

# 위치기반 서비스에서 위치 프라이버시를 보호하기 위한 효율적인 더미 생성<sup>☆</sup>

## Efficient dummy generation for protecting location privacy in location based services

채 천 원<sup>1</sup>  
Tian-yuan Cai

윤 지 혜<sup>1</sup>  
Ji-hye Youn

송 두 희<sup>1</sup>  
Doo-hee Song

박 광 진<sup>1\*</sup>  
Kwang-jin Park

### 요 약

사용자가 위치기반 서비스(Location based service: 이하 LBS)를 제공 받기 위해서 LBS 서버에게 사용자의 위치와 질의 내용을 공개해야만 한다. 따라서 사용자의 신분, 위치 등이 노출될 수 있다. 최근 사용자의 프라이버시를 보호하기 위하여 더미를 이용한 기법들이 연구되고 있다. 그러나 더미를 생성하기 위하여 고려해야 할 사항들이 다수 존재한다. 예를 들어 더미 생성 시 장애물과 더미간의 거리 등을 고려해야만 프라이버시 보호를 증가시킬 수 있다. 따라서 본 논문에서 우리는 사용자의 프라이버시 보호를 증가시킬 수 있는 효율적인 더미 생성 기법을 제안한다. 실험 결과를 통해 최근 기법보다 성능이 우수함을 증명하였다.

☞ 주제어 : 클로킹 영역, 더미,  $k$ -익명화, 위치 보호, 프라이버시

### ABSTRACT

For enjoying the convenience provided by location based services, the user needs to submit his or her location and query to the LBS server. So there is a probability that the untrusted LBS server may expose the user's id and location etc. To protect user's privacy so many approaches have been proposed in the literature. Recently, the approaches about using dummy are getting popular. However, there are a number of things to consider if we want to generate a dummy. For example, when generating a dummy, we have to take the obstacle and the distance between dummies into account so that we can improve the privacy level. Thus, in this paper we proposed an efficient dummy generation algorithm to achieve  $k$ -anonymity and protect user's privacy in LBS. Evaluation results show that the algorithm can significantly improve the privacy level when it was compared with others.

☞ keyword : cloaked region, dummy,  $k$ -anonymity, location protection, privacy

## 1. 서 론

무선 통신과 측위 기술의 발전으로 사용자는 언제, 어디서든 다양한 서비스를 이용할 수 있게 되었다. Location based service(LBS)는 사용자의 위치를 기준으로 질의자에게 원하는 객체 정보를 제공하는 서비스이다. 예를 들어

사용자가 자신의 위치에서 1km 반경 내에 원하는 객체 정보(e.g., 주유소, 레스토랑)를 찾고자 할 때, 사용자가 자신의 위치를 기준으로 LBS 제공자(LBS provider: 이하 LBS 서버)에게 질의를 요청하면 LBS 서버는 사용자의 위치에 따라 객체 정보를 사용자에게 전송한다. 초기 LBS는 비상사태에서 피해자의 위치를 검색하기 위해 사용되었고(e.g., 미국 E911, 유럽 E112 등), 최근에 군사, 교통, 물류, 의료, 생활 등 여러 영역에서 활용되고 있다. 그 예로 사용자가 모바일 기기 내 Global Positioning System (GPS)을 통해서 주변에 관심 있는 가게 또는 인접한 주유소를 찾거나 또는 박물관에서 관람객에게 박물관 안에 있는 전시품의 위치를 알려주는 서비스 등을 제공한다[1].

그림 1에서 LBS의 기본 시스템 모델은 이동 장치, 측위 시스템, 단일 LBS 서버로 구성된 것을 볼 수 있다. 만약 공격자가 LBS 서버를 공격하거나 LBS 서버가 신뢰

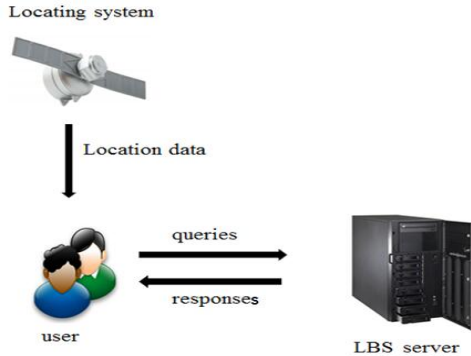
<sup>1</sup> College of Information and Communication Engineering, Wonkwang University, Iksan, 54538, Korea.

\* Corresponding author (kjpark@wku.ac.kr)

[Received 18 April 2017, Reviewed 2 June 2017(R2 27 July 2017), Accepted 21 August 2017]

☆ 이 논문은 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 과학기술인력 교류활성화 지원 사업 성과임(No. 2017H1D2A2000496), 이 논문은 2016년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 한국연구 NRF-2016R1D1A1B03930347)

할 수 없는 존재라면 질의자의 다양한 정보가 노출될 수 있기 때문에 LBS에서 위치 정보는 매우 중요하게 다루어지고 있다.



(그림 1) EDG 시스템 모델  
(Fig. 1) System model of EDG

최근까지 사용자의 프라이버시를 보호하기 위하여  $k$ -anonymity(이하  $k$ -익명화)를 이용한 연구가 제안되었다 [2]. [2]는 질의자와 다른  $k-1$ 명 사용자들을 같이 묶어서 cloaking region(CR)을 구성한 후 질의자의 실제 위치가 아닌 CR을 LBS 서버에게 전송한다. 그 외에 가상 사용자(dummy: 이하 더미)를 이용한 방법[3-7], 사용자의 정보를 암호화 시키는 연구[8] 등이 존재한다. 그러나 위 연구들 중에서 미들웨어(이하 익명 서버)가 필요하거나 주변 환경을 고려하지 않고 더미를 생성 또는 주변 환경을 고려하였으나 더미를 생성할 CR의 크기가 감소하여 사용자의 위치가 노출될 확률이 증가할 수 있다. 예를 들어 사용자는 A대학 캠퍼스 내의 학생이며 교내에서 도보 또는 차량으로 이동 중에 LBS를 제공받는다고 가정한다. 만일 사용자가 공과대학 내에서 단독으로 가장 가까운 편의점을 서버에게 질의한다면 서버는 사용자의 정확한 위치를 추측할 수 있다. 만일 서버가 해킹 당하거나 악용되어 사용된다면 사용자의 위치노출은 심각한 피해를 야기할 수 있다. 따라서 공과대학에 위치한 사용자가 자신의 위치를 보호하기 위해 공과대학뿐만 아니라 인문대학과 사회대학 주변에서도 더미를 생성한 후 서버에게 질의를 요청한다면 사용자는 자신의 위치정보보호를 좀 더 강화할 수 있다. 따라서 우리는 기존 연구들의 문제점을 개선하기 위하여 효율적인 더미 생성(Efficient dummy generation: 이하 EDG)을 제안한다. 본 연구에서 더미는 사용자가 자신의 위치를 보호하기 위한 목적으로 생성하는 것으로서

기지국 또는 서버가 관리하는 대상이 아니다. 서버는 사용자가 요청한  $0-n$ 개의 더미를 포함한 정보요청에 대하여 서비스를 제공해주는 역할만 수행한다고 가정한다. 제안기법에 대한 주요 기여는 다음과 같다.

- Circle-divided Dummy Generation(CDG)[9]은 주변 환경을 고려하지 않기 때문에 장애물을 확인하는 과정이 필요 없는 장점을 가진다. 그러나 장애물 위에 더미가 생성될 경우 서버가 사용자의 위치를 파악할 확률이 높아진다. 반면에 EDG는 장애물을 포함한 주변 환경을 고려하기 때문에 초기 맵 데이터를 확인하는 과정이 증가하는 반면에 장애물을 피해서 더미가 생성되기 때문에 사용자 위치의 노출 확률을 줄일 수 있다.
- Obstacle-based Dummy Generation(ODG)[10]은 EDG와 마찬가지로 더미 생성 시 맵 데이터를 확인해야 한다. ODG는 CR의 호 위에 더미를 생성하기 때문에 호 위  $2\pi(r=d_{max})$ 에 장애물만을 확인하면 된다. 그러나  $k$ 가 증가할수록 더미간의 거리가 인접해질 수 있다. 반면에 EDG는 CR의  $d_{min}$ 과  $d_{max}$ 를 설정한 범위  $\pi(d_{max})^2 - \pi(d_{min})^2$ 에 장애물을 확인해야 하지만 더미를 생성할 수 있는 공간을 확장시킴으로써 사용자의 위치 노출 확률을 감소시킨다.
- 실험 결과를 통하여 EDG가 CDG와 ODG보다 우수함을 증명한다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 소개하고, 3장에서 EDG를 설명한 후 4장에서 제안기법과 기존기법의 성능을 비교한다. 마지막으로 5장에서 결론을 내린다.

## 2. 관련연구

프라이버시를 보호하기 위한 연구들이 활발히 진행되고 있다[11]. 우리는 위치 정보 보호를 위한 시스템 모델을 크게 두 가지로 분류한다. 익명 서버(trusted anonymizer-based approaches)가 존재하는 위치 익명화 기법과 익명 서버 없이 사용자가 직접 위치를 익명화 시키는 기법(client-based approaches)이다.

익명 서버에서 공간 익명은 질의자의 위치를 기반으로 질의자가 요청한 범위만큼 위치를 보호하는 기법이다. 예를 들어 질의자가 자신에게 가까운 식당을 찾는다

고 가정한다. 질의자는 익명 서버에게 자신의 위치와 보호 범위를 전송하면 익명 서버는 질의자의 요구 사항에 맞도록 사용자의 정보를 보호한 후 LBS 서버에게 질의를 요청하는 구조를 취한다. LBS 서버는 질의자의 위치를 범위로 받기 때문에 질의자의 정확한 위치를 확인할 수 없다. 따라서 질의자의 위치 프라이버시를 보호할 수 있다[11-13].

그러나 기존의  $k$ -익명화라는 익명 서버가 존재하기 때문에 제 3자가 익명 서버를 공격하거나 공모할 경우 클라이언트들의 정보가 노출되는 문제가 발생할 수 있다. 따라서 익명 서버 없이  $p2p$ 를 이용하는  $k$ -익명화 기법이 제안되었다[14-15]. 익명 서버 없이 사용자들간의 통신을 하기 때문에 프라이버시 레벨이 높지만 다른 사용자들이 완전히 신뢰할 수 없어 개인 프라이버시가 노출될 수 있다.

자신의 위치를 보호하기 위하여 사용자가 직접 가상의 더미를 생성하는 연구가 제안되었다[16]. 질의자는 더미를 생성한 후 자신의 위치와 더미의 위치를 함께 서버에게 전송한다. 서버는 질의자와 더미의 위치를 기준으로 주변에 있는 식당의 정보를 질의자에게 제공한다. 더미 기법에서 주요 관심사는 더미를 생성하는 방법이다. 예를 들어 질의자는 자신의 위치에서 반경  $r$  범위 내에  $k-1$ 개 더미를 랜덤으로 생성해 질의자의 위치 프라이버시를 보호한다[17]. 이는 사용자의 의도와 상관없는 결과를 초래할 수 있는 문제를 가지고 있다. 예를 들어 서울이라고 범위를 한정 지으면 더미는 서울 내에서 생성하게 된다. 그러나 만일 더미가 서울역과 같이 특정지역에 집중되어 생성될 경우 사용자가 원하는 프라이버시 범위를 만족하지 못하는 문제가 발생할 수 있다. 즉, 사용자는 서울의 범위로 자신의 위치가 보호되길 바라며 질의를 요청했지만 서버는 사용자가 서울역 근처에서 질의한 것을 추측할 수 있다.

최근 논문에서 주변 환경을 고려해서 더미를 생성할 수 있는 기법들이 지속적으로 연구되고 있다[18]. 질의자는 자신의 위치에서 반경  $r$  범위 내에  $k-1$ 개 더미를 랜덤으로 생성하기 전에 주변 환경을 확인해서 장애물이 있는 부분을 제거함으로써 유효한 공간에서 더미를 생성할 수 있다. 그러나 장애물을 제거한 후 더미를 생성하면 더미를 생성할 수 있는 공간이 좁아질 수 있다. 반대로 장애물을 확인하지 않고 더미를 생성한 후 더미 생성 위치에 장애물이 있는지를 확인하는 기법도 존재한다. 그러나 장애물을 검사하는 과정이 반복될 경우 통신비용이 증가될 수 있다. 그 외에 더미를 원 호 위에 생성해야 하는 제약사항도 존재한다. 이처럼, 여러 가지 문제로 인하

여 질의자의 프라이버시 레벨이 떨어질 수 있다. 따라서 더미의 거리 및 위치가 어디에 존재하는지에 따라서 사용자의 위치 보호가 달라질 수 있기 때문에 우리는 이를 개선할 수 있는 연구를 하고자 한다.

### 3. 제안기법

(표 1) 기호 요약

(Table 1) Summary of Notations

기호	정의
CR	클로킹 영역
CR	여러 개의 예비 CR을 생성하기 위한 각도 (그림 3 예: ( : 90일 때, 4개의 예비 CR 생성))
$CR_{ref}$	장애물이 없는 공간에 더미를 생성할 수 있는 클로킹 영역
$CR_{ob}$	CR 내에 장애물이 존재하는 영역 ( $CR(d_{min})=0$ 일 때)
$CR_{e.ob}$	$CR_{ob}$ 에서 $CR(d_{min})$ 을 제외한 영역
$d_{max}$	CR의 반지름
$d_{min}$	$CR_{ref}$ 를 증가시키기 위한 반지름
$k$	질의자와 $k-1$ 의 더미를 합친 수
$r$	CR을 생성하기 전 가상의 중점을 생성하기 위한 범위
$k$	1개의 더미를 생성할 수 있는 각도
obs	CR에서 장애물이 포함되는 각도

질의자는 LBS를 제공 받기 위하여 질의자의 위치와 더미의 위치를 LBS 서버 전송한다. 그러나 그림 2와 같이 기존 기법은 CR의 중심 또는 호 위에 있다고 추측할 수 있다[19-20].



(그림 2) ODG의 더미 생성 예  
(Fig. 2) Example generation dummy of ODG

그림 2는 ODG기법으로 더미를 생성하는 방법을 보여 주고 있다[10]. 첫 번째, 사용자를 중심으로 원을 구성한다. 두 번째, 생성된 원의 호 중에서 장애물이 있는 지역을 제거한다. 세 번째, 남아있는 호를 기준으로 더미의 개수( $k-1$ )만큼 분할한다. 분할한 호의 각 영역마다 더미를 1개씩 생성한다. 그러나 그림 2와 같이 더미간의 거리는 밀집하게 모여있는 반면 사용자의 위치는 원의 중심에 있는 것을 확인할 수 있다. 즉 CR의 검색 범위가 감소하게 되어 사용자의 프라이버시 레벨이 감소하게 되는 것이다.



(그림 3) EDG의 CR 선택 방법  
(Fig. 3) CR selection method of EDG

그림 3은 질의자가 요청한  $d_{max}$ 와  $r$ 값에 따라 원이 생성된 것을 보여준다.  $d_{max}$ 의 설정을 통해서 더미를 생성할 원이 정하고, 식 (1)을 통하여 작은 원의 반지름  $r$ 를 설정한 후 사용자를 중심으로 작은 원을 생성한다. 작은 원을 생성하는 이유는 그림 2와 같이 사용자의 위치가 원의 중심에 위치하는 것을 피하고, 장애물이 적은 영역을 선별적으로 선택하기 위함이다. 만약 CR의 중심에 사용자가 존재한다면 LBS 서버는 사용자의 위치를 추측할 수 있다. 따라서 작은 원을 생성함으로써 질의자의 위치를 숨길 수 있다. 질의자가 더미를 생성하기 위한 CR의 생성 방법은 각도에 따라 다양하다. 그림 3에서 CR가 90도일 때 동, 서, 남, 북을 기준으로 중점(x)를 설정하고 그 중점들을 기준으로 큰 원을 생성한 것을 보여준다. r의 생성범위는 다음과 같다.

$$0 < r \leq d_{max}/2 \quad (1)$$

4개의 원을 생성하고  $d_{min}=0$ 일 때 각 원 내에 장애물이 있는 비율을 비교한 후 4개의 원 중에서 원 내에 장애물이 제일 적은 원을 선택한다( $CR_{obs} > CR_{obE} > CR_{obW} > CR_{obS}$ ). 질의자는 CR를 더 세부적으로 분할하고, 여러 개의 CR을 생성함으로써 장애물이 더 적은 원을 선택할 수 있다.  $CR_{e,ob}$ 의 크기는  $d_{min}$ 에 따라 달라질 수 있고 다음 수식과 같다.

$$CR_{e,ob} = CR_{ob} - CR(d_{min}) \quad (2)$$



(그림 4) EDG의 더미 생성 예  
(Fig. 4) Example generation dummy of EDG

그림 4는 그림 3에서 얻어진 결과를 토대로 선택된 CR을 보여주고 있다. Step 1: 그림 4에서 원의 중심을 기준으로 원의 최대 반지름  $d_{max}$ 와 최소 반지름  $d_{min}$ 에 해당하는 원을 생성한다. Step 2: 원 내에서 장애물이 있는 부분을 제거한다( $CR_{ef}$ ; 그림 4에서 바다에서 존재하는 영역은 장애물로 규정한다). Step 3: 장애물을 제외한 부분( $CR_{e,ob}$ ; 굵은 실선 내 영역)을  $k$ 개의 각도로 균일하게 분할(CR 내  $\theta$ )한다. Step 4: 그 후에 사용자를 제외한  $k-1$ 개만큼 분할한 부분에서 더미를 생성한다. EDG에서 장애물이 없는 유효한 CR의 범위는 다음과 같다.

$$CR_{ef} = CR(d_{max} - d_{min}) - CR_{ob} \quad (3)$$

그림 2에서 호와 각도만을 고려할 경우 더미들이 밀집되는 것을 확인하였다. 우리는 이러한 문제점을 개선하기 위하여 그림 4와 같이 빨간색 점선으로  $d_{min}$ 을 설정한다.  $d_{min}$ 의 범위는 다음과 같다.

$$0 \leq d_{min} \leq d_{max} \quad (4)$$

$d_{min}$ 의 크기를 조정하여 더미를 생성할 수 있는 영역을 증가시킴으로서 질의자의 위치 보호의 확률을 높일 수 있다. 그리고  $k$ 는 더미의 생성 각도를 나타내는 것으로 식 (5)와 같다.

$$k = (2\pi - \theta_{obs}) / k \quad (5)$$

EDG의 처리 과정은 알고리즘 1과 같다.

알고리즘 1. 유효한 더미 생성 방법
Input: 전체 맵 데이터, 질의자가 요청한 $d_{max}$ , $d_{min}$ , $k$ , $r$ , CR
Output: $CR_{ef}$
01: 자신의 위치와 전체 맵 데이터 확인;
02: $d_{max}$ , $d_{min}$ , $k$ , $r$ , CR 확인;
03: 질의자를 중심으로 $r$ 의 거리만큼 원을 생성;
04: CR에 따라 가상의 중점을 $m$ 개 생성;
05: $m$ 개의 중점에서 $d_{max}$ , $d_{min}$ , CR의 기준으로 예비 CR 생성;
06: while ( $m > 0$ )
07:     if ( $CR_{e,obs} > CR_{e,obj}$ )
08:         CR = $CR_i$ ;
09:     end if
10: $m = m - 1$ ;
11: end while
12: $CR_{ef} = CR(d_{max} - d_{min}) - CR_{obj}$ ;
13: return $CR_{ef}$ ;

## 4. 실험 결과

### 4.1 실험환경

본 절에서는 EDG, ODG, CDG의 성능을 비교하였다. 실험 환경은 Intel CPU G550 2.6GHz, memory 4GB이고, visual C++ 6.0을 이용하여 실험을 실행하였다. CDG는 장애물을 고려하지 않고, ODG는  $2\pi(r=d_{max})$ 에 해당하는 영역에 장애물을 확인하고, EDG는  $\pi(d_{max})^2 - \pi(d_{min})^2$ 에 해당하는 영역에 장애물을 확인한 후 더미를 생성한다고 가정한다. 사용된 데이터는 1,000\*1,000칸의 2차원 배열을 가정한다. 질의자가 요청하는 기본 클로킹 영역( $d_{max}$ )은 50\*50칸, 그리고  $k$ 개의 더미는 원의 호에 해당하는 그리드 수의 비율에 따라 랜덤하게 배치한다. 장애물의 배치는

배열의 비율에 따라 한 행 또는 열로 랜덤하게 배치한다. 실험 데이터 세트 값은 표 2와 같다. 장애물의 기본 설정 값과 더미의 수는 20%로 가정한다.

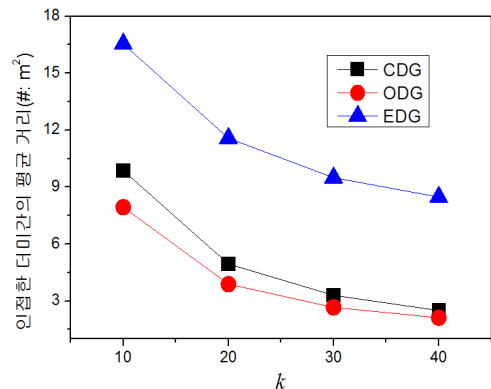
(표 2) 실험 데이터 세트 값  
(Table 2) Experimental dataset values

파라미터	데이터 세트 값
그리드(칸)	1,000 * 1,000
장애물(%)	10%, <20%>, 30%, 50%
$d_{max}$ (칸*칸)	30*30, <50*50>, 70*70, 100*100
$d_{min}$ (칸)	70%
더미의 수 $k$ (개)	$d_{max}$ 의 둘레에 해당하는 그리드 수의 비율 10%, <20%>, 30%, 40%

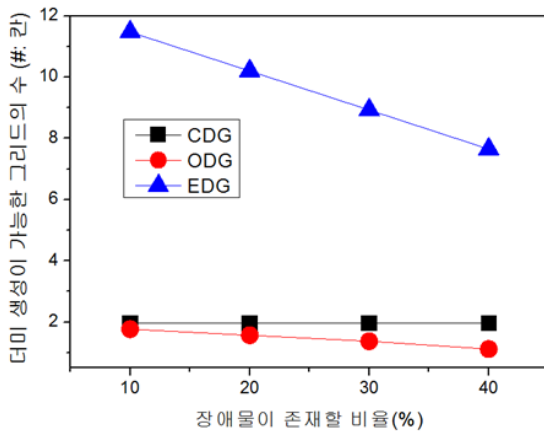
### 4.2 실험결과

그림 5는 더미를 생성하는  $k$ 의 수에 따른 더미간의 인접한 평균거리를 측정된 결과를 보여준다.

기본 설정 값은 표 2와 같다.  $k$ 의 수가 증가함에 따라 기법들의 인접 거리가 짧아지는 것을 확인할 수 있다. 특히 ODG에서 더미간의 인접한 평균거리가 가장 짧다. 더미가 인접할수록 단위 면적 당  $k$ 가 증가하기 때문에 프라이버시 레벨이 감소하게 된다. CDG는 ODG에 비해 전체 평균 24.1%가 더 멀지만 장애물을 고려하지 않았기 때문에 장애물 위에 더미가 생성될 수 있는 문제점을 가진다. EDG는 ODG에 비해 평균 177.4%, CDG에 비해 평균 127.3% 이상 향상시킨 것을 확인할 수 있다. EDG는 ODG와 CDG의 문제점을 모두 고려하였기 때문에 평균 거리와 장애물에 대한 문제점을 모두 개선하였다.



(그림 5)  $k$ 에 따른 인접한 더미간의 평균 거리  
(Fig. 5) Adjacent to the average distance between dummies with respect to  $k$



(그림 6) 장애물의 존재할 비율에 따른 유효한 그리드의 수 (Fig. 6) The number of effective grid with respect to obstacle' existence ratio

그림 6은 장애물이 존재할 비율에 따른 유효한 그리드의 수를 보여준다. 유효한 그리드란 장애물이 포함되지 않는 그리드를 의미한다. 기본 설정 값은 표 2과 같으며,  $k$ 의 수는 40으로 가정한다.

ODG와 EDG는 고정된 그리드 내에 장애물의 비율이 증가함에 따라 유효한 그리드의 수가 감소하는 반면 CDG는 장애물 환경을 고려하지 않아 장애물의 증가에 따른 유효 그리드 수가 변하지 않는 것을 확인할 수 있다.

## 5. 결 론

본 논문에서 우리는 사용자의 프라이버시를 보호하기 위하여 EDG를 제안하였다. EDG는 질의자 주변에 존재하는 장애물을 고려하여 더미를 생성하였기 때문에 질의자의 위치가 노출될 확률을 줄일 수 있었다. 그리고 EDG는 더미 생성 시  $d_{max}$  내에서 더미간의 생성 거리를 확장 시킴으로서 질의자의 프라이버시 레벨을 향상시켰다. 실험 결과를 통해 최근 기법보다 제안기법의 성능이 우수함을 검증하였다.

## 참고문헌(Reference)

[1] K. G. Shin, X. Ju, Z. Chen, et al., "Privacy protection for users of location-based services", *IEEE Wireless*

*Communications*, vol. 19, no. 1, pp. 30-39, 2012.

<https://doi.org/10.1109/MWC.2012.6155874>

[2] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing", *IEEE Pervasive computing*, vol. 2, no. 1, pp. 46-55, 2003.

<https://doi.org/10.1109/MPRV.2003.1186725>

[3] Y. H. Gustav, X. Wu, Y. Ren, et al., "Dummy Based Privacy Preservation in Continuous Querying Road Network Services", *IEEE International Conference Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 94-101, 2014.

DOI : 10.1109/CyberC.2014.24

[4] B. Niu, X. Zhu, W. Li, et al., "A personalized two-tier cloaking scheme for privacy-aware location-based services", *IEEE Computing, Networking and Communications*, pp. 94-98, 2015.

<https://doi.org/10.1109/ICCCNC.2015.7069322>

[5] P. R. Lei, W. C. Peng, I. J. Su, et al., "Dummy-based schemes for protecting movement trajectories", *Journal of Information Science and Engineering*, vol. 28, no. 2, pp. 335-350, 2012.

DOI : <https://ir.nctu.edu.tw/handle/11536/15826>

[6] B. Niu, Q. Li, X. Zhu, et al. "Achieving k-anonymity in privacy-aware location-based services", *IEEE International Conference on Computing, Networking and Communications*, pp. 754-762, 2014.

<https://doi.org/10.1109/INFOCOM.2014.6848002>

[7] T. Hara, A. Suzuki, M. Iwata, et al. "Dummy-Based User Location Anonymization Under Real-World Constraints", *IEEE Access*, vol. 4, pp. 673-687, 2016.

<https://doi.org/10.1109/ACCESS.2016.2526060>

[8] B. Niu, X. Zhu, H. Chi, et al. "3PLUS: Privacy-preserving pseudo-location updating system in location-based services", *IEEE Wireless Communications and Networking Conference*, pp. 4564-4569, 2013.

<https://doi.org/10.1109/CC.2013.6623499>

[9] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services", *Proceedings. International Conference on Pervasive Services*, pp. 88-97, 2005.

<http://ieeexplore.ieee.org/document/1506394/tp=&arnumber=1506394>

- [10] T. Y. Cai, D. H. Song, et al., "Efficient dummy generation for protecting location privacy", *Korea Institute of Information, Electronics and Communication Technology*, vol. 9, no. 6, pp.526-533, 2016.  
<http://dx.doi.org/10.17661/jkiiect.2016.9.6.526>
- [11] M. F. Mokbel, C. Y. Chow, and W. G. Aref, "The new Casper: query processing for location services without compromising privacy", *Proceedings of the 32nd international conference on Very large data bases*, pp. 763-774, 2006.  
 DOI : [https://www.cerias.purdue.edu/apps/reports\\_and\\_papers/view/3799](https://www.cerias.purdue.edu/apps/reports_and_papers/view/3799)
- [12] D. H. Song, J. Sim, K. J. Park, et al., "A privacy-preserving continuous location monitoring system for location-based services", *International Journal of Distributed Sensor Networks*, pp.1-10, 2015.  
<http://journals.sagepub.com/doi/full/10.1155/2015/815613>
- [13] T. Xu and Y. Cai, "Exploring historical location data for anonymity preservation in location-based services", *IEEE International Conference on Computer Communications*, pp. 1220-1228, 2008.  
<https://doi.org/10.1109/INFOCOM.2008.103>
- [14] B. Niu, X. Zhu, X. Lei, et al., "Eps: Encounter-based privacy-preserving scheme for location-based services", *IEEE Global Communications Conference*, pp. 2139-2144, 2013.  
<https://doi.org/10.1109/GLOCOM.2013.6831391>
- [15] B. Niu, X. Zhu, X. Lei, et al., "EPcloak: An Efficient and Privacy-Preserving Spatial Cloaking Scheme for LBSs", *IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 398-406, 2014.  
<https://doi.org/10.1109/GLOCOM.2013.6831391>
- [16] H. Zhao, J. Wan, and Z. Chen. "A Novel Dummy-Based KNN Query Anonymization Method in Mobile Services", *International Journal of Smart Home*, vol. 10, no. 6, pp. 137-154, 2016.  
<http://dl.acm.org/citation.cfm?id=2424354>
- [17] B. Niu, X. Zhu, X. Lei, et al., "Privacy-area aware dummy generation algorithms for location-based services", *IEEE International Conference on Communications*, pp. 957-962, 2014.  
<https://doi.org/10.1109/ICC.2014.6883443>
- [18] B. Niu, S. Gao, F. Li, et al., "Protection of location privacy in continuous LBSs against adversaries with background information", *IEEE International Conference on Computing, Networking and Communications*, pp. 1-6, 2016.  
 DOI : 10.1109/ICCNC.2016.7440649
- [19] F. Li, S. Wan, B. Niu, et al., "Time obfuscation-based privacy-preserving scheme for location-based services", *Wireless Communications and Networking Conference*, pp. 1-6, 2016.  
<https://doi.org/10.1109/WCNC.2016.7564715>
- [20] B. Niu, Q. Li, X. Zhu, et al., "Enhancing privacy through caching in location-based services", *IEEE International Conference on Computer Communications*, pp. 1017-1025, 2015.  
<https://doi.org/10.1109/INFOCOM.2015.7218474>

## ● 저 자 소 개 ●

### 채 천 원(Tian-yuan Cai)

2015년 원광대학교 정보통신공학과(공학사)  
2017년 원광대학교 정보통신공학과(공학석사)  
관심분야 : 정보통신, 위치기반서비스 etc.  
E-mail : midsky1000@naver.com



### 윤 지 혜(Ji-hye Youn)

2016년 원광대학교 정보통신공학과(공학사)  
2016년~현재 원광대학교 대학원 정보통신공학과 석사과정  
관심분야 : 위치기반서비스, 정보보호 etc.  
E-mail : yoonjh09@naver.com



### 송 두 희(Doo-hee Song)

2010년 원광대학교 정보통신공학과(공학사)  
2012년 원광대학교 정보통신공학과(공학석사)  
2016년 원광대학교 정보통신공학과(공학박사)  
2016년~현재 원광대학교 공업기술개발연구소 연구교수  
관심분야 : 공간질의처리, 위치정보보호 etc.  
E-mail : songdoohee@naver.com



### 박 광 진(Kwang-jin Park)

2000년 고려대학교 컴퓨터학과(이학사)  
2002년 고려대학교 컴퓨터학과(이학석사)  
2006년 고려대학교 컴퓨터학과(이학박사)  
2006년~2007년 프랑스 국립컴퓨터 과학연구소(INRIA) 박사 후 연구원  
2008년~현재 원광대학교 정보통신공학과 교수  
관심분야 : 데이터베이스, 분산컴퓨팅 etc.  
E-mail : kjpark@wku.ac.kr

