스마트모바일 기반의 u-Health시스템에서 HIGHT를 이용한 보안성 분석

이재필*, 김영혁*, 임일권, 이재광, 이재광*
*한남대학교 컴퓨터공학과
e-mail: jplee@netwk.hannam.ac.kr

An Analysis to security on SmartMobile based u-Healthcare system using by HIGHT

Jae-Pil Lee*, Young-Hyuk Kim*, Il-Kown Lim*
Jae-Gwang Lee, Jae-Kwang Lee*
*Dept of Computer Engineering, Han-Nam University

요 약

한국정보통신기술협회(TTA)에서 표준 제안한 WBAN(Wireless Body Area Network)은 인체 내부 통신(in-body or implant)과, 인체 외부 통신(on-body)통신으로 구분하고 있다.

생체측정 정보 중 체온, 호흡, 맥박, 운동량, 심박의 부분적인 데이터 수집을 바탕으로 환자의 생체정보 데이터를 수합 후 데이터 프레임구조로 변환하여 스마트모바일 애플리케이션 환경에서 사용자가 모바일기기 화면에 정보를 표시 할 수 있다.

이렇게 표시된 정보들은 환자의 상태를 실시간으로 자신의 스마트모바일을 이용하여 확인할 수 있으며, 이러한 정보를 보호하고 의료기관에 전송하기 위한 방법으로 국제표준암호알고리즘인 HIGHT 알고리즘을 적용하여 생체정보 데이터의 부분 암호화 적용을 설계 하였다. 이를 통해 의료기관의 인증서버에 대한 부하 감소 및 환자의 생체정보의 보안 강화를 제시한다.

1. 서론

세계적으로 원격의료 시장의 규모는 2010년부터 2015년까지 연평균 19%씩 성장할 것으로 예상하고 있다. 스마트모바일의 처리 능력 향상과 헬스케어 의료 주변기기의 호환성 향상으로 2016년까지 약 300만 명 이상의 환자가 원격 모니터링 서비스를 이용할 것이라고 전망하며 유비쿼터스 생활 속에서 삶의 질 향상과 밀접한 u-Health, 고령친화, 재활복지 등 미래시장 선도 가능 분야에서 댁내 생체신호 측정 및 진단이 가능한 시스템 및 서비스가 구현 보급중이다.

u-Health 분야에서 최근에 가장 관심을 받고 있는 분야는 장소에 관계없이 건강에 관련된 정보를 실시간으로 수집하고 건강관리 서비스 센터에 전송하여 건강 이상 발생 여부를 확인하고 적절한 조치를 취하며 지속적인 건강관리 및 질병관리 서비스를 제공하는 것이다. 이에 따라 u-Health는 고령화에 따른 여러 가지 사회의 문제를 해결해 줄 수 있을 것으로 전망되고 있다. 현재의 모바일 마켓에서 모바일 헬스케어와 의료관련 앱의 다운로드는 '2012년 4,400만 건에서 '2016년 1.42억 건으로 증가할 전망으로 모바일 애플리케이션 컨텐츠를 이용하는 사용자가 증가하는 추세를 알 수 있다. 특히 심장병 환자의 경우 모니터링 서비스에 많은 시장이 형성되고 있다. 이에 덧붙여 당뇨병, COPD(Chronic Obstructive Pulmonary Disorder, 만성폐쇄성폐질환) 및 만성 질환의 관리 역시 주요 시장을 형성하고 있다[1].

원격 환자의 모니터링 경우 스마트모바일기기(스마트폰, 스마트패드 등)를 허브로 사용하여 병원에 방문하지 않고 모바일 헬스 서비스를 이용하기에 서비스 비용을 상당히 낮출 것으로 전망하고 있으며, 이를 통하여 값비싼 맞춤 서비스에 대한 수요를 감소시킬 것이라고 전망 한다.

본 연구에서 생체정보의 보안 강화를 위하여 여타 알고리즘 보다 간단한 구조로 설계되어 빠른 암호화, 복호화를 통한 시간을 단축하는 모바일용 국산암호화기술 국제표준 알고리즘인 HIGHT(HIGh security and light weigHT)를 이용하여 본 연구의 핵심인 모바일 환경에 암호화 알고리즘을 적용하고 검토하였다. 2장에서는 관련연구에 대해 소개하였고, 3장에서는 생체 정보를 암호화하는 방법을 구현하고, 4장에서는 결론 및 향후 과제를 제시 하였다.

2. 관련연구

2.1 HIGHT관련 연구

USN(Ubiquitous Sensor Network) 환경은 IEEE802.15.4 기반으로 한 ZigBee와 같이 실질적인 구현사례가 제시되고 있어 센서 네트워크 활용도는 점차 확대되고 있다. Sensor 네트워크상에서는 메시지 전송 시 대칭키로 암호화된 암호문을 전송하도록 권장하고 있다. 현재 ZigBee와

같은 무선 네트워크 표준에서는 대표적인 대칭키 알고리즘인 AES를 메시지 전송 시 메시지 암호화에 사용하도록 권장하고 있다. 현재 사용되는 대부분의 센서노드들은 노드의 칩셋 단에서 하드웨어 모듈로써 암호화를 제공하고 있다 최근 HIGHT암호화 알고리즘은 기존의 AES에 비해 하드웨어 및 소프트웨어 구현 시 속도 관점에서 보다 우수한 성능을 나타낸다[2].

2.2 국내 WBAN 표준 PHY

인체통신을 이용한 서비스의 상호 연동성을 보장하고 호환성을 유지하기 위하여 인체통신의 네트워크 프로토콜 구조(TTAS.KO-10.0301) 중 물리 계층을 정의한다[3].

Parameters	Values
주파수대역	Frequency Selective Baseband (12 MHz ~ 16 MHz)
통신환경	Intra Body Communication
전송방식	Direct Digital Transmission
이중화 방식	TDD
프레임길이	10 ms
프리앰블	6bit PRBS with Manchester Encoding: P(z) = z6+z5+1, Initial value= [100000]
스크램블링	32bit PRBS generator : P(z) = z32+z31+ z11+ 1
확산방식	Frequency Selective 64 chip Walsh Modulation
데이터율	2 Mbps ~ 250 Kbps

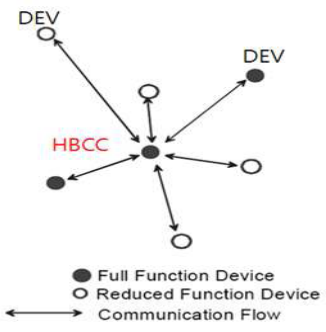
(그림 1) 인체통신 규격 개요

인체통신에 대한 네트워크 프로토콜 규격 중 물리계층에 대한 물리적 신호의 전송 규칙을 정의 하는 것으로 송신 및 인체를 통해 수신된 미약한 신호로부터 정보를 복원하는 규격 등을 정의하고 있다.

2.3 국내 WBAN 표준 MAC

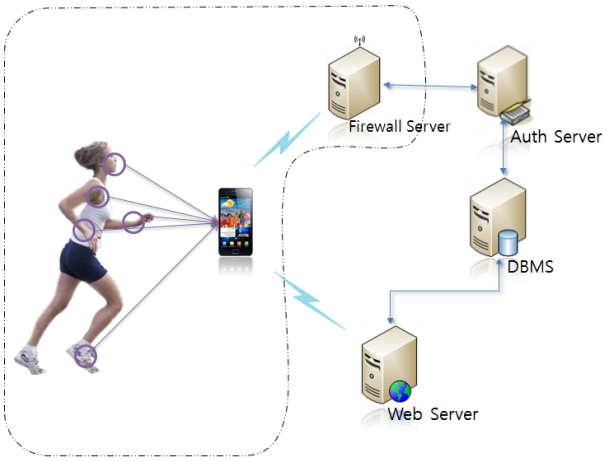
인체통신망의 MAC계층에 대한 표준은 'TTAS.KO-10.0344'에서 정의하고 있다. 이 표준에서는 인체통신에 대한 네트워크 프로토콜 규격 중 MAC계층에 대한 프레임구조, 다양한 전송 속도의 어플리케이션 수용방안, 신뢰성 있는 전송 방안 등의 규격에 대한 내용을 다루고 있다.

인체통신망은 (그림2)과 같은 스타 토폴로지로 구성되며, 각 디바이스들은 HBCC의 중재 하에 동작을 한다[4].



(그림 2) HBC 토폴로지

3. 시스템 설계



(그림 3) USN기반 원격 건강모니터링 서비스 구상도

(그림3) USN기반 원격 건강모니터링 서비스 구상도를 보여준다. 구성 요소에는 인체측정 정보를 수집 할 수 있도록 분산된 센서장비들과 개인용 스마트단말기가 있다.

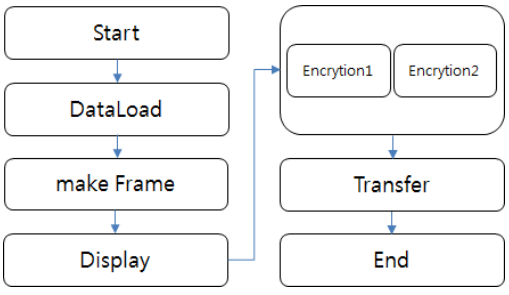
의료기관에서는 Firewall Server, Authentication Server, Data Base Management Server, Web Server로 구성이 된다.

각 환자들은 스마트모바일 장비를 확인하여 환자의 분산된 생체정보의 측정 및 수합 후 해당 의료기관의 데이터베이스에 전송하게 된다. 이렇게 누적된 데이터는 환자의 생체정보를 의사가 진단 내리는 기초자료로 활용되며 환자의 상태에 대한 소견서를 발부 받을 수 있다.

이렇게 되면 의사의 진단 후 전자 처방 서비스를 이용하여 가까운 약국에서 의약품등을 수령할 수 있는 서비스를 제공 받을 수 있다.

(그림3) 원격지의 의료기관서버와 개인 스마트모바일 간의 무선 데이터 전송 시의 두 구간으로의 보안 적용으로 범위를 제안 하였다. 이에 따라 저 전력, 경량화를 요구하는 네트워크 환경에 적합한 HIGHT 알고리즘을 이용하여 무선 구간 보안의 문제를 해결하기 위한 시스템 설계를 한다.

3.1 생체정보 보안설계 흐름도



(그림 4) 스마트기기(Client)측 생체정보 보안설계 흐름도

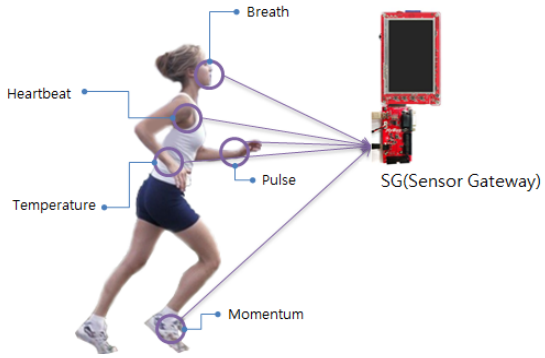
(그림4)는 생체측정 정보 보안 적용 시 보안 설계 흐름도 이다.

각 분산된 센서들의 정보를 수집 후 하나의 게이트웨이에 저장하고 프레임 구조에 맞게 데이터를 정렬 한다.

스마트모바일기기에 환자의 정보를 단말기 화면에 출력 후 HIGHT를 이용하여 생체정보를 부분 암호화를 적용한다.

암호화 된 데이터를 의료센터 방화벽 서버에서 인증을 거친 후 DBMS서버에 저장이 된다.

3.2 생체정보 수합 구성도



(그림 5) Sensor 수합 구성도

(그림5) 사용자의 몸에 분산되어 있는 센서들을 통해 체온, 호흡, 맥박, 운동량, 심박의 정보를 수집하여 안드로이드 개발 장비인 스마트패드로 적용한다.

수집된 데이터는 프레임 구조에 맞게 데이터를 구성한 후 각 환자의 스마트 모바일에 현재 생체정보를 표시 하도록 한다.

3.3 생체정보 통합 구조

u-Health 인체무선망에서는 한국정보통신기술협회(TTA)에서 표준 제안한 기본 프로토콜을 사용하고 있다.

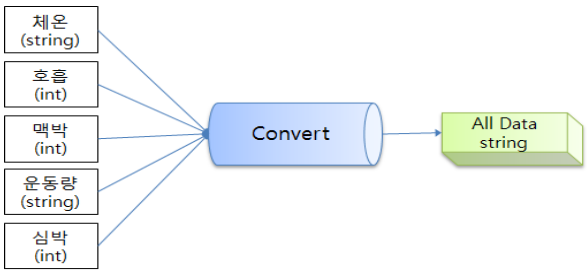
선행 연구[5] 중 환자의 생체측정 정보를 수집하여 일정한 프레임 구성안에 페이로드 구분자의 정보를 전송하는 과정에서 생체정보들이 보안에 쉽게 노출될 수 있다.

이러한 취약한 데이터페이로드를 보안하는 방안으로 HIGHT를 이용하여 암호화 시키는 방법을 제시한다.

이러한 데이터 암호화 수행 시 해당 의료기관 서버에 데이터 복호화를 수행할 경우에 서버에 부하를 증가시킬 수 있는 요인이 된다.

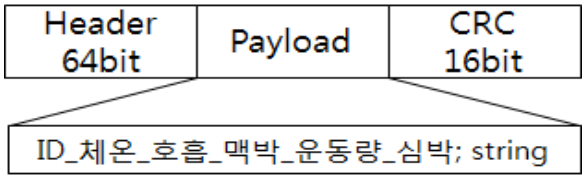
이러한 서버에 부하를 감소 하고자 데이터 페이로드에 전체 암호화 처리과정을 통하여 (그림9)과 같이 변경 적용하였다.

또한 생체정보의 수집 시 문제되는 사항이 있다. 각 데이터들 마다 특징이 있기 때문에 다양한 종류의 형태가 만들어 진다. 예컨대 전기신호, 음향신호, 역학신호, 화학신호, 광학신호등 인체의 다양한 종류들로 나열이 되어 있기에 이러한 데이터들을 문자열 형태로 변환하여 (그림6)과 같은 형태로 저장되는 작업이 필요하다.



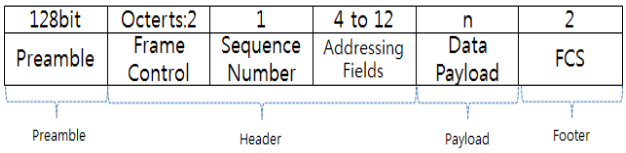
(그림 6) Data type 변환

문자열로 변환된 페이로드의 경우 국내 표준에 의거 데이터 프레임 규격을 유지하게 되며, 각 데이터들은 (그림7)과 같이 구분자 '_'를 설정하여 암호 알고리즘을 통하여 변환 후 암호화 된 상태로 서버에 저장 되게 된다.



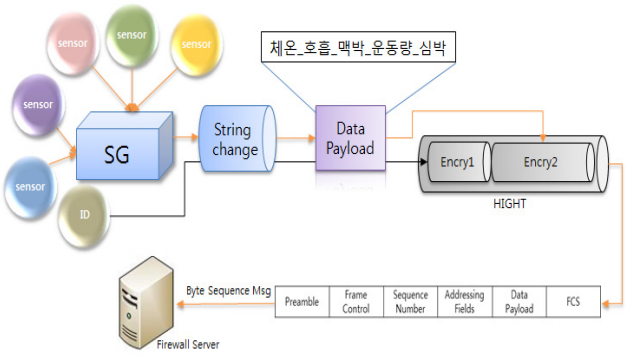
(그림 7) 구분자를 이용한 payload 생성

(그림7)과 같이 생성한 페이로드는 (그림8)과 같은 데이터 프레임 구조에 적용되며 MSDU는 PHY계층에 전달되어 PSDU가 된다.



(그림 8) Frame 구조

3.4 생체정보 암호화 흐름 과정



(그림 9) 생체정보 암호화 프로세스

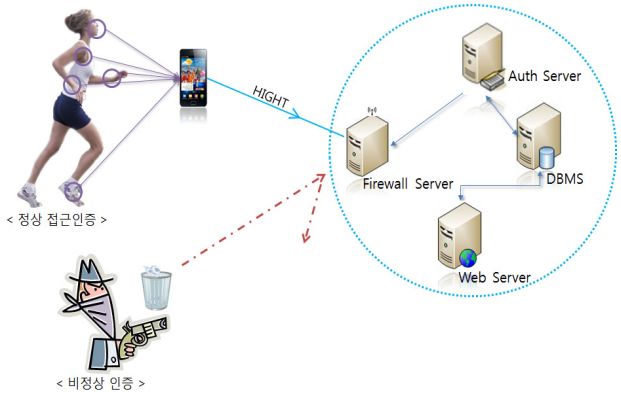
(그림 9)는 생체정보를 수집 후 암호화 하는 과정이다.

우선 SG(Sensor Gateway)구조 안에 생체측정 정보를 구성하여 문자열 형태로 변환하는 작업을 진행한다.

이때 데이터페이로드 부분의 환자의 체온, 호흡, 맥박, 운동량, 심박, ID(환자고유번호)의 정보를 가지고 암호화 하는 과정으로 진행하게 된다. 이러한 이유는 페이로드 와 프레임이 암호화되어 있지 않은 상태로 전송 시 데이터 도청 및 감청 등에 의해 보안 문제점을 야기 시킬 수 있다.

암호화를 진행하는 방법은 ID의 정보를 암호화 후 환자의 생체정보를 암호화 하는 순서로 설계 하였다. 암호화 진행 후 Firewall Server에서 ID값으로 인증을 받는 과정을 진행하게 된다.

3.5 생체정보 인증 시나리오 과정



(그림 10) 생체정보 인증 흐름 과정

(그림10)은 USN시스템 환경에서 정상적인 사용자 인증방식을 위한 시나리오 모델이다.

정상적인 접근방식으로 의료센터 FS(Firewall Server)에 인증을 받은 사용자가 있고 비정상적으로 인증을 받고자하는 하는 사용자의 경우가 있다고 가정 한다.

정상적으로 인증을 받은 사용자의 경우 프레임 구성안에 (그림5)와 같이 페이로드 값 안에 ID값과 생체정보 중 ID값만을 복호화 하여 실제 환자의 진위여부를 판단하게 된다.

비정상적으로 인증을 받은 사용자의 경우 ID값을 복호화 했을 경우 병원의 환자의 정보와 일치하지 않아 의료센터 FS서버에서 인증을 받지 못하며 서비스 또한 제공받을 수 없게 된다.

4. 결론

센서 네트워크 환경에서 데이터 전송 시 무선 구간에서의 보안을 해결하고자 각 알고리즘을 적용하여 보안상의 문제점을 해결할 수 있도록 설계 하였다.

본 연구에서는 암호화 방식을 기존 선행연구와 다른 방법으로 제시하였다. 선행연구 중 스마트단말기와 의료정보센터인 FS서버의 무선 구간 보안을 위해서 HIGHT을 이용하여 페이로드 전체 암호화를 진행 하였다.

이 논문에서는 프레임구조 안의 페이로드에서 부분적 암호화를 적용하는 구조로 설계하였다.

이렇게 설계 모델 시 수많은 사용자들이 FS서버에 접속하여 인증을 거치기 위해 복호화 작업을 진행하게 된다.

페이로드의 전체의 환자정보를 복호화 하는 경우 FS서버에 전체적인 부하를 야기 시킬 수가 있다. 그래서 페이로드의 환자정보 ID와 생체정보의 데이터 중 ID값만을 복호화 하여 FS서버에 인증여부를 확인하게 된다.

위 과정을 거쳐 서버 측 부하를 줄이고 재 암호화하는 과정을 생략함으로써 시스템효율성과 보안성을 강화할 수 있도록 설계 하였다.

향후 안드로이드 기반 플랫폼에 어플리케이션을 이용하여 HIGHT, SEED알고리즘을 사용하여 암호화 알고리즘을 적용 및 구현하고 네트워크상의 패킷 감소량에 대한 데이터 분석과 암·복호화 속도 비교 진행을 통한 기법을 적용할 예정이다.

"이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2011-0013029)"

참고문헌

[1] 한국정보화진흥원 "m-Gov. Weekly(제39호)" pp09, Feb, 2012

[2] Hwajeong Seo "Optimized implementation of HIGHT algorithm for sensor network" Jun, 2011

[3] TTAK.KO-10.0301: "인체통신 네트워크 물리계층 구조", 2008

[4] TTAK.KO-10.0344: "인체통신망 매체접근제어계층구조", 2009

[5] YoungHyuk Kim "A Study on Security Model for Secure Biometric Information of BAN" Feb, 2011