韓國컴퓨터情報學會 論文誌
第16卷 第1號, 2011. 1.

2011-16-1-1-2

RFID를 이용한 시스템 보안 장치 개발

장 재 혁*, 심 갑 식**

Development of a System Security Unit using RFID

Jae-Hyuk Jang, Gab-Sig Sim

요 약

본 연구에서는 RFID 카드 접촉에 의해 시스템 전원을 개폐하는 방식의 디지털 보안 장치를 개발했다. 이는 무선 데이터 송/수신 회로기반으로 설계되었으며, RS-232C전용 칩을 내장하여 컴퓨터나 기타 디지털 기기에도 적용할 수 있다. LED를 장착하여 본 장치의 동작 여부를 점검 할 수 있다. 본 시스템에서 13.56MHz의 주파수 회로가 ID 카드에 전원을 공급하고, 카드 유무를 체크하기 위해 DC 입력단이 카드의 필드 내 근접여부를 확인한다. 본 시스템의 보안 수준은 비교 시스템[13]에 비해 보안 수준이 아주 강력하다. 어떤 사용자일 경우라도 RFID 카드를 이용하지 않으면 시스템을 사용할 수 없다. 인가된 경로 외의 모든 불법적인 접근이 차단된다.

▸ Keyword : 유비쿼터스, RFID, 자동화, 보안

Abstract

This study developed a digital security device which power is on/off by the RFID card. This device is based on the wireless data transmit/receive circuits, built in RS-232C chip and applied to computer and other digital devices. We can check whether this device is operated or not by connecting the LED. In this system, 13.56MHz frequency circuit supplies power with ID card, and DC inputs check the proximity operating distance of the card field for verifying the existence of a card. The security level of this system is much stronger than that of a compared system[13]. Anyone cannot use the system without RFID card. All illegal access is prevented except for authorized path.

▸ Keyword : Ubiquitous, RFID, Automation, Security

• 제1저자 : 장재혁 교신저자 : 심갑식
• 투고일 : 2010. 08. 16, 심사일 : 2010. 09. 16, 게재확정일 : 2010. 10. 13.
* 경남과학기술대학교 교양학부(Gyeongnam National University of Science and Technology, Dept. of Liberal Arts)
** 경남과학기술대학교 교양학부(Gyeongnam National University of Science and Technology, Dept. of Liberal Arts)

Ⅰ. 서 론

한국은 2007년 UN 보고서에 의하면 세계 5위의 전자정부, 국가정보화지수 3위의 초대형 IT 강국이다. 그러나 정보보호 및 개인정보 보호에 관한한 세계 20위권 밖에 머물러 있다고 알려져 있다[1]. 그동안 정부를 비롯하여 각 기업은 정보보호 수준 제고를 위하여 많은 노력을 하였지만, 그 범위는 네트워크나 서버에서의 기술적 측면의 정보보호에 치중하였고 업무 차원에서의 정보보호 노력은 상대적으로 미흡하였다.

정부 및 기업의 활동이 네트워크 및 정보통신 기술을 통해 수행됨에 따라 전통적 문서 형태로 각 집단이 관리해 오던 각종 정보가 디지털화되어 정보시스템에 입력, 처리, 저장, 전송되고 있으며 이러한 정보의 축적 및 연계활동은 더욱 가속화, 대량화되고 있다. 그러나 대량의 정보 집중화 관리체계와 이를 다루는 서비스 인력의 증가로 인해 핵심정보의 유출 및 오남용 위험 역시 급속도로 증가하고 있다[2][3]. 이러한 사고를 발생시키는 기술적 측면의 원인으로는 외부의 불법적인 접근을 통한 정보의 유출, 내부자의 부주의 또는 의도에 의한 정보 유출, 웹사이트 등을 통한 정보의 유출 등 3가지로 요약할 수 있다. 따라서 정보보호에 대한 다양한 요구가 끊임없이 발생하고 있으며, 이에 부응하여 정보보호를 위한 다양한 연구 및 기술개발이 수행되어 국내 정보보호 기술이 급속히 발전하고 있다. 개인정보 보호를 위해서는 특히 업무 차원에서의 개인정보 흐름과 유출 가능성을 사전에 파악하여 차단하는 것이 필요하다.

정보시스템에서의 정보보호 활동의 효과를 높이기 위해서는 일회성 프로젝트 성격의 정보보호 영향평가 등과 같은 방식으로는 상존하는 개인정보 유출 위험을 효과적으로 관리하기 어렵다[3][4]. 정보를 지속적으로 보호하기 위해서는 지속적, 순환적 프로세스를 포함하는 관리체계 및 방법을 수립, 운영, 개선하는 노력이 필요하다. 이에 각 조직은 효율적인 정보보호를 위해 조직의 규모와 특성에 맞는 정보보호 시스템 도입과 인력 확충, 조직 구성원에 대한 교육 등에 투자하고 있다[5][6].

정보보호는 비인가자의 접근, 사용, 공개, 방해, 수정, 파괴로부터 정보와 정보시스템을 보호하여 궁극적인 정보시스템과 자원의 무결성, 가용성, 기밀성을 확보하는 것이다. 정보보호를 위한 일련의 활동을 정보보호 관리체계라 할 때 여기에 적용되는 통제수단, 즉 정보생산 및 관리의 최소단위인 개인 시스템의 기술적 통제, 인적 통제, 운영 통제 등 관리적 통제 수단이 요구된다[7][8]. 현재 전 세계적으로 산업기밀 또는 내부 자료 유출이 크게 문제시 되고 있는 현실에서 보안 관리 시스템을 통해 고객의 재산을 안전하게 보호하는 것이 절실히 필요하다.

본 논문에서는 RFID 카드의 인식여부에 따라 각 개인용 디지털 시스템의 전원 공급을 통제하는 방식의 보안시스템을 개발하였다.

기존의 보안기능을 제공하는 방법인 사용자 인증 방식에서는 비밀번호 입력 방식이 주를 이루었으나, 본 논문에서는 기본으로 설정한 RFID 카드를 본체에 대는 것으로 시스템의 전원을 통제한다. 그리고 어떤 디지털 시스템의 소유자라 할 지라도 카드를 소지하고 있지 않으면 그 시스템에 접근할 수 없다.

Ⅱ. 관련연구

2.1 시스템보안 방식

시스템보안 방식은 크게 보안영역 방식과 사용자 인증방식으로 나눌 수 있다.

1) 보안영역 방식

보안영역 방식은 크게 두 가지로, 하드웨어 방식과 소프트웨어 방식이 있다.

(1) 하드웨어 방식

암호화 칩 방식은 하드웨어를 사용하는 방식의 일종이며, 이 방식은 USB 포트와 메모리 사이에 보안을 제공하는 칩이 존재한다. 이 보안 칩은 사용자 인증과정에 통과해야만 메모리에 전원을 공급하며, 보안 칩 자체만으로도 바른 암·복호화 기능을 제공한다[9].

USB메모리는 데이터 저장과 설정 정보를 저장하기 위한 여러 개의 ROM으로 이루어져 있다. 또한 메모리에 저장된 데이터를 접근하기 위해서는 USB 컨트롤러를 통해야 하며, 이 컨트롤러를 보안 칩으로 대체하여 인증되지 않은 사용자 메모리칩의 특정 부분에 대한 접근을 거부할 수 있다. 하지만 USB메모리 내부의 플래시 메모리를 분리, 다른 USB메모리에 연결함으로 데이터를 얻는 인증 우회가 가능한 취약점을 가지고 있다.

(2) 소프트웨어 방식

소프트웨어 방식을 사용하는 경우 보안USB에서 제공하는 CD영역에 저장된 보안 프로그램을 실행하거나, USB메모리 제조사의 웹페이지에서 보안 프로그램을 다운받아 USB메모리를 사용할 단말기에 설치하여 사용하는 방식으로 가장 많이 사용되는 방식이다[10].

① 이미지 드라이브 방식

보안영역을 제공하기 위해 가상 드라이브 이미지 파일을 이용하는 방식이다. 가상 드라이브 방식은 보안영역에 접근하

기 위해 사용자 인증을 거치며, 인증과정에 입력한 비밀번호를 이용하여 암호화된 가상 드라이브의 이미지 파일을 복호화한다. 복호화된 이미지 파일로 가상의 드라이브를 운영체제에 인식시켜 보안영역을 제공한다[11].

② 예약영역 활용 방식

보안영역을 제공하기 위해 파일시스템 구조를 이용한 방식으로 파일시스템의 예약영역(Reserved Area)를 활용하여 사용자 인증을 거쳐 전용 브라우저 프로그램을 통하여 보안영역에 접근하는 방식이다[12].

③ 단순 파일 암호화 방식

보안영역을 따로 제공하지 않으며, 암호화 파일 시스템 혹은 일반영역에 선택적으로 파일을 암호화 하는 방식이다[9].

구현이 용이하고 손쉽게 사용할 수 있는 반면 암호화 파일의 노출에 비교적 취약하여 악의적인 제 3자의 공격에 대한 위험성을 가지고 있다.

2) 사용자 인증 방식

사용자 인증 방식은 크게 생체인식을 이용한 방식과 비밀번호를 이용한 방식의 두 가지로 분류할 수 있다.

(1) 생체인식 방식

사용자 인증을 위해 생체인식을 하는 방식으로 지문인식기를 이용하여 사용자를 인식하는 것이 보편적이다. 생체인식 과정은 인식기로부터 추출된 화상을 전처리하고, 이를 이진화상으로 바꾸어 특징을 추출한 후 사용자 인증 시 인식된 생체정보 특징과 비교하여 사용자 인증을 수행한다.

지문만을 이용하는 단일 생체인식의 경우 잘못된 사용자를 정당한 사용자로 인식할 수 있는 FAR(False Acceptance Rate)이 존재하여 완벽한 사용자 인증을 제공하지 못하여 지문인식 결과만으로 사용자 인증을 수행하는 것은 안전하지 않아 다중 매체를 이용한 사용자 인증 방식이 요구된다[9][12].

(2) 비밀번호 방식

사용자 인증을 위해 비밀번호를 이용하는 방식으로 미리 설정된 비밀번호와 인증을 위해 입력한 비밀번호를 대조하여 사용자 인증을 수행한다.

비밀번호를 이용한 사용자 인증 방법은 사용자 입력비밀번호를 대조하기 위한 사용자 인증 값이 평문으로 저장되어 비밀번호가 노출되는 취약성을 가지는 경우가 존재하며, 이를 해결하기 위해 사용자 인증 값을 평문이 아닌 해시값 혹은 암호문으로 대체하려는 방식이 요구된다[10].

2.2 최근 연구

최근에 사용되고 있는 시스템 보안 방식은 주로 보안영역 방식 중에서 하드웨어 방식이 사용되고 있다.

2007년에 (주)이월리서치는 RF카드를 이용하여 개인용 컴퓨터의 하드디스크를 선택적으로 부팅하는 방식으로 개인용 보안시스템을 개발하였다[13]. 이 보안시스템은 RF카드 방식을 사용하여 안테나 수신부에 RF카드를 인식하여 인가된 사용자에 한하여 시스템을 부팅되도록 해서 보안성을 확보하는 방식이다. 최대 10개까지 ID를 저장하여 보안을 관리하며 전원스위칭 방식을 사용하였다. 그러나 이 시스템은 최대 10매까지라는 사용자확장에 한계를 가지고 있으며, 전기적 스위칭 방식을 사용한 보안 방식 때문에 시스템 탈착에 위한 의도적 회피가 가능하다는 문제점을 가지고 있다. 또한 적용가능 범위가 시스템 내부의 저장장치에 한정되는 것과 RFID 수신부를 시스템 내부에 별도로 설치해야 하는 것도 문제점으로 들 수 있다.

III. 개발한 보안 시스템

본 절에서는 유비쿼터스 컴퓨팅 기술인 RFID를 이용하여 카드의 인식여부에 따라 각 개인용 디지털 시스템의 전원 공급을 통제하는 방식으로 개발된 보안시스템에 대해 기술한다.

본 논문에서 기술한 시스템은 RFID를 이용하여 카드의 인증여부에 따라 각 개인용 디지털 시스템의 전원 공급을 관리하는 방식으로 해당 시스템의 사용 여부를 통제한다. 이를 통해 보안시스템의 운영을 용이하게 한다. 이는 각 시스템에 초소형 RFID 리더기를 내장하여, 해당 시스템의 가용여부를 결정하는 방식이다.

3.1 시스템 구성

개발된 시스템은 무선 데이터 송/수신 회로기반으로 설계되었으며, RS-232C전용 칩을 내장하여 컴퓨터 및 기타 디지털 기기와 호환이 가능하도록 개발하였다. 그림 1은 개발된 RFID 시스템의 MCU(Microcontroller) 주변 블록도이다.

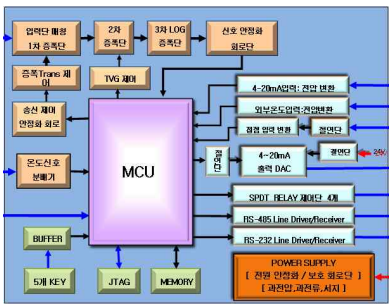

그림 1. RFID MCU 블록도
Fig. 1. The RFID MCU Block Diagram

그림 1에서 블록도 상단의 증폭단은 사용자 카드, 마스터 카드의 신호를 입력받는 역할을 한다. 입력된 각 카드의 신호들은 신호 안정화 회로단을 거쳐 MCU로 입력되어진다. MCU는 산술, 논리 요소뿐 아니라 데이터 저장을 위한 읽기 쓰기 메모리, 코드 저장을 위한 플래시와 같은 읽기 전용 메모리, 계속적인 데이터 저장을 위한 EEPROM, 주변 기기, 입출력 인터페이스 등의 부가 요소를 통합한다.

3.2 시스템 설계

개발 시스템은 크게 두 가지 범주로 나눈다. 하나는 하드웨어 범주이며, 또 다른 하나는 미들웨어 범주이다. 하드웨어 범주는 다시 크게 두 가지로 분류할 수 있으며, 본 논문에서는 하드웨어 범주를 주로 기술한다. 개발된 시스템은 RFID 장비류(태그, 리더, 안테나 등)와 시제품 부속류(본체, LED, 연결장치 등)로 구성된다. 개발 시스템의 RFID 무선 데이터 제어부의 사양은 실제 시제품 사양을 수치화한 것으로 입력된 전자태그내 정보를 시스템이 인식하는데 용이하도록 구성하였다. 정격전압은 DC 12V, 데이터 통신 방식은 RFID 태그 방식의 RS-232C를 사용하였고, 동작 표시의 경우에는 LED를 장착하여 전원의 연결 여부를 알 수 있게 하였다. 또한 별도의 LED를 추가하여 보안시스템의 작동 여부를 알 수 있도록 구성하였다. 전체 시스템 통제를 위한 MCU는 ATMEL사의 8bit RISC Processor인 AT90S2313 타입을 사용하였다. 안테나는 주파수 대역 13.56MHz의 내장형을 사용하였고, 전체 신호 제어는 릴레이 ON/OFF 제어 방식을 사용하였다. 시스템 사용 온도는 -20에서 80도까지 설정 되었고, 데이터 제어 거리는 0에서 10cm로 설정하였다. 사용 카드 입력은 최대 999장까지 가능하도록 하였다.

1) 회로설계

그림 2는 시스템 회로 설계도이다. 개발된 리더기 회로에서는 오실레이터를 통하여 13.56MHz의 주파수를 발생시키고 이를 통해 RF 카드에 전원을 공급하였다. 또한 카드 유무를 체크하기 위해 DC 입력단을 구성하여 카드의 필드 내 근접여부를 확인하도록 구성하였다.

배터리를 사용하는 리더기의 경우 MAX232 칩을 구동하여 카드의 필드 내 근접여부를 체크하는데, 소비 전류를 최소화하기 위하여 MAX232 칩도 전원 차단 상태로 대기 후 카드 체크 시만 구동하도록 하였다. 카드와 통신을 할 경우를 제외하고는 전원 차단 상태를 유지하고, 소량의 전류를 사용하여 카드를 체크하도록 하였다. 또한 카드를 체크하기 위한 동작 시간을 줄일 수 있도록 설계하였다.

2) 마이크로컨트롤러(AT90S2313) 인터페이스

CPU의 DC 입력단을 통해 리더 안테나로 들어오는 전압을 체크하여 카드 유무를 체크한다. 이 경우 오실레이터의 전류 소모를 줄이기 위해 카드 유무를 체크하는 동안에만 구동시키기 위한 Chip Select 핀을 구성하였다. CPU의 AREF단자로 DC로 입력되는 값을 AD변환하기 위한 기준 전압으로 3.3V를 설정하고, 제너다이오드를 거쳐 일정한 3.3V 값이 입력되도록 하였다.

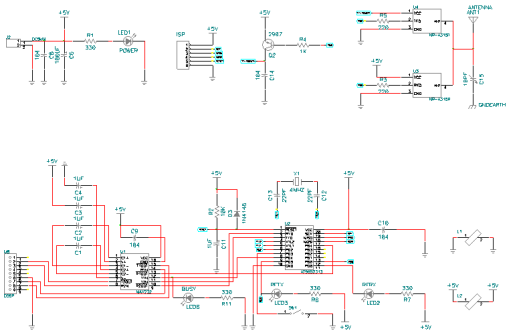

그림 2. 시스템 회로 설계도
Fig. 2. The Design for System Circuit

또한, 파워다운 상태로 진입한 CPU를 Wake-Up하기 위해 32.768KHZ 크리스탈을 사용하였으며 CPU에 프로그램을 저장하기 위한 JTAG 회로를 채용하였다.

3.3 프로토콜

㉠ HEX 모드로 카드 읽기
- 리더기로 0x02 0x68 0x03 을 전송
- 카드를 리더기 모듈에 접근
- 인식 비프음
- 리더기에서는 stx1E00EaB0F7ext 가 전송

㉡ BIN 모드로 카드 읽기
- 리더기로 0x02 0x62 0x03 을 전송
- 카드를 리더기 모듈에 접근
- 인식 비프음
- 인식된 카드 ID를 리더기에서는 stx111111111~0 etx 가 전송

㉢ 체크 모드로 카드 읽기
- 리더기로 0x02 0x63 0x03 을 전송

- 카드를 리더기 모듈에 접근
- 메모리상에 저장된 카드 ID와 읽은 ID의 일치 여부 판단
- 일치할 경우 -> ON
- 일치하지 않을 경우 -> LOCK

㉣ 카드 저장
- 리더기로 0x02 0x73 0x03 을 전송
- 카드를 리더기 모듈에 접근
- 인식된 후 정상 저장되면 비프음 출력
- 실패 시 무음
- 저장 후 자동으로 체크모드로 넘어감

㉤ 카드 삭제
- 리더기로 0x02 0x64 0x03 을 전송
- 카드를 리더기 모듈에 접근
- 인식된 후 정상 저장되면 비프음 출력
- 실패 시 무음
- 저장 후 자동으로 체크모드로 넘어감

㉥ 메모리 포멧
- 리더기로 0x02 0x52 0x03 을 전송
- 일정 시간 후 비프음 출력 후 모드 복귀

3.4 DC 입력단 및 안테나

그림 3은 RFID PCB이다. PCB의 경우 13.56MHz의 펄스가 PCB 패턴 안테나를 거쳐 CPU의 DC 0번 핀으로 입력되도록 하였다. 만약에 사용자 카드가 안테나의 필드 내에 없을 경우에는 2.5V의 전압이 입력되며 카드가 필드 내에 있을 경우 2.5V 이하의 값이 입력된다.

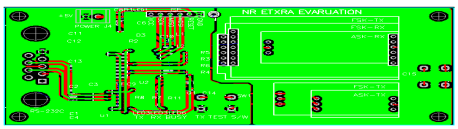

그림 3. RFID PCB
Fig. 3. The RFID PCB

PCB는 오차를 감안해 2.0V 이하 값이 입력되면 카드가 필드 내 있는 것으로 판별하며, 13.56MHz의 주파수를 발생시키기 위해 출력을 안테나에 연결하도록 하여 PCB 패턴을 안테나로 연결하였다.

3.5 송/수신부 보드

그림 4는 시제품의 송신부 보드의 이미지이다.

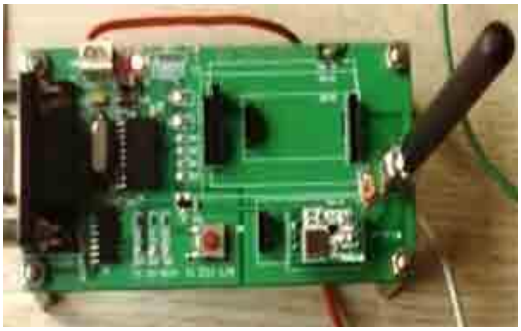

그림 4. 송신부 보드
Fig. 4. The TX Board

송신부 보드는 왼쪽에 PC 또는 기기의 RS-232C 포트를 연결하는 단자가 있다. 또한 안테나 연결단자(SMA 커넥터)로 ANT-con, 실험 데이터 송신을 위한 실험 스위치를 보드 전면에 배치하였다. RF 송신/수신 모듈을 장착하였으며, MCU 프로그램 변경 시 사용되는 Writing 포트로 ISP-Writer를 사용하였다. 전원은 5V를 연결하였다.

3.6 무선데이터 제어부

무선 데이터 제어부는 입력된 전자태그의 정보를 시스템이 인식하는데 용이하도록 구성 하였다. 정격전압은 DC 12V, 데이터 통신 방식은 RFID 태그 방식의 RS-232C를 사용하였다. 전체 시스템 통제를 위한 MCU는 ATMEL 8-bit를 사용하였다. 안테나는 주파수 대역 13.56MHz의 내장형을 사용하였고, 전체 신호 제어는 릴레이 ON/OFF 제어 방식을 사용하였다. 시스템 사용 온도는 -20에서 80도까지 설정 되었고, 데이터 제어 거리는 0에서 10cm로 설정하였다. 사용 카드 입력은 최대 999장까지 가능하도록 하였다.

3.7 미들웨어

개발된 시스템에서 적용된 RFID 미들웨어는 EPCglobal 표준을 준수하며 Edge 미들웨어와 ALE(Application Level Event) 미들웨어로 구성된다. Edge 미들웨어는 EPCglobal RP(Reader Protocol)의 관리 및 모니터링 기능을 담당한다. RP의 관리를 위해 RP의 구성 모듈에 대한 설정 정보를 파일로 관리하며, 이를 쉽게 조작하고 활용할 수 있는 관리 툴을

제공한다. 또한 모티터링 기능을 사용하여 현재 RP의 동작 상태 및 오류보고 사항을 확인 조치할 수 있는 기능을 제공한다. EPCglobal RP는 물리적 Reader장치를 이용해 Tag Data를 읽고 정보를 보고하는 방법 및 범용적인 인터페이스를 제공한다.

Ⅳ. 실 험

4.1 실험환경

개발된 시스템의 성능을 실험하기 위하여 실험 환경을 설정하였다. 전자 태그 인식 성능 향상 및 오인식 방지를 위한 안테나의 연결 및 위치를 조정하여 설정하였다. 실제로 개발된 제품이 사용되어야 할 환경의 종류, 즉 개발된 제품이 사용되어질 환경에 속하는 제품들의 형태와 재질이 다양하기 때문에 시제품의 경우에 일반적으로 실제 디지털 기기의 케이스에 상응하는 PVC재질로 시제품의 케이스를 별도 제작하고 실험용 시스템으로 사용하였다. 표 1은 실험환경 명세이다.

실험은 범주별로 나누어 환경을 설정 하였는데, 항목 범주는 설치환경, 인식환경 설정, 전자태그, 인식 프로세스, 오인식 방지, 외부 간섭으로 분류하였다. 이는 RFID 시스템의 특성상 RFID 리더에서 발산되는 전파의 불규칙성과 RFID 태그가 대상의 이동속도, 안테나와의 방향, 거리, 개수, 인체 영향 등에 의하여 동일한 RF 신호에서도 RFID 태그의 인식이 항상 일정하지 않을 수 있다는 것을 전제하였다. 이와 같은 RFID 태그를 인식하지 못하는 미 인식 상황에 대비하여 시스템의 환경을 다양하게 설정하였다.

표 1. 실험환경 명세서
Table 1. The Test Environment Specification

범 주	구 분	세 부 명 세	실험 형태
설치 환경	구조물 설치 방안	동선 확보	사용자의 태그 인식 동선 확인
		제약성 검증	시스템 설치 시 외형적으로 예상되는 문제점 파악
	인터페이스 연결	Input 연결 확인	센서 설치를 위한 위치 결정
		Output 연결 확인	외부출력장치 연결 여부 확인
인식 환경 설정	안테나 각도	0~90	각도 조절 후 태그가 인식되는 영역 확인
		91~180	각도 조절 후 태그가 인식되는 영역 확인
	안테나	Circular의 성능	태그 인식 거리 확인
		형태	Linear의 성능	태그 인식 거리 확인
		케이스	케이스 재질	실제 제품 인식 확인
전자 태그	전자태그 방향		가로	태그를 가로 방향으로 적용하여 인식거리 확인
			세로	태그를 세로 방향으로 적용하여 인식거리 확인
			사선	태그를 사선 방향으로 적용하여 인식거리 확인
	전자태그 거리		가깝게	태그를 리더기에 가깝게 적용하여 인식 확인
			멀게	태그를 리더기에 멀게 적용하여 인식 확인
인식 프로 세스	노출 시간 측정		태그 이동 측정	안정된 태그 이동 속도 측정
	동시 인식 측정		태그 동시 측정	인식 태그의 최대 개수 확인

4.2 실험고찰

RF 신호의 경우 인식 범위가 원하지 않는 범위까지 영향을 미쳐 오인식 되는 경우가 발생할 수 있으며 이런 문제 해결은 리더와 태그의 전파를 차단할 수 있는 환경이 구성되어야 한다. RFID 태그가 2개 이상인 경우에는 동일 공간에서 서로간의 전파 간섭 현상이 있어 태그의 인식률이 다소 하락할 수도 있다. 이러한 간섭 현상을 줄이기 위한 방법으로는 각각의 태그를 인식하는 리더기 동작시간을 분할하여 사용하거나 센서의 위치 및 각도를 조절하는 방법이 있다.

표 2는 시스템의 각 항목별 실험 결과이다.

표 2. 시스템 실험
Table 2. The System Test

항목	성능	동작	비고
동작 성능	ok	100%	
제어 거리	10cm 이내	100%	
인식 속도	106kbps	100%	
전압 변동	+(-)5%	100%	
카드체크 소비시간	200㎲	100%	
카드체크 소비전류	7mA	100%	

위의 실험은 시스템의 성능을 KS규격의 항목 중 직접 실험장비로 확인 가능한 항목만을 포함시킨 한계가 있지만, 그 동작성능에서는 오인식, 오작동의 문제는 발생하지 않았다.

개발된 시스템의 성능 비교를 위하여 2.2절에 기 언급한 제품[13]을 구입하여 비교 실험을 하였고, 표 3은 비교 시스템과 개발 시스템의 항목별 특징을 명시한 것이다.

비교 시스템의 경우, 멀티부팅 환경을 제공하는 장점이 있는 반면 탈착으로 인한 회피가 가능해 보안 측면에서는 다소 취약하다고 볼 수 있다. 그러나 개발된 시스템은 강력한 보안 수준이 목적이므로 기존의 보안기능을 제공하는 방법인 비밀번호 입력 방식과 달리 RFID 기술을 자물쇠와 열쇠로 활용하는 효과가 있다. 이를 통해 설정된 RFID 카드를 본체에 대는 것으로 시스템의 전원을 통제할 수 있다. 이는 RFID 카드가 없다면 사용자는 시스템에 접근할 수 없다는 뜻이다. 따라서 복잡한 암호를 입력, 기억해야하는 번거로움을 줄일 수 있는 동시에 유출의 가능성이 없고, 시스템 사용자일 경우라도 인증된 RFID 카드가 아니면 시스템을 사용할 수 없어 분실 등 승인된 경로 이외의 불법적인 사용을 차단하는 효과가 있다.

표 3. 항목비교
Table 3. The Comparison

항목	비교 시스템	개발 시스템
보안 방식	RFID 이용 DIP 스위칭 방식	RFID 이용 TURN ON/OFF방식
허용 RFID수	최대 10개	최대 999개
적용가능 범위	시스템 내 저장장치 (하드디스크)	다양한 디지털 기기
제어 거리	10cm이내	10cm이내
카드체크 소비시간	500㎲	200㎲
카드체크 소비전류	9mA	7mA
보안 수준	탈착으로 회피 가능	승인 카드 외 절대 사용 불가
구성 방식	RFID 수신부 별도 설치	RFID 수신부 보드내 구현

V. 결 론

본 논문에서는 기존의 소형 무선 센서노드 기술의 분석을 통한 임베디드 보드 분석 및 설계가 이루어졌으며, IEEE 802.15.4/ZigBee에 기반한 무선RF 모듈 설계가 완료되었다. 또한 설계된 보드의 경우 다수의 채널을 분배하여 사물 식별 코드 관리가 가능하도록 설계하였으며, 추후 필요할 경우 시스템의 업그레이드가 용이하다. 설계된 부분은 크게 수신부(RX)와 송신부(TX)로 나누어 설계하여 효율과 안정성을 도모하였다.

RFID 리더기 개발 분야에서 UHF 대역의 리더기를 탑재한 임베디드 보드 개발은 그 기술적 의미가 상당하다. 본 연구를 통하여 유비쿼터스 컴퓨팅 환경의 선형적인 모델을 제시할 수 있었고, RFID 리더기 관련 기술력의 축적이 가능하였다. 센서네트워크 관련 하드웨어 기술 발전을 도모하였으며, 하드웨어 소형화, 내장 기술 개발에 성공하였다. 또한 RFID 리더 프로토타입 설계 및 리더/태그간 무선 전송 기술 개발의 기반을 마련한 것은 큰 의미가 아닐 수 없다.

본 논문을 통하여 개발된 RFID 리더가 내장된 임베디드 보드는 RFID 기반의 보안 관리 시스템으로의 적용이 가능하다. 이를 기반으로 정보통신 기기, 음향기기, 군사용 기기 등 다양한 디지털기기의 제어 등의 보안장치로 활용이 가능하다. 또한 기 언급한 자동차 산업의 핵심 보안 기술 부분으로 사용이 가능하며, 강력한 보안 장비로 활용이 가능하다. 그리고 산업 현장에서는 보안장비의 통신선로로 활용이 가능하며 센서, 리모컨, 알람, 전등 및 제어기구의 제어용 시스템으로의 활용이 가능하다.

현재 RFID 기술의 한계에 따라 태그의 이동속도, 개수, 안테나 각도, 리더기와의 거리 등에 따라 인식률에 오차 범위 내의 차이가 있으나 이는 향후 펌웨어 개발 및 업그레이드, 장비 개선에 따른 인식률 개선 실험을 지속적으로 실행하고 일부 기기의 변경을 통하여 개선이 가능할 것이다.

향후 기존의 지문인식, DVR, 전원관리 시스템, 홈네트워크 등과 통합하여 강력한 통합형 보안 관리 시스템의 구축이 추후 연구과제이다.

참고문헌

[1] The KoreaTimes(2008. 7. 10) *http://news.hankooki.com/lpage/it_tech/200807/h2008071022191723630.htm*

[2] Yeon Hyun Yang, Sun Young Kim, Pil Joong Lee, “,Improved Authentication and Data Protection Protocol of Passive RFID Security Tag and Reader,” Journal of Korea Institute Of Information Security And Cryptology, vol 20, No. 1, pp.85-94, 2010.

[3] Hee-Joong Yang, June-Men Im, “Analysis of Present Tendencies and Strategic Direction for the Development in RFID Industry”. Journal of industrial and systems engineering , vol 28, No. 4, pp.69-78, 2005.

[4] Seung-Hak Rhee, Jong-Hun Chun, Jong-An Park , “Performance Improvement in Passive Tag Based RFID Reader,” Journal of the Korean institute of communication sciences, vol 31, No. 11A, pp.1159-1166, 2006.

[5] Dong-ho Jung, Jung-hyo Kim, Dong-hwan Ji, Yun ju Baek, “Design and Implementation of RTLS using Active RFID,” Journal of the Korean institute of communication sciences, vol 31, No. 12A, pp.1238-1245, 2006.

[6] Sang-Jin Lee, Kyung-Chang Park, Hanbyeori Kim, Seung-Youl Kim, Younggap You, “Block Cipher Circuit and Protocol for RFID in UHF Band,” Journal of Korea Contents Society, vol 9, No. 11, 2009.

[7] Fisher, Jill A, "Indoor Positioning and Digital Management: Emerging Surveillance Regimes in Healthcare", Technological Politics and Power in Everyday Life, pp.77-88. New York: Routledge, 2006.

[8] Cheng-hao Quan, Won-kee Hong, Yong-doo Lee, Hie-cheol Kim, “Performance Evaluation of Anti-collision Algorithms in the Low-cost RFID System,” Journal of the Korean institute of communication sciences, vol 30, No.1B, pp. 17-25, 2005.

[9] sun-Ho Lee, Im-Young Lee, “A Study on Security Solution for USB Flash Drive ,” Journal of Korea Multimedia Society, vol 13, No. 1, pp. 93-101, 2010.

[10] Hanjae Jeong, Younsung Choi, Woongryul Jeon, Fei Yang, Seungjoo Kim, Dongho Won, “Analysis on Vulnerability of Secure USB Flash Drive and Development Protection Profile based on Common Criteria Version 3.1,” Journal of Korea Institute Of Information Security And Cryptology vol 17, No. 6, , pp. 99-119. 2007.

[11] True Crypt, *http://truecrypt.org*

[12] Koh Chan, Park Youn, “Enhancement of Secourity Function on USB Memory Driver by Reserved Sector Storage Structure Technique,” Journal of the Korean Society for Industrial and Applied Mathematics, vol 9, No, 1, pp. 1-13, 2005.

[13] *http://academic.naver.com/view.nhn?doc_id=13873025&ApplicationNumber=1020070034037&dir_id=0&page=0&query=%EC%9D%B4%EC%9B%94%EB%A6%AC%EC%84%9C%EC%B9%98*

저 자 소 개

장 재 혁

2006년 2월 : 경상대학교 컴퓨터과학부 공학박사

현 재 : 국립경남과학기술대학교 교양학부

관심분야 : 유비쿼터스 컴퓨팅, 소프트웨어공학, 네트워크 보안

Email : speed_300@hanmail.net

심 갑 식

1993년 8월 : 전남대학교 전산통계학과 이학박사

2004. 3. ~ 2005. 2. : 미국 San Jose State University, CA 방문교수

1993. 10. ~ 2011. 현재 : 국립경남과학기술대학교 교양학부 교수

관심분야 : 유비쿼터스 컴퓨팅, 정보보안, 인터넷 윤리

Email : gssim@gntech.ac.kr