RFID/USN 기반 안전한 출입통제 시스템 구현

송복섭*, 최연식*, 김정호*, 김철수**,류환규**
*한밭대학교 정보통신전문대학원 컴퓨터공학과
**창신정보통신(주)
e-mail:serve73@hanbat.ac.kr

Implementation of a Secure Access Control System Based on RFID/USN

Bok-Sob Song, Yeon-Sik Choi, Jeong-Ho Kim, Chul-Su Kim, Hwan-Gyu Ryu
*Dept. of Computer Engineering Graduate School of Information & Communication Hanbat National University.

요 약

USN 기술은 센서노드의 전류소모 감소를 위한 저전력 기술개발과 관련 기술력 확보를 위해 많은 연구가 지행되고 있다. 유비쿼터스 환경에서 보안의 취약성과 낮은 신뢰성 문제는 USN 기술의 상용화 성공을 위해 선행되어야할 요소이다. 본 연구에서는 보안 문제로 W-Key 알고리즘을 도입하여 키분배 관리, 인증관리, 환경관리로 구성하여 무선 Key기법과 다른 RFID/USN기반의 안전한 출입통제 시스템을 구현하였다.

1. 서론

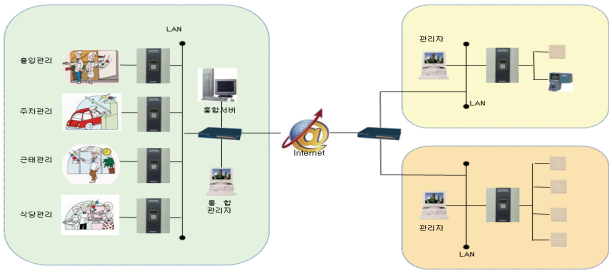
RFID 기술은 유통, 물류, 의류, 교육 등 다양한 분야에 적용되고 있으며 저주파, 고주파, 초고주파, 마이크로파 대역의 무선전파를 사용하여 각 대역의 전파 특성에 따라 동물추적, 교통카드, 물품관리, 전자화폐 등 다양한 분야에 선택적 적용되고 있다.

USN 기술은 센서노드의 전류소모 감소를 위한 저전력 기술개발과 관련 기술력 확보를 위해 연구기관과 기업의 적극적인 참여가 이루어지고 있으며, ETRI, KETI, 삼성, Radioplus, 태광 E&C, 옥타컴, 휴인스, Maxfo 등의 연구기관과 기업을 중심으로 다양한 형태의 센서노드를 개발 중에 있다. 국내의 USN 관련 기술 개발은 센서노드 플랫폼, 센서 네트워킹, 무선통신 및 미들웨어 기술 분야로 집중되어 왔었기 때문에 USN 관련 보안 기술은 USN의 다른 기술에 비해 초기 단계에 머물러 있다. 본 연구에서는 보안이 가장 중요한 핵심 요소인 출입통제 관리 분야에서 다양한 W-Key 알고리즘과 출입통제 서비스를 USN 응용에 적용할 수 있는 RFID/USN기반의 안전한 출입통제 시스템을 구현하고자 한다.

2. RFID/USN기반 안전한 출입통제시스템

RFID/USN 기반 안전한 출입통제 시스템은 특정 지역에 출입이 인가된 사람만 출입을 할 수 있도록 출입문의 개폐장치와 연동하여 시스템을 구성할 수 있다. 또한, 특정 지역을 출입하는 사람을 식별하여 식별된 정보를 제공함으로서, 해당 지역을 출입하는 사람에게 특화된 서비스를 제공 하거나 식별된 정보를 기반으로 대금을 지불하는 시스템 등을 위한 기반 장치로 활용될 수 있다. 본 연구에서 개발하고자 하는 RFID/USN 기반 안전한 출입통제 시스템은 (그림 1)에서 보듯이 입구에 RFID/USN 기반 안전한 출입통제 시스템을 설치하여 (그림 2)처럼 출입관리, 주차관리, 근태관리, 식대관리 등의 다양한 응용 서비스에서 사용자를 식별하여 서비스를 제공하기 위해 적용될 수 있으며, 통합관리 서버를 활용하여 여러 시스템/건물/지역/조직을 대상으로 서비스를 구성할 수 있다.

(그림 1) RFID/USN 기반 안전한 출입통제 시스템



(그림 2) RFID/USN 기반 안전한 출입통제시스템 구조

○ 출입통제장치(EECU : Entrance & Exit Control Unit): 기존의 RFID 출입 통제장치에 안전한 USN무선키 통

* 본 연구는 한밭대학교 2009년 산학협력중심대학 기술개발과제 사업화기술개발지원사업의 일환으로 수행하였음

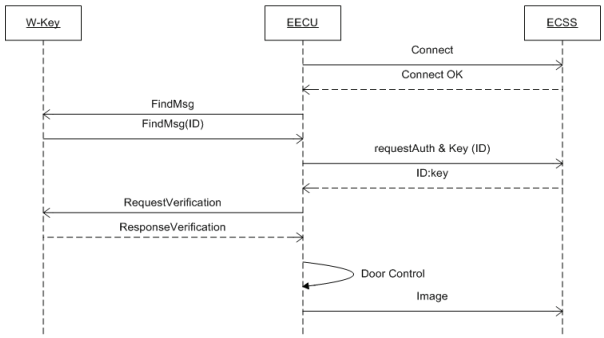
신을 도입하여 출입통제 서비스를 제공할 수 있도록 해주는 시스템으로 편리하면서도 기존 시스템 보다 안전하게 출입을 통제 할 수 있는 기능을 제공하는 출입통제장치

○ 개인용 무선 키(W-Key : Wireless Key):W-Key는 사용자 개인별로 소지하여 사용자를 대표하며, 출입통제 시스템에서 출입을 위한 인가를 위해 사용되는 무선 키로서, IEEE802.15.4 기반의 WPAN 무선통신 기술을 기반으로 Zigbee프로토콜을 이용하여 S-EECU와 무선으로 데이터를 교환하며, S-EECU와의 안전한 인증/인가 및 데이터 교환을 위해 보안기법을 사용하는 개인용 무선키

○ 출입통제 서비스 서버(ECSS : Entrance & exit Control Service Server):출입통제 시스템이 설치된 지역의 사용자가 특정 지역에 출입을 하려고 할때 해당 지역 출입의 허가 여부를 사용자별, 그룹별, 정책별로 관리하고, EECU가 W-Key와 정보를 교환 후 해당 정보를 이용하여 출입의 허가여부를 요청 시 출입 가능여부를 알려주는 시스템

2.1 출입통제 서비스 흐름

RFID/USN 기반 안전한 출입통제시스템 서비스의 흐름을 (그림 3)에 나타내었다.

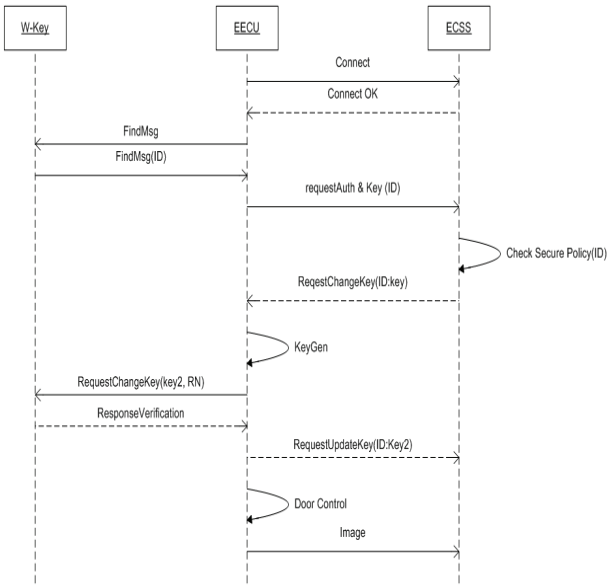


(그림 3) 출입통제 서비스 흐름도

1) EECU는 전원이 인가되면 설정되어 있는 ECSS의 정보를 이용하여 ECSS에게 연결을 요청한다.
2) EECU의 연결신호를 받은 ECSS는 이상이 없는 EECU일 경우 연결을 허락하는 메시지를 EECU에게 보낸다.
3) ECSS와 연결이 완료된 EECU는 출입을 하려는 사람이 갖고 있는 W-KEY를 깨워서 동작시키기 위한 시동신호(FindMsg)를 연속적으로 송신한다.
4) EECU의 시동신호를 받은 W-KEY는 W-Key의 ID 정보 ECSS에게 보낸다.
5) EECU는 W-Key의 ID를 이용하여 ECSS에게 출입이 가능한지 여부와 암/복호화에 사용할 Key를 물어본다.
6) ECSS는 출입이 허용되는 ID이면 해당 ID의 W-Key와 암/복호화에 사용할 Key를 EECU에게 보내준다.
7) EECU는 ID를 보낸 W-Key가 진짜 W-Key인지 확인하기 위해, 임의의 수를 생성하고, ECSS에게 받은 Key를 이용하여 암호화 한 후 W-Key에게 전송한다.
8) W-Key는 본인이 갖고 있는 Key를 이용하여 EECU에게 받은 메시지를 복호화 하고, EECU에게 받은 임의의 수를 1 증가시켜 다시 암호화 한 후 EECU에게 보낸다.
9) EECU는 W-Key에게 받은 메시지를 복호화하여 7)에서 보낸 임의의 수보다 1큰 수라는 것이 확인되면 출입문을 열어준다.
10) EECU는 문을 열고, EECU에 부착된 카메라를 이용하여 영상을 촬영하여 ECSS에게 전송한다.

2.2 키교환 및 출입통제 서비스 흐름

RFID/USN 기반 안전한 출입통제시스템 서비스를 위해 (그림 4)에 키교환 및 출입통제 흐름도를 제시하였다.



(그림 4) 키교환 및 출입통제 서비스 흐름도

1) EECU는 전원이 인가되면 설정되어 있는 ECSS의 정보를 이용하여 ECSS에게 연결을 요청한다.
2) EECU의 연결신호를 받은 ECSS는 이상이 없는 EECU일 경우 연결을 허락하는 메시지를 EECU에게 보낸다.
3) ECSS와 연결이 완료된 EECU는 출입을 하려는 사람이 갖고 있는 W-KEY를 깨워서 동작시키기 위한 시동신호(FindMsg)를 연속적으로 송신한다.
4) EECU의 시동신호를 받은 W-KEY는 W-Key의 ID 정보 ECSS에게 보낸다.
5) EECU는 W-Key의 ID를 이용하여 ECSS에게 출입이 가능한지 여부와 암/복호화에 사용할 Key를 물

어본다.

6) ECSS 는 출입이 허용되는 ID이면 Security Policy 를 확인하여 해당 ID의 W-Key의 암/복호화를 위한 key의 변경이 필요시 key의 변경을 요청 메시지를 EECU에게 보낸다.

7) EECU는 ECSS에게 W-Key의 이전 key와 key 변경 요청을 받으면, ID를 보낸 W-Key가 진짜 W-Key인지 확인하면서, 키의 변경을 요청하기 위해, 새로운 키와 임의의 수를 생성하고, ECSS에게 받은 Key를 이용하여 암호화 한 후 W-Key에게 전송한다.

8) W-Key는 본인이 갖고 있는 Key를 이용하여 EECU에게 받은 메시지를 복호화 하고, 새로운 Key가 들어있을 경우 새로운 키를 저장하고 EECU에게 받은 임의의 수를 1 증가시켜 새로운 키를 이용하여 암호화 한 후 EECU에게 보낸다.

9) EECU는 W-Key에게 받은 메시지를 복호화하여 7)에서 보낸 임의의 수보다 1큰 수라는 것이 확인되면 ECSS에게 W-Key의 새로운 Key를 보내준다.

10) EECU는 W-Key에게 받은 메시지를 복호화하여 7)에서 보낸 임의의 수보다 1큰 수라는 것이 확인되면 출입문을 열어준다.

11) EECU는 10)에서 출입문을 열어주었을 경우 EECU에 부착된 카메라를 이용하여 영상을 촬영하여 ECSS에게 전송한다.

2.3 출입통제 장치(EECU)

기존의 RFID 출입 통제장치에 안전한 USN무선키 통신을 도입하여 출입통제 서비스를 제공할 수 있도록 해주는 시스템으로 편리하면서도 기존 시스템 보다 안전하게 출입을 통제 할 수 있는 기능을 제공하는 출입통제장치이다.

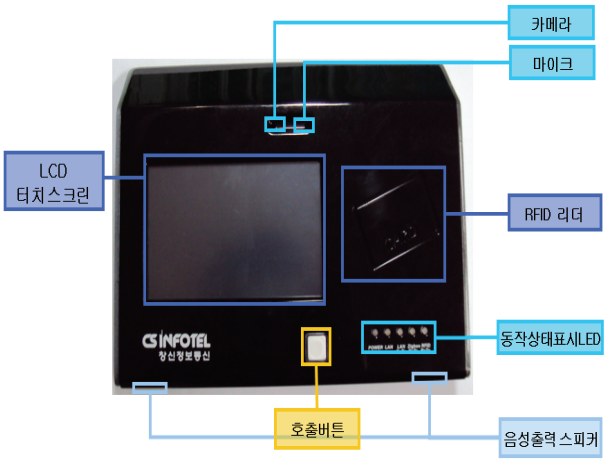
출입통제장치(EECU)는 S3C2443XL의 ARM 프로세서는 임베디드 시스템 응용에 적합하게 설계된 응용 프로세서이다. 최대 533MHz로 동작하며, 높은 성능을 요구하는 동영상 이미지 처리기능을 이용한 출입통제시스템에 적용될 주변장치로 UART, I2C, SD, USB, Audio Codec, RJ-45 통신, GPIO로 구성되어 출입통제 장치의 적합한 프로세서로 출입통제장치(EECU) 비상시 전력 소모를 줄이기 위해 응용프로그램에 요구에 따라 최소의 클럭 및 전압으로 동작하도록 다이나믹 볼테지, 다이나믹 프리쿼시 스케일 기능이 있다. 시스템의 대기 전류를 최소화하는 슬립모드와 출입통제시스템의 정전 및 화재 자연재해 발생시 외부 전력이 소실이 되었을 때 비상용 3.7V 리듐-폴리머 충전지를 탑재하여 긴급시에 도어의 제어가 가능하다.

2.4 출입통제 장치(EECU) S/W

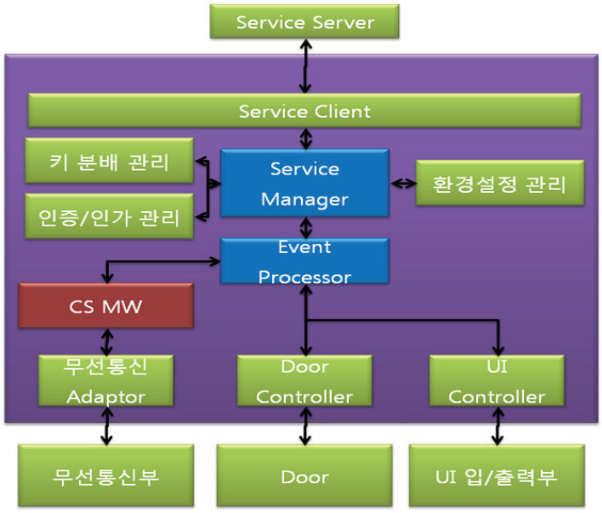
출입통제 장치의 SW 는 (그림 6)에서 보듯이 6가지 분류의 모듈로 구성이 된다.

1) Server Client

서버연결을 위한 서버 클라이언트 부분으로 서버에 접속을 유지/관리 하게 된다. 장치의 설정에 따라 장치 단독 수행 모드와 ECSS 모드로 구분되며 최초 설정시 ECSS 모드가 아닐 경우 각 출입 카드 및 키의 인증 정보 입력은 필수 사항이다. 서버의 연결은 ECSS 모드일 경우 활성 상태가 되며 입력된 서버의 주소에 연결을 시도하게 된다. 연결 시도 시 접속이 안될 경우 일정 시간이 지난 후 재 접속을 시도한다. 접속 연결이 지속적으로 되지 않을 경우 자체 인증 모드로 바뀌며 이 자체 인증 모드 상태에서도 서버에 접속 시도는 지속 적으로 이루어진다. 접속이 완료되면 자체 인증 모드에서 ECSS 인증 모드로 변경된다.



(그림 5) 출입통제 장치(EECU)



(그림 6) 출입통제 장치(EECU) S/W 구조

2) 관리 모듈

관리부분은 3개의 모듈로 구성된다.

가) 키분배 관리

장치 단독 수행 모드일 경우 키 Data를 관리하며, 분배 된 키의 유효성을 유지하는 역할을 한다. ECSS에서 키 분배 지시가 내려올 경우 해당 키에 대한 키 분배를 실시하도록 이벤트를 발생 시키며, 키 분배 이후 키 값을 저장하고 서버에 전송하는 역할을 한다.

나) 인증/인가 관리

장치 단독 수행 중 일 경우 각 카드에 대한 인증 인가 정보를 저장하고 관리 한다. ECSS 모드일 경우 ECSS에서 인증/인가 정보를 받아 갱신하는 역할을 겸한다.

다) 환경설정관리

장치 단독 수행 모드에서 관리자의 환경설정에 대한 내용을 반영하며, ECSS 모드에서는 ECSS에서 관리하는 환경 설정을 반영하여 갱신하는 역할을 겸한다.

3) Main Processing & Event Handler

관리 모듈들을 유기적으로 연결하여 관리하는 Service Manager 가 있으며, 이는 서비스 클라이언트에서 발생하는 모든 서비스 관련 처리를 담당한다. Event Processor에서 발생하여 서버에 전송하고 전송 받는 흐름에 대한 관리도 겸한다. Event Processor 는 출입 통제장치에서 일어나는 이벤트들에 대한 처리를 담당한다. 주로 인증을 위해 필요한 데이터 처리를 담당하며 장치의 각 Device에서 일어나는 일련의 이벤트를 모두 처리한다. Event 검출과 Control을 주로 담당하며 이에 대한 처리는 Service Manager에서 처리한다.

4) CS MW

CS MW 는 창신 독자 미들웨어 SW로서 무선통신부와 Key 와의 통신 및 보안 부분의 처리등을 담당한다.

5) 무선 통신 Adaptor

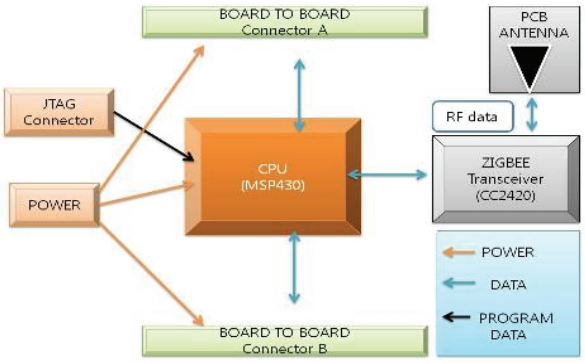
무선통신 Adaptor 는 RFID, W-Key 와 MW의 통신 중간에 위치하여 데이터 흐름을 관리하게 된다. 주로 W-Key 에 대한 Wake-up 신호를 주기 적으로 발생시켜 W-Key Detection 을 하며, Detection 이후 데이터 흐름을 관리한다.

6) Device Controller

Controller 는 2개로서 Door Controller, UI Controller 로 나뉘며 각각 문에 대한 제어, 사용자의 입력 및 메시지 출력등의 기능을 담당하게 된다. 각각 문에 대한 제어, 사용자의 입력 및 메시지 출력 등의 기능을 담당하게 된다.

2.5 무선키(W-Key)

W-Key는 AES128을 이용한 암복호화, 키분배 등의 보안관련 기능을 수행한다. 사용자 개인별로 소지하여 사용자를 대표하며, 출입통제시스템에서 출입을 위한 인가를 위해 사용되는 무선키로서, IEEE802.15.4 기반의 WPAN 무선통신 기술을 기반으로 Zigbee프로토콜을 이용하여 EECU와 무선으로 데이터를 교환하며, EECU와의 안전한 인증/인가 및 데이터 교환을 위해 보안기법을 사용하는 개인용 무선키이다. W-key가 DeviceControlBlock의 CC2420을 이용하여 메시지의 암/복호화를 수행할 수 있도록 해준다. EccProc은 KeyDist를 이용하여 키분배를 수행시 ECC 알고리즘을 이용할 수 있도록 해준다. NNM은 AES 128과 ECC 알고리즘을 처리 시 크기 128bit의 데이터 연산을 가능하도록 해주고, RSAREF2.0 기반으로 보다 빠른 자연수 연산을 수행할 수 있도록 해준다.(그림 7)에 무선키(W-Key) H/W를 나타내었다.



(그림 7) 무선키(W-Key) H/W 구조

3. 결론

u-City, u-Port 등 다양한 유비쿼터스 응용 분야의 핵심 요소 기술로 사용되어 AES128을 이용한 암복호화, 키분배 등 USN 기반의 서비스에 대한 안전성 및 신뢰성을 증대시킬 수 있다. USN 분야의 침입통제, 안전기반으로 기숙사, 아파트 등의 안전 서비스에 다양하게 적용시킬 수 있다. 또한 경제적측면에서 저전력 구현 기술을 활용하면, 적은 전력을 소비함으로서 무분별한 전력 사용으로 에너지 사용량을 줄이고, 무공해 대체 에너지로 활용하여 장기적으로는 환경오염을 방지에도 기여할 수 있을 것이다.

참고문헌

[1] 김정식, 권민성, 김호준,"USN/RFID모듈을 이용한 보안 시스템에 관한 연구", 한국정보기술학회 2009년도 Green IT 융합기술 워크숍 및 하계 종합 학술 대회 논문집, 2009. 6, pp820~pp825

[2] 이성휘, "RFID/USN: RFID/USN 산업 동향", 정보통신산업진흥원, [IITA] 정보통신연구진흥원 학술정보

[3] 박윤현, "RFID/USN 주파수 재배치 및 기술 기준 정책 동향", 한국전자파학회, 전자파기술 제20권 1호, 2009. 1, pp. 144 ~ 151

[4] 김창곤, "유비쿼터스 사회를 대비한 RFID/USN 정책방향", 한국통신학회, 한국통신학회지(정보와통신) 한국통신학회지 (정보와통신) 제25권 제1호, 2008. 1, pp. 52 ~ 58

[5] U. Karthaus and m. Fisher, "Fully inte grated Passive UHF RFID TransponderIC with 16.7-uW Minimum RF Input Power," IEEE Journal of Solid-State Circuits, Vol.38, No.10,pp. 1602-1608. Oct. 2003