http://dx.doi.org/10.14400/JDPM.2013.11.11.415

웰니스 환경에서 암호화 프로토콜 적용을 위한 모바일과 원격 서버간 트래픽 성능 평가

이재필*, 김영혁*, 이재광*
한남대학교, 컴퓨터공학과*

The traffic performance evaluation between remote server and mobile for applying to encryption protocol in the Wellness environment

Jae-Pil Lee*, Young-Hyuk Kim*, Jae-Kwang Lee*
Dept. of Computer Engineering Hannam University*

요 약 U-Wellness Healthcare System(U-WHS)이란, 웰빙(wellbeing)과 피트니스(fitness)를 결합한 원격 건강 관리 시스템을 말한다. 이러한 시스템에서는 시간과 공간에 제약 없이 언제 어디서나 환자의 생체정보를 측정 및 관리 할 수 있는 것이다. 본 논문에서는 스마트모바일기기와 HIS(Hospital Information System)간 생체정보 전송시 암호화 모듈이 통신 평가에 끼치는 영향을 알아보기 위해 수행하였다. U-WHS 모델의 경우 클라이언트는 iOS Xcode환경의 Objective-c 개발 언어를 이용하여 SEED, HIGHT 암호화 모듈 적용을 하였다. HIS의 경우 클라이언트와 서버간 통신을 위하여 HTML5의 WebSocket API와 관계형 데이터베이스 관리 시스템인 MySQL를 적용하였다. 그리하여 WIFI 통신 환경에서 Wireshark를 사용, 분석하여 생체 정보의 데이터 전송율, 지연율, 손실율에 대한 평가를 확인하였다.

주제어 : U-WHS, 생체정보, 암호화프로토콜, 웹소켓, 와이어샤크, 노드제이에스

Abstract U-WHS refers to a means of remote health monitoring service to combine fitness with wellbing. U-WHS is a system which can measure and manage biometric information of patients without any limitation on time and space. In this paper, we performed in order to look into the influence that the encryption module influences on the communication evaluation in the biometric information transmission gone to the smart mobile device and Hospital Information System.In the case of the U-WHS model, the client used the Objective-c programming language for software development of iOS Xcode environment and SEED and HIGHT encryption module was applied. In the case of HIS, the MySQL which is the Websocket API of the HTML5 and relational database management system for the client and inter-server communication was applied. Therefore, in WIFI communication environment, by using wireshark, data transfer rate of the biometric information, delay and loss rate was checked for the evaluation.

Key Words : U-WHS, Biometric information, encryption protocol, websocket, wireshark, node.js

* 본 논문은 2013년 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2011-0013029)
Received 4 October 2013, Revised 28 October 2013
Accepted 20 November 2013
Corresponding Author: Jae-Kwang Lee(Hannam University)
Email: jklee@newk.hnu.kr

ISSN: 1738-1916

1. 서론

고령화의 급진전, 생활수준의 향상과 높은 삶의 질을 성취 하고자 하는 현대인들의 요구가 증가하면서 웰니스(Wellness)에 대한 관심이 증가하고 있다. 전 세계적으로 예방과 관리를 통한 건강 수명 연장으로 변모하고 있다. 전 세계 웰니스 시장의 경우 규모는 약 2천 2백조 원($1.9 trillion)으로 추산되며, 이중 상위 3개 분야(미용 및 노화방지, 피트니스, 영양 및 체중감량)는 전체 산업의 70%를 차지하고 있다[1]. 위와 같이 치료에서 예방 중심으로 소비자의 건강관리 패러다임이 변화하고 있다.

미국의 경우, 공공부분의 의료산업 투자를 확대 중이며, 병원과 개인 건강관리 서비스 구축이 활발히 진행 중이다. 일본의 경우, 2011년 대지진 및 원전 피해로 인해 의료와 wellness에 대한 수요가 높아진 상황이며, 지역별 균형적 의료 발전 중이다. 유럽의 경우, 영국의 국가의료서비스(NHS)의 서비스를 통해 의료 데이터 활용 및 공유를 위한 정책적 노력을 부각하고 있다[2].

국내 웰니스 사업의 경우 u-Health 서비스에 포함되어 2007년부터 정부 주도로 지역 주민의 복지 향상을 위한 다양한 시범 사업이 추진되었다. 시범사업 대상으로는 저소득층 및 독거노인, 일반 지역 주민을 중심으로 진단을 통하여 사전 예방적 건강관리와 안전 관련 서비스 등을 제공한다. 특히 지속적으로 건강 상태를 확인해야 할 만성질환 환자의 경우 고령자에 그치지 않고 전 연령층에 거쳐 지속적으로 확대되고 있다. 이에 따라 만성질환자의 관리 대안으로 U-WHS서비스를 연구하였다.

U-WHS(Ubiquitous Wellness Healthcare System)이란 , 웰빙(wellbeing)과 피트니스(fitness)를 결합한 원격 건강관리 시스템으로 시간과 공간에 제약 없이 언제 어디서나 환자의 생체 정보를 측정 및 관리 할 수 있다. 또한 육체적, 정신적, 감성적, 사회적, 지적 영역에서의 최적의 상태를 추구를 의미한다[3]. 본 논문에서는 지속적으로 상태 확인이 필요한 고위험 환자와 독거노인을 대상으로 웰니스 환경에서 암호화 프로토콜 적용을 위한 모바일과 원격 HIS 서버간 트래픽 성능 평가를 목표로 한다. 기존의 선행 연구인 통신 프로토콜 설계[4][5] 모델을 기반으로 U-WHS의 환경에 암호 알고리즘 모델을 적용하였다. 이를 통하여 기존의 선행 연구인 U-WHS의 환경에서 스마트모바일과 HIS 서버간 데이터 전송율 평가의 연구[6]을 수정, 확장하여 SEED, HIGHT 암호화 모듈이 적용된 U-WHS모델 기반으로 스마트모바일 기기와 HIS간 데이터 전송을 하였다. 앞선 연구와 달리 모바일기반에서 암호화 모듈 적용을 통하여 HIS측 부하를 줄이고자 하였다. 이를 위해 node.js를 사용하여 모바일기기와 HIS간의 소켓 통신을 구축 하였다. 스마트모바일기기로는 iOS 기반 Objective-C 를 이용하여 암호화 모듈을 적용한 U-WHS Mobile App을 개발 하였다. 또한 데이터 트래픽 성능 평가를 위하여 wireshark를 사용하여 암호화 프로토콜 적용여부에 따른 특정한 구간의 시간에 대한 정보를 생성하여 HIS 환경에 DB를 구축 하였다. 그리하여 무선 통신 환경에서 wireshark를 사용하여 생체정보의 데이터 전송율, 지연율, 손실율에 대한 평가를 진행 하였다. 이 논문의 구성은 다음과 같다. 2장 관련 연구를 통한 선행 연구를 분석하고, 3장 시스템 설계와 암호화 프로토콜이 적용된 보안모델을 제시하고, 4장에서는 실험결과를 분석, 5장 결론으로 연구를 정리한다.

2. 관련연구

2.1 생체정보 보안기능 원격 모니터링 시스템

원격지에서 노약자 및 신체부자유자의 건강을 측정하고 모니터링을 하기 위한 시스템이다. 센서 장치를 갖는 건강 서버는 환자의 생체정보를 측정하고 이를 패킷 화하여 원격지 시스템에 전송하는 아키텍처로 구성 되었다. 제안된 시스템은 유선 통신 환경에서 AES 암호 알고리즘을 사용하여 호흡, 맥박, 온도 정보를 이용하여 원격지에서 Web Host를 이용하여 측정하고 인증철자와 웹 프로그램을 통한 구성하여 개인 건강정보 누출에 대비하는 원격 헬스케어 모니터링 시스템의 모델을 제안하였다[7]. 그러나 본 논문에서는 무선 환경에서 사용자의 스마트모바일 기기에서 암호화 적용, 성능 평가하는데 목적이 있다.

2.2 무선센서네트워크 기반 유헬스 시스템

낮은 무선 네트워크 대역폭은 환경의 변화에 따라 생체 데이터의 신뢰도를 변화시킨다. 또한 무선센서네트워크 기술은 환자의 생체신호를 측정하고 전송할 수 있도록 도와 다양한 메디컬과 헬스케어 솔루션을 제공한다. 무선센서네트워크 환경에서는 헬스케어 시스템에 적용

가능한 모바일 헬스케어 라우팅 프로토콜에 성능향상을 시킬 목적으로 RF 세기, 배터리 상태, 배치 상태 등의 조건을 이용하여 통신 실험을 수행하였다. 최적 통신 거리를 평가하고, 데이터 전송 수신율 평가를 위해 질의응답 횟수를 통해 수신율을 확인 하였다. 또한 노드 간 배치 상태와 RF 세기에 따른 패킷 수신율 평가를 하였다. 이를 통하여 모바일 헬스케어 라우팅 프로토콜의 최적 노드 전력제어 및 배치 방법을 제안하였다[8].

2.3 무선 센서 네트워크를 사용하여 실내 환경에서 노인의 에이전트 기반 건강 모니터링

실내 환경에서 노인의 건강 모니터링에 사용되는 멀티 에이전트 시스템을 모델을 제안하였다[9]. 멀티 에이전트 시스템(MAS)는 네 가지 에이전트로 구성되어 관리, 제어, 쿼리 데이터 에이전트로 구성되어 동적특성과 이동성에 적합한 센서정보로 부터 환자의 생체 신호를 분석, 수집, 저장하여 체온, 혈압, 맥박 및 호흡 등의 생체 신호를 모니터링 하였다. 데이터 에이전트는 Epsilon 근삿값 사용하여 수집된 데이터의 양을 감소하였다. 이러한 에이전트는 하나의 시스템에 상주 할 수 있으며 네트워크를 통해 연결되는 시스템의 필요에 따라 호출이 가능한 시스템으로 구성되었다. 그리하여 에이전트 사용을 통하여 데이터 트래픽 및 보조 스토리지 공간 요구 사항을 줄일 수 있도록 구성 되었다.

2.4 모바일 에드혹 네트워크를 통하여 환자 모니터링을 활성화하기 위한 프레임워크

애드혹(ad hoc) 네트워크는 네트워크 범위를 강화하고 기반망(infrastructure networks)네트워크에서 확장이용이하지 않거나 존재하지 않는 범위를 가지고 있는 영역에서 신호 전송의 잠재력을 제시하고 있다. 환자 모니터링 응용 프로그램은 크게 신호 전송을 위한 인프라 기반의 무선 네트워크에 의존하고 있다. 제안한 방법의 분석 평가는 종단간 환자 모니터링 장치 간에 형성된 모바일 애드혹 네트워크는 환자 모니터링 애플리케이션의 품질을 개선하여 신호 전송의 신뢰성을 향상하도록 구성되었다[10].

2.5 신뢰 기반의 멀티 캐스트 방식을 사용한 보안 모바일 의료 시스템

의료 센서를 사용한 유연한 이동성 모니터링으로 사고 단계에서 전문가 기반 치료를 시작할 수 있는 통신 장치가 장착된 시스템으로 구성된다. 제안한 시스템에서는 환자의 모바일 장치 및 센서로 구성된 시스템에서 무선으로 전송 시 노드의 오동작을 효과적으로 방지하고자 하였다[11]. 방지 기간 동안 신뢰할 수 있는 노드가 통신에 참여하는 것이 허용되도록 각 노드의 동작을 평가하기 위하여 신뢰 기반, 동적으로 노드를 관리하고 효율적 분산 방식으로 신뢰 평가 모델을 기반으로 비대칭 알고리즘 기반으로 암호화 알고리즘과 인증을 통하여 보안 멀티캐스트 방식을 제안하였다.

2.6 착용형 개인 건강관리 장치를 위한 실시간 생체신호 암호화 모듈의 설계

본 논문에서는 착용형 개인 건강관리 장치에서 생성, 전송되는 개인 의료 정보를 보호하기 위한 암호화 모듈을 설계 하였다[12]. 이를 위하여 무선 개인 영역 네트워크(Wireless Personal Area Network)에서 사용되는 착용형 PHD에서 사용자가 관리하는 비밀 키를 이용한 16비트 마이크로 컨트롤러 장치에 DES 알고리즘을 내장하여 실시간 암호화 생체 신호를 전송하는 시스템을 제안하였다. 그러나 본 논문에서는 U-WHS환경 센서 네트워크에서는 저전력 경량화를 요구하는 스마트 모바일 환경에서 적합한 HIGHT, SEED 알고리즘을 적용하여 연구를 진행하였다.

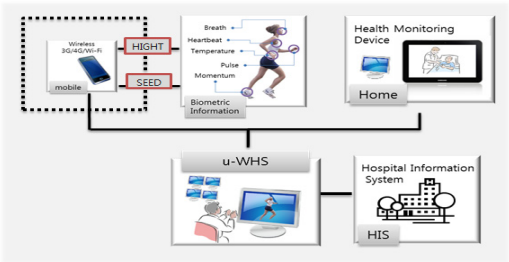
2.7 유헬스케어의 무선환경에 적합한 WiMAX 보안 측정 및 분석

이동성을 가지는 환자가 체내삽입장치내 환자의 생체정보를 무선 액세스 네트워크 구간에서 불법적으로 노출되지 않도록 무선 액세스 네트워크에 WiMAX 네트워크을 구축하는 방법을 제안하였다[13]. 생체정보를 불법적으로 수집하는 것을 예방하기 위하여 WiMAX 네트워크에서 환자의 초기 인증과정이 끝난 후 재접속시 초기 인증정보와 인증서를 이용하여 추가 인증을 수행하지 않았다. 또한 무선접근구간의 최적의 보안 성능을 얻기 위한 실험 모델의 특징은 서버이용률을 70%로 설정하고 로컬

도메인에서 한 개의 게이트웨이를 통하여 인증하는 형태로 구성되며 성능평가를 위하여 연결 지연, 인증 처리, 서버의 평균 처리를 설정 하였다.

3. 실험 및 결과 분석

3.1 U-WUS 설계 모델



[Fig. 1] U-WHS system configuration

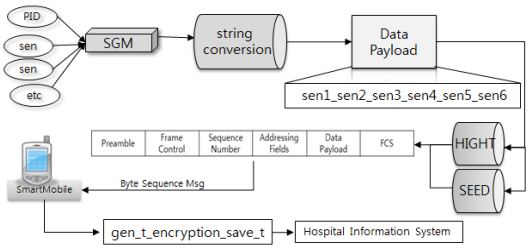
이 절에서는 "Fig. 1"과 같이 U-WHS 환경에서 만성질환자의 거주 공간을 대상으로 보안 성능을 평가하였다. U-WHS의 시스템 구성은 다음과 같다. 환자의 생체 센서 정보가 수집되어 스마트모바일, HIS(Hospital Information System)의 형태로 범위를 제안한다.

〈Table 1〉 Experiment environment

		Server	Emulator	S/W
Spec	CPU	Intel i5-2500 3.30GHz	Intel Core 2 Duo 1..4GHz	-
	RAM	8GB	2GB	-
	Network	Ethernet: 54Mbps	AirePort Extreme WiFi 802.11n	-
OS		Windows 7 Enterprise k	OS X Lion 10.7.5	-
S/W		Webpage: node.js	iOS 6.1 emulator	Wireshark
DB		MySQL 5.1.41	-	-

<Table 1>에서와 같이 실험을 위해 사용된 서버는 윈도우 기반 HTML5의 Websocket을 사용하여 웹페이지 서비스를 제공하고 모바일 환경 iOS Simulator 무선 환경 기반에서 실험을 하였다.

이러한 생체정보는 "Fig. 2"는 U-WHS 환경에서 HIGHT, SEED 암호화 알고리즘을 설계한 모델이다. 만

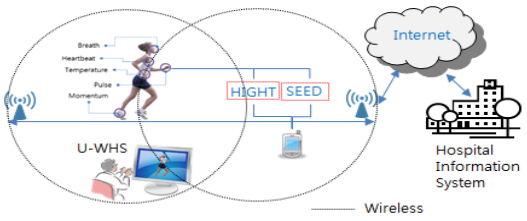


[Fig. 2] U-WHS apply encryption model

성질환자의 생체센서 정보를 입력받아 SGM(Security Gateway Manager)에서 수집하여 PID(patient identity), 호흡(Breath), 심박(Heartbeat), 체온(Temperature), 맥박(Pulse), 운동량(Momentum)의 생체 정보들로 구성 한다.

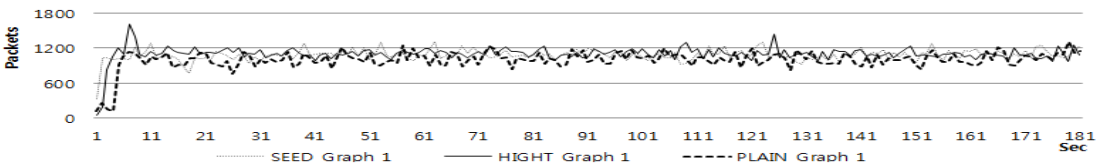
이와 같이 분산된 생체정보를 수집하고자 SGM을 두어 분산된 센서 노드(node)가 보내는 생체정보를 수집 후 데이터 타입을 'string'형으로 변환하여, 데이터 Payload 구분자 형태인 '_' 을 통해 각각의 데이터로 분리 저장한다[4][5]. 하나의 프레임으로 생성한 다음 두 가지의 유형으로 암호화가 적용된 HIGHT와 SEED알고리즘 제안과 PLAIN TEXT 형식으로 전송하는 방식을 적용 및 테스트를 진행 하였다. 이러한 과정에서 전송률 및 지연율 측정을 위하여 생성시간과 저장시간을 추가한다. 그리하여 환자의 이동성 및 활동 가능성 범위를 확인하기 위하여 실내에서 Mobile 과 HIS서버간 웹 소켓(node.js) 연결을 요청하고 받아들여 전송 Wi-Fi 환경에서 생체정보 데이터 전달시 wireshark를 이용한 트래픽 성능 평가 진행을 하였다.

3.2 U-WHS기반 통신 성능 평가

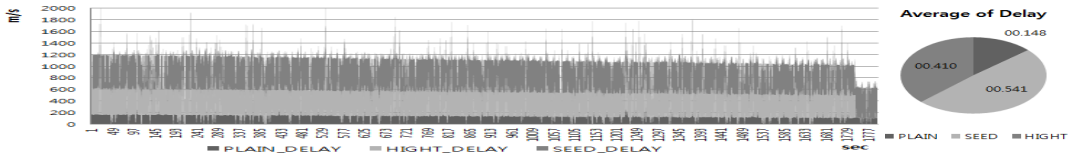


[Fig. 3] U-WHS Experiment environment

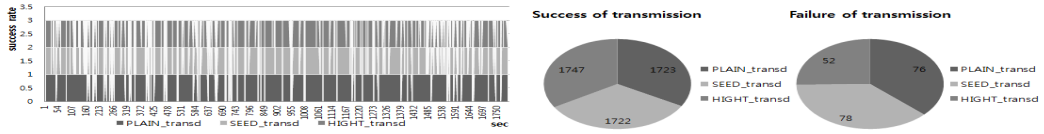
U-WHS 환경에서 만성질환자를 대상으로 무선 접근 구간에서 생체센서정보를 이용하여 통신 성능 평가를 하였다. 실험을 위해 3가지 유형별 PLAIN Text, HIGHT,



[Fig. 4] Statistics of Packet



[Fig. 5] Delay of packet



[Fig. 6] Loss of Packet

SEED 암호화 알고리즘을 각각 적용한 데이터를 전송하여 실험하였다. 통신 성능 평가 방법은 각 데이터 전송 시 30분 간격으로 테스트를 진행 하였다. “Fig. 4”는 만성질환자의 스마트모바일기기를 통한 이동성 상태를 확인하여 wireshark를 이용한 전송된 패킷의 통계를 나타낸다. 생체정보 SGM의 데이터를 전송하여 1초 간격으로 패킷(packetss)을 전송하여 총 1800초 동안 전송율을 확인하였다. 스마트모바일과 HIS간 평균 트래픽 전송율은 PLAIN Text(1000.3packets),SEED(1083.5 packets), HIGHT(1102.4packets) 순으로 패킷량을 확인 하였다.

"Fig. 5"는 스마트모바일기기에서 암호화 모듈 적용 유무에 따른 데이터 생성시간과 HIS 서버간 데이터베이스에 저장되는 타임스탬프(Timestamp)을 확인하여 데이터 패킷 지연율을 확인하였다. PLAIN TEXT, SEED, HIGHT순으로 각각 30분 동안의 실험을 통하여 평균 PLAIN TEXT(00.148m/s), HIGHT(00.410m/s), SEED (00.541 m/s), 순으로 SEED의 지연율이 높은 것으로 확인하였다. "Fig. 6"는 생체정보 SGM의 데이터를 전송하여 HIS 데이터베이스에 저장된 데이터를 기준으로 평가하였다. 1800개의 데이터의 생성값과 저장된 데이터값을 비교하여 평균 패킷 손실율을 계산하였다. 평균(packets) 패킷 손실율의 경우, HIGHT(2.97%), PLAIN TEXT (4.41%), SEED(4.52%)순으로 확인하였다. 이를 통하여 HIGHT의 손실율이 가장 적은 것으로 확인하였다.

4. 결론

본 연구는 건강상태를 지속적으로 확인 해야하는 만성질환자의 문제해결 방안으로 모바일 환경에서 암호화 프로토콜 적용에 따른 트래픽 분석 및 환자의 이동성 보장 연구를 진행하였다. 이에 본 논문에서는 모바일기기와 HIS 원격 서버간 생체정보 트래픽 성능 평가를 진행 하였다. U-WHS의 선행 연구[4][5]통신 프로토콜 설계를 기반으로 생체 정보의 보안 적용 및 통신 효율성을 평가하기 위하여 PLAIN TEXT와 HIGHT, SEED 알고리즘의 적용에 따른 전송율, 지연율, 손실율을 측정하였다. 실험을 통하여 환자의 활동 범위 및 이동성에 따라 데이터 트래픽 변화를 확인하였다. 전송율 경우 HIGHT알고리즘 패킷크기가 가장 높은 순으로 분류 되었으며, 지연율의 경우 SEED알고리즘의 지연율이 높은 것으로 확인되었다. 손실율의 경우 HIGHT 알고리즘이 가장 손실율이 적은 것으로 확인 하였다. 이와 같은 결과는 HIGHT가 SEED에 비해 절반의 입출력 키 길이를 사용한 결과로 데이터

지연, 손실율이 적은 것으로 확인하였다. 그리하여 본 연구에서는 암호화 프로토콜이 적용된 생체정보 전송시 암호화 모듈이 통신 평가에 미치는 영향을 파악, U-WHS 환경에 적합한 HIGHT적용을 통하여 시스템 성능 및 사용자의 서비스 품질 개선 향상을 할 것이라 평가 하였다. 향후 모바일 기반의 생체 데이터 처리 분석을 통한 사용자의 맞춤형 서비스를 제공하는 연구를 수행할 계획이다.

ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0013029)

REFERENCES

[1] National IT Industry Promotion Agency, “The industry development plan research through the business model analysis of the wellness industry”, 2012.

[2] National Information society agency, "ICT Convergence Industry Global trends and Implications", 2013-4

[3] S.H. Park, D.G. Jang, “The IT Convergence tendency of the field of the wellness”, 2013

[4] Y.H. Kim, “Mobile based HIGHT encryption for secure biometric information transfer of USN remote patient monitoring system”, 2011.

[5] Y.H. Kim, “Security Communication Implementation and Experiments for USN Fire Prevention System”, 2010.

[6] J.P. Lee, The communication performance evaluation between the remote server and SmartMobile using the Biometric information in the U-WHS environment, 2013.

[7] Y.H. Lee, Study on the Remote Health Monitoring System with Security code, 2008.

[8] S.C. Lee, Development of Mobile u-Healthcare System in WSN, 2012.

[9] V. Vaidehi, Agent Based Health Monitoring of Elderly People in Indoor Environments Using Wireless Sensor Networks, 2013.

[10] Sweta Sneha, A framework for enabling patient monitoring via mobile ad hoc network, 2013.

[11] Azzedine Boukerche, A Secure Mobile Healthcare System using Trust-Based Multicast Scheme, 2009.

[12] J.C. Kim, Design of Real-time Vital-Sign Encryption Module for Wearable Personal Healthcare Device, 2013.

[13] Y.S. Jeong, Measuring and Analyzing WiMAX Security adopt to Wireless Environment of U-Healthcare, 2013.

이 재 필(Lee, Jae Pil)

- 2008년 2월 : 중부대학교 정보보호학과(공학사)
- 2012년 2월 ~ 현재 : 한남대학교 컴퓨터공학과 석사과정
- 관심분야 : 정보보호 (Mobile, u-Health),모바일, 네트워크
- E-Mail : jplee@netwk.hnu.kr

김 영 혁(Kim, Young Hyuk)

- 2009년 2월 : 한남대학교 컴퓨터공과(공학사)
- 2011년 2월 : 한남대학교 컴퓨터공과(공학석사)
- 2011년 3월 ~ 현재 : 한남대학교 컴퓨터공학과 박사과정
- 관심분야 : 정보보호(Mobile, u-Health, 인증), 모바일 네트워크
- E-Mail : yhkim@netwk.hnu.kr

이 재 광(Lee, Jae Kwang)

- 1984년 2월 : 광운대학교 전자계산학과(이학사)
- 1986년 2월 : 광운대학교 전자계산학과(이학석사)
- 1993년 2월 : 광운대학교 전자계산학과(이학박사)
- 1993년 8월 ~ 현재 : 한남대학교 컴퓨터공학과 정교수
- 관심분야 : 네트워크, 정보보호
- E-Mail : jklee@hnu.kr