위치 기반 서비스에서 도로 네트워크의 거리 정보를 이용한 사용자 정보 은닉 기법

Road Network Distance based User Privacy Protection Scheme in Location-based Services

김 형 일[*] 신 영 성[**] 장 재 우[***]
Hyeong Il Kim Young Sung Shin Jae Woo Chang

요 약 최근 PDA, 휴대폰과 같은 모바일 기기 및 GPS와 같은 무선 통신 기술의 발달로 인하여 위치 기반 서비스의 이용이 확산되었다. 하지만 이러한 서비스는 사용자가 도로 네트워크에서 이동하면서 자신의 위치정보를 통해 LBS 서버에 질의를 요청하기 때문에, 심각한 개인 정보 누출의 위협이 될 수 있다. 따라서 모바일 사용자의 안전하고 편리한 위치기반 서비스 사용을 위한 개인 정보 보호 기법이 필요하다. 이를 위해 본 논문에서는 위치 기반 서비스에서 사용자 정보 보호를 지원하는 도로 네트워크 거리 기반 클로킹 기법을 제안한다. 제안하는 기법은 도로 네트워크에서 효율적이고 안전한 위치기반 서비스를 지원하기 위하여, 도로 네트워크의 거리를 고려하여 클로킹 영역을 설정한다. 아울러, 성능평가를 통해서 제안하는 기법이 클로킹 영역 및 서비스 시간 측면에서 기존 연구보다 우수함을 보인다.

키워드 : 위치 기반 서비스, 도로 네트워크, 개인 정보 보호, 거리 기반 클로킹 기법

Abstract Recent development in wireless communication technology like GPS as well as mobile equipments like PDA and cellular phone makes location-based services (LBSs) popular. However, because users request a query to LBS servers by using their exact locations while moving on the road network, users' privacy may not be protected in the LBSs. Therefore, a mechanism for users' privacy protection is required for the safe and comfortable use of LBSs by mobile users. For this, we, in this paper, propose a road network distance based cloaking scheme supporting user privacy protection in location-based services. The proposed scheme creates a cloaking area by considering road network distance, in order to support the efficient and safe LBSs on the road network. Finally, we show from our performance analysis that our cloaking scheme outperforms the existing cloaking scheme in terms of cloaking area and service time.

Keywords : Location-Based Services, Road network, Privacy protection, Distance-based cloaking scheme

1. 서 론

최근 PDA, 휴대폰과 같은 모바일 기기 및 GPS와 같은 무선 통신 기술의 발달로 인하여 위치 기반 서비스(Location-Based Service : LBS)의 이용이 확산되었다. LBS란 유무선 통신망을 통해 얻은 위치정보를 부가적인 정보와 결합하여 사용자가 필요로 하는 유용한 응용 서비스를 제공하는 것이다 [2, 4]. 모바일 사용자는 자신의 위치정보를 LBS 서버에 보내어 교통 정보, 친구 찾기, 인접한 POI(Point Of Interest) 찾기 등 다양한 종류의 위치 기반 서비스를 이용할 수 있다. 그러나 이와 같이 사용자의 정확한 위치정보를 통해 LBS 서버에 위치 기반 서비스를 요청하는 것은 심각한 개인 정

† 본 논문은 중소기업청에서 지원하는 2012년도 산학연공동기술개발사업(과제번호 C0055482)의 연구수행으로 인한 결과물임을 밝힙니다.

* 전북대학교 컴퓨터공학과 박사과정 melipion@jbnu.ac.kr
** 전북대학교 컴퓨터공학과 석사과정 twotoma@jbnu.ac.kr
*** 전북대학교 컴퓨터공학과 교수 jwchang@jbnu.ac.kr (교신저자)

보 누출의 위협이 될 수 있다. 이는 LBS 서버에 보내진 사용자의 위치정보가 유/무선 통신상에서 유출될 경우, 서비스 사용자가 어느 장소를 자주 방문하는지, 또한 이러한 방문이 어느 시간대에 주로 이뤄지는지를 파악하는 것이 가능하기 때문이다. 이를 통해 사용자의 생활 스타일, 질병 정보 등 개인 정보 유추가 가능하다. 실제로 위치 기반 서비스를 이용하는 사용자를 대상으로 하는 스토킹이나 개인정보 유출 사례가 빈번히 발생하고 있다[9, 10]. 따라서 사용자의 안전하고 편리한 위치기반 서비스 사용을 위한 개인 정보 보호 방법이 요구된다.

위치기반 서비스에서 사용자의 위치정보 보호를 위한 연구로는 K-Anonymity를 만족하는 클로킹 영역을 설정하는 연구가 대표적이다. 이 기법은 LBS 서버에 질의(서비스) 전송 시 질의를 요청한 사용자의 위치정보와 k-1명의 인접한 사용자의 위치정보를 포함하는 클로킹 영역을 전송함으로써, 사용자의 신원 노출 확률을 1/k로 감소시키고 사용자의 정확한 위치정보를 은닉한다. 그러나 이와 같은 기법은 유클리디언 공간 상의 사용자 위치를 고려하여 클로킹 영역을 설정하기 때문에, 실제 도로 네트워크를 고려한 환경에서는 다음과 같은 문제점을 보인다. 첫째, 설정된 클로킹 영역이 도로 네트워크상으로 연결되어 있지 않은 도로, 혹은 가깝지 않은 도로상의 사용자를 포함할 수 있기 때문에, 질의 결과의 정확도가 감소될 수 있다. 둘째, 설정된 클로킹 영역이 포함하는 도로의 수가 적을 수 있기 때문에, 사용자가 존재하는 도로 정보와 이를 통한 사용자의 이동 경로 및 위치정보(e.g., 건물)가 노출될 수 있다. 이러한 문제점을 해결하기 위한 대표적인 연구로 Ting Wang et al.의 연구[11]에서는 XStar를 제안하였다. XStar는 도로 네트워크상의 교차노드(intersection node)에 질의 요청자를 할당시킨 후, 해당 노드에 교차하는 도로의 집합을 클로킹 영역으로 설정하는 기법이다. 이때, 설정되는 클로킹 영역은 질의 요청자가 요청한 클로킹 영역 안에 포함되기를 원하는 사용자의 수(K-anonymity) 및 도로의 수(L-diversity)를 만족하며, 클로킹 영역에 포함된 노드 간 최대 hop 수(S-tolerance)를 벗어나지 않는다. 이처럼 도로 네트워크를 기반으로 한 클로킹 영역 설정을 통해, 사용자와 인접하지 않은 도로상의 사용자가 클로킹 영역에 포함되는 것을 방지하고, 아울러 사용자의 신원 및 사용자가 위치한 도로가 노출되는 것을 방지한다. 하지만, XStar는 사용자를 노드에 할당하거나 슈퍼스타(Super Star)를 구성할 때, 실제 도로 네트워크의 거리를 고려하지 않기 때문에 설정되는 클로킹 영역의 크기가 크다. 이로 인해, 실제로 질의 요청자와 인접하지 않은 질의 결과가 반환되거나, 질의 처리 시간이 증가되는 문제점을 보인다.

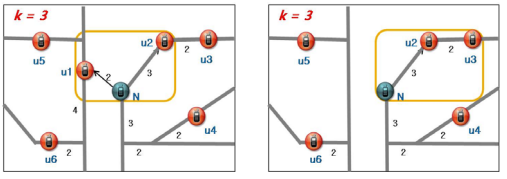
따라서 본 논문에서는 이러한 문제점을 해결하기 위해, 위치 기반 서비스에서 도로 네트워크의 거리 정보를 이용한 사용자 정보 은닉 기법을 제안한다. 이를 위해, 첫째, 질의 요청자를 교차 노드에 할당할 때 각 노드와 교차하는 도로의 거리를 고려하여, 설정되는 총 클로킹 영역이 작은 노드에 질의 요청자가 할당될 확률을 높인다. 둘째, 슈퍼스타 구성 시 인접한 노드까지의 도로 네트워크 거리를 고려하여, 비효율적인 클로킹 영역이 설정되는 것을 방지한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 클로킹 기법들을 소개한다. 3장에서는 사용자 정보 보호를 지원하는 도로 네트워크 거리 기반 클로킹 기법을 제안하고, 4장에서는 제안하는 기법과 기존 기법과의 성능 비교를 수행한다. 마지막으로 5장에서는 결론 및 향후 연구에 대해 기술한다.

2. 관련 연구

위치기반 서비스에서 사용자의 위치정보 보호를 위한 기법 중, K-anonymity를 고려하여 클로킹 영역을 설정하는 대표적인 연구는 다음과 같다[2, 3, 5, 7, 12]. 첫째, M. Gruteser et al. 연구[2]는 Quad-tree를 기반으로 K-anonymity를 이용한 클로킹 기법을 제안하였다. 아울러, M. Mokbel et al. 연구[7]는 그리드 기반의 피라미드 데이터 구조를 사용하여 클로킹 영역을 설정하는 기법을 제안하였다. 또한, G. Ghinita et al.의 연구[3]는 힐버트 커브를 이용하여 사용자의 위치를 1차원으로 암호화하고 분산 해쉬 테이블 구조인 Chord를 구성하여, 이를 기반으로 클로킹 영역을 설정하는 기법을 제안하였다. 마지막으로, T. Xu et al.의 연구[12] 및 A. Lee et al.의 연구[5]에서는 엔트로피(Entropy)를 사용하여 설정되는 클로킹 영역의 Anonymity 정도(Anonymity Degree)를 계산함으로써, 질의 요청자의 노출을 방지할 수 있는 기법을 제안하였다. 그러

나 이러한 클로킹 기법들은 유클리디언 공간 상의 사용자 위치를 고려하여 클로킹 영역을 설정하기 때문에 다음과 같은 문제점을 보인다. 첫째, 설정된 클로킹 영역이 도로 네트워크 상으로 연결되어 있지 않은 도로 혹은 가깝지 않은 도로 상의 사용자를 포함할 수 있기 때문에, 질의 결과의 정확도가 낮아질 수 있다는 문제를 지닌다. 예를 들어, 질의를 요청한 사용자(N)가 k=3를 요청한다고 가정할 때, 그림 1(a)는 이러한 문제점을 보여준다. N이 유클리디언 공간 상에서 가까운 2명의 사용자를 찾을 경우, u1과 u2가 설정되는 클로킹 영역에 포함된다. 하지만 실제 도로 네트워크 상에서 u1은 질의 요청자 N과 연결되어 있지 않은 도로상에 존재한다. 따라서 이러한 클로킹 영역을 통해서 질의를 요청할 경우, 실제로 질의 요청자가 원하지 않는 결과가 반환될 수 있다. 이러한 문제를 해결하기 위해, 도로 네트워크 상에서 가까운 사용자를 포함하는 클로킹 영역을 생성할 수 있다. 하지만, 이러한 기법은 설정되는 클로킹 영역이 포함하는 도로의 수가 적을 수 있기 때문에, 사용자가 존재하는 도로 정보와 이를 통한 사용자의 이동 경로 및 위치 파악이 가능하다는 문제점을 지닌다. 그림 1(b)는 이러한 문제점을 보여준다. 질의 요청자 N이 도로 네트워크 상으로 가까운 u2와 u3를 포함하는 클로킹 영역을 설정할 경우, 설정되는 클로킹 영역 안에는 하나의 도로만이 존재한다. 이러한 경우, 질의 요청자가 현재 존재하는 도로의 정보 뿐 아니라 사용자의 이동 경로 또한 예측이 가능하다는 문제점을 보인다.



(a) (b)

그림 1. 도로 네트워크를 고려하지 않을 때 발생하는 문제

이와 같은 문제점을 해결하기 위해, 도로 네트워크를 고려하여 클로킹 영역을 설정하는 연구[11, 13]가 수행되었다. 먼저, T. Wang et al.의 연구[11]인 XStar는 도로 네트워크 상의 교차 노드에 질의 요청자를 할당시킨 후, 해당 노드에 교차하는 도로의 집합을 클로킹 영역으로 설정하는 기법이다. 여기서 교차 노드란 3개 이상의 도로가 교차(degree ≥3)하는 지점을 말한다. 한편, XStar의 클로킹 영역 설정 과정은 다음과 같다. 첫째, 질의 요청자가 위치한 도로의 양 끝 교차 노드를 찾는다. 이 후, 각 교차 노드를 지나는 도로의 수(degree)를 고려하여 질의 요청자를 한 교차 노드에 할당한다. 이 때, degree가 작은 노드일수록, 사용자가 해당 노드에 할당될 확률이 높다. 만약 선택된 교차 노드를 지나는 도로의 집합이 해당 영역에 속한 모든 사용자의 K- anonymity 및 L-diversity 요구 수준을 만족한다면, 선택된 도로의 집합이 클로킹 영역으로 설정된다. 둘째, 선택된 교차 노드가 할당된 사용자의 요구 조건을 만족하지 못할 경우, 해당 노드는 인접한 교차 노드와의 병합을 통해 슈퍼스타를 구성한다. 만약 구성된 슈퍼스타가 해당 영역에 속한 모든 사용자의 K-anonymity 및 L-diversity 요구 수준을 만족한다면, 해당 슈퍼스타가 사용자들이 요구하는 S- tolerance를 만족하는지 검사한다. 여기서 S-tolerance란 사용자가 클로킹 영역으로 설정된 슈퍼스타 내에서 허용할 수 있는 교차 노드들 간의 최대 홉(hop) 수를 의미한다. 만약, 설정된 슈퍼스타가 사용자들의 S-tolerance 요구 조건에 위배되지 않는다면, 해당 슈퍼스타가 포함하는 도로의 집합이 클로킹 영역으로 설정된다. 다음으로, E. Yigitoglu의 연구[13]는 센시티브 지역(e.g., 공원, 병원, 학교 등)을 고려한 클로킹 영역 설정 기법을 제안하였다. 해당 기법은 사용자가 한 센시티브 지역에 장시간 머무르는 경우 사용자의 위치가 드러날 수 있는 문제를 해결하기 위해, 다수의 센시티브 지역을 포함하는 클로킹 영역을 설정한다.

한편, B. Palanisamy의 연구[8]인 MobiMix는 궤적 빈도가 높은 교차로를 mix-zone으로 정의하고, 이에 포함된 궤적의 pseudonym을 변경하여 정보 보호를 수행하는 기법이다. 하지만 해당 기법은 도로의 방향성을 고려하지 못하기 때문에, 실제 도로 네트워크 환경에서 발생하기 어려운 진입 및 진출 방향을 지니는 궤적이 생성될 수 있다. 따라서 이를 이용하여 공격자가 원본 궤적 데이터를 쉽게 유추할 수 있는 문제점이 존재한다.

3. 위치 기반 서비스에서 사용자 정보 보호를 지원하는 도로 네트워크 거리 기반 클로킹 기법

3.1 연구 동기

도로 네트워크를 고려하여 클로킹 영역을 설정하는 유일한 연구인 XStar는 기존 유클리디언 상의 위치를 기반으로 클로킹 영역을 설정하는 기법들이 갖는 문제점을 해결하였다. 그러나 XStar는 클로킹 영역을 설정할 때 도로 네트워크의 실제 거리를 고려하지 않기 때문에 다음과 같은 문제점을 지닌다. 첫째, 질의 요청자가 할당될 교차 노드를 선택하기 위해 교차 노드의 degree만을 고려하기 때문에, 설정되는 클로킹 영역의 크기가 커져, 질의 처리 비용이 증가할 수 있다. 그림 2에서 질의 요청자 N이 (l, k, s)=(4, 2, 1)을 요청했다고 가정할 때, n_1 노드는 degree가 3, n_2 노드는 degree가 4 이기 때문에, N은 n_1 노드에 할당될 확률이 높다. 하지만, n_1 노드에 교차하는 도로의 총 길이는 1,700, n_2 노드에 교차하는 도로의 총 길이는 800으로, n_1이 설정하는 클로킹 영역이 n_2가 설정하는 클로킹 영역보다 크며, 이러한 교차 노드로 질의 요청자가 할당될 경우 질의 처리 비용이 증가하게 된다. 한편, n_1 노드가 선택되었을 경우 설정되는 클로킹 영역은 그림의 굵은 실선으로 표시된 도로와 같다. 둘째, 슈퍼스타를 구성할 때 제약 조건으로 hop만을 고려하기 때문에, 실제 도로 네트워크 상으로 가까운 노드가 슈퍼스타 구성의 후보로 고려되지 않거나, 비효율적으로 먼 노드가 슈퍼스타 구성에 포함될 수 있다. 그림 2에서 질의 요청자 N이 n_1 노드에 할당되었고 n_1 노드만으로는 사용자 N의 질의를 충족할 수 없다고 가정할 때, n_1은 슈퍼스타 구성을 위해 인접한 교차 노드를 탐색한다. 이 때, N이 요구하는 S-tolerance가 1이기 때문에 n_1에서 1 hop 내에 있는 교차 노드들이 슈퍼스타 구성을 위한 후보 노드로 고려된다. 즉, n_2, n_3, n_8 노드가 슈퍼스타 구성을 위한 후보로 설정된다. 하지만, n_4, n_6와 같이 도로 네트워크 상으로 가까운 노드가 고려되지 않거나, n_8과 같이 비효율적으로 먼 노드가 후보로 고려될 수 있다. 따라서 본 논문에서는 도로 네트워크의 거리를 고려하여 효율적으로 위치기반 서비스를 지원할 수 있는 클로킹 영역 설정 기법을 제안한다.

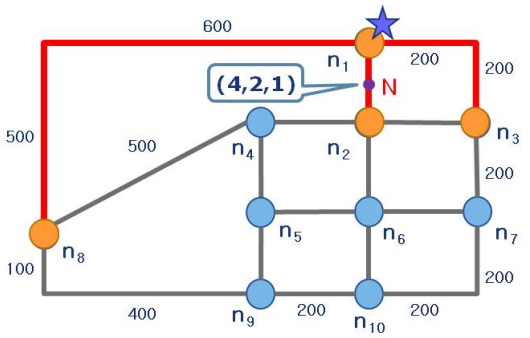


그림 2. XStar의 문제점

3.2 시스템 구조

본 논문에서는 클로킹 영역을 설정하는 주체가 anonymizer인 중앙 집중 방식을 사용하며, 시스템 구조는 그림 3과 같다. 시스템 구조는 크게 모바일 사용자와 anonymizer, 그리고 LBS 서버로 구성된다. 여기서 anonymizer란 모바일 사용자와 LBS 서버 중간에 존재하는 신뢰할 수 있는 서버로, 각 도로의 길이를 포함한 전체 도로 네트워크의 정보 및 모바일 사용자에 대한 정보를 저장하고 있으며, 클로킹 영역을 설정하는 주체이다.

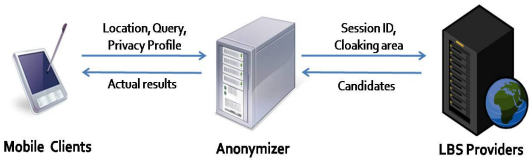


그림 3. 사용하는 시스템 구조

위의 시스템 구조를 고려하여 사용자의 질의를 수행하는 과정은 다음과 같다. 질의 요청자는 자신의 위치정보와 질의를 Privacy Profile과 함께 anonymizer로 전송한다. 여기서 Privacy Profile이란 사용자가 클로킹 영역이 제공해 주기를 원하는 정보보호 요구조건을 의미하며, K-anonymity, L-diversity, D-tolerance로 구성된다. K-anonymity와 L-diversity는 각각 질의 요청자가 클로킹 영역 안에 포함되기를 원하는 사용자의 수 및 도로의 수를 의미하며, D-tolerance는 질의 요청자가 설정되는 클로킹 영역 내에서 허용할 수 있는 교차 노드들 간의 최대 거리를 의미한다. 또한, anonymizer는 질의 요청자로부터 전송받은 정보들을 바탕으로 클로킹 영역을 설정한 후, session ID와 함께 이를 LBS

서버로 전송한다. LBS 서버는 전송받은 클로킹 영역을 기반으로 질의를 수행하고, 후보 결과 집합을 anonymizer로 전송한다. Anonymizer는 질의 요청자의 실제 위치를 고려하여 후보 결과 집합에서 정확한 결과를 얻고, 이를 질의 요청자에게 전송한다.

3.3 도로 네트워크 거리에 근거한 클로킹 영역 설정 기법

본 절에서는 위치 기반 서비스에서 사용자 정보 보호를 지원하는 도로 네트워크 거리 기반 클로킹 기법을 제안한다. 알고리즘은 크게 질의 요청자를 교차 노드에 할당하는 교차노드 선택 단계와, 해당 교차 노드가 질의 요청자의 service profile을 충족하지 못 할 경우 인접 교차노드와 병합하여 슈퍼스타를 구성하는 슈퍼스타 구성 단계로 수행된다.

수행단계 1. 교차노드 선택 단계

질의 요청자로부터 질의를 전송받으면, anonymizer는 질의 요청자가 위치한 도로와 해당 도로의 양 끝 교차 노드를 찾는다. 다음으로 질의 요청자와 질의 요청자가 속한 도로(s)를 이 중 한 노드에 할당하며, 할당 알고리즘은 다음과 같다. 첫째, 만약 s가 양 끝 교차 노드 중 이미 어느 한 교차 노드에 할당되어 있다면, 질의 요청자를 해당 교차 노드에 할당한 후, 알고리즘을 종료한다. 둘째, 양 끝 교차 노드가 다른 도로를 할당하고 있지만, s가 할당되어 있지 않다면, 각 교차 노드에서의 질의 처리 비용을 고려하여 s를 한 교차 노드에 할당한다. 셋째, s를 할당하고 있지 않더라도, 어느 한 교차 노드만이 다른 도로를 할당하고 있다면, s를 해당 교차 노드로 할당한다. 넷째, 양 끝 교차 노드 모두 어떠한 도로도 할당하고 있지 않다면, 각 교차 노드에서의 질의 처리 비용을 고려하여 s를 한 교차노드에 할당한다. 한편, 질의 처리 비용은 클로킹 영역으로 설정된 도로의 수와 설정된 도로의 총 길이에 영향을 받으며, (식) 1을 통해 계산한다.

$$cost(A)=\alpha*degree(A)+\beta*\sum Dist(A_i)/T \quad (1)$$

여기서 A는 교차 노드, α, β는 각각 degree와 네트워크 거리에 대한 가중치, degree(A)는 A 노드를 지나는 도로의 수를 의미하며, $Dist(A_i)$는 A 노드와 교차하는 각 도로의 길이, T는 거리의 한계 값(threshold)을 의미한다. 식을 통해 일정 한계 값을 넘지 않는 도로는 질의 처리 비용에 영향을 주지 않지만, 그렇지 않은 경우에는 한계 값을 벗어난 정도에 비례하여 질의 처리 비용에 영향을 줌을 알 수 있다. 각 노드의 cost가 계산된 후, 각 노드가 선택될 확률은 식 (2)와 같다.

$$Prob(A)=cost(B)/(cost(A)+cost(B)) \quad (2)$$

즉, 자신의 cost가 높을수록, 자신이 선택될 확률은 낮아진다. 한편, 질의 요청자가 속한 도로가 교차 노드에 할당되면, 해당 노드와 인접한 도로들의 집합이 클로킹 영역으로 고려된다. 만약 해당 영역이 할당된 질의 요청자가 요구한 K-anonymity 및 L-diversity를 보장한다면, 이를 최종 클로킹 영역으로 설정한다. 그림 4는 교차 노드 선택 단계에 대한 예제를 보인다. 그림에서 질의 요청자(N)가 위치한 도로는 노드 n_1와 n_2를 양 끝단 노드로 고려한다. 만약, 두 노드가 어떠한 도로도 포함하고 있지 않다면, 알고리즘의 네 번째 단계를 따라 각 노드에서의 질의 처리 비용을 계산한다. 예제에서 α, β는 1로 동일하며, T는 300이라고 가정한다. 이때 노드 n_1의 degree는 3(n_1n_2, n_1n_3, n_1n_8), 노드 n_1를 지나는 도로 중 길이가 T를 넘는 도로는 2(n_1n_3(400), n_1n_8(1,100)) 이므로, 노드 n_1의 cost는 다음과 같이 계산된다.

$$cost(n_1) = 1*3 + 1*(400/300 + 1{,}100/300) = 7$$

또한, 노드 n_2의 degree는 4(n_2n_1, n_2n_3, n_2n_4, n_2n_6)이며, 노드 n_2를 지나는 도로 중 길이가 T를 넘는 도로는 존재하지 않으므로, 노드 n_2의 cost는 다음

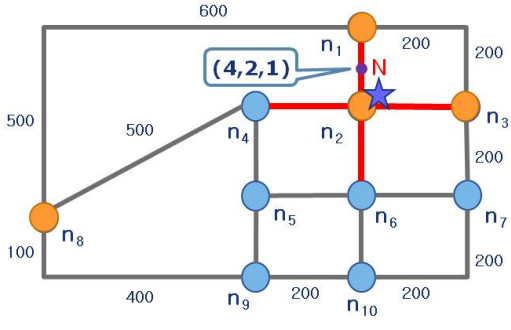


그림 4. 교차 노드 선택 단계 예제

과 같이 계산된다.

$cost(n_2) = 1*4 + 1*0 = 4$

따라서 식 (2)를 통해, 노드 n_1이 선택될 확률은 4/11, n_2가 선택될 확률은 7/11이 된다. 한편, n_2 노드가 선택되었을 경우 설정되는 클로킹 영역은 그림의 굵은 실선으로 표시된 도로와 같다.

수행단계 2. 슈퍼스타 구성 단계

만약 수행단계 1에서 설정된 클로킹 영역이 사용자가 요구한 service profile을 만족하지 못하는 경우, 해당 교차노드는 인접한 교차노드와의 병합을 수행한다. 이때 하나 이상의 도로를 할당하고 있는 노드만이 병합 대상이 된다. 병합을 통해 구성된 슈퍼스타가 해당 영역에 속한 모든 사용자의 K-anonymity 및 L-diversity 요구 수준을 만족하면, 해당 슈퍼스타가 사용자들이 요구하는 D-tolerance를 만족하는지 검사한다. 만약, 설정된 슈퍼스타가 사용자들의 D-tolerance 요구 조건을 만족하면, 해당 슈퍼스타가 포함하는 도로의 집합이 최종 클로킹 영역으로 설정된다. 그림 4에서 질의 요청자 N이 n_2 노드에 할당되고 n_2 노드만으로는 사용자 N의 질의를 충족할 수 없다고 가정할 때, n_2는 슈퍼스타 구성을 위해 인접한 교차 노드를 탐색한다. N이 요구하는 D-tolerance가 1이기 때문에 n2에서 1 hop 내에 있는 교차 노드들이 슈퍼스타 구성을 위한 후보 노드로 고려된다. 즉, n_1, n_3, n_4, n_6 노드가 슈퍼스타 구성을 위한 후보로 설정된다. 이러한 경우, 질의 요청자가 n_1에 할당되었을 때보다 N에 보다 가까운 노드들이 선택됨을 알 수 있다. 수행단계 1, 2를 고려한 알고리즘은 그림 5와 같다.

첫째, 질의 요청자의 위치정보를 통해 질의 요청자가 위치한 도로(s)를 찾는다(line 1). 둘째, 만약 s가 이미 양 끝단 노드 중 어느 한 노드에 할당되어 있다면, 해당 노드를 선택한다(line 2~3). s가 아직 할당되지 않았고, s의 양 끝단 노드가 다른 도로를 할당하고 있다면, 각 노드의 cost를 계산하여, 클로킹 영역 설정을 위한 노드를 선택한다(line 4~7). s가 아직 할당되지 않았고, s의 양 끝단 노드 중 한 노드만이 다른 도로로 할당되어 있으면, 해당 노드를 선택한다(line 8~9). s의 양 노드 모두 어떠한 도로도 포함하고 있지 않다면, 각 노드의 cost를 계

```
Distance-based Cloaking Algorithm
Input : <qx, qy>    //질의 요청자의 위치정보
        k, l, d     //Service Profile
Output : CS         //Cloaking Segments
1.  seg = FindSegment(qx, qy)
//Node Selection Phase
2.  if(seg is already assigend to one node)
3.    node = seg.node;
4.  else if(both end nodes of seg==active)
5.    if(seg is not yet assigned)
6.      CalculateCost(snode, enode);
7.      node = SelectNode(snode, enode)
8.  else if(only 1 node is active)
9.      node = activenode;
10. else
11.   CalculateCost(snode, enode);
12.   node = SelectNode(snode, enode);
13. if(CheckPrivacyProfile(k, l);
14.    CS=SetCloakSeg(node.adjseg);
15.    break;
//Superstar Construction Phase
15. else
16.   while(FindAdjNode())
17.     super=ExpandNode(node);
18.     if(CheckPrivacyProfile(k, l, d);
19.       CS=SetCloakSeg(super.adjseg);
20.       break;
End Algorithm
```

그림 5. 제안하는 기법의 수행 알고리즘

산하여, 클로킹 영역 설정을 위한 노드를 선택한다(line 10~12). 셋째, 선택된 노드가 사용자가 요구한 K-anonymity와 L-diversity를 만족하면, 해당 노드를 지나는 도로의 집합을 클로킹 영역으로 반환하고 알고리즘을 종료한다(line 13~15). 넷째, 선택된 노드가 사용자의 요구한 조건을 만족하지 못하면, 인접한 노드와의 병합을 통해 슈퍼스타를 구성한다(line 15~17). 만약, 구성된 슈퍼스타가 사용자가 요구하는 service profile을 만족할 경우, 해당 슈퍼스타를 지나는 도로의 집합을 클로킹 영역으로 반환하고 알고리즘을 종료한다(line 18~20).

4. 성능 평가

본 장에서는 위치 기반 서비스에서 사용자 정보 보호를 지원하는 도로 네트워크 거리 기반 클로킹 기법(이하 DStar)의 우수성을 검증하기 위하여 성능 평가를 수행한다. 본 연구는 도로 네트워크에서

지속적으로 이동하는 사용자를 고려하여 클로킹 영역 설정하기 때문에, 기존 기법 중 해당 환경을 고려하여 연구된 XStar와 성능평가를 수행한다. 한편, E. Yigitoglu의 연구[13]는 한 장소에 장시간 정체하는 사용자를 고려하기 때문에 지속적으로 이동하는 사용자를 고려하는 본 연구와는 서비스 대상이 다르다. 즉, 사용자의 이동 패턴에 따라 DStar와 병행하여 사용할 수 있는 기법이기 때문에 해당 기법과의 성능비교는 수행하지 않는다. 성능 평가 항목으로는 L-diversity, K-anonymity, D-tolerance의 변화에 따른 클로킹 영역의 총 길이, 클로킹 영역 내에 포함된 도로의 수, 총 서비스 시간, 그리고 클로킹 영역 설정 성공률을 측정한다. 여기에서 총 서비스 시간은 클로킹 영역 설정 시간과 설정된 클로킹 영역에 대한 영역 질의 처리 시간을 합한 시간이다. 성능 평가의 실험 환경은 표 1과 같다.

표 1. 실험 환경

항목	성능
CPU	Intel Core2 Duo CPU E4500 2.20GHz
Memory	2GB
OS	Windows XP professional
Compiler	Microsoft Visual Studio .Net 2003

아울러, 이동객체 데이터는 Network-based Generator[1]를 사용하여 미국 샌프란시스코의(600㎢) 실제 도로 네트워크를 기반으로 10,000건을 생성하였다. 또한 XStar의 홉(hop)과 제안하는 기법의 거리 간의 비교를 위해 샌프란시스코의 도로 정보를 분석하여, 1 홉 당 평균 거리인 약 410m를 제안하는 기법의 표준 거리로 사용하였다. 표 2는 성능 평가에 사용된 매개변수들이다.

표 2. 실험 환경 매개변수

매개변수	평균	분산
L-diversity	5	1
K-anonymity	5	1
D-diversity	410*4홉	410(m)
range	1km	-

4.1 L-diversity(이하 L) 변화에 따른 성능평가

그림 6은 L 변화에 따라 설정되는 클로킹 영역의 총 길이를 비교한 것이다. 두 기법 모두 L 값이 증가함에 따라 클로킹 영역의 총 길이가 증가한다. L이 6인 경우 XStar는 3,771m, DStar는 2,862m의 클로킹 영역을 설정한다. DStar가 XStar에 비해 작은 영역을 설정하는 이유는, 교차노드 선택 시 도로 네트워크의 실제 거리를 고려함으로써, 클로킹 영역이 작게 설정되는 교차 노드에 질의 요청자 및 질의 요청자가 포함된 도로가 할당될 확률을 높였기 때문이다. 또한, 슈퍼스타 구성 시 D-tolerance 검사를 통해, 제약조건에 위배되는 질의 요청자로부터 먼 거리의 노드가 슈퍼스타에 포함되지 못하게 했기 때문이다.

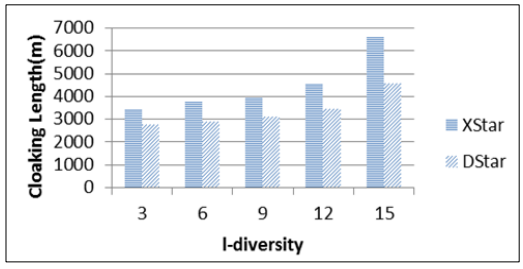


그림 6. L 변화에 따른 클러킹 영역

<그림 7>은 L 변화에 따라 설정되는 클로킹 영역 내 포함된 도로의 수를 비교한 것이다. 두 기법 모두 L 값이 증가함에 따라 클로킹 영역에 포함된 도로의 수가 증가한다. L이 6인 경우 XStar는 8.66개, DStar는 8.82개의 도로를 포함한다. DStar는 실제 도로 네트워크 거리를 고려하여 클로킹 영역을 설정하기 위한 도로를 선택하기 때문에, XStar에 비해 평균적으로 짧은 도로가 선택될 확률이 높다. 이로 인해, D-tolerance를 만족하는 범위 내에서 보다 많은 도로를 포함하는 것이 가능하다. 이를 통해 공격자가 클로킹 영역 내에서 실제로 질의 요청자가 존재하는 도로를 알아낼 확률이 낮아지기 때문에, DStar가 XStar에 비해 사용자 프라이버시 보호 측면에서 우수함을 알 수 있다.

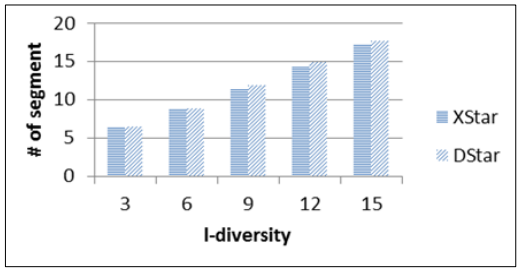


그림 7. L 변화에 따른 클러킹 영역 내 도로의 수

그림 8은 L 변화에 따른 총 서비스 시간을 나타낸다. 두 기법 모두 L 값이 증가함에 따라 소요 시간이 증가함을 알 수 있다. L이 6인 경우, XStar는 2.09, DStar는 1.92가 소요된다. 한편, 전체적인 서비스 시간 측면에서 DStar가 보다 우수한 성능을 보이는 이유는, DStar가 XStar에 비해 작은 클로킹 영역을 설정하여(그림 6) 영역 질의 처리 시간 측면에서 우수한 성능을 보이기 때문이다. 특히, LBS는 대량의 사용자에 대한 연속적인 질의를 전제로 하기 때문에, 질의 처리 시간을 개선함으로써 대량의 질의 처리를 수행해야 하는 서비스 제공자의 질의 처리 비용을 크게 감소시킬 수 있다.

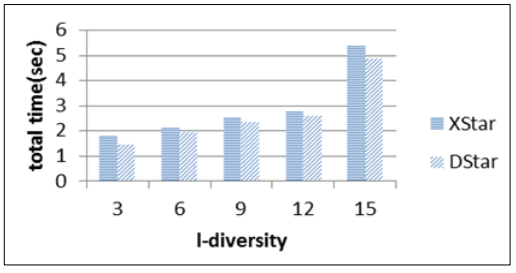


그림 8. L 변화에 따른 총 서비스 시간

<그림 9는 L변화에 따른 클로킹 영역 설정 성공률을 나타내기 위해, 총 만개의 질의 중에서 처리된 질의의 수를 로그로 표현한 것이다. DStar가 XStar에 비해 다소 낮은 성공률을 보이는 이유는, DStar는 슈퍼스타 구성 시 비효율적으로 먼 노드가 포함되는 것을 도로 네트워크의 실제 거리를 고려하여 방지하기 때문이다.

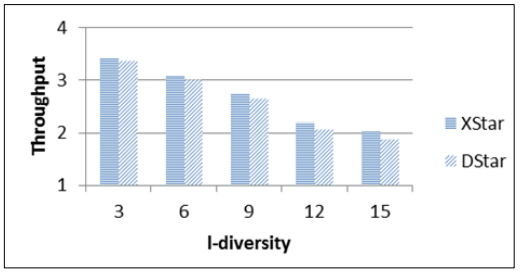


그림 9. L 변화에 따른 영역 설정 성공률

4.2 K-anonymity(이하 K) 변화에 따른 성능평가

그림 10은 K 변화에 따른 클로킹 영역의 총 길이를 비교한 것이다. 두 기법 모두 K값이 증가함에 따라 클로킹 영역의 총 길이가 증가한다. K가 6인 경우 XStar는 3,954m, DStar는 3,062m의 클로킹 영역을 설정한다. DStar는 도로의 거리를 고려하여 클로킹 영역을 설정하기 때문에, XStar에 비해 보다 작은 클로킹 영역을 설정함을 알 수 있다.

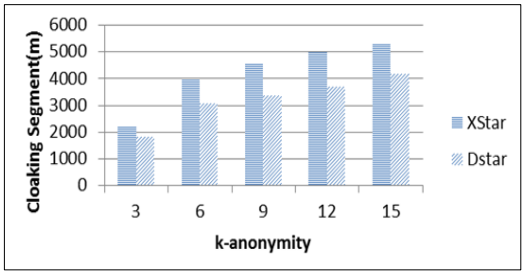


그림 10. K 변화에 따른 클러킹 영역

그림 11은 K 변화에 따라 설정되는 클로킹 영역 내 포함된 도로의 수를 비교한 것이다. 두 기법 모두 K 값이 증가함에 따라 클로킹 영역에 포함된 도로의 수가 증가한다. L이 6인 경우 XStar는 7.65개, DStar는 7.72개의 도로를 포함한다. 이는 DStar가 실제 도로 네트워크 거리를 고려하여 클로킹 영역을 설정하기 위한 도로를 선택하기 때문이다. 이를 통해 DStar는 클로킹 영역 내에서 질의 요청자가 존재하는 도로의 노출 확률을 감소시키며, 따라서 DStar가 XStar에 비해 사용자 프라이버시 보호 측면에서 우수함을 알 수 있다.

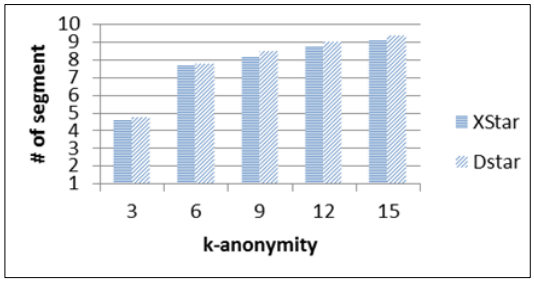


그림 11. K 변화에 따른 클러킹 영역 내 도로의 수

그림 12는 K 변화에 따른 총 서비스 시간을 나타낸 것이다. K 값이 증가할수록 두 기법 모두 총 서비스 시간이 증가함을 알 수 있다. K가 15일 때, XStar는 1.67초, DStar는 1.65초가 소요된다. DStar가 XStar에 비해 우수한 성능을 보이는 이유는, 클

로킹 영역 생성 시 도로 네트워크의 거리를 고려함으로써 XStar에 비해 작은 클로킹 영역을 설정하여 영역 질의 처리 시간 측면에서 우수한 성능을 보이기 때문이다

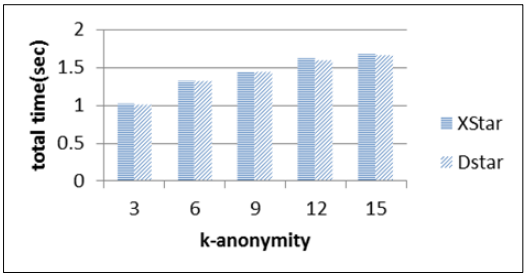


그림 12. K 변화에 따른 총 서비스 시간

4.3 D-tolerance(이하 D) 변화에 따른 성능평가

그림 13은 D 변화에 따른 클로킹 영역의 총 길이를 비교한 것이다. 두 기법 모두 허용할 수 있는 거리가 멀어질수록 넓은 범위의 영역을 설정함을 알 수 있다. 하지만, 도로의 거리를 고려하는 DStar가 XStar에 비해 보다 작은 영역을 설정함을 알 수 있다.

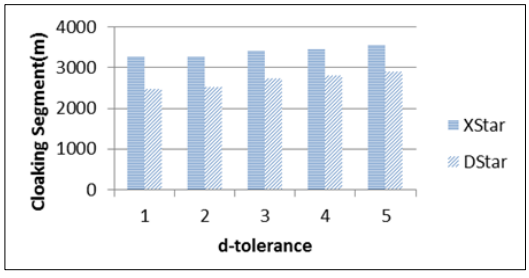


그림 13. D 변화에 따른 클로킹 영역

그림 14는 D 변화에 따른 총 서비스 시간을 비교한 것이다. 두 기법 모두 D변화에 크게 영향을 받지 않는 것을 확인할 수 있다. 이는 D 값은 확장을 위한 변수가 아닌, 슈퍼스타의 위배 조건을 검사하는 변수이기 때문이다.

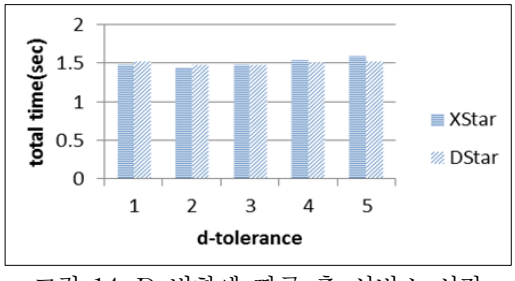


그림 14. D 변화에 따른 총 서비스 시간

5. 결론 및 향후연구

본 논문에서는 위치 기반 서비스에서 사용자 정보 보호를 지원하는 도로 네트워크 거리 기반 클로킹 기법을 제안하였다. 제안하는 기법은 사용자가 속한 도로의 교차 노드 선택 시 실제 네트워크 거리를 고려하고, 서비스 사용자가 실제 거리를 위배 조건으로 설정할 수 있도록 한다. 이를 통해, 사용자의 위치정보를 보호하면서 효율적으로 위치기반 서비스를 수행할 수 있다. 또한, 기존 연구인 XStar와의 성능 비교를 통해 제안하는 기법이 사용자 위치정보 보호와 서비스 시간 측면에서 우수함을 검증하였다.

향후 연구는 중앙 집중 방식에서 발생할 수 있는 병목 현상 등의 문제를 해결하기 위해, 분산 환경으로 본 연구를 확장하는 것이다.

참 고 문 헌

[1] T. Brinkhoff, "A Framework for Generating Network-Based Moving Objects", GeoInformatica, Vol.6, No.2, pp.153-180, 2002.

[2] D. Cho, "A Study on the State-of-the-Art of LBS through Patent Analysis", Journal of Korea Spatial Information System Society, Vol.9, No.3, pp.65-75, 2007.

[3] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," In Proc. of the International Conference on Mobile Systems, Applications and Services, pp. 31 - 42, 2003.

[4] G. Ghinita, P. Kalnis and S. Skiadopoulos, "MobiHide: A Mobilea Peer-to-Peer System for Anonymous Location-Based Queries," In Proc. of SSTD, Vol.4605, pp. 221-238, 2007.

[5] A. Lee, H. Kim, and J. Chang, "Grid-based Cloaking Area Creation Scheme supporting Continuous Location-Based Services", Journal of Korea Spatial Information System Society, Vol.11, No.3, pp. 19-30, 2009.

[6] M. Mokbel, W. Aref, S. Hambrusch, and S. Prabhakar, "Towards Scalable Location-aware Services : Requirements and Research Issues", In Proc. of the 11th ACM-GIS, pp. 110-117, 2003.

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

[8] B. Palanisamy and L. Liu, "MobiMix: Protecting Location Privacy with Mix-zones over Road Networks," In Proc. ICDE, pp. 494-505, 2011.

[9] J. Voelcker, "Stalked by Satellite: An Alarming Rise in GPS-enabled Harassment", IEEE Spectrum, Vol.47, NO.7, 2006, pp.15-16

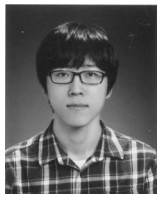
[10] J. Warrior, E. McHenry, and K. McGee, "They Know Where You Are", IEEE Spectrum, Vol.40, No.7, pp. 20-25, 2003.

[11] T. Wang and L. Liu, "Privacy-Aware Mobile Services over Road Networks", PVLDB, pp. 1042-1053, 2009.

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

[13] E. Yigitoglu, M. Damiani, O. Abul and C. Silverstri, "Privacy-preserving sharing of sensitive semantic locations under road-network constraints," In Proc. MDM, 2012.

논문접수 : 2012.08.20
수 정 일 : 1차 2012.10.24 / 2차 2012.10.28
심사완료 : 2012.10.29



김 형 일

2009년 전북대학교 컴퓨터공학과(공학사)
2011년 전북대학교 컴퓨터공학과(공학석사)
2011년~현재 전북대학교 컴퓨터공학과 박사과정
관심분야는 공간 데이터베이스, 위치 보안을 위한 클로킹 기법, 데이터베이스 아웃소싱

신 영 성

2010년 전북대학교 컴퓨터공학과 졸업(학사)
2011년~현재 전북대학교 컴퓨터공학과 석사과정
관심분야는 데이터베이스, 클라우드 컴퓨팅, SNS, LBS, 전문가 추천

장 재 우

1984년 서울대학교 전자계산기공학과(공학사)
1986년 한국과학기술원 전산학과(공학석사)
1991년 한국과학기술원 전산학과(공학박사)
1996년~1997년 Univ. of Minnesota, Visiting Scholar
2003년~2004년 Penn State Univ., Visiting Scholar.
1991년~현재 전북대학교 컴퓨터공학과 교수
관심분야는 공간 네트워크 데이터베이스, 하부저장구조, 센서네크워크