Smart Phone의 현재위치 GPS 역추적 애플리케이션 연구

표성배°, 김민기*, 박대우*
°인덕대학 소프트웨어과
*호서대학교 벤처전문대학원 IT응용기술학과
e-mail: baewhaoa@paran.com, mingi84@naver.com, prof1@paran.com

A Study on Smart Phone GPS Traceback Application of Current Location

Seong-Bae Pyo°, Min-gi Kim*, Dea-Woo Park*
°Dept. of, Computer Software, Induk University
*Dept. of IT Application Technology, Hoseo Graduate School of Venture

● 요 약 ●

Smart Phone의 사용이 증대되고, 서비스가 향상되면서, Smart Phone 사용자의 요구를 반영한 다양한 애플리케이션이 개발되고 있다. 또한, Smart Phone에 탑재되어 있는 GPS 모듈을 이용한 애플리케이션도 개발되고 있다. 본 논문에서는 Smart Phone의 국제 기기 식별번호(IMEI)를 이용하여, GPS 신호로부터 분석된 위도좌표, 경도좌표를 서버로 전송하고, 특정 Smart Phone의 현재 위치를 역추적 할 수 있는 Smart Phone 위치 역추적 애플리케이션을 연구 한다.

키워드: 스마트폰(Smart Phone), GPS, 역추적(Traceback), 애플리케이션(Application)

I. 서론

Smart Phone으로 e-mail, 메신저 등 정보전달과 정보교환뿐 아니라, 전자금융, 전자결제, 예약 등 업무에 까지 영역이 확대되고 있다.

그림 1과 같이, 2013년까지 전체 휴대폰의 약 45%를 Smart Phone이 차지할 것으로 예상하고 있다. 국내 통신사에서도 다양한 종류의 Smart Phone을 출시하고 있다. Smart Phone의 출시와 함께, 사용자들의 요구에 맞는, 다양한 형태의 애플리케이션 또한 개발되고 있다. 이중 GPS모듈과 관련된 애플리케이션은, Smart Phone의 휴대성과 맞물려, 증강현실 애플리케이션이나, 내비게이션 등의 형태로 개발되고 있다.

최근에 스마트폰 역추적[5][6]에 관한 연구가 있었으나, 애플리케이션으로 개발되어 상용화되는 것은 개인정보보호와 사생활보호에 관한 내용과 상관관계가 있어 기술개발과 사용화가 어려운 것으로 파악된다.

그림 1. 전 세계 Smart Phone 판매 추이[1]
Fig. 1. Smart Phone sales trends around the world

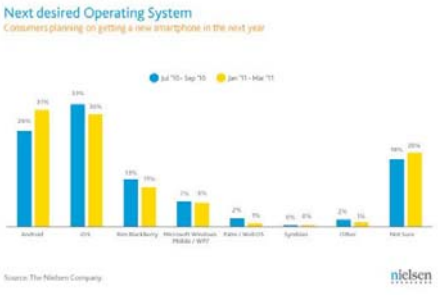

그림 2. Smart Phone O/S 선호도 조사[2]
Fig. 2. Smart Phone O / S preference survey

본 논문에서는, 그림 2의 Smart Phone O/S 선호도 조사에서 나온 것처럼, 상승세를 보이고 있는 안드로이드 O/S를 이용하여, Smart Phone의 GPS신호를 서버로 전송하고, Smart Phone의 국제 기기 식별번호(IMEI : International Mobile Equipment Identity)Code를 이용하여, 특정 Smart Phone의 현재 위치를 역추적 할 수 있는 애플리케이션 개발에 대하여 알아본다.

본 논문은 실험실환경에서 이루어진 Smart Phone과 애플리케이션 발전에 노력하려는 학문적인 여구차원에서 순수하게 연구되어 진 것임을 밝힌다.

II. 관련연구

2.1 IMEI Code

IMEI Code란, 전 지구적 이동 통신 시스템(GSM)을 사용하는 모든 이동 단말기가 서로를 고유하게 식별할 수 있도록, 이동 단말기에 할당된 식별번호이다. 이 번호는 형식승인Code, 최종조합 Code 및 일련번호를 포함하여 15자리로 구성된다. 이 Code는 USIM정보와 함께, 이용하여 복제폰을 만들거나, 각종 범죄에 악용될 여지가 있으나, USIM정보와는 다르게, 확인할 수 있는 방법이 매우 간단하며, 외부로 노출되어 있는 Code이다. 현재 국내의 경우, 이 Code를 개인정보로 보호하고 있어, 이를 무단으로 수집하거나, 이용하는 것에 대하여, Smart Phone 악성Code에 대한 기준이 확립되어 있지 않은 초기이기 때문에, IMEI 등의 단말정보 수집에 대한 기준이 모호한 상태이다. 하지만 USIM에 대부분의 개인정보가 암호화되어 저장되어 있기 때문에, 외부에서 쉽게 확인이 가능한 IMEI Code를 이용하는 것에 대해서는 제도적으로 정해져야 할 것이다.

2.2 화이트 리스트(White-List)

화이트리스트란, 입력검증의 두 가지 방법 중의 하나이다. 입력검증은 크게 화이트리스트, 블랙리스트 두 가지 방법이 있다.

첫째, 화이트리스트의 경우, 허용 가능한 입력값에 대한 리스트를 가지고, 해당 리스트에 입력된 값 이외에는 허용하지 않는 방법이다.

둘째, 블랙리스트의 경우, 허용되지 않는 입력값에 대한 리스트를 가지고, 모든 입력된 값에 대해서 허용하지만, 블랙리스트에 포함된 입력값만 허용하지 않는 방법이다.

이러한 두 가지 방법은, 어떠한 시스템에 적용되었느냐에 따라, 선택되어 사용되어지며, 화이트리스트는 아직까지 알려지지 않는 공격의 경우에 강한 장점이 있지만, 애플리케이션에 입력되는 다양한 데이터에 대하여, 많은 검증작업이 필요하다는 불편함이 있다.

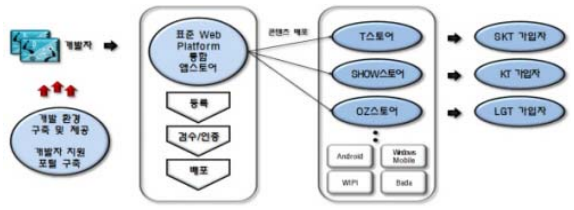

그림 3. 국내 통신망 서비스 순서
Fig. 3. Domestic Network Service Order

우리나라는 터키와 함께, 통신망에서 IMEI 화이트리스트 제도를 사용하는 유일한 국기이다. IMEI 블랙리스트 제도를 사용하는 대부분의 나라의 경우, IMEI Code를 체크하지만, 대부분의 사용자 정보는 USIM에 암호화되어 저장되어 있으며, 사용자는 USIM에 저장된 정보와 함께, 정식 승인된 IMEI Code를 가지고 있는 다양한 Smart Phone을 손쉽게 사용 가능하다. 국내에서는 그림 3과 같이 IMEI Code를 체크하여, 각 통신사에 등록되어 있는 IMEI Code를 가지고 있는 핸드폰에 대해서만, 서비스를 실시하고 있다.

2.3 Android SDK 2.2

2010년 5월 Android SDK 2.2 프로요 버전이 출시되며, 안드로이드 O/S점유율 또한 기존의 1.X버전에서 2.X버전으로 변화하고 있는 추세이다. 현재 국내에서 출시되는 모든 안드로이드폰은 2.1버전을 기준으로 출시되고 있다. 구글에서는 계속적으로 안드로이드 O/S 3.0 진저브레드를 발표하여, 개발용 SDK역시 지속적인 업그레이드를 하고 있다. 안드로이드에 대한 기본적인 시스템 구조[3]는 그림3과 같다.

그림 4. 안드로이드 시스템 구조
Fig. 4. Android System Architecture

III. Smart Phone에서 GPS 신호 역추적 시스템 설계

Smart Phone에서 GPS 신호 역추적 시스템 설계에 대한 순서도는 그림 5와 같다.

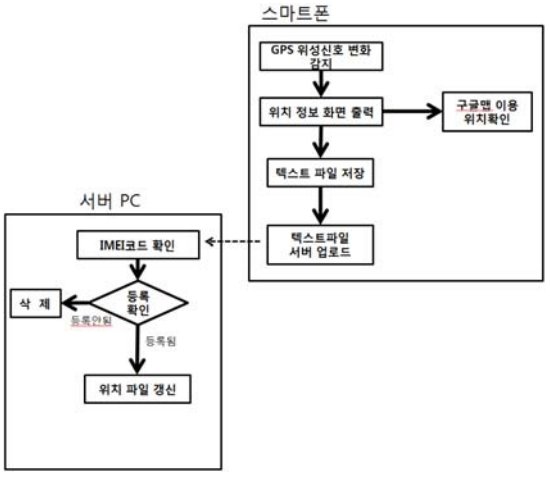

그림 5. GPS 신호 역추적 애플리케이션 설계
Fig. 5. GPS signal, traceback Application Design

Smart Phone에서 GPS 신호 역추적 애플리케이션을 구동하여, GPS 위성신호 변화를 감지한다[4]. 이때 Smart Phone의 IMEI Code와 함께, 현재 위치정보를 화면에 출력하며, Smart Phone에 내장되어 있는 구글맵 혹은 별도의 맵을 연동하여, 현재 위치를 지도에 표시한다. 또한, 내부적으로 현재 위치를 텍스트 파일에 저장하며, 이는 위치 데이터가 변동될 때 마다 자동적으로 현재 위치가 갱신되어 저장한다. 저장된 텍스트 파일을 소켓통신을 이용하여, 서버로 업로드하며, 업로드 할 때 서버에서는 현재 등록된 IMEI Code인지를 확인하고, 등록되어 있는 IMEI Code에 대해서, 현재 위치를 갱신한다. 서버 PC에는 항상 최근의 Smart Phone 위치정보가 저장되어 있기 때문에, 이를 이용하여 핸드폰의 위치를 역추적 할 수 있다. 하지만 GPS신호를 이용하기 때문에, GPS신호에 따른 오차가 발생하며, 건물 안에 있거나, 지하에 있을 경우는 정확한 위치를 알아낼 수 있는 방법이 없다.

IV. Smart Phone 역추적 애플리케이션 개발 및 테스트

실제 안드로이드 Smart Phone에 개발한 애플리케이션을 등록하고, 구동한 그림은 그림 6과 같다. 현재 위도와 경도가, 화면에 표시되며, Open Map버튼을 눌러, 현재 위치를 핸드폰에 내장되어 있는 맵을 이용하여, 확인할 수 있다. 안드로이드 O/S에서 현재 위치는 가상함수인 OnLocationChanged()함수를 이용하여, 받아오며, 이 함수는 현재 위치가 변동될 때마다 호출된다. 따라서 위의 함수를 재작성하면, 위치가 변동될 때마다 현재 위치값을 받아올 수 있다.

그림 6. 애플리케이션 구동화면
Fig. 6. Application driven screens

그림 6의 IMEI Code의 경우, 개인정보의 유출의 위험이 있기 때문에, 블록 처리하였으며, 이 장 이후의 화면에 대해서는 null값으로 표기하기로 한다.

표 1. 위치정보를 가지고 있는 LocationListener의 내부 메소드 구조[7]
Table 1. With the location information of the internal method nine trillion LocationListener

Methods	역할
public abstract void OnLocationChanged(Location location)	GPS위치값이 변화할 때 호출된다.
public abstract void OnProviderDisabled(String provider)	사용자에 의해 위치 provider가 비활성화 될 때 호출된다.
public abstract void OnProviderEnabled(String provider)	사용자에 의하 위치 provider가 활성화될 때 호출된다.
public abstract boid OnStatusChanged(String provider, int status, Bundle extras)	provider나, 현재 핸드폰의 상태가 변화될 때 호출된다.

표 1과 같이, OnLocationChanged이벤트에서 발생된 Location 변수의 getLatitude(), getLongitude () 함수를 이용하여, 위도와 경도값을 얻는다. 또한 이렇게 얻은 값을 텍스트파일로 저장하기 위하여, 그림 7과 같은 위치 로그 메시지 저장 함수를 생성한다.

```
public void LoggingLocationData(String strLocation)
{
    try{
        String strLocationFilePath = "LogLocation.txt";
        FileOutputStream fos = openFileOutput(strLocationFilePath, Context.MODE_APPEND);
        fos.write(strLocationFilePath.getBytes());
        fos.close();
    }
    catch(Exception e){;}
}
```

그림 7. 위치 데이터 저장 함수 구성
Fig. 7. Where the configuration data storage function

위치데이터는 FileOutputStream클래스를 이용하여, txt파일로 저장하며, 이때 파일의 저장위치는 Smart Phone 루트폴더의 data/data/files/min.GPS/LogLocation.txt의 위치에 저장되게 된다.

또한, 위치데이터가 변화함에 따라, Smart Phone의 IMEI Code를 얻어와, 함께 기록한다. 이때는 Android SDK 2.2버전에서 제공하는 TelephonyManager클래스를 이용하여, Smart Phone의 IMEI Code를 얻어오도록 한다. 이때 애플리케이션의 작동권한은 READ_PHONE_STATE권한을 부여하여, Smart Phone의 기기정보를 얻어오는 권한을 주도록 한다. TelephonyManager클래스의 경우, 현재 Smart Phone의 서비스타입, IMEICode, 활성화날짜, 서비스 국가, 서비스통신망, USIM상태, USIM의 소유정보 등의 Smart Phone에서 사용되는 정보를 얻어올 수 있다.

저장된, 위치정보를, 소켓통신을 이용하여, 서버로 전송하고, 서버에서는 전달받은 파일을 서버에 저장한다.

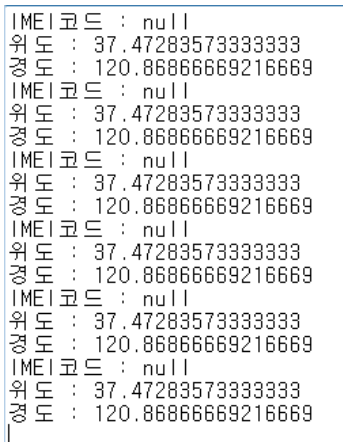

그림 8. 서버로 전송된 위치정보
Fig. 8. Location information is sent to the server

서버에는 각 IMEICode별 위도,경도가 기록으로 남으며, 본 논문에서 IMEICode는 개인정보 유출의 문제성이 검증되지 않았기 때문에, null로 표시한다. 이렇게 서버에 기록된 위치정보는, 구글 맵이나, 네이버 및 다음지도를 이용하여, 위치를 역추적 할 수 있고, 이와 더불어 IMEICode번호 식별을 통해, 다수개의 Smart Phone의 위치를 각각 역추적 할 수 있다.

V. 결론

Smart Phone 사용자가 급격히 늘어나고 있으며, 이에 따라 제조사들도, 다양한 Smart Phone을 개발 및 출시하고 있다. 또한 Smart Phone의 GPS모듈 사용의 편의성 때문에 GPS와 관련되어, 많은 애플리케이션이 나타나고 있는 실정이다. 하지만 GPS관련 애플리케이션의 경우, 애플리케이션 개발자가 임의로 사용자의 위치정보와, 기기정보를 가지고, 위치를 추적하는 기능의 경우에선 보안적인 측면과, 개인정보 보호의 측면으로는 매우 위험한 일이지만, 또 한편으로는 위치 역추적을 통하여, 실종자와 조난자 및 사회에서 필요한 위치 역추적 Smart Phone 등을 찾거나, 복제 Smart Phone을 밝혀내는 등의 편의성 또한 가져올 수 있다. 아직까지 IMEI Code를 악용한 사례가 발표되고 있지 않으며, 최근 많은 제조업체에서 IMEI Code는 공개정보라는 인식이 증가하고 있어, 이를 응용한다면, 사용자의 편의성을 제공하는 다양한 애플리케이션이 등장할 수 있을 것이다. 또한, 안드로이드 애플리케이션에 대한 보안기준 역시 제공되어야 할 것이다.

향후 연구로는, IMEI Code와 관련하여, 복제폰 역시 동일한 IMEI Code와 함께 위치정보가 다르게 입력되기 때문에, 서버에 기록되는 IMEI Code와 위치정보를 비교하여, 동시에 동 떨어진 위치에서 위치정보가 수집된다면, 복제폰의 존재 여부를 확인해주는 서버프로그램의 연구가 필요하다.

참고문헌

[1] “2011년 전세계 스마트폰 판매 4억 6000만매 예상,” http://news.sportsseoul.com/read/life/931541.htm, 2010. 4.

[2] 제갈병직, “스마트폰 시장과 모바일OS 동향,” Semiconductor Insight, pp9-18, 2010.

[3] Zhilong Yu, Mingjie Zheng, Xiaofeng Chen, “Google Android SDK development paradigm Encyclopedia[M],” Beijing:Posts & Telecom Press, 21-479쪽, 2009.

[4] Helena Leppakoski, Arto Perttula, “Indoor/Outdoor Seamless Positioning Technolohies Integrated on Smart Phone,” First International Conference on Advances in Satellite and Space Communications, 141-144쪽, 2009. 12.

[5] Heming Pang, Linying Jiang, Liu Yang, Kun Yue, “Research of Android Smart Phone Surveillance System,” International Conference On Computer Design And Applications, 374-376쪽, 2010.

[6] Yan Jin, Shanglang Yao, “Getting start with Google Android and Development[M],” Beijing: Posts & Telecom Press, 57-411쪽, 2009.

[7] “Android SDK 2.2 Development Doc,” http://developer.android.com/reference/android/location/LocationListener.html