다중 무선 보안네트워크 환경에서 의료데이터의 전송 성능 분석

연세대학교 대학원

생체공학협동과정

전기전자공학전공

서 국 진

다중 무선 보안네트워크 환경에서 의료데이터의 전송 성능 분석

지도 유 선 국 교수

이 논문을 석사 학위논문으로 제출함

2007년 7월 일

연세대학교 대학원
생체공학협동과정
전기전자공학전공
서 국 진

서국진의 석사 학위논문을 인준함

심사위원 _____ 인

심사위원 _____ 인

심사위원 _____ 인

연세대학교 대학원

2007년 7월 일

감사의 글

2005년 여름부터 지금까지 2년이란 시간이 이렇게 아침이슬처럼 빠르게 지나가리라고는 생각지 못했습니다. 연구실에 들어오기 이전 2005년 2월 의과대 종합관에서 교수님과의 첫 만남을 잊을 수가 없습니다. 무척이나 인자하신 모습으로 저를 반겨주시던 장면이 생생하게 떠오릅니다. 그때부터 졸업하는 지금까지 다양한 연구를 할 수 있도록 최선을 다해서 열정적으로 제 연구를 도와주신 유선국 교수님께 깊은 감사를 드립니다. 저의 논문심사를 위해 어려운 시간을 내어주신 김남현 교수님과 김기덕 교수님께도 감사의 말씀을 전하고 싶습니다.

의학공학교실에 입문하여 지금에 이르기까지 자주 마주치지는 못했지만, 볼때마다 정이 갔었던 김덕원 교수님과 서활 교수님 박종철 교수님께 진심으로 감사드립니다.

저와 옆에서 함께 연구했던 수많은 연구원들을 한명씩 떠올리며, 감사의 글을 이어가겠습니다. 먼저 저와 오랜 시간 함께 했었으며, 연구실 박사님으로서 너무 고생 많으신 동근이형, 조용하지만 강한 카리스마가 넘치시는 석명이형, 친 형처럼 저를 생각해 주시며, 고민 상담 전문 해결사 박순만이 형, 핑크팬더라는 별명이 어울리며 힘들 때마다 따뜻한 말로 자신감을 심어주신 호현이형, 이시대의 하나뿐인 순수남성 이만규 형님, 예전 종합관 5층 계단에서 Smoking Time을 가졌었던 기억이 난다. 지금은 졸업했지만, 여전히 떠오르는 카사이미지 윤하영, 아카라카 공연때마다 나에게 신경 써 주었으며, 여자친구가 무척 이쁘고, 나보다 어리지만 생각이 깊고, 잘생긴 직속후배 이충기박사과정. 나와 화끈한 2년 지낼 수 있도록 해주었으며, 전산원 과제 할때 부터 종합관 4층에서 급 친해졌고, 지금은 연애하느라 연락이 잘 안되는 박정진이. 나와 6개월관 룸메이트 였고, 착하디 착한 시커먼스 우영재. 널위해 외치고 싶다. 잘생겼다~! 돈 없을때 적시에 한번씩 쏴줬으며, 톡톡튀는 맛이 있는 김수정. 나와 함께 신입생으로 들어왔고, 메탈을 좋아하며, 기타, 드럼등을 잘 다루고, 사진마저 잘 찍는 내 직속후배 서럭찬이, 나랑 동갑이지만, 무척 어른스러우면서 웃길 줄 아는 김도윤, 목소리가 좋으며, 특히 몸이

잘빠졌고, 착하게 생긴 이동헌이. 질퍽했던 1년 반이었지만, 77년생 형으로서의 모습도 가끔 보여줬었던 기원이형, 내 두 번째 동기이며 연구실의 에이스&이쁜 박윤정이. 큰 체형을 가졌지만, 대단히 착하고, 나에게 최선을 다해 연구 파트너로서 역할을 다 해주었던 김정채, 사투리가 정감 있는 인호형, 연구실에 들어와서 나에게 너무나도 많은 연구도움을 주셨고, 최근 얄미운 사람을 즐겨부르며, 형제처럼 지내고 있는 댄서 장봉문이 형, 학부 3학년 때부터 친구로서 늘 나와함께 했던 입담꾼 한동훈. 의리파로서 졸업했지만, 종종연락이 되고 나에게 충성을 다했던 양건호, 성대묘사를 잘하는 연구실 분위기 메이커 이용귀, 시골의 느낌이 물신 풍기며 얼마전부터 이용귀를 제친 Best 후배 조한규, 내 직속후배이면서 조용하게 연구하는 것을 즐기는 김도성, 부사수 임동규는 앞으로 날 이어갈 또하나의 직속 후배. 넌 나보다 잘하리라 믿는다. 랩의 황제이며, 예의가 바르고, 즐길줄 아는 임승경. 작년 9월 너의 무대는 정말 최고였어. 지금은 퍼듀에 가서 박사과정을 밟고 있을 기재홍이. 나랑 동갑으로서 말도 잘 통하고, 함께할때마다 즐거웠다. 기독교 신자로서 행동 하나하나에도 교리를 실천해 나가는 한때 권상우 김상용. 그 외의 세브란스 병원 정보통신 팀의 김진응님과 이영기 부장님 그리고, 저와 함께 작업했었던 여러 회사 직원 여러분들과 WM, 또한 저에게 연구도움을 주셨던 서울대와 성균관대 연구원님들께 감사의 말씀을 드립니다. 마지막으로 저에게 따뜻한 마음으로 투정을 잘 받아주신 인자하신 어머니, 그리고 제가 공부할 수 있도록 저를 믿고, 가장 큰 힘이 되어 주셨던 아버지께 감사합니다.

지금까지 이렇게 많은 사람들이 제 곁에 있었다는 사실을 감사의 글을 쓰면서 다시 깨닫게 되었습니다. 여러분들이 없었다면, 석사학위를 얻지 못했을 것이라 생각합니다. 사회에 나가서도 마음만은 늘 우리 연구실과 함께 할 것이며, 지금 연구실에 남아계신 여러 선배, 후배님들께 행운이 함께하길 바랍니다.

2007년 7월

서 국 진 드림.

차 례

그 림 차 례

표 차 례

국문요약

다중 무선 보안네트워크 환경에서 의료데이터의 전송 성능 분석

원격 진료 시스템이란 어떠한 상황에 있어도 의료데이터의 송수신이 가능해야 하며, 데이터의 왜곡이나 끊김 불안정한 전송을 피하여 최대한 환자에게 빠르고 정확하게 응급조치를 취할 수 있도록 도와주는 역할을 해야 하는 시스템이다. 이 원격진료 시스템에 필수적인 요소 중의 하나는 통신망이며, 상황에 따른 적절한 통신망의 선택에 의해 더욱 질 높은 원격진료가 가능하다. 현대의 유선 통신망은 급속한 발전을 이루어 내어 실시간 멀티미디어 전송에 문제가 없을 정도이지만, 무선 통신망에서는 그동안 주로 사용되어진 1xCDMA2000은 500Kbps에도 미치지 못하는 낮은 대역폭을 가지며, Wireless LAN의 경우는 이동성에서의 문제점을 보였다. 최근에 이러한 무선 통신망에서도 기술의 업그레이드를 이루어 내어 Wibro(Wireless Broadband Internet), HSDPA(High Speed Down Link Packet Access)와 같은 최신 기술들이 도입되어 1Mbps ~ 3Mbps에 달하는 높은 대역폭(Throughput)을 제공하는 기술들을 선보이면서 무선 환경에서의 멀티미디어 서비스의 질을 높이고 있다. 이에 따라 원격의료시스템에 적용할 수 있는 통신망이 다양해 졌으며, 시간적, 공간적, 이동적인 제약 없이 환자를 진단하고, 적절한 조치를 취할 수 있게 되어 환자의 생존율과 회복율에 긍정적 효과를 끼치고 있다. 이러한 최신 네트워크 환경에서 원격진료시스템을 구성하고 테스트 하는 것은 빠르게 발전하는 통신망에 적응하기 위한 초석이 될 수 있다.

그리고 현재의 수많은 네트워크 인프라에도 불구하고, 네트워크 인프라가 손상되어 이용할 수 없는 최악의 재난상태, 또는 낙도·오지등과 같이 상용 네트워크 망이 도달하지 않는 음영지역에서의 응급상황이 발생할 수 있는 상황에서의 원격

진료시스템에 대한 연구가 진행되고 있지만, 다른 네트워크 인프라를 이용한 연구보다 활발하지 않은 것이 사실이다.

본 논문에서는 다양한 통신망의 보안이 보장되는 VPN 프로토콜 하에서 IP layer 기반에 적용 가능한 AH(MD5, SHA-1), ESP(3DES) 알고리즘을 변화시키며 시뮬레이션 환경에 적용시켰을 때의 프로세싱 타임과 네트워크 망의 상태를 평가할 수 있는 지표인 QoS를 통해 지연(Round Trip Time), 지터(Jitter), 대역폭(Throughput)을 산출하였으며, 원격 진료 시스템의 정책 결정에 기반이 될 수 있는 적절한 알고리즘을 제안하였으며, 이 결과를 바탕으로 무선통신 환경에서의 원격진료 시나리오를 테스트 해봄으로서 보안 적용 가능성을 파악하였다.

마지막으로 이를 종합하여 Wibro, HSDPA와 위성통신을 이용한 실시간 원격응급 진료 시스템의 유용성과 한계점에 대해 연구하였다.

제 1장 서 론

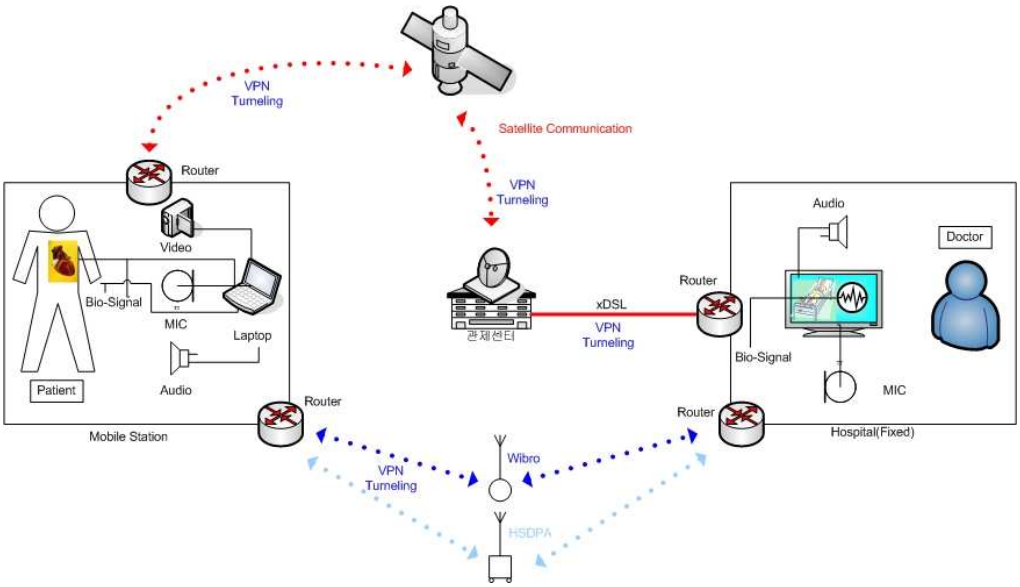


그림 1-1. 다양한 통신환경에서의 무선보안 원격진료 시스템

원격 진료 시스템이란 어떠한 상황에 있어도 의료데이터의 송수신이 가능해야 하며, 데이터의 왜곡이나 끊김 불안정한 전송을 피하여 최대한 환자에게 빠르고 정확하게 응급조치를 취할 수 있도록 도와주는 역할을 해야 하는 시스템이다. 이 원격진료 시스템에 필수적인 요소 중의 하나는 통신망이며, 상황에 따른 적절한 통신망의 선택에 의해 더욱 질 높은 원격진료가 가능하다[1]. 현대의 유선 통신망은 급속한 발전을 이루어 내어 ADSL과 VDSL 그 외에 광 랜 서비스까지 실시함에 따라 실시간 멀티미디어 전송에 문제가 없을 정도이지만, 무선 통신망에서는 그동안 주로 사용되어진 1xCDMA2000은 500Kbps에도 미치지 못하는 낮은 대역폭을 가지며, Wireless LAN의 경우는 이동성에서의 문제점을 보였다. 최근에 이러한 무선 통신망에서도 기술의 업그레이드를 이루어 내어 Wibro(Wireless Broadband Internet), HSDPA(High Speed Down Link Packet Access)와 같은 최신 기술들이 도입되어 1Mbps ~ 3Mbps에 달하는 높은 대역폭(Throughput)을 제공하는 기술들을 선보이면서 무선 환경에서의 멀티미디어 서비스의 질을 높이고 있다[2]. 이에

따라 원격의료시스템에 적용할 수 있는 통신망이 다양해 졌으며, 시간적, 공간적, 이동적인 제약 없이 환자를 진단하고, 적절한 조치를 취할 수 있게 되어 환자의 생존율과 회복율에 긍정적 효과를 끼치고 있다[3]. 이러한 최신 네트워크 환경에서 원격진료시스템을 구성하고 테스트 하는 것은 빠르게 발전하는 통신망에 적응하기 위한 초석이 될 수 있다.

그리고 현재의 수많은 네트워크 인프라에도 불구하고, 네트워크 인프라가 손상되어 이용할 수 없는 최악의 재난상태, 또는 낙도・오지등과 같이 상용 네트워크 망이 도달하지 않는 음영지역에서 응급상황이 발생할 수 있다. 이때 사용될 수 있는 위성통신망을 이용한 원격진료시스템의 연구가 진행되고 있지만, 다른 네트워크 인프라를 이용한 연구보다 활발하지 않은 것이 사실이다[4].

또한, 원격진료 시스템에 의해 전송되는 의료 정보는 환자의 신상 정보, 또는 응급 환자의 데이터와 같이 중요한 자료이기 때문에 그것의 변형이나 노출이 일어나게 된다면, 환자의 원격진료에 큰 문제를 가져올 수 있다. 그러나 현재 인터넷에서의 IP_layer는 패킷의 송수신에 있어서 신뢰성 있는 전송만을 염두에 두고 개발되었기 때문에 IP 스푸핑, IP 스니핑과 같은 패킷 해킹 공격에 대한 보안 취약점을 가진다. 따라서 상용망을 이용한 의료정보의 전송은 안전하고 신뢰성 있는 네트워크 사용을 보장하지 않는다. 따라서 본 논문에서는 최신 무선통신 환경인 Wibro, HSDPA와 위성통신 환경에서 개발된 HMRET 프로그램을 이용하여 실시간으로 의료데이터를 송수신할 때, 보안문제를 보완하기 위해서 VPN(Virtual Private Network) 프로토콜을 적용시켰다[5].

최종적으로는 VPN 프로토콜 하에서 IP layer 기반에 적용 가능한 AH(MD5, SHA-1), ESP(3DES) 알고리즘을 변화시키며 시뮬레이션 환경에 적용시켰을 때의 프로세싱 타임과 네트워크 망의 상태를 평가할 수 있는 지표인 QoS를 통해 지연(Round Trip Time), 지터(Jitter), 대역폭(Throughput)을 산출하였으며, 원격 진료 시스템의 정책 결정에 기반이 될 수 있는 적절한 알고리즘을 제안하였고, 이 결과를 바탕으로 무선통신 환경에서의 원격진료 시나리오를 테스트 해봄으로서 원격진료 시스템에 보안 적용 가능성을 파악하였다.

마지막으로 이를 종합하여 Wibro, HSDPA와 위성통신을 이용한 실시간 원격응급진료 시스템의 유용성과 한계점에 대해 연구하였다.

제 2장. 위성통신

2.1 무궁화 2호 위성

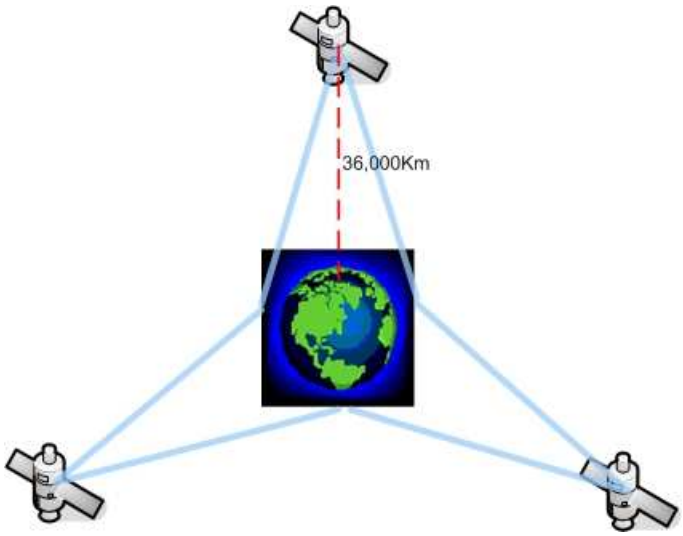


그림 2-1. 정지궤도 인공위성(Geostationary earth orbits)

무궁화 2호 위성은 정지위성으로서 통신, 방송 등의 역할을 하는 위성이다. 본 논문에서는 통신위성으로서 무궁화 2호를 이용하였다. 통신위성은 다른 위성들과는 달리 반드시 정지궤도에 위치하여야 한다. 정지궤도란 적도 위 약 36,000Km를 말하며 일반적으로 위성의 궤도가 높아질수록 위성이 지구를 1회전하는데 소요되는 시간이 길어진다. 즉, 약 36,000km 상공에서 위성이 지구를 1회전하는데 24시간이 소요되어 지구의 자전주기와 일치하게 되고 지상에서 올려다 보았을 때 위성은 정지해 있는 것처럼 보이게 된다. 만일 궤도의 높이가 40,000Km가 되면 28시간쯤 소요된다. 약 36,000Km 상공에 정지해 있는 통신위성에서는 지구면적의 43%가 내려다 보인다. 따라서 그림 2-1과 같이 이론적으로는 적당한 위치에 3개의 위성만 띄운다면 극지역을 제외한 지구전역의 통신중계를 할 수 있다[6].

그러나 실제로는 통신위성의 중계능력에 한계가 있기 때문에 세 개의 통신위성으로 지구전역의 통신을 수행하는 것은 불가능하다.

궤도	동경 116도의 정지궤도(35.786Km)
발사무게	1.464Kg
발사일	1996년 1월 14일
위성제작사	Lockheed Martin Astro Space(LMAS)
발사용역사	McDonnell Douglas
중계기수	12
출력	12W
사용대역/대역폭	Ku band(SHF, 12.4~18Ghz)/36Mhz
최대Throughput	400Kbps~1.5Mbps(수원위성관제센터:768Kbps)
Round_Trip_Time	700ms

표 2-1. 무궁화 2호 위성의 제원

우리 나라에서 쏘아올린 무궁화 위성은 700명이 동시통신이 가능한 통신용 트랜스폰더(36Mhz)를 12개, 4개 방송을 동시에 수행할 수 있는 방송용 트랜스폰더(27Mhz)를 3개 싣고 있다. Ku band이므로 12~14Ghz 에 해당하는 주파수 대역을 가지며, 대역폭은 약 36Mhz를 사용한다. Throughput은 400Kbps~1.5Mbps 해당하는 값을 가지며, 본 논문에서 실험한 수원위성관제센터의 위성서비스는 최대 768Kbps를 지원해 주었다. 정지위성인 무궁화 위성에서 발사된 전파는 지구 표면으로 발사되기 때문에 같은 전파를 다수의 지구국이 동시에 수신한다. 이것을 이용해서 다중접속 통신회선이 구성된다.[7]

2. 2 위성통신 시스템 구성

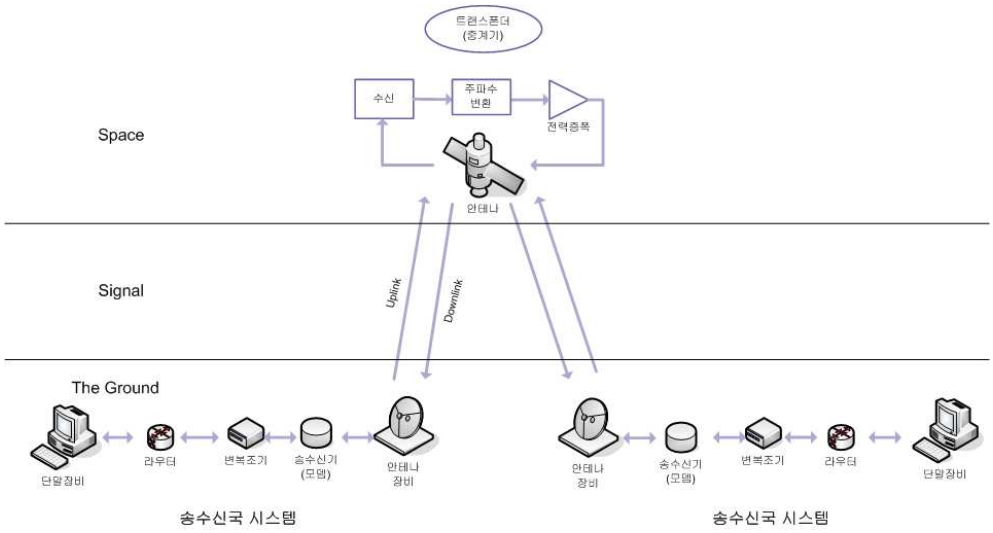


그림2-2. 위성통신 시스템 구성

위성통신 시스템은 우주 공간의 위성체와 이 위성체를 지상에서 제어하는 위성관제소 및 지상의 이용자들이 위성체 내의 페이로드를 이용하여 통신 서비스를 제공해 주거나 제공받을 수 있도록 하는 위성지구국으로 구성된다. 이 중에서 위성체는 위성이 성능을 제대로 발휘하는데 필요한 버스부분과 위성의 통신을 담당하는 페이로드 부분이 있다. 또한, 지구국으로부터 송신된 상향링크 신호를 수신하여 저잡음 증폭기에서 증폭한 다음에 하향링크 주파수로 변환시켜 고주파 증폭기에서 고전력으로 증폭한 다음 송신 안테나로 지구국에 송신하는 송수신 장치인 중계기와 위성체의 입출력 인터페이스로 취급되는 안테나가 있다[8].

본 논문에서 실험한 수원소방관제센터에는 그림2-2와 같이 위성통신의 신호를 주고 받을 수 있는 송수신국 시스템을 갖추고 있다. 초창기 지구국의 안테나는 미약한 신호를 받기 위해 엄청나게 큰 안테나(약 20~30m) 시스템을 구축해야 했으나, 기술의 발전으로 위성체까지 보내는 송신전력의 상승과 SHF(3~30Ghz)에 해당하는 높은 주파수를 사용하여 시스템의 크기가 작아졌으며, 비용도 줄일 수 있게 되었다.

2. 2. 1 위성통신의 전파 지연

위성통신에서는 매우 긴 거리차이 문제가 발생한다. GEO(무궁화 2호) 인공위성을 이용한다고 가정 하였을때, 한 지구국에서 또다른 지구국으로 데이터 패킷을 전송한다고 하면, RTT 딜레이는 2×250ms 곧, 500ms 정도의 지연이 발생한다[9]. 이 전파지연 시간은 다른 여타 상용 통신망 보다 매우 큰 수치이다. 주된 문제중의 하나는 전파지연으로 인해 음성신호의 에코현상을 일으키거나 영상신호가 실시간으로 전송될 수 없는 환경에 놓이게 한다.

2. 2. 2 위성통신의 접속방식

○ 주파수분할 다원접속(FDMA : Frequency Division Multiple Access)
- 하나의 중계기를 여러 지구국이 공용할 수 있도록 중계기의 주파수 대역폭을 분할
- 상호변조 잡음이 발생 및 주파수와 위상이 변화하는 단점있음
- SCPC(Single Channel Per Carrier) , MCPC(FDM/FM/FDMA) 방식

o 시분할 다원접속 (TDMA : Time Division Multiple Access)
- 시간적으로 분할된 버스트 (burst)를 위성 중계기에서 서로 중첩되지 않도록 사이사이에 삽입시켜 여러 지구국들에 의해 위성 중계기를 공유하는 방식
- 반송파들의 상호변조에 의한 간섭문제 없음
- 위성간 간섭에 의한 영향이 FDMA 보다 작고, 신호처리량이 FDMA 보다 큼

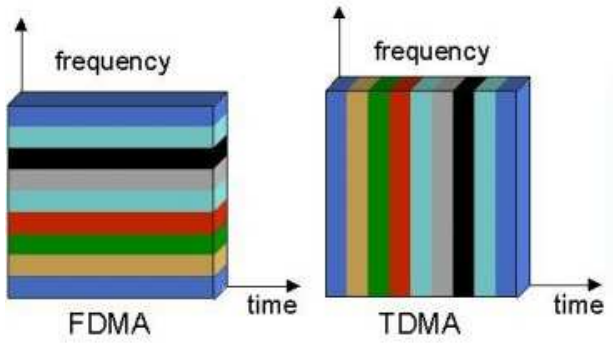


그림 2-3. 위성통신의 다원접속 방식

위성통신에서는 1개의 위성중계기에 복수개의 지구국이 붙게되는 Multiple

Access Scheme을 이용하게 된다. Uplink에는 FDMA가 이용되며, Downlink에는 TDMA를 사용한다. FDMA(Frequancy Division Multiple Access) 방식은 각각의 반송파에 서로 다른 주파수를 할당하여 한개의 위성중계기를 공유하는 방식이다. 이 방식은 동일한 위성 중계기가 복수개의 반송파를 공통 증폭하기 때문에 고출력증폭기의 진폭 및 위상의 비선형 전달특성으로 인한 혼변조잡음이 발생하여 전송 특성을 열화시키며 이를 방지하기 위해 고출력증폭기의 동작점을 포화점보다 충분히 낮은 지점에 설정하여야 하므로 위성전력을 유효하게 이용하는데 제한이 있다. TDMA(Time Division Multiple Access) 방식은 공통의 반송파를 복수개의 디지틀 신호가 시분할하여 위성중계기를 공유 사용하는 방식으로서 임의의 순간에 한개의 디지틀 신호가 위성 중계기를 점유하게 된다. 이 때문에 TDMA 방식에서 발생하는 혼변조잡음이 발생하지 않으므로 원리적으로는 위성중계기 출력을 포화점에서 사용할 수 있으나, 포화전 가까이에서 동작될 경우 부호간 간섭이 발생하므로 입력 동작점을 포화점으로부터 약 2~3dB 낮게 할 필요가 있다. TDMA 방식의 구현방법으로서는 디지틀 신호의 속도에 따라 저속 및 고속 TDMA 방식이 있다[10].

2. 2. 3 위성통신의 보안

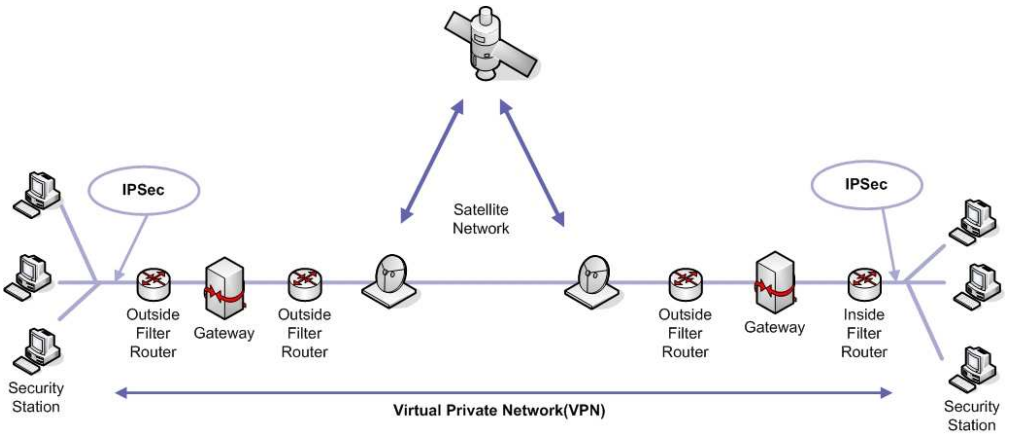


그림 2-4. 위성통신에서의 보안 프로토콜 적용

위성통신 환경에서 보안의 문제는 위성통신을 통한 데이터가 넓은 지역에 걸쳐서 뿌려지기 때문에 위성 수신기를 설치한 곳에서는 모두 데이터 수신이 가능하게 되므로 통신을 상용화 하는데 있어 큰 방해물이 될 수 있다. 게다가 긴 지연시간과 높은 비트 에러율은 보안을 허술하게 하는 원인으로 지적되고 있다. 그래서, 그림 2-4와 같은 형태로 VPN 터널링 프로토콜과 IPSec 알고리즘이 이용되고 있다 [11].

제 3장. Wibro(Wireless Broadband Internet)

3. 1 Wibro의 개념

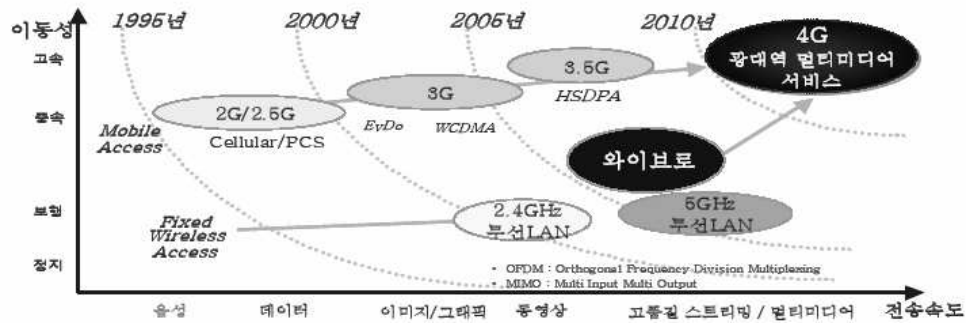


그림 3-1. Wibro의 발전방향

국내 통신 산업은 2002년 3/4분기를 기준으로 초고속 인터넷 가입자가 1000만을 넘고 이동통신 가입자가 3200만을 넘는 정보통신 산업의 고도성장에 힘입어, 전국에 걸쳐 언제 어디서나 음성 및 저속의 데이터 서비스가 가능한 이동통신환경과, 대부분의 가정에서 초고속 인터넷 서비스를 받을 수 있는 유선통신 환경이 구축되었다. 이에 따라 유선서비스를 사용자들에게 거의 만족시켰지만, 여전히 무선서비스에 대한 욕구가 커지게 되었고, 이에따라 CDMA2000 1xEVDO와 같은 이동통신 기반 무선인터넷이 나타나게 되었다. 그러나 이 이동통신기반의 무선인터넷은 고속의 이동성을 지원하는 대신 전송속도 및 사용요금에서 제약을 받아왔다. 이러한 문제를 해결하기 위해 나타난 것이 Wibro이며 휴대 인터넷이라는 이름으로 이동성과 전송속도에 대한 사용자의 욕구를 만족시키려 하고 있다[12].

국내에서 휴대인터넷 사업을 위해 2002년 10월 2.3Ghz 대역을 무선가입자망(WLL)용에서 휴대인터넷용으로 용도 변경을 하여, 2003년 1/4분기에 한국전자통신연구원(ETRI) 주도로 5개사가 참여한 HPi(High-speed Portable Internet) 프로젝트를 시작하였고, 2004년 7월 정부는 와이브로에 대하여 IEEE 802.16~1004와 802.16e D3 이상의 표준안과 5개의 성능 요구 사항을 만족할 것을 결정하였다. 이후, 2005년 6월에 한국정보통신기술협회(TTA, Telecommunications Technology

Association, TTA)에서 와이브로 시스템의 2차 표준을 완성하였다. 이와같이 표준화된 Wibro는 2005년 9월에 IEEE 802.16e의 표준규격위원회에서 국제 표준에 반영되었다. 무선으로 광대역 액세스를 가능하게 하는 와이브로 네트워크는 60Km 이상의 속도로 이동하면서도 1Mbps 이상의 하향 트래픽용 대역폭과 128Kbps 이상의 상향 트래픽용 대역폭을 제공할 수 있다. 그러므로 기존의 셀룰러 네트워크보다 저렴하고 무선랜보다 넓은 액세스 영역을 제공한다[13].

접속방식	OFDMA
최대 전송속도(Up/Down)	1Mbps/3Mbps
최소 전송속도(Up/Down)	128Kbps/512Kbps
표준	TTA(2005. 6)
음성서비스	VoIP
이동성	60Km

표 3-1. Wibro Specification

3. 2 Wibro 통신 및 프로토콜

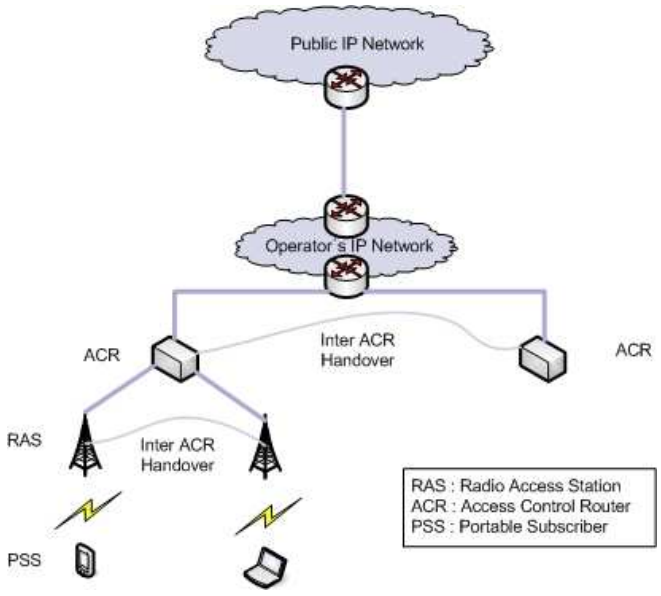


그림 3-2. Wibro 네트워크 구조

위 그림 3-2와 같이 액세스 네트워크인 Wibro 코어 네트워크(Wibro Core

Network)의 주요 구성요소는 액세스 제어 라우터(Access Control Router, ACR)와 무선 액세스 스테이션(Radio Access Station, RAS)이다.

3. 2. 1 RAS

Wibro 기지국으로서 무선접속이 가능하도록 하며, 무선자원의 효율적 관리 및 제어 기능 및 디지털 신호처리 기능을 한다. 이동성(핸드오프)을 지원하며, 하향링크 멀티캐스트를 하며, QoS 제공과 인터페이스 기능, RF 송수신과 동기화가 진행된다.

3. 2. 2 ACR

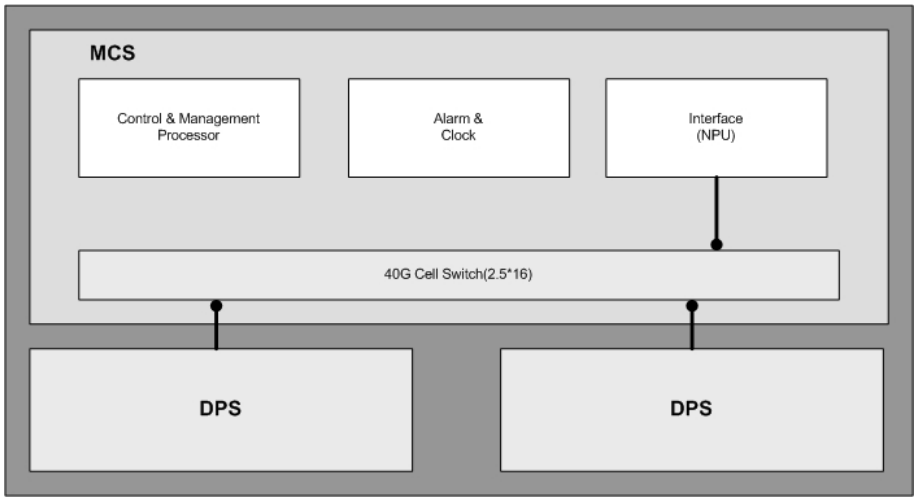


그림 3-3. ACR 구성도

ACR 시스템이란 무선 액세스 스테이션과의 연동을 통해 40G Cell Switch를 하여 다수의 DPS(Data Processing Shelf)를 하나로 결합하는 역할을 한다. 또한 이동 단말의 이동성 관리와 과금과 통계 정보의 생성 및 통보, QoS 제공, 인증과 보안 및 무선자원 관리 및 제어를 한다.

- DPS의 구성
  - SCMA(Subsystem master shelf Control and Management board Assembly)
    * Shelf당 2장 실장, Shelf master로 시스템제어
    * 내부 스위치, Cell Switch 인터페이스(NPU 프로세싱)
  - 프로세싱 보드

* DPSA(Data Processing Server board Assembly) : 제어 프로토콜 처리

* RPSA(Radio Protocol Server board Assembly) : 베어러 프로토콜 처리

* DPSA와 RPSA는 최대 12장 실장 가능, DPSA와 RPSA의 비율은 트래픽 특성에 의해 결정

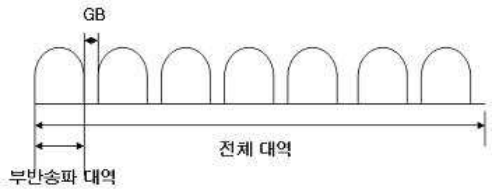
- MCS 구성

- 중앙제어 블록

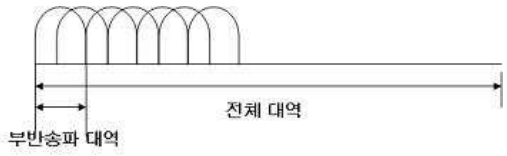
  * Cell Switch 및 인터페이스 제공(GE)

- 고속 인터페이스 카드(PEBA-Packet Engine Board Assembly)

3. 3 OFDM Symbol



(a) FDM(Frequency Division Modulation)



(b) OFDM(Orthogonal Frequency Division Modulation)

그림 3-4. FDM과 OFDM

일반적으로 여러개의 반송파를 사용하는 방법은 FDM(Frequency Division Modulation)이다. FDM 에서는 전체 주파수 대역을 여러개의 조그만 대역으로 나누기 위해서 각각의 부 반송파 사이에 서로간의 영향을 배제하기 위한 틈을 주게

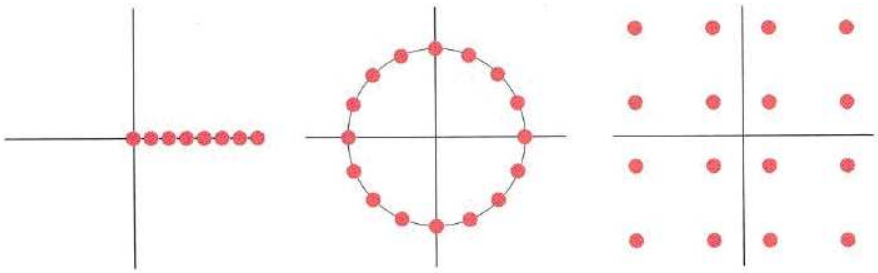
된다. 이렇게 함으로써 전체 대역을 여러 개의 부반송파로 나눌수 있게 되었으나 그림 3-4 (a)와 같이 여러개의 부반송파로 나누기위해서 각각의 부반송파 사이에 준 틈 (Guard band) 때문에 전체 대역모두를 사용할 수 없는 비효율성 발생하게 된다. OFDM 은 FDM의 이러한 비효율성을 보정해 주기 위해서 그림3-4 (b) 와 같이 원래의 반송파의 틈 사이에 직교하게 또 다른 반송파를 겹쳐 놓게 되는 것이다. 곧, 반송파 서로간의 영향을 주지 않도록 부반송파의 주파수를 설정하는 것이다[14].

3. 4 Adaptive Modulation

최근에는 단말(휴대전화)을 비롯한 무선통신 시스템의 상당수가 유저의 증가에 대응하기 위해 주파수 이용 효율과 보안성을 높이고, 소형화를 목적으로 디지털화화고 있는 추세이다. 더구나 고도의 정보통신 시스템에서 변조기술은 더욱 진화되어 복잡해지고 있다. Wibro 통신 시스템에 이용되고 있는 핵심 기술인 디지털 변복조 방식의 원리는 다음과 같다.

3. 4. 1 QPSK와 QAM의 원리와 변복조기의 구성

QSM의 원리는 ASK나 PSK에서 다치화를 진행해 나가면 그림 3-5 (a), (b)에 나타낸 바와 같이, 심벌간의 거리가 가까워져 심벌 하나하나를 구별하기가 어려워진다. ASK에서는 I축상에만, PSK에서는 원주상에만 심벌이 존재하여 평면상을 좋은 효율로 사용하지 않는다는 것을 알 수 있다. 그래서, 그림 3-5 (c)와 같이 진폭과 위상의 양쪽으로 데이터를 대응시킨 변조방식이 QAM(Quadrature Amplitude Modulation)이다.



(a) ASK(**Amplitude Shift Keying**) (b) PSK(**Phase Shift Keying**) (c) 16 QSM

그림 3-5 QSM과 QPSK의 변조방식

QAM 변조파를 발생시키려면 QPSK(**Quadrature Phase Shift Keying**) 변조에서 -1과 1밖에 취하지 않았던 진폭을 변화시키면 된다. 즉, 위상이 다른 사인파를 진폭변조하게 된다. 이 위상이 다른 사인파는 직교하고 있으므로 직교 진폭변조 QAM이라 부른다.그림 23에 16 QAM의 심벌 배치를 나타낸다. 16심벌이 있으므로 I와 Q 각각 4치의 조합으로 16점(=4 4)을 결정한다. 그림에서는 I와 Q 각각 등간격으로 4치를 배치했다. 정수로 했으므로 값은 -3, -1, 1, 3으로 된다.QAM는 다치변조가 기본으로 16 QAM이 가장 심벌수가 적은 변조방식이다. 현재는 64 QAM, 256 QAM 등이 실용화되어 있다. 따라서 Wibro에서는 QPSK와 64QAM를 다양하게 변화를 시켜 Wibro의 통신 대역을 조절한다[14].

3. 4. 2 시간 영역

역 푸리에 변환을 통해 시간 영역의 OFDM 파형을 생성하며 이 결과로 생성된 OFDM 파형의 심벌 지속 시간을 유효 심벌 시간 Tb 라고 한다. 유효 심벌 기간인 최종 Tg의 복사본은 CP(Copy)로 나타내며, OFDM 신호의 맨 앞에 위치시켜서 신호의 직교성(Orthogonal)을 유지하는 역할과 동시에 다중경로(Multipath)를 수집하는 역할을 수행한다. CP는 수신기에서 제거하며, OFDM 심벌의 시간 영역에서의 구조는 아래 그림 3-6 과 같다.

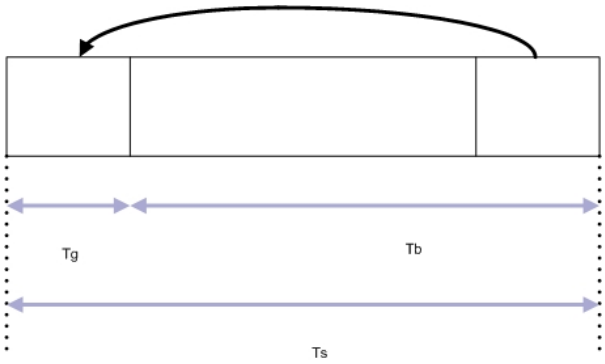


그림 3-6. OFDM Symbol

송신기 에너지는 보호 구간 길이에 비례하여 증가하지만, 수신기 에너지는 동일하게 유지되기 때문에, Eb/No는 10log(1-Tg/(Tb+Tg)/log(10))[dB] 만큼의 손실이

발생한다. 여기서 주기적인 확장개념을 적용하면, 확장된 부호의 구간 어느곳에서나 수신기에서 FFT를 수행하는데 필요한 샘플을 얻을 수 있다. 이는 다중경로 내성과 코드 시간의 동기 오류의 허용 한도를 제공할 수 있음을 의미하는 것이다.

단말기의 초기화 과정에서는 CP를 찾기위한 검색을 시도하며, 상향링크와 같은 CP를 사용한다. 따라서 CP가 바뀌면 단말기는 기지국과의 동기를 조절해야만 한다[15].

3. 4. 3 Frequency 영역

데이터 전송용으로 쓰이는 데이터 부반송파와 다양한 측정용으로 쓰이는 파일럿 부반송파, 신호가 없으며, 전송하지 않는 보호 대역 및 DC 부반송파용으로 쓰이는 널 부반송파의 수에 따라 FFT의 크기가 결정된다.

널 부반송파는 푸리에 변환을 시행하였을 때 인접 주파수의 간섭으로 작용되는 노이즈 신호를 줄이는데 사용한다. OFDMA 모드에서 유효 부반송파는 부반송파의 부분집합으로 나뉘어 진다. 이때 각각의 부분집합을 채널이라하며, 그림3-7 과 같은 채널을 형성할 수 있다.

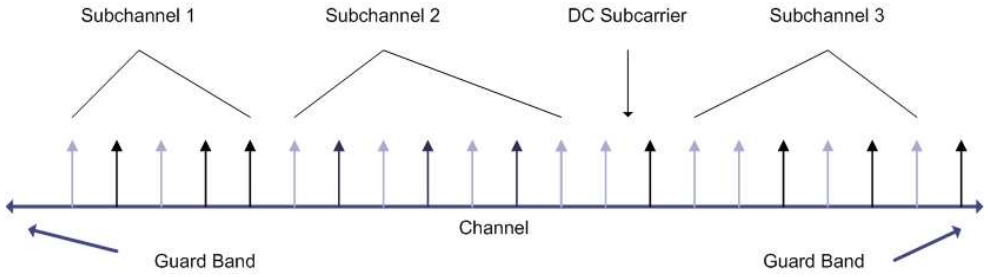


그림 3-7. OFDMA 3채널 주파수 영역

3. 4. 4 전송 신호

OFDM 심벌 구간 동안 안테나에서 전송되는 OFDM 심벌을 시간 함수로 표현하면 다음 식과 같다.

$$s(t) = e^{j2\pi fct} \cdot \sum_{k=-(Nused-1)-2, k\neq 0}^{(Nused-1)/2} Ck \cdot {}^{j2\pi k\triangle f(t-Tg)}$$

(t: 0<t<Ts 범위에서 OFDM 심벌의 초기부터 경과한 시간)

Ck : OFDMA 심벌 기간 동안 주파수 오프셋 인덱스가 k인 부 반송 파에 전송되는 복소수 데이터로 QAM 성상도에서의 한 점을 나타낸다.

Tg : 보호구간

Ts : 보호구간을 포함하는 OFDM의 심벌구간

⊿f : 부반송파의 주파수 간격

3. 4. 5 프레임 구조

TDD 시스템에서는 상향링크와 하향링크를 전송시간으로 구분된다. 하향링크는 하나의 프리앰블 심벌, FCH, DL-MAP, 데이터 심벌 순서로 시작된다. 상향링크는 제어심벌 전송부터 시작된다. 상하향 전송시간을 구분하는 보호시간인 TTG(121.2 μs) 및 RTG(40, 4μs)는 프레임의 중간과 마지막에서 하향링크나 상향링크에 삽입된다.(표 3-2)

프레임 구성 변수	변수 값
FFT 크기(N_{FFT})	1024
심벌시간(Ts)	115.2μs
프레임당 심벌 수	42
TTG 시간	121.2μs
RTG 시간	40.4μs

표 3-2. TDD 시스템 프레임과 변수

하향링크 프레임에는 PUSC 서브채널, 다이버시티 서브채널 및 AMC 서브채널이 있고, 상향링크 프레임에는 다이버시티 서브채널과 AMC 서브채널이 있다.

제 4장. HSDPA(High Speed Down Link Packet Access)

4. 1 HSDPA의 개요

비동기식 3.5세대 이동통신 서비스를 의미하는 HSDPA는 3세대 WCDMA의 진화형태로, 하향 고속화 패킷 접속 방식(High Speed Downlink Packet Access)라는 이름과 같이 하향 다운로드 속도가 WCDMA에 비해 최대 7배나 빨라진 혁신적인 차세대 통신 기술이다. 하향 링크의 속도를 14Mbps 까지 개선시키겠다는 목표를 가지고 HSDPA는 무선 이동통신 환경에서 다양한 종류의 멀티미디어 서비스 이용이 가능하도록 데이터를 고속 패킷 전송으로 제공할 전망이다. 이동 무선 통신 기술은 동기식과 비동기식 2가지 방식으로 발전하고 있다. 북미지역에서 시작된 IS95A 기반의 동기식과 유럽을 중심으로 한 GSM 기반의 비동기식이 그것이다.

3GPP 비동기식 표준화 기구에서 데이터 속도를 좀 더 높이기 위해 GSM/GPRS에서 사용한 TDMA 방식과는 다른 무선접속 기술인 CDMA를 채택해 WCDMA(Release 99)의 표준화를 완료했다. 그리고 무선 이동 환경에서의 고속 패킷 데이터 서비스 요구에 부응하기 위해, 보다 향상된 데이터 비율과 패킷 데이터 전송을 가능하게 하는 표준 개발을 시작했다. 그 결과, gigid 링크 속도를 14Mbps까지 제공할 수 있는 HSDPA(High Speed Downlink Packet Access)의 표준화를 완료 했으며, 현재 상용화 되고 있다[16].

Multiplex	TDM/CDM
DL/UL	3 Mbps/2 Mbps (실제 1 Mbps/0.37 Mbps)
단말속도	Over 200Km
음성서비스	Packet+Voice 지원
Frequency	2.0Ghz
Standardization	3GPP(2002.6)

표 4-1. HSDPA Specification

4. 2 HSDPA 통신 및 프로토콜

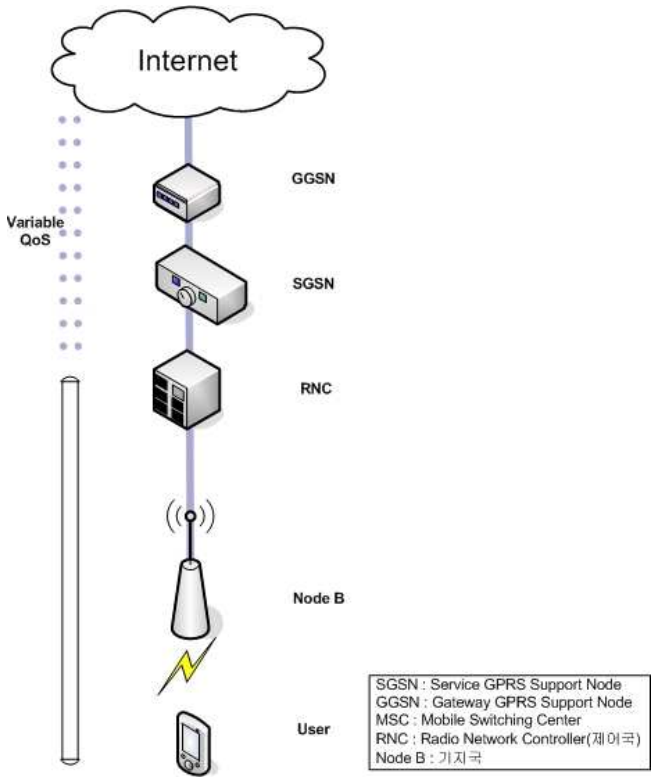


그림 4-1. HSDPA 통신 개념

HSDPA는 3GPP에서 고속 패킷 전송을 위해 하향 링크에 추가된 패킷 전용 접속 방식이다. 최초의 HSDPA 표준은 WCDMA FDD(Frequency Division Duplexing) 표준에서 제정되었으며, 상하향 10MHz 전송 대역을 사용하는 FDD 모드에서 최대 10Mbps 전송률을 제공한다. 또한 FDD에 이어서 TDD(Time Division Duplexing) 방식에 대한 HSDPA 표준이 제정되었다. 3GPP TDD 모드는 5MHz 대역에서 3.84 Mcps의 칩속도를 갖는 HCR(High Chip Rate) TDD 모드와 1.6MHz 대역에서 1.28Mcps의 칩속도를 갖는 LCR(Low Chip Rate) TDD 모드의 두 가지 모드가 존재한다. TDD 방식은 상하향 링크에 대한 자원 할당을 비대칭적으로 할당할 수 있으므로, 하향 링크 채널을 최대로 할당할 경우 HSDPA의 도입으로 인한 전송 효율을 극대화 할 수 있으며, HCR TDD 모드의 경우 최대

10.2Mbps, LCR TDD 모드의 경우 최대 2.8Mcps의 전송률을 지원한다[17].

① SGSN

SGSN(Serving GPRS Support Node)은 packet-mode 기술을 사용하여 high-speed 또는 low-speed data와 신호를 효율적으로 전달하기 위한 서비스인 GPRS(General Packet radio Service)를 위한 핵심망 장치이다. RNC와 정합하여 이동 단말의 패킷 데이터 서비스를 위한 단말의 이동성 관리 및 패킷호 처리 기능을 수행하고, GGSN과 정합하여 인터넷과 같은 외부 패킷망과의 패킷 터널링 기능을 수행한다. 그리고 패킷 호의 과금을 정산하기 위한 과금 상세정보를 생성하여 외부 과금 수집 장치(CG, Charging Gateway)로 해당 정보를 송부하는 기능을 수행한다.

SGSN 시스템은 현재 유럽 3GPP Release 99 규격에 맞춰 개발 되었고, R4 및 R5와 관련된 부가기능을 용이하게 수용하도록 설계되어 있다. 현재의 SGSN 시스템은 20Gbps의 ATM Switch를 기반으로 구성되며, 각 스위치 포트당 622Mbps 급의 Throughput을 기준으로 다중화 및 역다중화기술을 이용하여 2Mbps 저속 외부 정합부터 1Gbps급의 고속 외부 정합이 가능하도록 설계되었다. 또한 시스템의 안정성을 위해 각 주요 프로세서에 대한 이중화 기능과 트래픽 경로상의 다중화 및 역다중화 장치를 2중화시켜 트래픽에 대해서도 시스템 내부에서 보다 안정화된 연결 서비스를 제공하며, 다양한 외부 정합 카드인 Fast Ehternet, ATM, Gigabit Ehternet을 통해 인터페이스를 제공한다.

② GGSN

GGSN은 IMT-2000 패킷 게이트웨이 노드(GGSN:Gateway GpRS Support Node)로서, GPRS 망의 게이트웨이 역할을 감당하는 노드이고 외부적으로는 Internet 망과의 접속을 가능케 하는 Router 역할을 지원한다. 그리고 내부적으로는 SGSN과의 접속을 통해 GPRS 망 가입자에게 Packet Data 서비스를 제공한다. UMTS에서 Packet Data를 처리하는 GPRS Network에서 가입자를 위한 Packet Data 발/착신 서비스를 제공하는 기능을 제공한다.

- 특징

가. H/W적으로 ATM 스위칭 Fabric을 기반으로 Virtual Path 및 Virtual

Channel 교환기능에 의해 시스템 내부적으로 Non-blocking 방식의 Switched Router 구조로 구성

나. 시스템 외부로 정합되는 인터페이스는 Fast Ehternet, Gigabit Ehternet, OC3급 PoS, OC12급 그리고 PoS 그리고 STM-1급 ATM 정합이 가능하며, GGSN의 정합상태에 의존하지 않고, 시스템 형상 구성에 따라 설정하며, 확장이 용이한 구조로 구성

다. 시스템 내부의 처리구조는 제어부분과 트래픽 부분이 물리적으로 구분되어 상호 영향을 최소화할 수 있도록 구성

라. 시스템의 내부 처리는 주요 제어 부분과 ATM 스위치 부분이 이중화 처리되어 시스템의 신뢰성 보장

마. 핵심망을 관리하기 위해 Generex-GGSN 시스템은 망관리 Agent를 외부 장치로 두고, 망관리 센터와 Ethernet 기반의 IP 네트워킹을 통해 망관리 기능이 제공 가능.

바. 플랫폼을 사업자가 보유하고 있는 Generex-SGSN과 동일한 플랫폼구조로 설계 구현됨으로써 유지보수가 용이한 구조를 제공

③ RNC

RNC(Radio Network Controller)는 MSC(교환기)/SGSN(Serving GPRS Support Node)과 Node B 사이에 위치하며, E1/STM-1링크를 통해서 Node B 및 MSC/SGSN과 연동된다. RNC는 음성 호, Fax 등과 같은 회선 데이터(Circuit Data) 서비스를 제공하기 위해 Iub 인터페이스로 Node B와 연동되며, In-cs 인터페이스를 통해서 MSC와 연동하여 자원의 할당 및 링크 설정기능을 담당한다. 또한 인터넷 통신과 같은 패킷 데이터(Packet Data) 서비스를 위해 Node B와는 Inb 인터페이스로 연동하여 자원의 할당 및 링크 설정 기능을 담당한다.

RNC는 저속•중속•고속 데이터 서비스, 멀티미디어 서비스, Handover 등의 서비스가 원활이 이루어지도록 지원하며, 이때 보다 나은 품질을 보장하기 위하여 Macro diversity 기능을 수행한다. BSM(Base Station Manager)은 RNC(Radio Access Network)의 운용 유지 보수 기능을 담당하는 운용자 정합장치이다.

- 특징

가. 기능별 모듈화로 확장 및 증설이 용이

나. R4 및 R5 업그레이드가 용이함.

다. 고속패킷 데이터 처리 및 다양한 프로토콜 수용이 용이함.

라. RNC 1식으로 180,000만명의 가입자(음성기준)를 수용.

마. ATM 기반의 구조로서 5Gbps 처리 용량을 갖는 ATM Switch를 사용

바. 고성능 프로세서의 채택(MPC755, MPC8260).

사. 높은 신뢰성을 위해 이중화 구조로 설계됨.

④ Node B

무선 자원의 효율적인 사용을 위해 UMTS 시스템은 RRC(Radio Resource Control) 프로토콜을 사용한다. RRC는 사용자 및 데이터에 대한 효율적인 자원 분배를 수행하기 위해 사용되며, 무선 접속망의 RNC(Radio Network Controller)에 위치한다. RNC는 여러 개의 Node-B를 제어하며, 여러 Node-B로부터 수신된0. 정보를 이용하여 자원 할당 및 조정 기능을 수행한다.

그러나 RRC가 RNC에 위치하는 것은 네트워크상의 지연을 발생시키며, 빠르게 변화하는 채널 환경에 적응하는데 어려움이 있다. 또한, 패킷 전송은 매우 Bursty 한 특성을 가지므로 이러한 패킷 전송에 적응하기 위해서도 빠른 적응 방식이 요구된다. 이러한 문제의 해결을 위해 HSDPA에서는 기존에RRC에 존재하던 스케줄링 기능을 Node-B의 MAC로 이전하였다. 또한, 전송의 단위를 기존의 10ms에서 2ms로 줄여 패킷 전송 특성에 효과적으로 적응하도록 하였다. 자세한 내용은 다음장 Node B Scheduling에서 설명한다.

4. 2. 1 HSDPA 핵심기술

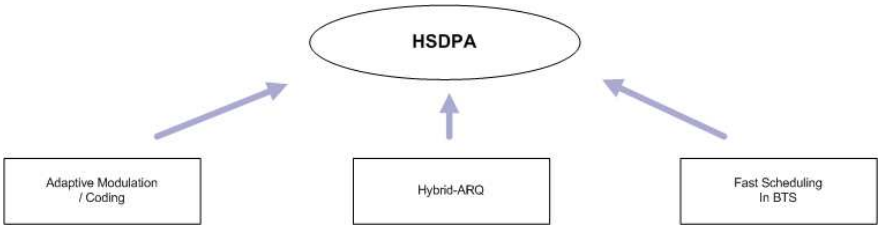


그림 4-2. HSDPA 핵심기술

HSDPA의 물리 계층의 동작은 기존의 R99와 큰 차이를 보이지만, 물리 계층의

상위에서는 HSDPA의 도입에 따른 변화를 최소화하여 이전 시스템과의 호환성을 보장하고자 한다. 하지만, HSDPA에 채택된 적응 변복조 기법이나 하이브리드 ARQ(Automatic Repeat reQuest)와 같은 링크 적응 기술들을 효율적으로 이용할 수 있으려면 이들을 관리하고 제어하는 부분이 되도록 무선접속 인터페이스와 가까운 곳에 위치하여야 한다. 더욱이 데이터의 스케줄링을 담당하는 부분이 기존처럼 제어국(RNC)에 위치하게 되는 경우에는 지연시간에 의해 채널 환경에 맞는 적절한 스케줄링이 이루어질 수 없게 된다. 이런 이유들로 HSDPA에서는 스케줄링 기능을 비롯한 대부분의 무선자원 제어기능이 제어국보다는 기지국(Node B)에 위치하도록 결정되었다. 따라서, HSDPA를 지원하기 위한 기존 프로토콜 구조 변화의 특징으로는 HSDPA를 지원하는 Node B에는 무선자원의 제어를 위해 MAC계층의 일부기능이 위치하게 되었다. 이 프로토콜 계층을 MAC-hs부 계층이라고 정의하며, MAC-hs부 계층은 프로토콜 구조상 MAC계층의 가장 하부에 위치하면서 채널 환경에 맞는 적절한 변조, 부호 방식을(MCS) 선택하거나, 데이터의 스케줄링 기능을 담당한다. MAC계층의 상위에 위치한 HSDPA를 위한 RLC계층은 기존 시스템과의 호환성을 위해 동작상의 변화가 거의 없지만 AM 또는 UM만이 사용되며 TM은 ciphering 문제로 사용되지 않는다[18].

① AMC

무선 링크의 효율적인 사용을 위해서 링크 적응(Link Adaptation) 기법이 사용되고 있다. 기존의 대표적인 링크 적응 기법은 전력 제어(Power Control) 기법이다. 전력 제어 기법은 무선 링크에 따라 전력을 제어하여 전송 품질을 유지시키는 방법으로 음성과 같이 고정된 전송률 상황에서 링크의 품질을 보장하기 위한 시스템에 효율적인 방식이다.

반면, 멀티미디어 데이터는 서비스 종류에 따라 다양한 전송률, 다양한 전송 품질 등을 요구하므로 기존의 음성 위주의 서비스 제공과는 다른 개념의 링크 적응 기법이 요구된다. AMC 기법은 이러한 데이터 전송에 효율적인 링크 적응 기법으로, 전송 전력이 아니라 전송률을 채널 환경에 맞게 변화시키는 적응 방식이다.

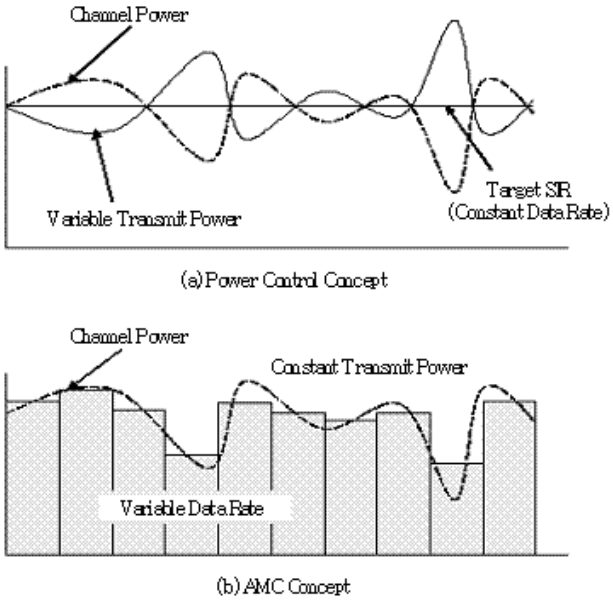


그림 4-3. AMC 와 전력제어의 비교

그림 4-3.은 전력제어와 AMC 간의 개념적인 차이를 설명하고 있다. 전력 제어의 경우 고정된 target SIR(Signal-to-Interference Ratio)을 얻기 위해 전송 전력을 채널에 따라 변화 시킨다. 반면, AMC는 채널의 특성에 따라 적절한 전송률을 결정하여 전송하므로 기본적으로 전송 전력은 고정된다. 전송률은 MCS(Modulation and Coding Selection) 레벨에 의해 결정되는데, MCS는 미리 정의된 변조 및 채널 코딩 조합에 대한 레벨이다. HSDPA에서는 QPSK, 16QAM의 두 가지 변조 방식과 코드율 1/3인 터보코드를 효율적으로 펑쳐링하여 다양한 MCS 레벨을 지원한다. MCS 레벨은 수신 SIR에 따라 결정되는데, SIR에 따라 가장 높은 효율을 보이는 레벨이 선택된다.

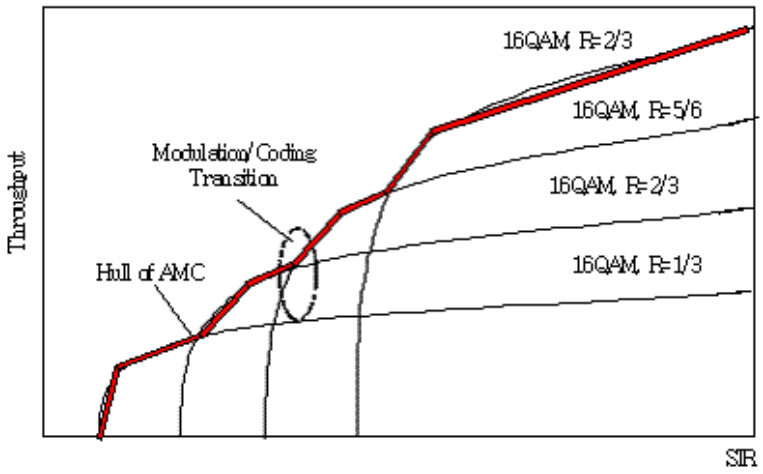


그림 4-4. MCS Level 결정 개념

그림 4-4는 AMC에서 MCS 레벨을 결정하는 과정을 개념적으로 보여주고 있다. SIR에 따라 가장 높은 throughput을 보이는 MCR 레벨을 결정하며, 결과적으로 그래프의 가장 바깥쪽에 위치한 throughput을 얻게 된다.

AMC의 지원을 위해서는 단말의 수신 SIR에 대한 정보를 기지국이 알고 있어야 하며, 단말의 수신 품질을 송신측에 전달하기 위해 CQI(Channel Quality Indicator)라는 인덱스를 사용한다.

② HARQ

HSDPA의 두 번째 핵심 기술은 물리 계층에서 ARQ를 사용하는 HARQ 기법이다. ARQ 기법은 수신 패킷에 오류가 발생하는 경우 재전송을 요청하여 이를 수정하는 기법으로 네트워크 프로토콜의 2계층인 데이터 링크 계층에서 널리 사용되는 기법이다. UTRAN 에서는 L2 RLC (Radio Link Control)에서 사용하고 있다. 반면, HARQ는 ARQ 기법을 물리 계층의 채널 코딩과 결합한 기술로 전송 채널의 동작 SIR을 낮출 수 있는 장점이 있다.

패킷 전송 시스템에서 전송 품질의 중요한 척도는 프레임 오류 확률(Frame Error Rate: FER)이다. 일반적인 패킷 전송 시 약 0.1%의 FER을 요구한다. FER 측면에서 프레임에 단 한 비트의 오류만 존재해도 오류로 처리되므로, FER을 낮추는데

매우 많은 전력이 요구된다. 만일 이 FER 요구 사항을 보다 높일 수 있다면 전송 전력 측면에서 큰 이득을 얻을 수 있을 것이다.

HSDPA에서는 동작 영역을 FER 10%로 설정하고, 이 때 발생하는 패킷 오류를 HARQ를 이용하여 수정하는 방법을 사용하여 전송 전력을 크게 낮출 수 있었다. HARQ 에서는 기존의 ARQ와 같이 재전송만을 적용하는 것이 아니라 Chase Combining 또는 Incremental Redundancy (IR)와 같은 방식을 적용하여 기존의 수신 데이터와 재전송된 수신 데이터를 효율적으로 조합하여 디코딩 성능을 높이게 된다.

이와 같은 HARQ 적용에 의해 발생하는 전력 마진에 의해서 16QAM과 같은 높은 전송 효율을 갖는 변조 기법의 사용이 가능해진 것이다. 결론적으로 HARQ 기법은 HSDPA 의 핵심 기술이라고 할 수 있다.

최근에는 HSDPA의 조기 상용화 일정을 위해 복잡한 16 QAM 기술을 제외한 QPSK only HSDPA가 추가적으로 등장하였다.

③ Node B Scheduling

Node-B는 3세대 통신인 IMT-2000 네트워크의 기지국으로, 기지국 제어기(RNC : Radio Network Controller)의 제어하에 이동국(MS : Mobile Station)과 무선 접속을 하고, BSM과 연동하여 유지 보수하는 기능을 수행하며, Node-B는 이동국과 무선 채널(Radio Channel)을 통해 접속하며, CAI(Common Air Interface)로 W-CDMA를 지원한다. Node-B는 RNC와의 정합방법으로 기존에 주로 사용하였던 EI 링크로 정합할 수 있으며, 이를 이용하여 Node-B와 RNC 사잉에 송/수신되는 각종 제어 신호와 Traffic 신호를 안정적으로 신속하게 처리할 수 있게 되어, 신뢰성 있는 서비스를 제공한다. NOde-B는 표준형(옥내형)과 옥외형, 지하철용, 소형(pico) 등으로 나누어지며 표준형은 1rack으로 최대 4FA/3Sector까지 지원 가능하며 4FA/6Sector까지 확장 rack 구성이 가능하다.

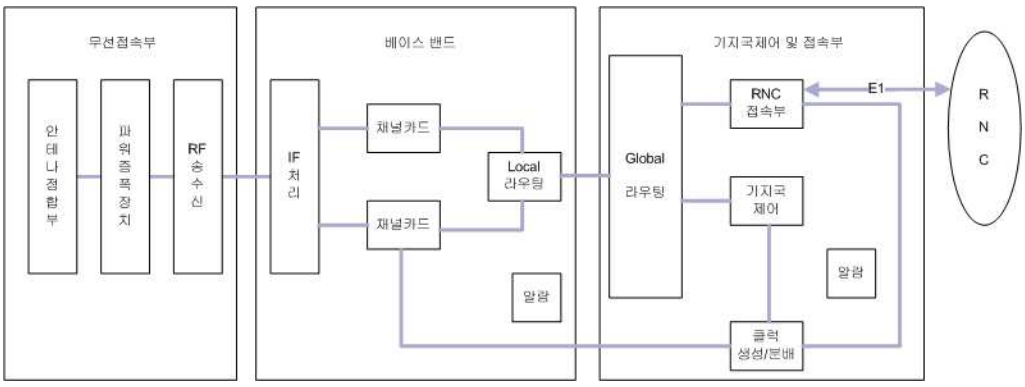


그림 4-5. Node-B Structure

- Node-B의 특징

가. 새로운 기능 지원

• 고속 데이터 서비스

• 송신 Diversity 기능

• Compressed mode

나. Pooling 구조

채널 카드당 96 채널을 지원하는 고집적화된 채널 카드는 동일한 채널 차원으로 다양한 FA, sector 구성을 통한 다양한 채널을 할당할 수 있는 Pooling 체계를 갖는다.

다. H/W 및 S/W의 module 화

Node-B는 각 H/W 및 S/W를 Module화하여, 기존 설치된 시스템의 구조를 변경하지 않고, 해당 Module을 실장 또는 탈장하는 방법으로 기지국 용량의 증감을 용이하게 하였다. S/W도 기능 및 Moduleaks 변경하게 되므로 시스템의 변경폭을 최소화하는 동시에 서비스 중단이 발생하지 않도록 하였다.

라. 편리한 운영 및 유지 보수 기능

Node-B는 운용자가 보다 편하게 시스템의 상태를 확인하고 적절한 조치를 취할 수 있도록, 시스템에 실장된 각 장치의 상태를 BSM을 통해 한글 메뉴와 함께 그래픽 화면으로 나타내었다. 또한 기지국은 원격으로 BSM과 Ethernet 및 Dial-Up Modem을 통해 비상시 디버그 및 원격 관리할 수 있는 기능을 제공한다.

마. ATM 기반 전송 기능

상위 RNC와 연결된 E1 구간의 Traffic 신호 전송에 AAL2(ATM Adaptive Layer type 2) 방식을 사용하였다. AAL2 방식은 하나의 ATM Cell에 여러 가입자의 Traffic 신호를 다중화하여 송/수신 하는 방법이다. 따라서 중계선의 사용 효율이 증대하고, 보다 저렴한 비용으로 망을 구축 할 수 있다.

4 .2 .2 HSDPA 채널 Sharing

그림 4-6. HSDPA Code 맵핑

각 슬롯(Resource)은 코드 도메인 환경 뿐만아니라 시간 도메인 환경에서 나뉘어 질 수 있어, TDMA와 CDMA의 복합 기술로서 요약될 수 있다. HSDPA에 가장 중요한 특징은 이 맵핑 기술에 의해 Throughput의 상승을 가져올수 있으며, 이에 따라 높은 데이터 저장 용량을 가질 수 있다.

제 5장. VPN(Virtual Private Network)

5. 1 VPN의 개요

공중망을 경유하지 않는 사설망은 외부로의 데이터 유출이나 외부로 부터의 보안 공격이 없다. 하지만, 이러한 사설망을 확장하여 본사와 지사간 또는 본사와 출장중인 구성원들간의 연결시에는 경제적인 이류로 전용선 대신에 공중망(Public Network)을 경유하게 되는데, 이 공중망에서의 데이터 유출이나 외부로의 공격에 취약하게 되는 문제점이 있다. 이러한 문제점을 해결하기 위하여 공중망을 경유하더라도 네트워크 구성 요소들 간에 전송되는 프레임들을 보호함으로써, 보안 면에서는 전용 사설망과 같은 보안을 제공할 수 있는 망을 가상 사설망(VPN:Virtual Private Network)이라고 한다. 이러한 VPN의 경우, 두 컴퓨터 또는 지사와 본사의 라우터간에 안전한 연결을 설정하기 위한 방법으로 사용자 인증절차를 수행한 후, 암호기법을 사용하여 공중망을 경유하는 연결이 마치 사설 링크로 연결된 것과 같은 서비스를 제공한다. 따라서, 사용자 관점에서의 VPN은 자신의 컴퓨터와 회사 서버간에 마치 전용선으로 연결된 것과 같으므로 경유하는 공중망에서의 보안 문제를 해결할 수 있게 된다[19].

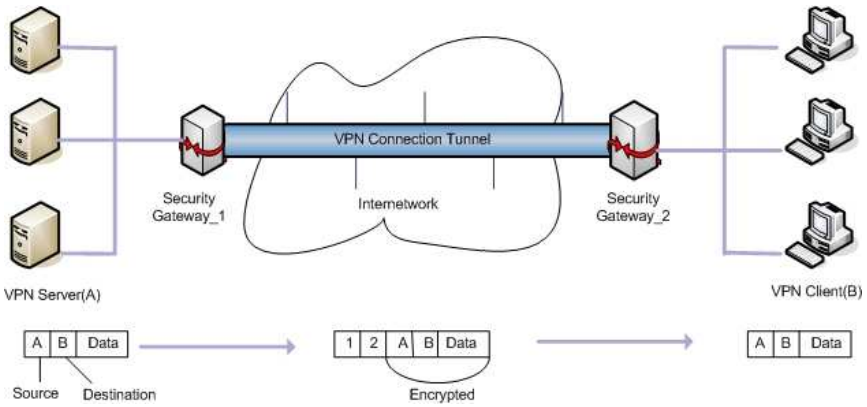


그림 5-1. 가상사설망

5. 2 VPN의 구성

VPN 망은 크게 3가지로 분류된다.

① 종점간 보안 : 전송계층 이상에서의 보안을 제공하는 Secure MIME, Secure Shell(SSH) 또는 Secure Sockets Layer(SSL)/Transport Layer Security(TLS)를 사용하여 단말간 직접 보안전송을 수행한다.

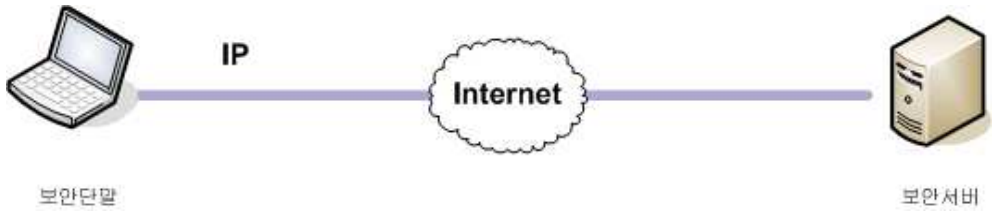


그림 5-2. 종단간 VPN

② 라우터와 라우터간 보안 : 본사와 지사를 연결하는 라우터간에 설치된 IPSec 기능을 이용하여 서로 떨어진 LAN들을 안전한 보안 터널로 연결한 경우로서, IP 계층에서의 보안을 제공한다. 따라서, 본사와 지사망 내부에 있는 컴퓨터들간에는 특별한 보안 기법을 사용하지 않고도 상호간에 신뢰성 있는 전송이 가능하다.

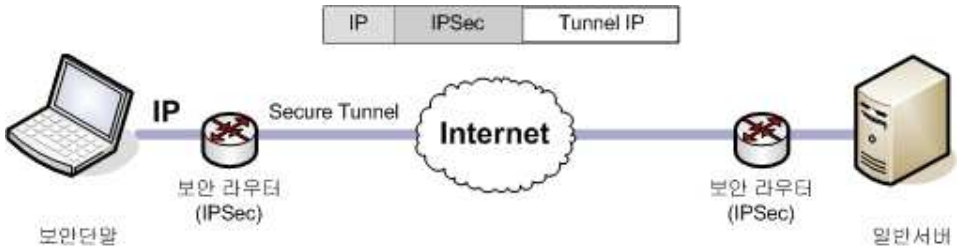


그림 5-3. Site to Site VPN

③ 클라이언트와 라우터간 보안(Secure Remote Access) : 예전에는 모바일 사용자들이 Home LAN에 접근할 때 전화선 모뎀을 사용하여 직접 HomeLAN의 원격 접속 서버(Remote Access Server : RAS)와의 point-to-point(PPP) 연결을 설정하

여, 이 장치로 부터의 사용자 인증과 내부망용 IP주소를 할당받았다. 이 경우, 전화망을 경유하므로 이 망에서의 보안은 지켜진다고 믿을 수 있었다. 인터넷을 경유하여 단말과 RAS 장치간에 PPP 연결을 설정하고자 하는 모바일 사용자에 대해서도 이러한 전화선 모뎀 활용 방법과 유사한 사용자 인증절차와 HomeLAN 용 IP주소 할당을 할 수 있다. 즉, PPP 프레임을 PPTP나 L2TP에 수납하고, 이것을 다시 단말과 RAS 장치간에만 유효한 새로운 Ip에 수납하는 기법을 사용하여 RAS 장치까지 전달한다. 이때, IPSec과 같은 기법으로 내용을 보호한다. 이것을 수신한 RAS 장치는 PPP 프레임을 취하여 사용자 인증과정을 수행하고, 내부망용 IP주소를 할당한다. 겨과적으로 PPPdusruf이 공중망을 경유하여 단말과 RAS 장치까지 연장된다. 따라서, 이 방법은 전화선 모뎀을 사용한 다이얼링 접속 서비스와 유사한 서비스를 제공하므로, Virtual Private Dial Network 기능을 제공한다고 한다. 그리고 이러한 RAS 장치를 VPN 서버 또는 L2TP Network Server(LNS), PPTP Network Server(PNS)라고 부른다[20].

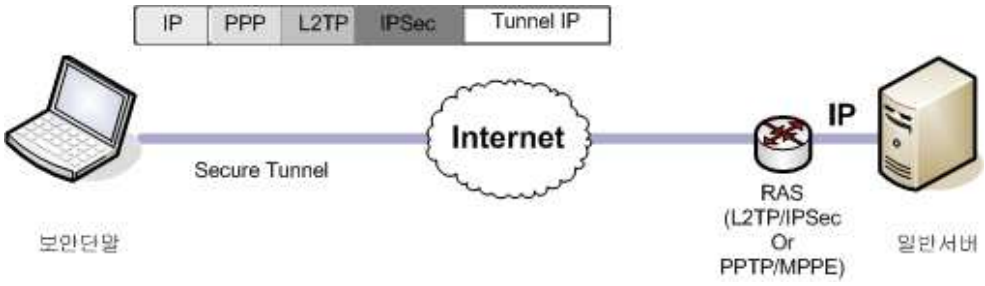


그림 5-4. Remote Access VPN

5. 3 VPN 프로토콜의 종류

VPN에서 사용되는 각 프로토콜들은 상대방과의 보안협상을 통하여 다음과 같은 기능을 모두, 또는 일부를 제공한다[21].

- 기밀성 : 데이터에 대한 암호화를 통하여 내용의 유출을 방지한다.
- 데이터 무결성(메시지 인증) : 데이터의 전송과정에서의 변조를 감지할 수 있도록 한다.
- 사용자 인증 : 망에 접속할 수 있는 자격에 대한 사용자 인증과정을 제공한다.

구분	프로토콜
응용계층에서의 메시지 보안 프로토콜	S/MIME : 보안 e-mail 프로토콜
	SSH : Secure Shell 프로토콜
트랜스포트 계층에서의 메시지 보안 프로토콜	SSL/TLS(Secure Socket Layer/Transport Layer Security) 프로토콜
망 계층에서의 메시지 보안 프로토콜	IPSec(IP Security) 프로토콜
링크계층 PPP 프로토콜에 의한 사용자 인증 프로토콜	PPP PAP (Password Authentication Protocol)
	PPP CHAP (Challenge Handshaking Authentication Protocol)
	PPP MS CHAP(Microsoft CHAP)
	EAP-MD5(Extensible Authentication Protocol-Message Digest 5), EAP-TLS
링크계층 암호화 프로토콜	WEP(Wire-Equivalent Privacy)
링크계층 PPP 패킷을 수납하는 터널링 프로토콜/암호화 프로토콜	PPTP/MPPE(Point to Point Tunneling Protocol/Microsoft Point to Point Encryption)
	L2TP/IPSec(Layer 2 Tunneling Protocol/IPSec)
인증서버와 클라이언트간 인증 프로토콜	RADIUS(Remote Authentication Dial In User Service)프로토콜
	DIAMETER
LAN/WLAN에서의 스위치 포트 활성화를 위한 사용자 인증 프로토콜	IEEE 802.1x/EAP

표 5-1. VPN용 프로토콜의 계층별 정리

제 6장. IPSec(IP Layer Security Protocol)

인터넷에서 정보 보호는 인터넷을 구성하는 여러 계층(layer)에서 이루어 질 수 있다. 그 중 IP계층은 패킷 교환망에서 단순히 데이터의 신뢰성 있는 전송만을 염두에 두고 개발되었다. 때문에 IP sfoofing(IP 데이터 프로그램의 주소 변조), IP sniffing(IP 데이터 프로그램 도청)과 같은 보안 취약점이 있다. 또한 메일·웹 보안, 디지털 서명, 공개 키 기반구조 등은 응용 계층(application layer)의 정보 보호 방식이라 할 수 있으므로 네트워크 계층의 IP 패킷 보호를 위한 인터넷 표준 방식인 IPSec이 개발되었다. 원래 IPSEC이란 이름은 이 방식의 표준화를 추진해 온 IETF (Internet Engineering Task Force)의 해당 워킹 그룹의 이름 (IPSEC WG)에서 따 왔으며 지금도 발전되고 있는 표준이다[22].

6. 1 IPSec 보안 서비스

IPSEC 워킹 그룹은 IP 패킷의 무결성, 인증, 기밀성 보안 서비스를 지원할 수 있는 보안 프로토콜과 암호 알고리즘 표준의 개발을 임무로 하여 1993년 발족되었다. 패킷의 무결성 (integrity) 서비스란 송신자가 발송한 패킷이 중간에 제3자에 의해 임의로 수정 또는 변경되지 않고 무사히 수신자에 까지도착되었음을 보장하는 서비스이다. 패킷의 인증 (authentication) 서비스는 보다 정확히 송신자인증을 가리키며, 이는 수신한 패킷에 기록된 송신자가 정말 그 패킷을 발송한 송신자임에 틀림이 없는지를 보장하는 서비스이다.끝으로, 패킷의 기밀성 (confidentiality)이란 패킷이 전달되는 도중 제3자가 그 내용을 들여다 볼 수 없도록 암호화하는 서비스를 의미한다. IETF는 인터넷에 필요한 여러 프로토콜 기술에 대한 표준화를 추진하는 기구로서 8 개 기술 분야 (Area)로 나뉘어져 있고, 이 중 한 분야가 보안 분야 (Security Area)이며 보안 분야는 다시 15개 워킹 그룹으로세분되어 있다. IPSEC 워킹 그룹은 이 들 중 네트워크 계층에서 인터넷 보안 기술을 다루는 유일한 워킹 그룹으로, LAN과 라우터 등 전통적으로 보안 관리 상 취약한 요소로 구성된 인터넷 네트워크를 경유하는 IP 패킷의 보안 문제를 다루고 있다[23].

6. 2 IPSec 구현

IPsec은 호스트와 호스트 사이, 호스트와 보안 게이트웨이 사이, 보안 게이트웨이와 보안 게이트웨이 사이에 구현될 수 있다.

보안 게이트웨이는 IP계층에 IPsec이 구현되어 있는 시스템으로서 다음과 같은 특징이 있다. 보안 게이트웨이는 외부의 신뢰할수 없는 시스템과 자신의 서브넷 상의 신뢰 시스템 사이에서 통신을 중개하는 역할을 하는 시스템으로서, 이는 외부의 신뢰할수 없는 시스템과 통신을 할 때 신뢰하는 내부의 호스트에게 보안서비스를 제공한다. 보안 게이트웨이가 신뢰하는 서브넷 상에 위치한 하나 이상의 호스트를 대신하여 서비스를 제공하는 경우, 보안 게이트웨이는 신뢰하는 호스트를 대신하여 SA를 생성하고, 보안 게이트웨이와 외부 시스템 사이에 보안서비스를 제공한다. 이 경우 게이트웨이만 AH(Authentication Header), ESP(Encapsulating Security Payload) 프로토콜을 구현하면 되고, 신뢰하는 서브넷 상에서 게이트웨이를 이용하는 모든 시스템들은 게이트웨이와 외부시스템 사이에서 AH와 ESP서비스를 이용할 수 있다.

IPsec을 구현하는 방법에는 다음과 같은 것이 있다.

- IPsec을 기존의 IP환경에 통합하여 구축이 방법은 IP 소스코드를 수정해야 하며, 호스트나 보안 게이트웨이 모두에 적용될 수 있다.
- Bump-in-the-stack(BITS)구현 기존의 IP계층과 물리적 계층사이에 구현하는 방법으로서 소스코드의 수정이 필요 없으며, 대부분의 호스트에서 적용될 수 있다.
- Bump-in-the-wire(BITW)구현외부장치에 따로 구현하는 방식으로, 호스트에 구현되면 BITS와 유사하며, 라우터나 방화벽에 구현되면 보안 게이트웨이처럼 작동한다[24].

6. 3 IPSec 프로토콜 분석

IPSec 동작에는 세 가지 기본 구성요소[SecurityAssociation(SA), Authentication Header(AH), Encapsulation Security Payload(ESP)]가 필요하다.

AH는 접근 제어(Access Control), 비연결형 무결성(Connectionless Integrity), IP 데이터그램에 대한 데이터 발신 인증(Data Origin Authenti-cation) 등의 보안 서

비스를 제공하며, 선택적으로 재전송 공격 방지(Anti-Replay) 서비스를 제공할 수 있다. 재전송 공격 방지 서비스의 경우는 디폴트로 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 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 사용자측으로부터 발생된 패킷 전체를 암호화할 수 있다[25].

가. Security Association

데이터 송수신자간에 비밀데이터(인증되었거나, 암호화된 데이터)를 교환할 때 사전에 암호 알고리즘, 키 교환방법, 키교환 주기 등에 대한 합의가 이루어져야 한다. 데이터 교환 전에 통일되어야 할 이러한 요소들을 IPSec에서는 SA로 정의한다. 데이터 송수신자간의 안전한 통신을 위해서는 적어도 하나의 SA가 필요하다. 그러므로 패킷 인증과 암호를 위해서는 SA가 선행되어야 한다. 동일한 알고리즘이 사용되어도 서로 다른 두 개의 키가 요구될 경우에는 두 개의 SA가 필요하다. SA를 대인간 또는 그룹간, 네트워크간의 네트워크 보안 채널로 생각할 수도 있다. SA는 다중 VPN 구성에 유리하다. 다수의 상대방이 있을경우 개인별로 SA를 별도로 정의하므로서 서로 다른 VPN을 구성할 수 있음으로 다른 VPN 구성에 유리하다. 또한 SA는 일방향 전송도 가능하다. 하나의 SA가 정의될 경우 송신자는 수신자에게 데이터를 전송할 수 있으나 동일한 SA로 데이터의 수신은 불가능하다. 따라서 양방향 통신을 위해서는 수신자가 전송자에게 보내는 SA가 별도로 정의되어야 한다. IPSEC의 처리는 SA에 의하여 결정되며 각 객체들은 이association들을 공유하고 있다고 가정한다. 각 SA은 각 종단시스템에서의 속성 집합에 의하여 정의되고 SPI(Security Parameter Index)와 목적지 주소에 의하여 식별된다. 일반적

으로 SA에는 다음과 같은 매개변수를 포함하며 이밖에 다른 매개변수를 부가적으로 포함할 수 있다.

- IP AH와 함께 사용될 인증 알고리즘과 모드
- 인증 알고리즘에 사용될 키
- IP ESP와 함께 사용될 암호 알고리즘과 모드
- 암호 알고리즘에 사용될 키
- 암호 알고리즘을 위한 암호화 동기 또는 초기 벡터영역의 존재 유무의 크기
- ESP 변환에 사용되는 인증 알고리즘과 모드
- ESP 변환을 위한 인증 알고리즘에 사용될 키
- 키의 수명 및 키 변환이 일어나야만 하는 시간
- SA의 수명
- SA의 발신지 주소
- 보호되는 데이터의 민간도 레벨

나. IKE(Internet Key Exchange)

IPSec의 구성요소의 하나로 SA를 성립, 유지, 보수하는데 필요한 데이터들을 안전하게 전달하기 위해 사용된다. IPSec에서 키를 교환하고, 관리하는데 현재 사용되고 있는 방법은 Manual Key를 이용하는 것과 IKE를 이용하는 2가지가 있다. 소규모의 사이트에서는 Manual Key를 이용하는 것이 좋고, 보다 간편하게관리하기 위해서는 IKE를 이용한 Automated 방식을 쓰는 것이 좋다. IKE를 이용하는 대표적인 방법이 ISAKMP/Oakley로 다음과 같은 서비스를 제공한다.

어떤 프로토콜, 알고리즘과 키를 이용할 것인지와 상대방에 대한 인증, 양쪽이 동의한 후, 보안관계를 관리하며, 안전한 Key Exchange 처리를 담당한다. Key Exchange는 SA 성립(보안관계)과 밀접한 관계를 가지고 있어, 새로운 SA를 생성할 때마다 그전에 Key Exchange는 실행되어야만 한다.

다. Authentivation Header(AH)

AH는 IPSec에서 IP 데이터에 대한 인증서비스와 데이터 무결성서비스를 제공한다.

AH는

1)next header field

2)payload length

3)security parameter index(SPI)

4)sequence number

5)authentication data

다섯 가지 필드를 포함한다. 다섯 가지 필드 중에서 SPI는 송신자가 사용하는 보안 프로토콜에 대한 정보를 알려주며, authentication data는 SPI에서 정의된 암호 알고리즘으로 패킷의 payload를 암호화하여 얻어진다.

IPSec은 인증 기능의 향상을 위해 패킷 체크섬 계산 방법을 기존 MD5 방식 대신 HMAC(Hash-based Message Authentication Code)-MD5와 HMAC-SHA 방식 중 하나를 사용하고 있다.

AH 프로토콜은 무결성과 데이터 기원 인증 및 재생(replay)에 대항한 보호를 제공하기 위해 사용된다. 따라서 AH는 침입자의 공격에 대항한 다양한방어책을 제공한다. 이 프로토콜은 모든 패킷을 인증하기 때문에 세션을 도용하는 프로그램은 비효율적으로 간주된다. 또한 이 프로토콜의 기본적인 재생 카운터는 가짜 혹은 파괴성 데이터가 포함되어 있을 수도 있는 재생 공격을 중지시킬 수 있다.

AH는 또한 가능한 한 다수의 IP 헤더에 대한 인증을 제공하는데, 심지어 IP 헤더가 AH 봉함 외부에 있을 때도 그렇다. AH 인증은 IP 헤더 패킷이 전송중일 때 그에 대한 조작을 불가능하게 만든다. 따라서 AH의 이러한 특성은 NAT (Network Address Translation) 종단간 환경에서의 사용을 부적절하게 만든다. IP 헤더를 조작하는 것이 NAT 기능에서는 필수적이기 때문이다.

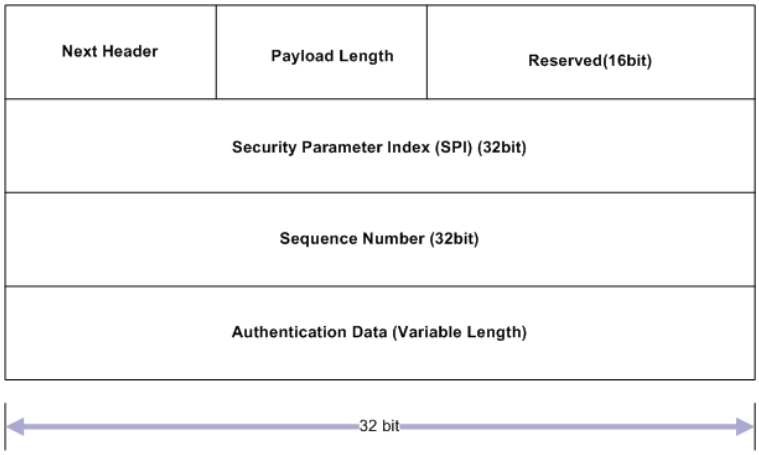


그림 6-1. AH format

- Next Header(8비트) : 인증헤더 뒤에있는 헤더의 형태 식별자
- Payload Length : 32 bit word에서 AH의 길이를 기록
- Reserved(16비트) : 미래를 위해 예약된 공간
- SPI(Security Parameter Index) : Destination IP Address와 Security Protocol(ESP)를 조합하 여 이 Datagram에 대한 Security Association을 식별하게 해주는 값
- Sequence Number : Unsigned 32bit Field로써 일정하게 증가하는 Counter 값
- Authentication Data(가변) : ICV(Integrity Check Value)로 구성된 가변길이 Data Field. 32비트 단어의 정수

"Next Header"는 AH 다음에 나타날 헤더 또는 페이로드의 형태를 지정하는 8비트 필드로 IANA(Internet Assigned Numbers Authority)에서 지정한 값을 사용한다. "Payload Length"는 4바이트 단위로 계산되며 실제 크기에서 2를 뺀 값이 저장된다. 일반적으로 4 값을 가지며, 디버깅을 위한 'null' 인증을 사용할 때 IPv4의 경우는 1, IPv6의 경우는 2가 된다. "Reserved" 필드는 항상 0 값을 갖는다. "SPI(Security Payload Index)" 필드는 32비트로 유일한 SA를 식별하는데 사용되는 인자 중 하나이다. SA를 구분하는데 사용하는 인자는 {SPI, AH, 목적지주소}이다. "Sequence Number" 필드는 unsigned 32비트 값으로 SA가 설정될 때 송수신

측에서 모두 0으로 셋팅된다. 그 후 전송시마다 송신측에서는 그 값을 1씩 증가시키고 수신측에서는 이 값을 검사하여 재전송 공격(Replay Attack)을 검사한다. 수신측에서 이 값을 검사함으로써 재전송 방지 서비스(Anti-Replay)가 성립된다. "Authentication Data" 필드는 4바이트의 정수배 크기로 ICV(Integrity Check Value) 값을 의미한다. 뒷부분에 패딩이 추가되면서 AH 크기가 IPv4에서는 32비트의 정수배, IPv6에서는 64비트의 정수배가 된다.

라. Encapsulation Security Payload(ESP)

ESP는 패킷의 암호화 서비스를 제공한다. AH처럼 패킷 처리에 필요한 SA정보를 수신자에게 알려주기 위해 SPI를 포함하고 있다. ESP는 다양한암호화 알고리즘을 지원하며 사용자는 상대방에 따라 서로 다른 암호알고리즘을 사용할 수 있다. ESP에서도 인증서비스를 제공할 수 있으나 이 경우 AH와 달리 IP 헤더에 대한 인증서비스는 제공하지 못한다. ESP 프로토콜은 데이터의 비밀성(privacy)을 제공하는데, 암호화되어 있지만 인증되지 않은 데이터 스트림에 대한공격을 막기 위해 AH의 모든 기능이 포함돼 있다.

IPSec 사양은 AH 기능을 제외한 ESP를 허용하고 있지만, 하고 있는 일에 대해 정확히 이해하지 못한다면 이것을 사용하지 말 것을 권장한다. ESP는 또한 널null 암호화를 사용할 수 있다.

널 암호화란 IP 헤더 인증을 제외한 AH와 거의 흡사한데, IP 헤더에서의 주소가 변하기 때문에 NAT 전송을 허용할 수 있다.

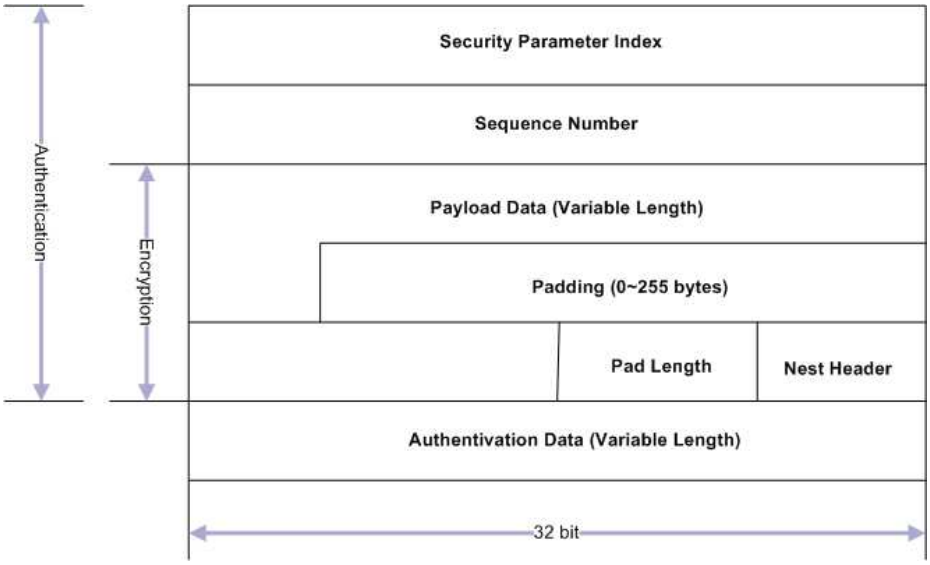


그림 6-2. ESP Format

- SPI(Security Parameter Index) : Destination IP Address와 Security Protocol(ESP)를 조합하여 이 Datagram에 대한 Security Association을 식별하게 해주는 값
- Sequence Number : Unsigned 32bit Field로써 일정하게 증가하는 Counter 값
- Payload Data : Next Header Field에 의해 묘사된 Data를 포함하는 가변길이 Field
- Padding : 암호화된 bits가 사용된 알고리즘의 Block Size의 배수가 되도록 만들기 위해서 사용되는 가변길이 Field
- Pad Length : Padding에서 사용된 Padding Data의 길이
- Next Header(8 bit) : Payload Data Field에 포함된 Data의 타입을 식별해주는 Field
- Authentication Data : ICV(Integrity Check Value)로 구성된 가변길이 Data Field

"Security Payload Index" 필드는 32비트로 유일한 SA를 식별하는데 사용되는 인자 중하나이다. SA를 구분하는데 사용하는 인자는 {SPI, AH, 목적지주소}이다. "Sequence Number" 필드는 unsigned 32비트 값으로 SA가 설정될 때 송수신측에

서 모두 0으로 셋팅된다. 그 후 전송시마다 송신측에서는 그 값을 1씩 증가시키고 수신측에서는 이 값을 검사하여 재전송 공격(Replay Attack)을 검사한다. 수신측에서 이 값을 검사함으로써 재전송 방지 서비스(Anti-Replay)가 성립된다. "Payload Data"는 Next Header 필드에서 지정한 상위 계층의 데이터가 기록되는 필드로 길이는 가변적이다. "Padding"는 바이트 정렬을 맞추기 위해 사용되는 필드로 0~255 사이의 값을 가질 수 있으며, 패딩된 크기는 "Pad Length" 필드에 기록된다. "Next Header"는 페이로드 데이터의 형태를 지정하는 8비트 필드로 IANA에서 지정한 값을 사용한다. "Authentication Data" 필드는 선택 사항이며 사용 인증 함수에 의해 필드 크기가 결정된다.

6. 4 보안 프로토콜의 동작 모드

AH 프로토콜과 ESP 프로토콜 모두, 이들 프로토콜 헤더가 어디에 위치하는지에 따라, 두 가지 모드로 동작된다.

(그림 참조.) 하나는 보통 IP 패킷 경우로, 보안 헤더가 IP 패킷의 패킷 헤더와 페이로드 사이에 위치하는 것으로 트랜스포트 모드라 하며, 또 하나는 터널 IP 패킷의 경우로, 터널을 위해 앞에 새로 붙은 패킷 헤더와 원래 패킷 헤더 사이에 보안 헤더가 위치하는 것으로 터널 모드라 한다[26].

트랜스포트 모드는 종단 대 종단에 위치한 두 호스트간에 이용되며 IP 패킷의 페이로드, 즉, TCP와 UDP와 같은 상위계층 프로토콜 데이터만을 보호하게 된다. 이 경우 패킷 헤더는 보호 영역 밖이므로, 송신자와 수신자 주소가 노출되게 되어 트래픽 흐름이 노출될 수 있다. 하지만, 터널 모드의 경우는 원래 패킷의 전체가보호 영역안에 놓이므로, 트래픽 흐름의 기밀성도 유지할 수 있게 된다.

보안 통신의 한 쪽이 호스트가 아닌 라우터 (통상, 어떤 인트라넷의 Security Gateway에 해당됨)인 경우는 반드시 터널 모드를 적용해야 한다. 터널 모드는 호스트- 호스트 간에도 적용할 수 있다.

즉, IPSEC이 적용되는 전형적인 네트워크 구성을 H1 - Intranet - SG1 - Internet - SG2 - Intranet - H2로 가정할 때, 트랜스포트 모드는 H1 … H2간에만 적용되는데 반해, 터널 모드는 H1 … SG2 또는 SG1 … H2 또는 SG1 … SG2 및 H1 …

H2 간에도 적용 될 수 있다.

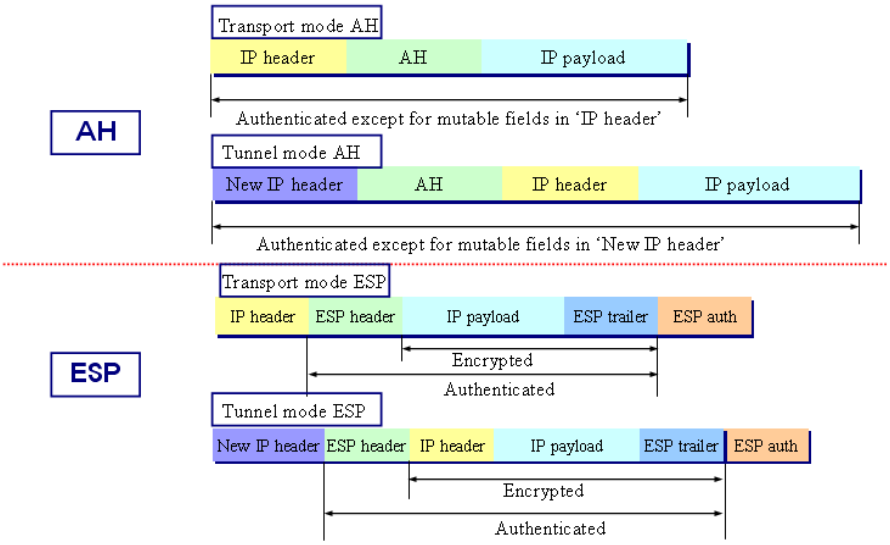


그림 6-3. IPSec 동작모드

IPSec 프로토콜은 전송 모드나 터널 모드에서 모두 사용될 수 있다. 전송 모드에서 IPSec은 네트워크(IP)와 전송(TCP 혹은 UDP) 봉함간의 평범한 IP 패킷으로 진입한다. 전송 모드는 종단 시스템용으로 개발되었는데, 그 사용은 완전히 집단에 속한 모든 시스템에서의 전개용으로 서술되어 있기 때문에 대부분의 경우 애플리케이션의 재 프로그래밍이 필요할 것이다.

IPSec의 터널 모드는 게이트웨이에 의해 사용되도록 개발된 것이다. 터널 모드에서 일상적인 IP 패킷은 IPSec 봉함내에 놓여지며 그 IPSec은 다시 또다른 IP 봉함으로 들어간다.

이 모드에서 사용자는 네트웍의 페러미터에서 IPSec 터널 장비를 신속하게 전개할 수 있다. 구성이 비슷한 네트웍간에 트래픽의 안전을 보장하는 것은 간단하며, 특수한 최종사용자 소프트웨어나 새 애플리케이션을 전개할 필요가 없다.

터널 모드를 지원하는 소프트웨어는 게이트웨이나 종단 시스템상에서 동작할 수 있다.

종단 시스템상에서 터널 소프트웨어가 가장 흔하게 사용될 때는 원격 및 이동 사용자를 지원할 때이다. 게이트웨이가 터널을 통해 대부분의 종단 사용자 데이터를 전송함에도 불구하고 동료 게이트웨이간의 통신을 안전하게 보호하려면 전송 모드를 사용할 수도 있다. 이러한 방식은 라우터, ATM 스위치, 방화벽 및 기타 핵심적인 하부구조 컴포넌트를 원격에서 안전하게 관리하는 훌륭한 방편이 될 수 있다.

6.4.1 AH 프로토콜 처리

AH 프로토콜은 트랜스포드(Transport Mode)와 터널 모드(Tunnel Mode) 두 가지의 운용 모드를 가지고 있다. 트랜스포드 모드는 일반적으로 보안 호스트 구현시 사용되며 상위 계층 프로토콜에 대한 보호 서비스를 제공한다. 터널 모드의 경우는 보안 호스트 및 게이트웨이 구현시 모두 적용되며 outer IP 헤더를 새로이 생성하여 inner IP 헤더를 포함한 inner IP 패킷 전체에 대한 보호 서비스를 제공한다. 패킷을 송신하는 단계인 Outbound 패킷 처리 과정 및 수신 단계인 Inbound 패킷 처리 과정은 다음 그림 6-4와 같은 순서로 이루어 진다.

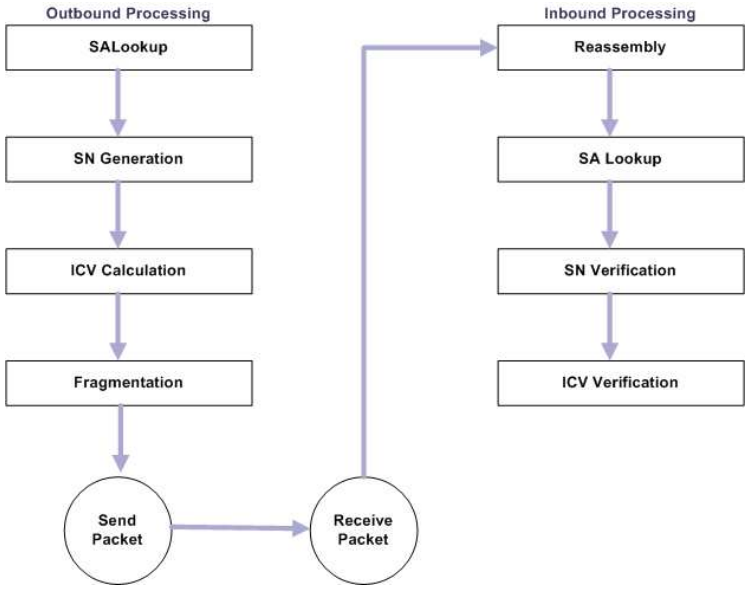


그림 6-4. AH Inbound/Outbound 패킷 처리과정

패킷을 송신하는 단계인 Outbound 패킷 처리 과정에서는 먼저 SA가 설정되어 있는지 SAD를 찾는다. 만약 설정된 SA가 없으면 정책에 따라 새로운 SA를 설정하고, 이미 설정된 SA가 있으면 재전송 공격 방지 서비스를 위하여 SN(Sequence Number)을 생성한다. 이때SN 값은 초기값인 '0'으로 설정한다. 다음으로 전송 중 변하지 않거나 수신측에서 예측 가능한 필드 값을 이용하여 ICV를 계산하고, 패딩을 추가한 후 전송할 패킷 단위로 분할한 후 패킷을 전송한다.

패킷을 수신하는 단계인 Inbound 패킷 처리 과정은 송신 단계의 역순과 유사한 처리를 한다. 먼저 수신된 패킷을 조합한 후 AH 헤더의 {SPI, AH, 목적지주소}를 이용하여 관련 SA를 찾는다. 만약 설정된 SA가 없는 경우는 해당 패킷을 폐기하게 된다. 이미 설정된 SA가 있는 경우는 Sliding Receive Window와 Bit Masking 방법을 이용하여 SN과 ICV에 대한 검증을 수행한다. ICV 검증 단계에서 수신 패킷 내의 ICV 값이 AH 내의 값과 일치하면 통과시키고, 그렇지 않으면 해당 패킷을 폐기한다.

6.4.2 ESP 프로토콜 처리

ESP 프로토콜은 트랜스포드(Transport Mode)와 터널 모드(Tunnel Mode) 두 가지의 운용 모드를 가지고 있다. 트랜스포드 모드는 일반적으로 보안 호스트 구현시 사용되며 상위 계층 프로토콜에 대한 보호 서비스를 제공한다. 터널 모드의 경우는 보안 호스트 및 게이트웨이 구현시 모두 적용되며 outer IP 헤더를 새로이 생성하여 inner IP 헤더를 포함한 inner IP 패킷 전체에 대한 보호 서비스를 제공한다.

패킷을 송신하는 단계인 Outbound 패킷 처리 과정 및 수신 단계인 Inbound 패킷 처리 과정은 다음과 같은 순서로 이루어 진다.

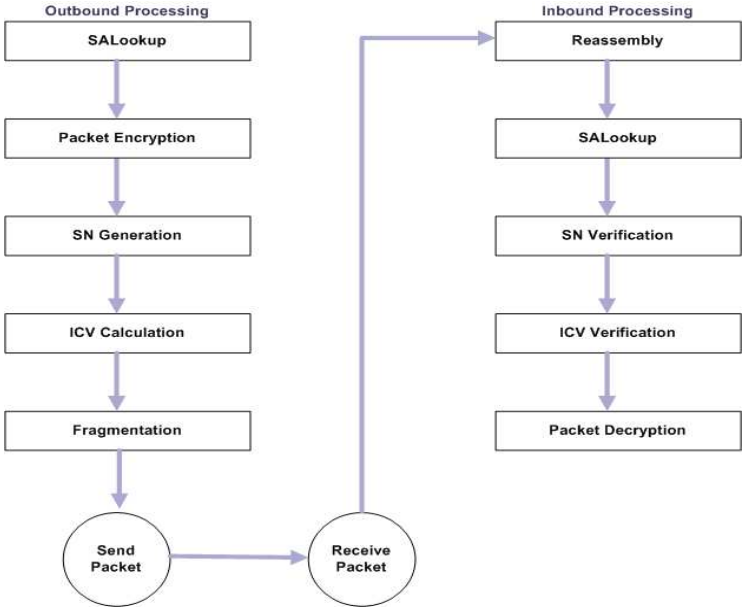


그림 6-5. ESP Inbound/Outbound 패킷 처리과정

패킷을 송신하는 단계인 Outbound 패킷 처리 과정에서는 먼저 SA가 설정되어 있는지 SAD를 찾는다. 만약 설정된 SA가 없으면 정책에 따라 새로운 SA를 설정하고, 이미 설정된 SA가 있으면 전송하고자 하는 패킷을 암호화한 후, 재전송 공격 방지 서비스를 위하여 SN(Sequence Number)을 생성한다. 이때 SN 값은 초기값인 '0'으로 설정한다. 다음으로 전송 중 변하지 않거나 수신측에서 예측 가능한 필드 값을 이용하여 ICV를 계산하고, 패딩을 추가한 후 전송할 패킷 단위로 분할한 후 패킷을 전송한다.

패킷을 수신하는 단계인 Inbound 패킷 처리 과정은 송신 단계의 역순과 유사한 처리를 한다. 먼저 수신된 패킷을 조합한 후 AH 헤더의 {SPI, AH, 목적지주소}를 이용하여 관련 SA를 찾는다. 만약 설정된 SA가 없는 경우는 해당 패킷을 폐기하게 된다. 이미 설정된 SA가 있는 경우는 Sliding Receive Window와 Bit Masking 방법을 이용하여 SN과 ICV에 대한 검증을 수행한 후 패킷의 복호화를 수행한다. ICV 검증 단계에서 수신 패킷 내의 ICV 값이 AH내의 값과 일치하면 통과시키고, 그렇지 않으면 해당 패킷을 폐기한다.

제 7장. 3DES 알고리즘 구현 및 Processing Power 테스트

7. 1 DES

DES는 거의 25년 동안 사용되어 왔다. DES는 광범위 하게 연구되어졌고, 이것의 구조는 잘 이해되었다. DES는 여러 암호학적 분석에 잘 견딜 수있다고 증명되었다. DES에 대한 문제는 설계 측면에 있기보다는 키의 길이에 있다고 알려졌다.

DES는 64비트의 평문을 암호화 하기 위하여 56비트 길이의 암호키 K를 사용한다. 64비트 평문 x, 평문 x를 DES로 암호화한 64비트 암호문 y가 주어졌을 경우, 하나의 56비트 DES 키 K는 2^{55}의 연산을 수행하면 발견될 수 있다[27].

DES 알고리즘은 다음과 같은 3단계로 수행된다.

① 64비트 블록 평문 x는 초기 치환(Initial Permutation)함수 IP로 입력되며, Ip 함수의 결과는 64비트 출력 x_0 이 된다. 이 결과 x_0=IP(x)=L_0R_0로 표현된다. x_0의 처음 32비트를 L_0로 표현하고, 나머지 32비트를 R_0로 표현한다.

② 출력 x_0는 키 스케줄링(Scheduling) 함수 KS와 암호함수 f와 연관되는 16라운드로 반복되는 키-종속 연산에 입력된다. 만약, 각 라운드의 출력을 x_i=L_iR_i(1≤i≤16)로 표현하면, 각 라운드의 출력은

L_i=R_i-1

R_i=$L_i \oplus f(R_{i-1}, K_i)$

이 된다. 여기서 ⊕은 두 비트 스트링의 비트 단위의 배타적 논리 OR을 나타낸다. 48비트 블록 K_i은 키 스케줄링 함수 KS를 사용하여 원래의 56비트 암호키로부터 도출된다.

③ 역 치환함수 IP^{-1}은 64비트 암호문 블록 c을 생성하기 위하여 $R_{16}L_{16}$에 적용된다. 즉, c=$IP^{-1}(R_{16}L_{16})$이다. R_{16}과 L_{16}의 순서가 바뀌였다. 이것은 IP의 역이다. 이는 만약 역 치환함수가 IP로 입력된다면, 결과는 IP로 입력된 비트스트림과 일

치함을 의미한다. 즉, $IP^{-1}(IP(x))=1$이다.(그림 7-1)

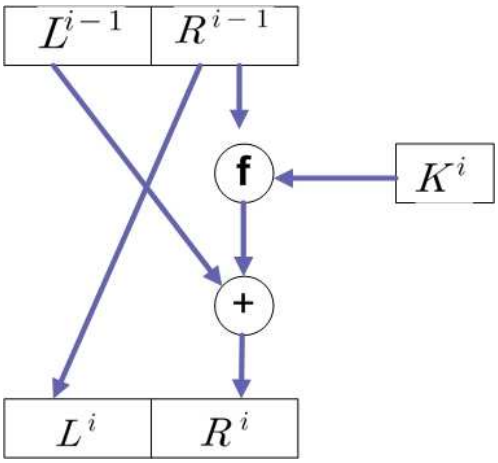


그림 7-1. One round of DES encryption

④ 아래그림 7-2. 은 f 함수를 보여주고 있으며, 과정은 다음과 같다.

(a) A는 함수 E에 의하여 32bit에서 48bit길이의 비트스트링으로 확장된다.

(b) E(A)와 J 사이에 XOR을 취하면, 6-bit의 비트스트링을 같은 갖는 8개의 블록으로 나뉘어지게 되어 $B = B_1B_2B_3B_4B_5B_6B_7B_8$와 같이 표현된다.

(c) 각 B 블록은 S box를 통과하여 각 4-bit의 비트스트링을 갖는 8개의 블록으로 최종적으로 표현된다.

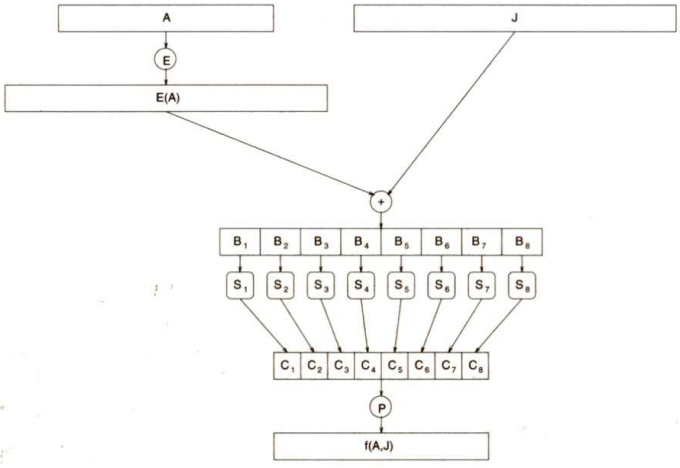


그림 7-2. DES f Function

7. 2 Triple DES(3-DES)

DES(Data Encryption Standard)은 56비트라는 짧은 키 길이로 인해 더 이상 안전하지 않다고 보는 것이 일반적인 견해이며, IPSec나 PKIX등 새로운 응용들에서는 DES를 3회 반복하는 3DES를 사용하도록 권고하고 있다.

3DES는 속도가 DES보다 3배 정도 느리다는 단점에도 불구하고, 기존의 DES를 이용하여 쉽게 구현되며 DES의 안전성 문제를 해결하는 장점으로 인하여 여러 표준에서 사용되고 있다[28].

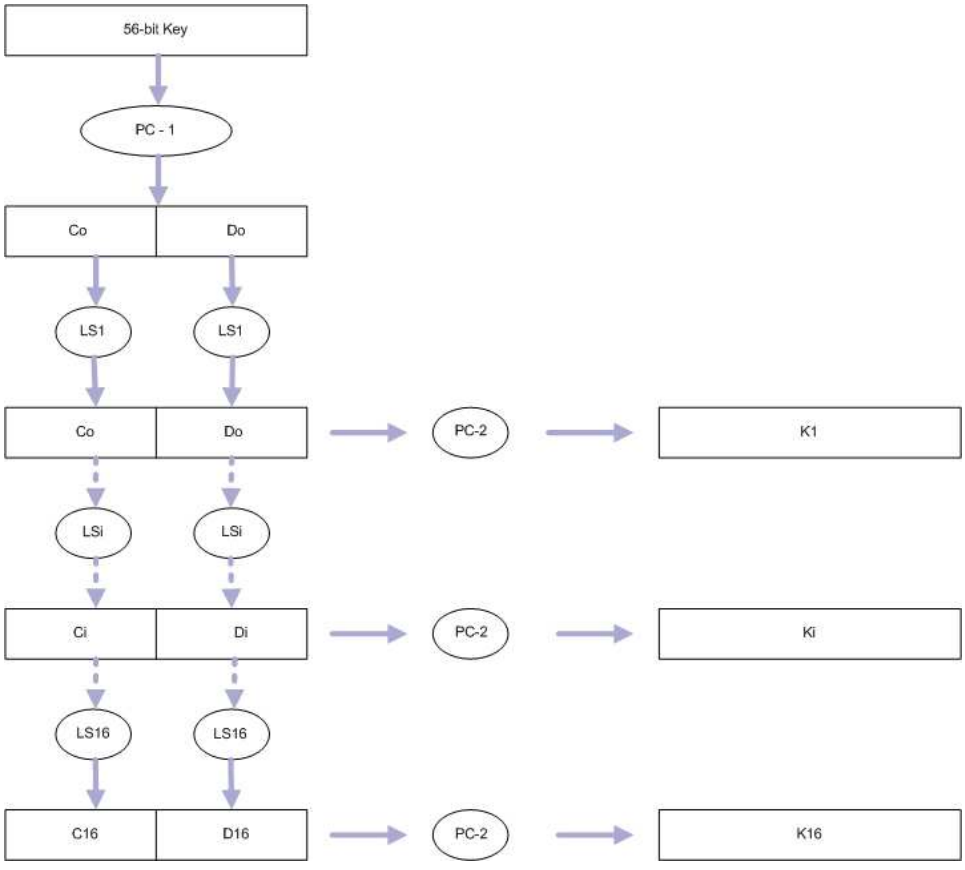


그림 7-3. DES Key Scheduling 계산

3DES는 위의 그림 7-3. 과 같이 설명될 수 있다. $e_k(x)$와 $d_k(x)$를 암호키 k를 갖는 DES 알고리즘을 이용하여 64비트의 비트 스트림 x를 각각 암호화 및 복호한 결과로 각각 표현한다. 64 비트의 암호문 c는 다음과 같은 수식으로 구해진다.

$$c=e_{K_3}(d_{K_2}(e_{K_1}(x)))$$

여기서, K_1, K_2, K_3는 56비트의 DES 키 암호이다. 곧, 168 비트 길이의 키로 암호화하는 것과 동일한 것이다.

암호문 c로부터 평문 x를 유도하는 3DES의 복호화 과정은 암호화 과정의 역이다. 수식은 다음과 같다.

$$x=d_{K_1}(e_{K_2}(d_{K_3}(x)))$$

7. 3 3DES Algorithm Program과 Processing Time

① 3DES Algorithm Programming

```
if(!CryptEncrypt(
    hKey,
    0,
    FALSE,
    0,
    pbBuffer,
    &dwCount,
    dwBufferLen))
{
   AfxMessageBox("Error during CryptEncrypt. Wn");
}
```

Encryption Function

```
if(!CryptDecrypt(hKey, 0, feof(hSource), 0, pbBuffer, &dwCount))
{
   HandleError("Error during CryptDecrypt!");
}
```

Decryption Function

그림 7-4. Encryption & Decryption Functions

위 그림 7-4와 같이 Encryption과 Decryption 함수 Library를 이용하여 3DES 알고리즘 구현이 가능하였으며, 이를 적용 시켰을 때, Encryption Time값을 구할 수 있었다.

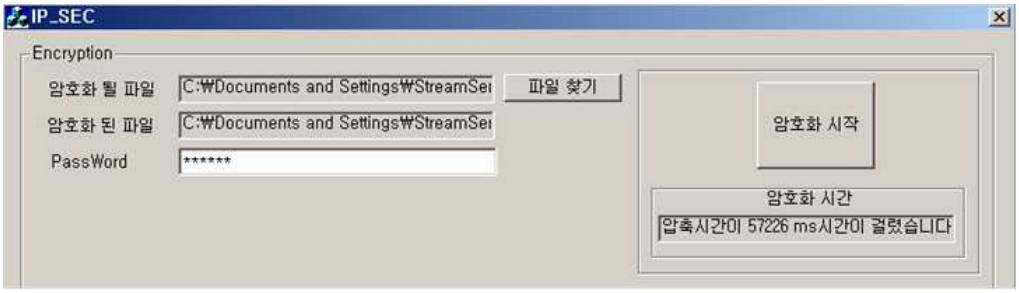


그림 7-5. Encryption & Decryption UI

UI는 위 그림 7-5 처럼 구현하였으며, 암호화 될 파일을 선택하여 함호화를 시키면, 암호화된 파일이 따로 생성되는 형태를 가진다. 또한 Encryption 및 Decryption Time을 구하기 위해 timeGetTime()를 사용하였다.

② 3DES의 File Size와 Processing Time

아래 표는 File Type에 따른 Encryption Size의 변화를 나타내고 있다. Avi, Doc, Mp3, Zip 총 4가지 종류의 임의의 File을 선택하여 Encryption을 실행 하였을 때, 결과는 모두 동일하게 24Byte 값만큼의 데이터 상승만 나타내게 되었다.

24Byte는 ESP 과정에서 암호화를 진행하면서 Hash Function을 이용하여 발생한 Header 값이다. Hash Function은 파일크기에 관계없이 동일한 Header 값을 나타내는 축약 알고리즘이다. (표 7-1)

(단위 : Byte)

File Type / Process	Avi File	Doc File	Mp3 File	Zip File
3DES 실행전 (Normal)	734,238,720	21,951,488	1,160,632	13,162,496
3DES 실행후 (Encryption)	734,238,744	21,951,512	1,160,656	13,162,520
Decryption	734,238,720	21,951,488	1,160,632	13,162,496

표 7-1. File Type에 따른 Encryption Size 변화

3DES의 Processing Time은 암호화 과정에 있어서 가장 많은 시간이 걸리게된다.

앞서 확인한 3DES의 특징을 보면, 3회의 DES를 위해서 64비트 블록을 3회 반복해야하며, 192비트 암호화 결과를 얻기 위해서는 Packet 전체의 64비트 블록을 갖고 있는 DES 암호화를 3회 진행한다. AH의 MD5나 SHA-1은 IP 인증을 위해서 사용되는 데, 인증헤더의 추가는 Packet 자체의 암호화를 하는 시간보다 훨씬 더 적게 걸린다. 결과적으로 AH와 ESP를 Packet에 동시 적용한다고 했을때, 가장 영향을 많이 주는 것은 ESP 과정이며, 실험에서 사용한 3DES 알고리즘에 의한 결과라고 말할 수 있다. 이에 따라 3DES Decryption 시간은 AH의 IP 인증에 해당하는 시간에 비해 매우크기 때문에 본 논문에서는 AH의 인증헤더 추가에 걸리는 Delay Time을 고려하지 않았고, 3DES의 Encryption Time에 초점을 맞추었다.

Processing Time은 Laptop, Desktop, PDA, 등 단말의 성능에 따라 각기 다른 값이 측정된다. 물론 Desktop과 같은 Workstation에서 좋은 결과를 기대할 수 있겠지만, 응급상황에서는 사용자 입장에서 최대한 간편한 응급진료가 가능하도록 해야하기 때문에 어느 정도 성능 이상의 단말을 선택하는 가에 대한 문제의 해답을 찾는 것은 중요하다. 이 해답을 찾기 위해서 21,951,488 Byte의 Doc File을 Intel Core to Duo 3.40Ghz의 성능을 가진 컴퓨터를 통해 Cpu Processing Speed 조절을 해 가며 Encryption Time 도출해 내었다. (표 7-2)

CPU Utilization(%)	Encryption_Time	CPU Utilization(%)	Encryption_Time
5	41050 ms	55	799 ms
10	37080 ms	60	159 ms
15	33040 ms	65	79 ms
20	28770 ms	70	53 ms
25	24630 ms	75	40 ms
30	20400 ms	80	32 ms
35	18300 ms	85	26 ms
40	12150 ms	90	22 ms
45	8110 ms	95	20 ms
50	4035 ms	100	18 ms

표 7-2. 3DES 알고리즘을 사용하였을 때의 Encryption Time

아래 그림 7-6 은 표 7-2를 그래프 형태로 나타낸 것이다. CPU 사용률이 55% 에 이르기 이전까지는 4000ms 만큼 계속적인 감소를 보이다가 그 이 후에는 거의 변화량이 없음을 알 수 있었다. 변화량이 작았다는 것은 CPU의 55% 이상 사용하였을 때는 거의 비슷한 처리시간이 걸리는 것을 의미한다. 곧, 55% 이상의 성능을 갖는 단말을 이용해야 Processing Time을 최소화 할 수 있다는 사실을 알 수 있다.

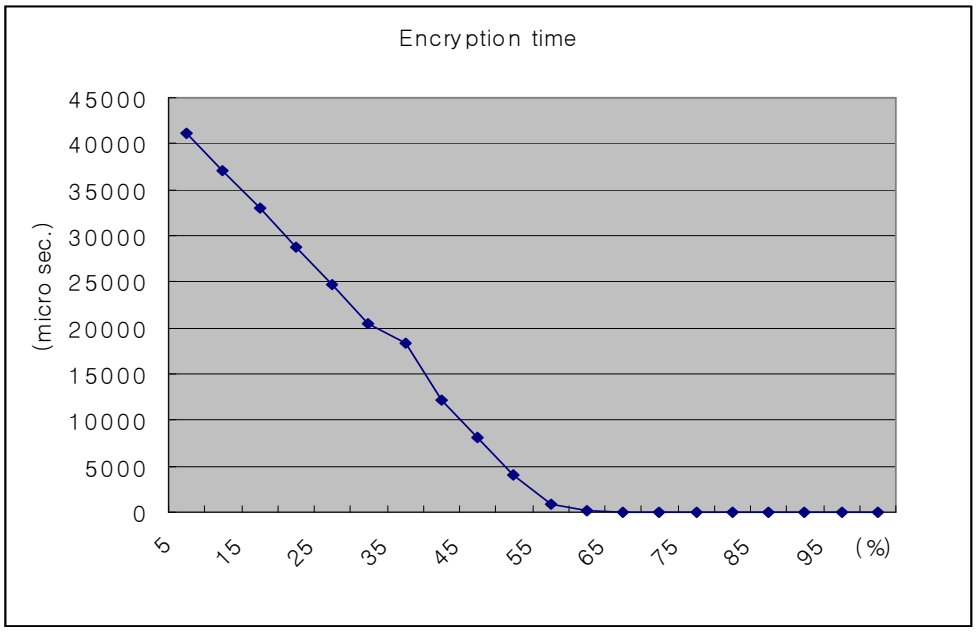


그림 7-6. DES 알고리즘을 사용하였을 때의 Encryption Time

제 8장. 가상 원격진료 시나리오의 구현 및 테스트

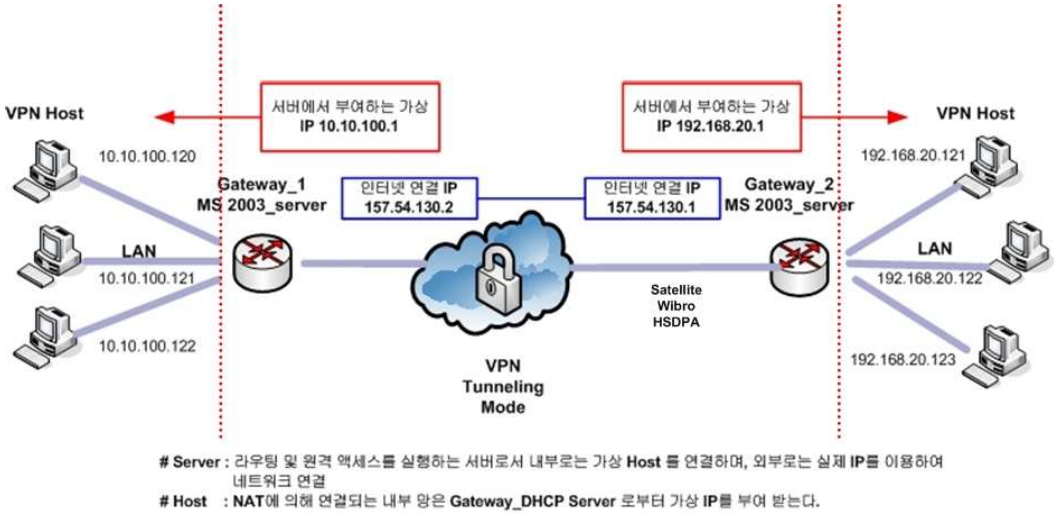


그림 8·1. 가상네트워크 환경 셋팅

8. 1 AH, ESP 포팅에 따른 테스트 결과

앞장에서 3 DES에 따른 데이터의 크기 증가와 Processing Time에 대하여 알아보았다. 이번 장에서는 AH, ESP를 가상 시나리오 환경에서 적용하였을 때, QoS의 변화가 어떻게 일어나는지 알아보며, 데이터의 크기 변화율을 Packet 단위별로 확인해 보았다.

그림 8-1 은 Intel CPU 3.40 Ghz Core to Duo 과 2.0G Memory 사양을 갖춘 Desktop 에 VM_ware 라는 소프트웨어를 이용하여 가상OS 환경에서 구성한 것이다. Gateway를 송•수신 측에 각각 하나씩 설치하였으며, 이 둘을 VPN으로 연결하였다. Gateway 사이는 VPN Tunneling Protocol이 이용되었는데, 실제IPSec 처리를 Security Gateway인 Gateway 1과 Gateway 2 끼리 처리하기 때문에 호스트에 걸리는 부하나 설정 방법등과 같은 문제는 생각 하지 않아도 된다. 따라서 Gateway에서만 IPSec의 알고리즘인 AH(MD5, SHA-1)와 ESP(3DES)를 적용하여 네트워크 상에서 어떠한 변화가 있는지 측정하였다.

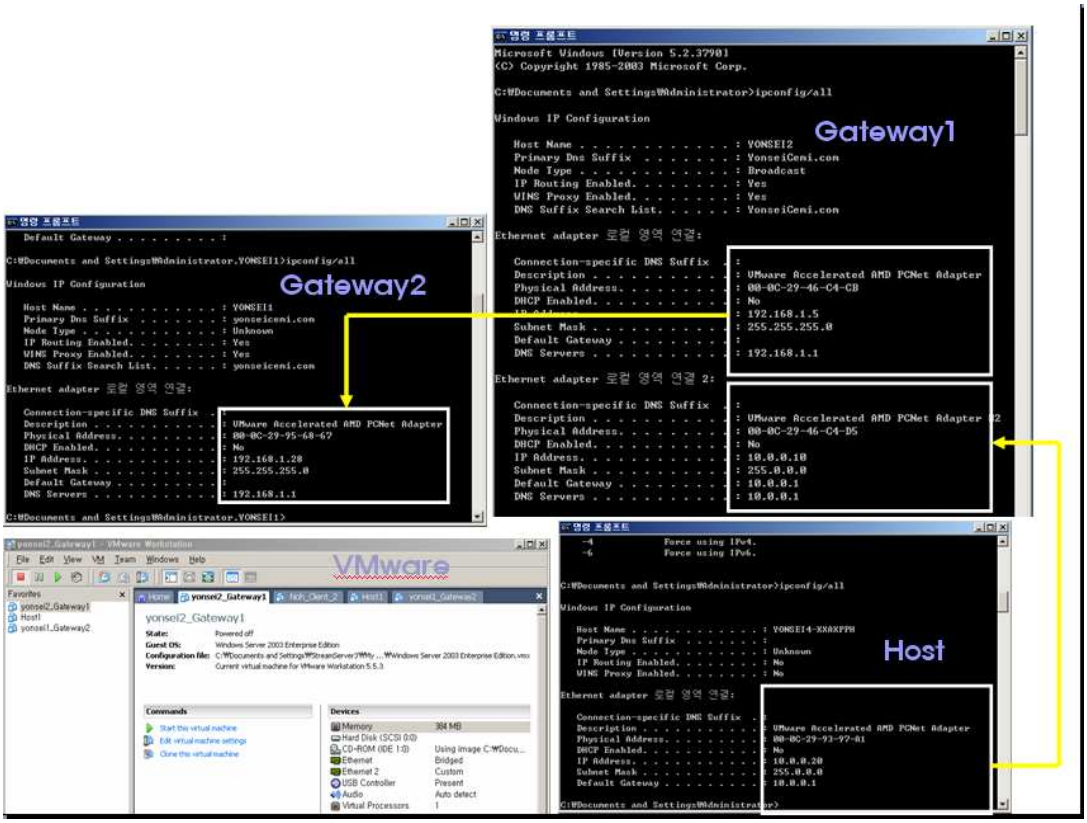


그림 8-2 가상 VPN 설치 이후 IP 흐름

그림 8-2는 그림 8·1의 가상 VPN Protocol을 사용하였을 때, Gateway와 Host에 어떻게 IP가 부여되었는가를 보여주는 화면이다. Gateway 1 에서는 NAT Server를 이용하여 Host에게 주소를 할당해 주었으며, Gateway 2 와 동일한 DNS Server를 가지며, 같은 Subnet Mask를 가지고 있다. 이로서 Gateway1과 Gateway2는 가상으로 사설망이 연결된 것이고, Host는 Gateway 1을 통해 주소를 부여받았기 때문에 Gateway1 에서만, Gateway2로 통신이 가능하게 되어있다.

AH		ESP			
MD5	SHA-1	MD5	SHA-1	3DES	Case #
0					1
	0				2
		0			3
			0		4
0				0	5
	0			0	6
		0		0	7
			0	0	8
0		0		0	9
0			0	0	10
	0	0		0	11
	0		0	0	12
					13(Default)

표 8-1. IPSec 설정항목

표 8-1 은 IPSec 설정항목으로서 AH와 ESP 알고리즘에 변화를 주어 총 13 Case 의 실험을 진행하였다. AH에서 IP 인증을 위해 MD5, SHA-1만을 적용 하였을 때와 ESP에서 ESP 자체인증을 위한 MD5, SHA-1이 사용되었을 때를 먼저 측정하였으며, AH와 ESP를 둘 다 적용 시켰을 때를 5~12 Case로 나누어 실험을 진행하였다. 특별한 부분은 ESP의 3DES를 적용 시킬 때는 반드시 AH를 이용하여 IP 인증을 하거나 ESP의 자체 인증 프로토콜을 사용하여야 한다는 것이다. 이는 3DES 암호화 알고리즘이 사용되기 위해서는 IP 또는 ESP 자체인증이 필수적으로 사용되어야 한다는 것을 의미한다. 또한 9~12 Case에서는 AH, ESP 모두 인증을 사용하며, 3DES 알고리즘까지 적용시켰을 때의 실험을 셋팅한 것이다.

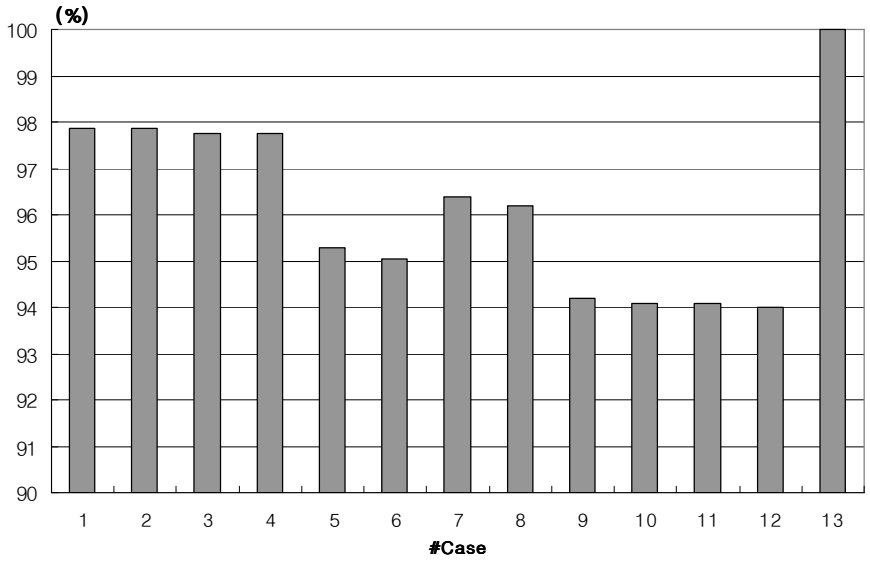


그림 8-3. Case에 따른 Utilization

그림 8-3을 보면, Case 별로 Throughput의 증감을 알 수 있다. 1~4에서는 알고리즘을 AH의 MD5와 SHA-1과 ESP의 MD5와 SHA-1 알고리즘 중에서 각각 1가지 알고리즘을 적용시켰을때의 Utilization이다. 1~4까지는 Case 13의 Nomal 인 경우와 비교해서 약 2%의 하락을 가져왔음을 알 수 있는데, 거의 동일한 값을 나타내었다. 하지만, SHA-1에서 조금 더 큰 Utilization의 하락을 보여주었다. 128-bit의 해쉬를 생성하는 MD5(Message Digest)와 160-bit의 해쉬를 생성하는 SHA-1(Secured Hash Algorithm) 메시지 압축 알고리즘의 메시지 인증 코드에 의하여 인증과 암호화가 진행되는데, 32-bit 만큼 해쉬 값이 더 큰 SHA-1의 영향에 의해 전체 Utilization이 줄어들었음을 확인 할 수 있었다. Case 5, 6은 AH에서의 인증을 위해 1가지 알고리즘을 선택하였고, ESP의 3DES 암호화 알고리즘 1가지를 적용시켰을 때의 해당 Utilization을 나타낸다. 여기서 AH와 ESP 값은 각각 1가지씩의 알고리즘을 선택했으므로, Packet 별로 AH의 Hash Function에 의한 Header 값은 24Byte이고, ESP의 3DES Hash Function에 의해 발생된 Header 값 또한 24 Byte이기 때문에 총 48Byte의 Packet 값을 IPSec에 이용되었다. 따라서 Utilization

값은 약 4.8~4.9% 까지 줄어들었다.

Case 7과 8에서는 ESP 내부의 인증과 3DES 알고리즘을 적용시켰을 때의 Utilization 값이다. 이때 Packet당 차지하는 암호화 바이트 수는 36Byte 이며, 인증에 12Byte가 사용되고, 24Byte가 Encryption에 사용된다는 사실을 알 수 있다.

Case 9~12까지에서는 ESP의 인증과 Encryption을 모두 사용하였으며, AH에서도 1가지 알고리즘을 선택하여 Packet에 붙여 통신을 했을 때의 데이터이다. 3가지 알고리즘을 이용하였기 때문에 Packet 당 이용할 수 있는 데이터의 양은 앞서 실험한 값보다 더욱 많이 줄어들게 되었다. 곧, AH에서 24Byte가 사용되고, ESP에서 36Byte가 사용되기 때문에 총 60Byte에 해당하는 값이 데이터에 붙여졌다. 9~12까지의 데이터 값은 거의 6% 가량 Utilization이 감소되었음을 알 수 있으며, 근소한 차이이지만, MD5보다 더욱 인증이 강화된 SHA-1 알고리즘에서 Utilization이 0.1~0.2% 가량 줄어들었음을 확인할 수 있었다.

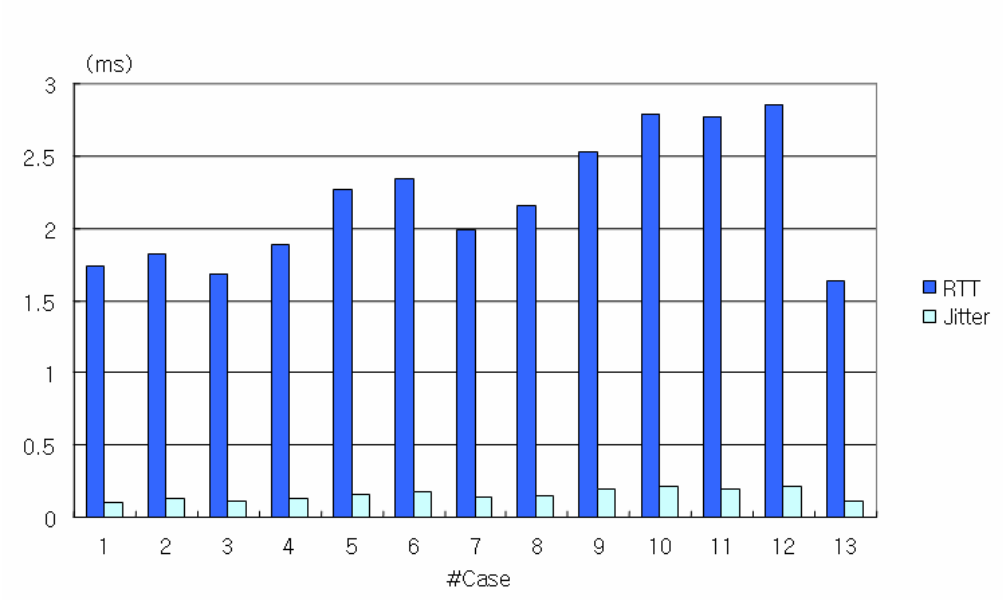


그림 8-4. Case에 따른 RTT&Jitter

그림 8-4는 RTT와 Jitter 값을 나타낸 것이다. 가상환경에서 IPSec 적용 시 Gateway 1에서 Gateway 2까지 데이터의 Latency는 그림과 같다. 총 1000Byte의

더미 Packet 데이터를 전송하였을 때, 전체 패킷의 양이 Case 별로 다르게 측정된다는 사실을 확인하였다. 패킷의 양이 증가하면, 그만큼 Latency가 증가하게 되므로 Case 1~4, 5~6, 7~8, 9~12까지 값이 다르게 측정되는 사실을 확인할 수 있다. 앞서 측정한 Utilization과 반비례 하여 Latency 값이 측정된다. 데이터를 확인 해 보면, Case 9~12에서 3가지의 알고리즘을 적용시켰을 때, Default Case보다 약 0.38ms(over 18%) 증가한 Latency 값을 나타내었다. Jitter역시 마찬가지로 Latency 증가율과 유사하게 Case 9~12에서 Default Case 보다 약 0.045ms(over 28%)의 증가를 보였다.

Normal	Case (1,2)	Case (3,4)	Case (5,6)	Case (7,8)	Case (9,10,11,12)
DLC Header	DLC Header	DLC Header	DLC Header	DLC Header	DLC Header
IP Header	IP Header	IP Header	IP Header	IP Header	IP Header
ICMP Header	AH Header	ESP Header	AH Header	ESP Header	AH Header
	ICMP Header		ESP Header		ESP Header

표 8-2 IPSec을 이용하였을 때, Packet의 구조

표 8-2에서는 각 Case 별로 Packet의 블록의 구조가 어떻게 되었는가를 보여주고 있다. 이 실험을 하기 위해서 Ping Test를 함께 진행하였는데, 아래의 값들은 이 Ping Test에 의해 측정된 Packet의 블록을 나타낸다. Ping Test에 사용되는 ICMP는 TCP와 UDP를 사용하지 않는 별도의 프로토콜로서 IP 계층인 Level 3 까지의 테스트가 가능하다. 본 논문에서 실험한 부분은 IPSec이기 때문에 IP 계층의 진단을 위해 적합한 프로토콜이라 할 수 있다.

DLC Header는 Data Link Control에 해당하는 Header로서 Destination 과 Source 단말 이름을 기록 하며, 이더넷 타입을 저장하는 하드웨어 계층 프로토콜이다. 이더넷 Header라고도 부르며, 14Byte의 블록 사이즈를 가진다. IP Header값은 IP 버전, IP Header CheckSum과 Source와 Destination의 IP 주소등을 저장하며 총 20Byte의 블록 사이즈를 가진다. ICMP Header는 Internet Control Message Protocol 로서 IP와 조합하여 통신 중에 발생하는 오류의 처리와 전송 경로의 변경 등을 위한 제어 메시지를 취급한다. 총 8 Byte의 블록 사이즈를 가진다.

제 9장. 실제 VPN 기반 원격진료 시나리오의 구현 및 테스트

9. 1 실험 방법

9. 1. 1 HMRET 소개

응급 원격 진료시스템은 전송되는 응급환자의 멀티미디머 데이터를 특성상 표 7-1과 같은 네트워크 프로토콜을 사용하여 전송한다. 환자의 상태를 진단하기 위한 실시간 고화질 영상 데이터는 고용량의 데이터를 전송하기 위해 본 논문에서 제안한 UDP 메커니즘에 의해 전송하고 전문의들간의 화상회의 데이터는 실시간 데이터 전송에 적합한 기존의 UDP 프로토콜을 사용하였다. 또한 환자의 생명에 직접적인 영향을 주는 환자의 이미지 파일이나 생체 신호 데이터는 신뢰적인 데이터 송수신을 보장하는 TCP 프로토콜을 사용하였다.

의료 데이터	프로토콜
HQ_Video (High Quality Video)	UDP
Conference Video & Audio	UDP
File(Dicom ,jpeg,bmp etc)	TCP/IP
Signal (ECG, Resp, NIBP, SpO2)	TCP/IP

표 9-1. 원격진료 시스템 파라미터 프로토콜

표 9-2는 720 * 480의 고화질 데이터를 MPEG4 계열의 인코더 코덱으로 압축하였을 때의 데이터 사이즈이다. 예를들어 30frame으로 설정되었을 때 1초 데이터는 MPEG4로 압축했을시에 약 1.67Mbps의 데이터가 발생함으로 이를 네트워크로 실시간으로 전송되어진다.

압축 Protocol \ Frame	1 frame	5 frame	10frame	15frame	30frame
XviD MPEG-4 Codec	0.055 Mbps	0.25 Mbps	0.53 Mbps	0.883 Mbps	1.671 Mbps
DivX MPEG-4 Fast-Motion	0.66 Mbps	0.312 Mbps	0.612 Mbps	0.92Mbps	1.722 Mbps
DivX MPEG-4 Low-Motion	0.65 Mbps	0.35 Mbps	0.653 Mbps	0.901 Mbps	1.73 Mbps

표 9-2 High Quality Video 의 프레임 별 데이터 사이즈

아래의 표 9-3은 생체신호 데이터 Size 및 구조를 나타낸다. 응급환자의 생체신호는 ECG, SpO2, Resp, IBP등의 데이터를 의사측 시스템과 통신함으로써 환자에 대한 진단을 효율적으로 수행한다. 원격 진료 시스템에서 환자측 시스템과 Pateint monitor간에 interface 하기 위해 환자측 시스템의 RS-232C를 이용한 시리얼 통신을 한다. 전체 생체신호 모두를 통신하기 위해서는 초당 1140Byte의 대역을 보장해 주어야 한다. HQ_Video의 송수신을 진행하면서 나온 데이터로부터 IPSec의 영향을 파악 하였다.

초당 Data(Wave+Parameter) (1140 Bytes)				
Wave Data (1050 Byte)				Parameters (90 Byte)
ECG	SpO2	IBP	Resp	
600Byte	150Byte	150Byte	150Byte	90Byte

표 9-3. 생체신호 데이터 Size 및 구조

9. 1. 2 실험 Tool과 조건

실험은 HMRET의 HQ_Video와 Bio_Signal에 대해 진행을 하였다. HQ_Video는 Frame 수를 각 통신망 상태에 따라 줄여가며 실험을 하였으며, Bio_Signal의 경우에는 모든 실험환경에서 우선적으로 전송 시킨 이후에, HQ_Video를 전송하였다. 네트워크의 Throughput과 RTT, Jitter를 측정하기 위해서는 Sniffer Pro 4.75라는 네트워크 분석 프로그램을 이용하였으며, 이외에 전산원에서 개발한 North Star라는 네트워크 상태 측정 프로그램을 사용하였다. 또한 Iperf 공개용 프로그램을 이용하여 데이터 송수신 할때의 Throughput과 Jitter 값의 변화를 Sniffer Pro 4.75와

비교 분석하여 결과를 내었다. 특히 RTT의 신뢰성을 확인해 보기 위해서 Dos 명령어인 Ping Test를 사용하여 전체적인 네트워크 상태를 측정하여 다른 측정프로그램으로 나온 결과를 비교분석하였다.

	위성통신 (HQ_Video 데이터 전송)	Wibro/HSDPA (HQ_Video 데이터 전송)	Wibro/HSDPA (시간&속도에따른데이터전송)
Desktop	·	Intel CPU 3.40Ghz 듀얼코어Memory 2Ghz	Intel CPU 3.40Ghz 듀얼코어Memory 2Ghz
Laptop	Toshiba M5 Intel CPU 2.0Ghz 듀얼코어 Memory 1Ghz	Toshiba M5 Intel CPU 2.0Ghz 듀얼코어 Memory 1Ghz	Toshiba M5 Intel CPU 2.0Ghz 듀얼코어 Memory 1Ghz
Operation System	Microsoft XP Pro Service Pack 2	Microsoft XP Pro Service Pack 2	Microsoft XP Pro Service Pack 2
통신 모뎀	FDMA/TDM 중계용 모뎀	SPH-H1100/SKY-IM-H100	SPH-H1100/SKY-IM-H100
실험 시간	2Hour/Frame (12:00~15:00사이)	2Hour/Frame (12:00~15:00사이)	3000 Packet/1Hour & 3000 Packet/10Km
실험 속도	정지 상태	정지 상태	0~100Km
Camera	Sony HQ_Video	Sony HQ_Video	·

표 9-4. 위성통신과 Wibro/HSDPA의 실험조건

9. 2 위성통신을 통한 원격진료

9. 2. 1 위성통신을 이용한 보안 원격진료 시나리오

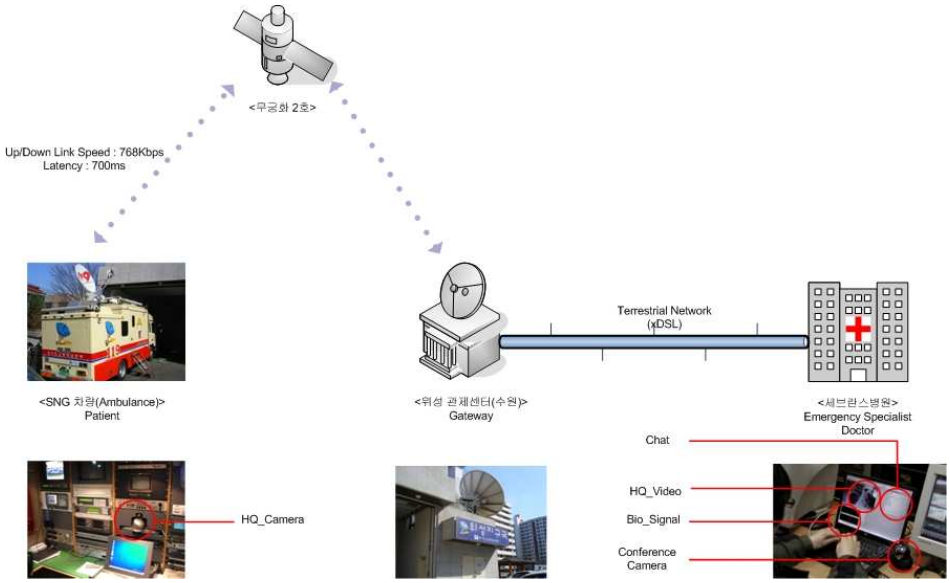


그림 9-1. 위성통신을 이용한 원격진료 시스템

위성통신을 이용한 보안 원격진료 시스템은 그림 9-1과 같은 형태로 이루어 진다. SNG 차량에는 HQ_Camera와 Laptop, Bio-Signal 측정 장비 등이 탑재 된다. 의료 데이터는 768Kbps의 Bandwidth 내에서 약 700ms의 지연을 가지고, 위성 관제센터로 전송이 이루어진다. 실험은 VPN과 IPSec을 사용하지 않은 Normal 상태에서 실험을 먼저 진행하고, 그 이후에 VPN과 IPSec을 적용한 시나리오 모델을 실험하여 비교분석을 하였다.

9. 2. 2 위성통신을 이용한 원격진료 시스템의 QoS 분석

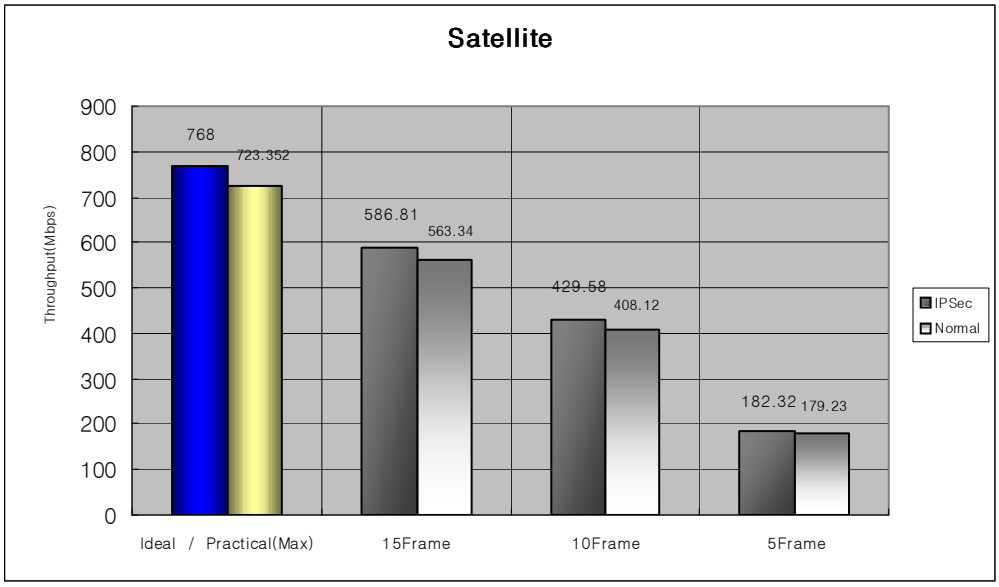


그림 9-2. 프레임별 Throughput

위 그림은 프레임 별 Throughput을 나타낸다. 그림에서 보는바와 같이 Ideal 상태에서는 768Kbps를 제시해 주었으며, 실제 최대 대역폭을 측정해 보았을 때는 728Kbps가 나와 ideal 값에 비해 5.2% 못 미치는 Throughput을 나타내었다.

실제 실험에서는 30Frame의 평균 Throughput인 1.67Mbps를 수용하지 못한다는 점에 착안하여 15Frame부터 5Frame까지 줄여가며, 영상데이터의 송수신을 하였다. IPSec을 포팅하였을 때는 프레임 별로 약 3,2%~6%의 차이를 나타내었는데, 이는 AH에서의 패킷당 24Byte의 오버헤드가 생기며, ESP에서 또한 24Byte의 오버헤드가 생겨 총 1024Byte의 패킷이 초당 전송이 될 때, 48Byte의 오버헤드가 가중되어 데이터가 크게 측정되었다.

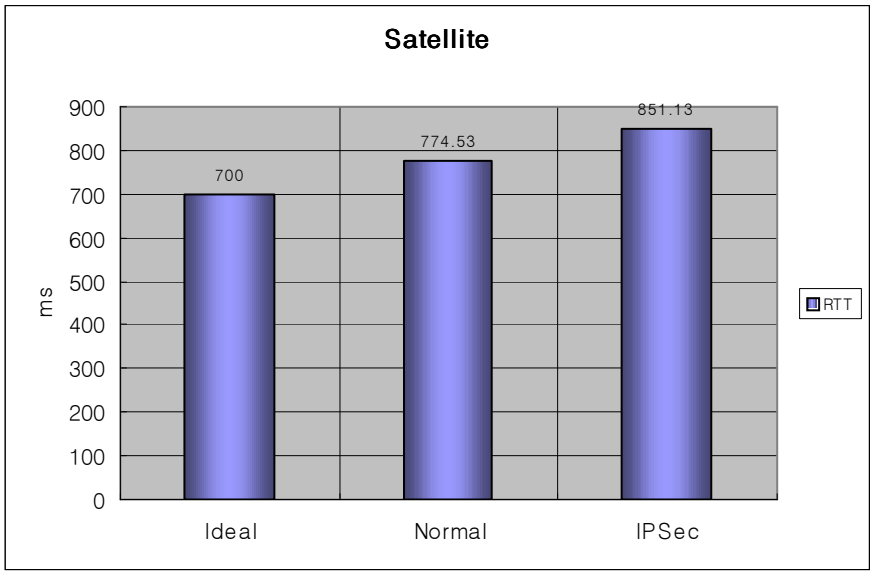


그림 9-3 Normal 과 IPSec 에서의 RTT

위성통신에서의 RTT의 이상적인 값은 700ms이다. 곧, 상향링크에서 350ms가 걸리며 하향링크에서 350ms가 걸린다. 그러나 실제 RTT의 측정결과 Normal 상태에서 10% 더 큰 774.53ms가 측정되었고, IPSec을 포팅시켰을 때는 이상적인 값에 비해 무려 21.6%나 더욱 큰 RTT값이 측정되었다. 위성통신의 경우 일반적인 이동통신이나 Wired 통신에 비해 원거리 통신을 하기 때문에 전파지연의 영향을 많이 받는다. 따라서 기상상태나 주위환경의 간섭전파에 의해 RTT의 값이 커질 가능성이 매우 높다. 실제로 황사나 강우에 의해 선형적으로 위성신호의 감쇄가 일어난다고 연구결과가 보고되고 있으며, 신호감쇄에 의해 Throughput이나 RTT, jitter 값의 변화를 초래할 수 있다.

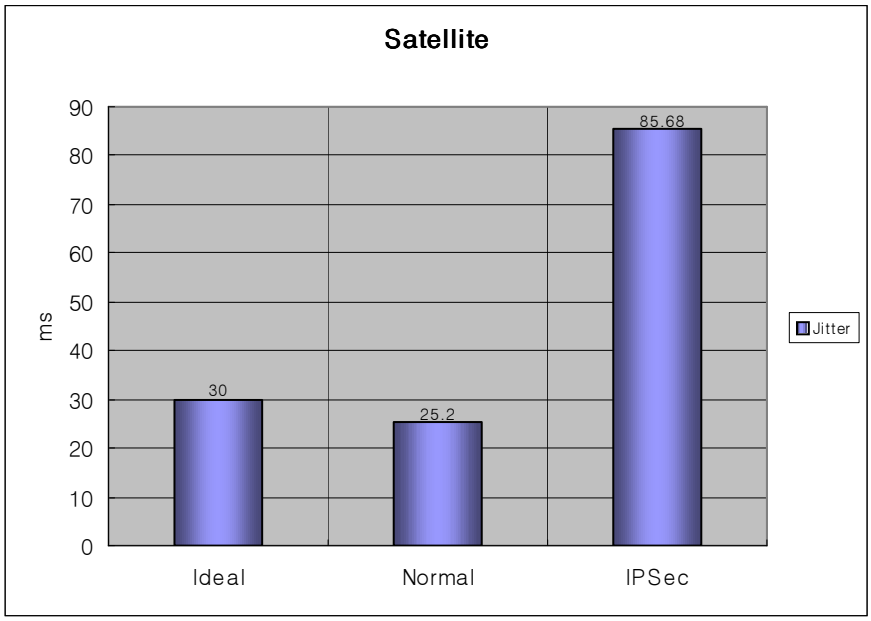


그림 9-4. Normal과 IPSec에서의 Jitter

위성통신에서의 Jitter 값은 위 그림과 같다. 이상적인 값은 30ms 내외로 보고되고 있으며[참고문헌], Normal 상태에서 25.2ms로 16% 낮은 Jitter 값이 측정되어 영상 전송에 왜곡현상은 거의 보이지 않았다. 하지만, IPSec을 포팅하였을 때, 결과는 85.88ms로서 이상적인 값보다 무려 186%나 높은 값을 나타내었다. IPSec을 적용시켰을 때, Host와 Host 사이 AH를 통한 인증과 64bit 마다 한번씩 수행되는 3DES 알고리즘의 연산 수행에 의해 앞서 확인한 그림 9-4의 그래프와 같이 RTT 값의 급격한 증가가 일어났다. 특히 3DES 알고리즘이 적용되고, 또다시 전파지연과 같은 현상이 부가가 되어 더욱 큰 RTT를 가지게 되었으며, Jitter 값의 증가로 연결되었다고 볼 수 있다.

9. 3 Wibro와 HSDPA를 이용한 보안 원격진료

9. 3. 1 Wibro를 이용한 보안 원격진료 시스템

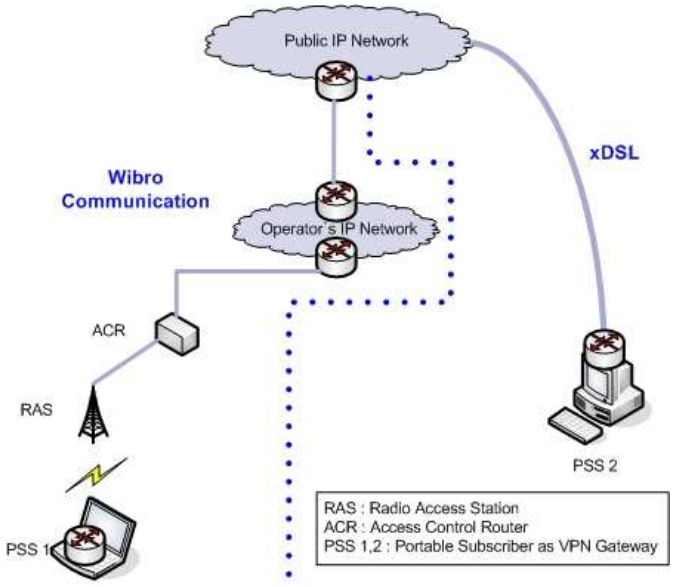


그림 9-5. Wibro를 이용한 보안 원격진료 시스템 시나리오

그림 9-5 는 Wibro를 이용한 보안 원격진료 시스템 시나리오이다. 실제 실험 환경의 구현 시 PSS 1과 PSS 2 사이는 간단히 연결되는 것처럼 보이지만 위처럼 다소 복잡한 구조를 나타낸다. 먼저 Wibro 네트워크 망은 Gateway로 동작하는 PSS에서 무선 액세스 스테이션인 RAS(기지국)로 의료 데이터를 전송 시켜주며, ACR을 통해 무선자원의 관리를 통하여 QoS와 Wibro 자체의 인증과 보안의 동작이 이루어 진 뒤에 IP Network 관리자의 라우터를 통해 공용 IP Network로 통신이 이루어 질 수 있다. 공용 IP Network는 xDSL 과 연결이 되어 최종적으로 PSS 2로의 의료 데이터의 전송이 완료된다.

그림 9-6. Wibro Performance Check(NorthStar)

위 그림 9-6 은 한국정보사회진흥원(NIA)에서 제공하고 있는 네트워크 퍼포먼스 측청 툴이다. 이 툴을 이용하면, 실시간 대역폭(Speed) 나 RTT는 알 수 없지만, 현 시간대의 대역과 RTT의 평균치를 구할 수 있다. 이 결과를 이용해 실시간 데이터를 예상해 볼 수 있다. Wibro의 평균 대역폭(Speed)은 1.2Mbps의 Upload 와 958.3Kbps의 Download 속도를 내며, 평균 RTT 값은 109.4ms 정도가 나오는 것을 확인 해 볼 수 있다. 이는 실제로 KT나 SKtelecom에서 제공하고 있는 3Mbps/1Mbps(Down/Up)에 훨씬 못미치는 속도이며, 이상적인 환경이 아닌 단말기와 기지국 간의 송, 수신 강도의 변화 때문이라고 볼 수 있다.

9. 3. 2 HSDPA를 이용한 보안원격 진료 시스템

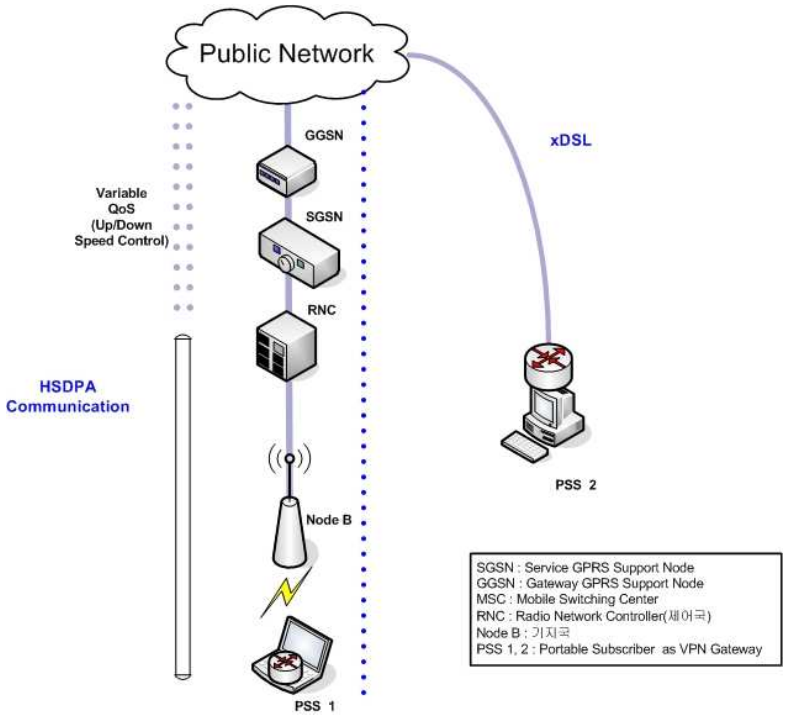


그림 9-7. HSDPA를 이용한 보안 원격진료 시스템 시나리오

그림 9-7은 HSDPA를 이용한 보안 원격진료 시스템 시나리오이다. 먼저 HSDPA 네트워크 망은 VPN Gateway로 동작하는 PSS 1에서 Node B(기지국)로 의료 데이터를 전송 시켜주며, ACR을 통해 무선자원의 관리를 통하여 QoS와 Wibro 자체의 인증과 보안의 동작이 이루어 진 뒤에 IP Network 관리자의 라우터를 통해 공용 IP Network로 통신이 이루어 질 수 있다. 공용 IP Network는 xDSL 과 연결이 되어 최종적으로 PSS 2로의 의료 데이터의 전송이 완료된다.

그림 9-8. HSDPA Performance Check(NorthStar)

실험 당시 HSDPA의 평균 대역폭(Speed)은 351.1Kbps의 Upload 와 955.5Kbps의 Download 속도를 내며, RTT 값은 109.4ms 정도가 나오는 것을 확인 해 볼 수 있다. SKtelecom에서 제공하고 있는 3Mbps/2Mbps(Down/Up)의 속도를 내지 못하는 것은 Wibro와 동일한 이유 이외에 기지국 내 접속자수의 증감 등으로 인한 네트워크 성능의 영향으로 볼 수 있다.

9. 3. 3 시간과 속도에 따른 Wibro와 HSDPA의 성능 비교

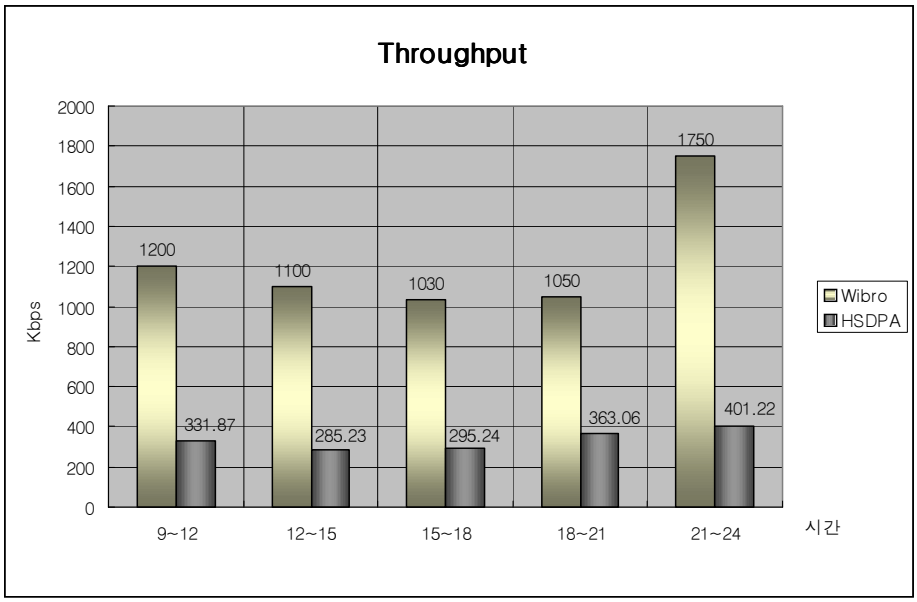


그림 9-9. 시간대에 따른 Wibro와 HSDPA의 Throughput 변화

위 그림 9-9는 시간대에 따른 Wibro와 HSDPA의 Throughput 변화를 나타낸다. Wibro와 HSDPA는 원격지의 의료데이터를 송신하는 역할을 하기 때문에 Up-load 값이 의미가 있다. 따라서 우리는 Up-load 값을 측정하였으며, Wibro가 HSDPA에 비해 약 3~4배에 해당하는 높은 Throughput 값을 보여주었다. Wibro는 HSDPA가 변조에 QPSK와 16QAM 방식을 사용하는 것에서 한단계 뛰어넘은 64QAM 방식까지 커버를 하고 있기 때문에 더욱 높은 Throughput 값을 낼 수 있다.[The Performance Comparison between Wibro and HSDPA, 2005, IEEE, Simon Shindhl 3명, SK Telecom] 또한 Wibro는 8.3Mhz의 신호 대역을 이용하며, HSDPA는 3.82Mhz의 신호 대역을 이용하므로, 더욱 높은 Upload 속도를 예상해 볼수 있다. 시간대 별 데이터의 변화는 12~21시까지 사용자 수가 많을 때, Throughput이 낮아짐을 확인할 수 있었으며, 21~24시까지의 시간대에서는 15~18시 사이의 Throughput 보다 66%나 증가한 값을 보여, 이용 시간대에 의해 큰 영향을 받는다는 사실을 확인할 수 있었다.

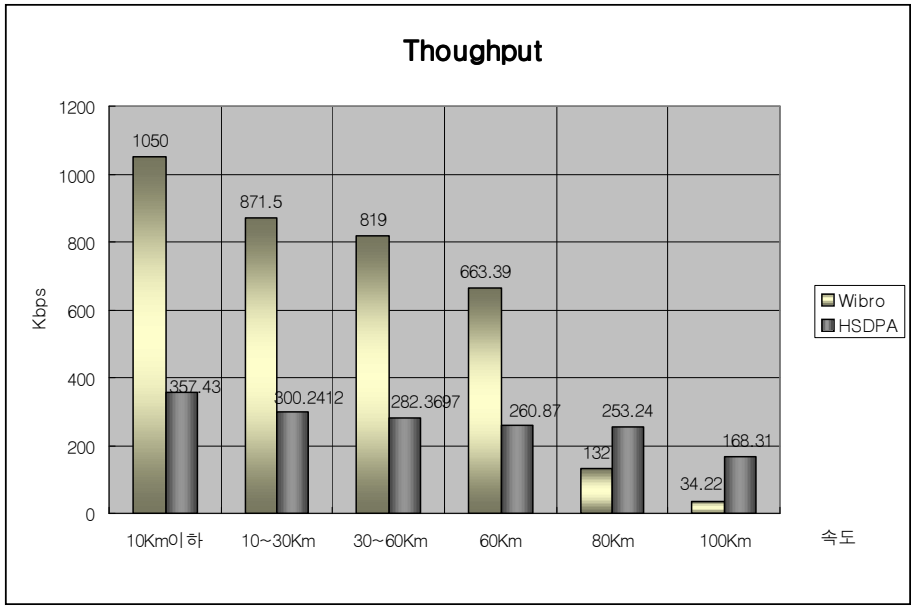
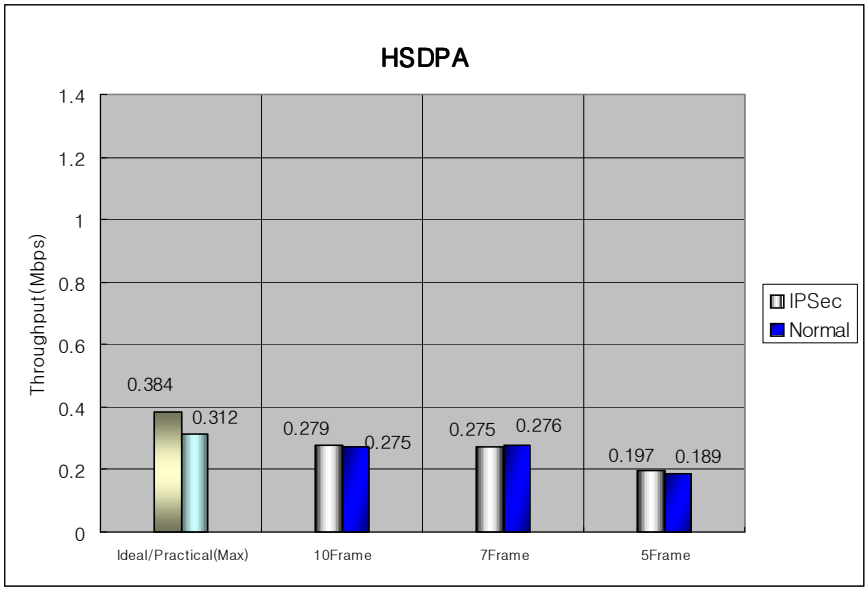


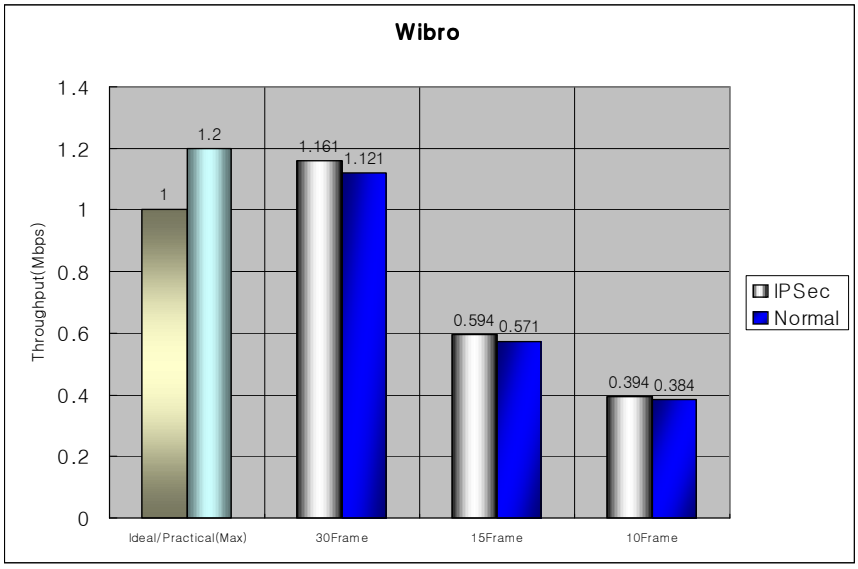
그림 9-10. 속도에 따른 Wibro와 HSDPA의 Throughput 변화

그림 9-10은 속도에 따른 Wibro와 HSDPA의 Throughput의 변화를 나타낸다. Wibro는 9Mhz의 대역중에서 1/3을 UP-load 값으로 이용을 하며, 거의 1Mbps의 속도를 낼 수 있다. 하지만, HSDPA는 3.82Mhz의 대부분을 Down-load 값으로 이용하며, 일부만을 Up-load에 이용하므로 Wibro보다 낮은 성능을 나타낸다고 볼 수 있다. 10Km는 보행이나 가벼운 조깅을 하고 있을 때로 볼 수 있으며, 10~100Km까지는 자동차를 이용하여 이동할 때의 결과이다. 속도가 증가함에 따라 Throughput 값은 줄어들게 되는데, Wibro에서 더욱 큰 하강폭을 보였다. 이유는 TTI 간격이 Wibro의 경우 5ms이며, HSDPA의 경우에는 2ms로 더욱 짧기 때문에 Wibro보다 데이터의 전송을 빠른 시간 내에 할 수 있는 이점이 있어서 속도에 강한 성능을 보인 것이다. 따라서 60Km 이하까지는 Wibro가 HSDPA보다 월등히 높은 성능을 보이지만, 80Km 이후 부터는 HSDPA의 Throughput 대역이 오히려 Wibro보다 높은 현상을 확인 할 수 있다.

9. 3. 4 Wibro와 HSDPA를 이용한 보안원격진료 시스템의 QoS 분석



(a) HSDPA



(b) Wibro

그림 9-11. Normal과 IPSec Throughput 비교

위 그림 9-11 그래프는 HQ_Video의 정상 상태일 때와 IPSec을 적용시켰을때의

Wibro와 HSDPA의 결과 그래프이다. Wibro에서 Upload 속도가 Ideal한 상태에서 1Mbps가 측정되었으며, 실제 측정결과는 1.2Mbps가 측정되었다. HSDPA에서는 Upload 속도가 Ideal한 상태에서는 0.384Mbps라고 알려져 있으며, 실제 최대 Upload 속도는 0.312Mbps가 측정되었다. 앞서 속도와 시간대에 따른 성능분석에서 확인해 보았듯이 HSDPA보다 더 좋은 변조성능 개선(64 QAM)이 진행된 Wibro의 Throughput이 더욱 크게 측정되었다. HQ_Video를 감소시켜가면서 Wibro와 HSDPA에 적합한 Frame Rate를 찾기 위해 Wibro에서는 30, 15, 10 Frame으로 줄여가면서 HQ_Video를 전송하였고, HSDPA에서는 수용가능한 수준을 예상하여 10, 7, 5 Frame 순으로 줄여가며 HQ_Video 전송을 실험하였다.

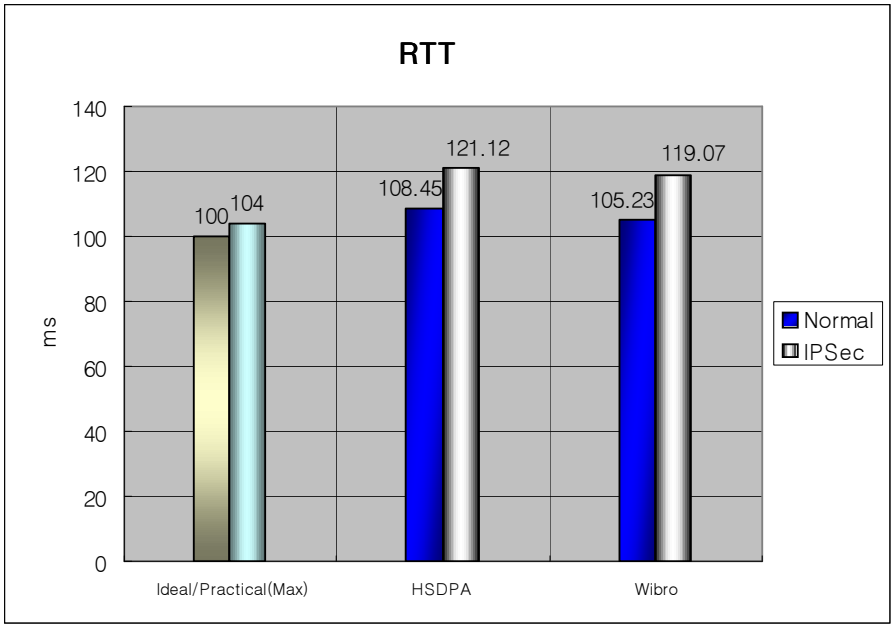
먼저 Wibro를 보면, 30 Frame에서는 앞서 확인한 XviD MPEG-4 Codec Protocol을 이용하였을 때, 평균 1.67Mbps의 크기로 전송이 이루어진다. HQ_Video와 BioSignal을 모두 송수신을 한다고 가정하면, 초당 1140Byte가 추가되므로, 약 9.120Kbps가 추가된다고 볼 수 있으며, 1.67Mbps에 약 0.01Mbps가 더해진다고 생각 할 수 있다. 0.01Mbps의 작은 값이 생체신호로 들어오지만, 연결지향의 전달 서비스인 TCP/IP로 송수신이 이루어지며, 에러가 있을 경우 지속적인 재전송을 하기때문에 UDP로 전송되고 있는 HQ_Video의 전송 용량이 Bio_Signal의 전송 용량을 1k넘어서게 되면, Bio_Signal을 수신측에서 얻지 못하는 경우가 발생 할 수 있다. 이를 극복하기 위해서는 HQ_Video의 전송 용량을 네트워크 상태보다 높게 책정해서는 안 된다. Bio_Signal 전송을 위해 10Kbps의 전송대역은 보장을 해주어야 하는 것이다. 그러므로 30Frame의 HQ_Video의 전송은 Wibro에서 실시간 의료영상 데이터의 전송에 부적합하며, Bio_Signal의 대역을 보장해 주기 위해서 15Frame의 HQ_Video 전송이 적합하다는 판단을 내릴 수 있다.

Normal 상태와 IPSec을 포팅 했을 때의 변화는 앞서 실험했던 가상환경에서의 VPN 기반 IPSec 프로토콜 실험에서 확인했듯이 Utilization측면에서 보았을 때, 4%정도 Payload 데이터 양이 줄어들었기 때문에 데이터 패킷 사이즈 1000Byte에서 약 4%정도가 늘어난 1048Byte의 패킷이 전송된 것을 확인할 수 있다. 30 Frame 에서는 Wibro가 수용할 수 있는 대역(1.2Mbps)을 넘어서기 때문에 Normal 상태와 IPSec이 포팅된 상태에서의 정확한 Throughput 증감을 확인할 수

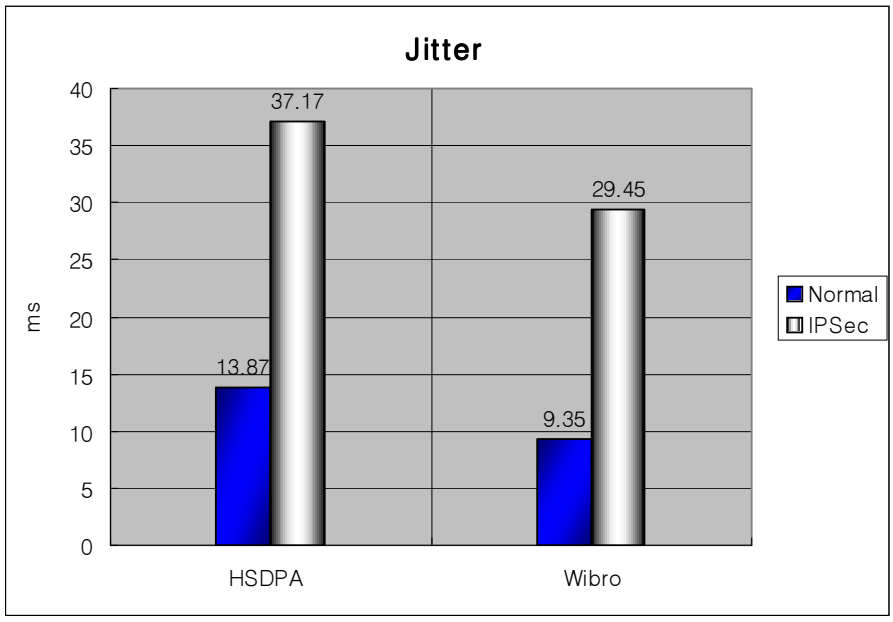
없었으며, 15Frame에서는 Normal 상태 평균 Throughput 0.571Mbps, IPSec 적용 시 Throughput 0.594 Mbps가 나와서 약 4%의 Throughput 차이가 확인 되었다.

HSDPA 역시 Wibro와 마찬가지로 생체신호의 대역을 남겨두고 남은 대역을 이용하여 HQ_Video를 전송한다고 생각하면, 10, 7Frame에서는 약 0.27~0.28Mbps의 전송속도를 보여주었는데, 10Frame에서 평균 0.53Mbps, 7Frame에서 평균 0.4Mbps를 수용할 수 있는 정도의 대역을 유지해야하지만, HQ_Video의 전송이 가능하다. 하지만 0.27~0,28Mbps의 사이의 대역으로는 HQ_Video의 원활한 전송이 불가능하다는 사실을 확인 할 수 있었다. 실제로 10, 7Frame에서 UDP로 전송되는 HQ_Video의 왜곡이 10~15초 간격으로 심하게 나타났으며, TCP로 전송되는 Bio_Signal은 정지상태로 유지되었다. 5Frame 으로 영상을 전송할 때는 평균 0.18~19Mbps의 값을 나타내었으며, Bio_Signal의 대역을 보장해 주기 위해 적합한 Frame Rate이었다.

Normal 상태와 IPSec을 포팅 했을 때의 변화는 앞서 실험했던 가상환경에서의 VPN 기반 IPSec 프로토콜 실험에서 확인했듯이 Utilization측면에서 보았을 때, 4%정도 Payload 데이터 양이 줄어들었기 때문에 데이터 패킷 사이즈 1000Byte에서 약 4%정도가 늘어난 1048Byte의 패킷이 전송된 것을 확인할 수 있다. 10, 7 Frame 에서는 HSDPA가 수용할 수 있는 대역(300Kbps)을 넘어서기 때문에 정확한 Throughput을 확인할 수 없었으며, 5Frame에서는 Normal 상태 평균 Throughput 0.18Mbps, IPSec 적용 시 Throughput 0.19 Mbps가 나와서 약 4%의 Throughput 차이가 확인 되었다.



(a)



(b)

그림 9-12. Wibro와 HSDPA의 RTT와 Jitter

위 그림 9-12는 Wibro와 HSDPA의 Normal 상태와 IPSec이 포팅된 상태에서의 RTT와 Jitter 값을 나타낸다. 그림 9-11의 그래프에서 확인한 바와 같이 Throughput 값이 IPSec이 포팅 되었을 때는 Normal 상태보다 높은 값을 갖는다는 것을 확인했다. 따라서 RTT와 Jitter 값도 영향을 받아 IPSec이 적용 되었을 때, 좀 더 높은 RTT와 Jitter를 갖게 된다. Wibro에서 RTT값은 Normal 상태일 때, 평균 105.23ms이 나왔으며, IPSec이 적용 되었을 때 119.07ms라는 값이 나와서 IPSec이 적용되었을 때보다 약 13.15% 더 높게 측정되었다. Jitter는 Normal 상태에서 9.35ms가 측정되었으며, IPSec이 적용되었을 때, 29.45ms가 측정되어 IPSec이 적용되었을 때보다 약 3배정도 큰 Jitter값이 측정되었다. HSDPA에서도 RTT값은 Normal 상태일 때, 평균 108.45ms이 나왔으며, IPSec이 적용 되었을 때, 121.12ms 이라는 값이 나와서 IPSec이 적용되었을 때, 약 10.46% 더 높게 측정되었다. Jitter 에서는 Normal 상태에서 13.87ms가 측정되었으며, IPSec이 적용되었을 때, 37.17ms가 측정되어 IPSec이 적용되었을 때보다 3배정도 큰 Jitter값이 측정되었다.

IPSec의 AH, ESP 설정 시, 지연 값이 증가하는 것은 아래 그림 9-13과 같이 AH에서의 인증에 사용되는 해쉬 연산과정이 요구되며, ESP에서 ESP에서 제공하는 3DES 알고리즘은 64bit마다 수행되어 암호화 및 복호화 시간을 증가시키기 때문이다.

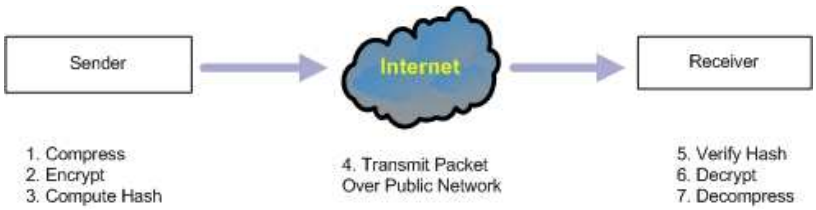


그림 9-13. System 지연의 원인

제 10장. 결론 및 토의

본 논문에서는 최신 무선통신 환경인 Wibro, HSDPA와 위성통신 환경에서 개발된 HMRET 프로그램을 이용하여 실시간으로 의료데이터를 송수신할 때, 보안문제를 보완하기 위해서 VPN 프로토콜 하에서 IP layer 기반에 적용 가능한 AH(MD5, SHA-1), ESP(3DES) 알고리즘을 변화시키며 시뮬레이션 환경에 적용시켰을 때의 프로세싱 시간과 네트워크 망의 상태를 평가할 수 있는 지표인 QoS를 통해 지연(Round Trip Time), 지터(Jitter), 대역폭(Throughput)을 산출하였으며, 원격 진료 시스템의 정책 결정에 기반이 될 수 있는 적절한 알고리즘을 제안하였고, 이 결과를 바탕으로 무선통신 환경에서의 원격진료 시나리오를 테스트 해봄으로서 원격 진료 시스템에 보안 적용 가능성을 파악하였다.

첫 번째 보안 알고리즘 실험에서는 IPSec 프로토콜의 AH, ESP에서 제공하는 인증과 암호화 프로토콜을 둘 다 사용해야 IP의 인증과 내부 데이터의 암호화를 모두 만족시킬 수 있다. 따라서 AH에서는 MD5보다 32비트 높은 헤더값을 갖지만 맹목 단순형 공격에 덜 취약한 SHA-1 프로토콜을 선택하는 것이 바람직 하며, ESP에서는 DES의 단순한 암호체계에서 발전하여 슈퍼컴퓨터로도 암호화 해독이 거의 불가능한 3DES 알고리즘을 선택이 권장된다. 3DES 알고리즘은 IPSec의 알고리즘 중에서 데이터 패킷 전체의 암호화(Encryption)를 하기 때문에 프로세싱 타임이 오래 걸리는 주된 이유가 되는데, 실험결과 노트북이나 PDA와 같은 저 사양의 단말을 이용할 경우 3DES의 계산량에 의해 지연시간의 급격한 증가를 예상할 수 있었다. 이제 3가지 통신망에 대해서 VPN 기반하의 IPSec 프로토콜(SHA-1, 3DES)을 적용시켰을 때의 원격 진료 시스템을 실험하였고, Normal 환경에서의 실험결과와 비교분석하였다.

두 번째 위성통신망은 36,000Km에 달하는 거리에 의해 700ms 정도의 지연이 발생한다. 이 전파지연 시간은 다른 여타 상용 통신망 보다 매우 큰 수치이다. 주된 문제 중의 하나는 전파지연으로 인해 음성신호의 에코현상을 일으키거나 영상신호와 생체신호가 실시간으로 전송될 수 없는 환경에 놓이게 한다. 여기서는 위성체의 성능이 좋아지지 않는 한 지연 시간을 줄이기 불가능하기 때문에 지연시간

을 수용하되 최저 지연시간을 유지해 주는 것이 중요한데, 이를 위해서 실험 위성통신의 768Kbps를 넘지 않는 범위에서의 최적화된 HQ_Video 전송 프레임을 확인해 본 결과, 평균 약 15Frame 으로 유지된 상태에서 Bio_Signal과 HQ_Video의 원격진료가 가능할 것이란 결과를 얻었다. IPSec을 적용하였을 때, 인공위성을 이용한 원격진료 시스템은 AH와 ESP 두가지 프로토콜의 인증과 암호화와 원래 위성통신의 특성상 전파지연과 기상상태 그리고 주위환경의 간섭전파에 의해 RTT와 Jitter의 증가를 확인 할 수 있었고, 특히 Jitter 값의 증가가 두드러졌는데, 이는 원활한 영상데이터의 송수신이 되지 않고, 왜곡되는 현상이 나타났다. 이처럼 왜곡이나 끊김 현상을 커버하기 위해서는 고용량의 데이터를 송수신 할 수 있는 Ka Band 대역의 고주파수 대역을 이용하거나, 저궤도 위성을 이용하여 RTT값의 영향을 줄일 수 있는 방법을 택해야 할 것이다.

세 번째 Wibro 와 HSDPA 통신망을 이용하여 의료 영상데이터의 송수신을 하기 이전에 Wibro와 HSDPA의 이동성과 시간대에 따른 성능을 알아 본 결과 두 통신망 모두 21~24시 사이에는 통신이 단말기 접속자들의 수가 많은 낮 시간대에 비해 훨씬 좋은 성능을 낸다는 사실을 바탕으로 의료데이터의 전송 프레임 대역을 증가시키는 방법을 사용해야 하며, 속도에 따른 평가는 Wibro가 60Km/h 대까지 HSDPA보다 훨씬 좋은 Up_load 성능을 보이기 때문에 보행중이나 60Km/h이하의 낮은 속도에서의 의료 데이터 전송이 적합하며, HSDPA는 60Km/h를 초과하는 고속의 환경에서의 의료 데이터 전송에 적합한 통신망이라고 판단할 수 있다.

네 번째 Wibro와 HSDPA의 원격진료시스템을 비교해 보면, Normal 상태에서는 전송할 수 있는 대역에 따라 전송 프레임 양의 차이는 있었으나 Wibro와 HSDPA 둘다 각각 15Frame과 5Frame에서 HQ_Video와 Bio_Signal 데이터의 원활한 송수신이 가능했다. 그러나 IPSec의 인증과 암호화에 의한 RTT와 Jitter값의 현저한 증가로 Wibro에서 HQ_Video가 왜곡되는 현상이 분당 1회 발생하였으며, HSDPA에서는 분당 3회 정도 발생 하였다. IPSec 적용 시 Wibro의 경우에는 데이터의 송신을 하는데, 충분한 대역폭을 지원하고 있으며, Jitter 값이 증가하기는 하지만, 원격진료에 방해가 될 정도는 아니다. 하지만, HSDPA의 경우 Jitter 값이 Normal 상태일 때보다 3배가까이 높은 값을 가지기 때문에 화면의 왜곡과 정지현상이 두드

러지게 나타나 원격진료가 거의 불가능했다. 결국 최신 이동통신 환경인 Wibro와 HSDPA를 통해 VPN 기반의 IPSec 프로토콜을 적용하여 보안이 보장되는 환경에서 원격진료 시스템을 운용하기에는 Wibro가 더욱 만족스럽다고 말할 수 있으나, 통신망의 발전에 따라 향후 3~4년 이후이면, HSDPA의 성능이 발전되어 Wibro와 함께 원격진료에 이용되어질 시기가 올 것이다.

참고문헌

[1] C. S. Pattichis, E. Kyriacou, S. Voskarides, M. S. Pattichis, R. Istepanian, C. N. Schizas, "Wireless Telemedicine Systems: An Overview", IEEE Antenna's and Propagation Magazine, Vol. 44, No. 2, April 2002.

[2] J. R Gallego, A. Hernandez-Solana, M. Canales, J. Lafuente, A. Valdovinos, J. Fernandez-Navajas, "Performance Analysis of Multiplexed Medical Data Transmission for Mobile Emergency Care Over the UMTS Channel", IEEE Transactions on Information Technology in Biomedicine, 9, 1, March 2005, pp. 13-22.

[3] L. Pierucci, D. R. Enrico, "An Interactive Multimedia Satellite Telemedicine Service", IEEE Multimedia, April-June, 2000.

[4] G. Graschew, T. A. Roelofs, S. Rakowsky, P. M. Schlag, "Telepresence over satellite", International Congress Series, 1206(2003), 2003, pp. 273-178.

[5] W. Qu, S. Srinivas, "IPSec-BASED SECURE WIRELESS VIRTUAL PRIVATE NETWORK", IEEE British Crown, 2002, pp. 1107-1112.

[6] 문명호, "무궁화 위성의 기술적인 특성과 위성 통신의 응용", 논문, 1994. pp. 329-349.

[7] 박성태 외 2인, "정보통신개론," 생능출판사, 1999. pp. 122-159.

[8] 정길현, "Study of the Mobile and Satellite Communications", 장안논문(24), 2004, pp. 250-260.

[9] Z. Sun, "Satellite Networking", Wiley, 2005, pp. 63-72.

[10] T. Pratt, C. Bostian, J. Allnutt, "Satellite Communications", Wiley International Edition, 2002, pp. 421-438.

[11] Z. Sun, "Satellite Networking", Wiley, 2005, pp. 231-237.

[12] 김용석 외, "Take out 첨단지식 훤히 보이는 Wibro", u-북, 2004, pp. 177-238.

[13] TTa, TTAS.KO-06.0064, Specifications for 2.3 GHz band Portable Internet

Service-Physical Layer.

[14] Taesoo Kwon, Sunghyun Cho et. al., "Design and Implementation of a Simulator Based on a Cross-Layer Protocol between MAC and PHY layers in a WiBro Compatible IEEE 802.16e OFDMA System", IEEE Communications Magazine, Vol. 43(2), Dec. 2005, pp. 136-146.

[15] Michael W. Thelander, "WIMAX or WIBRO: Similar names, yet dissimilar technologies", shite paper developed by Nortel, Apr. 2006.

[16] R. Love, A. Ghosh, W. Xiao, R. Ratasuk., "Performance of 3GPP High Speed Downlink Packet Access(HSDPA)", IEEE Communication Magazine, 2004, pp.3359-3363.

[17] 3GPP Technical Specification (TS) 25.211-215, Version 5.3.0.

[18] 3GPP Technical Specification (TS) 25.211-215, Version 5.3.0.

[19] 인터넷보안기술포럼, “IP계층에서의 VPN 보안 기술 표준”, ISTF-003, 2001.

[20] O’Guin, S., C.K.Williams, "Application of Virtual Private Network Technology to Standards-based Management Protocols across Heterogeneous Networks", Proceedings of IEEE Military Communications Conference, 1999, vol. 2, pp.1251-1255.

[21] "VPN", http://www.sharpened.net/.

[22] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", IETF RFC 2401, 1998.

[23] 주식회사 니츠 편저, “인터넷 보안 기술 -1”, 도서출판 동서, pp. 20~51.

[24] 이주원, 이항주, “How to Windows Server 2003”, (주) 프리랙, pp. 246-269.

[25] C. R. Davis, 역 염홍열외 2명, “안전한 VPN을 위한 인터넷 보안 프로토콜”, 한티미디어, 2003, 197-212.

[26] C. R. Davis, 역 염홍열외 2명, “안전한 VPN을 위한 인터넷 보안 프로토콜”, 한티미디어, 2003, 231-245.

[27] D. R. Stinson, "Cryptography Theory and Practice", Chanpman & Hall/CRC, 2002. pp. 96~116.

[28] B. Schneier, "Applied Cryptography", Wiley, 1996. pp. 265-300.

ABSTRACT

The Transmission Performance Analysis of Remote Healthcare Data over Secure Wireless Networks

Seo, Kuk Jin
Graduate Program in
Biomedical Engineering
The Graduate School
Yonsei University

In whatever situation, telemedicine system should be available to the transmission of healthcare data, it is system that have to act so that can do emergency aid fast and exactly to avoiding distortion or cut of data that unstable transmission.

One of essential element is network to telemedicine system and quality high telemedicine service is available by selection of suitable network according to situation. Although recently wired network may not be problem in real time multimedia transmission through the rapid development of wired network, 1xCDMA2000 used mainly meantime in wireless network has low bandwidth that do not reach to 500Kbps and WLAN has problem in mobility.

Lately, in wireless network, technology upgraded such as Wibro (Wireless Broadband Internet), HSDPA (High Speed Down Link Packet Access) are improving quality of multimedia service that offer high bandwidth that reach

to 1~3Mbps.

Accordingly, wireless network adapted for telemedicine system became various and doctor could treat patients regardless of time · spaces · mobility and the network affirmatively has an effect on patient's the survival rate and the recovery rate. It can become the cornerstone to adapt to fast developing wireless network that compose and test telemedicine system in these newest network environment.

And, we progressed the test of telemedicine system using by satellite communication as well as newest wireless networks. Although research is proceeding on telemedicine system using by satellite communication that consider emergency situation in area that network doesn't reach as worst disaster states or remote islands and desert that network infra can't use being damaged, Satellite communication is not active than research made use of other network infra.

In this study, we applied IPSec(AH, ESP) algorithms under VPN(Virtual Private Network) protocol that security is guaranteed and found adequate algorithm combinations to security network when applied in OS(Operating System) simulation environment. At that time, performance estimation of network system was RTT(Round Trip Time), Jitter, Bandwidth that indicate to QoS(Quality Of Service).

Finally, in wireless environment we researched possibility of security application as test telemedicine scenario based on results of pretest and studied about usefulness and limitation of telemedicine system using by Satellite, Wibro and HSDPA.