IPv6용 IPsec 프로토콜의 하드웨어 설계 및 구현

김경태° 류준우 이정태
부 산 대 학 교 컴 퓨 터 공 학 과
(ktkim°, jwryu, jtlee)@pusan.ac.kr

Hardware Design and Implementation of IPsec Protocol for IPv6

Kyung-Tae Kim° Jun-Woo Ryu Jung-Tae Lee
Dept. of Computer Engineering, Pusan National University

요 약

인터넷 상에서 IP 주소의 부족 문제를 해결하기 위해 IPv6 프로토콜이 제안되었고 현재 실용화 단계에 접어들었다. IPv6에서는 보안기능의 강화를 위해 IPsec 프로토콜을 기본 요구사항으로 채택하였고, 본 논문에서는 이러한 IPsec 프로토콜을 하드웨어로 설계하고 구현하였다. 이를 위해 IPv6에서 보안기능을 담당하는 헤더와 IPsec의 기본 암호화 알고리즘을 설계하여 각각 VHDL로 구현하였고, 전용 FPGA 보드와 IPv6 테스트망에서 그 기능과 성능을 검증하였다. 구현된 IPsec 프로토콜 칩은 TCP/IPv6와 IPsec 프로토콜을 하나의 칩으로 구현함으로써 별도의 프로세서 없이 인터넷 접속 기능과 보안기능을 동시에 제공하며 소프트웨어 모듈보다 뛰어난 성능을 나타낸다.

1. 서 론

최근 초고속 통신망의 보급 등으로 인한 인터넷 이용자들의 폭발적인 증가로 인하여 IP 주소의 부족 문제가 제기되었다. 또한, 인터넷을 통한 전자상거래 등이 증가함에 따라 인터넷의 보안 기능에 대한 요구가 크게 늘어났다. 이를 해결하기 위해 차세대 IP 프로토콜인 IPv6 프로토콜이 제안되었고, 현재 IPv6에 대한 많은 연구가 이루어 지고 있다. IPv6 프로토콜은 기존의 IPv4에 비해 128bit의 넓은 주소 영역으로 주소 부족 문제를 해결하였을 뿐만 아니라 IPv6에서는 IPsec 프로토콜을 기본 요구사항으로 채택함으로써 인터넷 상에서의 보안 서비스를 제공한다[1].

그러나, 기존의 IPsec 프로토콜은 OS(Operating System)내에 소프트웨어로 구현되어 있기 때문에 OS가 지원되지 않는 소규모의 기기에는 적용 할 수 없으며, 성능면에서도 한계가 있다. 따라서 본 논문에서는 IPsec 프로토콜을 하드웨어로 설계하고 구현함으로써, TCP/IPv6 프로토콜의 인터넷 접속 및 데이터 전송 기능과 IPsec 프로토콜의 보안 기능을 OS 없이 동시에 제공할 수 있도록 하였다.

하드웨어 IPsec 프로토콜 모듈은 IPv6에서 보안기능을 제공하는 AH (Authentication Header), ESP (Encapsulating Security Payload) 확장 헤더 모듈과 암호화 알고리즘 모듈로 나뉜다. AH, ESP 확장 헤더 모듈은 본 연구실에서 기 구현된 TCP/IPv6 프로토콜 모듈을 기반으로 설계 및 구현하였고 별도의 인터페이스를 정의하여 암호화 알고리즘 모듈과의 상호 통신이 가능하도록 하였다. 암호화 알고리즘 모듈은 IPsec에서 사용되는 알고리즘인 3DES, AES, HMAC-MD5, HMAC-SHA-1의 네 가지 모듈을 설계 및 구현하였다.

하드웨어로 구현된 IPsec 프로토콜의 테스트에 있어서는 전용 FPGA 보드를 제작하고 별도의 IPv6 시험망을 구축하였다. 이를 기반으로 IPsec 프로토콜의 동작을 검증하였고, 그 결과 소프트웨어 스택의 IPsec 프로토콜 보다 뛰어난 처리 속도를 나타내었다.

2. IPsec 프로토콜

IPsec 프로토콜은 IPv6에서 AH, ESP 확장 헤더의 형태로 구현되며 제공되는 보안 기능은 표 1과 같다[2].

표 1. IPsec 프로토콜의 보안 서비스

보 안 서 비 스	AH	ESP
접근제어 (Access Control)	O	O
비연결성 무결성 (Connectionless Interity)	O	O
데이터 발신 인증 (Data Origin Authentication)	O	O
재전송 방지 (Anti-Replay)	O(opt)	O
비밀성 (Confidentiality)		O
재한적 트래픽 흐름의 비밀성 (Limited Traffic Flow Confidentiality)		O

이러한 기능을 제공하기 위해 IPsec 프로토콜은 3DES, AES, HMAC-MD5, HMAC-SHA-1의 네 가지 암호화 알고리즘을 규정하고 있다.

2.1 AH 헤더

AH 헤더의 구조는 그림 1과 같다[2][3].

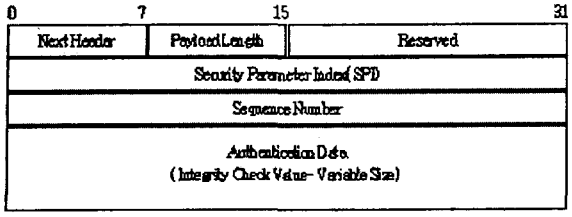

그림 1. AH 헤더의 구조

" Next Header" 는 AH 헤더 다음에 나타날 헤더 또는 페이로드의 형태를 지정하는 8비트 필드로서 IANA(Internet Assigned Numbers Authority)에서 지정한 값을 사용한다. " Payload Length" 는 4바이트 단위로 계산되는 전체 길이에서 2를 뺀 값이 저장된다. 일반적으로 4 값을 가지며, 디버깅을 위한 ' null' 인증을 사용하는 경우에는 1(IPv4) 또는 2(IPv6)의 값으로 설정된다. " Reserved" 필드는 항상 0 값을 갖는다. " SPI(Security Payload Index)" 필드는 32비트로 유일한 SA를 식별하는데 사용되는 인자{SPI, AH, 목적지주소} 중 하나이다. " Sequence Number" 필드는 unsigned 32비트 값으로 SA가 설정될 때 송수신측에서 모두 0으로 셋팅된다. 그 후 송신측에서는 전송시마다 그 값을 1씩 증가시키고 수신측에서는 이 값을 체크하여 재전송 공격(Replay Attack)을 검사한다. " Authentication Data" 필드는 4바이트의 정수배 크기로 ICV(Integrity Check Value) 값을 저장하는 필드이다. 여기서 ICV는 인증과 데이터의 무결성을 위해 사용되는 값이다. Authentication Data의 길이는 가변이므로 패딩을 추가하여 IPv4에서는 32비트의 정수배, IPv6에서는 64비트의 정수배로 AH의 크기를 맞춰 준다.

2.2 ESP 헤더

ESP 헤더의 구조는 그림 2와 같다[2][4].

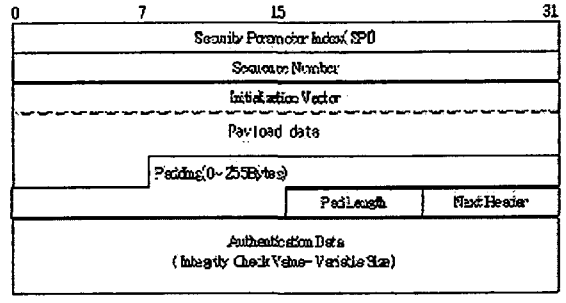

그림 2. ESP 헤더의 구조

"Security Payload Index" 와 " Sequence Number", " Next Header", " Authentication Data" 필드는 AH 헤더의 각 필드와 동일한 용도로 사용된다. " Payload Data" 는 Next Header 필드에서 지정한 상위 계층의 데이터가 기록되는 가변 길이의 필드로서, 암호화 알고리즘에서 사용하는 초기 값인 Initialization Vector를 앞부분에 포함하고 있다. " Padding" 은 바이트 정렬을 맞추기 위해 사용되는 필드로 0~255 사이의 값을 가질 수 있으며, 패딩된 크기는 " Pad Length" 필드에 기록된다.

2.3 암호화 알고리즘

IPsec에 사용되는 암호화 알고리즘은 3DES, AES, HMAC-MD5, HMAC-SHA-1의 네가지가 표준으로 정의되어 있다. 3DES[5]는 64비트의 키를 사용하는 대칭키 구조를 가지는 블록 암호화/복호화 알고리즘이다. AES는 128비트의 키를 사용하는 대칭키 구조의 블록 암호화/복호화 알고리즘이다. HMAC-MD5[6]는 128비트의 MD5 해시 결과값에 키를 적용하여 96비트의 인증 데이터를 생성하는 알고리즘이다. HMAC-SHA-1[7]은 160비트의 SHA-1 해시 결과값에 키를 적용하여 96비트의 인증 데이터를 생성하는 알고리즘이다.

3. 하드웨어 IPsec 프로토콜의 설계 및 구현

3.1 하드웨어 IPsec 프로토콜

하드웨어 IPsec 프로토콜의 전체 구조는 그림 3과 같다.

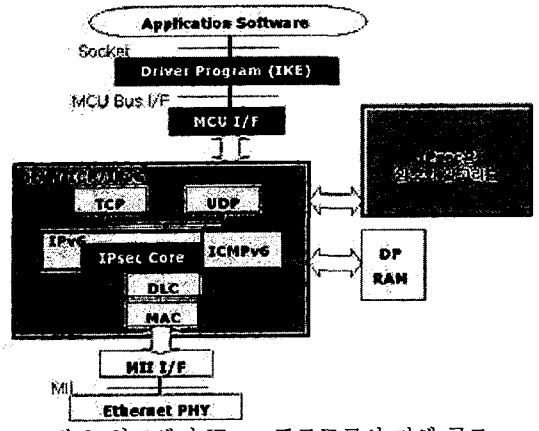

그림 3. 하드웨어 IPsec 프로토콜의 전체 구조

MCU는 상대 호스트와 키와 사용 알고리즘을 협상하는 IKE 드라이버 프로그램을 구동시키고, 전체 모듈을 제어하는 마이크로 컨트롤러이다. AH, ESP 헤더를 처리하는 IPsec Core 모듈은 기 구현된 하드웨어 TCP/IPv6 프로토콜 모듈을 기반으로 구현하였다. Ethernet PHY와 연동하기 위해서는 MII 인터페이스를 사용하였으며, IPsec Core에서 사용하는 암호화 알고리즘은 별도의 인터페이스를 정의하여 모듈화 하였다. IKE 드라이버의 구현에 관한 내용은 별도의 논문으로 제출하였다[8].

3.2 IPsec Core 모듈

IPsec Core 모듈의 구조는 그림 4와 같다.

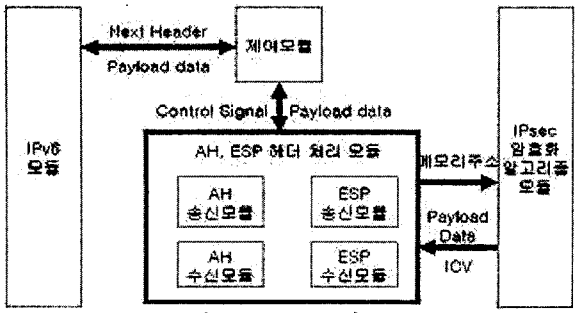

그림 4. IPsec Core의 구조

제어모듈은 IPv6 모듈과 통신을 통해 주고 받는 IP 패킷의 AH, ESP 헤더 사용 유무를 체크하여 AH, ESP 헤더 처리 모듈을 구동시키는 등의 전체 동작을 제어하는 역할을 한다. AH, ESP 헤더 처리 모듈은 크게 AH 송신모듈, AH 수신모듈, ESP 송신모듈, ESP 수신모듈로 나뉘며 각각 AH와 ESP 헤더를 송수신하는 역할을 한다. 이때, AH와 ESP 헤더에 들어가는 ICV 값과 Payload Data는 암호화 알고리즘과 상호 통신을 통해 생성된다.

3.3 IPsec용 암호화 알고리즘 모듈

암호화 알고리즘 모듈의 구조는 그림 5와 같다.

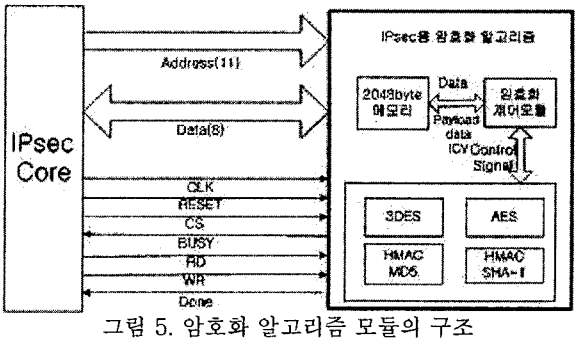

그림 5. 암호화 알고리즘 모듈의 구조

2048byte의 메모리는 각각 암호화 알고리즘에 사용할 데이터와 결과 값을 제공하기 위해 사용된다. 암호화 제어모듈은 IPsec Core로부터 데이터를 패치하고 결과 값을 리턴하는 등의 전체 동작을 통제하는 역할을 한다. 3DES, AES, HMAC-MD5, HMAC-SHA-1 모듈은 암호화 제어모듈의 명령에 따라 데이터를 암호화/복호화 하거나 인증 데이터를 생성한다. AES[9]와 HMAC-SHA-1[10]의 구현은 별도의 논문으로 정리하였다.

3.4 구현과 검증

하드웨어 IPsec 프로토콜은 각각의 모듈 별로 VHDL을 사용하여 구현한 후 통합하였다. 각 모듈들의 동작을 검증하기 위해서는 소프트웨어 시뮬레이션 툴을 사용하였고 전체 모듈의 동작은 별도의 FPGA 보드를 제작하여 테스트 하였다. 동작 검증을 위한 테스트 환경은 그림 6과 같다.

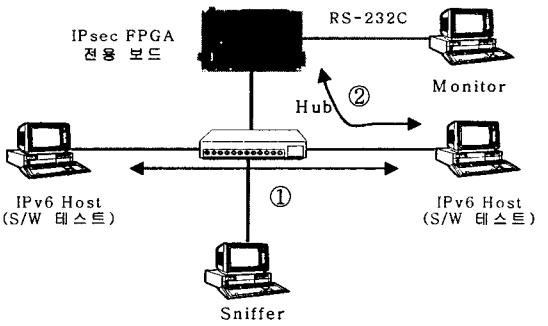

그림 6. 하드웨어 IPsec 프로토콜의 테스트 환경

먼저 IPv6 Host간의 통신을 통하여 소프트웨어 IPsec 프로토콜의 동작을 테스트하였다(①). 그리고 구현된 IPsec 프로토콜은 IPsec FPGA 전용보드에 탑재하여 IPv6 Host와의 보안 통신을 수행함으로써 기능을 검증하였다(②).

4. 결론 및 향후 과제

IPv6에서 기본 요구사항으로 정의된 보안 프로토콜인 IPsec은 OS에 종속적인 소프트웨어로 구현되어 있어 OS가 지원되지 않는 기기에는 적용할 수 없고 성능면에도 한계가 있다. 이를 해결하기 위해 본 논문에서는 OS가 지원되지 않는 장치에 인터넷 접속 기능과 보안기능을 동시에 제공 할 수 있는 IPv6용 IPsec 프로토콜을 하드웨어로 설계하고 구현하였다. 테스트 결과 하드웨어 IPsec 프로토콜 모듈은 기존 소프트웨어 모듈과 호환되며 소프트웨어 모듈간의 전송속도보다 나은 성능을 나타내었다. 향후 과제로는 IPsec Core 모듈과 암호화 알고리즘 모듈을 최적화 하여, FPGA에서 사용하는 회로 면적을 줄이고 전송 속도를 향상시키는 연구를 진행할 예정이다.

5. 참고문헌

[1] 이정태 외 9명, "USB 카메라용 인터넷어댑터 설계 결과보고서", wiznet㈜, Dec. 2001
[2] 한국전자통신연구원, "IPsec 표준화 동향 및 제품 현황", 주간기술동향 952호
[3] S. Kent , "IP Authentication Header(AH)", IETF RFC 2402 Nov. 1998
[4] R. Atkinson, IP Encapsulating Security Payload (ESP)", IETF RFC 2406, Nov. 1998
[5] C. Madson, "The ESP DES-CBC Cipher Algorithm With Explicit IV", IETF RFC 2405, Nov. 1998
[6] C. Madson, "The Use of HMAC-MD5-96 within ESP and AH", IETF RFC 2403, Nov. 1998
[7] C. Madson, "The Use of HMAC-SHA-1-96 within ESP and AH", IETF RFC 2404, Nov. 1998
[8] 박동익 외 3명, "IPv6용 하드웨어 IPsec을 위한 키 교환 시스템의 설계 및 구현", 정보과학회 추계 학술대회 제출, 2002
[9] 김경태 외 5명, "IPv6용 AES 하드웨어 모듈의 설계 및 구현", 멀티미디어학회, May. 2002
[10] 김지욱 외 1명, "IPv6용 HMAC-SHA-1 하드웨어 모듈의 설계 및 구현", 정보과학회 추계 학술대회 제출, 2002