무선센서네트워크 환경하에서 RFID 헬스 시스템을 위한 보안 모델

김정태*

Privacy and Security Model for RFID Healthcare System in Wireless Communication Network

Jung Tae Kim*

이 논문은 2011년도 교육과학기술부의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2011-0026950)

요 약

무선 통신 환경 하에서 병원 등에서 모바일 에이전트의 사용은 환자, 병원의 의사 등의 관계자들에게 훨씬 더 좋은 서비스를 제공한다. 더군다나 이러한 의료 진단의 과정을 더욱더 효율적이며 안전하게 하기 위하여 모바일 환경하에서의 융복합 기술이 도입됨에 따라 의료의 기록 오류의 감소 및 편의성을 가져왔다. 다가오는 미래에는 더욱더 의료 환경하에서의 융복합 기술의 도입으로 활용도가 더욱더 높아질 것이다. 따라서 본 논문에서는 이러한 유비쿼터스 환경 하에서의 헬스케어를 위한 보안 메카니즘을 제안하고 이러한 무선 환경 하에서 발생할 수 있는 보안적인 문제점을 분석하였다.

ABSTRACT

The use of a mobile agent in hospital environment offers an opportunity to deliver better services for patients and staffs. Furthermore, medical errors will be reduced because M-health system helps to verify the medical process. Optimized security protocols and mechanisms are employed for the high performance and security. Finally, a challenge in the near future will be converge the integration of Ubiquitous Sensor Network (USN) with security protocols for applying the hospital environment. We proposed secure authentication and protocol with Mobile Agent for ubiquitous sensor network under healthcare system surroundings.

키워드

RFID, 유비쿼터스 헬스케어, 프로토콜, 네트워크보안

Key word

RFID, Ubiquitous Healthcare, Protocol, Network Security

* 종신회원 : 목원대학교 (교신저자, jtkim3050@mokwon.ac.kr)

접수일자 : 2012. 06. 01
심사완료일자 : 2012. 06. 01

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.6.1223

Ⅰ. 서 론

일반적으로 RFID 기술은 유비쿼터스 환경하에서의 원거리에 있는 물체를 인식하는 기술 중의 하나이다. RFID(Radio Frequency Identification)는 각종 물체에 소형 칩을 부착해 사물 및 센서노드와 같은 주변 환경정보를 무선 주파수로 전송 및 처리하는 비접촉식 인식 시스템이다. 1980년대부터 등장한 RFID 시스템은 근거리 통신 또는 무선 식별 시스템이라고도 불린다. 전형적인 RFID 시스템은 태그, 리더기, 백 엔드 서버로 구성되어 있다. 일반적으로 리더기는 태그의 반응을 서버에 전달하는 역할을 한다. 백 엔드 서버는 태그의 반응에 대한 태그에 대한 정보를 인증하는 역할을 한다. 저가의 RFID를 설계하기 위해서는 태그 측에서의 계산 성능에 관련된 문제이다. 이러한 문제는 제한된 연산 능력, 저 용량의 메모리, 낮은 전력 등의 문제를 가진다. 정보기술의 발전으로 공공 기관, 회사 등에서 이루어지는 정보의 전달 과정 등이 많은 발전을 가져왔다. 최근에는 전세계적으로 의료 기관 등에서 네트워크과 데이터베이스에 기반한 정보의 공유를 이루기 위한 방향으로 발전되고 있다. 현재까지도 많은 병원들은 이러한 정보기술을 이용한 시스템의 기술 개발 도입에 많은 진전을 보이지 못하고 있고, 기존의 오프라인 구조에 기만한 업무 프로세서를 고집하고 있다. 예를 들어 기존의 서류 기반의 시스템은 많은 사람들의 사용과 의료 기록의 오류 등을 종종 동반하는 등 제약적인 자원을 사용하는 단점을 가진다. 기존의 EMR (Electronic Medical Record), PACS (Picture Archiving and Communication System), OCS (Order Communication System)과 같은 E-health 시스템은 가격, 시간적인 감소, 정보의 확신, 실시간 처리, 소비자 중심의 서비스를 가져오는 계기가 되었다. 최근에는 기술의 발전으로 인하여 정보기술에 기반한 헬스캐어 시스템으로 발전하여 디지털 시스템으로의 융복합, 개인적인 홈 네트워킹 헬스캐어와 같은 유비쿼터스 환경으로 발전되고 있다. 이러한 기술의 발전으로 인하여 실시간 모니터링, 진단, 내재해 있는 병 등을 유무선 통신 채널을 통하여 환자와 의사간의 의료 진단을 위한 정보를 가능하게 한다[1,2,3].

Ⅱ. 관련 연구

21세기가 접어들면서 전 세계 인구는 급속하게 증가하고 있으며, 또한 노인 인구도 증가하고 있다. 이러한 의료 산업에 대한 요구를 효과적으로 대응하기 위하여 기존의 E-health에서 U-health 에 대한 수요가 증가되고 있다. 따라서 미국을 비롯한 유럽의 여러 나라에서 유비쿼터스 환경에 적합한 기술을 개발하고 있으며 최근에는 많은 기술적인 발전을 보이고 있다. 유비쿼터스 기반의 헬스시스템은 의학적인 E-commerce 와 원거리의 의약 정보와 같은 여러 가지의 요소를 구성하며, 인터넷과 무선 환경을 결합한 최신의 정보기술을 융합한 기술로 발전되고 있다. 이러한 기술을 통하여 헬스에 관련된 정보, 서비스를 언제 어디에서나 정보를 공유 할 수 있게 되었으며, 이러한 이유로 인하여 많은 국가들이 국가적인 프로젝트로 유비쿼터스에 기반한 헬스시스템의 개발에 많은 관심을 가지고 있다. 특히 병원에서의 업무 분장을 위하여 서로 다른 많은 요소를 가지고 업무를 분류하고 있다. 따라서 RFID 을 사용한 자료의 인식화 방안은 헬스캐어 서비스의 개선을 가져왔으며, 특히 환자, 의사, 스탭들이 RFID 태그가 내장된 리더기를 사용하여 정보의 인식 및 공유 등을 가능하게 되었다. 이와 관련된 많은 연구가 진행 되고 있다.

특히 HIS(Hospital Information System)에서 응용 가능한 RFID 시스템의 융합 기술은 자동화된 보안 문제를 해결하고 환자 들을 돌보고 관리하고, 병원에서의 여러 가지의 업무 할당 등을 위하여 유비쿼터스 환경 하에서 서로 유대 관계를 통하여 통합할 수 있는 기술로 발전되고 있다. 특히 호주의 뉴사우즈웰즈 정부에서는 100만불 이상을 투자하여 188개의 공공 병원을 대상으로 하여 기존의 문서기반의 헬스 정보를 대체할 목적으로 프로젝트를 실시하고 있다. 데이터, 정보, 통신의 효과적인 융합화로 인하여 호주인을 위한 국가적인 주요 프로젝트로 삼고 있다 [4,5,6].

Ⅲ. 제안한 보안 메카니즘

일반적으로 유비쿼터스 기반의 헬스시스템의 구성은다음과 같이 크게 4가지의 주요 구성 요소로 이루어지며 기본적인 개념도는 (그림 1)과 같다.

- Electronic Medical Record (EMR) System
- Schedule Management Application
- RFID Technology
- Remote Diagnosis (U-Healthcare system)

(그림 2)에서 보는바와 같이 주요 구성 요소는 크게 조직 행적에서의 보안 과 기술적인 보안 문제로 구분된다. 조직 행정에서의 보안적인 문제는 주로 보안 정책을 결정하기 위한 부분을 제어하기 위한 부분이다. 특히 고려해야 할 사항으로는 여러 가지의 보안 기술사이의 상관 관계를 고려하여 각 요소들을 잘 정의하여 유무선 통신에 적합한 기술들을 선택하여야 한다[7].

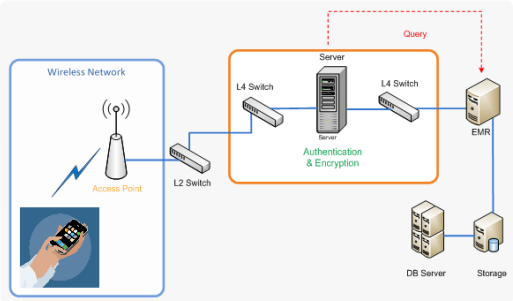

그림 1. 일반 병원의 네트워크 구성도
Fig. 1 Configuration of General Network in Hospital

이러한 기술을 선택하기 위한 전제 조건으로는 모든 보안적인 기술적인 요소들은 보안 정책에 의거하여 그 보안 등급을 결정해야 한다. 이러한 보안 정책들은 (그림 2)에선 보는바와 같이 네트워크보안, 시스템보안, 응용보안 등의 구성 요소를 정의하여야 한다.

그림 2. 헬스시스템에서의 보안 요구사항
Fig. 2 Requirement of Security for Healthcare System

보안 정책들의 구성 요소들은 데이터를 보호하고, 여러 가지의 보안 규정을 준수하기 위한 행정적인 자료로서 구성되어 지며 다음과 같은 사항을 포함한 자료이어야 한다.

- 목차: 서류의 간단한 정의
- 순서: 정책 서류의 유일한 인식표
- 제정일: 공식적으로 승인된 날짜
- 범위: 정책의 내용을 준수하는 보안상의 자산
- 정책 문서: 법률화된 정책
- 인가: 정책으로 입안된 문서
- DMZ (Demilitarized Zone): 내외부적인 접근사이의 데이터 거래의 제어
- 방화벽 : 내부의 네트워크 접근을 정책적 요소로 접근 금지
- 접근 제어 : 사용자의 신원 인증을 통한 접근
- 안전한와 토큰 : 외부의 악의적인 사람을 제어하기 위한 데이터의 교류 접근 방지

또한 이러한 시스템을 구성하기 위한 요소를 나타내면 다음 (그림 3)과 같다.

- Health Informatics Access Control (HIAC)
- Health Informatics Application Security (HIAS)
- Health Informatics Network Security (HINS)

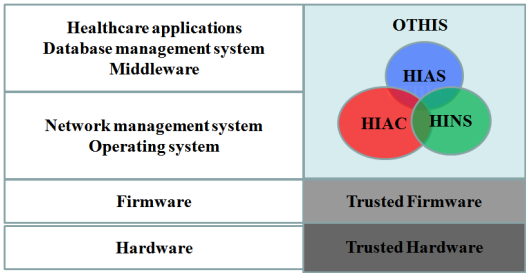

그림 3. 헬스케어 시스템의 구성도
Fig. 3 Configuration of Healthcare System

헬스 시스템에서의 위협 요소 중 대표적인 요소는 다음과 같으며, 일반적인 네트워크, 응용시스템, 데이터베이스 시스템에서 고려되고 있는 모든 내용을 포함하고 있다.

- User anonymity
- Message privacy
- Message confidentiality
- User authentication and authorization
- Replay attacks
- Confidentiality
- Integrity
- Availability

다음의 (그림3)은 사용자와 데이터베이스에서의 인증과정을 나타낸 프로토콜의 구성도이다. 프로토콜의 인증 과정을 나타내면 다음과 같다.

1. 사용자가 모바일 에이전트를 사용하여 일반적 802.11 프로토콜을 사용하여 Access point에 접근한다.
2. 엑세스 포인터에서 접근이 허용되면 SSL등의 네트워크 프로토콜을 이용하여 인증 서버에 접근한다.
3. 인증된 사용자는 challenge-response handshake에 기반한 인증 프로토콜을 사용하여 연결한다.
4. 인증된 사용자는 AES-CCMP 등과 같이 암호화된 세션 키를 사용하여 인증 서버에 연결된다.
5. 세션 키를 사용하여 인증된 사용자는 EMR 인증 서버에 연결되어 EMR 데이터베이스에 연결된다.

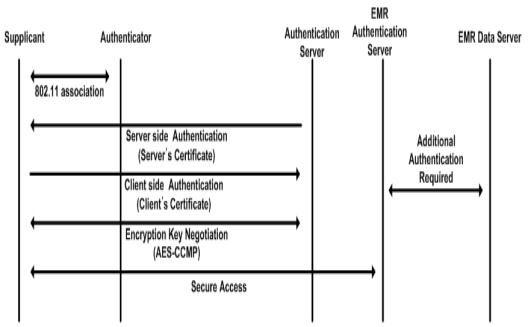

그림 4. 사용자와 데이터베이스에서의 인증 과정
Fig. 4 Process of Authentication Between Client and Database

이러한 인증 프로토콜의 안정성을 보장하기 위해서는 RFID 등과 같은 사용자의 모바일에이전트와 인증서버와 같은 리더기 사이의 데이터의 안정성을 증가시키기 위한 방법이 요구되어진다. 다음은 현재까지 연구되고 있는 대표적인 방법을 나타내고 있다.

- Full-fledged 방법 : 전자여권과 같은 분야에 응용되고 있으면 기존의 암호학적 방법인 단방향 해쉬함수 등을 사용한 방법이나 하드웨어적인 구성 요소가 많이 증가되는 단점을 가진다.
- simple 방법 : 태그에 단방향 해쉬함수를 사용하거나 의사유도난수 발생기를 이용한 방법으로서 태그에서의 저용량 메모리를 고려할 때 현실적인 대안이 되지 못하고 있다.
- Lightweight 방법 : 의사난수 발생기, CRC(Cyclic redundancy code) 등을 사용하여 하드웨어적인 구성요소를 줄이는 방법을 개선한 방법이다.
- Ultra-lightweight 방법 : XOR, AND, OR 과 같은 비트 연산을 사용한 단순한 방법을 사용하여 저가격의 RFID 시스템에 적용가능하나 보안상의 취약성을 가진다.

따라서 위에서 언급한 여러 가지의 방법을 사용하여 인증을 위한 프로토콜의 개발 및 태그의 암호화 엔진을 위한 경량화된 암호 알고리즘의 개발이 시급한다. 현재 2012년 1월 WG7은 공식 회의를 통하여 RFID에 대한 보안 서비스 제공에 필요한 요구사항을 만족하는 표준 기술을 위하여 많은 노력을 경주하고 있으며, 특히 수동형 UHF RFID 서비스의 본격적인 활성화를 위하여 보안기술의 표준화는 많은 진전을 보일 것으로 사료된다.

Ⅳ. 보안 메카니즘의 구성 요소

일반적으로 RFID 프로토콜의 취약성을 살펴보면 다음과 같다 .프로토콜의 보안성을 강화하기 위하여 일반적인 연산적인 방법이 태그에서의 용량에 의하여 기존의 방법이 사용되기가 어렵다. 따라서 태그에서의 정보를 유출하기 위한 외부의 여러 가지의 공격에 대한 방법을 고려하여야 한다. 따라서 다음의 사항을 고려하여야 한다. 일반적으로 RFID 기술을 이용한 응용기술들이 많이 발전되고 있다 [8]. 그러나 RFID 태그에서의 보안적인 취약점 및 위협으로부터 방어하기 위한 기술적인 발전이 다음과 같은 방법으로 발전되고 있다. 저가의 RFID를 위한 보안 기법을 내장한 설계가 많이 연구되고 있으나, 기존의 방법인 단방향 해쉬함수를 사용한 기법들이 사용되었는데, 이는 저가의 태그 구현에 적합하지 않다.

이러한 연구와는 상반된 개념으로 태그에 해쉬함수를 지원하는 구조로 설계할 경우, 태그의 저용량 리소스로 인하여 고비도의 암호 알고리즘을 제공하기는 불가능 한다. RFID 시스템의 경우, 연산 능력과 저장 능력에 제한이 있으므로 기존의 공개키 방식이나 대칭키 방식의 암호화 알고리즘을 적용하기는 적절하지 않다. 그러나 지금까지 발표된 연구결과의 대부분은 태그 내부에서의 실질적인 대칭키 암호 연산을 통한 보안 문제 해결로 접근하는 연구결과를 찾아보기 힘들다. 특히 수동형 RFID 태그가 가지는 자원 제약적인 환경 때문에 실제적인 표준 알고리즘인 AES 알고리즘을 사용하는 프로토콜의 사용이 현재 개발 진행 중에 있다. 일반적으로 저가형 태그는 배터리가 없어 제한적인 연산 능력과 메모리 공간을 가진 것으로 간주되고 있다. 하지만 기술적인 발전으로 인하여 최근에는 저가형 태그에 적합한 암호 알고리즘에 대한 연구가 활발히 진행 중에 있으며 A.Bogdanov 등은 저가형 태그 보안을 위한 보안 프리미티브의 요구사항인 2000 게이트 이하, 10uW 이하의 소비 전력, 10,000 클럭 사이클을 만족하는 암호학적 해쉬함수의 구현이 가능하다는 연구 결과를 발표하였다 [9]. 또한 M Feldhofer 등은 AES(Advanced Encryption Standard) 역시 저가형 태그에 구현이 가능하다는 연구결과를 발표하였다 [10].

- 경량화된 암호 기능
- 암화학 기능 수행을 위한 확률론적 방법에 기반한 프리 미티브의 개발
- 다중 태그 인식을 위한 새로운 형태의 보안 모델
- 사이드 채널 분석을 통한 위협적인 요소 제거 기술

그러나, 태그의 경우 작은 용량의 메모리의 구조 및 낮은 연산 능력으로 인하여 현재 개발된 기존의 암호 알고리즘을 채용하기에는 많은 보안상의 취약성을 나타낸다. 또한 일반적인 보안사항은 ISO/IEC FDIS 29167-1에서 권고한 암호학적인 보안 서비스를 요구하고 있다.

암호학적인 보안 서비스라 함은 태그 내부에서 암호 엔진을 구동하여 지원할 수 있는 보안 서비스를 의미하며 다음과 같은 기능을 내재하고 있어야 한다.

- 추적불가(Untraceability): 태그 아이디의 전부 또는 일부를 감출 수 있는 기능
- 진품 검증(Certify authentication): 하나 혹은 다수의 공중파를 이용한 인터페이스 명령에 대해 태그가 진품인지를 확인 할 수 있는 메카니즘을 증명
- 태그 데이터와 기능에 대한 안전한 접근(Secure access to tag data and functions): 태그 데이터 접근 제어와 기능 설정 접근 제어를 제공하며, 또한 전송데이터가 안전하게 통신할 수 있는 서비스
- 키 관리(Key management): 보안키가 안전하게 전달 되거나 저장될 수 있는 기능

V. 결 론

본 논문에서는 유비쿼터스 환경에 적합한 헬스 시스템의 보안적인 구성 요소에 대하여 제안하고 분석하였다. 주된 구성 요소로는 네트워크 보안, 시스템 보안, 응요 보안등으로 구성되며, 현재의 기술적인 기술 요소로서 기존의 관용 암호시스템을 이용하여 데이터베이스 보안, 네트워크 보안 등을 구성할 수 있으나, 외부에서의 개인적인 신분 인증 및 데이터를 인증하기 위한 RFID 태그에서의 보안적인 프리미티브의 취약성으로 인하여 현재에는 태그 보안 및 경량화 된 프로토콜 보안에 대한 연구가 진행되고 있다. 따라서 본 논문에서는 이에 대한 보안적인 문제점 해결을 위한 방안을 제시하였다. 태그에서의 연산능력의 부족으로 인하여 위협요소가 발생하고 있다. 따라서 이러한 문제점을 해결하기 위한 성능분석 및 위협요소에 대한 분석이 필수불가결하다. 또한 이러한 요소를 해결하기 위한 방법 중의 하나로 경량화된 프로토콜을 제안하여 문제를 해결하기 위한 여러 가지의 연구가 진행 중에 있다. 이 또한 디지털논리로 구현할 경우 태그에서의 면적의 문제로 인하여 해결이 어려움에 처할 수 있다. 따라서 반도체 칩의 공정 및 간단한 프로토콜의 개발이 필수적인 대안으로 자리를 잡을 것으로 생각된다.

감사의 글

이 논문은 2011년도 교육과학기술부의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2011-0026950)

참고문헌

[1] Ari Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal of selected areas in communications, V.24, N.2, pp.381-394, February, 2006

[2] H.Y. Chien. "SASI: A New Ultra-weight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions on Dependable and Secure Computing., vol.4, n.4, pp.337-340, Oct. 2007

[3] Feldhofer, etcs, "Strong authentication for RFID systems using the AES algorithm," Cryptographic hardware and embedded systems", CHES 2004, v.31, n.56, pp.357-370, 2004

[4] Azzedine Boukerche, et al, "A Secure Mobile Health System Using Trust-Based Multicast Scheme", IEEE J. On selected areas in communications, v.27, n.4, may 2009, pp.387-399.

[5] J.H.Kim and Sahama, T. "A Study on the Encryption Model for Numerical Data,", International Journal of KIMICS , vol.7, pp.31-34. 2009.

[6] Shinyoung Lim, "Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring", 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pp.327-332, 2010.

[7] Bong-Keun Rhee, etcs, "Privacy Model based on RBAC for U-Healthcare Service Environment", KIICE(Journal of The Korea Institute of Information and Communication Engineering), Vo.16, N.3, March 2012, pp.605-614

[8] Young-Jae Park, "On the Accuracy of RFID Tag Estimation Functions", JICCE(Journal of Information and Communication Convergency Engineering), V.10, N. 1, March 2012, pp.33-39

[9] Jung-Hyun Oh, etcs, "A Secure Communication Protocol for Low-cost RFID System", Seventh International Conference on Computer and Information Technology, pp.949-954, 2007.

[10] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "EMAP: A Efficient Mutual Authentication Protocol for Low-Cost RFID Tags," Proc. OTM Information Security Workshop (IS '06), pp. 352-361, 2006.

저자소개

김정태(Jung Tae Kim)

2001년 8월 : 연세대학교 대학원 전자공학과 박사
1991년 8월～1996년 2월 : 한국전자통신연구원(ETRI) 선임연구원
2002년 10월～현재 : 목원대학교 전자공학과 교수
※관심 분야: Network Security, 보안 컨설팅, RFID& USN Security, 통신용 ASIC Design.