KIPS Trans. Comp. and Comm. Sys.
Vol.10, No.8 pp.231~234
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2021.10.8.231

Efficient *k*-ATY Method to Protect the User's Trajectory in Continuous Queries

Song Doo Hee†

ABSTRACT

Various problems arise as applications using locations increase. In order to solve this problem, related works are being conducted to protect the location of users. A fundamental reason for this problem is that users must provide their location information to the service provider (server) to receive the service. To improve these problems, there are works such as generating cloaking regions or generating dummies around them. However, if a user periodically asks the server for queries, the user's trajectory may be exposed by time zone. To improve this problem, in this paper, we propose a *k*-Anonymity Trajectory (*k*-ATY) technique that can improve the exposure probability of the trajectory even if the user requests continuous queries. Experimental results demonstrated the superiority of the proposed technique.

Keywords : Continuous Queries, Information Protection, Trajectory, *k*-anonymity

연속적인 질의에서 사용자의 이동 경로를 보호할 수 있는 효율적인 *k*-ATY 기법

송 두 희†

요 약

위치를 이용한 애플리케이션이 증가함에 따라 사용자의 위치 정보 및 이동 패턴의 노출 등 다양한 문제점들이 야기되고 있다. 이러한 문제점을 해결하기 위하여 사용자의 위치를 보호하기 위한 다양한 연구들이 진행되고 있다. 사용자의 위치 정보가 노출되는 근본적인 이유는 사용자가 서비스 제공자(서버)에게 자신의 위치 정보를 제공해야만 서비스를 제공받기 때문이다. 이러한 문제를 개선하기 위하여 클로킹(cloaking) 영역을 생성하거나 자신의 주변에 더미(dummy; 가상의 사용자)를 생성하는 연구 등이 존재한다. 그러나 사용자가 주기적으로 서버에게 질의를 요청할 경우 사용자의 시간대별 이동 경로가 노출될 수 있다. 본 논문에서는 이러한 문제점을 개선하고자 사용자가 연속적인 질의를 요청하더라도 이동 경로의 노출 확률을 개선할 수 있는 *k*-Anonymity Trajectory(*k*-ATY) 기법을 제안한다. 실험 결과를 통하여 제안 기법의 우수성을 증명했다.

키워드 : 연속적인 질의, 정보 보호, 이동 경로, *k*-익명화

1. 서 론

최근 위치를 활용한 애플리케이션이 개발됨에 따라 사용자의 위치 정보 및 이동 패턴의 노출 등 다양한 문제들이 발생하고 있다. 문제의 근본적인 원인은 사용자가 서비스 제공자(서버)에게 자신의 위치 정보 등을 공개해야 애플리케이션을 사용할 수 있기 때문이다. 사용자가 개인정보(위치, 사진 등) 대한 공개를 동의를 하지 않을 경우 애플리케이션 사용이 불가한 서비스들도 다수 존재한다. 이러한 문제를 개선하고자 다양한 연구들이 제안됐다. 예를 들면, 사용자의 위치가 아닌 특정 건물을 지정하거나 서버에게 자신의 위치를 포함하는 클로킹 영역을 생성한 후 서버에게 질의를 요청하는 기법이다[1,2]. 또한 가상의 사용자(dummy; 더미)를 활용하여 사용자가 어디 있는지 알 수 없게 만드는 기법도 존재한다[3-5]. 그러나 사용자가 서버에게 연속적인 질의를 요청할 경우 서버는 사용자의 위치 정보를 확인 할 수 있다. 즉, 질의 요청시간과 누적된 지점들을 연결한다면 이동 경로를 유추할 수 있다.

Fig. 1은 사용자(U_1)와 더미들(D_1, D_2, D_3)이 t부터 t+3까지 연속적으로 질의를 요청한 결과를 보여주고 있다. D_1은

※ 이 논문은 2019년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2019R1H1A1035598).
※ 이 논문은 2021년 한국정보처리학회 춘계학술발표대회에서 "연속적인 질의에서 사용자의 이동 경로를 보호하기 위한 연구"의 제목으로 발표된 논문을 확장한 것임.
† 종신회원 : 서울한영대학교 교양학과 교수
Manuscript Received : June 29, 2021
Accepted : July 14, 2021
* Corresponding Author : Song Doo Hee(dhsong@hytu.ac.kr)

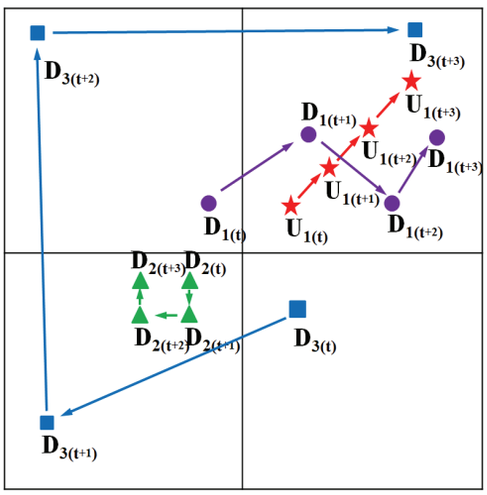

Fig. 1. *k*-anonymity Method for Trajectory Protection

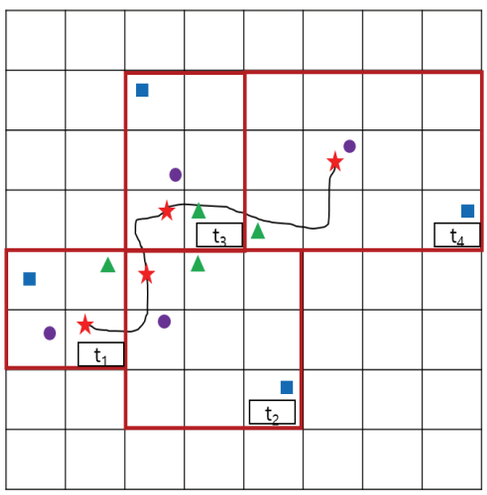

Fig. 2. Example of a Query Request using a *k*-anonymity(GTC)

U_1과 일정한 범위를 두고 생성될 수 있으나 이동 경로가 노출될 수 있고, D_2는 제자리를 맴돌고 있으며 D_3는 사용자가 이동할 수 있는 속도의 범위를 넘어선 그림이다. 이처럼, 사용자가 임의로 생성한 더미를 이용하여 연속적으로 질의를 요청할 경우 시간 간격을 통해 더미를 파악하거나 사용자의 이동 방향 등을 예측할 수 있다. 따라서 연속적인 질의를 요청하는 상황에서 사용자의 이동 경로를 보호할 수 있는 기법을 제안한다.

본 논문의 주요 기여는 다음과 같다.

제안기법은(*k*-ATY) 사용자의 이동속도 및 방향 고려하여 가상의 더미를 만들기 때문에 기존의 기법(*k*-익명화)보다 더미의 노출확률을 줄일 수 있다.

사용자 인근에 임의로 생성되는 더미는 연속적으로 질의를 요청할 경우 이동 경로가 노출될 수 있으나 *k*-ATY는 *k*-1개의 다른 방향으로 이동하기 때문에 이동 경로가 노출될 확률을 줄인다.

사용자와 더미에 클로킹 영역을 생성할 경우 겹치는 영역을 줄임으로서 보호영역의 크기를 유지할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 간단히 소개하고, 3장에서 *k*-ATY를 이용한 연속적인 더미생성 방법을 설명한다. 4장에서 기존 기법과 *k*-ATY의 기법에 대한 실험결과를 비교하고, 마지막으로 5장에서 결론을 내린다.

2. 관련 연구

사용자의 위치를 보호하기 위하여 다양한 연구들이 진행되고 있다. 기존의 *k*-익명화 기법은 익명 서버를 따로 구축한 후 가상의 더미를 생성했다. 그러나 제 3자가 익명 서버와 공모하여 사용자의 정보를 공유하는 문제가 발생함에 따라 사용자가 직접 자신의 위치 정보를 보호하는 기법이 제안됐다[6-9].

Fig. 2는 [10]에서 제안한 GTC(Grid-based Trajectory Cloaking)기법을 보여주고 있다. t_1에서 4칸의 클로킹 영역(CR)은 t_1 시간에 더미가 임의로 생성될 수 있는 범위를 의미한다. 클로킹 영역 내에서 사용자 및 더미가 생성되고 생성되는 CR의 범위는 Equation (1)과 같이 정의할 수 있다.

$$CR(t_i) = 2^{m-1} \times 2^{n-1} \quad (1)$$

$CR(t_i)$은 사용자가 지정한 보호범위에 따라 그 크기가 수정될 수 있다고 소개하고 있다. 그리고 사용자의 이동경로 노출에 대한 정의는 다음과 같다.

이동경로 노출확률 : 사용자의 $CR(t_i)$ ∩ 더미의 $CR(t_i)$

Fig. 1에서 소개했듯이 범위가 설정되지 않은 상태에서 임의로 더미가 생성될 경우 사용자가 아님을 예측할 수 있다. 더미의 노출은 사용자의 위치 노출로 이어질 수 있는 문제점을 내포하고 있다. 이를 해결하기 위해서 GTC가 제안됐으나 GTC에서 사용자의 $CR(t_i)$과 더미의 $CR(t_i)$이 동일하기 때문에 이동경로가 노출된다고 볼 수 있다. 따라서 위에서 언급된 관련연구들의 문제점을 개선할 수 있는 연구가 부족한 실정이다.

3. 제안 기법

3장에서는 *k*-ATY를 이용한 더미 생성 방법에 대해 설명한다.

Fig. 3은 *k*-ATY를 이용하여 사용자의 이동경로를 보호하는 과정을 보여주고 있다. Fig. 1과 같이 기존 *k*-익명화 기법은 임의의 장소에 더미를 생성하거나 사용자 인근에 더미가 생성되어 사용자의 위치 또는 이동경로가 노출될 수 있다고 설명했다.

k-ATY는 사용자의 이동 속도(v)와 방향(θ)을 고려하여 더미를 생성하는 기법이다(Algorithm 1). Fig. 3에서 U_1은 실제 사용자이며, t부터 t+3까지 1씩 증가할 때마다 질의를 요청한 것을 보여주고 있다. 사용자와 더미를 포함한 k는 4, 분

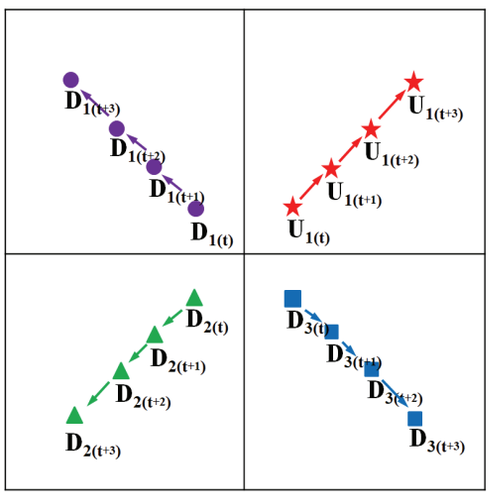

Fig. 3. k-ATY Based Trajectory Protection

할된 각도(θ_k)는 U_1의 $2\pi/4$를 나눈 90도이다(Algorithm 1, line 1). 사용자를 제외한 k-1개인 3개의 더미가 생성될 때까지 더미를 생성한다(Algorithm 1, line 2).

Equation (2)는 더미의 방향을 설명하기 위한 수식이다.

$$\angle d_k = \theta+(k-1)\cdot\theta_k \quad (2)$$

Fig. 3에서 사용자의 θ는 45도로 가정했을 때, 더미의 $\angle d_k$는 90도이고, 첫 번째 더미 생성 시 Equation (2)을 통해 $\theta+1\cdot\theta_k$ 수식이 도출한다. 수식에 θ, $\angle d_k$을 대입한 결과 135도의 더미 방향이 설정되고 이를 2번 더 반복한다(Algorithm 1, line 3). 설정된 방향에 사용자의 v를 추가하면 연속적인 더미 생성이 가능하다. 만약 더미 생성 중 $\angle d_k$ 각도가 2π 이상일 때 $\angle d_k = \angle d_k - 2\pi$ 통해서 방향을 재설정한다(Algorithm 1, line 4-5). t부터 t+3까지 각 지점을 연결한 것이 사용자의 이동 경로(빨간색 실선)이다. 사용자는 서버에게 자신과 3개의 더미의 위치를 포함시킨 후 질의를 요청한다. 그리고 t가 1씩 증가할 때마다 이동 속도와 방향을 고려하여 더미(D_1, D_2, D_3)를 생성함으로서 각각 이동 경로를 다르게 설정했다(Algorithm 1, line 8).

연속적인 질의 과정에서 더미를 생성하기 위한 k-ATY는 Algorithm 1과 같다.

Algorithm 1. k-ATY dummy generation method

User's velocity : v, user's direction : θ;
User query processing:
1 : $\theta_k = 2\pi / k$;
2 : **while** (number of dummy $>= k$-1) **do**
3 : k++;
4 : $\angle d_k = \theta+(k-1)\cdot\theta_k$
5 : **if** ($\angle d_k >= 2\pi$) then
6 : $\angle d_k = \angle d_k - 2\pi$;
7 : **else**
8 : continue;
9 : return k-ATY;

Table 1. Comparison of Exposure Probabilities between k-anonymity and k-ATY

Parameter	Data Settings Value
x-axis*y-axis	10,000 * 10,000
k	2, 3, 4
cloaking area	2*2, 3*3, 4*4

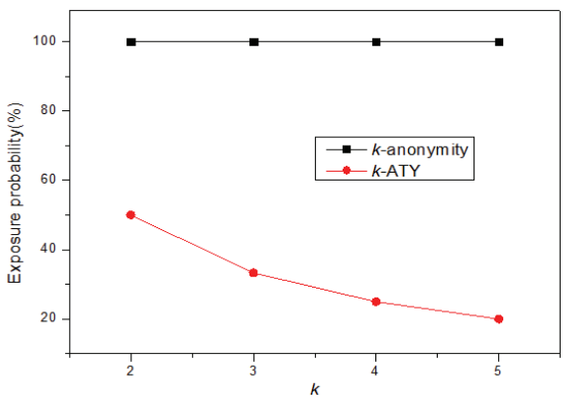

Fig. 4. User's Trajectory Exposure Probability

4. 실험 결과

4.1 실험 환경

본 절에서는 k-익명화 기법과 k-ATY 기법을 비교한다. 실험환경은 Intel i7-7700 CPU 3.6Ghz, memory 16GB이고, visual studio 2019를 이용하여 실험을 실행했으며 10,000번 실험한 후 평균값으로 그래픽의 결과를 나타냈다.

Table 1은 실험환경에 필요한 변수를 다음과 같이 정리했다.

본 논문에서는 사용자가 서버에게 질의 요청 시 사용자의 위치 또는 클로킹 영역과 사용자 및 더미의 id를 제공한다고 가정한다. 사용자가 이동할 수 있는 속도는 5칸, k-익명화 기법에서 더미 생성 시 사용자를 중심으로 9*9칸 내 임의로 생성되며 클로킹 영역 안에는 사용자가 존재한다고 가정했다.

4.2 실험 결과

Fig. 4는 연속적인 질의를 요청하는 과정에서 k-익명화 기법과 k-ATY 기법을 이용하여 보호할 경우 서버에게 이동경로가 노출될 확률을 보여주고 있다. k-익명화 기법의 그래프를 확인한 결과 k가 증가하더라도 사용자 인근에 더미가 생성되기 때문에 이동경로가 노출되는 반면 k-ATY는 k가 증가할수록 노출확률이 줄어드는 것을 확인할 수 있다. k-ATY의 이동경로 노출 확률이 줄어드는 이유는 Fig. 3과 같이 사용자가 이동하는 경로와 다른 방향으로 더미를 생성하기 때문이다.

Fig. 5는 질의자가 서버에게 자신의 위치가 노출되더라도 최소한의 위치 보호를 받기 위하여 클로킹 영역을 설정한 결과를 보여주고 있다. 사용자가 클로킹 영역을 생성하면 더미도 동일하게 클로킹 영역을 생성하며 Fig. 5에서는 k를 10개로 설정했다. Fig. 5의 결과를 보면, 사용자가 클로킹 영역을

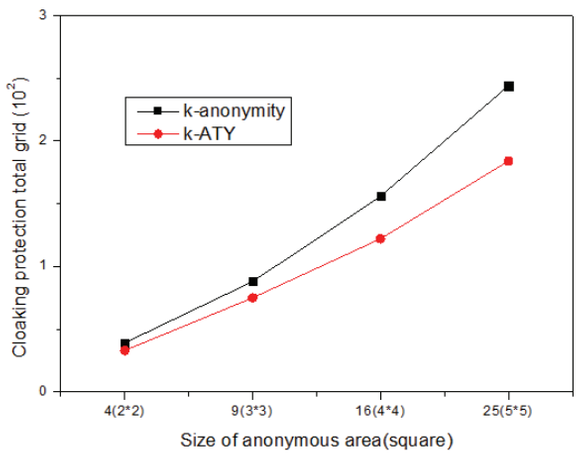

Fig. 5. Cloaking Protection Total Region According to the Size of the Anonymous Area

증가시킬수록 *k*-익명화 기법에 비해 *k*-ATY의 클로킹 영역의 크기가 평균 21.4% 더 큰 것으로 확인됐다. 그 이유는 *k*-익명화에서 생성된 더미는 서로 인접한 영역에 존재하고 클로킹 영역 커질수록 중복되는 클로킹 영역이 증가하기 때문이다.

5. 결 론

본 논문에서는 연속적인 질의에서 사용자의 이동 경로를 보호 및 클로킹 영역의 보호 구간을 보장할 수 있는 *k*-ATY 기법을 제안했다. 4장 실험결과에서 확인했듯이 *k*-익명화 기법에서 사용자의 이동경로는 서버에게 노출된 반면, *k*-ATY 기법을 이용할 경우 k개 이상의 경로를 확인해야하기 때문에 사용자 이동경로의 노출확률은 감소한다. 또한 클로킹 영역의 중복되는 영역을 줄임으로 인해서 보호 영역을 보장했다. 향후 연구에서는 사용자가 이동하는 방향과 속도 외에 환경 등을 고려하여 더미를 생성 할 때 발생할 수 있는 문제점을 찾고 이를 개선할 수 있는 연구를 진행하고자 한다.

References

[1] T. Allard, G. Hebrail, F. Masseglia, and E. Pacitti, "A new privacy-preserving solution for clustering massively distributed personal times-series," in *International Conference on Data Engineering*, pp.1370-1373, 2016.

[2] R. Yu, Z. Bai, L. Yang, P. Wang, O. A. Move, and Y. Liu, "A location cloaking algorithm based on combinatorial optimization for location-based services in 5G networks," *IEEE Access*, Vol.4, pp.6515-6527, 2016.

[3] M. H. Afifi, K. Zhou, and J. Ren, "Privacy characterization and quantification in data publishing," *IEEE Transactions on Knowledge and Data Engineering*, Vol.30, No.9, pp.1756-1769, 2018.

[4] B. Niu, Z. Zhang, X. Li, and H. Li, "Privacy-area aware dummy generation algorithms for location-based services," in *IEEE International Conference on Communications*, pp.957-962, 2014.

[5] D. Wu, Y. Zhang, and Y. Liu, "Dummy location selection scheme for k-anonymity in location based services," in *IEEE Trustcom/BigDataSE/ICESS*, pp.441-448, 2017.

[6] D. Song, M. Song, and K. Park, "A privacy-preserving spatial index for spatial query processing," *Wireless Communications and Mobile Computing*, pp.1-10, 2018.

[7] C. Y. Chow and M. F. Mokbel, "Trajectory privacyin location-based services and data publication," *ACM SIGKDD Explorations Newsletter*, Vol.13, No.1, pp.19-29, 2011.

[8] H. Liu, X. Li, H. Li, J. Ma, and X. Ma, "Spatiotemporal correlation-aware dummy-based privacy protection scheme for location-based services," in *IEEE Conference on Computer Communications*, pp.1-9, 2017.

[9] D. Liao, H. Li, G. Sun, and V. Anand, "Protecting user trajectory in location-based services," *IEEE Global Communications Conference*, 2015.

[10] J. Youn, D. Song, T. Cai, and K. Park, "Grid-based Trajectory cloaking method for protecting trajectory privacy in location-based services," *Korean Society for Internet Information*, Vol.18, No.5, pp.1-6, 2017.

송 두 희

https://orcid.org/0000-0002-9802-7257

e-mail : dhsong@hytu.ac.kr

2010년 원광대학교 전기전자및정보공학부 (학사)

2012년 원광대학교 정보통신공학과(석사)

2016년 원광대학교 정보통신공학과(박사)

2016년 ~ 2019년 원광대학교 정보통신공학과 시간강사 및 초빙교수

2019년 ~ 현 재 서울한영대학교 교양학과 교수

관심분야 : Database, Privacy Protection, ect.