무선 인체 영역 네트워크(WBAN)를 위한 실용적인 인증 시스템

정회원 안 해 순*, 종신회원 윤 은 준**, 정회원 부 기 동***°

A Practical Authentication System for Wireless Body Area Networks(WBAN)

Hae-Soon Ahn* *Regular Member*, Eun-Jun Yoon** *Lifelong Member*,
Ki-Dong Bu***° *Regular Member*

요 약

본 논문에서는 U-헬스케어 의료 정보 환경을 위한 무선 인체 영역 네트워크(WBAN) 기반의 실용적인 인증 시스템을 제안한다. 제안한 인증 시스템은 AES와 같은 대칭키 암호 시스템을 기반으로 동작하며 데이터 기밀성, 데이터 인증, 데이터 무결성 등의 보안성을 보장할 뿐만 아니라 타임스탬프 기술을 적용하여 재전송 공격 방지 및 센서 노드, 마스터 노드, 베이스 스테이션, 의료 서버 사이에 안전한 인증을 수행하도록 설계하였다.

Key Words : WBAN, Authentication, Wireless Body Area Networks, U-healthcare, Replay attack

ABSTRACT

In this paper, we propose a practical authentication system based on Wireless Body Area Networks(WBAN) for U-healthcare medical information environments. The proposed authentication system is based on symmetric cryptosystem such as AES and is designed to not only provide security such as data secrecy, data authentication, data integrity, but also prevent replay attack by adopting timestamp technique and perform secure authentication between sensor node, master node, base-station, and medical server.

Ⅰ. 서 론

무선 인체 영역 네트워크를 의미하는 WBAN(Wireless Body Area Network) 기술은 인체에서 3m 이내의 착용 또는 체내에 이식된 장치들 간의 무선 네트워킹 기술을 의미한다[1,2]. WBAN 기술은 인체의 내부 및 외부에서 여러 가지 용도에 따라 다양한 서비스를 제공할 수 있으므로 인간과 가장 가까운 환경에서 구현되는 네트워크 기술이다. 차세대 컴퓨팅, 입는 컴퓨터인 Wearable Computing의 핵심 네트워킹 기술, IT와 BT의 융합에 의한 U-HealthCare 요구 등으로 인해 WBAN 기술이 등장하게 되었다. WBAN은 기존 무선 개인 통신망(WPAN: Wireless Personal Area Network) 표준인 IEEE 802.15과 비교하여 초저전력의 전력소모 보장, 초저가 및 초소형 전력원 이용, 응용에 따른 지연 보장 요구사항, 별도로 승인된 주파수 대역 활용, 무선과 인체 인터페이스 매체 활용 등의 특징을 가진다[3,4]. WBAN은 용도에 따라 의료용과 비의료용으로 구분된

* 대구대학교 기초교육원 컴퓨터과정(ahs221@hanmail.net),
** 경일대학교 사이버보안학과(ejyoon@kiu.ac.kr),
*** 경일대학교 컴퓨터공학과(kdbu@kiu.ac.kr) (° : 교신저자)
논문번호 : KICS2012-01-042, 접수일자 : 2012년 1월 31일, 최종논문접수일자 : 2012년 4월 6일

다. 의료용은 심전도, 근전도, 내시경 등이 있고, 비의료용은 운동, Wearable Computer, 주변기기 등이 있다. 특히, 의료 분야에서는 환자의 건강상태를 감지하고 지속적으로 상황을 파악할 수 있는 체내 건강상태 모니터링을 통해 인체에 이상이 발생하였을 경우 무선으로 데이터를 전송할 수 있다[5]. 장착유형별로는 인간의 이동성, 동작에 관심이 있는 장착형과 인체조직의 특수성 고려, 의료용 MICS 대역 형태의 이식형으로 구분한다. WBAN의 응용분야는 의료, 운동기기, 디지털 가전, Motion Capture, 게임 등 다양하다. 특히 WBAN은 인체에 영향을 미칠 수 있으므로 전자파의 적합성을 의미하는 EMC(Electro Magnetic Compatibility) 및 흡수율을 의미하는 SAR(Specific Absorption Rate)의 안전성을 반드시 고려해야 한다. 게다가 해킹시 생명을 위협하는 문제가 발생할 수 있기 때문에 암호화 및 인증 기술을 기반으로 신뢰성 확보가 반드시 고려되어야 한다[6-10]. 또한, 저전력 환경을 고려한 배터리 기술, 절전 기술 개발 등이 필요하다. 현재 국제적으로 IEEE 802.15.6 TG 승인 및 PHY/MAC 표준화 연구가 진행 중이며 국내 TTA에서는 Project Group 317을 신설하여 표준화 수행 및 기업체, 연구소에서 PHY/MAC와 응용서비스 연구가 진행 중이다[11-16].

2009년에 Tan등은 WBAN을 위한 ID기반 암호시스템인 IBE-Lite를 제안하였다[17]. Tan등이 제안한 기법은 공개키 암호 알고리즘을 기반으로 함으로 효율성이 낮은 단점을 가진다. 또한 최근 Cornelius등은 WBAN에 적용 가능한 생체정보와 난수를 이용한 비밀키를 활용한 데이터 기반 인증 기법을 소개하였지만 구체적인 인증 기법은 제안하지 않았다[18].

따라서 본 논문에서는 U-헬스케어 의료 정보 환경을 위한 WBAN 기반 인증 시스템을 제안한다. 제안한 인증 시스템은 다음과 같은 특징을 가진다. (1) AES와 같은 대칭키 암호 시스템을 기반으로 동작한다. (2) 데이터 기밀성, 데이터 인증, 데이터 무결성 등을 보장한다. (3) 타임스탬프 기술을 적용하여 재전송 공격 보호 및 센서 노드, 마스터 노드, 베이스 스테이션, 의료 서버 사이에 안전한 인증을 수행한다.

본 논문의 구성은 다음과 같다. 2장에서는 WBAN 시스템 환경에 대해서 살펴보고, 3장에서는 제안한 WBAN 기반 인증 스킴에 대해 설명한다. 그리고 4장에서는 제안한 인증 스킴에 대한 안전성과 효율성을 분석하고, 5장에서는 본 논문의 결론을 맺는다.

Ⅱ. WBAN 시스템 환경

2.1. 무선 인체 영역 네트워크(WBAN) 구조

WBAN은 인체와 인간의 이동을 모니터링하기 위해 인체 또는 주위의 센서 노드 간의 통신에 사용되는 무선 네트워크이다. 일반적으로 WBAN의 센서 노드는 인체에서 신호의 정확한 감지를 위해 센서 신호의 낮은 수준의 프로세싱을 수행하고, 무선 로컬 처리 장치로 처리된 신호를 전송해야 한다[3-5].

그림 1은 WBAN 네트워크 구조를 보여주고 있다[4]. 그림 1과 같이 WBAN 네트워크 구조는 의료 환자의 상태 정보를 다양한 통신 기기를 기반으로 네트워크를 통해 의료 종사자들에게 전송 및 활용된다. 이때, WBAN의 보안은 환자 개인의 중요한 데이터를 보장하고 보호하기 위해 매우 중요하다. 그리고 인체에서의 센서 신호는 안전하고 제한적으로 액세스할 수 있어야 하며, 어떤 한 사람의 센서 신호가 다른 사람의 센서 신호와 절대로 혼합되어서는 안된다. 결국 WBAN이 WLAN 등과 같은 다른 네트워크와 구별되는 가장 큰 특징 중 하나는 의료용 장치로서 사용되거나 인체에 이식되는 장치로 응용 및 활용된다는 점이다. 최근 기술의 발달과 고령화 사회로 인해 전 세계적으로 인간의 의료용 이식 장치에 더욱 많이 의존하고 있는 상황이다.

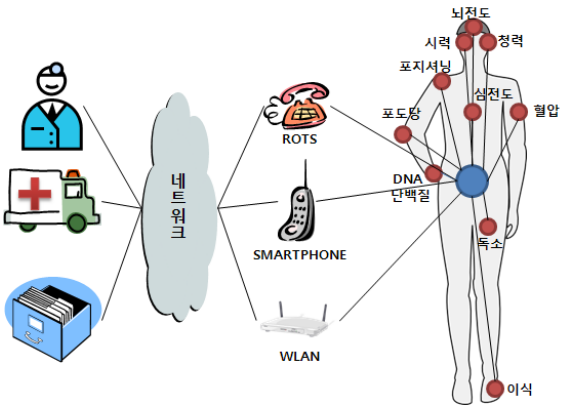

그림 1. 무선 인체 영역 네트워크 구조
Fig. 1. Architecture of Wireless Body Area Network

2.2. U-헬스케어 WBAN 기반 네트워크 구조

그림 2는 제안하는 U-헬스케어 의료 정보 환경을 위한 WBAN 기반 네트워크 구조를 보여주고 있다[1-6]. 의료 환자의 인체에는 센서 노드와 마스터 노드가 설치되며 센서 노드가 전송하는 센싱 데이터를 마스터 노드가 획득하여 베이스 스테이션을 통해 의사, 인가된 사용자, 그리고 의료 서버에 전송되어 활용된다. 여기서 마스터 노드는 의료 직원과 같이 제

한된 사용자 가 액세스할 수 있는 권한이 있는 서버에 무선 또는 유선으로 보안 연결되어 인체에서 센서 신호는 안전하고 제한적으로 액세스할 수 있어야 한다. 일반적으로 의료 서버는 병원 내부에 위치하고 있으며 여러 WBAN들이 동시에 지정된 서버에 연결되어 사용되며, 서버는 무선 센서 ID 및 해당키를 안전하게 저장하고 있다.

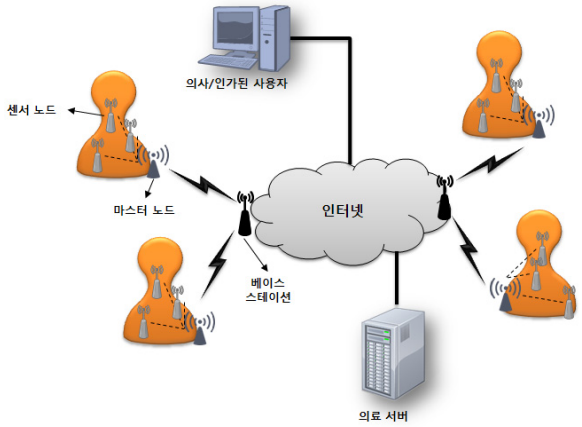

그림 2. WBAN 기반 의료 정보 네트워크 구조
Fig. 2. WBAN based Medical Information Network

의료 정보 환경을 위한 WBAN 기반 네트워크상에서 무선 센서로 메시지를 송신하거나 다른 무선 센서로부터 메시지를 수신할 경우 데이터 인증, 데이터 기밀성, 데이터 무결성을 제공하고, 재전송 공격에 안전한 보안성을 제공해야 한다. 데이터 인증은 안전한 인증 프로토콜을 통해 이루어져야 하고, 비밀키를 공유하여 복호화된 메시지와 통신할 수 있기 때문에 암호화 알고리즘을 통해 공격자들의 접근으로부터 메시지를 보호함으로써 데이터 기밀성을 제공한다. 또한, 공격자에 의해 수행되는 메시지 변경을 방지하고 WSN에서 전송된 메시지가 유효하지 않은 사용자에 의해 조작되지 않았음을 보장하는 데이터 무결성을 제공해야 한다. 그리고 무선 통신 네트워크를 사용하기 때문에 메시지를 수신할 때 증명자와 검증자가 각각 메시지 검증을 통해 인증에 성공함으로써 재전송 공격에도 안전해야 한다.

Ⅲ. 제안하는 WBAN 기반 인증 스킴

본 장에서는 U-헬스케어 의료 정보 환경을 위한 WBAN 기반 인증 스킴을 제안한다. 제안하는 인증 스킴은 AES와 같은 안전한 대칭키 암복호화 알고리즘과 재전송 공격 방어를 위해 타임스탬프 기법을 적용하여 설계하였다[14-16]. 또한 메시지 인증 코드(MAC)를 활용하여 의료 서버가 WBAN 환경에 구축된 환자의 센서가 송신하는 정보를 안전하게 검증 및 활용하도록 설계하였다. 표 1은 본 논문에서 사용되는 시스템 파라미터들을 보여준다.

표 1. 시스템 파라미터
Table. 1. System Parameters

기호	의미
ID_S, ID_M, ID_B	센서노드, 마스터노드, 베이스스테이션 식별자
K_{ms}	마스터 노드와 센서 노드 간 공유 비밀키
K_{ss}	의료 서버와 센서 노드 간 공유 비밀키
K_{bm}	베이스 스테이션과 마스터 노드 간 공유 비밀키
K_{sb}	의료 서버와 베이스 스테이션 간 공유 비밀키
$E(), D()$	AES 대칭키 기반 암호화 및 복호화 함수
T_S	센서 노드가 생성한 타임스탬프 (timestamp)
$h()$	일방향 해쉬 함수(one-way hash function)
$A \rightarrow B : X$	X가 A에서 B로 전송

3.1. 시스템 설정 과정

의료 서버는 센서 노드 등록 및 인증을 위해 각 센서 노드를 위한 공유 비밀키 K_{ss}와 마스터 노드와의 비밀 통신을 위한 공유 비밀키 K_{ms}를 생성하여 해당 센서 노드에 저장한 후 U-헬스케어 응용 환경에 맞게 적절한 의료 환경 위치에 배치한다. 제안한 시스템에서 공유 비밀키 생성은 Zhang 등[19]이 제안한 빠른 비밀 키 생성 기법을 기반으로 생성되며 분배 방법은 사전에 약속된 안전한 통신 채널을 통해 의료 서버에 의해 비밀 키 분배가 이루어짐을 가정한다.

3.2. 인증 수행 과정

그림 3과 같이 본 논문에서 제안하는 인증 스킴에서 센서 노드가 발생한 센싱 데이터를 마스터 노드 및 베이스 스테이션의 도움을 통해 의료 서버가 안전하게 인증 및 활용할 수 있도록 다음과 같은 과정을 수행한다.

(1) 마스터 노드 → 센서 노드: *Query*
마스터 노드는 센서 노드가 수집한 센싱 데이터를 수집하기 위해 센서 노드에게 *Query*

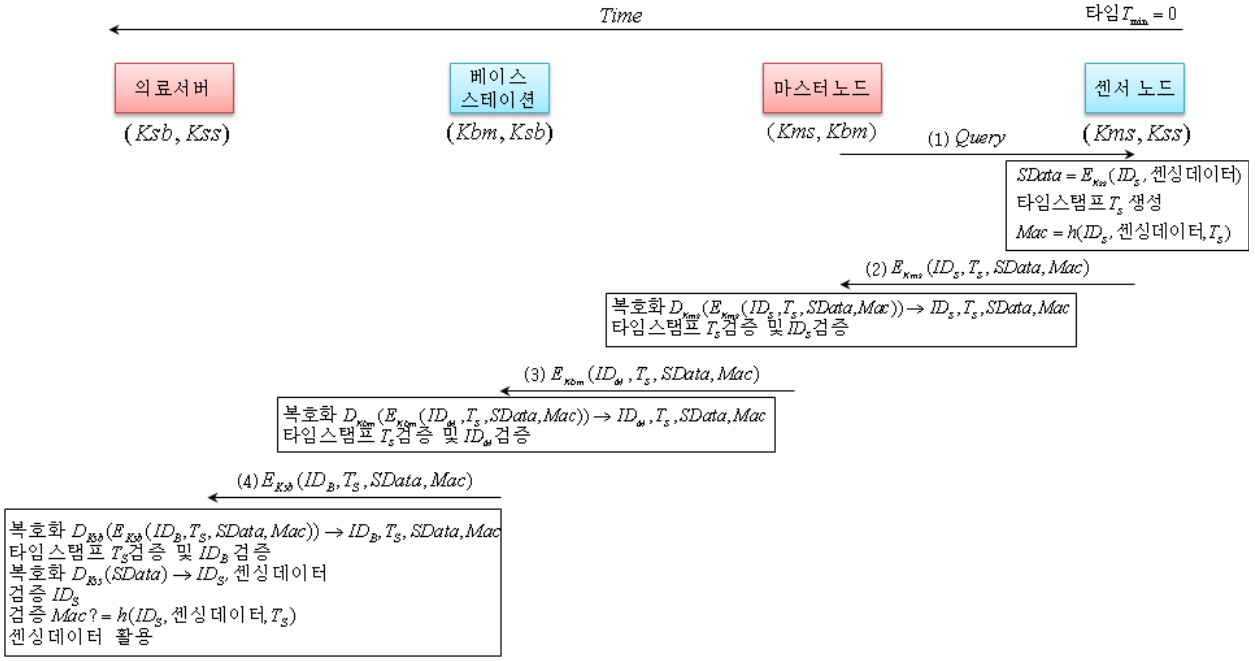

그림 3. 제안하는 WBAN 기반 인증 스킴
Fig. 3. Proposed WBAN based Authentication Scheme

를 보낸다.

(2) 센서 노드 → 마스터 노드:
$E_{Kms}(ID_S, T_S, SData, Mac)$
센서 노드는 자신의 식별자 ID_S와 센싱 데이터를 의료 서버와의 공유 비밀키 K_{ss}를 이용하여 암호화 한다. 타임스탬프 T_S를 생성한 후 메시지 인증 코드 값인 $Mac = h(ID_S$, 센싱데이터, $T_S)$을 계산하여 마스터 노드와의 비밀키인 K_{ms}를 이용하여 암호화 한 $E_{Kms}(ID_S, T_S, SData, Mac)$ 메시지를 마스터 노드에게 전송한다.

(3) 마스터 노드 → 베이스 스테이션:
$E_{Kbm}(ID_M, T_S, SData, Mac)$
$E_{Kms}(ID_S, T_S, SData, Mac)$를 수신한 마스터 노드는 센서 노드와의 공유 비밀키인 K_{ms}를 이용하여 복호화하여 ID_S, T_S, $SData$, Mac을 각각 얻는다. 마스터 노드는 먼저 타임스탬프 T_S의 유효성을 $(T_M - T_S) \leq \Delta T_{MS}$와 같이 검증하여 재전송 공격여부를 판단한다. 타임스탬프 검증 과정에서 T_M는 메시지를 수신한 시간을 나타내며, ΔT_{MS}는 유효 시간 범위를 의미한다. T_S가 유효하면 ID_S 검증을 통해 자신이 관리하고 있는 센서 노드인지를 검증한다. 식별자 검증이 성공되면 베이스 스테이션과 공유된 비밀키 K_{bm}을 이용하여 $E_{Kbm}(ID_M, T_S, SData, Mac)$ 메시지를 생성하여 베이스 스테이션에게 전송한다.

(4) 베이스 스테이션 → 의료 서버:
$E_{Ksb}(ID_B, T_S, SData, Mac)$
$E_{Kbm}(ID_M, T_S, SData, Mac)$를 수신한 베이스 스테이션은 마스터 노드와의 공유 비밀키인 K_{bm}를 가지고 복호화하여 ID_M, T_S, $SData$, Mac 값을 각각 얻는다. 베이스 스테이션은 먼저 타임스탬프 T_S의 유효성을 $(T_B - T_S) \leq \Delta T_{BM}$와 같이 검증하여 재전송 공격여부를 판단한다. 타임스탬프 검증 과정에서 T_B는 메시지를 수신한 시간을 나타내며, ΔT_{BS}는 유효 시간 범위를 의미한다. T_S가 유효하면 ID_M 검증을 통해 자신이 관리하고 있는 마스터 노드인지를 검증한다. 식별자 검증에 성공하면 의료 서버와 공유된 비밀키 K_{sb}를 이용하여 $E_{Ksb}(ID_B, T_S, SData, Mac)$ 메시지 생성 후 의료 서버에게 전송한다.

(5) 의료 서버의 검증
$E_{Ksb}(ID_B, T_S, SData, Mac)$를 수신한 사용자

의료 서버는 베이스 스테이션과의 공유 비밀키인 K_{sb}를 가지고 복호화하여 ID_B, T_S, $SData$, Mac 값을 각각 얻는다. 의료 서버는 먼저 타임스탬프 T_S의 유효성을 $(T_{SB} - T_S) \leq \Delta T_{SB}$와 같이 검증하여 재전송 공격여부를 판단한다. 타임스탬프 검증 과정에서 T_{SB}는 메시지를 수신한 시간을 나타내며, ΔT_{SB}는 유효 시간 범위를 의미한다. T_S가 유효하면 ID_B 검증을 통해 자신이 관리하고 있는 베이스 스테이션인지를 검증한다. 식별자 검증에 성공하면 의료 서버는 센서 노드와 공유된 비밀키 K_{ss}를 이용하여 $SData$를 복호화하여 ID_S와 센싱 데이터를 얻은 후 MAC 기반의 해쉬 인증 값 $h(ID_S, \text{센싱데이터}, T_S)$을 계산한 후 수신한 Mac과 동일한지를 검증한다. 만약 $Mac \equiv h(ID_S, \text{센싱데이터}, T_S)$이면 의료 서버는 센서 노드에 대한 인증을 성공적으로 수행하게 되어 획득한 센싱 데이터 정보를 목적에 맞게 활용한다.

Ⅳ. 보안성 분석

본 장에서는 제안한 U-헬스케어 의료 정보 환경을 위한 WBAN 기반 인증 스킴의 수행 과정에서 의료 서버, 베이스 스테이션, 마스터 노드, 그리고 센서 노드에 대한 안전성과 효율성에 대해 살펴본다[12].

4.1 안전성 분석

본 논문에서 제안한 인증 스킴은 그림 1과 2의 WBAN 기반 의료 정보 시스템에 그림 3의 제안한 AES 대칭키 기반의 인증 스킴의 적용으로 인해 해커 또는 악의적인 공격자가 비록 송수신 메시지를 도청하더라도 재전송 공격(replay attack), 위장 공격(impersonation attack), 메시지 기밀성 파괴 공격 등에 안전할 뿐만 아니라 의료 서버, 베이스 스테이션 및 마스터 노드가 센서 노드를 안전하게 인증할 수 있으므로 다양한 암호학적 및 네트워크 보안 공격들에 대해 안전하다.

표 2에서는 제안한 스킴의 안전성을 분석한 결과로 대칭키 기반의 안전한 데이터 인증을 제공하며, MAC과 암호화 알고리즘을 이용하여 송수신 메시지에 대한 기밀성과 무결성을 보장한다. 또한 타임스탬프 기법을 적용하여 공격자에 의한 재전송 공격에도 안전한다.

표 2. 제안한 스킴의 안전성
Table. 2. Security of Proposed Scheme

보안성	제안스킴
데이터 인증	안전함
데이터 기밀성	제공함
데이터 무결성	제공함
재전송 공격	안전함

(1) 데이터 인증(data authentication): 제안한 스킴의 인증 단계 (2)~(5)에서 AES 대칭키 기반의 암호화 및 복호화하여 인증 과정을 수행하므로 의료 서버, 베이스 스테이션 및 마스터 노드가 센서 노드에 대해 안전한 데이터 인증을 제공한다.

(2) 데이터 기밀성(data confidentiality): 무선 경로상의 통신은 공격자의 엿보기 또는 도청 공격이 쉽게 이루어진다. 따라서 본 논문에서는 공유된 비밀키를 사용한 AES 기반의 암호화를 통해 안전한 데이터 인증을 수행한다. 또한 비밀키를 공유하여 복호화된 메시지와 통신할 수 있기 때문에 암호화 알고리즘을 통해 공격자들의 접근으로부터 메시지를 보호함으로써 데이터 기밀성을 제공한다.

(3) 데이터 무결성(data integrity): 제안 스킴에서는 공격자에 의해 수행되는 메시지 변경을 방지하고 WSN에서 전송된 메시지가 유효하지 않은 사용자에 의해 조작되지 않았음을 보장하는 데이터 무결성을 제공함을 알 수 있다.

(4) 재전송 공격(replay attack): 재전송 공격은 수동적인 공격 유형으로 과거 세션에서 도청한 통신 메시지를 이용하여 현재 또는 미래 세션에서 임의의 통신 당사자로 위장하여 도청한 메시지를 재전송하여 통신 상대방으로부터 인증을 성공적으로 받게 되는 공격이다. 제안한 스킴은 (3)~(5) 인증 단계에서 마스터 노드, 베이스 스테이션, 의료 서버가 각각 수신한 타임스탬프 T_S의 유효성을 검증하여 재전송 공격여부를 판단한다. 유효성 검증을 통해 타임스탬프 T_S가 유효하면 자신이 관리하고 있는 비밀 식별자 값을 각각 검증하게 된다. 이때 식별자 검증을 통과해야만 각 통신 당사자는 공유된 비밀키를 이용하여 메시지 생성 후 전송한다. 또한, 제안한 인증 기법에서는 AES 대칭키 기반의 인증 스킴의 적용으로 인해 해커

또는 악의적인 공격자가 비록 송수신 메시지를 도청하더라도 재전송 공격, 위장 공격, 메시지 기밀성 파괴 공격 등에 안전함을 알 수 있다.

표 3. 제안한 스킴의 연산 효율성
Table. 3. Computational Efficiency of Proposed Scheme

	의료서버	베이스 스테이션	마스터 노드	센서 노드
대칭키 암호화	0	1	1	2
대칭키 복호화	2	1	1	0
MAC 연산	1	0	0	1
통신 라운드 수	4			

4.2 효율성 분석

표 3에서는 제안한 스킴의 효율성을 분석할 결과를 보여준다. 제안한 스킴에서 의료 환자의 몸에 부착된 개별 센서노드는 2번의 대칭키 암호화 연산과 1번의 MAC 연산을 수행하며, 센서노드가 송신하는 정보를 수집 및 전송하는 마스터 노드는 1번의 대칭키 암호화 연산과 1번의 대칭키 복호화 연산 수행하며, 마스터 노드가 송신하는 정보를 수신하여 의료 서버에게 전송하는 베이스 스테이션 또한 1번의 대칭키 암호화 연산과 1번의 대칭키 복호화 연산 수행하며, 최종 인증을 수행하는 의료 서버는 2번의 대칭키 복호화 연산 수행과 1번의 MAC 연산을 수행하여 센서노드를 인증하게 된다. 최근 RFID나 센서네트워크 환경에 적용 가능한 경량 대칭키 및 공개키 암호 알고리즘의 개발로 제안한 스킴에서 센서 노드가 수행하는 대칭키 암복호화 연산은 1~2회만 요구됨으로 효율적인 인증을 수행할 수 있다[14-16].

V. 결 론

본 논문에서는 U-헬스케어 의료 정보 환경을 위한 무선 인체 영역 네트워크(WBAN) 기반의 실용적인 인증 시스템을 제안하였다. 제안한 인증 시스템은 AES와 같은 대칭키 암호 시스템을 기반으로 동작하며 데이터 기밀성, 데이터 인증, 데이터 무결성 등의 보안성을 보장할 뿐만 아니라 타임스탬프 기술을 적용하여 재전송 공격 방지 및 센서 노드, 마스터 노드, 베이스 스테이션, 의료 서버 사이에 안전한 인증을 수행하도록 설계하였다.

참 고 문 헌

[1] K. Van Dam, S. Pitchers, and M. Barnard, “Body area networks: Towards a wearable future,” in Proceedings of WWRF kick off meeting,, March 2001.

[2] L. Benoit, B. Braem, I. Moerman, C. Blondia, and P. Demeester, “A survey on wireless body area networks,” Wireless Networks, pp. 1.18, 2010.

[3] H. S. Lee, “WBAN Frequency Distribution Trends and Frequency Band Proposition”, Korea Information and Communication Society, vol. 25(2), February 2008, pp.6-10.

[4] Georgios Selimis et al, “A Lightweight Security Scheme for Wireless Body Area Networks: Design”, Energy Evaluation and Proposed Microprocessor Design, Journal of Medical Systems, vol. 35(5), 2011, pp. 1289-1298.

[5] H. Li and J. Tan, “An ultra-low-power medium access control protocol for body sensor network,” in Engineering in Medicine and Biology Society, 2005, pp. 2451-2454.

[6] F. Shu et al, IMEC UWB MAC Proposal for IEEE 802.15.6, 2009.

[7] Sana Ullah, Henry Higgins, Bart Braem, Benoit Latre, Chris Blondia, Ingrid Moerman, Shahnaz Saleem, Ziaur Rahman, Kyung Kwak, “A Comprehensive Survey of Wireless Body Area Networks”, Journal of Medical Systems, pp. 1-30, (2010).

[8] E. Jovanov et al., “A Wireless Body Area Network of Intelligent Motion Sensors for Computer Assisted Physical Rehabilitation,” J. NeuroEng. and Rehab., vol. 2, no. 11, Mar. 2005, p. 6.

[9] U. Uludag et al., “Biometric Cryptosystems: Issues and Challenges,” Proc. IEEE, vol. 92, no. 6, June 2004, pp. 948.60.

[10] S. D. Bao, Y. T. Zhang, and L. F. Shen, “A New Symmetric Cryptosystem of Body Area Sensor Networks for Telemedicine,” Proc. 6th Asian-Pacific Conf. Med. and Bio. Eng., Japan, Apr. 2005.

[11] CY Poon et al, “A Novel Biometrics Method to

Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health", IEEE Communications Magazine, pp. 73-81, (2006).

[12] H. S. Ng, M. L. Sim, and C. M. Tan, "Security issues of wireless sensor networks in healthcare applications," BT Technology Journal, vol. 24, no. 2, pp. 138-144, 2006.

[13] D. Singelee, B. Latre, B. Braem, M. Peeters, M. D. Soete, P. D. Cleyn, B. Preneel, I. Moerman, and C. Blondia, "A secure low-delay protocol for multi-hop wireless body area networks," Ad-hoc, Mobile and Wireless Networks, pp. 94-107, Sep. 20, 2008.

[14] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the limits of elliptic curve cryptography in sensor networks," Proceedings of the 5th European conference on Wireless Sensor Networks, LNCS 4913, pp. 305-320, Springer-Verlag, 2008.

[15] L. Uhsadel, A. Poschmann, and C. Paar, "Enabling full-size public- key algorithms on 8-bit sensor nodes," Proceedings of European Workshop on Security in Ad-Hoc and Sensor Networks, LNCS 4572, pp. 73-86, Springer-Verlag, 2007.

[16] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," IEEE Conference on Computer Communications Workshops, pp. 1-6, 2008.

[17] Chiu C. Tan, Haodong Wang, Sheng Zhong, and Qun Li. IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks. IEEE Transactions on Information Technology in Biomedicine, 13(6):926.932, November 2009.

[18] C. Cornelius and D. Kotz, "On usable authentication for wireless body area networks," In USENIX Workshop on Health Security (HealthSec), August, 2010.

[19] G. H. Zhang, Carmen C. Y. Poon, Member, IEEE, and Y. T. Zhang, "A fast key generation method based on dynamic biometrics to secure wireless body sensor networks for p-health," Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE, pp. 2034-2036, 2010.

안 해 순 (Hae-Soon Ahn) 정회원

1996년 2월 경일대학교 컴퓨터공학과(공학사)
2001년 경일대학교 컴퓨터공학과(공학석사)
2010년 대구대학교 컴퓨터정보공학과(공학박사)
2004년~2008년 경일대학교 컴퓨터공학부 전임강사
2008년~현재 대구대학교 기초교육원 컴퓨터과정 초빙교수
<관심분야> 데이터베이스, 정보보안, 정보검색, 데이터베이스 보안, RFID 보안

윤 은 준 (Eun-Jun Yoon) 종신회원

2003년 경일대학교 컴퓨터공학과(공학석사)
2007년 경북대학교 컴퓨터공학과(공학박사)
2007년~2008년 대구산업정보대학 컴퓨터정보계열 전임강사
2008년~2011년 경북대학교 전자전기컴퓨터학부 계약교수
2011년~현재 경일대학교 사이버보안학과 조교수
<관심분야> 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피

부 기 동 (Ki-Dong Bu) 정회원

1984년 경북대학교 전자공학과(공학사)
1988년 경북대학교 전자공학과(공학석사)
1996년 경북대학교 전자공학과(공학박사)
1983년~1985년 포항종합제철 시스템개발실
2001년~2002년 일본 게이오대학 방문교수
1988년~현재 경일대학교 컴퓨터공학과 교수
<관심분야> 데이터베이스, GIS, 시멘틱 웹, 데이터베이스 보안, RFID 보안