항공응급의료 환경에서 환자 개인정보의 보안 전송에 관한 고찰

Study on Security Transmission of Personal Patient Information in Aerial Emergency Medical Environments

김순석*, 이용희*, 김동호*, 정호영**, 박세일**

Soon-Seok Kim*, Yong-Hee Lee*, Dong-Ho Kim*, Ho-Young Jeong**, and Se-Il Park**

요 약

항공응급의료 환경에서 기본적인 서비스 모델은 응급구조헬기 내에 장착된 각종 의료장비들로부터 게이트웨이로 수집된 환자 개인건강정보들을 최종 목적지인 후송 병원에 전송하는 과정이라 볼 수 있다. 본 논문에서는 이 과정에서 의료장비에서 게이트웨이로 환자개인정보를 전송시 가장 안전한 전송방식에 대해 고찰하고자 한다. 또한 국제 표준인 ISO/IEEE 11073을 기본 모델로 하여 기존에 나와있는 여러 전송 방식들 중 항공응급의료 환경에 가장 적합한 보안 전송 방식을 비교 분석하여 그 대안을 제시하고자 한다.

Abstract

The basic service model is to be process transmting patient health information from various medical devices to evacuation hospital through gateway collecting it in aerial emergency medicine environments. In this paper, we study on the most secure transmission scheme in case that personal patient informations are transmitted from medical devices to gateway. Moreover we compare and analyze existing methods on secure transmission and suggest an optimal alternative on the basis of international standard, ISO/IEEE 11073.

Key words : Aerial emergency medical, Patient information security, Security transmission, IT convergence

I. 서 론

도서나 산간 오지 등에 살고있는 노인이나 임산부 등 응급 환자의 경우, 헬기 등을 이용한 신속한 구조나 의료 서비스를 요구한다. 이때 헬기 내에는 응급 구조 활동을 위한 다양한 의료 장비가 갖추어져 있는 것이 필수적이다. 이러한 의료장비 들은 심장제세동기와 같은 독립된 형태의 성격을 띤 것도 있지만 산소포화도 측정이나 체온, 혈압, 맥박, 심전도와 같은 진단이나 검사를 위한 장비도 있다. 우리는 흔히 후자와 같은 이러한 장비들을 일컬어 개인건강의료장비(PHD, Personal Health Device)라 부른다[1]. 이러한 장비들은 대개 진단이나 생체 신호

* 한라대학교 컴퓨터공학과(Department of Computer Eng., Halla University)
** 한라대학교 정보산업대학원(Graduate School of Information and Industry, Halla University)
· 제1저자 (First Author) : 김순석
· 투고일자 : 2011년 12월 12일
· 심사(수정)일자 : 2011년 12월 13일 (수정일자 : 2012년 2월 23일)
· 게재일자 : 2012년 2월 28일

의 측정과 같은 본연의 역할도 있지만 그 외에 헬기 내에서 측정된 응급 환자의 생체 정보를 후송 목적지 병원에 소재하고 있는 응급의료센터에 전송하는 역할도 수행하고 있다.

그 이유는 응급환자의 경우 현장에서 실시하는 응급처치가 가장 중요하지만 병원과 연계하여 환자의 생체 정보를 실시간으로 전송하고 파악하는 것이 후송 후 병원에서의 응급 치료에 큰 도움이 되기 때문이다.

대개 환자의 정보라 함은 이러한 진단이나 측정 장비를 통해 전달되는 개인 생체 정보를 생각해 볼 수 있지만 그 외에도 환자의 개인 프라이버시와 관련된 환자 식별 정보라든가 나아가 과거 병력 정보 등을 통칭하여 생각하는 것이 일반적이다.

최근에는 단순한 환자의 치료에 관한 범위를 넘어서서 환자뿐 아니라 일반 개인의 건강차원에서 질병을 사전에 예방하고 관리하는 것을 보다 중요하게 여기는 추세이다. 이를 대표적으로 표현한 것이 유헬스니 헬스케어라는 용어이다.

유헬스 또는 헬스케어의 차원에서 생각해보면 앞서 언급한 응급환자는 과거 병력정보라든가 현재의 건강정보 등이 구글헬스[2]나 마이크로소프트사의 헬스볼트[3] 등 인터넷 포털사이트를 통해 이미 지속적으로 저장되고 관리되어오고 있을 수도 있다. 이러한 환자나 개인의 건강정보를 개인건강기록(PHR, Personal Health Record 또는 EHR, Electronic Health Record)[4]이라 부른다.

현대, 그리고 가까운 미래의 의료 서비스는 단순히 환자 개인에 대한 그때그때의 치료가 아닌 질병 예방이나 평생 건강관리차원에서 보다 폭넓게 작용하게 될 것이다.

따라서 앞서 언급한 헬기 내의 응급 환자는 그동안 지속적으로 저장 관리된 개인건강기록이 포털 사이트에 존재할 수 있으며 후송된 병원에서는 기존 개인건강기록과 헬기 내에서 측정된 실시간 생체 정보를 종합하여 가장 최적의 치료를 이끌어 낼 수 있을 것이다.

최근 국제표준화기구인 ISO의 의료정보관련 기술위원회인 TC215에서는 이러한 종합적인 환자 개인정보관리를 위해 일명 세계 공용 건강관리 아이디(UHID, Universal Healthcare Identifier)[5]라는 국제적으로 통용된 환자의 개인 ID를 표준으로 제정하고 있는 추세이다.

본 연구는 앞서 언급한 헬기 내에서 개인건강의료장비인 PHD 장비를 통해 측정된 환자 개인의 생체정보를 후송 병원 내 응급의료센터로 실시간으로 전송시 현재 국제 표준화된 흐름과 연계하여 프라이버시 보호 차원에서 보다 안전하게 전송하기위한 방법들을 고찰해보고 그 대안을 제시해 보고자 한다.

본 논문의 2장에서는 관련 연구로 현재 의료환경에서 환자개인정보의 보안 전송과 관련한 국제적인 표준화 동향들을 살펴보고 3장에서 보안 전송을 위한 기술적인 차원에서 그 대안을 모색한 후 4장을 끝으로 결론을 맺고자 한다.

Ⅱ. 관련 연구

본 장에서는 앞서 서론에서 언급한 응급의료환경에서 개인건강의료장비로부터 측정된 생체의료정보를 후송 병원으로 전송하는 부분에서 보안 전송과 관련한 국제 표준화 동향 및 기술적인 동향에 대해 살펴보고자 한다.

앞서 언급한 ISO TC215 WG7에서는 주로 의료장비와 관련한 표준화 작업을 수행하고 있다. 그 중 최근 발표된 ISO/IEEE 11073의 경우 심전도계, 산소포화도측정기, 체온계, 혈압계, 체중계와 같은 각종 개인건강의료장비로부터 측정된 생체 정보를 수집하여 게이트웨이로 전송하는 부분과 관련된 표준이다. 이렇게 수집된 각종 생체정보는 게이트웨이를 통해 병원으로 전송된다. 이때 게이트웨이는 스마트폰이나 스마트탭과 같은 이동형 단말기일 수도 있고 노트북이나 PC와 같은 고정된 형태일 수도 있다. 만일 헬기와 같은 응급의료의 경우는 아마도 이동형 단말기를 이용하여 CDMA나 3G와 같은 기존 이동통신망을 통해 전송하는 것이 가장 효과적일 것이다. 또한 게이트웨이로부터 후송 병원까지의 전송부분은 HL7[6]이라는 국제표준기구에서 담당하고 있다. 이들 관계를 정리하면 [그림 1]과 같다.

한편 개인건강의료장비인 PHD 장비들과 게이트웨이간의 전송부분에서 보안 및 프라이버시와 관련

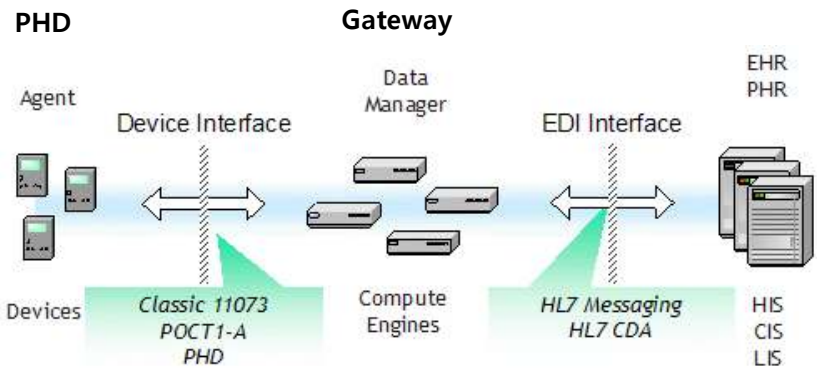

그림 1. 생체의료정보전송관련 국제 표준흐름도[6]-[7]

Fig. 1. International standard flow with bio-medical information transmission[6]-[7].

한 국제표준은 아직 제정되지 못한 상태이다. 즉, 기존 ISO/IEEE 11073-20601[7] 표준에서는 이들간의 전송 프로토콜만 다루고 있는 상태이다. 현재 국내에서는 일부 연구실 수준에서 연구가 이루어 지고 있는 실정이다. 다만 이 부분에 대한 보안 요구사항들에 대해서는 기존에 본 저자가 [8]의 논문을 통해 발표한 바 있다. 따라서 본 환경에서의 보안 위협 및 요구사항들에 관해서는 [8]을 참고하기 바란다.

그러나 인텔과 삼성이 주도하고 있는 CHA(Continua Health Alliance)[9]에서는 산업계 표준을 만들기 위해 이 부분에 대한 연구가 현재 활발히 논의 중에 있다.

그러나 게이트웨이로부터 후송 병원에 이르는 보안 전송부분의 경우 [그림 1]에서 보는 바와 같이 HL7이라는 국제표준화기구에서 활발히 다루고 있다. HL7의 경우 지난 버전 2.6에서 모든 전송 메시지에 UAC(User Authetication Credential) 세그먼트를 추가하거나 사용자에 대한 전자서명을 추가함으로서 공격자로부터의 재사용 공격을 방지하는 등 일부 수준에서 보안성을 제공한 바 있고, 또 최근 버전 3.0의 경우 거의 전 메커니즘에서 보안부분을 적용한 상태이다.

따라서 본 논문에서는 연구 범위를 게이트웨이로부터 후송 병원에 이르는 전송 부분이 아닌 환자의 건강정보를 측정한 PHD들로부터 게이트웨이에 이르는 전송 보안부분에 대해 다루고자 한다.

Ⅲ. PHD와 게이트웨이간 보안 전송

앞서 2장의 관련 연구에서 언급한 바 개인건강의료장비인 PHD로부터 게이트웨이에 이르는 전송부분은 이미 ISO/IEEE 11073-20601에서 표준화가 제정된 상태이다. 이 표준에서는 전송을 위한 하위계층의 방식에 대해서는 블루투스, 유에스비, 지그비, RS232 등 유무선의 모든 장비들이 지원가능한 것으로 규정하고 있다[7].

그러나 본 논문의 범위가 헬기를 통한 응급구조 환경인 것을 감안하면 앞서 2장의 관련 연구에서 언급한 대로 게이트웨이는 일반 PC나 노트북이 아닌 스마트폰과 같은 이동형 단말기를 이용하는 것이 가장 최적이다. 따라서 이 부분의 전송을 위한 전송매체는 블루투스나 지그비 통신을 이용하는 것이 가장 최선의 대안이다.

본 장에서는 블루투스와 지그비 두 가지 방식을 대상으로 개인건강의료장비의 특성인 저전력, 낮은 컴퓨팅 파워에 적합한 보안 메커니즘을 제안하고자 한다.

블루투스 기술은 2.4GHz 주파수를 이용한 저가격, 저전력 근거리 무선 디지털 통신 규격으로, 1999년 Bluetooth SIG에서 데이터 전송속도 1Mbps(최대 3Mbps), 전송거리 10~100m 이내로 규정한 버전 1.0을 시작으로 2007년에 버전 2.1이 발표된 상태이다.

현재 제공되고 있는 보안 서비스와 관련해서는 4가지의 보안 모드를 아래와 같이 제공하고 있다.

- 모드 1 : non-secure
- 모드 2 : service level (특정 장치나 서비스에 대한 인증 및 인가를 담당)
- 모드 3 : link level (모든 장치나 서비스에 대해 인증 및 인가 담당)
- 모드 4 : mode 2에 보안기능 강화로 암호 키 교환 기능이 추가됨

또한 인증을 위해 개인 아이디 번호(PIN, Personal Identification Number) 또는 저장된 링크 키를 이용하고 있으며, 기밀성을 위해 선형 피드백 시프트 레지스터 기반의 스트림 암호를 적용하고 있고, 인가를 위해 장치별로 허용 가능한 서비스만을 대상으로 제공하고 있다. 그러나 접근통제나 무결성 서비스는 현재 제공되고 있지 않는 상태이다.

한편 올해 9월 블루투스 저에너지 호환 센서 디바이스의 시장개발 가속화를 위해 블루투스 저에어지 기술인 SMART와 SMART READY 버전 4.0[10]을 발표하고 프로파일을 공개한 바 있다. 여기서 SMART 버전은 GATT기반 아키텍처로 듀얼모드(저에너지와 클래식 방식 모두 지원)로 동작하며 소비자가 자체적으로 장치 소프트웨어를 업데이트 할 수 있으며 주로 허브 장치로 폰 이나 PC에 적합한 사양을 가지고 있다. 반면 SMART READY 버전의 경우 동일한 GATT기반 아키텍처로 오직 저에너지의 싱글 모드로 동작하며 심전도 모니터링 작치와 같은 센서 타입의 장치에 적합하다. 따라서 제안 환경의 경우 SMART 버전은 게이트웨이로서 스마트 폰 등

표 1. 지그비 보안 운영 모드

Table 1. Gigbee security operation mode.

식별자	security suite name	보안 서비스			
		접근통제	데이터 암호화	프레임 무결성	신규성 (옵션)
0x00	none				
0x01	AES-CTR	O	O		O
0x02	AES-CCM-128	O	O	O	O
0x03	AES-CCM-64	O	O	O	O
0x04	AES-CCM-32	O	O	O	O
0x05	AES-CBC-MAC-128	O		O	
0x06	AES-CBC-MAC-128	O		O	
0x07	AES-CBC-MAC-128	O		O	

으로 구현하고 SMART READY 버전은 센서 디바이스로서 개인건강의료장비 등에 활용하는 것이 가장 효과적인 것으로 사료된다.

따라서 향후 실질적인 구현을 위해서는 이들 버전 4.0을 기본으로 하여 필요할 경우 보안 옵션으로 앞서 언급한 접근통제 서비스를 추가로 제공하는 방안이 대안이 될 수 있다. 접근통제 기술의 경우 환자 개인 프라이버시 보호를 위해 환자의 개인 정보를 역할에 따라 인가된 사용자만이 접근할 수 있도록 단계별 통제 서비스를 제공하는 것으로 의료 환경에서는 환자 프라이버시 보장을 위해 매우 중요한 서비스 중 하나이다.

다음으로 지그비 기술[11]은 블루투스와 달리 BAN(Body Area Network)[12] 보다는 무선 LAN(Local Area Network)과 같은 보다 넓은 범위에 적합한 방식이다. 장치가 일반 모드가 아닌 안전 모드로 운영될 경우, 제공되는 타입에 따라 <표 1>과 같이 7가지로 나누어 신규성, 무결성, 인증, 기밀성 등의 보안 서비스가 제공되고 있다. 참고로 <표 1>에서 CTR의 의미는 주어진 키와 난수를 이용, 블록암호를 사용하여 암호 키를 만들고 암호문은 평문과 무결성 코드를 키 스트림과 XOR 연산을 통해 생성하는 방식을 말한다. CCM의 의미는 앞서 설명한 CTR 방식에 블록암호 방식인 AES의 CBC(Cipher Block Chaining) MAC(Message Authencation Code) 모드 방식을 함께 적용한 것을 말한다.

그밖에 보안 모드로는 크게 아래와 같이 2가지 모드로 운영되고 있다.

- Residential mode : 일반 모드로 보안성이 취약함
- Commercial mode : 암호키 설정, 신규성, 중앙제어 등 강화된 보안 서비스가 가능

블루투스와 달리 지그비 기술의 장점은 보안성에 있어 접근통제라든가 신규성(freshness) 서비스 등 블루투스에 없는 보안 서비스를 제공하고 있다는 점이다. 여기서 신규성 서비스라 함은 카운터 값을 이용하여 공격자로부터 전송 메시지의 재사용 공격을 막는 기술을 일컫는다. 그러나 단점으로는 무선 환경의 서비스를 제공하지만 개인건강의료장치인 PHD가 센서 위주의 저전력이고 계산량이 적다는 특성을 감안 할 때, 보안 적용을 위해 블루투스 보다 많은 계산량을 요구한다는 점에서 효율성이 떨어지는 문제가 있다. 또한 우선 지그비 기술을 제안 환경

표 2. 항공응급의료서비스를 위한 블루투스 및 지그비 보안 방식 비교

Table 2. Comparison bluetooth with gigbee for aerial emergency medical service.

운영기술		블루투스 v4.0	지그비 AES-CCM-32
보안성		다소 낮음	높음
	접근제어	X	O
	인증	O	O
	기밀성	O	O
	인가	O	△
	무결성	O	O
	신규성	X	O
효율성		높음	다소낮음
일반원격의료환경		적합	적합
항공응급의료환경		매우 적합	부적합

에 적용하기 위해서는 개인 건강관리 고객에 대한 프라이버시 강화와 보다 세밀한 접근제어 기법이 추가로 요구된다.

한마디로 말해 블루투스의 경우 보안성은 다소 떨어지지만 저전력에 맞는 효율성을 가진다는 점이 있는 반면, 지그비의 경우 그 반대로 보안성이 보다 높은 것이 장점이지만 그만큼 높은 계산량을 요구하기 때문에 효율성이 떨어진다는 단점이 있다.

따라서 본 논문에서 제안하는 환경이 항공응급의료인 점을 감안하고 PHD 장비들이 저전력 에너지를 갖는다는 특성에 비추어 볼 때, 지그비 보다는 보다 가벼운 블루투스 4.0 (보안 모드 적용) 기술을 적용하여 앞서 언급한 ISO/IEEE 11073-20601 표준에 탑재하는 방식이 가장 최적의 방식인 것으로 결론지을 수 있다.

지금까지 두 가지 기술에 대해 살펴본 결과를 비교해 보면 <표 2>와 같이 요약될 수 있다.

Ⅵ. 결 론

우리는 지금까지 항공응급의료 즉, 환자가 헬기를 이용하여 응급구조나 의료서비스를 받는 환경에서 헬기 내에 구비된 각종 PHD 의료장비들로부터 게이트웨이를 거쳐 후송 병원에 이르는 과정에서 특히, PHD 의료장비에서 게이트웨이에 이르는 보안 전송부분에 대해 다루었다. 여기서 현재 제정된 전송관련 표준인 ISO/IEEE 11073-20601 표준을 기본 모델로 하여 네트워크 하위계층에 전송 표준인 블루투스, 지그비, USB, RS232 가운데 특히 무선 환경에 적합한 블루투스와 지그비의 보안 특성을 비교 연구하여 제안하는 항공응급의료 환경에 가장 적합한 기술이 현 블루투스 버전 4.0 방식임을 도출할 수 있었다.

현재 우리는 체중계를 기본 PHD 센서로 하여 기존 표준인 ISO/IEEE 11073-20601 통신 프로토콜을 적용, 인터넷 환경에서 TCP/IP로 구현한 상태이며 향후 연구과제로 본 논문에서 제안한 블루투스와 지그비를 현 표준에 탑재하고 구현하여 그 성능을 비교 검증하려 한다.

감사의 글

본 연구는 2011년 교육과학기술부와 한국연구재단의 지역혁신 인력양성사업으로 수행된 연구결과임.

참 고 문 헌

[1] ISO/IEEE 11073-10101 Health informatics-Point-of-care medical device communication-Part 10101: Nomenclature, http://www.iso.org, 2004.

[2] Google health, http://www.google.com/heal th/

[3] HealthVault, http://www.healthvault.com/

[4] Personal Health Record, http://en.wiki- pedia.org/wiki/Personal_health_record

[5] ASTM E1714 - 07 Standard Guide for Properties of a Universal Healthcare Identifier (UHID), http://www.astm.org

[6] Health Level Seven International, http:// www.hl7.org

[7] ISO/IEEE 11073-20601 Health informatics -Personal health device communication-Part 20601: Application profile-Optimized exchange protocol, http://www.iso.org, 2010.

[8] 김순석, 박홍진, “u-헬스 환경에서 개인건강관리를 위한 보안 위협 및 요구사항에 관한 연구,” *한국항행학회논문지*, 제 14권, 제 4호, pp 504-511, 2010. 8.

[9] Continua Health Aliance, http://www. continuaalliance.org/

[10] Bluetooth, http://www.bluetooth.com/Pages/ Smart-Energy.aspx

[11] Zigbee Alliance, http://www.zigbee.org/

[12] Body Area Network, http://en.wiki pedia.org/wiki/Body_area_network

김순석(Soon-Seok Kim)

1997년 2월 경남과학기술대학교 컴퓨터공학과(공학사)
1999년 2월 중앙대학교 컴퓨터공학과 (공학석사)
2003년 2월 중앙대학교 컴퓨터공학과 (공학박사)
2003년 3월~현재 한라대학교 컴퓨터공학과 교수
관심분야 :정보보호, 암호응용, 생체보안

이용희(Yong-Hee Lee)

1991년 2월 한양대학교 전자공학과 (공학사)
1993년 2월 한양대학교 전자공학과 (공학석사)
1998년 2월 한양대학교 전자공학과 (공학박사)
1999년 3월~현재 한라대학교 컴퓨터공학과 교수
관심분야 : 생체신호처리, 임베디드시스템

김동호(Dong-Ho Kim)

1991년 2월 고려대학교 전자공학과 (공학사)
1993년 2월 고려대학교 전자공학과 (공학석사)
2008년 2월 고려대학교 전자공학과 (공학박사)
2002년 3월~현재 한라대학교 컴퓨터공학과 교수
관심분야 : 센서네트워크, 네트웍 프로토콜

정호영(Ho-Young Jeung)

2012년 2월 한라대학교 컴퓨터공학과 (공학사)
2012년 3월 현재 한라대학교 정보산업대학원 컴퓨터공학과 (석사과정)
관심분야 : 의료정보보안표준화

박세일(Se-Il Park)

2006년 2월 한라대학교 컴퓨터공학과 (공학사)
2012년 2월 현재 한라대학교 정보산업대학원 컴퓨터공학과 (석사과정)
관심분야 : 의료정보표준화