차분 프라이버시를 만족하는 접두사 트리의 경로 데이터 통계 질의 연구

신지환[1], 송예지[2], 안진현[3], 이태휘[4], 임동혁[5]
[1]광운대학교 인공지능응용학과 석사과정
[2]광운대학교 인공지능융합학과 박사과정
[3]제주대학교 경영정보학과 교수
[4]한국전자통신연구원 스마트데이터연구실 책임연구원
[5]광운대학교 정보융합학부 교수

shinjihwan1997@kw.ac.kr, yeah9song@kw.ac.kr, jha@jejunu.ac.kr, taewhi@etri.re.kr, dhim@kw.ac.kr

A Study on trajectory data statistical queries of prefix trees satisfying differential privacy

Ji Hwan Shin[1], Ye Ji Song[2], Jin Hyun Ahn[3], Taewhi Lee[4], Dong-Hyuk Im[5]
[1]Dept. of Artificial Intelligence Application, Kwangwoon University
[2]Dept. of Artificial Intelligence Convergence, Kwangwoon University
[3]Dept. of Management Information System, Jeju National University
[4]Smart Data Research Section, Electronics and Telecommunications Research Institute
[5]School of Information Convergence, Kwangwoon University

요 약

최근 정보 기술의 급격한 발전으로 스마트폰이 우리의 일상 생활에 점점 더 많이 들어오고 있으며, 사용자들은 많은 서비스들을 누릴 수 있게 되었다. 위치 기반 서비스(LBS)의 경우 스마트폰에 탑재된 위치 확인 기능을 통해 음식점 추천, 길찾기 등 개인형 맞춤 서비스를 제공하며, 사용자는 간단한 동의를 통해 자신의 위치를 LBS 서버에 전송하게 된다. 이는 사용자의 개인정보 침해의 요소가 될 수 있으며, 사용자의 민감한 정보가 공개될 수 있다. 따라서 본 논문에서는 사용자의 경로 데이터의 민감 정점을 보호하고, 통계적 질의를 할 때, 절대적으로 개인정보를 보호할 수 있는 방법을 제시한다.

1. 서론

최근 정보 기술의 급격한 발전으로 인해 스마트폰이 우리의 일상 생활에 점점 더 많이 들어오고 있다 [1]. 사용자들은 스마트폰을 통해 쇼핑, 영화 시청, 음악 감상등 여가 생활을 즐길 수 있게 되었다. 뿐만 아니라 위치 기반 서비스(LBS)가 많이 등장하면서 스마트폰의 위치 확인 기능을 통한 음식점 추천, 길 찾기 등 개인형 맞춤 서비스를 사용할 수 있게 되었다 [2]. 그러나 이러한 장치는 사용자의 간단한 동의만으로 경로 데이터를 수집할 수 있으며, 수집된 데이터는 사용자 권한이 부여된 후 다양한 서비스 제공업체에 업로드 될 수 있다 [3]. 이는 사용자의 개인정보 침해의 위험 요소가 될 수 있다. 공격자는 데이터 마이닝 알고리즘을 통해 경로 데이터에서 사용자의 개인정보를 얻을 수 있으며, 민감한 사용자의 정보가 공개될 수 있다. 다양한 서비스로 경로 데이터의 양과 활용 가치가 증가하면서 개인정보 비식별화에 대한 연구가 많은 관심을 끌고 있다.

GAN[4]은 합성 이미지 생성에 많이 사용되는 생성 모델이다. 또한 경로 데이터를 비식별화 할 때 많이 사용된다. 그러나 GAN은 출력물에 대한 제어가 어렵기 때문에 이를 개선한 레이블을 통한 클래스 조건부 생성이 가능한 GAN기반의 연구[5, 6, 7]가 등장했다.

개인정보 비식별화의 대표적인 방법으로는 k-익명성[8]과 이를 개선한 l-다양성[9] 등이 존재한다. 그러나 이러한 방법들은 공격자의 배경지식에 취약하며, 절대적인 프라이버시 보호를 보장할 수 없다.

차분 프라이버시[10]는 개인정보 비식별화에 대

한 새로운 접근 방식으로 엄격한 수학적 증명을 제공한다. 공격자가 배경지식을 가지고 있어도 사용자의 개인정보를 유추하는 것이 불가능하다.

따라서 본 논문에서는 ACGAN을 사용하여 사용자의 민감한 지점을 보호하는 합성 경로를 생성하고, k-means clustering을 통해 일반화된 경로를 생성한다. 생성된 일반화된 경로를 접두사 트리에 삽입하여 Laplace 메커니즘을 기반으로 다양한 개인정보 보호 예산으로 노이즈를 추가하고, Markov 전이 확률과 결합하여 각 위치에 추가되는 노이즈를 제한하는 방법을 보인다.

2. 배경지식

2.1 ACGAN

ACGAN은 이미지 합성을 위해 개선된 훈련 방법을 사용하는 클래스 조건부 이미지 합성 모델이다. ACGAN은 두 가지 모델인 생성기와 판별기로 구성된다. 생성기는 라벨을 통해 조건부 이미지를 생성하고, 판별기는 이미지의 진위 여부와 클래스를 예측하게 된다.

$$L_s = E[\log P(S = real|X_{real})] + E[\log P(S = fake|X_{fake})]$$

$$L_c = E[\log P(C = c|X_{real})] + E[\log P(C = c|X_{fake})]$$

L_s는 실제 데이터와 가짜 데이터를 구분하는 추정치의 합을 나타낸다. 또한 L_c는 실제 클래스와 가짜 클래스를 구분하는 추정치의 합을 나타낸다. 판별자는 L_s와 L_c의 합을 최대화되도록 훈련되며 생성자는 L_c와 L_s의 차이가 최대화되도록 훈련된다.

2.2 K-means Clustering

K-means Clustering은 주어진 데이터를 클러스터의 중심으로부터 가까운 데이터를 병합시켜 k개의 클러스터를 생성하는 비지도 학습 알고리즘이다.

본 논문에서는 ACGAN이 생성한 합성 경로를 일반화하기 위한 방법으로 K-means Clusetering을 사용한다.

2.3 ϵ-차분 프라이버시(ϵ-differential privacy)

하나의 레코드만 다른 인접한 두 데이터 셋을 D, D', 데이터 변조 알고리즘 함수를 A라고 할 때, A의 생성 가능한 모든 결과 값 O에 대하여 다음의 식을 만족하면 A는 ϵ-차분 프라이버시를 만족한다.

$$\Pr[A(D) = O] \le exp(\epsilon) \times Pr[A(D') = O]$$

ϵ이 작을수록 함수 A의 결과가 많이 변조되며 ϵ이 클수록 함수 A의 결과가 적게 변조된다.

2.4 민감도(sensitivity)

주어진 함수 f와 인접한 두 데이터 셋 D, D'에 대해 민감도 $\triangle f$는 다음과 같이 정의한다.

$$\triangle f = \max_{D,D'} \|f(D) - f(D')\|_1$$

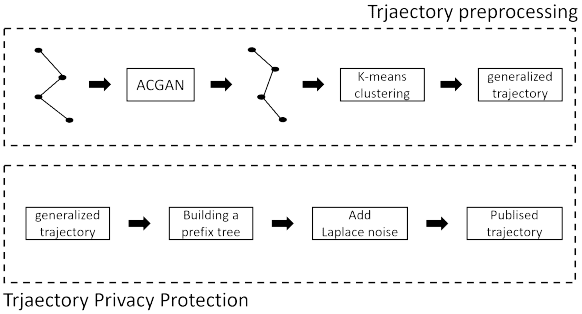
임의의 데이터 셋에 대해서 함수 f의 결과 값의 차이를 측정하는 방법이다.

2.5 라플라스 메커니즘(Laplace mechanism)

데이터 셋 D와 쿼리 함수 $f : D \rightarrow R^d$가 주어지면, 라플라스 메커니즘 M은 함수 f의 출력에 노이즈를 추가한다. 이때, $f(D) + Lap(\triangle f/\epsilon)$은 ϵ-차분 프라이버시를 만족한다.

3. 방법론

경로 데이터의 프라이버시 보호를 위한 과정은 크게 경로 전처리 과정, 경로 프라이버시 보호 과정 두 가지로 나눌 수 있다. 그림 1은 전체 과정의 흐름을 보여준다.



(그림 1) 경로 데이터 프라이버시 보호 과정

첫 번째는 경로 전처리 과정이다. 먼저 원본 경로 데이터를 입력으로 취한 ACGAN은 원본 데이터와 유사한 합성 경로 데이터를 생성하며 쿼리를 위해 접두사 트리에 삽입되는 원본 경로 데이터의 대안으로 사용된다. 생성된 합성 경로 데이터는 k-means 알고리즘을 사용하여 유클리드 거리를 기준으로 timestamp에 따라 경로를 클러스터링하고, 클러스터의 중심 좌표를 사용하여 일반화된 경로를 얻는다.

두 번째는 경로 프라이버시 보호 과정이다. 먼저 일반화된 경로를 접두사 트리에 삽입한다. 그림 2는 접두사 트리에 경로를 삽입한 예를 보여준다.

L_{ij}에서 i는 timestmap를 의미하며, j는 timestamp 내

의 클러스터를 의미한다. 그림 2와 같이 일반화된 경로를 접두사 트리에 삽입 후 전체 개인 정보 보호 예산인 ϵ을 트리의 높이 h로 나눈다. 이를 통해 각 레이어 별로 예산 $\tilde{\epsilon}$을 할당하고, 모든 노드들의 마코프 전이 확률을 계산하여 Laplace 분포로부터 노이즈를 생성한다. 생성된 노이즈와 마코프 전이 확률을 곱한 값을 각 노드의 count 값에 더한다. 접두사 트리의 각 노드에 Laplace 노이즈를 추가하는 알고리즘은 $\tilde{\epsilon}$-차분 프라이버시를 만족하며, 다음과 같이 증명된다.

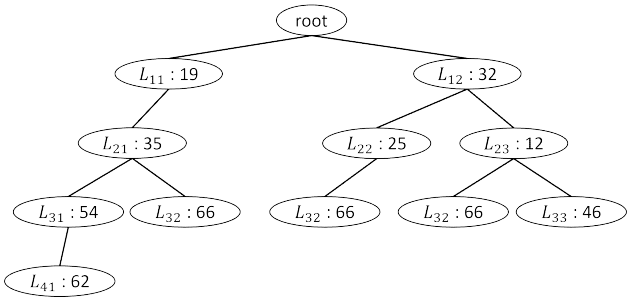
P_1을 데이터 세트 D의 확률 밀도 함수로 두고, P_2를 노이즈 Z의 확률 밀도 함수라고 하고, 전체 개인 정보 보호 예산을 트리의 높이로 나눈 각 레이어의 개인 정보 보호 예산을 $\tilde{\epsilon}$라고 할 때, 다음과 같이 나타낼 수 있다.

$$\frac{\Pr[f(D)\in O]}{\Pr[f(D')\in O]} = \frac{\Pr[d+z=o]}{\Pr[d'+z=o]} = \frac{P_2[o-P_1(d)]}{P_2[o-P_1(d)]}$$

여기서 $z\in Z$, $o\in O$, Z는 라플라스 분포를 따르므로,

$$\frac{P_2[o-P_1(d)]}{P_2[o-P_1(d')]} \le \epsilon^{\frac{\epsilon}{f}\cdot|d-d'|} = \epsilon^{\frac{\epsilon}{f}\cdot\frac{f}{h}} = \epsilon^{\tilde{\epsilon}}$$

접두사 트리에 노이즈를 삽입하는 과정은 ϵ-차분 프라이버시를 만족한다는 것을 알 수 있다.



(그림 2) 접두사 트리 경로 삽입의 예

4. 실험

4.1 ACGAN 모델의 성능 평가

본 논문의 실험은 뉴욕시(NYC)에 대한 Foursquare 주간 경로 데이터 셋을 사용하였다[11]. 첫 번째로 ACGAN이 생성한 데이터의 유용성과 익명성을 평가하기 위해 선행 연구에서 제안한 LSTM과 GAN을 결합한 생성 모델 LSTM-TrajGAN[12]과 Hausdorff distance, TUL-Test을 측정하였다. <표 1>은 LSTM-TrajGAN 모델과 ACGAN 모델이 생성한 합성 경로 데이터의 Hausdorff distance를 측정한 값을 나타낸다. 모든 측정 항목에서 ACGAN이 생성한 경로 데이터가 LSTM-TrajGAN보다 낮은 점수를 가지는 것을 확인할 수 있다. 이는 원본 경로 데이터와 더욱 유사하다는 것을 의미하며 유용성이 높음을 의미한다. TUL-Test는 Trajectory User Linking Test로 경로 데이터를 통해 사용자를 예측하는 정확도를 평가하는 실험이다. 따라서 정확도가 높을수록 사용자를 더욱 잘 예측한다는 것을 의미하므로 익명성이 낮음을 의미한다. 반대로 정확도가 낮을수록 익명성이 높음을 의미한다. <표 2>의 결과에서 LSTM-TrajGAN보다 모든 측면에서 정확도가 낮은 것을 확인할 수 있다. 이는 ACGAN을 통해 생성된 합성 경로 데이터의 익명성이 높음을 의미한다.

<표 1> Hausdorff distance 결과

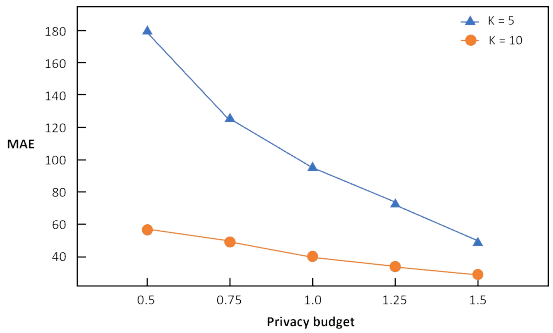
	LSTM-TrajGAN	Proposed
MIN	0.0068387	0.0044394
MAX	0.0628863	0.0529816
AVG	0.0206473	0.0171546
MEAN	0.0197523	0.0159778

<표 2> TUL-Test 결과

	LSTM-TrajGAN	Proposed
ACC@1	0.406037	0.308666
ACC@5	0.651412	0.587147
Macro-P	0.345144	0.230609
Macro-R	0.390910	0.256103
Macro-F1	0.374779	0.293933

4.2 개인 정보 보호 예산에 따른 MAE 변화

두 번째 실험은 개인 정보 보호 예산을 변경하여 평균 절대 오차의 변동을 측정하였다. 평균 절대 오차는 노이즈를 삽입한 카운트 값의 합과 노이즈가 더해지지 않은 원본 카운트 값의 차이를 측정하였다. 개인 정보 예산의 값 범위는 0.5, 0.75, 1.0, 1.25, 1.5이다. 그림 3은 개인 정보 예산에 따른 mae 변화를 보여준다. 모든 경우에서 프라이버시 예산이 증가할 때 mae의 값이 낮아지는 것을 확인할 수 있다. 또한 k값이 많아질 때 mae 값이 낮아지는 것을 확인할 수 있다.



(그림 3) 개인 정보 예산에 따른 MAE 변화

5. 결론

위치 기반 서비스(LBS)의 증가는 경로 데이터 생성을 증가시켰다. 생성된 경로 데이터는 사용자의 간단한 동의만으로 여러 기업들이 수집할 수 있으며, 이는 사용자의 개인정보 유출의 문제가 될 수 있다. 본 논문에서는 경로 데이터의 통계 질의에 대한 프라이버시를 보호 연구를 진행하였다. 경로 데이터의 통계 질의를 위해 LBS 서버에 전송할 때, 사용자의 원본 경로 데이터를 통한 개인정보 유출 방지를 위해 ACGAN을 사용하여 합성 경로를 생성하였으며, 생성된 경로 데이터를 접두사 트리에 삽입하였다. 또한 차분 프라이버시를 만족하는 Laplace 노이즈 삽입을 통해 경로 데이터의 통계 질의를 절대적으로 보호할 수 있는 방법을 제안하였다.

Acknowledgement

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No. 2021-0-00231, 빅데이터 대상의 빠른 질의 처리가 가능한 탐사 데이터 분석 지원 근사질의 DBMS 기술 개발, 40%)과 한국연구재단의 지원(No. NRF-2021R1F1A1054739), 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터지원사업의 연구결과로 수행되었음 (IITP-2023-2018-0-01417, 10%).

참고문헌

[1] Tian, J., and Zhu, Q., "A differential privacy trajectory data storage and publishing scheme based on radix tree", *Concurrency and Computation: Practice and Experience*, pp. 7731, 2023.

[2] Shin, K. G., Chen, Z., and Hu, X., "Privacy protection for users of location-based services.", *IEEE Wireless Communications*, vol. 19, no. 1, pp. 30-39, 2012.

[3] Zhao, X., Pi, D., and Chen, J., "Novel trajectory privacy-preserving method based on prefix tree using differential privacy.", *Knowledge-Based Systems*, vol. 198, pp. 105940, 2020.

[4] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., and Bengio, Y., "Generative adversarial nets.", *Proceedings of the 27th International Conference on Neural Information Processing Systems*, pp. 2672-2680, 2014.

[5] Odena, A., Olah, C., and Shlens, J., "Conditional image synthesis with auxiliary classifier GANs.", *Proceedings of the 34th International Conference on Machine Learning*, pp. 2642-2651, 2017.

[6] Shin, J., Song, Y., Ahn, J., Lee, T., and Im, D, H., "TCAC-GAN: Synthetic Trajectory Generation Model Using Auxiliary Classifier Generative Adversarial Networks for Improved Protection of Trajectory Data," *IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 314-315, 2023.

[7] Song, Y., Shin, J., Ahn, J., Lee, T., and Im, D, H., "Except-Condition Generative Adversarial Network for Generating Trajectory Data," *International Conference on Database and Expert Systems Applications*, pp. 289-294, 2023.

[8] Sweeny, L., "k-anonymity: A model for protecting privacy.", *International journal of uncertainty, fuzziness and knowledge-based systems*, vol. 10, no. 5, pp. 557-570, 2002.

[9] Machanavajjhala, A., Kifer, D., Gehrke, J., and Venkitasubramaniam, M., "l-diversity: Privacy beyond k-anonymity.", *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 1, no. 1, pp. 3-es, 2007.

[10] Dwork, C., "Differential privacy.", *International colloquium on automata, languages, and programming*, 2006.

[11] Yang, D., Zhang, V., Zheng, W., and Yu, Z., "Modeling user activity preference by leveraging user spatial temporal characteristics in LBSNs.", *IEEE Transactions on Systems*, Man, and Cybernetics: Systems, vol. 45, no. 1, pp. 129-142, 2015.

[12] Rao, J., Gao, S., Kang, Y., and Huang, Q., "LSTM-TrajGAN: A Deep Learning Approach to Trajectory Privacy Protection.", *11th International Conference on Geographic Information Science (GIScience 2021)*, 2020.