위치정보보호시스템의 설계 및 구현
Design and Implementation of Privacy Control System for Location Based Services

안경환*, 민경욱**, 김광수***, 김주완****
Kyounghwan An, Kyoungwook Min, Kwangsoo Kim, and Juwan Kim
* : 한국전자통신연구원 텔레매틱스·USN연구단 연구원, E-mail : mobileguru@etri.re.kr
** : 한국전자통신연구원 텔레매틱스·USN연구단 선임연구원, E-mail : kwmin92@etro.re.kr
*** : 한국전자통신연구원 텔레매틱스·USN연구단 선임연구원, E-mail : enoch@etri.re.kr
**** : 한국전자통신연구원 텔레매틱스·USN연구단 LBS 연구팀장, E-mail : juwan@etri.re.kr

요 약

최근 측위 장치와 모바일 단말 장치, 이동 통신 기술이 발달함에 따라 위치기반서비스에 대한 요구가 증가하고 있다. 그러나 위치기반서비스는 이용자에게 편리하고 유용한 정보를 제공하지만 개인의 프라이버시를 침해할 수 있는 가능성을 함께 가지고 있다. 특히 개인이 깨닫지 못하는 사이에 측위 장치가 탑재되어, 개인의 위치가 제3자에 의해 추적된다면 심각한 프라이버시 침해라 할 수 있다. 이러한 개인 위치정보를 보호하기 위해서는 법적인 규제와 기술적인 장치가 함께 마련되어야 한다. 이 논문에서는 위치정보를 보호하기 위한 위치정보보호시스템을 제시한다. 제시된 위치정보보호시스템은 법적인 규제와 표준 그리고 위치정보를 보호하기 위한 방법들이 설계 및 구현되어 있다.

1. 서 론

위치기반서비스(LBS: Location Based Services)는 사물이나 사람의 위치를 이용하여 다양한 부가 정보를 제공하는 서비스를 말한다. 위치기반서비스는 모바일 단말 장치, 이동 통신, 측위장치를 이용하여 이루어지는데, 이러한 장치들은 이미 널리 보급되어 있으므로, 미래에는 더 많은 위치기반서비스가 제공될 것이다. 위치기반서비스의 대표적인 예로는 가족이나 친구의 위치를 찾기 위한 친구찾기 서비스, 운전자에게 길을 안내하기 위한 네비게이션 서비스, 고객의 위치에 기반하여 쿠폰을 제공하거나 안심결제 등의 기능을 제공하는 위치기반 상거래 서비스, 긴급구조전화를 처리하기 위한 긴급구조 서비스 등이 있다.

앞서 예에서 보듯이, 위치기반서비스는 편리한 기능과 긴급구조와 같은 순기능을 가지고 있는 반면에 개인의 프라이버시를 침해할 수 있는 역기능 또한 가지고 있다. 일반적으로 위치기반서비스를 제공하기 위해서는 개인의 위치정보가 하나 또는 그 이상의 위치기반서비스사업자에게 알려져야 하고, 제3자에게 제공될 수도 있다. 또한 개인이 깨닫지 못하는 사이에 측위장치를 통해 추적당할 가능성이 있다. 만약 개인의 위치를 보호하기 위한 적절한 방법이 없다면, 원하지 않는 제3자에게 노출될 수 있다. 위치정보는 개인 프라이버시와 밀접한 연관이 있기 때문에 법적, 기술적 조치가 함께 고려되어야 한다.

최근에는 위치정보에 대한 법률이 미국, 유럽, 일본, 한국등지에서 점차 입법되고 있다[6]. 이러한 법률들은 긴급구조의 경우 사용자의 동의없이 위치정보를 수집할 수 있도록 하고, 그 이외의 모든 서비스는 사용자의 동의를 반드시 얻도록 하고 있다.

그러나 이러한 법적 규제들은 기술적인 뒷받침 없이는 개인의 사생활을 충분히 보호할 수 없다. 현재 3GPP (3rd Generation Partnership Project)와 OMA (Open Mobile Alliance)와 같은 표준 단체는 모바일 네트워크에서 위치기반서비스를

위한 표준 명세를 제정하고 있다. 이러한 표준화 단체들은 공통적으로 모바일 네트워크상에서 개인의 위치정보를 보호하기 위한 명세를 작업중에 있다.

이전의 프라이버시 제어(Privacy Control)에 관한 연구들은 익명성(Anonymity)과 프라이버시 정책(Privacy Policy)에 관한 기술 방법이 주를 이루었다 [1, 2, 3, 4, 5]. 그러나 이들 연구들은 프라이버시 보호를 위해 반드시 고려해야 하는 법적 규제와 표준을 동시에 고려하고 있지 못하다. 또한 이들은 위치정보에 대한 프라이버시 보호를 위해 반드시 필요한 (1) 자기정보통제와 (2) 위치정보제공에 대한 인지라는 두 가지 큰 원칙을 완전하게 보호해주지 못한다. 이 논문에서는 위치정보와 개인정보 사이의 차이점에 대해서 살펴본 뒤, LBS에서 프라이버시 제어를 위한 이슈들을 제시한다. 마지막으로 법적 규제와 표준을 동시에 만족하는 플랫폼을 제시한다.

이 논문은 다음과 같이 구성된다. 2장에서는 LBS에서 프라이버시 관련 이슈에 대해서 설명하고, 3장에서는 위치기반서비스를 제공하는 모든 단계에서의 프라이버시 제어에 관해 설명한다. 4장에서는 위치정보를 보호하기 위한 플랫폼의 구조를 제시하고, 5장에서는 결론을 맺고, 향후 연구에 대해서 설명한다.

2. 프라이버시 이슈

이 장에서는 프라이버시와 관련된 몇 가지 이슈들에 대해서 설명한다. 여기에서 제시된 이슈들은 LBS를 위한 위치정보보호시스템의 설계에 반영되어야 한다.

2.1 공공/상용 서비스에서 위치정보보호

위치정보와 관련된 법들은 대부분 공공의 목적과 상업적인 목적의 위치정보 이용을 구분하고 있다. 긴급구조의 경우 개인의 프라이버시 보다 긴급상황이 더 우선한다고 생각할 수 있으므로 동의를 얻지 않고도 위치를 획득할 수 있도록 한 반면 상업적 목적을 위해서는 동의를 필수로 하고 있다. 한 가지 고려해야 할 사항은 긴급구조가 아닌 공공의 목적을 위해서도 동의 없이 위치획득을 허락해야 하는가이다.

2.2 권한부여와 동의

프라이버시 보호에서 가장 중요한 것은 서비스에 대한 사전동의를 얻는 것이다. 동의를 얻을 때에는 서비스와 연관된 모든 주체들과 서비스에 대한 목적이 명시되어야 한다. 그리고 위치정보를 제공하기 전에 프라이버시 설정을 먼저 검사해보아야 한다.

2.3 위치정보보호대상

실제 위치기반서비스에서는 보호해야할 대상이 불분명할 때가 있다. 예를 들어 휴대전화를 이용한 위치기반서비스를 한다고 할 때 실사용자와 명의자가 다를 경우나 택배나 물류 서비스와 같이 물건의 소유주와 그것을 운반하는 사람이 다를 경우의 처리 문제를 들 수 있다. 전자의 경우 실사용자의 위치를 보호하는 것이 합당하다고 생각할 수 있으나 위치기반서비스제공자가 실사용자를 알지 못하는 경우가 다수 발생하고, 후자의 경우 물건의 소유권과 프라이버시가 충돌하는 경우로 볼 수 있다.

2.4 위치정보의 정확도

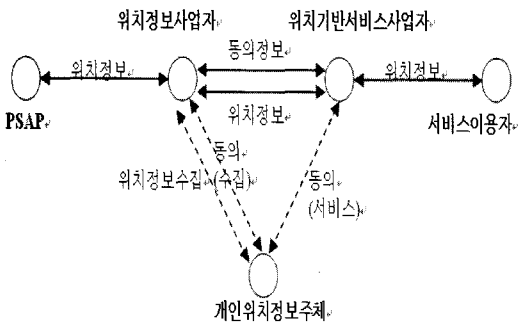
개인의 프라이버시 측면을 고려할 때, 반드시 높은 정확도가 좋은 서비스를 의미하는 것은 아니다. 이 경우 사용자의 프라이버시 설정에 따라 서비스를 제공하는 것이 가장 바람직하다고 할 수 있다. 즉 프라이버시 설정 부분에 QoS (Quality of Service) 부분을 포함하는 것이 필요하다.

3. 단계별 프라이버시 제어

위치기반서비스는 여러 단계로 이루어져 있어 각 단계들 사이에 위치정보가 노출될 가능성이 많다. 이 장에서는 위치기반서비스의 모든 단계에서 프라이버시를 제어하는 방법에 대해 설명한다.

3.1 위치기반서비스에서 주체들 간 관계

이 절에서는 먼저 위치기반서비스에 참여하는 주체들과 그들의 관계에 대해서 알아본다. 그림1은 우리나라의 법률인 "위치정보의보호및이용등에관한법률"에서 정의하고 있는 주체들과 그 들의 관계이다.



<그림 1> 주체들 간의 관계

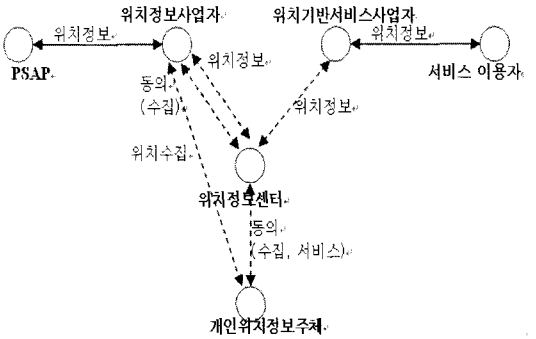
- ***개인위치정보주체:*** 위치를 수집하는 대상이 되는 주체를 말한다.
- ***위치정보사업자:*** 개인위치정보주체에 대해 위치정보를 수집하고 이를 위치기반서비스사업자에게 제공하는 주체를 말한다. 위치정보사업자의 예로는 이동통신사업자와 GPS등 단말기를 이용해 위치정보를 수집하는 사업자가 있다.
- ***위치기반서비스사업자:*** 위치정보사업자로부터 위치정보를 제공받아 서비스 이용자에게 위치기반서비스를 제공하는 주체를 말한다. 예를 들어 컨텐츠 제공자가 이 분류에 속한다. 일반적으로 이동통신사업자는 위치정보사업자와 위치기반서비스사업자를 겸하는 경우가 많다.
- ***서비스 이용자:*** 위치기반서비스를 제공받는 주체를 말한다.
- ***PSAP(Public Safety Access Point):*** 긴급구조호출을 받아 긴급구조서비스를 행하는 주체를 말한다.

아래는 "친구찾기"와 같은 일반적인 위치기반서비스에서 각 주체들 간의 관계에 대해서 설명한다.

- 서비스 이용자는 위치기반서비스사업자에게 개인위치정보주체의 ID를 이용하여 서비스를 요청한다.
- 위치기반서비스사업자는 개인위치정보주체로부터 서비스에 대한 동의를 먼저 획득한 뒤, 만약 동의할 경우 위치정보사업자에게 위치정보를 요청한다.
- 위치정보사업자는 위치기반서비스사업자로부터 동의 정보를 확인하고나 위치정보 수집에 대한 동의를 개인위치정보주체로부터 획득한다. 동의를 획득한 경우 위치정보사업자는 위치를 수집하여 위치기반서비스사업자에게 제공한다.
- 위치기반서비스사업자는 위치정보와 부가정보를 결합하여 서비스를 제공한다.

PSAP의 경우는 정부에 의해서 운영되며, 긴급구조호출시에 사용자의 동의없이도 위치정보를 수집할 수 있다.

그림1은 위치기반서비스를 위한 가장 기본적인 모델로 몇 가지 문제점을 가지고 있다. 첫째, 동의 정보를 관리하기가 힘들다. 동의 정보의 경우 위치기반서비스사업자와 위치정보사업자 모두에게 필요한데 동의정보의 관리주체가 누가 될 것 인가하는 문제가 있다. 만약 위치정보사업자가 위치기반서비스사업자를 신뢰하지 않는다면, 위치정보사업자는 매번 동의 정보를 다시 개인위치정보주체에게 확인해야 한다. 개인위치정보주체의 입장에서는 동의를 다시 하는 것은 서비스를 이용하는 데 장애물이 될 수 있다. 두 번째로 개인위치정보주체는 프라이버시 설정을 관리하기가 힘들다. 개인위치정보주체의 경우 많은 사업자들이 존재할 수 있기 때문에 어떤 위치정보사업자와 위치기반서비스사업자가 자신의 위치를 수집하고 이용하는지를 관리하기 어렵다.



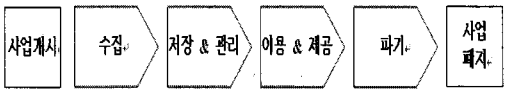
<그림 2> 새로운 주체들 간의 관계

그림2는 새로운 주체인 위치정보센터가 포함된 모델을 보여주고 있다. 이 모델에서 모든 위치정보와 동의 정보는 신뢰받는 기관(정부기관 또는 신뢰받는 회사)인 위치정보센터에 의해 관리되어지고 제공되어 진다. 이 경우 모든 주체들은 동의정보(프라이버시 설정을 포함)와 위치정보를 신뢰할 수 있고 쉽게 관리할 수 있다. 이 논문에서는

위치정보 센터에 설치되어 사용될 수 있는 위치정보보호 플랫폼을 제시한다.

3.2 프라이버시 제어

이 절에서는 위치기반서비스에서 단계별로 고려해야할 사항에 대해서 설명한다. 프라이버시 제어에서 가장 중요한 것은 자기정보통제권의 확보와 개인위치정보 제공에 대한 인지라고 할 수 있다[4]. 만약 어떤 사람이 상황을 알고 자신이 조절할 수 있다고 느낀다면, 위치기반서비스에서 프라이버시는 더 이상 문제가 되지 않을 것이다. 아래 단계에서는 위의 두가지 원칙이 고려되며, 모든 단계에서 중간에 가로채기를 방지하기 위해서 자동화된 동작이 필요하다. 그림3은 위치기반서비스의 모든 단계들을 보여주고 있다.



<그림 3> 위치기반서비스의 단계

- ***사업개시:*** 사업을 개시하기 위해서는 위치정보사업자는 허가를 위치기반서비스사업자는 신고를 해야 한다. 이렇게 진입장벽을 둠으로써 위치정보의 오남용을 방지할 수 있다.
- ***수집:*** 누구든지 위치정보를 수집하기 위해서는 개인위치정보주체의 동의를 얻어야 한다. 만약 측위장치가 장착되어 있을 경우 그것을 가지거나 운반하는 사람에게 반드시 그 사실을 알려야 한다. 개인 위치정보주체는 자신의 개인위치정보에 대한 통제권을 가져야 하며, 동의 정보를 조회하고, 변경할 수 있어야 한다. 법에서 정하는 중요한 내용 중의 하나는 수집에 대한 사실확인자료(로그)를 기록해야 한다는 것이다. 이 로그에는 수집시간, 요청자, 목적, 개인위치정보주체등 위치정보를 제외한 필드들이 존재해야 한다. 이 사실확인자료는 개인위치정보주체가 추후에 조회가능해야 한다.
- ***저장 & 관리:*** 만약 위치기반서비스의 종류에 따라 위치정보가 저장될 필요가 있다면 위치정보를 보호하기 위한 기술적, 관리적 조치가 필요하다. 기술적 조치로는 방화벽설치나 암호화 소프트웨어의 설치를 들 수 있으며, 관리적 조치로는 위치정보보호조직의 구성 및 운영을 들 수 있다. 또한 서비스 목적이 달성된 후에는 반드시 파기되어야 한다.
- ***이용 & 제공:*** 위치기반서비스사업자는 개인위치정보주체와 서비스 이용자와의 계약 범위를 벗어나서 위치정보를 이용해서는 안된다. 위치정보의 이용에 대한 개인위치정보주체의 인지를 돕기 위해서 이용 및 제공사실이 개인위치정보주체에게 즉시 통보되어야 한다. 통보의 방법으로는 SMS, 이메일등 개인위치정보주체가 쉽게 사실을 확인할 수 있는 방법을 이용하는 것이 필요하다. 위치기반서비스사업자 또한 서비스 제공사실확인자료를 기록하여야 한다. 나중에 프라이버시 설정 위반여부를 확인하기 위해서 사실확인자료에는 시간, 요청자, 목적등이 기록되어야 한다. 위치정보는 안전하고 신뢰성 있는 방법으로 전송되어야하며 중간에 없어지거나 손상되어서는 안된다. 이를 위해 HTTPS와 같은 프로토콜이 쓰여질 수도 있다.
- ***파기:*** 위치정보는 서비스 목적이 달성되었거나 이용자가 동의를 철회한 경우 반드시 파기되어야 한다.
- ***사업폐지:*** 만약 위치정보사업자 또는 위치기반서비스사업자가 사업을 폐지하고자 하는 경우 그 사실을 미리 이용자와 개인위치정보주체에게 통보해야 하며, 위치정보 및 사실확인 자료를 모두 파기해야 한다.

4. 위치정보보호시스템

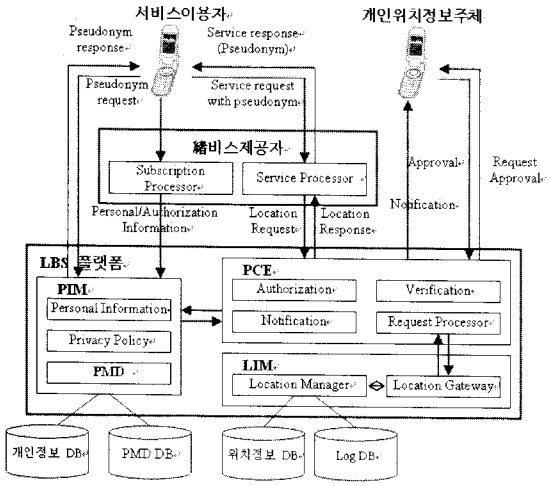
이 장에서는 프라이버시 제어를 위해 법적 규제와 표준을 준수하는 플랫폼을 제시한다. 그리고 제시된 플랫폼을 이용하는 시나리오에 대해 설명한다.

4.1 플랫폼 구조

이 절에서는 프라이버시 제어를 위한 플랫폼 구조에 대해서 설명한다.

- ***PIM***(Personal Information Management)***:*** 이용자가 서비스에 가입할 때, 개인 정보와 위치정보를 다루는 정책을 관리하는 모듈이다. 정책의 내용에 관해서는 이절의 마지막에서 설명된다. PMD (Pseudonym Mediation Device)는 pseudonym을 생성하고 관리하며, pseudonym과 verinym간의 변환을 담당하는 모듈이다. Pseudonym은 개인위치정보주체의

실제 ID를 숨기기위한 가상의 ID를 의미하며, verinym은 MSISDN, SIP URL, IMSI와 같은 실제 ID를 의미한다.



<그림 4> 위치정보보호 플랫폼 구조

- *PCE*(Privacy Control Entity): 위치정보가 요청될 때 verification 모듈은 개인위치정보주체가 설정한 프라이버시 정책을 검사한다. 만약 프라이버시 정책이 측위를 허용하는 것이면 request processor가 LIM으로부터 위치를 획득하게 된다. 만약 정책에서 통보를 원할 경우 notification 모듈은 메시지를 개인위치정보주체로 전송한다.
- *LIM*(Location Information Management): 만약 위치정보가 요청되면, location gateway는 자신의 측위 알고리즘을 이용하여 위치를 획득한다. 위치정보를 전달한 뒤에는 4.2절에서 언급한 로그를 기록하게 된다. 위치정보는 나중에 사용되기 위해서 위치정보 DB에 저장될 수 있다.

앞서 언급한 정책은 가입자 프로파일에 저장된다. 가입자 프로파일은 3GPP의 표준 명세에 잘 나타나있다[7]. 프로파일은 프라이버시 예외리스트, 프라이버시 설정등을 포함하고 있다. 개인위치정보주체는 이용자가 프라이버시 예외리스트에 포함되어 있을 경우에는 위치가 수집될 수 있다. 개인위치정보주체는 다음 설정중에 하나를 선택할 수 있다: (i) 측위 허락 불가, (ii) 통보하지 않고 측위 허락, (iii) 통보하고 측위 허락, (iv) 통보하고 측위를 허락할 것인지를 문의.

4.2 위치정보보호 플랫폼 이용 시나리오

먼저 서비스 이용자가 위치기반서비스에 가입하는 시나리오에 대해서 설명한다. 과금뿐만 아니라 프라이버시 제어를 위해서도 가입절차가 반드시 필요하다.

- 서비스 이용자는 개인정보를 입력하고, 가입페이지에서 프라이버시 정책을 설정한다. (Subscription Processor)
- 서비스제공자는 입력된 정보를 PIM에 등록한다.
- 만약 서비스 이용자가 pseudonym을 사용하기를 원한다면, PMD는 pseudonym을 생성해서 서비스 이용자에게 제공한다. (PMD)
- 등록을 한 뒤에 서비스 이용자는 언제나 등록된 정보를 조회하거나 수정, 삭제할 수 있다. (PIM)

두 번째로, 서비스 이용자가 위치정보를 요청하는 시나리오를 설명한다.

- 이용자가 개인위치정보주체에 대한 pseudonym을 요청한다.
- PMD는 pseudonym이 존재하지 않을 경우 생성하여 전달한다.
- 이용자는 pseudonym을 이용하여 서비스 제공자에게 서비스를 요청한다.
- 서비스 제공자는 플랫폼의 PCE에게 요청을 전달한다.
- PCE의 인증모듈은 이용자가 해당 서비스에 가입하였는가를 체크한다.
- Verification 모듈은 프라이버시 정책을 검사한다. 만약 개인위치정보주체가 자신의 위치를 수집하는 것을 원하지 않을 경우 즉시 에러를 리턴하고, 만약 개인위치정보주체가 서비스에 가입되어 있지 않다면 가입할 것을 요청하는 메시지를 전송한다.
- 서비스가 허락되면 request processor는 LIM에게 개인위치정보주체의 위치를 요청한다.
- LIM은 위치를 수집하고 log DB에 기록한다.
- 획득된 위치정보는 서비스 제공자에게 pseudonym과 함께 전송된다. 프라이버시 설정에 따라 통보 메시지가 전송될 수도 있다. 서비스 제공자는 위치정보와 연관된 부가정보를 이용자에게 제공한다.

5. 결 론

이 논문에서는 위치기반서비스에서 프라이버시와 관련된 이슈들을 살펴보고, 모든 단계에서의 프라이버시에 대해서 살펴보았다. 개인위치정보는 개인정보와는 다르기 때문에 새로운 보호 방법이 필요하다. 이 논문에서는 법적 규제와 표준을 모두 준수하는 플랫폼을 설계하고 구현하였다. 향후 연구로는 프라이버시 정책을 기술하기 위해서 W3C에서 표준화된 P3P포맷을 위치정보에 맞게 수정, 적용하고, 시스템에 반영하는 것이다.

참 고 문 헌

1. C. Hauser, and M. Kabatnik, "Towards Privacy Support in a Global Location Service," Proceedings of the IFIP Workshop on IP and ATM Traffic Management (WATM/EUNICE 2001), pp. 81-89, 2001.
2. E. Snekkenes, "Concepts for Personal Location Privacy Policies," In Proceedings of the 3rd ACM conference on Electronic Commerce, pp. 48-57, 2001.
3. B. Schilit, J. Hong, and M. Gruteser, "Wireless Location Privacy Protection," IEEE Computer, pp. 135 - 137, 2003.
4. T. Rodden, A. Friday, H. Muller, and A.Dix, "A Lightweigth Approach to Managing Privacy in Location-Based Services," Technical Report Equator-02-058, University of Nottingham and Lancaster University and University of Bristol 2002.
5. C. A. Gunter, M. J. May, and S. G. Stubblebine, "A Formal Privacy System and its Application to Location Based Services," In Privacy Enhancing Technologies (PET), 2004.
6. L. Ackerman, J. Kempf, and T. Miki, "Wireless Location Privacy: A Report on Law and Policy in the United States, the Europrean Union, and Japan," DoCoMo USA Labs Technical Report DCL-TR2003-001, 2003.
7. 3rd Generation Partnership Project (3GPP), http://www.3gpp.org/
8. Location Interoperability Forum ,http://www.openmobilealliance.org/lif/
9. W3C Platform for Privacy Preferences (P3P) Project, http://www.w3.org/P3P/