논문 2008-45CI-6-8

RFID와 TCP/IP를 활용한 원격 보안 출입 제어 시스템

(Remote Secure Entrance Control System using RFID and TCP/IP)

김 정 숙*, 김 천 식**, 윤 은 준***, 홍 유 식****

(Jeong-Sook Kim, Cheonshik Kim, Eun-Jun Yoon, and You-Sik Hong)

요 약

RFID 시스템은 현재 다양한 분야에서 사용되어 지고 있는 바코드 인식 시스템이나 자기 인식 장치들이 근본적으로 내재하고 있는 실용성 및 보안성 문제점들을 보완할 수 있는 대체 시스템으로 각광받고 있다. 특히 RFID 시스템은 교통카드, 출입구 보안 및 출결 카드 분야를 포함한 상거래와 직접적인 관련이 있는 물류관리, 재고관리, 항만관리, 동물관리 등 물류 및 유통 분야에서도 빠르게 응용 및 확산되어 사용되어 지고 있다. 본 논문에서는 유비쿼터스 컴퓨팅의 한 예로서 RFID시스템을 TCP/IP를 이용하여 네트워크화하여 구성한 안전하고 효율적인 원격 출입 제어 시스템을 제안한다. 먼저 원격 출입 제어에 적합한 인증 프로토콜을 제안하며, 제안한 인증 프로토콜 기반의 원격 보안 출입 제어 시스템이 원활한 자동문 제어가 가능함을 임베디드 시스템과 TCP/IP 기반의 RFID 시스템으로 구성된 자동문 세트를 활용한 모의실험을 통해 실용성을 증명한다.

Abstract

At present, RFID system is highly welcomed as a substitute system with its bar code recognition system and self recognition equipment. Consequently, the system has multi applications and can be complementing to its security. In particular, RFID system is significantly related with electronic transaction equipments : transportation card, ID card in check point, attendance sheet. Based upon these characteristic, the system is becoming extremely popular in the field of logistics, harbor and stock management, animal control and product circulation & distribution. In this dissertation, I would like to present a more efficient and stable remote entry control system with the network-based TCP/IP. It is a simple example of ubiquitous computing function. Above all, approved protocol system should be applied to the remote entry control function. Its efficient function with the applied approval protocol based-remote entry control system should be confirmed. Therefore, a preliminary test should be prerequisite in automatic entrance function with the embedded and TCP/IP-based RFID system.

Keywords : RFID, Ubiquitous, TCP/IP, Remote Security, Protocol

I. 서 론

최근 IT산업의 새로운 패러다임인 유비쿼터스 컴퓨팅 기술은 현재의 경기 불황을 극복하기 위한 한 방안으로 IT 전문가들에 의해 활발히 연구되어지고 있다. 유비쿼터스는 인터넷 기능을 구현해 언제, 어디서나 온라인에 손쉽게 접속할 수 있도록 해주는 기술로써, 알람시계, 부엌용 전자기기, 스테레오 장비 등과 같은 소형 전자기기에 임베디드 되어 활용되어진다[1~4]. 최근 무선통신기술의 진보와 보급률 증가로 수작업과 유선통신에 의존하고 있던 전통적인 물류시스템에 새로운 도전적 변화를 보이고 있다. RFID (Radio Frequency Identification)기술은, 뿐만 아니라, 수출입 업무에서 유통물류비 절감을 할 수 있는 기술로 각광받고 있으며, 우리나라도, 수출입 유통·물류산업에서 RFID 기술에 많은 관심을 가지고 있다. 본 논문에서는 물류정보시스

* 정회원, 명지대학교 국제통상학부
(Dept. of International Business and Trade, Myongji University)
** 정회원, 안양대학교 교양학부
(Dept. of Liberal Arts, Anyang Univ.)
*** 정회원, 대구산업정보대학
(Dept. of Computer&Information, Daegu-Polytechnic College)
**** 정회원, 상지대학교 컴퓨터공학과
(Dept. of Computer Science, Sangji Univ.)
접수일자: 2008년10월10일, 수정완료일: 2008년10월30일

템 구성요소의 하나인 RFID 기술을 이용한 원격보안 출입제어시스템을 제안 한다. 유비쿼터스 기술의 실현으로 실세계의 각종 사물들과 언제 어디서나 누구나 정보를 실시간으로 송수신 할 수 있는 시스템이 개발되고 있다. 유비쿼터스 컴퓨팅 혹은 네트워킹 기술이 초래하는 일종의 IT 혁명은 조용하게 추진되는 혁명일지는 모르나 그것이 가져올 파급효과는 클 것으로 생각된다.

특히 유비쿼터스 컴퓨팅의 핵심 역할을 하는 RFID (Radio Frequency Identification) 시스템은 현재 다양한 분야에서 사용되어 지고 있는 바코드 인식 시스템이나 자기 인식 장치들이 근본적으로 내재하고 있는 실용성 및 보안성 문제점들을 보완할 수 있는 대체 시스템으로 각광받고 있다. 특히 RFID 시스템은 교통카드, 출입구 보안 및 출결 카드 분야를 포함한 상거래와 직접적인 관련이 있는 물류관리, 재고관리, 항만관리, 동물관리 등 물류 및 유통 분야에서도 빠르게 응용 및 확산되어 사용되어 지고 있다[5~11]. 이에 본 논문에서는 유비쿼터스 컴퓨팅의 한 예로서 우리 실생활에 이미 적용되어 쓰이고 있는 교통카드 시스템과 같은 시스템과 RFID시스템을 TCP/IP를 이용하여 네트워크화 하여 구성한 원격 출입 제어 시스템을 제안한다. 먼저 원격 출입 제어에 적합한 인증 프로토콜[11]을 제안하며, 제안한 인증 프로토콜 기반의 원격 보안 출입 제어 시스템이 원활한 자동문 제어가 가능함을 임베디드 시스템과 TCP/IP 기반의 RFID 시스템으로 구성된 자동문 세트를 활용한 모의실험을 통해 실용성을 증명한다. 본 논문의 구성은 다음과 같다. Ⅱ장에서 제안한 원격 보안 출입 제어 시스템을 위한 국내 개발 환경을 설명하고, Ⅲ장에서 제안한 원격 보안 출입 제어 시스템에 적합한 RFID 인증 프로토콜을 설명한다. Ⅳ장에서는 제안한 원격 보안 출입 제어 시스템의 모의 실험결과를 보이며, Ⅴ장에서 결론을 맺는다.

Ⅱ. 국내 RFID 시스템 개발 환경

IT 기술의 발달과 이로 인한 전자상거래가 활성화되면서 수출입 물류도 웹을 기반으로 한 전자물류로 변화하고 있는 추세이다. 특히 대기업체 물류기업은 운송관리시스템(TMS), 창고관리시스템(WMS), 주문관리시스템(OMS) 뿐 아니라 수송최적화를 위한 물류활동의 전 분야를 정보화하고 있으며 화주기업의 ERP(전사적 자원관리) 구축이 일반화되면서 정보화는 물류기업이 필수적으로 갖춰야할 역량이 되고 있다. RFID는 제품에

표 1. RFID와 바코드의 특징 비교
Table 1. Comparison of characteristic rfid and bar-code.

구 분	RFID	바코드
상품식별	개별상품식별	상품군 식별
부착범위	개별상품, 팔레트 등	개별상품, 팔레트 등
정보전달	실시간(동적)	배치방식(정적)
비 용	칩 가격(0.5 ~ 1 USD)	거의 없음
표준화	국제표준제정진행	국제표준있음
읽기/쓰기	읽기/쓰기 가능	1회 입력(인쇄)
정보량	많은 정보입력 가능	거의 없음
재활용(사용기간)	가능(약 10 만번 ; 60년)	불가능
투과	가 능	불가능
인식거리	0 ~ 100m	0 ~ 50Cm
인식속도	0.01 ~ 0.1 초	4초
보완능력	복제불가	없음
card 손상률	거의 없음	매우 잦음

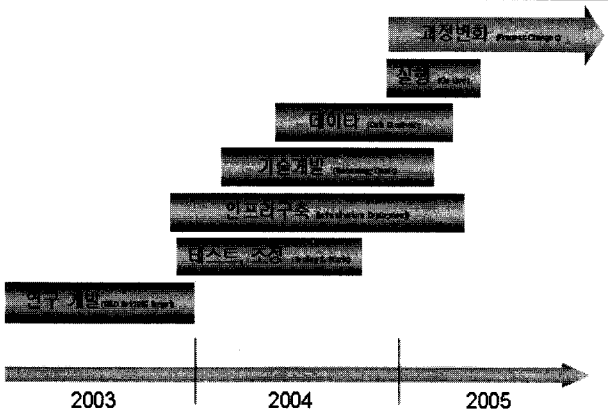


그림 1. 월마트의 RFID 발전단계
Fig. 1. Wal-Mart of RFID development step.

부착하는 태그(Tag)에 생산, 유통, 보관, 소비 등의 정보를 저장할 수 있고 자체 안테나를 갖추고 있으며, 리더(Reader)로 하여 이러한 정보를 읽고, 이동통신망과 연계하여 데이터를 통합하여 사용할 수 있는 칩을 말한다. RFID tag는 정보인식을 위한 직접적인 접촉 없이 데이터를 읽거나 쓸 수 있으며 상대적으로 많은 정보를 저장 할 수 있는 등 바코드와는 많은 차이점을 지닌다. 바코드와 RFID tag를 간략하게 비교하면 표 1과 같다.

특히 최근에는 첨단 RFID 무선인식 기술을 활용한 RTLS(실시간 위치시스템) 서비스 등을 통해 위치 추적, 재고관리, 고객관리, 물류경로 최적화 서비스등을 제공하는 유비쿼터스 물류(U-Logistics)로까지 진화하고 있는 상황이며 그림 1에서는 이러한 RFID 도입과정을 설명하고 있다.

해외사례로는 2004년 4월 Dallas/Fort worth 지역의 몇몇 마트 및 물류창고에서 8개 공급업체를 대상으로 RFID 태그 부착 테스트를 시작하였으며, 2005년 1월

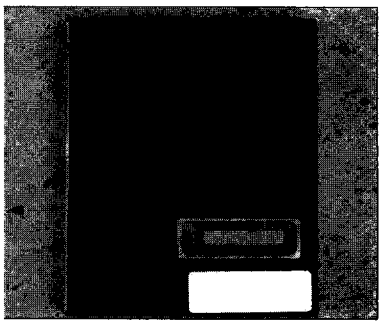


그림 2. Tesco 제품 RFID tag
Fig. 2. Tesco product RFID tag.

본격적으로 Dallas/Fort worth 지역의 36개의 샘스클럽(SAM's club), 104개의 Wal-Mart, 그리고 3개의 물류센터에 RFID 기술을 도입하여 230 마일 길이의 케이블(data cable & coax)이 사용되고 있으며, 14,000개 이상의 하드웨어가 사용되고 있다. 이러한 결과, 57개의 공급업체가 RFID 태그를 부착하여 공급하였고 7,161개의 태그가 부착된 팔레트로 제품을 납품하게 되었다. 그리고 태그가 부착된 210,390 개의 제품이 납품 되었고 150만개의 태그가 작동 하고 있다.

RFID 태그 부착은 현재 공급업자 측 의무가 아니며 Tesco의 밀턴케인즈 물류센터에서 해당상품배송오더 접수 시 Tesco 자기비용으로 태그를 부착하고 요청매장으로 배송하고 있는 추세이다. Tesco측은 시범운영품목의 성과를 보아가며 추진할 예정으로 점진적으로 도입할 예정이다. 그림 2는 DVD 타이틀과 컴퓨터 개인 소프트웨어에 대해서만 시범운영매장에 전시된 RFID Tag 사진을 보여주고 있다. 우리나라에서도 이러한 물류산업이 중요성을 인식하고 그간 인천공항, 부산항 신항, 광양항 등 물류인프라를 확충하고 항공자유화, 포트얼라이언스 등을 통해 글로벌 네트워크를 확대해 왔다. 뿐만 아니라, 인프라와 네트워크를 활용해 우리나라에 세계의 화물, 정보, 사람을 끌어들일 수 있는 글로벌 시장에서 경쟁력 있는 물류기업을 육성하기 위한 물류기업 육성정책도 지속적으로 추진하는 계획을 수립하고 있다. 본 논문에서는 이러한 물류 시스템에 이용될 수 있는 RFID와 TCP/IP를 활용한 원격 출입 제어 시스템을 제안한다. 본 shamans에서 제안한 시스템은 RFID 리더보드와 임베디드(Embedded) 보드, 그리고 스텝모터 드라이브, 자동문 세트로 구성되어 진다. RFID 리더보드는 크게 RFID와 CPU 부분으로 나눌 수 있다. 134.2㎑ RFID 리더를 구성하기 위하여 RFID는 TI사의 LF Base Station IC TMS3705A를 선정하였다. 3705A는 안테나를 직접 구동할 수 있는 구성요소들을 내장

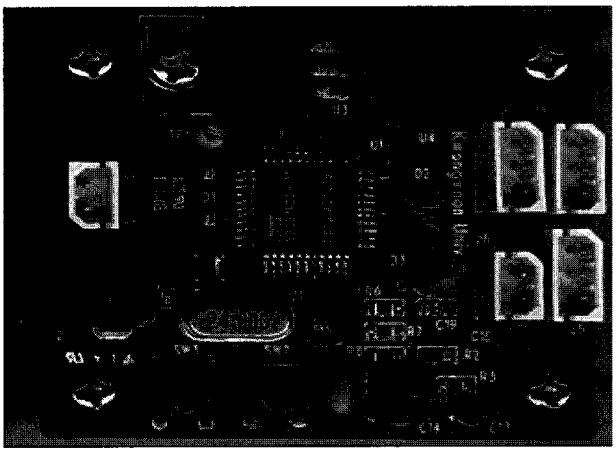


그림 3. RFID 리더 보드
Fig. 3. RFID reader board.

하고 있으며, PLL 내장, FSK 변조방식을 사용하고, 각종 필요한 기능이 내장되어 있기 때문에 3705A를 선정하여 실험에 활용하였다[5~8]. 그림 3은 완성된 RFID 리더 보드를 보여준다.

TCP/IP 네트워킹 기능을 갖춘 임베디드 보드는 크게 H/W부와 S/W부로 구성된다[12~14]. H/W부의 구성: 그림 2는 네트워크 임베디드 보드를 보여준다. S/W부의 구성: S/W부는 크게 PC와 TCP/IP 프로그램 부분과 RFID와 UART (Universal Asynchronous Receiver /Transmitter) 통신 프로그램 부분으로 구성된다.

① PC와 TCP/IP 프로그램 - 네트워크 임베디드 보드는 원격지의 PC로부터 RFID 리더로 명령을 내려 보내는 과정에서 중간 매개체에 해당한다. 네트워크 임베디드 보드는 PC로부터 문을 열라는 명령이나 문을 닫으라는 명령을 받으면, 해당명령을 UART를 통해 RFID 리더로 전송하는 역할을 한다. 즉, 네트워크 임베디드 보드는 RFID로부터 UART를 통해 받아들인 태그의 ID 정보를 원격지에 있는 PC로 이더넷을 통하여 전송한다. 이때 전송프로토콜로는 TCP/IP를 사용한다. DS80C400 CPU는 자체 네트워크가 가능한 TCP/IP 스택을 포함하고 있다. 사용자는 단지 라이브러리 파일을 사용하여 프로그램하면 된다. Maxim-Dallas사는 자사 홈페이지를 통해 Keil C Complier 환경에서 사용할 수 있는 각종 라이브러리 파일을 무료로 제공해준다.

② RFID와 UART 통신 프로그램 - 네트워크 임베디드 보드는 RFID 리더에 시리얼 포트 0를 사용하여 데이터를 전송한다. 이때 프로토콜로는 '0x30' 과 '0x31' 이라는 각 한 바이트의 데이터를 이용하여 'OpenDoor', 'Close Door' 라는 명령 포맷을 만들었다. 자동문 세트는 시중에서 판매하는 것으로 스텝모터와 타이밍벨트,

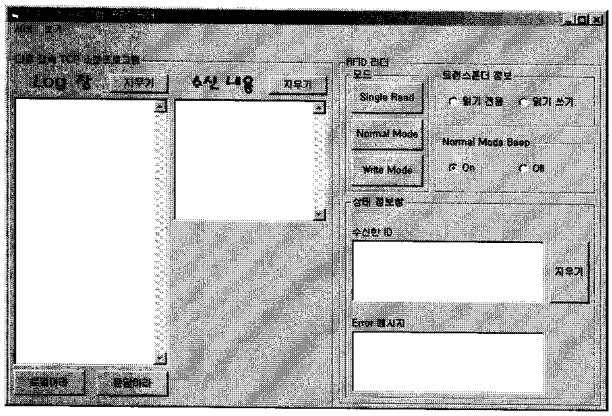


그림 4. TCP/IP 소켓 프로그램
Fig. 4. TCP/IP Socket program.

베어링을 이용하는 것으로 구입하였다[15~16]. 그림 3은 자동문 세트를 보여준다. 제안한 시스템에서는 윈도우즈 환경 하에서 실행 가능한 TCP/IP 소켓프로그램 및 RFID 리더 제어용 어플리케이션을 작성하기 위하여, 배우기 쉽고 사용하기 간편한 비주얼베이직 6.0 버전을 사용하여 프로그램 하였다[17]. 그림 4는 TCP/IP 소켓프로그램 부분과 RFID 리더프로그램 부분을 보여준다.

Log 창은 출입한 사람의 이름과 시각이 저장되고, 수신내용에는 임베디드 네트워크 보드로부터 수신한 데이터를 그대로 가공하지 않고 나타내며, 수신한 ID에는 현재 인식된 태그의 ID 값 96비트가 아스키 문자 형태로 나타나며, 에러 메시지 창에는 에러내용이 표시된다.

III. 제안한 보안 원격 출입 제어 시스템

본 논문에서 제안한 보안 원격 출입 제어 시스템의 동작 과정과 인증 프로토콜의 수행 과정에 관해 설명한다.

제안한 보안 원격 출입 제어 시스템은 다음과 같이 7단계로 동작한다.

[단계 1]. PC상에서 TCP/IP 소켓프로그램과 RFID 리더 프로그램을 실행하여 서버를 실행한다.

[단계 2]. 서버가 실행된 후, 임베디드 네트워크 보드의 전원을 인가하여, 소켓을 생성한다.

[단계 3]. 생성된 소켓을 기반으로, TCP/IP 소켓프로그램과 RFID 리더프로그램의 정상 모드 버튼을 클릭하여 0.5초 간격으로 RFID 리더를 동작시킨다.

[단계 4]. RFDI 리더는 0.5초 간격으로 센싱 동작을 수행한다. 이때 만약 인식되는 태그가 있으면 그 태그의 ID를 수신 ID에 보여주며, 더 나아가 만약 DB내에 등록된 ID일 경우 ID에 해당하는 사람의 사진을 보여준다.

[단계 5]. Log 표시 창에 ID에 해당하는 사람의 이름과 출입 날짜 및 출입 시각을 표시한다. 이때, 만약 등록되지 않은 ID일 경우에는 기본 사진을 보여준다.

[단계 6]. 등록된 ID가 인식되었을 경우 스텝 모터 구동 드라이버로 "Open Door" 명령을 내려 보낸다.

[단계 7]. 스텝모터는 Open Loop로 제어되며, 정확한 길이만큼 문을 열기 위해 미리 실험하여 얻은 수치만큼 스텝모터를 회전시킨다. 더 이상 같은 ID가 인식되지 않는다면, TCP/IP 소켓프로그램과 RFID 리더 프로그램은 스텝 모터 구동드라이버로 "Close Door" 라는 명령을 내려 보내고, 문은 닫히게 된다.

제안한 보안 원격 출입 제어 시스템의 안전성 및 효율성 보장을 위해 다음과 RFID 태그와 리더 간의 인증 프로토콜을 수행한 후 출입문을 개폐하게 된다. 먼저 제안한 RFID 인증 프로토콜에서 사용할 용어들은 아래와 같다.

- $query$: 태그의 응답을 요청하는 리더의 요청
- ID : 태그에 할당된 고유정보
- $h(\cdot)$: 안전한 일방향 해쉬함수
- n_R : 리더가 생성한 난수
- $\oplus$: 비트단위 배타적논리합(XOR) 연산

그림 5는 제안한 RFID 인증 프로토콜의 전체적인 구성과 동작 과정을 보여주며, 아래와 같이 인증 프로토콜이 수행된다. 그림 5에서 리더와 백-엔드 데이터베이

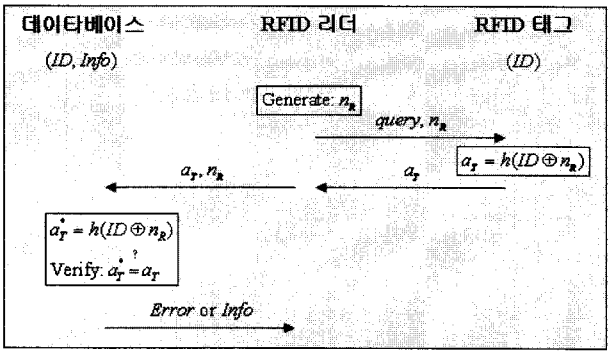


그림 5. RFID 인증 프로토콜
Fig. 5. RFID certification protocol.

스 사이의 통신 채널은 공격자로부터 안전한 채널임을 가정한다.

[단계 1]. 리더 → 태그: $query$, n_R
리더는 태그를 인증하기 위해 난수 n_R을 생성하여 $query$와 함께 태그에게 전송한다.

[단계 2]. 태그 → 리더: a_T
태그는 $query$와 n_R을 수신한 후, DB가 자신을 인증할 수 있도록 인증 메시지 $a_T = h(ID \oplus n_R)$를 계산하여 리더에게 전송한다.

[단계 3]. 리더 → DB: a_T, n_R
리더는 수신한 a_T 메시지와 자신이 생성한 n_R을 DB에게 전송한다.

[단계 4]. DB → 리더: $Info$
DB는 자신의 데이터베이스 내에 저장되어 있는 태그들의 ID와 수신한 n_R을 이용하여 $a_T^* = h(ID \oplus n_R)$를 계산한 후, 수신된 a_T와 일치하는 값을 찾는다. 만약 수신된 a_T가 DB에서 계산된 a_T^* 값들과 일치하지 않는다면, DB는 Error 메시지를 리더에게 전송한다. 만약 수신된 a_T와 DB에서 계산된 a_T^*이 일치한다면 해당 태그를 인증하게 되고, 리더가 필요로 하는 "Open Door" 또는 "Close Door"에 관한 정보를 담고 있는 $Info$를 리더에게 전송한다.

[단계 5]. 리더는 Error메시지를 수신한 경우, 태그와의 통신을 중단하고, $Info$ 메시지를 수신한 경우 태그에 관한 정보를 담고 있는 $Info$ 정보를 활용하여 "Open Door" 또는 "Close Door" 명령을 수행한다.

본 절에서는 제안한 RFID 인증 프로토콜에 대한 안전성과 효율성을 분석한다. 제안한 RFID 인증 프로토콜은 간단한 단방향 인증을 통해 효율성을 보장하며, 도청 공격, 재전송 공격, 스푸핑 공격 등에 안전하다[5~11].

① 단방향인증(Unitary authentication): 제안한 인증 프로토콜의 단 계 4에서 DB는 태그로부터 수신한 $a_T = h(ID \oplus n_R)$가 DB 자신이 계산한 $a_T^* = h(ID \oplus n_R)$과 동일한지를 검증하여, 맞으면 태그를 인증하고 틀리면 통신을 중단하게 된다. 태그와 DB 사이에 공유된 비밀키 역할을 하는 ID를 모르는 공격자는 태그로 위장하여 위장 공격 등을 수행할 수 없게 된다. 즉 비밀 값인 ID는 태그와 DB측에서 내부적으로 활용되어 지며 공개된 통신 채널로 전송되어 지지 않기에 공격자는 ID를 구할 수 없다. 따라서 제안한 프로토콜은 단방향 인증을 통한 효율적인 인증을 제공한다.

② 도청 공격(Eavesdropping attack): 제안한 인증 프로토콜에서 공격자는 송수신되는 통신 메시지 $query$, n_R , a_T를 도청할 수 있다. 하지만 도청한 내용으로부터 공격자는 태그와 리더의 DB 간에 공유된 비밀키 역할을 하는 ID를 구할 수 없다. 즉, ID를 얻기 위해서는 공격자가 $a_T = h(ID \oplus n_R)$로부터 ID를 구할 수 있어야 한다. 하지만 안전한 일방향 해쉬 함수의 성질에 의해 공격자는 a_T로부터 ID를 얻는 것은 불가능하다. 따라서 제안한 프로토콜은 도청 공격에 안전하다.

③ 재전송 공격(Replay attack): 제안한 인증 프로토콜에서는 매 세션마다 새로운 난수n_R을 리더가 생성하여 인증을 수행하기 때문에 과거에 공격자에 의해 재전송된 난수 값은 DB의 검증 과정 중에 쉽게 검출된다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

④ 스푸핑 공격(Spoofing attack): 제안한 인증 프로토콜에서 공격자가 리더의 DB와 태그간에 공유된 비밀 ID를 얻을 수 있으면 스푸핑 공격을 수행할 수 있다. 하지만 공격자는 리더의 DB와 태그내에 각각 안전하게 저장하고 있는 비밀 ID를 직접적으로 얻을 수 있는 방법이 없다. 또한 송수신되는 통신 메시지 $a_T = h(ID \oplus n_R)$ 내의 비밀 ID는 난수 n_R과 안전한 일방향 해쉬함수에 의해 보호되어져 있다. 따라서 제안한 프로토콜은 스푸핑 공격에 안전하다.

IV. 시뮬레이션 결과

본 장에서는 III장에서 제안한 RFID 인증 프로토콜을 적용하여 구성한 원격 보안 출입 제어 시스템의 모의 실험결과를 보인다.

제안한 RFID 인증 프로토콜의 구현에 대한 정보는 다음과 같다. 현재 EPCGlobal이 사실상의 RFID 산업계 표준을 주도하고 있다. 이에, 본 논문에서 제안한 RFID 인증 프로토콜은 EPC Class 1 Generation 2 표준을 준수하기 위해 Class 1의 읽고 쓰기 태그(Read/Write

Tag)를 사용하여 13.56MHz주파수 대역을 기반으로 구현하였다. RFID 태그는 수동적이며, 전원은 리더에 의해서 유인 받는다. 태그의 제한된 자원은 많은 자원을 필요로 하는 공개키 방식의 암호화와 같은 대칭 암호화를 사용할 여유가 없기에 난수 생성기로 16비트 PRNG(Pseudo-Random Number Generator)를 지원하게 하였다. 태그에는 EPC라는 고유의 코드를 가지고 있다. EPC 코드는 태그를 구분하는 유일한 ID 값으로써 본 시뮬레이션에서는 헤더(8bit) + 업체코드(28bit) + 사용자정보코드(24bit) + 일련번호(36bit)로 총 96비트로 구성되어 있다. 또한 본 시뮬레이션에서 사용된 해쉬 함수는 8,400개의 회로 게이트를 사용하는 MD5 해쉬 함수를 사용하였다. 물론 MD5 해쉬 함수의 충돌 저항성 문제가 최근 중요한 보안 이슈가 되고 있으나 본 실험에서는 수동적 RFID 태그의 특성상 일방향 성질에 초점을 두어 MD5 해쉬 함수를 적용하였다. 만약 보다 높은 안전성 확보를 원하면 SHA-256과 같은 안전한 해쉬 함수를 적용할 수 있다. 다음은 본 시뮬레이션에서 사용된 실험데이터 값들의 비트 길이를 보여준다.

실험데이터 값들의 비트 길이	
ID값 (EPC 코드)	96bit
PRNG 난수값 (n_R)	16bit
MD5 해쉬결과값 ($a_T = h(ID \oplus n_R)$)	128bit

그림 6은 TCP/IP 소켓프로그램과 RFID 리더 프로그램의 시작 모습을 보여준다.

프로그램을 시작하려면, 먼저 상단의 메뉴 중에 [서버]-[시작]을 클릭하고, 네트워크 임베디드 보드의 전원을 인가함으로써 시스템이 시작된다. 이후 그림 6의 우측 RFID 리더부분의 정상 모드 버튼을 클릭하여 RFID로부터 0.5초 간격으로 RFID 태그를 감지하는 RF파를 전파하도록 시뮬레이션 하였다.

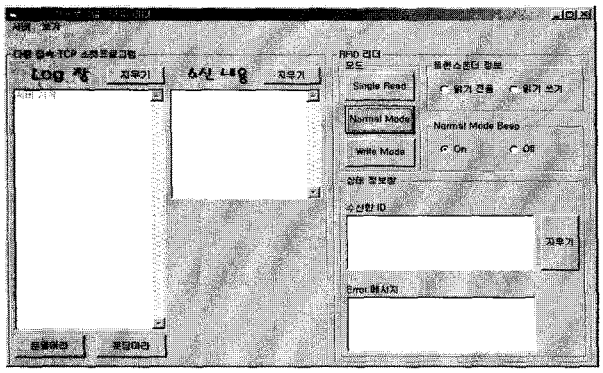


그림 6. 프로그램 시뮬레이션
Fig. 6. Program simulation.

이후의 RFID와 TCP/IP를 활용한 원격 보안 출입 제어 시스템의 작동 절차는 다음과 같다.

① 시스템 대기 상태로 대상의 접근을 기다린다.

② 대상이 접근함을 센서로 감지 시스템을 작동시킨다.

③ 음성 또는 판넬을 통하여 RFID 태그 기반의 ID 카드를 사용하라고 대상에게 알려준다. 이때 리더는 난수 값을 생성하여 ID 카드에게 전송한다.

④ ID 카드는 리더와 공유된 ID 정보를 수신한 난수와 해쉬 함수를 이용하여 암호화하여 복제 불가능하게 만들어 리더에게 송신한다.

⑤ 리더는 수신한 정보를 기반으로 신원 조회 후 허가된 사용자인 경우 문을 열어준다. 만약 허가된 사용자가 아닌 경우 경고메시지를 발생시킨다.

⑥ 인증을 받은 합법적인 ID 카드 소유자는 문을 통과하며, 리더는 사용자가 완전히 빠져나갔는지 여부를 감지하고 나서 문을 닫는다.

⑦ 새로운 대상의 접근을 대비해 시스템 대기 상태로 전환한다.

⑧ 반대로 대상이 외부로 나갈 시에는 리더의 센서로 대상을 감지한 후 별도의 인증 절차 없이 문을 열어 대상을 밖으로 나갈 수 있도록 동작시킨다.

제안한 시스템의 모의실험에서는 별도의 센싱 절차를 거치지 않은 채 카드 리더기가 계속 동작하도록 하였다. 또한 대상이 완전히 출입문을 통과하는 시간은 대략 10초정도면 충분하다고 가정하여 일정시간 후에 문이 닫히도록 설계하였다. 이로 인해 만약 대상이 10초안으로 출입문을 통과하지 못하면 문 사이에 끼이게 되는 불행한 사태가 벌어질 수도 있다.

V. 결 론

본 논문에서는 원격 출입 제어에 적합한 안전하고 효율적인 단방향 RFID 인증 프로토콜을 개발하였으며, 이를 임베디드 시스템과 TCP/IP 기반의 RFID 시스템으로 구성된 자동문 세트를 활용한 원격 보안 출입 제어 시스템에 적용하여 원활한 자동문 제어가 가능함을 모의실험을 통해 증명하였다.

향후 연구과제로는 만약 대상이 10초안으로 출입문

을 통과하지 못하면 문 사이에 끼이게 되는 불행한 사태가 벌어질 수도 있는데 이러한 문제점 해결 방안이 필요할 것이다. 또 다른 문제점은 허가되지 않은 제3의 인물이 허가된 ID카드를 사용하여 출입을 하게 되는 경우 리더가 인증하게 되는 문제가 있다. 이와 같은 문제는 ID카드로 대상을 인식한 후 별도로 각 대상에게 부여된 비밀번호를 입력하는 키패드 등을 추가하여 2중으로 보안시스템을 구성하면 해결가능하다고 생각된다. 더 나아가 얼굴 명암의 극심한 변화와 포즈의 많은 변화가 있는 얼굴 데이터베이스에 추가적인 기하학적 특징을 적용하는 방안과 실시간 얼굴 인식 시스템에 제안한 방법을 적용시키는 연구도 필요할 것으로 생각된다.

참 고 문 헌

[1] M. Weiser, "Some Computer Science Problems in Ubiquitous Computing", Communications of the ACM, July 1993.

[2] M. Weiser, "Ubiquitous Computing", Nikkei Electronics, pp. 137-143, December 1993.

이근호, 이기혁, 한호현, 유비쿼터스 컴퓨팅 핸드북, 진한도서, 2003.

[3] A. Jule, "Authentication Pervasive Devices with Human Protocols", To appear Crypto 2005, Aug 2005.

[4] KLAUS FINKENZELLER, RFID HAND BOOK Second Edition, WILEY, 2002.

[5] S. E. Sarma, "Towards the Fivecent Tag", MIT Auto ID Center, Technical Report MIT-AUTOID -WH-006.2001.(http://autoid center.org)

[6] A. Juels, R. L. Rivest, and M. Szydlo "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", In Proceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp.103-111, 2003.

[7] A. Jule and R. Pappu, "Squealing Euros: Privacy Protection in RFID-enable Banknote", In proceedings of Financial Cryptography-FC'03, Vol. 2742 LNCS, pp. 103-121, Sep. 2003.

[8] 정병호, "RFID/USN 환경에서의 정보보호", 제9회 정보보보심포지움, pp. 447-463, 2004.

[9] 최은영, 이동훈, "RFID 정보보호 기술 동향", 정보처리학회지, 제12권, 제5호, 2005.

[10] 강전일, 박주성, 양대헌, "RFID 시스템에서의 프라이버시 보호기술", 정보보호학회지, 제14권, 제6호, 2004.

[11] Don Eisenreich and Brian DeMuch, Designing Embedded Internet Devices, Elsevier- Science, 2003.

[12] Don Loomis, The TINITM Specification and Developer's Guide, ADDISON-WESLEY, 2001.

[13] DS80C400, DStinim400, DStinis400 DataSheet (Maxim-Dallas semiconductor)

[14] 조영준, AVR AT90S5815, Ohm사, 2001.

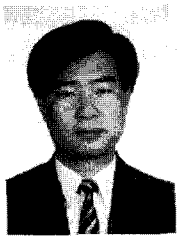
[15] 신대섭, 정상봉, C가 미는 로보트, 도서출판 세화, 2000.

[16] 윤성우, TCP/IP 소켓 프로그래밍, FREELEC, 2003김완석, 김정국, 김효기, 김창석, 구홍서, 이상범, 박태웅, 이성국 공역, "유비쿼터스

저 자 소 개

김 정 숙(정회원)
1994년 세종대학교경제학과 (경제학석사)
1998년 세종대학교경제학과 (경제학박사)
2000년~2001년 ETRI근무
2001년~2003년 고려대, 단국대, 성신여대경제학
2004년~현재 명지대학교 국제통상학과
2006년~현재 대한전자공학회 정회원
1999년~현재 국제무역학회 정회원
1999년~현재 산업조직학회 정회원
2005년~현재 한국관세학회 정회원
2008년~현재 한국컨설팅학회 이사
2006년~현재 인터넷 방송통신TV학회 협동이사
<주관심분야 : 통신, 컴퓨터, 신호처리, 반도체,경제법,산업조직,미시경제,국제무역관세>

윤 은 준(정회원)
2003년 경일대학교 컴퓨터공학과 (공학석사)
2007년 경북대학교 컴퓨터공학과 (공학박사)
2007년~현재 대구산업정보대학 컴퓨터정보계열 전임강사
2007년~현재 보안공학연구지원센터 보안공학 논문지 편집위원
<주관심분야: 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜>



김 천 식(정회원)
1997년 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학석사)
2003년 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학박사)
2000년~2003년 경동대학교 정보통신공학부 교수
2004년~현재 안양대학교 교수
2007년~현재 대한전자공학회 컴퓨터소사이어티 분과위원장
2008년~현재 인터넷 방송통신 TV학회 상임이사
2006년~현재 인터넷 정보학회 학회편집위원
2006년~현재 대한교통학회 정회원
2005년~현재 한국데이터베이스학회 정회원
<주관심분야: 데이터베이스, 데이터마이닝, 이미지처리, e-Learning, Agent system>

홍 유 식(정회원)
1984년 경희대학교 전자공학과 (학사)
1989년 뉴욕공과대학교 전산학과 (석사)
1997년 경희대학교 전자공학과 (박사)
1985년~1987년 대한항공(N.Y.지점 근무)
1989년~1990년 삼성전자 종합기술원 연구원
1991년~현재 상지대학교 컴퓨터공학부 교수
2000년~현재 한국 퍼지 및 지능시스템학회 이사
2004년~현재 대한 전자 공학회 ITS 분과위원장
2001년~2003년 한국 정보과학회 편집위원
2001년~2003년 한국 컴퓨터 교육산업학회 이사, 편집위원
2004년~현재 건설교통부 ITS 전문심사위원
2004년~현재 원주 시 인공지능신호등 심사위원
2005년~현재 정보처리학회 이사
2005년~현재 인터넷 정보학회 이사
2005년~현재 정보처리학회 강원지부 부회장
2008년~현재 인터넷 방송통신 TV학회 부회장
<주관심분야: 퍼지 시스템, 전문가시스템, 신경망, 교통제어>