대한의료정보학회지 제14권 제4호
J Kor Soc Med Informatics 2008;14(4):439-449

원저

위성 보안 네트워크 기반의 의료 데이터 전송성능 평가

임동규[1,3], 유선국[2,3], 김동근[2,3], 김정채[1,3], 좌민홍[4]

연세대학교 생체공학 협동과정[1], 연세대학교 의과대학 의학공학교실[2],
이동형 응급의료정보시스템 개발센터[3], 연세대학교 의과대학 응급의학교실[4]

The Transmission Performance Evaluation of Remote Healthcare Data over Secure Satellite Network

Dong kyu Lim[1,3], Sun K. Yoo[2,3], Dong keun Kim[2,3], Jung chae Kim[1,3], Min hong Choa[4]

Graduate School of Biomedical Engineering, Yonsei Univ[1],
Dept. of Medical Engineering, Yonsei Univ. College of Medicine[2],
Center for Emergency Medical Informatics[3],
Dept. of Emergency Medicine, College of Medicine, Yonsei Univ.[4]

Abstract

Objectives: We have not only examined telemedicine scenario but also applied IPSec(AH, ESP) algorithms under VPN(Virtual Private Network) for performance evaluation of telemedicine system's security and transmission. **Methods:** In this study, we applied IPSec(AH, ESP) algorithms under VPN(Virtual Private Network) protocol when transmit healthcare data through Satellite Network. At that time, we evaluated performance of telemedicine system through RTT(Round Trip Time), Jitter, Bandwidth that indicate to QoS(Quality Of Service). **Results:** It is possible to transfer remote healthcare data over Satellite Network under provided image of 15 frame and bio-signal of 10 kbps and RTT(Round Trip Time) of 774.53ms, Jitter of 25.2ms. But applying IPsec(AH, ESP) under VPN(Virtual Private Network), it is frequently happened distortion of image data affected SHA-1 and 3DES algorithm. **Conclusion:** In this study, it is possible to use telemedicine system for Secure Satellite Network, but demand to be based QoS(Quality Of Service) limited. We expected that it is possible to use the designed system in the disaster area. ***(Journal of Korean Society of Medical Informatics 14-4, 439-449, 2008)***

Key words: Telemedicine, Satellite, IPSec, Healthcare Data, QoS

논문투고일: 2007년 8월 3일, **심사완료일:** 2008년 7월 29일
교신저자: 유선국, 서울특별시 서대문구 신촌동 134 연세대학교 의과대학 의학공학교실 (120-749)
Tel: 02-2228-1919, **Fax:** 02-363-9923, **E-mail:** sunkyoo@yuhs.ac
* 본 연구는 2007년도 보건복지부지정 특정센터연구지원 연구개발 사업 연구비에 의하여 연구되었음.
(과제번호: 02-PJ3-PG6-EV08-0001).

Ⅰ. 서론

최근 유무선 네트워크 인프라의 비약적인 발전을 통해 원격 진료 시스템 같은 고품질 의료서비스를 제공하게 되었다. 의료기관은 보건소와 가정에 유선 네트워크 기반의 원격 진료 시스템을 구축하여 환자에게 양질의 의료서비스를 제공하며, 의료기관과 응급차간 무선 네트워크 기반 하 원격 진료 시스템을 구축하여 환자의 생존율과 회복률에 긍정적 효과를 끼치고 있다[1-5].

하지만 수많은 기존 유무선 네트워크 인프라에도 불구하고, 위성 네트워크를 이용한 원격 응급의료 시스템의 적용이 필요한 이유는 기존 유무선 네트워크 인프라가 손상된 최악의 재난상태에서 응급상황이 발생할 수 있기 때문이다.

위성 네트워크 환경은 다른 네트워크 환경보다 훨씬 제한적이고 특성상 브로드캐스팅 방식을 이용하기 때문에 IP 스푸핑, IP 스니핑과 같은 공격에 보안 취약점을 가지고 있다. 특히 환자의 상태를 표현하는 중요 파라미터들의 위조, 누락, 변조는 환자 진단에 큰 영향을 끼칠 수 있다[6].

본 논문에서는 이러한 문제점을 해결하기 위해 재난 지역과 의료기관 간 Secure Virtual Private Network (VPN)을 구축하고 의료 데이터 전송에 필요한 적절한 IPsec 알고리즘을 구현하여 의료데이터 보안을 한층 강화시킨 위성 네트워크 원격 진료 시스템을 구성하였다. 아울러 새롭게 구성된 원격 진료 시스템에서 의료 데이터 전송 평가 및 의료 영상 임상 테스트를 실시하여 차후 인공위성을 이용한 원격진료시스템의 정책결정에 기반이 되고자 하였다.

Ⅱ. 재료 및 방법

1. 무궁화 2호 위성

무궁화 2호 인공위성은 지구와 36,000Km 거리에 떨어져 있는 정지궤도위성(Geo-stationary Earth Orbit)으로서 회전주기가 24시간이기 때문에 지구의 자전주기와 일치하여 정지된 것처럼 보이는 특징이 있다. 36,000Km 상공에 정지해 있는 인공위성에서는 지구면적의 43%가 내려다보이며, 이론적으로는 적당한 위치에 3개의 위성만을 띄워서 지구전역의 통신 중계를 할 수 있다(Fig. 1). 주파수는 Ku-band를 사용하며 대역폭은 400Kbps~3Mbps까지 보장한다(Table 1). 본 연구가 진행된 수원 위성관제센터에서는 최대 768Kbps의 서비스를 받을 수 있었다. 지상에서 신호를 위성체로 보내고, 다시 위성체에서 지상으로 오는데 걸리는 RTT(Round Trip Time)은 700ms 정도이다 [7-9].

Table 1. Specifications of Satellite Network

Orbit	the 116th degree of east longitude(35.786Km)
Weight	1.464Kg
Lunch Day	1996. 1. 14
Manufacture Co.	Lockheed Martin Astro Space(LMAS)
Lunch Service Co.	McDonnell Douglas
Band	Ku band(12~14Ghz)
Bandwidth	400Kbps~3Mbps (Suwon Control Tower:768Kbps)
RTT	700ms

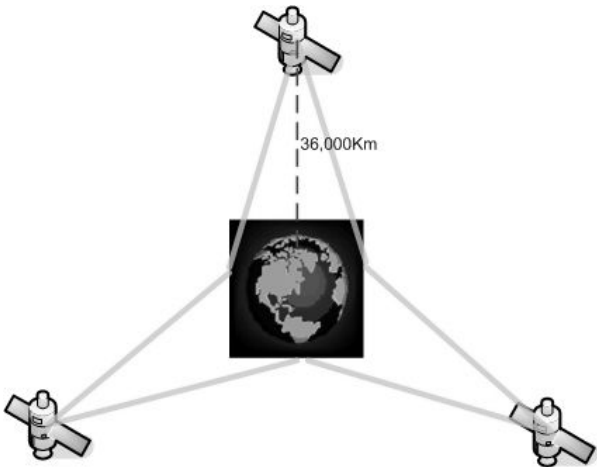


Figure 1. Geostationary earth orbits

2. 가상 사설망 및 IPSec 보안 프로토콜

(1) 가상 사설망 (Virtual Private Network)

VPN(Virtual Private Network)이란 공중망을 기반으로 구현된 가상의 사설망으로 보안성과 신뢰성, 관리 편이성, 사설 주소 지원, 우선순위 설정 등과 같은 기능을 제공하면서도 사설망에 비해 경제적인 네트워크 구성방식이다.

VPN을 형성할 수 있는 프로토콜을 각 계층별로 정

의된다. 네트워크 프로토콜을 터널링 프로토콜에 캡슐화하는 계층 2 터널링(L2TP, Layer 2 Tunneling)이 있으며 네트워크 프로토콜을 직접 터널링 프로토콜로 캡슐화하는 계층 3 터널링(Layer 3 Tunneling)이 있다. 이러한 터널링 프로토콜에 의한 보안 정책 형태는 통신의 각 계층에서 이루어질 수 있다. 계층 3 터널링 프로토콜인 IPSec은 IETF(Internet Engineering Task Force) 표준 프로토콜로서 IP 프로토콜을 사용하면서 키 관리, 인증, 암호화 기능을 제공하며, IPv4에서 구현이 가능한 보안 프로토콜이다[10-12].

(2) IPSec 프로토콜 (Internet Protocol Security)

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

AH는 접근 제어(Access Control), 비연결형 무결성(Connectionless Integrity), IP 데이터그램에 대한 데이터 발신 인증(Data Origin Authenti-cation) 등의 보안 서비스를 제공하며, 선택적으로 재전송 공격 방지(Anti-Replay) 서비스를 제공할 수 있다. 재전송 공격 방지 서비스의 경우는 기본적으로 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[13-15].

Figure 2는 IPSec의 동작모드를 나타낸다. 트랜스포트 모드(Transport Mode)에서는 TCP/UDP 헤더와 사용자 데이터 전체를 암호화하며, 터널 모드(Tunnel Mode)에서는 사용자측으로부터 발생된 패킷 전체를 암호화할 수 있다. 또한 IPSec 프로토콜의 AH, ESP에서 제공하는 인증과 암호화 프로토콜을 모두 사용해야 IP의 인증과 내부 데이터의 암호화를 모두 만족시킬 수 있다. [16]

3. 위성 네트워크 기반 원격 진료 시스템 구조

본 논문에서 제안한 위성 네트워크 기반 원격 진료 시스템은 Figure 3와 같이 위성 차량 (SNG, Satellite News Gathering)에서 응급환자의 멀티미디어 데이터 및 생체 데이터를 전송하는 환자측 시스템, 수원 관제센터, 환자 정보 데이터를 바탕으로 환자를 진단하는 의사측 시스템으로 구성되어 있다.

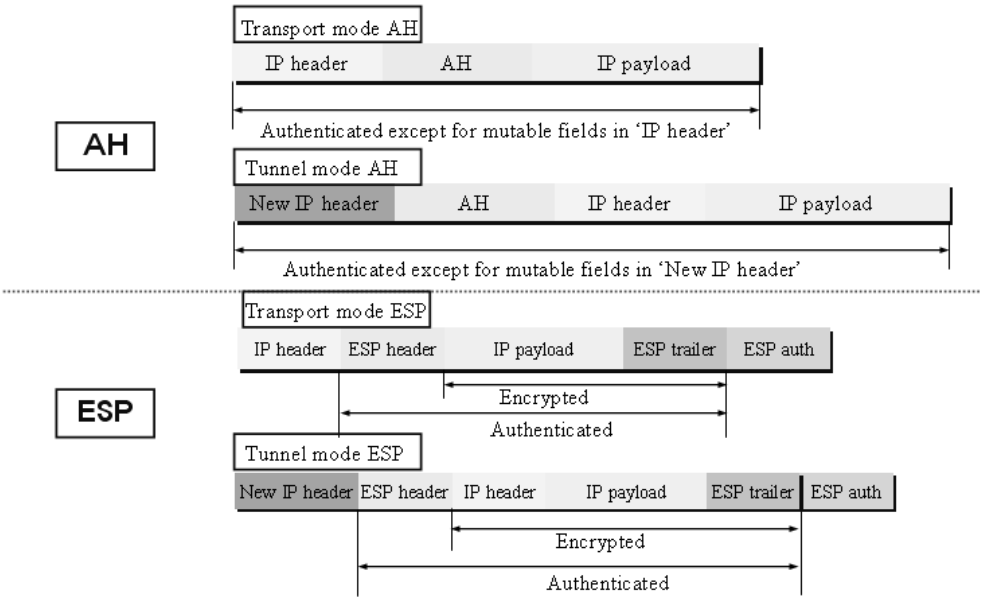


Figure 2. Operation Modes of IPSec

(1) 환자측 시스템

환자측 시스템은 의료 영상과 생체 신호, 방사선 영상을 의사측 시스템에 전송하며, 화상 회의를 통하여 응급의와 전문의 간 협업 진료를 지원한다. 생체 신호와 같이 중요한 데이터는 TCP/IP로 전송하며, 영상 데이터의 실시간 전송을 위해 UDP를 이용하여 전송한다. 의료 데이터의 전송 프로토콜은 다음과 같다 (Table 2).

1) 의료 영상

환자의 환부를 실시간으로 전송하여 전문의가 진단하는데 도움을 주는 실질적인 의료정보이다. 고화질 캠코더로부터 얻은 영상은 720×480의 해상도를 가지고 있으며 1프레임부터 30프레임까지 조절할 수 있다. 위성 네트워크의 낮은 대역폭을 충족시키기 위해 높은 압축률을 가지는 MPEG4(Moving Picture Experts Group 4)계열의 Xvid 코덱으로 압축하여 UDP를 사용하여 전송한다.

2) 생체 신호

생체 신호 데이터는 생체계측장비를 통해 환자의 심전도, 혈중산소포화도, 혈압, 호흡량의 생체 신호를 획득하고 획득한 생체신호 데이터는 실시간으로 의사측 시스템에 전송한다. 생체신호 전송은 MFER 표준을 이용한다. MFER은 의료분야 파형자료를 기술하기 위한 표준으로서 JAHIS(Japanese Association of Healthcare Information Systems Industry)에서 제안하였다. MFER은 간단하고 쉬운 구현을 가지며 다른 표준과 조화롭게 사용할 수 있다는 장점을 가지고 있다. 또한 재택 진료로부터 원격진료, 병원, 실험실에 이르기까지 폭넓은 적용범위를 가지고 있으며 생체신호의 인코딩 및 디코딩 방식을 표준화할 수 있어 계측 데이터의 교환과 분석, 재사용이 수월한 장점을 지니고 있다[17-18].

3) 방사선 영상

X-ray 또는 CT 이미지와 같이 환자의 의료정보가 담긴 DICOM 이미지를 환자측 시스템과 의사측 시스템 간 송수신할 수 있으며 상대편의 화면에 동일하게 표시되는 전송 이미지를 바탕으로 응급의와 전문의 간 의견교환을 할 수 있다. DICOM은 표준 Version 3.0은 의료화상 및 관련된 정보의 상호 인식에 필요한 공통의 데이터 집합, 데이터 표현 방법, 정보 이송 과정 등 상호 일치를 위해서 만들어졌다. DICOM 표준 3.0은 Figure 2와 같이 통신 프로토콜, 데이터 표현 운용절차 세 영역의 주제로 구성되어 있다. 데이터 표현 영역은 데이터 사전, 데이터 의미, 정보 객체 부분에

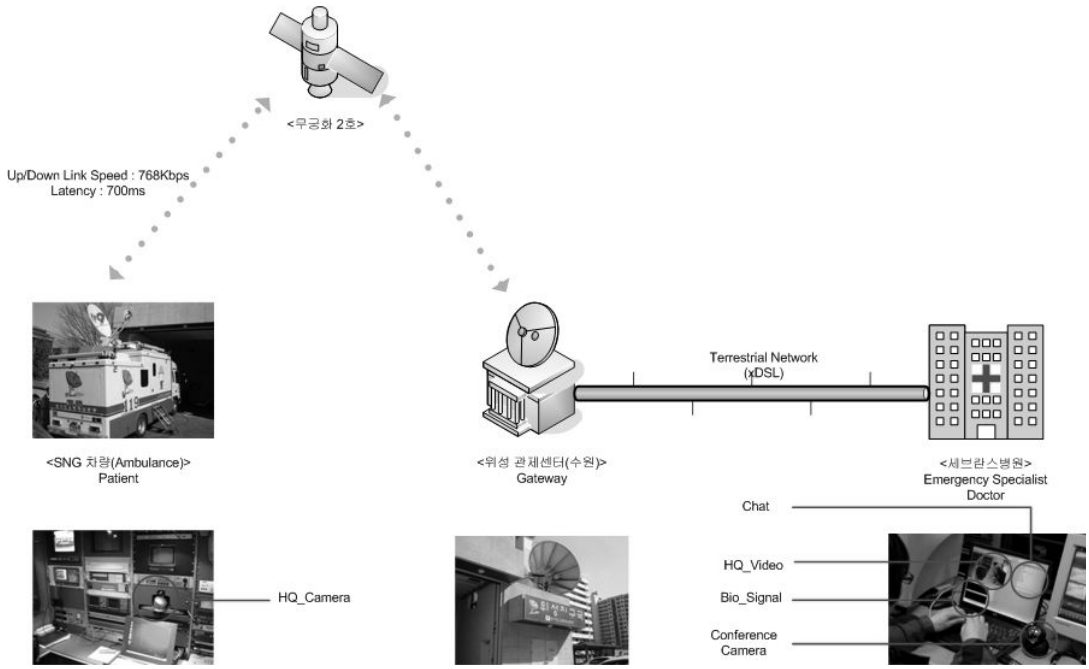


Figure 3. Scenario of Telemedicine System through the Satellite Network

정의되어 있고 운용절차 영역은 메시지 교환 부분과 서비스 객체 규격부분에 정의되어 있다. 그리고 통신 프로토콜 영역은 메시지 교환을 위한 네트워크 지원 부분과 메시지 교환을 위한 일대일 통신 지원 부분에 정의되어 있다[19-21].

4) 화상회의 시스템

화상회의 기능을 통하여 응급의와 전문의 간 원활한 협업진료를 할 수 있다. 화상 회의 영상 데이터는 H.263코덱으로 압축한 174×144 해상도의 QCIF(Quater Common Intermediate Format)영상을 전송하며 30프레임으로 고정되어 있다. 음성데이터는 GSM 6.10으로 압축하여 상대방에게 전송한다.

Table 2. Specifications of Healthcare Data

	Transmission Type	Correlation Time
High Quality Video	UDP	Real-Time
Bio Signal	TCP/IP	Real-Time
Radiograph	TCP/IP	Non Real-Time
Video Conference	UDP	Real-Time
Audio Conference	UDP	Real-Time

(2) 의사측 시스템

의사측 시스템은 환자측 시스템으로부터 전송받은 의료 데이터를 바탕으로 환자를 진단할 수 있도록 구성되어 있다.

4. 실험 환경

(1) 위성 네트워크 가상 사설망 및 보안 프로토콜 구축

위성 네트워크는 특성상 브로드캐스팅 방식을 이용하기 때문에 환자의 생체 정보를 전송하는데 보안상 큰 문제로 작용한다. 또한 긴 지연 시간과 높은 비트 에러율 역시 보안을 허술하게 하는 원인으로 지적되고 있다. 따라서 이번 연구에서는 Figure 4와 같은 형태로 VPN 터널링 프로토콜과 IPSec 알고리즘을 제안하였다[22-23].

(2) IPSec 보안 프로토콜 조합

보안에 강인한 원격진료시스템을 구축하기 위해 IPSec 프로토콜 구성 요소인 AH와 ESP 의 해쉬 함수 알고리즘에 변화를 주어 실험을 진행하였다(Table 3). AH에서 IP 인증을 위해 각각 MD5와 SHA-1를 적용하였을 때와 ESP에서 ESP 자체인증을 위한 MD5와 SHA-1이 사용되었을 때를 먼저 측정하였으며, AH와 ESP를 둘 다 적용 시켰을 때를 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. 마지막으로 AH, ESP 모두 인증을 사용하며, 3DES 알고리즘까지 적용하여 실험을 진행하였다[23-24].

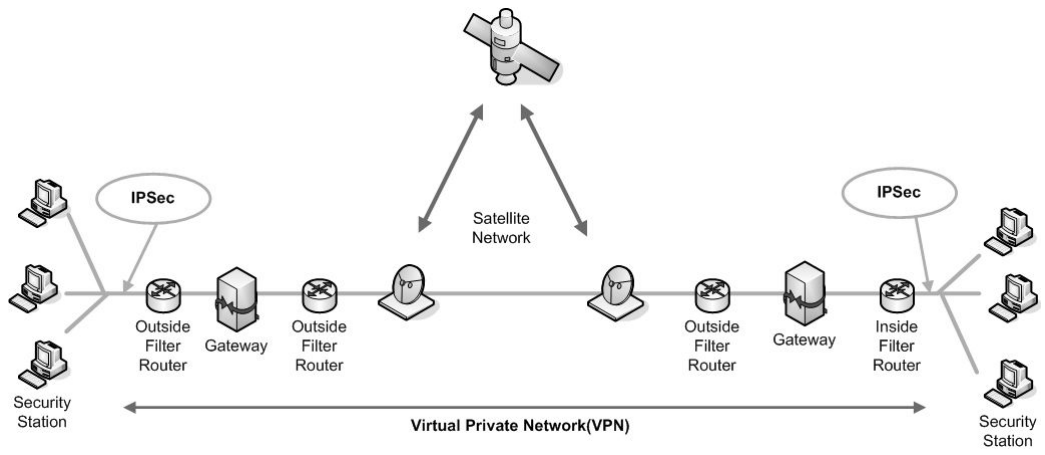


Figure 4. Applying for IPSec in Satellite Network

Table 3. Combinations of IPSec Algorithm

Case	AH		ESP		
	MD5	SHA-1	MD5	SHA-1	3DES
1	○				
2		○			
3			○		
4				○	
5	○				○
6		○			○
7			○		○
8				○	○
9	○		○		○
10	○			○	○
11		○	○		○
12		○		○	○
Non-IPSec					

Ⅲ. 결과

1. VPN 기반 IPSec의 프로토콜 적용

Figure 5는 IPSec을 적용 유무에 따른 Utilization을 나타낸다. AH의 MD5와 SHA-1과 ESP의 MD5와 SHA-1 알고리즘 중 각각 한 가지 알고리즘을 적용시켰을 경우 IPSec 프로토콜이 적용되지 않은 경우와 비교하여 약 2%의 하락하였다. SHA-1을 적용하였을 경우 조금 더 큰 하락값을 나타내었다. 각각 128비트의 해쉬를 생성하는 MD5(Message Digest)와 160비트의 해쉬를 생성하는 SHA-1(Secured Hash Algorithm) 메시지 압축 알고리즘의 메시지 인증 코드에 의하여 인증과 암호화가 진행되는데, 32비트만큼 해쉬 값이 더 큰 SHA-1이 더 많은 영향을 주는 것을 확인 할 수 있었다. 다음은 AH에서의 인증을 위해 1가지 알고리즘을 선택하였고, ESP의 3DES 암호화 알고리즘 1가지를 적용시켰을 때의 해당 Utilization을 나타낸다. 여기서 AH와 ESP 값은 각각 1가지씩의 알고리즘을 선택했으므로, 패킷 별로 AH의 해쉬 함수에 의한 헤더 값은 24Byte이고, ESP의 3DES 해쉬 함수에 의해 발생된 헤더값 또한 24 Byte이기 때문에 총 48Byte의 패킷 값을 IPSec에 이용되었다. 따라서 Utilization 값은 약 4.8~4.9% 까지 줄어들었다. Case 7과 8에서는 ESP 내부의 인증과 3DES 알고리즘을 적용시켰을 때의 측정값이다. 이때 패킷당 차지하는 암호화 바이트 수는 36Byte 이며, 인증에 12Byte가 사용되고, 24Byte가 암호화(Encryption)에 사용된다는 사실을 알 수 있다.

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

Figure 7은 IPSec을 적용하였을 시 RTT와 Jitter 값을 나타낸 것이다. IPSec 적용시 인증과 암호화에 필요한 패킷이 증가함에 따라 RTT와 Jitter 값도 증가하는 것을 볼 수 있다. 특히 MD5, SHA-1, 3DES 알고리즘을 모두 적용시켰을 때 RTT 측정값은 IPSec을 적용하지 않았을 때에 비해 0.38ms 이상 증가하였고 Jitter 값 역시 0.045ms 이상 증가하였다.

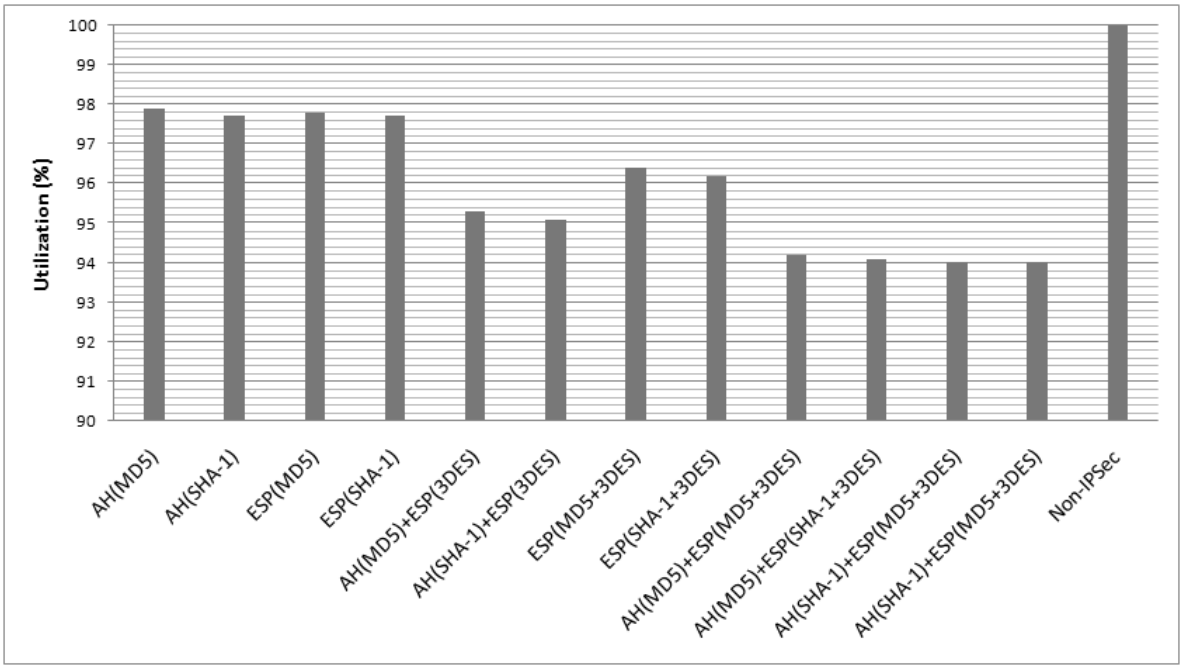


Figure 5. Utilization on the Case

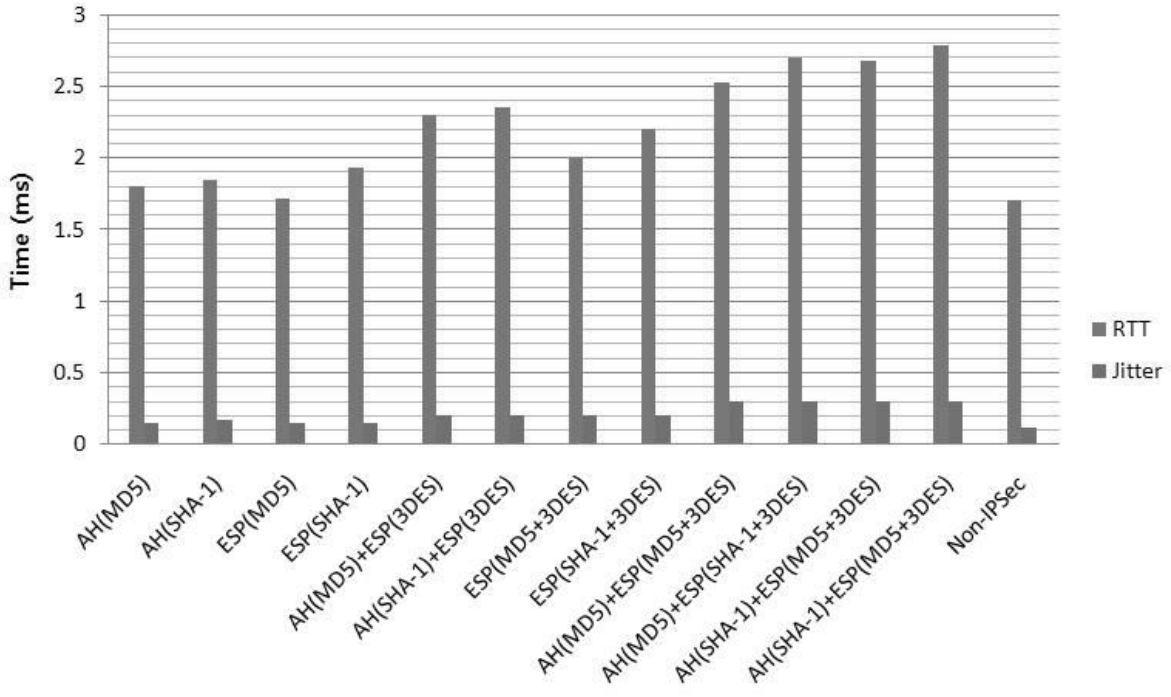


Figure 6. RTT and Jitter on the Case

2. 위성 네트워크를 이용한 원격진료시스템 구현

VPN 기반 IPSec의 프로토콜 적용 결과를 바탕으로 최저 지연시간을 유지하면서 최적화된 의료 데이터를 전송하기 위하여 AH(SHA-1)+ESP(3DES) 알고리즘을 선택하였다.

위 Figure 7은 IPSec을 적용하였을 때와 적용하지 않았을 경우 프레임별 의료 영상 데이터의 전송속도를 나타낸다. IPSec을 적용하였을 때 프레임 별로 약 3,2%~6%의 증가하였다 이는 AH와 ESP에서 패킷당 각각 24Byte의 오버헤드가 생겨 48Byte의 오버헤드가 가중된 결과라고 볼 수 있다.

원격진료시스템 구현 시 RTT와 Jitter의 측정값은 Figure 8과 같다. IPSec 프로토콜이 적용 되지 않은 상태에서 RTT와 Jitter는 각각 774.53ms, 25.2ms로 영상 전송 시 왜곡현상은 거의 보이지 않았다. 하지만, IPSec을 적용하였을 때 AH를 통한 인증과 64bit 마다 한 번씩 수행되는 3DES 알고리즘의 연산 수행 결과

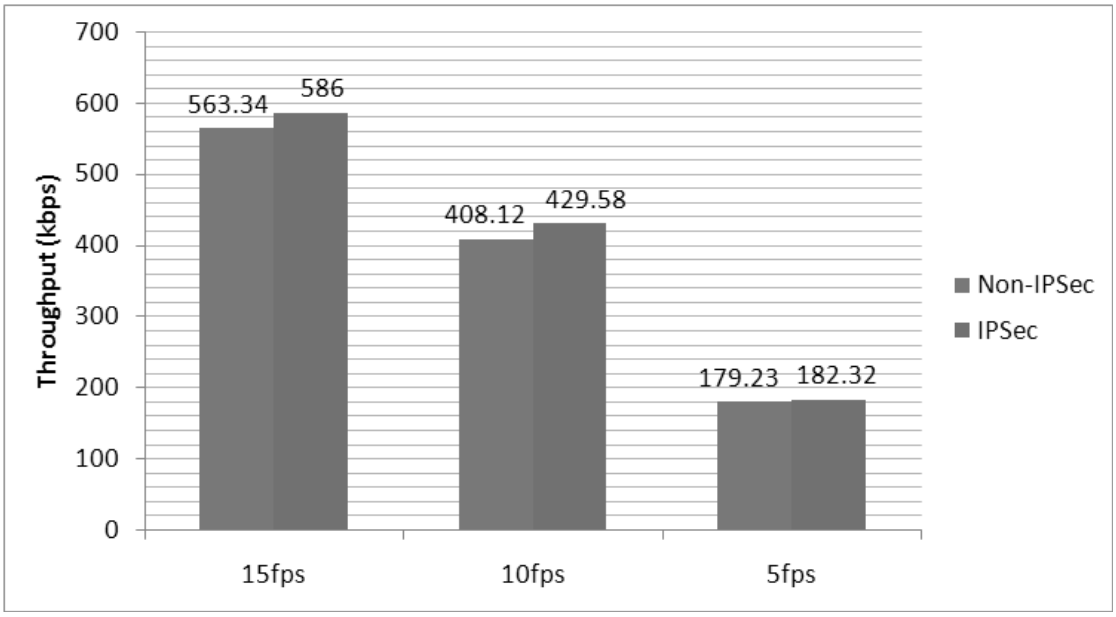


Figure 7. Throughput of Telemedicine through the Satellite Network

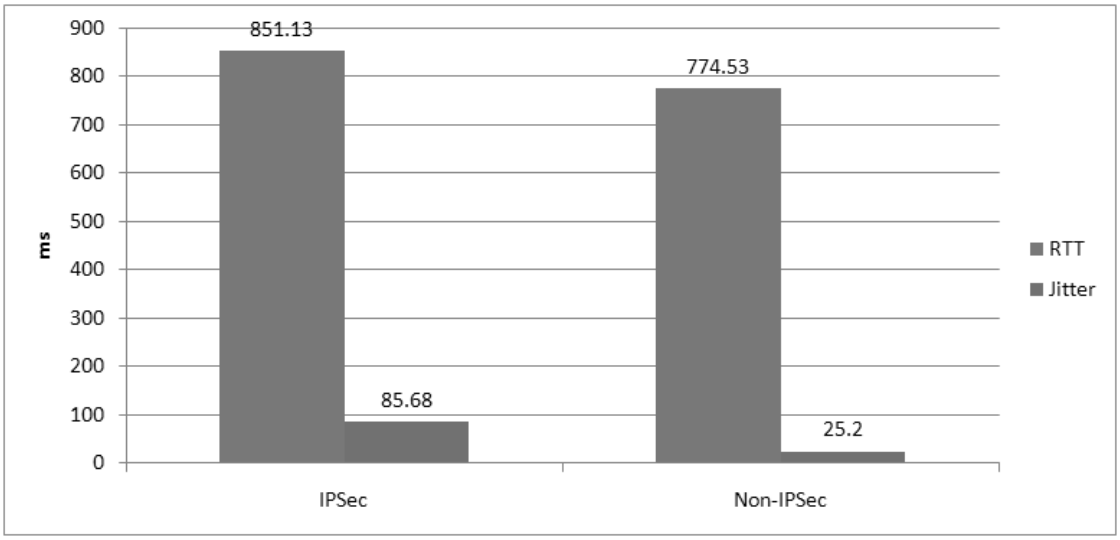


Figure 8. RTT and Jitter of Telemedicine through the Satellite Network

RTT 및 Jitter값이 급격한 증가하였다. IPSec의 AH, ESP 설정 시, 지연 값이 증가하는 이유 Figure 9와 같이 AH에서의 인증에 사용되는 해쉬 연산과정이 요구되며, ESP에서 제공하는 3DES 알고리즘은 64비트마다 수행되어 암호화 및 복호화 시간을 증가시키기 때문이다.

의사측 시스템은 환자측 시스템으로부터 전송받은 의료 데이터를 바탕으로 환자를 진단할 수 있도록 구성되어 있다. Figure 10은 보안 프로토콜을 적용하였을 때 의료 영상과 보안 프로토콜을 적용하지 않았을 때 의료 영상을 비교한 장면이다. 보안 프로토콜을 적용하였을 시 부분적으로 블러링 현상을 확인할 수 있었으나 응급 전문의가 외상 환자의 환부 위치, 깊이, 상태를 진단하는데 문제를 주지 않았다.

Ⅳ. 고찰

위성 네트워크는 기존 유무선 네트워크 인프라에 비해 구축비용이 많이 들기 때문에 일반적으로 활용되지 않으며 산간, 낙도, 오지 등에서 부분적으로 활용되고 있다. 따라서 지금까지 원격 진료 서비스에 관한 연구는 충분한 대역폭과 짧은 지연시간을 제공하는 다양한 유무선 네트워크 환경에서 주로 이루어졌으며 이처럼 제한된 위성 네트워크 환경에서의 원격 진료 서비스에 대한 연구는 제대로 이루어진 바 없다.

본 연구에서는 도심지역 내 기존 네트워크 인프라가 손상되어 위성 네트워크밖에 사용할 수 없는 최악의 재난 사태 시나리오를 가정하여 긴급한 치료를 요구하는 외상 환자의 의료데이터를 전송 및 평가하였다. 위성 네트워크는 기상상태나 주위 환경의 간섭전파에 의해 지연시간이 증가할 수 있으며 실제로 황사

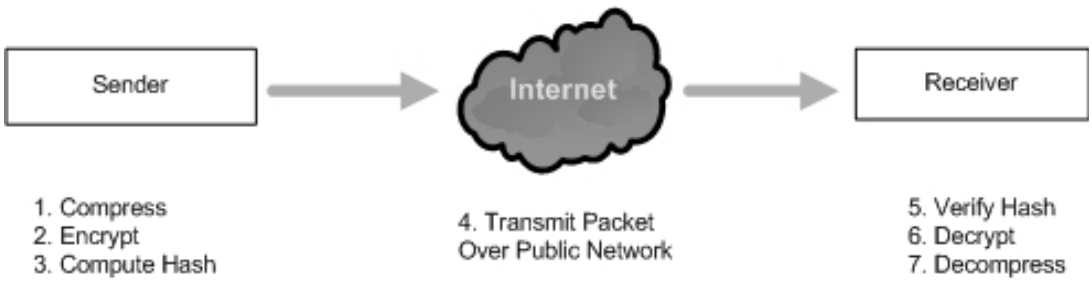
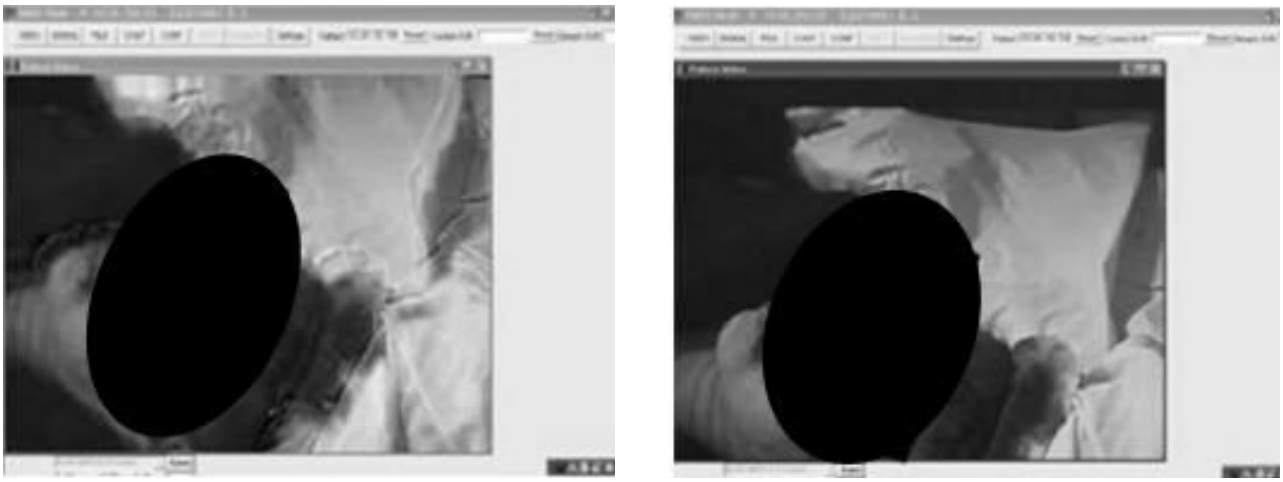


Figure 9. Factors of Latency



(a) IPSec (b) Non-IPSec

Figure 10. HQ_Video of Telemedicine System through the Satellite Network

에 의해 선형적으로 위성신호의 감쇄가 일어난다고 연구결과가 보고되고 있다[25]. 따라서 긴 지연 시간을 가지는 위성 네트워크 환경을 고려하여 최저 지연 시간을 유지하면서도 최적의 의료데이터를 전송할 수 있는 원격 진료 시스템 구성 모델을 구축하는데 중점을 두었다. 또한 가상 사설망 구축 및 보안 프로토콜 조합을 제안하여 위성 네트워크가 가지는 보안 취약점을 해결하고자 하였다. 보안 프로토콜 적용 결과 지연 시간 및 Jitter의 증가로 의사측 시스템에서 의료 영상 데이터의 블러링 현상을 확인할 수 있었으나 응급 전문의가 외상 환자의 환부 위치, 깊이, 상태를 판단하는데 문제를 주지 않았다. 본 연구를 통해 기존 네트워크 인프라가 손상된 재난 상황에서 위성 네트워크를 통한 원격 진료 서비스의 가능성을 확인하였다.

차후 연구에서는 의료 데이터 QoS 레벨 정책을 세워 기존 원격진료시스템이 제공하는 프레임 비율 변환 이외에 위성네트워크 대역폭을 고려한 해상도(Resolution) 및 컬러 정도(Color depth) 등을 제어할 수 시스템을 개발하고 이를 평가할 생각이다.

참고문헌

1. Mary Moore, The evolution of telemedicine, FGCS 15, 1999, pp.245-254
2. Sotiris A. Pavlopoulos and Anastasios N. Delopoulos, Designing and Implementing the Transition to a Fully Digital Hospital, IEEE Trans. Inform. Technol. Biomed. 1999;3(1);pp.6-19
3. Hiroshi Takeda, Kotaro Mianato, Takashi Takahasi, High quality image oriented telemedicine with multimedia technology, International Journal of Medical Informatics 1999;55;23-31
4. Mendoca EA. Chen ES, Stetson PD, Mcknight LK, Lei J, Cimino JJ. Approach to mobile information and communication for healthcare. International Journal of Medical Informatics 2004:73(1):25-34
5. 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, 2005;3:13-22.
6. L. Pierucci, D. R. Enrico, An Interactive Multimedia Satellite Telemedicine Service, IEEE Multimedia, 2000(4-6);76-83.
7. Timothy Pratt, Charles W. Bostian, and Jeremy E. Allnutt, Satellite Communications. 2nd ed. Wiley; 2002, pp421-423.
8. Xiamong Zhou, Baras, J. S TCP over GEO satellite hybrid networks, MILCOM 2002 Proceeding, 2002;1;29-34
9. Akyildiz, I.F.; Morabito, G.; Palazzo, S. , TCP-Peach: a new congestion control scheme for satellite IPnetworks. IEEE/ACM Transactions on networking, 2001;9(3); pp307-321
10. R. Venkateswaran, Virtual Private Networks, IEEE Potentials, 2001;20(1);pp11-15
11. Khanvilkar, S.; Khokhar, A. Virtual private networks: an overview with performance evaluation, IEEE Communications Magazine, 2004;42(10);pp146-154
12. W. Qu, S. Srinivas, IPSec-Based Secure Wireless Virtual Private Network, IEEE British Crown, 2002;1107-1112.
13. S. Kent, and R. Atkinson, IP Authentication Header, IETF RFC 2402,1998.
14. S. Kent, and R. Atkinson, IP Encapsulating security Payload (ESP),"" IETF RFC 2406,1998.
15. O. Elkeelany et al., Performance analysis of IPsec protocol:encryption and authentication, in: IEEE Communications Conference (ICC 2002), 2002, pp. 1164 - .1168.
16. C. R. Davis, H.W. Yeum, IPSec: Securing VPNs, Hanti media, 2001, 197-212.
17. J. P Kim, M.S Choi, H.K Park, J.W Choi, Development of Biosignal Telemonitoring System Based on HL7 and MFER Standard, J Journal of Korean Society of Medical Informatics, 2004;10(4):387-395.
18. S. Y Yoo, S. W Jung, J.W Choi, D. W Rho, Development of Ubiquitous Health Monitoring System, International Conference on Convergence Information Technology, 2007;11;1116-1120
19. J. S Nam, S, K Kim, Journal of Korean Institute of Information Scientists and engineers, The DICOM standard for PACS, 1996;14;4;30~38.
20. G. B Kwon, I. K Kim, Web-based Medical Information System supporting DICOM Specification, Journal of Korean Institute of Information Scientists and engineers, Computing Practice; 2001;7;4;317~323.
21. William R. Riddle, David R. Pickens, Extracting data from a DICOM file, Medical Physics 2005;32; 1537~1541;
22. Avesh K. Agarwal Wenye Wang, Measuring performance impact of security protocols in wireless

local area networks, Broadband Networks, 2005 2nd International Conference, 2005;1;581-590.
23. Christos Xenakis, Nikolaos Laoutaris, Lazaros Merakos, Ioannis Stavrakakis, A generic characterization of the overheads imposed by IPsec and associated cryptographic algorithms, Computer Networks: The International Journal of Computer and Telecommunications Networking, 2006;50(17);3225-3241
24. C. R. Davis, H.W. Yeum, IPSec: Securing VPNs, Hanti media, 2001, 122-135
25. W. P Hong, Y. S Chun, "A Study on the effects of Asian Dust to the Signal of Satellite Communication", Journal of Korean Institute of Electromagnetic Engineering and Science, 2004;15;8;722