PKI기반의 전자서명을 이용한 LBS 응용서비스에서의 보안 모델 연구

이진우*, 이민수*, 송오영*, 박세현*

*중앙대학교, 전자전기공학부

A Study of LBS Security Model in the Application Service using PKI based digital signature

Chin-U Lee*, Min-Soo Lee*, Oh-Young Song*, Se-Hyun Park*

*School of Electrical and Electronic Engineering, Chung-Ang University

요 약

위치기반 서비스(Location Based Service)는 이동통신망 또는 GPS 등을 기반으로 사람이나 사물의 위치를 정확하게 파악하고 이를 활용하여 다양한 응용이 가능한 서비스를 의미한다. 최근 위치기반 서비스는 이동통신 기지국이나 GPS를 통해 개인이나 차량 등의 위치를 파악하여 긴급구조, 교통정보, 재난관리 등을 서비스하는 신 산업 분야로서의 중요성이 증대됨에 따라 이에 대한 관심이 급증하고 있다. 그러나 이러한 산업 파급효과와 서비스 유형을 고려할 때, 공간정보의 활용과 위치기반서비스의 구현에서 핵심적인 역할을 하는 것이 위치정보인데 이러한 위치정보는 여타의 정보와 다른 특성을 가지게 된다. 즉, 위치정보는 개인정보보호 및 프라이버시(사생활)보호의 문제와 직결된다는 것이다. 특히 위치정보가 성명, 주민등록번호, 주소, 전화번호 등과 함께 직접적으로 사생활 침해의 문제를 강하게 발생시킬 수 있어 위치정보는 여타의 정보에 비하여 보다 강력한 보호를 필요로 한다. 본 논문에서는 LBS에 대한 전반적인 사항을 분석하여 문제점을 도출하고, LBS Privacy 문제점을 보호할 수 있는 방안을 제시한다. 최종적으로 제안된 모델은 차세대 LBS 시스템의 개인정보 및 Privacy 보호를 위한 기술적인 대안을 제시하였으며, 차세대 이동통신의 기반 기술이 될 것으로 기대한다.

I. 서론

이동성과 정보화가 강조되는 현대인들에게 무선 인터넷은 아주 유용하다. 그러나 무선 인터넷은 유선 인터넷과 달리 화면, 컨텐츠, 로밍(Roaming), 인증(Authentication) 등에 한계가 많아 확산 속도가 예상보다 느린 상황이다. 이에 따라 그 동안 무선 인터넷 서비스 가운데 사용자의 활용도를 제고시키고 기업들에게 높은 수익을 가져다줄 킬러 어플리케이션(Killer Application)이 과연 무엇일까라는 의문이 빈번하게 제기되어 왔다. 이에 대한 해답으로 최근 주목받고 있는 유망 기술이 바로 위치기반 서비스 LBS(Location-Based Service)이다.

LBS란 이동 통신 기지국과 위성 위치 확인 시스템(Global Positioning System)을 통해 개인이나 차량의 위치 정보를 파악하고 이를 기반으로 각종 첨단 서비스를 제공하는 것을 가리킨다. 사실 위성을 이용한 위치 추적 시스템인 GPS는 이미 국방, 교통, 물류 및 환경 분야에서 사용되면서 그 효용이 입증된 기술이다. [1] 그런데 이러한 위치정보를 활용하는 서비스로 LBS가 큰 기대를 모으고 있는 것은 위치정보가 이동통신망과 연결되면서 대중적이고 일반적인 서비스로 거듭날 수 있기 때문이다. 따라서 국내에서도 IT관련 업계와 정부 및 학계가 공동 참여한 LBS포럼이 발족되어 국제표준과 연계할 수 있는 국내표준제정의 기반이 마련되어 LBS가 국가 경쟁력 면에서도 핵심 산업으로 자리 매김 하게 되었다.

위치기반 서비스의 활성화를 위해서는 서비스의 순기능 홍보도 중요하지만 역기능의 조기 해소에

도 노력을 기울일 필요가 있다. LBS의 역기능 가운데 가장 자주 언급되는 부분이 바로 이용자 개개인의 위치가 24시간 실시간으로 노출된다는 것이다. 이러한 정보를 악용할 경우 개인의 사생활 노출로 인한 프라이버시 침해는 물론 범죄에도 악용될 소지가 많다. 그리고 네트워크의 해킹 문제가 이미 심각한 사회적 문제로 대두되고 있는 상황에서 개인의 위치정보가 인터넷에 유통되는 것을 철저히 막는다는 것은 쉬운 일이 아닐 것이다.

본 논문에서는 LBS에 대한 전반적인 사항을 분석하여 문제점을 도출하고, LBS Privacy 문제점을 보호할 수 있는 방안을 제시한다. 최종적으로 제안된 모델은 차세대 LBS 시스템의 개인정보 및 Privacy 보호를 위한 기술적인 대안을 제시하였으며, 차세대 이동통신의 기반 기술이 될 것으로 기대한다.

Ⅱ. LBS의 개요

LBS는 Location-Based Service의 약어로서 위치기반 서비스로 통칭되며 이동통신망을 기반으로 사람이나 사물의 위치를 정확하게 파악하고 이를 활용하는 응용시스템 및 서비스라고 일반적으로 정의된다.

3GPP(The 3rd Generation Partnership Project)는 LBS를 위치기반 서비스 제공이 가능한 네트워크를 이용한 표준화된 서비스로 정의하고 있으며, OGC(Open GIS Consortium)은 위치정보의 접속, 제공 또는 위치정보에 의해 작용하는 모든 응용소프트웨어 서비스라고 정의하고 있다. 또한 FCC(Federal Communication Commission)는 이동식 사용자가 그들의 지리학적 위치, 소재 또는 알려진 존재에 대해 서비스를 받도록 하는 것이라고 정의하고 있다. 세계 각 국가에서 LBS는 그 도입 및 검토가 각각 진행되어 왔는데 사회적 관점 등 배경이 다르기 때문에 그 목적도 국가별로 다르다. 세계의 이동통신 업자들은 GPS기반 LBS에 관심을 갖고 있으며 대표적으로 미국과 일본 그리고 한국에서 이 서비스가 채용되고 있다.

미국에서의 LBS는 주로 범죄방지나 인명구조 등 Security면에 중점을 두고 있으며, 유럽의 경우는 유통관리 시스템의 일환으로서 업무용 애플리케이션으로서 중점을 둔 LBS구축이 진행되고 있으며 GPS기반의 서비스 보다 기지국 중심의 Cell 방식을 취하고 있다. 일본에서는 주로 상업적인 목적을 위해 서비스 사업자가 중심이 되어 위치기반 서비스를 도입하고 있다. 국내의 위치기반 서비스는 추로 3개 이동통신사업자 중심의 서비스가 근간을 이루고 있으며, 위치기반서비스의 가치사슬을 형성하는 모든 업체들이 통신사업자의 공급전략에 따른 위치기반 서비스를 위한 기술 개발에 참여하고, 컨텐츠 및 서비스 제공자들은 통신망을 통한 서비스를 제공하고 있다. [2][3]

1. LBS 서비스 영역

LBS는 위치정보에 기반한 다양한 응용서비스를 제공하는 것이다. 여기에는 비상구조지원, 위치정보서비스, 교통혼잡 및 네비게이션(Navigation) 정보, 위치 밀착형 빌링 등이 포함된다. 이외에도 ITS 연계분야, 장애인을 위한 보조수단, 위치정보를 기반으로 한 L-Commerce, 휴대 전화기를 그대로 사용하는 Cell ID 기반의 친구 찾기 등 그 적용분야는 무한하다. 다음 표 1은 LBS 서비스 활용 분야의 예이다.

표 1 LBS 서비스 활용 분야

활용분야	기대 효과
어린이나 치매 노인의 위치추적	미아방지, 사고예방
애완동물 위치 추적	분실, 사고 예방
차량 네비게이션	차량의 이동 경로 파악
외근직원의 위치 파악	외근직원의 효과적 관리
현재 위치의 주변정보 제공	극장, 주유소, 식당, 백화점 등 주변 정보를 제공함으로서 고부가 서비스 제공
경찰/보안/군용차량 관리	범죄예방
택배/화물의 위치정보 제공	유류/교통비/통신비 절감

2. 위치기반 서비스 모델에서의 다양한 보안 취약점

위치기반 서비스가 이루어지기 위해서는 기본적으로 위치정보가 필요하다. 그런데 이러한 위치정보는 앞서도 간단히 언급한 바와 같이 개인의 프라이버시와 직접적으로 연관될 수밖에 없다. 즉 위치기반 서비스가 사용자들에게 많은 편리성을 제공하게 될 것은 자명하지만 그 이면에는 무분별한 위치 추적에 의한 프라이버시 침해 위협을 내재하고 있다. 그림 1은 위치기반 서비스의 일반적

인 모델에서 발생할 수 있는 보안 취약점을 나타낸 것이다.

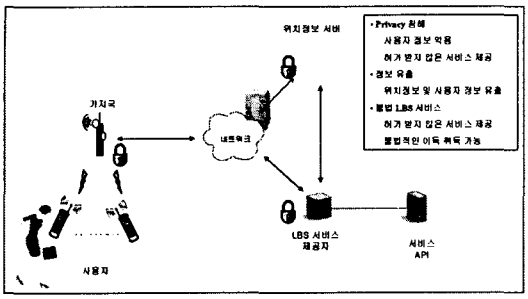

그림 1 위치기반 서비스에서의 다양한 보안 취약점

다음 3절에서 이러한 LBS 시스템의 발전 방향에 필요한 Mobile Terminal과 LBS SP간의 위치정보 송수신과 부인 방지를 위한 신뢰관계(Trust Relationship)를 보장하고, 개인정보 및 프라이버시를 보호할 수 있는 LBS Architecture 및 프로토콜을 제안한다.

3. LBS Privacy 문제 해결을 위한 모델 제안

기존의 LBS 시스템에서는 MT(Mobile Terminal) 와 LBS-SP(LBS Service Provider) 사이의 신뢰관계를 보증하기가 어려웠다. 따라서 본 논문에서는 W-PKI 보안 구조와 LBS 시스템을 결합하여 새로운 형태의 LBS 보안 모델을 제안한다. 그림 2는 제안하는 보안 구조를 보여주고 각 중요 구성요소는 다음과 같다.

BS(Base Station) : LBS 시스템의 위치정보를 전송하는 위치정보 시스템의 정보전달 링크 서비스를 제공하는 무선 기지국

DB(Data Base) : 한 번 인증 받은 MT 그리고 LBS SP의 인증서와 공개키를 저장한다.

CA(Certification Authority) : 인증서의 발행 및 폐기, 갱신 등을 수행하고 폐기에 따른 인증서 폐기 목록을 관리한다. CA 서버는 일관된 인증 정책을 적용해서 인증서를 발행한다. 또한 다른 공인 인증기관의 상호인증을 기반으로 인증서 패스를 설정할 수 있으므로 인증서 사용의 효율성을 극대화 할 수 있다. LBS SP(LBS Service Provider) : 다양한 위치기반 서비스를 제공하는 주체로 위치정보를 기반으로 하는 다양한 응용 서비스를 제공 및 LBS Platform의 기능과 연계를 통한 다양한 서비스를 제공한다.

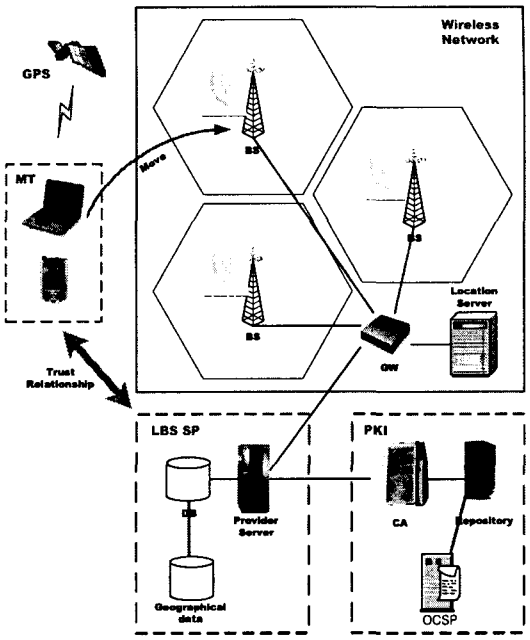

그림 2 제안 모델

4. 보안 프로토콜 제안

제안된 보안 모델에서 LBS-SP와 MT간 신뢰관계를 보장 할 수 있는 프로토콜을 제안한다. 다음 MT 와 LBS-SP 사이의 신뢰관계를 구축하기 위해 W-PKI 구조의 보안 프로토콜을 변형하여 적용하고 있다. 그림 3의 프로토콜과 같이 MT는 SP와의 상호 인증(Mutual Authentication)을 통해 메시지를 보낼 대상에 대한 인증을 수행하고, 보낸 정보에 대한 부인 방지를 통해 개인 위치정보 및 Privacy를 보호하게 된다.

기존의 LBS시스템에서는 MT가 ID와 인증서를 포함한 메시지를 LBS-SP로 전송하면 LBS-SP는 전송 받은 메시지를 검증하지 못하고 바로 MT는 자신의 위치정보를 LBS-SP로 전송하여 서비스를 시작하는 방식으로 개인정보 및 Privacy를 보호할 수가 없었다. 하지만 본 논문에서 제안한 프로토콜은 MT가 자신의 비밀키로 서명된 ID와 인증서를 포함한 메시지를 LBS-SP로 전송하면 LBS-SP는 인증서의 검증을 위해 W-PKI로 전송하여 전송된 메시지를 검증 받을 수 있게된다.

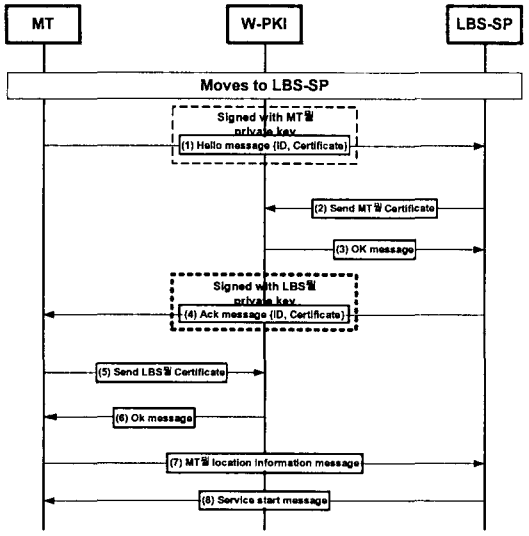

그림 3 안전한 서비스를 위한 보안 프로토콜

그리고 LBS-SP는 자신의 비밀키로 서명된 ID와 인증서를 포함한 메시지를 MT로 전송한다. MT는 전송받은 메시지를 검증하기 위해 전송받은 메시지를 W-PKI로 전송한다. W-PKI 서버는 전송 받은 메시지를 검증하고 그 결과를 MT로 전송한다.

인증서의 서명검증이 확인되면 MT는 자신의 위치정보를 LBS-SP로 전송하고, LBS-SP는 MT에게 적합한 응용 서비스를 시작한다. [4][5]

위에서 제안한 프로토콜은 MT가 LBS-SP를 인증할 수 있어 확실한 신뢰관계에 의한 위치정보 전달과 부인 방지로 개인정보 및 개인 Privacy를 보호할 수가 있게되어 사용자의 의도에 적합한 LBS 응용서비스를 안전하게 제공할 수 있다.

Ⅳ. 결론

본 논문에서 제안한 보안모델 및 프로토콜 도입의 기대효과로는 능동적인 시스템 참여를 통해 개인정보에 대한 중앙 집중적인 제어를 사용자 중심의 보안적인 정책으로 적용할 수 있게 되어, 사용자의 의도에 적합한 사용자 정보 보호 대책을 제공할 수 있다. 차세대 네트워크 환경에 사용될 위치정보 수집 시스템에 적합한 형태로 사용자 위치정보를 보고하는 MT와 그 MT가 보내주는 정보를 수집하고 가공하는 LBS-SP 사이의 보안을 보장할 수 있는 보안 구조와 프로토콜의 제안으로 차세대 LBS 시스템의 개인정보 및 Privacy 보호를 위한 기술적인 대안을 제시하여 차세대 이동통신망의 중요한 축으로 발전할 수 있을 것이다.

또한 지리/공간/위치정보기술의 발달 정도와 무선 통신의 수요를 짐작해 볼 때, 위치기반 서비스 시장의 확장은 명약관화(明若觀火)하다. 이러한 서비스를 제공함에 있어 위치정보에 대한 보호장치가 미흡하다면 사용자와 서비스 제공자의 신뢰를 잃게될 것이다. 따라서 본 논문에서는 위치정보 서비스의 다양한 value-chain의 신뢰성과 상호연동성을 보장할 수 있는 방안을 제시함으로써 LBS 산업이 모바일 서비스 산업의 성장을 위한 주요한 Killer-Application으로 급부상 할 것으로 기대된다.

참고문헌

[1] Giordano A, Chan M, Habal H, "A novel location-based service and architecture", Indoor and Mobile Radio Communications, 1995. PIMRC95. Sept. 1995

[2] Rui Jose, Adriano Moreira, Filipe Meneses, "An Open Architecture for Developing Mobile Location-Based Application over the Internet", Computers and Communications, 2001. Proceedings. July 2001.

[3] Soliman S, Agashe P, Fernandez I, Vayanos A, "gpsOne: a hybrid position location system", Spread Spectrum Techniques and Applications, Sept 2000

[4] Stojanovic D. H, Djordjevic-Kajan S. J, "Developing location-based services from a GIS perspective", Telecommunications in Modern Satellite, Cable and Broadcasting Service, Sept 2001

[5] Dorothy E. Denning, Peter F. MacDoran "Location-Based Authentication: Grounding Cyberspace for Better Security", Computer Fraud & Security, 1996