Journal of The Korea Society of Computer and Information
Vol. 17, No. 10, October 2012
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci/2012.17.10.079

홈헬스 환경에서 생체정보전송의 안전성을 고려한 랜덤유효세션기반의 상호인증 프로토콜

임 헌 철*, 박 태 현**, 권 구 인*

Mutual Authentication Protocol based on the Random Divided Session for the Security of Medical Information in Home-Health

Heon-Cheol Lim*, Tae-Hyun Park**, Gu-In Kwon*

요 약

본 연구에서는 센서와 게이트웨이간의 응용레벨 전송 세션을 세분화하고 각 세션을 주기적으로 갱신하는 기법을 적용하여 모델화하였다. 또한 이 모델에서의 인증을 위한 전송오버헤드를 최소화하기 위해 생체정보의 측정주기에 따른 동적인 유효 세션기법을 적용하였고 비인가 게이트웨이가 유효세션 시간을 예측하지 못하도록 유효세션 시간을 랜덤화 하였다. 이 모델은 비인가 센서기기의 무결성 침해와 기밀성 침해를 차단하는 효과가 있다. 본 모델의 평가를 위해 TinyOS 2.1 환경에서 구현하여 실험하였다. 따라서 전송할 생체정보가 서로 다른 측정주기를 갖는 것을 통해 효율성을 제공하도록 하였다. 결과적으로 제안한 기법을 3가지 실험을 통해 유효성을 확인하였다.

▸ Keywords : 홈헬스, 생체정보, 안전성, 랜덤유효세션, 상호인증

Abstract

In this paper, we design a mutual authentication protocol which divided sessions from an authenticated session are updated periodically. And in order to minimize the traffic overhead for session authentication, we also introduce dynamic session management according to sampling rate

• 제1저자 : 임헌철 • 교신저자 : 권구인
• 투 고 일 : 2012. 09. 03, 심사일 : 2012. 09. 12, 게재확정일 : 2012. 09. 19.
* 인하대학교 컴퓨터정보공학과(Dept. of Computer Information and Science, Inha University)
** 인하대학교 컴퓨터정보공학과(Dept. of Computer Information and Science, Inha University)
* 이 논문은 인하대학교의 지원에 의하여 연구되었음.
* 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것. (2012-0001720)

of medical sensor type. And randomize the divided session time. This model has the effect of blocking the integrity and confidentiality intrusion of rogue gateway. Moreover, efficiency is provided through medical data to be transmitted have different sampling rate. In order to evaluate this model, it was embodied and experimented in TinyOS 2.1 environment. The result, we got an overall validity from three types of experiment.

▸ Keywords : Home-Health, Medical Information, Security, Random Divided Session, Mutual Authentication

I. 서 론

인구 고령화가 증진됨에 따라 만성질환자의 자가 관리에 관한 관심 또한 증가하고 있다. 이에 따른 사회적 의료서비스 환경의 변화는 홈헬스를 등장시켰다. 홈헬스 서비스를 제공하려면 홈헬스용 MSN(Medical Sensor Node)와 홈헬스 서버가 필요하다. 홈헬스는 가정에서 MSN를 이용해 측정된 생체정보를 게이트웨이를 통해 서버로 전송하는 서비스이다. 이때 사용자의 생체정보는 매우 중요한 개인정보이기에 게이트웨이를 통해 안전하게 전송되어야 한다. 그러나 홈헬스에서 사용되는 무선의 센서네트워크 환경은 브로드캐스트 전송방식의 특성상 데이터가 모두에게 노출될 위험이 있기에 데이터 유출 문제가 발생한다[1]. 이러한 문제 해결을 위해 IEEE 802.15.4 MAC과 같은 표준 규격에서는 AES기반의 보안모드를 지원한다. 그러나 최근 연구 결과에 따르면 안전하다고 판명되던 AES조차도 취약점이 발견되어 다양한 형태의 침해 가능성이 제기되고 있다. 이것은 MAC계층과 네트워크 계층은 물론 응용계층에서도 다양한 형태의 침해가능성을 고려한 보안기능이 필요하다는 것을 의미한다[2,10].

특히 홈헬스 환경에서는 응용계층에서의 특성에 따라 취약성의 내용도 다르다. 일단 홈헬스용 MSN는 휴대하기가 간편하여야 하고 기기의 특성에 따라 데이터의 생성주기가 많은 차이를 보인다. 또한 홈헬스 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 과정에서 안전한 생체정보 전송이 필요하다[3,4,16,17].

이와 같은 맥락에서 볼 때 MSN에서 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[4,11,12]. 따라서 MSN와 게이트웨이간의 신뢰성 문제가 매우 중요하다. 즉 기기간의 상호인증이 필요할 뿐만 아니라 어플리케이션간의 상호인증도 필요하다는 것이다. 특히 사용자가 MSN를 사용할 때 휴대가 간편하고 쉽게 이동시킬 수 있어야 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. 하지만 동적인 인증이라 하더라도 생체정보 특성에 따라 유효세션 시간은 정해져 있기에 비인증 게이트웨이가 생체정보를 갈취하는 과정에서 유효세션 시간이 유출될 수 있다. 이때 만일 생체정보가 유출되더라도 생체정보에 따른 유효세션 시간을 예측할 수 없다면 더욱더 안전하게 생체정보를 전송할 수 있게 된다.

따라서 본 연구에서는 이와같은 동적인 인증방식기반의 유효세션 시간을 랜덤화하여 모델링하고 이를 구현하기 위한 상호인증 프로토콜을 제안하고자 한다. 또한 랜덤 유효세션은 적정의 오차범위를 주고 적용할 것이며 제안하는 인증모델의 유효성을 확인하기 위해 MSN에 인증모듈을 구현하여 실험을 통해 유효성을 보이고자 한다.

본 논문의 구성은 2장에서는 홈헬스에서의 생체정보 보안위협에 대한 사항을 시나리오를 통해 기술하고, 3장에서는 본 논문에서 제안하는 랜덤 유효세션 기반의 상호인증 프로토콜에 대한 사항을 기술한다. 4장에서는 실험 및 평가를 하고 마지막 5장에서는 결론으로 끝을 맺는다.

II. 관련 연구

1. 홈헬스 환경에서의 생체정보 보안위협

1.1 홈헬스 시스템 모델

홈헬스 시스템은 〔그림 1〕 같이 MSN, 가정용 무선 게이트웨이 그리고 홈헬스 서버로 구성된다[5].

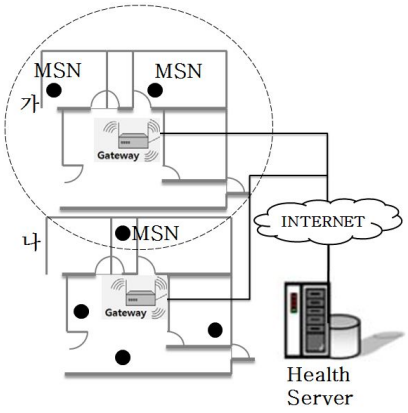

그림 1. 홈헬스 시스템 모델
Fig 1. Home-Health System Model

그림 1은 가정에서 홈헬스 서비스를 이용할 경우 구성할 수 있는 홈헬스 시스템을 보여준다. 예를 들어 이웃한 2개의 가정(가, 나)이 있다고 하자. 가의 경우 MSN이 측정한 생체정보(심전도(ECG), 산소포화도(SpO_2), 혈압, 혈당)를 게이트웨이로 전송하고 인터넷을 통해서 외부의 홈헬스 서버에 저장한다[13,14]. 이 때 사용자는 가정내에서의 사용과정에서 홈헬스 MSN를 쉽게 이동시킬 수 있다. 다음에서 시나리오를 통해 자세히 살펴보자.

1.2 홈헬스 MSN의 이동성

게이트웨이가 측정된 생체정보를 정확히 수신하려면 게이트웨이의 수신범위에 홈헬스 MSN가 있어야 한다. 그러나 사용자는 안과 밖으로 MSN를 휴대하여 쉽게 이동 시킬 수 있기 때문에 게이트웨이의 수신범위에서 벗어날 수 있다. 그림 2를 살펴보자. 기기가 MSN_1 지점에서 GW로 생체정보를 전송하다가 MSN_2 지점으로 이동하면 GW의 수신범위 밖이 되기 때문에 GW는 생체정보를 수신하지 못하게 된다. 잠시 후 MSN가 MSN_2 지점에서 MSN_3 지점으로 이동하게 되면 GW가 다시 생체정보를 수신할 수 있다. 이 과정에서 홈헬스 기기와 게이트웨이간의 응용계층에서는 세션을 유지하게 되기 때문에 생체정보를 그대로 받을 수 있다. 이와 같이 사용자는 MSN를 자유롭게 이동하며 사용할 수 있으나 MSN가 게이트웨이의 수신범위 밖과 안으로 이동하는 과정에서 악의적인 사용자에 의해 생체정보가 유출될 수 있고 위조될 수 있는 취약점이 생긴다. 다음절에서 위와 같은 운영시나리오별 취약상황에 대해서 살펴보자.

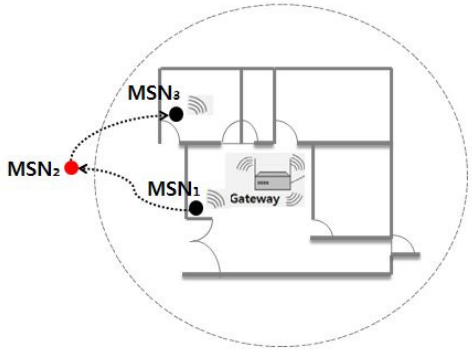

그림 2. 홈헬스 MSN의 이동성
Fig 2. Mobility of Home-Health MSN

1.3 이동성에 따른 취약성

생체정보를 측정하는 Zigbee 와 같은 센서 네트워크는 무선의 특성 때문에 전송데이터의 기밀성과 무결성 보호에 취약하다[6,7]. 먼저 그림 3을 통해 기밀성 침해 문제를 살펴보자. 처음에 MSN_1 은 GW에게 생체정보를 전송하고 있었다. 이때 MSN_1 은 GW의 수신범위내에서 벗어나지 않고 MSN_2 지점으로 이동한다. 동시에 비인가된 Fake GW 도 이동하여 MSN_2 의 수신범위로 접근해 온다면 MSN_2 에서 전송하는 생체정보가 Fake GW 로 유출될 수 있는 기밀성 침해문제가 생긴다.

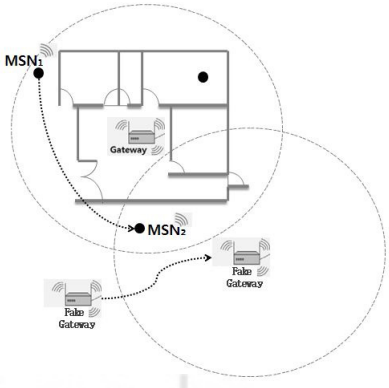

그림 3. 기밀성 침해 공격 시나리오
Fig 3. Scenario of Confidentiality Intrusion Attack

이번에는 무결성을 침해받을 수 있는 경우를 살펴보자. 먼저 MSN_1 이 GW의 수신범위 밖으로 벗어나는 경우를 생각해볼 수 있다. 그림 4와 같이 GW와 생체정보를 주고받던 MSN_1 이 게이트웨이 수신범위 밖으로 이동하였다고 가정할 때 악의적인 공격자 MSNattacker가 MSN_1 으로 위장하여 위조된 생체정보를 전송할 수 있다. 이 경우에 게이트웨이는 MSN_1 과 위장한 $MSN'1$을 정확히 구별할 수 없으며 수신범위 밖에 있던 동안에 공격을 받을 수 있는 가능성이 충분히 발생할 수 있다. 이와 같이 게이트웨이와 홈헬스 MSN간에는 상호인증이 반드시 필요하다.

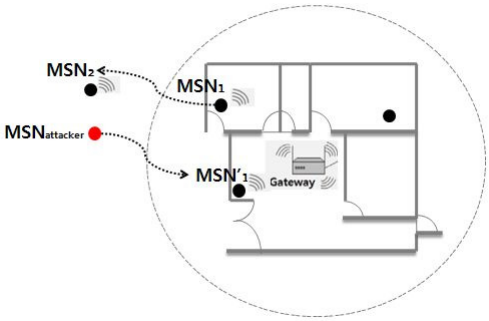

그림 4. 무결성 침해 공격의 시나리오
Fig 4. Scenario of Integrity Intrusion Attack

따라서 위와 같은 무결성, 기밀성 침해 문제들을 해결하기 위해서 홈헬스 MSN와 게이트웨이 간의 생체정보를 전송하는 과정에서 유효세션 시간을 동적으로 할당하는 랜덤 유효세션 기반의 상호인증 모델을 제안하고자 한다.

III. 랜덤 유효세션 기반의 상호인증 프로토콜

1. 랜덤 유효세션 기반 상호인증모델의 제안

제안하는 상호인증 모델의 가장 큰 특징은 홈헬스 MSN와 게이트웨이간에 있어 비인가 기기에게 유출될 수 있는 개인의 생체정보를 차단하는 효과를 제공해 준다는 것이다. 본 모델을 자세히 정의하면 전송세션을 여러 개의 유효세션으로 나누고 각 유효세션을 생체정보의 특성에 따라 랜덤화하여 유효세션간에 상호인증과정을 두는 것이 기본적인 아이디어이다. 따라서 비인가 기기가 중간에 끼어들더라도 데이터 유출을 막을 수 있다. 그러나 유효세션마다 상호인증과정을 매번 수행하면 불필요한 네트워크 트래픽과 기기 처리과정에서의 오버헤드가 발생된다. 이러한 문제를 최소화하기 위해 세션의 갱신주기를 모두 동일하게 적용하지 않고 데이터 측정빈도가 많은 홈헬스 MSN[8]에는 세션시간을 많게 할당하면서 랜덤화하고 측정빈도가 적은 홈헬스 MSN에는 세션시간을 적게 할당하면서 랜덤화하는 동적인 유효세션 기법을 적용한다. 그림 5는 제안하고자 하는 상호인증 모델이다. 그림 5를 살펴보면 생체정보 발생주기가 낮은 MSN_A 타입은 게이트웨이와의 전송세션 시간은 길지만 데이터 전송주기가 길어 홈헬스 기기가 이동하였을 때 이를 인식하는데 상대적으로 오랜시간이 걸린다.

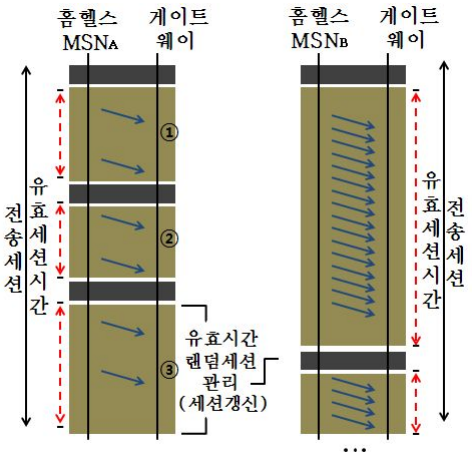

그림 5. 랜덤 유효세션 기반의 인증전송모델
Fig 5. Authentication Model with Random Divided Session

이에 비하여 MSN_B 타입은 게이트웨이와의 전송세션 시간이 길지만 데이터 전송주기가 짧아 이동하였을 때 이를 MSN_A에 비하여 빠르게 인식할 수 있다. 따라서 이러한 특성을 고려하여 MSN_B 에게는 유효세션 시간을 길게 할당하고 MSN_A 에게는 유효세션 시간을 짧게 할당하여 세션 갱신과정에서 발생하는 오버헤드를 줄이고 효율적인 유효시간 세션관리가 가능하도록 모델화였다. 또한 유효세션 시간을 통해 효율적으로 세션을 관리하더라도 비인가 기기에게 생체정보의 특성이 유출되어 유효세션 시간을 예측할 수 있게 된다면 상호인증모델이 효과를 발휘하지 못하게 된다. 따라서 생체정보의 특성이 유출되더라도 유효세션 시간을 예측하지 못하도록 그림 5의 ①~③과 같이 유효세션 시간을 랜덤화하였다.

표 1. 생체정보별 측정주기와 유효세션 시간
Table 1. Sampling Rate and Divided Session Time depending on Medical Data

생체정보	유효세션 시간(sec)	측정주기 ,측정량	센서타입(ST)
심전도	600(±100)	20ms,다량	1
근전도	600(±100)	20ms,다량	2
위전도	600(±100)	20ms,다량	3
심박수	600(±100)	20ms,다량	4
산소포화도	300(±100)	1sec,소량	11
활동량	300(±100)	1sec,소량	12
혈압	60(±10)	2회/1일, 소량	21
체온	60(±10)	2회/1일, 소량	22
체중	60(±10)	2회/1일, 소량	23
혈당	60(±10)	2회/1일, 소량	24

먼저 표 1은 기존의 각 생체정보의 특성에 따른 유효세션 시간을 보여준다. 심전도, 근전도, 위전도, 심박수와 같이 측정주기가 짧아 단위시간당 측정량과 트래픽이 많은 경우에는 세션의 유효세션 시간을 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.

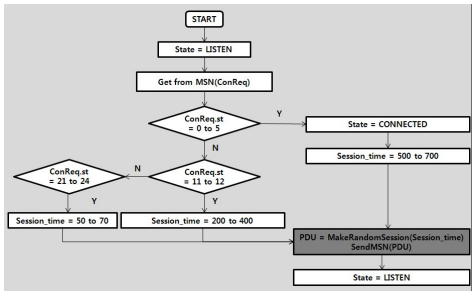

그림 6. 게이트웨이의 랜덤 유효세션 알고리즘
Fig. 6. Random Divided Session Algorithm of Gateway

따라서 유효세션 시간을 상대적으로 긴 600초로 설정하고 오차범위를 ±100으로 정의한다. 그에 비해서 혈압, 체온, 체중, 혈당의 경우에는 1일에 1회~2회정도 측정하게 되어 단위시간당 전송량이나 트래픽이 매우 적다[15]. 따라서 전송세션 동안 데이터의 전송량이 매우 적은 특징을 갖기 때문에 이 경우에는 세션의 유효시간을 60초로 설정하고 오차범위를 ±10으로 짧게 정의하여 기기의 이동을 보다 적극적으로 탐지할 수 있게 한다. 그림 6은 게이트웨이에서 동작하는 랜덤유효세션 알고리즘을 표현한 것이다. 알고리즘에서는 최초로 State를 LISTEN으로 설정하고 홈헬스 MSN로부터 ConReq를 수신한다. 그리고 데이터의 센서 타입에 따라 랜덤 유효세션시간을 적용한다. 예를 들어 센서 타입이 1번이라고 가정하자. 표 1을 살펴보면 1번은 상대적으로 유효세션 시간이 긴 심전도를 나타내므로 500~700초의 랜덤 유효세션 시간을 갖게되고 이를 MakeRandomSession에 의해 동작하게 된다. 동작 후에는 데이터를 수신하는 단계로 돌아간다. 다음에서 랜덤 유효세션 알고리즘이 적용된 상호인증 모델을 홈헬스 MSN과 게이트웨이간의 프로토콜로 상세하게 정의하여 보자.

2. 프로토콜 정의 및 설계

본 연구에서 정의한 프로토콜은 크게 4가지 단계로써 연결설정단계, 데이터전송단계, 랜덤 유효세션 재설정단계, 연결해제단계로 나눈다.

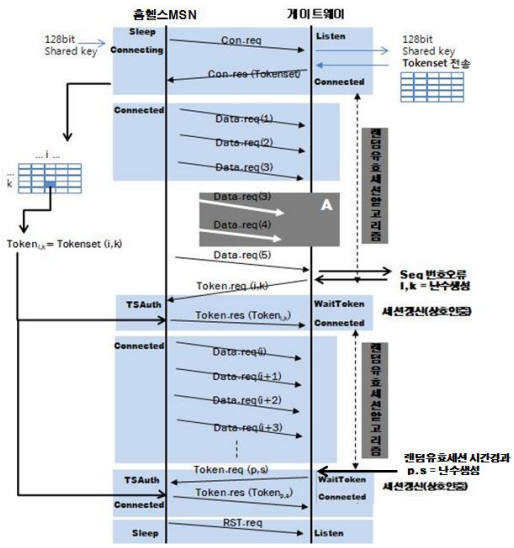

그림 7. 랜덤 유효세션 기반의 상호인증 프로토콜
Fig. 7. Mutual Authentication Protocol based on the Random Divided Session

그림 6에서 보면 연결설정 단계에서는 기기에서 128bit 공유키와 RC4 암호화알고리즘[9]을 이용해 Challenge Text를 암호화해 Con.req에 포함시켜 전송하고 게이트웨이가 이를 수신하여 상호 초기인증을 수행한다. 이때 게이트웨이는 MSN 타입별로 유지하는 인증키 세트(Tokenset)를 전송한다. 홈헬스 MSN는 인증키 세트(Tokenset)를 수신함으로써 연결설정과정과 인증과정을 마친다. 이제 측정순서에 맞는 생체정보를 전송할 수 있다. 그림 7의 A와 같이 기기가 게

이트웨이의 수신범위를 벗어나면 3번째와 4번째 데이터를 수신할 수 없으며, 추후에 수신범위내로 들어오게 되면 5번째 데이터를 받게 되어 Seq번호오류가 발생된다. 이것으로 기기가 이동하였음을 알 수 있다. 이 경우 랜덤 유효세션 재설정 과정을 통해 상호인증을 제공할 수 있다. 또한 랜덤 유효세션 시간이 경과된 경우에도 랜덤 유효세션을 재설정할 수 있으므로 홈헬스 MSN와 게이트웨이간에 상호 인증과정을 주기적으로 실행할 수 있다. 랜덤 유효세션시간의 재설정과정은 게이트웨이에서 임의의 난수로 생성된 i, k 값을 생성해 주면 기기는 이 값을 Tokenset 의 인덱스값으로 활용하여 Tokeni,k 값을 전송한다. 바로 이 과정에서 설정되었던 전송세션의 연속적인 인증을 가능하도록 랜덤 유효세션 시간을 연장하게 된다.

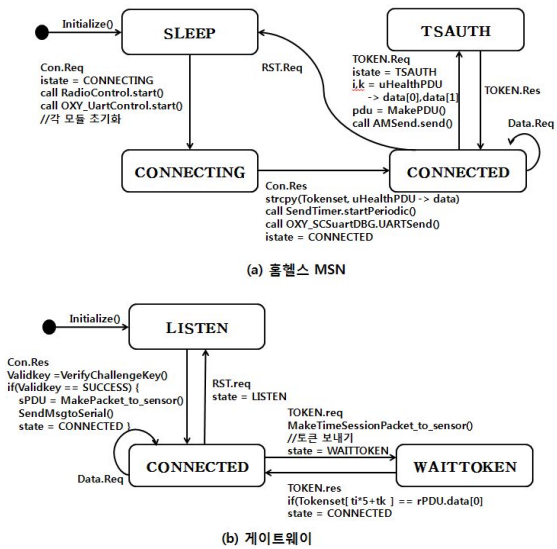

그림 8. 랜덤 유효세션의 상태 다이어그램
Fig. 8. State Diagram of Random Divided Session State Diagram

랜덤 유효세션을 이용한 프로토콜을 정의하기 위해서 그림 8과 같이 홈헬스 MSN과 게이트웨이에 상태에 따른 처리를 State Diagram으로 표현하였다. 다음은 송수신과정에서 필요한 전송 데이터의 구조를 정의한다. 전송 데이터는 그림 9에서처럼 6가지 종류로 구분한다.

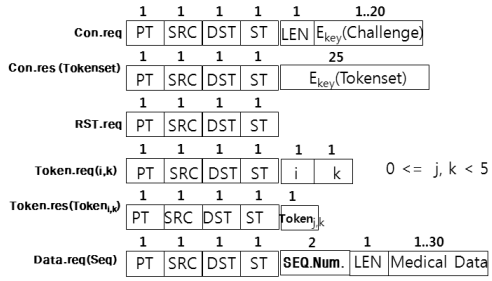

그림 9. 데이터 포맷
Fig. 9. Data format

첫 번째 필드는 전송 데이터의 종류를 식별하기 위한 목적으로 패킷타입 PT이며, 두 번째와 세 번째는 각각 기기의 출발지 주소 값과 목적지 주소 값이다. 네 번째는 생체정보의 유형 ST으로 표 1의 한 종류를 구분하기 위한 정보이다. 다섯 번째 필드부터는 각 데이터의 종류에 따라 기능에 맞는 정보로 구성한다. 이와 같이 설계한 랜덤 유효세션 기반의 상호인증 프로토콜을 이용해서 구현하여 보자. 기밀성과 무결성 침해에 대한 대응이 제대로 이루어지는지 실험을 통해 확인하여 보자.

IV. 프로토콜의 구현

1. 실험환경 및 구현

본 연구에서 제안한 모델의 유효성을 확인하고 평가하기 위해 그림 10에서처럼 한백전자의 센서장비(ZigbeXII Mote)에 SpO2 옵션모듈(③)을 장착하여 구현하였으며 제안한 모델이 의도대로 동작하는지 확인할 필요가 있기 때문에 홈헬스 MSN과 게이트웨이 모두 랜덤 유효세션 인증기능을 구현하였다.

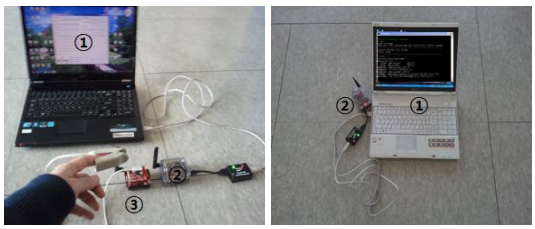

그림 10. 테스트 베드
Fig. 10. Test-bed

게이트웨이(①②)는 한백전자에서 제공하는 Serial Tool과 리눅스 기반의 Cygwin환경에서 인증기능을 제공하는 게이트웨이 프로그램과 인증기능을 제공하지 않는 프로그램으

로 나누어 C로 구현하였다. 센서노드의 프로토콜은 TinyOS 2.1 환경에서 Eclipse 개발툴을 이용해 nesC 프로그램으로 구현하였다. TinyOS 2.1은 이벤트 처리방식으로 센서의 모든 동작을 이벤트 핸들러에 의해 처리하기 때문에 그림 11에서처럼 구현하였다. 센서노드가 기동할 때 Boot.booted() 이벤트가 발생되면서 RF통신을 위한 RadioControl을 비롯한 여러 가지 센서모듈의 컴포넌트를 초기화시킨다. 또한 상태도 CONNECTING으로 설정하며 게이트웨이와의 연결 설정을 위한 ActiveTimer를 작동시켜 1초 후에 Timer이벤트를 발생시켜 Con.req 패킷을 게이트웨이로 전송하도록 한다.

```
uint8_t key{ }= { 0x12,0x34,0x43,0xAA,0x19,0xC7,0xC8, 0x
21,0x43,0x66,0x6B,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){
    RandomSession = uHealthPDU->Session_time;
    strcpy(Tokenset, uHealthPDU->data);
    call SendTimer.startPeriodic(1000);  /* 1초 */
    call OXY_SCSuartDBG.UARTSend(&SpO2_start,
                        RandomSession);
    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 11. 메디컬 센서노드의 인증프로토콜 구현
Fig. 11. Authentication Protocol Implementation of Medical Sensor Node

게이트웨이로부터 Con.res이 오면 Receive.receive 이벤트 핸들러가 호출되어 처리한다. 이때 Tokenset과 Session_time을 수신하여 이후 랜덤 유효세션을 유지하는데 사용한다. 또한 SendTimer 콤포넌트를 이용하여 1초 간격으로 데이터를 측정하고 전송할 수 있도록 구현하였다. 다음에서 구현한 모델을 통해 기밀성과 무결성 침해에 대한 대응이 제대로 이루어지는지 실험을 통해 확인하여 보자.

V. 실험 및 성능평가

1. 성능실험 시나리오

실험은 그림 12에서처럼 무결성과 기밀성 침해에 대한 2가지 경우의 시나리오로 진행 하였다.

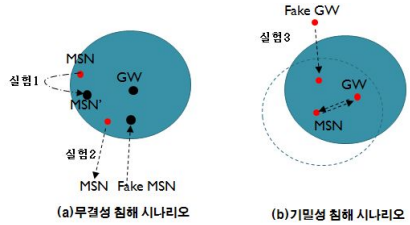

그림 12. 성능평가 시나리오
Fig. 12. Scenario of the Performance Evaluation

그림 12의 (a)는 무결성 침해에 관한 시나리오로 홈헬스 MSN과 게이트웨이가 상호 인증된 경우에만 데이터를 전송하고 받을 수 있는 지를 확인하는 실험이다. 그 이유는 인증되지 않는 홈헬스 MSN에서는 위조된 생체정보가 전송될 수 있기 때문이다. 실험 1의 경우에는 MSN가 GW의 수신범위 밖으로 이동하였다가 다시 GW수신범위 안으로 들어오는 경우이며, 1000회의 실험을 하였다. 실험2의 경우에는 MSN가 수신범위 밖으로 나간 사이에 MSN로 위장한 Fake MSN이 들어왔을 경우를 나타내며 1000회를 실험 하였다. 그림 12의 (b)는 기밀성 침해에 관한 시나리오로 실험 3은 MSN으로부터 전송되는 생체정보를 상호 인증된 게이트웨이만 받을 수 있는지를 확인하는 실험이다. 이유는 비 인증된 게이트웨이에게도 생체정보가 전송된다면 기밀성 침해가 발생할 수 있기 때문이다. 예를 들어 GW와 MSN간의 서로 데이터를 주고받는 도중에 비 인증 게이트웨이(Fake GW)가 전송범위로 들어왔다고 가정하자. 이 경우에 GW가 정상적으로 데이터를 수신하게 되지만 Fake GW의 경우에 데이터 수신을 하지 못하는 지를 확인하는 실험이다. 위의 실험은 GW와 MSN간의 상호 인증이 실현되고 있는지를 확인하는 바이기 때문에 표 2에서처럼 성능 평가기준 방법을 정의하였다. 성능 평가기준을 보면 TP는 MSN'를 원래의 MSN로 인지하는 경우를 의미하며, TN은 MSN'를 원래의 MSN로 인지하지 못하는 경우를 의미한다. 또한 실험2와 같이 Fake MSN은 MSN와 다르지만 이를 잘못 인식하는 경우를 FP라 정의하고 Fake MSN는 MSN와 다르다고 인식하는 경우를 FN으로 정의한다. 실험 3에서의 평가기준은 TP는 인증된 게이트웨이를 인증 게이트웨이로 식별하여 생체정보를 의도대로 전송하는 경우를 의미하고 TN은 인증된 GW를 인증된 GW가 아닌 것으로 식별하여 처리하는 경우를 의미하고 FP는 비 인증 FakeGW와 인증 GW를 다른 것으로 식별하여 처리하는 것, 마지막 FN은 비인증 FakeGW와 인증 GW를 같다고 식별하는 경우를 의미한다.

표 2. 성능 평가기준
Table 2. Performance Evaluation Standard

구분	MSN 비교	결과구분
실험 1	MSN = MSN	TP(True Positive)
	MSN ≠ MSN'	TN(True Negative)
실험 2	MSN = Fake MSN	FP(False Positive)
	MSN ≠ Fake MSN	FN(False Negative)
실험 3	GW = GW	TP(True Positive)
	GW ≠ GW	TN(True Negative)
	FakeGW ≠ GW	FP(False Positive)
	FakeGW = GW	FN(False Negative)

이와 같이 실험을 한 결과를 각각 표 3과 그림 13에서 보여주고 있다.

표 3. 성능 평가
Table 3. Performance Evaluation

실험	TP	TN	FP	FN
실험 1	990회	10회	-	-
실험 2	-	-	0회	1000회
실험 3	1000회	0회	1000회	회

그림 13의 실험 1을 살펴보면 990회가 성공적으로 랜덤 유효세션을 갱신하여 상호인증을 통한 안전한 생체정보 전송을 한 것으로 나타나고 있다. TN의 10회의 수치는 랜덤 유효세션 시간과 Token.req 전송이 중첩되면서 또는 Timer 이벤트들의 중첩문제로 데이터 전송이 실패한 경우이다. 자세한 실험 결과 내용은 그림 14에서 나타내고 있다. 실험 2는 위장한 악의적인 MSN의 차단이 1000회 모두 성공하였음을 나타내는 수치이다.

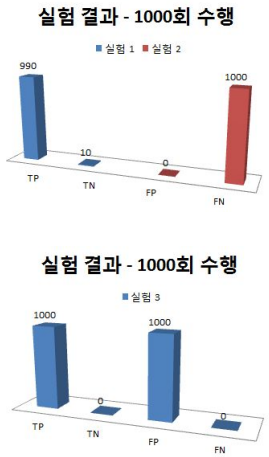

그림 13. 성능평가
Fig. 13. Performance Evaluation

실험 3은 실제로 Fake GW가 데이터 수신은 하였으나 생체정보부분이 주어진 암호키에 의해 암호화되어 있어서 해독할 수 없었으며 오로지 인증된 GW만이 정상적인 데이터를 1000회 모두 받을 수 있었다. 또한 Fake GW는 비 인증 GW로 식별이 되어 1000회의 모든 실험에서 단 한 번의 정확한 생체정보를 수신할 수 없었다. 결국 인증 GW로 인해서 개인의 생체정보를 Fake GW에게도 전송할 수 있는 것을 차단함으로써 보다 안전하게 전송할 수 있게 되었다. 따라서 지

금까지의 무결성 실험과 기밀성 실험을 통해 본 연구에서 제안하고 있는 랜덤 유효세션 기반 상호인증모델의 유효성을 확인할 수 있었다.

그림 14. 실험 결과
Fig. 14. Experimental Result

Ⅵ. 결론

홈헬스 환경에서는 보다 안전하게 개인의 생체정보를 게이트웨이를 통해 전송하여야만 한다. 이러한 구조적 특징을 갖고 있기 때문에 홈헬스 MSN와 게이트웨이간의 신뢰성 문제는 매우 중요하다. 다시 말하면, 생체정보를 전송할 때 기밀성 침해와 무결성 침해의 문제가 발생한다. 본 연구에서 이러한 문제들을 해결하기 위해 홈헬스 MSN와 게이트웨이간에 응용레벨에서의 상호인증을 도입하되 생체정보의 측정주기에 따른 랜덤 유효세션관리 기법을 제안하였다. 제안된 기법을 실제 TinyOS 2.1 환경에서 구현하여 3가지의 실험을 통해 유효성을 확인하였다. 향후 홈헬스 서비스가 점차 보편화되기 위해서는 개인 의료정보에 대한 보안문제를 반드시 고려해야 하는데 본 연구를 통해 2가지의 침해 가능성에 대한 문제에 대해 해결책을 제시하였다.

참고문헌

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

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

[3] T. T. May, "Medical information security: the evolving challenge", 32nd Annual 1998 International Carnahan Conferenece on. of Security Technology, pp. 85-92, 2000.

[4] C. S. Jang, W. J. Han, "Security Requirement Analysis for WBAN environment", Fall 2008, KIMICS Integrated Conference, pp. 260-263. 2008.

[5] H. S Chen, M. J. Su, T. H. Tsai, S. S. Teng, 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, June. 2007.

[6] C. W. Jeong, D. H. Kim, M. H. Kim, S. J. Joo, "A Dynamic Security Service using Access Control Model in Distributed Framewirk Support for u-Healthcare", Journal of Korean Society for Internet Information, Vol.8, No.6, pp. 29-42, 2007.

[7] J. E. Song, S. H. Kim, M. E. Jeong, K. I. Jeong, "Security Issues and Its Technology Trends in u-Healthcare", Electronics and Telecommunications Trends Vol.22, No.1, pp. 119-129, Feb. 2007.

[8] F. W. Xuan, D. M. Chui, 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, W. Xingwei, "Enhancing RC4 algorithm for WLAN WEP protocol", Control and Decision Conference (CCDC) Chinese, pp. 3623-3627, 2010.
[10] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique Cryptanalysis of the Full AES", Proc. of Int'l Conference on Theory and Application of Cryptology and Information Security ASIACRYPT 2011, pp. 344-371, Dec. 2011.
[11] M. H. Kim, J. S. Kim, A. R. Kim, K. J. Chae, "New Security Technology Trends of Wireless Sensor Network", Korea Information Processing Society Review, Vol. 17, No. 1, pp. 139-147, 2008.
[12] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, "Protocol for self-organization of a wireless sensor network", Personal Communications IEEE, Vol. 7, pp. 16-27, Oct. 2000.
[13] K. Fall, "A delay-tolerant network architecture for challenged internets", ACM SIGCOMM 2003, pp.27-34, Aug. 2003.
[14] S. J. Lee, and W. W. Su, "An adaptive and fault-tolerant gateway assignment in sensor networks", 2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems, Vol. 6, No.5, PP.576-578, April 2004.
[15] M. Paksuniemi, H. Sorvoja, E. Alasaarela, and R. Myllyla, "Wireless sensor and data transmission needs and technologies for patient monitoring in the operating room and intensive care unit", Engineering in Medicine and Biology Society 2005 IEEE-EMBS 2005 27th Annual international Conference, pp. 5182-5185, Jan. 2006.
[16] Y. R. Lee, D. G. Park, E. "Role based access control of healthcare information system for Mobile environments", Journal of the Korea Society of Computer and Information, Vol. 10, No.5, pp. 119-132, July. 2005.
[17] J. W. Kim, H. "Implementation of a pervasive health care system for cardiac patient on mobile environment", Journal of the Korea Society of Computer and Information, Vol. 13, No.2, pp. 117-124, Sep. 2008.

저 자 소 개

임 헌 철

2011 : 가천의과학대학교 IT학과 공학사
2011 : 인하대학교 컴퓨터정보공학과 공학 석사
현 재 : 인하대학교 컴퓨터정보공학과 공학 석사과정
관심분야 : 무선센서네트워크, 유헬스, USN Security, Network Protocol
Email : ydgvnk70@naver.com

박 태 현

2003 : 홍익대학교 컴퓨터공학과 공학사
2005 : 울산대학교 컴퓨터정보공학과 공학석사
현 재 : 인하대학교 컴퓨터정보공학과 공학 박사과정
관심분야 : 센서네트워크, 무선 에드혹 네트워크, 멀티홉 무선 센서 네트워크
Email : th_park@naver.com

권 구 인

1995 : 인하대학교 컴퓨터공학과 공학사
1998 : City University of NewYork 컴퓨터공학과 공학석사
2005 : Boston University Computer Science 공학박사
현 재 : 인하대학교 컴퓨터정보공학부 교수
관심분야 : Multicast, Congestion Control, Overay Network, 센서네트워크
Email : gikwon@inha.ac.kr