특

IPSec 프로토콜의 하드웨어 구현

김 경 태[1] 김 동 규[2] 이 정 태[3]

목 차

1. 서 론

IPSec 프로토콜은 IP 계층에서 기밀성(confidentiality), 무결성(integrity), 인증(authentication), 재전송 방지 등의 보안 서비스를 제공하는 프로토콜로 IETF에 의해 표준화되었다. IPSec은 IP 계층에서 직접 보안 서비스를 제공함에 따라 상위 계층 프로그램의 변경이 필요하지 않으며, 또한 추가적인 비용의 부담없이 사용중인 응용 서비스를 그대로 유지하면서 송수신되는 정보에 대한 보안 서비스를 제공할 수 있는 장점을 가진다.

IPSec 프로토콜은 Key 교환을 담당하는 IKE(Internet Key Exchange), 보안 통신을 담당하는 AH(Authentication Header), ESP(Encapsulating Security Payload) 프로토콜, 암호화/복호화 알고리즘 부분으로 구성된다[1][2][3][4]. 최근에는 IPSec 프로토콜의 속도를 향상시키기 위하여 각 부분을 하드웨어 모듈로 구현하여 최적화하는 연구가 진행되고 있다.

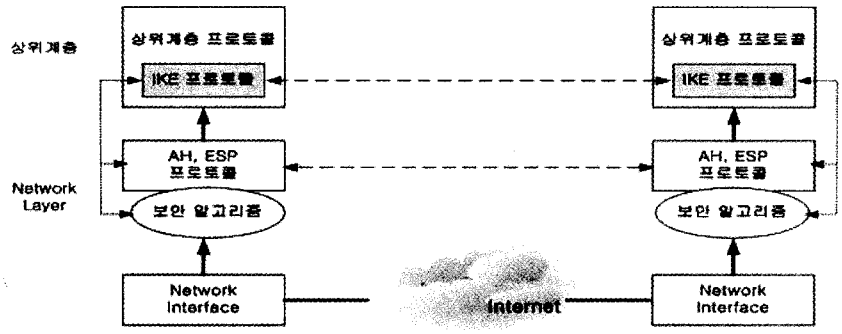
하드웨어로 구현된 IPSec 프로토콜은 주로 가상 사설망(Virtual Private Network : VPN)의 기반 기술로 사용되고 있다. 반면 미래의 IP 네트워크인 IPv6 프로토콜에서는 IPSec 프로토콜이 필수 요구사항으로 채택되어 각각의 호스트에 구현되고 있으며, IPv6 프로토콜을 지원하는 하드웨어 IPsec 프로토콜은 하드웨어 TCP/IPv6 프로토콜, MIPv6(Mobile IPv6) 프로토콜, 무선 통신 환경 등과 통합되어 유비쿼터스 네트워크의 구축에 사용될 것으로 전망된다[5].

본 고에서는 먼저 IPSec 프로토콜과 VPN에 대하여 간략히 설명하고, 주로 사용되는 VPN용 하드웨어 IPSec 프로토콜의 구조와 연구 동향에 대해 설명한 다음 앞으로 사용될 유비쿼터스용 하드웨어 IPSec 프로토콜의 구조와 전망을 제시한다.

2. IPSec 프로토콜 개요

IPSec 프로토콜은 IP 계층에서 보안 서비스를 제공하기 위한 프로토콜로, 서론에서 설명한 바와 같이 IKE 프로토콜, AH · ESP 프로토콜, 보안

1) 부산대학교 컴퓨터공학과 박사과정
2) 부산대학교 컴퓨터공학과 조교수
3) 부산대학교 컴퓨터공학과 교수



(그림 1) IPSec 프로토콜의 구조

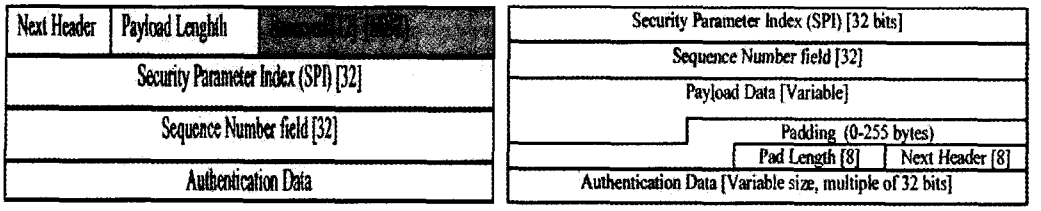
알고리즘의 세 부분으로 구성되며 구조는 (그림 1)과 같다. 먼저 IKE(Internet Key Exchange) 프로토콜은 상위계층의 프로토콜과 연동하며 보안 통신을 하는 호스트 간에 사용할 키를 교환하고 알고리즘 종류를 협상하는 역할을 한다.

IPSec 프로토콜에서 가장 중심적인 역할을 담당하는 보안 통신 프로토콜로 AH (Authentication Header), ESP(Encapsu - lating Security Payload) 프로토콜이 있다. AH와 ESP에 의하여 제공되는 보안 서비스는 〈표 1〉과 같다[6]. 표에서 보는 바와 같이 AH는 접근 제어, 비연결형 무결성, IP 데이터그램에 대한 데이터 발신 인증 등의 보안 서비스를 제공하며, 선택적으로 재전송 공격 방지 서비스를 제공할 수 있다. 재전송 공격 방지의 경우, 송신측에서는 디폴트(default)로 순차번호를 증가시키지만 수신측에서 이를 검사하지 않으면 성립되지 않는 서비스로 수신측의 선택사항으로 되어 있다. ESP는 AH가 가진 서비스 외에 페이로드(payload) 데이터에 대한 기밀성 서비스와 사용자측에서 발생된 패킷 전체를 암호화함으로써 제한적 트래픽 흐름의 기밀성 서비스를 제공한다.

AH · ESP 프로토콜은 IP 계층에서 인터넷 보안 서비스를 구현하기 위하여 추가로 확장된 헤더를 정의하고 생성한다. (그림 2)에서는 AH · ESP 프로토콜의 확장 헤더 구조를 보여주고 있으며, AH 헤더의 포맷은 좌측에, ESP 헤더의 포맷은 우측에 도시하였다. AH 헤더의 각 필드들을 기술하면 다음과 같다. 'Next Header' 필드는 AH 헤더 다음에 나타날 헤더 또는 페이로드의 형태를 지정하는 필드이고, 'Payload Length' 필드는 4바이트 단위로 계산되는 AH 헤더의 전체 길이를 나타내며, 'Reserved' 필드는 항상 0 값을 갖는다. 'Security Parameter Index(SPI)' 필드는 32비트로 유일한 SA(Security Association)를 식별하는데 사용되는 인자중 하나며, 'Sequence Number' 필드는 재전송 공격(replay attack)을 검사하는데 사용되고, 마지막으로 'Authentication Data' 필드는 데이터의

〈표 1〉 IPSec 프로토콜이 제공하는 보안 서비스

보 안 서 비 스	AH 프로토콜	ESP 프로토콜
접근 제어 (Access Control)	O	O
비연결성 무결성 (Connectionless Integrity)	O	O
데이터 발신 인증 (Data Origin Authentication)	O	O
재전송 방지 (Anti-Replay)	O(opt)	O
기밀성 (Confidentiality)		O
제한적 트래픽 흐름의 기밀성 (Limited Traffic Flow Confidentiality)		O

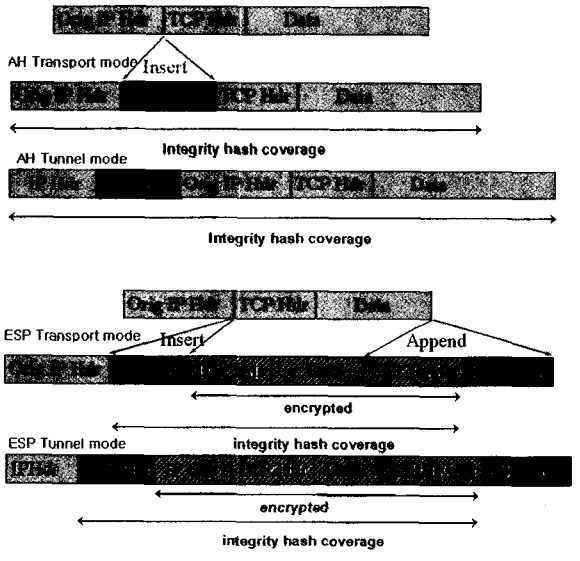


(그림 2) AH · ESP 헤더의 포맷

무결성과 인증을 위해 사용되는 값이다. ESP 헤더의 필드들을 기술하면 다음과 같다. 'Security Payload Index', 'Sequence Number', 'Next Header', 'Authentication Data' 필드는 AH 헤더의 각 필드와 동일한 용도로 사용되고, 'Payload Data' 필드는 Next Header 필드에서 지정한 상위 계층의 데이터가 기록되는 가변 길이의 필드로 보안 알고리즘에서 사용하는 초기 값인 IV(Initialization Vector)를 앞부분에 포함한다. 'Padding' 필드는 바이트 정렬을 맞추기 위해 사용되는 필드이고, 패딩된 크기는 'Pad Length' 필드에 기록된다.

IPSec 프로토콜에서 현재까지 사용되는 보안 알고리즘으로는 인증과 무결성을 제공하기 위한 HMAC-MD5, HMAC-SHA1과 기밀성을 제공하기 위한 DES, 3DES, AES 알고리즘 등을 표준으로 채택하고 있다.

IPsec 프로토콜을 적용시키는 방법으로 전체 패킷의 구조는 트랜스포트 모드(transport mode)와 터널 모드(tunnel mode)의 두 가지 형태를 가진다. (그림 3)은 AH와 ESP를 각각 적용했을 때 전체 패킷의 구조와 보안 서비스를 제공하는 범위를 보여주고 있다. 트랜스포트 모드는 호스트 간에 IPsec 프로토콜을 이용하여 직접 통신할 경우 적용되고 터널 모드는 라우터 사이에 IP 보안 터널(secure IP tunnel)을 형성할 경우 사용된다.

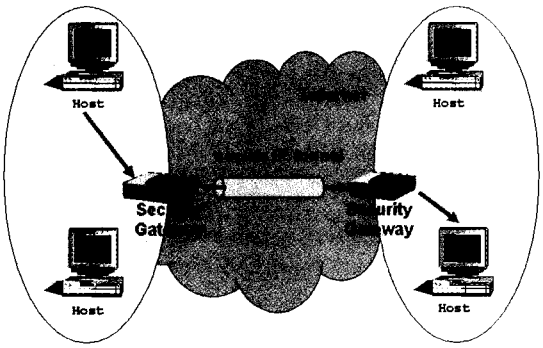


(그림 3) AH · ESP 프로토콜 적용 시 전체 패킷 구조

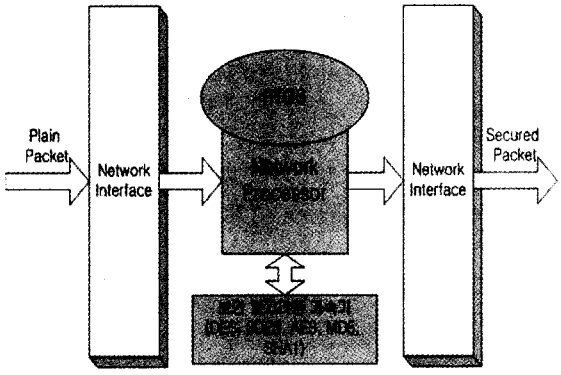
3. IPSec 프로토콜과 VPN

VPN(Virtual Private Network)은 터널링 기술을 이용하여 인터넷과 같은 공중망을 마치 사설망 같이 안전하게 이용할 수 있도록 함으로써 통합 보안 관리가 가능한 가상 사설 네트워크다. VPN에서 사용되는 방식에는 데이터 링크 계층에서 사용되는 L2TP(Layer 2 Tunnel Protocol) · PPTP(Point to Point Tunnel Protocol), 네트워크 계층에서 사용되는 IPSec 프로토콜이 있다. 이 중 IPSec 프로토콜은 다른 제품간 호환성 및 확장성이 뛰어나기 때문에 현재 가장 많이 사용되는 방식이다[7]. 현재 사용되고 있는 IPSec 프로토콜은 원래 목적인 "인터넷상의 패킷들에 대한 보안 서비스 제공"과는 달리 VPN의 구축에

주로 사용되고 있다[7][8]. (그림 4)는 이러한 VPN의 구조를 보여준다.



(그림 4) VPN의 구조



(그림 5) 하드웨어 IPSec 프로토콜 시스템

(그림 4)에서 도시한 바와 같이 IPSec 프로토콜은 보안 게이트웨이(security gateway)에 탑재되며 보안 게이트웨이 사이에 IP 보안 터널을 형성하여 보안 서비스를 제공한다. 초기에 사용된 IPSec을 이용한 VPN의 경우 일반 라우터에 소프트웨어 스택의 IPSec 프로토콜을 적용시킨 형태였으나, 네트워크 기술의 발전으로 수백 Mbps~Gbps까지 대역폭이 늘어남에 따라 속도에 한계를 가져 왔고, 이에 대한 해결책으로 하드웨어로 구현된 IPSec 프로토콜이 사용되기 시작하였다.

VPN상에서 사용되고 있는 하드웨어 IPSec 프로토콜 시스템은 하나의 보드 형태로 구현되어 보안 게이트웨이에 탑재되며 (그림 5)와 같이 네트워크 프로세서, RTOS(Real Time Operation System), 보안 알고리즘 가속기의 세 부분으로 크게 나누어진다. 네트워크 프로세서는 RTOS를 수행하며 전체를 제어하는 역할을 하고 RTOS는 각 하드웨어 구조에 맞도록 최적화된 OS (Operation System)로 IKE 프로토콜, AH · ESP 헤더와 상위 프로토콜들을 처리하는 역할을 하며, 보안 알고리즘 가속기는 IPSec 프로토콜에 사용되는 보안 알고리즘들을 하드웨어 칩으로 구현하여 암호화 · 복호화, 인증 코드 생성의 성능을 높인 모듈이다. 이러한 하드웨어 IPSec 프로토콜은 양단의 네트워크 인터페이스(network interface)를 통해 일반 패킷(plain packet)을 보안 패킷(secured packet)으로 변환하는 과정을 수행한다.

4. 하드웨어 IPSec을 채용한 VPN 제품 동향

VPN에서 성능 향상을 위한 하드웨어 IPSec 프로토콜의 탑재는 크게 두 가지 방향으로 전개되었다. 첫째는 IPSec 프로토콜을 동작시키는 네트워크 프로세서의 성능 향상과 최적화된 RTOS의 개발이고, 둘째는 Gbps의 성능을 낼 수 있는 암호화/복호화 알고리즘들을 탑재한 칩의 개발이다. 같은 네트워크 프로세서와 RTOS를 사용할 경우 하드웨어 보안 가속기 칩을 적용시켰을 때 소프트웨어 보안 알고리즘보다 30%이상의 성능이 개선된다. 이에 따라 국내외 VPN 벤더들은 대부분 이러한 하드웨어 IPSec 프로토콜을 탑재하여 제품을 출시하였거나 개발을 수행하고 있다. 〈표 2〉와 〈표 3〉은 기존에 출시된 하드웨어 IPSec 프로토콜 적용한 대표적인 국내외 VPN 벤더와 제품을 보여준다[9].

〈표 2〉 하드웨어 IPSec 프로토콜을 적용한 국외 VPN 벤더 및 제품

업 체	제 품	특 징	비 고
Cisco	-7200 VPN Module -VPN Acceleration Module	-IPSec gateway/filewall -IKE, X.509 지원 -DES/3DES/RC4 지원 -MD5/SHA1 지원 -침입탐지기능 제공	세계시장 1위 라우터 기능 통합
CheckPoint	-VPN Gateway -VPN SecureServer -VPN-1 SecureRemote -VPN-1 Accelerator Card	-IPSec gateway/firewall -IKE, manual 키 관리 지원 -DES/3DES/RC4 지원 -MD5/SHA1 지원	
3Com	-SuperStack Ⅱ Firewall	-IPSec gateway -IKE 지원 -DES/3DES/RC5 지원 -MD5/SHA1 지원	라우터 스위치 기능 통합
NetScreen	-NetScreen 1000/500/100/10	-IPSec gateway/firewall -IKE, X.509 지원 -DES/3DES 지원 -MD5/SHA1 지원	
RedGreek	-Ravlin 3300/5300/7150/7160	-IPSec gateway -IKE, X.509 지원 -DES/3DES 지원 -MD5/SHA1 지원	
Lucent	-Lucent VPN Gateway -IPSS	-IPSec gateway/firewall -IKE 지원 -DES/3DES/RC4 지원 -MD5/SHA1 지원	라우터 스위치 기능 통합
NewBridge	-Secure VPN Gateway 230	-IPSec gateway -IKE, PKI 지원 -DES/3DES/RC5 지원 -MD5/SHA1 지원 -소프트웨어 RSA signature 지원	
RedGuard	-clPro 5000 -clPro 2000/3000	-IPSec gateway/firewall -IKE 지원 -DES/3DES 지원 -MD5/SHA1 지원 -소프트웨어 RSA 지원	

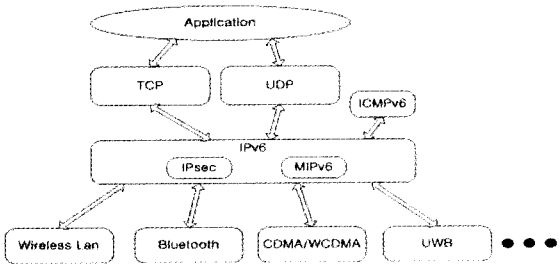
〈표 3〉 하드웨어 IPSec 프로토콜을 적용한 국내 VPN 벤더 및 제품

업 체	제 품	특 징	비 고
퓨처시스템	-SecuwayGate 2000	-IPsec gateway -IKE 지원 -DES/3DES/SEED/RC5 지원 -MD5/SHA1 지원 -전용 보안 알고리즘칩, OS 사용	국내시장 1위
시큐아이	-SecuiVPN100 Gateway	-IPSec gateway -IKE, manual/auto Key 관리 지원 -DES/3DES/Blowfish/SEED 지원 -MD5/SHA1 지원 -내부/외부 인증 서버 지원	
어울림정보기술	-Secureworks VPN	-IPSec gateway -IKE 지원 -DES/3DES/SEED/IDEA 지원 -MD5/SHA1 지원	
사이젠텍	-SOS B1100	-IPsec gateway/firewall -DES/3DES/SEED/AES/RSA 지원 -MD5/SHA1 지원 -QoS 지원	
시그엔	-isec gateway	-IPSec gateway -IKE, X.509 지원 -DES/3DES 지원 -MD5/SHA1 지원	
시큐어넥서스	-SecureVPN	-IPSec gateway -IKE, PKI 지원 -DES/3DES/SEED 지원 -MD5/SHA1/RSA signature 지원	
니츠	-NITZ VPN Suite	-IPSec gateway -IKE 지원 -DES/3DES 지원 -MD5/SHA1 지원 -IPv4/IPv6 연동	

하드웨어로 구현된 IPSec 프로토콜을 이용한 VPN 시스템은 전 세계적으로 급성장하고 있는 상태다. IDC(Internet Data Center)에 따르면 전 세계적으로 2002년의 시장 규모는 약 35억달러인 것으로 조사되었고, 2005년에는 최대 70억 달러의 시장이 될 것으로 전망하고 있다. 국내 시장은 아직 활성화되지 못한 상태나 많은 기업들이 VPN의 필요성을 느낌에 따라 큰 폭의 성장이 전망되고 있다[10]. 한국정보보호산업협회(KISIA)의 조사에 따르면 2002년의 시장 규모는 384억원이었으며 2004년에는 708억원으로 성장할 것으로 전망했다. 하지만 현재의 매출 추세를 볼 때 국내의 시장 전망은 KISIA의 수치를 크게 상회할 것으로 예상된다.

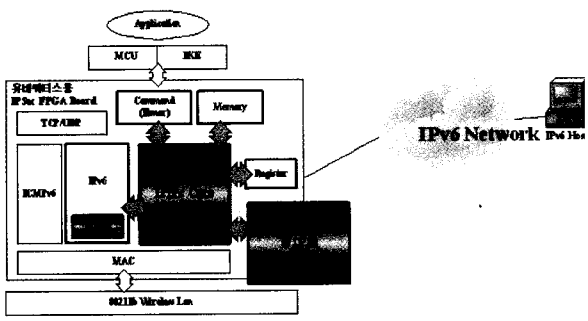
5. 유비쿼터스용 하드웨어 IPSec 프로토콜의 구현

유비쿼터스(Ubiqitous)는 "언제, 어디서나 있는"을 의미하는 라틴어로 사용자가 시간과 장소에 구애받지 않고 자유롭게 네트워크에 접속하는 것을 의미한다[11]. 이러한 유비쿼터스 네트워크에서는 물리 계층의 무선 통신용 프로토콜, 차세대 인터넷인 IPv6 프로토콜, TCP/UDP 프로토콜, 각종 응용 프로토콜이 사용될 것으로 예상된다. 무선 통신용 프로토콜들에는 802.11의 표준을 따르는 무선 랜(wireless lan), 802.15의 표준을 따르는 부루투스(bluetooth), 휴대폰에서 사용되는 CDMA/WCDMA, 802.15.3a의 표준을 따르는 UWB(Ultra Wideband Bandwidth) 등이 상황에 따라 사용될 것으로 전망된다. IPv6 프로토콜은 IPv4 프로토콜에 비해 주소 공간을 비약적으로 늘리고, IPSec 프로토콜과 MIPv6 프로토콜을 채택하여 보안과 모바일 기능을 강화한 프로토콜이다. (그림 6)는 유비쿼터스 네트워크의 프로토콜 스택을 보여준다.



(그림 6) 유비쿼터스 네트워크에서의 프로토콜 스택

유비쿼터스 네트워크에서의 각종 프로토콜은 소형화와 이식의 용이성을 위해 하드웨어화가 기본적으로 요구된다. 따라서 유비쿼터스 네트워크에서 보안 기능을 담당하는 IPSec 프로토콜 또한 유비쿼터스 네트워크를 지원하기 위한 하드웨어화가 요구된다. 이러한 유비쿼터스용 하드웨어 IPSec 프로토콜은 하드웨어 TCP/IPv6 프로토콜, 하드웨어 MIPv6 프로토콜과 통합하여 구현될 것으로 전망된다[12]. (그림 7)은 부산대학교의 본 연구실에서 개발 중인 유비쿼터스용 하드웨어 IPSec 프로토콜 시스템을 보여주고 있다[13].



(그림 7) 유비쿼터스용 하드웨어 IPSec 프로토콜 시스템

현재 개발 중인 유비쿼터스 용 하드웨어 IPSec 프로토콜은 기 개발된 하드웨어 TCP/IPv6 프로토콜을 기반으로 하고 있으며 물리 계층으로는 802.11b의 무선 랜을 사용하고, 모바일 지원을 위한 드래프트 20번 기반의 MIPv6 프로토콜을

지원하며, 키 교환 프로토콜인 IKE와 3DES, AES, HMAC-MD5, HMAC-SHA1의 IPSec 프로토콜 표준 보안 알고리즘을 하드웨어로 지원한다. IPSec 프로토콜에서 현재 지원중인 표준 보안 알고리즘들은 아직 비밀키 암호 시스템들이지만 보안 강도를 높인 RSA, ECC와 같은 공개키 기반 보안 알고리즘의 지원이 요구되고 있다[14]. 이와 같은 추세에 맞추어 본 연구실에서는 보안 알고리즘 모듈에 RSA, ECC 알고리즘을 하드웨어로 구현하였으며 이를 이식하여 높은 강도의 보안을 제공할 수 있도록 개발 중에 있다.

6. 결 론

IP 계층에서 보안 서비스를 제공하는 IPSec 프로토콜은 현재 VPN의 표준 프로토콜로 사용되고 있다. 네트워크 기술의 발전으로 인한 고속화로 소프트웨어 스택의 IPSec 프로토콜은 한계를 가져 왔고 현재 이를 해결한 하드웨어 IPSec 프로토콜을 탑재한 VPN 제품들이 주종을 이루고 있다. 이러한 하드웨어 IPSec 프로토콜 제품은 보안에 대한 수요가 날로 증가함에 따라 급속히 시장이 확대되고 있다.

미래의 유비쿼터스 네트워크에서는 소프트웨어 스택의 IPSec 프로토콜이 다른 기기들에 이식이 힘들고 소형화에 어려움이 있으므로 하드웨어 모듈로 상용될 전망이다. 뿐만 아니라, IPSec 프로토콜이 독자적인 하드웨어로 지원되기 보다는 물리 계층의 무선 통신용 프로토콜, 차세대 인터넷인 IPv6 프로토콜, TCP/UDP 프로토콜 등의 각종 응용 프로토콜과 연동하는 칩의 형태로 사용될 것으로 예상된다. 본 고에서는 이를 위하여 현재 실험실에서 개발 중인 유비쿼터스용 IPSec 프로토콜을 설명하였다. 제시된 IPSec의 하드웨어 모듈은 공개키 기반 알고리즘을 탑재하고 있으며, IPSec 프로토콜만의 독립 모듈이 아니라 무선 랜과 같은 무선 통신 환경과 MIPv6와 같은 모바일 지원 프로토콜, 하드웨어 TCP/IPv6 프로토콜이 연동하여 동작하는 통합된 시스템으로 설계하였다.

참고문헌

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

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

[3] S. Deering외 3명, "Internet Protocol, Version 6 (IPv6) Specification", IETF RFC 1883, Jan. 1996.

[4] R.Atkinson, S.Kent, " Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998.

[5] D.Harkins, D.Carrel, "The Internet Key Exchange(IKE)," RFC 2409, Nov. 1998.

[6] 권혁찬, 나재훈, 손승원, "IPv6 Security 동향", 한국전자통신연구원 주간기술동향 1064호, Sep. 2002.

[7] 아닌영, 허재두, 이형호, "L2/L3 MPLS 기반 VPN 기술 동향", 한국전자통신연구원 주간기술동향 1080호, Jan. 2003

[8] 정지훈, 이종태, 송승원, "IPsec 표준화 동향 및 제품 현황", 한국전자통신연구원 주간기술동향 952호, Jul. 2002.

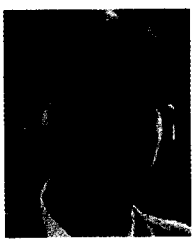
[9] 이윤철, "VPN기술 및 국내외 시장 동향", 한국전자통신연구원 주간기술동향 1075호, Nov. 2002.

[10] IDC Bulletin, "Worldwide Firewall/VPN Software Forecast, 2002~2006," IDC, Feb. 2002.

[11] 이성룡, 정현수, "Ubiquitous 연구 동향 및

향후 전망", IT World News Letter, Oct. 2002.
[12] 오승희 외 5명, "54차 IETF 회의 Security Area 동향", 한국전자통신연구원 주간기술동향 1069호, Oct. 2002
[13] 김경태 외 2명, "IPv6용 하드웨어 IPsec 프로토콜의 설계 및 구현", 정보과학회 추계 학술대회 발표 논문집(Ⅲ), Oct. 2002
[14] 류희수, 정교일, "차세대 암호 알고리듬 동향", 한국전자통신연구원 주간기술동향 1052호, Jun. 2002
[15] 전자신문, http://www.etimesi.com

저자약력



김 경 태

2001년 부산대학교 컴퓨터공학과 (공학사)
2003년 부산대학교 대학원 컴퓨터공학과 (공학석사)
2003년-현재 부산대학교 컴퓨터공학과 박사과정
관심분야 : TCP/IPv6, IPSec 프로토콜, MIPv6, Wireless Lan
이 메 일 : ktkim@pusan.ac.kr

김 동 규

1992년 서울대학교 컴퓨터공학과 (공학사)
1994년 서울대학교 컴퓨터공학과 (공학석사)
1999년 서울대학교 컴퓨터공학과 (공학박사)
1999-현재 부산대학교 컴퓨터공학과 조교수
관심분야 : 컴퓨터 보안 및 암호학, 알고리즘 설계, Bioinformatics
이 메 일 : dkkim1@pusan.ac.kr

이 정 태

1976년 부산대학교 전자공학과 (공학사)
1983년 서울대학교 컴퓨터공학과 (공학석사)
1989년 서울대학교 컴퓨터공학과 (공학박사)
1977년 한국전자통신연구소 연구원
1978-1984년 한국전자통신연구소 선임연구원
1985-1987년 동아대학교 공과대학 조교수
1992-1993년 일본 NTT 연구소 초빙 연구원
1988-현재 부산대학교 컴퓨터공학과 교수
관심분야 : 고속 TCP/IP, Mobile IP, IPsec, IPv6
이 메 일 : jtlee@pusan.ac.kr