HFC망에서의 VPN성능에 관한 연구

김선희*, 문종섭, 임종인

(주) 데이콤*

고려대학교 정보보호대학원, 정보보호기술연구센터

A Study of VPN Performance on HFC Network

Sun-Hee Kim, Jong-Sub Moon, Jong-In Lim

Department of Information Security, Korea Univ.

요 약

어디서나 접속할 수 있는 인터넷의 광역성과 최근 들어 인터넷을 통한 전자상거래의 급진전, 네트웍을 통한 다양한 형태의 원격 접속 확대 등으로 이제 많은 기업들이 통신비가 상대적으로 저렴하면서도 기밀성이 보장되는 인터넷을 기반으로 하는Internet Protocol Virtual Private Network(IP VPN)의 도입을 서두르고 있다. VPN은 공중망 인프라를 공유하여 구축된 가상 사설망을 의미한다. IP VPN으로 기업은 본사와 지사를 연결하는 Intranet, 협력사와 연결되는 Extranet 그리고 최근 들어 급증하고 있는 이동 근무자와 재택 근무자를 회사에 안전하게 연결시킬 수 있는 원격 접속 등을 경제적으로 구축할 수 있다. 또한 광케이블과 동축케이블이 혼합된 Hybrid Fiber & Coaxial(HFC)망이 초고속인터넷, 디지털방송, 주문형비디오(VOD) 등의 멀티미디어 서비스를 수용하기에 가장 좋은 방안으로 최근 각광을 받고 있다. HFC망은 기존의 CATV망을 기반으로 하므로 신규 투자비가 적게 들면서도 다양한 형태의 고속 데이터 통신이 가능하다. 이에 본 논문에서는 HFC망에서의 IP VPN의 성능을 전송 프로토콜과 암호화 알고리즘을 달리 하면서 어떤 요소가 성능에 얼마나 영향을 주는지와 요소간 상호작용이 어떻게 일어나는지, 또한 어떤 조합으로 VPN 통신을 할 때 가장 좋은 성능을 보이는지를 비교 분석한다.

I. 서론

인터넷이 보편화된 정보통신수단으로 빠르게 확산되면서, 사용자들은 더욱 저렴하고 빠른 인터넷의 사용을 요구하고 이런 요구에 부응할 수 있는 고속 인터넷 접속 솔루션으로 여러 서비스들이 새로이 부상하고 있다.

최근 들어 어디서나 접속할 수 있는 인터넷의 광역성과 보안기술의 발전에 따라 공중망인 인터넷을 마치 사설 전용망처럼 보안이 유지되면서도 비용이 상대적으로 저렴한 Virtual Private Network(VPN)이 크게 확산되고 있다. VPN의 종류로는 IP Security Protocol(IPSEC)을 이용한 IP VPN, Multi Protocol Lable Switching (MPLS)네트워크를 기반으로 하여 각 데이터 패킷에 레이블을 붙이고, 이 레이블을 통해서 각 그룹간의 트래픽을 서로 분리하여 전달하는MPLS VPN, Secure Socket Layer(SSL)프로토콜을 이용한 SSL VPN, 이동 사용자 또는 무선 인터넷 사용자에게 적합한 무선 VPN이 있다. 본 논문에서는

IPSEC이라는 프로토콜 기반으로 하는 IP VPN을 이용하였다. IP VPN으로 기업은 본사와 지사를 연결하는 Intranet, 협력사와 연결되는 Extranet 그리고 최근 들어 급증하고 있는 이동 근무자와 재택 근무자를 회사에 안전하게 연결시킬 수 있는 원격 접속 등을 경제적으로 구축할 수 있다.

HFC망은 기존의 CATV 인프라 망을 활용하므로 신규 투자비가 적게 들면서도 다양한 형태의 멀티미디어 서비스를 가능하게 한다. 초고속 멀티미디어 서비스 구현을 위해 ADSL과 HFC망이 강력히 대두되고 있다. 이중에서 HFC망은 외국의 경우 ADSL 보다 훨씬 먼저 상용화되고 발전되었음에도 불구하고, 국내에서는 통신사업자의 선택에 밀려 한 단계 더딘 모습을 보였으나 최근 그 장점이 부각되면서 크게 주목 받고 있다. HFC망은 초고속인터넷은 물론 디지털TV서비스, 인터넷 TV, VoIP, 홈네트워크, VOD와 같은 통신방송 융합서비스의 실현을 앞당길 수 있는 전달 수단이 된다.

이에 본 논문에서는 HFC망에서의 IP VPN의 성능을 전송 프로토콜과 암호화 알고리즘을 달리하면서 어떤 요소가 성능에 얼마나 영향을 주는지와 요소간 상호작용이 어떻게 일어나는지, 또한 어떤 조합으로 VPN 통신을 할 때 가장 좋은 성능을 보이는지를 비교 분석하고자 한다. 따라서 본 논문은 HFC 망을 이용한 VPN 서비스에서의 성능 가이드를 제시 하는데 그 목적이 있다.

II. 본문

1. VPN에 대한 고찰

VPN은 인터넷과 같은 공중망(Public Network)을 이용하여 사설망 (Private Network)을 구성하는 기술로 기존의 전용선을 이용한 사설망에 비해 훨씬 저렴한 비용으로 보다 연결성이 뛰어나면서도 안전한 망을 구성할 수 있다는 면에서 인터넷의 활성화와 더불어 각광을 받기 시작한 보안 솔루션의 하나이다.

1) 네트웍 상에서의 위협과 보안형태

현재 네트웍 상에서의 위협과 보안에 대해 알아봄으로써 VPN의 필요성을 알 수 있을 것이다. 네트웍 상에서의 공격은 크게 수동공격(Passive Attack)과 능동공격(Active Attack)으로 구분해 볼 수 있다. 이때 수동공격은 실제로 네트웍 상에서 지나가는 패켓을 훔쳐보는 것으로 네트웍 트래픽을 생성하지 않는 반면 능동공격은 공격자가 네트웍에서 패켓을 위조하거나 변조하는 공격방법이다.

수동공격의 대표적인 것으로는 스니핑(Sniffing)이나 스케닝(Scanning) 등이 있으며 능동공격에는 스프핑(Spoofing), 맨인더 미들

(Man-In-The-Middle) 공격 등이 있다. 이러한 공격법 중 능동공격의 경우에는 공격 대상이 되는 시스템에 직접적인 피해를 초래하게 된다. 이러한 공격으로부터 우리의 네트웍을 보호하기 위해서 우리가 갖추어야 할 보안 요소들은 다음과 같다.

1) 기밀성(Confidentiality)
2) 무결성(Integrity)
3) 가용성(Availability)
4) 부인방지(Non-Reputation)

여기서 기밀성은 전달하고자 하는 내용을 수신자만이 풀 수 있는 키로 암호화 하는 서비스로 정당한 수신자만이 보내진 메시지를 볼 수 있다. 무결성은 전달하고자 하는 내용이 도중에 위조되거나 변조되지 않았다는 확신을 주는 서비스로 해쉬 함수를 사용하는 방법이 일반적이다. VPN 에서는 keyed-hash 의 함수가 사용되게 된다. 다음으로 가용성은 적절한 사용자에게 미리 정의된 수준의 서비스가 가능하게 하는 성질을 말한다. 부인방지 기능은 송신자 또는 수신자가 수신한 사실 또한 수신한 사실을 나중에 거부하지 못하도록 하는 서비스이다.

본 논문에서 사용하고 있는 VPN은 네트웍의 위협으로부터 보호하기 위해 앞에서 제시했던 4가지 보안서비스를 만족하는 시스템이다.

2) 보안관점에서 VPN

- VPN은 인터넷과 같은 공중망에서 두 지점간의 통신 도중에 예상되는 공격을 막

고 데이터의 유출이나 변조를 방지하기 위하여 필요하다.

- VPN은 주로 본사, 지사와 같이 멀리 떨어진 지역과의 안전한 통신을 위해 양단의 입구에 암호화 장비를 설치하고 보안 터널을 구성하여 보호하는 것이다.
- VPN은 공중망으로 나가는 입구에 설치하 므로 사용자들의 시스템에 보안 프로그램을 설치할 필요 없이 자연스럽게 보안 서비스를 적용할 수 있다.

3) VPN 터널링(Tunneling)

터널링 기술은 VPN의 기본이 되는 기술이다. 인터넷을 통하여 데이터가 전달될 때 암호화를 통해 다른 네트웍을 통하지 않고목적지까지 하나의 Hop으로 이동하는 것처럼 보이게 하는 기술을 말하는데, 터널링 기술의 목적은 사용자에게 투명한 통신 서비스를 제공하고 인터넷과 같은 안전하지 못한 네트웍 환경에서 강력한 보안서비스를 제공하기 위한 것이다.

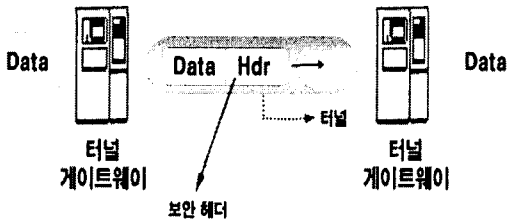

그림 1: VPN의 구성과 터널링

그림1은 VPN의 구성을 통한 터널링의 생성을 보여 준다. 양단의 터널 게이트웨이를 통해 VPN 터널링이 생성되어 인터넷 공중망 구간을 마치 전용선과 같이 보이게 한다. 미리 보안협상이 되어 있는 양단의 터널 게이트웨이를 통해서만이 복호화 또는 무결성 인증이 이루어져 정상적인 메시지를 볼 수 있게 되는 것이다.

2. HFC(Hybrid&FiberCoaxial)에 대한고찰

HFC는 성형(Star)구조를 갖는 광케이블과 수지형(Tree&Branch) 구조인 동축케이블을 혼합한 선로 기술을 말한다. 쉽게 말하면 기존의 CATV망에 광케이블을 도입한 양방향 CATV 형태의 망을 말한다.

전송망 구조에 따른 분류로 광전송 부문은 하향 신호 전송 경로인 광송신기 광케이블 ONU(광수신 모듈)와 상향 신호 전송 경로인 ONU(광 수신 모듈) 광 케이블 광 수신기로 구분되어 구성되어 있다. 동축전송 부문은 증폭기, 전원공급기, 수동소자, 동축케이블, 콘넥터로 구성되어 진다. (그림2참조)

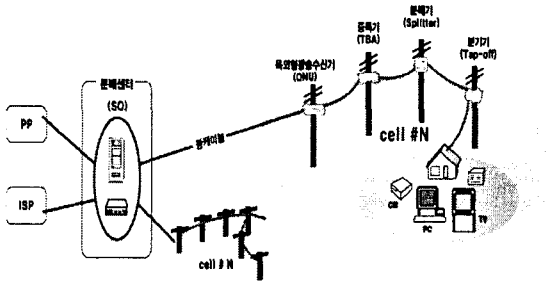

그림 2: HFC망 구성요소

또 일반적으로 HFC망에서 사용하는 전체 주파수 대역폭은 약 750MHz이다. 이는 Sub Split방식의 주파수 대역 중 5~42MHz대역은 상향 신호 전송을 위해 54~552MHz 대역은 하향 신호전송을 위해 그리고 552~750MHz대역은 향후 추가될 하향 신호를 위해 할당되었다.(그림3 참조)

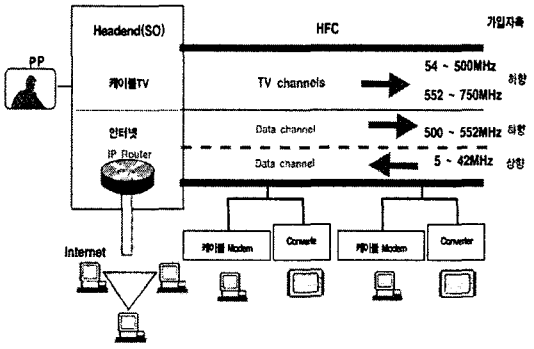

그림 3: HFC망 Sub Split방식 주파수 배치도

3. 시험방법제안

HFC망에서의 VPN 성능 분석을 위해서 먼저

실제 HFC망을 경유한 HFC망의 성능과 WAN 구간이 없이 직접 연결한 Direct망의 성능을 측정하여 두 방식간의 성능을 비교 분석하기로 한다.

1) 망 구성 방법

실제 HFC망은 타 트래픽이나 노이즈 등 외부 환경의 영향을 불규칙적으로 받기 때문에 VPN 암호화알고리즘간 성능분석을 위해서는 외부영향을 전혀 받지 않는 Direct망과의 비교를 통해 상대적 분석을 할 필요가 있다.

Direct망의 개념도는 그림5와 같이 라우터간 Serial로 회선을 구성하여 Local에서 Remote로 VPN 장비를 통해 Direct로 연결한다. Local 장비에서Remote 장비로 Uploading 트래픽을 측정한다.

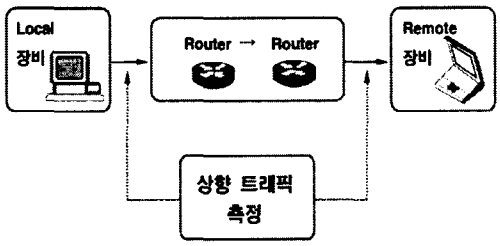

그림 4: Direct망 구성

HFC망의 개념도는 그림6과 같이 동축케이블을 통해 분배기로 보내진 전기신호는 ONU(광 송수신기-Optical Network Unit)에서 광신호로 광수신기에 보내 상향 분배함으로 보내지며, CMTS(Cable Modem Termination System)를 통해서 ISP 사업자의 인터넷망과 HFC망간 인터페이스가 일어난다. Local 장비에서Remote 장비로 Uploading 트래픽을 측정한다.

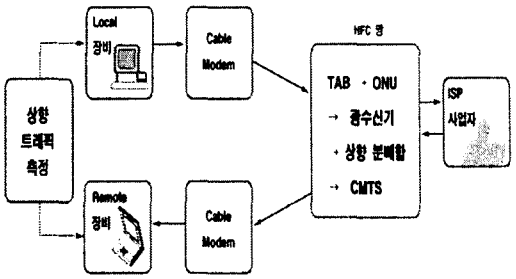

그림 5: HFC망 구성

2) 성능비교 항목

성능 비교를 위해 표1과 같이 성능 비교 항목으로 네트웍, 전송프로토콜, 그리고 Key인증, Key서명, DATA암호, DATA서명에서 사용된 알고리즘 등을 선정하여 통계분석을 통해 항목간 성능 차이가 있는지, 그리고 항목간 상호작용이 있는지를 검증한다. 또한 이를 통해 최상의 성능을 위한 조합이 어떠한 것인지를 알아본다.

표1: 성능 비교 항목

구 분		성능 비교 항목
네트웍		Direct망, HFC망
프로토콜		TCP, UDP
인증 단계	Key인증알고리즘	3DES, AES256
	Key서명알고리즘	MD5, SHA
암호화 단계	DATA암호 알고리즘	3DES,AES256, SEED
	DATA서명 알고리즘	MD5, SHA

3) 시험 절차

- VPN 성능 분석을 위해 Direct망과 HFC을 구성하고 장비별 파라메타를 설정한다.
- VPN장비 사이에 IPSEC 터널을 생성한다
- 암호 알고리즘별 성능 분석을 위해 Throughput을 측정한다.
- 통계분석 기법을 통해 전송 프로토콜별, 암 호 알고리즘별 유의성 검증과 상호 작용 여부를 분석한다
- HFC망에서의 최적의 전송 프로토콜과 암호 알고리즘을 도출한다.

4) 통계분석 기법에 의한 유의성 검증

성능 비교 항목간 유의성 검증 및 상호작용에 대한 유의성 검증에 있어 각 요인들의 조합은 통계학 실험계획법의 '일원분할법'을 이용한다.

4.1) 성능 비교 항목간 유의성 검증

HFC망 성능에 영향을 주는 요인간 통계적으로 유의성이 있는지를 알아본다.

- 네트웍간 즉 Direct망과 HFC망간에는 성능 차이가 나는가?
- 전송프로토콜간 즉 UDP와 TCP간에는 성능 차이가 나는가?
- Key인증알고리즘간 즉 3DES과 AES256 간에는 성능 차이가 나는가?
- Key서명알고리즘간 즉 MD5, SHA 간에는 성능 차이가 나는가?
- DATA암호알고리즘간 즉3DES,AES256, SEED 간에는 성능 차이가 나는가?
- DATA서명알고리즘간 즉 MD5, SHA 간에는 성능 차이가 나는가?

4.2) 상호작용에 대한 유의성 검증

요소 간 상호작용이 HFC망 성능에 영향을 주는 지를 통계적으로 유의성 검증을 한다

- 네트웍과 전송 프로토콜간에는 상호작용이 있는가?
- 전송 프로토콜과 VPN 암호화 알고리즘간에는 상호작용이 있는가?
- 네트웍과 VPN 암호화 알고리즘간에는 상호작용이 있는가?

4. 시험환경

1) 시험 망 구성

1.1) Direct망 시험 환경

HFC망의 상대적 성능 비교를 위해 트래픽이나 노이즈 등 외부 영향이 없는 망으로 그림6과 같이 두개의 라우터를 직접 연결하는 Direct망을 구성한다. 이때 라우터에서 상대 라우터로의 연결은 Serial로 세팅하여 WAN 구간을 경유하는 것과 같은 효과가 나타나게 한다.

Local PC에서 VPN 장비와 라우터를 통해 상대방인 Remote PC로 연결하여IPSec을 프로토콜로 데이터Uploading 성능 시험을 한다.

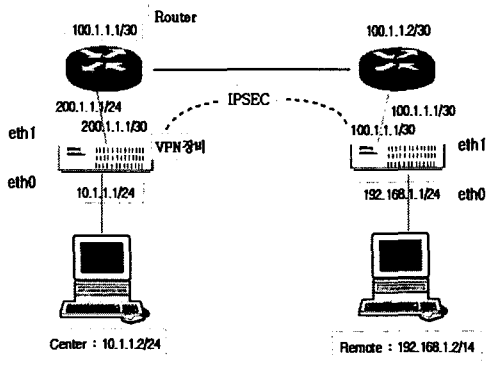

그림 6: Direct망에서의 시험 환경

1.2) HFC망 시험 환경

실제 HFC망에 가입하여 HFC망을 통한 VPN 성능을 측정한다. HFC망 시험망은 그림7과 같이 가입자 구간에서 케이블 모뎀을 통해 CMTS를 경유하고 인터넷망을 거쳐 상대방에게 연결되는 일반적인 HFC망을 구성한다. 이때 HFC망에서는 외부 트래픽이나 노이즈 등 외부 영향이 발생하게 된다.

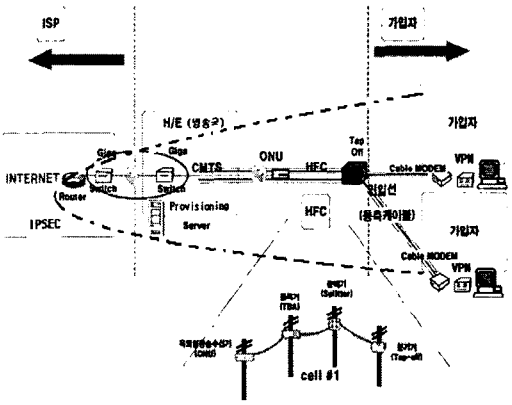

그림 7: HFC망에서의 시험 환경

2) 시험 장비

- Traffic Generator : 네트웍에서 발생되는

트래픽을 가상 생성하여 망Application 계층상에서 테스트 하는 소프트웨어 (NetIQ사의 'CHARIOT')

- VPN장비 : Local 및 Remote용 장비 각 1 대 (NEXG사의 'Vforce110')
- Router : Local 및 Remote용 장비 각 1대 (CISCO2500)
- PC : Local 및 Remote용 각 1대 (Pentium IV)

표2: 측정 기준

구 분	내 용
전송 속도	MAX : 2Mbps
측정 시간	30초/1회
파일 크기	100,000 Byte

5. 시험결과

1) 각 변수들의 유의성

시험 변수인 네트웍(HFC망, Direct망), 전송 프로토콜(TCP, UDP), Key인증 알고리즘(3DES, AES256), Key서명알고리즘(MD5, SHA), 데이타암호알고리즘(3DES, AES256, SEED), 데이타서명알고리즘(MD5, SHA) 들에 대한 유의성 검증 결과 유의한 요인은 네트웍, 전송 프로토콜, Key인증 알고리즘, 데이터암호알고리즘으로 나타났으며 유의한 상호작용은 네트웍*전송 프로토콜, 네트웍*Key인증 알고리즘, 네트웍*데이터암호알고리즘, 전송 프로토콜*데이터암호알고리즘, 네트웍*전송프로토콜*데이터서명알고리즘으로 나타났다. 성능에 영향을 미치는 최종모형은 다음과 같다.

성능 = 네트웍 + 전송 프로토콜 + Key인증 알고리즘 + 데이터암호알고리즘+ 네트웍*전송 프로토콜 + 네트웍*Key인증 알고리즘 + 네트웍*데이터암호알고리즘 + 전송프로토콜*데이터암호알고리즘 + 네트웍*전송프로토콜*데이터서명알고리즘

2) HFC망에서의 효율적인 성능 조합

유의한 상호작용들에 대해 시험결과를 토대로 각각의 성능들을 비교 분석한다.

여기서 평균값은 클수록 좋은 성능임을 나타낸다.

2.1) HFC망에서의 효율적인 성능 조합

Key인증암호화 알고리즘은 HFC망에 영향을 미치는 요인으로서 사용되는 3DES와 AES256알고리즘간에는 성능 차이가 존재한다. 이때 알고리즘간 평균을 살펴보면 아래 표3과 같다. 따라서 Key 인증 단계에서의 알고리즘은 AES256의 성능이 더 좋다

표3: Key인증암호화 알고리즘간 성능분석

Key인증 알고리즘	시험 횟수	평균	
		평균값	표준편차
3DES	240	0.6385	0.0914
AES256	240	**0.6762**	0.0706

2.2) DATA암호단계에서의 알고리즘성능분석

DATA암호 알고리즘은 HFC망에 영향을 미치는 요인으로 사용되는 3DES, AES256,과 SEED 알고리즘간에는 성능 차이가 존재한다. 이때 알고리즘간 평균 차이를 살펴보면 아래 표4와 같다. 따라서 DATA 암호화 단계에서의 알고리즘은 SEED의 성능이 더 좋다.

표4: DATA암호 단계에서의 알고리즘 성능분석

DATA암호 알고리즘	시험 횟수	평균		Grouping
		평균값	표준편차	
3DES	160	0.6205	0.5724	C
AES256	160	0.6523	0.5537	B
SEED	160	**0.6941**	0.5249	A

2.3) 전송프로토콜과 DATA암호알고리즘 간 상호작용에 따른 성능분석

전송프로토콜과 DATA암호 알고리즘간의 상호작용은 HFC망에 영향을 미치는 요인으로서 두 요인의 결합간에는 평균차이가 존재한다. 이때 두 결합들간 평균차이를 살펴보면 아래 표5와 같다. 따라서 전송프로토콜은 TCP, DATA암호 알고리즘으로는 SEED를 사용할 때 성능이 더 좋다.

또한 UDP에서의 SEED는 TCP에서의 3DES,

AES256과 같은 Group에 속하며, 같은 수준의 성능을 낸다고 할 수 있다.

여기서 Grouping(G)이란, 두 집단 A와 B의 각각의 평균 $\mathfrak{M}_0$, $\mathfrak{M}_1$ 이 같다는 가설이 기각 되었을 때는 서로 다른 그룹으로 분류 된다.

표5: 전송프로토콜과 DATA암호 알고리즘 간 상호작용에 따른 성능분석

전송 프로토콜	DATA암호 알고리즘	시험 횟수	평균		G
			평균값	표준편차	
TCP	3DES	80	0.6667	0.0652	B
TCP	AES256	80	0.6847	0.0656	A or B
TCP	SEED	80	**0.7020**	0.032	A
UDP	3DES	80	0.5743	0.0966	C
UDP	AES256	80	0.6199	0.1004	C
UDP	SEED	80	0.6862	0.032	B

2.4) 전송프로토콜과 Key인증 알고리즘 간 상호작용에 따른 성능분석

전송프로토콜과 KEY인증 알고리즘간 상호작용은 HFC망에 영향을 미치는 요인으로서 두 요인의 결합들간에는 평균차이가 존재한다. 이때 두 결합들간의 평균의 크기를 살펴보면 아래 표6과 같다. 따라서 전송프로토콜은 UDP를 사용하면서 DATA암호 알고리즘은 AES256을 사용할 때 성능이 더 좋다. 또한 나머지요인들은 같은 Group에 속하므로 같은 성능들을 낸다고 볼 수 있다.

표6: 전송프로토콜과 Key인증알고리즘 간 상호작용에 따른 성능분석

전송 프로토콜	Key인증 알고리즘	시험 횟수	평균		G
			평균값	표준편차	
TCP	3DES	120	0.6764	0.0664	B
TCP	AES256	120	0.6925	0.0472	B
UDP	3DES	120	**0.6007**	0.0973	A
UDP	AES256	120	0.6529	0.0836	B

2.5) 전송프로토콜과 Key서명 알고리즘 간 상호작용에 따른 성능분석

전송프로토콜과 KEY서명알고리즘 간 상호작용은 HFC망에 영향을 미치는 요인으로서 두 요인의 결합들 간에는 평균차이가 존재한다. 이때 두 결합들간의 평균의 크기를 살펴보면 표7과 같다. 따라서 전송프로토콜은 TCP와 Key서명알고리즘은 MD5나 SHA를 사용하였을 때 성능이 좋다. 여기서는 전송프로토콜을 TCP를 사용하면 어떤 알고리즘을 사용하여도 좋은 성능을 낸다. 또한 어떠한 전송프로토콜을 사용하느냐에 따라 성능에 차이가 난다는 것을 알 수 있다.

표7: 전송프로토콜과 Key서명 알고리즘 간 상호작용에 따른 성능분석

전송 프로토콜	Key서명 알고리즘	시험 횟수	평균		G
			평균값	표준편차	
TCP	MD5	120	**0.6830**	0.0584	A
TCP	SHA	120	**0.6860**	0.058	A
UDP	MD5	120	0.6129	0.0955	B
UDP	SHA	120	0.6407	0.0912	B

2.6) DATA암호와 DATA서명 알고리즘 간 상호작용에 따른 성능분석

DATA암호 알고리즘과 DATA서명알고리즘간 상호작용은 HFC망에 영향을 주는 요인으로서 두 요인의 결합간에는 평균차이가 존재한다. 이때 두 결합들간의 평균 크기를 살펴보면 표8과 같다. 따라서 DATA암호 알고리즘은 SEED를 사용하면서 DATA서명알고리즘은 MD5나 SHA를 사용하였을 때 성능이 좋다. 또한 DATA암호 알고리즘을 3DES를 사용하면서 DATA서명알고리즘을 SHA로 사용하였을 때는 성능이 좋지 않다.

표8: DATA암호와 DATA서명 알고리즘 간 상호작용에 따른 성능분석

DATA 암호 알고리즘	DATA 서명 알고리즘	시험 횟수	평균		G
			평균값	표준편차	
3DES	MD5	80	0.6433	0.0821	B
3DES	SHA	80	0.5977	0.1006	C
AES256	MD5	80	0.6550	0.0844	B
AES256	SHA	80	0.6497	0.0968	B
SEED	MD5	80	**0.6947**	0.0262	A
SEED	SHA	80	**0.6935**	0.0386	A

2.7) Key인증과 DATA암호 알고리즘 간 상호작용에 따른 성능 분석

Key인증알고리즘과 DATA암호 알고리즘간 상호작용은 HFC망에 영향을 주는 요인으로서 두 요인의 결합간에는 평균차이가 존재한다. 이때 두 결합들간의 평균 크기를 살펴보면 표9와 같다. DATA암호알고리즘을 SEED를 사용할 때 Key 인증알고리즘을 어떠한 것을 사용하여도 무방하며, DATA암호 알고리즘을 AES256을 사용할 때에는 Key인증 알고리즘을 같이 AES256을 사용할 때 같이 좋은 성능을 낼 수 있다.

표9: Key인증과 DATA암호 알고리즘 간 상호작용에 따른 성능 분석

Key 인증 알고리즘	DATA 암호 알고리즘	시험 횟수	평균		G
			평균값	표준편차	
3DES	3DES	80	0.6122	0.1028	B
3DES	AES256	80	0.6139	0.1009	B
3DES	SEED	80	**0.6896**	0.0238	A
AES256	3DES	80	0.6287	0.0848	B
AES256	AES256	80	**0.6908**	0.0577	A
AES256	SEED	80	**0.6986**	0.0396	A

2.8) 전체 상호작용에 대한 성능분석

네트웍, Key인증 및 Key서명 알고리즘, DATA암호 알고리즘 및 DATA서명 알고리즘 요소의 결합간에는 성능차이가 존재한다. 본 실험결과에서 전송 프로토콜은 TCP일 때 UDP보다는 성능이 더 좋다. 그러나 전체상호작용에 대한 통계분석 결과, 전송 프로토콜 UDP를 사용할 경우 Key인증알고리즘은 AES256, Key서명알고리즘은 SHA, DATA암호알고리즘은AES256, DATA서명 알고리즘은 SHA로 사용할 때 전송 프로토콜이 TCP를 사용 할 때와 같은 성능을 나타내는 것으로 나타났다.

2.9) 네트웍 간 성능분석

네트웍 구성에 따라 성능차이가 나타나는데, 본 실험에서는 HFC망 성능을 알아보기 위해 Noise를 최소화한 Direct망과 비교해 봄으로서 HFC망 성능을 알아보고자 했다. 각 망성능의 평균 크기를 살펴보면 표11과 같다. 따라서HFC망에서의 잡음(Noise)으로 인한 성능저하는 약 3배정도 임을 알 수 있다.

표10: 네트웍 간 성능 분석

네트웍	시험 횟수	평균	
		평균값	표준편차
HFC	480	0.6556	0.0833
Direct	480	1.7438	0.0769

III. 결론

본 논문은 최근 확산되고 있는 VPN과 HFC망에 대한 기술적 특성과 발전 동향에 대해 먼저 알아보고 이를 토대로 HFC망에서의 IP VPN의 성능을 전송 프로토콜과 암호화 알고리즘을 달리 하면서 어떤 요소가 성능에 얼마나 영향을 주는지와 요소간 상호작용이 어떻게 일어나는지, 또한 어떤 조합으로 VPN 통신을 할 때 가장 좋은 성능을 보이는지를 비교 분석하였다.

시험을 위해 실제 HFC망에 가입하여 Local 장비에서 Remote 장비로 데이터 Uploading 시험을 실시하였다. HFC망에서 VPN 성능 비교를 위해 성능에 영향을 주는 요소로 전송 프로토콜로는 TCP와 UDP를 구분 측정하고, IPSec 프로토콜의 암호화 알고리즘으로는 DES, AES256, SEED, MD5, SHA를 각각 적용 측정하였다.

측정 결과에 대한 성능 비교 요소 간 유의성 검증 및 상호작용에 대한 유의성 검증에 있어 각 요인들의 조합은 통계학 실험계획법의 '일원분할법'을 이용하였다.

먼저 성능에 영향을 주는 요소간 비교에서는 TCP가 UDP보다 더 좋은 성능을 보였으며, Key 인증암호화 알고리즘에서는 AES256알고리즘이 3DES보다 좋은 결과를 보였고, DATA암호 알고리즘에서는 SEED알고리즘이 가장 좋게 나타났으며 다음으로 AES256알고리즘, 3DES알고리즘 순으로 나타났다.

요소간 상호작용 분석에서는 전송프로토콜과 DATA암호 알고리즘간의 상호작용은 HFC망에 영향을 미치는 것으로 나타났으며 전송프로토콜을 TCP로 DATA암호알고리즘으로 SEED를 사용할 때 다른 조합에 비해 성능이 더 좋게 나타났다. 또한 전송프로토콜과 KEY인증알고리즘간 상호작용에서는 전송프로토콜은 UDP를 사용하면서 DATA암호 알고리즘은 AES256을 사용할 때 성능이 더 좋게 나타났다. 전송프로토콜과 KEY서명알고리즘간 상호작용에서는 전송프로토콜은 UDP로 Key서명알고리즘은 MD5나 SHA를 사용하였을 때 성능이 좋게 나타났다. DATA암호 알고리즘과 DATA서명알고리즘간 상호작용에서는 DATA암호 알고리즘은 SEED를 사용하고 DATA서명알고리즘은 MD5나 SHA를 사용하였을 때 성능이 좋은 것으로 나타났다.

본 논문에서는 한 가지 형태의 HFC망에서만 시험을 하였기 때문에 시험 결과 모두를 일반화시키기에는 부족한 점이 있으나 HFC망에서 IPSec 프로토콜의 다양한 암호화 알고리즘과 전송 프로토콜을 사용하여 상호 작용 시험에 통계기법을 이용하여 유의성 검증을 한 것이므로 HFC망에서 효율적인 VPN 구성 시 성능 분석에 유용한 기초 자료가 될 것이라 사료된다.

참고문헌

[1] S. Kent, R. Atkinson, " Security Architecture for the Internet Protocol", RFC2401, November 1998.

[2] S. Kent, R. Atkinson, " IP Encapsulating Security Payload (ESP)",RFC2406, November 1998.

[3] Virtual Private Networking(Chapter 9), http://www.microsoft.com/WINDOWS 2000library/resources/reskit/samplechapters/inbe/inbe vpn ymsi.asp

[3] Haller, N., and R. Atkinson, "On Internet Authentication", RFC 1704, October 1994.

[4] Harkins, D., and D. Carrel, "The Internet Key Exchange(IKE)", RFC 2409, November 1998.

[5] Kent, S., and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[6] Maughan, D., Schertler, M., Schneider, M., and J. Turner,"Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.

[7] Orman, H., "The OAKLEY Key Determination Protocol", RFC 2412, November 1998.

[8] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407,

November 1998.
[9] Thayer, R., Doraswamy, N., and R. Glenn, "IP Security Document Roadmap", RFC 2411, November 1998.
[10] Atkinson, R., "The IP Authentication Header", RFC 1826, August 1995.
[11] Madson, C., and R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", RFC 2403, November 1998.
[12] den Boer, B., and Bosselaers, A., "Collisions for theCompression function of MD5", Advances in Cryptology Eurocrypt '93 Proceedings, Berlin: Springer-Verlag 1994
[13] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, MIT and RSA Data Security, Inc., April 1992.
[14] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.
[15] Kent, S. and R. Atkinson, "IP Authentication Header",RFC 2402, November 1998.
[16] 안철수 연구소, 강권학 "안철수_VPN_1"
[17] 국가정보원 "국가기관용 게이트웨이형 가상 사설망보호 프로파일V1.1"
[18] RFC868. Internet Time Protocol(ITP)
[19] RFC1350. Trivial File Transfer Protocol (TFTP)
[20] RFC1541/1542. Dynamic Host Configuration Protocol(DHCP)
[21] Cable Television Laboratories, Inc. (CableLabs) (http://www.cablelabs.com/)
[22] Cisco Systems, Inc. (http://www.cisco.com)
[23] DOCSIS 2.0 White Papers (http://www.terayon.com/cat.html?Cat_id=9.5.1)
[24] IDC. "Attack of the Phone" , 2002. 1
[25] http://www.cableguy.x-y.net/main.html
[26] http://www.gi.com/nis/hfc_access.html
[27] http://www.powercomm.com/