Mobile IPv6용 IPSec Core Module의 하드웨어 설계 및 구현

신민철[O] 류준우 김경태 공인엽 이정태
부산대학교 컴퓨터공학과
{mcshin78[O], jwryu, ktkim, leafgirl, jtlee}@pusan.ac.kr

Hardware Design and Implementation of IPSec Core Module for Mobile IPv6

Min-Chul Shin[O] June-Woo Ryu Kyung-Tae Kim In-Yeup Kong Jung-Tae Lee
Dept. of Computer Engineering, Pusan National University

요 약

Mobile IPv6는 차세대 인터넷 프로토콜인 IPv6를 기반으로 단말기기간에 이동성을 제공하는 프로토콜이다. 하지만 Mobile기기간의 정보 유출 및 서비스 거부 등과 같은 공격에 대해 보안 서비스의 필요성이 대두되었다. 이에 IPSec 프로토콜은 이러한 요구사항을 만족시켜 줄 수 있는 다양한 보안 서비스를 제공함에 따라 Mobile IPv6에서는 필수 구현사항으로 채택하고 있다. 이에 IPSec 프로토콜을 하드웨어로 모듈화함으로써 소프트웨어상에서 발생하는 단점을 제거하고, 하드웨어상의 Mobile기기와도 손쉽게 인터페이스 할 수 있도록 구현하였다. IPSec Core Module은 AH 및 ESP를 각각 송수신하는 모듈과 IPSec Control 모듈로 구성 하였으며, IPv6 테스트 망을 이용하여 전용 FPGA보드상에서 그 기능을 검증하였다.

1. 서 론

인터넷과 이동 통신의 확산에 따라 무선 환경에서 인터넷을 이용하고자 하는 요구가 크게 늘고 있다. 이러한 요구를 충족시키기 위해 IETF(Internet Engineering Task Force)에서는 Mobile IP 프로토콜을 제안하여 인터넷에 대한 무선 환경에서의 이동성을 제공해 주고자 하였다. 하지만 기존의 Mobile IPv4는 삼각 라우팅(Triangular Routing)과 같은 통신상의 문제점을 내재하고 있기 때문에 차세대 인터넷 프로토콜인 IPv6를 기반으로 하는 Mobile IPv6로의 개선이 요구되고 있다.

그러나, Mobile IPv6의 경우에 있어서도 Mobile 기기간의 정보 유출 및 서비스 거부(DoS)등과 같은 다양한 공격에 노출되어 있기 때문에 Mobile 기기에 대한 보안 서비스가 필요하다. 이에 대해 Mobile IPv6에서는 IP 계층에서 보안 서비스를 제공해 줄 수 있는 프로토콜인 IPSec(IP Security)을 제안하였다.

하지만, IPSec 프로토콜은 대부분 소프트웨어를 기반으로 구현되고 있고, 이는 특정 OS(Operating System)에 의존적일 뿐만 아니라, 고속의 알고리즘 처리시 성능 저하 및 소규모 기기에 적용할 수 없는 문제가 있으므로 무선 이동 통신 단말기에서 적용하기에는 적합하지 않다.

본 논문에서는 이러한 문제를 해결하기 위해 IPSec 프로토콜을 하드웨어로 설계 및 구현하여 소프트웨어 기반의 IPSec이 갖는 단점들을 해결하였고, 이를 모듈화하여 Mobile IPv6를 지원하는 하드웨어 모듈과 연동하여 보안 서비스를 제공할 수 있도록 하였다.

2. IPSec 프로토콜

IPSec은 네트워크 계층의 보안 서비스를 제공해 주기 위한 프로토콜로써 접근제어(Access Control), 무결성(Integrity), 데이터 발신 인증(Data Origin Authentication), 재전송 방지(Anti-Reply), 기밀성(Confidentiality) 및 제한적 트래픽 흐름의 기밀성(Limited Traffic Flow Confidentiality)을 포함한다. IPSec은 트래픽 보안을 위해 AH 및 ESP 프로토콜을 사용하는데, Mobile IPv6에서는 ESP 프로토콜을 기본으로 사용하므로 여기서는 ESP 프로토콜을 주로 다룬다.

2.1 ESP 프로토콜

ESP(Encapsulating Security Payload) 프로토콜은 상위 계층의 데이터에 대한 기밀성을 제공해 주기 위해 암호화된 데이터를 포함하는 프로토콜이다. IANA에서 지정한 프로토콜 번호는 50이며, ESP 프로토콜을 위한 확장 헤더의 구조는 그림 1과 같다.

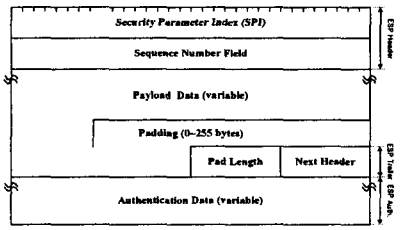
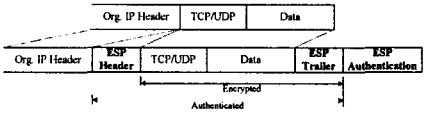


그림 1. ESP 프로토콜의 확장 헤더

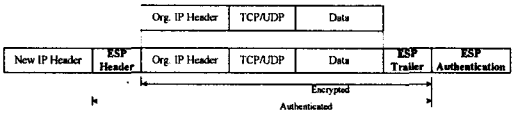
SPI(Security Parameters Index)필드는 임의의 32비트 값으로서, 목적지 IP 주소와 함께 SA(Security Association)를 식별하는 역할을 한다. 32비트의 Sequence Number 필드는 패킷이 전송될 때마다 1씩 증가하는 일련번호를 포함한다. 수신측에서는 이 필드를 이용하여 중복된 패킷을 체크함으로써, 재전송 공격을 방지할 수 있다. Next Header는 Payload Data 필드에 포함된 상위 프로토콜을 식별하기 위해 사용한다. Payload Data는 Next Header 필드에 의해 기술되는 상위 데이터를 포함하는 가변길이 필드이다. ESP 확장 헤더는 4바이트의 정수배로

정렬되어야 하는데 이를 위해서는 Padding이 추가될 수 있다. Pad Length는 정렬을 위해 추가한 Padding의 바이트 수를 나타내며, 0~255사이의 값으로 표시한다.

ESP 프로토콜 헤더의 위치는 그림 2에 표시한 바와 같으며, 암호화의 적용범위는 상위 프로토콜에서부터 ESP Trailer까지 해당된다.



(a) ESP Transport Mode



(b) ESP Tunnel Mode

그림 2. ESP 프로토콜

그림 2에서 Transport Mode는 주로 상위 계층의 프로토콜을 위해, Tunnel Mode는 터널링된 IP 패킷에 대한 보안 서비스를 제공하는데, 이 두 Mode는 AH에서도 동일하게 적용된다.

2.2 AH 프로토콜

AH(Authentication Header) 프로토콜은 ESP와 유사한 확장헤더로서, IP 패킷에 대한 무결성을 제공한다. ESP는 상위 계층의 데이터만을 인증하는데 비해 AH는 IP 패킷 전체에 대한 인증 여부를 결정한다.

2.3 Mobile IPv6에서의 IPSec

Mobile IP는 MN(Mobile Node)가 네트워크를 이동하였을 때 기존의 연결을 유지하면서 통신이 가능하도록 이동성을 제공한다. 특히 Mobile IPv6는 Address auto-configuration이나 Neighbor Discovery 메커니즘과 같이 IPv6에서 지원하는 기능들을 사용함으로써 IPv4보다 간단한 방법으로 이동성을 지원할 수 있다. 또한, MN는 BU(Binding Update) 메시지를 통해 자신의 HA(Home Agent)나 CN(Correspondent Node)에게 자신의 새로운 CoA(Care-of-Address)를 알리게 되는데 BU 과정에서의 보안의 취약성으로 인해 다양한 공격 기법이 가능하며 새롭게 추가된 패킷 옵션에서 역시 취약성이 알려져 있다. 이러한 취약성들로 인해 DoS(Denial of Service)공격, MITM(Man-In-The-Middle) 공격, hijacking등 다수의 공격기법이 가능하다.

따라서 Mobile IPv6에서의 안전한 통신을 위해서는 IPSec과의 연동이 필수적이며, BU에서와 같은 보안의 취약성을 해결하기 위하여 AH나 ESP를 적용함으로써 송수신 패킷에 대한 무결성 및 기밀성을 제공해 줄 수 있다.

3. Mobile IPv6를 위한 IPSec Core Module의 설계 및 구현

3.1 하드웨어 IPSec Core Module

전체 하드웨어 IPSec System의 구성도는 그림 3과 같다. IPSec Core Module과 통신하는 나머지 모듈들은 본 연구실에서 기 구현한 모듈을 사용하였다[6][7].

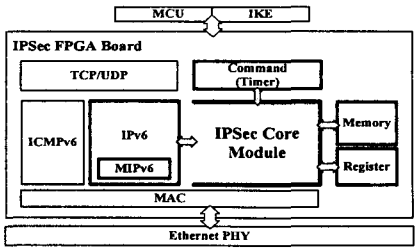


그림 3. 하드웨어 IPSec System 구성도

3.2 세부 Module

구현한 하드웨어 IPSec Core Module의 세부 구조는 그림 4와 같다.

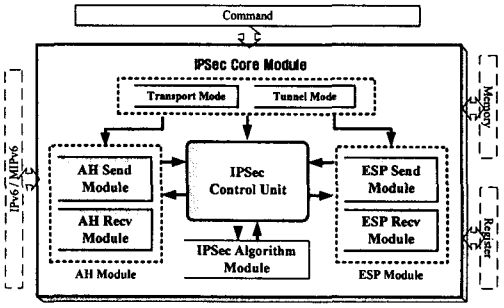


그림 4. 하드웨어 IPSec Core Module의 세부 모듈 구성

IPSec Core Module의 내부는 보안 서비스의 종류에 따른 AH와 ESP Module, 그리고 이를 제어하기 위한 Control Unit으로 구성된다. AH와 ESP Module은 각각 송신(Send)과 수신(Recv) Module을 분리하였다. 다음절에서는 대표적으로 ESP Send Module에 대해서 자세히 설명하고, 그 외 나머지 모듈에 대해서는 시그널 정의 및 동작 메커니즘이 유사하기 때문에 구체적인 설명은 생략한다.

IPSec Algorithm Module은 IPSec에서 요구되는 HMAC-MD5, HMAC-SHA-1, 3DES, AES를 포함하며, IPSec Control Unit과 표준화된 인터페이스로 동작한다. 이는 본 연구실에서 기 구현한 모듈을 사용하였다[7].

3.2.1 ESP Module

ESP Module은 상위 계층의 데이터에 대한 암호화 및 복호화를 통해 기밀성을 보장하기 위한 기능을 제공한다. ESP Send Module은 ESP 프로토콜 헤더를 생성하고 Payload Data 필드에 들어갈 상위 계층의 데이터를 알고리즘 모듈로부터 암호화하여 Start 시그널에 따라 송신하도록 구현하였다.

ESP Send Module은 Command, Register, Control 모듈과의 통신을 통해 헤더를 생성하여 전송하는 기능을 담당한다. ESP Send Module의 블록다이어그램은 그림 5와 같고, 인터페이스 정의는 표 1과 같다.

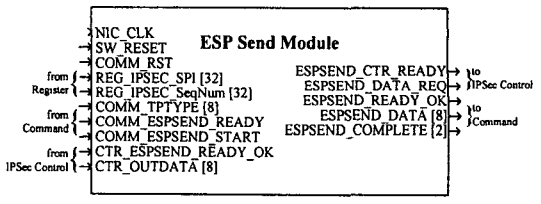


그림 5. ESP Send Module

표 1. IPSec ESP Send Module의 인터페이스 정의

인터페이스	설 명	I/O
NIC_CLK	클럭	In
SW_RESET	하드웨어 Reset	In
COMM_RST	Command Reset	In
REG_IPSEC_SPI	레지스터에 저장된 SPI값	In
REG_IPSEC_SEQNUM	레지스터에 저장된 순서번호	In
COMM_TPTYPE	상위 프로토콜의 유형	In
COMM_ESPSEND_READY	ESP 송신의 준비 시그널	In
COMM_ESPSEND_START	ESP 송신의 시작	In
ESPSEND_READY_OK	CTR이 ESPS 준비완료	In
ESPSEND_CTR_READY	CTR의 준비요청	Out
ESPSEND_DATA	최종 ESP 헤더 출력	Out
ESPSEND_COMPLETE	현재 진행상황 보고	Out
ESPSEND_DATA_REQ	암호화 데이터를 요청	Out
CTR_ESPSEND_READY_OK	IPSec_CTR이 ESPS준비완료	Out
CTR_OUTDATA	IPSec_CTR에서의 데이터수신	In

ESP 송신 과정은 그림 6에서 보는 바와 같이 암호화 이전에 ESP 헤더를 구성하기 위한 A 단계와 암호화된 데이터를 전송하기 위한 B단계의 두 단계로 이루어진다.

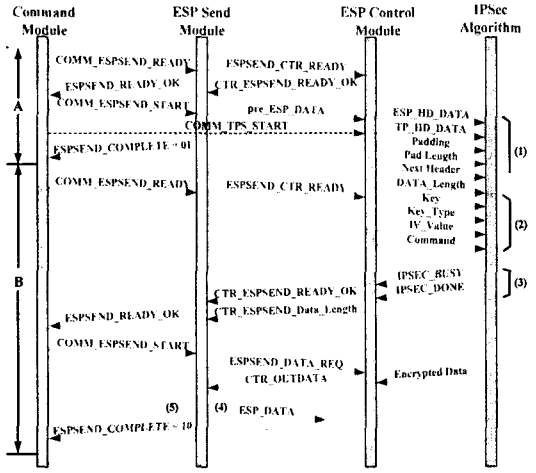


그림 6. ESP Send Module의 송신 절차

각 단계에서는 공통적으로 전송준비를 위한 Ready과정과 실제 헤더를 출력하는 Start과정을 반복적으로 진행한다. 먼저 ESP 헤더를 비롯하여 상위 데이터 및 패딩 값을 알고리즘 모듈로 전송하고(1), 이어서 레지스터의 설정 값도 전송한다(2). IPSec Control Module은 알고리즘 모듈의 진행상황을 모니터링하는데(3), 암호화가 완료되면 ESP Send Module을 통해 최종 ESP 헤더를 출력하고(4), 이와 동시에 처리 결과를 보고함으로써 동작을 완료한다(5).

ESP Recv Module은 수신한 ESP 프로토콜 헤더 내의 암호화된 데이터를 복호화하여 해당하는 상위 프로토콜로 전송하도록 구현하였으며 동작 메커니즘은 ESP Send Module과 유사하게 구현하였다.

3.2.2 AH Module

AH Module은 그림 4에서 보는 바와 같이 AH Send Module과 AH Recv Module로 구성된다. AH Send Module은 IP 패킷 전체를 차례대로 알고리즘 모듈로 전송하고, 알고리즘 모듈에 의해 계산된 Integrity Value를 이용하여 최종 AH를 구성한 후, Start 시그널에 따라 AH를 송신하도록 구현하였다. AH Recv Module은 수신한 AH 프로토콜 헤더 내부의 Authentication Data 필드와 알고리즘 모듈을 통해 계산된 값을 비교하여 수신한 IP 패킷에 대한 무결성을 체크하고 이를 보고하도록 구현하였다.

3.2.3 IPSec Control Module

IPSec Control Module은 AH 및 ESP Module과 IPSec Algorithm Module 사이에서 각 모듈을 제어하는 역할을 한다. 암호화/복호화에 필요로 하는 파라미터 값을 해당 모듈로 전송하고, 각각의 모듈에 대한 제어신호를 생성하는 중요한 기능을 담당한다.

3.3 구현 및 검증

하드웨어 IPSec Core Module은 VHDL을 사용하여 각각의 세부 모듈을 구현한 후, 이를 통합하였다. 구현된 모듈의 검증에 있어서는 먼저 소프트웨어 시뮬레이션을 수행하였고, 전용 FPGA 보드에 탑재한 후 PC 기반의 IPSec 호스트와의 테스트를 통해 그 기능과 호환성을 검증하였다.

4. 결론

본 논문에서는 Mobile IPv6에서 보안 서비스를 제공하기 위한 IPSec 프로토콜을 하드웨어로 설계 및 구현하였다. 본 논문에서 구현한 Mobile IPv6용 하드웨어 IPSec 프로토콜은 기존의 소프트웨어 IPSec 프로토콜이 가지고 있는 특정 OS의 의존성과 고속 처리시 성능 저하 문제, 소형화가 어려운 문제점을 해결하여 무선 환경에서 효율적이면서도 안전한 인터넷 서비스가 가능하도록 하였다.

향후 과제로는 구현한 IPSec Core Module을 최적화하여 FPGA상에서의 면적을 최소화하고, 전송속도를 향상시킬 수 있도록 최적화 시키는 것이다.

참고 문헌

[1] S. Deering and B. Hinden, "Internet Protocol, Version 6(IPv6) specification", IETF RFC 2460, December 1998.

[2] S. Kent, "IP Authentication Header(AH)", IETF RFC 2402, November 1998.

[3] R. Atkinson, IP Encapsulating Security Payload(ESP)", IETF RFC 2406, November 1998.

[4] Neil Dunbar, "IPSec Networking Standards", Information Security Technical Report, Vol. 6, No. 1, pp.35-48, 2001.

[5] 김경태 외 2명, "IPv6용 IPSec 프로토콜의 하드웨어 설계 및 구현", 2002년 한국정보과학회 가을학술발표논문집(III), 제29권, 제2호, 385-387, October 2002.

[6] 박동익 외 3명, "IPv6용 하드웨어 IPsec을 위한 키 교환 시스템의 설계 및 구현", 2002년 한국정보과학회 가을학술발표논문집(III), 제29권, 제2호, pp.415-417, Oct. 2002.

[7] 김지욱 외 1명, "IPv6 보안시스템용 HMAC-SHA-1 하드웨어 모듈의 설계 및 구현", 2002년 한국정보과학회 가을학술발표논문집(III), 제29권, 제2호, pp.277-279, Oct. 2002.