가설사설망의 정보보호를 위한 하드웨어 구조 설계

김정태*

목원대학교

Hardware Architecture Design for Information Security of Virtual Private Network

Jung-Tae Kim

Mokwon University

E-mail : jtkim5068@hanmail.net

요 약

가상사설망(VPN)은 인터넷을 통하여 특정한 영역의 커뮤니터를 통합적으로 연결하여 상호간의 정보 전달을 인터넷을 통하여 통신하는 방법 중의 하나이다. 따라서, 가상사설망의 경우 정보보호를 위한 알고리즘의 성능 분석이 필수적이다. 따라서, 본 논문에서는 VPN 게이트웨이 데이타의 정보보호를 위한 IPSec에 적용 가능한 알고리즘을 시간 복잡도와 공간 복잡도에 대해 성능을 분석한다.

Ⅰ. 서론

지금까지는 많은 기업들이 외부 정보의 획득을 주 목적으로 인터넷의 도입을 추진하였으나, 이제는 보다 구체적으로 본사 지사, 또는 본사와 관련된 협력업체나 이동중인 원격 사용자들과의 원활한 정보교류를 위해 VPN(Virtual Private Network : 가상사설망)의 도입을 적극 검토하고 있다. 효율적인 구조를 갖는 기업의 통신망은 제품과 서비스에 대한 생산성을 증진시킬 수 있으며, 지역적으로 분산된 기업 거점들을 원활하게 관리할 수 있다. VPN은 공중망 및 전용 사설 망의 장점을 한군데로 결합하는 특성을 갖으며, 기존의 공중 교환 망 장비를 이용하여 사설 전용망이 갖는 사용자 그룹의 폐역화를 위한 터널링, 데이터의 암호화, 사용자 인증 및 리소스 엑세스 제어 기능 등을 제공함으로써 가입자는 저렴한 비용으로 효율적인 전용 overlay 망을 구축할 수 있다. 하지만, 이 기술은 관리의 복잡성, 터널링에 수반되는 오버헤드에 기인한 성능상의 문제점을 야기 시킬 수 있다. 일반적으로 VPN의 성능은 두가지 요소에 의해 영향을 받는데, 하나는 인터넷이나 공공 IP 백본 네트워크를 통한 전송속도이며, 다른 하나는 VPN 양 끝단에서의 VPN 처리(안전한 세션의 생성,터널링, 패킷의 암호화)등의 효율성에 의한 속도이다.

최근 하드웨어 기반의 VPN 전용장비가 많이 개발되고 있으나 속도가 100 Mbps를 넘는 VPN을 개발하는 것은 매우 어렵다. 최근 100 Mbps LAN이 이미 보편화되어 있고 Gbps 기술이 발전하고 있는 네트워크 환경에서, 소프트웨어 기반의 VPN 장비는 하위 계층의 물리적 네트워크가 제공하는 대역폭의 50% 정도의 성능만을 갖게된다. 특히, 보안의 강도가 비교적 높은 3DES 알고리즘을 사용하는 경우의 성능 저하는 아주 크다고 알려져 있다. 전체 대역폭을 점유할 만한 정도의 대량의 패킷을 일일이 암·복호화하는 작업이 단순히 소프트웨어적으로만 처리하기에는 현재로서는 불가능한 작업이기 때문이다[1]. 따라서, 본 논문에서는 VPN 게이트웨이의 정보보호를 위한 알고리즘의 성능에 대해 비교 분석해 본다. .

Ⅱ. 관련연구

2.1 VPN 기술의 개요

인터넷망은 누구나 쉽게 접속할 수 있고 무한한 확장성을 갖고 있지만, 개인 혹은 기업의 정보가 손쉽게 노출되기 쉬운 환경을 제공한다는 단점도 갖고 있다. VPN은 인터넷과 같은 공중망상에서 사설망을 구축하는 것이므로, 데이터의 보안이 무엇보다도 중요하다. 이를 위해서는 암호화, 사용자 인증 및 액세스 제한과 터널링 기술 등의 기능이 요구된다. 터널링은 VPN을 구현하기 위한 핵심기술이며 그림1에 나타난 바와 같이 라우팅 정보를 포함하는 추가헤더정보로 프레임을 캡슐화하여 전송하면, 캡슐화된 프레임은 추가헤더 정보내의 라우팅 정보를 기반으로 공중망을 경유하여 터

널 엔드 포인트로 전송되며, 망의 목적지에 도달한 프레임은 디캡슐되어 최종 목적지로 전송되는 과정을 포함한다. 현재 널리 사용되고 있는 터널링 프로토콜로는 PPTP, L2TP, IPSec 등을 들 수 있다. PPTP는 마이크로소프트사가 제안한 것으로서, 윈도우 안에 내장되어 있어 현재로서는 가장 널리 사용되고 있으며, 시험용 VPN 구축에 많이 채택되고 있다. L2TP는 시스코사가 기존에 제안한 L2F와 PPTP를 혼합한 터널링 규약으로서, 전용선 VPN 구축에 적합한 방법이다. IPSec은 IP 패킷을 보호하기 위해 보안 방식으로 개발한 인터넷 표준 규약으로서, 최근 발표되고 있는 거의 모든 VPN 제품들은 모두 IPSec을 준수하고 있거나 준수하는 제품을 발표할 예정에 있다. 국제컴퓨터보안협회(ICSA : International Computer Security Association)에서는 IPSec을 지원하는 VPN 제품에 대한 인증을 해주고 있다. 또한, VPN에서는 데이터가 인터넷이나 ISP의 기간망 등의 공중망을 이용하여 전송되기 때문에 암호화는 중요한 요소기술이다. 인터넷에서 터널링만으로 패킷의 보안이 완벽하게 이루어 질 수 없고 반드시 암호화 알고리즘이 병행적으로 구성하여야 한다. 암호화와 터널링을 동시에 강조하는 이유는, 암호화 기능은 패킷을 암호화하여 외부에 노출되지 않게 하며, 터널링은 패킷을 캡슐화하여 그 전송경로를 보이지 않게 하여, 각각의 다른 보안 특징을 가지기 때문이다. 터널링 기법을 사용하면, 주소와 라우팅 체계를 외부에 숨길 수 있으며, 이는 하나의 VPN 군에서 사용하는 주소와 라우팅 체계가 공중망 또는 다른 VPN 군이 사용하는 것이 가능함을 의미한다. 대부분의 VPN 장비들은 비슷한 수준의 암호화 기능을 제공하고 있으며, DES 와 3DES가 많이 사용되고 있는 암호화 알고리즘이다[2].

암호화와 함께 언급되는 항목은 각각의 인증된 VPN 사용자들에게 암호화된 인증키를 전달하기 위한 키관리 방식이다. IPSec에서 제안한 방식은 ISAKMP/IKE(Internet Security Association Key Management Protocol/Internet Key Exchange)이다. 거의 모든 VPN 제품들은 사용자 인증(Authentication)을 위하여 PPP의 인증 규약인 PAP(Password Authentication Protocol)이나 CHAP(Challenge Handshake Authentication Protocol)을 지원하고 있다.

2.2 IPSec 기술

IPSec에서 보안 서비스 제공을 위한 프로토콜은 AH(Authentication Header)와 ESP(Encapsulation Security Payload)가 있다. AH와 ESP는 IPv6와 IPsec(IPv4)에 새로 추가된 IP 헤더로서 인터넷 보안 서비스를 실현하기 위한 노력의 결과이다[3-5]. IP 패킷은 헤더와 페이로드 두 부분으로 나눌 수 있고, IP 헤더의 내용에 대한 보안 서비스를 적용하기 위하여 AH 헤더를 IP 확장 헤더로 추가하고 IP 페이로드의 내용에 대한 보안 서비스를 적용시키기 위하여 사용자 데이터를 ESP로 캡슐화(Encapsulation)한 후 헤더에 추가한다.

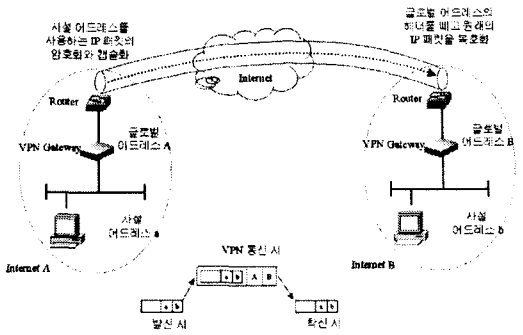

Fig 1. Tunneling mechanism

AH(Authentication Header)는 접근 제어(Access Control), 비연결형 무결성(Connectionless Integrity), IP 데이터그램에 대한 데이터 발신 인증(Data Origin Authentication) 등의 보안 서비스를 제공하며, 선택적으로 재전송 공격 방지(Anti-Replay) 서비스를 제공할 수 있다. 재전송 공격 방지 서비스의 경우는 반드시 송신측에서 순차 번호(Sequence Number)를 증가시키지만, 수신측에서 이를 검사하지 않으면 성립되지 않는 서비스로 수신측의 선택 사항으로 되어 있다. 또한, AH는 IP 헤더의 변경되지 않는 필드(Immutable Field)에 대해서만 보안 서비스를 제공한다. 따라서 통신로 상의 네트워크 장비에 의해서 변경되는 필드의 정보에 대해서는 초기 값을 '0' 으로 둔 다음 ICV(Integrity Check Value) 계산에 의해서 필드 값의 무결성을 검사한다.

ESP(Encapsulation Security Payload) 헤더는 페이로드에 대해서 AH가 제공하는 서비스 외에 추가적으로 비밀성(Confidentiality) 서비스를 제공한다. 트랜스포트 모드(Transport Mode)에서는 TCP/UDP 헤더와 사용자 데이터 전체를 암호화하며, 터널 모드(Tunnel Mode)에서는 사용자 측으로 부터 발생된 패킷 전체를 암호화할 수 있다. IPSec의 두 가지 프로토콜(AH, ESP)은 각 프로토콜 내부에서 사용하는 암호화 및 인증 등의 알고리즘과 무관한 구조를 가지고 있으며, IP 계층에서 사용하는 프로토콜 이외의 다른 보안 메커니즘을 필요치 않는다. 이와 같이 IPSec은 프로토콜 내부에서 사용하는 알고리즘과 독립적인 구조를 가지고 있으며, 규칙성을 만족하도록 설계되어 있다. 또한 프

로토콜 내부에서 사용하는 알고리즘들의 표준화 작업을 통해서 인터넷 사용자간의 호환성을 제공하도록 노력을 기울이고 있다.

IPSec은 인터넷에서의 보안 기술을 제공하지만, 구현 환경 조건에 따라 성능이 달라질 수 있다. 운영 체제, 난수 발생기의 성능, 시스템 관리 프로토콜의 효율 및 구현 형태에 따라 매우 다양한 성능의 차이를 보일 수 있다. 이러한 실제 구현 환경 조성에 관한 문제들은 IPSec의 표준화 범위에 들어있지 않지만, IPSec의 실용화에 미치는 영향은 매우 크다고 할 수 있다. 표1과 2는 IPSec의 AH와 ESP의 헤드 형식을 나타낸다.

Table 1 IPSec AH Header format

Next Header	Payload Length	Reserved[12](MBZ)
Security Parameter Index(SPI)[32]		
Sequence Number [32]		
Authentication Data		

Table 2 IPSec ESP Header format

Security Parameter Index(SPI) [32bits]		
Sequence Number field [32]		
Payload Data [Variable]		
	Padding (0-255 bytes)	
	Pay Length[8]	Next Header[8]
Authentication Data[variable size, multiple of 32 bits]		

III. 해석적인 성능 분석

IPSec 인증에 대한 인증 알고리즘과 암호 알고리즘의 공간 복잡도, 계산 시간 복잡도에 대해서 알아보기로 한다. 표3은 일반적인 IPSec 헤드의 영역의 크기를 나타내고 있다. 여기서 IPSec ESP의 암호화는 여분의 0에서 255 바이트의 padding 바이트를 사용한다.

Table 3 IPSec Header field sizes (bytes)

Protocol	IPSec AH			IPSec ESP		
	Fixed	Variable	Total	Fixed	Variable	Total
Transport Mode	12	12	24	10	12	22
Tunnel Mode	12/20	12	44	10/20	12	42

표4는 일반적으로 사용되고 있는 DES 알고리즘의 기본적인 연산을 나타내고 있다. 일반적으로 3DES의 구조는 알고리즘의 복잡도를 높이기 위해 연산 동작의 경우 일반적인 DES 알고리즘의 3배의 연산을 포함하고 있다.[?]

Table 4 DES basic operation

Basic Operation	Equivalent simple operation		
	Type	Times needed	Space needed
b it transposition	One dimensional table look-up	b	b
Table dimensional table map	Multiply	1	
	Add	1	
	One dimensional table look-up	1	4 rows x 16 cols.

그림2에서 그림7 까지의 내용은 IPSec에 사용될 수 있는 알고리즘의 입력 블록과 수행 능력에 대한 비교를 나타내고 있다. 여기서 64 비트의 입력 패킷 크기의 함수로써 계산된 시간을 나타낸다. 또한, D100은 100MPIS를 표현한다.

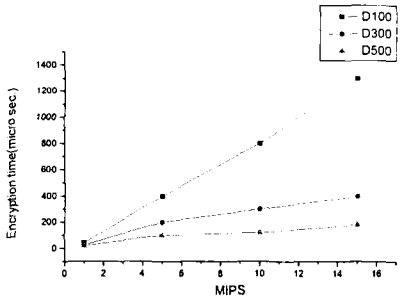

Fig. 2 DES Encryption time vs. of input blocks and processing power

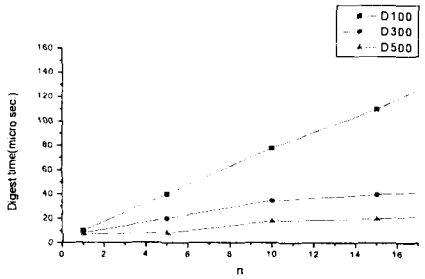

Fig. 3 MD5 digest time vs. of input blocks and processing power

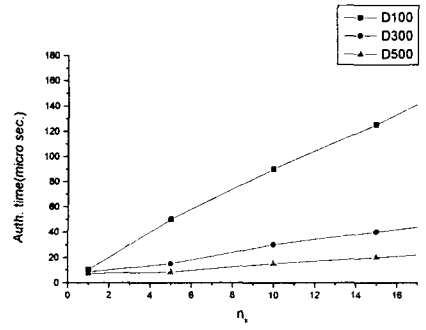

Fig. 4 HMAC MD5 Authentication time vs. of input blocks and processing power

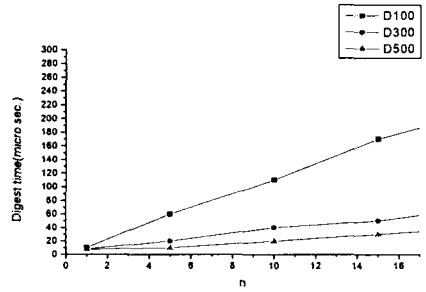

Fig. 5 SHA1 digest time vs. of input blocks and processing power

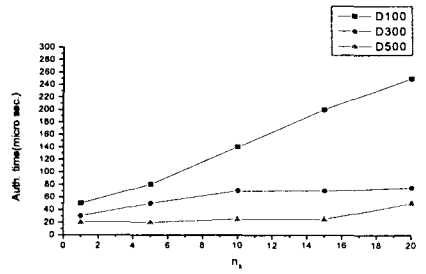

Fig. 6 HMAC-SHA1 Authentication time vs. of input blocks and processing power

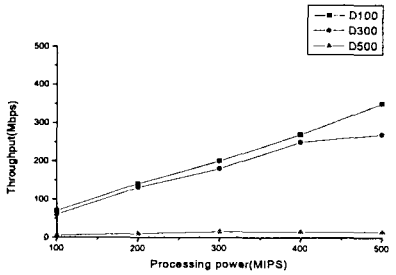

Fig. 7 Throughput comparison vs. input blocks and processing power

IV. 결론

본 논문에서는 IPSec에 대한 정보보호를 위한 암호 알고리즘을 수행할 시 성능 분석을 통하여 최적화된 알고리즘의 선택이 중요하다. MD5와 SHA1은 IPSec 인증에 대한 HMAC와 함께 사용될 수 있는 단방향 해쉬 함수이다. 따라서, 본 성능 평가를 통하여 MD5는 SHA1에 비해 높은 throughput를 가짐을 알 수 있다.

참고문헌

[1] T.Braun, M.Kasumi, et al., "Virtual Private Network Architecture", IAM-99-01, April 1999.

[2] Jung-Tae Kim, et al., "A Study on the VPN Gateway Architecture for Speed Acceleration", Journal of KICS, Vol.23, No. 8T, pp.127-133, Aug 2002.

[3] Erik L, et al., "A High-performance Active Network Node Supporting Multiple Mobile Code Systems", Proceedings IEEE Opeanarch '99, pp.100-111., March 1999.

[4] D.Tennenhouse, J.Smith, D.Sincoskie, et al., "A Survey of active network research," IEEE Communications Magazine, Vol, 35, pp.80-86, January 1997.

[5] D.Scott Alexander, et al., "The switch ware active network architecture," IEEE Network Magizine, Vol,12, No.3, June 1998.

[6] 신순자 외2인, "공인인증기반의 가상사설망 구축", pp.42-53, 한국통신학회지, 제18권9호. 2002