IPv6 환경에서 IPsec과 SEND 간 상호운영 문제점 분석*

경계현, 고광선, 엄영익
성균관대학교 정보통신공학부
e-mail:{gyehyeon, rilla91, yieom}@ece.skku.ac.kr

Cooperation Analysis for IPsec and SEND in the IPv6 Environments

Gyehyeon Gyeong, Kwang Sun Ko, Young IK Eom
School of Info. and Comm. Eng., Sungkyunkwan University

요 약

IPv6 프로토콜에서는 ND(Neighbor Discovery) 프로토콜의 보안을 위해 SEND(Secure ND) 프로토콜을 사용하고, IP 헤더와 데이터의 보안을 위해 IPsec(IP Security) 프로토콜을 사용하도록 하고 있다. 개별적인 목적을 갖고 운용되는 두 보안 메커니즘은 보안에 사용되는 옵션의 형태가 비슷하여 상호 운영하는 경우 보안 연산의 중복으로 이동형 기기의 성능 저하 및 네트워크에 불필요한 부하를 발생시킨다. 따라서 본 논문에서는 IPsec과 SEND 프로토콜이 동시에 사용되는 환경을 구분하고, 이러한 환경에서 발생할 수 문제점을 발견하고 분석함을 보인다.

1. 서론

IPv6(IP Version 6) 네트워크에서는 IPv4 네트워크에서의 보안 문제점을 해결하기 위하여 IPsec(IP Security)을 기본적인 보안 프로토콜로 사용하도록 정의하고 있다[1]. IPsec 프로토콜을 이용할 경우 통신 양단간에 전송되는 데이터에 대한 무결성과 기밀성을 제공할 수 있으며 통신 주체에 대하여 인증할 수 있다[2]. 하지만 IPsec 프로토콜은 IPv6 네트워크의 몇몇 상황에서는 사용할 수 없으며, 이러한 환경에서 네트워크 관리에 중요하게 사용되는 ND(Neighbor Discovery) 메시지를 공격으로부터 보호하기 위하여 SEND(Secure ND) 프로토콜이 새롭게 도입되었다[3]. 이러한 SEND 프로토콜을 이용하여 ND 메시지의 무결성 지원과 통신 주체에 대한 인증을 할 수 있다.

하지만 두 보안 프로토콜을 상호 운영하는 경우 보안 연산이 중복되는 문제가 발생하며 두 보안 프로토콜 처리에 많은 부하를 동반하게 된다. 이러한 부하는 이동형 기기의 성능 저하를 발생시키며, 네트워크에 불필요한 부하를 발생시키게 된다.

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음. (IITA-2006-C1090-0603-0027)

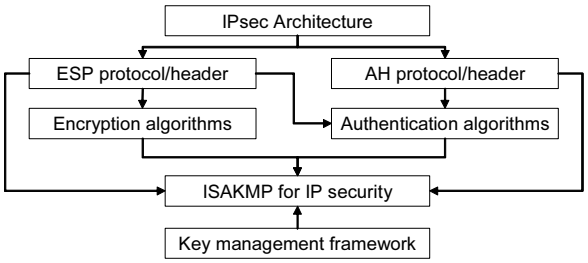
이에 따라 본 논문에서는 IPsec과 SEND 프로토콜 각각의 특징을 설명한 후, 두 보안 프로토콜이 상호 운영되는 환경을 구분한다. 그리고 이러한 환경에서 나타날 수 있는 문제점 발견하고 이에 대하여 분석하고자 한다.

2. IPv6의 보안 옵션

본 절에서는 IPv6 프로토콜에서 보안을 위해 사용하는 IPsec과 SEND 프로토콜에 대하여 간단하게 소개하고 각 특징에 대해 설명한다.

2.1 IPsec 프로토콜

IPSec 프로토콜은 IP 계층과 전송 계층 사이에서 IP와 데이터의 보안을 제공하며, 어플리케이션 독립적으로 네트워크 보안이 가능하고 호스트 간 보안 통신을 가능하도록 하는 보안 프로토콜이다. IPSec 프로토콜은 IPv6 프로토콜에 기본적인 보안 기술로 사용하도록 확장헤더로 정의되어 있으며, 제공하는 서비스로는 접근제어, 데이터 무결성, 데이터 근원 인증, 재실행된 패킷의 거부, 기밀성 제공 등이 있다.



(그림 1) IPsec 구성 요소간 관계

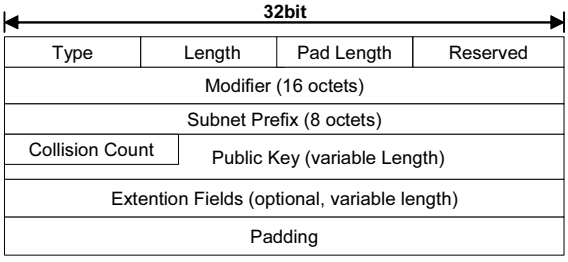
IPSec 프로토콜은 그림 1과 같이 ESP(Encrypted Security Payload)와 AH(Authentication Header)로 구성되어 있으며 표 1에서 보이는 바와 같이 전송 모드와 터널 모드에서 개별적 또는 동시에 사용될 수 있다[4, 5].

<표 1> 환경에 따른 IPsec 헤더의 구성

모드 구분	적용 옵션	사용 목적
전송 모드	AH	무결성 지원
	ESP	기밀성 지원
	ESP + AH	기밀성과 무결성 지원
터널 모드	AH	무결성 지원
	ESP	기밀성 지원
	ESP + AH	기밀성과 무결성 지원

2.2 SEND 프로토콜

SEND 프로토콜은 ND 프로토콜에 보안기능을 지원하기 위하여 발표되었으며, IPsec 프로토콜과 같은 보안 인프라가 존재하지 않거나 사용할 수 없는 환경 하에서 ND 메시지에 보안을 제공한다[6]. SEND 프로토콜을 사용하는 노드는 먼저 PKI 기반의 공개키/개인키 쌍을 미리 보유하고 있어야 하며, 여기서 생성된 공개키는 CGA (Cryptographically Generated Address) 보안 옵션을 통하여 주소를 생성하는데 사용한다. SEND 프로토콜은 공개키에 대한 인증서를 통하여 사용자를 인증하고, 인증된 사용자의 ND 메시지만 받아들이고 처리하게 된다[7].



(그림 2) CGA 검증을 위한 자료구조

CGA로 생성된 주소를 이용하여 통신하는 경우에는 그림 2와 같은 주소 생성에 사용된 정보가 수신 노드에 함께 전송되며, 주소를 수신한 노드는 정보들을 이용하여 사용된 주소의 위변조 여부를 판별할 수 있다. 특히 함께 전송된 공개키에 해당하는 인증서를 통하여 주소 소유자에 대한 인증을 할 수 있다[7].

추가적으로 RSA 기반의 전자서명을 이용하여 CGA 주소와 그림 2의 자료구조가 담긴 SEND 메시지의 무결성을 제공할 수 있다. 서명 검증에 필요한 공개키는 인증서 또는 송신자의 메시지 옵션 형태로 제공받을 수 있다.

3. IPsec과 SEND 프로토콜 상호운영상의 문제점

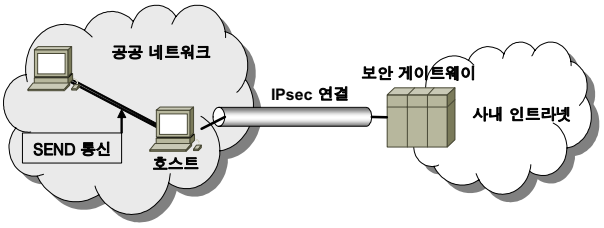
IPsec과 SEND 프로토콜은 서로 다른 목적을 갖고 개발 되었지만, 두 종류의 보안 프로토콜이 상호 운영되는 경우 중복되는 보안 연산으로 인하여 이동형 기기의 성능 저하 및 네트워크에 불필요한 부하를 발생시킨다. 이러한 문제의 해결을 위해 중복 연산에 대한 관리와 정보 공유를 필요로 한다.

3.1 네트워크 구분

관리나 인증이 없는 공공 네트워크는 다양한 보안 위협이 존재하고 따라서 보안 프로토콜을 필요로 하는 환경이다[8]. IPv6의 대표적인 보안 프로토콜인 IPsec과 SEND 프로토콜은 이러한 환경에서 둘 중 하나만 사용되거나 두 가지 프로토콜 모두 사용될 수 있다.

SEND 프로토콜의 경우 호스트가 네트워크에 처음 진입하는 단계부터 사용되는 ND 메시지를 보호해야 하기 때문에 IPsec 프로토콜 설정단계 이전부터 사용되며, IPsec 프로토콜과 같은 필요에 따라 사용되는 옵션 형태가 아니라 ND 프로토콜 자체를 변경하는 필수 사용 형태가 되므로 기본적으로 모든 호스트는 SEND 프로토콜을 사용한다고 가정한다.

IPsec과 SEND 프로토콜이 동시에 사용되는 네트워크 환경은 SEND의 적용범위인 하나의 도메인으로 한정된다.



(그림 3) IPsec 터널 모드 네트워크 구성도

먼저 그림 3은 IPsec 터널 모드의 형태로 외부의 호스트가 VPN을 통하여 사내 인트라넷 도메인에 참여하는 형태이다. 먼저 호스트가 외부의 공공 네트워크 진입하기 위해서는 주소자동설정 메커니즘을 이용하여 사용할 IP 주소를 생성해야 한다[9]. 이때 사용되는 ND 메시지의 보안을 위하여 SEND 프로토콜을 사용한다. 호스트는 다음으로 사내 인트라넷 진입을 위하여 IPsec 프로토콜로 구성된 VPN을 사용하게 되는데, 이 경우 IPsec과 SEND 프로토콜이 동시에 사용되게 되어 사용자와 사내 인트라넷 사이에 많은 부하가 발생하게 된다.

(그림 4) IPsec 전송 모드 네트워크 구성도

그림 4는 IPsec 전송 모드의 형태로 동일한 도메인 내의 호스트 간 보안통신을 하는 경우이다. 서로 다른 두 호스트는 SEND 프로토콜을 기본으로 사용하고 있으며 두 호스트 간 보안 통신의 필요에 의해 IPsec 통신을 수행하게 된다. 이 경우 SEND와 IPsec 프로토콜이 동시에 사용되어 호스트 간 불필요한 부하가 발생하게 된다.

3.2 보안 프로토콜의 처리비용

처리비용은 프로토콜에서 사용하는 알고리즘 처리에 필요한 시간적인 측면과, 프로토콜에 따라 전송되는 패킷의 크기적인 측면으로 구분할 수 있다.

<표 2> 알고리즘 처리 비용 표기법

표기	의미
C_{Hash}	해쉬 함수 처리 비용
C_{Cert}	인증서 검증 처리 비용
C_{RSA}	RSA 전자서명 처리 비용
C_{SK}	대칭키 암호화 처리 비용

표 3에서는 표 2의 표기법을 이용하여 SEND와 IPsec 프로토콜의 처리비용을 보인다. SEND 프로토콜은 CGA 주소 생성에 두 번의 해쉬 함수가 사용되며, 이렇게 생성된 주소의 검증에는 해쉬값의 검사를 위해 생성과 동일하게 두 번의 해쉬 함수를 사용하고, 주소 생성자의 공개키에 해당하는 인증서를 검사함으로써 CGA 주소를 사용한 소유자의 신원을 인증하게 된다. 또한 CGA 주소와 함께 전송되는 데이터와 SEND 메시지의 무결성을 지원하기 위하여 RSA 전자서명을 사용할 수 있으며 이 경우 전자서명 처리에 추가적인 작업이 필요하다.

<표 3> 보안 프로토콜의 처리비용

	보안 처리 단계	처리비용
SEND	CGA 주소 생성	$2C_{Hash}+(C_{RSA})^*$
	CGA 소유권 검증	$2C_{Hash}+C_{Cert}+(C_{RSA})^*$
	RSA 전자 서명	C_{RSA}
IPsec	AH 생성/검증 비용	C_{Hash}
	ESP 생성/검증 비용	$C_{SK}+C_{Hash}$
	AH+ESP 검증 비용	$C_{SK}+2C_{Hash}$

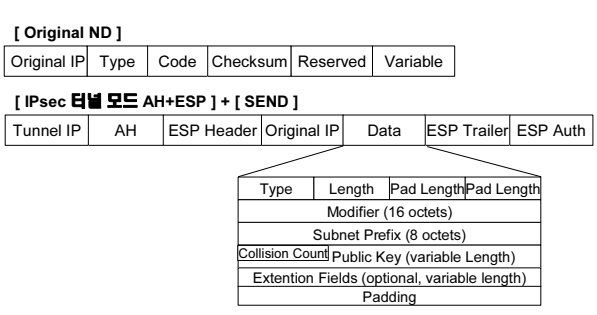
* CGA 자료구조의 무결성 지원 (필요에 따라 사용)

IPsec 프로토콜의 경우 AH 적용 시 무결성을 위해 해쉬 함수를 사용하고, ESP 적용 시 기밀성을 위해 대칭키를 이용한 암호화 및 복호화를 이용하므로 이에 따른 작업이 필요하게 된다. 이렇게 각각 요구되는 처리비용이 IPsec과 SEND 프로토콜이 함께 사용될 경우 최악의 경우(고강도 보안 옵션 적용) 표 4와 같은 처리 비용을 요구하게 된다.

<표 4> SEND와 IPsec 동시 사용 처리 비용

구분	처리 비용
SEND	$2C_{Hash} + C_{Cert} + 2C_{RSA}$
IPsec	$C_{SK} + 2C_{Hash}$
SEND + IPsec	$4C_{Hash} + 2C_{RSA} + C_{Cert} + C_{SK}$

또한 IPsec과 SEND 프로토콜이 동시에 사용될 경우 한번의 ND 메시지 전송 시 필요로 하는 패킷의 크기는 그림 5에서 보이는 바와 같이 원래 ND 메시지 패킷 크기에 비해 더욱 많은 크기를 필요로 함을 알 수 있다.



(그림 5) SEND와 IPsec 동시 사용 시 패킷 크기

3.3 보안 연산의 중복 분석

IPsec과 SEND 프로토콜이 사용운영 되는 경우 두 프로토콜의 보안 연산이 중복하여 동작하는데 두 프로토콜이 서로 정보를 공유하게 된다면 보안 연산의 비용을 감소시킬 수 있다.

<표 5> 보안 프로토콜의 보안 연산

보안 연산	IPsec	SEND
사용자 인증	O	O
무결성 지원	O	O
기밀성 지원	O	X

O : 보안 연산 수행, X : 보안 연산 없음

표 5는 IPsec과 SEND 프로토콜에서 제공하는 보안 연산을 보이고 있다. 사용자 인증의 경우 두 프로토콜에 모두 존재하지만 현재 상태에서는 IPsec과 SEND 프로토콜 각각 별도의 사용자 인증을 수행하게 된다. 또한 전송되는 메시지의 무결성 지원 부분도 두 프로토콜이 각각 별도로 수행하고 있다.

이러한 경우 먼저 설정되어 사용되는 SEND 프로토콜의 사용자 인증 정보를 IPsec에서 공유하게 되면 IPsec 설정단계를 단축시킬 수 있고, SEND 메시지를 전송할 경우 IPsec에서만 무결성을 지원해주면 보안 연산의 단계를 줄이고, 전송되는 패킷의 크기를 감소시킬 수 있다.

4. 결론

IPsec 프로토콜은 IP 헤더와 데이터의 무결성과 기밀성을 위해 개발되었고, SEND는 ND 메시지의 송신자에 대한 신원 인증과 ND 메시지의 무결성을 제공하기 위해 개발되었다. IPv6 네트워크에서는 두 보안 프로토콜이 상호 운영될 수 있지만, 현재의 상황에서는 중복되는 보안 연산으로 인하여 이동형 기기의 성능을 저하시키고, 전송되어야 하는 패킷 크기가 커짐으로써 네트워크에 불필요한 부하를 발생시키게 된다.

IPsec과 SEND 프로토콜은 별도의 목적을 갖는 보안 메커니즘이지만 내부 처리과정 비슷하여 중복되는 보안 연산이 존재한다. 따라서 두 프로토콜을 상호 운영하는 경우에는 별도의 관리를 통하여 네트워크 환경에 따른 관리와, 중복되는 보안 연산 부분은 연산 결과를 서로 공유하여 두 보안 프로토콜 간 한번의 보안 연산 수행으로 효율적인 동작이 가능하도록 하는 관리를 필요로 한다.

참고문헌

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

[2] J. Thomas and A. J. Elbirt, “Understanding Internet Protocol Security,″ The (ISC)2 Journal, Vol. 13, Issue 4, pp.39-43, 2004.

[3] J. Arkko, J. Kempf, B. Zill, and P. Nikander, RFC 3971, *SEcure Neighbor Discovery (SEND)*, 2005.

[4] S. Kent, RFC 4302, *IP Authentication Header*, 2005.

[5] S. Kent, RFC 4303, *IP Encapsulating Security Payload*, 2005.

[6] J. Arkko, T. Aura, J. Kempf, V. m. Mäntylä, P. Nikander, and M. Roe, ″Securing IPv6 neighbor and router discovery,″ Proc. of the 3rd ACM workshop on Wireless Security′02, pp. 77-86, 2002.

[7] J. Arkko, J. Kempf, B. Zill, and P. Nikander, RFC 3971, *SEcure Neighbor Discovery (SEND)*, 2005.

[8] T. Aura, RFC 3972, *Cryptographically Generated Addresses (CGA)*, 2005.

[9] S. Thomson andT. Narten, RFC 2462, *IPv6 Stateless Address Autoconfiguration*, 1998.

[10] P. Nikander, J. Kempf, and E. Nordmark, RFC 3756, *IPv6 ND Trust Models and Threats*, 2004.