情報保護學會論文誌
第 21 卷 第 2 號, 2011. 4

스마트폰 위치정보에 대한 안전한 접근제어 시스템 개발*

장 원 준,† 이 형 우‡
한신대학교 컴퓨터공학부

Development of Secure Access Control System for Location Information on Smart Phone*

Won-jun Jang†, Hyung-Woo Lee‡
School of Computer Engineering, Hanshin University

요 약

스마트폰에서 제공되는 위치정보 서비스를 이용하면 사용자는 편리하고 다양한 고부가가치 응용 프로그램을 사용할 수 있다. 하지만 스마트폰을 통해 제공되는 개인의 위치정보 서비스는 오히려 프라이버시 침해 문제를 야기할 수 있다. 따라서 스마트폰 위치정보는 각 개인이 자신의 위치 정보에 대한 접근허가 대상자 등을 직접 제어/관리할 수 있어야 한다. 본 연구에서는 스마트폰에서 OTP 기반 인증 메커니즘을 적용하고 사용자 스스로 개인 위치정보를 접근 제어할 수 있는 프로토콜을 구현하였고 이를 통해 개인 위치정보를 보다 안전하게 관리할 수 있는 시스템을 개발하였다.

ABSTRACT

More convenient and value-added application services can be provided to user in case of using location-based service on Smart phone. However, privacy problem will be happen when an application disclosures the personal location information. Therefore, each user should securely control and manage his own personal location information by specifying access control list and profiles. In this study, we implemented personal location information self-control protocol and developed secure personal location management system with OTP based authentication procedure.

Keywords: Android, Access Control, Authentication, Location-based Service, Privacy

I. 서 론

스마트폰 사용자를 대상으로 다양한 종류의 어플리케이션이 개발 및 배포되고 있다[1,2,3]. 특히 Google에서 개발한 안드로이드 운영체제인 경우 오픈 소스 정책을 채택하였기 때문에 사용자가 직접 어플리케이션을 제작할 수 있으며 멀티태스킹 서비스를 지원함과 동시에 기존의 구글 서비스와 연계할 수 있다는 장점이 있다. 또한 안드로이드 운영체제에서 Layar, Wikitude, Sherpa 및 a2b 등과 같이 스마트폰 환경에서 개인위치정보를 이용한 어플리케이션이 개발되어 다양한 서비스를 제공하고 있다[4,5,6]. 현재 안드로이드 OS 환경에서 사용자 단말기의 GPS 모듈을 기반으로 사용자의 위치정보를 실시간으로 파악하며 공공안전 서비스, 위치추적 서비스, 교통안내 서비스, 정보제공 서비스 등이 제공되고 있다[7].

통신 사업자 또는 위치정보 서비스 사업자는 스마트폰으로부터 각 개인의 위치정보를 자유롭게 수집/획득할 수 있기 때문에 개인 위치정보에 대한 유출 시 프라이버시 문제가 발생한다는 문제점이 있다[4]. 스마트폰에 설치되는 각종 프로그램에 따라서 얼마든지 개

접수일(2011년 1월 20일), 수정일(2011년 3월 25일), 게재확정일(2011년 4월 11일)
* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2010-0016882)
† 주저자, jangwjfly@hanmail.net
‡ 교신저자, hwlee@hs.ac.kr

인 위치정보가 유출될 가능성이 있기 때문에 사회적으로 많은 문제점이 발생하게 될 것으로 예상된다. 따라서 본 연구에서는 안드로이드 OS 환경에서 개인위치정보 자기제어 시스템 설계를 통해 스마트폰 사용자 개인의 프라이버시를 보호하면서도 공공안전 서비스 등에 적용할 수 있도록 안전한 개인위치정보 관리 시스템을 개발하였다.

본 연구에서는 우선 안드로이드 OS 환경에서 이용가능한 GPS 기반 서비스에 대해 분석하였고, 각 서비스에서 이용하고 있는 위치정보에 대한 보안성을 강화하기 위해 우선 스마트폰에서 OTP(One-Time Password) 방식을 적용하다. 그리고 OTP 인증 과정과 함께 스마트폰 사용자가 자신의 위치정보를 안전하게 외부에 제공하고 또한 제 3자에 의해 안전하게 접속/검색 등을 할 수 있도록 위치정보에 대한 접근을 제어할 수 있는 프로토콜을 설계/구현하였다. 본 연구에서 개발한 인증 및 접근제어 기술을 직접 안드로이드 OS 환경에서 구현하였다.

II. 안드로이드 응용 SW[7]

2.1 위치정보 기반 서비스

위치정보 기반 서비스는 크게 2가지 형태로 나누어진다. 그 중 하나는 Multi-Layer System으로 대체적으로 각 사용자들 간에 위치 좌표를 맵 위에 씌우는 형태로 되어 있다. 또 다른 방식은 Search Based System이다. 이 방식은 사용자 좌표를 중심으로 범위 내의 맵 정보를 불러온 후 맵 정보 안에서 사용자가 원하는 정보를 검색하여 보여주는 방식이다.

현재 제공되고 있는 위치기반 서비스(Location Based Service : LBS)는 아래 표와 같이 주변정보 서비스, 안전 및 구난서비스, 물류/관제 서비스 및 위치확인 서비스 등 적용 분야가 상당히 다양하다.

〔표 1〕 위치정보 기반 서비스

분류		개념	제공대상
Information	주변정보서비스	개인의 현재 위치정보에 기반한 주변정보 (날씨, 생활정보 등) 검색서비스	개인
Entertainment	엔터테인먼트서비스	개인의 위치정보에 기반한 오락용서비스 (게임, 미팅 등)	개인
Safe & Security	안전 및 구난서비스	개인/기업의 안전 및 구조요청과 연관된 서비스	개인/기업
Tracking	물류 · 관제서비스	사람, 차량 및 물류의 위치정보를 추적하고 통제하는 기업용 서비스	기업
	위치확인서비스	타인 및 사물의 위치정보에 기반한 개인용 서비스	개인
Navigation	교통 · 항법서비스	운전자의 위치에 기반한 교통정보 및 길안내 서비스	개인/기업
Commerce	거래 · 광고서비스	개인의 위치정보와 상품 또는 광고 등의 서비스와 연계된 서비스	개인

〈자료 : KISA, 위치정보의 활용현황 조사분석, 2006〉

2.2 Multi-Layer System

Multi-Layer 시스템은 현재 자신의 위치 정보를 포함하여 등록된 사용자들 간에 그룹을 형성하여 서로의 위치정보를 확인할 수 있는 시스템으로 서로간의 위치정보가 지도에 표시되는 기능을 제공한다. 이 같은 시스템은 동일한 서비스를 제공하는 사용자들 간의 위치정보 확인 및 개별 성향에 따라 인연 만들기 등 다양한 형태의 커뮤니티 서비스로 제공되며 대체적으로 커뮤니티 기능을 제공하고 있는 만큼 메신저 서비스와 같이 사용되는 경우가 많다. Commandro[9]는 이와 같이 커뮤니티 기능을 제공하는 어플리케이션 중 하나로서 위치기반의 SNS 인스턴트 메시지 프로그램으로 실시간으로 사용자들 간의 위치와 활동을 표시하고 초대하거나 메시지를 보낼 수 있는 도구이다.

〔그림 1〕 Commendro SW(좌)와 오빠믿지(우)

최근 국내에서 이슈가 되었던 '오빠믿지' 어플리케이션의 경우도 앞에서 제시된 것과 마찬가지로 상대방의 위치를 실시간으로 파악할 수 있는 것은 물론 메신저 대화도 가능한 커뮤니티 형태의 어플리케이션이다.

2.3 Search Based System

사용자의 위치 정보를 중심으로 해당 범위의 지도를 불러온 후 사용자가 원하는 쿼리문에 따라 지도 내의 검색 정보를 불러오는 형태의 시스템이다. 일반적으로 사용자가 직접 쿼리를 입력하여 자신이 속한 범위 내 정보를 뿌려주는 형태로 되어 있으나 쿼리문을 고정적으로 두어 해당 어플리케이션 실행시 검색 결과를 바로 보여주는 형태의 어플리케이션도 있다. 이러

한 시스템은 주로 커뮤니티 기능 보다는 사용자 중심의 편의성을 띄고 있으나 대표적인 소셜 네트워크 서비스인 페이스북이나 트위터 등과 연동하여 해당 지역에 대한 리뷰 등을 업로드함으로써 커뮤니티 기능을 제공하는 어플리케이션도 있다. 이의 한 예로 Foursquare[11]는 근처를 검색하면 인근에 있는 각종 식당 및 공원 등 여러 장소의 정보를 한눈에 볼 수 있는 어플리케이션으로서 각 장소에 대한 간단한 방문 의견 등을 남길 수 있다.

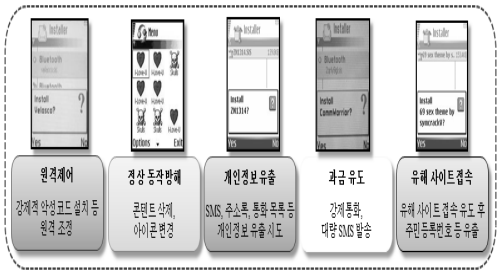
kr.Bus Manager는 고정적인 쿼리문을 통해 검색하는 프로그램 실행 시 원하는 정류장을 검색하는 어플리케이션이며 CallACab 또한 마찬가지로 사용자의 위치 주위에 빈 차로 운행하는 택시를 보여주며 Call Cab 버튼을 통해 현재 위치에 해당하는 정보를 택시에 전송하여 호출할 수 있다.

〔그림 2〕 Foursquare SW(좌), kr.Bus Manager SW (중앙). CallACab(우)

2.4 기존 어플리케이션의 취약성

안드로이드 기반 스마트폰의 점유율이 높아짐에 따라 금융정보/업무정보 유출 및 개인정보유출/프라이버시 침해 등의 공격이 빈번하게 일어나고 있다[5][10]. 스마트폰을 이용하여 개인 금융정보 또는 업무정보가 유출되는 등의 문제가 발생할 수 있을 뿐만아니라 원격제어, 동작방해, 과금유도 및 유해사이트 접속 등의 문제가 발생할 수 있다. 그 중에서도 가장 큰 보안 위협중 하나는 스마트폰내 개인정보에 대한 유출에 해당한다. SMS, 주소록, 통화 목록 등에 대한 개인정보가 유출될 수 있으며 최근에는 개인 위치정보 유출을 통해 악의적인 공격 등이 발생하고 있어서 사회적인 문제로 대두되고 있다.

위치정보를 통한 발생할 수 있는 개인정보 유출이나 프라이버시 침해 공격 형태는 다음과 같이 분류할 수 있다.



〔그림 3〕 안드로이드 보안 취약성

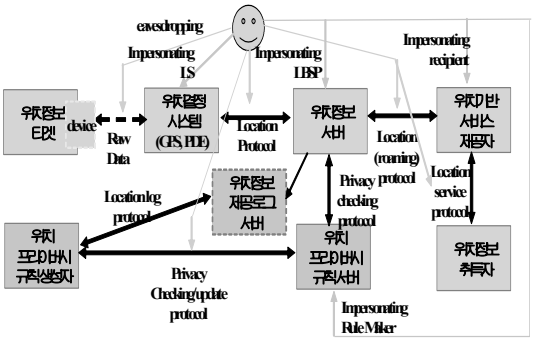
〔표 2〕 위치정보 시스템 공격 형태 및 목적

공격 형태	공격 목적
비인증 취득자	- 대상 위치정보 주체의 위치를 파악
인증된 취득자	- 허용된 위치정보 정확도보다 높은 정확도의 위치 획득 - 위치정보를 누출하거나 동의된 것 이상 축적하는 경우
Whoever	- 위치정보 주체의 위치정보가 배포되는 것을 막는 경우 - 위치정보를 수정하거나 파괴하고자 하는 경우 - 허용되지 않은 제 3자에게 redirect하고자 하는 경우 - 시스템 자체를 멈추게 하고자 하는 경우

위치정보 위·변조 공격 및 개인위치정보 노출 공격은 악의적인 사용자에 의한 상대방 사용자의 위치정보 위·변조 문제로 대두되고 있다. 이는 사용자 개개인의 위치가 24시간 실시간으로 노출될 수 있으며, 이동통신사에 의해 개인의 위치정보가 누출될 수 있음을 의미한다. 따라서 현재 스마트폰을 이용할 경우 다음과 같은 문제점 및 취약점이 존재한다〔그림 4 참조〕.

1) 개인위치정보에 대한 누출시 프라이버시 침해 위협 문제
2) 제 3자에 의한 불법적인 개인위치정보 검색으로 인한 문제
3) 위치정보에 대한 개인별 시간대 및 영역 설정 방식 부재로 인한 프라이버시 침해

위의 〔표 2〕에서 제시된 것처럼 대부분의 위치정보를 이용한 공격들은 위치결정시스템과 위치정보 타겟 디바이스간 전송 내용에 대한 접근 및 가로채기 등을 수행할 수 있다. 이러한 공격은 위치 프라이버시 규칙 서버에 전송되는 내용에 접근하여 도청 및 가로채기 혹은 변조 등의 공격을 수행하게 된다. 따라서 이에



〔그림 4〕 GPS 개인 위치정보 가로채기 위협

대한 대책으로 위치정보에 대한 접근제어 설정 및 관리 프로토콜이 개발되어야 하고 이를 이용한 안전한 시스템이 개발되어야 한다.

이를 위해서는 스마트폰에서 각 사용자는 자신의 위치정보를 제공할 수 있는 대상을 추가/삭제할 수 있어야 하며 또한 자신의 위치정보를 제공할 수 있는 시간대/위치/요일 등에 대한 정보 등을 설정할 수 있어야 한다. 따라서 본 연구에서는 다음과 같이 시스템 구조를 설계하고 이를 구현하였다.

III. 제안한 시스템 구조

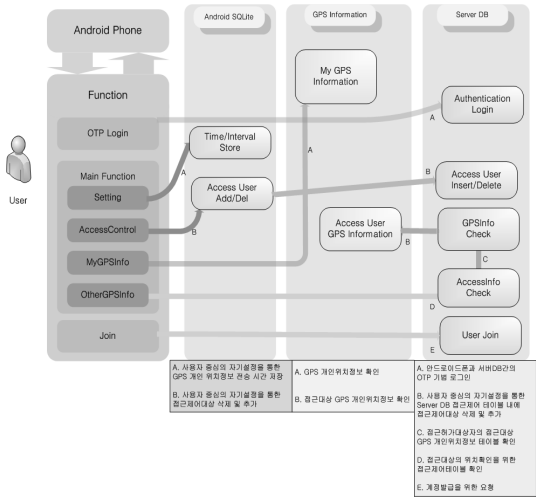
3.1 사용자 중심 개인위치정보 설정 구조

본 연구에서 설계한 시스템 구조는 다음과 같다. 〔그림 5〕 에서 보는 바와 같이 안드로이드 폰을 중심으로 각 사용자에 대한 프라이버시 프로파일(Privacy Profile) 설정/변경 및 갱신 방법을 구축하였으며, 안드로이드 기반 클라이언트-서버 시스템 구조를 이용하여 사용자는 클라이언트 스마트폰내 개인 위치정보에 대한 수집 허가 시간/장소/주기 등의 설정할 수 있도록 하였고, 또한 이를 서버로 전송하여 관리/검색할 수 있도록 설계하였다.

3.2 GPS 개인위치정보 접근제어 구조

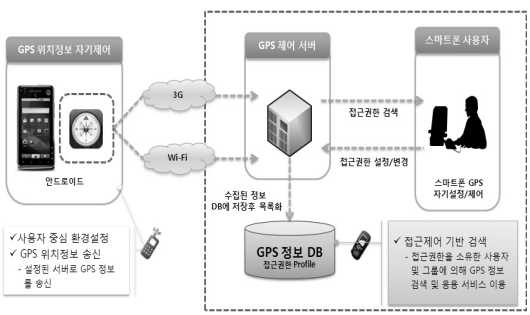
본 연구에서 개발한 시스템은 스마트폰 기반 개인위치정보 자기제어를 위해 위치정보 프라이버시 설정 프로토콜을 개발하였고 프라이버시 프로파일 구조를 기반으로 〔그림 6〕과 같이 위치정보 접근 제어 서버를 구축하여 사용자에 위치정보를 관리하도록 하였다.

개인 모바일 단말로부터 수집된 위치정보는 3G



〔그림 5〕 사용자 중심 시스템에서의 기능적 내부 구조

및 Wi-Fi망을 이용하여 위치정보 제어 서버로 전송되며, 서버는 수집된 정보를 DB에 저장하고 목록화한다. 또한 개인위치정보에 대해 제어 서버에 접근 권한을 설정한다. 위치정보 접근 허가 대상 설정은 사용자 위치정보 접근 허가 권한을 설정하고, 위치정보 접근 가능 그룹 설정은 사용자 위치정보에 대한 접근 가능 그룹을 설정하도록 하였다. 스마트폰 사용자는 자신의 스마트폰에서 접근 가능한 사용자에 대한 권한을 설정/변경할 수 있도록 하였으며, 개인 위치정보 제공 시간 및 기간, 요일 등에 대한 정보를 설정하여 이를 접근권한 프로파일(profile)로 생성토록 하였다. 그리고 설정된 접근제어 프로파일을 기반으로 본인 또는 접근권한을 소유한 제 3의 사용자에 의해 특정 사용자의 개인 위치정보를 안전하게 검색/확인할 수 있도록 하였다. 이와 같은 위치정보 접근제어 및 개인 위치정보 관리 시스템을 이용할 경우 공공보안 관리/범죄 예방 등 다양한 응용 프로그램에 적용할 수 있다.

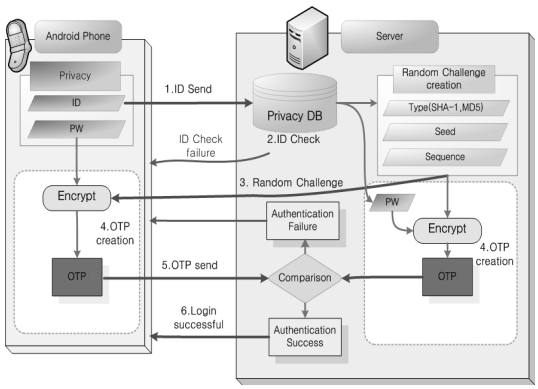


〔그림 6〕 위치정보 저장 및 접근권한 설정/변경

3.3 OTP 기반 스마트폰 인증 구조

스마트폰 환경에서 사용자 인증을 강화하기 위해 사용 가능한 OTP 방식은 다음과 같이 설계할 수 있다. 우선 사용자는 아래 그림과 같이 자신이 서버에 안전한 방식으로 ID/PW에 대한 등록 과정(Step1)을 수행하게 된다. 이제 등록한 ID/PW 중에서 ID만을 서버로 전송(Step 2)하게 된다. 이때 만일 전송된 ID가 서버에 등록이 되어 있지 않은 ID라면 인증불가 또는 접근불가 과정에 해당하게 된다.

만일 사전에 등록된 ID일 경우 서버는 Seed 값과 Sequence 값을 이용하여 임의 난수 도전값(Random Challenge)을 생성한 후에 이를 클라이언트로 전송(Step 3)하게 된다. 이제 클라이언트는 수신된 도전값과 패스워드 정보를 이용하여 OTP 값을 생성하고 이를 서버에 전송(Step 4)한다. 마지막 단계로 서버는 자신이 생성한 도전값과 패스워드를 이용하여 OTP 생성 한 후에 클라이언트로부터 전송 받은 OTP 값과 비교하여 사용자에 대한 인증/확인 과정을 종료(Step 5)하게 된다. 서버는 클라이언트로부터 수신된 OTP값과 자신이 생성한 OTP값을 비교하여 만일 OTP 값이 같으면, OTP 인증 및 로그인 성공에 해당하고, OTP 값이 다르면 OTP 인증 및 로그인 실패에 해당한다. 이와 같은 방식을 적용하여 스마트폰을 이용한 일회용 패스워드를 생성할 수 있다. 이와 같은 스마트폰 인증 구조를 통해 스마트폰에서 생성되는 개인 위치정보에 대한 보안성을 향상시킬 수 있으며, 네트워크 전송 과정에서의 인증 기능을 강화하며 보다 안전한 시스템을 구축할 수 있다. 다음의 〔그림 7〕은 스마트폰 기반의 OTP 기반 인증 구조이다.

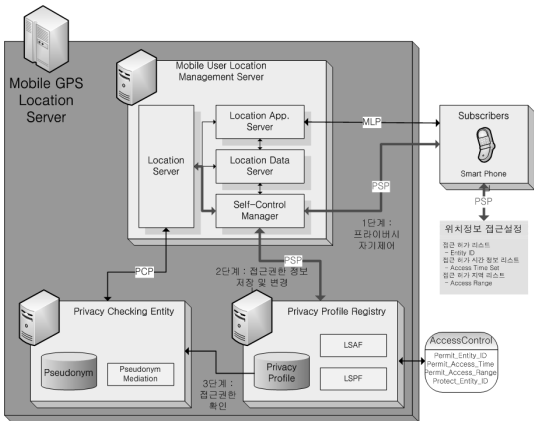


〔그림 7〕 OTP 기반 스마트폰 인증 구조

IV. 위치정보 접근제어 시스템

4.1 개인 위치정보 프라이버시 설정 프로토콜

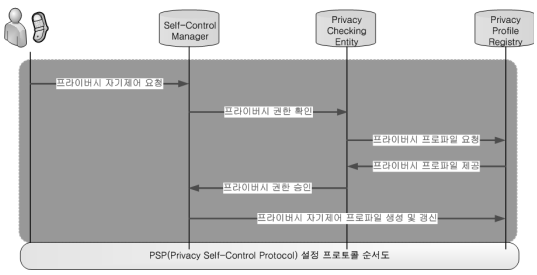
본 연구에서는 개인 모바일 단말로부터 수집된 위치정보에 대해 제안하는 프라이버시 자기제어 프로토콜(PSP : Privacy Self-control Protocol)을 이용하여 프라이버시 프로파일(Privacy Profile)을 생성/갱신하도록 하고, 접근권한을 부여받은 응용 서비스 사용자에게만 개인위치정보를 제공할 수 있도록 하여 프라이버시 보호 기능을 제공한다[7].



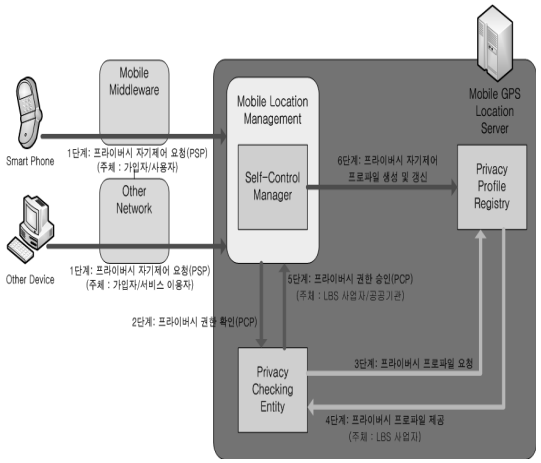
〔그림 8〕 위치정보 프라이버시 설정 프로토콜

4.2 프라이버시 설정 프로토콜

〔그림 9〕와 같이 프라이버시 자기제어 프로토콜을 이용하여 기존의 MLP(Mobile Location Protocol), PCP(Privacy Check Protocol) 프로토콜과 연동하여 사용자 개인이 자신의 위치정보에 대한 프라이버시 설정 기능을 제공하는 단계 및 작동방식을 설계 하였다. 또한 〔그림 10〕과 같이 프로토콜(MLS



〔그림 9〕 PSP 설정 프로토콜 순서도



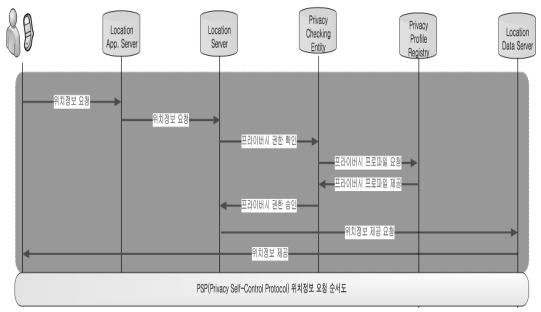
〔그림 10〕 위치정보 프라이버시 설정 프로토콜 작동 방식

PCP/PSP with HTTP)을 이용하여 위치정보에 대한 송수신 메시지 포맷 및 내용을 서버에 저장/설정하도록 하였다.

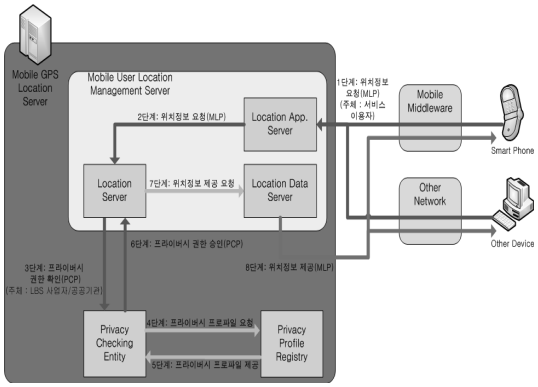
4.3 위치정보 프라이버시 설정 및 제공요청 프로토콜

〔그림 11〕과 같이 프라이버시 자기제어 프로토콜을 이용하여 Privacy Profile을 참조하여 접근권한 등에 대한 검증/확인 과정을 거쳐 접근권한을 획득한 후 응용 서비스 이용자에게 원하는 개인 사용자에 대한 위치정보를 제공하는 과정에 대해 설계하고 해당 프로토콜 구조는 〔그림 12〕와 같다. 스마트폰에서 위치정보 제어와 송수신 방법(PSP-HTTP) 및 메시지 포맷(XML 형태)을 설계하여 스마트폰 위치정보에 대한 접근제어 기능을 제공할 수 있었다.

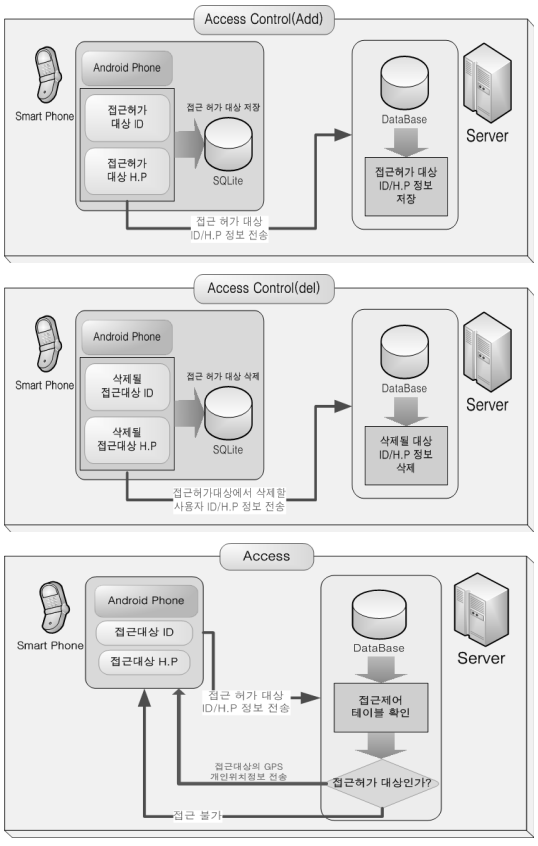
사용자는 자신이 접근하고자 하는 대상의 위치를 파악할 수 있다. 접근 대상의 위치를 확인하기 위해서는 접근하고자 하는 대상의 접근 허가 목록에 자신이



〔그림 11〕 PSP 위치정보 요청 순서도



〔그림 12〕 위치정보 프라이버시 설정 및 위치정보 제공 요청 프로토콜



〔그림 13〕 접근허가 대상 추가 및 삭제, 위치정보 확인 모듈

설정되어 있어야 한다.

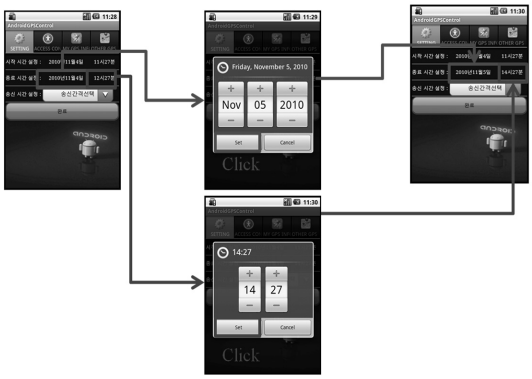
PSP 프로토콜을 기반으로 개인 위치정보에 대한 접근제어 profile을 설정하고 이를 변경/삭제 및 확인하는 과정은 다음의 〔그림 13〕와 같다. 안드로이드 OS 기반 스마트폰을 이용하여 사용자는 자신의 클라

이언트 디바이스에서 서버에 접속하여 (1단계) 자신의 위치정보를 접근할 수 있는 사용자를 추가할 수 있도록 하였다. 위치정보에 대해 접근을 허용할 경우 해당 사용자에 대한 휴대폰 번호, ID 등의 신상정보를 제공자가 직접 DB에 등록하도록 하였다. 또한 (2단계) 개인 위치정보에 대한 접근을 제한하거나 변경하고자 할 경우 마찬가지로 개인 위치정보 소유자가 직접 자신의 스마트폰을 통해 접근제어 프로파일에 대한 접근 및 변경 등의 과정을 수행하도록 하였다. 마지막으로 (3단계) 제 3의 사용자가 특정 사용자에 대한 위치 정보를 확인하고자 할 경우에는 DB에 접속하여 접근권한을 확인한 후에 만일 접근 권한이 부여된 경우에는 특정 사용자의 위치정보를 검색할 수 있도록 시스템을 개발하였다.

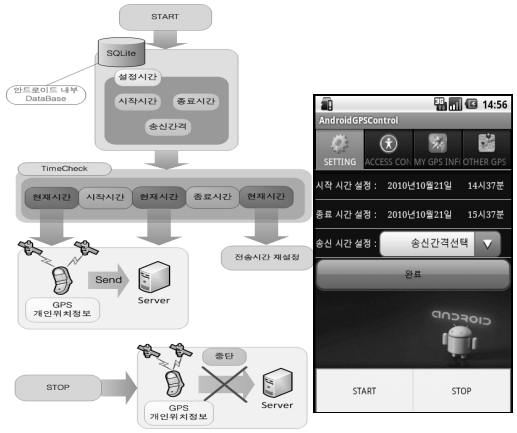
4.4 자기제어 시스템 모듈 개발

사용자는 설정에서 자신이 원하는 시간/요일/주기를 설정하여 개인위치정보를 서버로 전송한다. 시간/요일/주기의 설정 방법은 시작 시간 설정, 종료 시간 설정 및 송신 시간 설정으로 자기 설정이 이루어진다. 시작 시간과 종료 시간은 각각 년/월/일 과 시/분 설정으로 구성되어 있으며 자신이 원하는 시간을 설정하면 된다. 송신 시간 설정은 GPS 개인위치정보의 송신간격을 의미하며 사용자가 직접 설정할 수 있다. 자기 설정이 끝나고 완료 버튼을 누르면 자신이 설정한 시간과 송신간격이 SQLite 내에 저장이 된다. 다음의 〔그림 14〕은 자기제어 모듈을 구현한 결과이다.

시간에 대한 자기 설정이 끝나면 GPS 개인위치정보를 설정한 시간에 맞게 서버로 보내야 한다. 위치정보의 전송은 사용자가 메뉴를 선택하면 START 버튼과 STOP 버튼이 보여 지는데, START 버튼을 누르면 사전에 사용자가 설정한 시간/요일/주기에 따라 자신의 GPS 개인위치정보가 서버로 보내진다. 다음의 〔그림 15〕에서 이에 대한 내용을 도식화 하였다.



〔그림 14〕 자기설정 절차 GUI 및 GPS 개인 위치 정보 전송

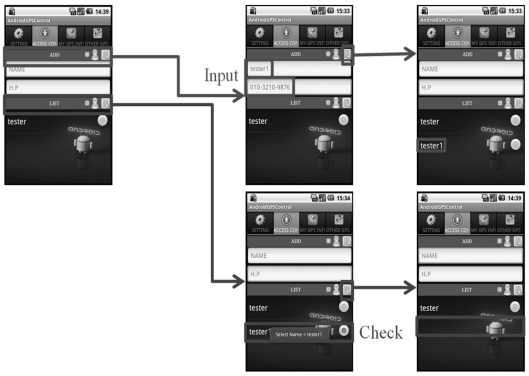


〔그림 15〕 GPS 개인위치정보 전송

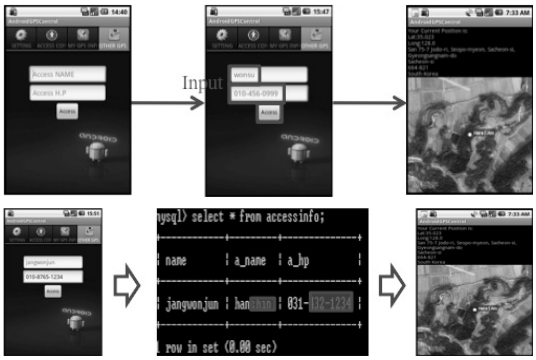
사용자가 설정한 시작 시간과 종료 시간은 현재 시간을 중심으로 첫 번째, 현재 시간이 시작 시간의 앞에 있는 경우. 두 번째, 현재 시간이 시작 시간과 종료 시간 사이에 있는 경우. 세 번째, 현재 시간이 종료시간 후에 있는 경우로 나뉠 수 있다. 첫 번째와 두 번째의 경우는 사용자의 올바른 설정으로 GPS 개인위치정보를 시간과 송신간격에 맞춰서 서버로 전송하게 된다. 그 후 사용자는 자신의 GPS 위치정보를 확인할 수 있는 대상에 대해 설정/삭제할 수 있다.

접근 허가 대상을 설정하는 방법은 대상의 이름과 핸드폰 번호를 등록함으로써 이루어진다. 사용자는 접근 허가 대상의 이름과 핸드폰 번호를 입력하고 추가 버튼을 누르면 입력된 정보가 SQLite에 자신의 ID, 대상의 이름, 대상의 핸드폰 번호 형태로 저장이 되며, 서버로는 보안성을 높이기 위하여 이름 정보 대신 ID정보를 전송한다. 접근 허가 대상은 LIST로 보여지며, 접근 허가 대상을 삭제할 경우에도 LIST에서 이름을 체크하고 삭제 버튼을 누르면 SQLite와 서버 DB(MySQL)의 접근 허가 테이블에서 해당 대상의 정보가 삭제된다. 다음의 〔그림 16〕은 접근 허가 대상 추가 및 삭제에 대한 구현 결과이다.

사용자는 자신이 접근하고자 하는 대상의 이름과 핸드폰 번호를 입력한다. 접근 허가 대상의 확인 방법은 첫 번째, 입력한 대상의 이름과 핸드폰 번호, 자신의 이름이 서버로 보내진다. 두 번째, 전송된 정보를 받은 서버는 서버 DB(MySQL)의 접근 허가 테이블



〔그림 16〕 접근 허가 대상 추가 및 삭제 구현 결과



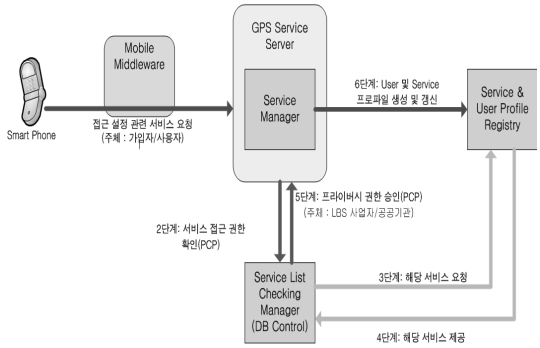
〔그림 17〕 접근하고자 하는 대상의 GPS 위치 정보 확인

을 검색한다. 접근 허가 테이블에 전송된 정보의 대상 이름이 전송한 사용자의 이름을 접근 허가 대상으로 설정 하였는지 확인한다. 접근 허가 대상으로 설정이 되어 있다면 대상에 대한 접근 허가가 확인된다.

다른 사용자의 위치를 확인하기 위해서는 접근하고자 하는 상대의 이름과 핸드폰 번호를 입력하면 정보가 자신의 이름과 같이 서버로 보내지고, 서버는 접근하고자 하는 대상이 자신을 접근 허가 대상으로 설정하였는지 확인한다. 확인 결과 설정되어 있으면 GPS 정보를 사용자에게 전송한다. 다음의 〔그림 17〕은 접근하고자 하는 대상의 GPS 개인위치정보 확인에 대한 구현 결과이다.

4.5 기존 시스템과 비교

기존 시스템은 〔그림 18〕과 같이 사용자 및 사용자 주변인들에 대해 각 사용자 위치정보를 확인시켜주는 시스템을 서버에서 관리를 하는 것은 물론 사용자의 임의대로 위치정보를 제어하기 보다는 정해진 형태의



〔그림 18〕 기존 위치정보 시스템

서비스로서 제공하는 경우가 일반적이다.

위 그림 에서 보이는 것과 같이 User A가 User B와의 위치정보를 확인하려 하였을 경우 각각의 GPS 정보는 DB Control 서버에 있는 서비스 데이터베이스와 User의 데이터베이스를 비교하여 정해진 형태의 서비스를 제공하는 형태로 되어 있다. 이 때 제공되는 서비스는 데이터베이스 내에 저장된 형태로 제공되는 것이기 때문에 서비스를 제공 받는 User A나 User B가 임의로 원하는 형태로 설정이 불가능하거나 서버에서 정해놓은 규칙에 따라 좁은 형태의 제어권만 허락받을 수 있었다.

그러나 이번 연구를 통해 개발된 시스템의 경우 사용자 자신을 포함한 위치정보에 대하여 서비스 형태에 따라 서버의 허락을 받아 제어권을 획득하는 것이 아니라 스스로 제어권을 지니고 있는 상태에서 접근해오든 다른 사용자들에 대해 확인 및 접근제어 설정을 하고 서버는 DB를 통해 설정한 내용을 저장함으로써 유지되는 형태로 되어있다. 서비스 제어권이 관리 서버에서 사용자에게 넘어가는 것은 물론 주 서버는 이에 대한 내용을 DB에 저장 및 접근해오는 다른 사용자들에 대해 실시간 모니터링 하는 역할을 하므로 서버의 권한이 대폭 축소된 반면 사용자의 권한이 대폭 향상되었으므로 기존 시스템에 비해 보다 손쉬운 자기 제어 및 모니터링을 통한 감시 작업과 이에 대한 설정을 통한 접근 제어가 가능하다.

V. 결 론

본 연구에서는 국내외 위치기반 서비스의 시장규모 및 현황 분석 등을 통하여 기존에 위치정보 기술 및 이에 대한 문제점에 대해 분석하였으며 이에 대한 해결방안으로서 침해 위험성이 높은 공격을 사전에 방지

하고자 기술적인 대응방안을 제시하였다. 먼저 발생할 수 있는 주요 문제점인 프라이버시 침해 위협 및 이동통신 사업자에 의해 무분별한 개인위치정보 검색/모니터링, 제 3자에 의한 불법적인 개인 위치정보 검색이나 위치정보에 대한 도청/가로채기, 불법 정보수집 공격 등이 가능하다는 취약점을 도출할 수 있었다.

따라서 본 연구에서는 안드로이드 환경에서의 위치정보 자기설정 방식을 설계하였고, 개인 위치정보 접근제어 서버 모듈을 구현 하였다. 또한 구현된 시스템에서의 안정성 향상을 위하여 OTP 모듈을 개발하여 안드로이드 환경에서 위치정보에 대한 인증 방식을 강화할 수 있었다. 수집된 위치정보에 대해 사용자 본인이 접근제어 기능을 설정하도록 하였으며, 수집된 위치정보에 대해 서버 저장 과정에서 접근권한을 설정할 수 있도록 하였다. 따라서 본 논문에서 개발된 기술에 대해 활용할 경우 공공 보안 및 범죄예방, 노약자 보호, 긴급출동 서비스 및 웹 연동 서비스, 알람 서비스 등 다양한 스마트폰 인증 및 접근제어 서비스에 적용될 수 있을 것이라 기대된다.

참고문헌

〔1〕 고석훈, "안드로이드 플랫폼 동향," 한국콘텐츠학회지, 8(2), pp. 45-49, 2010년 6월.

〔2〕 김상형, 안드로이드 프로그래밍 정복, 한빛미디어, pp. 804-842, 2010년 7월.

〔3〕 김평중, "안드로이드 플랫폼과 애플리케이션 프레임워크 기술," 한국정보처리학회지, 17(3), pp. 51-60, 2010년 5월.

〔4〕 셰인 콘더, 로런 다시, 시작하세요 안드로이드 프로그래밍: 모바일 소프트웨어 개발, 위키북스, pp. 54-138, 2009년 11월.

〔5〕 배준현, 구글 안드로이드 프로그래밍 : 애플리케이션 구조 분석, 마소인터렉티브, pp. 236-242, 2008년 1월.

〔6〕 곽범진, "실시간 버스 운행정보를 이용한 안드로이드 기반 모바일 애플리케이션 구현," 정보창의교육논문지, 4(2), pp. 15-21, 2010년 4월.

〔7〕 장원준, 이형우, "안드로이드 기반 GPS 개인위치정보 자기제어 구조 설계," 한국융합학회논문지, 1(1), pp. 23-29, 2011년 2월.

〔8〕 황선창, 美, 2008년 주요 IT 산업별 전망, KOTRA, 2008년 1월.

〔9〕 정승일, "안드로이드 플랫폼과 스마트폰 기술 발전 동향," 2010년도 대한전자공학회 하계학술대회발표집, pp. 2000-2001, 2010년 6월.

〔10〕 Reto Meier, Professional Android Application Development, JPUB, pp. 241-254, July. 2009.

〔11〕 Rick Rogers, Android Application Development, O'Reilly Media, May. 2009.

〈著者紹介〉

장 원 준 (Won-jun Jang) 학생회원
2010년 2월: 한신대학교 정보시스템공학과 졸업
2010년 2월~현재: 한신대학교 일반대학원 컴퓨터공학부 석사과정
〈관심분야〉 스마트폰 보안, 네트워크 보안, 정보보호

이 형 우 (Hyung-woo Lee) 종신회원
1994년 2월: 고려대학교 전산과학과 졸업
1996년 2월: 고려대학교 일반대학원 전산과학과 석사
1999년 2월: 고려대학교 일반대학원 전산과학과 박사
2003년 3월~현재: 한신대학교 컴퓨터공학부 교수
〈관심분야〉 네트워크 보안, 정보보호, 무선네트워크, SIP 보안, 디지털포렌식스