DOI : 10.5392/JKCA.2011.11.2.142

유헬스에서 안전한 생체정보전송을 위한 동적인 유효세션기반의 상호인증 프로토콜

Mutual Authentication Protocol based on the Effective Divided Session for the Secure Transmission of Medical Information in u-Health

이병문*, 임헌철**, 강운구***
가천의과학대학교 정보공학부*, 가천의과학대학교 IT학과**, 유-헬스케어연구소***

Byung-Mun Lee(bmlee@gachon.ac.kr)*, Heon-Cheol Lim(ydgvnk70@naver.com)**,
Un-Ku Kang(ugkang@gachon.ac.kr)***

요약

무선센서 네트워크를 기반으로 한 유헬스 서비스는 개인의 의료건강정보를 보다 안전하게 전송하고 처리하여야 한다. 대부분의 유헬스 센서기기는 게이트웨이를 통해 전송하는 구조이므로 기기와 게이트웨이 간의 신뢰성 문제는 매우 중요하다. 사용자가 센서기기를 휴대하면서 이동하게 되면 게이트웨이의 수신범위 밖으로 멀어지므로 데이터 전송이 불가하다. 이 틈을 이용한 비인가 센서기기의 데이터 무결성 침해가 발생할 수 있다. 뿐만 아니라 비인증 게이트웨이가 허가받지 않고 생체정보를 갈취할 가능성도 있다. 이경우도 데이터 기밀성 침해문제가 발생된다. 따라서 유헬스 센서기기와 게이트웨이 간에는 응용레벨에서의 상호인증이 반드시 필요하다. 기기와 게이트웨이간의 어플리케이션 전송세션을 세분화하고 각 세션을 주기적으로 갱신하면 침해를 차단하는 효과가 있다. 그러나 이 과정에서의 인증을 위한 전송오버헤드를 최소화하려면 생체정보의 측정주기에 따른 동적인 유효 세션기법이 필요하다. 본 연구에서는 이 기법을 제안하였고 3가지 실험을 통해 상호인증 성공결과를 확인하였다.

■ 중심어 : | 유헬스 | 유효세션 | 상호인증 프로토콜 | 보안위협 | 센서네트워크 | 보안 |

Abstract

All medical information over sensor networks need to transmit and process securely in the u-Health services. The reliability of transmission between u-Health medical sensor devices and gateway is very important issue. When the user moves to other place with u-Health devices, its signal strength is going down and is far from the coverage of gateway. In this case, Malicious user can be carried out an intrusion under the situation. And also rogue gateway can be tried to steal medical information. Therefore, it needs mutual authentication between sensor devices and gateway. In this paper, we design a mutual authentication protocol which divided sessions from an authenticated session are updated periodically. And in order to reduce the traffic overhead for session authentication, we also introduce dynamic session management according to sampling rate of medical sensor type. In order to verify this, we implemented the programs for the test-bed, and got an overall success from three types of experiment.

■ keyword : | Authentication | Protocol | u-Health | Security | Medical Infomation | Sensor Network |

* 본 연구는 지식경제부 산업원천기술개발사업의 지원을 받아 수행되었습니다.
접수번호 : #110117-004
접수일자 : 2011년 01월 17일
심사완료일 : 2011년 01월 24일
교신저자 : 강운구, e-mail : ugkang@gachon.ac.kr

I. 서 론

유헬스는 인구 고령화에 따른 만성질환 관리의 한계를 극복하는 하나의 대안이다. 유헬스 서비스를 제공하려면 유헬스 기기와 유헬스 서버가 필요하다. 유헬스 기기는 가정을 포함한 일상생활에서 사용될 수 있으며, 유헬스 서버는 병원과 같은 의료기관에서 건강관리가 필요한 모든 사람의 정보를 저장하고 관리할 수 있다. 최근에 들어 ISO/IEEE와 같은 국제표준기구에서도 유헬스 기기에 대한 표준화 규격을 제정중이며 이를 기반으로 한 연구가 진행 중이다[1].

유헬스 기기는 가정에서 사용할 수 있는 의료기기에 무선 전송모듈을 탑재한 서비스를 제공한다. 최근에 만성질환이 많아지면서 자가 건강관리에 관심을 늘게 되고 유헬스 기기의 요구가 증가되고 있다. 그러나 유헬스 기기를 사용하게 된다면 개인의 생체정보가 무선으로 전송되는 과정에서 노출될 수 있기 때문에 데이터 유출문제가 발생한다. 센서네트워크 차체에 대한 데이터 보호연구는 여러 가지 연구가 진행되고 있으나 어플리케이션 레벨에서의 데이터특성에 맞는 보안에 대한 연구는 미미하다[2]. 특히 유헬스 기기는 휴대하기가 간편하여야 하고 기기의 특성에 따라 데이터의 생성주기가 많은 차이를 보인다. 예를 들면 혈압 데이터는 대개 하루 2~3번 측정할 때 마다 발생되며 심전도 데이터는 10ms~20ms 마다 발생한다. 또한 유헬스 기기가 갖는 배터리 전원문제, 낮은 처리능력과 적은 대역폭, 전송속도의 한계등 제한적 특성이 많은 처리를 어렵게 만든다. 특히 사용자에게는 휴대의 용이성이 매우 중요하다. 언제 어디서나 건강을 관리하기 위해 생체정보 측정이 필요하고 휴대과정에서 쉽게 이동할 수 있어야 하며 이 과정에서도 안전한 생체정보 전송이 필요하다[3][4].

이와 같은 맥락에서 볼 때 유헬스 기기에서 측정된 생체정보가 안전하게 가정용 게이트웨이로 전송될 수 있어야 한다. 센서네트워크는 유선네트워크에 비해 구조적으로 매우 취약하다[1]. 악의적인 사용자가 가정용 게이트웨이의 수신범위 안에 들어온다면 인가되지 않은 접근이 가능할 뿐만 아니라 생체정보의 갈취가 가능하다[4]. 따라서 유헬스 기기와 게이트웨이간의 신뢰성 문제가 중요하다. 즉 기기간의 상호인증이 필요할 뿐만 아니라 어플리케이션간의 상호인증도 필요하다는 것이다. 특히 사용자가 유헬스 기기를 사용할 때 휴대가 간편하여야 하고 이동이 쉬워야 한다. 이와 같은 조건을 만족하려면 인증방법에 동적인 개념이 포함되어야 한다. 동적인 인증은 한번 연결된 인증세션을 사용하되 상황에 맞게 세션을 적용함으로써 악의적인 사용자가 비인증 게이트웨이를 통해 생체정보를 변조하거나 유출할 수 있는 문제를 해결할 수 있다.

따라서 본 연구에서는 이와 같은 동적인 인증방식을 모델링하고 이를 구현하기 위한 유효세션기반의 상호인증 프로토콜을 제안하고자 한다. 또한 유효세션기반의 인증모델의 유효성을 확인하기 위해 센서노드에 동적 인증모듈을 구현하여 실험을 통해 유효성을 보이고자 한다.

본 논문의 구성은 2장에서는 유헬스에서의 데이터 노출위협에 대한 사항을 기술하고, 3장에서는 본 논문에서 제안하는 유효세션 기반의 상호인증 프로토콜에 대한 모델을 제시한다. 4장에서는 이를 토대로 구현하고 5장에서는 구현한 결과를 이용하여 실험과 평가를 하며 마지막 6장에서는 결론으로 끝을 맺는다.

II. 유헬스에서의 생체정보 보안위협

1. 유헬스 시스템의 구성

유헬스 시스템은 유헬스 기기와 가정용 무선 게이트웨이 그리고 유헬스 서버로 구성된다[5].

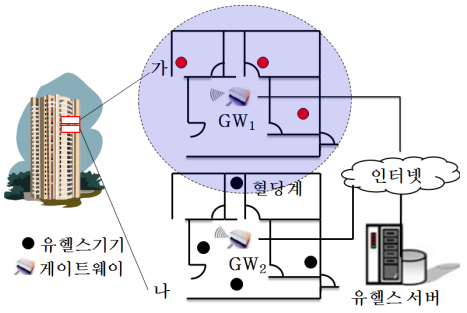


그림 1. 유헬스 시스템 구성

[그림 1]은 아파트와 같은 가정이나 사무실에서 유헬스 서비스를 이용할 경우 구성할 수 있는 유헬스 시스템을 보여준다. 한 빌딩에 이웃한 2개의 가정(가, 나)이 있다고 하자. 가의 경우 사용자가 유헬스 기기(무선혈압계, 무선체지방계, 무선혈당계)에서 측정한 생체정보를 게이트웨이(GW_1)를 통해서 유헬스 서버에 저장한다. 이 때 사용자는 가정에서 유헬스 기기를 사용하면서 쉽게 이동할 수 있다. 다음으로 유헬스 기기의 이동성에 대해 살펴보자.

2. 유헬스 기기의 이동성

게이트웨이가 측정된 생체정보를 정확히 수신하려면 게이트웨이의 수신범위에 유헬스 기기가 있어야 한다. 그러나 사용자는 안과 밖으로 유헬스 기기를 쉽게 가지고 다닐 수 있기 때문에 게이트웨이의 수신범위에서 벗어날 수 있다. [그림 2]의 예를 들면 기기가 S_1 지점에서 게이트웨이(GW_1)로 생체정보를 전송하다가 S_2 지점으로 이동하면 GW_1의 수신범위 밖이 되기 때문에 GW_1는 생체정보를 수신하지 못하게 된다.

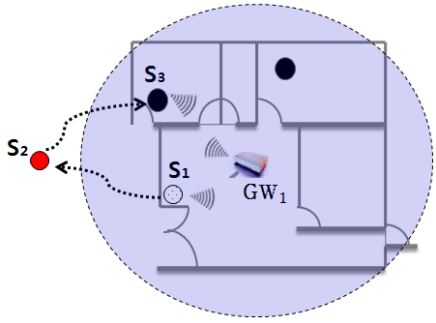


그림 2. 생체정보 센서기기의 자유로운 이동성

얼마 후 기기는 S_2 지점에서 S_3 지점으로 이동하게 되면 GW_1가 다시 생체정보를 수신할 수 있다. 이 과정에서 유헬스 기기와 게이트웨이간의 어플리케이션 레벨은 세션을 유지하게 되기 때문에 생체정보를 그대로 받을 수 있다. 이와 같이 사용자는 유헬스 기기를 자유롭게 이동하며 사용할 수 있으나 센서기기가 게이트웨이의 수신범위 밖과 안으로 이동하는 과정에서 악의적인 사용자에 의해 생체정보가 유출될 수 있고 위조될 수 있는 취약점이 생긴다. 다음절에서 위와 같은 운영 시나리오별 취약상황에 대해서 살펴보자.

3. 이동성에 따른 취약성

생체정보를 측정하는 센서 네트워크 환경은 Bluetooth 나 Zigbee 를 고려할 수 있는데 전력소모량이 더 적은 Zigbee가 효율적이라는 연구가 주로 진행되고 있다. Zigbee 와 같은 센서 네트워크는 무선특성 때문에 전송데이터의 무결성과 기밀성 보호에 취약하다[6][7]. [그림 3]에서 살펴보자. 처음에 S_1은 GW_1에게 생체정보를 전송하고 있었다. 이때 S_1는 GW_1의 수신범위에서 벗어나지 않고 S_2 지점으로 이동한다. 동시에 비인가된 Fake GW_2 도 S_2의 수신범위로 접근해 온다면 S_2에서 전송하는 생체정보가 Fake GW_2 로 유출될 수 있는 기밀성 침해문제가 생긴다.

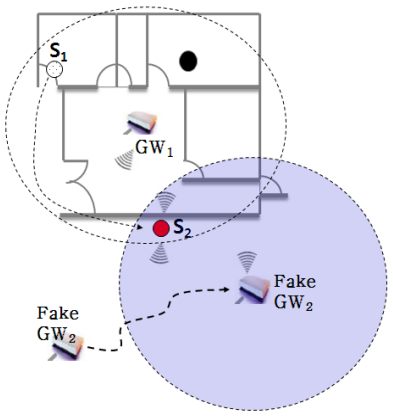


그림 3. GW 수신범위내에서의 이동(기밀성침해)

이번에는 무결성을 침해받을 수 있는 다른 경우를 살펴보자. 예를 들면, S_1은 GW_1의 수신범위 밖으로 벗어나는 경우를 생각해볼 수 있다. [그림 4]가 그런 경우이다. [그림 4]를 살펴보면 GW_1와 생체정보를 주고받던 S_1 은게이트웨이 수신범위 밖으로 이동한다고 가정하자. 이때 악의적인 공격자($S_{attacker}$)가 S_1 으로 위장(S'_1)하여 위조된 생체정보를 전송할 수 있다. 만약에 S_1이 수신범위 밖에 있다가 안으로 들어오더라도 게이트웨이는 정확히 알 수 없으며 수신범위 밖에 있던 동안에

공격을 받을 수 있는 가능성이 얼마든지 발생할 수 있다. 이와 같이 게이트웨이와 유헬스 기기간의 상호인증은 매우 중요하다.

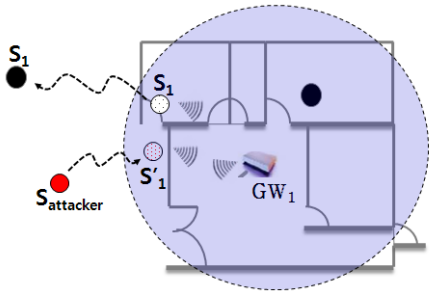


그림 4. GW 수신범위 밖으로의 이동(무결성침해)

따라서 위와 같은 문제들을 해결하려면 유헬스 기기와 게이트웨이 간에 생체정보를 전송하는 과정에서 세션의 유효시간을 동적으로 할당하는 유효세션 기반의 상호인증 모델이 필요하며, 이를 제안하고자 한다.

Ⅲ. 유효세션기반의 상호인증 프로토콜

1. 유효세션기반 상호인증모델의 제안

상호인증 모델은 유헬스 기기와 게이트웨이간의 어플리케이션 생체정보 전송세션을 세분화하고 각 세션을 주기적으로 갱신함으로써 비인가 기기에게 유출되는 데이터를 차단하는 효과를 제공한다. 다시 말하면 전송세션을 여러 개의 유효세션으로 나누고 각 유효세션간에 상호인증과정을 둔다면 비인가 기기가 중간에 끼어들더라도 데이터 유출을 막을 수 있다. 그러나 유효세션마다 상호인증과정을 수행하면 불필요한 네트워크 트래픽과 처리과정에서의 오버헤드가 발생된다. 이러한 문제를 최소화하기 위해 세션의 갱신주기를 모두 동일하게 적용하지 않고 데이터 측정빈도가 많은 유헬스 기기[8]에는 세션시간을 많게 할당하게 하고 측정빈도가 적은 유헬스 기기에는 세션시간을 적게 할당하는 동적인 유효세션 기법이 필요하다. [그림 5]는 이 모델의 개념을 보여준다. 생체정보 발생주기가 낮은 센서A타입은 게이트웨이와의 전송세션 시간은 길지만 데이터 전송주기가 길어 유헬스 기기가 이동하였을 때 이를 인식하는데 상대적으로 오랜시간이 걸린다. 이에 비하여 센서B타입은 게이트웨이와의 전송세션 시간이 길지만 데이터 전송주기가 짧아 이동하였을 때 이를 센서A에 비하여 빠르게 인식할 수 있다. 따라서 센서B에게는 유효세션 시간을 길게 할당하고 센서A에게는 유효 세션시간을 짧게 할당하여 세션 갱신과정에서 발생하는 오버헤드를 줄일 수 있다.

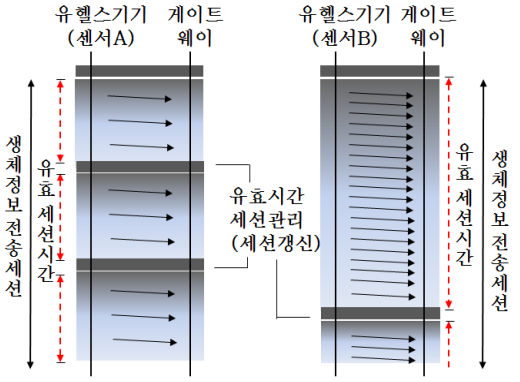


그림 5. 유효세션기반의 인증전송모델

표 1. 생체정보별 측정주기와 유효세션시간

생체정보	측정주기,측정량	유효세션시간(sec)
심 전 도	20ms, 다량	600
근 전 도	20ms, 다량	600
위 전 도	20ms, 다량	600
심 박 수	20ms, 다량	600
호 흡 수	20ms, 다량	600
산소포화도	1sec, 소량	300
활 동 량	1sec, 소량	300
혈 압	2회/1일, 소량	60
체 온	2회/1일, 소량	60
체 중	2회/1일, 소량	60
체 지 방	2회/1일, 소량	60
혈 당	2회/1일, 소량	60

이와 같은 기준으로 각 생체정보의 특성에 따라 유효세션시간을 [표 1]과 같이 정의한다. 심전도와 같이 측정주기가 짧아 단위시간당 측정량과 트래픽이 많은 경우에는 세션의 유효시간을 길게 정의하도록 한다. 그 이유는 사용자가 심전도계를 이동시킴으로써 게이트웨이의 수신범위를 이탈하게 되면 게이트웨이가 심전도 데이터를 더 이상 수신하지 못해 전송이 중단된 형태로

지속되기 때문에 이동사실을 쉽게 탐지할 수 있다. 따라서 유효 세션시간을 상대적으로 긴 600초로 설정한다. 그에 비해서 혈압의 경우에는 1일에 1회~2회정도 측정하게 되어 단위시간당 전송량이나 트랙픽이 매우 적다. 따라서 전송세션 동안 데이터의 전송량이 매우 적은 특징을 갖기 때문에 이때는 세션의 유효시간을 짧게 하여 기기의 이동을 보다 적극적으로 탐지할 수 있게 된다. 이를 토대로 유효세션 기반의 상호인증 프로토콜을 정의하고 설계하여보자.

2. 프로토콜 정의 및 설계

본 연구에서는 크게 4가지 단계로 프로토콜을 정의한다. 즉, 연결설정단계, 데이터전송단계, 유효세션 재설정단계, 연결해제단계로 나눈다. 연결설정 단계에서는 그림6에서처럼 기기에서 128bit 공유키와 RC4 암호화 알고리즘[9]을 이용해 Challenge Text를 암호화해 Con.req 에 포함시켜 전송하고 게이트웨이가 이를 수신하여 상호 초기인증을 수행한다. 이때 게이트웨이는 기기별로 유지하는 인증키 세트(Tokenset)를 전송한다.

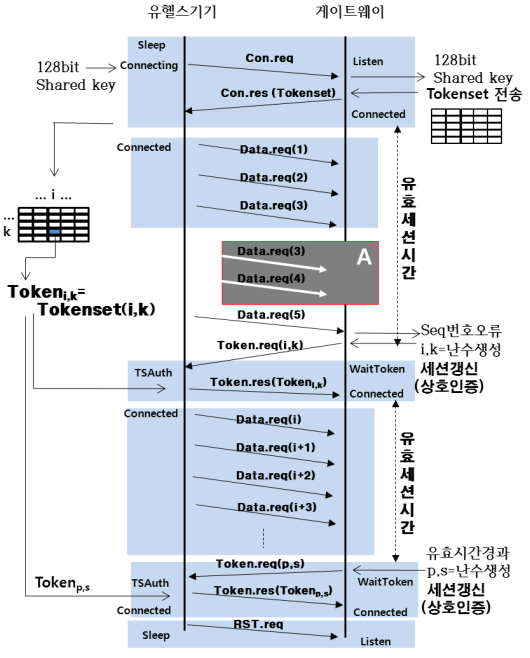
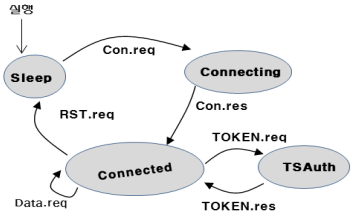


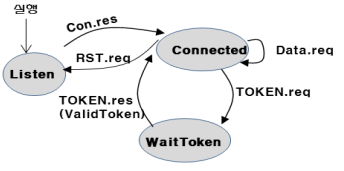
그림 6. 유효세션기반 상호인증 프로토콜과정

기기는 인증키 세트(Tokenset)를 수신함으로써 연결설정과정과 인증과정을 마친다. 이제 측정순서에 맞는 생체정보를 전송할 수 있다. [그림 6]의 A부분에서 보듯이 기기가 게이트웨이의 수신범위를 벗어나면 3번째와 4번째 데이터를 수신할 수 없으며, 추후에 수신범위 내로 들어오게 되면 5번째 데이터를 받게 되어 Seq번호오류가 발생된다. 이것으로 기기가 이동하였음을 알 수 있다. 이 경우 유효세션 재설정과정을 통해 상호인증을 제공할 수 있다. 또한 유효시간이 경과된 경우에도 유효세션을 재설정할 수 있으므로 기기와 게이트웨이간에 상호 인증과정을 주기적으로 실행할 수 있다. 유효시간의 재설정과정은 게이트웨이에서 임의의 난수로 생성된 i, k 값을 생성해 주면 기기는 이 값을 Tokenset 의 인덱스 값으로 활용하여 $Token_{i,k}$ 값을 전송한다. 바로 이 과정에서 설정되었던 전송세션의 연속적인 인증을 가능하도록 유효 세션시간을 연장하게 된다.

유효세션을 이용한 프로토콜로 정의하기 위해서 [그림 7]에서처럼 상태에 따른 처리가 필요하다. [그림 7]의 (a)는 유헬스 기기가 동작할 때 갖게 되는 4가지 상태를 정의하고 있다. 최초의 Sleep 상태에서 연결설정(Con.req)을 하면 Connecting 상태로 전이되며 게이트웨이로부터 연결응답(Con.res)이 오면 Connected 상태로 전환되어 생체정보를 측정하여 전송할 수 있다.



(a)유헬스기기



(b)게이트웨이

그림 7. 유효세션처리 상태도

만약에 유효세션 재설정(TOKEN.req)이 수신되면 TSAuth 상태로 전환되어 유효세션의 재설정처리를 하게 된다. [그림 7]의 (b)에서는 게이트웨이의 상태 처리도를 보여주고 있다. 연결설정 응답(Con.res)을 보낸 후 Connected 상태로 전환되어 생체정보를 수신할 수 있게 된다. 유효세션 시간이 초과되면 유효세션 재설정(Token. req)을 보내면서 WaitToken 상태로 전환된다. 이러한 상태변화를 통해서 기기와 게이트웨이는 안전하게 생체정보를 송수신할 수 있다.

다음은 송수신과정에서 필요한 전송 데이터의 구조를 정의한다. 전송 데이터는 [그림 8]에서처럼 6가지 Service Primitive로 정의한다.

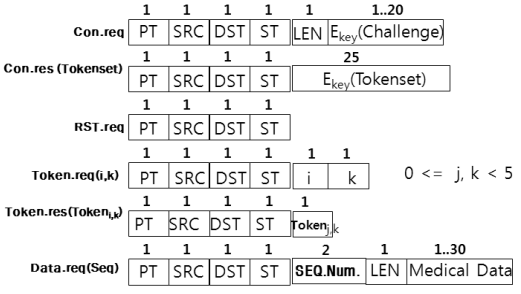


그림 8. 전송데이터 포맷

첫 번째 필드는 전송 데이터의 종류를 식별하기 위한 목적으로 패킷타입(PT)이며, 두 번째와 세 번째는 각각 기기의 출발지 주소값과 목적지 주소값이다. 네 번째는 생체정보의 유형(ST)으로 [표 1]의 한 종류를 구분하기 위한 정보이다. 다섯 번째 필드는 각 데이터의 종류에 따라 기능에 맞는 정보로 구성한다. 이와 같이 정의하고 설계한 유효 세션기반의 상호인증 프로토콜의 유효성을 확인하기 위해 다음에서 구현하여 보자.

Ⅳ. 프로토콜의 구현

유효성을 확인하려면 제안한 프로토콜이 의도대로 동작하는지 확인하여야 하기 때문에 유헬스 기기와 게이트웨이 모두 세션 인증기능을 구현하여야 한다. [그림 9]의 센서노드(③)는 한백전자의 ZigbeXII 모트에 SpO_2 센서모듈을 이용하여 산소포화도를 측정하도록 구현하였으며, 게이트웨이(①②)는 리눅스 플랫폼에서 인증기능을 제공하는 게이트웨이 프로그램과 인증기능을 제공하지 않는 프로그램으로 나누어 구현하였다.

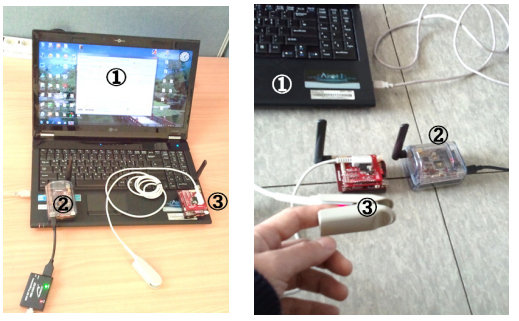


그림 9. 실험환경(test-bed)

센서노드의 프로토콜은 TinyOS 2.1.1 환경에서 이클립스 개발툴을 이용하여 nesC 프로그램으로 구현하였다. nesC 프로그램은 이벤트 처리방식으로 구동되기 때문에 [그림 10]에서처럼 이벤트 핸들러 형태로 구현하였다. 구현된 알고리즘을 살펴보자. 센서노드가 부팅하면서 booted()함수가 실행될 때 센서네트워크와 산소포화도(SpO_2)모듈을 초기화시키고 상태도 CONNECTING으로 설정한다. 또한 ActivateTimer 콤포넌트를 이용하여 1초 후에 Timer이벤트를 발생시켜 Con.req 패킷을 게이트웨이로 전송하도록 한다.

```
uint8_t key[ ]= { 0x12, 0x34, 0x43, 0xAA, 0x19, 0xC7,
0xC8, 0x21, 0x43, 0x66, 0x6B, 0x11, 0xFF, 0xBC,
0xDD,0x1E };
uint8_t TokenSet[25];

event void Boot.booted() {
   istate = CONNECTING;
   call RadioControl.start();        // 센서네트워크 초기화
   call OXY_UartControl.start();  // SpO2 모듈초기화
   call UartControl.start();
   call Oxy9C_Power.makeOutput();
   call Oxy9C_Power.set();
   call ActivateTimer.startOneShot(INTERVAL);
}
event void ActivateTimer.fired() {
 // 생략(변수초기화)
   state = INIT;
   RC4(key, sizeof(key), ChallTXT, sizeof(ChallTXT));
   pdu = MakePDU(CON_REQ,1,2,SPO2,ChallengerTXT)
   memcpy(call AMSend.getPayload(&SendMsg),
              pdu, sizeof(uHealthPDU));
```

```
   call AMSend.send(AM_BROADCAST_ADDR,
                    &SendMsg, sizeof(uHealthPDU);
}
event msg_t* Receive.receive(msg, payload, len) {
   // 변수정의   생략
  uHealthPDU = payload;
  PT = uHealthPDU->pt;

  switch(istate){
   case CONNECTING:
    if(PT == CON_RES){
     strcpy(Tokenset, uHealthPDU->data);
     call SendTimer.startPeriodic(1000);  /* 1초 */
     call OXY_SCSuartDBG.UARTSend(&SpO2_start, 1);
     istate = CONNECTED;
    }
    break;
   case CONNECTED :
     if (PT == TOKEN_REQ){
     istate = TAuth;
     i = uHealthPDU->data[0];
     k =uHealthPDU->data[1];
     Token = Tokenset[5*k+i];
     pdu=MakePDU(TOKEN_RES,1,9,SPO2,Token)
     memcpy(call AMSend.getPayload(&SendMsg),
              &pdu, sizeof(uHealthPDU));
     call AMSend.send(AM_BROADCAST_ADDR,
                      &SendMsg, sizeof(uHealthPDU);
     istate = CONNECTED
     }
     break;
   }
}
event void SendTimer.fired() {
   // 생략 (변수초기화)
   if (istate == CONNECTED) {
    if(state == SENDING) {  // 산소포화도 측정완료시
    RC4(key, sizeof(key), SPO2_Data, sizeof(SPO2_N));
   pdu=MakeDataPDU(DATA_REQ,1,9,seq++,SPO2,Data)
     memcpy(call AMSend.getPayload(&SendMsg),
              pdu, sizeof(uHealthPDU));
     call AMSend.send(AM_BROADCAST_ADDR,
                      &SendMsg, sizeof(uHealthPDU);
     state = INIT; // 산소포화도 데이터버퍼링
    }
   }
}
```

그림 10. 센서노드의 인증프로토콜 구현

게이트웨이로부터 Con.res이 오면 Receive.receive 이벤트 핸들러가 호출되어 처리한다. 이때 Tokenset을 수신하여 이후 유효세션을 유지하는데 사용한다. 또한 SendTimer 콤포넌트를 이용하여 1초 간격으로 데이터를 측정하고 전송할 수 있도록 구현하였다. 이와 같이 구현한 시스템을 이용하여 무결성 실험과 기밀성 실험을 하여보자.

V. 실험 및 평가

1. 무결성 실험 및 평가

무결성 실험은 기기와 게이트웨이가 상호 인증된 경우에만 데이터를 전송하고 받을 수 있는가를 확인하는데 그 목적이 있다. 그 이유는 인증되지 않은 유헬스 기기에서 위조된 생체정보가 올 수 있기 때문이다. [그림 11]의 실험1은 센서노드 A가 GW의 수신범위 밖으로 이동하였다가 다시 GW수신범위 안으로 들어오는 경우이며, 100회의 실험을 하였다. 실험2는 센서노드A가 수신범위 밖으로 나간 사이에 센서노드A로 위장한 B가 들어왔을 경우를 100회 실험하였다.

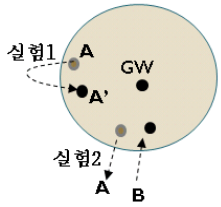


그림 11. 무결성 침해 실험 시나리오

이와 같은 실험은 GW와 노드간의 상호인증이 실현되고 있는가를 확인하여야 하기 때문에 [표 2]에서처럼 측정기준을 정의하였다. 즉, TP는 A′센서노드를 원래의 A로 인지하는 경우로 정하며, TN은 A′센서노드를 원래의 A로 인지하지 못하는 경우로 정한다. 또 실험2에서처럼 B센서노드는 A와 다르지만 이를 잘못 인식하는 경우를 FP로 정하고, B는 A와 다르다고 인식하는 경우를 FN으로 정하였다.

표 2. 실험측정 평가기준

구분	센서노드비교	결과구분
실험1	A=A	TP(True Positive)
	A≠A'	TN(True Negative)
실험2	A=B	FP(False Positive)
	A≠B	FN(False Negative)

이와 같이 실험을 한 결과 [그림 12]에서처럼 게이트웨이에서 수신한 결과를 얻었다. [그림 12]의 화면을 보면 게이트웨이가 Con.req를 수신한 후 SpO_2 정보를 수신하는 과정이 나와 있다. 전송도중에 유효세션 시간이 초과되어 유효세션 시간을 갱신하는 과정을 볼 수 있으며 이런 과정을 통해 유헬스 기기와 게이트웨이간의 무

결성 침해를 해결 할 수 있다.

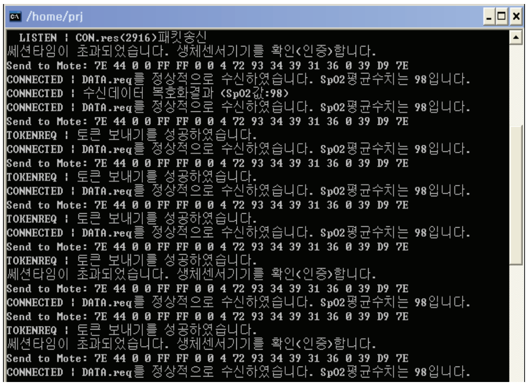


그림 12. 실험내용(게이트웨이 동작화면)

실험결과는 [표 3]에 나와 있다. [표 3]의 실험1은 95회가 성공적으로 유효세션의 갱신하여 상호인증을 통한 안전한 생체정보 전송을 하였다. 다만 5회는 세션시간과 Token.req 전송이 중첩되면서 데이터 전송이 실패한 경우이다. 실험2는 위장한 악의적인 센서기기의 차단이 100회 모두 성공적으로 되었음을 확인할 수 있었다.

표 3. 실험결과 (100회 시행)

실험	TP	TN	FP	FN
실험1	95회	5회	-	-
실험2	-	-	0회	100회
실험3	100회	0회	0회	100회

2. 기밀성 실험 및 평가

기밀성 실험은 기기로부터 전송되는 생체정보를 상호인증된 게이트웨이만 받을 수 있는가를 확인하는 데 그 목적이 있다. 그 이유는 비인증된 게이트웨이에게도 생체정보가 전송될 수 있다면 기밀성 침해가 발생할 수 있기 때문이다. [그림 13]은 기밀성 침해 실험의 시나리오를 보여준다. 즉, GW와 S간의 데이터 전송이 일어나는 도중에 비인증 게이트웨이(R.GW)가 전송범위로 들어왔을 때 GW는 정상적으로 데이터를 수신하지만 R.GW는 그러지 못하는 가를 확인하는 실험이다. 실험은 100회를 시행하였다.

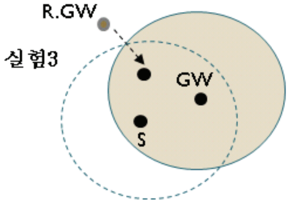


그림 13. 기밀성 침해 실험 시나리오

이 경우의 실험3에서 측정할 실험기준은 [표 4]와 같다. 즉, 인증된 게이트웨이를 인증된 게이트웨이로 식별하여 생체정보를 의도대로 전송하는 경우를 TP, 인증된 GW를 인증된 GW가 아닌 것으로 식별하여 처리하는 경우를 TN, 비인가 GW(R.GW)와 인증GW를 다른 것으로 식별하여 처리하는 것을 FP, 비인가 GW와 인증게이트웨이를 같다고 식별하는 경우를 FN으로 정한다.

표 4. 실험측정 평가기준

구분	센서노드비교	결과구분
실험3	GW=GW	TP(True Positive)
	GW≠GW	TN(True Negative)
	R.GW≠GW	FP(False Positive)
	R.GW=GW	FN(False Negative)

이와 같은 기준을 실험한 결과 [표 5]의 결과를 얻었다.

표 5. 실험결과 (100회 시행)

실험	TP	TN	FP	FN
실험3	100회	0회	100회	0회

[표 5]의 실험3은 실제로 R.GW가 데이터수신은 하였으나 생체정보부분이 주어진 암호키에 의해 암호화되어 있어서 해독할 수 없었으며, 오로지 인증된 GW만이 정상적인 데이터를 100회 모두 받을 수 있었다. 또한 R.GW는 비인가 GW로 식별되어 100회의 모든 실험에서 단 한 번의 정확한 생체정보를 수신할 수 없었다. 따라서 무결성 실험과 기밀성 실험에서 유효세션 기반의 상호인증 프로토콜의 효과를 확인할 수 있었다.

Ⅵ. 결론

유헬스 센서기기는 게이트웨이를 통해 전송하는 구조이므로 센서기기와 게이트웨이간의 신뢰성은 매우 중요한 문제이다. 즉, 생체정보를 전송할 때 기밀성 침해와 무결성 침해의 문제가 발생한다. 본 연구에서 이러한 문제를 해결하기 위해 유헬스 센서기기와 게이트웨이간에 응용레벨에서의 상호인증을 도입하되 생체정보의 측정주기에 따라 동적인 세션관리 기법을 제안하였다. 제안된 기법의 실제 TinyOS 환경에서 구현하여 실험을 통해 유효성을 확인하였다. 향후 유헬스 서비스가 가정을 중심으로 제공되려면 개인 의료정보에 대한 보안을 반드시 해결하여야 하는데 본 연구를 통해 침해 가능성에 대한 해법을 제시하였다.

참 고 문 헌

[1] C. S. Wang and Y. R. Tzeng, "A Wireless Networking Technologies Overview Over Ubiquitous Ser vice Applications," Proc. of Networked Computing and Advanced Information Mana gement, pp.156-161, 2000.

[2] R. Sulaiman, D. Sharma, W. Ma, and D. Tran, "A Security Architecture for e-Health Services," Proc. of International Conference on Advanced Communication Technology, pp.999-1004, 2008.

[3] T. T. May, "Medical information security: the evolving challenge," Proc. of Security Technology, pp.85-92, 2000.

[4] 장철순, 한종욱, "WBAN 환경의 보안 요구사항 분석", 한국해양정보통신학회 2008년도 춘계종합학술대회, pp.260-263, 2008.

[5] H. S Chen, M. J. Su, T. H. Tsai, S. S. Teng, and H. W. Zhang, "U-Care for the elderly Implementation of a Comprehensive Living and Health Care Network," e-Health networking, Application and Services, pp.187-190, 2007.

[6] 정창원, 김동호, 김명희, 주수종, "u-헬스케어 지원 분산 프레임워크에서 접근 제어 모델을 이용한 동적 보안 서비스", 인터넷정보학회논문지, 제8권, 제6호, pp.29-42, 2007.

[7] 송지은, 김신효, 정명애, 정교일, "u-헬스케어 보안 이슈 및 기술 동향", 전자통신동향분석, 제22권, 제1호, pp.119-129, 2007.

[8] F. W. Xuan, D. M. Chui, and L. W. Kei, "Novel system sampling multi vital signs for e-Home Healthcare," Proc. of 7th Int'l Conference on Information, Communications and Signal Processing, pp.1-5, 2009.

[9] Y. Yao, J. Chong, and W. Xingwei, "Enhancing RC4 algorithm for WLAN WEP protocol," Control and Decision Conference (CCDC) Chinese, pp.3623-3627, 2010.

저 자 소 개

이 병 문(Byung-Mun Lee) 정회원

- 1988년 2월 : 동국대학교 전자계산학과(공학사)
- 1990년 2월 : 서강대학교 전자계산학과(공학석사)
- 2007년 2월 : 인천대학교 컴퓨터공학과(공학박사)
- 1998년 3월 ~ 현재 : 가천의과학대학교 정보공학부 부교수

<관심분야> : 유헬스, 센서네트워크, 센서운영체제

임 헌 철(Heon-Cheol Lim) 준회원

- 2011년 2월 : 가천의과학대학교 의료공학부 IT학과(공학사)
- 2009년 12월 : 가천의과학대학교 유-헬스케어연구소 연구원
- 2011년 3월 : 인하대학교 정보공학과 컴퓨터정보공학 전공 석사

과정

<관심분야> : u-헬스케어, 센서네트워크, 보안

강 운 구(Un-Ku Kang) 정회원

- 2001년 2월 : 인하대학교 대학원 전자계산공학과(공학박사)
- 2002년 ~ 2006년 : 뉴미디어연구소장
- 2007년 ~ 현재 : 유-헬스케어연구소장
- 1994년 ~ 현재 : 가천의과학대학교 정보공학부 교수

<관심분야> : 의료IT융합, 유헬스, 의료정보, 소프트웨어공학