위치정보 프라이버시 S/W 프로토콜의 설계

박장유*, 이응재**, 남광우*
*군산대학교 컴퓨터정보공학과
**한국인터넷진흥원
e-mail:*{parkstar, kwnam}@kunsan.ac.kr, **ejlee@nida.or.kr

Design of a Protocol for Location Privacy S/W

Jang-Yoo Park*, Eung Jae Lee**, Kwang Woo Nam*
*Department of Computer Information Engineering, Kunsan National University
**National Internet Development Agency of Korea

요 약

이 논문은 위치정보 프라이버시 S/W를 위한 프로토콜을 제안하고 있다. 위치정보 프라이버시 보호 방안을 포괄적으로 조사 및 분석하여 향후 유비쿼터스 위치기반서비스에서의 위치정보 보호 방안을 개발하고, 위치정보 보호를 위한 기본 구성요소와 아키텍쳐를 설계하였다. 또한 이를 기반으로 개인 위치정보를 개인이 직접 제어할 수 있는 자기 제어 S/W 프로토콜과 프로토타입을 제안한다.

1. 서 론

위치정보는 위치정보업자가 설치 및 보급한 위치인식 장치에 의해서 획득된 특별한 개인정보로서 성명이나 주민등록번호와 같이 이용자가 직접 입력한 일반적인 개인정보와 차별성을 갖는다. 위치정보는 이동통신단말을 이용함으로써 시시각각으로 그 내용이 바뀌는 동적인 정보라는 특성을 갖는다. 바로 이러한 특성으로 인해 이동통신사업자들은 특정 지역 내에 존재하는 사물이나 이용자의 위치를 파악하고 변경된 위치정보를 실시간으로 획득하여 서비스를 제공할 수 있는 것이다. 하지만 위치정보는 이동통신사업자의 의지에 따라 얼마든지 누출 될 수 있다는 큰 위험성을 수반한다.

위치정보가 누출될 시에 개인의 위치 추적이 가능하여 위험인물로부터의 표적이 될 수 있으며, 위치정보의 오류·왜곡을 유발하여 생명과 재산에도 큰 피해를 안겨 줄 수 있다. 따라서 이러한 위치정보는 개인의 사생활 보호와, 더 나아가 이용자 전체에 대한 심각한 피해를 막기 위해서 보다 안전하게 다루어져야 한다.

또한 개인위치정보의 보호와는 별도로 이용자의 긴급구조를 위한 공공의 활용도를 높일 필요가 있으며 물류나 보험, 경호, 관광정보, 교통 등 산업 전반에 걸친 활용도를 높여 다양한 응용서비스의 제공이 가능해질 수 있을 것으로 판단된다.

이 논문은 위치정보 프라이버시 보호 방안을 포괄적으로 조사 및 분석하여 향후 유비쿼토스 위치기반서비스에서의 위치정보 보호 방안을 개발하고, 위치정보 보호를 위한 기본 구성요소와 아키텍처를 설계하며, 이를 기반으로 개인 위치정보를 직접 제어할 수 있는 자기 제어 S/W 프로토타입을 제안한다.

†본 연구는 국토해양부 첨단도시기술개발사업 - 지능형국토정보기술혁신사업과제의 연구비 지원(07국토정보C05)에 의해 수행되었습니다.

2. 위치정보 프라이버시 프로토콜 요소

2.1 위치정보 자기제어를 위한 예외 리스트

위치정보 프라이버시 예외 리스트의 기본 구성 요소는 다음과 같이 위치정보사업자 관련 사항, 위치기반서비스사업자 관련 사항, 위치정보 취득자 관련 사항, 위치정보 프라이버시 제한 사항 등으로 구성된다.

<operator, lbsp, client, restrictions>

이 네가지 주요 구성 요소는 위치정보주체의 프라이버시 보호를 위하여 다음과 같이 운용될 수 있다.

위치정보사업자 : 위치정보사업자 관련 사항의 주요 요소는 위치정보사업자의 식별자, 위치정보사업자의 위치정보 수집 시스템의 식별자이다. 위치정보사업자의 식별자는 위치정보사업자를 식별하는 것으로 예외 리스트가 위치정보사업자별로 관리 될 경우에는 생략될 수 있다. 위치정보사업자의 위치정보 수집 시스템의 식별자는 위치정보사업자가 다양한 위치정보 수집을 동시에 제공할 경우 특정 수집 장치 또는 방법을 식별하기 위하여 사용된다. 예를 들면, 휴대폰 사업자의 경우 A-GPS와 같이 일반적인 위치정보 수집을 하는 것과 동시에 모바일 RFID 등과 같은 방법으로 위치정보 수집을 할 수 있다. 그러므로 각 수집 방식에 대한 식별자를 사용하여 구분할 필요성이 있다.

위치기반서비스사업자 : 위치기반서비스사업자 관련 사항의 주요 요소는 위치기반서비스사업자 식별자와 위치기반서비스사업자 클래스, 위치기반서비스 식별자와 위치기반서비스 클래스이다. 위치기반서비스사업자 식별자는 위

치정보주체가 서비스를 제공하도록 허용한 위치기반서비스 사업자를 구분하기 위한 식별자이며, 위치기반서비스 식별자는 위치기반서비스사업자가 제공하는 위치기반서비스 중에서 각 위치기반서비스를 구분하기 위한 식별자이다. 위치정보주체는 위치기반서비스사업자의 식별자와 위치기반서비스식별자를 통하여 위치기반서비스에 대한 프라이버시 제한을 하게 된다. 위치정보사업자가 사업자당 할당하거나 정부 또는 중앙 인증기관에 의해 할당된 식별자를 사용하여 위치정보주체가 좀 더 안전하게 위치기반서비스를 선택할 수 있도록 할 수 있다.

2.2 위치정보 프라이버시 보호 액션

2.2.1 위치정보 보호 액션

위치정보 주체는 위치정보사업자 또는 위치기반서비스사업자가 서비스를 위해 위치정보를 수집할 경우 각 서비스 또는 서비스의 타입에 따라 위치정보 수집에 대한 보호 액션을 설정할 수 있어야 한다.

3GPP의 위치정보 서비스 표준과 OMA의 PCP 표준에서는 위치정보 보호 액션에 대하여 가장 높은 수준의 위치정보 수집 거부부터 가장 낮은 보호 수준의 통지없이 위치정보 수집 허용까지 5단계로 구분하였다. 국내의 경우 위치정보법은 법상에서 '매회 통지'를 의무화 해놓았으며 매회 통지를 포함하여 최소 6단계로 구성될 필요가 있다.

위치정보 프라이버시 보호 액션은 위치정보 수집 거부(position not allowed), 위치정보 수집 통지 후 허용시 수집(notify position if granted), 위치정보 수집 통지 후 무 응답시 수집(notify position if no response), 통지 후 수집(notify position), 수집 후 통지(position notify), 통지 없이 수집(position without notify) 등으로 구성되어야 한다.

2.2.2 위치정보 수집 또는 통지 시기

위치정보 수집 통지 후 허용시 수집, 위치정보 수집 통지 후 무 응답시 수집, 매회 통지, 통지 후 수집, 제공시 통지 등의 프라이버시 액션은 위치정보 주체에 대한 통지에 기반하고 있다. 통지는 서비스의 타입에 따라 편의를 위해 다양한 통지 주기를 갖도록 설정할 필요가 있다. 친구찾기 서비스의 예를 들면 제 3자가 위치정보 주체의 위치정보를 수집하는 매회에 통지하도록 할 수도 있다. 이때 매회 통지되는 위치정보 수집에 대하여 허용 또는 거부를 하는 것은 위치정보 주체에게 상당히 번거로운 일이다. 그러므로 특정 시간 주기 또는 특정 수집 횟수 마다 통지토록 함으로서 위치정보 주체의 서비스 편의를 확장할 수 있다.

2.3 위치정보 정확도 기반 프라이버시 설정

위치 정확도는 위치정보의 품질을 구성하는 가장 중요한 요소이면서, 동시에 위치정보 주체의 위치정보가 누출 또는 침해 되었을 경우 오용될 수 있는 정보의 품질을 의미한다. 그러므로 위치정보 주체는 각 서비스 또는 제공받는 제 3자의 신뢰성과 필요 정확도에 따라 제공되는 위치정보의 정확도 수준을 조절하여 제공할 수 있도록 할 필요가 있다.

위치 정확도 기반 프라이버시 설정 클래스는 좌표 정확도 클래스, 등급화된 정확도 클래스, 주소 기반 클래스, 가상 위치 클래스 등으로 구분될 수 있다.

2.4 프라이버시 보호 시간 및 공간 설정

2.4.1 시간 기반 프라이버시 보호 설정

시간 프라이버시 보호 설정은 위치정보 주체가 특정 시간 범위 안에서 본인의 위치정보 프라이버시가 보호되도록 설정하기 위해 사용된다. 시간 설정에는 1회 시간 설정, 달력 시간 설정 등이 사용될 수 있다.

2.4.2 공간 기반 프라이버시 보호 설정

공간 기반의 프라이버시 보호 설정은 위치정보 주체가 특정 공간 지역 내에 있거나 벗어났을 때와 같이 공간적인 특성에 따라 위치정보 프라이버시 보호를 설정할 수 있도록 하는 것이다.

공간 기반의 설정은 크게 특정 영역기반 설정 클래스(shapeClass)와 영역 타입 기반 설정 클래스(areaTypeClass)로 구분될 수 있다. 영역기반 설정 클래스는 특정 박스나 다각형 영역을 지정하고 그 지역에 존재여부에 따라 프라이버시를 설정하는 것이며, 영역 타입 기반 설정 클래스는 유흥가, 대학교 등과 같이 위치정보 주체가 존재하는 영역의 특성에 따라 프라이버시를 설정하는 것이다.

공간 기반의 위치정보 프라이버시 보호 설정에서 사용될 수 있는 지정 영역을 정의하기 위한 Area는 사각형(BOX), 원(CIRCLE), 다각형(POLYGON), 라인 버퍼(Line Buffer) 중의 한 가지 형태로 정의될 수 있다. 라인 버터는 도로와 같이 선 성분을 갖는 공간 정보를 기반으로 하며, 선(Line)으로부터 허용 가능한 거리 이내의 영역을 Area 영역으로 정의하며, 사각형, 원, 다각형 등도 비슷한 특정 지역을 나타내기 위해 사용 될 수 있다.

영역기반 클래스 설정에서 사용되는 영역은 MoveIn, MoveOut, StayIn, StayOut, MoveNearBy와 같은 영역에 대한 특성 설정과 함께 사용될 수 있다.

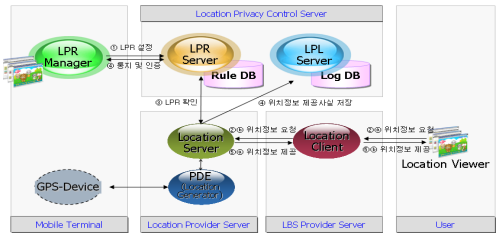
3. 위치정보 프라이버시 시스템 구조

위치정보 프라이버시 제어를 위한 시스템은 크게 위치정보 프라이버시 규칙을 관리하고, 규칙정보의 추가, 삭제, 갱신, 참조 등의 기능을 수행하는 위치정보 프라이버시 규칙 제어 모듈과 위치정보 보호 대상의 실제적인 위치 정보를 관리하기 위한 위치정보 제어 모듈로 구성된다. 그림 1은 위치정보 프라이버시 규칙 제어를 위한 모듈의 기본 요소를 보이고 있다.

LPR Manager는 위치정보제공자가 자신의 프라이버시와 관련된 규칙(LPR: Location Privacy Rule)을 추가, 삭제, 갱신, 참조 등의 작업을 통해 관리하기 위한 기능을 수행

하며 LPR Server는 LPR 정보를 통합 관리한다. LPR Agent는 LPR Server에서 관리하고 있는 이용자 프라이버시 규칙 정보를 단순히 참조만 하는 기능을 수행한다.

위치정보 제어 모듈은 위치정보제공자가 위치정보사업자



(그림 1) 위치정보 프라이버시 제어모듈의 배치 및 제어 흐름도

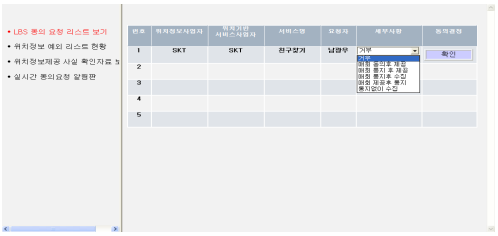
에 자신의 위치정보를 전송할 때 사용된 MS(Mobile Station) Agent와 위치정보를 통합 관리하는 Location Server, 이용자들의 위치정보를 제3자에게 제공한 내역을 관리하기 위한 LPL(Location Privacy Log) Server, 그리고 다른 사람의 위치 정보를 요청하고 전송받기 위한 Location Client로 구성된다.

4. 위치정보 프라이버시 시스템 구현

4.1 위치정보 프라이버시 제어 시스템 구현

4.1.1 위치정보 프라이버시 제어 인터페이스

위치정보제공자는 LBS Provider Server 등에 대하여 자신의 위치정보의 제공 요청에 대한 승인을 할 수 있고, 이때 위치정보 프라이버시 보호와 관련된 액션을 설정할 수 있다. 그림 2는 위치정보제공자의 위치에 대한 제공 요청 리스트 및 위치정보 프라이버시 보호 액션을 설정하는 인터페이스 화면을 보여준다.



(그림 2) LBS 동의 요청 리스트 보기

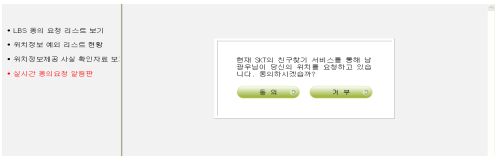
그림 2에서와 같이 위치정보를 요청한 위치정보사업자 및 위치기반서비스사업자, 위치정보 요청 서비스명 및 요청자 등에 대한 정보를 보여주고, 각각의 위치정보 요청에 대한 동의 결정을 하게 된다. 그림 3은 위치정보 프라이버시 예외 리스트 및 이들에 대한 위치정보 프라이버시 규칙의 동의 내용을 변경할 수 있게 하는 인터페이스를 보여준다.

위치정보제공자는 제 3자에게 자신의 위치정보를 제공한 사실을 확인할 수 있어야 한다. 그림 4는 위치정보제공자가 자신의 위치정보의 제공 사실을 확인하기 위해 제공되는 인터페이스를 보여준다.

(그림 3) 위치정보 예외 리스트 현황

(그림 4) 위치정보 제공사실 확인자료 보기

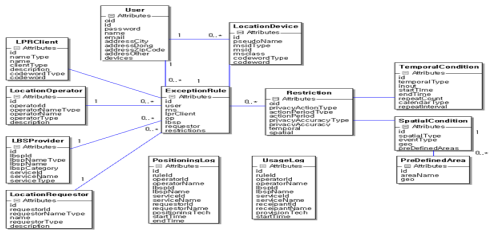
그림 5는 위치정보제공자가 자신의 위치정보에 대한 제공사실을 실시간으로 확인하여 승인할 수 있도록 이용자의 위치정보 제공 요청에 대한 알림판을 제공하는 인터페이스를 보여준다.



(그림 5) 실시간 동의 요청 처리

4.1.2 위치정보 프라이버시 규칙 데이터베이스

위치정보 프라이버시 규칙들은 LPR Server와 LPL Server의 데이터베이스에 저장된다. 그림 6은 위치정보 프라이버시 규칙 데이터베이스 모델링을 보이고 있다.



(그림 6) 위치정보 프라이버시 규칙 데이터베이스

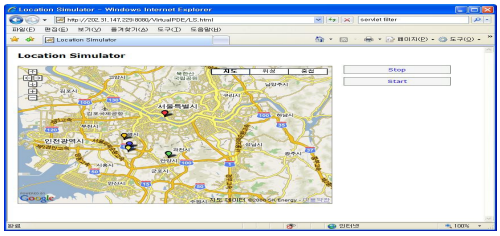
4.2 가상 PDE와 위치기반서비스의 구현

위치정보 수집과 제공을 실제 구현하기 위해서는 이동통신사의 서비스와 직접적인 연동이 필요하다. 그러나 이러한 작업은 상당한 비즈니스적 절차를 필요로 하므로 이 논문에서는 가상 PDE와 위치기반서비스를 구현하여 이동통신사의 서비스를 구성하였다.

4.2.1 가상 PDE와 위치정보 시뮬레이터

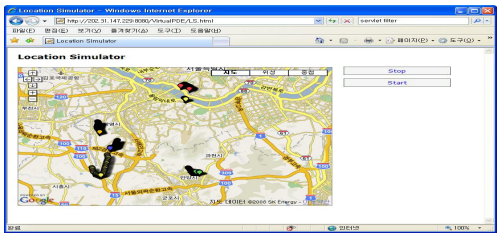
위치정보 시뮬레이터는 서울시의 도로정보를 기반으로 실제 위치정보를 생성하였으며, 이 정보들을 지도상에 표현하는 시스템이다. 그림 7은 위치정보제공자들의 위치정보를 시뮬레이션 한 예를 보여준다. 그림에서와 같이 여러 사람의 위치정보제공자들의 위치정보를 출력하며, 이들의

위치 이동 경로를 이용하여 시뮬레이션 하였다.



(그림 7) 여러 위치정보제공자의 위치정보 시뮬레이션(1)

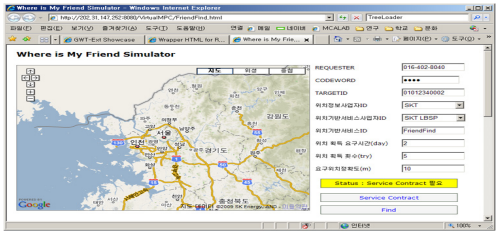
이 논문에서 구현한 위치정보 시뮬레이터는 위치정보를 화면에 표현하는 역할외에 HTTP 프로토콜을 통하여 특정 ID의 사용자 위치를 요청하면 사용자의 서울시내 가상위치를 WGS84 포맷으로 제공하는 가상 PDE의 역할을 함께 수행한다. 그림 8은 시뮬레이션을 통하여 얻어진 여러 위치정보제공자들의 이동 경로를 보여준다. 그림 8에서와 같이 위치정보제공자의 이동 경로는 사전에 정의된 도로 정보를 이용하여 서로 다른 속도로 이동하는 상황을 시뮬레이션 하였다.



(그림 8) 여러 위치정보제공자의 위치정보 시뮬레이션(2)

4.2.2 친구찾기 서비스와 프라이버시 설정 구현

이 논문에서는 친구찾기 서비스를 통하여 위치정보 프라이버시 규칙이 실제 올바르게 작동되는지를 보여주고 있다. 그림 9은 친구찾기 서비스의 실제 구현 화면을 보여준다.

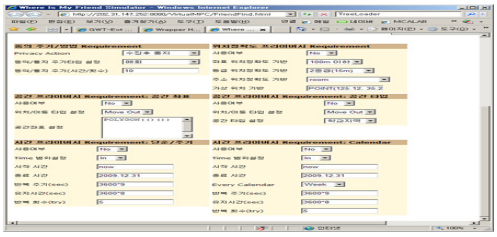


(그림 9) 친구찾기 서비스

각각의 위치정보제공자는 고유 번호로 관리되며 위치정보 뿐만 아니라 위치정보제공자의 이동 속도 및 시간 정보 등이 함께 제공된다. 그림 10은 위치기반 서비스 제공을 위해 사용되는 프라이버시 규칙 설정 화면이다.

5. 결 론

이 논문은 위치정보 프라이버시 보호 방안을 포괄적으로



(그림 10) 프라이버시 계약 설정 구현

조사 및 분석하여 향후 유비쿼터스 위치기반서비스에서의 위치정보 보호 방안을 개발하고, 위치정보 보호를 위한 기본 구성요소와 아키텍처를 설계하며, 이를 기반으로 개인 위치정보를 직접 제어할 수 있는 자기 제어 S/W 프로토타입을 개발하였다.

이 논문은 이동통신 사업자 등 위치정보사업자와 위치기반서비스사업자에서의 개인 위치정보 프라이버시 보호를 위한 실제 적용 가능한 표준 인터페이스를 개발하기 위한 기초적 자료로서 사용될 수 있다. 또한, 현재 위치정보법의 위치기반서비스의 측위 고도화와 프라이버시 보호 방안에 대한 법률 재개정에서 위치정보 프라이버시 보호에 대한 기술적 지원 자료로 이용될 수 있을 것이다.

참고문헌

[1] 곽진, 이근우, 김승주, 원동호, “프라이버시 보호 기능과 추적 기능을 동시에 제공하는 RFID 시스템 기반 미아 위치추적 시스템”, http://dosan.skku.ac.kr/~atrc/

[2] 김용운, 이준섭, 유상근, 김형준, “모바일 RFID 서비스 네트워크 구조 및 표준화 현황”, TTA Journal, 2005.

[3] 남기효, 개인정보보호 기술 동향: P3P, 주간기술동향 제1250호, 06, 2006.

[4] D. Anthony, D. Kotz, and T. Henderson, "Privacy in Location-Aware Computing Environment," Pervacive Computing, pp.64-72, October 2007.

[5] P. Bahl and V. Padmanabhan, "RADAR: an in-buildi ng RF-based user location and tracking system," Pro c. of IEEE INFOCOM, pp.775-784, March 2000.

[6] S. Consolvo et al., “Location Disclosure to Social Rel ations: Why, When and What People Want to Shar e,” Proc. SIGCHI Conf. Human Factors in Computing Systems (CHI 05), ACM Press, pp. 81.90, 2005.

[7] G. Danezis, S. Lewis, and R. Anderson, "How Much is Location Privacy Worth?," Proceedings of WISE 2 005.

[8] G. M. Djuknic and R. E. Richton. "Geolocation and a ssisted GPS". IEEE Computer, pp.123-125, February 2001.

[9] Q. He, D. Wu, and P. Khosla, “The Quest for Perso nal Control over Mobile Location Privacy,” IEEE Co mm., vol. 42, no. 5, pp. 130-136, 2004.