RFID를 활용한 안전한 정보교환 시스템†

*김일중 **최은영 ***이동훈

고려대학교 정보경영공학전문대학원

*wyvern99@korea.ac.kr **bluecey@cist.korea.ac.kr ***donghlee@korea.ac.kr

Secure information exchange system using RFID

*Il Jung Kim **Eun Young Choi ***Dong Hoon Lee

Graduate School of Information Management and Security, Korea University

요약

유비쿼터스의 핵심 기술인 RFID는 무선으로 사물을 인식하는 이점 때문에 많은 분야에서 적용되고 있다. 특히 위치추적 및 효율적인 자원관리가 가능하여 사용자의 건강과 관련된 헬스케어 서비스 시스템에서의 활용에 많은 연구가 진행되고 있다. 현재 RFID를 이용한 헬스케어 시스템에서는 사용자의 신상정보 및 사용자의 상태정보, 처방전등 민감한 의료 정보가 시스템의 무선 통신과정에서 사용된다. 하지만 환자의 신상정보와 처방전 같은 무선 통신과정의 정보는 공격자에 의해서 쉽게 도청 가능하기 때문에 사용자의 프라이버시 침해가 발생할 수 있다.

본 논문에서는 기존에 제안된RFID를 이용한 헬스케어 시스템에 대해 살펴보고 RFID를 이용한 헬스케어 시스템에서 발생하는 보안상의 문제점과 프라이버시 침해 문제점에 대하여 지적하고 그에 대한 해결방안을 제시한다.

1. 서론

RFID(Radio Frequency IDentification)는 유비쿼터스의 핵심기술로 RF(Rdio Frequrncy) 신호를 이용하여 사물에 직접적인 접촉하지 않고 사물의 정보를 자동으로 인식하는 기술이다. RFID가 가지는 비접촉통신, 많은양의 정보를 저장할 수 있는 능력과 같은 장점들은 기존의 바코드 시스템을 대체할 수 있다. 이러한 RFID 시스템의 장점들을 많은 분야에서 연구되고 있다[2,3,4,5,6,7,8,9,10]. 최근 RFID를 적용한 많은 분야 중에서 의료장비와 환자 건강관리에 관련된 헬스케어 시스템에 대해 큰 주목을 받으며 많은 연구가 이루어지고 있다[1]. RFID를 이용한 헬스케어 시스템에서는 RFID 리더를 사용하여 신상 정보, 처방전, 진료기록 등 환자에 대한 정보를 읽어온다. RFID 리더를 사용하여 환자의 태그로부터 RF(Radio Frequency) 신호를 이용하여 환자의 정보를 읽어오는 과정에서 환자의 정보가 그대로 들어나기 때문에 악의적인 공격자에 의해서 도청될 수 있다. 공격자에게 환자의 정보가 유출되면 환자의 프라이버시를 침해할 수 있으며 환자에 대한 정보가 위조 또는 변조될 수 있어 심각한 문제를 발생 시킬 수 있다.

본 논문에서는 기존에 제안된 RFID를 이용한 헬스케어 시스템의 보안 및 프라이버시 침해 문제에 대하여 분석하고 취약점에 대한 요구사항들을 제안한다.

† 본 논문은 서울시 산학연 협력사업(10665)의 지원으로 수행된 연구임

본 논문의 2장은 기존에 제안된 RFID를 이용한 헬스케어 시스템[1]에 대하여 설명하고, 3장에서는 2장에서 설명한 RFID를 이용한 헬스케어 시스템[1]의 보안상의 문제점과 프라이버시 문제점에 대하여 이야기하고 환자의 프라이버시 침해를 예방할 수 있는 보안 및 프라이버시 요구사항에 대하여 제안하고, 4장을 끝으로 결론을 맺는다.

2. 기존 연구

본 장에서는 기존에 RFID를 이용한 헬스케어 시스템을 제안한 [1]에 대해서 설명한다.

2.1 RFID를 이용한 헬스케어 시스템

[1]에서 제안한 프로토콜 중에서 스케줄링 프로토콜, 모니터닝 프로토콜에 대하여 설명한다. 표 1은 [1]에서 사용하는 용어의 정의이다.

2.2 스케줄링 프로토콜

스케줄링 프로토콜은 의사와 환자 사이의 스케줄링 프로토콜, 간호사와 의사 사이의 스케줄링 프로토콜, 환자와 간호사 사이의 스케줄링 프로토콜로 나누어진다.

(1) 의사 - 환자 스케줄링 프로토콜

그림 1은 의사와 환자사이의 스케줄링 프로토콜을 나타낸

용 어	정 의
RFID, DID, NID	환자 ID, 의사 ID, 간호사 ID
UInfo	초기에 환자가 병원에 등록한 사용자 신상정보
IS(Initial State)	초기 환자의 상태 정보
Message	의사가 발급하는 처방에 대한 확인정보
S	환자의 초기 처방
S'	진찰 후 갱신된 환자의 처방
T	타임스탬프
NotiM	수신 메시지에 대한 확인 메시지
LI	초기에 환자가 입원한 위치에 설치된 송신기의 지역위치정보
LR	병원내부에 설치된 송신기의 지역위치 정보
LRn	n번째 송신기의 위치정보
Alert Message	환자에 대한 응급 메시지

표 1 용어정의

것이다. RFID 리더가 포함된 송신기는 환자의 태그로부터 환자의 ID값을 받는다. 송신기는 환자의 ID와 초기 환자의 신상정보를 함께 의사의 PDA로 전송한다. 의사는 자신의 ID와 수신한 환자의 ID, 초기 환자의 상태 정보, 처방전에 대한 확인정보를 송신기로 보낸다. 송신기는 의사의 ID와 처방에 대한 정보를 환자의 태그에 전송한다.

환자와 송신기 사이에 RF통신을 이용하여 이루어지기 때문에 악의적인 제 삼자에 의해서 도청 당할 수 있어 환자의 프라이버시를 침해 할 수 있다.

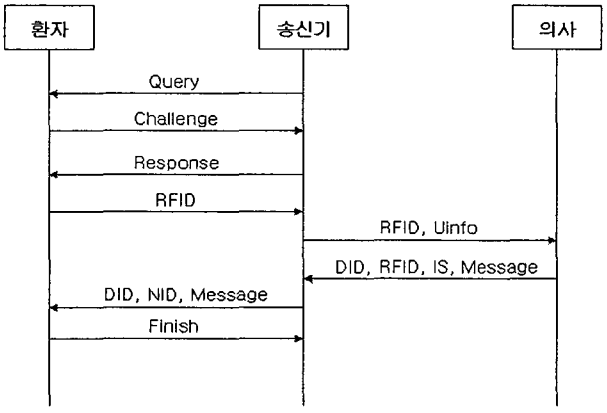

그림 1 의사 - 환자 스케줄링 프로토콜

(2) 간호사 - 의사 스케줄링 프로토콜

그림 2는 간호사 의사사이의 스케줄링 프로토콜을 나타낸 것이다. IMS를 통한 처방전을 확인 후 간호사 ID와 현재의 환자 처방 정보를 의사에게 전송한다. 의사는 간호사 ID와 환자의 ID를 확인한 후 환자 처방의 갱신여부를 판단한다. 의사는 IMS 서버에 의사 ID와 처방확인 메시지와 환자 정보를 전송한다. 의사는 IMS에 저장된 환자의 정보를 간호사의 PDA로 전송한다.

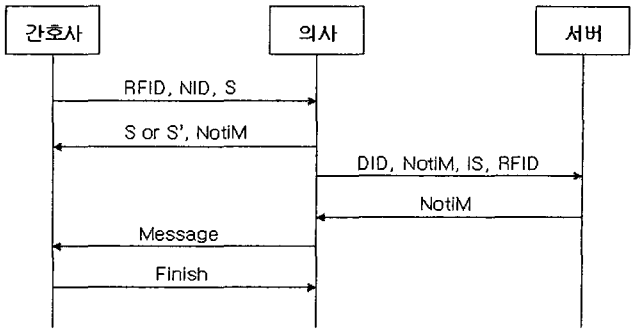

그림 2 간호사 - 의사 스케줄링 프로토콜

(3) 환자 - 간호사 스케줄링 프로토콜

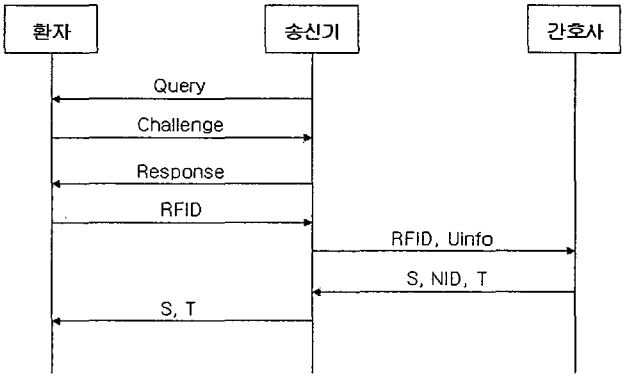

그림 3 환자 - 간호사 스케줄링 프로토콜

그림 3은 환자 간호사사이의 스케줄링 프로토콜을 나타낸 것이다. RFID 리더가 포함된 송신기는 환자의 태그로부터 환자 ID를 받는다. 송신기는 환자 ID와 초기 환자의 신상 정보를 간호사에게 보낸다. 간호사는 환자 ID와 초기 환자의 신상 정보를 확인하고 간호사 ID, 처방정보, 처방 정보를 보낸 시간의 타임스탬프를 송신기에 전송한다. 송신기는 간호사로부터 받은 처방 정보와 타임스탬프를 환자에게 전송한다.

2.3 모니터링 프로토콜

모니터링 프로토콜은 환자의 위치를 검색하기 위한 프로토콜이다.(그림 4)

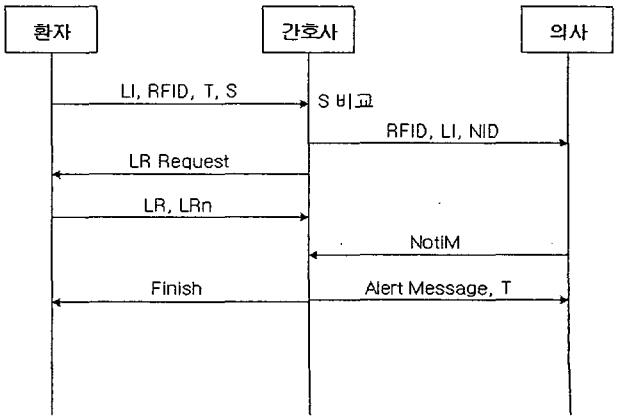

그림 4 모니터링 프로토콜

RFID 리더를 포함하고 있는 송신기는 환자의 위치정보 LI, 환자 ID, 처방 정보, 타임스탬프를 간호사의 PDA로 전송한다. 간호사는 환자의 처방 정보에 따라 정당한 이동경로일 경우 해당 환자 ID, 위치정보 LI, 간호사 ID를 의사에게 전송한다.

간호사는 현재 환자의 위치정보에 따른 송신기(리더)의 위치 정보를 요청한다. 위치정보를 요청받은 송신기(리더)는 현재 송신기의 고유번호 LRn과 지역 위치 정보 LR을 간호사에게 전송한다. 간호사는 LR, LRn을 확인 후 환자가 정당한 위치에 있지 않거나 응급상황이 발생하면 이에 대한 응급 메세지를 의사에게 보낸다.

3. 보안 및 프라이버시 문제점과 요구사항

2장에서 RFID를 적용한 헬스케어 시스템을 제안한 [1]에 대하여 설명하였다. 본 장에서는 [1]에서 제안한 프로토콜들의 보안 및 프라이버시 문제에 대하여 지적하고 그에 대한 보안 및 프라이버시 침해 문제 예방에 필요한 요구사항들을 제시한다. [1]에서 제안한 프로토콜에서 다음과 같은 보안성에 대한 요구사항을 제시하였다.

- 환자의 태그에서 초기사용자 정보를 신뢰할 수 있는 개체의 인증을 거쳐 수행
- 인증시 참여자의 태그에 기반을 둔 인증을 수행하고 PDA는 사전에 배포된 PTD로 교려하여 인증과 보안성을 유지
- IMS에 대한 접근제어는 의사의 ID와 접근시 요구되는 타임스탬프를 통해 불법 사용자에 대한 접근의 최소화
- 각 개체의 모바일 기기는 서록 독립적으로 구성되어 상호 처리되는 정보의 프로세스가 기밀저장 형식을 갖도록 하기 위해 PDA의 PTD를 기반으로 수행

하지만 위의 4가지 요구사항이 충족되더라도 RFID 시스템의 특성상 RF신호를 이용하여 환자의 태그로부터 환자의 정보를 주거나 받기 때문에 공격자에 의해서 도청 당할 수 있다. 환자의 정보를 공격자에 의해 도청되면 환자의 프라이버시를 침해할 뿐만 아니라 환자의 정보를 변조하거나 위조가 가능하여 심각한 문제를 발생시킬 수 있다. 위의 4가지의 요구사항에 추가적인 보안 및 프라이버시 침해 문제를 예방하기위한 요구사항이 필요하다. 다음과 같은 보안 및 프라이버시 침해 문제를 예방하기위한 요구사항을 제시한다.

(1) 정보 유출 방지
공격자에 의해서 환자 ID, 간호사 ID, 의사 ID가 노출되지 않아야한다. 위에서 제안된 요구사항에 따라 PDA와 송신기 그리고 서버 사이의 통신이 안전하더라도 태그와 리더가 포함된 송신기 사이의 통신이 RF신호를 통하여 정보를 주고 받기 때문에 태그에서 자신의 ID를 감출 수 있는 연산과정이 필요하다. 그리고 송신기는 감추어진 ID에서 원래의 ID를 복원하는 연산과정이 요구된다.

(2) 위치 추적 불가능
모니터링 프로토콜에서 송신기는 환자 ID를 추적하여 환자의 위치를 추적가능 하다. 하지만 다른 여러 개의 RFID 리더를 가진 공격자 또한 환자의 위치를 추적가능하게 된다. 그렇기 때문에 송신기는 환자 ID를 추적할 수 있으되 공격자는 환자의 ID를 추적할 수 없게 해야 한다. 그렇기 위해서는 환자의 태그가 매번 다른 값으로 ID를 감추어 RFID 리더에게 ID를 응답해야하며 송신기는 매번 환자의 태그와의 통신에서 환자 ID를 복원 할 수 있어야한다.

(3) 태그 위조 불가능
환자의 태그에 대하여 공격자가 재전송 공격이나 스푸핑 공격을 이용하여 병원의 송신기에 환자인척 할 수 있다. 이러한 문제점도 위치 추적 불가능에서 사용한 방법과 같이 송신기와 환자 태그사이의 통신을 할 때 매번 다른 값으로 ID를 감추어 현제 세션에서 얻은 정보를 다음 세션에서 사용할 수 없게 하면 된다.

4. 결론

RFID 시스템이 유비쿼터스의 핵심 기술로서 많은 분야에서 널리 사용되고 있다. 최근 RFID 시스템을 적용한 헬스케어 시스템에 대한 많은 연구가 이루어지고 있다. 하지만 서버와의 통신에 관련된 보안에 대한 요구사항들이 제시되고 있지만 RFID 리더가 환자의 태그사이에 RF신호를 통하여 이루어지는 정보교환에 대한 보안이 미흡하여 환자의 프라이버시 침해 문제가 발생 할 수 있다. 본 논문에서는 기존의 RFID가 적용된 헬스케어 시스템[1]의 보안 및 프라이버시 침해 문제에 대하여 지적하고 예방하기위한 요구사항들을 제시하였다. 기존의 RFID 시스템에서 보안 및 프라이버시 침해 문제를 예방하기위해 제안된 요구사항들과 보안 기법들을 RFID를 이용한 헬스케어 시스템에 적용하여 효율적이면서 환자의 프라이버시가 침해되지 않는 헬스케어 시스템을 만들어야한다.

[참고문헌]

[1] 백장미, 홍인식, "RFID를 이용한 효율적인 환자관리 애플리케이션 시스템 개발에 관한 연구", 멀티미디어학회 논문지, pp 1142-1151, 2005.
[2] Eun Young Choi, Su-Mi Lee and Dong Hoon Lee. "Efficient RFID Authentication Protocol for Ubiquitous Computing Enviro- nment", EUC Workshops, 2005.

[3] K. Finkenzeller. "RFID handbook". John Wiley & Sons, 1999.

[4] A. Juels, R. Rivest, and M. Szydlo. "The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy". ACM CCS 2003, pp. 27-30, 2003.

[5] A. Juels, P. Syverson, and D. Bailey, "High-Power Proxies for Enhancing RFID Privacy and Utility", CHACS 2005, LNCS 3856, pp.210-226 ,2005

[6] H. Knospe and H. Pob. "RFID Security". Infomation Security Technical Report, vol. 9, no. 4, pp. 39-50, Elsevier, 2004.

[7] Soo-Cheol Kim, Sang-Soo Yeo, Sung Kwon Kim. "MARP: Mobile Agent for RFID Privacy Protection". 7th Smart Card Research and Advanced Application IFIP Conference (CARDIS'06), Lecture Notes in Computer Science, vol. 3928, pp. 300-312, 2006.

[8] M. Ohkubo, K. Suzuki, and S. Kinoshita. "A Cryptographic Approach to "Privacy-Friendly" tag". RFID Privacy Workshop, 2003.

[9] Damith Ranasinghe, Daniel Engels, and Peter Cole. "Low-Cost RFID Systems: Confronting Security and Privacy". Auto-ID Labs Research Workshop, 2004

[10] S. A. Weis, S. Sarma, R. Rivest, and D. Engels. "Security and privacy aspects of low-cost radio frequency identification systems". SPC 2004, LNCS 2802, pp. 201-212, 2004.