비록 실제 구현을 통해 성능을 측정한 것이 아니기 때문에 정확한 수치의 성능 비교는 아니지만 이 실험을 통해 본 논문에서 제안하는 방법이 성능 향상에 도움이 된다는 것을 입증할 수 있는 근거 자료가 될 수 있을 것이다.

Ⅴ. 결 론

본 논문에서 제안하는 방식은 기존의 보안 이웃 탐색 기술의 보안 수준을 현실적으로 충분히 허용할 수 있는 범위 내에서 낮추는 대신 응답성과 에너지 효율성 측면에서 성능을 한층 개선시켰다.

이번 성능 실험 내용은 악의적인 노드가 공격하지 않은 평범한 상황을 가정하였다. 공격이 발생하면 기존의 보안 이웃 탐색 보다 가용성 측면에서 성능이 낮아질 수 있다. 주소 해석 기능의 경우, 두 번의 해시와 Router flag를 비교하는데 만일 캐시 데이터와 값이 다를 경우 디지털 서명을 포함한 이웃 탐색 메시지를 이용하게 되므로 기존 보안 이웃 탐색 보다 $2C_{SHA-1}+C_{CMP\_RFLAG}$ 만큼의 비용이 추가적으로 들게 된다. 이 비용은 부담을 줄만큼 큰 값은 아니기 때문에 큰 문제가 되지는 않을 것으로 예상된다.

향후 공격 발생을 가정하여 어느 정도의 성능 저하가 있을지에 대해 비교 실험을 통한 분석이 필요하며, 실제 구현을 통해서 정확한 성능을 측정해야할 것이다. 그리고 또한 기존 보안 이웃 탐색과의 호환성에 대한 연구도 필요하다.

참고문헌

[1] S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460, Dec 1998.

[2] R. Hinden, S. Deering, “IP Version 6 Addressing Architecture”, RFC 4291, Feb 2006.

[3] T. Narten, E. Nordmark, W. Simpson, “Neighbor

Discovery for IP Version 6 (IPv6)", RFC 2461, Dec 1998.
[4] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, Dec 1998.
[5] A. Conta, S. Deering, M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC4443, Mar 2006.
[6] S. Kent, "IP Authentication Header", RFC4302, Dec 2005.
[7] S. Kent, "IP Encapsulating Security Payload (ESP)", RFC4303, Dec 2005.
[8] S. Kent, K. Seo, "Security Architecture for the Internet Protocol", RFC4301, Dec 2005.
[9] C. Kaufman, Ed., "Internet Key Exchange (IKEv2) Protocol", RFC4306, Dec 2005.
[10] T. Aura, "Cryptographically Generated Addresses (CGA)". RFC 3972, Mar 2005.
[11] J. Arkko, Ed., J. Kempf, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, Mar 2005.
[12] RSA Laboratories, "RSA Encryption Standard, Version 2.1", PKCS 1, Nov 2002.
[13] P.Nikander, J.Kempf, E.Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.
[14] "RDTSC--Read Time-Stamp Counter", http://softwarecommunity.intel.com/isn/Community/en-US/forums /thread/30235396.aspx
[15] "Intel Software Network-RDTSC Latency", http://www.intel.com/software/products/documentation/ vlin/ mergedprojects/analyzer_ec/ mergedprojects/reference_olh/mergedProjects/instructions/instruct32_hh/vc275.htm
[16] http://openssl.org/
[17] 경계현, 고광선, 엄영익, "IPv6 환경에서 해쉬 함수 기반 강건한 주소 생성 및 검증 기법", 정보보호학회논문지 제17권 제1호, 2007. 2.
[18] 안개일, 나재훈, "IPv6 네트워크에서 SEND 프로토콜의 구현", 한국통신학회논문지 제32권 제7호, 2007. 7.

<著者紹介>

박 진 호 (Jin-Ho Park) 학생회원
2006년 2월 : 용인대학교 컴퓨터정보처리학과 졸업
2008년 8월 : 한양대학교 전자컴퓨터통신공학과 석사 졸업
<관심분야> 정보보호, 네트워크 통신

임 을 규 (Eul-Gyu Im) 종신회원
2002년 5월: University of Southern California 컴퓨터과학 박사
2000년~2002년 : WiseNut Inc. Sr. SW Engineer
2002년~2005년 : 국가보안기술연구소 선임연구원
2005년~2007년 : 한양대학교 정보통신대학 컴퓨터전공 전임강사
2007년~현재 : 한양대학교 정보통신대학 컴퓨터전공 조교수
<관심분야> 유무선 네트워크 보안, 정보보안