휴대폰을 통한 보안 시스템

박상균 김희동 김복기
LG전자 CDMA연구소, 한국외국어대학교 정보통신공학과, 광운대학교 전자공학부

Security System with Mobile Phone

Sang-Kyun Park Hee-Dong Kim
LG Electronics Inc. CDMA LAB Hankuk University of Foreign Studies

Abstract

이동통신 단말기의 지능이 높아짐에 따라, 통신망과 연동되는 휴대폰을 결재수단으로 사용하는 m-commerce와 같은 다양한 부가서비스가 가능하게 되었다.

본 논문에서는 단말기의 고기능화에 따른 응용부가서비스의 하나로, 휴대폰을 통해 통제되는 Security System을 제안하고 시스템의 구현 방법에 대해서 기술한다.

1 서론

이동통신 단말기의 지능이 높아짐에 따라, 통신망과 연동되는 휴대폰을 이용한 결재수단으로 사용하는 m-commerce와 같은 다양한 부가서비스가 가능하게 되었을 뿐 아니라, 단말기에 디지털 사진기 혹은 TV 수신기를 내장 시키는 등 휴대폰의 기능이 날로 다양화, 다기능화 되어가고 있다. 향후 이동단말기는 개인이 필수적으로 휴대하는 단말장치로서, 주민등록증과 같이 개인의 신분을 나타내는 역할과, 이와 연계하여 신용카드를 대신하는 m-commerce로 확대될 것이다. 이러한 동향은 단말기 제조업체, 망 운영 사업자, 제3의 서비스 제공 업체들이 서로 새로운 응용을 개발하면서, 영역을 확대 함으로서, 더욱 가속될 것으로 예견된다

본 논문에서는 단말기의 고기능화에 따른 응용부가서비스의 하나로, 휴대폰을 통해 통제되는 보안(Security) System을 제안한다. 종래의 Security 장치의 경우 각각의 열쇠를 가져야 하는 불편함이나, 카드나 비밀번호만 알고 있는 타인에 도용의 우려가 있다. 반면에 이동통신망에서는 단말과 망 사이에 특별한 보안시스템을 보유하고 있어서, 이 보안기능을 집, 사무실, 자동차 등의 일상생활의 보안시스템에 적용하는 방식이다. 휴대폰을 통한 Security System을 구현하기 위해서는, Security 장치에서 접속 가능한 휴대폰 및 비밀번호를 등록하는 단계; 휴대폰에서 Security 장치로 망을 통해 open 메시지를 전송하는 단계; 기존 망의 보안절차로 신분을 확인하는 단계: Security 장치에서 open 메시지 수신 후 접속가능 휴대폰번호 및 비밀번호를 확인하는 단계를 포함하여야 한다. 본 논문에서는 이러한 단계에 요구되는 구현방안을 제시하였다. 서론에 이어 2장에서는 이동통신망의 보안시스템에 대해서 개괄하고, 제3장에서는 제안 시스템의 구성에 대해서 기술한다. 제4장에서 시스템의 인증절차를 제시한 후 마지막으로 5장에서 결론 및 향후 응용방법을 설명한다.

2 이동통신망의 보안 절차

이동통신망에서 인증이라 함은 시스템의 HLR(Home Location Register) 및 AuC(Authentication Center)에 저장된 가

입자 정보와 단말기 정보가 일치하는가를 확인하는 절차이다. 이동통신망에 따라서 서로 다른 인증절차가 정의되어 있으나, 여기서는 국내에 사용되는 CDMA 이동통신망의 인증방식에 대해서 간단히 설명하도록 한다.

단말기가 최초 망 Access 시 단말기 고유 전자식별 번호인 ESN을 통한 인증(1차보안)을 거친다. 그러나 단말기가 일방적으로 가지고 있는 ESN은 단말기 복제로 인한 불법사용에 노출되어 있다. 이에 대한 보완으로 ESN을 망과 공유하고 또 다른 2차 비밀정보를 생성하여 호 시도,등록,착신 시에 검증(2차보안)하는 방법을 사용하고 있다. 인증은 반드시 시스템과 단말기가 동일한 인증키(SSD)를 가지고 수행하며, AuC에서 가입자 키 관리, 인증 알고리즘 동작 등의 인증 절차를 수행한다. 이 절차는 기존 음성호 처리와 별도로 수행되어 시스템의 부하문제를 고려하여, 가입자의 매 발-수신호마다 수행하거나 혹은 선택적(origination message 내 AUTH_MODE field setting)으로 수행할 수 있게 구현되어 있다.

A_Key는 단말기와 AuC에 동일한 값으로 저장된 primary key로서 인증절차에는 직접적으로 사용되지 않고, 실제 working 인증키(SSD)의 생성에만 사용된다. SSD(Shared Secret Data)는 단말기의 반영구적 메모리에 저장된 128 Bit 크기의 정보로 초기 가입 시 결정되는 A_Key(64Bit로 단말기의 영구보안 및 식별 메모리에 저장되며 HLR 및 AuC에서만 알 수 있슴)를 통해 생성된다.

SSD_A 64 Bit는 인증절차에 SSD_B 64 Bit는 음성보안 및 메시지 암호화에 사용된다. 기지국이 단말기로 호출채널을 통해서 전송한 최근의 Access Parameter Message 중 32Bit인 RAND(Random Challenge Memory)를 단말기가 보유하게 된다. Parameter 갱신명령이 Forward 통화채널을 통해 수신되었을 때 단말기에 의해서 갱신된다.

표1.SSD계산

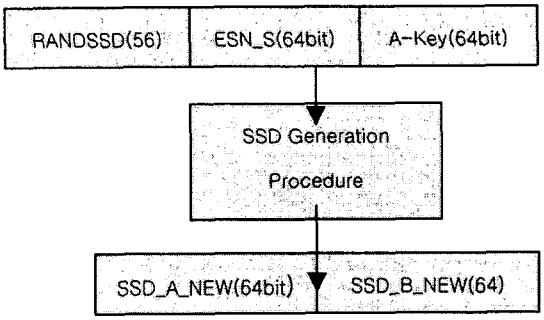
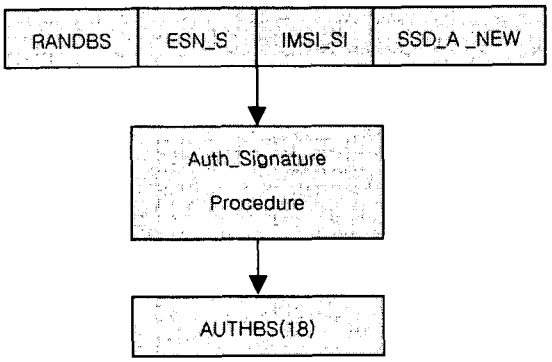


표2.AUTHBS 계산



3. 제안시스템의 구성본론

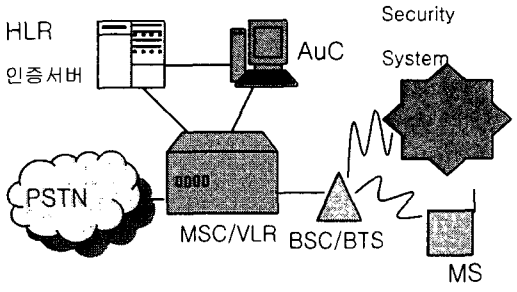


그림 1. 인증 서비스를 위한 시스템 구성도

3.1 시스템의 구성 및 서비스 시나리오

그림 1에는 인증서비스를 위한 시스템의 구성을 나타내었다. 보안시스템은 단말기와 같이 기지국을 통한 이동통신망 접근 방식을 갖는다. 각각에서 보낸 메시지는 기지국을 통해 BSC(Base Station Controller)를 거쳐서 MSC(Mobile Switching Center, 교환기)로 보내어진다. MSC에서 보안 메시지라는 것을 인식하고, 보안시스템에 필요한 기본 사용자 정보를 담고 있는 HLR 혹은 서비스 제공업체의 보안서버로 보낸다. 여기서 상호간의 Interface에 사용되는 Security Message는 기존 DBM(Data Burst Message)의 format(표1)으로 AUTH_MODE를 항상 1로 갖는 새로운 TID(Teleservice ID)를 추가한다.

표1. Access Channel에서의 DBM 구조

Fields	설명
MSG_TYPE	DBM표시 00000011
ACK_SEQ	Layer 2 Signaling 위한 field values
MSG_SEQ	
ACK_REG	
VALID_ACK	
ACK_TYPE	
MSID_TYPE	MO 단말기 Identification
MSID_LEN	
MSID	
AUTH_MODE	인증수행여부 등
AUTHR	
RANDC	인증관련 정보
COUNT	
MSG_NUMBER	Message 속성 필드
BURST_TYPE	
NUM_MSGS	
NUM_FIELDS	
CHARi	메시지 내용

DBM은 IS-2000에 정의되어 있는 메시지의 하나로 SMS 메시지를 전달하는 frame을 제공하는 것이다. 전송할 채널에 따른 필요 정보가 달라서, field 가 조금씩 차이가 난다. 이 새로운 TID를 갖은 Security Message는 단말기 혹은 보안시스템에 의해 송수신 되며 각각 기지국을 통해 이동망의 보안 절차를 거친다. 이 때 HLR 혹은 보안서버로부터 가져온 사용자 등록 정보와의 일치 여부를 AuC(Authentication Center)에서 확인 후 메시지를 전송한다.

3.1.1 보안시스템

보안시스템은 유선 혹은 무선으로 연결되어 있어야 하며, 직접 이동망을 통하는 무선시스템과, 전용라인을 통하는 유선시스템으로 구현할 수 있다. 무선시스템은 자동차 등에서 이동성을 효과를 가질 수 있고, 유선시스템은 집 혹은 오피스등에서 기 설치된 유선망을 이용함으로써의 비용절감을 장점으로 들 수 있다.

우선 접속 가능한 휴대폰 및 비밀번호 등록 기능을 갖는다. 더 높은 보안성이 필요한 경우에는 사용자의 요구에 따라 동시에 다수의 승인을 요구하는 설정 기능을 제안한다.

Open 혹은 Lock Message 수신 시 등록된 휴대폰과 비밀번호를 통한 인증 절차를 거친다. 다자간의 동시 승인 설정의 경우 마스터 휴대번호(혹은 등록된 다수의 휴대번호)로 요청된 open message에 대한 확인 인증 메시지를 발신한다. 부재중 방문객 도착 시 마스터에게 인증 받기 위한 절차로,

내장 카메라를 이용한 방문객의 사진을 전송을 통한 확인 기능을 제안한다.
GPS를 통해 등록된 휴대폰이 일정거리 이상 떨어질 때 자동 잠금 및 경고 메시지를 발신한다.

3.1.2 휴대폰

Security System과의 Interface를 위한 application 모듈이 추가된다. Security Message 발-수신시 사용자와의 Interface를 위한 구성이어야 한다. 단지 Software적인 부가서비스 기능 추가만으로, 현재 이용하고 있는 단말기의 변경 사항을 최소화한다. 상호간의 Interface시 Security Message는 기존 DBM(Data Burst Message) format의 새로운 TID(Teleservice ID)를 추가한다.

3.1.3 망(Home Location Register 및 Authentication Center)에서의 사용자 인증

기본적으로 위에 언급된 이동통신 보안 시스템을 이용한다. Security Message 전송시 인증에 필요한 Data가 HLR 혹은 보안서버에 등록된다. 사용자 인증 시 이 등록된 Data를 AuC으로 전송하여 인증절차를 걸친다. 휴대폰 혹은 Security System으로부터 Security TID 메시지 수신시, 위의 기 인증절차를 거치고, HLR 에서 가져온 Security Data와의 일치여부를 확인(3차보안)한 후 Security System으로 Message를 전송한다.

주기적으로 파악되는 사용자 위치정보를 보안시스템과 공유하여, 보안시스템이 사용자 위치에 따른 서비스(자동 잠금, 경고 메시지 전송 등)를 할 수 있도록 한다.

4. 결론

휴대폰을 통한 이동망 시스템에서의 보안절차를 이용한 Security System 에 대한 제안을 했다. 제안된 Security System은 현재 구현된 이동망 시스템에서 최소한의 변경으로 이루어진 것이다. 원거리에서의 제어능력, 설정에 따라 제어권을 가질 단말기 수의 무제한성, 공간적인 동시성이 없는 다자간의 동시 승인 기능, GPS를 통한 경고메시지 알림 기능 등을 고려할 때, 임의의 부가적인 부품(ex: IC)이나 IrDA (Infrared Data Association)를 이용한 Security 설계가 갖는 한계성(공간적인 제약, 동시성 등…)을 넘어 분명 좀 더 적극적이고 다양한 서비스를 제공할 수 있을 것으로 기대된다.

4 참고문헌

[1] IMT-2000 이동통신 원리 (저자 : 김현욱 외 3명, 진한도서)

[2] CDMA (저자: 옥윤철, 진한도서)