u-헬스케어를 위한 RFID 기반 환자 인증 프로토콜

유기영*

An RFID-based Patient Authentication Protocol for u-Healthcare

Kee-young Yoo*

요 약 본 논문에서는 u-헬스케어 환경 상에서 안전하고 효율적으로 환자 인증 및 환자 개인 의료 정보를 보호할 수 있는 RFID 기반 환자 인증 프로토콜을 제안한다. 제안한 RFID 기반 환자 인증 프로토콜은 강인한 보안성과 효율성을 제공하여 주어, u-Hospital 및 u-Healthcare 같은 첨단 의료 환경상에서 환자 인증뿐만 아니라 환자 개인의 의료 정보를 안전하게 보호할 수 있음으로 실용적으로 사용되어 질 수 있다.

ABSTRACT In this paper, we propose a secure and efficient RFID-based patient authentication protocol to not only authenticate patients' authenticity but also protect patients' personal medical informations for u-Healthcare environments. Since the proposed RFID-based patient authentication protocol provides strong security and efficiency, it can be used practically for patient authentication and personal medical information protection on the high technology medical environments such as u-Hospital and u-Healthcare.

Key Word : 의료 정보 보안, 인증, RFID, 프로토콜, 프라이버시, u-Hospital, u-Healthcare

Ⅰ. 서 론

첨단 의료 환경 상에서는 의료 과실을 줄이기 위한 방법으로 환자의 의료 프로필(Profile)을 이용하여 정확하게 환자를 식별할 수 있도록 RFID(Radio Frequency IDentification) 기술을 많이 적용하고 있다.일반적으로 의료 환경에서의 RFID 기술은초단파나 장파의 무선 주파수를 이용하여환자의 의료정보를 물리적인 접촉 없이 비접촉 방식으로 읽거나 정보를 기록할 수 있는 최첨단 기술로 정의할 수 있다[1-3]. 이로 인해 RFID 기술은 USN(Ubiquitous sensor network) 기술과 더불어 유비쿼터스 컴퓨팅(Ubiquitous Computing) 환경 실현을 위한 중요한 핵심 기술로 가장 주목을 받고 있는 기술이다[4-6]. 의료 환경에서 위와 같은 RFID 기술을 이용하면 환자들에 대한 의료처방 및 치료를 정확하게 수행 할 수 있다.

본 논문에서는 위와 같은 의료 환경을 기반으로 안전하고 효율적으로 환자 인증 및 환자 개인 정보를 보호할 수 있는 RFID 기반 의 환자 인증 프로토콜을 제안한다. 한 결론으로서, 제안한 RFID 인증 시스템은 강인한 보안성과 효율성을 제공하여 주어, u-Hospital 및 u-Healthcare 같은 첨단 의료 환경에서 환자 개인의 프라이버시 제공 및 정보 보호를 위해 실용적으로 사용되어 질 수 있다.

* Corresponding Author : Computer Science and Engineering Professor of Kyungpook National University
Received : January 10, 2014 Revised : January 17, 2014 Accepted : January 29, 2014

Ⅱ. 제안한 RFID 기반 환자 인증 프로토콜

RFID 시스템은 그림 1과 같이 백-엔드 데이터베이스 서버(DB), RFID 리더(Reader), RFID 태그(Tag)들의 3종류의 컴포넌트들로 구성되어 진다.표 1은 본 논문에서 사용되어 지는 시스템 파라미터들을 보여준다.

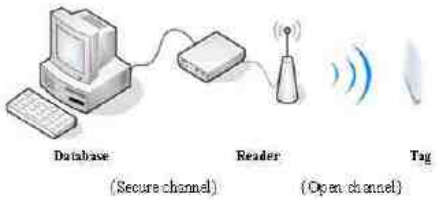

그림 1. RFID 시스템 구성요소
Fig1. RFID System Components

용 어	정 의
Tag	환자가 착용하고 있는 RFID 태그
$Reader$	의사가 소지하고 있는 RFID 리더
DB	의료정보 백-엔드 데이터베이스
$query$	리더의 요청 메시지
TID	Tag에게 할당된 고유 ID 정보
k_{TID}	Tag의 고유 비밀키
$h()$	안전한 일방향 해쉬 함수
$time$	$Reader$가 생성한 타임스탬프 값
$prng()$	의사난수생성기
T_{rand}	Tag가 생성한 랜덤 값
$\oplus$	배타적 논리합(XOR) 연산
$\|$	연접 연산(concatenation) 연산
$A \rightarrow B : X$	X가 A에서 B로 전송

표 1. 시스템 파라미터
Table 1. System parameters

1. 시스템 환경

제안한 RFID 기반 환자 인증 프로토콜에서는 병원 내의 모든 환자들이 자신들의 의료정보를 식별할 수 있는 RFID 태그를 전자팔찌(Bracelet) 또는 전자발찌(Ankles) 등의 스마트 밴드(Smart Band) 형태로 착용하고 있음을 가정한다[1-3]. 또한 병원 내의 RFID 백-엔드 데이터베이스와 병원 내의 의사 또는 간호사가 소지하고 있는 리더 간의 통신 채널(CommunicationChannel) 은 안전한 채널(Secure Channel)임을 가정한다[23].

2. 환자 인증 프로토콜

그림 2는 제안한 RFID 기반 환자 인증 프로토콜의 구성과 동작 과정을 보여주며, 다음의 5 단계를 거쳐 인증 과정이 이루어진다. 여기에서 병원(리더)는 의사 또는 간호사가 소지한 리더기를 의미한다.

(1)병원(리더)→환자(태그):
$\{Query, Time\}$
병원(리더)는 타임스탬프 $Time$을 생성한 후, 환자(태그)에게 $Query$와 함께 전송한다. 여기에서 타임스탬프 $Time$은 시간 동기화를 위한 목적이 아니라 해당 환자(태그)가 병원 반경 내에 있는 지 여부를 리더가 빨리 검증하기 위해 사용된다.

(2) 환자(태그)→병원(리더):
$\{H_{TID}, T_{rand}, Time\}$
환자(태그)는 랜덤 값 T_{rand}를 $prng()$로부터 생

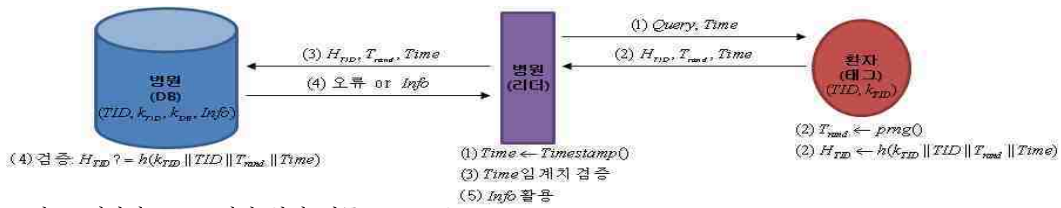

그림 2. 제안한 RFID 기반 환자 인증 프로토콜
Fig 2. RFID-based authentication protocol proposed by patients

성한 후, 병원(리더)로부터 수신한 $Time$과 자신의 식별자인 및 비밀 키 k_{TID}를 함께 이용하여 랜덤 해쉬 값 $H_{TID} = h(\| k_{TID} \| \| T_{rand} \| Time)$을 계산한 후, 병원(리더)에게 계산된 H_{TID}를 T_{rand}및 $Time$과 함께 전송한다.

(3) 병원(리더)→병원(DB):
$\{H_{TID}, T_{rand}, Time\}$
병원(리더)는 먼저 수신한 메시지가 자신이 정한 임계 시간(Threshold Time) 내에 도착 하였는지 여부를 수신한 $Time$을 이용하여 검증한다. 만약 검증을 통과하여 환자(태그)가 병원 반경 내에 존재함이 확인되면, 수신한 메시지들을 병원(DB)에게 전송한다.

(4) 병원(DB)→병원(리더): $\{Info\}$
병원(DB)는 병원(리더)로부터 전송받은 $\{H_{TID}, T_{rand}, Time\}$와 자신의 데이터베이스 내에 저장하고 있는 모든 TID와 k_{TID}쌍을 이용하여 병원(리더)로부터 수신한 H_{TID}값과 일치하는 TID와 k_{TID}쌍을 검색한다. 만약 일치하는 값이 검색되지 않으면, 해당 환자(태그)가 존재하지 않는다는 오류(error) 메시지를 병원(리더)에게 전송하고, 만약 일치하는 값이 검색되면 해당 환자(태그)를 인증하고 환자(태그)에 대한 의료 관련정보(related information)인 $Info$ 병원(리더)에게 전송한다.

(5) 병원(리더)는 병원(DB)로부터 수신한 값이 오류일 경우, 환자(태그)와의 통신을 중단하고, 정상적인 인증이 되었을 경우에서는 병원(DB)로부터 수신한 의료 관련정보(related information)인 $Info$를 활용하여 해당 환자(태그)에 대해 원하는 의료 업무를 수행한다.

Ⅲ. 안전성 분석

본 장에서는 제안한 RFID 기반 환자 인증 시스템에 대한 보안성 분석을 한다.

(1) 재전송 공격(Replay attack): 공격자는 임의의 세션에서 병원(리더)와 환자(태그)사이에서 전송되는 정보를 모두 도청한 후, 다음 세션에서 정당한 병원(리더)나 환자(태그)로 위장을 시도하는 재전송 공격을 수행할 수 있다. 하지만 제안한 RFID 인증 시스템에서는 매 세션마다 병원(리더)가 생성하는 새로운 타임스탬프$Time$와 환자(태그)가 생성하는 새로운 랜덤 값 T_{rand}를 이용하여 병원(DB)에 의해 인증을 수행하기 때문에, 과거에 공격자에 의해 재전송된 랜덤 값들은 병원(DB)의 인증 과정 중에 쉽게 검출됨으로 재전송 공격을 수행할 수 없다.

(2) 스푸핑 공격(Spoofing attack): 공격자가 병원(DB)와 환자(태그) 간에 공유된 비밀키인 k_{TID}를 얻을 수 있으면, 병원(리더) 또는 환자(태그)로의 스푸핑 공격을 성공할 수 있다. 하지만 위 [정의 1]과 [정의 2]에 의해 제안한 RFID 인증 시스템에서 공개 통신 채널 상으로 전송되는 정보들인 $\{H_{TID}, T_{rand}, Time\}$을 이용하더라도, 공격자는 병원(DB)와 환자(태그) 내에 각각 안전하게 저장하고 있는 비밀 키인 k_{TID}를 직접적으로 얻을 수 있는 방법이 없게 되어 스푸핑 공격을 수행할 수 없다.

(3) 위치 트래킹 공격(Location tracking attack) 및 위치 프라이버시(Location privacy): 환자(태그) 측에서 생성하는 랜덤값 T_{rand}는 매 세션마다 다른 값으로 생성되기 때문에 이로부터 계산된 $H_{TID} = h(\| k_{TID} \| \| T_{rand} \| Time)$ 또한 매 세션마다 변경된다. 따라서 공격자는 현재 세션에서 환자(태그)의 응답이 과거 세션에 도청한 응답과 동일한지를 쉽게 구별할 수 없다. 이

로 인해, 공격자는 태그의 이동경로를 쉽게 추적을 할 수 없을 뿐만 아니라, 특정한 태그를 식별할 수 없기에 위치 트래킹 공격을 수행 할 수 없게 되어 위치 프라이버시를 제공할 수 있다.

(4) 태그 익명성(Tag anonymity): 병원(리더)는 타임스탬프 $Time$을 생성하여 환자(태그)에게 전송하고, 환자(태그)는 수신한 $Time$과 자신이 생성한 임의의 랜덤 값 T_{rand}그리고 식별자인TID와 비밀 키인 k_{TID}를 이용하여 해쉬 함수의 도움으로 $H_{TID} = h(\| k_{TID} \| \| T_{rand} \| Time)$을 계산한 후 병원(리더)에게 전송한다. 이로 인해, H_{TID}을 도청한 공격자는 환자(태그)의 비밀 키인 k_{TID}를 알지 않고서는 환자(태그)의 식별자인 TID를 추측할 수 없을 뿐만 아니라, 일방향 해쉬 함수의 성질에 의해 H_{TID}로부터 환자(태그)의 TID정보를 직접적으로 얻을 수 없게 됨으로 환자(태그)의 익명성을 제공할 수 있다.

Ⅳ. 효율성 분석

본 장에서는 표 2와 같이 제안한 RFID 기반 환자 인증 시스템에 대한 효율성을 분석한다.

표2. 효율성 분석
Table 2. Efficiency Analysis

	병원(DB)	병원(리더)	환자(태그)
랜덤 값	0	0	1
타임스탬프	0	1	0
해쉬 연산	n	0	1
XOR 연산	0	0	0
라운드 수	4		

n:병원(DB) 서버 내에서 저장된 최대 환자(태그) 수

제안된 RFID 인증 시스템은 환자(태그) 측에서 하나의 랜덤 값 생성이 요구되며, 병원(DB) 측에서는 n의 해쉬 연산이 요구된다. 환자(태그)와 달리 병원(DB)는 높은 시스템 성능과 연산 능력을 가짐으로 n번의 해쉬 연산을 통한 환자(태그) 인증은 빠른 시간 내에 이루어 질 수 있다. 결론적으로 RFID 기반 환자 인증 시스템은 안전성과 효율성 및 실용성을 제공함을 알 수 있다.

Ⅴ. 결 론

본 논문에서는 의료 과실을 줄여주며 정확한 환자의 개인 의료 정보를 활용할 수 있게 하는 RFID 기반의 환자 인증 프로토콜을 제안하였다. 제안한 인증 프로토콜은 안전하고 효율적으로 환자 인증 및 환자 개인의 의료 정보를 보호할 수 있어, u-Hospital 및 u-헬스케어와 같은 첨단 의료 환경 상에서 환자 안전한 인증뿐만 아니라 환자 개인의 프라이버시 제공 및 의료 정보 보호를 위해 실용적으로 사용되어 질 수 있다.

감사의 글

본 연구는 2단계 두뇌한국 21 프로젝트(2009)의 연구결과로 수행되었습니다.

Reference

[1] B. Starfield, “Is US health really the best in the world?,” Journal of the American Medical Association, Vol. 284, No. 4, pp. 483-485, 2000.

[2] J. A. Fisher, “Indoor positioning and digital management: emerging surveillance regimes in healthcare,” In T. Monahan (Ed), Surveillance and Security: Technological Politics and Power in Everyday Life, New York: Routledge, pp. 7788, 2006

[3] M. Anshel and S. Levitan, “Reducing medical errors using secure RFID technology,” ACM SIGCSE Bulletin, Vol.

39. No. 2, pp. 157-159, 2007.
[4] F. Klaus, “RFID handbook,” Second Edition, Jone Willey & Sons, 2003.
[5] S. A. Weis, “Security an privacy in radio-frequency identification devices,” MS Thesis. MIT. May, 2003.
[6] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, “Security and privacy aspects of low-cost radio frequency identification systems,” Security in Pervasive Computing 2003, LNCS 2802, pp. 201-212, Springer-Verlag Heidelberg, 2004.

저자약력

유 기 영(Yoo Kee-young) **정회원**

현재 경북대학교 IT대학
컴퓨터학부 교수

<관심분야> 정보보호, 암호,보안