JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 19, No. 10 : 2473~2480 Oct. 2015

BYOD를 활용한 스마트헬스 환경에서 안전한 원격의료 시스템

조영복[1] · 우성희[2*] · 이상호[1] · 박종배[3]

A Secure Telemedicaine System in Smart Health Environment using BYOD

Young-bok Cho[1] · Sung-hee Woo[2*] · Sang-ho Lee[1] · Jong-bae Park[3]

[1]Department of Computer Science, Chungbuk National University, Cheongju 361-763, Korea
[2*]Department of Medical Information&Engineering, Korea National University of Transportation, Chungbuk, 380-702, Korea
[3]Department of Radiology, Chungbuk Health&Science University, Chungbuk, 363-794, Korea

요 약

원격의료는 사용자가 시간적이나 공간적 제약을 받지 않고 어디서나 PC 또는 스마트폰을 통해 지속적으로 건강 관련정보에 대한 서비스가 가능하다. 원격지 병원에서 환자 의료 데이터를 암호화 하지 않고 전송하는 경우 환자는 심각한 장애를 받을 수 있고 BYOD를 활용해 개인의 건강과 생명에 직결 된 데이터가 송수신됨으로 개인의 프라이버시 보장과 데이터 보안이 가장 중요한 요소가 된다. 이 논문에서는 BYOD를 활용해 개인건강정보 데이터의 안전성은 제공하기 위해 서명방식과 개인키 방식의 암호화를 제공한다. 스마트헬스 환경의 보안성 문제로 대두되는 재전송 공격과 중간자 공격에 대비해 타임스탬프와 서명방식을 사용하였고 암호화를 제공하면서도 통신오버헤드가 평균 1.499mJ와 1.212mJ로 낮았으며 위급상황에서도 약 59%로 빠르게 응답하는 것을 시뮬레이션을 통해 보였다.

ABSTRACT

In telemedicaine, people can make their health checked at anywhere from temporal and spatial constraints and It's environment can provide continuous health information regardless of the location of customers through PCs and smart phones. In addition, personal health information collected utilizing the BYOD(bring your own device) is the most important factor data security and guaranteed personal privacy because it's directly connected to the individual's health and life. In this paper, we provide a signature of the private key encryption system and method for providing the security of personal health information data collected utilizing the BYOD. Against replay attacks and man-in-the-middle attacks on security issues that are emerging as a smart environmental health was used as the timestamp and signature methods. Proposed method provides encryption overhead, while a communication was lower compared to the pre-encrypted with a mean 1.499mJ 1.212mJ shown by simulation to respond quickly in an emergency situation to be about 59%.

키워드 : 원격의료, BYOD, 정보보호, 사용자 인증, m-헬스케어

Key word : Telemedicaine, Bring Your Own Device, Information Security, User Authentication, m-Healthcare

Received 08 July 2015, **Revised** 12 August 2015, **Accepted** 26 August 2015

*** Corresponding Author** Sung-hee Woo(E-mail:shwoo@ut.ac.kr, Tel:+82-43-820-5323)
Department of Medical Information&Engineering, Korea National University, Chungbuk 380-702, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2015.19.10.2473 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

개인 건강의 관심도 증가와 모바일 건강관리 시대의 도래로 의료 관련 정보가 양산되고, 의료기관간 의료정보교류도 활성화되고, 개인 건강 보조・진단 기구 사용 확대로 개인건강정보가 폭증되고 있다. 이에 보안 취약성과 사이버 위협・공격 요소가 많아짐에 따라, 정보보호의 필요성이 증대되고 있으며 개인정보보호에 대한 관심이 높아지고 있다[1,2]. 스마트폰이 대중적으로 사용되면서 국내 의료생활에도 큰 변화가 나타나고 있다. 스마트 폰, 태블릿, 패드 등과 같은 개인이 소유한 스마트기기(BYOD: Bring Your Own Device)를 이용해 모바일 애플리케이션 스토어에는 '의료(Medical) 카테고리'로 정의된 3,600여 가지의 상품이 존재하며, 이 중 절반 이상은 건강, 질환 정보를 제공하는 원격의료 형태가 가미된 애플리케이션이다[3-5].

또한 주요 스마트폰 앱 스토어에는 17,000개의 모바일 헬스 애플리케이션이 존재하며, 2015년에는 스마트폰 이용자의 1/3 인 5억명 이상이 모바일을 통한 유헬스(u-Health) 서비스를 이용할 것으로 예상되고 있으며, 모바일 서비스를 기반으로 개인 건강관리(일일 운동량, 혈압, 혈당, 심전도 등)를 체계적이고 종합적으로 수행할 수 있는 다양한 개인건강 의료 서비스(u-Healthcare, m-Healthcare Service, Smart Healthcare)가 활발하게 나타나고 있다. 그러나 이와 같이 사회 각 분야의 정보화가 진전됨에 따라 개인정보보호와 정보시스템 보안 문제에 대한 우려는 더욱 커지고 있다. 해킹・바이러스 등 정보보호 위협요인이 단시간 내에 전 세계 네트워크 인프라를 마비시켰던 경험을 돌이켜 보면 정보보호에 대한 노력이 얼마나 중요한지 알 수 있다[3,6,7]. 전자적으로 취급하는 정보의 종류와 양이 많아짐에 따라 정보보호 수준제고를 위한 관심과 노력이 강화되어야 하고 의료 분야의 경우도 개별 의료기관의 정보화 수준이 높아지고, 인터넷을 통한 의료정보의 전송 및 공유 등에 대한 논의가 진행되면서 개인의료정보의 보호 문제가 부각되고 있다[8]. 의료기관에서 취급하는 개인의료정보는 일반적인 개인정보나 금융정보 등 타 분야에서 다루는 정보에 비해 매우 민감한 정보로 인식되고 있어 개인의료정보보호 수준 제고를 위한 국가 차원의 종합적이고 체계적인 노력이 요구된다. 또한, 대형병원에서는 어느 정도 정보보호 체계를 갖추어서 관리하고 운영하고 있으나, 중소규모 병·의원, 약국에서 환자와 관련된 민감한 개인정보를 저장·보관하고 전송하는 과정에서 유출되거나 노출될 수 있는 상황이 더욱 많아지게 된다[9,10]. 따라서 이 논문에서는 BYOD를 활용한 스마트헬스 환경에서 안전한 원격의료 시스템을 제안한다. 제안기법은 원격진료에서 사용되는 모든 개인의료정보보호를 위해 비밀키 방식 암호화 기반의 통신을 기반으로 동작한다. 암호화를 과정에서 타임스템프를 이용해 재전송공격을 방지하고 개인키를 이용해 암호화함으로 무선통신에서 발생되는 중간자 공격에 안전성을 제공한다.

이 논문의 구성은 2장에서는 원격의료에 대해 기술하고, 3장에서는 제안하는 BYOD를 활용한 스마트 헬스 환경에서 안전한 원격의료 시스템을 기술한다. 4장에서는 제안 하는 시스템의 효율성과 보안성을 평가하고 5장에서는 결론을 기술한다.

Ⅱ. 본 론

2.1. 원격의료 국내 동향

원격의료(telemedicaine)란 원거리부터 원격통신체계를 통해 전달된 임상자료・기록・기타 정보를 토대로 질병에 대한 중재, 진단 및 치료를 결정하는 의료의 실행이라 정의한다. 우리나라에서는 1991년도에 원격의료가 처음 시행되었다. 한국통신의 지원으로 서울대학교병원과 경기도 연천보건의료원, 한림대 춘천성심병원과 강원도 화천보건의료원, 경북대학교병원과 경북 울진보건의료원 간에 일반 공중 통신망(PSTN)을 이용한 원격의료영상진단 및 원격문진을 시범 실시한 것이 국내 원격의료의 시초라 할 수 있다. 이후 국내 주요 대학병원 및 각 분야 연구소의 참여와 급격한 기술력의 확보를 통해 1996년 6월 11일 정부의 '정보화촉진기본계획'이 확정되고, '정보기술을 활용한 의료서비스의 고도화'가 '정보화촉진 10대 과제'의 하나로 선정되면서 국내 원격의료사업이 활기를 띠게 되었다[3,8]. 가장 최근 통계 자료에 의하면 자체적으로 수집한 약 9백만 개에 달하는 노출된 정보에 대해 총 데이터 침해 건수는 614건이었다. 이 중 보건의료 관련 정보는 269건의 데이터 침해 사고가 발생했다고 발표하였다. 이는 전체에서 43.8%에 달하는 수치이며, 다른

분야와 비교할 때 금융관련 정보 중 23건의 데이터 침해 사고가 발생한 점을 감안할 때, 의료 관련 정보에 대한 해커들의 관심이 매우 높다는 증거이다[11]. [표 1]과 같이 산업분야별 데이터 침해 중 보건의료 관련 데이터 도난과 유출사고 건수는 2005년 이후 약 300% 가량 증가했다.

표 1. 산업 분야별 데이터 침해 변화추세
Table. 1 Industry-specific data breach trends

industry	2005	2006	2007	2008	2009	2010	2011	2012	2013
Business	28	69	130	243	208	279	198	172(36.4%)	211(34.3%)
Education	75	80	111	131	78	65	60	65(13.7%)	55(9.0%)
Goverment	21	98	110	110	90	104	48	53(11.2%)	56(9.1%)
Medical	13	43	64	94	65	160	87	165(34.9%)	269(43.8%)
Finance	20	31	31	78	57	54	28	18(3.8%)	23(3.7%)
Total	157	321	446	656	498	662	421	473	614

국내외적으로 원격·재택진료에 적용할 수 있는 휴대용 기기 또는 가정용 의료기기 개발에 많은 투자가 이루어지는 등 스마트 헬스케어 시스템에 대한 연구가 다양하게 이루어지고 있다.

2.2. 원격의료의 보안 취약점

원격의료는 개인 건강·의료 정보 권한과 관련된 다양한 이해당사자가 존재할 수 있다는 점에서 보안 및 프라이버시에 여러 취약점과 위험 요소를 지니고 있다. 또한 개인의료정보보호에 대한 리스트 또한 정보보호의 3요소 즉 기밀성, 무결성, 가용성에 대한 위협으로 구분할 수 있다. 의료정보의 손실이나 파손등과 같이 무결성 침해로 인한 환자 안전에 대해 위협 환자 진료정보나 개인 정보에 대한 권한이 없는 자의 접근이나 정보유출로 인한 기밀성 침해, 필요한 정보서비스 제공의 불가 등 안전성에 위협요소를 갖는다[10-12]. 또한 개인의료정보보호 리스크의 경우 환자 개인의 프라이버시에 대한 침해뿐만 아니라 정보의 무결성을 침해하여 부정확한 정보를 제공할 경우 환자 진료 시 막중한 위험을 초래할 수 있다는 점에서 정보보보호의 중요성이 대두된다[13,14]. 그럼에도 불구하고 현재 원격의료 시스템 내 의료정보 보호에 대한 구체적인 국내 법률이나 표준안은 부재한 실정이다. 원격의료서비스를 통한 개인정보의 수집, 관리, 전송, 노출 시 책임 소재 등은 유헬스 시스템에 있어 매우 중요한 문제이며 이에 관해 정부의 획일화된 법적 규제가 반드시 필요하다[7,12]. 또한 시스템 내 환자 의료정보 관리에 대해서는 사용자 단말기인 스마트폰 애플리케이션에 대한 불법 접근, 네트워크를 통한 의료정보시스템 불법 접근, 의료정보에 대한 위변조 등 광범위한 분야의 보안 취약점을 구체적으로 표준화하고 이를 통하여 서비스 이용자에게는 개인정보 전송에 대한 신뢰성을 높인다. 또한 기술적으로는 시스템 안전성을 보장할 수 있을 것이며, 개발자에게는 기술개발 시 획일화된 표준 지침으로 활용될 수 있을 것이다[8,15]. 대한 의사협회의 원격진료 현장의 기술적 안전취약점을 분석한 결과 비 암호화 통신, 악성코드 감염 노출, 비밀번호 설정 취약, 개인 PC처럼 사용, 백신 설치 여부, 저 품질의 영상을 취약점으로 정리하고 있다[8].

Ⅲ. 빅 데이터를 이용한 BYOD 기반의 안전한 원격의료 시스템

3.1. 제안 시스템 구성도

이 논문에서 BYOD 기반의 안전한 원격의료 시스템을 위한 전체 구성도는 [그림 1]과 같다. 제안 시스템에서는 환자들이 사용하는 의료디바이스(BYOD)와 개인 스마트폰(PSP : Personal Smart Phone), 안전한 의료 데이터 사용을 위한 인증센터(TC), 의사나 간호사 등 의료진(DTG : DoctorGroup), 병원정보 시스템(HIS)와 클라우드 기반의 개인의료정보(CPHR)로 구성된다.

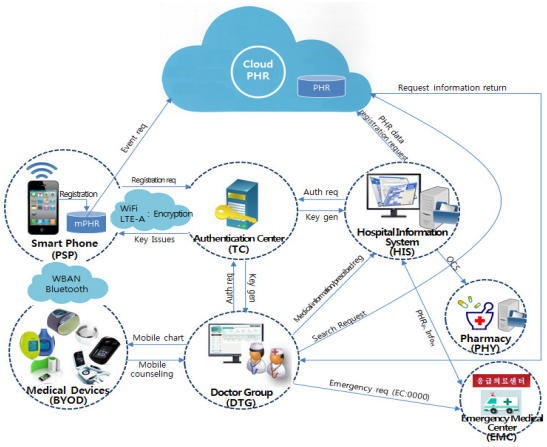

그림 1. 제안 시스템
Fig. 1 Proposal System

제안 시스템은 3단계로 디바이스와 사용자 등록단계, 건강정보 수집과 의료정보 전달 및 저장단계인 원격의료 단계, 마지막으로 환자의 응급상황이나 사용자의 병원 방문시 의료 데이터 접근을 위한 응급단계로 구성된다. 제안 시스템에서 사용되는 변수는 [표 2]과 같이 정의한다.

표 2. 기호정의
Table. 2 Symbol definitions

Variable	Meaning
cPHR	Cloud Personal health information record
HID_p / HID_p	Patient's private key/Private key of a doctor
Mac_d	MAC value of BYOD
HIS	Hospital information system
PS_{info}/DTG_{info}	patient / doctors infor
ID_p / ID_d	patient ID/ Doctor ID
none	Randome value
SK_d	signing keys
TS	Time Stamp
EC	emergency stars verification code
PHR_p	patient's personal health information record
$eOCS_p$	emergency prescriptions

3.2. 제안 시스템 설계

3.2.1. 등록단계

BYOD 환경에서 원격의료를 사용할 사용자 등록 및 개인키를 발급하는 과정으로 구성된다.

① 의료용 디바이스는 환자의 스마트폰에 디바이스(Mac_d)을 등록한다.

BYOD → 환자 : *Req* REG(Mac_d)

② 환자는 사용할 원격의료가 등록된 병원시스템에 자신의 아이디와 개인키로 암호화한 정보(자신이 소유한 BYOD와 환자의 정보)를 등록을 위해 전달한다.

환자 → HIS : *Req* REG(ID_p,EK_{pub-p}(Mac_d,PS_{info}))

③ HIS는 수신한 환자정보를 이용해 개인키(HIDpru-p)를 생성하고 환자에게 BYOD의 Mac을 이용해 암호화 하여 전달한다.

HIS: $HID_{pru-p}=(ID_p \oplus Mac_d \oplus PS_{info})$

HIS → 환자 : *Resp* EK_{Mac-p}(HID_{pri-p})

④ 의료진(의사나 간호사)은 자신의 정보(아이디, 의료진정보, 타임스탬프)를 HIS에 등록한다.

의료진 → HIS : *Req* CRT((ID_d, DTG_{info}, TS)

⑤ HIS는 수신하나 정보를 이용해 개인키를 생성하고 인증서버로 생성한 의료진 정보와 none을 전달한다.

$HID_d=(ID_d \oplus TS_d \oplus DTG_{info})$

HIS → TC : *Req* (HID_d, HID_{info}, none)

⑥ 인증서버는 HIS에게 수신한 의료진 정보를 검증하고, 서명에 사용한 서명키를 생성하고 의료진에게 발급한다.

$SK_d=(ID_d \oplus TS_d \oplus DTG_{info}$

TC → DTG : *Resp* EK_{Mac-d}(SK_d ,none)

3.2.2. 원격의료 단계

원격의료 단계는 BYOD가 수집한 건강정보를 원격의료시스템으로 전달하고 의료진은 의료정보/처방전을 서명키를 이용해 암호화하여 전달한다. 환자의 원격의료시스템에서 생성된 개인의료정보는 클라우드 서버에 암호화 되어 저장 관리되는 과정으로 구성된다.

① BYOD환경의 의료용 디바이스는 환자의 건강정보를 스캔하고 스캔 정보를 환자가 소유한 스마트폰으로 전달하게 된다. 이때 건강정보의 보안을 위해 WBAN 통신을 사용한다.

BYOD → 환자, *Scan* ($Info_H$, TS)

② 환자는 자신의 스마트 폰으로 수집된 건강정보데이터와 자신의 아이디를 자신의 개인키로 암호화하여 병원시스템으로 전달한다.

환자 → HIS : *Req* (ID_p ,EK_{HIDp}(ID_d, Mac_d, $Info_H$))

③ HIS는 수신한 정보를 환자의 병원키로 복호화해서 건강정보를 획득하고 담당의사에게 전달한다.

$\boldsymbol{M_{IDp}=DK_{HIDp}(Mac_d, Info)}$

HIS → 의료진 : *Resp* EK_{HIDd} (EMR_{IDp} , $Info_H$)

④ 의료진은 HIS로부터 수신한 환자 건강정보를 판단해서 응급상황(EMG)이 아닐 경우는 원격시스템을 통해 서명한 처방을 전달하고 HIS에 개인의료데이터를 저장한다. (만약 응급상황일 경우 응급코드(EC:0000)를 함께 전달)

의료진 → 환자 : *Resp* EK_{Mac-p} (HID_p,Sig_{SKd}(OCS_p))

의료진 → HIS : *save* (HID_p, Sig_{SKd}(EMR_{IDp},, OCS_{IDp}))

3.2.3. 응급단계

BYOD 환경에서 원격의료 시스템은 지속적인 환자의 모니터링을 통해 위급한 상황에 대비할 수 있다. BYOD에서 응급상황이 센싱되면 이는 바로 HIS로 전달되고 응급센터와 연결되어 호출된다.

① BYOD는 센싱한 데이터가 임계값을 넘어 응급상황이 발생하면 응급상황정보를 환자의 스마트폰에 알리는 동시에 등록된 HIS로 전달한다.

BYOD → 환자 : *sensing* (EC, $Info_H$, TS)

환자 → HIS : *Req* (EC, $Info_H$, TS)

② 의료진은 환자의 상태를 원격의료시스템을 통해 실시간 모니터링을 수행한다.

Real Time checking

의료진 → 환자 : *Resp* (PHR_P, $Info_H$)

③ 의료진은 실시간 모니터링을 수행하며 긴급수송 차량에 처방이 필요한 경우 BYOD 환경을 이용해 응급처방을 전달한다.

의료진 → EMC : *Req* (PHR_P, $Sig_{SKd}(eOCS_P)$)

④ 응급이동 중 응급의료센터 차량 안에서 발생되는 응급의료정보를 원격의료 시스템으로 전달한다.

EMC → 의료진 : Resp (PHR_P ,$eOCS_P$,ID_E,TS)

[그림 2]는 제안방식의 BYOD를 활용한 스마트헬스 환경에서의 메시지 플로우를 나타낸 것이다. 제안방식은 BYOD를 활용한 스마트헬스 환경에서 건강정보를 수집하는 의료용 디바이스의 상호운용성과 확장성을 제공하기 위해 환자의 스마트폰과 IEEE 802.15의 표준을 지원하는 무선인체 네트워크(WBAN: wireless body area network)와 블루투스를 이용한다. 또한 환자(스마트폰)는 원격지의 병원정보시스템(HIS) 연결은 ITU-U에 의해 인증되고 LTE-A 또는 WiFi 모바일 네트워크 표준을 사용하고 의료용 디바이스와 환자의 스마트폰은 무선인체네트워크를 사용함으로 안전성을 제공한다. WBAN은 인체나 인체 인근에 부착된 다양한 의료센서나 기기와 연결되기에 환자의 이동성을 지원하고 어떤 기기와도 연동이 가능하기에 상호운용성(inter-operability)을 제공할 수 있다.

Ⅳ. 제안시스템의 안전성 평가

4.1. 실험환경

제안 논문의 효율성과 안전성을 평가하기 위해 Qual Net 4.5 시뮬레이터를 이용해 접근 사용자별로 디바이스를 서로 다르게 지정하고 데이터 전송시 소요되는 통

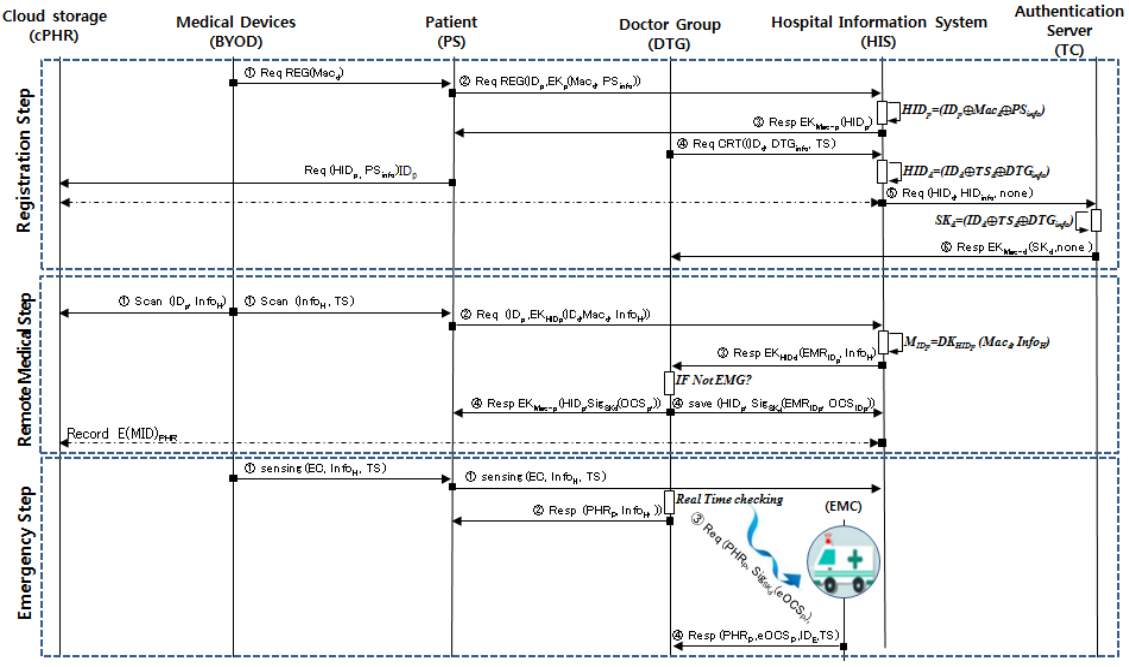

그림 2. 메시지 플로우
Fig. 2 Message flow

신 오버헤드를 데이터의 암호화 전후를 비교한다. [그림 3]은 시뮬레이션 환경으로 총 10명의 환자와 각 환자가 서로 다른 BYOD 디바이스를 이용해 건강데이터를 수집한다.

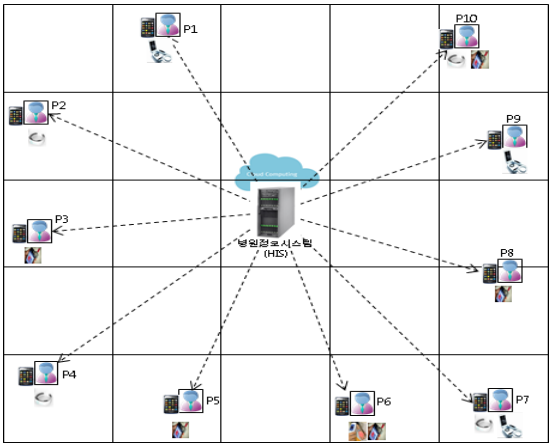

그림 3. 시뮬레이션 환경
Fig. 3 Simulation environment

환자들의 디바이스 등록시간은 디바이스가 1개인 경우 평균0.38sec, 2개의 디바이스를 등록하는 경우 평균 0.59sec, 3개의 디바이스를 등록하는 경우 0.63sec가 소모된다. 또한 제안 시스템의 데이터 전송에서 발생하는 통신 오버헤드를 비교한 결과 [그림 4]와 같이 나타났다.

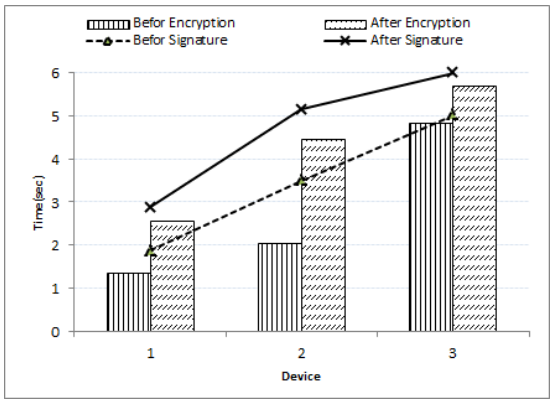

그림 4. 데이터 전송시 소요되는 통신 오버헤드
Fig. 4 Communication overhead to transmit data

[그림 4]와 같이 제안 알고리즘의 전송데이터의 암호화를 하지 않고 데이터를 전송하는 경우와 암호화 데이터를 전송하는 경우 통신오버헤드를 비교한 결과 평균 1.499mJ정도의 속도차이를 보였다. 또한 진료진의 서명을 통해 데이터를 전달하는 경우와 서명을 수행하지 않은 상태로 전달하는 경우를 비교한 결과 1.212mJ의 차이를 보였다. [그림 5]는 제안방법의 일반모드와 긴급모드 상태에서 통신오버헤를 비교한 결과 일반모드에서는 평균 3.778sec가 소요되는 반면 긴급모드에서는 2.262sec가 소요된다.

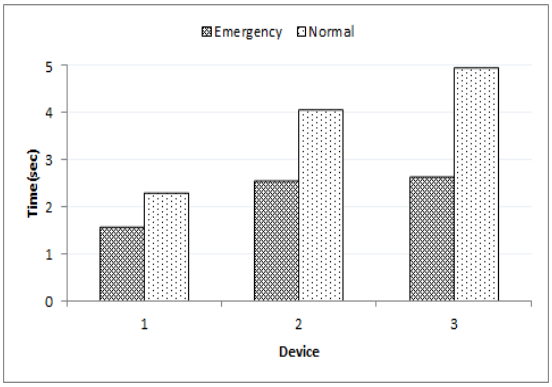

그림 5. 응급과 일반상태에서의 통신 오버헤드
Fig. 5 Communication overhead in the emergency and normal state

4.2. 보안성 분석

4.2.1. 가장공격(Impersonation attack)

악의적인 사용자가 사용자 정보를 이용하여 올바른 사용자로서 위장하는 공격기법으로 사용자 등록 프로토콜에서 사용자의 PS_{info}와 DTG_{info})를 검증함으로써 사용자의 진위여부를 확인한다. 또한 서명에 따라 사용자 권한을 분석함으로써 가장공격은 실패한다.

4.2.2. 재전송 공격 (reply attack)

재전송 공격은 사용자가 과거 세션에서 서버와 통신했던 메시지를 공격자가 저장했다가 이후의 세션에 서이 메시지를 재전송하여 서버로부터 인증 받게 되는 공격이다. 제안 논문에서는 건강정보와 의료정보를 전달시 타임스탬프를 함께 전송(Req CRT((ID_d, DTG_{info}, TS))함으로 재전송 공격은 실패한다.

4.2.3. 중간자 공격(man-in-the-middle attack)

일반적으로 무선네트워크에서는 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법인 중간자 공격에 취약하다. 그러나 제안 논문에서는 중요 의료정보와 건강정보를 암호화 연산을 수행하고 ($ID_d \oplus TS_d \oplus DTG_{info}$) 비밀키로(Resp $EK_{Mac\text{-}d}(SK_d$, none))안전하게 전달한다. 개인키를 가지고 있어야 위장이 가능하므로 중간자 공격은 불가능하다.

Ⅴ. 결 론

제안 논문은 스마트기기의 발달과 더불어 의료기기의 급속한 발달을 이용해 BYOD를 활용해 스마트 헬스 환경에서 수집된 건강정보를 활용해 원격의료 활용에 있어 안전한 데이터 전송을 제안한다. 민감한 건강정보 및 의료정보데이터의 전송을 위해 암호화를 수행함으로 데이터의 보안성을 향상하고 통신 오버헤드를 감소함으로 BYOD를 활용한 스마트헬스 환경에 적합한 방식이라고 할 수 있다.

또한 다양한 디바이스의 활용을 위해 확장성이 높은 WBAN과 블루투스를 기반으로 제안되어 다양한 의료용 기기의 확장성을 보장한다. 제안 방식은 특히나 만성질환을 앓고 있는 환자를 대상으로 보다 효율성을 높일 수 있고 일반모드에서 원격의료를 사용하는 것과 긴급모드에서 원격의료를 사용하는 경우 시뮬레이션 결과 통신오버헤드를 약 1.5sec 빠르게 긴급 상황에 대비할 수 있음을 보였다.

또한 매우 민감한 건강 및 의료데이터의 안전성을 위해 암호화를 제공함으로 안전한 개인정보보호가 가능함을 보였다. 그러나 이 논문의 제약점으로는 실제 환경에 적용이 어려운 문제점으로 시뮬레이션 툴을 활용해 실험함으로써 실제 환경에서 발생되는 디바이스 호환성이나 통신 오버헤드가 발생하는지 정확한 계산이 안 되었다는 점이지만 이미 WBAN의 상호호환성은 증명이 된 것이어서 크게 문제가 되지는 않을 것이라 생각된다.

향후 이 논문은 실제 병원 환경에서 사용되는 다양한 프로토콜 기반으로 실험함으로써 보다 안전한 원격의료 서비스 지원이 가능할 것으로 기대된다.

REFERENCES

[1] H. W Kim, " Market expected to enable telemedicine pilot project conducted", *KISTI MARKET REPORT,* vol. 4, no.12, pp. 20-23, Dec.2014.

[2] G. Y. Noh, M. S. Kwon and H. J. Jang, "The Acceptance Model of Telemedicine for Chronic Disease in Rural Community", *Journal of korea contents association,* vol. 14, no. 8, pp. 287-296, 2014.

[3] Y. Min, B. W. Jin, K. H. Lee and K. W. Lee, "A Study for Key Generation and Access Control Protocol in BYOD Environments", *Journal of korea contents association,* vol. 15, no. 5, pp. 27-35, 2014.

[4] C. Y. Heo and B. Y. Yu, "Telemedicine trends at home and abroad with a smartphone application", *Journal of TTA (U-health special report),* vol.145, pp. 38-43, 2013.

[5] H. S. Park, H. S. Kim, H. J. Jung and H. Cho, "Development of m-Health Application based on Medical Informatics Standards", *Journal of Korea Multimedia Society,* vol.7, no.5, pp. 640-653, May.2014.

[6] W. H. Kim, S. K. Lee, C. W. Jeong, K. H. Yoon and S. C. Joo, "Medical Information System Based on Data Synchronization Using Dynamic Access Control Mechanism In Multi-Devices Environment", *in Proceeding of KSII Conference,* pp.39-40, 2014.

[7] J. S. Yang, Y. S. Lee and Y. S Hong, " Implementation of secured remote EMR Medical Information using Encryption algorithm", *Journal of the institute of internet, Broadcastiong and communication,* vol.14, no.4, pp.133-139, 2014.

[8] http://www.dailymedi.com/news/view.html?section=1&category=4&no=790031

[9] C. O. Rolim, F. L. ,Koch, C. B. Westphall, J. Werner, J. A. Fracalossi and G. S. Salvador, "A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions", *in Proceeding of the Bio informatics and Bioengineering (BIBE), 2013 IEEE 13th International Conference on*, pp.1-4, 2013.

[10] C. G. Song, K. H. Lee and G. S. Ryu, "Process of the Encryption key using a Physical Information in the U-Healthcare Service", *Journal of society of digital policy &management,* vol 12, no.1, pp.573-578, 2014.

[11] C. H. Liu, F.Q. Lin, D. L. Chiang, T. L. Chen, C. S. Chen, H. Y. Lin, Y. F. Chung and T. S. Chen, "Secure PHR Access Control Scheme for Healthcare Application Clouds", *in Proceeding of 42nd International Conference*

on Parallel Processing, pp.1069-1076, 2013.

[12] D. G. Park, "A Development of Standard and Bio-Authentication Technology for Telemedicine", Korea Information Security agency report 2007, 2007.

[13] National internet development agency of korea. http://seed.kisa.or

[14] H. J. Kim, "Privacy, Confidentiality, and Informed Consent Issues Relating to Telemedicine in the United States", *Journal of the kangwon national university institute of comparative legal studies,* vol 43, pp. 199-235, 2014.

[15] N. K. Lee and J. O. Lee, "A Comparative Study on the telehealth regulations between U.S.A, Australia and Japan for developing the Korean telehealth system", *Journal of The e-Business Studies,* vol.15, no.3, pp. 97-123, 2014.

조영복(Young-bok Cho)

2005: 충북대학교 전자계산학과 공학석사.
2012: 충북대학교 전자계산학과 공학박사
현 재: 충북대학교 의학과 박사과정. 충북대학교 전자정보대학 소프트웨어학과 초빙교수
※관심분야: 인증, 정보보안, 의료정보보호
Email : bogicho@cbnu.ac.kr

우성희(Sung-hee Woo)

1993: 충북대학교 전자계산학과 이학석사.
1999: 충북대학교 전자계산학과 이학박사
현재: 한국교통대학교 의료정보공학과 교수
※ 관심분야: 침입차단 및 방지, 의료정보보호, 정보보안, 컴퓨터네트워크
Email : shwoo@ut.ac.kr

이상호(Sang-ho Lee)

1989: 숭실대학교 전자계산학과 공학박사.
현 재: 충북대학교 전자정보대학 소프트웨어학과 교수
※관심분야: 컴퓨터네트워크, 정보보호, 데이터통신
Email : shlee@cbnu.ac.kr

박종배(Jong-bae Park)

2004 : 대전대학교 이학석사
2011 : 대전대학교 이학박사
현재 : 현 충북보건과학대학교 방사선과 교수. 현) 학과장
※관심분야: IT융합, 의료정보
Email : pjbcbdr@ch충북보건대학교 방사선과su.ac.kr