2013년 10월 전자공학회 논문지 제 50 권 제 10 호
Journal of The Institute of Electronics Engineers of Korea Vol. 50, NO. 10, October 2013 http://dx.doi.org/10.5573/ieek.2013.50.10.107

논문 2013-50-10-12

개선된 RFID 기술을 이용한 u-헬스케어 서비스 인증 프로토콜

(Improved u-Healthcare Service Authentication Protocol based on RFID Technology)

안 해 순*, 윤 은 준**, 부 기 동***

(Hae-Soon Ahn, Eun-Jun Yoon, and Ki-Dong Bu©)

요 약

최근 RFID 기술은 u-헬스케어 서비스와 접목되어 의료서비스 분야에서 주목 받고 있는 추세이다. u-헬스케어 서비스는 개인 의료 정보를 다루는 분야로서 단순한 건강 검진 및 치료의 수준을 넘어 생명과도 밀접한 관계가 있다. 만약 개인 의료 정보가 불법적으로 노출되거나 악용될 경우 프라이버시 침해 뿐만아니라 생명까지도 위협받을 수 있으므로 보안성을 고려한 u-헬스케어 서비스 인증이 필수적으로 요구된다. 2012년에 Jeong 등은 RFID 기술을 이용하여 초기화 과정과 환자 인증 과정을 구분한 J-L 환자 인증 프로토콜을 제안하였다. Jeong등은 제안한 프로토콜에서 재사용 공격, 스푸핑 공격, 정보노출방지 및 불추적성에 대해 안전하다고 주장하였지만 보안성과 연산 효율성 문제를 발생시킨다. 따라서 본 논문에서는 Jeong 등이 제안한 프로토콜의 보안성과 연산 효율성 문제를 증명하고, 안전성과 효율성을 강화한 RFID 기술의 기반으로 하는 실용적인 u-헬스케어 서비스 인증 프로토콜을 제안한다.

Abstract

Recently, the RFID technology is combined with a u-healthcare services is an emerging trend in the field of medical services. u-healthcare service, as covering the field of personal health information beyond the level of simple health screening and treatment of life are closely related. Considering security, invasion of privacy, as well as life may be threatened even if your personal health information to be exposed or exploited illegally u-Healthcare services certification is essential. In 2012, Jeong proposed J-L patient authentication protocol that Initialization process, and patients using RFID technology separates the certification process. Jeong, such as the claim that the proposed protocol for reuse attacks, spoofing attacks, prevent information disclosure and traceability fire safety, but raises issues of security and operations efficiency. Therefore, in this paper, Jeong, such as the security of the proposed protocol and to prove the computational efficiency issues, and to enhance the safety and efficiency of RFID technology based on practical u-Healthcare services authentication protocol is proposed.

Keywords : RFID, u-Healthcare, mutual authentication protocol, attacks

* 정회원, 대구대학교 기초교육원
(College of General Education, Daegu University)
** 정회원, 경일대학교 사이버보안학과
(Dept. of Cyber Security, Kyungil University)
*** 정회원, 경일대학교 컴퓨터공학과
(Dept. of Computer Engineering, Kyungil University)
© Corresponding Author(E-mail: kdbu@kiu.ac..kr)
※ 본 연구는 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No. 2010-0010106)과 2013년도 미래창조과학부 및 정보통신산업진흥원의 대학IT연구센터육성 지원사업의 연구결과로 수행되었음(NIPA-2013-H0301-13-2004)
접수일자: 2013년4월29일, 수정완료일: 2013년9월26일

Ⅰ. 서 론

언제 어디서나 서비스 이용이 가능한 유비쿼터스 컴퓨팅 기술의 등장과 건강한 삶을 유지하고자 하는 현대인들의 욕구 및 의료 기술의 발전으로 인해 유비쿼터스 헬스케어(이하 u-헬스케어) 서비스가 등장하였다[1-2]. 따라서 u-헬스케어 서비스는 환자가 병원에 오지 않더라도 환자의 건강관련 정보를 시간과 장소에 구애받지 않고 안정된 유무선 네트워크를 통해 환자가 생활 공간속에서 자신의 건강을 체크하고 다양한 의료 서비스를 받을 수 있다. 이러한 u-헬스케어 서비스는 바이오 센서 및 의료기기의 발달로 더욱 가속화 되고 있다. 대표적인 u-헬스케어 서비스로는 원격진료, 의료정보 온라인 제공, 모바일 건강 관리 및 질병 모니터링 등으로써 환자의 질병을 체크하고 치료할 수 있는 의료서비스로 관심이 증가되고 있는 추세이다[3-5]. 또한 무선 인체 영역 네트워크를 의미하는 WBAN(Wireless Body Area Network) 기술 및 전자 처방 기록, 전자 처방전, 진단 정보 시스템 등을 포함한 통합 의료 정보 시스템등의 연구도 활발하다. WBAN 기술은 인체의 내부 및 외부에서 용도에 따라 다양한 의료 서비스를 제공할 수 있으므로 헬스케어와 관련된 많은 연구가 지속적으로 이루어지고 있다[6~8].

무엇보다 유비쿼터스 환경의 가장 핵심적인 기술인 RFID는 빠른 인식 속도 및 반영구성의 장점을 가지고 있으므로 u-헬스케어에서 실용적으로 사용된다. 그러나 u-헬스케어 기술의 발전은 다양한 편의성과 의료 서비스를 제공하지만 이에 따른 개인의 정보가 노출 및 프라이버시 침해의 우려가 발생할 수 있다. RFID 태그에 저장되어 있는 정보를 리더의 신호에 의해 노출되어 도청, 트래픽 분석, 데이터 위조 및 변조 등의 보안 공격들에 취약하다. 특히 의료 정보를 다루는 분야이므로 환자에 대한 단순한 진료가 아니라 생명과도 밀접한 관계가 있기 때문에 무엇보다 안전한 개인 의료 정보 공유 및 인증 방법이 중요하다. 그러므로 RFID 기술을 이용한 u-헬스케어 서비스 인증 프로토콜에 대한 연구가 암호학적 접근 방법인 해시 함수, 공개키 암호화, 대칭키 암호화 등을 기반으로 최근 활발히 진행되고 있다[9~10]. u-헬스케어 서비스 환경에서 가장 중요한 것은 프라이버시를 제공하는 것이므로 서비스 인증, 기밀성, 무결성, 통신로 보안, 효율성 등의 보안 요구 사항을 만족해야 한다.

최근 Jeong[11]등은 RFID 기술을 이용하여 초기화 과정과 환자 인증 과정을 구분한 J-L 환자 인증 프로토콜을 제안하였다. Jeong등은 제안한 프로토콜에서 재사용 공격, 스푸핑 공격, 정보노출방지 및 불추적성에 대해 안전하다고 주장하였지만 보안성과 연산 효율성 문제를 발생시킨다. 따라서 본 논문에서는 Jeong 등이 제안한 프로토콜의 보안성과 연산 효율성 문제를 증명하고, 안전성과 효율성을 강화한 RFID 기술의 기반으로 하는 실용적인 u-헬스케어 서비스 인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 J-L 환자 인증 프로토콜을 간단히 설명하고, Ⅲ장에서는 Jeong[11] 등이 제안한 J-L 환자 인증 프로토콜에 대한 보안성에 대해 분석한다. Ⅳ장에서는 안전성을 강화하고 효율성을 높인 RFID 기술 기반의 u-헬스케어 서비스 인증 프로토콜을 제안하고, Ⅴ장에서는 안전성과 효율성에 대해 각각 검증한다. 마지막 Ⅵ장에서는 본 논문의 결론을 맺는다.

Ⅱ. J-L 환자 인증 프로토콜 소개

최근 u-헬스케어 서비스와 관련된 다양한 정보보호 기술에 대한 연구가 활발히 진행되고 있다[12-15]. u-헬스케어 서비스는 환자 개인의 정보 및 프라이버시 보호와 관련된 다양한 보안 취약점과 위협요소들이 존재하기 때문에 안전성을 보장하는 서비스 인증 프로토콜 개발이 필수적이다. 최근 Jeong[11]등은 RFID 기술을 이용하여 초기화 과정과 환자 인증 과정을 구분한 환자 인증 프로토콜을 제안하였다. 따라서 본 장에서는 Jeong 등이 제안한 J-L 환자 인증 프로토콜의 전체적인 수행 과정을 살

표 1. 용어 정의
Table 1. Notations.

기호	의 미
SN	태그의 시리얼 번호
ID_P	환자의 인식자
K_{HT}	리더와 태그의 사전 공유키
SID	SN과 대응되는 랜덤하게 생성된 보안 인식자
R_H	리더가 생성한 랜덤 값
$h(.)$	일방향 해쉬함수
$E(.), D(.)$	대칭키 알고리즘
R_T	환자(태그)가 생성한 랜덤 값
I	현재 세션의 통신 연결 상태 정보
SK	세션키
K_{DB-H}	리더와 데이터베이스간 공유키
$\|$	연접(Concatenation) 연산

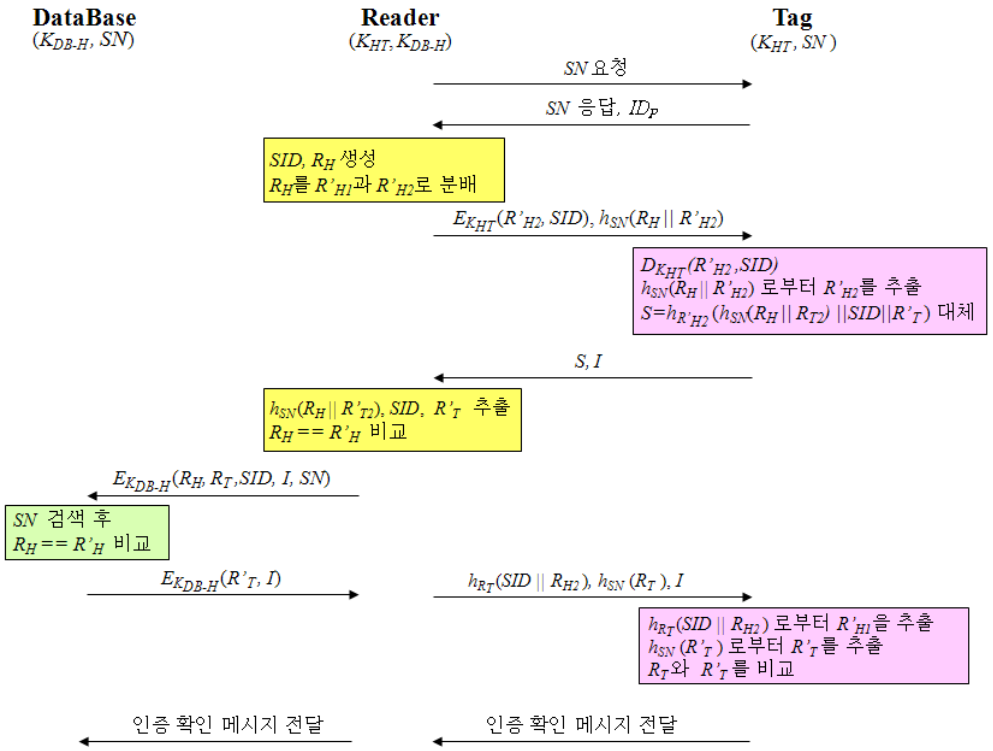

그림 1. J-L 환자 인증 프로토콜
Fig. 1. J-L Patient Authentication protocol.

펴본다. 본 논문에서 사용할 용어들의 표기법 및 정의는 표 1과 같다.

그림 1은 Jeong등이 제안한 J-L 환자 인증 프로토콜을 보여주며 다음과 같이 동작한다. 리더와 태그는 사전에 메시지 암호화를 위한 해쉬함수 기반의 공유키 K_{TH}를 공유한다.

Step 1. 리더 → 태그: SN 요청

RFID 리더는 환자에게 부착된 태그의 시리얼 번호 SN을 태그에게 요청한다.

Step 2. 태그 → 리더: SN 응답, ID_P

태그는 리더에게 태그 시리얼 번호인 SN을 응답하고 환자의 인식자 ID_P를 전송한다.

Step 3. 리더 → 태그: $E_{K_{HT}}(R'_{H2}, SID), h_{SN}(R_H \| R'_{H2})$

리더는 태그로부터 수신한 SN을 난수 생성기에 적용하여 랜덤수 R_H와 보안 인식자 SID를 생성한다. 생성된 랜덤수 R_H와 환자의 인식자 ID_P를 이용하여 $R_H \oplus ID_P$를 계산하여 임의의 크기 R'_{H1} 과 R'_{H2} 로 분할한다. 대칭키 암호 알고리즘 기반의 공유키 K_{HT}를 이용하여 암호화 한 값 $E_{K_{HT}}(R'_{H2}, SID)$와 해쉬함수 값 $h_{SN}(R_H \| R'_{H2})$를 계산하여 태그에게 전송한다.

Step 4. 태그: → 리더: S, I

태그는 리더로부터 수신한 메시지 $E_{K_{HT}}(R'_{H2}, SID)$를 공유키 K_{TH}로 복호화하여 SID를 추출하고, SN을 이용하여 해쉬 값 $h_{SN}(R_H \| R'_{H2})$로부터 랜덤 수 R'_{H2}를 얻어 검증을 통해 불법적으로 환자 정보를 악용하려는 스푸핑 공격이 발생했는지 검증한다. 계속해서 해쉬 값 $h_{SN}(R_H \| R'_{H2})$와 환자의 보안 인식자 SID, 그리고 환자가 생성한 랜덤 값 R_T를 연접한 후 랜덤 수 R'_{H2}를 이용하여 해쉬 값 $S = h_{R'_{H2}}(h_{SN}(R_H \| R_{T2}) \| SID \| R'_T)$ 를 계산하여 현재 세션의 통신 연결 상태 정보 I와 함께 리더에게 전송한다.

Step 5. 리더 → DB: $E_{K_{DB-H}}(R_H, R_T, SID, I, SN)$

리더는 태그로부터 수신한 메시지를 이용하여 태그와 동기화 유무를 확인하기 위해 리더의 분할 비밀키 $R_{H2}^{'}$로 S를 해쉬하여 $h_{SN}(R_H \| R_{T2}^{'}), SID, R_T^{'}$ 를 추출한다. 또한, 리더는 $h_{SN}(R_H \| R_{H2}^{'})$에서 추출한 $R_{H2}^{'}$와 리더가 가지고 있는 $R_{H1}^{'}$을 이용하여 $R_H == R_H^{'}$를 비교한다. 만약 일치한다면 재동기화를 위해 리더와 데이터베이스간 공유키 K_{DB-H}를 이용하여 암호화한 값 $E_{K_{DB-H}}(R_H, R_T, SID, I, SN)$을 데이터베이스에게 전송한다.

Step 6. DB → 리더: $E_{K_{DB-H}}(R_T^{'}, I)$

데이터베이스는 SN을 검색한 후 $R_H == R_H^{'}$를 비교한다. 만약 일치하지 않는다면 전송과정에서 비동기화가 발생했음을 탐지하고 재동기화를 위해 동기화 요청 메시지와 $h_{SN}(R_H \| R_{H2})$를 태그에게 재전송한다. 그리고 환자의 시리얼 번호 SN을 이용하여 $h_{SN}(R_T^{'} \| R_H)$를 생성하여 리더에게 $E_{K_{DB-H}}(R_T^{'}, I)$ 값을 전송한다.

Step 7. 리더 → 태그: $h_{RT}(SID \| R_{H2}), h_{SN}(R_T), I$

리더는 태그에게 $h_{RT}(SID \| R_{H2}), h_{SN}(R_T), I$ 값을 전송한다.

Step 8. 태그 → 리더: 인증 메시지 전달

태그는 리더로부터 수신한 메시지 $h_{RT}(SID \| R_{H2})$로부터 $R_{H1}^{'}$을 추출하고, $h_{SN}(R_T^{'})$로부터 $R_T^{'}$를 추출하여 R_T와 $R_T^{'}$를 비교한 후 인증에 성공하게 되면 리더에게 인증 확인 메시지를 전달하고, 그렇지 않으면 종료한다.

Step 9. 리더 → DB: 인증 메시지 전달

리더는 태그로부터 인증 메시지를 수신하면 바로 데이터베이스에게 인증 메시지를 전달한다.

Ⅲ. 보안성 분석

본 장에서는 Jeong[11]등이 제안한 J-L 환자 인증 프로토콜에 대한 보안성을 분석한다.

1. 위치추적 공격 및 프라이버시 침해 문제

Jeong등이 제안한 J-L 환자 인증 프로토콜의 <Step 1>에서 리더가 태그에게 태그의 고유 시리얼 번호인 SN을 요청하고, 태그는 리더에게 SN과 환자의 인식자인 ID_P를 전송한다. 이때, 악의적인 공격자는 송신 메시지 SN과 ID_P를 도청하거나 가로챌 수 있다. SN과 ID_P는 매 세션마다 고정된 값으로 공격자는 해당 메시지가 어떤 환자로부터 송신되었는지를 쉽게 알 수 있다. 따라서 Jeong등이 제안한 프로토콜은 환자 즉, 태그의 위치추적 공격에 안전하지 않으며 심각한 환자 프라이버시 침해 문제를 가진다.

2. 스푸핑 공격

Jeong등이 제안한 J-L 환자 인증 프로토콜의 <Step 4>에서 태그는 리더로부터 수신한 메시지를 복호화 $D_{K_{HT}}(R_{H2}^{'}, SID)$하여 SID를 추출하고, SN을 이용하여 해쉬 값 $h_{SN}(R_H \| R_{H2}^{'})$를 추출한 후 랜덤 수 $R_{H2}^{'}$을 얻음으로써 불법적으로 환자 정보를 악용하려는 스푸핑 공격을 예방할 수 있다고 주장 하였지만 다음과 같은 이유로 잘못된 주장이다. 공격자는 SN을 이용하여 도청한 $h_{SN}(R_H \| R_{H2}^{'})$로부터 R_H와 $R_{H2}^{'}$를 획득할 수 있으며 더 나아가 S로부터 $R_{H2}^{'}$를 이용하여 SID, R_T를 획득할 수 있으므로 공격자는 자유롭게 리더 또는 태그로 위장 공격을 수행할 수 있다.

3. 해쉬함수 연산오류 문제

Jeong등이 제안한 J-L 환자 인증 프로토콜의 <Step 4>에서 SN을 이용하여 해쉬 값 $h_{SN}(R_H \| R_{H2}^{'})$를 추출한 후 랜덤 수 $R_{H2}^{'}$을 얻음으로써 불법적으로 환자 정보를 악용하려는 스푸핑 공격을 예방할 수 있다고 하였다. 그러나 다음 [정의]와 같이 일방향 해쉬 함수의 one-way 성질로 인해 정확한 해쉬 값을 추출할 수 없다.

[정의] 안전한 메시지 인증 코드 함수 $y = F(x)$에서 주어진 x로 y를 계산하는 것은 쉽고, 주어진 y로 x를 계산하는 것은 어렵다.

또한 <Step 5>에서도 리더의 분할 비밀키 $R_{H2}^{'}$로 S를 해쉬하여 $h_{SN}(R_H \| R_{T2}^{'}), SID, R_T^{'}$ 를 추출한다고 하였고, <Step 8>에서도 태그는 리더로부터 수신한 메시지 $h_{RT}(SID \| R_{H2})$로부터 $R_{H1}^{'}$을 추출하고, $h_{SN}(R_T^{'})$로부터 $R_T^{'}$를 추출하여 R_T와 $R_T^{'}$를 비교한다고 하였으므로 프로토콜 수행과정에서 일방향 해쉬 함수의 성질에 맞지 않으므로 연산 오류가 발생함을 알 수 있다.

Ⅳ. 제안하는 u-헬스케어 서비스 인증 프로토콜

본 장에서는 Jeong[11]등이 제안한 J-L 환자 인증 프로토콜이 가지는 1) 위치추적 공격 및 프라이버시 침해 문제, 2) 스푸핑 공격 취약성, 3) 해쉬함수 연산오류 문제 등의 심각한 보안성과 연산 효율성 문제를 해결할 수 있는 보안성 및 효율성을 강화하여 더욱 강력한 안전성을 제공하고 연산 효율성이 높은 u-헬스케어 서비스 인증 프로토콜을 제안한다. 프로토콜의 전체적인 수행 과정은 다음과 같다.

Step 1. 리더 → 태그: SN 요청 및 R_H 전송

RFID 리더는 랜덤수 R_H를 생성한 후 환자에게 부착된 태그의 시리얼 번호 SN을 태그에게 요청 및 랜덤수 R_H를 전송 한다.

Step 2. 태그 → 리더: C_1, R_T, I, MAC_1

태그는 랜덤수 R_T를 생성한 후 사전 공유키 K_{HT}, 리더로부터 수신한 랜덤수 R_H, 태그가 생성한 랜덤수 R_T, 그리고 현재 세션의 통신 연결 상태 정보 I를 이용하여 세션 키로 사용할 $SK = h(K_{HT} \| R_H \| R_T \| I)$를 해쉬함수를 사용하여 해쉬값을 계산한다. 그런 다음 SN과 세션키 SK를 사용하여 $C_1 = SN \oplus SK$를 계산하고, 메시지 인증 코드 값 $MAC_1 = h(SK \| SN)$을 해쉬함수를 사용하여 해쉬값을 계산한 후 C_1, R_T, I, MAC_1을 리더에게 전송한다.

Step 3. 리더 → 태그: $Auth$

리더 → DB: C_2, MAC_2, R_H, R_T, I

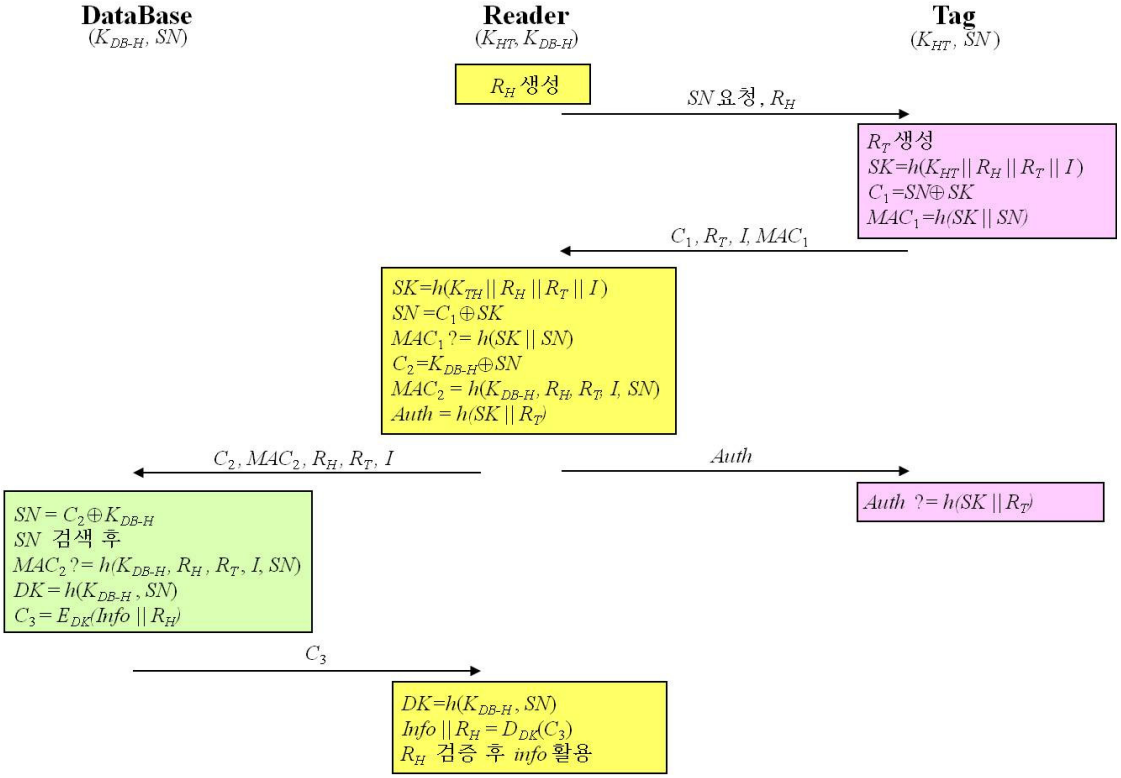

그림 2. 제안하는 u-헬스케어 서비스 인증 프로토콜
Fig. 2. proposed u-Healthcare Service Authentication protocol.

리더 역시 현재 세션키 값 $SK = h(K_{TH} \| R_H \| R_T \| I)$를 해쉬함수를 사용하여 계산한 후 XOR 연산 $SN = C_1 \oplus SK$를 수행하여 SN 값을 계산한다. 그런다음 $MAC_1 = h(SK \| SN)$을 계산하여 태그로부터 수신한 MAC_1 값과 일치하는지 검증한다. 만약 두 값이 일치하면 리더는 데이터베이스와의 인증을 위해 $C_2 = K_{DB-H} \oplus SN$으로 XOR 연산을 수행하고 메시지 인증 코드 값인 $MAC_2 = h(K_{DB-H}, R_H, R_T, I, SN)$을 해쉬함수를 사용하여 해쉬값을 계산한다. 리더는 태그와의 상호 인증을 위해 $Auth = h(SK \| R_T)$를 해쉬값으로 구한 후 태그에게 전송하고, 데이터베이스와의 상호 인증을 위해 C_2, MAC_2, R_H, R_T, I 값을 데이터베이스에게 동시에 전송한다.

Step 4. DB: → 리더: C_3

리더로부터 메시지를 수신한 데이터베이스는 XOR 연산을 수행하여 $SN = C_2 \oplus K_{DB-H}$ 값을 얻는다. 그런다음 SN을 검색한 후 해쉬함수를 사용하여 $MAC_2 = h(K_{DB-H}, R_H, R_T, I, SN)$ 값을 계산하고 리더로부터 수신한 값 MAC_2과 일치하는지 검증한다. 만약 두 값이 일치하면 DB는 $DK = h(K_{DB-H}, SN)$ 해쉬 값을 계산하여 얻은 값 DK를 대칭키 암호 알고리즘에 사용하여 $C_3 = E_{DK}(Info \| R_H)$ 값을 계산한 후 리더에게 전송한다.

Step 5. 리더는 데이터베이스로부터 수신한 C_3를 복호화하기 위해 $DK = h(K_{DB-H}, SN)$ 해쉬 값을 먼저 계산한 후 $Info \| R_H = D_{DK}(C_3)$ 값으로 복호화한다. 그런다음 R_H를 검증한 후 일치하여 검증에 성공하면 리더가 필요로 하는 정보인 $Info$를 활용한다.

Ⅴ. 안전성과 효율성 분석

1. 안전성 분석

본 절에서는 제안한 프로토콜이 병원측인 리더와 환자가 부착하고 있는 태그 간의 상호 인증 과정에서 악의적인 공격자의 위치추적 공격, 프라이버시 침해 및 스푸핑 공격 등에 안전함을 증명한다. 표 2는 J-L 프로토콜과 제안한 프로토콜의 안전성을 비교한 것이다. 일반적으로 RFID 시스템 환경에서는 안전하지 않은 무선 통신 채널을 사용하여 메시지를 교환하므로 리더와 태그간에 전송되는 모든 메시지는 공격자에 의해 도청 및 메시지를 가로챌 수 밖에 없다. 따라서 J-L 환자 인증 프로토콜에서는 리더가 요청한 태그의 고유 번호인 SN과 환자의 인식자인 ID_P를 도청하여 환자의 위치를 추적할 수 있을 뿐만 아니라 심각한 프라이버시 침해 문제를 발생시킨다. 또한 공격자는 SN을 이용하여 도청한 메시지 $h_{SN}(R_H \| R'_{H2})$로부터 R_H와 R'_{H2}를 획득할 수 있으며 S로부터 R'_{H2}를 이용하여 SID, R_T 값까지 알수 있게 된다. 따라서 공격자는 리더 또는 태그로 위장 공격을 수행할 수 있다. 그러나 본 논문에서 제안한 프로토콜은 다음과 같이 안전한 상호 인증을 제공하여 위치추적 공격 및 프라이버시 침해에도 안전할 뿐 아니라 스푸핑 및 위장 공격에도 안전하다.

(1) 위치추적 공격 및 프라이버시 침해 : 제안한 프로토콜의 Step 2에서 태그는 리더의 SN 요청 및 랜덤수 R_H를 수신하게 되면 랜덤수 R_T를 생성한 후 사전 공유키 K_{TH}, 리더로부터 수신한 랜덤수 R_H, 태그가 생성한 랜덤수 R_T, 그리고 현재 세션의 통신 연결 상태 정보 I를 이용하여 세션 키로 사용할 $SK = h(K_{HT} \| R_H \| R_T \| I)$를 해쉬함수를 사용하여 해쉬값을 계산한다. 그런 다음 SN과 세션키 SK를 사용하여 $C_1 = SN \oplus SK$를 계산하고, 메시지 인증 코드 값 역시 해쉬함수로 계산한 $MAC_1 = h(SK \| SN)$ 해쉬값과 C_1, R_T, I 와 함께 리더에게 전송한다. 해쉬함수는 일방향 함수로서 메시지로부터 해쉬값을 계산할 수는 있어도 반대로 해쉬값으로부터 메시지를 복원할 수는 없다. 따라서 태그는 메시지 인증 코드인 MAC_1 해쉬값을 리더에게 전송하고, 리더는 자신이 계산한 MAC_1 해쉬값과 일치하는지 검증함으로써 메시지의 무결성을 보증할 수 있다. 따라서 제안한 프로토콜은 태그의 위치추적 공격 및 환자 프라이버시 침해에 안전함을 알 수 있다.

(2) 상호인증, 스푸핑 공격 및 위장 공격: 제안한 프로토콜의 Step 2, 3, 4에서는 모두 메시지를 일방향 해쉬함수를 사용하여 해쉬값으로 계산한 후 전송한다. Step 3에서 리더는 태그와의 인증을 위해 태그로부터 수신한 $MAC_1 = h(SK \| SN)$ 해쉬값을 자신이 계산한 MAC_1

해쉬값과 일치하는지 검증하고, Step 4에서 데이터베이스는 리더와의 인증을 위해 리더로부터 수신한 $MAC_2 = h(K_{DB-H}, R_H, R_T, I, SN)$ 해쉬값을 자신이 계산한 MAC_2 해쉬값과 일치하는지 검증한다. 또한 Step 3에서 리더는 태그와의 상호 인증을 위해 $Auth = h(SK \| R_T)$를 해쉬값으로 계산한 후 태그에게 전송하고, 동시에 데이터베이스와의 상호 인증을 위해 C_2, MAC_2, R_H, R_T, I를 데이터베이스에게 전송한다. Step 4에서 데이터베이스는 리더로부터 수신한 $MAC_2 ? = h(K_{DB-H}, R_H, R_T, I, SN)$ 해쉬값이 자신이 계산한 값과 일치하는지 검증하고, Step 5에서 태그 역시 리더로부터 수신한 $Info$ 값을 검증하여 일치하게 되면 리더와 태그는 상호 인증에 성공하여 정보를 활용하게 된다. 따라서 제안한 프로토콜은 안전한 상호인증을 제공할 뿐만 아니라 스푸핑 공격 및 위장 공격에도 안전함을 알 수 있다.

표 2. 안전성 비교
Table 2. Security Comparision.

보안성 항목	J-L 프로토콜[11]	제안한 프로토콜
위치추적 공격	안전하지 않음	안전함
프라이버시 침해	안전하지 않음	안전함
스푸핑 공격	안전하지 않음	안전함
위장 공격	안전하지 않음	안전함

2. 효율성 분석

표 3은 J-L 프로토콜과 제안한 프로토콜의 효율성을 비교한 결과를 보여주고 있다. J-L 프로토콜은 대칭키 연산이 태그에서 1번, 리더에서 2번, 데이터베이스에서 1번을 수행하고, 해쉬 연산은 태그에서 5번, 리더에서 4번을 수행한다. 반면 본 논문에서 제안한 프로토콜에서는 태그에서는 대칭키 연산을 수행하지 않으며, 해쉬 연산도 3회만 수행한다. 그러나 저비용 수동형 RFID 태그는 메모리가 작으며 연산 수행 능력이 리더나 데이터베이스에 비해 느리다. 따라서 태그 측에서 대칭키 연산과 5회의 해쉬 연산을 수행하게 되면 연산 효율성이 낮아진다. 또한 리더와 태그, 그리고 데이터베이스 간의 통신 메시지량은 9번의 단계를 거친 후에 인증하는 반면 제안한 프로토콜은 4단계의 통신 메시지량을 수행한다. 그러므로 제안한 프로토콜이 효율성 측면에서도 우수함을 알 수 있다.

표 3. 효율성 분석
Table 3. A Comparison of efficiency.

프로토콜 / 연산종류	J-L 프로토콜[11]			제안한 프로토콜		
	태그	리더	DB	태그	리더	DB
대칭키 연산	1	2	1	0	1	1
해쉬 연산	5	4	0	3	5	2
리더, 태그, DB간 통신 메시지량	9			4		
연산/통신 효율성	낮음			높음		

VI. 결 론

최근 유비쿼터스 컴퓨팅 기술과 RFID 시스템의 결합으로 u-헬스케어 서비스에 대한 관심과 개발이 증대되고 있는 추세이다. 무엇보다 u-헬스케어 서비스 환경에서 가장 중요한 것은 환자의 프라이버시를 보호하고 건강과치료에 대한 개인의 정보가 유출되거나 위조 및 변조되지 않도록 서비스 인증, 기밀성, 무결성, 통신로 보안, 효율성 등의 보안 요구 사항들을 만족해야 한다. 최근 Jeong[11]등은 RFID 기술을 이용하여 초기화 과정과 환자 인증 과정을 구분한 J-L 환자 인증 프로토콜을 제안하였다. Jeong등은 제안한 프로토콜에서 재사용 공격, 스푸핑 공격, 정보노출방지 및 불추적성에 대해 안전하다고 주장하였지만 보안성과 연산 효율성 문제를 발생시킨다. 따라서 본 논문에서는 Jeong 등이 제안한 프로토콜이 위치추적 공격 및 프라이버시 침해 문제, 스푸핑 공격 취약성, 해쉬함수 연산오류 문제 등의 심각한 보안성과 연산 효율성 문제들이 있음을 증명하였고, 안전성과 효율성을 강화한 RFID 기술 기반의 개선된 u-헬스케어 서비스 인증 프로토콜을 제안하였다. 제안한 프로토콜은 안전한 상호인증을 제공할 뿐만 아니라 환자의 위치추적 공격 및 프라이버시 침해에 안전하고, 스푸핑 공격 및 위장 공격에도 안전한 높은 보안성과 연산 및 통신 효율성을 제공하는 실용적인 u-헬스케어 서비스 프로토콜로서 활용될 수 있다.

REFERENCES

[1] Richard Lenz, Manfred Reichert, “IT Support for Healthcare Processes”, LNCS 3649, pp. 354-363, 2005.

[2] J. M. Choi et al., “A System of Ubiquitous Health Monitoring in the Bedroom via a Bluetooth Network and Wireless LAN,” in Pro. of the 26th Annual International Conference of the IEEE EMBS San Franciso, CA, USA, Sept. 1-5, 2004.

[3] J.E. Song et al., “Security Issues and Its Technology Trends in u-Healthcare”, ETRI, Electronics and Telecommunications Trends, vol.22, no.1, 2007.

[4] M. S. Jang et al., “Design and Implementation of U-healthcare system with zigbee in service integration system”, The Institute of Electronics Englineers of Korea, vol. 43, no. 11, pp. 16-24, 2006.

[5] S. I. Yoon et al., “The Implementation of Art Therapy Service asan Ubiquitous Health-care Service,” TENCON 2004, 2004 IEEE Region 10 Conference Vol. C, pp. 200-203, Nov. 2004.

[6] H. S. Ahn et al., “A Practical Authentication System for Wireless Body Area Networks(WBAN)”, The Journal of Korea Information and Communications Society, vol.37, no.4, pp.290-296, 2012.

[7] S.T. Ali et al., “Authentication of Lossy Data in Body-Sensor Networks for Healthcare Monitoring,”2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks(SECON), pp.470-478, 2012.

[8] 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), pp. 1289-1298, 2011.

[9] E. J. Yoon, K. Y. Yoo, “Patient Authentication System for Medical Information Security using RFID”, The Journal of Korea Information and Communications Society, vol.35, no.6, pp.962-969, 2010.

[10] J. h. Park, S. Y. Kang, “A Research on Information Security Issue of RFID in U-Healthcare Environment”, Journal of Security Engineering, vol.5, no.5, pp.359-370, 2008.

[11] Y. S. Jeong and S. H. Lee, “u-Healthcare Service Authentication Protocol based on RFID Technology”, 디지털정책연구, vol. 10, no. 2, pp.153-159, 2012.

[12] Yu-Yi Chen, Jun-Chao Lu, Jinn-Ke Jan, “A Secure EHR System Based on Hybrid Clouds.”, J Med Syst, 36:3375-3384, 2012.

[13] Tsung-Chih Hsiao et al., “An Authentication Scheme to Healthcare Security under Wireless Sensor Networks”, J Med Syst (2012) DOI 10.1007/s10916-012-9839-x.

[14] Chien-Lung Hsu, Chung-Fu Lu, “A Security and Privacy Preserving E-Prescription System Based on Smart Cards”, J Med Syst (2012) DOI 10.1007/s10916-012-9838-y.

[15] H. S. Ahn et al., “Improved Authentication Protocol for RFID/USN Environment”, The Institute of Electronics Englineers of Korea, vol. 46, no. 1, pp. 1-10, 2009.

저 자 소 개

안 해 순(정회원)
1996년 경일대학교 컴퓨터공학과 (공학사)
2001년 경일대학교 컴퓨터공학과 (공학석사)
2009년 대구대학교 컴퓨터정보공학과(공학박사)
2004년～2008년 경일대학교 컴퓨터공학부 전임강사
2008년～현재 대구대학교 교양대학 초빙교수
<주관심분야: 데이터베이스, 정보보안, 정보검색, 모바일 GIS, 데이터베이스 보안, RFID 보안>

부 기 동(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
<주관심분야: 데이터베이스, GIS, 시멘틱 웹, 데이터베이스 보안, RFID 보안>

윤 은 준(정회원)
1995년 경일대학교 졸업 (공학사)
2003년 경일대학교 컴퓨터공학과 (공학석사)
2007년 경북대학교 컴퓨터공학과 (공학박사)
2011년～현재 경일대학교 사이버보안학과 교수
2010년～현재 대한전자공학회 컴퓨터소사이어티 융합컴퓨팅연구회 위원장
<주관심분야: 암호학, 정보보호, 데이터베이스보안, 네트워크보안, 스테가노그라피>