IPv6 보안시스템용 HMAC-SHA-1 하드웨어 모듈의 설계 및 구현

김지욱° 이정태*
° 부산대학교 정보시스템공학과
* 부산대학교 컴퓨터공학과
(jwkim8, jtlee)@pusan.ac.kr

Design and Implementation of HMAC-SHA-1 Hardware Module for IPv6 Security System

Ji-Wook Kim° Jung-Tae Lee*
° Department of Information System Engineering, Pusan National University
* Department of Computer Engineering, Pusan National University

요 약

전자상거래, 무선 인터넷 등의 활성화를 위해서는 신뢰성있는 통신 서비스를 제공하는 IPv6용 보안시스템이 필요하다. 이를 위한 기존의 암호화 알고리즘은 소프트웨어 및 하드웨어로 많이 구현되어 있으나 IPv4를 기반으로 한 운영체제에 종속되어 있다. 이를 해결하기 위하여 운영체제 없이 고성능의 보안서비스를 제공하는 IPv6용 보안시스템이 하드웨어로 구현되었다. 본 논문에서는 이러한 IPv6용 하드웨어 보안시스템에 요구되는 암호화 알고리즘 중에서 HMAC-SHA-1을 하드웨어 모듈로 구현하였다. 그리고 구현한 HMAC-SHA-1 모듈에 대하여 시뮬레이션 테스트를 수행하고 IPv6 하드웨어 보안시스템과 연동함으로써 기능을 검증하였다.

1. 서 론

인터넷 접속을 위한 단말(PC, PDA, 정보가전 등)의 수가 급증하고 있으며 전자상거래, 인터넷 뱅킹 등의 이용이 증가하고 있다. 그러나, 현재의 IPv4는 모든 단말들을 수용할 수 없고 보안에 있어서도 취약하다. 이와 같은 주소 부족과 보안 문제를 해결하기 위하여 차세대 인터넷 프로토콜인 IPv6가 제안되어 실용화 단계까지 진행되고 있다[1].

특히 IPv6의 IPsec(IP security)은 필수적인 요구사항 중의 하나로써 IP 계층에서 암호화와 인증 서비스를 제공한다[2].

IPsec의 기본 암호화 알고리즘으로는 3DES, AES, HMAC- MD5와 더불어 HMAC-SHA-1이 요구되고 있다. 이러한 알고리즘들은 소프트웨어나 하드웨어로 많이 구현되어 있으나 모두 IPv4용으로 운영체제 내 IPv4 스택과의 연동만 가능하다.

본 연구에서는 연구실에서 기 구현된 TCP/IPv6와 IPsec 하드웨어 모듈과 연동되는 HMAC-SHA-1 암호화 알고리즘 모듈을 VHDL로 구현하였고 검증하였다.

본 논문의 구성을 살펴보면, 먼저 2장에서는 IPv6용 보안시스템의 구성을 기술하였고, 3장에서는 IPv6 하드웨어 보안시스템용 HMAC-SHA-1 모듈의 설계에 대해 설명하였으며, 4장에서는 HMAC-SHA-1 모듈의 동작 실험 결과를 보였고 5장에서는 결론을 제시하였다.

2. IPv6용 보안시스템의 구성

2.1 IPv6와 IPsec

IPv6는 IETF에서 제안한 차세대 인터넷 프로토콜로서, QoS나 실시간 서비스 지원, 자동 설정 기능(auto-configuration), 대규모 라우팅 기능에 추가하여 인증, 데이터의 무결성, 데이터의 기밀성 등의 향상된 보안기능을 제공한다.

IPsec은 IP 계층 자체의 보안 서비스를 제공하기 위한 방안으로서 IPsec의 AH(Authentication Header)[3], ESP(Encapsulating Security Payload)[4] 확장 헤더를 통해 구현된다.

AH 프로토콜은 HMAC-MD5와 HMAC-SHA-1을 사용하여 메시지 인증코드(MAC: Message Authentication Code)를 생성함으로써 데이터의 무결성과 인증을 제공한다. 또한 ESP 프로토콜은 3DES, AES 등을 통하여 데이터를 암호화함으로써 IP 패킷의 기밀성을 제공한다.

2.2 HMAC-SHA-1

SHA-1은 1995년 NIST(National Institute of Standards and Technology)에 의해 FIPS PUB 180-1으로 공포된 해쉬 알고리즘으로서, MD4 알고리즘에 기반을 두고 있다. SHA-1의 입력 메시지는 512비트 블록으로 처리되고, 160비트의 해쉬값(Message Digest)이 생성된다[5].

HMAC(Keyed-Hash Message Authentication Code)은 그림 1에서와 같이 FIPS에서 승인한 해쉬 함수, 발신자

(Originator)와 수신자(receiver) 사이에 공유된 비밀키(a shared secret), 그리고 메시지 인증코드를 산출하고자 하는 평문 데이터 등을 조합하여 메시지 인증코드를 생성하는 알고리즘이다[6].

$$MAC(text)_t = HMAC(K,text)_t$$
$$= H((K_0 \text{ XOR opad}) \| H((K_0 \text{ XOR ipad}) \| text))_t$$

text : 데이터를 암호화 해야할 즉, MAC을 계산해야 할 평문 데이터
t : MAC의 byte 수
K : 발신자와 수신자 사이에 공유된 Secret Key
H : FIPS에 공인된 해쉬 알고리즘
B: 64byte block size
K_0: K에 0을 덧붙혀 형성된 B byte길이의 키
x'N' : Hexadecimal notation, 'N' 은 Hexadecimal
ipad: Inner pad; x'36' 이 B번 반복된 길이
opad: Outer pad; x'5c' 이 B번 반복된 길이
||: 연결(Concatenation)
XOR: Exclusive-Orperation

그림 1. HMAC 알고리즘

HMAC-SHA-1은 메시지 인증 코드를 생성하기 위해 SHA-1 해쉬 함수를 사용한 것으로써, 데이터의 무결성과 인증을 제공하는 알고리즘이다. 현재 HMAC-SHA-1에서는 그림 1의 t를 12 바이트, K를 160비트로 정의하고 있다[7].

3. IPv6 하드웨어 보안시스템용 HMAC-SHA-1 모듈의 설계

3.1 IPv6용 하드웨어 보안시스템

IPv6용 하드웨어 보안시스템의 구조는 그림 2와 같으며 MCU, IKE, IPsec core 모듈, HMAC-SHA-1 모듈의 네 부분으로 구성된다[8].

IKE는 상대편 IPv6 호스트와 통신하기 앞서 사용할 암호화 알고리즘과 키를 협상하여 교환하는 역할을 한다[9].

MCU는 IKE를 포함한 드라이버 프로그램의 내용에 따라 전체 모듈을 제어하는 기능을 담당한다.

IPsec core는 IKE로부터 암호화 알고리즘 정보와 사용될 키의 정보와 값을 받아오고, AH 또는 ESP 헤더에 첨부될 메시지 인증코드를 HMAC-SHA-1 칩과 통신하여 생성하는 역할을 한다[10].

HMAC-SHA-1 모듈은 메시지 인증 코드를 생성할 평문 데이터와 160비트의 키를 IPsec core로부터 받아들여 구동되며 수행결과로 생성된 160비트의 해쉬(Hash)값을 다시 IPsec core 모듈에 넘겨준다.

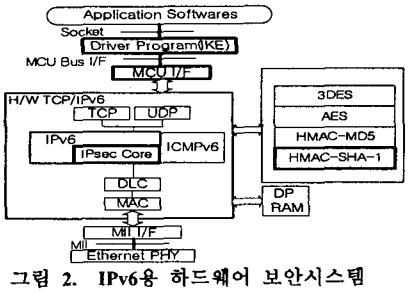

그림 2. IPv6용 하드웨어 보안시스템

3.2. HMAC-SHA-1 모듈의 인터페이스

HMAC-SHA-1 모듈은 IPsec core 모듈과 포트맵(port map)으로 연결된다. 그림 3에서는 두 모듈간의 인터페이스 신호들을 보여주고 있으며 각 신호들의 정의를 기술하면 다음과 같다.

입력신호 중 Data_in은 IPsec 코어로부터 160비트의 해쉬값을 산출할 실제 데이터를 128 비트씩 입력받고, Key_in은 2비트의 Key_type 설정값이 '00', '01', '10', '11' 일 때 각각 128, 160, 196, 256비트의 키를 입력받는다. Data_in_valid, key_in_valid,는 각각 데이터 값 입력, 키 값 입력을 의미하며 유효하면 '1'로 설정된다.

출력신호 중 busy는 모듈이 동작중일 때 '1'로 설정되고 Dout_valid는 해쉬값을 출력할 때 '1'의 값을 가진다. Data_out은 HMAC-SHA-1 모듈의 동작에 의한 160비트의 해쉬값을 IPsec 코어로 되돌려 보낼 경우 사용되는 신호이다.

HMAC-SHA-1에서의 키의 길이는 160비트가 표준으로 고정되어 있다. 그럼에도 불구하고 다른 길이의 키도 입력받을 수 있도록 한 것은 향후 다른 암호화 알고리즘 설계 및 구현을 위해 인터페이스를 통일하고 쉽게 확장 가능하도록 하기 위함이다. Enc_dec, Chip_select도 이런 의미에서 사용되며 본 모듈에서는 큰 의미가 없다.

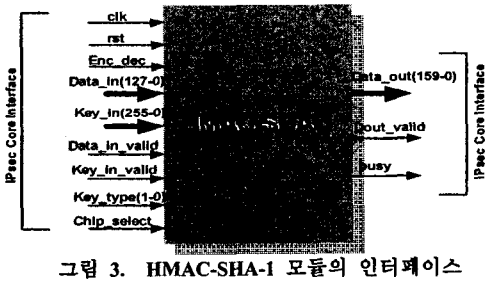

그림 3. HMAC-SHA-1 모듈의 인터페이스

3.3 HMAC-SHA-1 모듈의 세부모듈

HMAC-SHA-1 모듈은 그림 4에서 보는 바와 같이 크게 HMAC 모듈과 SHA-1 모듈의 두가지 모듈로 구성되고, SHA-1 모듈은 내부적으로 5가지 모듈로 구성된다. 각 모듈의 기능을 간략히 설명하면 다음과 같다[11].

1) **HMAC 모듈** : IPsec 코어로부터 데이터와 키를 받아 HMAC 알고리즘을 수행한다. 그 결과로, 블럭(block)의 수와 512비트의 데이터를 SHA-1 모듈에 넘겨주고 SHA-1모듈로부터 생성된 해쉬값을 다시 받아 IPsec 코어로 출력한다.
2) **SHA-1 모듈** : HMAC 모듈로부터 블럭의 수와 512비트의 데이터를 입력받아 SHA-1을 수행한다. 블럭의 수만큼 각각 32비트 크기의IV(Initial Vector)값 H0,H1,H2,H3,H4를 업데이트(Update) 시키고 마지막에 IV값을 결합(concatenation)시킨 160비트의 해쉬값을 HMAC 모듈로 출력한다.

① Controller 모듈 : Counter 모듈, Kt 모듈, Wt 모듈, Md 모듈의 동작을 제어한다.

② Counter 모듈 : 각 20 step씩 네개의 라운드(즉, 80 step)를 비롯해 총 82 step의 카운트를 생성한다.
③ Kt 모듈 : 카운트에 따라 각 라운드마다 정의된 상수값 K를 출력한다.
④ Wt 모듈 : 512비트 입력 데이터로부터 각 step 마다 하나씩 총 80개의 W(32비트)를 생성한다.
⑤ Md 모듈 : HMAC으로부터 입력받은 512비트 블럭의 수, Kt 모듈과 Wt 모듈로부터 입력받은 각 step의 K값과 W값에 대하여 160비트의 해쉬값을 생성한다.

4. HMAC-SHA-1 모듈의 동작 실험

본 논문에서는 IPv6 하드웨어 보안시스템용 HMAC-SHA-1를 VHDL로 구현하였다. 구현된 VHDL 코드는 ModelSim5.2c로 시뮬레이션 하였으며, Synplify Pro 7.0.1에서 로직 합성(logic Synthesis)을 하였다.

HMAC 모듈은 HMAC 알고리즘의 수식을 그대로 구현한 것으로써, 단순하므로 여기에 나타내지 않았다.

그림 5는 SHA-1 모듈이 HMAC 모듈로부터 블럭의 수와 512비트 크기의 데이터를 블럭의 수만큼 입력받아 160비트의 해쉬값을 얻는 과정의 시뮬레이션 결과를 보인 것이다.

5. 결론

IPsec을 위한 암호화 알고리즘은 소프트웨어나 하드웨어로 많이 구현되어 있으나 모두 IPv4용으로 운영체제 내 IPv4 스택과 연동하여 동작한다.

본 논문에서는 IPsec의 고속 처리를 위하여 구현된 IPv6용 하드웨어 보안시스템과 연동되는 HMAC-SHA-1 암호화 알고리즘을 하드웨어 모듈로 설계하여 이를 VHDL로 구현하고 소프트웨어 툴로 시뮬레이션을 수행하였다. 수행결과 SHA-1 모듈에서 소모되는 클럭(clock)의 수는 81 클럭이고 18Mhz에서 114Mbit/s의 성능을 보였다.

향후 과제로는 HMAC-SHA-1 하드웨어 모듈의 회로 면적을 줄이는 최적화 작업과 나머지 AES, 3DES, HMAC-MD5 알고리즘과도 연계하여 하나의 칩으로 구현하는 연구가 행하여질 것이다.

6. 참고 문헌

[1] Mark A. Miller, P.E.,"Implementing IPv6." M&T Books, PP.1~17,Oct.1999.
[2] IETF, "IP security Protocol (IPsec) ", URL http:// www.ietf.org/html.charters/ipsec-charter.html, 2002.
[3] S. Kent, R. Atkinson, "IP Ahthentication Header", IETF RFC 2402, Nov. 1998.
[4] S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)", IETF RFC 2406, Nov. 1998.
[5] NIST, FIPS PUB 180-1, "Secure Hash Standard", Apr. 1995
[6] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", IETF RFC 2104, Feb.1997
[7] C.Madson, R.Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", IETF RFC 2404, Nov. 1998.
[8] 이정태 외 9 명, "USB 카메라용 인터넷어댑터 설계 결과보고서", Dec, 2001.
[9] 김경태 외 2 명, "IPv6 용 IPsec 프로토콜의 하드웨어 설계 및 구현", 정보과학회 추계학술대회 제출, 2002.
[10] 박동익 외 3 명, "IPv6 용 하드웨어 IPsec 을 위한 키 교환 시스템의 설계 및 구현", 정보과학회 추계학술대회 제출, 2002.
[11] K.Y. Lee, J.C. Kwak, "Implementation of a Cryptographic Accelerator for IPsec authentications", ITC-CSCC 2002, Jul. 2002.

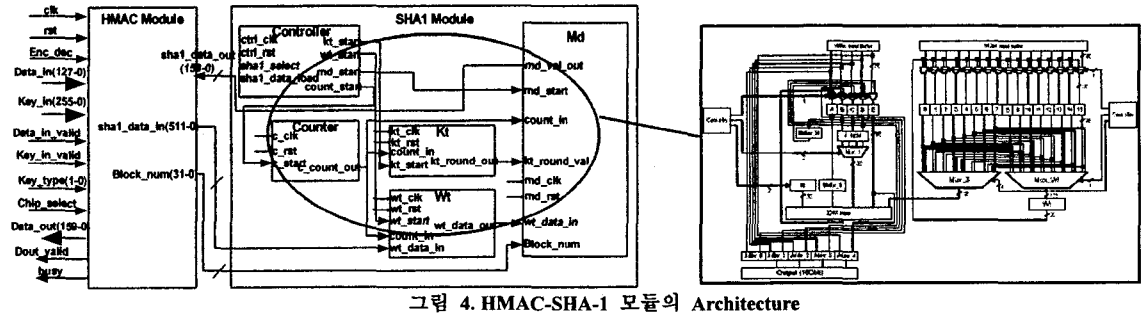

그림 4. HMAC-SHA-1 모듈의 Architecture

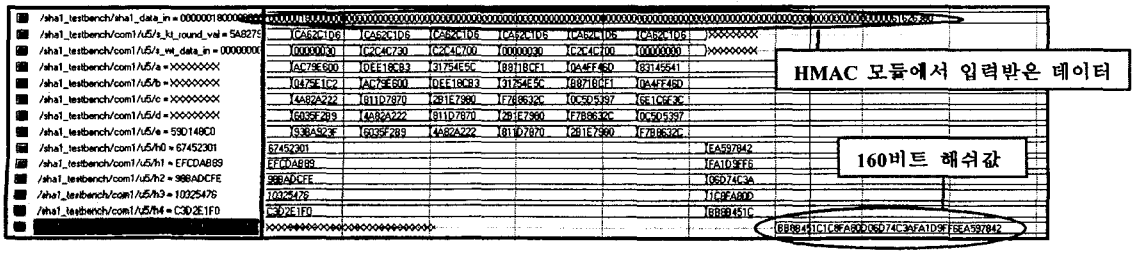

그림 5. SHA-1 모듈의 시뮬레이션