프라이버시 자기제어를 지원하는 위치정보 프라이버시 시스템의 설계 및 구현

(Design and Implementation of a Location Privacy System supporting Privacy Self Controls)

이 응 재 † 주 용 완 † 남 광 우 ††
(Eung Jae Lee) (Yong Wan Ju) (Kwang Woo Nam)

요 약 모바일 기기 및 와이브로, HSDPA 등의 초고속무선인터넷 보급/확산으로 개인의 위치 정보에 기반을 둔 다양한 광고 및 서비스가 가능해졌다. 그러나 이러한 편리성과 함께 실시간으로 개인의 위치 및 이동 행태 등 개인 프라이버시가 타인에게 노출될 가능성이 커졌고, 또한 개인 프라이버시가 유출될 경우 생명 및 재산 등에 큰 피해를 줄 수 있어 사회적인 문제가 되고 있다. 이 논문에서는 모바일 환경에서 이용자들의 위치정보와 관련된 프라이버시 보호를 위한 필요한 요소들을 분석하고 이를 기반으로 자신의 위치정보 프라이버시를 직접 제어하고 관리하도록 하기 위한 위치정보 프라이버시 프로토콜을 제안한다. 그리고 제안된 위치정보 프라이버시 프로토콜을 이용하여 이용자 스스로가 자신의 위치정보 프라이버시를 관리할 수 있는 개인위치정보 프라이버시 자기제어 시스템의 프로토타입을 설계하고 구현하였다.

키워드 : 위치기반서비스, 개인위치정보, 위치정보 프라이버시, 위치정보 프라이버시 제어 프로토콜

Abstract As the mobile device and broadband wireless internet such as WiBro, HSDPA is widely spreading, various types of advertisement and services based on personal location information can be provided. However, with convenience supported by these services, it is possible to be increased an invasion of privacy such as personal location and moving pattern. In this paper, we analysis an essential element for protection of privacy related on location information in mobile environment and propose location privacy protocol for managing location privacy self-control. And we design and implementation prototype of location privacy self-control system which is able to manage user's location privacy condition oneself using the proposed location privacy protocol.

Key words : Location-Based Services, Personal Location Information, Location Privacy, Location Privacy Protocol

· 본 연구는 국토해양부 첨단도시기술개발사업 - 지능형국토정보기술혁신사업과제의 연구비 지원(07국토정보C05)과 2008년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(No. 2008-0061967)

† 정 회 원 : 한국인터넷진흥원 인터넷기반진흥단
eungjae@kisa.or.kr
ywju@kisa.or.kr
†† 종신회원 : 군산대학교 컴퓨터정보공학과 교수
kwnam@kunsan.ac.kr
(Corresponding author임)

논문접수 : 2010년 1월 7일
심사완료 : 2010년 5월 13일

정보과학회논문지: 컴퓨팅의 실제 및 레터 제16권 제8호(2010.8)

1. 서 론

최근 이동통신 기술의 발달과 함께 이동단말의 위치를 파악하여 이를 기반으로 다양한 서비스를 제공하고자 하는 위치기반서비스(Location-Based Services; LBS)가 활성화되고 있다[1-4]. 위치기반서비스에 대한 수요가 증가함에 따라 많은 국내외 민간기업, 공공기관과 지자체 등에서는 이 위치정보를 가공하여 민간과 공공부문에 서비스할 다양한 콘텐츠를 개발하고 있으며, 아이폰등과 같은 스마트폰에서 킬러 어플리케이션으로 지목되고 있다[5]. 그러나, 이러한 위치정보의 이용확대와 더불어 개인의 위치정보 프라이버시의 침해에 대한 위험성 또한 증가하고 있다[6].

이동통신사업자들은 네트워크의 구조적 특성으로 인하여 추가적인 비용없이 특정 지역 내에서 이동하는 이

용자의 위치정보를 실시간으로 획득하여 서비스를 제공할 수 있다. 이러한 위치정보는 이동통신사업자등의 위치정보사업자가 설치 및 보급한 단말에 내장된 통신장치 또는 GPS 등의 위치인식 장치에 의해서 획득되며, 성명이나 주민등록번호와 같이 이용자가 직접 입력한 일반적인 개인정보보다 유출시 위험성에서 보다 높은 보호가 필요하다[7,8]. 위치정보가 누출될 시에 개인의 위치 추적이 가능하여 위험인물로부터의 표적이 될 수 있으며, 위치정보의 오류·왜곡을 유발하여 생명과 재산에도 큰 피해를 안겨 줄 수 있다. 프라이버시 위협의 실제적인 예는 텔레매틱스와 LBS 등에서 이미 나타나고 있다. 예를 들어 사망자 휴대폰으로 삼성 SDI 노조원의 위치를 불법적으로 추적한 사건이 있었으며, 휴대폰 복제에 의한 불법 위치 추적 서비스에 대한 보도 등 이용자의 위치정보 프라이버시에 대한 침해 사례들이 상당수 있어왔다. 이러한 단점에도 불구하고 이용자의 위치정보는 개인의 사생활 보호와 함께 활용에서의 필요성이 복합적으로 요구된다. 개인위치정보의 보호와는 별도로 이용자의 긴급구조를 위한 중요한 정보이며, 사용자의 요구에 따라 물류나 보험, 경호, 관광정보, 교통 등 산업 전반에 걸친 다양한 응용 서비스에 제공될 필요성이 있다[1,5]. 그러므로, 개인 위치정보 프라이버시를 보호하면서, 필요한 응용에 따라 개인이 위치정보의 이용 및 제공을 직접 확인하고 제어할 수 있도록 해주는 프로토콜은 필수적이라고 할 수 있다.

위치정보 및 위치기반서비스 제공을 위한 프로토콜에 대한 연구는 주로 표준화와 함께 진행되었다[9-12]. 대표적인 위치기반서비스 관련 표준화 기관들은 OMA (Open Mobile Alliance), OGC(Open Geospatial Consortium), 3GPP(3rd Generation Partnership Project), 3GPP2(3rd Generation Partnership Project 2), W3C (World Wide Web Consortium), IETF(Internet Engineering Task Force) 등이다. 이 표준들 중 특히 OMA와 IETF의 표준들은 개인 위치정보의 제어와 관련된 표준들을 포함하고 있다. 즉, IETF에서는 인터넷망에서의 지리적 위치정보 전달과 보호를 위하여 GeoPriv 표준을 개발하고 있다[11,12]. 이 중에서 OMA의 LOC WG에서 위치정보 프라이버시에 대한 표준화 작업이 진행 중에 있다[10]. 그러나 이러한 기존의 표준들은 단순한 형태의 위치정보 프라이버시에 제어에 관한 프로토콜 표준화에 초점을 맞추고 있으며, 가장 기본적인 위치정보 제공 사실 확인자료의 확인과 다양한 즉시적 보호체계를 갖고 있지 못하다. 또한, 이러한 표준들이 실제 프로토타입이 제시된 사례는 없는 상황이다. 세부적으로는 익명성을 이용하여 위치정보 프라이버시를 보호를 보호하려는 연구들[13-17]과 위치기반서비스 응용에서 발생할 수있는 상황에서 위치정보 프라이버시를 보호하려는 연구[18-20], 위치정보 접근권한을 제어하는 방법에 대한 연구[21] 등이 있다. 이러한 세부적인 연구들은 각 기술적인 기반을 제공하나 개인 위치정보 프라이버시의 이용자 중심적 자기 제어에 대한 통합적 프로토콜을 제안하지는 못하고 있다. 따라서 이 논문에서는 이용자들의 위치정보 프라이버시 보호를 위한 기본 구성요소와 위치정보 프라이버시를 위한 통합적인 자기제어 프로토콜을 설계한다. 그리고 위치정보 프라이버시를 위한 자기제어 시스템 프로토타입을 제시하는데 차별성이 있다.

이 논문의 구성은 다음과 같다. 먼저 2장에서는 위치정보 프라이버시에 관한 프로토콜 표준화 현황을 살펴보고, 3장에서는 이 논문에서 제안하는 위치정보 프라이버시 프로토콜을 기술한다. 4장에서는 3장에서 제안한 프로토콜을 기반으로 한 자기제어 시스템 프로토타입을 설계·구현하고, 마지막 장에서 결론을 맺는다.

2. 관련 연구

지금까지 위치정보 프라이버시에 대한 연구[22-25]들은 많이 진행되어 왔지만 대부분은 위치정보 전송시의 암호화 등에 의한 프라이버시 보호에 집중되어 연구되었다. 그러나 위치정보 프라이버시를 효과적으로 보호하기 위해서 이용자 스스로 자신의 위치정보 관련 설정을 제어할 수 있어야 한다. 위치정보 프라이버시 제어를 위한 기존 연구로는 크게 OMA의 PCP(Privacy Checking Protocol) 표준[10]과 IETF의 GeoPriv 표준[11,12]이 진행 중에 있다.

2.1 OMA PCP 표준

OMA LOC WG은 2002년 6월 OMA 설립당시 Location Interoperability Forum(LIF)라는 표준화기구를 합병하는 것으로 시작되었으며, 현재 LIF로부터 작업해온 MLP(Mobile Location Protocol)과 RLP(Roaming Location Protocol), SUPL(Secure User Plane Location), PCP(Privacy Check Protocol), Location Architecture Overview 등에 대한 표준화가 진행 중이다.

이 표준들 중에서 위치정보 프라이버시와 관련된 프로토콜인 PCP는 사용자가 미리 설정한 위치 정보와 관련된 프라이버시 설정정보를 기반으로 위치서버가 위치정보를 요청하는 위치 클라이언트에 대한 프라이버시 보호를 목적으로 하는 프로토콜이다. 위치정보 보호 및 인증 기술 규격은 위치정보를 수집 및 제공하는 위치서버와 외부 프라이버시 인증부 간의 프로토콜로 사용될 수도 있다. PCP 표준에서 프라이버시 설정 정보를 갖는 서버를 PCE(Privacy Checking Entity)라고 하며, PCP는 PCE와 위치서버간의 프로토콜을 정의하고 있다.

표 1 PCP의 서비스 프로토콜 메세지들

서비스	구성 메세지
위치 프라이버시 인증 서비스 (Location Privacy Assertion Service)	- 위치 프라이버시 인증 요구(Location Privacy Assertion Request) - 위치 프라이버시 인증 응답(Location Privacy Assertion Response)
익명/실명 매개 서비스 (Pseudonym/Verinym Mediation Service)	- 익명 요구(Pseudonym Request) - 익명 응답(Pseudonym Response) - 실명 요구(Verinym Request) - 실명 응답(Verinym Response)
프라이버시 프로파일 갱신 알림 서비스 (Privacy Profile Update Notification Service)	- 위치 프라이버시 프로파일 갱신 알림(Location Privacy Profile Update Notification) - 위치 프라이버시 프로파일 갱신 알림 인식(Location Privacy Profile Update Notification Ack)

표 1은 PCP의 서비스 프로토콜 메세지들을 보이고 있다.

PCP의 프라이버시 체킹 서비스는 위치추적 대상 모바일 가입자의 프라이버시 설정을 인증하기 위한 표준 서비스인 위치 프라이버시 인증 서비스 프로토콜(Location Privacy Assertion Service), 모바일 가입자의 익명과 실명을 매개하기 위한 표준서비스인 익명/실명 매개 서비스 프로토콜(Pseudonym/Verinym Mediation Service), 위치 추적 대상 모바일 가입자의 프라버시 프로파일 갱신을 위치서버 등에게 알리기 위한 표준 서비스인 프라이버시 프로파일 갱신 알림 서비스(Privacy Profile Update Notification Service)로 구성된다.

2.2 IETF GeoPriv 표준

IETF의 GeoPriv WG은 자원이나 엔터티에 대한 지리적 위치 정보를 전달하는 방법을 개발하기 위해 설립되었다. GeoPriv 표준에는 지리적 위치정보를 전달하기 위한 인증(authorization), 완전성(integrity), 프라이버시 요구사항 등이 포함되어 있으며, 이 밖에 위치정보의 프라이버시 관리를 위한 데이터 포맷 통합, 요청자와 대응자의 인증, 프록시 인증, 요청자와 대응자의 분류, 주어진 정보의 정확성 등을 포함한다.

GeoPriv 표준은 기본적으로 그림 1과 같이 위치 생성자(Location Generator), 위치 서버(Location Server), 위치 송신자(Location Recipient), 규칙보유자(Rule Holder) 등 네 개의 기본 요소를 기반으로 한다.

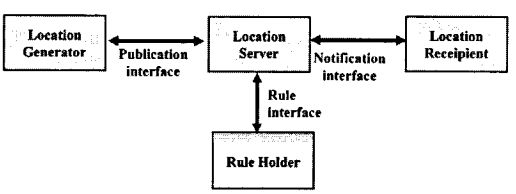


그림 1 GeoPriv 표준의 주요 구성요소

위치 생성자(Location Generator)는 처음에 위치정보 타겟(Target)의 위치를 결정하거나 수집하고 그 위치를 기술하는 위치 객체(Location Object)를 생성하는 엔티티로서 위치정보서버(Location Server)들에게 위치 객체를 알린다(publish). 위치서버(Location Server)는 위치 생성자로부터 위치 객체들의 발행(publication)을 수신하고 위치 수신자(Location Recipient)들로부터 등록(subscription)을 받을 수 있는 요소이다. 그리고 위치생성자으로부터 받은 위치객체들에게 규칙보유자(Rule Holder)로부터 학습한 규칙을 적용하고, 필요에 따라 위치객체들의 위치수신자를 통지한다. 위치수신자는 위치서버들로부터 통지되는 위치 객체를 수신하는 요소이다. 위치수신자는 어떠한 방법으로 유저 또는 자동장치에 이들 위치 객체들을 넘겨줄 수 있다. 규칙보유자는 특정한 위치정보타겟(Target)들을 위해 위치 객체들을 수신, 필터링, 분배하기 위한 프라이버시 규칙들이 수용하는 요소이다. 위치정보서버는 규칙의 집합을 위해 규칙보유자에 질의하거나, 규칙들은 규칙보유자로부터 위치정보서버까지 푸쉬될 수 있다. 규칙보유자에 있는 규칙들은 위치프라이버시규칙생성자(Rule Maker)에 의해 관리된다.

3. 위치정보 프라이버시 보호 설계

3.1 위치정보와 공간정보

위치정보는 프라이버시 보호 대상의 위치를 표현하기 위한 가장 기본적인 방법으로 보통 <point, time>의 형태로 인식되나, 위치 기반 서비스에서 사용되는 위치는 위치 측위의 방법이나 위치 정확도의 오차, 서비스의 요구사항에 따른 좀 더 확장된 표현을 필요로 한다. 예를 들면 공간상의 위치는 <x, y> 형태 뿐만 아니라 선, 면을 포함한 공간 shape의 형태로 표현 될 수도 있으며 특정 좌표 값을 추출할 수 없는 경우 주소의 형태로 표현될 수도 있다.

그림 2는 위치정보의 최소 표현 요소로서 시간(time), 공간정보(shape), 고도(alt), 이동속도(speed), 이동방향(direction) 및 위치정보의 정확도를 표현하기 위한 확률(probability) 등으로 구성된다.

```
LocationType ::= SEQUENCE {
   time       TimeType,                    -- 시간 정보
   shape      Shape,                       -- 공간 정보
   sequence SEQUENCE {
      alt     Altitude,                    -- 고도
      alt-unc AltitudeUncertainty  OPTIONAL
   } OPTIONAL,
   speed      Speed          OPTIONAL,          -- 속도
   direction Direction       OPTIONAL,          -- 방향
   lev-conf Probability      OPTIONAL           -- 확률
}
```

그림 2 위치 정보 표현 요소

공간정보는 위치정보가 공간 좌표 체계의 형태로 표현될 때 사용된다. 공간정보는 OGC에서 정의한 단순 피처 모델 표준을 기반으로 정의되는 것이 일반적이다. 이 단순 피처 모델은 점(point), 선(linestring), 면(polygon), 점집합(multipoint), 선집합(multilinestring), 면집합(multipolygon)의 공간 데이터 타입과 선과 면을 표현하기 위한 추상 타입으로 선형링(linearing), 표면(surface) 등의 공간 데이터 타입을 포함한다. 이 밖에도 OGC 단순 피처 모델에서 포함되어 있지않은 사각형(box), 원(circularArea), 원뿔(circularArcArea), 데이터 타입과 타원형(ellipticalArea) 데이터 타입이 포함될 수 있다.

3.2 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 다섯 가지 주요 구성 요소는 위치정보주체의 프라이버시 보호를 위하여 다음과 같이 운용될 수 있다.

```
PrivacyRule ::= SEQUENCE {
    ruleID      [1] RuleID,
    operator    [2] LocationOperator,
    lbsp        [3] LBSProvider,
    client      [4] LPRClient,
    -- restrictions...
    privacyAction          [5] LPRActionType,
    actionPeriod           [6] ActionPeriod,
    accuracy               [7] Accuracy,
    spatialCondition       [8] SpatialCondition,
    temporalCondition      [9] TemporalCondition
}
```

그림 3 위치정보 프라이버시 예외 리스트의 기본 구조

위치정보사업자는 예외 리스트가 위치정보사업자 별로 관리 될 경우에는 생략될 수 있다. 위치기반서비스사업자와 관련된 주요 정보로는 위치기반서비스사업자와 위치기반서비스 형태 등이 있다. 위치정보주체는 위치기반서비스사업자 및 위치기반서비스 정보를 통하여 위치기반서비스에 대한 프라이버시 제한을 하게 된다.

위치정보 취득자는 위치정보를 실제 제공받는 제3자로서 법인이거나 개인일 수 있다. 위치정보 취득자에 대한 정보는 식별자와 이름으로 구성된다. 이동통신의 경우 개인은 휴대폰 식별번호일 수 있으며, 법인의 경우에는 사전에 위치기반서비스사업자에게 인증된 식별번호일 수 있다. 위치정보 제한 사항은 프라이버시 보호 액션과 정확도 설정, 시공간 설정, 최대 위치정보 제공 횟수 설정 등이 가능하며, 위치정보를 제공하는 위치기반서비스사업자, 위치기반서비스, 위치정보 취득자에 대하여 위치정보 주체의 프라이버시 제한을 설정하기 위해 사용된다.

3.3 위치정보 프라이버시 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. 이 논문에서는 국내 위치정보법에서 의무화한 '매회 통지'를 포함하여 최소 6단계로 구성하였다.

위치정보 프라이버시 보호 액션은 그림 4와 같이 위치정보 수집 거부(position not allowed), 위치정보 수집 통지 후 허용시 수집(notify position if granted), 위치정보 수집 통지 후 무 응답시 수집(granted or if no response), 통지 후 수집(notify and position), 수집 후 통지(position and notify), 통지 없이 수집(position without notify) 등으로 구성된다.

```
LPRActionType ::= ENUMERATED {
    not-allowed                (0),
    if-granted                 (1),
    granted-or-no-response     (2),
    notify-and-position        (3),
    position-and-notify        (4),
    position-without-notify    (5)
}
```

그림 4 위치정보 프라이버시 보호 액션 설정

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 있는데 친구찾기 서비스의 예를 들면 제3자가 위치정보 주체의 위치정보를 수집하는 매회에 통지하도록 할 수도 있다. 이 때 매회 통지되는 위치정보 수집에 대하여 허용 또는 거부를 하는 것은 위치정보 주체에게 상당히 번거로운 일이기 때문에 특정 시간 주기 또는 특정 수집 횟수 마다 통지토록 함으로서 위치정보 주체의 서비

스 편의를 확장할 수 있다. 이러한 통지 주기는 그림 5와 같이 위치정보 수집 또는 제공되는 매 회(every position or providing)마다 통지를 하는 설정, 위치정보 수집 등의 최초 1회 통지 후 매 횟수(every frequency)마다 통지되도록 하는 설정, 위치정보 수집 등의 최초 1회 통지 후 매 주기시간(every periodic time) 마다 통지되도록 하는 설정, 서비스가 실제 시작되는 시점에 1회에 한하여 통지되도록 하는 서비스 활성화시 통지(service activation) 설정 등이 있다.

```
ActionPeriodType ::= ENUMERATED {
    every-position-or-providing     (0),        -- 매회
    every-frequency     (1),        -- 매 횟수
    every-periodic-time (2),        -- 매 주기 시간
    service-activation  (3)         -- 서비스 활성화 시
}
```

그림 5 위치정보 수집 또는 제공 통지 시기 설정

위치정보 프라이버시 액션과 통지 주기는 위치정보 주체의 필요에 따라 상호 조합하여 설정할 수 있어야 한다. 예를 들면 위치정보 수집 통지 후 허용시 수집과 매 주기 시간 통지 주기를 함께 사용함으로서 매 시간별로 위치정보 수집에 대한 허용허가를 받도록 설정할 수 있다.

3.4 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 제3자의 신뢰성과 필요 정확도에 따라 제공되는 위치정보의 정확도 수준을 조절하여 제공할 수 있도록 할 필요가 있다.

위치 정확도 기반 프라이버시 설정은 그림 6과 같이 좌표 정확도, 등급화된 정확도, 주소 기반 위치, 가상 위치 등으로 구분된다.

좌표 정확도(Coordinate Type)는 위치정보가 좌표 참조 시스템 내의 특정 좌표로 표현된다. 이 좌표는 정밀한 위치 측정 장치인 경우에는 cm급의 위치정보를 보일 수도 있으며, GPS의 경우에는 10m급의 위치정보를 측정할 수 있다. 등급 정확도(Graded Accuracy Type)는 좌표 정확도와 같이 m, km 단위의 위치 정확도 범위를 직접 조절하는 것이 일반 이용자에게 어려운 작업이 될 수 있기 때문에 미리 정의된 특정한 수준의 등급 또는 수준으로 위치정보 정확도를 구분하여 제공하고, 일반 이용자는 제시된 등급 또는 수준 중에 하나를 선택하는 형태로 프라이버시 보호 설정이 제공된다. 이러한 예는 포털 등의 지도 제공 서비스에서 지도 표현 레벨을 디테일 수준별로 나누어 제공하는 것과 같다. 주소 기반 위치(Civic Address Type)는 일반인이 표현하는 가장 보편적인 방법인 주소를 위치정보로 이용하는 것이다. 가상 위치(Psuedo Type)는 필요에 따라 실제 주체가 위치한 장소를 숨기고 특정 시간 또는 특정 주기 시간 동안 가상의 위치정보가 제공되도록 하는 방법으로 위치정보 프라이버시 보호를 위한 중요한 설정이 될 수 있다.

```
AccuracyData ::= CHOICE {
    coordinate              CoordinateType,
            -- 좌표정확도 기반 설정
    gradedAccuracy          GradedAccuracyType,
            -- 등급 정확도 기반 설정
    civicAddress            CivicAddressType,
            -- 주소 기반 위치 설정
    psuedo   PsuedoType-- 가상 위치 설정
}
```

그림 6 위치 정확도 기반 프라이버시 설정

3.5 프라이버시 보호 시간 및 공간 설정

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

```
TemporalData ::= CHOICE {
    simple   [1] SimpleTime,        -- 1회 시간설정
    calendar [2] CalendarTime       -- 달력 시간설정
}
```

그림 7 시간 기반의 프라이버시 보호 종류

1회 시간 설정은 그림 8과 같이 위치정보주체가 특정 시간 범위에 대하여 1회만이 활성화될 수 있는 시간 설정이다. 1회 시간 설정에는 설정 시작 시간(startTime)과 종료시간(endTime), 설정 시간의 안쪽 또는 설정시간을 제외한 시간을 나타내는지를 표현하는 시간 설정 타입(type)으로 구성될 수 있다. 예를 들면 In을 사용하여 '2006년 11월 11일 오전 9시부터 오후 6시까지'와 같이 설정하거나, Out을 사용하여 '2006년 11월 11일 오전 9시부터 오후 6시를 제외한 시간동안'과 같이 사용할 수도 있다.

```
SimpleTime ::= SEQUENCE {
    type        TimeActionType,     -- 시간 설정 타입
    startTime               TimeType, -- 설정 시작 시간
    endTime TimeType,  -- 설정 종료 시간
    repeatCount             INTEGER,  -- 설정 반복 횟수
    repeatInterval          INTEGER   -- 설정 반복 주기
}
```

그림 8 1회 시간 기반의 프라이버시 보호 설정

달력 시간 설정은 달력에 표시된 시간에 기반하여 위치정보 프라이버시를 설정하는 것을 의미한다. 예를 들면 '공휴일' 또는 '명절'과 같은 설정은 모든 국가마다 달라질 수 있는 특수한 달력에 해당한다고 볼 수 있다. 이러한 달력 특성에 따라 프라이버시 보호를 설정할 경우 위치정보 주체의 프라이버시 보호 설정의 편의성을 높일 수 있다.

공간 프라이버시 보호 설정에서 공간영역 설정은 그림 9와 같이 크게 특정영역 기반 설정과 영역타입 기반 설정으로 구분될 수 있다. 특정영역 기반 설정은 특정 박스나 다각형 영역을 지정하고 영역 내의 존재여부에 따라 프라이버시를 설정하는 것이며, 영역타입 기반 설정은 유흥가, 대학 등과 같이 위치정보 주체가 존재하는 영역의 특성에 따라 프라이버시를 설정하는 것이다.

```
SpatialData ::= CHOICE {
    shape   [1] Shape,
            -- 특정영역 기반 설정
    predefinedAreaID   [2] INTEGER
            -- 영역타입 기반 설정
}
```

그림 9 공간영역 설정

특정영역 기반 설정을 위한 영역의 형태는 사각형(BOX), 원(CIRCLE), 다각형(POLYGON), 라인 버퍼(Line Buffer) 등으로 정의할 수 있다. 라인 버퍼는 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 사용될 수 있다.

공간 프라이버시 보호 설정은 앞에서 설명한 공간영역 설정과 더불어 MoveIn, MoveOut, StayIn, StayOut, MoveNearBy와 같이 위치정보주체의 이동특성에 대한 설정들을 함께 사용할 수 있다(그림 10).

```
MovingEventType ::= ENUMERATED {
    stay-in   (0),
    stay-out (1),
    move-in (2),
    move-out          (3),
    nearby   (4)
}
```

그림 10 위치정보주체의 이동특성 설정

위치정보주체의 이동특성은 특정 영역의 안(Stay In)이나 밖(Stay Out)에서 특정 시간 이상 동안 있었을 때 프라이버시 보호 설정을 변경할 수 있다. 그리고 특정 영역으로 진입하는 순간(Move In) 또는 특정 영역을 벗어나는 순간(Move Out)에 프라이버시 보호 설정을 할 수 있다. 마지막으로 특정 지점을 설정하고 그 곳으로 부터 특정 거리이내나 밖에 있을 때 위치정보 프라이버시 보호 설정을 하는 것을 의미한다. 가장 간단하게 공간에 기반하여 프라이버시 보호를 설정할 수 있는 방안이 될 수 있다.

4. 자기제어 시스템 프로토타입 설계 및 구현

4.1 자기제어 시스템의 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 11은 위치정보 프라이버시 제어모듈들이 위치정보 프라이버시 시스템을 구성하는 각각의 요소에 배치된 상태를 보여준다. 위치정보 프라이버시 규칙 제어를 위한 모듈은 기본적으로 LPR Manager, LPR Server, LPR Agent로 구성된다. LPR Manager는 위치정보제공자가 자신의 프라이버시와 관련된 규칙(LPR: Location Privacy Rule)을 추가, 삭제, 갱신, 참조 등의 작업을 통해 관리하기 위한 기능을 수행하며 LPR Server는 LPR 정보를 통합 관리한다. LPR Agent는 LPR Server에서 관리하고 있는 이용자 프라이버시 규칙 정보를 단순히 참조만 하는 기능을 수행한다. 그리고 위치정보 제어를 위한 모듈은 위치정보제공자가 위치정보사업자에 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. 위치정보 프라이버시 시스

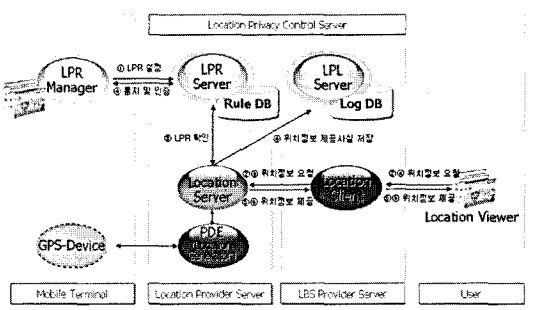


그림 11 위치정보 프라이버시 제어모듈의 배치 및 제어 흐름도

템의 기본 요소로는 위치 단말기(Mobile Terminal), 위치정보 관리 서버(Location Provider Server), 위치기반 서비스 제공 서버(LBS Provider Server), 위치정보 프라이버시 제어 서버(Location Privacy Control Server), 그리고 위치정보를 참조하는 이용자로 구성된다.

프라이버시 자기제어를 위한 시스템의 위치정보 및 프라이버시 프로토콜을 구성하고 있는 메시지 서비스의 기본 동작은 다음과 같다.

1) 위치정보 주체의 프라이버시 규칙 관리 : 위치정보주체는 자신의 위치 단말기에 내장되거나 웹상에서 접근가능한 LPR Manager를 통하여 LPR Server에게 자신과 관련된 위치정보 프라이버시 규칙들의 리스트를 보거나(listup) 갱신·삭제(update)한다. 이 때 LPR Server는 위치정보 주체가 프라이버시 규칙을 갱신하였다는 것을 알림(notification)으로서 Location Server들이 기존의 위치정보 제공을 프라이버시 규칙에 맞게 변경할 수 있도록 한다.
2) 위치정보 요청과 동의 확보 : 제3의 이용자가 LBS Provider Server를 통하여 위치정보제공자의 위치정보를 요청하면 Location Sever는 LPR Server에게 위치정보주체가 설정한 프라이버시 규칙에 의해 제공해도 되는지를 검증(assertion)한다. LPR Server는 Location Server의 요청을 받아 위치정보제공자에게 위치정보 제공 요청 사실을 통지 및 요청 인증(certification)을 받은 후 그 결과를 Location Server에게 전달한다. 만일 위치정보 제공 요청에 대한 인증을 받았다면 Location Server는 Location Client를 통하여 제3자에게 위치정보제공자의 위치정보를 제공하게 된다.
3) 위치정보 접근 사실 확인 자료의 로깅과 확인 : 위치정보 주체에 대한 위치정보를 수집할 경우 Location Server는 관련 사실을 LPL Server에 로깅(positioning log)하여야 하며, 비슷하게 LBS Provider 등이 위치정보를 제공·이용하는 경우에도 로깅(usage log)하여야 한다. 이 때 위치정보 주체는 LPR Manager를 통하여 LPL Server에 저장된 위치정보 접근 사실 확인자료를 확인(listup)할 수 있는 기능을 지원해야 한다.

4.2 위치정보 프라이버시 제어 인터페이스

위치정보제공자는 LBS Provider Server 등에 대하여 자신의 위치정보의 제공 요청에 대한 승인을 할 수 있고, 이 때 위치정보 프라이버시 보호와 관련된 액션을 설정할 수 있다. 그림 12는 위치정보제공자의 위치에 대한 제공 요청 리스트 및 위치정보 프라이버시 보호 액션을 설정하는 인터페이스 화면을 보여준다.

그림 12와 같이 위치정보를 요청한 위치정보사업자

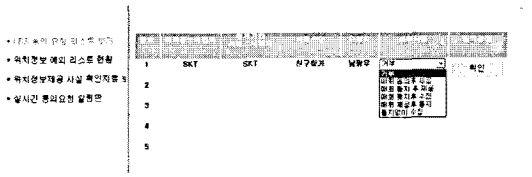


그림 12 LBS 동의 요청 리스트 보기

및 위치기반서비스사업자, 위치정보 요청 서비스명 및 요청자 등에 대한 정보를 보여주고, 각각의 위치정보 요청에 대한 동의 결정을 하게 된다. 그림 13은 위치정보 프라이버시 예외 리스트 및 이들에 대한 위치정보 프라이버시 규칙의 동의 내용을 변경할 수 있게 하는 인터페이스를 보여준다.

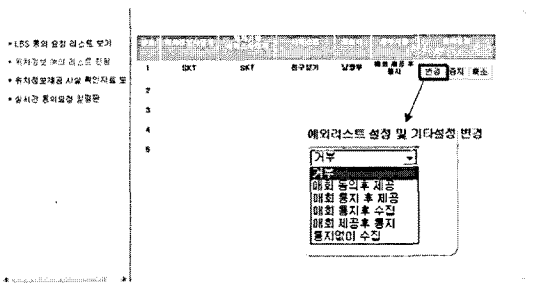


그림 13 위치정보 예외 리스트 현황

위치정보제공자는 제3자에게 자신의 위치정보를 제공한 사실을 확인할 수 있어야 한다. 그림 14는 위치정보 제공자가 자신의 위치정보의 제공 사실을 확인하기 위해 제공되는 인터페이스를 보여준다.

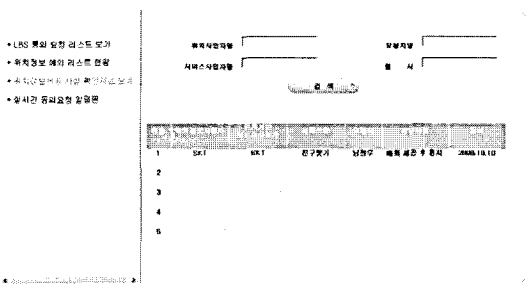


그림 14 위치정보 제공사실 확인자료 보기

4.3 가상 PDE와 위치기반서비스

위치정보 수집과 제공을 실제 구현하기 위해서는 이동통신사의 서비스와 직접적인 연동이 필요하다. 이 논문에서는 가상 PDE와 위치기반서비스를 구현하여 이동통신사의 서비스를 구성하였다.

위치정보 시뮬레이터는 서울시의 도로정보를 기반으

로 실제 위치정보를 생성하였으며, 이 정보들을 지도상에 표현하는 시스템이다. 그림 15는 위치정보제공자들의 위치정보를 시뮬레이션 한 예를 보여준다. 그림 15에서는 6명의 위치정보제공자들의 위치정보를 출력하며, 이들의 위치 이동 경로를 이용하여 시뮬레이션 하였다.

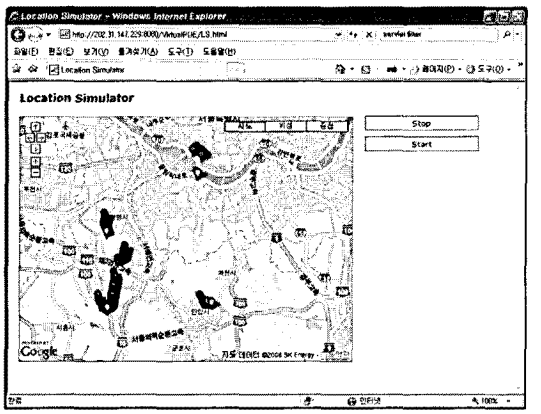


그림 15 여러 위치정보제공자의 위치정보 시뮬레이션

그림 16은 친구찾기서비스의 실제 구현화면을 보여준다. 이 그림에서는 친구찾기 서비스를 통하여 위치정보 프라이버시 규칙이 실제 올바르게 작동되는지를 보여주고 있다.

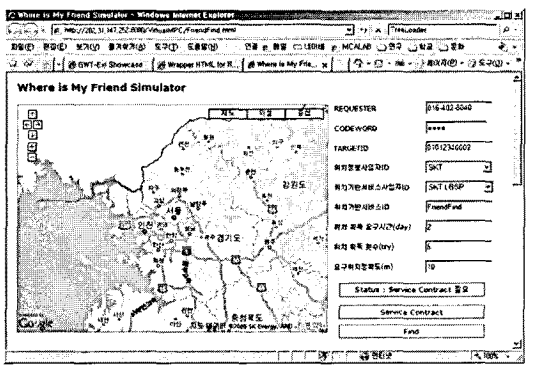


그림 16 친구찾기 서비스

각각의 위치정보제공자는 고유 번호로 관리되며 위치정보 뿐만 아니라 위치정보제공자의 이동 속도 및 시간 정보 등이 함께 제공된다. 그림 17은 위치기반 서비스 제공을 위해 사용되는 프라이버시 규칙 설정 화면이다.

4.4 위치정보 프라이버시 제어 관련 연구 비교

위치정보 프라이버시 제어를 위한 기존 연구들은 표 2와 같이 기본적인 위치측위방법 및 위치의 정확도 제어가 가능하며 위치 측위의 시작 및 종료 시간 설정, 공간적으로 단순한 위치정보에 대한 제어 등이 가능하다.

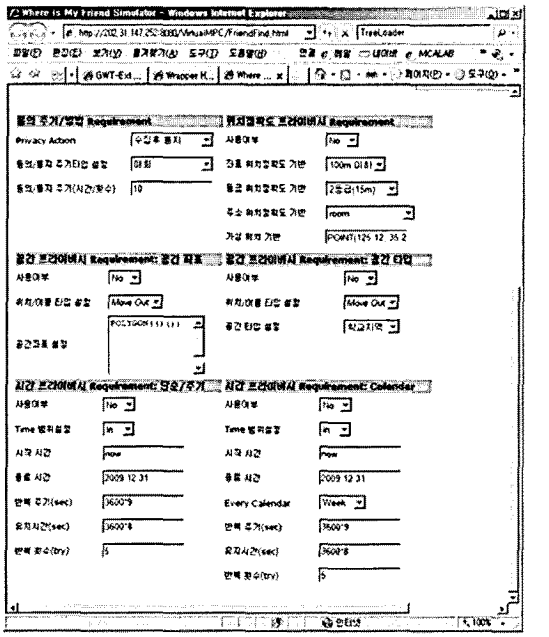


그림 17 프라이버시 계약 설정 구현

표 2 위치정보 프라이버시 제어기능 지원 비교

구 분		OMA PCP	IETF GeoPriv	제안프로토콜
위치정확도 지정		○	○	○
위치측위 방법		○	○	○
시간 속성	Periodic	○	○	○
	Calendar	×	×	○
공간 속성	In, Out	○	○	○
	Entering, Outing	×	×	○
시·공간 속성	Periodic-In/Out	○	○	○
	Periodic-Enter/Out	×	×	○
	Calendar-In/Out	×	×	○
	Calendar-Enter/Out	×	×	○

그러나 효과적인 위치기반 서비스 제공을 위해서는 보다 세분화된 시간 속성 및 시간에 따른 위치 이동 등 다양한 조건에 대한 위치정보 프라이버시 제어가 필요하다. 예를 들어 초등학생 자녀를 둔 부모가 유괴 등의 사회 문제를 걱정하여 매주 주중의 학교 등·하교 시간에 자신의 자녀가 등·하교하는 경로를 벗어나는 상황 정보를 얻고자 할 경우, 보다 복잡한 위치정보 프라이버시 제어가 필요하다. 따라서 제안된 위치정보 프라이버시 제어 프로토콜은 기존 연구에서 지원하는 단순한 위치 정보 뿐만 아니라 이용자의 동적 속성 및 보다 다양하고 세분화된 시간 속성 제어가 가능하다. 그리고 시간

과 공간속성을 결합한 속성들에 대한 제어가 가능한 장점이 있다.

5. 결론 및 향후 연구

이 논문에서는 개인의 위치정보와 관련된 프라이버시 보호에 필요한 필수 요소들을 분석하고 이를 관리하기 위한 프로토콜을 제안하였다. 그리고, 이를 기반으로 이용자가 자신의 위치정보 프라이버시와 관련된 설정을 직접 제어할 수 있는 위치정보 프라이버시 자기제어 시스템 프로토타입을 설계·구현하였다.

지금까지 위치정보 프라이버시 관리를 위한 표준화 작업들은 진행되어 왔으나 실제 프로토타입으로 제시된 사례는 없는 상황이다. 더구나 우리나라는 최근 위치정보보호법이 제정됨에 따라 개인의 위치정보 프라이버시 보호를 위한 방안마련이 시급한 상황이다. 따라서 이 논문에서 제안된 프로토콜 및 위치정보 프라이버시 자기제어 시스템의 프로토타입을 활용하여 이동통신용 위치기반 서비스 플랫폼 뿐만 아니라 텔레매틱스 서비스 시스템, T-Money 교통카드 시스템, GIS플랫폼과 같은 다양한 서비스 제공시스템에 활용될 수 있다.

참 고 문 헌

[1] J. Hightower and G. Borriello, "Location Systems for Ubiquitous Computing," *Computer*, vol.34, no.8, pp.57-66, IEEE Computer Society Press, Aug. 2001.

[2] J. S. Lee and S. K. Kim, "Technology Trends and World-wide Industry Market Analysis of Location-Based Services(LBS)," IITA, vol.5, no.2, 2003.

[3] Q. Jones et al., "Putting Systems into Place: A Qualitative Study of Design Requirements for Location-Aware Community Systems," *Proc. ACM Conf. Computer Supported Cooperative Work (CSCW 04)*, ACM Press, pp.202-211, 2004.

[4] S. H. Lee, K. W. Min, J. C. Kim, J. W. Kim, and J. H. Park, "LBS Technology Trends," *Electronics and Communication Trends Analysis*, vol.20, no.3, pp.33-42, 2005.

[5] SERI, Rasing LBS, CEO Information, vol.615, 2007.

[6] J. Warrior, E. McHenry, and K. McGee, "They Know Where You Are," *IEEE Spectrum*, vol.40 no.7, pp.20-25, 2003.

[7] J. Kwak, K. W. Lee, S. J. Kim, and D. H. Won, "RFID System based Missing Child Location Tracking System with Fairness," 5th RFID/USN Research Paper Awards, 2005.

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

[9] N. H. Lee, J. H. Park, and B. I. Ahn, "LBS Standard Reference System supporting Location-based Application Services," *Proceedings of Korea Spatial Information System Society Conference*, pp.33-38, 2004.

[10] Open Mobile Alliance, Mobile Location Service V1.1 : Privacy Checking Protocol, Open Mobile Alliance Enabler Standard, 2006.

[11] IETF Georaphic Location/Privacy Charter, Geopriv Requirements, IETF RFC Document 3693, 2004.

[12] H. Tschofenig, H. Schulzrinne, A. Newton, and J. Peterson, "The IETF Geopriv and Presence Architecture Focusing on Location Privacy," W3C Workshop on Languages for Privacy Policy Negotiation and Sematics-Driven Enforcement, October 2006.

[13] K. Tang, J. Fogarty, P. Keyani, and J. Hong, "An Anonymous and Privacy-Sensitive Approach to Collecting Sensed Data in Location-Based Applications," *Proc. SIGCHI Conf. Human Factors in Computing Systems(CHI 06)*, ACM Press, pp.93-102, 2006.

[14] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," MobiSys, pp.31-42, 2003.

[15] T. Xu and Y. Cai, "Location Anonymity in Continuous Location-based Services," ACMGIS, pp.221-238, 2007.

[16] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving User Location Privacy in Mobile Data Management Infrastructures," *Privacy Enhancing Technology Workshop*, vol.4258, pp.393-412, 2006.

[17] J. H. Kim, A. R. Lee, Y. K. Kim, J. H. Um, and J. W. Chang, "Cloaking Method supporting K-anonymity and L-diversity for Privacy Protection in Location-Based Services," *Journal of Korea Spatial Information Society*, vol.10, no.4, pp.1-10, 2008.

[18] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model," *ICDCS*, pp.620-629, 2005.

[19] M. Gruteser and X. Liu, "Protecting Privacy in Continuous Location-Tracking Applications," *IEEE Security and Privacy*, vol.2, no.2, 2004.

[20] M.F. Mokbel, C.Y. Chow, and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," *VLDB*, pp.763-774, 2006.

[21] Z. Xiao, X. Meng, and J. Xu, "Quality Aware Privacy Protection for Location-based Services," *Database Systems for Advanced Applications*, vol.4443, pp.434-446, 2007.

[22] S. Patil and J. Lai, "Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application," *Proc. SIGCHI Conf. Human Factors in Computing Systems (CHI 05)*, ACM Press, pp.101-110, 2005.

[23] D.V. Oheimb and J. Cuellar, "Designing and Verifying Core Protocols for Location Privacy,"

Proc. 9th Information Security Conf., pp.502-516, 2006.

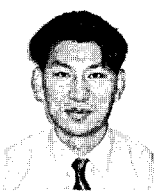
[24] A. Gupta, M. Saini, and A. Mathuria, "Security Analysis of The Louis Protocol for Location Privacy," *Proc. 1st Int. Conf. on COMmunicaiton Systems and NETworks*, pp.200-207, 2009.

[25] Q. He, D. Wu, and P. Khosla, "A Mechanism for Personal Control over Mobile Location Privacy," *BroadWISE2004*, 2004.

[26] L. Kang, "Protecting Location Privacy in Large-Scale Wireless Sensor Networks," *Proc. IEEE Int. Conf. on Communications(ICC2009)*, pp.1-6, 2009.

이 웅 재

1994년 충북대학교 컴퓨터과학과 졸업(학사). 1996년 충북대학교 전자계산학과 졸업(석사). 2005년 충북대학교 전자계산학과 졸업(박사). 2006년~현재 한국인터넷진흥원 인터넷기획팀 선임연구원. 관심분야는 이동객체데이터베이스, 위치기반서비스, 지리정보시스템, 센서네트워크, 인터넷 기술정책, 인터넷 보안 등



주 용 완

1997년 한국외국어대학교 경영학과 졸업(학사). 2002년 한국외국어대학교 경영학과 졸업(석사). 2007년 숭실대학교 컴퓨터공학과 졸업(박사). 1997년~1999년 한국정보화진흥원(구 한국전산원) 주임. 2000년~현재 한국인터넷진흥원 인터넷기반진흥단 단장. 관심분야는 인터넷 기술정책, 인터넷 보안, 공간정보시스템

남 광 우

1995년 충북대학교 전자계산학과 졸업(학사). 1997년 충북대학교 전자계산학과 졸업(석사). 2001년 충북대학교 전자계산학과 졸업(박사). 2001년~2004년 한국전자통신연구원 텔레매틱스연구단 선임연구원. 2004년~현재 군산대학교 컴퓨터정보공학과 조교수. 관심분야는 데이터베이스, GIS, LBS 정책 및 기술, 데이터스트림, 지오 센서네트워크