http://dx.doi.org/10.5392/JKCA.2015.15.02.101

위치공유기반 서비스의 프라이버시 보호 방안의 설계 방향 제시

Direction Presentation of Design on Privacy Preserving Mechanism for Location-Sharing Based Services

김미희
한경대학교 컴퓨터웹정보공학과

Mihui Kim(mhkim@hknu.ac.kr)

요약

위치공유기반 서비스(Location-sharing based service)는 사용자가 친구관계를 맺고 있는 다른 사용자와 자신의 위치정보를 공유하는 서비스를 일컫는다. 이 때, 이 위치정보는 서비스 제공자(SP, Service Provider)를 통해 공유되며, 자신의 위치정보는 서비스 제공자에게 노출되게 된다. 이로써 개인의 위치정보가 SP에게 노출되는 프라이버시 문제가 제기되어 왔고, 이를 보호하기 위한 메커니즘들이 제안되었다. 본 논문에서는 위치공유기반 서비스의 종류와 그 특징을 살펴보고, 이를 위한 프라이버시 보호 메커니즘들의 연구 동향을 조사한다. 조사된 기존 메커니즘 분석을 통해, 현 서비스에 적합한 프라이버시 메커니즘 설계 방향 및 향후 연구 방향을 제언한다.

■ 중심어 : | 위치공유기반 서비스 | 위치정보 노출 | 프라이버시 보호 | 연구동향 |

Abstract

Location-sharing based service (LSBS) refers to a service that users share their location information with other users with whom friendship. At this time, the location information is shared through service provider, and then their position information is exposed to the service provider. The exposure of this personal position information to the service provider has raised a privacy problem, and thus privacy preserving mechanisms have been proposed to protect them. In this paper, we examine the types and features of the proposed location-sharing based services so far, and survey the research trend of privacy preserving mechanisms for them. Through the analysis on existing privacy preserving mechanisms, we present design factors for a privacy preserving mechanism for the current LSBS services, and suggest future work.

■ keyword : | Location-Sharing Based Services | Location Information Exposure | Privacy Preserving | Research Trend |

I. 서 론

GPS(Global Positioning System) 등과 같이 자신의 위치정보를 측정할 수 있는 기능을 탑재한 이동 단말기 사용이 증가하면서 위치기반 서비스(Location Based Service, LBS)가 출현하였다. 이는 현재 위치정보를 활용하여 근처에 대한 정보(예, 기온)나 근처에 있는 관심있는 장소(예, 식당 등) 정보를 제공할 수 있고, 주변의 교통정보 상황을 안내해 줄 수 있다. 또한 이러한 LBS의 하나로서 위치공유기반 서비스(Location-Sharing

접수일자 : 2015년 01월 29일
수정일자 : 2015년 02월 09일
심사완료일 : 2015년 02월 10일
교신저자 : 김미희, e-mail : mhkim@hknu.ac.kr

Based Service, LSBS)가 있다. LSBS는 사용자가 친구 관계를 맺고 있는 다른 사용자와 자신의 위치정보를 공유하는 서비스이다.

대표적인 LSBS로 소셜네트워크서비스 (Social Network Service, SNS)에 기반한 페이스북(Facebook)의 체크인(check-in) 서비스가 있다[1]. 체크인을 하면 체크인 했다는 정보가 자신의 담벼락에 게시되고 친구의 뉴스피드에 자연스럽게 노출되어 공유된다. 포스퀘어(Foursquare)는 위치공유에 기반 한 SNS로 설계되었으며, 뱃지를 주고 메이어(Mayer)라는 칭호를 수여하는 등 게임요소를 제공하고 있다[2]. 국내에서는 카카오톡(KakaoTalk)과 연계하여 실시간으로 친구 위치를 지도에서 확인할 수 있는 "카카오디" 앱을 출시하였다[3]. 그러나 이러한 서비스는 소셜네트워크라는 관계 인프라를 통해 위치정보를 이용한 서비스로 쉽게 자리매김 하였지만, 개인 위치정보가 서비스 제공자(Service Provider, SP)에게 노출되어 프라이버시 문제가 제기되고, 이를 보호하기 위한 연구가 새로운 주제로 대두되었다.

기본적으로 일반적인 LSB를 위해 제공된 프라이버시 보호 메커니즘이 LSBS에 적용될 수 있을 것이다. 예를 들어, 더미 위치정보를 추가하거나[4][5], 위치정보의 정확성을 낮추는 기법[6] 등이 있다. 그러나 이러한 난독화(obfuscation) 기법들은 친구와 공유하는 정보 자체도 부정확하게 만들어 서비스 자체의 목적에 위배된다. 또한 위치정보를 암호화하여 제공[7]할 수 있으나 대부분의 LSBS 서비스들이 무료라는 점을 감안할 때 처리에 대한 부담이 될 수 있다. 이에 LSBS에 특화된 프라이버시 보호 메커니즘들[8-14]이 제시되고 있다. 초기 메커니즘들[8][9]은 특정 LSBS서비스(예, 공평하게 만남의 장소 정해주는 서비스)에 특화된 프라이버시 보호 메커니즘이 제안되었다. 한 단계 더 나아가[11]에서는 일반적인 지오소셜(geosocial) 응용에 적용가능한 메커니즘이 제안되었다. 이 메커니즘은 사용자 정보와 위치정보를 따로 저장하여 소극적인(honest-but-curious) 공격을 배제시켰다. 또한 위치정보뿐 아니라 체크인 기록, 기호정보(preference), 위치정보에 대한 2차 정보(side information)에 대한 프라이버시 보호 메커니즘들[12][13]이 제안되었다. 또한 [14]에서는 송신자 프라이버시 제공 기법(위치 암호화)과 수신자 프라이버시 제공 기법(수신자 리스트 보호), 더 나아가 위치 방문 횟수에 대한 간헐적 통계정보 제공 기법으로 나누어 단계별 메커니즘을 제안하였다. 그러나 이 메커니즘은 장소에 따른 프라이버시 수준 개인이 요구하는 프라이버시 수준에 따라 적응적으로 제공하지 못하는 한계가 있다. 이에 본 논문에서는 현 LSBS에 특징에 맞추고 위치의 프라이버시 보호 수준을 맞출 수 있는 등, 프라이버시 보호 메커니즘들이 제공해야할 요소들을 제시한다.

본 논문은 1장 서론에 이어, 2장에 LSBS와 특징을 살펴보고, 3장에 LSBS의 프라이버시 침해 공격 유형을 소개한다. 4장에 기존에 제안된 프라이버시 보호 메커니즘을 소개하고, 5장 프라이버시 보호 메커니즘의 설계 방향을 제시하며, 본 논문의 결론을 맺는다.

II. 위치공유기반 서비스와 그 특징

2009년 3월에 발표한 포스퀘어는 SNS를 활용한 위치공유기반 서비스이다[그림 1]. 이는 전세계적인 SNS인 페이스북, 트위터 그리고 국내의 카카오톡 등과 함께 많은 사용자를 확보하고 있는 SNS 서비스이다. 이러한 성공에는 친구와의 위치정보를 공유함으로써 상대가 어디서 무엇을 하는지 알고 싶어 하고, 자신을 표현하는 과시욕을 활용하였다. 또한 체크인을 통해 위치정보 제공의 보상으로 뱃지를 수여하고 메이어라는 칭호를 수여하는 등 수집욕과 소유욕을 자극하며 게임요소 등을 제공하고 있다. 이러한 위치공유기반 서비스는 사용자가 체크인이라는 능동적 공유 행위를 통해 스스로 자신의 위치를 노출하는 시스템으로서 폐쇄형 LBS를 제공한다[15]. 그러나 이 역시 서비스 제공자에게 사용자의 위치정보를 노출시키는 보안상 치명적인 문제가 내재되어 있다.

대표적 SNS인 페이스북에서도 체크인 서비스를 통해 내 친구 중에서 어디를 방문해서 어떤 이야기를 남겨놓았는지 제공하는 위치공유기반 서비스를 제공한

다. 페이스북에서는 이 체크인서비스의 활성화를 위해 미국 전역에 체크인과 연계한 무료 와이파이를 제공하고 있다[1]. 작동원리는 다음과 같다. 상점에서는 시스코에서 제공하는 프로그램을 설치하고, 가게를 방문한 사람은 와이파이 비밀번호를 물어볼 필요 없이 특정 랜딩 페이지에 접속해서 그 가게에 대한 페이스북 체크인을 하면 비밀번호를 입력하지 않아도 와이파이에 무료로 접속할 수 있다. 페이스북 체크인이 친구들의 뉴스피드에 노출되어 또 하나의 마케팅 제공방법이 될 수 있다. 페이스북 체크인도 포스퀘어와 비슷한 프라이버시 노출 문제가 있지만, 더욱이 'Tag friends with you'라는 기능으로 다른 친구의 허가 없이 친구를 같이 체크인할 수 있어 또 다른 프라이버시 문제가 내재되어 있다.

구글은 2009년 구글 래티튜드(Google Latitude)를 통해 이용자의 현재 위치정보를 친구와 공유할 수 있고, 친구의 위치정보를 구글 맵스 상에서 볼 수 있는 기능을 제공하였다[16]. 이 서비스는 실시간 위치추적서비스(Real-time locating service)를 제공하여 위치저장 논란 즉 위치정보 유출 문제가 이슈화되며 2013년 종료되었다. 대신 Google+를 통해 Google+ 내의 친구와 위치 공유하고 기록할 수 있는 체크인 기능으로 한정하였다.

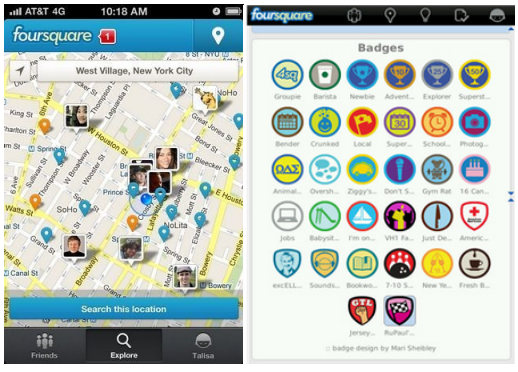

그림 1. 대표적 SNS기반 LSBS 포스퀘어

카카오톡에서도 2014년부터 친구들과 위치를 공유하여 실시간으로 친구 위치를 지도에서 확인할 수 있는 '카카오디' 앱을 출시하였다[그림 2]. 이는 카카오톡과 연계해 친구추천 기능을 통해 친구가 되면 서로 위치를 공유할 수 있는 서비스 앱이다. 기존 위치추적 어플들은 서로 친구 등록만 하면 무조건 위치가 파악돼 의도하지 않은 상황에서도 위치가 공개되어 사생활이 침해되는 경우가 있었다. 반면 카카오디는 위치확인 대상 상대방에게 'Where' 버튼을 눌러 신호를 보내면 10분 이내에 'Here' 버튼을 눌러줘야만 위치가 전송된다. 전송된 위치는 실시간으로 구글 지도를 바탕으로 네비게이션 어플과 연동해 바로 길찾기 안내를 시행할 수 있다[3]. 매번 확인을 통해 친구의 위치 확인을 할 수 있다는데 조금 더 프라이버시 보호를 제공하지만 관련 정보가 서비스제공자에게 제공된다는 문제는 여전하다.

[표 1]은 지금까지 소개한 최근 많이 사용되는 LSBS의 비교 표이다.

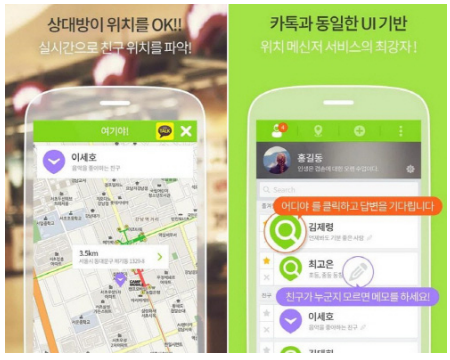

그림 2. 대표적 국내 LSBS 카카오디

표 1. 위치공유기반 서비스 비교

서비스명	특징*, 활성화 방법+, 프라이버시 문제-
포스퀘어	* 위치기반 SNS 시작, 체크인(능동적 공유행위) 통한 폐쇄적 LSBS + 뱃지/메이어 등 게임요소 - SP에게 위치정보 노출
페이스북	* 기존 SNS에 체크인이라는 LBS 추가 + 체크인과 무료 와이파이 서비스 연계 - SP에게 위치정보 노출, 친구 동의 없이 함께 체크인 가능
구글	* 실시간 위치추적 가능한 구글 래티튜드로 시작, 프라이버시 문제로 Google+ 체크인(폐쇄형 LSBS)로 전환 - SP에게 위치정보 노출
카카오디	* 기존 카카오톡 SNS 기반 LSBS, 매번 상대방 확인버튼 통해 위치 공유 - 강화된 위치 공유 제공하지만, 역시 SP에게 위치정보 노출

III. LSBS의 프라이버시 침해 공격 유형

기 소개된 LSBS들은 소셜(social)을 강화한 또는 기반한 위치기반서비스로 소셜 플랫폼을 기반으로 전 산업 영역에 활용 가능한 스마트 LBS로 진화하고 있다. 이에 LSBS는 많은 사용자들에게 널리 사용되는 이면에 그 사용자들의 위치정보가 SP에게 노출되는 문제가 있다. 이러한 위치정보의 노출로 인해 가해질 수 있는 공격 유형을 정보 흐름 주기로 나누어 보면 다음과 같다[17].

- 수집단계: 위치정보의 부적절한 접근 및 수집
- 이용 및 제공단계: 악의적인 위치정보 분석, 부적절한 위치정보의 제공, 원하지 않는 마케팅 수단 활용
- 보관 및 파기 단계: 부적절한 저장, 개인정보와 위치정보의 노출, 관리기간 이후 저장, 부적절한 위치정보 파기

이러한 공격은 결론적으로 위치정보의 부적절한 활용으로 요약될 수 있고, 더 나아가 위치정보로부터 얻을 수 있는 추가정보(side information)의 노출, 예를 들어 개인의 생활패턴 분석 등에 의해 물리적 침해 및 공격(예, 외출 시 주거 침입 및 절도)으로 이어질 수 있어 그 어떤 공격보다 위협정도가 크다고 할 수 있다.

정도에 따른 공격유형으로 나누어 보면, 적극적 공격과 소극적 공격으로 나누어 볼 수 있다. 그러나 대부분 방어 메커니즘들은 소극적 공격을 가정하여 제안되었다[12][13].

- 적극적 공격: 타 사용자의 위치정보를 알아내기 위해 SP 서버 공격, 또는 타 사용자의 위치를 알기위해 협업공격
- 소극적 공격: SP든 사용자든 각자의 역할을 충실히 하지만 타사용자의 위치정보에 관심을 갖는 honest-but-curious 공격자, SP 경우 상업적 목적, 사용자는 타사용자의 기호 정보를 알기를 원해 공격

표 2. LSBS를 위한 최신 프라이버시 보호 메커니즘의 비교

메커니즘	특징*, 방법+ 가정공격@, 단점-
만남장소를 정하는 서비스를 위한 프라이버시 보호 메커니즘[8]	* LSBS를 위한 초창기 프라이버시 보호 메커니즘 + BGN, ElGamal, Paillier 공개키 암호를 이용하여 SP나 다른 사용자들에게 위치정보를 노출시키지 않으면서도 SP가 공평하게 만남의 장소(Fair Rendez-Vous Point, FRVP)를 계산할 수 있도록 메커니즘을 설계 @ 적극적 공격(가짜 사용자에 의한 공격, replay 공격, 협업공격), 소극적 공격(honest-but-curious) 모두 가정 - 특정 서비스에 국한됨
지오소셜 응용의 프라이버시 보호 메커니즘[11]	* 일반적인 지오소셜 응용에 적용 가능하도록 고안 + 사용자정보와 위치정보를 따로 저장하여 상호 링크되는 엔터티가 없도록 하고, 응용에서 저장된 데이터를 사용할 때 허가된 접근만 가능하도록 함 @ 소극적 공격(honest-but-curious)만 가정 - 협업 공격, 트래킹(tracking) 공격 등 적극적 공격을 배제
LBSN에서 사용자 위치와 체크인 기록도 보호하는 프레임워크[12]	* 자주 방문하는 곳을 찾을 때 빠른 검색이 가능하고, 단말에 계산부하가 심하지 않으며, 친구 그룹이 변경되어도 적용이 가능한 프라이버시 보호 프레임워크 제안 - 빠른 검색을 위해 새로운 인덱스 구조 사용하고, 복잡한 암호계산은 서버활용하며, 폐지된 친구나 새로운 친구 등 친구그룹 변화에 간단한 계산이 적용 @ 소극적 공격(honest-but-curious)만 가정 - 서버 모니터링 공격(공격자가 오랫동안 시스템의 DB 상황을 모니터링하면 체크인 기록 증가 알 수 있음)에 취약
MSN을 위한 Privacy-preserving framework [13]	* 사용자 기호정보(preference), 아이디(identity), 위치정보 보호 + 기호정보 보호를 위해 k-Anonymity와 l-Diversity 성질을 만족하는 Privacy-preserving request aggregation protocol을 제안하고, 아이디와 위치정보 보호를 위해 unlinkable pseudo-ID 기법을 제안 @ 소극적 공격(honest-but-curious)만 가정 - 적극적 공격을 배제
LSBS를 위한 실용적인 프라이버시 보호 메커니즘[14]	* 위치정보만 보호하는 메커니즘(IBBE), 위치정보와 수신자리스트 정보도 보호하는 메커니즘(Anonymous IBBE), 실용성을 높이기 위해 SP에게 통계정보를 제공할 수 있는 확장버전 제안 + IBBE를 위해 Bilinear map이 사용되었고, Anonymous IBBE를 위해 identity기반 암호화기법이 적용되어 위치정보 뿐 아니라 수신자 리스트 모두 암호화하여 서비스 제공자에게 전달하면 이를 모든 사용자에게 포워딩하고 해당 그룹에 포함된 사용자만 위치정보를 복호화 가능, 실용화 확장버전을 위해 P-commitment를 적용 @ 적극적 공격(협업공격), 소극적 공격(honest-but-curious) 모두 가정 - 암복호화를 위한 런타임이 그룹수에 지수적으로 증가

IV. LSBS의 프라이버시 보호 메커니즘

위치공유기반 서비스의 프라이버시 보호를 위해 일반적인 LBS의 프라이버시 보호 메커니즘을 생각할 수도 있다. 예를 들어, Pseudonymity Mix-zones[18], Spatial cloaking k-anonymity[6], Noise based solutions[19], Cryptographic protocols[20] 등이 있다. Pseudonymity Mix-zones[18]은 가명을 씀으로 해서 제시된 존 영역에 타 사용자가 입출입 하더라도 그 연관성을 찾을 수 없게 하는 메커니즘이다. Spatial cloaking k-anonymity[6]는 사용자 근처의 k명 사용자가 포함된 위치영역 정보를 제공함으로써 개인의 위치정보를 보호하는 메커니즘이다. Noise based solutions[19]는 위치정보의 정확도를 떨어뜨려 제공함으로써 정확한 위치정보를 보호하는 메커니즘이다. 마지막으로 Cryptographic protocols[20]는 위치정보를 암호화하여 제공함으로써 서비스 제공자 및 제 3자가 해당 정보를 알 수 없게 하는 메커니즘이다. 그러나 이 모든 메커니즘들은 친구와 위치정보를 공유한다는 측면에서 그 정확도가 떨어진다면 해당 서비스의 목적에 위배되어 사용할 수 없게 된다. 또한 암호화하는 경우에도 복호화해야 하는 복잡한 프로세스를 서비스 제공자에게 부담시킨다면 대부분 무료로 제공하는 비즈니스 모델상 상충이 되며, 순수히 위치정보를 모두 노출시키지 않는다면 그 정보를 활용하여 이익을 내는 서비스 제공자 입장으로 보면 이익 창출의 패러다임을 막게 한다. 이에 기존 LBS를 위한 프라이버시 보호 메커니즘은 LSBS에 그대로 사용할 수 없다는 결론이다.

2009년 LSBS의 서비스가 출현하면서 2011년 이에 대한 프라이버시 보호 메커니즘 연구 결과가 나오기 시작했다[8]. 공평한 만남장소(Fair Rendez-Vous Point, FRVP)를 정하는 서비스에 국한하여 두 프라이버시 보호 메커니즘(Boneh-Goh-Nissim 공개키 암호이용, ElGamal과 Paillier 공개키 암호이용)을 제안하였다. 이들 암호화 알고리즘의 multiplicative/additive homomorphic 특성을 이용하여 암호화를 하여 SP나 다른 사용자들에게 위치정보를 노출시키지 않으면서도 SP가 공평하게 만남의 장소를 계산할 수 있도록 메커니즘을 설계하였다. 이로써 가짜 사용자를 만들어 공격하거나 replay 공격, 협업공격 등 적극적 공격과 honest-but-curious 공격자에 의한 소극적 공격 모두에 안전함을 보이고 복잡도를 비교하였으며, 구현을 통해 처리 성능을 보였다. 이 외에도 초창기 LSBS 프라이버시 메커니즘들은 특정 서비스(예, 특정 거리 내 상대방 존재여부를 판단[9], 같은 관심사(interest)를 갖고 있는 사람들이 근처에 있는지 판단[10])에 국한하여 위치정보 또는 개인정보를 노출시키지 않는 연구가 진행되었다. 이러한 결과들은 일반적인 LSBS에 적용하기 어려움 단점이 있다.

이러한 단점을 보완하고자 일반적인 지오소셜 응용에 적용 가능하도록 고안된 프라이버시 보호 메커니즘이 제안되었다[11]. 이 메커니즘은 사용자정보와 위치정보를 따로 저장하여 상호 링크되는 엔터티가 없도록 하고, 응용에서 저장된 데이터를 사용할 때 허가된 접근만 가능하도록 하였다. 그러나 협업 공격, 트래킹(tracking) 공격 등 적극적 공격을 배제한 체, 소극적 공격(honest-but-curious)만 가정하여 프라이버시 보호 메커니즘을 제공한다.

[12]에서는 위치기반 소셜 네트워크(Location based Social Network)에서 사용자 위치와 함께 체크인 기록도 보호하는 프레임워크를 제안하였다. 특히 자주 방문하는 곳을 검색 시 빠른 검색이 가능하도록 새로운 인덱스 구조를 사용하였고, 복잡한 암호계산은 서버를 활용하여 단말의 계산부하를 줄였다. 또한 소셜 그룹은 새로운 친구 등록이나 기존 친구 폐지에 의해 그룹 변화가 잦을 수 있으므로 그런 경우에도 간단한 계산으로 새로운 그룹에 적용이 가능한 프라이버시 보호 프레임워크이다. 그러나 이 메커니즘에서도 소극적 공격(honest-but-curious)만 가정하였고, 서버 모니터링 공격, 즉 공격자가 오랫동안 시스템의 DB 상황을 모니터링하면 체크인 기록 증가를 알 수 있다는 취약점이 존재한다.

[13]에서는 이동 소셜 네트워크(MSN, Mobile Social Network)에서 프라이버시 보호를 위해 PLAM(Privacy-preserving framework for Local-Area Mobile social networks)이라는 프레임워크를 제안하였다. 사용자 기

호정보 보호 (User preference privacy)를 위해 k-Anonymity와 l-Diversity 성질을 만족하는 프라이버시 보호 요청 통합 프로토콜을 제안하였다. 여기에서 사용자 기호정보란, 예를 들어 한 사용자가 병원에 있다는 위치정보를 제공하면 이로부터 '건강상 문제가 있다'라는 사용자 기호정보가 함께 제공된다. 이러한 사이드 정보를 보호하기 위한 프로토콜이고 이는 별도의 신뢰성 있는 익명성 서버 없이 설계되었다. 또한, ID보호(identity privacy)와 위치보호(location privacy)를 위해 unlinkable pseudo-ID 기법을 적용하였다. 그러나 이 연구에서도 적극적 공격은 배제하였다.

또한 실용적인 LSBS 프라이버시 보호 메커니즘(PPPM; Practical Privacy-Preserving Mechanism)이 제안되었다[14]. 이 메커니즘은 크게 3개의 기법으로 나뉜다. 첫째, Identity based broadcast encryption (IBBE)으로 송신자의 위치정보를 보호하는 기법이다. 즉 이 기법은 서비스 제공자에게 위치정보를 암호화하여 제공하면 이를 중계하여 수신자리스트에 있는 사용자에게 전달하므로 서비스 제공자에게 위치정보 노출을 막는 기법이다. 둘째, Anonymous IBBE로 위치정보뿐 아니라 수신자 리스트 모두 암호화하여 서비스 제공자에게 전달하면 이를 모든 사용자에게 포워딩한다. 이때 이를 수신한 사용자 중 수신자리스트에 포함된 사용자는 자신의 키로 해당 내용을 복호화 하여 볼 수 있게 된다. 셋째, 서비스 제공자의 이익 창출을 위해 사용자의 위치방문 정보에 대한 통합된 통계정보를 제공하기 위한 확장 기법이다. 그러나 이 메커니즘들은 암복호화를 위한 런타임이 그룹 수에 지수적으로 증가한다는 단점이 있다. [표 2]는 지금까지 소개한 LSBS를 위한 최신 프라이버시 보호 메커니즘의 비교 표이다.

지금까지 제안된 메커니즘들은 장소에 따른 프라이버시 수준이나 개인이 요구하는 프라이버시 수준에 따라 적응적으로 제공하지 못하는 등의 한계가 있다. 이에 본 논문에서는 현 LSBS에 특징에 맞추고, 앞으로의 LSBS 프라이버시 보호 메커니즘들이 갖추어야 한 설계 요소들을 소개한다.

V. LSBS 프라이버시 보호 메커니즘의 설계 방향 및 결론

지금까지의 LSBS의 서비스 특징 및 공격유형 분석, 기 제안된 프라이버시 보호 메커니즘을 소개하였다. 본 장에서는 현재 LSBS를 위한 프라이버시 보호 메커니즘의 설계 방향을 제언한다.

첫째, 서비스 사용자들은 자신이 요구하는 프라이버시 보호 수준이 다르다. 사용자가 요구하는 수준별 프라이버시 보호 메커니즘이 제공되어야 하며, 그 설정은 누구나 이해하고 설정하기 쉬워야 한다.

둘째, 장소와 시간에 따라 사람이 모이는 정도와 프라이버시 노출 문제의 정도가 다르다. 장소와 시간에 따라 프라이버시 노출 민감도에 따라 프라이버시 제공 정도를 조절할 수 있는 메커니즘이 필요하다.

셋째, 서비스 제공자는 간단한 프로세스가 요구되어야 하며, 서비스 제공자에게 이익을 창출할 수 있도록 프라이버시를 침해하지 않는 범위에서 사용자들의 장소 방문에 대한 통계정보를 제공받을 수 있어야 한다.

넷째, 적용되는 암호학적 기술들이 오버헤드가 커서는 안 된다. 즉, 통신, 계산, 저장, 사용에너지 등에 대한 오버헤드를 고려하여 설계해야 한다. 특히 사용자들이 사용하는 이동 단말의 하드웨어 스펙을 고려하여 적정한 오버헤드 내에서 메커니즘이 설계되어야 한다.

다섯째, 제안되는 메커니즘은 실용성을 가져야 하며, 사용자의 실제 위치정보 데이터로 실험되어 그 성능이 입증되어 실용성 보장을 보여야 한다.

여섯째, 그룹 변화 시 지속적으로 적용 가능한 프라이버시 보호 메커니즘이 제공되어야 한다. 한 사용자의 그룹에 새로운 친구가 추가되는 경우, 그 친구는 해당 사용자의 과거 위치정보도 모두 볼 수 있어야 하며, 친구가 탈퇴한 경우 해당 과거 정보 및 새로운 위치정보가 노출되어서는 안 된다. 또한 이로 인한 처리 오버헤드가 작아야 한다.

일곱째, 그룹의 사이즈에 따라 오버헤드 증가가 크지 않아야 한다. 2014년 미국에서 조사된 페이스북의 평균 친구 수는 350명으로 조사되었고, 18-24살의 평균 수는 649명이나 된다[21]. 큰 그룹이여도 그 계산 및 저장, 통

신 오버헤드가 크지 않도록 설계해야 한다.

여덟째, 소극적 공격뿐 아니라 협업 공격, 트랙킹 공격 등 적극적 공격을 고려하여 프라이버시 보호 메커니즘을 설계해야 한다.

본 논문에서는 지금까지 제안된 위치공유기반 서비스의 종류와 그 특징을 살펴보고, 이를 위한 프라이버시 보호 메커니즘들의 연구 동향을 조사하였다. 조사된 기존 메커니즘 분석을 통해, 현 서비스에 적합한 프라이버시 메커니즘 설계 방향 및 향후 연구 방향을 제언하였다. 이를 통해 안전한 위치정보 공유가 가능한 LSBS 서비스가 가능해 질 것이다.

참 고 문 헌

[1] 페이스북 체크인하면 무료 와이파이 이용한다, http://mushman.co.kr/m/post/2692019

[2] 소셜위치기반 서비스 포스퀘어(Foursquare), http://cafe.naver.com/koreahrdacademy/1971

[3] 스마트폰용 위치공유 앱 '카카오디' 출시, http://www.asiatoday.co.kr/view.php?key=20141224010014442

[4] A. Lewko, A. Sahai, and B. Waters, "Revocation systems with very small private keys," IEEE Security and Privacy (SP) Symposium, pp.273-285, 2010.

[5] B. Libert, K.Paterson, and E. Quaglia, "Anonymous broadcast encryption: adaptive security and effcient constructions in the standard model," Public Key Cryptography, pp.206-224, 2012.

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

[7] C. Dong and N. Dulay. "Longitude: A privacy-preserving location sharing protocol for mobile applications," Trust Management of IFIP Advances in Information and Communication Technology, Vol.358 pp.133-148, Springer Berlin Heidelberg, 2011.

[8] I. Bilogrevic, M.Jadliwala, K. Kalkan, J. Hubaux, and I. Aad, "Privacy in Mobile Computing for Location-Sharing-Based Services," Privacy Enhancing Technologies, Lecture Notes in Computer Science, Vol.6794, pp.77-96, 2011.

[9] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location Privacy via Private Proximity Testing," NDSS, 2011.

[10] E. D. Cristofaro, A. Durussel, and I. Aad, "Reclaiming Privacy for Smartphone Applications," PerCom, 2011.

[11] S. Pidcock and U. Hengartner, "Zerosquare: A Privacy-Friendly Location Hub for Geosocial Applications," IEEE CS Security and Privacy Workshop, 2013(5).

[12] X. Zhao, L. Li, and G. Xue, "Checking in without worries: Location privacy in location based social networks," IEEE INFOCOM, pp.3003-3011, 2013(4).

[13] R. Lu, X. Lin, Z. Shi, and J. Shao, "PLAM: A privacy-preserving framework for local-area mobile social networks," IEEE INFOCOM, pp.763-771, 2014(4-5).

[14] M. Herrmann, A. Rial, C. Diaz, and B. Preneel, "Practical privacy-preserving location-sharing based services with aggregate statistics," ACM WiSec, pp.87-98, 2014(7).

[15] 임홍택, *포스퀘어 스토리: 쇼셜미디어를 넘어 위치기반 플랫폼으로*, e비즈북스, 2011.

[16] 구글, 친구 위치정보 서비스 '래티튜드' 발표, http://www.zdnet.co.kr/news/news_view.asp?artice_id=20090205090146&type=det

[17] 오수현, 곽진, "위치기반 서비스의 프라이버시 위협 요소 분석 및 보안 대책에 관한 연구", 한국항행학회논문지, 제13권, 제2호, 통권 제35호,

pp.272-279, 2009.

[18] A. R. Beresford and F. Stajano, “Mix Zones: User Privacy in Location-aware Services,” PERCOMW, 2004.

[19] J. Krumm, “Inference attacks on location tracks,” Pervasive Computing, LNCS, Vol.4480, pp.127-143, 2007.

[20] K. P. N. Puttaswamy, S. Wang, T. Steinbauer, D. Agrawal, A. Abbadi, C. Kruegel, and B. Y. Zhao, “Preserving location privacy in geosocial applications,” IEEE Transactions on Mobile Computing, Vol.13, No.1, pp.159-173, 2014(1).

[21] Average number of Facebook friends of U.S. users in 2014, http://www.statista.com/statistics/232499/americans-who-use-social-networking-sites-several-times-per-day/

저 자 소 개

김 미 희(Mihui Kim) 정회원

- 1997년 2월 : 이화여대 전자계산학과(공학사)
- 1999년 2월 : 이화여대 컴퓨터학과(공학석사)
- 1999년 ~ 2003년 : 한국전자통신연구원 연구원
- 2007년 2월 : 이화여대 컴퓨터학과(공학박사)
- 2007년 ~ 2009년 : 이화여대 컴퓨터학과 전임강사
- 2009년 ~ 2010년 : 노스캐롤라이나주립대학교 연구원
- 2011년 3월 ~ 현재 : 한경대학교 컴퓨터웹정보공학과 교수

<관심분야> : 네트워크 성능 분석 및 보안, 무선네트워크 보안, 침입대응