유헬스케어의 무선환경에 적합한 WiMAX 보안 측정 및 분석

정윤수*

Measuring and Analyzing WiMAX Security adopt to Wireless Environment of U-Healthcare

Yoon-Su Jeong*

요 약 IT 기술에 의료기술이 접목되면서 유헬스케어 서비스에 적용한 체내삽입장치는 환자의 민감한 생체정보를 제3자에게 쉽게 유출되어 환자의 프라이버시 침해되지 않도록 무선 액세스 네트워크 구간에 높은 데이터율과 이동성을 지원하는 강한 보안이 필요하다. 본 논문에서는 이동성을 가지는 환자가 체내삽입장치내 환자의 생체정보를 무선 액세스 네트워크 구간에서 제3자에게 불법적으로 노출되지 않도록 무선 액세스 네트워크에 WiMAX 네트워크을 구축하여 이동 환자의 생체정보가 안전하게 송·수신될 수 있도록 테스트 베드를 구축하여 WiMAX 네트워크의 보안 성능 측정 및 평가를 수행한다. 특히, 본 논문에서는 WiMAX 보안 compliance, WiMAX MAC 상의 IPSec, MAC 계층에서 ECDH 수행 등에서 데이터 보안, MAC 제어 메시지 보안, 핸드오버 연결 지연, 프레임 손실 및 대역폭 등을 비교평가한다.

주제어 : 유헬스케어, 체내삽입장치, 와이맥스, 인증

Abstract Wireless access network section needs strong security which supports high data rate and mobility not to invade patient's privacy by exposing patient's sensitive biometric from automatic implantable device that is adapted to u-healthcare service. This paper builds test bed and performs assessment and measurement of security ability of WiMAX network to transmit and receive mobile patient's biometric by building WiMAX network in wireless access network not to expose paitne's biometirc at wireless access network section to the third person. Specially, this paper compares and assesses data security, MAC control message security, handover conection delay, and frame loss and bandwidth of ECDH at the layer of WiMAX security compliance, WiMAX MAC IPSec, and MAC.

Key Words : u-Healthcare, Implantable Medical Devices, WiMAX, Authentication

1. 서론

IT 기술의 발전과 함께 유헬스케어 서비스는 환자의 질병에 따라 다양한 종류의 소형, 휴대 가능한 장치들을 체내에 삽입하여 환자의 건강상태를 모니터링하거나 환자의 건강상태를 관리한다[1]. 유헬스케어 서비스는 건강진단이나 질별관리, 응급관리,의사와의 만남 등 기존 병원에서 이루고 있던 행위보다 더 편리한 형태로 사용자에게 활용되고 있다.

유헤스케어 서비스에서 사용되는 체내삽입장치는 심장질환이나 당뇨병과 같은 만성질환 환자에게서 폭넓게 사용되고 있다. 체내삽입장치는 무선 통신 수행능력을 가지고 있어 외부 프로그래머/병원관계자(의사, 간호사 등)과 무선 통신이 가능하다.

체내삽입장치는 무선 구간에서 무선 프로그래밍이 가능한 통신 인터페이스를 사용하기 때문에 제3자가 환자에게 근접하지 않고 의학 장비의 기능을 모니터링하고 변경할 수 있는 문제점이 있다[2,3]. 또한, 제3자는 체내

*목원대학교 정보통신공학과 조교수 : 교신저자
논문접수: 2013년 2월 20일, 1차 수정을 거쳐, 심사완료: 2013년 3월 15일, 확정일: 2013년 3월 20일

삽입장치의 도청뿐만 아니라 체내삽입장치의 리더 기능을 가지는 이동전화를 통하여 환자의 프라이버시 정보를 손쉽게 얻을 수 있다[4,5].

현재까지 연구된 체내삽입장치와 관련된 연구는 사용자의 정보를 개인이 관리할 수 있도록 개인정보 자기 통제권 확보 기술, 개인정보를 전송하고자 하는 대상자만이 해설할 수 있도록 암호화하는 방법 그리고 정보 활용 시 개인 정보를 통해 개인을 식별하지 못하도록 하는 익명화 방법 등을 중심으로 연구되어 왔다[6].

그러나, 이동성을 갖는 체내삽입장치를 부착한 환자의 의료 서비스를 지원하기 위해서 유헬스케어 서비스 환경은 의료 정보 서비스 확대 및 의료 도메인간의 데이터 교환 상호 호환성을 위한 환경으로 변화하고 있다. 이질적인 의료 도메인간 체내삽입장치내 저장된 정보를 교환시 안전하게 가용한 정보만을 송·수신할 수 있는 무선 접근 네트워크의 보안 강화가 필요하다.

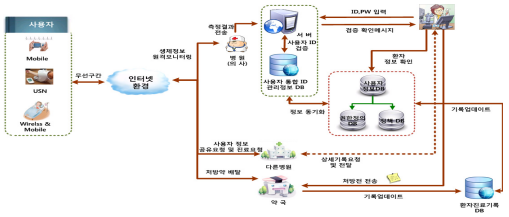
본 논문에서는 무선 액세스 네트워크 구간에서 제3자에게 체내삽입장치내 정보를 불법적으로 노출되지 않도록 안전하게 병원관계자에게 송·수신하도록 무선 액세스 네트워크 구간에 WiMAX 네트워크를 구축하여 WiMAX 네트워크 보안 성능을 측정 및 평가한다. 특히, 본 논문에서는 WiMAX 보안 compliance, WiMAX MAC 상의 IPSec, MAC 계층에서 ECDH 수행 등의 데이터 보안, MAC 제어 메시지 보안, 핸드오버 연결 지연, 프레임 손실 및 대역폭 등을 비교평가한다.

이 논문의 구성은 다음과 같다. 2장에서는 유헬스케어와 WiMAX 보안에 대해서 분석한다. 3장에서는 유헬스케어 환경에서 무선접근네트워크를 적용한 보안 모델을 제시하고, 4장에서는 WiMAX 네트워크로 테스트베드를 구축하여 WiMAX 보안 성능에 대한 효율성 및 안전성에 대하여 분석·평가한다. 마지막으로 5장에서는 이 연구의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

2. 관련연구

2.1 유헬스케어

유헬스케어는 정보통신 기술이 의료와 접목되어 환자의 생체정보를 병원관계자(의사, 간호사, 약사 등)가 실시간으로 모니터링하고 자동으로 병원 및 의사와 연결되어 시간과 공간에 구애 받지 않고 언제 어디서나 건강을 관리하는 의료 서비스를 의미한다[1,3]. 유헬스케어 서비스는 과거 전통적인 헬스케어의 영역에서 물리적, 시간적으로 제약되어 있던 서비스의 편리성을 높이기 위해 유·무선 온라인 네트워크를 활용하여 전자적 의료정보 및 진료 예약관리 등을 제공하던 e-헬스케어 단계에서 한 단계 더 진화된 서비스이다[1].

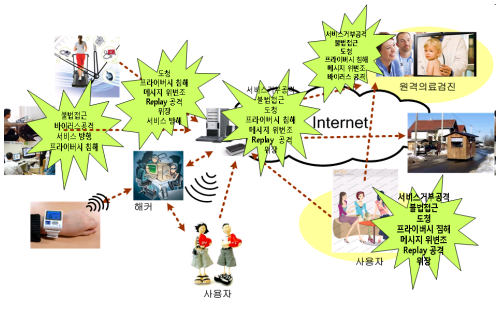


[그림 1] 체내삽입장치을 가지는 유헬스케어 서비스 개념도

그림 1은 유헬스케어 서비스에 대한 개념도이다. 그림 1에서 체내삽입장치는 환자의 생체 정보를 수집하기 위해서 환자 몸에 부착한 장치를 말한다. 환자와 병원관계자(의사) 사이는 WiMAX 네트워크 환경의 무선구간의 통신환경으로써 병원원관계자(의사)는 원거리에 있는 체내삽입장치를 부착한 환자의 생체정보를 요청한다. 병원관계자(의사)는 실시간으로 환자의 상태를 손쉽게 체크하기 위해서 체내삽입장치를 사용한다. 관리자는 병원관계자가 요청한 환자의 생체정보를 전송해주는 게이트웨이 역할을 수행한다. 체내삽입장치를 부착한 환자는 응급상황이 발생할 경우 타병원으로 진찰을 요청하거나 외부 장치를 통해 환자의 상태를 환자가 확인할 수 있다.

2.2 유헬스케어 보안 문제

유헬스케어 환경에서 이동성을 가지는 체내삽입장치를 부착한 환자의 생체정보를 병원관계자(의사, 간호사, 약사 등)에게 송·수신할 때 발생 가능한 보안 취약점과 위협 요소들은 그림 2와 같다[7,8].



[그림 2] 유헬스케어 환경의 보안 위협

그림 2처럼 유헬스케어 환경에서 발생가능한 보안 취약점은 서비스를 지원하는 서버를 공격하는 DoS 공격 유형, 바이러스/웜 해킹 공격 유형 의료정보 도청/위변조 공격 유형, 유·무선 인프라에서 가능한 여러 불법 접근 공격 유형, 오프라인을 통한 방범 시스템 고장 및 인위적인 기기 마비, 방해전파, 화재와 같은 인재 또는 악의적인 행위를 통한 공격유형 등이 있다.

최근 유헬스케어 보안 연구중에는 은폐장치나 소리 신호를 이용하여 체내삽입형 장치의 프라이버시 보호하는 연구와 액세스 접근 유·무와 알람을 이용하는 접근제어 연구 그리고 액세스 토큰이나 통신 위장자(Cloaker)같은 추가적인 외부장치를 사용하는 연구가 있다. 마지막으로 리더의 근접성이 검증되지 않은 체내삽입형 장치와 원거리 무선 상호작용이 거부되는 연구도 있다.

3. WiMAX 네트워크를 이용한 유헬스케어 환경의 보안 성능 평가

이 절에서는 유헬스케어 환경의 무선접근구간에서 제3자가 체내삽입장치를 부착한 환자의 생체정보를 불법적으로 수집하는 것을 예방하기 위해서 보안성이 강화된 WiMAX 네트워크를 무선접근구간에 구축하였을 때의 보안 성능을 측정 및 평가한다. 또한, 환자의 초기 인증과정이 끝난 후 환자가 일정 시간이 지난 후에 WiMAX 시스템에 재접속할 경우 환자는 초기 인증정보와 인증서를 이용하여 관리자의 추가적인 인증 과정을 수행하지 않고 WiMAX 서비스를 지원받기 위한 통신을 지원 받을 수 있도록 한다.

3.1 가정

유헬스케어 환경에서 무선 구간을 WiMAX 네트워크로 무선접근구간을 구축한 후 최적의 보안 성능을 얻기 위한 실험 모델의 가정은 아래와 같다.

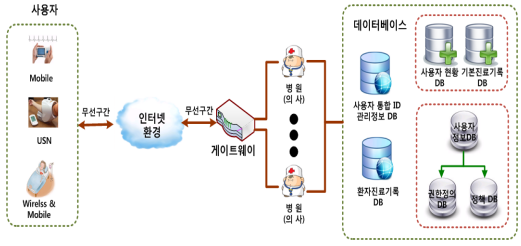
① 유헬스케어 서비스를 제공하는 각 서버의 이용율은 서버의 안정적 운영을 위하여 70% 수준으로 설정한다.

② 무선접근구간의 WiMAX 네트워크는 환자와 병원 관계자(의사, 간호사, 약사 등) 사이에 하나의 local 도메인으로 구성되며, WiMAX의 보안 성능은 실험 시간동안 동일하다.

③ WiMAX 네트워크는 한 개의 게이트웨를 통해 경유하여 인증서버에 접근한다.

3.2 모델설계

WiMAX 네트워크를 통해 병원관계자가 체내삽입장치를 부착한 환자의 생체정보를 안전하게 수집 및 검사하기 위한 모델은 (그림 3)과 같다.



[그림 3] 실험 환경

표 1은 WiMAX 네트워크에서 사용되는 표준 MAC 계층 보안과 IPSec의 연결 시간값을 나타내고 있다.

〈표 1〉 연결 시간

보안 기법	연결 지연시간
WiMAX MAC 보안만 사용	6 초
MAC 계층과 IPSec 보안 모두 사용	10 초

3.3 성능 평가를 위한 파라미터 설정

성능평가 실험을 위해 필요한 파라미터 설정값은 구성요소, Compliance, 주파수 명세서, 성능 분석자, OPNET 프레임 명세서, IPSec 등이 있으며, 서버의 평균 처리 시간은 CMS(Cryptographic Message Syntax) 처리시간, 등록 처리 시간, 인증 처리 시간, 연결 지연 시간 등의 프로세스 수치값을 합하여 구한다.

3.3.1 환자로부터의 인증요청

유헬스케어 환경에서 체내삽입장치를 부착한 환자를 인증하는 모델은 WiMAX 보안 compliance 표준을 사용하는 경우, WiMAX MAC 상단에서 IPSec을 사용하는 경우, MAC 계층에서 ECDH를 수행하는 경우 중에 선택하고 인증 서버의 서비스 입력 유형은 크게 인트라(Intra) 도메인과 인터(Inter) 도메인으로 분류한다. 인트라 도메인의 경우 평균 도착시간 간격을 0.17의 지수분포로 서비

스하는 유형을 말하고, 인터 도메인의 경우는 지역 도메인간의 평균 도착시간 간격을 0.5의 지수분포로 서비스하는 유형을 말한다. 인터 도메인과 인트라 도메인의 평균 도착시간 간격은 [ ]에서 사용한 수치값이다. 유헬스케어 환경에서 인증 서버가 사용자 인증을 처리하는데 소용되는 시간의 오차 범위는 서비스 환경에 영향을 줄 수 있는 여러 가지 요소들을 감안하여 ±5%의 이항분포로 설정한다.

3.3.2 암/복호 처리시간

WiMAX 네트워크에서 사용되고 있는 CMS (Cryptographic Message Syntax) 프로세스 시간은 ECDH를 이용한 Digital Signature와 RSA를 통한 암호화 처리시간를 사용하고 있으며, 암호 알고리즘에 사용되는 속도는 속도 Benchmarks를 참조하였으며, 각 암호화 알고리즘의 Signature와 Verification 수치는 암호화 알고리즘을 평가한 연구를 참조하였다[4,9].

3.3.3 등록/인증 수행 시간

등록메시지에 대한 환자별 평균 인증 처리시간은 각 환자별 프로세싱 시간을 가정하여 등록 요청하도록 하였으며, 인증서버는 병원관계자 수에 관계없이 동일한 수행시간을 갖도록 가정한다. 환자의 인증 메시지 등록 처리 시간은 WiMAX 성능 관련 결과를 참조하여 P-4.0GHz에서의 연산 속도 가정치를 구하면 표 2와 같다[10].

〈표 2〉 P-4.0GH에서의 연산 속도 가정치 단위: μs

처리시간 \ 서 버		인증서버	
		인터	인트라
평균 처리시간	등록 요구처리	38,100	824
	등록 응답처리		824

3.3.4 인증 수행시간

인증 수행시간은 512 비트의 키를 비밀키로 사용한다고 가정하고 해싱하는 총 길이는 1024비트t가 되고, ECDH 연산 시간은 327.541 MByte/Second(1,809.9344 bit/μs)이 된다. 1024 비트를 해싱하는 총 시간은 0.09μs가 되고, ECDH는 WiMAX 네트워크 구간과 인증서버 모두에서 이루어진다.

3.3.5 링크 통신시간

환자와 병원관계자(의사, 간호사, 약사 등) 사이의 구간에서 링크 통신시간은 [7,8]에서 실험한 실험 연구를 통해 얻은 링크 수치를 이용한다. 환자와 병원관계자(의사, 간호사, 약사 등) 사이의 구간은 환경에 따라 링크 통신시간이 변경될 수 있다고 가정하며, 본 논문에서는 다른 환경적 요소가 없는 것으로 링크 통신시간을 정하였다.

4. 평가

이 절에서는 유헬스케어 환경내 무선구간을 WiMAX 네트워크로 구축하여 환자와 병원관계자 사이의 무선구간에 대한 보안 성능을 평가한다.

4.1 실험환경

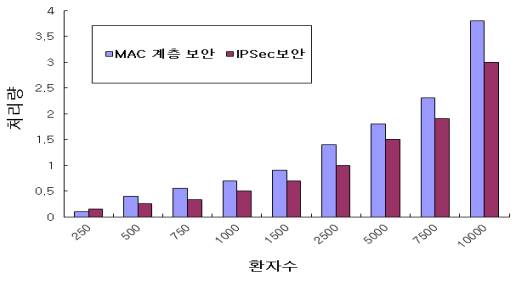
실험을 위해 사용되는 시뮬레이터는 OPNET을 사용하고, 실험에 사용되는 인증 메시지는 Intra/Inter 도메인에서 총 1만건이 요청되는 것으로 한다. 또한 실험 환경에서 인증 요청메세지가 모두 처리되는데 소용되는 시간은 총 8시간이며 실험 환경은 표 3와 같다.

〈표 3〉 실험 환경

구 분	내 용
시뮬레이션 툴	OPNET 4.0
인증 메시지 수	10,000
총 소요시간	8시간

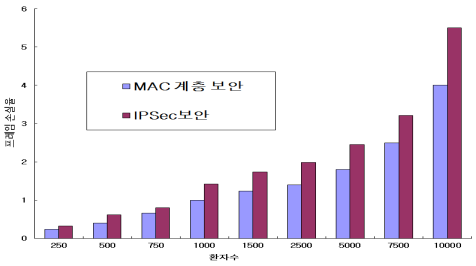
4.1 실험 및 결과

그림 4는 유헬스케어의 무선구간에 WiMAX 네트워크를 설치하여 MAC 계층 보안과 IPSec 보안을 적용하였을 때의 처리량을 비교분석한 결과이다. 실험 결과, IPSec 보안의 처리량이 MAC 계층 보안의 처리량 보다 3.7% 낮게 나타났다. 이 같은 결과는 각 프레임에 40바이트의 IPSec 헤더가 추가되었기 때문이다.



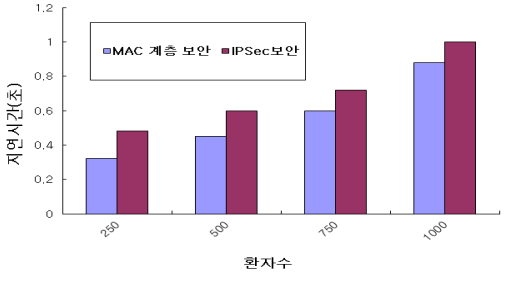
[그림 4] 처리량 실험

그림 5는 무선구간의 총 연결 수용능력 측면에서 프레임 손실에 대한 성능평가를 수행한 결과이다. 실험결과, 표준 MAC 계층 보안은 MAC 계층 오버헤드가 10바이트 정도의 작은 프레임을 드롭한데 반해 IPSec 보안은 IPSec 터널에 들어가기전에 40바이트의 IPSec 헤드가 추가되어 MAC 계층 보안보다 프레임 손실이 11.3% 높게 나타났다.



[그림 5] 프레임 손실 실험

그림 6는 서로 다른 링크 수용능력에 대한 트래픽의 평균 지연에 대한 실험 결과이다. 실험 결과, IPSec 보안이 MAC 계층 보안보다 2.8% 높은 지연 시간을 나타났다. 이 같은 결과는 동일한 무선 링크 수용량을 가지고 있다하더라도 무선 인터페이스이 들어가기전에 페이로드 크가가 계층 2와 계층3 헤더의 오버헤드가 추가적으로 증가하였기 때문이다.



[그림 6] 지연시간

5. 결론

체내삽입형 장치를 사용하는 유헬스케어 서비스의 환자 정보는 병원관계자(의사, 약사, 간호사 등)가 환자의 상태를 체크하기 위해서 이동성이 갖는 환자에게 환자의 생체 정보를 요청할 경우 무선 구간에서 병원관계자에게 전달될 때 안전성이 문제가 된다. 본 논문에서는 무선구간의 안전성을 보장하기 위해서 WiMAX 네트워크를 통해 환자의 생체정보를 병원관계자에게 전달될 수 있는 환경을 구축하여 WiMAX 네트워크의 보안성능을 수행하였다. 성능 평가 결과, WiMAX 네트워크에 MAC 계층 보안과 IPSec 보안를 비교평가 결과는 처리량은 IPSec 보안이 MAC 계층 보안 보다 3.7% 낮았지만 프레임 손실과 지연시간에서는 IPSec 보안이 각각 11.3%와 2.8% 높게 나타났다. 이 같은 결과는 IPSec 보안이 프레임 정보의 크기가 MAC 계층 보안의 프레임보다 크기 때문이다. 향후 연구에서는 다른 통신망과 연동하는 WiMAX 환경에서 발생되는 다양한 보안 공격에 안전한 통신 프로토콜에 대한 연구를 수행할 계획이다.

참 고 문 헌

[1] D. W. Kim, J. W. Han, and K. I. Chung(2008), "Trend of Home Device Authentication/ Authorization Technology", Weekly IT BRIEF, No. 1329, pp. 1-11.

[2] T. Denning, K. Fu, and T. Kohno(2008), "Absence makes ithe heart grow fonder: new directions for implantable medical device security", in Proc. of the 3rd Conf. on Hot topics in security, pp. 1-7, Jul.

[3] USPTO Patent Application 20080044014, "Secure telemetric link", http://www.freshpatents.com.

[4] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun(2009), "Proxymity-based Access Control for Implantable Medical Devices", 16th ACM conference on Computer and communications security, pp. 411-419, Nov.

[5] Z. Omary, f. Mtenzi, B. Wu, C. O'Driscoll(2010), "Accessing sensitive patient information in ubiquitous healthcare systems", 2010 International conference for internet Technology and Secured Transactions(ICITST), pp. 1-3, Nov.

[6] P. Inchingolo, S. Bergamasco, and M. Bon(2001), "Medical data protection with a new generation of hardware authentication tokens", in Proc. of Mediterranean Conf. on Medical and Biological

Engineering and Computing, pp. 12-15, Jun.
[7] T. Denning, Y. Matsuoka, and T. Kohno(2009), “Neurosecurity: Security and Privacy for Neural Devices”, Neurosurgical Focus, Vol. 27, Jul.
[8] D. Panescu(2008), “Emergingg technologies: wireless communication systems for implantable medical devices”, Engineering in Medicine and Biology Magazine, vol. 27, pp. 96-101, Mar.-Apr.

정 윤 수

- 2000년 2월 : 충북대학교 대학원 전자계산학 이학석사
- 2008년 2월 : 충북대학교 대학원 전자계산학 박사
- 2009년 8월~2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월~현재 : 목원대학교 정보통신공학과 조교수
- 관심분야 : 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
- E-Mail : bukmunro@gmail.com