논문 2013-50-2-25

착용형 개인 건강관리 장치를 위한 실시간 생체신호 암호화 모듈의 설계

(Design of Real-time Vital-Sign Encryption Module for Wearable Personal Healthcare Device)

김 정 채*, 유 선 국**

(Jungchae Kim and Sun Kook Yoo)

요 약

정보통신 기술을 이용한 개인 의료정보의 교환은 건강관리 서비스의 중요한 과정이다. 그러나 그 과정은 정보유출의 위험성을 내포하므로 건강관리 서비스의 신뢰성을 보장하기 위하여 개인 의료정보는 보호되어야 한다. 본 논문에서는 착용형 개인 건강관리 장치에서 생성되고 전송되는 개인의료 정보를 보호하기 위한 암호화 모듈을 설계하였다. 설계의 주요 목표는 실시간으로 암호화되어 전송 된 개인 의료정보가 당사자의 허가 없이 조회, 수정 및 활용될 수 없음을 보장하는 것이다. 이를 위하여 암호화 알고리즘으로 DES와 3DES를 Telos Rev B(16bit RISC, 8Mhz)에서 운용되는 모듈로 개발하였다. 그리고 실험은 착용형 개인 건강관리 장치에서 측정되는 생체신호에 대한 암호화 및 복호화 성능을 평가하기 위하여 수행되었다. 실험 결과 단위 블록에 대한 암호화에 DES가 1.802 ms, 3DES가 6.683 ms가 소요되었다. 또한 Telos Rev B에서 암호화 된 정보가 다른 장치에서 오류 없이 복호화 될 수 있음을 확인함으로써 이종 기기 간 상호 운용성을 확인하였다. 결과적으로, 암호화 모듈이 사용자에게 개인 건강정보 접근권한에 대한 매우 강력한 의사결정권을 부여 할 수 있는 방법이므로 향후 신뢰적인 건강관리 서비스 구축에 기여 할 수 있을 것이다.

Abstract

Exchanging personal health information(PHI) is an essential process of healthcare services using information and communication technology. But the process have the inherent risk of information disclosure, so the PHI should be protected to ensure the reliability of healthcare services. In this paper, we designed encryption module for wearable personal health devices(PHD). A main goal is to guarantee that the real-time encoded and transmitted PHI cannot be allowed to be read, revised and utilized without user's permission. To achieve this, encryption algorithms as DES and 3DES were implemented in modules operating in Telos Rev B(16bit RISC, 8Mhz). And the experiments were performed in order to evaluate the performance of encryption and decryption using vital-sign measured by PHD. As experimental results, an block encryption was measured the followings: DES required 1.802 ms and 3DES required 6.683 ms. Also, we verified the interoperability among heterogeneous devices by testing that the encrypted data in Telos could be decoded in other machines without errors. In conclusion, the encryption module is the method that a PHD user is given the powerful right to decide for authority of accessing his PHI, so it is expected to contribute the trusted healthcare service distribution.

Keywords : Personal health device, vital-sign, real-time encryption, wearable, u-healthcare

* 학생회원, 연세대학교 일반대학원 생체공학협동과정
(Graduate School of Biomedical Engineering, Yonsei University, Seoul, Korea)
** 정회원, 연세대학교 의과대학 의학공학교실
(Department of Medical Engineering, College of Medicine, Yonsei University, Seoul, Korea)
※ 본 연구는 2012년도 정부(교육과학기술부) 한국연구재단(No. 2010-0023833), 지식경제부 한국산업기술진흥원의 전략기술인력양성사업(No.2012-8-1382)과 산업융합원천기술개발사업(10031977)으로 지원된 연구결과입니다.
접수일자: 2012년11월9일, 수정완료일: 2013년1월20일

Ⅰ. 서 론

고령화 사회에는 질병 관리를 위한 의료비용이 필연적으로 증가하게 된다. 이에 대응하기 위하여 건강관리(Healthcare) 서비스를 질병관리에 활용하기 위한 노력이 이루어지고 있다. 건강관리 서비스는 IT 시스템과 생체계측 시스템을 이용하여 질병, 만성질환의 예방 목적으로 제공되는 서비스이며, 일반적으로 IT 기술을 이용하여 언제 어디서나 개인의 건강을 증진시키기 위한 인프라와 요소기술 개발, 서비스 구축을 목표로 한다.[1~4] 그 중에서 개인건강기기(Personal Health Device, 이하 PHD)는 생체 계측 기술을 기반으로 생성되는 개인건강 정보(Personal Health Information, PHI)를 의료정보 저장 및 교환소(Health Care Repository and Clearinghouse, HCRC)으로 전송 할 수 있는 기능을 갖춘 사용자 휴대용 단말이다.[5] 따라서, PHD에서 수집되는 PHI는 건강관리 서비스 제공자(Healthcare Service Provider, HSP)에 의해 수집 및 관리되고 자동화 된 의사결정 시스템(Decision Support System, DSS) 등을 기반으로 개인 중심의 건강관리 서비스가 제공 될 수 있다. 이러한 정보의 수집을 토대로 개인 평생 전자건강기록 관리(Personal Health Record, 이하 PHR) 서비스가 활성화 될 수 있다. PHR은 기존의 전자진료기록(Electronic Health Record)에서 진화 된 형태로써 개인이 접근, 관리 할 수 있고 그들의 건강 정보를 사적이고 안전하게, 그리고 기밀한 환경에 있는 인증 된 타인에게 공유하는 전자적 어플리케이션으로 정의 할 수 있다.[6]

PHR의 활성화를 위한 방향에 대해서 Paul C. Tang[6]의 연구에서는 EHR과 테더링 되거나 상호 간 연결 되도록 통합 된 PHR이 독립형의 PHR 보다 더 유익하다고 설명하고 있다. 즉, PHR의 상호 운용을 위한 하여 PHR에 저장 된 PHI가 전자적으로 통합 된 형태의 문서로 교환 될 수 있어야 함을 의미한다. 그러나 PHI는 매우 중요한 개인 정보이므로 교환 과정에 절대 임의로 조회 되거나 유출 되어서는 안 되며, 저장 혹은 전송 시 반드시 보호 되어야 한다.[6,7] 따라서 건강관리 서비스가 활성화되기 위해서는 먼저 PHR이 EHR과 연동 되어 PHI를 관리 할 수 있는 인프라를 구축하고 HSP 및 이해당사자간 신뢰적인 시스템 구축이 선행되어야 할 것이라 판단된다. 또한 신뢰적 시스템 구축을 위하여 PHI 보호에 대한 기술적인 방법을 구체적으로 제시해야 할 필요가 있다.

PHD에 대한 구체적인 정의 및 데이터 교환, 통신 프로토콜, 장비별 권고사항에 대한 표준은 ISO/IEEE 11073에 의하여 제정되어 있으며,[9] HIPAA(Health Insurance Portability and Accountability Act)에서 건강 정보 보호와 관련 된 법률을 제정하여 그 보호의 의무를 명시하고 있다.[7] 그러나 PHD 관련 정보 보호에 대한 구체적인 방법론은 아직 권고사항에 머물러 있는 실정이다. 따라서 본 연구에서는 PHD에서 생산되는 PHI를 전송 시 보호 할 수 있는 시스템을 제안하고, 그 성능평가를 통해 활용 가능성을 확인하고자 한다.

일반적으로 PHD에서는 HSP의 HCRC으로 전송하는 과정에 대해서 대부분 정보 보호 및 암호화와 관련 된 측면이 고려되지 않거나, 개인 스마트폰 또는 라우터와 같은 게이트웨이 역할을 수행하는 단말에서 수행하고 있다.[9~10] 이러한 방식의 PHI 암호화는 크게 두 가지 문제점을 앉고 있다. 첫 번째로 대부분의 PHD 사용자는 게이트웨이에서 암호화를 정확히 수행하는 지를 신뢰하지 않는다. 그 이유는 스마트폰과 같은 오픈 플랫폼 장치가 개인 정보 유출의 위험에 노출 되어 있기 때문이다. 두 번째는 게이트웨이에서 제공하는 정보보호 방식이 PHI 접근에 대한 권한 부여를 당사자가 관리하기 어렵게 만든다는 것이다. 이러한 문제점이 개인 정보의 수집에 대한 불쾌감 혹은 거부감으로 작용하여 PHD가 활성화되는데 매우 중요한 장애물로 작용 할 수 있다.[11~12]

본 연구에서는 무선 개인 영역 네트워크(Wireless Personal Area Network, 이하 WPAN)에서 사용되는 착용형 PHD에서 사용자가 관리하는 비밀 키(56bit 또는 168bit)를 이용한 DES(Data Encryption Standard) 알고리즘으로 실시간암호화 생체신호를 전송하는 시스템을 개발하였다. 연구개발의 목적은 두 가지로 설명할 수 있다. 첫 번째로 개인이 착용한 PHD에서 비밀키로 암호화 되어 전송되는 PHI는 본인의 허락 및 비밀 키 관련 정보 제공 없이는 누구도 해석 할 수 없기 때문에 사용자가 신뢰 할 수 있는 시스템을 구축하기가 용이하다. 두 번째로 향후 건강관리 서비스가 활성화되면 HCRC로 막대한 양의 건강 데이터(Health Big Data, 이하 HBD) 수집 될 것으로 예상되는데 게이트웨이와 같은 중계기에서 다수의 착용형 PHD의 암호화를

수행하는 것은 데이터 처리 및 관리의 측면에서 비효율적이다. 따라서 착용형 PHD에서 직접 암호화 된 데이터를 전송 할 경우 게이트웨이 단말에서의 처리부하를 분산 시킬 수 있는 장점이 있다.

논문의 구성으로 먼저 PHD와 건강관리 서비스에 대하여 소개하고 본 연구에서 제안한 모듈의 설계 및 개발 방법에 대하여 설명한 다음 개발 된 암호화 표준 방법의 검증과 실시간 생체신호 암호화 전송 성능평가를 수행하여 활용 가능성을 평가하고자 한다.

Ⅱ. 본 론

1. PHD 기반 건강관리 서비스

본 연구에서 제안 한 암호화 모듈이 적용된 착용형 PHD 기반 건강관리 서비스의 시나리오를 그림 1에 표현하였다. 가장 먼저 PHD USER(사용자)가 비밀키를 본인의 단말에 설정하면, 측정되는 생체신호와 이를 기반으로 생성 된 PHI는 암호화되어 WPAN과 게이트웨이를 통해 HSP의 HCRC로 전송 및 저장된다. 이로써 사용자는 본인의 단말에서 암호화 된 PHI에 대한 접근 및 해석 할 수 있는 권한을 관리하게 된다. 그러므로 HSP으로부터 요청되는 비밀키 배포 및 배포대행 여부를 PHD 사용자가 스스로 결정 할 수 있다.

다음으로 HSP는 HCRC에 사용자가 암호화하여 전송한 데이터를 관리, 저장, 그리고 자동화 된 DSS를 이용하여 건강관리 서비스를 사용자에게 제공한다. 핵심은 사용자 이외에 PHI에 접근하여 해석하려는 Demanders (이하 접근자)를 제어하는 역할이다. HSP는 사용자에

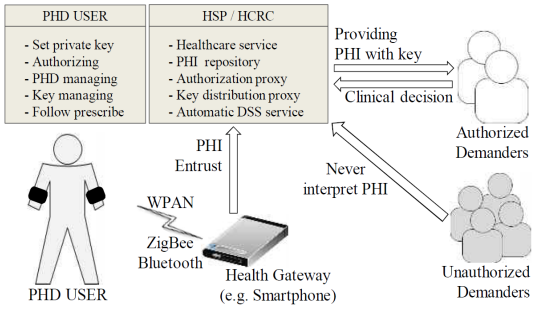


그림 1. 제안 된 암호화 모듈이 적용 된 착용형 PHD 기반 건강관리 서비스 시나리오

Fig. 1. The wearable PHD based healthcare service scenario applied with proposed encryption module.

게 특정 접근자에게 사용자의 PHI에 대한 접근 권한 부여에 대해 결정하도록 알리고, PHI에 대한 비밀키의 배포는 사용자의 결정을 따른다. 이 때, 사용자의 허가에 의하여 HSP가 그 결정을 대행 할 경우 PHI와 비밀키 배포를 HSP가 결정한다. 즉, 이런 경우 HSP는 PHI를 비밀키와 함께 접근자에 전달한다.

접근자는 특정 사용자의 PHI에 접근 할 때 HSP에게 권한을 요청하고 사용자로부터 권한을 부여 받게 되면 PHI와 함께 비밀키를 전송받아 해당 정보를 해석 할 수 있게 된다. 만약, 권한을 부여받지 못한 접근자가 비정상적으로 PHI를 유출하여 조회하게 되더라도 비밀키 없이 정보를 해석하는 것은 매우 어렵기 때문에 사용자의 PHI를 최대한 보호 할 수 있는 것이다. 그림 1에 나타낸 시나리오의 강점은 사용자에게 본인의 PHI에 대한 접근 및 해석의 권한을 부여 할 수 있는 결정권을 갖게 함으로써 착용형 PHD 사용에 대한 개인 정보 보호를 보장하고, 정보유출 가능성에 대한 거부감을 억제 할 수 있다는 점이다.

2. 실시간 생체신호 암호화 시스템 설계

가. 착용형 PHD 플랫폼의 구성

(1) 하드웨어 플랫폼

계측 회로로부터 생체신호를 획득하고 암호화하여 WPAN을 이용하여 전송 할 하드웨어 플랫폼으로 Telos Rev B를 이용하였다. 이는 초저전력 무선 센서 모듈로써 UC Berkeley에서 개발하여, 무선 센서 네트워크(Wireless Sensor Network, 이하 WSN) 연구에 사용되는 플랫폼이다. TI MSP430 16bit RISC 마이크로 컨트롤러를 사용하여 12bit ADC를 내장하고 있으며, 48KB의 프로그램 메모리와 10KB의 램을 지원한다. 무선 인터페이스로 IEEE 802.15.4를 지원하며, 이를 위해 Chipcon CC2420을 이용한다. 초저전력 모듈로써 최소 1.8v의 전압에서도 동작하도록 설계되어 있으며, USB 인터페이스를 이용하여 PC와 시리얼통신을 할 수 있도록 설계 되었다.[13]

(2) 생체신호 계측 센서 플랫폼

착용형 PHD 플랫폼 구성을 위한 회로는 심전도와 반사형 PPG(Photoplethysmography)를 측정하는 회로

표 1. 생체 계측 센서 플랫폼 설계 사항
Table 1. The specification of bio sensor platform.

Target	Bandwidth	Gain	Body interface
PPG	0.05~16 Hz	4	TDS2000, BIOPAC
ECG	0.01~250 Hz	1000	Ag-AgCl

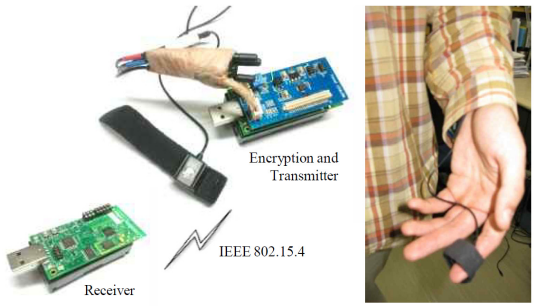


그림 2. 착용형 PHD 플랫폼 구성
Fig. 2. Wearable PHD platform configuration.

로 구성 된다(표 1). 각 회로의 설계 사항으로 3-리드 심전도 측정 회로는 0.5~100 Hz의 대역폭과 60 Hz 전원잡음제거 회로를 포함하고, 이득 1000배로 설계하였다. 반사형 PPG(Replextion plethysmography) 측정 회로는 0.5~16 Hz의 대역폭과 이득 4배로 설계하였다. 각 센서로는 심전도가 Ag-AgCl 전극을 이용하고, PPG는 TDS200(BIOPAC)을 이용한다. 본 연구에 사용 된 착용형 PHD는 그림 2에서 확인 할 수 있다.

(3) 무선 센서네트워크 운영체제

본 연구에서는 Telos에서 활용 될 수 있는 운영체제로로 RETOS(Resilient, Expandable, and Threaded Operating System for Wireless Sensor Networks)를 사용하였다. 그 특징으로 멀티스레드 프로그래밍 인터페이스를 제공하고 커널과 응용 프로그램 분리로 강인한 시스템 운용을 보장하며, 동적 모듈 프로그래밍으로 커널의 확장성을 지원한다. 즉, 생체계측 센서보드를 연결하고 응용프로그램에서 사용 할 수 있는 디바이스 드라이버를 개발함으로써 동적으로 소프트웨어를 구성할 수 있다. 또한, 표준 C 언어를 지원하기 때문에 TinyOS에서 사용하는 nesC와는 차별화 된 편리한 개발 환경을 지원한다.[14] 본 연구에서는 멀티스레딩을 지원하는 운영체제의 특성을 활용하여 병렬 프로그래밍이 가능하기 때문에 효과적으로 소프트웨어를 설계하였다.

나. DES/3DES 알고리즘 구현

(1) DES/3DES의 소개

DES(Data Encryption Standard)는 미국의 NIST (National Institute of Standards and Technology)에서 1977년 최초로 채택 된 암호화 알고리즘으로 64비트의 암호화키(56비트-암호화키, 8비트-검사용키)를 이용하여 64비트의 블록을 암호화 한다. 1993년 이후 DES가 안전하지 않은 알고리즘으로 알려지면서, 암호화키가 3배이며 DES를 3회 수행하는 3DES가 임시 표준 사용되어져 오다가 2001년 AES(Advanced Encryption Standard)으로 Rijindeal이 새로운 표준으로 채택되어 현재까지 암호화 표준으로 사용되고 있다.[15] 그러나 본 연구에서는 착용형 PHD의 목표 시스템이 초저전력 16비트 마이크로컨트롤러임을 감안하였을 때, 비트에 관한 연산자를 이용해 처리 가능한 DES를 내장하여 생체신호를 실시간 암호화 하자 하였다. 그리고 부족한 암호화 안전성을 보완하기 위해 3DES 알고리즘을 구현하여 암호화 모듈을 선택적으로 사용할 수 있도록 하였다.

(2) 16bit MCU용 DES/3DES 라이브러리 구현

그림 3의 순서도는 16비트 MCU에서 64비트 블록 암호화를 수행하는 DES/3DES 알고리즘을 설계한 순서도이다. MCU의 내장메모리와 프로그램메모리의 크기에

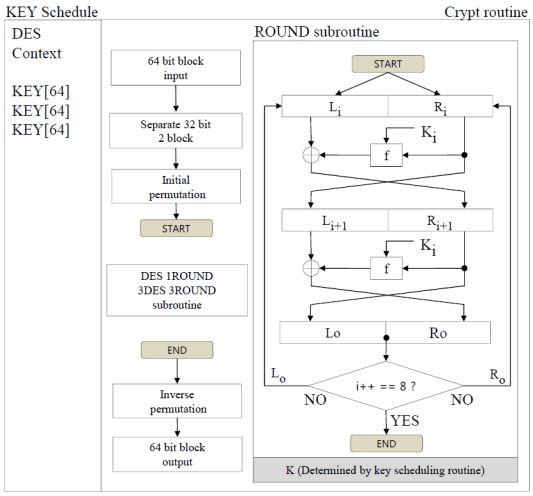


그림 3. 16bit 마이크로컨트롤러에 최적화 된 DES/3DES 알고리즘설계
Fig. 3. Design of optimized DES/3DES algorithm for 16bit micro-controller.

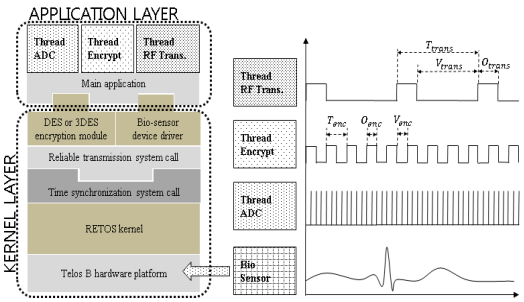


그림 4. 멀티스레딩 기반 소프트웨어와 타이밍도 설계
Fig. 4. Multi-threading based software and timing diagram design.

적합하도록 ROUND를 서브루틴으로 설계하여 코드 사이즈를 최적화 하였다. 또한, 16비트 코어에서 암호화 된 블록이 32비트, 64비트 코어에서 정상적으로 복호화 되도록 하기 위하여 필수적으로 키 스케줄링 루틴과 이니셜 퍼뮤테이션, 인버스 퍼뮤테이션 코드의 비트관련 연산자에서 오버플로우가 발생하지 않도록 알고리즘을 구현하였다. 오버플로우가 발생 할 경우 복호화 불가능한 블록을 출력하는 등의 문제가 발생 할 수 있으므로 16비트 연산에 최적화 된 코드를 작성하였다. 추가로 3DES는 ROUND 서브루틴을 3회 수행하는 등 DES 코드를 기반으로 수정하여 구현하였다.

다. PHD 소프트웨어 설계 및 구현

(1) 멀티스레드 스케줄링

설계 된 소프트웨어의 개요를 그림 4에 정리하였다. 생체 계측 센서플랫폼으로부터 데이터를 수집하기 위한 디바이스 드라이버와 DES/3DES 암호화 라이브러리를 동적 모듈화하여 설치하였다. 메인 어플리케이션을 효율적으로 운용하기 위한 멀티스레드 스케줄링은 다음의 파라미터를 이용하여 설계하였다. T_{adc}는 양자화 표본 추출 주기이고, T_{enc}은 암호화 수행 주기이다. T_{trans}는 무선 전송 주기이다. 식 (1)~(5)는 각 파라미터 간의 관계를 설명한다. 기본적으로는 표본추출 비율에 따라서 각 파라미터가 동적으로 변화하도록 소프트웨어를 설계하였다. 그 이유는 생체 계측 센서 플랫폼이 측정하고자 하는 생체신호마다 표본추출 비율이 다르기 때문이다. 설계 된 소프트웨어는 센서 플랫폼을 교체 할 때 디바이스 드라이버의 변경으로 멀티스레드 스케줄링을 위한 식 (1)~(5)를 갱신하기 때문에 메인 어플리케이션의 수정이 필요 없도록 설계하였다. 이러한 방식의 멀티스레드 스케줄링을 통해 불필요한 스레드의 동작을 억제하고 스레드 간 충돌을 방지 할 수 있다. 그러므로 스레드가 작업을 수행한 뒤 스스로 비활성화 되고 필요한 시점에 활성화 되도록 스케줄링 하였기 때문에 불필요한 리소스를 낭비하지 않을 수 있다.

$$SamplePerBlock\,(SPB) = 4 \tag{1}$$

$$BlockPerFrame\,(BPF) = 4 \tag{2}$$

$$T_{adc} = \frac{1}{SampleRate} \tag{3}$$

$$T_{enc} = SPB \times T_{adc} \tag{4}$$

$$T_{trans} = BPF \times T_{enc} \tag{5}$$

그러나 각 스레드에서 코드가 비정상적으로 오랜 시간 시스템 자원을 점유하였을 경우 멀티스레드의 스케줄링 오차 문제를 방지하기 위하여 식 (6)~(8)의 파라미터를 사용한다. 각 스레드의 주기에서 작업 수행에 걸린 시간을 제외한 시간만큼 비활성화 되도록 하였다.

$$V_{adc} = T_{adc} - O_{adc} \tag{6}$$

$$V_{enc} = T_{enc} - O_{enc} \tag{7}$$

$$V_{trans} = T_{trans} - O_{trans} \tag{8}$$

(2) 멀티스레드의 공유 버퍼 설계

3개의 멀티스레드가 각각의 데이터 버퍼를 가지고 작업을 처리하기에 MCU의 내장 메모리와 프로세싱 자원이 제한적이다. 따라서 중복 된 처리를 최소화하기 위하여 스레드 간 데이터 버퍼를 공유하도록 하였다. 공유 버퍼는 원형 버퍼 기반으로 설계하였으며, 크기는 무선 전송 패킷에 포함되는 32 바이트의 배수인 256 바이트로 결정하였다. 공유 버퍼 사용 시 각 스레드가 유효하지 않은 데이터에 대한 접근 시 비정상적인 데이터 처리가 발생할 수 있다. 이 문제를 해결하기 위하여 각 스레드가 작업 수행 후 버퍼 오프셋 정보를 갱신하고 다음 작업 수행 전 버퍼 접근 여부를 오프셋 정보를 토

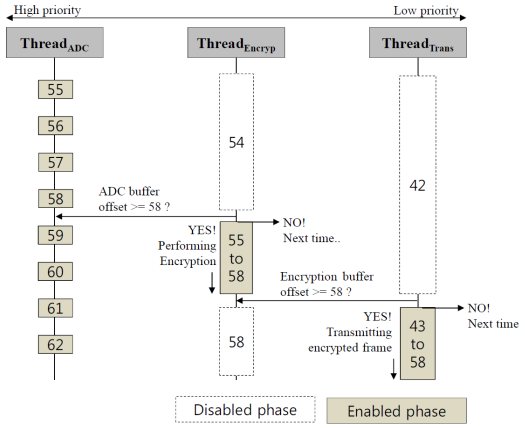


그림 5. 공유버퍼에 대한 멀티스레드 접근제어의 예
Fig. 5. The example of access control about shared buffer.

대로 결정하도록 하였다. 이를 수행하기 위한 소프트웨어 동작의 예를 그림 5에 정리하였다. 공유 버퍼에 대한 접근 우선순위가 가장 높은 것은 $Thread_{adc}$이며, 다음으로 $Thread_{Encrypt}$, $Thread_{Trans}$ 순으로 설계하였다. 각 스레드는 작업 수행 전 참조하는 버퍼 오프셋 정보를 토대로 접근 여부를 결정하도록 하였다.

3. 실험의 설계

가. 암호화 모듈 검증

암호화 모듈 검증을 위해 다음의 두 가지 실험을 수행한다. 첫 번째로 16비트 MCU 최적화 전/후의 코드 사이즈를 비교하고, 멀티스레드 스케줄링과 버퍼 공유 접근제어 동작을 검증한다. 두 번째로 고정 된 8 바이트 블록에 미리 정해진 값을 이용해 암호화/복호화 테스트를 진행한다. 본 실험의 목적은 개발 된 암호화 모듈이 16 비트 MCU와 32 비트 PC 간 상호 운용성을 검

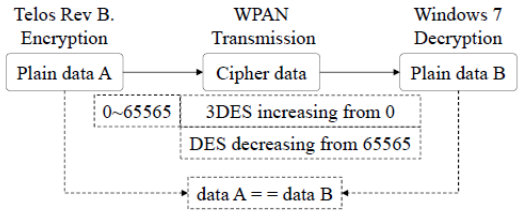


그림 6. 암호화 모듈 검증실험 설계
Fig. 6. The experimental design for cryptographic module.

증하기 위함이다. 실험 방법을 그림 6에 정리하였다.

나. 실시간 암호화 성능평가

MCU에 적용 된 암호화 모듈이 64 비트 데이터 블록을 암호화 하는데 필요한 시간을 측정하였다. 실험은 DES/3DES로 구분하고, 암호화 반복수행 횟수를 1 에서 10으로 변경하면서 자원을 점유하는 시간을 측정한다. 측정은 오실로스코프(DPO 3034, Tektronix 社)를 이용하였다. 두 번째로 실시간 생체신호 암호화 전송 시 암호화/복호화 과정에서의 오류 발생 여부 이용한 성능평가를 수행하고자 한다.

다. 생체신호 별 실시간 암호화 전송 정리

표 2에 제시 된 생체신호의 로우 데이터 양자화에 최소로 요구되는 표본추출 비율에 대한 실시간 암호화 가능 조건을 정리하고자 한다. 표 2는 John G. Webster의 저서[16]를 참조한 생체신호의 주파수 대역을 참조하여 Nyquist-Shannon sampling theorem을 근거로 양자화에 최소로 요구되는 표본추출 비율을 정리하였다. 이를 토대로 본 연구의 실시간 암호화 모듈이 각 생체신호에 적용 될 수 있는 조건을 정리 할 것이다.

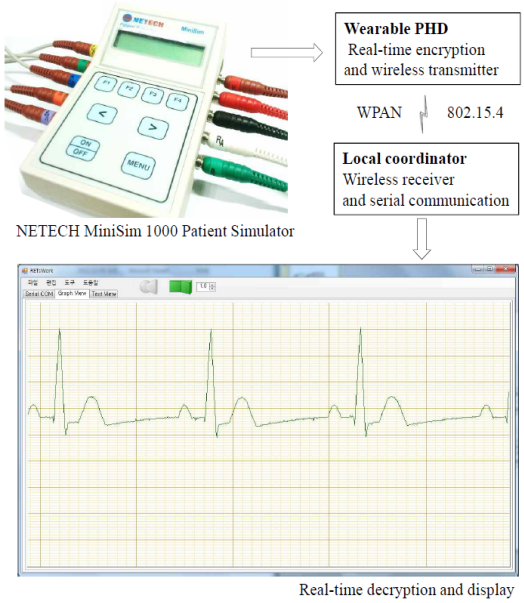


그림 7. 암호화 모듈 검증실험 설계
Fig. 7. The experimental design for cryptographic module.

표 2. 생체신호 특성에 따른 최소표본추출속도
Table 2. The minimum sampling rate according to bio-signals characteristic

Bio-signals	Frequency(Hz)	samples/sec
Phonocardiography, PCG	0.01~2000	4000
Electrocardiography, ECG	0.01-250	500
Electroencephalography, EEG	dc-150	300
Electrooculography, EOG	dc-50	100
Electroretinography, ERG	dc-50	100
Blood pressure, NIBP	dc-50	100
Plethysmography, PG	dc-30	60
Respiratory rate, RR	0.1-10	20
Electrogastrography, EGG	dc-1	2
Galvanic skin response, GSR	0.01-1	2

Ⅲ. 실 험

1. 암호화 모듈 검증 실험결과

가. 코드사이즈 및 멀티스레드 제어 검증

(1) DES/3DES 모듈 코드사이즈 비교

그림 3을 토대로 16비트 MCU에 최적화 된 암호화 모듈의 코드사이즈 비교 결과를 표 3에 정리하였다. DES의 경우 42.9%, 3DES의 경우 62.2%의 코드 사이즈 감소를 보였다. 최적화 전 코드에서 가장 큰 부분을 차지하는 ROUND를 서브루틴으로 변경했기 때문으로 판단되며, 서브루틴 반복호출에 따른 알고리즘 수행속도에 약간의 저하가 발생 할 것으로 예상된다. 그러나 내장 메모리 크기가 부족한 MCU에서 동작해야 될 모듈이므로 코드 사이즈 감소측면에서 더 유리하다. 특히 3DES의 경우 DES보다 반복적인 코드의 중복이 많기 때문에 그림 3의 최적화 방식이 매우 적합하다.

표 3. 16 비트 MCU를 위한 최적화 전/후의 코드 사이즈 비교
Table 3. Code size comparison of before and after optimization for 16bit micro controller.

(byte)	DES		3DES	
	ROM	RAM	ROM	RAM
Before	14628	2176	27804	2176
After	8358	2176	8854	2176

(2) 멀티스레드 동작 검증

PHD 소프트웨어의 동작을 검증하기 위하여 표본추출속도를 초당 300 샘플로 수행하면서 동시에 4 샘플당 블록 1개가 암호화가 수행되고 암호화 블록 4개가 완성되면 무선으로 데이터를 전송함을 그림 8에서 확인할 수 있다. 본 실험을 통해 그림 4와 5의 멀티스레드 스케줄링과 버퍼 공유를 위한 접근 제어가 정상 동작함을 검증하였다.

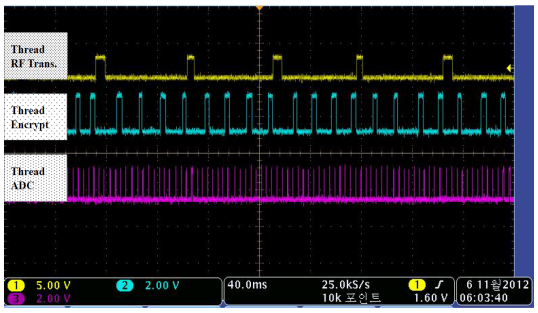


그림 8. 암호화 모듈 검증실험 설계
Fig. 8. The experimental design for cryptographic module.

나. 상호운용성 검증 결과

16비트 MCU에서 암호화 된 데이터를 일반 PC에서 복호화 가능함을 본 실험을 통하여 검증하였다. 그림 6의 실험 설계와 같이 그림 9의 결과를 보면, 복호화 결

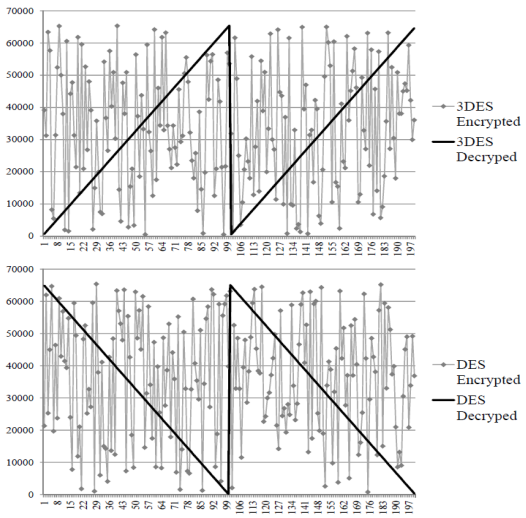


그림 9. 암호화/복호화 검증실험 결과
Fig. 9. The experimental design for cryptographic module.

과 DES가 65535 부터 감소하는 것을 확인 할 수 있으며, 3DES가 0 부터 증가하는 것을 확인 할 수 있다. 즉, 최적화 된 암호화 알고리즘이 2바이트 내에서 전송 될 수 있는 모든 값에 대한 암호화/복호화가 정상적으로 수행 되는 것을 의미한다.

2. 실시간 암호화 성능평가 결과

가. DES/3DES의 알고리즘 수행 속도 비교

Telos B에서 수행 한 DES와 3DES의 암호화 횟수별 소요시간을 오실로스코프로 측정 한 결과를 표 4, 5에 정리하였다. 실험 결과 DES 암호화 1회 수행에 평균 1.802 ms가 측정 되었고, 복호화 1회 수행에 평균 1.897 ms가 측정 되었다. 그리고 암호화, 복호화 모두 횟수가 증가함에 따라 소요시간이 선형적인 추세로 증가하였다. 3DES 암호화 1회 수행에 평균 6.683 ms가 측정 되었고, 복호화 1회 수행에 평균 6.210 ms가 측정 되었다. 마찬가지로 암호화, 복호화 모두 횟수가 증가함에 따라 소요시간도 선형적인 추세로 증가하였다. 알고리즘 별 수행 속도의 차이는 암호화 시 3DES가 DES보다 평균 3.44배 더 시간이 소요 되었고, 복호화 시 3DES가 DES 보다 평균 3.31배 더 시간이 소요 되었다.

표 4. DES 반복에 따른 자원점유시간(O_{enc})
Table 4. Resource occupancy time due to repeat DES.

ms	Encryption		Decryption	
	Mean	Std dev.	Mean	Std dev.
1	1.802	.000	1.897	.000
2	3.674	.622	3.642	1.031
3	5.921	.795	5.821	.733
4	7.440	.822	7.739	.579
5	9.870	.471	9.740	.686

표 5. 3DES 반복에 따른 자원점유시간(O_{enc})
Table 5. Resource occupancy time due to repeat 3DES.

ms	Encryption		Decryption	
	Mean	Std dev.	Mean	Std dev.
1	6.683	.794	6.210	.798
2	12.63	.339	12.86	.611
3	19.49	.622	18.62	.712
4	25.92	.850	25.49	.857
5	32.42	.905	31.61	1.09

나. 실시간 생체신호 암호화 전송

그림 7의 실험 환경을 구성하고 NETECH MiniSim 1000 Patient Simulator로 실시간 심전도 암호화 전송을 수행하였다. 이 때, 표본 추출 속도는 초당 300 샘플이었으며, 먼저 DES로 암호화 된 60 BPM의 정상 심전도와 심실조동(Ventricular flutter beat) 신호를 차례로 전송하였고, 다음으로 3DES로 암호화 된 80 BPM의 정상 심전도와 심방세동(Artrial fibrillation) 신호를 전송하였다. 암호화 된 데이터를 PC에서 디스플레이 하였을 때, 그림 10의 좌측 그래프들과 같이 숫자 0~65535 사이에 고루 분포 된 해독 불가능한 신호를 볼 수 있다. 그림 10의 우측 그래프들은 PC에서 복호화 된 신호로써 0~4096 범위로 복호화 되어 생체신호의 특징을 해독 할 수 있는 신호가 디스플레이 되는 것을 볼 수 있다.

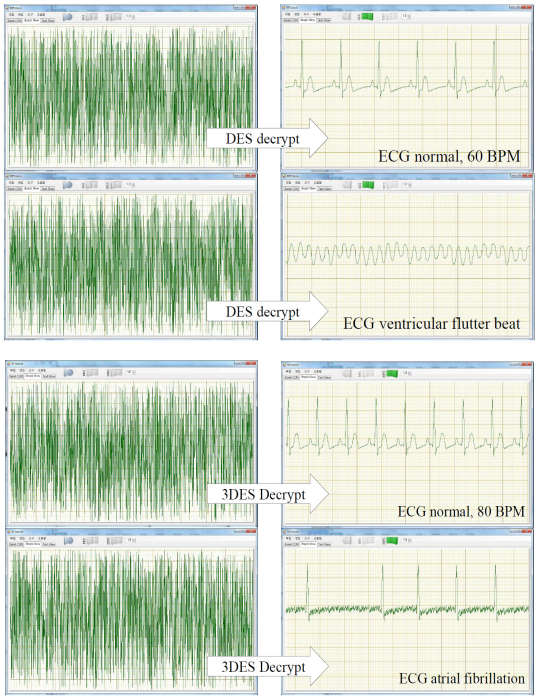


그림 10. 실시간 생체신호 암호화/복호화 결과
Fig. 10. The results of real-time bio-signal encryption and decryption.

3. 생체신호 별 실시간 암호화 전송 정리

본 연구에서 암호화 모듈의 이론적인 최대 표본 추출 속도가 식(9)~(13)에 의해 계산된다. 먼저, k번째 전송 스레드의 주기는 식 (9)로 정리 할 수 있다.

$$T_{trans}(k) = \sum_{i=1}^{BPF}(O_{enc}(i) + V_{enc}(i) \quad (9)$$

$O_{enc}(i)$와 $V_{enc}(i)$가 k번째 암호화 스레드에서 일정하다는 가정 하에 식 (10)을 유도한다.

$$T_{trans} = BPF \times (O_{enc} + V_{enc}) \quad (10)$$

그리고 식 (10)에서 $V_{enc} \geq 0$ 임을 이용하여,

$$T_{trans} \geq BPF \times O_{enc} \quad (11)$$

식 (11)에서 식(4),(5)를 이용하여 $T_{enc} \geq O_{enc}$를 유도하고, 다시 식 (3)으로 식 (12)를 유도한다.

$$SampleRate_{\max} \leq \frac{SPB}{O_{enc}}, (sec) \quad (12)$$

그리고 식 (12)에 암호화 반복 횟수 n을 추가하면 식 (13)이 유도된다.

$$SampleRate_{\max}(n) \leq \frac{SPB}{n \times O_{enc}}, (sec) \quad (13)$$

식 (13)을 이용하여 알고리즘과 이론적인 암호화 반복 횟수 별 최대 표본추출 속도를 계산 할 수 있다. 그러나, 양자화 ,암호화, 무선전송을 동시 수행 할 경우 O_{enc}가 증가하여 실제 가능한 단위 암호화 속도는 DES($\approx$500 samples/sec), 3DES($\approx$300 samples/sec) 수준까지 문제없이 동작하였다.

표 5. 생체신호 특성에 따른 실시간암호화 가능수준
Table 5. The level of available real-time encryption according to bio-signals characteristic.

Hz/sec	Sampling Rate	Encryption method
PCG	4000	3DES(N/A), DES(N/A)
ECG	500	3DES(N/A), DES(1)
EEG	300	3DES(1), DES(3)
EOG	100	3DES(5), DES(14)
ERG	100	3DES(5), DES(14)
NIBP	100	3DES(5), DES(14)
PPG	60	3DES(9), DES(27)
RESP	20	3DES(30), DES(85)
EGG	2	3DES(298), DES(865)
GSR	2	3DES(298), DES(865)

( ): 괄호 안은 암호화 반복 횟수 임

표 5는 실제 실험으로 생체신호 별 적용 가능한 암호화 수준을 정리한 것이다. 실험 결과 표본추출 속도가 낮을수록 암호화 반복횟수가 증가하였고, 적용 가능한 반복 횟수의 알고리즘 간 비율에 약 3배 차이가 있었다. 이는 이론상 두 알고리즘의 성능 차이에 해당한다.

4. 실험 결과 토의

본 연구에서 개발한 실시간 암호화 알고리즘 모듈에 대한 16비트 MCU 최적화 및 그 성능을 실험을 통해 검증하였다. 실시간 생체신호 전송 시 암호화 및 복호화 오류는 발견되지 않았고, 단위 암호화에 필요한 알고리즘별 소요시간을 측정하여 생체신호 특성에 따른 암호화 수준을 표 5에 정리하였다. 실험 결과를 토대로 계산 된 암호화 수준이 절대적인 기준이 될 수는 없다. 그 이유는 생체신호 계측기 설계 시 생체신호의 종류와 측정 목적에 따라서 주파수 범위가 변경 될 수 있고, 다양한 분석을 위해 일반적으로 더 높은 표본추출 속도를 이용 할 수 있기 때문이고, 또한 개선 된 암호화 알고리즘을 사용하거나 더 강력한 프로세서를 사용 할 경우 단위 암호화 소요시간이 감소하기 때문이다. 단, Telos B에 개발 된 암호화 모듈을 적용하였을 때 위와 같은 성능을 기대 할 수 있다.

마지막으로 반드시 강력한 암호화를 착용형 PHD에 적용하는 것이 최선은 아니다. 그 이유는 휴대하며 장시간 측정해야 되는 장비의 특성 상 배터리 소모를 따른 동작시간을 고려해야 하기 때문이다. 이 문제는 신호의 중요도와 암호화 수준에 따른 배터리 소모를 고려하여 주어진 시스템의 설계기준에 따라 결정해야 한다.

Ⅳ. 결 론

건강관리 서비스는 질병의 관리와 예방의 측면에서 중요한 역할을 담당한다.[1~2, 4] 그러나 PHI에 대한 정보보호 수준은 아직 사용자가 신뢰 할 수 없는 수준이다.[17~18] 향후 건강관리 서비스가 활성화 되고, 서비스 사용자가 증가하게 되면 PHI의 수집 및 관리의 수요가 증가함에 따른 PHI 유출의 가능성도 더 커질 것이다.

본 연구에서는 위에서 언급 된 문제를 해결하기 위해

착용형 PHD에서 사용자가 관리하는 비밀키로 암호화 된 PHI를 HSRC로 정보를 전송 할 수 있도록 하였고 그 성능을 검증하였다. 본 연구에서 설계한 모듈을 활용 할 경우 사용자가 본인의 PHI에 대한 비밀키 관리를 해야 하는 불편함을 감수해야 하지만 누구나 PHI에 포함 된 본인의 건강 정보가 노출되는 것에 거부감을 갖고 있기 때문에 본 연구의 방법이 타인에 의한 PHI 수집 및 관리에 대한 거부감을 억제 시키는 방법으로써 건강관리서비스 활성화에 기여 할 수 있을 것으로 기대한다.

참 고 문 헌

[1] 김인영, “Need for Ubiquitous Healthcare Technology,” *전자공학회지*, 제32권, 제12호, 19-28쪽, 2005년 12월

[2] 김진태, “Roadmap and Solution Framework for Ubiquitous Healthcare Business,” *전자공학회지*, 제32권, 제12호, 76-87쪽, 2005년 12월

[3] 김현우, 변성호, 박희정, 이승환, 정유석, 조위덕, “유비쿼터스 지능공간에서 멀티모달센서를 이용한 향상된 u-헬스케어 서비스 구현에 대한 연구,” *전자공학회논문지*, 제46권 CI편, 제2호, 27-35쪽, 2009년 3월

[4] A. Fano, A. Gershman, “The future of business services in the age of ubiquitous computin,” *Communications of the ACM*, Vol. 45, no.12, pp. 83-87, Dec 2002

[5] I. Martinez, J. Escayola, M. Martinez-Espronceda, P. Munoz, J.D. Triago, A. Munoz, S. Led, L. Serrano, J. Garcia, “Seamless Integration of ISO/IEEE11073 Personal Health Devices and ISO/EN13606 Electronic Health Records into an End-to-ENd Interoperable Solution,” *Telemedicine and e-Health*, Vol.16, no.10, pp. 993-1004, Dec 2010

[6] P. C Tang, J. S Ash, D. W Bates, J Marc Overhage, D. Z Sands, “Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption,” *J Am Med Inform Assoc*, Vol. 13, no. 2, pp. 121-126, Mar 2006.

[7] HIPAA, “Summary of the HIPAA Privacy Rule,” http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (last accessed Nov. 2012.)

[8] 송지은, 김신효, 정명애, “u-헬스케어 서비스에서의 의료정보보호,” *정보보호학회지*, 제17권, 제1호, 47-56쪽, 2007년 2월

[9] IEEE Standards Association, “ISO/IEEE11073-Personal Health Devices standard (X73-PHD). Health informatics.[P11073-00103.Technical report-Overview][P11073-104xx.Device specializations][P11073-20601.Application profile-Optimized exchange protocol], 1st ed.,” http://standards.ieee.org (last accessed Nov 2012)

[10] M. Martinez-Espronceda, L. Serrano, I. Martinez, J. Escayola, S. Led, J. Trigo, J. Garcia, “Implementing ISO/IEEE 11073: Proposal of two different strategic approaches,” *in Proc. of IEEE EMBS Conference*, pp. 20-25, Vancouver, Camada, Aug 2008

[11] 전성철, 김인경, “인터넷 이용자의 개인정보 유출 가능성에 대한 심리적 불안에 관한 연구: 성별, 이용량, 이용 빈도를 중심으로,” *한국전자통신학회논문지*, 제 6권 제 5호, 731-738쪽, 2011년 10월

[12] 김홍근, 김윤정, “지식정보사회 의료 패러다임 변화와 정보보안,” *한국정보보호진흥원 정책보호 정책동향 보고서*, 2006년 5월

[13] J. Polastre, R. Szewczyk, D. Culler, “Telos: Enabling Ultra-Low Power Wireless Research,” *Information Processing in Sensor Networks 4th International Symposium on*, pp. 364-369, Los Angeles, USA, April 2005,

[14] H. Cha, S. Choi, I. Jung, H. Kim, H.Shin, J. Yoo, C. Yoon, “RETOS: resilient, expandable, and threaded operating system for wireless sensor networks,” *In Proc. of IPSN'07*, New York, USA, 2007

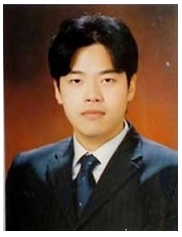
[15] J. Daemen, V. Rijmen. “AES Proposal: Rijndael”, Banksys/Katholieke Universiteit Leuven, Belgium, AES submission, Jun 1998

[16] J.G. Webster, *Medical Instrumentation, Application and Design*, pp.10-11, 1998

[17] A C Edmonson, “Learning from failure in health care: frequent opportunities, pervasive barriers,” *Qual Saf Health Care*, Vol. 13, sup.2, pp. ii3-ii9, Dec 2004

[18] S. Haas, S. Wohlgemuth, I. Echizen, N. SOnehara, G. Muller, “Aspects of privacy for electronic health records,” *International Journal of Medical Informatics*, Vol. 80, no. 2, pp. e26-e31, Feb 2011

저 자 소 개



김 정 채(학생회원)
2006년 경희대학교
동서의료공학과 학사
2006년～현재 연세대학교 대학원
생체공학협동과정
박사 과정

<주관심분야 : 생체시스템 모델링, 생체계측 시스템>

유 선 국(정회원)-교신저자
1981년 연세대학교
전기공학과 학사
1985년 연세대학교
전기공학과 석사
1989년 연세대학교
전기공학과 박사
1995년～현재 연세대학교 의과대학 의학공학교실
교수

<주관심분야 : u-Health, 의료영상, 스마트 디바이스, 생체신호처리 및 패턴인식, 감성공학>