http://dx.doi.org/10.3745/KIPSTC.2012.19C.1.019

의료 센서 네트워크에서 휴대폰을 이용한 사용자 인증 및 안전한 데이터 통신 방안

김 지 현[†] · 도 인 실[††] · 박 정 민[†††] · 채 기 준[††††]

요 약

무선 센서 네트워크는 언제, 어디에서든, 때와 장소를 가리지 않고 사용자가 원하는 서비스를 제공해주는 시스템이다. 특히, 바이오 센서를 이용한 의료센서네트워크는 생명공학, 의료공학 분야에서 활발하게 활용이 되고 있다. 의료센서네트워크에서는 사용자가 시간적이나 공간적 제약을 받지 않고 집에서 건강을 모니터링 할 수 있는 환경이다. U-healthcare환경에서 긴급 상황이 발생 했을 때 빠르게 환자를 도와줄 수 있으며, 병원에서도 손쉽게 환자를 관리 할 수 있다는 장점을 갖는다. 이 환경에서는 개인의 건강과 생명에 직결된 데이터가 송수신되므로 개인의 프라이버시 보장과 데이터의 보안이 가장 중요한 요소이다. 본 논문에서는 휴대폰을 이용한 사용자 인증 방안과 데이터의 종류에 따라 긴급모드와 일반모드의 구분을 두어 안전하면서도 빠르게 데이터를 전송하는 방안을 제안하였다.

키워드 : 의료 센서 네트워크, 보안, 사용자 인증, 데이터 통신

User Authentication and Secure Data Communication Based on Mobile Phone for Medical Sensor Network

Jeehyun Kim[†] · Inshil Doh[††] · Jung-Min Park[†††] · Kijoon Chae[††††]

ABSTRACT

Wireless sensor network provides services anytime and anywhere they are requested. Especially, medical sensor network based on biosensors is applied a lot to biotechnology and medical engineering. In medical sensor network, people can make their health checked at home free from temporal and spatial constraints. In ubiquitous healthcare environment, people can get instant help even in the emergency, and in hospital, patients can be taken care of efficiently. In this environment, health and life related data are delivered, and the privacy and security of personal data are very important. In this paper, we propose user authentication and data communication mechanism in two modes, normal and urgent situation using cellular phone. Through our proposal, data can be transferred in quick and secure manner.

Keywords : Medical Sensor Network, Security, User Authentication, Data Communication

1. 서 론

최근 고령화 사회에 진입하면서 건강에 대한 관심증가로 유비쿼터스 기술을 활용한 U-헬스 서비스에 대한 관심이 증가하고 있다. 이러한 서비스를 제공하기 위해 소형의 센서 노드를 사용하여 언제, 어디에서든, 때와 장소를 가리지 않고 사용자가 원하는 서비스를 제공해 주는 시스템이 활발히 연구되고 있다. 특히, 인간의 신체이상 유무를 판독하기 위한 바이오센서는 생명공학 분야와 의료분야에서 활발하게 사용되며 최근 휴대용 의료기기 분야에서도 활용되고 있다.

이러한 바이오센서를 활용하는 유비쿼터스 사회에서의 의료서비스는 환자의 몸에 여러 개의 작은 센서를 착용하여 생체신호를 감지하고 이를 네트워크를 통해 의료진에게 통보를 하는 형태로 이루어진다. 이러한 환경에서는 환자가 가정에서 일상적인 생활을 하면서도 건강상태를 확인 받을 수 있을 뿐만 아니라 의료진은 멀리 떨어져 있는 환자를 원격으로 관리 할 수 있다. 또한 환자의 데이터를 저장해 놓음으로 환자의 건강 동향을 파악할 수 있으며, 위급상황 발생 시에 적절한 대응 방법을 빠르게 제공할 수 있다. 이러한 환경에서 사용자의 민감한 개인 정보가 외부로 유출되는 것을 방지하기 위한 개인의 프라이버시 보호와 데이터 전송

※ 이 연구는 2011학년도 이화여자대학교 Ewha Global Top 5 Project 연구비 지원 및 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 중점연구소지원사업으로 수행된 연구임(2011-0018397).
† 정 회 원 : 이화여자대학교 컴퓨터공학과 석사
†† 정 회 원 : 성균관대학교 정보통신공학부 연구교수(교신저자)
††† 정 회 원 : 한국과학기술연구원 실감교류로보틱스연구센터 선임연구원
†††† 종신회원 : 이화여자대학교 컴퓨터공학과 교수
논문접수 : 2011년 8월 23일
수 정 일 : 1차 2011년 11월 2일
심사완료 : 2011년 11월 9일

과정에서의 보안은 중요한 문제가 된다.

본 논문에서는 의료 센서 네트워크에서 휴대폰을 사용하여 데이터를 전송하는 과정에서의 안전한 인증 및 전송 방안에 대하여 소개한다. 휴대폰을 사용하여 정상적인 사용자만이 데이터를 전송할 수 있는 사용자 인증 방안과 데이터의 등급에 따른 전송 방안을 제안하였다. 긴급한 상황에서의 데이터가 발생하게 되면 매우 빠르게 전송하며, 일반적인 데이터를 전송할 때에는 공격으로부터 안전하게 전송 할 수 있도록 한다.

본문의 구성은 다음과 같다. 2장에서는 의료센서네트워크의 구조와 기존 연구 동향에 대해 기술하였다. 3장에서는 제안 메커니즘에 대한 자세한 기술을 하였으며, 이 메커니즘을 바탕으로 시뮬레이션을 한 결과와 분석을 4장에 기술하고 5장에서 결론을 맺는다.

2. 관련 연구

2.1 MSN 구조

의료 센서 네트워크는 (그림 1)과 같이 사람의 생체 정보를 병원까지 전송하는 네트워크이다. 사용자의 몸에는 바이오센서가 부착이 되어있어 센서의 종류에 따라 근전도, 혈압, 맥박, 산소포화도, 혈당 등을 측정 할 수 있다. 센서가 측정한 데이터는 사용자의 휴대폰으로 전송이 되며, 수집된 정보는 무선 네트워크를 통해 병원에 위치하고 있는 서버로 전송이 된다. 전문가는 이 정보를 저장 및 분석하여 사용자에게 적절한 처리를 할 수 있도록 한다.

2.2 연구 동향

[1], [2]에서는 Electrocardiography (ECG 또는 EKG) 와 같은 생체신호를 사용하여 키를 생성하는 방법에 대해 소개하였다. 동일한 사용자의 몸에 부착이 되어있는 센서라면 동일한 생체 신호를 측정한다. 이 신호를 바탕으로 키를 만들어 통신을 하는 방법이다. 하지만, 메디컬 센서 네트워크의 특수한 환경에서는 사용자의 몸에는 극소수의 센서만이 부착이 되어있기 때문에 센서들끼리 데이터를 주고 받는 일보다는 측정 데이터를 외부로 보낼 때의 보안이 더 중요하다. 위 논문들에서는 외부로 전송이 되는 데이터의 보안과 관련된 내용을 다루지 않고 있다.

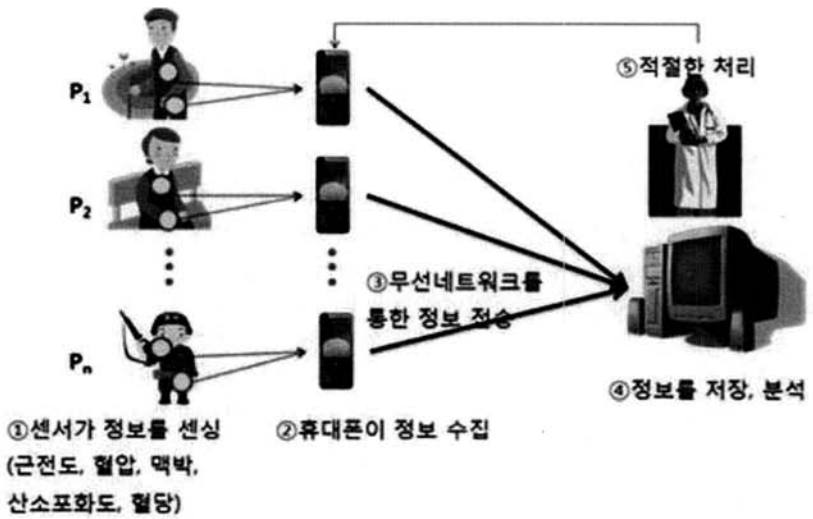
[3]에서는 사용자의 지문을 바탕으로 사용자 인증을 한 후 ECC를 기반으로 하여 생성이 된 키를 바탕으로 센서와 서버간의 통신을 제안하였다. 하지만, 일반적인 바이오 센서들이 모두 지문을 센싱하는 추가의 모듈을 가지고 있지 않기 때문에 이러한 방법으로 사용자를 인증하는 것에는 한계가 있다.

[4]에서는 신원기반암호화(Identity-Based Encryption) 방법을 사용하여 서버와 센서간의 안전한 통신 방법을 제안하였다. 이 방법은 공개키 기반의 암호화 방식을 사용하기 때문에 메모리와 배터리가 제한적인 센서에서는 계산량이 많고 저장해야 할 정보가 많다. 그렇기 때문에 센서에서의 배터리 소모가 빠르게 되어 네트워크의 수명이 줄어들어 적합하지 않다.

[5]에서는 pseudoinverse 행렬을 사용하여 센서와 서버간의 pairwise key를 생성하여 안전한 통신을 하는 방법을 소개하였다. 하지만, 데이터 인증 및 사용자 인증방안에 대해서는 언급하지 않고 있다.

[3], [4], [5]와 같은 메커니즘들은 몸에 부착이 되어있는 센서에서 바로 서버로 전송을 하기 때문에 센서의 통신 범위 내에 항상 서버가 존재해야 한다. 그러기 위해서는 사용자가 반드시 병원 내에 존재해야 한다는 단점이 있어서 원거리 서비스를 제공하는 데에는 적합하지 않다.

[6]에서는 센서와 PDA사이에서 블루투스를 이용한 통신을 할 때 공유키를 생성하는 방법을 제안하였다. 하지만 PDA를 사용자가 소유하는 것이 아니라 병원 내의 의사가 소유하고 있는 PDA와 환자의 센서간의 통신이기 때문에 이 방법 역시 환자가 반드시 병원 내에 존재해야 한다는 단점



(그림 1) 의료센서네트워크의 구조

이 있다. 이러한 단점을 극복하기 위해서는 센서가 측정한 데이터를 서버까지 전송해 줄 수 있는 중간 매체를 사용자가 휴대하고 있어야 한다. 이를 위해 사용자의 PDA, 노트북, 휴대폰 등을 사용하는 방법이 있다.

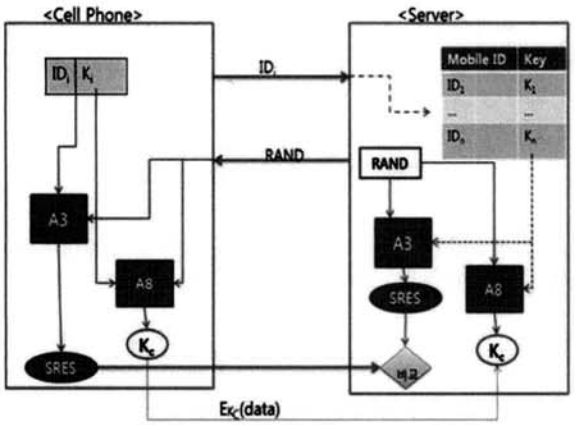
Tsai, Y., 등은 [7]에서 무선랜 환경에서 가입자를 인증하기 위해 SIM카드를 사용하는 방안으로 무선랜의 인증과정을 GSM/GPRS 네트워크의 인증방안과 통합하는 Global System for Mobile Communications / General Packet Radio Service (GSM/GPRS) SIM-기반 인증메커니즘을 제안하였다. 그러나 이 방안에서는 데이터 전송 시마다 A3,A8 알고리즘을 적용함으로써 전송데이터의 양이 많아지는 경우 통신 및 계산 오버헤드가 그에 따라 급격히 커질 뿐 아니라 replay 공격이나 man-in-the-middle 공격 등에 취약하다는 한계를 갖는다.

본 논문에서는 휴대폰을 사용하여 데이터를 전송할 때 휴대폰에서의 사용자 인증 및 일반 데이터와 긴급 데이터를 구분하는 안전한 전송 방안에 대하여 제안하였다.

2.3 USIM을 사용한 데이터 전송 방법

2.3.1 데이터 전송 메커니즘

IMT-2000(UMTS)에서는 휴대폰 사용자의 인증 및 암호화 키 생성을 위한 메커니즘을 표준으로 정의하고 있다. 휴대폰의 USIM 카드 내에는 아이디, 유일한 가입자 인증 키(Ki), 인증 알고리즘(A3, A8) 등이 저장되어 있다. 서버의 데이터베이스에는 등록이 된 사용자의 아이디와 이에 해당하는 키정보, 인증 알고리즘 (A3, A8) 이 저장되어 있다.



(그림 2) USIM 카드를 사용한 사용자 인증 및 키 생성

사용자의 휴대폰과 서버 사이의 인증 및 키 생성은 다음과 같은 순서로 진행된다.

i. 휴대폰은 USIM카드에 저장된 아이디를 서버로 전송한다.

ii. 서버에서는 데이터베이스에 저장된 정보를 바탕으로 해당 아이디에 상응하는 키를 찾는다.

iii. 서버는 휴대폰에게 임의의 난수값을 전송한다.

iv. 휴대폰과 서버는 키와 난수값을 사용하여 A3 알고리즘과 A8 알고리즘을 계산한다.

v. 휴대폰은 A3 알고리즘을 통해 생성된 값을 서버에게 전송한다.

vi. 서버는 휴대폰이 보낸 값과 계산된 값의 비교를 통해 사용자 인증을 완료한다.

vii. 이 후 데이터를 전송할 때 A8 알고리즘을 통해 도출된 값을 키로 사용하여 암호화하여 전송한다.

2.3.2 A3 및 A8 알고리즘

GSM에서 사용되는 A3과 A8 모두 K_i를 입력으로 하여 그 결과 값만을 사용하기 때문에 결과 값으로부터 원래의 키 값을 알아낼 수 없는 단방향 해쉬의 성격을 가진다. 또한 휴대폰과 서버에서 같은 키를 사용하여 암호화 및 복호화 작업을 하기 때문에 대칭키 알고리즘 방식을 사용하고 있다. 각각의 성격은 다음과 같다.

- A3: 사용자 인증을 위한 알고리즘으로 128비트의 키(K_i)와 128 비트 RAND를 입력으로 하여 32 비트의 결과(SRES)를 출력한다.
- A8: 암호화 키 생성을 위한 알고리즘으로 128비트의 키(K_i)와 128 비트 RAND를 입력으로 하여 64 비트의 결과(K_c)를 출력한다.

3. 제안 메커니즘

제안 메커니즘에서는 USIM 카드를 포함하고 있는 휴대폰을 이용하여 사용자 인증 및 안전한 데이터 전송을 한다. 이는 USIM에 적재되어있는 A3, A8 알고리즘 및 K_i를 사용하여 추가적으로 저장해야 하는 정보를 최소화함으로써 자원이 제약되어있는 휴대폰의 메모리를 효율적으로 활용하기 위함이다.

3.1 가정사항

- 센서와 휴대폰 사이의 공유키(K_{SC})가 미리 적재되어 있다.
- 휴대폰은 자신과 통신을 하는 센서의 아이디를 알고 있다.

〈표 1〉 기호 표기법

표기법	의 미
ID_{temp}	실제 ID를 대체하는 임시 ID
K_{SC}	센서 노드와 휴대폰 간의 pairwise key
$H(K_i)$	USIM 카드 안에 저장되어있는 키의 해쉬값
$a_1, a_2, \cdots$	해쉬에 입력되는 seed 값
$N_1, N_2, \cdots$	난수값
K_{tmp}	임시키(긴급모드에서 사용되는 키)
K_{normal}	일반 모드에서 사용되는 키
RES	Response 값
H	해쉬함수

- 서버는 휴대폰 내의 USIM카드 아이디와 USIM에 저장되어있는 키의 해쉬값 $H(K_i)$를 알고 있다.
- 익명성 보장을 위해 휴대폰과 의료 서버는 실제 아이디가 아닌 익명의 임시 아이디(ID_{temp})를 사용하기 위해 사전에 임시 ID와 $H(K_i)$의 정보를 갖고 있다.

3.2 사용자 인증 메커니즘

3.2.1 센서노드와 휴대폰 간의 인증

사용자의 몸에 부착된 센서는 주기적으로 생체신호를 측정하여 휴대폰으로 전송한다. 이 때, 악의적인 공격으로부터 데이터를 안전하게 보호하기 위해 휴대폰과 센서 사이의 공유키(K_{SC})로 암호화한다. 이 키는 사전에 휴대폰과 센서에 미리 적재되어 있다. 또한 휴대폰의 통신범위 내에 다른 센서가 위치하게 되어 다른 사람의 정보가 전송이 되는 것을 막기 위해 센서는 데이터 전송 시 자신의 아이디 정보를 함께 보낸다. 휴대폰은 자신과 통신하는 센서들의 아이디 정보를 저장하고 있다. 센서에서 휴대폰으로 전송이 되는 형태는 다음과 같다.

$$E_{K_{SC}}(ID_{sensor}||\text{sensing data})$$

휴대폰은 메디컬 서비스를 위한 정보를 셋팅하는 과정에서 자신과 통신하게 될 센서 노드의 ID 리스트 및 대칭키를 갖고 있으므로 휴대폰에서 복호화할 수 없는 데이터는 근접한 다른 사용자의 정보나 악의적인 데이터의 유입이라고 판단하여 이 정보를 버린다. 받은 정보를 복호화함으로써 정상적인 센서임을 확인하고 전송된 데이터를 처리한다.

휴대폰은 여러 개의 센서들로부터, 혹은 하나의 센서 노드로부터 일정 시간 동안 받은 데이터를 바탕으로 데이터 통합을 수행하고 계산된 값이 임계치를 벗어나는지의 여부에 따라 일반모드 혹은 긴급모드로 전송한다.

3.2.2 휴대폰 인증을 위한 셋업 과정

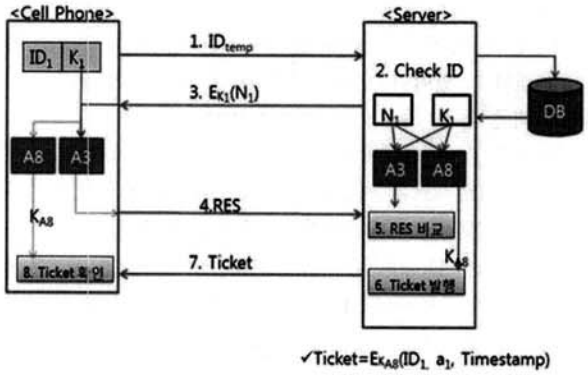
사용자의 휴대폰과 병원 내의 서버 사이의 인증은 다음과 같은 순서로 진행된다.

i. 휴대폰은 사용자의 익명성 보장을 위하여 USIM카드에 저장된 아이디가 아닌 임시 아이디를 서버로 전송한다. 의료 센서 네트워크에서는 사용자의 지극히 개인적인 데이터가 전송이 되기 때문에 특정 사용자가 개인적인 정보를 보내고 있다는 사실이 외부에 알려지는 것 자체만으로도 사생활 침해가 된다. 그렇기 때문에 휴대폰과 서버만이 미리 약속을 해둔 임시 아이디를 사용함으로써 외부에서는 어떤 사용자가 데이터를 보내는지 알 수 없게 한다.

ii. 임시아이디를 받은 서버는 자신의 데이터베이스에서 매칭되는 정보를 찾고, 그 아이디에 해당하는 키Ki의 해쉬값 $H(K_i)$를 찾는다.

iii. 서버는 임의의 난수를 생성하여 이를 미리 저장해두었던 $H(K_i)$로 암호화하여 휴대폰으로 전송한다.

iv. 휴대폰과 서버에서는 각각 다음과 같은 연산을 수행한다.



(그림 3) 휴대폰을 인증하기 위한 셋업 단계

A. 암호화된 난수를 받은 휴대폰은 USIM에 저장된 $H(K_i)$로 복호화하여 난수를 얻어낸다. $H(K_i)$와 난수를 사용하여 USIM에 내장된 해쉬 알고리즘인 A3 알고리즘과 A8 알고리즘을 수행한다.

B. 서버에서는 해당 키와 생성한 난수를 사용하여 A3 알고리즘과 A8 알고리즘 연산을 수행한다.

v. 휴대폰에서는 계산된 내용 중 A3 연산을 거쳐 생성된 결과값(RES)을 서버로 전송한다.

vi. 서버에서는 휴대폰에서 전송한 RES 값과 서버가 같은 방법으로 A3 알고리즘을 연산하여 도출된 값을 비교하여 두 값이 일치하는지 확인한다. 만약 비정상적인 사용자라면 키 값이나 난수값을 모르기 때문에 올바른 결과를 도출 할 수 없다.

vii. 서버는 비교를 통해 두 값이 일치하여 사용자 인증이 완료되면 정상적인 사용자임을 나타낼 수 있는 티켓을 발행한다. 티켓에는 휴대폰의 아이디, seed 값, 현재의 Timestamp값이 포함되어 있으며, 이를 A8 알고리즘을 통해 형성된 키로 암호화한다.

$$\text{Ticket: } K_{A8}(ID_i, a_i, \text{Timestamp})$$

위 과정을 통해 정상적으로 등록이 되어있는 휴대폰 사용자만이 인증을 통해 서비스를 받을 수 있게 된다.

3.3 데이터의 긴급 여부에 따른 전송 모드

휴대폰에서 받은 데이터의 범위를 보고 긴급히 전송해야하는 경우와 정상적인 과정을 거쳐 모아진 데이터를 전송해야하는 경우로 구분하여 긴급한 경우는 일반적인 모드에서 사전에 계산해놓은 키를 사용하여 바로 전송할 수 있도록 한다.

3.3.1 일반 모드 전송

휴대폰에서 모아진 정보의 통합 결과가 미리 정해놓은 범위 내에 존재하면 일반모드로 전송을 한다. 일반 모드에서의 전송은 다음과 같은 순서로 진행된다.

i. 일반모드에서는 휴대폰이 셋업 단계에서 저장해 놓은 티켓을 서버로 전송한다.

ii. 서버에서는 티켓을 확인하여, 아이디 등록 여부를 확

(그림 4) 일반모드에서 휴대폰으로부터 서버로 데이터를 전송하는 과정

인하고 Timestamp가 유효한지 확인한다. 만약 Timestamp가 만료되었다면 휴대폰은 셋업 단계를 다시 반복하여 새로운 Timestamp를 발급받아야 한다.

iii. 서버는 티켓 내의 seed값에 해쉬 연산을 하여 임시키(K_{tmp})를 계산하고, 새로운 난수(N_2)를 생성하여 임시키로 암호화하여 전송한다.

iv. 휴대폰에서는 같은 방법으로 계산한 임시키(K_{tmp})로 N_2를 복호화한다.

v. Seed 값과 N_2를 사용하여 해쉬 연산을 한 결과를 일반모드에서 데이터를 전송할 때 암호화하는 키(K_{normal})로 사용한다.

vi. K_{normal}을 업데이트 하기 위해 iii~v는 일정한 주기마다 반복된다.

vii. 휴대폰에 모아진 데이터를 K_{normal}로 암호화하고, 메시지의 무결성 확인을 위한 Message Authentication Code (MAC)를 붙여서 서버로 전송한다. 또한 replay attack을 막기 위해 sequence number를 암호화하여 함께 전송한다.

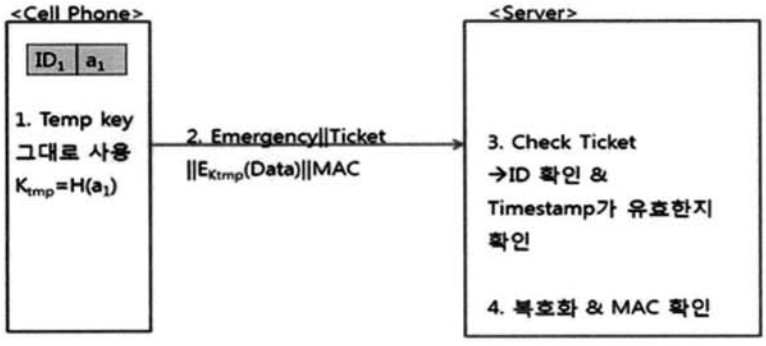
viii. 서버에서는 seed 값과 N_2를 사용하여 해쉬 연산을 하여 생성된 K_{normal}을 만들고 다음과 같은 작업을 한다.

A. sequence number를 복호화하여 확인한다. 만약 이전에 받았던 sequence number를 다시 받았다면 이는 공격자가 이 메시지를 가로채 다시 같은 메시지를 보낸 것으로 간주하여 이후 해당 아이디로부터 오는 데이터를 무시한다.

B. 올바른 sequence number 라는 것이 확인이 되면, 티켓 내의 Timestamp의 유효성을 확인한다.

C. $_{normal}$로 수신 데이터를 복호화하고 MAC을 비교하여 전송되는 중간에 변조가 되지 않았는지 확인을 한다.

위와 같은 과정을 통해 일반 모드에서는 데이터를 안전하게 전송할 수 있다.



(그림 5) 긴급모드에서 데이터를 휴대폰에서 서버로 전송하는 과정

3.3.2 긴급 모드 전송

휴대폰에서 모아진 정보값이 한계치를 벗어나면 사용자의 건강이 위험하다고 판단하여 긴급 모드로 전송한다. 긴급 모드에서는 빠르게 보내는 것이 중요하다. 그렇기 때문에 키를 만들기 위해 추가적인 데이터를 교환하고 계산하는 데에 많은 시간을 허비할 수 없다. 긴급모드에서의 데이터 전송은 아래와 같다.

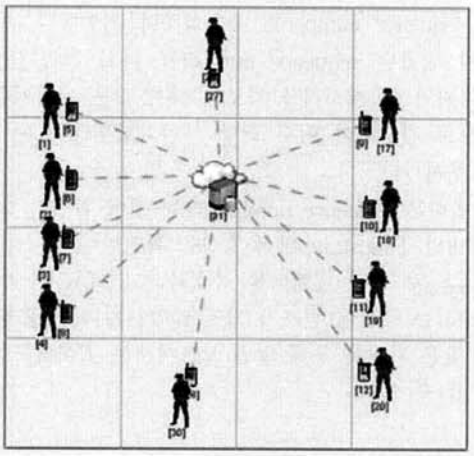
i. 휴대폰에서는 측정된 데이터를 일반모드에서 미리 계산해놓은 임시키(K_{tmp})로 암호화하고 티켓과 MAC을 함께 전송한다.

ii. 서버에서는 티켓을 바탕으로 아이디와 Timestamp의 유효성을 판단하며, 수신 데이터와 MAC을 통해 데이터의 무결성 및 기밀성을 보장할 수 있다.

4. 시뮬레이션 및 결과 분석

4.1 시뮬레이션 환경

QualNet은 가상의 네트워크 기반에서 다양한 프로토콜 설계 분석 검증과 네트워크 어플리케이션 등을 실제로 구출하기 전에 가상의 공간에 구축하여 문제점을 분석하고 예측할 수 있는 소프트웨어이다. 센서네트워크를 비롯하여, WLAN, Mobile Ad hoc Network, 무선랜, 셀룰러 네트워크, 위성 네트워크에 대한 기본적인 라이브러리를 가지고 있으며 사용자가 이 프로토콜을 수정하여 확장 사용할 수 있다.

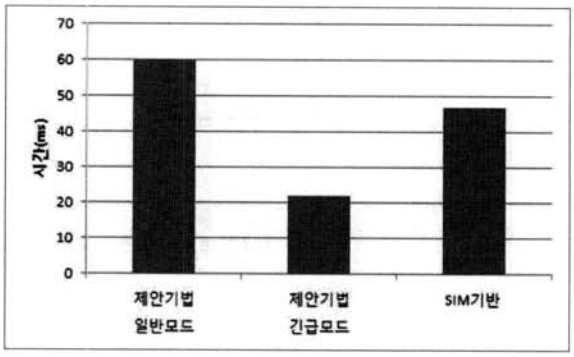


(그림 6) 시뮬레이션 환경

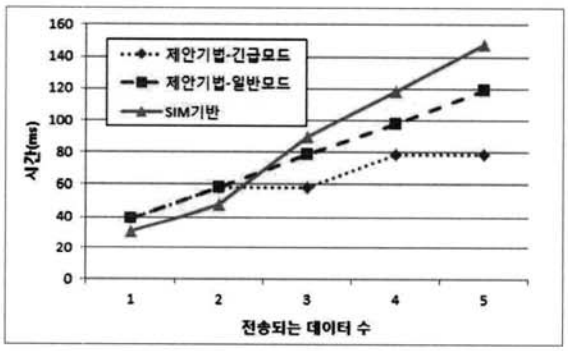
시뮬레이션은 QualNet 4.5 버전을 사용하여 진행하였다. (그림 6)과 같이 무선 네트워크 환경에서 각 사용자마다 5개씩의 센서가 부착이 되어있으며, 총 10명의 사용자가 서버로 데이터를 전송하는 환경을 구성하였다. QualNet을 기반으로 [7]과 비교하여 소비시간 및 통신오버헤드를 측정하였으며 [8]을 바탕으로 계산오버헤드를 계산하였다.

4.2 시뮬레이션 결과 및 분석

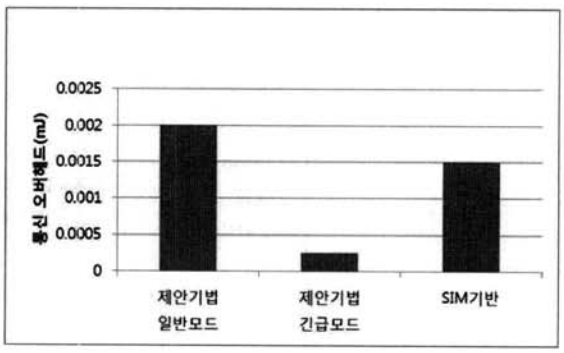
(그림 7)에서 볼 수 있듯이 제안 메커니즘에서 초기화를 거쳐 최초로 데이터를 전송할 때 소요되는 시간은 [7]의 SIM을 사용하여 데이터를 전송하였을 때보다 일반모드에서는 약 15ms 더 소요되고, 긴급모드에서는 20ms정도 빠르게 전송이 되는 것을 볼 수 있다. 이처럼 초기화 과정을 통해 최초로 데이터를 전송할 때는 SIM기반 방식에 비해 일반모드의 경우 좀 더 시간이 걸리지만 전송하는 데이터의 수가 많아질수록 (그림 8)처럼 제안 메커니즘이 더 빠르게 전송되는 것을 확인 할 수 있다. 일반 모드에서도 약 3개 이상만 되어도 SIM기반 방식에 비해 시간이 적게 소모되며 긴급 모드에서는 그 차이가 더 커진다. 특히 긴급 모드에서는 데이터가 매우 빠르게 전송이 되기 때문에 환자의 위급한 상태에 신속히 대응할 수 있다는 장점을 갖는다.



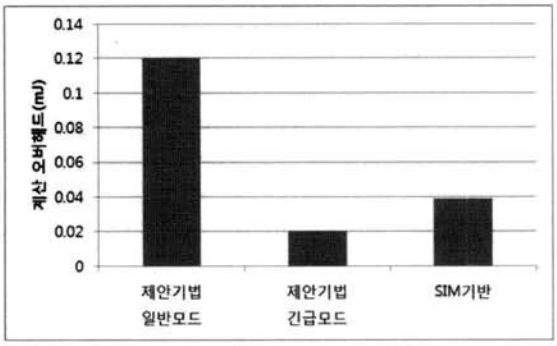
(그림 7) 초기화에 필요한 소요시간



(그림 8) 데이터 전송 횟수에 따라 소요되는 시간 비교

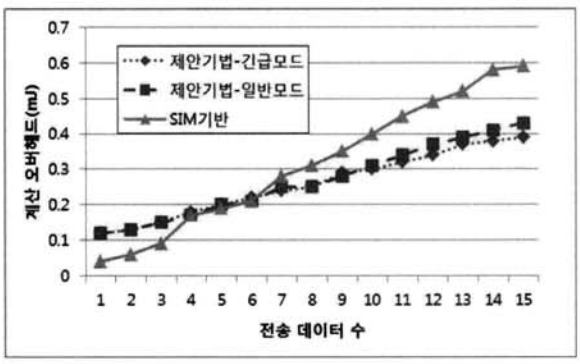


(그림 9) 초기화 및 최초 데이터 전송 시 소요되는 통신 오버헤드

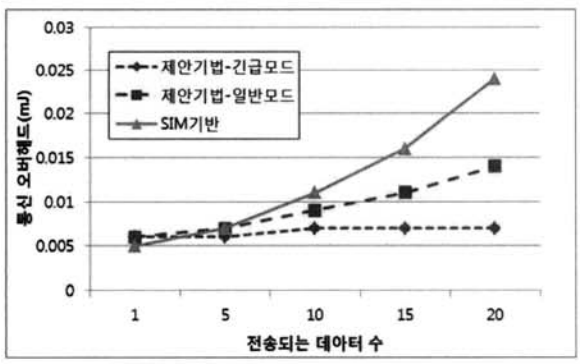


(그림 10) 초기화 및 최초 데이터 전송 시 소요되는 계산 오버헤드

(그림 9)와 (그림 10)에서는 초기화를 거쳐 최초로 데이터를 전송했을 때의 통신 오버헤드와 계산 오버헤드를 나타낸다. 제안 메커니즘에서는 셋업 과정을 통해 티켓을 할당받는 작업이 추가됨으로 인해 초기화를 거쳐 최초로 데이터를 전송할 때까지는SIM을 사용하였을 때보다 통신이나 계산에 있어서 많은 오버헤드를 나타내는 것을 볼 수 있다. 특히 일반 모드의 경우 긴급모드에서 별도의 계산 없이 사용하기 위한 키를 사전에 계산하기 위해 SIM에 비해 더 많은 오버헤드가 필요하지만 초기화 과정에서만 필요한 내용이므로 시스템이 안정화 단계에 들어서면서 오히려 오버헤드가 줄어드는 것을 확인할 수 있다.

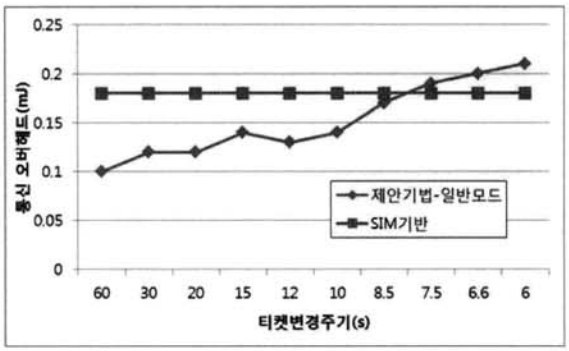


(그림 11) 데이터 전송 횟수에 따른 계산 오버헤드



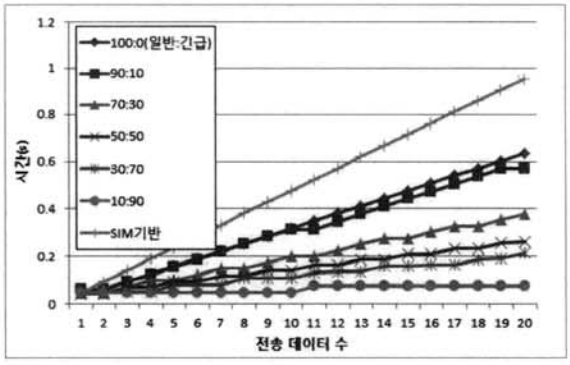
(그림 12) 데이터 전송 횟수에 따른 통신 오버헤드

(그림 11)과 (그림 12)에서 볼 수 있듯이 전송되는 데이터의 수가 많을수록 제안 메커니즘의 오버헤드가 적게 나타나는 것을 알 수 있다. 그 이유는 SIM을 사용하여 데이터를 전송할 때에는 매 전송 시마다 A3, A8 알고리즘을 반복해서 사용을 하기 때문에 그만큼 반복적인 계산을 해야 한다. 하지만 제안 메커니즘은 이 알고리즘을 셋업 과정으로 두어 주기적으로 반복하기 때문에 그 만큼의 오버헤드를 줄일 수 있다. 또한, 긴급 모드에서는 별도로 키를 만드는 작업을 하는 것이 아니라 일반 모드에서 만들어져 있던 키를 그대로 사용하기 때문에 오버헤드를 좀 더 줄일 수 있다. 특히, 통신 오버헤드의 경우 긴급 모드에서는 서버와의 사이에 주고받는 데이터를 최소화함으로써 전송되는 데이터 양이 증가하는 경우에도 큰 차이는 보이지 않음을 확인할 수 있다.



(그림 13) 티켓 변경 주기에 따른 통신 오버헤드

(그림 13)은 티켓 변경 주기에 따른 통신 오버헤드를 나타낸다. 티켓의 변경 주기가 짧아질수록 자주 티켓을 변경해야 하기 때문에 제안 메커니즘이 점점 오버헤드가 커지는 것을 확인 할 수 있다. SIM을 이용한 데이터 전송 시에는 티켓을 두지 않기 때문에 일정한 오버헤드를 나타낸다. 티켓의 변경주기가 7.5초보다 짧아지기 전까지는 제안 메커니즘의 오버헤드가 적기 때문에 티켓을 자주 바꾸더라도 효율적인 에너지 소비를 나타내는 것을 알 수 있다. 실제 상황에서는 티켓 변경주기가 1분 이하로 설정되는 경우가 거의 없을 것으로 보이므로 제안 기법이 SIM 방식에 비해 훨씬 효율적으로 운용될 수 있음을 알 수 있다.



(그림 14) 긴급모드 비율에 따른 시간 변화

일반적으로 전송하는 데이터의 수가 많아질수록 많은 시간을 소비하게 된다. 제안 메커니즘도 마찬가지인데 이 때 전송하는 데이터의 긴급모드 비율이 많아지면 더 빠르게 전송하는 것을 (그림 14)를 통해 확인할 수 있다. 그 이유는 긴급모드에서는 이미 만들어진 키를 사용하여 바로 전송을 하기 때문에 일반모드의 비율이 많을 때에 실시되는 키 생성 과정이 생략이 되기 때문이다. 긴급 모드가 많이 발생할수록 환자의 위급 상황을 빠르게 전송할 수 있고, 발생 비율에 무관하게 전체적으로SIM을 이용한 데이터 전송 방법으로 전송했을 때보다 빠르게 전송하는 것을 보여준다.

〈표 2〉 일반모드와 긴급모드의 비교

비교		일반모드	긴급모드
키 생성		2개 (K_{tmp}, K_{normal})	없음
암호화 횟수	휴대폰	1번	1번
	서버	1번	없음
복호화 횟수	휴대폰	1번	없음
	서버	2번	2번
메시지 전송 횟수	휴대폰	2번	1번
	서버	1번	없음
목적		안전하게 데이터 전송	빠르게 데이터 전송

일반 모드와 긴급모드의 비교는 <표 2>와 같다. 일반모드에서는 2개의 키를 생성하는 반면 긴급모드에서는 일반모드에서 만들어놓았던 키를 그대로 사용하기 때문에 키를 생성하는 연산이 필요하지 않다. 또한 암호화 횟수, 복호화 횟수, 메시지 전송 횟수를 비교하면 일반모드에서 더 많은 연산을 하는 것을 알 수 있다. 긴급모드에서는 불필요한 연산을 줄이고 미리 계산해놓은 값들을 주로 사용함으로써 신속하게 데이터를 전송할 수 있고, 일반모드에서는 데이터를 안전하게 전송하는데 초점을 맞춤으로써 긴급모드에서는 일반모드의 도움을 받아 안전하면서도 빠르게 전송할 수 있다는 장점이 있다.

4.3 보안분석

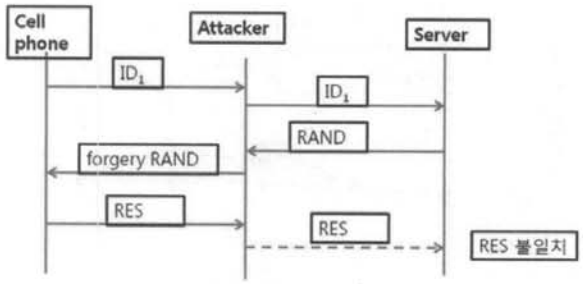
SIM카드를 사용한 데이터 전송 방법과 제안 메커니즘의 일반모드의 전송방법을 비교하면 <표 3>과 같다. SIM을 사용한 방법에는 2개의 키를 사용하는 반면 제안 메커니즘은 총 4개의 키를 사용한다. 두 방법 모두 A3 알고리즘을 통한 사용자 인증을 하지만 제안 메커니즘에서는 MAC 사용을 추가함으로써 메시지 인증까지 함께 하고 있다. 또한, 두 메커니즘 모두 암호화를 통한 데이터의 기밀성을 보장하지만, 제안 메커니즘에서는 임시 아이디를 사용하고 실제 아이디는 티켓 안에 넣어 암호화하여 전송함으로써 아이디의 익명성을 보장하여 사용자의 프라이버시를 보호할 수 있다.

〈표 3〉 보안성 비교

비교	SIM	제안기법-일반모드
키 사용	2개 (K_i, K_{A8})	4개 ($H(K_i)$, K_{A8}, K_{tmp}, K_{normal})
메시지 인증	X	O (MAC 사용)
사용자 인증	O	O
ID 익명성보장	X	O (ID_{temp}, Ticket사용)
기밀성	O	O
Reply attack 가능성	공격가능	공격불가능 (Sequence number 사용)
Man-in-the-middle attack	공격가능	공격불가능
전송 메시지 형태	Nonce값이 plaintext로 전송됨	모든 정보가 암호화되어 전송됨

또한 통신 중에는 악의적인 목적을 가진 공격자가 존재하고, 암호화된 데이터를 중간에 가로채 복사한 후 나중에 그 메시지를 재전송하는 reply attack이 발생할 수도 있는데 SIM을 이용한 방법에서는 이 공격을 막을 수 있는 방법이 없기 때문에 같은 메시지가 반복해서 서버로 전송이 되면 이 메시지를 복호화하기 위해 끊임없이 연산을 하여야 할 것이다. 반면, 제안 메커니즘은 sequence number를 사용하고 있기 때문에 만약 공격자가 보낸 메시지의 sequence number가 이전에 받았던 동일번호라면 공격이라고 판단하여 이후 같은 아이디로부터 오는 메시지는 모두 무시함으로써 공격을 막을 수 있다.

한편, SIM을 사용한 데이터 전송 방법에서는 (그림 15)같은 Man-In-the-Middle [16] 공격이 가능하다. 휴대폰이 전송하는 데이터를 공격자가 가로채서 정상적인 사용자인 것처럼 서버에게 전송하고, 서버가 전송하는 난수값을 받아 변조한 난수값을 휴대폰으로 전송하면 휴대폰에서는 잘못된 난수값을 바탕으로 RES를 계산하게 되고 공격자는 이 값을 서버로 전송하여 정상적인 사용자가 서비스를 받지 못하도록 할 수 있다. 하지만, 제안 메커니즘에서는 어떠한 정보도 plaintext로 전송이 되는 것이 없기 때문에 이러한 공격을 막을 수 있다.



(그림 15) SIM을 사용한 데이터 전송에서의 Man-in-the-Middle공격

5. 결 론

본 논문에서는 의료센서네트워크에서 휴대폰을 이용한 데이터 전송 시 사용자 인증 방법과 안전한 데이터 전송 방안 및 데이터의 종류에 따른 안전한 전송 방법에 대하여 제안하였다. 사용자 인증을 통해 합법적인 사용자만 서비스를 받을 수 있도록 하였고 특히 긴급상황에 신속하게 대처하기 위해 모드를 두 가지로 분류하여 좀 더 빠르게 데이터를 전송하도록 하였다. 시뮬레이션과 분석을 통해 제안한 메커니즘은 안전하면서도 효율적으로 데이터 전송이 가능함을 증명하였다.

참 고 문 헌

[1] Bui, F. M. and Hatzinakos, D., "Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling," EURASIP, Adv. 2008.

[2] Venkatasubramanian, K., Banerjee, A., and Gupta, S. K. S., "EKG-based Key Agreement in Body Sensor Networks," The Second Workshop on Mission Critical Networks, IEEE, 1 - 6, 2008.

[3] Malasri, K. and Wang, L., "Addressing security in medical sensor networks," HealthNet '07: Proc. of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments, pp.7-12, 2007.

[4] Tan, C. C., Wang, Zhong, H. S., and Li, Q., "Body sensor network security: an identity-based cryptography approach," ACM Conference on Wireless Network Security (WiSec). ACM Press. pp.148-153, 2008.

[5] Haque, M. M., Pathan, A. S. K., and Hong, C. S., "Securing U-Healthcare Sensor Networks using Public Key Based Scheme," IEEE ICACT 20, 2008.

[6] Huang, Y. M., Hsieh, M.Y., Chao, H.C., Hung, S. H., and Park, J.H., "Pervasive, Secure Access to a Hierarchical Sensor-based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks," IEEE Journal on Selected Areas in Communications, Vol.27, No.4, May, 2009.

[7] Tsai, Y., Chang, C., "SIM-based subscriber authentication mechanism for wireless local area networks," Computer Communications, pp.1744-1753, 2006.

[8] Potlapally, N., Ravi, S., Raghunathan, A., and Jha, N. K., "Analyzing the energy consumption of security protocols," The International Symposium on Low Power Electronics & Design, pp.30-35, 2003.

[9] Morchon, O. G., Baldus, H. and Sanchez, D. S., "Resource-Efficient Security for Medical Body Sensor Networks," Proc. of BSN'06, pp.80-83, 2006.

[10] Bao, S.-D. and Zhang,Y.-T., "A design proposal of security architecture for medical body sensor networks," International Workshop on Wearable and Implantable Body Sensor Networks IEEE., 2006.

[11] Challa, N., Cam, Hasan., and Sikri, M., "Secure and Efficient Data Transmission over Body Sensor and Wireless Networks," EURASIP Journal on Wireless Communications and Networking, 2008.

[12] Malasri, K.; Wang, L., "Design and Implementation of a Secure Wireless Mote-Based Medical Sensor Network," 10th international conference on Ubiquitous computing, Vol.344, pp.172-181, 2008.

[13] Bao, S.-D., Zhang, Y.-T., and Zhang, Y.-T., "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems," Proc. of the IEEE 27th conference on Engineering in Medicine and Biology, 2005.

[14] Venkatasubramanian, K., Banerjee, A., and Gupta, S. K. S., "Plethysmogram-based Secure Inter-Sensor Communication in Body Area Networks," Proc. of the Military Communications Conference, IEEE, pp.1-7, 2008.

[15] Keoh, S. L., Lupu, E., and Sloman, M., "Securing body sensor networks: Sensor association and key management," IEEE International Conference on Pervasive Computing and Communications (PerCom), pp.87-92. IEEE, 2009.

[16] D. N. Serpanos, R. J. Lipton, "Defense Against Man-in-the-Middle Attack in Client-Server Systems," Sixth IEEE Symposium on Computers and Communications (ISCC'01), 2001.

김 지 현

e-mail : tobajh@naver.com
2003년 서울여대 정보보호학(학사)
2010년 이화여자대학교 컴퓨터공학과(석사)
2010년~현 재 LS CNS 재직
관심분야 : 센서 네트워크, 네트워크 보안, 의료센서 네트워크

도 인 실

e-mail : isdoh@ewhain.net
1993년, 1995년 이화여자대학교 전자계산학과(학사, 석사)
1995년~1998년 삼성SDS
2002년~2007년 이화여자대학교 컴퓨터공학과(박사)
2007년~2008년 서울대학교 박사후연구원
2008년~2011년 이화여자대학교 컴퓨터공학과 연구교수
2011년~현 재 성균관대학교 정보통신공학부 연구교수
관심분야 : 유무선 네트워크 보안, 유무선네트워크

박 정 민

e-mail : pjm@kist.re.kr

1989년 이화여자대학교 전자계산학과(학사)

1991년 이화여자대학교 전자계산학과 (이학석사)

2008년 이화여자대학교 컴퓨터정보통신공학과(공학박사)

1991년~현 재 한국과학기술연구원 실감교류로보틱스연구센터 선임연구원

관심분야 : 이동 네트워크 보안, 로봇 지능 소프트웨어 구조, HRI 등

채 기 준

e-mail : kjchae@ewha.ac.kr

1982년 연세대학교 수학과(학사)

1984년 미국 Syracuse University 컴퓨터학과(석사)

1990년 미국 North Carolina State University 컴퓨터공학과(박사)

1990년~1992년 미국 해군사관학교 컴퓨터학과 조교수

1992년~현 재 이화여자대학교 컴퓨터공학과 교수

관심분야 : 네트워크 보안, 센서 네트워크, 네트워크 프로토콜 설계 및 성능분석