WBAN 환경의 보안 요구사항 분석

장철순* · 한종욱**
*UST-ETRI, **ETRI

Security Requirement Analysis for WBAN environment

Chol-soon Jang* · Jong-wook Han**
*University of Science & Technology - ETRI
**Electronics and Telecommunication Research Institute
E-mail : jangcs99@etri.re.kr

요 약

최근 들어 헬쓰케어 서비스나 웨어러블 컴퓨터 등에 대한 연구가 진행됨에 따라 몸에 장착된 디바이스들을 무선으로 연결하기 위한 WBAN기술이 주목을 받고 있다. 향후 네트워크 환경은 개인의 다양한 생체정보 등을 기반으로 최적의 맞춤형 서비스를 제공하는 IT-BT-NT 융합서비스 환경으로 진화할 것이므로 WBAN기술의 활용성은 더욱 높아질 것이다. 따라서 본 논문에서는 안전한 WBAN 환경 구축을 위해서 발생이 예상되는 보안 이슈를 분석하고 이를 해결하기 위한 보안 요구사항을 제안하였다.

키워드

WBAN, u-Health, 개인의료정보, 정보보호

Ⅰ. 서 론

인구의 고령화로 건강에 대한 관심이 증가하게 되고, 양호한 건강 상태를 계속 유지하고자 언제 어디서나 개인의 건강관리 서비스를 제공받을 수 있는 u-Health 서비스에 IT-BT-NT 기술들이 집중되고 있다.

성공적인 u-Health 구현을 위한 핵심구성요소는 센싱(Sensing)부분, 모니터링(Monitoring)부분, 분석(Analyzing)부분, 피드백(Feedback)부분이며, 현재 기술 수준 및 의료서비스 형태를 고려해 볼 때, 센싱부분, 분석부분, 피드백부분에 많은 연구가 필요하다. 특히 센싱부분에서 WBAN (Wireless Body Area Network) 기술은 사용자의 활동영역인 가정(Home)과 이동(Mobile)환경에서 측정된 다양한 생체정보의 전송을 가능하게 한다.[1]

WBAN 환경에서 수집된 생체정보는 개인의 사생활보호 차원에서 매우 신중하게 취급해야 하며, 사람의 생명을 다루는 의료분야는 측정데이터의 신뢰성이 무엇보다도 중요하므로 정보보호 문제에 대한 중요성이 커지고 있다.

또한 WBAN 환경의 의료 서비스는 병원 내에서 벗어나 환자의 집이나 이동 공간을 포함한 생활공간으로 확대됨에 따라 새로운 보안 요구사항이 발생하게 된다.

본 논문에서는 WBAN의 개요와 연구 동향에 대하여 살펴본 후, 안전한 WBAN 환경 구축을 위해서 발생이 예상되는 보안 이슈를 분석하고 이를 해결하기 위한 보안 요구사항을 제안한다.

Ⅱ. WBAN

언제 어디서나 인간 중심의 맞춤형 서비스를 제공받을 수 있는 유비쿼터스 환경을 구축하기 위해서 WBAN은 인간으로부터 정보를 수집하고, 인간에게 최적의 서비스를 제공하는 대표적인 응용 기술이다.

WBAN은 사람이 착용하는 옷이나 인체의 여러 디바이스 간을 연결하여 통신할 수 있는 새로운 유형의 무선 네트워크로써 인체를 중심으로 센서, 통신, 구동체 등의 다양한 기술이 복합적으로 적용된 IT-BT-NT의 기술 융합 및 융합 산업 활성화에 필수적인 요소로 각광을 받고 있다.

현재 IEEE 802.15.6 TG BAN에서 주파수 분배, PHY/MAC 및 응용 서비스 등을 중심으로 표준화가 활발히 진행되고 있다.[2]

WBAN은 인간을 중심으로 모든 IT기술이 집중화, 융합화를 위한 연결 고리 역할을 수행할 것으로 예상된다. WBAN은 의료용 무선기술로 주목 받기 시작해서 디지털 가전 제어, 게임

interface, 스포츠, 다이어트를 위한 건강 모니터링 등 그 응용분야가 다양하며, 현재 비의료분야를 위한 WBAN과 의료분야를 위한 WBAN으로 구분하여 연구를 진행하고 있다.

WBAN은 인체 내·외부에 장착되는 장치들을 무선 네트워크 환경에서 연결하기 때문에 응용에 따른 다양한 전송속도와 전력소모를 요구한다. <표 1>은 WBAN의 응용을 의료 및 디지털 가전(비의료분야)으로 구분하여 전송속도에 따른 세부 요구사항들을 보여주고 있다.[3]

표 1. WBAN 응용에 따른 요구사항

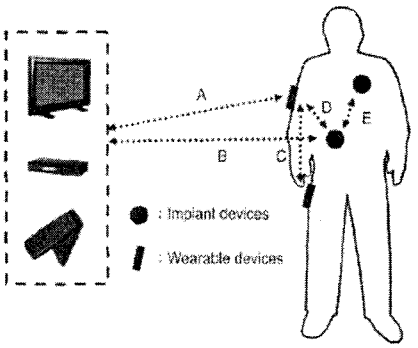
	저속/제어	중속/소리	고속/비디오
의료	·원격 진단 모니터링 ·당뇨병 모니터링 ·지능적인 약품 배달 ·병원의 환자 ·이식 장치 제어	·심장병 모니터링 ·태아 모니터링 ·EEG(24 lead) ·보청기 ·이식 장치 제어	·비디오 내시경 (lowRes) ·비디오 내시경 (HighRes) ·기타 비디오
디지털 가 전	·스포츠/휘트니스 ·휴대용 CE 제어 ·게임 제어(손동작) ·게임 제어(몸동작) ·애드혹(Ad-hoc)게임 ·스마트 키	·헤드폰 ·헤드셋 ·모션 캡쳐 ·데이터 기억장치	·원격 RGB 디스플레이

즉, WBAN은 응용에 따라 광범위하게 전송속도가 요구되며, 전력 소모량은 기존의 기술들보다 적으나, 응용에 따라 전력 소모량도 결정된다.

WBAN의 응용은 장착 형태에 따라 장착형(wearable)과 이식형(implant)으로도 구분할 수 있다. 장착형 BAN에서는 신호 감쇠나 차단에 의한 다중경로 문제와 사람의 이동성에 대해 주로 관심을 가지고 있으며, 이식형 BAN에서는 신체 조직과 피부조직에서의 각기 다른 경로손실을 해결할 수 있는 방안들을 활발하게 논의하고 있다.[3] 이식형 BAN은 미국, 일본 등지에서 의료용으로 할당된 400MHz 대역의 MICS(Medical Implant Communication Service)대역을 사용하며, 배터리 교환의 어려움 때문에 기존의 센서 네트워크 기술들에 비해 더 효과적인 저전력 기술이 요구된다.

WBAN 환경은 현재까지의 무선 네트워크 환경 중에서 인체 특성을 가장 많이 고려해야 한다. 높은 유전율과 도전율의 특성을 지닌 체내 매질을 고려한 네트워크 환경을 구현하기 위해 인체 매질에 의한 채널 특성의 변화를 고려한 안테나 설계가 WBAN 기술에서 우선시 되어야 할 것이다.

<그림 1>은 채널 특성에 따라 WBAN을 분류하고 각 통신 범위에서 활용될 응용분야를 보여주고 있다.



분류	내 용	응용분야
A	인체 외부와 인체 표면	바이오센서, 무선의료기기
B	인체 외부와 인체 내부	심장박동기, 소형로봇
C	인체 표면과 인체 표면	Wearable devices
D	인체 표면과 인체 내부	바이오센서, 캡슐내시경
E	인체 내부와 인체 내부	소형로봇, sensor network

그림 1. 채널 특성에 따른 WBAN 분류

이식형 장치를 이용한 B, D, E 채널의 경우는 주로 의료용, 장착형 장치를 이용한 A, C 채널의 경우는 엔터테인먼트 등의 용도로도 활용될 가능성이 높다. 특히 장착형 장치간의 통신을 이용한 C채널의 경우 여러 형태의 서비스를 제공할 수 있는 가능성을 제시한다.[4]

<표 3>는 WBAN의 다양한 기술적인 요구사항들을 나열하고 있다.

표 3. WBAN 기술 요구사항

항 목	내 용
전송거리	최대 3m
전송속도	1kbps~10Mbps
사용 주파수 대역	MICS, UWB, ISM
Topology 및 Piconet 밀도	멀티홉 지원, 2 ~ 4개의 네트워크/m^2
네트워트당 최대 센서 및 디바이스 개수	100
Duty Cycle	0.1 ~ 100%
전력 소모	1m 거리 통신시, 배터리 소모전력 1mW/Mbps
보안	사용자 인증, 암호화
안전성	SAR(Specific Absorption Ratio)용 규제 요구사항 만족
위치정보	수cm 이내의 위치 측정

WBAN은 3미터 이내의 통신거리와 최대 10Mbps의 전송속도를 요구하며, 가능한 주파수

대역으로 의료 서비스 주파수인 MICS(Medical Implant Communication Service), MEDS(Medical Data Service), WMTS(Wireless Medical Telemetry Service) 등과 저전력 주파수 인 ISM(Industrial, Scientific & Medical), UWB(Ultra Wide Band) 대역이 고려되고 있다.

특히, WBAN은 사람의 생명에 직접적인 영향을 줄 수 있기 때문에 EMC, SAR(Specific Absorption Ratio) 등을 고려한 높은 신뢰성과 안전성이 요구되며, 이를 위한 토폴로지는 멀티 홉을 지원하고, 암호화 및 인증 등의 보안 기술과 초저전력 네트워크 및 통신 기술이 요구된다.[5]

WBAN은 초기에 센서 네트워크의 한 분야로 연구가 시작되면서, 최근에서야 학문적 중요성과 다양성을 인정받아 WBAN만의 표준화가 활발하게 진행되고 있다. 2007년 11월 IEEE 802.15.6 TG BAN으로 승격되면서 2009년까지 표준화가 진행될 예정이며, 국내에서도 2008년 2월에 전파통신기술위원회(TC3) 산하 WBAN 프로젝트 그룹(PG317)이 구성되어 아래와 같은 과제를 선정하여 WBAN 표준화 활동을 진행하고 있다.[6]

- QoS 보장형 MAC
- 인체특성을 고려한 채널 모델링
- WBAN 주파수 이용 표준
- WBAN응용서비스(디바이스 프로파일)
- 인체내부와 외부간의 PHY/MAC 및 네트워크 프로토콜

III. WBAN 보안 요구 사항 분석

WBAN은 3m 이내의 비교적 짧은 통신범위에서 전송이 이루어지기 때문에 상대적으로 보안 위협 범위도 좁아지는 이점이 있다. 하지만, 취약한 무선 네트워크 환경과 중요한 개인(의료)정보의 취급은 높은 보안 요구사항을 필요로 한다.

본 장에서는 u-Health 서비스를 중심으로 WBAN의 보안 위협을 분석하고 이를 해결하기 위한 보안 요구사항에 대하여 기술하고자 한다.

1. WBAN 환경의 보안 위협

WBAN 환경에서 발생할 수 있는 보안 위협을 데이터, 접근 제어, 서비스 관점으로 구분하여 설명한다.

1.1 데이터 보안 위협

WBAN 네트워크 환경에서 전송되는 데이터 중 개인의료정보는 사적인 영역의 매우 민감한 정보로 의사가 환자에 대한 의료행위를 하면서 수집된 자료들과 이 자료들을 기초로 연구 분석된 정보들을 포함한다.

미국 HIPAA(Health Insurance Portability and Accountability Act)의 프라이버시 규정은 전자화된 의료정보를 포함한 모든 유형의 의료정보를 보호 대상으로 하여 개인의료정보의 프라이버시 보장에 관한 중요성을 강조하고 있다.

개인의료정보 보호에 대한 위협은 정보보호의 3 요소 즉, 기밀성, 무결성, 가용성으로 구분하여 설명할 수 있다. 환자 진료정보나 개인정보에 대한 권한이 없는 자의 접근이나 정보유출로 인한 기밀성 침해, 의료정보의 손실이나 파손 등 무결성 침해로 인한 환자 생명에 대한 위협, 적절한 시기에 필요한 정보서비스 제공의 불가 등 가용성 침해가 있다.

특히, 개인의료정보의 무결성 침해로 부정확한 정보를 제공할 경우, 환자 진료 시 생명까지 위협하는 막중한 위험을 초래할 수 있다.[7]

1.2 접근 제어 보안 위협

WBAN 환경에서 인체 내·외 및 인터넷망의 연결은 중앙장치(Central Device)를 통해 제어 및 관리가 이루어진다. 중앙장치는 MBU(Mobile Base Unit) 유형으로 인체와 접한 여러 휴대 장치이며, 현재 휴대폰이 최적의 장치로 예상된다.

중앙장치의 절도나 분실은 기밀성에 대한 위협으로 공격자가 접근해서는 안 되는 정보를 접근 및 수신할 수 있게 된다. 또한 중앙장치에 저장된 MAC 주소 등과 같은 다양한 인증정보를 소유로 인한 다른 네트워크 침해로 이어질 수 있다.

WBAN 환경은 원격 진료 등과 같은 양방향 통신이며, 개인마다 형성되는 수많은 WBAN 과의 일시적이고 불확실한 연결을 제공한다. 그래서 비합법적인 자의 접근이 발생하고, 기존의 인증 기술로는 빈번한 인증 요청에 따른 불편함과 접근 권한 관리에 어려움이 발생한다.

1.3 서비스 보안 위협

WBAN 환경은 사용자에게 최적화된 다양한 서비스를 제공하는 한편, DoS(Denial-of-Service) 공격 위협에 노출되어 있다. WBAN 환경은 망구조가 고정되어 있지 않으며 수시로 망구조가 변경되기 때문에 임시로 구성된 노드들 간 데이터 교환을 위해서는 멀티 홉 라우팅 프로토콜에 의존하며 노드들은 인접한 노드의 패킷을 전송해 주어야 한다. 하지만 노드들 중 하나의 협력을 거부할 경우 DoS 공격으로 이루어진다.

또한 WBAN 환경에 사용되는 장치들은 제한된 자원 안에서의 운영으로 인한 배터리 소진 공격에 노출된다. 공격자는 계속적으로 제한된 자원을 가진 장치에 데이터 전송 요청이나 네트워크 연결 요청을 보냄으로 장치가 제대로 기능을 할 수 없게 된다.

이러한 공격은 네트워크 보안을 침해하지는 않지만, 장치의 기능을 마비시키는 가용성의 침해로, 특히 의료 서비스 분야에서는 생명과 직관되는 관계로 치명적인 피해를 초래하게 된다.

2. WBAN 환경의 보안 요구 사항

앞 절에서 기술된 WBAN 환경에서의 보안 위협에 대처하기 위해서는 기본 보안 서비스인 기밀성, 무결성, 인증 외에도 <그림2>와 같이 부인방지, 권한관리, 가용성, 안전한 핸드오프 등의 보안 요구사항이 추가 제공되어야 하며, 높은 보안 수준을 유지하여야 한다.

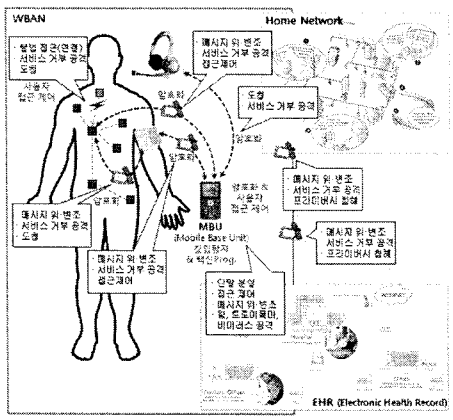


그림 2. WBAN환경에서의 보안 요구 사항

첫째, WBAN 네트워크 환경에서는 생체정보 등의 중요한 개인 정보를 취급하기 때문에 모든 트래픽 데이터를 포함해 장치에 저장되는 데이터까지 암호화해야 한다. 또한 WBAN은 여러 제약조건이 있는 환경에서 다양한 기술들이 서로 연결되므로, 각각의 환경에 적용될 채널에 따른 최적화 된 보안 수준과 경량화 된 암호 알고리즘이 자동적으로 결정되어야 한다.

둘째, WBAN 기술은 특정 공간이 아닌 정상적인 생활공간 안에서 수집된 생체 정보를 포함한 정확한 개인의료정보로 신뢰성 있는 의료서비스를 제공하는 기반이 된다. 정확한 개인의료정보를 보장하기 위해서는 메시지의 무결성을 유지하고, 불확실한 연결에서 제공되는 부정확한 데이터 및 DoS 공격으로부터의 서비스 차단을 방지할 수 있는 인증 및 자원 관리 솔루션이 개발되어야 한다.

셋째, WBAN 환경은 센서 네트워크 등 다양한 소규모 네트워크들의 집합 형태로써 중앙장치를 통한 모든 네트워크 제어 및 관리가 이루어진다. 특히 인터넷 등의 외부망과의 접속시 발생되는 트로이목마, 웜, 바이러스 등의 위협은 가용성에 영향을 미칠 수 있고, 기밀성, 무결성에도 침해를 가할 수 있으므로 철저한 침입 탐지 및 백신 프로그램 개발이 필요하다.

마지막으로 사용자는 WBAN 환경에서 개인, 병원, 각종 기관 등의 다양한 서비스가 제공받는다. 따라서 수많은 사용자와의 자원 공유가 불가피하기 때문에 공유된 자원 및 서비스에 대한 기밀성, 사용자 정보 접근 제어, 서비스 제공자의 신뢰성 검증 등 어플리케이션 계층에서 사용자의 편리성을 고려한 시스템이 개발되어야 한다. 또한 WBAN은 모든 서비스가 무선 공중망을 통해 제공되므로 핸드오프 과정에서 보안 접속 유지와 보안 컨텍스트 정의 및 관리 등을 고려하여 안전한 핸드오프 기술이 제공되어야 한다.

Ⅳ. 결 론

현재 WBAN 기술은 국내·외적으로 활발한 활동으로 표준화가 진행되고 있다. WBAN은 의료분야를 비롯해 인간이 활동하는 모든 영역에서 활용될 것으로 전망된다.

본 논문에서는 WBAN 정의 및 표준화 동향을 살펴본 후, WBAN 환경에서의 보안 위협을 데이터, 접근 제어, 서비스 관점에서의 분석과 보안 요구사항을 제안하였다.

향후 연구 과제로는 WBAN 표준화에 발맞춰 네트워크 각 계층에 상응하는 보안 프로토콜 구현, 보안 수준에 맞는 암호 알고리즘 및 키 관리 시스템 설계 등의 연구가 포함될 것이다.

참고문헌

[1] 지경용 외, 유비쿼터스 시대의 보건의료, jinhan M&B, pp.156~164, 2006
[2] Application Class Structure, IEEE802.15-15-08-0096-00-0006
[3] 장병준, Trend on BAN with Bio-sensor for Early Detection, KRnet 2007
[4] 윤영종, 이상훈, 김기준, WBAN안테나 설계 기술, 한국통신학회지(정보와통신) 제25권 제2호, pp.32~40, 2008. 2
[5] Frequency band consideration of SG-MBAN, IEEE 802.15-07-0640-10-0ban
[6] 신준호, 시험인증기술동향 WPAN/WBAN, TTA저널 No.116, pp.114~118, 2008. 3-4
[7] 김동수, 김민수, e-Health 시대의 진전에 따른 의료정보보호 쟁점 및 정책방향, 정보화정책 제13권 제4호 pp.128~148, 2006년