U-헬스케어를 위한 IEEE 11073 기반 원격 생체정보 모니터링 보안 기술

나재욱, 윤은준*, 우연경, 박종태
경북대학교, *경일대학교

요 약

전 세계적으로 노령인구가 급격히 증가하면서 만성질환자도 급증하고 있는 추세이다. 또한, 고도화된 현대사회와 과도한 업무, 서양화된 식습관, 그리고 운동부족은 젊은 층에서의 성인병 및 만성질환 증가를 부추기고 있다. 만성질환의 증가는 의료비 증가로 이어지고 결국은 국가재정 부담으로 돌아가게 된다.

만성질환자의 대부분은 지속적인 생체정보 측정과 이를 통한 관리가 필수적인데 매번 병원을 방문해 관리하는 것은 현실적으로나 비용적인 측면으로나 무리가 있는 것이 사실이다. 이러한 문제를 해결하고 언제 어디서나 시간과 공간에 구애받지 않고 생체정보를 원격에서 측정하고 관리 받을 수 있도록 하는 것이 U-헬스케어 서비스이다.

U-헬스케어 서비스는 전통적인 의료 서비스에 정보통신 기술을 접목한 형태로 고령인구 및 만성질환자의 지속적인 관리를 위해 현재 주목 받고 있는 기술이다. U-헬스케어 서비스의 가장 중요하면서도 기본적인 요소는 원격지 사용자의 생체정보를 측정하고 수집할 수 있는 원격 생체정보 모니터링 기술이다. 이를 위해서는 다양한 종류의 생체정보 측정기기가 필요한데 장비나 시스템 간 통신 인터페이스의 상호 호환성이 매우 중요하다.

본 논문에서는 원격 생체정보 모니터링을 위한 표준 기술인 IEEE 11073 PHD를 소개하고 현재 IEEE 11073 PHD 표준에서 명시하고 있지 않은 보안 문제점과 필요 기술들을 분석하고자 한다. 또한, IEEE 11073 PHD에서 IEEE 11073-20601 표준 프로토콜을 이용한 사용자 인증 구조를 제안한다.

Ⅰ. 서 론

노령인구와 함께 고혈압, 당뇨 등 만성질환자의 급격한 증가는 U-헬스케어 서비스에 대한 필요성을 증대시키고 있다. 즉, 전통적인 헬스케어의 개념에 IT 기술을 접목시켜 시공간을 초월하여 언제 어디서나 생체정보 측정 및 관리를 할 수 있도록 하는 것이다. 이러한 혁신적인 의료 서비스 패러다임은 기존의 병원 중심 의료 서비스를 소비자 중심의 의료 서비스로, 사후치료 중심의 의료 서비스를 예방 중심의 의료 서비스로 진화 시키고 있다.

U-헬스케어 서비스는 센서 기술을 이용해 사용자의 심전도, 혈압, 맥박, 체온, 산소포화도, 혈당 등 각종 생체 정보를 간편하고 정확하게 감지하거나 측정할 수 있는 생체정보 감지 기술과 감지된 생체정보를 스마트폰, 스마트 패드, PC 등으로 전송하고 취합할 수 있는 통신 기술, 그리고 원격지에서 수집된 생체 정보의 저장, 분류 및 분석할 수 있는 생체정보 처리 및 분석 기술 등 세 가지 요소 기술로 구성된다.

이중에서 가장 중요하고 기본적인 요소는 원격지 사용자의 생체정보를 측정하고 수집할 수 있는 원격 생체정보 모니터링 기술이다. 이를 위해서는 다양한 종류의 생체정보 측정기기가 필요한데 다양한 생체정보 측정 기기로부터 측정된 생체정보를 수집, 전송 및 관리를 위해서는 각 단계별 장비나 시스템 간 상호 호환성이 매우 중요하다. 하지만 현재 혈압, 심전도, 혈당 등을 측정하는 생체정보 측정기기는 다양한 벤더들의 독자적인 통신 프로토콜을 사용하고 있어 상호 호환성이 거의 없다.

IEEE 11073 WG에서는 위와 같은 문제를 해결하기 위해 혈압, 심전도, 혈당, 체중, 활동량 등을 측정할 수 있는 개인용 생체정보 측정 장치인 PHD (Personal Health Device) 에 대한 표준화 작업을 진행하고 있다. IEEE 11073 PHD는 생체정보 데이터 모델과 프로토콜을 정의한 것으로 IEEE 11073 PHD 에이전트가 탑재된 원격 개인용 생체정보 측정 장치와 PC, 셋톱박스, 혹은 스마트 폰 등에 탑재된 IEEE 11073 PHD 매니저 간 정보 교환을 위한 표준이다.

현재 산소포화도 측정기, 심전도 측정기, 혈압계, 혈당계 등을 포함한 13개 종류의 생체정보 측정 장치에 대한 표준화가 완료되었으며 IEEE 11073 PHD 에이전트와 매니저 간 프로토콜과 데이터 모델도 표준화가 완료되었다. 또한, 인슐린 펌프나 뇨 분석기 등을 포함한 6개 종류의 생체정보 측정 장치에 대한 표준화가 진행 중이다. 그러므로 IEEE 11073 PHD 표준을 이

용해 원격 생체정보 모니터링 서비스를 구현할 경우 장치 간 호환성 보장과 표준화된 데이터 획득이 가능하므로 U-헬스케어 서비스에서 반드시 필요한 기술이다.

IEEE 11073 PHD 기반 원격 생체정보 모니터링 기술은 U-헬스케어 서비스에서 매우 중요한 부분임에 틀림없지만 한 가지 큰 문제점을 가지고 있다. U-헬스케어 서비스는 지극히 개인적인 정보를 다루고 있으므로 반드시 강력하고 안전한 보안 기술이 적용되어야 한다. 하지만 IEEE 11073 PHD 표준에는 아직 보안기술에 대한 정의가 되어 있지 않아 각 벤더들이 자체적으로 보안 솔루션을 개발 적용할 책임이 있다. 특히, 사용자 인증이나 장치 인증 등에 아무런 규정이 없어 인가되지 않은 사용자의 생체정보가 악용될 수 있는 문제가 있다. 이러한 문제를 해결하기 위해 현재 IEEE 11073 PHD WG 내에서도 보안기술 범위와 종류에 대한 논의가 활발히 진행되고 있다.

본 논문에서는 IEEE 11073 PHD를 이용한 원격 생체정보 모니터링을 위한 보안 문제점을 분석하고 IEEE 11073 PHD에서 사용자 인증을 위한 구조를 제시하고자 한다. 본 논문의 구조는 다음과 같다. Ⅱ.1절에서 원격 생체정보 모니터링 보안 기술 동향에 대해서 살펴보고 Ⅱ.2절에서는 IEEE 11073 PHD 기술과 보안 문제점을 살펴본다. 그리고 Ⅱ.3절에서는 IEEE 11073 PHD를 위한 사용자 인증 구조를 제안하고 마지막으로 Ⅲ장에서 결론을 맺도록 한다.

Ⅱ. 본 론

1. 원격 생체정보 모니터링 보안 기술 동향

최근에 ISO/IEEE는 PAN(Personal Area Network)에서 모바일 의료 기기를 통한 생체 신호를 전송, 모니터링, 제어 할 수 있는 11073 관련 표준들을 제정하였다. 하지만 ISO/IEEE 11073 관련 표준들에는 식별자 인증과 데이터 암호화에 관한 보안 절차를 포함하지 않고 있다. ISO/IEEE 11073-20601 Optimized Exchange Protocol(OEP) 프로토콜은 에이전트(Agent)와 매니저(Manager) 간의 포인트-투-포인트 방식의 통신 프로토콜로 에이전트는 혈당, 체온 등과 같은 정보를 개인 건강 정보를 환자로부터 바로 수집하는 장치(device)로 표현된다. 매니저는 에이전트로부터 개인 건강 정보를 수집하는 장치로 표현되며 스마트 폰, 노트북, 처리 터미널과 같은 로컬 호스팅 장치들을 의미한다. 2012년에 Egner 등은 ISO/IEEE 11073-20601 표준의 IEEE 11073-20601 프로토콜에 응용 가능한 생체 가변 지문 측정(biometric cancelable fingerprint measure) 기반의 식별자 관리(identity management system)을 이용한 개선된 보안 인증 프로토콜을 제안하였다 [1]. 제안된 인증 기법은 1) 에이전트 관리자 인증과 2) 환자 에이전트 링크 생성의 두 단계로 구성된다. 〈그림 1〉은 시도-응답 방식의 상호인증 프로토콜을 보여주며 각 객체들은 자신의 비밀 정보인 패스워드 또는 사전 공유키로 상대방을 인증하게 된다.

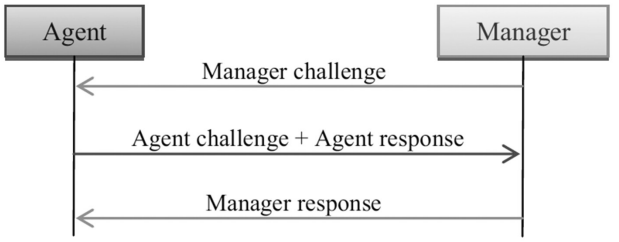

그림 1. 시도-응답 방식 상호인증 프로토콜

〈그림 2〉는 협약(association) 과정을 첨부한 IEEE 11073-20601 기반 상호인증 프로토콜을 보여준다. 첫 번째 AarqApdu는 협약을 요청하는 메시지이며, 두 번째 AareApdu는 협약 요청에 대한 매니저의 응답 메시지이다. 매니저는 해당 메시지를 통해 에이전트에게 인증 요청을 한다. 세 번째 AarqApdu는 매니저의 시도에 대한 에이전트의 응답 메시지로 상호 인증 요청 메시지가 포함되어 있으며, 네 번째 AareApdu에서 매니저는 인증 결과를 에이전트에게 전송하여 상호인증을 마친다.

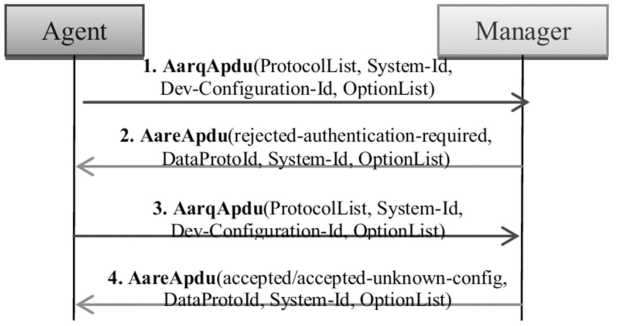

그림 2. IEEE 11073-20601 기반 상호인증 프로토콜 협약 과정

아래 〈그림 3〉는 freescale사에서 소개하는 IEEE 11073 PHD 통신에서 응용 가능한 ZigBee 헬스케어 구조(ZigBee Health Care Architecture)를 보여주고 있다.

ZigBee 헬스케어에서 필요한 기본 보안 요구사항 만족을 위해 개인 의료 정보 보호를 위한 AES 128 암호(encryption) 메커니즘을 사용하며, 보안, 수용 인원, 조명, 모션 감지와 편의를 위해 제어와 모니터링 장치를 통합하여 활용한다 [2]. ZigBee 헬스케어에서 필요에 따라 높은 프라이버시 제공이 필요한 의료 정보를 다룰 때가 있다. 이때에는 링크 키 보안(link key security), 효율적인 키 분배(efficient key distribution), 접

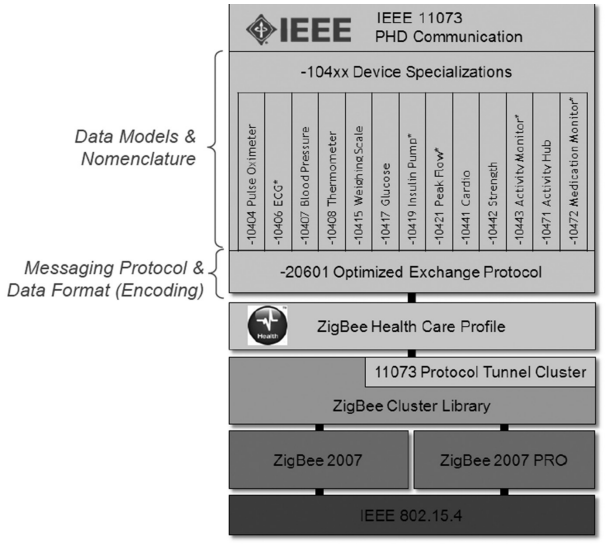

그림 3. ZigBee U-헬스케어 구조

근 제어(access control) 등의 보안 기술이 요구된다. 강력한 보안을 제공하기 위해 두 개의 ZCL 클러스터(ASKE와 ASAC)로 구성된 AlphaSec을 이용할 수 있다. ASKE는 안전한 통신 링크 설정을 위해 필요하며, 〈그림 4〉에서 보여주는 것과 같이 ASAC는 접근제어 기능을 담당하며, ASKE는 키 분배와 설정 기능을 담당한다. AlphaSec 솔루션은 효율적이며, 사용자 불편성이 없으며 확장성이 뛰어난 장점을 가진다.

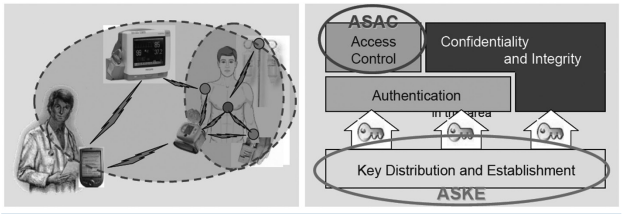

그림 4. AlphsSec 솔루션 [3]

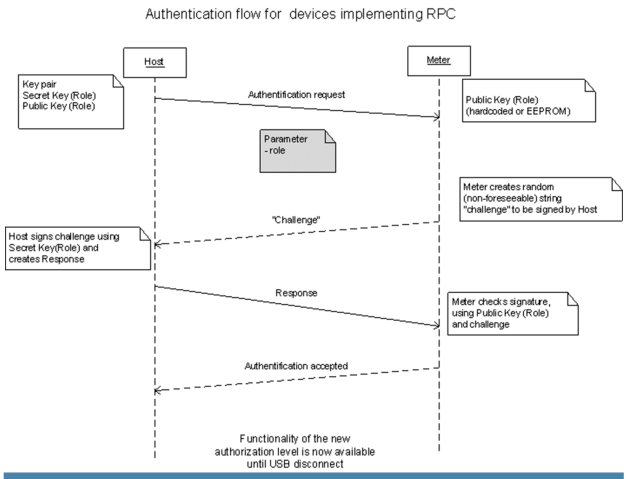

그림 5. 호스트와 ACCU-CHEK 기기간의 상호 인증

Roche 사에서 개발한 혈당 측정기(Blood Glucose Meters)인 ACCU-CHEK는 USB 통신 인터페이스로 기능이 동작하며 모든 기능들은 암호학적 보안 기술에 의해 안전하게 동작한다. 높은 수준의 보안 수준을 보장하기 위해 인증 메커니즘과 필요에 따라 무선 인터페이스 환경에서는 프라이버시 보호 기능도 활성화하여 사용할 수 있다. 암호학적 메커니즘들은 자원이 제한된 임베디드 시스템을 지원하기 위해 사용자 인증 3초 이내에 이루어 질 수 있는 2048 비트 키 길이의 경량 RSA 암호 알고리즘을 사용한다.

〈그림 5〉는 ACCU-CHEK 기기와 호스트 간의 상호 인증 과정을 보여주고 있다. 혈당 측정기는 인증을 위해 공개키(public key)만을 저장하며 개인키(private key)는 내부 소프트웨어 내에 안전하게 저장되어 있으며 외부에 공개되지 않는다. 키 갱신(update)은 제조사에서 새로운 공개키를 로드하는 방법으로 처리된다. 파일 전송과 소프트웨어 업데이트는 무선 통신 환경을 위한 대칭키 암호 세션키를 이용한 안전한 통신 방식, 파일 서

표 1. IEEE 11073 PHD를 활용한 U-헬스케어 서비스 예 [4]

적용영역	사용 예	IEEE 11073 PHD 생체정보 측정 장치의 조합
비만 관리	체중 관리, 운동과 식이 관리	10415 체중계, 10442 운동기기, 10472 약물 자동 분배기 + 개인 건강 기록(Personal Health Record), 온라인 식이 다이어리, 콜레스테롤 관리
고혈압	스트레스 레벨 관리, 혈압 관리	10472 약물 자동 분배기, 10407 혈압계, 10415 체중계, 10442 운동기기
당뇨	질병관리	10417 혈당측정기, 10407 혈압계, 10415 체중계, 10472 약물 자동 분배기
요양원	독거관리	10471 독립생활 행위허브, 10472 약물 자동 분배기, 10407 혈압계, 10415 체중계, 10408 체온계 10404 산소 포화측정기, 10442 운동기기 10406 심전도
심장병 환자	심장병 발병 시 원거리 모니터링. 생활방식 관리	10471 독립생활 행위허브, 10472 약물 자동 분배기, 10407 혈압계, 10415 체중계, 10408 체온계 10404 산소 포화측정기, 10442 운동기기 10406 심전도
노인관리	사고 예방, 모니터링, 삶의 편의성	10471 독립생활 행위허브, 10472 약물 자동 분배기, 10407 혈압계, 10415 체중계, 10408 체온계, 10417 혈당 측정기, 10404 산소 포화 측정기, 10406 기초 심전도
재활	능력 회복, 모니터링, 재생기전, 운동	10471 독립생활 행위허브, 10472 약물 자동 분배기, 10407 혈압계, 10415 체중계, 10408 체온계, 10417 혈당 측정기, 10404 산소 포화 측정기, 10406 기초 심전도

명 기법을 사용한 임베디드 시스템과의 안전한 파일 교환, 그리고 동일한 보안 메커니즘을 활용한 이미지 파일을 통한 안전한 소프트웨어 갱신 등의 다양한 방법을 제공한다.

2. IEEE 11073 표준 및 보안 문제점

IEEE 11073 PHD는 생체정보 데이터의 전송 포맷으로 IEEE 11073 PHD 에이전트가 탑재된 원격 개인용 생체정보 측정 장치와 PC, 셋톱박스, 혹은 스마트 폰 등에 탑재된 IEEE 11073 PHD 매니저 간 정보 교환을 위한 표준이다.

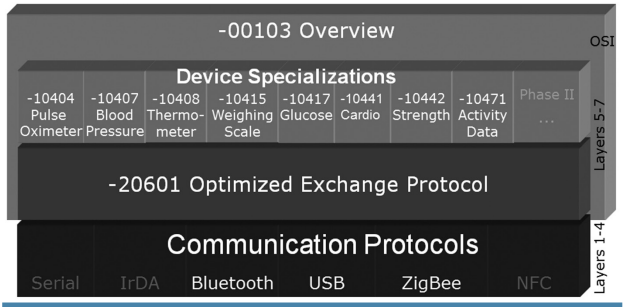

그림 6. IEEE 11073 PHD 개요 [8]

IEEE 11073 PHD 는 〈그림 6〉에서 보는 바와 같이 전송레이어 (Transport Layer), 최적화된 교환 프로토콜 (Optimized Exchange Protocol)인 IEEE 11073 -20601, 그리고 생체정보 측정 장치 특성화 (Device Specialization)인 IEEE 11073-104xx 시리즈 등으로 나눌 수 있다.

전송 레이어의 경우 IEEE 11073 PHD 표준에서는 명시된 물리계층 전송 방법은 없으며 Bluetooth, ZigBee, USB 등 현존하는 다양한 전송방법을 허용하고 있다.

IEEE 11073-20601 Optimized Exchange Protocol은 IEEE 11073 PHD 에이전트와 매니저 간 생체정보 측정 데이터 교환을 위한 최적화된 프로토콜을 정의한다. 즉, 에이전트와 매니저 간 연결관리, 데이터 전송 및 요청, 데이터 구조 등을 포함하고 있다.

IEEE 11073-104xx은 IEEE 11073-20601 상위에 정의된 것으로 혈압계 (10407), 심전도 측정계 (10441), 혈당계 (10417), 체중계 (10415)등과 같은 개인 생체정보 측정 장치가 각 생체정보의 특성에 맞춰 반드시 포함해야 할 오브젝트 속성에 대한 세부사항 (생체정보의 종류, 매니저와의 동작방식 등)을 명시한 것이다.

〈표 1〉은 IEEE 11073 PHD 기반의 원격 생체정보 측정 정보를 활용한 U-헬스케어 서비스 구성 예를 보여준다. IEEE 11073 PHD는 각기 다른 개인 생체정보를 측정하기 위한 표준이다. 하지만 다양한 생체정보 측정 정보를 조합하여 만성질환자 관리나 노인관리 및 재활 등에도 활용할 수 있음을 알 수 있다. 예를 들어 당뇨나 고혈압 등은 유전적인 영향도 있지만 대부분 생활 습관병이다. 즉, 운동이나 식이요법을 통한 체중 조절과 지속적인 약물 치료가 수행되어야 하고 매일 정해진 시간에 혈당이나 혈압 등을 점검하여야 한다. 이를 위해 IEEE 11073-10415 체중계, IEEE 11073-10417 혈당측정기, IEEE 11073-10407 혈압계, 그리고 IEEE 11073-10472 약물 자동 분배기 등을 구성하여 당뇨 및 고혈압 관리를 할 수 있다.

IEEE 11073 전체 시스템 구조는 〈그림 7〉과 같다. 이 구조는 크게 의료 환자인 U-헬스케어 사용자, U-헬스케어 서비스 제공자인 U-헬스케어 공급자, 의료기관, 유관기관, 연계서비스 등으로 구성되어 진다. U-헬스케어 사용자는 개인의 생체정보를 측정하는 개인용 생체정보 측정 장치(PHDs)와 컴퓨터 엔진(CE)으로 구성되며, U-헬스케어 서비스 제공자는 전송받은 생체정보를 처리하는 원격 모니터링 서버와 EHR 서버로 구성된다[5-7].

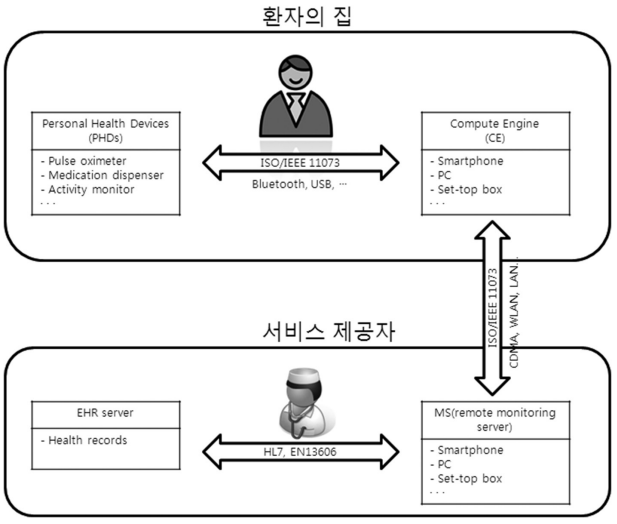

그림 7. IEEE 11073 시스템 구조 [6]

U-헬스케어 서비스는 U-헬스케어 사용자의 생체정보 및 개인 건강기록 등이 대상이므로 U-헬스케어 시스템 구축 및 운용 시 사용되는 개인생체정보, 시스템, 사용자 인증 등과 관련하여 U-헬스케어 시스템의 정보보호 안전성과 신뢰성 확보를 위해 기술적 대책이 반드시 요구된다. U-헬스케어 IEEE 11073 시스템 구조에서 각 구성 요소의 내부와 구성 요소 간 전달되는 생체정보의 기밀성 및 무결성과 시스템의 가용성을 보장하기 위한 여러가지 정보보호 요구 사항들이 필요하다 [7-12].

첫째, 모든 네트워크 구성요소들 간의 전송되는 정보들은 비인가된 접속, 비 인가된 수정, 또는 비 인가된 상대로부터 보호되어야 한다.

둘째, U-헬스케어 서비스는 기본적으로 인터넷과 같은 공용 네트워크를 사용하기 때문에 이를 통해 개인용 생체정보 측정 장치로부터 획득된 생체정보를 포함한 전송되는 모든 데이터에 대하여 사용자인증, 키 관리, 암호화, 무결성 등의 보안기능을 가져야 한다.

셋째, U-헬스케어 서비스를 사용하는 사용자 식별을 위한 사용자 인증이 필요하다. 넷째, 효과적인 보안을 위해 접근제어 방식을 활용한 사용자별 권한 관리 및 사용내역이 관리되어야 한다. 다섯째, 개인 생체정보 측정 장치로부터 획득된 생체정보에 대해 무결성 보장을 위한 생체 정보 인증 및 검증 기능을 가져야 한다.

U-헬스케어 IEEE 11073 시스템에서는 공용 네트워크를 사용하여 개인의 생체정보 및 건강기록 등을 전달하므로 다음과 같은 다양한 보안 위협 요소들이 존재한다 [12].

① 데이터 엿보기(data eavesdropping) 공격: 공격자가 전송중의 의료 정보를 불법적으로 가로채어 메시지 내용을 엿볼 수 있다.
② 트래픽 스니핑(traffic sniffing) 공격: 공격자가 ISO/IEEE 11073 네트워크의 중간에서 타인의 의료 패킷 정보를 도청할 수 있다.
③ 메시지 변경(message modification) 공격: 공격자가 ISO/IEEE 11073 데이터 통신을 하는 도중에 송신한 데이터를 정상적인 권한이 없이 그 내용(데이터)을 변경할 수 있다.
④ 위장 메시지 전송(faked message transmission) 공격: 공격자가 악의적으로 위해성이나 불필요한 데이터를 정상적인 권한이 없이 수신자에게 위장하여 송신할 수 있다.
⑤ 메시지 재사용(message replay) 공격: 공격자가 ISO/IEEE 11073 데이터 통신을 하는 도중에 송신한 데이터를 반복하여 전송하게 하여 불법적 인증 및 그에 대한 응답 내용을 추정하여 위장 공격을 할 수 있다.
⑥ 서비스 거부(DoS: Denial of Service) 공격: 공격자가 시스템에 과도한 부하 등을 일으켜 의료 서비스 제공자 내의 의료 정보 시스템의 중요 의료 데이터나 자원을 정당한 사용자가 적절한 대기 시간 내에 사용하는 것을 방해하는 서비스 거부 공격을 수행할 수 있다.
⑦ 자원 고갈(resource exhaustion) 공격: 공격자가 시스템의 자원을 불필요하게 소모시켜 실질적 통신이 이루어지지 않게 할 수 있다.
⑧ 악성 코드(malicious code) 공격: 공격자가 악의적인 목적을 위해 작성된 실행 가능한 코드를 사용자 또는 서버에 설치되게 할 수 있다.
⑨ 위장(impersonation) 공격: 공격자가 시스템에 접근하기 위해 허가받은 사용자로 위장할 수 있다.
⑩ 세션 하이재킹(session hijacking) 공격: 공격자가 다른 의료 서비스 사용자의 세션 상태를 훔치거나 도용하여 해당 서비스에 액세스 할 수 있다.
⑪ 터미널 하이재킹(terminal hijacking) 공격: 공격자가 다른 의료 서비스 사용자가 사용 중인 터미널 상태를 도청하거나 세션을 제어하여 해당 서비스에 엑세스 할 수 있다.
⑫ 부인(repudiation) 공격: 악의적인 메시지의 송수신자가 정당한 메시지의 송수신한 사실을 부인할 수 있다.

현재 ISO/IEEE11073에서 표준으로 정해진 개인용 건강단말 규격의 맥박산소측정기, 심박계, 혈압측정기, 온도계, 체중계, 혈당계, 심혈관기 등 종류가 다양하며, 신체를 직접적으로 계측하는 기기인 개인용 건강 단말기(PHDs)를 중심으로 표준이 제정되고 있다[5-12]. 또한 U-헬스케어 서비스의 컴퓨터 엔진(CE)은 다양한 개인 건강정보를 계측하여 서비스 제공자의 원격 모니터링 서버로 전송하는 역할을 한다. 기본적으로 U-헬스케어 ISO/IEEE 11073 서비스의 안전성을 보장하기 위해서는 개인용 건강 단말기(PHDs)부터 정보보호기술을 적용하여 제작해야 한다. 또한 안전한 키 분배 및 저장 등 키 관련 관리 기능을 포함해야 한다. 그렇지만, U-헬스케어 서비스 시스템에 사용되는 단말기는 자원이 제한적이고, U-헬스케어 서비스의 보급과 활용을 고려할 때 그 크기와 가격의 상한이 존재하여 암호모듈이나 인증모듈과 같은 조건보다는 본래의 기능 구현을 권고한다. 또한 개인용 건강 단말기(PHDs)와 컴퓨터 엔진(CE)이 일체형이거나 홈네트워크 등을 사용하는 이 구간에서는 다른 구간에 비해 외부로부터의 공격에 노출이 덜 되기 때문에 방화벽의 수준도 시스템 사양에 맞추어 융통성 있게 조절할 수 있다. 개인용 건강 단말기(PHDs)와 컴퓨터 엔진(CE) 사이의 ISO/IEEE 11073 기반 통신시 발생할 수 있는 보안 취약점들은 데이터 엿보기 공격, 트래픽 스니핑 공격, 메시지 변경 공격, 위장 메시지 전송 공격, 메시지 재사용 공격, 서비스 거부 공격, 자원 고갈 공격, 악성 코드 공격, 위장 공격, 하이재킹 공격, 부인 공격 등이 있으며 이들 공격을 방어하기 위해서는 기밀성, 무결성, 가용성, 접근 제어, 부인 방지를 제공할 수 있는 보안 기술 개발이 필요하다. 사용자 개인용 생체정보 측정 장치로부터 전송된 데이터는 서비스 제공자의 원격 모니터링 서버를 통해 다양한 네트워크를 경유하여 U-헬스케어 서버 등으로 전달된다. U-헬스케어 서비스의 특성상 각 병원마다 독립된 특정 망을 사용하기 보다는 언제 어디서나 서비스를 지원하기 위해 기존의 인프라를 활용하는 개방망의 형태로 나타난다. 일반적으로 U-헬스케어 서비스는 UWB (Ultra Wideband)와 Bluetooth 방식을 많이 사용한다. 이에 따라 발생할 수 있는 각

표 2. IEEE 11073 PHD에서 필요한 보안 기술

보안기술	적용 내용
에이전트 인증	IEEE 11073 PHD 에이전트가 현재 인가된 올바른 장치임을 보장
에이전트 제조업체 인증	제조업체 인증을 통해 IEEE 11073 PHD 생체정보 측정 장치의 복제 방지
매니저 인증	생체정보 측정 장치로부터 생체정보를 수집하는 IEEE 11073 PHD 매니저가 인가된 것이지 보장 (EUI-64를 이용한 인증)
환자 (사용자) 인증	IEEE 11073 PHD 생체정보 측정 장치를 사용하는 환자나 사용자에 대한 인증을 통해 인가된 사용자임을 확인하고 수집되는 생체정보와 실제 사용자 관계의 신뢰도 제공
원격 명령 및 제어 인증	IEEE 11073 PHD 매니저에서 발생할 수 있는 잘못된 요청이나 명령 방지
디지털 서명	생체정보 측정 요구나 수집에서 인가된 장치나 사용자임을 확인할 수 있는 발신자 확인

종 공격에 대하여 기밀성, 무결성 및 가용성 등의 정보보호 특성을 보장하여야 한다. 특히 이 구간에서는 단말기로부터 측정된 정보가 U-헬스케어 서버와 서비스에 적시에 전달되는 가용성을 반드시 고려해야 한다. 만약 가용성이 보장되지 않는 경우 U-헬스케어 사용자의 건강상태가 제대로 전달되지 못해 질병의 발생 경고를 놓쳐 적절한 서비스를 제공하지 못해 응급한 상황이 발생될 수 있기 때문이다.

〈표 2〉는 IEEE 11073 PHD 표준에서 명시하여야 할 보안 기술들을 보여준다. 표 2에서 보여주고 있는 보안 이슈들은 현재 IEEE 11073 PHD WG에서 활발히 논의되고 있는 것들을 간추려 놓은 것이다. IEEE 11073 PHD 표준에서는 기본적인 보안 문제점과 제조업체에서 고려야 할 몇 가지 보안 위협의 예만 소개할 뿐 보안 조치에 대한 충분한 지침을 전혀 제공하지 않고 있다. 표 2에서 볼 수 있듯이 IEEE 11073 PHD 기반의 U-헬스케어 서비스의 활성화를 위해서는 에이전트와 매니저 인증, 사용자 인증, 제조업체 인증, 명령 및 제어 인증 그리고 디지털 서명 기술이 적용된 표준 기술이 반드시 명시되어야 한다.

궁극적인 U-헬스케어 서비스의 목적을 만족하려면 단말기에서 측정된 개인생체정보가 직접적인 의료서비스를 제공할 수 있는 의료기관에 전달되어야 한다. 또한 측정, 전달되는 개인생체정보에 대해 의료기관이 의미 있는 의료 서비스를 사용자에게 제공할 수 있어야 한다. 이는 U-헬스케어 시스템을 구성하고 있는 단말기와 U-헬스케어 서버 그리고 모든 의료기관 간의 통신 프로토콜이 동일해야 함을 의미한다. 특히 U-헬스케어 서버와 서비스시스템을 거쳐 의료기관으로 전달되는 데이터의 변형 등으로 인해 환자의 상태를 오판하여 잘못된 서비스를 제공하는 경우, 전반적인 U-헬스케어 서비스 시스템의 신뢰성에 손상이 갈뿐 아니라 의료기관의 자원 낭비가 발생하여 서비스의 효율성이 저하될 수 있기 때문에 서비스의 가용성과 함께 무결성이 중요한 사항이 된다. U-헬스케어 단말기로부터 U-헬스케어 서버를 경유한 정보가 유관기관에 전달되기 위해 기존의 구간들과 동일하게 개방된 망을 사용하게 되므로 전달되는 의료정보가 사용자의 프라이버시를 헤칠만한 정보를 포함하는 경우 반드시 기밀성과 접근제어를 고려해야 한다. U-헬스케어 서비스는 단말기로부터 의료기관 또는 유관기관을 통해 전반적인 시스템이 운영되지만, 이와 연계된 지불시스템, IP-TV 등 U-헬스케어 서비스가 다양한 플랫폼에서 지원 가능하도록 돕는 다양한 연계 서비스도 함께 일어난다. 따라서 연계기관에 전달되는 개인의 의료정보는 반드시 역할과 목적에 맞게 전달되어야 하며 기밀성과 접근제어를 고려해야 한다 [12].

결론적으로 U-헬스케어 IEEE 11073 시스템의 안전성과 신뢰성을 보장하기 위해서는 정보보호 기술을 반드시 부가하여야 한다. U-헬스케어 서비스가 기존의 구축된 네트워크를 통해 제공되므로 현존하는 여러 공격에 대응하는 기술과 시스템을 U-헬스케어 서비스에도 모두 적용하는 것이 바람직하다. 그러나 개인용 단말기기(체중계, 혈압계 등)처럼 단순한 정보만을 제공하는 기기에 암호 및 인증 메커니즘을 포함한 모듈(칩 포함)을 부가하고, 이에 수반되는 키 관리 인터페이스를 구현하는 경우, 가용성이 저하되어 효율적이지 못한 점이 있음으로 통신 및 연산 효율성을 고려한 다양한 경량 보안 메커니즘 개발도 반드시 필요하다 [12]. 또한 세계 동향으로 HL7 Ver 3.0에서 보안기술이 이미 탑재된 규격을 제정 중에 있으며, ISO/NP TS 25237 표준의 Health informatics에서는 프라이버시 보호 강화 방안을 마련 중이며 ISO/TS 22600 표준의 Health informatics에서 의료정보 보호를 정의하고 있다. 국내 동향으로 국내 보안기술이 탑재된 u-헬스케어 국제 표준(ISO/IEEE 11073, HL7)을 채택 중에 있다. 결론적으로 미래 대응전략으로는 ISO/IEEE 11073의 경우 국내와 동일하게, 전송규격일 뿐 아직 보안요소에 대한 표준안을 추진 중임으로 계속적인 정보보호 기술 연구개발이 필요하다.

3. IEEE 11073 표준 기반 개인 생체정보 측정 장치의 사용자 인증을 위한 제안 구조

본 절에서는 IEEE 11073 PHD를 사용하는 사용자의 인증을 위한 구조를 제안하고자 한다. 앞서 기술한 바와 같이 IEEE 11073 PHD 표준은 사용자 인증 등을 포함하는 보안 기술에 대해서는 명시하지 않고 있어 다중 사용자가 하나의 IEEE 11073 PHD 생체정보 측정 장치를 사용할 경우 문제가 발생할 수 있다. 예를 들어, IEEE 11073-10417 에이전트가 탑재된 혈당계를 사용할 경우 어떤 사용자가 측정한 혈당인지 검증할 수 없다. 이런 문제는 원격 측정된 생체정보가 인가된 사용자가 측정한 것인지 아니면 비인가자가 측정한 것인지 구분할 수 없기 때문에 측정된 데이터와 사용자와의 관계에서 신뢰도가 떨어지게 된다. 그러므로, 하나의 IEEE 11073 PHD 원격 생체정보 측정 장치를 이용해 가족단위나 그룹단위 등의 공동 사용은 사실상 불가능한 것이 사실이다.

〈그림 8〉은 이러한 문제점을 해결하기 위해 IEEE 11073 PHD 원격 생체정보 측정 장치를 사용하는 사용자 정보를 기반으로 DIAMETER AAA (Authentication, Authorization, Accounting) 서버를 이용해 사용자 키를 생성하고 IEEE 11073-20601에 명시한 표준 협약 절차를 이용해 에이전트와 매니저 간 사용자 인증을 위한 구조를 보여준다.

사용자는 사용자 정보 입력 단말, 즉, IEEE 11073 PHD 매니저가 탑재된 단말을 이용해 사용자의 이름, 나이, 성별, ID, 패스워드 등을 입력하고 사용자 정보를 전송 받은 DIAMETER AAA 서버에서는 사용자 중복 여부를 검증하고 중복된 사 용자가 아니면 사용자 정보를 등록함과 동시에 사용자 인증 키 를 생성하게 된다. 생성된 사용자 인증 키는 DIAMETER 프로토콜을 통해 사용자 정보 입력 단말로 전송된다. 사용자 인증 키를 수신 받은 사용자 정보 입력 단말은 사용자 인증 키를 IEEE 11073 PHD 에이전트로 WPAN을 이용해 전송한다. 이때 무선 링크 구간은 각 통신 표준에서 지원하는 암호화 기법을 사용한다. 사용자 인증 키를 수신 받은 IEEE 11073 PHD 에이전트는 IEEE 11073 PHD 매니저에게 협약 요청 매개변수 중 option-list에 사용자 인증 키를 포함하여 협약 요청 메시지를 전송하게 된다. IEEE 11073 PHD 매니저는 에이전트로부터 전달받은 사용자 인증키를 DIAMETER AAA 서버로 전송하여 사용자 인증키 검증을 요구하고 그 결과에 따라 에이전트의 접속 여부를 결정한다. IEEE 11073 PHD 매니저는 사용자 인증 키 검증에 성공하였을 경우 DIAMETER AAA 서버로부터 등록된 사용자 등록 정보를 전송받아 해당 사용자 정보와 측정되는 생체정보를 매칭 시키는데 사용한다.

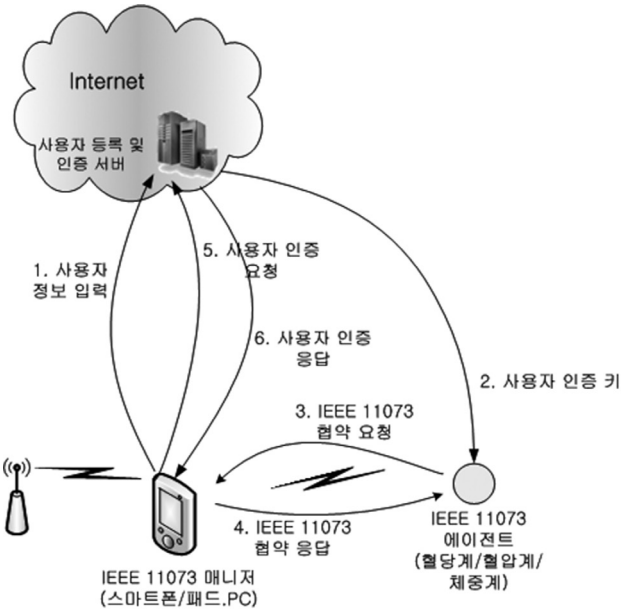

그림 8. 제안된 IEEE 11073 PHD 사용자 인증 구조

Ⅲ. 결 론

본고에서는 U-헬스케어 서비스에서 핵심적인 요소인 IEEE 11073 PHD 표준 기반 원격 생체정보 모니터링 기술에 대해 알아보고 비표준 원격 생체정모 모니터링 장치에서 보안기술 동향을 살펴보았다. 또한, IEEE 11073 PHD 표준에서 명시하고 있지 않는 보안기술과 관련하여 현재 IEEE 11073 PHD WG에서 논의되고 있는 보안이슈들을 소개하고 반드시 적용하여야 할 보안 기술들에 대해 살펴보았으며, 마지막으로 IEEE 11073 PHD 사용자 인증을 위한 구조를 제시하였다.

U-헬스케어 기술의 활성화를 위해 중요한 두 가지 이슈는 장치 간 상호호환성과 보안기술에 있다. 장치 간 상호호환성은 IEEE 11073 PHD 표준을 통해 해결할 수 있으나 아직 보안기술을 명시하지 않아 또 하나의 큰 과제로 남아 있는 것이 사실이다.

상기 기술한 IEEE 11073 PHD를 이용한 상호환성 확보와 보안 기술의 해결이 이루어진다면 고령자, 만성질환자 등의 지속적인 관리를 위한 진정한 U-헬스케어 서비스가 활성화 될 것이라 사료된다. 이를 통해 치료 중심에서 예방 중심으로 새로운 의료 서비스 패러다임의 변화와 맞물려 U-헬스케어 서비스는 새로운 블루오션이 될 것이다.

Acknowledgement

본 연구는 지식경제부 및 정보통신산업진흥원의 대학IT연구센터 지원사업 (NIPA-2012-(C1090-1121-0002)), 2단계 BK21 프로젝트 및 경북대학교 학술연구비에 의하여 연구 되었음.

참 고 문 헌

[1] Egner et al., "Managing Secure Authentication for Standard Mobile Medical Networks", 2012 IEEE Symposium on Computers and Communications (ISCC), pp.390-393, 2012.

[2] J. Adams, "ZigBee and Health Care (Part 1)", FTF-IND-F0460, freescale, 2010.

[3] U. Porsch, "Communication Security in Blood Glucose Meters", ACCU-CHEK, Roche, 2012.

[4] IEEE P11073-00103 TM/D11 Drafe Guide for Health Informatics-Personal Health Device Communication - Overview.

[5] Part et al., "An Integrated Gateway for Various PHDs in U-Healthcare Environments", vol. 2012, Article ID 954603, pp.1-7, 2012.

[6] J. G. Pak and K. H. Park, "Design of an ISO/IEEE, 11073 gateway for u-healthcare services," in Proceedings of the International Conference on Information Science and Technology, pp.152-154, 2012.

[7] IEEE Std. 11073 Standard for Medical Device communication. Part 00000: Framework and Overview.

[8] IEEE Std 11073-20601, Health informatics - Personal health device communication - Part 20601: Application profile - Optimized Exchange Protocol.

[9] IEEE Std 11073-10404, Health informatics - Personal health device communication - Part 10404: Device specialization - Pulse oximeter.

[10] ISO/IEEE 11073-10201:2004, Health informatics - Point-of-care medical device communication - Part 10201: Domain information model.

[11] Tutorial material by Douglas P. Bogia, "ISO/IEEE 11073 Personal Health Devices Tutorial".

[12] TTA, 유헬스 서비스 정보보호 참조모델, 정보통신단체표준 TTAK.KO-10.0464, 2010.

약 력

나 재 욱

2001년 경북대학교 농업경제학과(경제학사)/컴퓨터공학과(공학사)
2003년 경북대학교 정보통신학과(공학석사)
2009년 경북대학교 정보통신학과 (공학박사)
2009년~현재 경북대학교 U-헬스케어 융합 네트워크 연구센터 Post-Doc. 과정
관심분야: U-헬스케어 서비스, 유비쿼터스 컴퓨팅, 차세대 유무선 융합망, 모바일 통신

윤 은 준

1995년 경일대학교 공학사
2003년 경일대학교 컴퓨터공학과 공학석사
2007년 경북대학교 컴퓨터공학과 공학박사
2007년~2008년 수성대학교 컴퓨터정보계열 전임강사
2009년~2011년 경북대학교 대학원 전자전기컴퓨터학부 계약교수
2011년~현재 경일대학교 사이버보안학과 조교수
관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜

우 연 경

2011년 영남대학교 전자공학과 공학사
2012년~현재 경북대학교 정보통신학과 석사과정
관심분야: U-헬스케어 서비스, 무선 네트워크 관리, 차세대 통신망운용, 네트워크 이동성 관리

박 종 태

1978년 경북대학교 전자공학과 졸업(공학사)
1981년 서울대학교 전자 공학과 졸업(공학석사)
1987년 Univ. of Michigan EECS 졸업(공학박사)
1984년~1987년 미국 CITI 연구원
1987년~1988년 미국 AT&T Bell 연구소 연구위원
1988년~1989년 삼성전자 컴퓨터시스템 사업부 수석연구원
1989년~현재 경북대학교 전자공학과 교수
2000년~2003년 IEEE Technical Committee on Information Infrastructure(TCII) 의장
관심분야: 이동통신, 모바일, 차세대 통신망운용, 네트워크 보안, 헬스케어 서비스