스마트 더미를 이용한 위치기반서비스(LBS)의 익명성 보장 방법

임현수†, 조은애†, 문창주††, 박대하†††, 백두권†
† 고려대학교 컴퓨터학과
†† 건국대학교 컴퓨터응용과학부
††† 한국디지털대학교 디지털정보학과
{fribirdz, eacho99, baikdk }software.korea.ac.kr, cjmoon@kku.ac.kr, summer69@kdu.edu

Anonymous Ensure Method for Location-Based Service using Smart Dummy

Im Hyun-Soo†, Cho Eun-Ae†, Moon Chang-Joo††, Park Dae-Ha†††, Baik Doo-Kwon†
† Dept. of Computer Science and Engineering, Korea University
†† Dept. of Computer Science, Konkuk University
††† Dept. of Computer and Information Science, Korea Digital University

요 약

개인정보의 유출을 방지하는 것은 유비쿼터스 컴퓨팅 서비스의 주요 이슈중 하나이다. 대표적인 유비쿼터스 서비스인 위치기반 서비스(LBS)는 개인의 위치 정보를 바탕으로 서비스를 제공한다. 이런 개인의 위치 정보는 개인 정보와 밀접한 연관이 있기 때문에, 개인의 위치 정보 노출을 방지하는 것은 위치 기반 서비스의 필수 과제이다. 본 논문에서는 서비스 업체가 개인의 위치 정보를 파악 또는 추적하는 것을 방지하기 위해 개인의 실제 이동경로와 거짓 이동경로를 함께 보내는 알고리즘을 제안한다. 기존의 알고리즘은 이러한 거짓 이동경로를 단순한 랜덤 값을 기반으로 생성했기 때문에 서비스 제공자가 실제 사용자의 이동경로와 거짓 이동경로를 쉽게 구별할 수 있었다. 본 논문에서는 거짓 이동경로를 다른 사용자의 이동경로와 GIS 정보를 바탕으로 생성하는 알고리즘을 제안한다. 본 논문에서 제안하는 알고리즘은 실제 사용자와 비슷한 이동경로를 갖는 거짓 이동경로를 생성하기 때문에 익명성을 향상시킬 수 있다.

1. 서론

유비쿼터스 컴퓨팅 환경은 시간, 장소, 기기에 구애받지 않고 컴퓨터와 네트워크에 항상 접속할 수 있는 환경을 제공한다[1]. 유비쿼터스 컴퓨팅의 이런 특성은 사용자에게 다양한 서비스와 편리함을 제공해주지만, 이로 인해 개인정보의 침해가 심각한 문제점으로 발생하게 된다[2].

위치기반 서비스(LBS)는 유비쿼터스 컴퓨팅의 대표적인 서비스이다. GPS와 같은 위치감지 기기들로부터 얻어진 위치 정보에 기반을 두어 CMU의 Aura Project, 투어 가이드 서비스, 주변 지역 정보와 같은 다양한 서비스들이 제공되고 있다[3]. 그런데 사용자의 위치 정보는 사용자에 대한 민감한 개인 정보를 포함하고 있다. 따라서 사용자의 위치 정보가 외부에 노출될 때에는 보안과 프라이버시에 대한 문제가 발생할 수 있다[4]. 사용자는 특정 업체의 LBS를 이용하더라도 사용자 자신의 신분을 드러내지 않거나, 서비스 제공자가 사용자의 이동경로를 추적, 저장하는 것을 원하지 않을 수 있다.

본 논문에서는 LBS를 이용할 때 발생할 수 있는 개인 정보의 유출을 막기 위해 사용자의 익명성을 보장하는 방법을 제안한다. 본 논문에서 제안하는 스마트 더미 방법은 서비스 제공자가 개인의 위치 정보를 파악 또는 추적하는 것을 방지하기 위해 개인의 실제 이동경로와 거짓 이동경로를 함께 보낸다. 기존의 더미 방법은 이러한 거짓 이동경로를 단순한 랜덤 값을 기반으로 생성했기 때문에 서비스 제공자가 실제 사용자의 이동경로와 거짓 이동경로를 쉽게 구별할 수 있었다. 본 논문에서는 거짓 이동경로를 다른 사용자의 이동경로와 GIS 정보를 바탕으로 생성하는 모델과 알고리즘 제안한다. 본 논문에서 제안하는 스마트 더미는 실제 사용자와 비슷한 이동경로를 갖는 거짓 이동경로를 생성하기 때문에 익명성을 향상시킬 수 있다.

2장에서는 LBS의 개인정보 보호를 위한 기존 연구에 대해 살펴본다. 3장에서는 본 논문에서 제안하는 스마트 더미에 대해 설명한다. 4장에서 결론 및 향후 과제에 대해 기술한다.

2. 관련연구

위치기반 서비스에서 개인 정보유출을 방지하기 위한 연구들은 크게 세 가지 분야로 나뉜다[5]. 첫째, 송수신되는 메시지들을 암호화해서 메시지를 암호화하는 연구이다. 둘째, 사용자가 개인 정보제공에 대한 정책을 결정하는 연구이다. 셋째, 사용자의 익명성 보장에 관한 연구이다. 본 논문에서는 익명성 보장에 관해 논한다. 익명성 보장에 대한 연구들은 서비스 제공자가 사용자의 신분을 확인할 수 없거나, 사용자의 이동경로를 추적 또는 저장하는 것을 막기 위해 익명성을 제공한다.

2-1. 더미를 사용한 익명성 보장 방법

더미(dummy)를 사용한 익명성 보장 방법[6]은 익명성을 제공하기 위한 대표적인 방법의 하나이다. LBS를 이용하기 위해서 사용자는 서비스 제공자에게 자신의 위치 정보를 제공해야 한다. 더미 방법은 사용자가 서비스 제공자에 서비스를 요청할 때 사용자의 실제 위치 정보와 N개의 거짓 위치 정보들을 함께 전송해서 서비스 제공자가 사용자의 실제 위치를 알 수 없도록 하는 방법이다.

이 방법에서 더미의 이동경로는 랜덤 함수를 이용해 결정한다. 즉, 더미의 다음 위치는 더미의 현재 위치에 일정 범위 내의 임의의 값을 더해서 결정한다. 보완된 더미 이동경로 생성 방법은 이렇게 생성된 더미가 너무 밀집되어 있으면 임의의 값을 다시 생성

함으로써 더미의 분포를 고르게 한다.

2-2. Mix Zone Model

Mix Zone Model[7]은 서비스 제공자가 사용자의 이동경로를 추적하는 것을 막기 위해 사용자들의 신분을 서로 뒤바꾸는 방법이다. 서비스 제공자들이 접근하는 영역을 Application Zone이라고 정의하고, 서비스 제공자들이 접근하지 않는 영역을 Mix Zone이라고 정의한다. 2명 이상의 사용자들이 Mix Zone에 들어오면 사용자들의 신분을 서로 섞어서 추적을 방지한다.

3. 스마트 더미

기존의 더미 방법은 더미의 이동경로를 적은 연산으로 생성하는 잠점이 있다. 더미의 생성과 관리는 적은 자원량을 가진 Low-Computing기기인 사용자의 모바일 기기에서 이루어진다. 따라서 연산 부하가 적을수록 유리하다. 하지만, 더미의 이동경로가 단지 랜덤 함수에 의해 만들어지므로 실제 사용자의 이동경로와는 다른 단순하거나 잘못된 움직임을 보일 수 있다. 예를 들어 일방통행로인 도로를 반대로 이동하거나, 유턴할 수 없는 지역에서 유턴을 한다거나, 빌딩이나, 강, 숲을 가로질러 가는 등의 행동을 한다면 서비스 제공자는 실제 사용자와 더미를 쉽게 판별할 수 있다. 또한, 사용자는 더미의 위치 정보와 결과값도 주고 받기 때문에 불필요한 전송량이 증가한다. 현재 무선 네트워크 환경은 유선 네트워크 환경보다 안전성, 대역폭이 떨어지기 때문에 이런 점은 사용자의 원활한 서비스를 저해하게 된다.

본 논문에서는 기존의 더미 기법에서 발생할 수 있는 이런 문제점을 해결할 수 있는 새로운 더미 기법을 제안하고, 이렇게 생성된 더미를 스마트 더미(Smart Dummy)라고 명명했다.

스마트 더미는 사용자와 서비스 제공자 사이에 에이전트를 두고, 더미의 생성과 관리를 에이전트에서 수행한다. 에이전트는 High-Computing 기기이며, 다수의 사용자과 서비스 제공자 사이에 위치한다. 따라서 사용자들의 이동경로와 지리 정보를 사용해서 복잡한 연산을 사용해 더미를 생성하고 관리할 수 있다. 스마트 더미는 실제 사용자들의 이동경로를 사용하여 더미의 이동경로를 생성한다. 따라서 실제 사용자의 이동경로와 유사한 움직임을 갖는 더미를 제공함으로써 익명성을 보장한다.

사용자와 에이전트는 실제 위치정보와 결과값만 주고 받는다. 더미 위치 정보와 결과값은 에이전트와 서비스 제공자 사이에서만 전달된다. 에이전트와 서비스 제공자 간의 환경은 유선 유선 인터넷 환경이므로 대역폭에 대한 부담을 덜게 된다.

<그림 1>은 기존의 더미 방법과 스마트 더미 방법을 비교한 것이다. u는 사용자의 Unique ID이며, L_x는 위치 정보를 나타내는 좌표값이다. 서비스 제공자는 이 중 어떤 위치 정보가 실제 사용자의 것인지 알 수 없기 때문에, 수신된 모든 위치 정보에 대한 서비스를 제공하게 된다. 예를 들어 사용자 주변의 주유소를 알려주는 서비스라면, 서비스 제공자는 사용자로부터 수신된 L_1, L_2, L_3 세 곳의 주변의 주유소에 대한 정보를 전달한다.

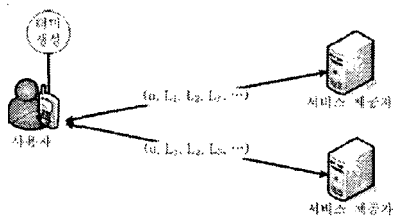
3.1. 스마트 모델 흐름도

본 논문에서 제안하는 스마트 더미의 서비스 흐름은 <그림 3>와 같다.

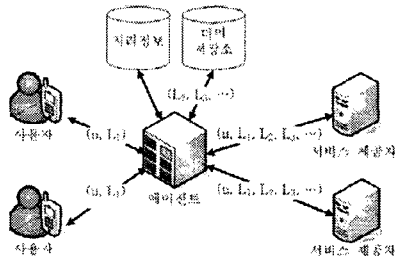
(1) 사용자는 서비스 제공자에 직접 정보를 요청하는 대신, 에이전트에게 정보 요청을 하고, 자신의 위치 정보를 보낸다.

(2) 사용자가 해당 서비스를 처음 사용한다면, 에이전트는 더미 저장소에서 더미를 하나 선택한다.

(3) 더미 저장소에서 적절한 더미를 제공하고, 사용자에게 할당



<그림 1> 기존의 더미 방법



<그림 2> 스마트 더미 방법

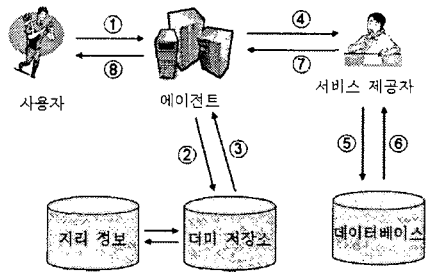
한다. 남아 있는 더미가 없다면 더미를 새로 생성한다.

(4) 에이전트는 사용자의 실제 위치와 사용자에게 할당된 N개의 더미의 위치에 대한 정보를 서비스 제공자에게 전송한다.

(5),(6) 서비스 제공자는 에이전트가 보낸 N+1개의 위치에 대한 정보를 데이터베이스에서 모두 검색한다.

(7) 모든 결과값을 에이전트로 전송한다.

(8) 에이전트는 거짓 위치 정보에 대한 결과값을 버리고, 사용자에게 사용자의 실제 위치에 대한 결과값만 전달한다.



<그림 3> 스마트 더미 모델

3.2. 스마트 더미 생성 알고리즘

스마트 더미는 다른 사용자들의 과거의 이동경로들과 지리 정보를 사용해서 생성된다. 에이전트는 다수의 사용자와 다수의 서비스 업체와 정보를 주고 받는다. Mix Zone Model[7]의 사용자들의 신분을 뒤섞어서 추적을 막는다는 개념에서 착안하여, 사용자들의 이동경로들을 연결해서 새로운 더미의 이동경로를 생성한다. 이런 알고리즘을 사용하면 적은 연산으로 실제 사람의 이동경로와 유사한 이동경로를 만들 수 있다.

에이전트는 사용자들의 신분을 제외한 이동경로만을 저장해둔다. 주기적으로 더미 생성 알고리즘을 통해 더미를 생성한다. 더미를 생성하는 슈도코드는 <그림 4>와 같다. 저장된 사용자들의 이동경로중 임의의 이동경로를 하나 추출하여 스마트 더미의 이동경로의 시작점으로 사용한다. 이 이동경로를 순서대로 따라가며, 다

른 사용자들의 이동경로와 겹치거나 근접하는 지점이 있는지를 조사한다. 만일 그러한 지점이 있다면 발견한 사용자의 이동경로를 스마트 더미의 이동경로로 연결한다. 그리고 발견한 사용자의 이동경로를 다시 하나씩 따라가며, 또 다른 사용자들의 이동경로와 겹치는지를 조사한다. 더미가 가질 최대 노드 수에 접하거나, 더 이상 이동경로가 존재하지 않을 때까지 이를 반복한다.

```
#define NB_RANGE 50 // 주변으로 인정할 범위
#define MAX_NODE 100 // 더미가 가질 최대 노드 수

CDummy CreateDummy(){
  // 저장된 사용자들의 이동경로중 하나를 얻고, 시작 경로로 사용한다.
  CUser currUser, nextUser;
  CDummy dummy = new CDummy;
  currUser = GetUser();

  while( currUser.GetNextNode() == null or
Dummy.Size() >= MAX_NODE ){
    dummy.insertNode(currUser.GetCurrentNode());

    // 다른 사용자의 이동경로의 좌표값들 중에 인접한 것이 있는지 순차적
으로 검색한다.
    while( nextUser = Search(dummy.GetCurrentNode())
{
      if(node != NULL) {
        // 발견했으면 새롭게 발견한 사용자의 이동경로를 사용한다. 새
로운 사용자의 이동경로의 시작점은 이전 사용자와 인접한 지점이다.
        ChangeUser(nextUser);
      }else{
        // 인접한 것이 없다면, 다음 이동경로의 좌표값을 검색한다.
        dummy.insertNode(currUser.GetNextNode());
      }
    }
  }

  return dummy;
}

// 다른 유저들의 이동경로를 순차적으로 검색한다. 주어진 좌표와 일치하거
나 지정 범위(NB_RANGE) 안에 있는 위치를 검색한다.
CDummy Search(CNode Node);

// 현재 참조하는 사용자의 이동경로를 폐기하고, 새롭게 발견한 사용자의 이
동경로를 사용한다.
void ChangeUser(CUser NewUser);
```

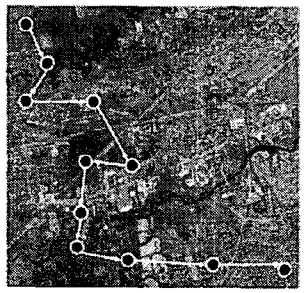
<그림 4> 스마트 더미 생성 알고리즘

<그림 5>는 세 명의 사용자들의 각기 다른 이동경로이고, <그림 6>는 이를 바탕으로 만들어진 스마트 더미의 이동경로이다.

3.3. 스마트 더미 사용 정책

스마트 더미를 생성할 때는 다른 사용자들의 이동경로를 사용한다. 이때 사용자들의 신분은 포함되어 있지 않더라도, 이동경로 자체만으로도 개인정보의 유출이 발생할 수 있다. 이를 방지하고, 익명성도 유지하기 위해서 스마트 더미의 생성과 관리에 대한 몇 가지 정책을 세워야 한다. 아래에 나오는 날짜의 범위나 횟수는 서비스의 특징이나 관련 환경에 따라 적절히 수정될 수 있다.

<그림 5> 사용자들의 이동경로



<그림 6> 스마트 더미의 이동경로

더미의 생성 : 생성을 위해 수집된 사용자의 이동 경로는 수집된지 1주일이 지난 후부터 사용할 수 있다.

더미의 사용 : 스마트 더미는 동일한 서비스 업체에 1회 이상 사용되지 않는다.

더미의 삭제 : 모든 서비스 업체에 사용되었거나, 총 20회 이상 사용된 더미 또는 4주 이상 보유된 더미는 삭제한다.

4. 결과 및 향후 과제

본 논문에서는 LBS의 익명성을 보장하기 위해 실제 사용자와 비슷한 이동경로를 갖는 스마트 더미 모델을 제안했다. 기존의 방법에서 만들어진 더미들은 랜덤 함수에 의해 만들어진 단순한 움직임을 본 논문에서 제안한 알고리즘으로 생성된 더미들은 실제 사용자와 유사한 움직임을 보인다. 따라서 사용자와 더미들의 움직임을 구별해내기 어렵기 때문에 익명성을 향상시킬 수 있다.

또한, 사용자의 모바일 기기에서 이루어졌던 더미의 생성 및 관리에 대한 연산 부하와 메시지 송수신의 부하를 에이전트에서 담당하는 모델을 제안했다.

차후 연구 과제로는 충분한 사용자들의 이동경로가 수집되지 않아도 더미를 생성할 수 있는 알고리즘의 개선이 필요하다. 또한, 에이전트와 서비스 제공자 사이의 불필요한 데이터 전송량을 줄이기 위한 알고리즘 및 메시지 프로토콜 개선이 필요하다.

5. 참고문헌

[1] M. Weiser, The Computer for the 21st Century, *Scientific America*, 1991.

[2] 홍도원 외 3명, "유비쿼터스 환경을 위한 암호 기술 동향", *전자통신동향분석*, 2005.

[3] O. 3, P.Sistla, B. Xu, J. Zhou, S.Chamberlain, DOMINO: Databases fOr MovINg Objects tracking, *SIGMOD Conference*, p.p. 547-549, 1999.

[4] Urs Hengartner, Peter Steenkiste. Protecting Access to People Location Information. *First International Conference on Security in Pervasive Computing*, 2003.

[5] J. I. Hong, J. A. Landay, An Architecture for Privacy-Sensitive Ubiquitous Computing. Second International Conference on Mobile Systems, *Applications, and Services (Mobisys 2004)*, p.p. 177-189, 2004.

[6] Hidetoshi Kido, Yutaka Yanagisawa, Tetsuji Satoh, An Anonymous Communication Technique using Dummies, *IEEE International Conference on Pervasive Services*, 2005.

[7] A Beresford, F Stajano, Mix zones: User privacy in location-aware services, *IEEE International Workshop on Pervasive Computing and Communications Workshops*, 2004.