원격의료환경에서 개인생체정보 보호 및 무결성에 관한 연구

(Study on Protection and Access Control of Personal Bioinformation in Telemecine Environment)

김순석*, 이재현**

(Soon Seok Kim, Jae Hyun Lee)

요 약

본 논문에서는 일반 가정이나 건물 내에서 일종의 바이오센서인 개인건강 디바이스를 이용함에 있어, 각 디바이스들과 이들로부터 개인 생체정보를 수집하는 게이트웨이간 통신 시 환자의 개인정보를 보호할 수 있는 새로운 프라이버시 보호 방법을 제안한다. 제안하는 방법은 이전 [1]에서 제안한 프라이버시 보호 방법보다 추가적인 무결성 보장 및 전송 보안을 통해 훨씬 강건하고 안전하며 국제 표준인 ISO/IEEE 11073-20601[2]을 준수하고 있어 다양한 개인건강 디바이스들에 상호 호환이 가능하다는 장점이 있다.

■ 중심어 : 개인건강디바이스, 무결성, 생체정보 보호, ISO/IEEE 11073-20601, 프라이버시

Abstract

By using personal health devices, a type of bio-censor at home and building, for telemedicine, this paper proposes a new method to protect more robust patient's privacy than before scheme [1] by ensuring the integrity and the secure transmission further when it communicates with gateway which collecting bio-information from them. As the suggested method is designed to conform with ISO/IEEE 11073-20601 [2], which is international standard, it considered interoperability with various health devices.

■ keywords : Personal Health Device, Intergrity, bioinformation protection, ISO/IEEE 11073-20601, Privacy

Ⅰ. 서 론

의료분야와 관련한 그 동안의 보안 기술은 주로 병원 내 또는 병원 간에 이루어지는 의료정보의 흐름에 관심이 많았던 것이 사실이다. 표준화에 있어서도 주로 병원 내 의료정보 소프트웨어의 보안 기술이 그 주류를 이루고 있다. 일례가 바로 전자의무기록(EMR, Electronic Medical Record)에 대한 보안이며 이 분야 또한 현재 국내외에서 활발히 연구가 진행 중에 있다.

그러나 최근 의료의 중심이 진료를 통한 치료에서 웰빙, 웰니스의 영향에 따른 예방이나 건강관리로 이동하면서 의료 장비에 있어서도 일반가정 내에서 혈압, 혈당, 체중계와 같이 사용자가 간단히 검사를 할 수 있는 진단, 검사 장비들이 연이어 출시되고 있다. 이를 흔히 병원 내 현장 진료형 의료장비인 PoC(Point of Care)와 대변된 가정용 헬스 장비 즉, 개인건강디바이스(PHD, Personal Health Device)라 부른다. 다시 말해 개인건강디바이스란 IEEE에서 정의한 용어로 가정에서 원격 진료를 위해 만성질환자나 특히 노인들이 측정하는 장비를 일컫는 것으로, 이들의 종류로는 혈압계, 체중계, 체온계, 혈당계 등이 있으며 다른 말로 바이오센서라고 불리기도 한다.

이러한 건강 디바이스들을 이용하여 가정 내 여러 사용자 또는 환자들로부터 측정된 생체 정보들은 게이트웨이라 불리우는 컴퓨터나 모바일 폰 혹은 태블릿 PC 등에 수집된다. 수집된 정보들은 응급 상황 발생 시 병원 내 응급의료센터나 혹은 개인건강관리센터로 전송되어 개인건강 관리나 혹은 응급 치료에 소스 데이터로 이용된다.

이와 관련하여 지난 2011년 ISO와 IEEE에서는 공동으로 가정 내에서의 개인건강디바이스 통신과 관련한 표준 프로토콜(ISO/IEEE 11073-20601)을 제정한 바 있으며 현재까지 개정작업을 진행해 오고 있다[2]. 여기서 말하는 통신이란 여러 개인건강 디바이스들과 게이트웨이 상호간 정보 교환 프로토콜을 말한다.

한편 이러한 각 통신 상호간 전달되는 정보는 개인의 생체정보 또는 병력정보인 만큼 이들 정보에 대한 안전한 교환이 반드

* 정회원, 한라대학교 컴퓨터공학과
** 정회원, 강릉원주대학교 정보기술공학과

접수일자 : 2016년 08월 16일
수정일자 : 2016년 12월 26일
게재확정일 : 2016년 12월 08일
교신저자 : 김순석 e-mail : sskim@halla.ac.kr

시 전제되어야 한다. 특히 전송과정에서 악의 있는 제삼자로부터 개인 건강 정보의 오남용과 위변조, 해킹 등으로 인한 사생활 침해 문제는 반드시 해결되어야 하는 선결과제이다. 그럼에도 불구하고 이 표준은 현재 상호간 통신 프로토콜과 프레임워크에 대해서만 다루고 있을 뿐 앞서 말한 각종 보안 침해에도 불구하고 현재까지 보안에 대한 요소는 전혀 고려되고 있지 않는 실정이다.

개인건강 디바이스 통신에서의 보안 분야와 관련한 연구는 그동안 여러 가지 수행되어 왔다[3,4]. 지난 2010년 Appari 등[5]은 헬스케어 환경에서 정보보호의 중요성에 대해 언급한 바 있으며, Kumer 등[6]은 지난 2012년 헬스케어 환경에서 보안과 관련된 정책의 필요성에 대해 언급한 바 있다. 지난 2012년 Kliem 등[7]은 개인건강 디바이스의 모바일 환경에서 보안 통신을 위한 아키텍처를 제안한 바 있으며, 같은 해 Rubio 등[8]은 그 가운데 심전도 장비에 대해 강건하면서도 심플한 보안 확장에 대해 논문을 발표한 바 있다. 또한 2012년 Denis Foo Kune 등[9]이 발표한 논문에 의하면 본 연구와 관련한 보안 요구사항들을 제시하고 현존 표준 프로토콜인 ISO/IEEE 11073에 대한 보안 요구사항 만족여부에 대한 연구가 있었다.

그러나 현재까지의 연구는 주로 보안 프레임워크나 정책, 요구사항 등에 관한 것일 뿐 구체적인 방법에 대한 제시가 없었던 것이 사실이다. 이러한 개인건강 디바이스들과 게이트웨이 상호간 안전한 통신과 사용자 프라이버시 보호를 위해 우리는 지난 2014년 새로운 보안 프로토콜을 제안한 바 있다[1].

본 논문에서는 이전 [1]에서 제안한 프로토콜을 보다 확장하여 사용자 프라이버시 보호뿐만 아니라 전송 정보의 무결성과 안전한 전송을 함께 보장하는 보다 강건한 프로토콜을 제안하고자 한다.

본 논문의 2장에서는 ISO/IEEE 110730-20601에서 제시한 기본 통신 프로토콜과 이전 [1]에서 제안한 방법에 대해 소개하고 3장에서는 2장에서 제시한 표준 통신 프로토콜의 기반 하에서 이전 [1]의 방법을 보다 확장한 강건한 프로토콜을 새롭게 제안한 후 4장을 끝으로 결론을 맺고자 한다.

Ⅱ. 관련연구

1. ISO/IEEE 11073-20601 통신 프로토콜[2]

본 표준은 한마디로 개인건강 디바이스와 게이트웨이 간의 생체정보에 대한 상호 교환을 정의한 프로토콜로, 이 프로토콜은 어플리케이션 계층 서비스와 개인건강 디바이스와 게이트웨이 사이에서의 데이터 교환 프로토콜의 정의라는 2개의 측면으로 구성된다. 데이터 교환 프로토콜은 명령어, 개인건강 디바이스 구성 정보, 데이터 포맷 및 전체 프로토콜로 정의된다. 또한 세부적으로는 그림 1과 같이 3 개의 시스템 모델로 나뉘며 각 모델의 역할은 다음과 같다. 이 3개의 모델들은 데이터를 표시하고, 데이터 접근 및 명령 방법론을 정의하며 데이터를 개인건강 디바이스로부터 게이트웨이로 전달하기 위해 함께 동작한다.

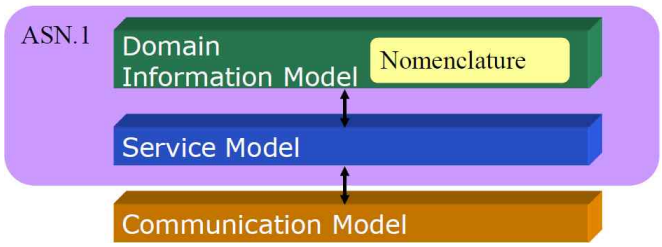

그림 1. ISO/IEEE 11073-20601 모델링[2]

▪ DIM(Domain Information Model) : 개인건강 디바이스와 생체 데이터 포맷(ASN.1)에 대해 기술한 것으로 디바이스로부터 측정된 개인 생체 정보를 일련의 객체들로 특성화한다. 각각의 객체는 한 개 또는 다수의 속성들을 가지고 있는데 이 속성들은 행동을 제어하고 디바이스의 상태에 기초하여 보고하는 요소들뿐만 아니라 게이트웨이에게 전달되는 특정 데이터를 기술하고 있다.

▪ Service Model : 개인건강 디바이스와 데이터의 상호작용에 대해 기술한 것으로 DIM으로부터 데이터를 교환하기 위하여 디바이스와 게이트웨이 사이에서 전송된 데이터 접근 프리미티브(Get, Set, Action 및 event report 등과 같은 명령어들)를 제공한다.

▪ Communication Model : 연결 상태 머신과 통신 특성에 대해 기술한 것으로 단일 관리자에게 점-대-점 연결 기능을 전송하는 한 개 또는 다수 개인건강 디바이스들 위치를 지원한다. 각 점-대-점 연결의 경우, 동적인 액션은 연결 상태 관리자에 의해 정의되는데, 이때 연결 상태 머신이 상태를 정의하고 개인건강 디바이스를 설정하며, 연결, 연관성 및 운용과 관련된 상태를 포함한다. 아울러 통신 모델은 측정 데이터 전송을 위한 다양한 운용 절차를 포함한 각각의 상태들에 대한 입력, 출력 및 에러 상태를 상세하게 정의한다.

그 외 프로토콜에 대한 자세한 사항들은 표준 문건[2]을 참조하기 바란다.

2. 사용자 프라이버시보호를 위한 이전의 방법[1]

본 절에서는 우리가 지난 2014년에 발표한 이전의 프라이버시 보호 방법[1]에 대해 소개하고자 한다.

앞서 살펴본 ISO/IEEE 11073-20601에서는 개인건강 디바이스와 게이트웨이 간 상호 정보 전송을 위해 ASN.1 부호화

규칙인 MDER(Medical Device Encoding Rule)을 사용하고 있다. ASN.1은 국제전기통신연합(ITU)에서 정의한 네트워크 상의 데이터 교환을 정의한 프로토콜로 다른 기종 간 추상화된 메시지를 교환하기 위한 형식적인 언어이다. 단순히 표준을 정의한 언어이며, ASN.1으로 작성된 데이터가 표준이 된다. MDER을 C언어로 구현하면 구조체들로 선언하여 사용하는데, 기본 데이터를 전송하는 구조체로는 APDU라는 구조체를 사용하여 데이터를 전송한다. APDU 구조체 안에는 다시 AARQ_apdu, AARE_apdu, RLRQ_apdu, RLRE_apdu, ABRE_apdu, PRST_apdu의 6개의 메시지 포맷이 존재하며 상황에 따라 6개의 메시지 중 한 가지의 메시지로 통신을 하게 된다.

한편 개인건강 디바이스 측에서는 먼저 자신의 구성정보를 보내고, 게이트웨이는 이 구성정보를 받아서 확인한다. 그 후 처음 접속 시 구성정보를 저장하여 또다시 접속을 시도할 경우 구성정보의 아이디만 확인하여 바로 통신을 할 수 있도록 한다(그림 2 참조).

그림 2에서 프라이버시 보호와 관련하여 사용자의 신분을 알리는 값은 system-id이며 개인건강 디바이스의 신분을 알리는 값은 dev-config-id 단 두 가지이다. 이 두 값은 그림 2에서 첫 번째와 두 번째 단계인 association Request(AARQ_APDU)와 association response(AARE_APDU)에 해당한다. 먼저 AARQ_APDU의 데이터 포맷은 다음과 같이 구성된다(그림 3 참조). AARE_APDU의 경우는 이전 AARQ_APDU에 대한 응답으로서 그림 3에서 PHD association information 중 option list가 제외되며 그 외는 동일하다. 여기서 종전 표준의

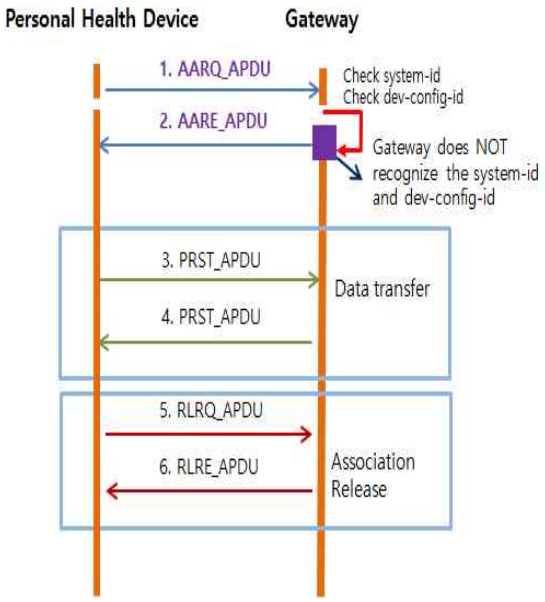

그림 2. ISO/IEEE 11073-20601 통신절차[2]

문제점을 발견 할 수 있다. 그것은 바로 이들 두 값(system-id and dev-config-id)이 신뢰할 수 없는 제 삼자에게 그대로 노출된다는 점이며 이는 다시 말해 환자의 프라이버시가 보호받지 못하고 있다는 점이다.

이러한 문제점을 해결하기 위한 기본 아이디어는 환자의 ID가 포함된 필드를 잘 알려진 대칭키 암호화 알고리즘들(예를 들어 AES, Blowfish 등)을 이용하여 암호화 하는 것이다. 이를 위해 개인건강 디바이스와 게이트웨이 측에서는 사전에 비밀키가 분배되어 있다고 가정한다. 이것은 제품 생산이나 판

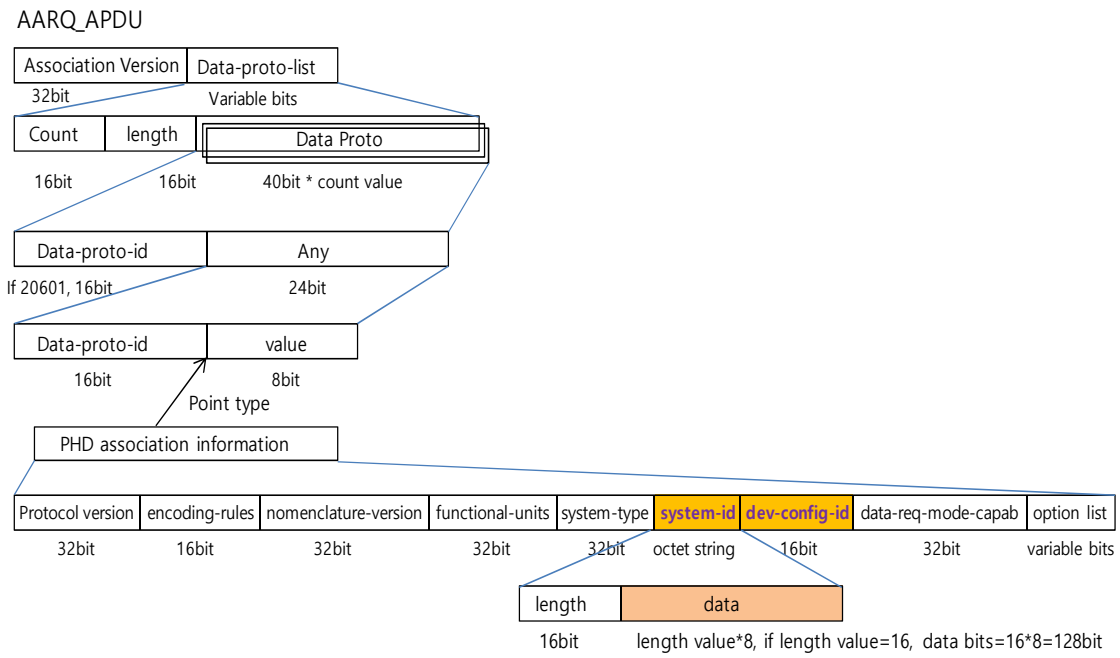

그림 3. AARQ_APDU 메시지 데이터 포맷

매 시 인증 서버 등을 통해 사전에 미리 분배할 수 있을 것이다(그림 4 참조). 본 프로토콜에 대한 그밖에 자세한 사항들은 논문 [1]을 참조하기 바란다.

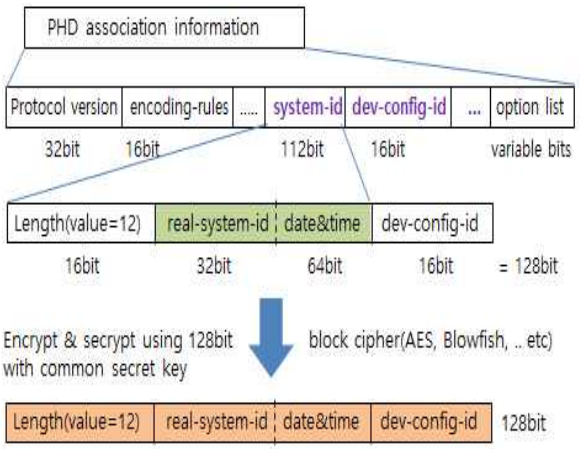

그림 4. 프라이버시 보호를 위한 이전 방법[1]

III. 제안하는 방법

본 장에서는 이전에 제안한 사용자 프라이버시 보호를 위한 기본 방법 [1]을 개선하여 새로운 확장된 방법을 제안하고자 한다. 제안하는 방법은 기존 방법에 비해 무결성을 보장하고 전송 시 대칭키 암호화를 통해 보다 안전한 전송을 추가로 보장한다.

제안하는 방법의 기본 아이디어는 기존 PHD association information 가운데 option 필드를 제외한 부분을 대칭키 암호 알고리즘을 이용하여 1차로 암호화 하고 암호화된 부분을 암호학적인 해시함수를 이용하여 해시된 MAC(Message Authentication) 값을 option list 필드에 저장하여 게이트웨이로 전송한다. 이때 최종 전송 시 보안 전송을 위해 PHD association information가 포함된 AARQ_APDU 메시지 전체를 다시 한번 대칭키로 암호화하여 최종 전송한다. 한편 수신된 메시지를 전송받은 게이트웨이 측에서는 공통 비밀키를 이용하여 암호화된 메시지를 복호화한 다음, 개인건강 디바이스에서 보내온 MAC 값을 확인하여 전송받은 정보에 위변조가 없었는지를 추가로 확인하게 된다.

제안하는 프로토콜은 아래와 같다(그림 5 참조).

[단계 1] 개인건강 디바이스가 최초로 AARQ_APDU 메시지를 게이트웨이로 보낼 때 PHD association information 내에 고정된 길이 값 12([그림 5]에서 System ID와 Date&time의 길이를 합한 12*8=96비트를 의미함)와 함께 system-id를 32비트로 구성(이를 real-system-id로 부름) 한 뒤 보낼 당시의 날짜(date)와 시간(time) 값(64bit로서 개인건강 디바이스

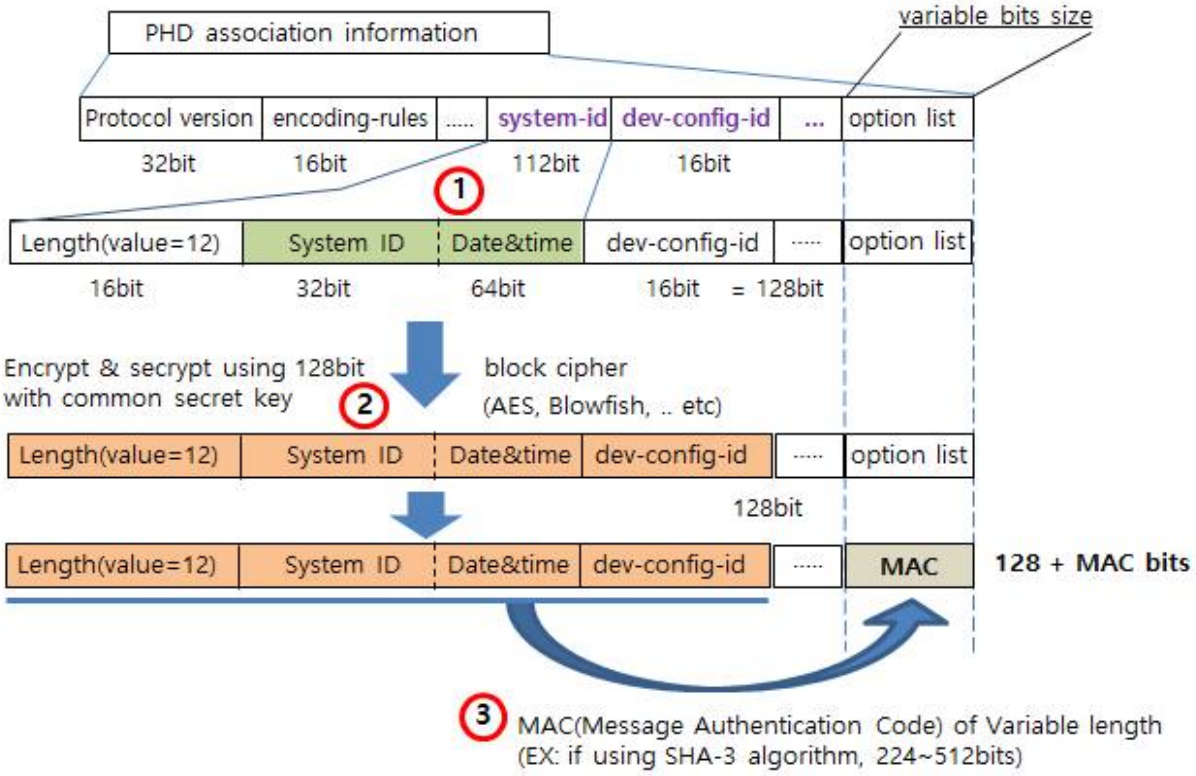

그림 5. 제안하는 방법의 기존 절차도

내에 자체 내장된 값을 이용함), 그리고 dev-config-id 값을 붙여 함께 저장한다.

[단계 2] 그 후 개인건강 디바이스와 게이트웨이가 사전에 분배하고 있는 공통 비밀키인 세션키 Sk를 이용하여 앞서 [단계 1]에서 저장한 메시지를 AES나 Blowfish와 같은 대칭키 암호 알고리즘을 이용하여 암호화한다.

[단계 3] 개인건강 디바이스는 앞서 [단계 2]에서 생성한 메시지를 암호학적인 해쉬함수(예 : SHA-3 등)를 이용하여 계산한 후, 계산된 MAC 값을 PHD association information의 option list에 저장한다.

[단계 4] 앞서 [단계 3]에서 생성한 메시지가 포함된 전체 AARQ_APDU 메시지(그림 3 참조)를 MDER에 따라 인코딩한 후 [단계 2]에서 사용한 세션키 Sk를 이용하여 AES나 Blowfish와 같은 대칭키 암호 알고리즘을 이용하여 암호화한 다음 이를 게이트웨이에게 전송한다.

[단계 5] 게이트웨이는 개인건강 디바이스로부터 전송받은 AARQ_APDU 메시지를 개인건강 디바이스와 공유하고 있는 공통 비밀키인 세션키 Sk를 이용하여 복호화한 후 MDER에 따라 디코딩한다.

[단계 6] 게이트웨이는 앞서 [단계 2]를 통해 암호화되어 있는 메시지를 세션키 Sk를 이용하여 복호화하여 real-system-id와 dev-config-id, 그리고 해시값 MAC을 확인하고 저장한 후 개인건강 디바이스에게 AARQ_APDU 메시지에 대한 응답으로 AARE_APDU 메시지를 보낸다.

[단계 7] [단계 6] 이후의 과정은 기존의 ISO/IEEE 11073-20601 표준 통신 프로토콜과 동일하게 진행한다.

1. 제안하는 방법에 대한 무결성 및 안전성 분석

제안하는 방법은 이전 [1]의 방법과 동일하게 암호화된 필드의 값 중 date&time 값을 사용하기 때문에 매번 AARQ_APDU 메시지를 보낼 때마다 값이 바뀌게 된다. 따라서 신뢰할 수 없는 제 삼자로부터 재사용 공격(replay attack)을 막을 수 있으며 개인건강 디바이스를 이용하는 환자의 프라이버시 또한 보호받을 수 있다. 예를 들어 동일한 디바이스를 이용하는 여러 환자들이라든가 디바이스가 다른 동일한 환자의 경우 또한 마찬가지이다.

[단계 3]에서는 [단계 2]에서 암호화 한 128비트 값의 무결성 보장을 위해 option list 필드에 암호학적인 해시값 MAC를 제안하고 있다. 암호학적인 해시함수의 경우 이미 이론적으로 무결성에 대한 정확성과 안정성이 검증된 것으로 특히, MAC의 경우는 가변 길이의 메시지들에 대해 유연한 대처가 가능하고 [단계 2]에서 사용한 세션키 Sk를 이용하여 해시함수 계산이 가능한 이점이 있다. 실제 사용 시는 예를 들어, SHA-3 해시 알고리즘을 이용하여 224비트 길이의 고정된 MAC 값을 얻을 수 있다.

제안하는 방법은 기본적으로 128비트 대칭키 블록암호 알고리즘을 채택하였다. 물론 저전력의 특성을 지닌 개인건강 디바이스 즉, 바이오센서의 경우 계산 능력이나 메모리 등에 있어 한계가 있기 때문에 응용에 따라서는 128비트 보다 적은 암호 알고리즘을 이용할 수 있을 것이다. 이 경우에는 반드시 system-id 필드의 길이 부분을 출력 사이즈에 맞게 값을 게이트웨이와 함께 조정하고 고정할 필요가 있다. 고정하는 이유는 게이트웨이에서 디코딩 시에 길이 값에 따라 뒤따르는 데이터 필드의 길이가 정해지기 때문이다.

한편 제안하는 방법의 [단계 4]에서는 개인건강 디바이스가 AARQ_APDU 메시지 전체를 암호화하는 방법을 제안하고 있으나 이 경우는 앞서 말한 저전력의 센서 특성을 감안할 때 추가적인 오버헤드가 발생하여 실제 사용 시 부담이 될 수 있다. 그러나 이 방법은 전송 데이터의 안전성을 감안할 때 필요한 사항이지만 응용에 따라 효율성을 위해 [단계 4]와 [단계 5]에서 제시한 암복호화 과정은 생략될 수도 있을 것이다.

Ⅳ. 결론 및 향후 연구방향

우리는 지금까지 가정 내에서 원격진료를 이용하는 개인건강 디바이스 통신 환경에서 이전 [1]에서 제안한 환자 프라이버시를 보호를 위한 기본 방법에 이어 전송 데이터의 무결성과 안전성을 보장하는 보다 강건한 프로토콜을 제안하였다.

제안한 방법은 기존 제품들과의 상호 호환성을 위해 국제 표준 프로토콜인 ISO/IEEE 11073-20601 규격을 기본 프레임워크로 이용하였다. 또한 향후 Continua Health Alliance [10]나 관련된 ISO 혹은 IEEE 그룹에서 보안에 대한 추가적인 규격을 제안할 때 기초적인 자료로 매우 활용 가치가 높을 것으로 사료된다.

향후 연구로는 제안한 방법을 실험을 통해 기존 프로토콜과의 성능차이를 확인하고 개인건강 디바이스와 게이트웨이간 보안성을 보다 강화하기 위해 사용자 역할 또는 등급별 접근제어에 관한 새로운 프로토콜을 제안해보고자 한다.

References

[1] Soon Seok Kim, Yong Hee Lee, Jong Mo Kim, Deok Seok Seo, Gwang Hee Kim, and Yoon Seok Shin, "Privacy Protection for Personal Health Device Communication and Healthcare Building Applications", *Journal of Applied Mathmatics*. Vol.2014, 2014.

[2] ISO/IEEE, 11073-20601: health informatics-personal health device communication, application profile optimized exchange protocol, http://www.iso.org.

[3] Inyong Lee, Soonki Jeong, Sangsoo Yeo, and Jongsub Moon, "A novel method for SQL injection attack detection based on removing SQL query attribute value", *Mathematical and Computer Modelling*,

Elsevier, Vol. 55, Issues 1-2, pp.58-68, January 2012.
[4] Binod Vaidya, Jong Hyuk Park, Sang-Soo Yeo, and Joel J.P.C. Rodrigues, "Robust one-time password authentication scheme using smart card for home network environment", *Computer Communications*, Elsevier, Volume 34, Issue 3, pp. 326-336, 15 March 2011.
[5] A. Appari, and M. E. Johnson, "Information security and privacy in healthcare: current state of research", *Int. J. Internet and Enterprise Management*, v. 6, n. 4, pp. 279-314, 2010.
[6] P. Kumar and H. J. Lee, "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey", *Sensors*, v. 12, pp. 55-91, 2012.
[7] A Kliem, M Hovestadt, and O Kao, "Security and Communication Architecture for Networked Medical Devices in Mobility-Aware eHealth Environments", *IEEE First International Conference on Mobile Services (MS)*, 2012.
[8] OJ Rubio, A Alesanco, and J Garcia, "A robust and simple security extension for the medical standard SCP-ECG", *Journal of Biomedical Informatics*, 2012.
[9] Denis Foo Kune, Yongdae Kim, Krishna Venkatasubramanian, Insup Lee, and Eugene Vasserman, "Toward a Safe Integrated Clinical Environment: A Communication Security Perspective", *MedCOMM'12, Proceedings of the 2012 ACM workshop on Medical communication systems*, pp. 7-12, 2012.
[10] Continua Health Alliance, http://www.contiuaalliance.Org
[11] 이창무, 오승교, 최덕재, "활성산초 측정 데이터를 위한 모바일기반의 U헬스 시스템 설계 및 구현, 스마트미디어저널, Vol. 1, No. 4, pp 59-71, 2012년 12월

저 자 소 개

김순석(정회원)

1999년 한국정보보호진흥원 기술기준팀 연구원.
2003년 중앙대학교 컴퓨터공학과 박사 졸업.
2016년 현재 한라대학교 컴퓨터공학과 재직 중
<주관심분야 : 의료정보보안, 표준>

이재현(정회원)

1989년 중앙대학교 컴퓨터공학과 학사 졸업.
2001년 중앙대학교 컴퓨터공학과 석사 졸업.
2007년 연세대학교 인지과학 박사 졸업.
2016년 현재 강릉원주대 정보기술공학과 재직 중
<주관심분야 : 의료정보윤리, 의료정보보안 표준>