IPv6환경에서 안전한 데이터 전송을 위한 SEND 프로토콜의 개선

류재현°, 허준, 홍충선

경희 대학교

jhryu@networking.khu.ac.kr, joonheo@khu.ac.kr, cshong@khu.ac.kr

Enhanced SEND Protocol for Secure Data Transmission in IPv6 Environment

JaeHyun Ryu° , Joon Heo ,ChoonSeon Hong

KyungHee university

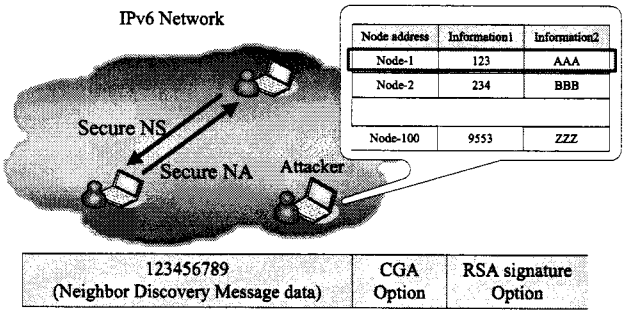
요 약

네트워크 초기 설정을 하는 경우와 동일한 프리픽스를 사용하는 인접 노드와 정보를 주고 받기 위해 사용되는 인접 노드 탐색 프로토콜에 보안 기능을 지원하는 SEND 프로토콜은 메시지의 무결성과 부인 방지 기능은 제공하지만 메시지의 기밀성은 제공 할 수 없다. 본 논문에서는 SEND 프로토콜의 보안 기능을 분석하고, 대칭 키 암호화 방식을 적용하여 메시지의 무결성을 제공하는 기법을 제안 한다.

1. 서 론

여러 기능이 통합된 인접 노드 탐색 프로토콜(ND, Neighbor Discovery)은 IPv6 환경에서 노드가 네트워크 초기 설정을 하는 경우와 동일한 프리픽스를 사용하는 인접 노드와 정보를 주고 받는 경우에 사용 한다. ND 프로토콜 메시지를 보호하기 위해 IPSec의 사용을 언급하였으나 구체적인 방법은 제시 하지 않았다. IPSec 기술은 주소가 설정되어 있지 않다면, 노드의 주소를 수동으로 설정하여 IPSec 기술을 적용할 수 있다. 시스템 부팅과 같은 경우에 IKE를 사용하기 위해서는 SA가 필요하고, SA을 위해서는 IP주소가 필요하지만 Bootstrapping 문제로 키 교환 과정이 이루어질 수 없으며, 신뢰된 제 3자로부터 키를 받을 수 없다.

2. 관련 연구



(그림 1) SEND 프로토콜 메시지의 무결성 문제

[표 1] SEND 프로토콜의 보안 위협

	ND Protocol	SEND Protocol	Enhanced SEND Protocol
Non-repudiation	Low	High	High
Integrity	Low	High	High
Confidentiality	Low	Low	High

SEND 프로토콜은 ND 프로토콜에 보안 기능을 제공하기 위해 메시지의 서명 정보를 입력하는 RSA Signature option과 서명 정보 생성에 사용한 키 소유주임을 증명하기 위해 자신의 CGA 주소 생성시 사용한 값들을 입력하는 CGA option을 추가하였다. 두 옵션은 메시지 무결성은 제공하지만, 메시지 암호화를 하지 않은 평문 상태로 상대방에게 전송하기 때문에, (그림1)처럼 수신 노드 뿐만 아니라 모든 노드들은 이 메시지의 내용을 볼 수 있다. 이 기밀성 문제는 개인의 privacy 정보를 중요하게 여기는 요즘 추세에 역행하는 행위이며, 또한 공격 노드는 자신이 수신할 수 있는 모든 메시지의 변조 여부까지 확인할 수 있기 때문에 다른 네트워크에 공격을 시도하기 위한 기초 정보의 정확성까지 확인하여 수집할 수 있다. [표 1]은 SEND 프로토콜의 보안 위협을 나타낸 표이다.

3. 제안 사항

3.1 Encrypted Symmetric Key option 정의

본 논문에서는 암호화된 대칭 키 전송을 위하여 Encrypted Symmetric Key option 필드를 (그림1)과 [표1]처럼 정의 하였다.

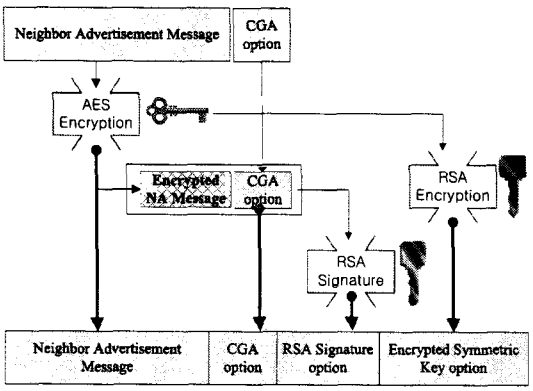
Type (17)	Length	Reserved
Symmetric Key Hash		
Encrypted Symmetric Key		
Padding		

(그림 2) Encrypted Symmetric option field

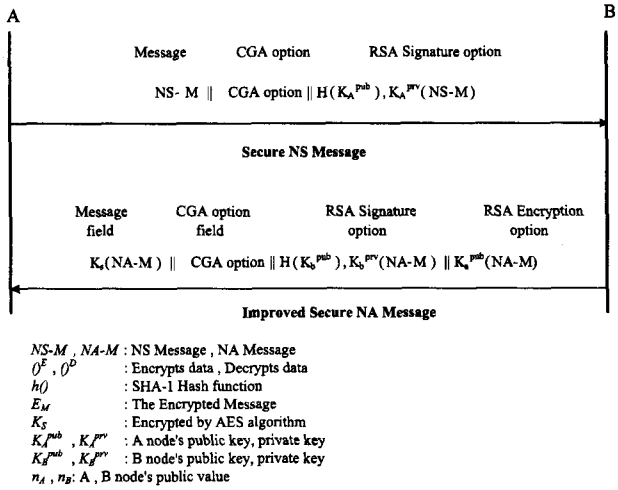
[표 2] Encrypted Symmetric Key option 필드 값

필드 이름	입력값
Type	17
Length	Option 필드의 전체 길이
Reserved	예약된 필드
Symmetric Key Hash	대칭 키의 해쉬 값의 왼쪽 128bit
Encrypted Symmetric Key	대칭 키를 암호화한 값
Padding	비트수를 맞추기위한 비트

3.2 Secure NA 메시지 암호화 기법



(그림 3) 기밀성을 제공하는 SEND 프로토콜 구조



(그림 4) 시퀀스 다이어그램

(그림 3)과 (그림 4)는 SEND 프로토콜 메시지에 기밀성을 제공하기 위한 방법이다. 그 절차는 다음과 같다.

1. Secure NS 메시지에 대한 검증을 한다. (기존의 SEND 프로토콜에서 하는 방법과 동일함.)
2. 전송할 NA 메시지 필드와 CGA 옵션 필드를 채우고, 임의의 128bit 대칭 키를 생성 한다.
3. 임의의 128bit 대칭 키를 사용하여 NA 메시지를 AES 암호화 알고리즘으로 암호화 한다.
4. NA 메시지 송신자의 비밀 키로 암호화된 NA 메시지와 CGA 옵션에 대한 서명 정보를 생성한다.
5. NS 메시지의 서명정보 검증에 사용된 공개 키로 128bit 대칭 키를 RSA 알고리즘으로 암호화 한다
6. 암호화된 NA 메시지는 Neighbor Advertisement Message 필드에, CGA 주소 생성에 사용한 입력 값은 CGA option필드에, 생성된 서명 정보는 RSA Signature option 필드에 입력하고, 암호화된 대칭 키는 본 논문에서 정의한 Encrypted Symmetric Key option 필드에 입력한 후 전송한다.

5. 결론

키 교환 과정이나 키 분배 과정을 사용하지 않고 대칭 키 알고리즘을 이용한 메시지 암호화 방식을 제안하였다. 대칭 키를 전달하기 위한 방법으로 RSA 기반의 전자 서명과 암호화 방식에서 사용되는 공통적인 특징을 이용하고, 암호화 된 대칭 키는 복호화 키를 소유 하고 있는 수신자만이 메시지를 볼 수 있기 때문에 SEND 프로토콜 메시지의 기밀성을 유지할 수 있다. 뿐만 아니라 두 노드 사이에 다른 프로토콜을 사용하여 정보를 교환할 때 SEND 프로토콜에서 사용한 대칭 키를 사용하면 메시지 암호화에 필요한 키 교환 과정을 줄일 수 있다.