

논문 2010-3-17

병원 의료시설 내 U-Healthcare 환경에서 환자 정보 관리를 위한 환자 세분화 기법

Patient Classification Scheme for Patient Information Management in Hospital U-Healthcare System

이기정*, 박성원**

Kijeong Lee, Sungwon Park

요 약 UMSN (Ubiquitous Medical Sensor Network)은 실시간 객체식별과 센서 정보 수집으로 병원 등 의료시설의 u-Healthcare 시스템에 사용되고 있다. RF 무선 주파수로 리더기를 이용해 태그를 식별하는 RFID는 특히 환자 관리에 많이 쓰인다. 하지만 RFID 태그는 리더기의 질의에 항상 자신의 ID를 응답하기 때문에 불법적인 리더기에 ID를 전송하거나 불필요한 질의에 응답하여 도청, 스푸핑 등의 보안 취약점이 발생할 수 있다. 본 논문은 UMSN 기반의 환자관리 시스템에서 리더기가 환자, 의료기기, 의료진, 각종센서 등에 부착된 태그에 과도한 인증을 요청하여 발생할 수 있는 RFID Back-end Server의 트래픽을 줄이고 이 과정에서 발생 가능한 도청, 스푸핑 등의 보안 위협을 줄이기 위해 태그 ID 세분화 기법을 제안한다. 제안 기법은 환자의 태그 ID 문자열을 기준으로 환자를 분류하여 집단으로 구분하고 해당 집단에 인가된 리더기가 태그를 읽었을 때만 Back-end Server가 태그 인증절차를 수행하도록 하여 Back-end Server 트래픽과 보안 위협을 줄일 수 있다.

Abstract UMSN (Ubiquitous Medical Sensor Network) is being used in u-Healthcare system of various medical facilities to identify objects and get information from sensors in real-time. RFID using radio frequency determines objects using Reader, which reads Tags attached to patients. However, there is a security vulnerability wherein Tag send its ID to illegal Reader because Tags always response to Readers request regarding of its Tag ID. In this paper, we propose Tag ID Classification Scheme to reduce Back-end Server traffic that caused by requests to authenticate between Readers and Tags that are attached to medical devices, patients, and sensors; To reduce security threats like eavesdropping and spoofing that sometimes occurred during authentication procedure. The proposed scheme specifies the patient category as a group based on patients Tag ID string. Only allowed Reader can perform authentication procedure with Back-end Server. As a result, we can reduce Back-end Server traffic and security threats.

Key Words : UMSN, u-Healthcare, 환자 관리 시스템, RFID Tag Group

I. 서 론

인구 고령화로 의료시설 증가에 따른 병원 환자들의 효율적인 관리가 요구되고 있다. 유비쿼터스 컴퓨팅 기

술의 발달로 실시간으로 환자의 생체정보를 수집해 모니터링하고 관리할 수 있는 u-Healthcare 서비스 제공이 가능해져 일부 병원에서는 u-Healthcare 서비스로 입원 환자의 실시간 모니터링 시스템을 구축해 운영 중이다. 의료진들은 전자 차트로 실시간 환자모니터링을 통해 위급상황에 빠른 대처가 가능하고 RFID를 의료자산에 도

*준회원, 한남대학교 대학원

**중신회원, 한남대학교 간호학과 교수

(교신저자: 박성원, sungwon@hnu.kr)

접수일자 2010.06.01 수정일자 2010.06.17

입해 관리가 가능하다. u-Healthcare 서비스를 위해 RFID/UMSN (Radio-Frequency Identification/ Ubiquitous Medical Sensor Network) 기반의 실시간 객체 식별과 센서 정보 수집 기술이 사용되고 있다. RFID 태그 내장 바이오센서를 환자에게 부착하여 전송되는 환자 생체정보를 실시간 모니터링해 이상여부를 감지하고 센서에 부착된 태그로 환자를 식별한다.^[1] 하지만 RFID는 RF 무선신호로 비접촉 방식으로 태그를 인식 때문에 보안 취약점을 가지며 이를 보완하기 위해 인증 프로토콜을 사용한다. 그러나 리더와 태그의 수가 늘어날수록 인증횟수 증가로 Back-end Server 트래픽이 증가해 전체 시스템 성능 저하가 발생할 수 있다. 또한 불필요한 인증 증가로 도청, 스푸핑 등의 보안 위협이 증가할 수 있다. 따라서 본 논문에서는 의료시설 내 RFID/UMSN 기반 u-Healthcare 시스템에서 효율적인 인증과 보안위협문제 최소화를 위한 환자 태그 ID 세분화 기법과 그 시스템을 제안한다.

본 논문의 구성은 2장에서 RFID/UMSN의 개요와 보안 위협 문제점 및 보안인증 프로토콜에 대해 알아보고 3장에서는 제안하는 환자 태그 ID 세분화 및 그룹화 기법에 대해 설명한다. 4장에서는 제안 기법의 시스템 성능 분석 비교를 하고 5장에서 결론 및 고찰을 한다.

II. 관련 연구

1. UMSN (Ubiquitous Medical Sensor Network)

UMSN은 유비쿼터스 컴퓨팅 기술과 무선 센서 기술을 접목하여 주변에 부착된 태그나 센서로부터 주변 환경의 정보를 감지하고 전송할 수 있도록 네트워크로 구성된 인프라로 유비쿼터스 사회 구현을 위해 주목받고 있다. 전자태그가 부착된 사물이나 객체를 인식하고 식별하는 단계에서 시작해 현재는 태그에 주변 환경정보를 감지하고 전송할 수 있는 센서들을 추가하여 태그 상호간 통신으로 Ad hoc 네트워크를 구축하고 실시간으로 이들을 모니터링할 수 있는 단계까지 발전했다. UMSN은 여러 센서노드들로 구성된 센서 네트워크가 gateway를 통해 외부 네트워크에 연결되는 구조로 되어 있으며 무선 네트워크 등을 이용하여 인터넷에 접속해 어디서든 이들의 정보를 확인할 수 있다. UMSN은 많은 수의 센서노드들로 구성되어 있고 이를 식별하기 위해 RFID 기술

이 사용되는 것이 RFID/UMSN이다.

2. RFID (Radio-frequency Identification)

RFID 시스템은 상품이나 사물에 부착된 RFID 태그를 비접촉 방식으로 읽어 식별하고 관리하는 기술로 태그와 태그 정보를 읽는 리더, 태그가 부착된 사물의 정보가 담긴 Back-end Server로 구성된다.^{[1][2]} 리더가 태그에 질의를 보내 태그가 자신의 ID를 응답하면 리더는 이를 Back-end Server로 전송하여 인증절차를 수행하고 태그의 정보를 불러온다. 그림 1은 RFID 시스템의 구성요소와 동작 절차를 보여준다. 의료분야에서 RFID는 환자, 의사, 의료자산, 혈액, 의약품, 의료기기 등에 태그를 부착하고 병원 내부 설치된 리더기를 통해 환자의 상태나 위치를 파악하고 의료자산 및 의료진의 자원 활용도를 높인다. 또한 투약, 수혈, 수술 중 사고를 방지하기 위해 사용된다. 앞으로의 의료분야는 RFID를 활용하여 환자 관리, 모니터링, 병원 자원관리 등을 실시간으로 제어할 것으로 전망하고 있다.^[3]

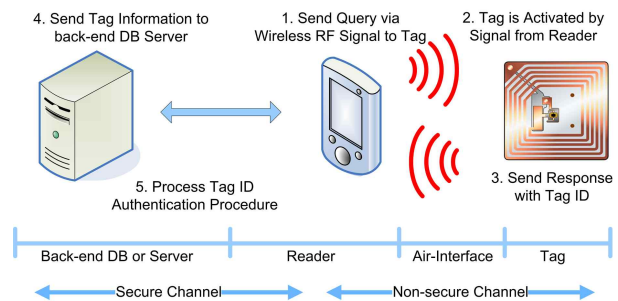


그림 1. RFID System 동작 절차

Fig 1. Operating Procedure of RFID System

III. 환자 태그 ID 세분화 기법

3장에서는 RFID/UMSN 환경에서 각종 의료시설 및 병원 내 u-Healthcare 서비스 시스템의 효율적인 인증과 위치 추적, 도청 등의 보안 위협을 최소화하기 위한 환자 태그 ID 세분화 기법을 제안한다. RFID/UMSN 환경에서 환자와 의료진, 의료기기, 각종 의료자산 등에 많은 수의 태그가 부착되고 병원 내 설치된 리더기들이 이들 모두를 인식하여 Back-end Server로 인증을 요청한다면 여러 개의 리더기가 하나의 태그에 대해 중복된 인증을 요청하는 경우가 생기고 Back-end Server는 이에 대해

여 불필요한 중복된 인증을 수행할 것이다. 따라서 Back-end Server에 걸리는 트래픽은 증가되고 전체 시스템의 효율이 떨어지게 된다. 예를 들어 환자, 의료진, 의료기기, 의약품, 의료자산 등에 부착된 태그가 서로 다른 관리 시스템의 리더기에 읽혀 인증이 요청되면 Back-end Server가 불필요하고 중복된 인증을 수행함으로써 트래픽이 증가하고 다른 태그의 인증을 수행하기 위한 자원을 낭비하여 전체적인 시스템 효율이 저하된다. 제안 기법은 환자, 의료진, 기타 의료자산 등을 집단으로 나누거나 환자 집단을 각 과별로 세분화하여 그룹화 하고 리더가 지정한 집단의 태그에 대해서만 Back-end Server와 인증절차를 수행하게 해 연산량을 줄인다. 제안 기법의 시스템은 리더간 간섭이 없는 안정된 리더 네트워크 기반이라 가정한다.

1. 환자 태그의 ID를 이용한 환자 집단 구분

병원 내 u-Healthcare 시스템은 환자뿐만 아니라 의료 기기, 의약품 등의 의료자산과 의료진까지 RFID 시스템을 이용해 관리할 수도 있다. 이 때 환자 관리용 시스템에 의료자산 관리용으로 의료기기에 의약품에 부착된 태그가 읽혀 태그 인증이 요청될 경우 환자 관리 시스템의 Back-end Server는 불필요한 인증을 수행하게 되고, 따라서 트래픽 증가와 자원 낭비가 발생한다. 또한 환자 관리에서도 서로 다른 과로 구분된 환자들 중 자신의 진료과가 아닌 다른과의 리더에 의해 태그가 읽혀 불필요하게 다른과 시스템의 Back-end Server에 인증을 요청하고 Back-end Server는 이를 수행해 트래픽 증가와 자원

낭비를 유발할 수 있다. 제안 기법은 관리하고자 하는 환자들의 태그를 태그 ID 문자열을 이용해 분류하여 집단으로 구분하고 이 집단에 인가된 리더를 설정한 후 집단에 인가된 리더에 의해 전송된 태그 ID에 대해서만 Back-end Server가 인증절차를 수행하도록 한다. 병원의 병실이나 진료과에서 특정 환자들만 인식해 인증을 수행해야 할 필요가 있을 경우 인식을 원하는 집단에 인가된 리더로 인식하면 불필요하거나 중복된 인증으로 발생하는 Back-end Server의 트래픽을 줄이고 그 과정에서 발생할 수 있는 보안 위협을 줄일 수 있다.

RFID 태그는 식별을 위해 유일성을 가진 ID를 지니고 있다. 제안 시스템은 Back-end Server에 구축되어 태그 고유 ID 문자열을 비교해 집단을 구분하고 리더에 인가된 환자 태그 집단을 지정한 후 태그 정보를 DB에 저장해 리더가 환자 태그를 인식했을 때 환자 태그의 ID로 집단 정보를 비교하여 인가된 집단의 태그에 대해서만 인증 절차를 수행하도록 한다. 표 1은 태그 ID 문자열 표기를 이용해 환자 태그를 그룹으로 나눈 예이다. 태그 1부터 태그 10까지 ID 문자열의 10번째 문자까지가 모두 같고 11번째 문자가 태그 1부터 7까지는 '7', 태그 8부터 10까지는 '9'로 다르다. 11번째 문자부터 두 그룹의 태그 ID가 구분되기 때문에 Tree Walking^[4] 알고리즘에 의해 두 태그가 서로 다른 집단으로 구분될 수 있다. 표 2은 환자 태그 집단을 계속해서 세분화 할 경우 마지막 문자열에서는 결국 하나의 환자 태그가 하나의 집단으로 구분되는 과정을 보여준다.

표 1. 환자 태그 ID 11번째 문자열 기준 집단 구분 예
Table 1. Patient Group Classification by 11th ID String

환자 Group	Group	1	1	1	1	1	1	1	1	1	2	2	2	5	8	9	10	
	No	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
환자 Group A	Tag 1	E	0	0	4	0	1	0	0	0	0	7	7	8	8	F	C	2
	Tag 2	E	0	0	4	0	1	0	0	0	0	7	7	8	7	4	4	5
	Tag 3	E	0	0	4	0	1	0	0	0	0	7	7	8	A	3	D	9
	Tag 4	E	0	0	4	0	1	0	0	0	0	7	7	8	A	4	8	4
	Tag 5	E	0	0	4	0	1	0	0	0	0	7	7	8	B	4	A	2
	Tag 6	E	0	0	4	0	1	0	0	0	0	7	7	8	B	4	6	3
	Tag 7	E	0	0	4	0	1	0	0	0	0	7	7	8	B	5	F	4
환자 Group B	Tag 8	E	0	0	4	0	1	0	0	0	0	9	A	C	D	B	E	D
	Tag 9	E	0	0	4	0	1	0	0	0	0	9	A	C	D	B	E	0
	Tag 10	E	0	0	4	0	1	0	0	0	0	9	A	C	D	D	5	4

표 2. 환자 태그 ID 문자열을 이용한 집단 구분 과정
Table 2. Procedure of Patient Tag Grouping by ID String

환자 Group	Group No	1	1	1	1	1	1	1	1	1	2	2	2	5	8	9	10	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Group A	Tag 1	E	0	0	4	0	1	0	0	0	0	7	7	8	8	F	C	2
Group B	Tag 2	E	0	0	4	0	1	0	0	0	0	7	7	8	7	4	4	5
Group C	Tag 3	E	0	0	4	0	1	0	0	0	0	7	7	8	A	3	D	9
Group D	Tag 4	E	0	0	4	0	1	0	0	0	0	7	7	8	A	4	8	4
Group E	Tag 5	E	0	0	4	0	1	0	0	0	0	7	7	8	B	4	A	2
Group F	Tag 6	E	0	0	4	0	1	0	0	0	0	7	7	8	B	4	6	3
Group G	Tag 7	E	0	0	4	0	1	0	0	0	0	7	7	8	B	5	F	4
Group H	Tag 8	E	0	0	4	0	1	0	0	0	0	9	A	C	D	B	E	D
Group I	Tag 9	E	0	0	4	0	1	0	0	0	0	9	A	C	D	B	E	0
Group J	Tag 10	E	0	0	4	0	1	0	0	0	0	9	A	C	D	D	5	4

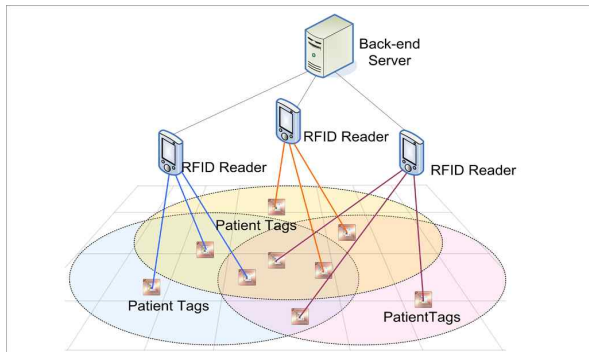


그림 2. 제안 시스템 RFID 시스템 환경
Fig. 2. RFID System Environment of Proposed System

2. 제안 시스템의 환자 태그 집단 인증 절차

그림 3은 제안 시스템이 RFID 리더로부터 환자 태그의 ID를 전송받아 Back-end Server와 인증을 수행하기 위한 절차이다. 환자 태그 ID로 집단을 설정하면 DB의 태그 정보에 각각의 태그가 속한 집단 정보를 저장한다. 환자 태그별로 집단이 정해지고 그 정보가 저장되면 리더에 태그를 인식할 때 어느 집단의 태그만 읽을 것인지 지정할 수 있다. 먼저 RFID 리더가 인식할 환자의 집단을 지정하고 태그를 인식해 ID를 전송하면 제안 시스템은 DB에서 태그 정보를 불러온다. 불러온 태그 정보의 태그 ID목록과 인식한 태그의 ID를 비교하여 인식한 태그의 ID가 DB에서 불러온 태그 ID목록에 존재하면 DB에서 불러온 태그 정보 중 인식한 태그의 집단정보가 리더에 지정한 집단과 같은지 비교한다. 이 때 환자가 속한 집단이 태그 ID를 전송한 리더에 인가된 집단일 경우 시스템은 이 태그의 정보를 Back-end Server로 보내 인증

절차를 수행하도록 한다. 인증절차를 거치면 Back-end Server는 환자의 정보를 환자관리 시스템에 전송하여 저장하거나 실시간으로 의료진의 전자차트로 전송하여 실시간으로 환자의 위치, 상태 등을 파악할 수 있게 한다. 환자의 태그가 인가된 집단에 속해있지 않을 경우 Back-end Server는 인증절차를 수행하지 않고 다시 다음 태그의 정보를 받을 준비를 한다.

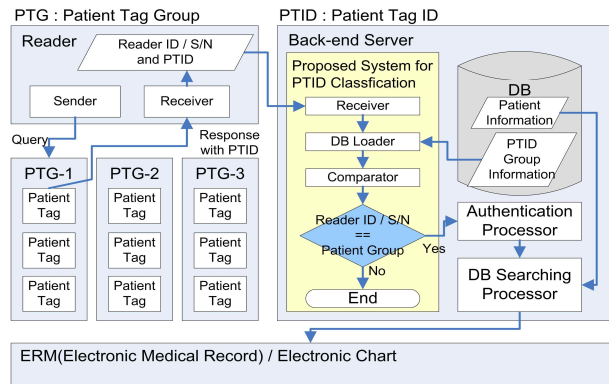


그림 3 제안 기법의 환자 태그 인증절차
Fig. 3. Patient Tag Authentication Procedure

3. 환자 태그 집단 설정을 위한 인터페이스

그림 4는 태그 ID를 이용해 환자의 집단을 분류하기 위한 환자 태그 집단 설정 어플리케이션의 인터페이스이다. 전체 환자의 태그 ID를 문자열로 DB에 저장하고 저장된 태그 ID를 몇 개의 집단으로 설정할 것인지 선택한다. 프로그램은 태그 ID 문자열을 비교해 생성할 수 있는 집단의 수를 보여준다. 좌측이 환자 태그 ID를 몇 개의 집단으로 만들 것인지 선택해 설정 하는 부분이다. 몇 개의 집단으로 나눌 것인지 선택하면 DB에 저장된 태그 목록

과 태그별로 지정된 집단의 그룹번호가 나타난다. 우측의 목록은 인증하고자 하는 환자 집단의 그룹 번호를 지정하고 태그를 인식했을 때 현재 리더에 인가된 집단의 환자 태그일 경우만 인증을 수행하고 태그 정보를 출력한다. 하단은 RFID 리더의 포트 설정과 태그 메모리 공간의 데이터 입출력 기능이다.

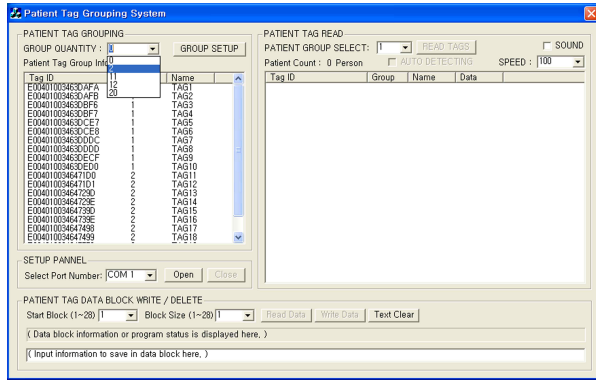


그림 4. 제안 시스템의 환자 태그 집단 설정 인터페이스
Fig. 4 Patient Tag Grouping Interface of Proposed System

IV. 성능분석 및 비교

제안한 기법의 성능분석을 위해 전체 환자의 태그를 인증하는데 걸린 총소요시간을 기준으로 제안 기법을 적용하지 않았을 때와 비교하여 분석했다.

1. 성능평가를 위한 전체 인증 소요시간 분석

전체 인증 소요시간 분석을 위해 파라미터를 표 3과 같이 정의하고 13.56MHz RFID의 신호 전송시간을 기준으로 각 구간별 인증을 위한 데이터와 메시지 전송시간을 설정하였다. 태그와 리더간에는 해쉬함수를 이용한 인증 프로토콜을 사용하고 리더 네트워크는 리더간 간섭이 없다고 가정한다. 그림 5는 제안 기법을 사용하지 않았을 때 전체 인증 소요시간 분석이다. 태그 집단 구분이 없어 모든 리더가 모든 태그를 읽어 Back-end Server에 인증을 요청한다. 따라서 똑같은 태그에 대해 리더의 수만큼 중복된 인증절차를 수행한다. 식 1은 인증에 걸리는 총소요시간을 식으로 나타낸 것이다.

표 3. 전체 인증 소요시간을 구하기 위한 파라미터
Table 3. Parameter Definition for Performance Analysis

TTot	전체 환자 태그의 인증 소요시간
TRP	전체 환자 태그를 읽고 Back-end Server와 리더가 메시지를 송신하거나 수신하는 시간(2ms)
Ta	Back-end Server가 태그 1개를 인증하기 위한 인증프로토콜 수행, DB 검색에 걸리는 시간 (=240ms)
nGT	환자 집단 내 환자(태그) 수 (default : 20명)
nR	리더기 개수 (default : 5EA)

- 리더 하나에 환자 태그 집단을 하나씩 지정
- 하나의 집단에 환자(태그)의 수는 모두 같음
- 전체 환자(태그)수 = 리더수(nR) × 환자 집단의 수(nGT)

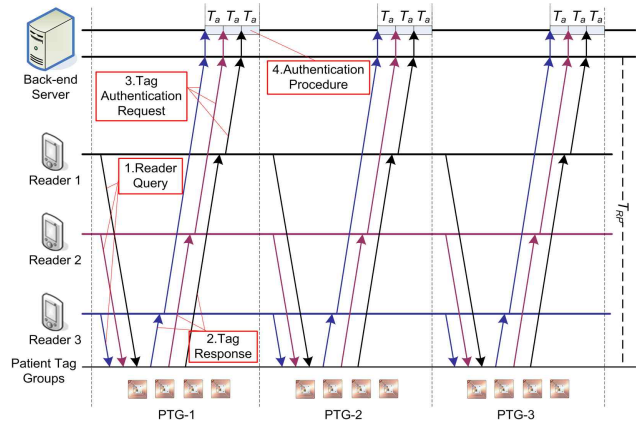


그림 5. 환자 집단 구분이 없는 전체 인증 소요시간 분석
Fig. 5. Total Authentication Latency Analysis of No PTG

$$T_{Tot} = \{n_R(n_{GT}n_R)\}T_a + \{(n_Rn_{GT})T_{RP}\}n_R \quad (1)$$

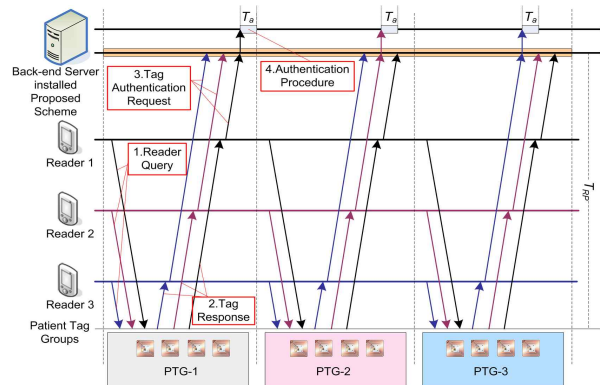


그림 6. 환자 집단을 구분한 전체 인증 소요시간 분석
Fig. 6. Total Authentication Latency Analysis of PTG

그림 6은 제안 기법을 적용하였을 때 모든 환자 태그의 인증에 소요되는 시간을 분석한 그림이다. 태그를 부착한 환자를 집단으로 나누고 해당 집단에 인가된 리더를 설정한다. Back-end Server가 리더로부터 환자 태그 ID를 받았을 때 인가된 리더로부터 전송된 태그 ID에 대해서만 인증절차를 수행한다. 따라서 Back-end Server는 모든 리더가 모든 태그를 읽어 리더의 수만큼 중복된 인증을 요청해도 중복 없이 한 번만 인증을 수행해 전체 인증 소요시간이 줄어든다. 식 2는 제안 기법으로 전체 환자 태그의 인증절차를 수행하는데 걸리는 소요시간을 식으로 나타낸 것이다.

$$T_{Tot} = (n_{GT}n_R)T_a + \{(n_Rn_{GT})T_{RP}\}n_R \quad (2)$$

2. 성능 평가 및 비교

성능 평가와 비교를 위해 각 집단 내에 속한 환자 수가 증가할 때, 리더와 환자 집단의 수가 증가할 때, 그리고 Back-end Server의 DB 검색시간과 태그 인증프로토콜 처리 시간이 증가할 때 제안 기법을 적용한 경우와 그렇지 않았을 경우 전체 태그를 인증하는데 걸린 총 인증 소요시간 변화를 그래프로 나타내었다. 그림 7은 한 환자 집단 내 환자 수를 20명으로 고정하여 설정하고 리더와 환자집단의 수가 증가할 때 전체 인증 소요시간의 증가를 보여준다. 제안 기법을 적용하지 않은 경우 리더와 환자 집단의 수가 늘어남에 따라 발생하는 중복 인증 횟수가 늘어나 제안 기법을 적용했을 때 보다 훨씬 증가율이 큰 것을 볼 수 있다. 그림 8은 리더와 환자 집단의 수를 5개로 설정하고 하나의 집단에 속한 환자들의 수가 10명씩 증가할 때 전체 인증 소요시간의 증가율을 보여준다. 전체 인증 소요시간의 증가율이 제안기법을 사용하였을 경우 훨씬 낮은 것을 확인할 수 있다. Back-end Server는 인증 처리에 걸리는 시간이 줄어들면서 트래픽이 감소하고 자원의 낭비를 줄인다. 따라서 환자 태그 인증과 시스템 및 의료진에게의 환자 정보 전달을 보다 효율적으로 할 수 있다. 그림 9는 Back-end Server가 환자 태그 인증 프로토콜 수행과 DB 검색시간이 증가함에 따라 전체 인증 소요시간의 변화를 보여준다. 좀 더 복잡한 인증 프로토콜을 사용해 수행 시간이 늘어나면 환자 집단을 구분한 경우, 그렇지 않을 때 보다 효율적인 것을 확인할 수 있다.

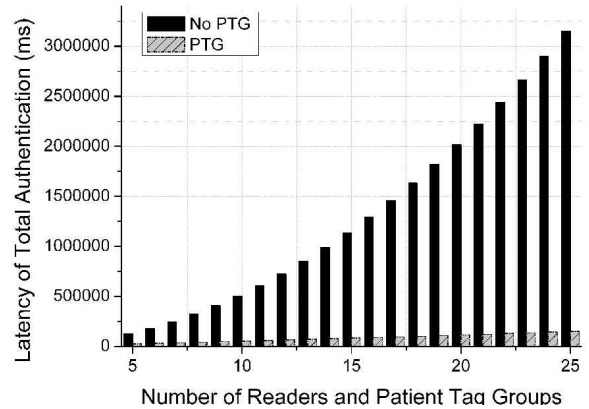


그림 7. 리더와 환자집단 증가에 따른 전체 인증지연시간
Fig. 7. Total Authentication Latency According to Number of Readers Increasing

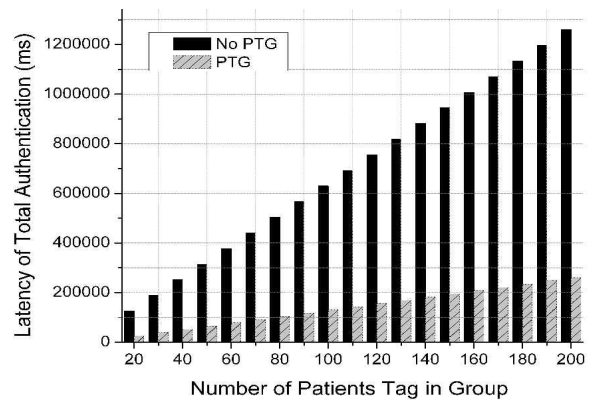


그림 8. 집단 내 환자 수 증가에 따른 전체 인증지연시간
Fig. 8. Total Authentication Latency According to Number of Patients Increasing in Group

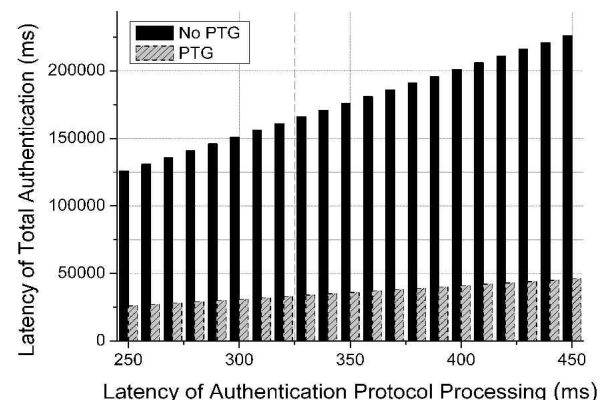


그림 9. DB검색/인증시간 증가에 따른 전체 인증지연시간
Fig. 9. Total Authentication Latency According to DB Searching/Authentication latency Increasing

V. 결 론

본 논문에서는 의료시설 내 RFID/UMSN 기반의 환자관리 시스템에서 의료자산, 의료진, 서로 다른 과에 속한 환자의 태그를 리더가 중복으로 인식함에 따라 발생할 수 있는 Back-end Server의 트래픽을 줄이고 불필요한 인증 과정에서 발생할 수 있는 보안위협을 최소화하기 위해 환자의 태그 ID로 환자 집단을 구분하는 환자 태그 ID 세분화 기법을 제안했다. 제안 기법은 환자집단에 인가된 리더가 읽은 태그만 Back-end Server가 인증절차를 수행하도록 해 불필요하게 인식된 태그의 인증절차를 차단한다. 따라서 Back-end Server가 인증을 처리하는데 소요되는 총 지연시간이 줄어들어 트래픽을 줄이고 시스템의 효율성을 높일 수 있다.

참 고 문 헌

- [1] 박동균, 정은영, 정국상 “의료분야에서의 RFID/UMSN 기술 적용 현황” 한국통신학회지 제25권 제10호, p.50~57, 2008.
- [2] F. Klaus, "RFID handbook" Second Edition, Jone Willey & Sons, 2003, pp.61-110
- [3] 최길영, 성낙선, 모희숙, 박찬원, 권성호, "RFID 기술 및 표준화 동향" 전자통신동향분석 제22권 제3호, p.30, 2007
- [4] RFID in Healthcare, IDTechEX. Jan 02. 2005
- [5] Marcel Jacomet, Adrian Ehram, Urs Gehrig, "Contactless Identification Device With Anticollision Algorithm" IEEE Computer Society, CSCC'99, Conference on Circuits, Systems, Computers and Communications, 4-8 July 1999

※ 이 논문은 2010학년도 한남대학교 학술연구조성비 지원에 의하여 연구되었음.

저자 소개

이 기 정(준회원)



- 2009년 2월 : 한남대학교 (학사)
- 2009년 3월~현재 : 한남대학교 (석사과정)
- <주관심분야 : Ubiquitous Health Care, 무선 네트워크, IPv6, Seamless Handover, IPTV, NGN, IMS, SOA.>

박 성 원(회원)



- 1998년 연세대학교 간호학과 (학사)
- 2004년 연세대학교 간호학과 (석사)
- 2005년 연세대학교 간호학과 (박사)
- 2006년~2010년 2월 해천대학 간호학과 교수
- 2010년 3월~현재 한남대학교 간호학과 교수

<주관심분야 : Ubiquitous Health Care, Schizophrenia, Social Emotion Theory.>