Bluetooth 통신을 이용한 홈 오토메이션 보안 시스템

정윤화° 윤주대 안광선
경북대학교 컴퓨터 공학과
{withfun0425°, yjoodae, gsahn}@knu.ac.kr

Security System to use Bluetooth Communication for Home Automation

Yunhwa Jung° Joodae Yoon Gwangseon Ahn
Dept. of Computer Engineering, Kyungpook National University

요 약

본 논문에서는 주거생활의 안전을 위해 암호화 코드를 포함한 홈 서버를 설계하고, 블루투스 통신을 이용하여 암호화 코드를 송수신하는 시스템을 구현하였다. 제안한 홈 시큐리티 시스템은 적외선 통신이나 무선랜 등 다양한 인터페이스를 활용할 수 있다는 장점을 가진다. 이와 더불어 제안된 보안 시스템은 건물이나 공장, 자동차 등에서도 적용가능하다. 본 논문에서는 홈 오토메이션 을 위한 DES 암호화 알고리즘 기반의 디지털 도어 락 시스템을 제안한다. 암호화 코드를 이용하는 보안 시스템을 구성하면 높은 수준의 보안성을 얻을 수 있고, 키의 분배가 용이하다. 제안하는 보안 시스템은 스마트 폰을 키로 이용함으로써 사용자 편이성을 증대시켰다.

1. 서 론

전통적인 홈 오토메이션 시스템은 화재나 가스누출, 외부인 침입에 대해 이상이 감지되면 경계신호를 전송하는 수준의 초보적인 보안성만을 제공하는 제한된 자동화였다. 또한 관련 장치도 하드웨어에 기반을 두고 있었기 때문에 소비자의 입장에서 더 높은 수준의 보안 기능을 원할 경우 부가적인 비용과 노동력이 투입되어야 한다는 맹점이 있었다[1]. 최근에는 정보 통신 기술의 발달로 홈 시큐리티는 물론 실내 모든 장치를 홈서버 하나로 제어하는 향상된 홈 오토메이션 시스템이 출현하였다[2]. 홈 오토메이션에 접근하는 출발점은 현관문이고 이는 곧 홈 시큐리티의 출발점이기도 하다. 이를 위해 현재 디지털 도어 락, 지문 인식 시스템과 생체 인식 시스템 등이 개발되어 이미 상용화 되어 있다. 그러나 디지털 도어 락은 10개의 숫자를 이용하는 중복순열이므로 $1/10^n$의 확률을 가지는 제한적인 보안 시스템일 뿐만 아니라 매일 출입하는 현관문을 열기 위해 긴 수열을 암기하여 누르는 사용자가 많지 않다는 점을 감안한다면 보안성이 취약하다고 할 수 있다. 패스워드는 입으로 전달되는 것이므로 언제든 많은 복제가 있을 수 있는 단점이 있다.
생체 인식 시스템도 많은 단점을 가지고 있다. 지문인식은 복제가 가능하고, 얼굴인식은 화장, 가발 등으로 인식률이 좋지 않다. 장문인식은 인식 장치가 크고 타인을 본인으로 오인하는 오류률이 높다. 본 논문에서는 생활필수품이 된 휴대폰(스마트폰)에 보안 기능을 추가하여 홈 시큐리티 시스템에 접근하는 인증서로 사용하는 기법을 제안한다. 홍체 인식은 카메라의 오염에 따른 오작동 가능성이 있다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 관련 연구에 대해 알아보고, 3장에서는 논문에서 제안한 전체 시스템의 구조를 설명한다. 4장에서는 암호화 모듈설계를 살펴보고 5장에서 블루투스 통신 구조, 6장에서 임베디드 락 시스템 설계를 기술한다. 7장은 실험 및 결과를 마지막 8장에는 결론을 맺고 앞으로의 연구방향을 제시한다.

2. 관련 연구

2.1 암호화

암호화란 정보를 보내거나 받을 때 그 정보의 비밀성을 보장하기 위하여 해독할 수 없도록 다른 형태의 정보로 변환하는 것을 말한다. 암호화 방법에는 공개키 방식과 비밀키 방식이 있다. 공개키 방법은 암호화하는 키와 복호화키(암호를 푸는 키)가 다른 알고리즘이고 비밀키 방식은 암호화하는 키와 복호화키가 동일한 알고리즘이다[3]. 암호화는 3가지 중요한 특징을 만족시켜야 한다. 기밀성(secrecy), 무결성(integrity), 인증성(authenticity)이다. 기밀성은 메시지를 볼 수 있는 사람을 제한하는 성질이고, 무결성은 전달과정에서 제 3자에 의해 변조되지 않았는가 확인하는 기능, 그리고 인증성은 메시지 생성자의 신분을 확인 하는 것을 말한다. 현재까지 제안된 암호 알고리즘들은 충분한 안정성을 가지며 이러한 특성을 모두 만족해야 한다.

2.2 블루투스

블루투스(Bluetooth)는 가정이나 사무실 내에 있는 컴퓨터, 프린터, 휴대폰, PDA 등 정보통신 기기는 디지털

가전제품을 물리적인 케이블 접속 없이 무선으로 연결해 주는 근거리 무선접속기술이다[4]. 2.4Hz(2.4~2.4835)의 ISM(Industrial Scientific Medical) 무면허 밴드의 대역폭을 사용하며, 저전력 저가격에 아주 작은 칩을 사용하므로 어떤 종류의 전자제품에도 장착해서 무선 연결을 가능하게 한다. 최대 데이터 전송속도는 1Mb/s이고, 풀듀플렉스 전송을 위해서는 시간분할 다중 방식(Time-Division Duplex scheme)이 사용 된다[5]. 본 논문에서 텔레매틱스 기반에 블루투스 통신을 통하여 암호화하여 보안 시스템을 설계하는데 주안점을 둔다.

3. 전체 시스템 구조

본 논문은 스마트폰의 인증서를 블루투스를 통해 홈 서버에 전송하여 복호화 후 검증을 거쳐 문을 오픈한다. 그림 1은 본 논문에서 제안하는 시스템의 전체적인 구성도이다.

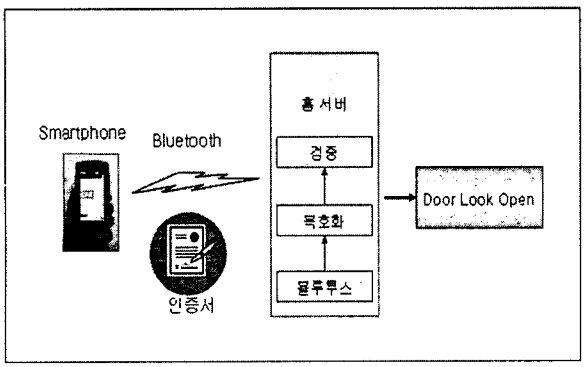

그림 1. 제안된 시스템 구조

그림 1에서 스마트폰은 먼저 키 생성/분배기(Key generator/distributor)에서 암호화를 거친 암호를 받는다. 키 생성/분배기는 필요한 수만큼의 암호를 생성하고 분배하는 역할을 한다. 암호를 블루투스를 통해 전송을 하면 도어 락 시스템에서 암호를 받아 복호화를 한다. 복호화된 암호는 락 시스템이 이미 키 생성/분배기에서 받은 원본 암호와 대조작업을 한다. 암호의 무결성이 확인되면 락을 해제한다.

임베디드 도어 락 시스템은 다음과 같이 크게 세 부분으로 구성된다.

- 스마트 폰을 위한 암호화
  암호를 키 생성/분배기로부터 받아 블루투스를 통해 도어 락 시스템으로 전송하는 모듈을 설계한다
- 블루투스 통신 설계
  스마트폰과 임베디드 락 시스템사이의 통신 환경을 구축한다.
- 도어 락 시스템 설계
  블루투스 모듈에서 데이터를 전송받아 락을 해제하는 시스템을 설계한다.

4. 암호화 모듈 설계

본 논문에서는 대칭키 암호화를 사용한다. 대표적인 알고리즘으로 DES(Data Encryption Standard)가 있다. DES는 오래 동안 연구되어 안전성으로 보았을 때 검증이 많이 이루어져 있다. 이 논문에서는 Rivest가 개발한 가변길이의 키를 가진 블록 암호 알고리즘 RC4를 사용한다. RC4는 DES보다 암호화 속도가 빠르고 128비트 이하의 길이를 가지는 가변키를 사용한다. 다음 그림 2는 홈 서버에서 인증서를 암호화하는 방법을 보여준다.

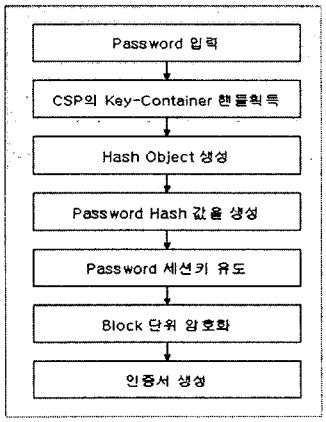

그림 2. 암호화 방법

암호화 기능을 구현하기 위해 MS Platform SDK에서 제공하는 CryptoAPI를 사용하였다. API를 사용함으로써 CSP(Cryptographic Service Provider)의 기능을 사용 할 수 있다. 속도의 최적화를 위해서 프로그램을 MFC나 .net framework을 사용하지 않고 순수 Win32 API를 이용해서 구현하였다. 그림 3은 암호화하는 코드의 일부분이다[6][7].

```
hSource = fopen(OpenfileName, "rb");
hDestination = fopen(OutPutFileName, "wb");
CryptAcquireContext(&hCryptProv, NULL, MS_ENHANCED_PROV,PROV_RSA_FULL,0);
CryptCreateHash(hCryptProv,CALG_MD5,0,0,&hHash);
CryptHashData(hHash, (BYTE *)szPassword,strlen(szPassword),0);
CryptDeriveKey(hCryptProv, ENCRYPT_ALGORITHM,hHash, KEYLENGTH, &hKey);
    CryptDestroyHash(hHash);
hHash = 0;

dwBlockLen = 1000-1000 % ENCRYPT_BLOCK_SIZE;
if(ENCRYPT_BLOCK_SIZE >1)
    dwBufferLen = dwBlockLen + ENCRYPT_BLOCK_SIZE;
else
    dwBufferLen = dwBlockLen;
do
{
    dwCount = fread(pbBuffer, 1, dwBlockLen, hSource);
    CryptEncrypt(hKey, 0, feof(hSource), 0, pbBuffer, &dwCount, dwBufferLen);
    fwrite(pbBuffer, 1, dwCount, hDestination);
}while(!feof(hSource));
```

그림 3. 암호화하는 부분

5. 블루투스 통신 구조

스마트 폰에서 먼저 주변의 블루투스장치를 검색한다. 그리고 홈 서버의 블루투스로 접속을 한다. 한번 검색한

뒤에는 특별한 설정 없이 홈 서버의 블루투스와 연결된다.
홈 서버의 블루투스는 포트를 하나를 사용하지만 스마트폰, PDA등은 기기의 특성 상 두 개의 포트를 각각 송신, 수신전용으로 사용한다. 스마트폰의 프로그램은 두 개의 포트를 열어 홈 서버와 통신한다. 블루투스 모듈과 도어 락 간의 통신은 RS-232c 직렬 통신 프로그램을 이용하였다[8][9].

6. 임베디드 락 컨트롤러 설계

임베디드 락 컨트롤러는 홈 서버에서 OK신호를 받아 도어를 오픈하는 역할만 한다. 락 컨트롤러 자체에서 복호화하여 여는 방법도 있겠으나 컨트롤러가 복잡해지고, 또한 홈 서버가 있으므로 굳이 락 자체에 검증 기능을 넣지 않았다. 블루투스 통신으로 TxD에서 신호를 받아 TR을 작동시켜 락의 모터를 구동시킨다. 시리얼 전송을 하는 블루투스에는 따로 전원이 들어가야 된다. 그림 4은 락 컨트롤러의 회로도이다.

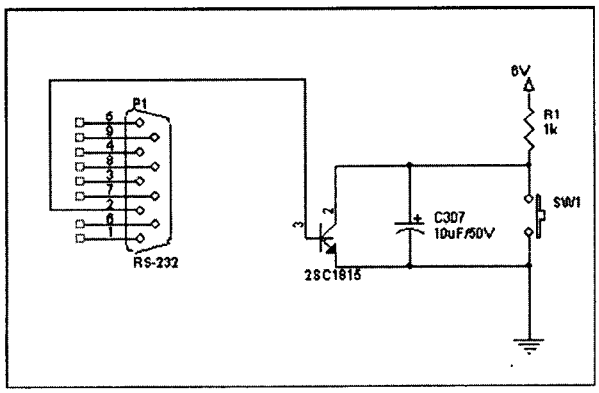

그림 4. 락 컨트롤러 회로도

7. 실험 및 결과

본 논문에서는 홈 오토메이션 기반의 보안 시스템을 제안한다. 현재 홈 오토메이션용 서버역할을 하는 장치가 판매되고 있다. 우리는 서버역할을 PC로 대체한다. 가정집에서 PC를 대부분 보유하고 있으므로 추가 비용이 들지 않는 장점이 있다. 서버에서 인증서를 암호화 하여 스마트 폰으로 전송을 한다. 이 방식은 서버의 인증서 생성과 복제를 이용해 가족들에게 부여하는 방식이기에 제한된 범위의 복제가 일어나고 복제 개수를 정확히 파악할 수 있다. 스마트 폰에서는 추가로 비밀 번호나 비밀 키를 입력하는 것이 아니라 인증서를 전송하는 것만으로 작동할 수 있도록 간편화를 도모했다. 서버는 받은 인증서를 복호화 하고 다시 원본과 검증을 하여 무결성을 확인한다. 원본 인증서의 크기가 클수록 비밀 번호가 길어질수록 약간의 Delay가 증가 되었고 블루투스 모듈에 따라 거리에 대한 특성을 보였다.
그림 5는 전체 시스템의 구현 상황을 나타낸다.

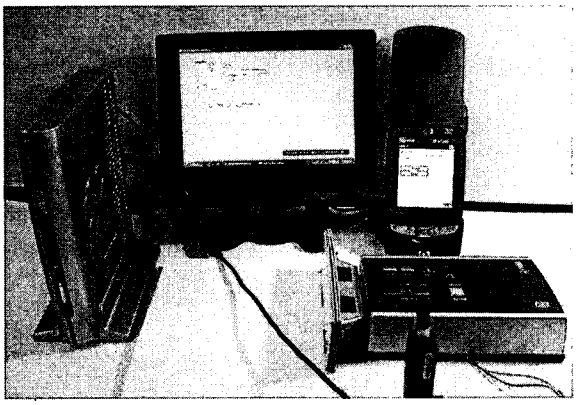

그림 5. 락 시스템 구현 화면

8. 결론 및 향후 연구

본 논문은 홈 오토메이션기반의 DES방식의 보안 시스템을 제안한다. 최근 웰빙의 영향으로 홈과 홈 오토메이션에 관심이 증가하고 있다. 여기에 사람들마다 많은 열쇠를 가지고 다니는 것을 편리하게 하고자 본 시스템을 제안한다. 제안된 시스템이 유비쿼터스 시대에 맞춰 사무실, 공장, 기타 등등의 건물에 적용된다면 사용자는 많은 열쇠 꾸러미 없이 휴대폰 하나만으로 모든 것을 해결할 수 있다. 본 시스템에서는 무선통신의 예로 블루투스를 이용하였지만 적외선 통신이나 무선랜 등 다양한 인터페이스를 활용할 수 있을 것이다. 또한 홈 서버의 홈 오토메이션 제어 능력을 이용하면 외부 침입에 대해 다양한 작업을 자동적으로 수행할 수 있을 것이다.

참고 문헌

[1] Chao-Lin Wa, "Mobile agent based integrated control architecture for home automation system", IROS 2004, 3668p~3673p vol4.
[2] Bergstrom, P., "Making home automation communications secure", Computer, 2001, 50p~56p
[3] H.X.Mel Doris Baker, "Cryptography Decrypted", Addison Wesley, 2000, 37p~40p
[4] Chakrabarti, S., "A remotely controlled Bluetooth enabled environment", CCNC 2004. First IEEE 5-8 Jan, 2004, 77p~ 81p
[5] Youquan Zheng, "Simplifications of the Bluetooth radio devices", 2002 IEEE 4th International Workshop, 2002, 107p~115p
[6] 김상형, "Windows API 정복", 가남사, 2002, 1154p~1169p
[7] MSDN Library, http://msdn.microsoft.com/
[8] Douglas Boling, "Microsoft Programming Windows CE.NET Third Edition", Microsoft, 2004
[9] 김재근, "C프로그래머를 위한 시리얼 커뮤니케이션", 인포북, 1995, 456p~542p