사용자 위치 정보 및 POI 정보 보호를 고려한 Approximate k-최근접점 질의처리 알고리즘

An Approximate k-NN Query Processing Algorithm Supporting both Location Cloaking and POI Protection

장미영* · Amina Hossain · 엄정호, 장재우°
Mi-Young Jang* · Amina Hossain · Jung-Ho Um · Jae-Woo Chang
전북대학교 컴퓨터 공학과, 영상정보 신기술 연구소°
{myjang,ah,jhum}@dblab.chonbuk.ac.kr · jwchang@chonbuk.ac.kr

요 약

위치 기반 서비스(Location-Based Services: LBS)에서 질의 요청자가 자신의 위치 정보와 원하는 질의를 전송하면, 위치 기반 서버는 이를 기반으로 질의를 처리하고 결과를 전송한다. 이 때 질의 요청자는 자신의 정확한 위치 좌표를 서버에 전송하기 때문에 개인 정보가 악용될 수 있는 위험에 노출된다. 이러한 문제를 해결하기 위하여 제안된 연구는 크게 Location Cloaking 기법과 Private Information Retrieval(PIR) 기법으로 분류된다. Location Cloaking 기법은 사용자의 위치 좌표를 k-1개의 다른 사용자와 함께 묶어 하나의 Cloaking 영역을 생성하고 이를 바탕으로 질의를 처리한다. 그러나 영역에 대한 질의 후보 집합을 결과로 전송하므로 사용자에게 노출되는 POI의 수가 증가하는 문제점을 지닌다. PIR은 암호화 기법으로 위치 기반 서버나 공격자에게 사용자의 위치와 질의 타입을 드러내지 않고 질의를 수행한다. 그러나 암호화 된 질의 결과로 사용자에게 데이터 전체를 전송하기 때문에 막대한 통신비용을 초래한다. 따라서 본 논문에서는 Location Cloaking과 PIR 기법의 장점을 결합하여 사용자의 개인 정보와 위치 기반 서버의 POI 정보 보호를 고려한 Approximate k-최근접점 질의 처리 알고리즘을 제안한다. 질의 전송시, 질의 요청자는 Cloaking 영역을 생성하여 위치 좌표를 감추고, 질의 결과 전송 시Cloaking 영역에 제한된 PIR 프로토콜을 적용한다. 또한 k-최근접점 질의 수행 시, 반환되는 POI의 수를 최소화하고, 정확도 높은 질의 결과를 만족하기 위해 Overlapping parameter를 적용한 색인 기법을 제안한다.

1. 서론

최근 위치 측정 장치가 장착된 스마트폰, 내비게이션 등의 사용이 증가함에 따라 다양한 위치 기반 서비스 (Location-Based Services: LBS)가 꾸준히 개발되고 있다.[1,2,3] 위치 기반 서비스는 이동 중인 사용자가 휴대한 단말기의 위치에 기반 하여 사용자에게 특화된 응용 서비스 정보를 제공한다. 일반적으로 질의 요청자는 자신의 위치에서 가장 근접한 POI (Points Of Interest: 건물, 지리 정보, 모바일 사용자 등) 정보를 탐색하는 최근접점 (Nearest Neighbour: NN) 질의 또는 k개의 근접한 POI를 탐색하는 k-최근접점 (k-Nearest Neighbour: k-NN) 질의를 수행하며, 이를 위해 [1]자신의 위치 정보와 원하는 질의를 무선 통신 단말을 통해 전송한다. 위치기반 서버에서는 자신이

1) 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. 2010-0000202)

소유하고 있는 POI 정보를 기반으로 질의를 처리하고 사용자에게 결과를 전송한다. 하지만 위치 기반 서비스를 제공받기 위해 질의 요청자는 자신의 공간 좌표나 시간 정보를 위치 기반 서버에 전송하기 때문에 개인정보가 악용될 수 있는 위험에 노출된다. 이는 사용자가 신뢰할 수 없는 서비스 제공자에게 자신의 위치 정보를 전송하거나 접근 권한이 없는 공격자(adversary)에게 자신의 실시간 위치정보나 연속적인 방문 장소 등의 정보가 노출 되는 형태로 발생한다.[4,5]

따라서, LBS 환경에서 사용자의 개인정보 보호를 위해 다수의 기법들이 연구되었다. 이러한 기법들은 질의 요청 시 사용자의 정확한 위치 정보를 전송하지 않고도 신뢰할 수 있는 질의 결과를 얻기 위한 알고리즘이다. 서비스 사용자는 위치좌표를 일정 영역으로 확장하여 질의를 수행하기 때문에 서버로부터 정확한 질의 결과를 보장받기 위해, 다수의 질의 결과 후보 집합을 전송 받는다. 그러나 위치 기반 서버는 POI 정보가 질의 요청자에게 노출되는 것을 최소화하기 위해 POI 정보를 보호 한다. 예를 들어, (그림 1)과 같이 위치 기반 서비스 사용자가 “현재 위치 근처에 있는 의류 쇼핑몰을 탐색하라”라는 질의를 요청하였을 때, 서비스 제공자는 차별화된 서비스를 제공하기 위해 결과 후보 집합과 함께 의류 할인쿠폰을 무료로 전송한다고 가정하자. 이때 사용자가 악의적으로 질의를 남용하여 많은 양의 쿠폰을 다운로드하는 경우, 서비스 제공자는 큰 손실을 입게 된다.

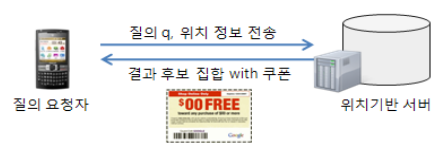

그림 1. POI 정보 보호의 필요성

반대로, 서비스 이용자에게 부과되는 이용 요금이 검색되는 POI의 정보량에 비례한다면, 사용자 또한 전송 받는 결과 후보 집합을 최소화하고자 요구할 것이다. 이러한 문제는 효율적인 위치기반 서비스를 제공하고 사용자의 만족도를 높이기 위해 사용자 위치 정보 보호와 함께 반드시 고려해야 할 사항이다.

사용자 위치정보 보호를 위한 연구는 크게 Location Cloaking 기법과 Private Information Retrieval(PIR) 기법으로 분류된다. 먼저, Location Cloaking 기법[6,7,8,9,10,11,12]은 사용자가 요구하는 Privacy profile을 만족하도록 Cloaking 영역을 생성하여 이를 기반으로 질의를 수행한다. Privacy profile 요소에 의해 사용자는 질의 전송 시 자신의 위치정보가 다른 사용자와 구분되지 않을 만큼 최소한의 정보를 노출하면서, 아울러 효율적으로 질의를 수행 할 수 있도록 한다. 한편, PIR 기법[13,14]은 암호화 기법으로 위치기반 서버나 공격자에게 사용자의 질의를 드러내지 않고 질의를 수행한다. 전처리 단계는 서버에서 지원하는 질의 형식에 따라 효율적인 영역 변환 기법을 선택하여 POI 정보를 맵핑(mapping,변환)하고 저장한다. 질의 요청 시, 질의 또한 사용자가 원하는 질의 결과의 인덱스(index,색인) 정보를 탐색하기 위한 형태로 변환하여 전송된다. 서버에서도 수학적 연산을 통해 사용자가 원하는 특정 정보를 얻지 않고도 결과를 탐색하여 사용자에게 전송한다. 그러나 기존의 연구는 다음과 같은 문제점을 지닌다. 첫째, Cloaking 기법은 사용자의 위치 좌표를 영역정보로 변환하고, 영역에 대해 탐색한 POI 후보 집합을 전송받기 때문에 Cloaking 영역에 따라 , 영는 POI의 양이 좌우된다. 즉, Cloaking 영역의 크기가 커질수록, 사용자의 응집도가 높을수록 노출되는 POI의 양은 많아진다. 둘째, PIR 기법[14]의 경우 노출되는 POI의 양은 최대 ($O\sqrt{D}$)로 감소하지만, 질의 요청자에게 데이터베이스 전체를 전송

하여 막대한 통신비용을 초래하며, 복잡한 수학 연산을 위한 물리적 자원을 요구한다. 따라서 Ghinita et al.[15]의 연구에서는 Cloaking 기법과 PIR을 모두 사용하는 Hybrid Technique 을 제안하여 질의 요청자의 위치 정보와 질의를 보호하고, 반환되는 POI 정보를 최소화하는 기법을 제안하였다. 그러나 이 기법은 Approxi-mate 최근접점 질의만을 지원하는 문제점을 지닌다. 따라서 본 논문에서는 기존의 Hybrid Technique[15]연구를 확장한 Approximate k-최근접점 질의 처리 알고리즘을 제안한다. 이를 위해 전처리 단계에서 서버는 Overlapping(영역 중복 저장) 기법을 적용한 Indexing 구조를 사용하여 POI를 색인, 저장한다. 이를 통해 분할된 노드에 저장하는 POI 수를 증가시켜, k-최근접점 탐색 시 정확도를 높이고 결과 후보 POI 수를 증가시켜 확장을 최소화하는 기법이다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구 및 Hybrid Approximate NN 질의처리 알고리즘에 대해 서술하고 3장에서는 제안하는 Approximate k-최근접점 질의 처리 알고리즘을 기술한다. 마지막으로 5장에서는 결론 및 향후연구에 대해 설명한다.

2. 관련 연구

LBS에서 사용자 위치 정보 보호를 위해 다양한 연구가 수행되었다. 기존 연구는 크게 사용자 위치 정보를 Cloaking 영역으로 확장하여 질의 처리를 수행하는 Location Cloaking 기법과 사용자의 질의 및 POI보호를 위한 PIR 기법으로 분류된다. Location Cloaking 기법은 사용자가 요구하는 privacy profile을 만족하도록 Cloaking 영역을 생성하여 이를 기반으로 질의를 수행한다. 이때 생성되는 Cloaking 영역은 반드시 질의 요청자의 위치 좌표를 포함해야 한다. 대부분의 Cloaking 기법은 질의 요청자를 포함한 k 명의 사용자를 포함하여 Cloaking 영역을 생성하는 K-anonymity를 공통으로 지원한다[6,7,8,9]. 그 외에 최소 Cloaking 영역 크기인 Amin을 보장하여 POI 밀집도가 높은 지역에서도 사용자 위치 정보를 보호하는 기법[10,11], Cloaking 영역 내에 L개의 건물을 포함하는 L-diversity를 지원하는 알고리즘[12] 등이 있다. 각각의 요소에 의해 사용자는 질의 전송 시 자신의 위치정보가 다른 사용자와 구분되지 않을 만큼 최소한의 정보를 노출하면서, 효율적으로 질의를 수행할 수 있도록 한다. 그러나 Location Cloaking 기법은 질의 처리 시 영역에 대해 탐색한 POI 후보 집합을 전송 받기 때문에 Cloaking 영역에 따라 노출되는 POI의 양이 좌우된다. Cloaking 영역의 크기가 커질수록, 사용자의 밀도가 높을수록, 노출되는 POI의 양은 증가한다.

또한 G. Ghinita et al.에서 제안한 PIR 기법[14]은 개인 정보 보호를 위한 근접 POI 탐색 알고리즘으로 수학적 연산을 증가시켜 질의를 암호화하는 연구이다(그림 2).

그림 2. PIR 프로토콜

제안된 PIR 기법은 다음과 같다. 사용자는 자신만이 알고 있는 매우 큰 두 소수의 곱으로 이루어진 N을 정하고, 데이터가 두 소수의 값에 의해 정의되는 비트 정보인 QR(Quadratic Residue) 또는 QNR (Quadratic Non-Residue)에 포함되는 지를 판단한다. 이 때, 공격자(adversary)가 전체 데이터 영역 중에 사용자가 어떠한 데이터를 원하는지를 표시한 QR, QNR 영역을 구분하기 Q서는 두 소수를 알아야 한다. 그러나 공격자가 N을 알고 있다고 하더라도 이는 매우 큰 값이기 때문에 두

소수를 찾기 Q서는 막대(Qu산이 필요하며, 필요하알지 못하면 전송 하더뎄이터를 판단하기가 어렵다. sary)가 위한 전처리 작곅격자(서버에서하더전체 POI 뎄이터에 대해 보로노이 다이어그램을 적용하여 각 보로노이 셀 정보와 그 안에 포함된 POI 정보를 저장한다. 또한 전체 데이터 영역을 일정한 크기ar그리드자(나누어 각 그리드 영역에 겹치하더보로노이 셀 정보를 저장한하테이블 정보를 유지한다. 사용자는 질의가 전송할 하더자신이 속한하그리드 셀 id를 탐색하여 매우 큰 값 N을 계산하고, 자신이 속한하그리드 셀을 QNR뤬드 영역의 셀은 QR자(표시한다. 이를 서버에 전송 면, 서버에서하더사용자가 속한하열에 대한 POI 정보가 QNR이 되도록 비트 연산을 전체 맠 원하는에게 전송한다. 사용자는 전송 받은 데이터 영역의 연산을 통해 만약드 영값이 QNR인 경우 이를 결과에 반영한다. 이러한 암호화 기법을 통해 사용자는 자신의 속한하그리와 질의가 드러내 맠 맠 정확한 sar 결과를 탐색을 통해 으며 서버에서도 전송한다POI그리만Dr결과와 질으로 반환하는 장점걄 전닌다. 그러나,암호화된 전체 데이터 영역을 결과와 질으로 전송므로 이색을 비통신량이 증가versary) 비용과와시간와측면에서 비은 데인 문제점걄 전닌다. 또한 서버와측에서 전체 데이터 영역에 대해 비트 연산을 전체므로, sa 처리 시간이 증가하여 한 번에 처리할 수 있는 질의 수가 제한된다.

따라서 Ghinita et al.[15]의 연구 에서는 사용자 위치 정보를 위한 Location Cloaking과 POI정보 보호를 동시에 고려한 Hybrid Approximate 최근접점 질의처리 알고리즘을 제안하였다. 질의 요청시, 사용자는 Cloaking 영역을 생성하고 Paillier Public Key Encryption 기법[16]을 이용하여 자신의 위치좌표를 암호화한다. 서버에서는 전송받은 Cloaking 영역을 포함하는 트리영역을 탐색하고, Paillier Homomorphism[16]을 기반으로 한 Private Point- Rectangle Enclosure 기법을 사용하여 암호화된 좌표가 탐색한 후보 영역에 포함되는 지 여부를 확인하여 Approxi-mate 최근접점 질의를 수행한다. 마지막으로 모든 조건을 만족하는 후보 영역을 질의 요청자에게 반환한다. 질의 요청자는 전송받은 후보 영역 중에 자신이 원하는 질의 결과를 포함하는 영역의 id를 확인하고, 이를 바탕으로 서버와 PIR 프로토콜을 통해 최종 질의 영역에 대한 POI 후보 집합을 전송받는다. 이 기법은 Location Cloaking 기법과 PIR 기법을 동시에 고려하여 사용자의 위치 정보, 질의 보호와 함께 서버의 POI 노출을 최소화하는 최초의 연구로 매우 큰 의미를 지니지만, Approximate 최근접점 질의만을 지원하는 한계를 가진다.

3. Approximate k-최근접점 질의처리 알고리즘

본 절에서는 사용자의 위치 정보를 보호하고, 동시에 서버에서 노출되는 POI를 최소화하기 위한 Approximate k-최근접점 질의처리 알고리즘을 제안한다. 이를 위해 제안하는 기법의 시스템 구조를 설명한다. 또한, 효과적인 k-최근접점 탐색을 위해 Overlap Indexing 기법을 제안한다. 마지막으로 제안하는 Approximate k-최근접점 질의 처리 알고리즘에 대해 기술한다.

3.1 시스템 구조

제안하는 기법의 시스템 구조는 (그림 3)과 같다. 첫째, 질의 요청자는 자신이 원하는 방법으로 Cloaking 영역을 생성하고, Paillier Public Key 생성 기법을 사용하여 자신의 위치정보를 암호화하여 서버에 전송한다. 둘째, 서버에서는 Cloaking 영역과 암호화 된 위치정보 E(Xu), E(Yu), 그리고 암호화 Key(i.e., 공개키)를 바탕으로 트리를 탐색하여 Cloaking 영역과 겹치는 노드를 찾는다. (그림 2)에서는 {R1,

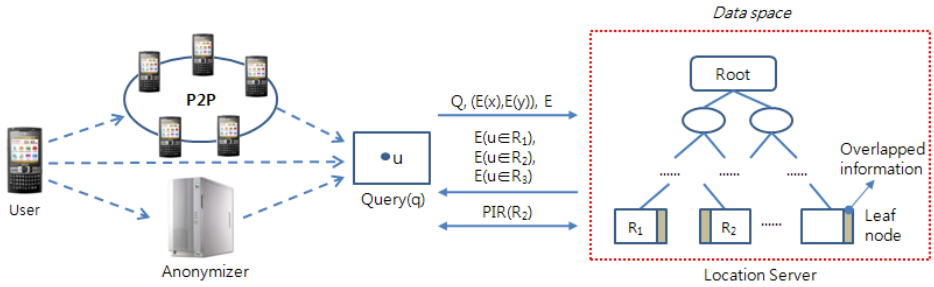

그림 3. 시스템 구조

R2, R3}가 탐색되었다. 셋째, 탐색한 후보 노드 중에 실제로 질의 요청자를 포함하는 영역을 찾기 위해 homomorphic encryption[16]을 사용하여 실제 사용자가 위치한 후보 영역을 반환한다. 이때, 질의 요청자가 원하는 k를 만족하는 경우 최종 후보 영역(R2)이 사용자에게 반환된다. 만약 후보 결과 셋이 사용자가 요청한 k를 만족하지 않는 경우, 인접한 노드를 기준으로 k를 만족할 때까지 확장하여 전송한다. 마지막으로 질의 요청자는 전송받은 후보 영역 중 실제로 자신이 위치한 영역을 기준으로 k를 만족하는 영역을 선택하여 Cloaking 영역에 대한 결과 영역의 id를 PIR 프로토콜을 통해 전송하면, 서버는 해당 영역 내에 포함된 최종 POI 후보 집합을 사용자에게 전송 한다.

3.2 Overlapped Indexing

본 절에서는 질의 요청자에게 노출되는 POI의 정보를 최소화하고, k-최근접점 질의 처리의 정확성 및 효율을 최대화하기 위한 Overlapping Indexing 기법을 제안한다. 제안하는 색인 구조는 k-d-tree와 유사한 방식을 사용한다. k-최근접점 질의를 제공하기 위해 영역 분할시 Overlap parameter (α) 만큼 분할 축을 이동하여 POI를 중복 저장하여 질의 처리 효율을 높인다. 제안하는 Overlap Indexing 수행 과정은 다음과 같다. 먼저 질의 요청자로부터 Cloaking 영역을 전송 받으면, 서버는 해당 영역과 교차하는 영역을 탐색한다. 탐색된 노드에서 사용자에게 노출되는 POI 수를 최소화하기 위해 시스템 파라미터인 F (Node Cardinality, 최대 POI 저장 허용치)를 기준으로 노드를 분할한다.

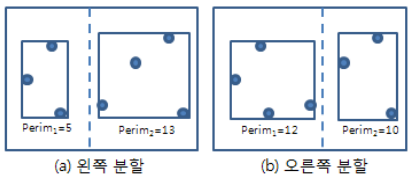

그림 4. 영역 분할 방식

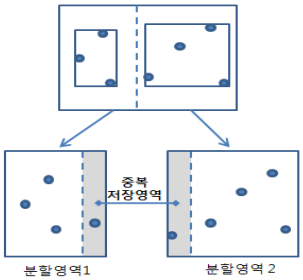

그림 5. Overlap 저장 구조

F 는 한 노드에 저장할 수 있는 최대 POI의 허용치로, 위치 기반 서버는 F 값을 조정하여 자신이 허용하는 POI 노출 정도를 관리한다. 만약 F =3인 경우, (그림 4)와 같이 영역 분할은 왼쪽과 오른쪽을 기준으로 수행할 수 있다. 두 경우에서 각 분할된 영역 내에 POI를 모두 포함하는 최소 사각형을 그리고, 그 둘레의 합이 작은 분할 축을 최종 영역 분할 축

으로 선택한다. 따라서 예제에서는 왼쪽 분할 방식이 선택되고, 왼쪽 분할 노드에는 3개의 POI가, 오른쪽 분할 노드에는 4개의 POI가 저장된다. 영역 분할 방향을 기준으로 F 만큼 POI를 저장하므로, 반대쪽 분할 노드에는 최대 2F -1개의 POI가 저장된다, 아울러, 분할된 노드를 저장할 때 (그림 5)와 같이 사용자가 정의한 Overlap parameter (α) 만큼 영역을 확장하여 중복 저장한다. 이를 통해 한 분할된 영역에 저장되는 POI수를 최대화 하여 정확도를 높이고 k를 만족하기 위한 확장 탐색을 최소화한다.

3.3 Approximate K-최근접점 질의처리 알고리즘

(그림 6)은 Approximate K-최근접점 질의처리 알고리즘의 전체적인 흐름을 나타낸다. (그림 6-①)과 같이 사용자가 암호화된 위치 좌표, Cloaking 영역과 함께 질의를 요청하면, 위치 기반 서버에서는 Approximate k-최근접점 질의를 수행한다. 먼저, POI가 저장된 R*-트리를 탐색하여 Cloaking 영역과 교차하는 후보 노드를 탐색하고, 탐색한 노드에 대해 3.2장에서 설명한 Overlap Indexing 기법을 사용하여 서브 노드로 분할한다. 아울러, Homomorphism Encryption을 기반으로 한 Private Enclosure 기법을 사용하여 사용자가 위치한 자식노드를 탐색한다(그림 6-②). Private Enclosure 탐색은 식 (1)과 같이 Paillier Homomorphism[16]에서 제안한 수학적 결합, 교환법칙 등을 이용하여 매우 큰소수 N을 기반으로 암호화 된 두 좌표의 차를 구하고 그 값이 양수인지, 음수인지를 판별하는 기법이다.

$$D(E(m_1) \cdot E(m_2)) = (m_1 + m_2) \mod N$$
$$D(E(m)^r) = r \cdot m \mod N \quad (1)$$

이를 통해 (그림 7)과 같이 사용자의 위치 좌표가 선택한 영역 내에 위치하는지에 대한 여부를 결정한다. 이때, 질의 요청자를 포함하는 자식 노드에 속한 POI의

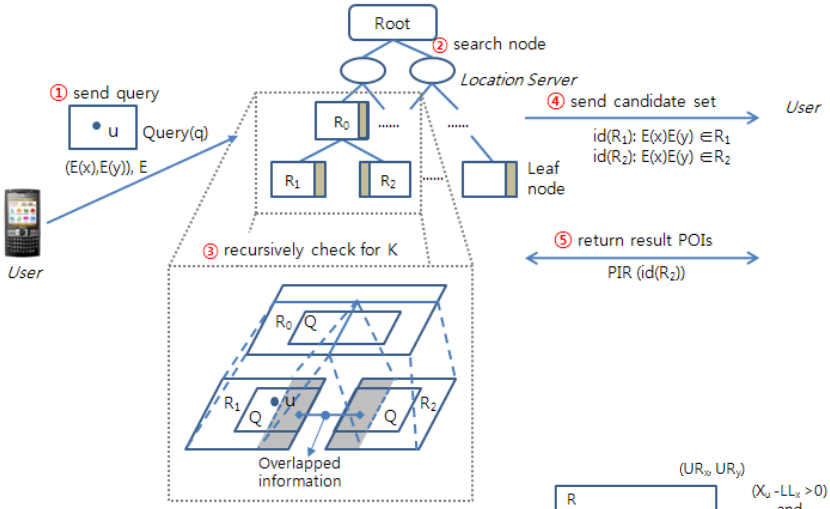

그림 6. Approximate k-최근접점

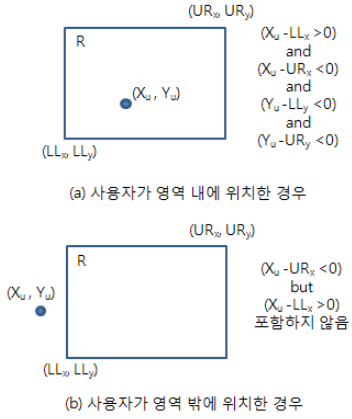

그림 7. Private Enclosure 탐색

수가 k를 만족하는 경우, 질의 처리 서버는 이를 사용자에게 반환한다. 만약 탐색된 노드가 k를 만족하지 않으면, 해당 노드와 분할 축을 공유하는 이웃노드를 포함하는 영역을 찾고, 두 영역을 다시 병합하여 전체 영역에 포함된 POI의 수가 k를 만족하는 지의 여부를 탐색하는 알고리즘을 반복적으로 수행한다(그림 6-③). 위치 기반 서버는 최종으로 선택된 노드를 사용자에게 반환함으로써 k-최근접점 탐색 알고리즘을 종료한다(그림 6-④). 영역 정보를 전송 받은 사용자는 자신이 원하는 영역의 id를 확인하고, cloaking 영역에 대해 PIR 프로토콜을 사용하여 최종 POI 결과 집합을 전송받는다(그림 6-⑤).

제안하는 기법에서 사용자가 원하는 k를 만족하기 위한 탐색 알고리즘은 (그림 8)과 같다. 알고리즘에서 분할 된 노드 중 사용자를 포함하는 노드가 k를 만족하는 경우 이를 반환한다.(1~2줄) 만약 k를 만족하지 못하면, 해당 영역이 포함하는 POI수가 k 이상이 될 때까지 이웃노드 및 부모 노드를 탐색하고 영역을 확장한다.(3~9줄) 마지막으로 병합된 노드를 최종으로 탐색하고 사용자에게 반환하며 질의 처리가 종료된다.(7줄)

k-최근접점 탐색 알고리즘

```
//입력: Root,
      질의 요청자를 포함하는 노드 Nk
      node split 집합 {N1...NS}
//출력: k를 만족하는 결과 노드(집합)
1. if( POIs in Nk > k)
2.     return  Nk
3. else{
4.     search sibling node
5.     merge searched nodes
6.     if (POIs in merged N > k)
7.         return N
8.     else
9.         search parent node
      /*repeat 3~9 until k satisfied*/
```

그림 8. k-최근접점 탐색 알고리즘

4. 결론 및 향후 연구

본 논문에서는 사용자의 위치 정보와 POI정보 보호를 모두 고려한 Approximate k-최근접점 질의처리 알고리즘을 제안하였다. 제안하는 기법은 Location Cloaking 영역 기반으로 질의를 수행하기 때문에 질의 요청자의 위치 정보 및 질의를 보호한다. 또한, 서버에서 POI 색인 시에 Overlapped Indexing 기법을 통해 한 노드에 저장되는 POI 수를 증가하여 k-최근접점 탐색의 정확도를 높이고, 결과 후보 POI 수를 증가시켜 확장을 최소화하였다. 아울러 결과 집합을 Cloaking 영역에 대한 PIR 프로토콜을 사용하여 통신함으로써 사용자에게 반환되는 POI 수를 최소화하고, 위치 기반 서버에서도 POI 정보 유출을 최소화하는 기법이다.

향후 연구로는 제안하는 알고리즘을 구현하여 그 성능을 입증하는 것이다.

참고 문헌

이준석, 김서균, "위치기반서비스(LBS)의 기 술 동향 및 국내외 산업 동향 분석", 정보통 신 연구진흥 5권 2호 (통권 16호), 2003

USA Central Intelligence Agency, https://www.cia.gov/library/publications/the-world-factbook/rankorder/2153rank.html, 2006

International Telecommunication Union (ITU) http://www.itu.int/

Foxs News. Man Accused of Stalking Ex-Girlfriend With GPS, http://www.foxnews.com/story/0,2933,131487 ,00.html, 2004

USA TODAY News, GPS System used to stalk woman, http://www.usatoday.com/tech/news/2002-12-30-gps-stalker_x.htm, 2002

G. Ghinita, P. Kalnis and S. Skiadopoulos, "PRIVE: Anonymous Location-Based

Queries in Distributed Mobile Systems," In Proc of World Wide Web, May 2007

G. Ghinita, P. Kalnis and S. Skiadopoulos, "MobiHide: A Mobilea Peer-to-Peer System for Anonymous Location-Based Queries," In Proc. of International Symposium on Spatial and Temporal Databases, vol.4605/2007, pp. 221-238, November 2007

P. Kalnis, G. Ghinita, K. Mouratidis and D. Papadias, "Preventing Location -Based Identity Inference in Anonymous Spatial Queries," In Proc. of Transactions on Knowledge and Data Engineering, February 2007.

W. Ku, Y. Chen and R. Zimmermann, "Privacy Protected Spatial Query Processing for Advanced LBSs" Wireless Personal Communications 2009 Volume 51, Number 1, October 2009

M. Mokbel, C. Chow, and W. Aref, "The New Casper:Query Processing for Location Services without Compromising Privacy," In Proc. of the International Conference on Very Large Data Bases, pp. 763-774, September 2006.

C. Y. Chow, M. F. Mokbel, and X. Liu. A, "Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-based Services," In Proc. of the ACM International Symposium on Advances in Geographic Information Systems, pp. 171-178, November 2006.

B. Bamba and L. Liu, "PRIVACYGRID: Supporting Anonymous Location Queries in Mobile Environments" Research report in National Technical Information Service, 2007.

Kushilevitz, E., Ostrovsky, R.: Replication is NOT Needed: SINGLE Database, Computationally-Private Information Retrieval. In: FOCS (1997)

G. Ghinita et al, "Private Queries in Location Based Services: Anonymizers are not Necessary" In Proc. of ACM SIGMOD international conference on Management of data, 2008

G. Ghinita et al, "A Hybrid Technique for Private Location-Based Queries with Database Protection" In Proc. of SSTD International Symposium, 2009

Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223-238. Springer, Heidelberg (1999)