TAP-GAN: 어텐션 메커니즘이 적용된 ACGAN 기반의 경로 프라이버시 강화

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

TAP-GAN: Enhanced Trajectory Privacy Based on ACGAN with Attention Mechanism

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

위치 기반 서비스(LBS)의 확산으로 다양한 분야에서 활용할 수 있는 많은 양의 경로 데이터가 생성되고 있다. 하지만 공격자가 경로 데이터를 통해 잠재적으로 사용자의 개인정보를 유추할 수 있다는 문제점이 존재한다. 따라서 경로 데이터의 프라이버시를 보존하며 유용성을 유지할 수 있는 GAN(Generative Adversarial Network)을 사용한 많은 연구가 진행되고 있다. 그러나 GAN은 생성된 결과물을 제어하지 못한다는 한계점을 가지고 있다. 본 논문에서는 ACGAN(Auxiliary classifier GAN)을 통해 생성된 결과물을 제어함으로써 경로 데이터의 민감한 정점을 숨기고, Attention mechanism을 결합하여 높은 유용성과 익명성을 제공하는 합성 경로 생성 모델인 TAP-GAN(Trajectory attention and protection-GAN)을 제안한다. 또한 모델의 성능을 입증하기 위해 유용성 및 익명성 실험을 진행하고, 선행 연구 모델과의 비교를 통해 TAP-GAN이 경로 데이터의 유용성을 보장하면서 사용자의 프라이버시를 효과적으로 보호할 수 있음을 확인하였다.

1. 서론

위치 기반 서비스(LBS)는 스마트폰 사용자의 위치 정보를 활용하여 개인 맞춤형 서비스를 제공한다. 최근에는 음식점 추천, 길 찾기 등 다양한 편의 기능을 제공하는 LBS 애플리케이션이 많이 등장하고 있다 [1]. 그러나 이러한 서비스는 민감한 개인 정보 노출 가능성이 있다. 예를 들어, 공격자는 경로 데이터를 통해 잠재적으로 위치 정보를 수집하고 사용자의 집 주소를 포함한 민감한 개인 정보를 유추할 수 있다. 사용자 경로 데이터의 개인 정보를 보호하기 위해 GAN(Generative Adversarial Network)을 사용한 연구가 많이 진행되고 있다. GAN은 원본과 유사한 합성 데이터를 생성할 수 있기 때문에 데이터의 프라이버시를 보존하며 유용성을 유지할 수 있다. 그러나 GAN은 생성된 출력물을 제어할 수 없다는 한계점을 가지고 있다. 따라서 본 논문에서는 ACGAN(Auxiliary Classifier GAN) [2]을 사용하여 생성된 경로 데이터의 민감한 정점을 보호하고, Attention mechanism을 결합하여 높은 유용성과 익명성을 가지는 경로 생성 모델인 TAP-GAN(Trajectory attention and protection GAN)을 제안한다. 또한 TAP-GAN이 생성한 합성 경로 데이터의 유용성과 익명성을 측정하고, 선행 연구 모델과 비교 분석한다.

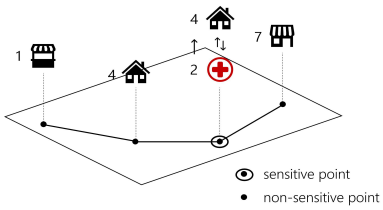
2. 관련연구

사용자 경로 데이터는 여러 분야에서 유용하게 사용될 수 있다. 그러나 경로 데이터는 민감한 정보를 포함하기 때문에 사용자의 개인 정보가 위협받을 수

있다. 따라서 개인 정보를 보호하면서 데이터의 유용성은 유지시킬 수 있도록 하는 연구가 많이 진행되고 있다. [3]은 Long Short-Term Memory(LSTM)와 GAN을 결합하여 경로 데이터의 시공간적 정보를 보존하면서 기존의 경로 데이터와 유사한 합성 경로 데이터를 생성하는 LSTM-TrajGAN을 제안했다. [4]은 LSTM과 ACGAN을 결합하여 시공간적 정보를 보존하는 동시에 Generator의 조건부 생성을 통해 경로 데이터의 원하는 정점을 숨길 수 있는 TCAC-GAN을 제안했다.

3. TAP-GAN

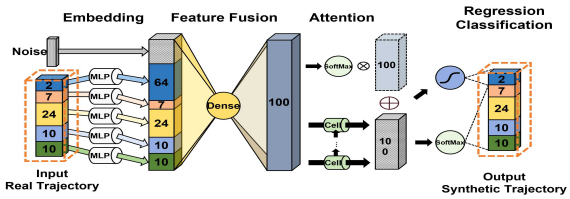
본 논문에서 제안하는 합성 경로 생성 작업은 세 단계로 나눌 수 있다. 첫 번째는 Generator와 Discriminator에서 사용할 레이블을 생성하는 단계이다. TAP-GAN의 입력으로 사용되는 경로 데이터는 위치, 날짜, 시간, 카테고리, 레이블로 이루어져 있다 [5]. 위치 데이터는 위도와 경도 값으로 이루어져 있으며 날짜, 시간, 카테고리, 레이블은 각각 7, 24, 10, 10의 vocab size를 가진다. 카테고리는 해당 정점의 속성(예: Food, Shop&Service 등)을 의미하며, 레이블은 민감한 정점을 숨긴 카테고리 값을 의미한다. 그림 1은 민감 정점을 숨기기 위한 레이블 생성 예시이다. 병원의 카테고리 값은 2이고, 민감한 카테고리라고 가정할 때, 해당 카테고리 값을 균등한 확률을 통해 다른 카테고리 값으로 변경한다. 변경된 경로의 카테고리 값들은 해당 경로의 레이블 값으로 사용한다. 이를 통해 카테고리 값은 레이블 값에 근사하게 조건부 생성을 하며, 위치 값 또한 해당 카테고리 값에 근사하게 생성된다.



(그림 1) 레이블 생성의 예

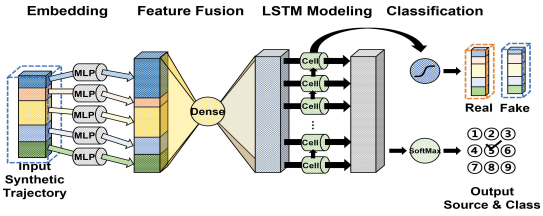
두 번째는 데이터 인코딩 작업이다. 위치 데이터의 경우 경로의 중심 지점에서 각 정점까지의 편차 값으로 모든 정점을 정규화 시킨다. 이를 통해 정점 간의 편차 차이를 더욱 잘 학습할 수 있다. 위치 데이터를 제외한 데이터(날짜, 시간, 카테고리, 레이블)들은 자신의 vocab size로 원-핫 인코딩 된다.

세 번째는 TAP-GAN을 이용한 경로 생성 작업이다. 그림 2는 Generator의 아키텍쳐를 보여준다. Generator는 Embedding Layer, Feature fusion Layer, Attention Layer, Regression/Classification Layer로 구성되어 있다. Embedding Layer는 입력된 경로 데이터를 벡터화 시킨다. Feature fusion Layer는 한 정점에 해당하는 특징 벡터들을 100크기의 벡터로 융합시킨다. 이는 서로의 특징 학습을 용이하게 한다. Attention Layer는 경로의 각 정점을 모델링 할 때, 관련이 있는 이전 Layer의 특정 정점에 집중하는 역할을 한다. 이를 통해 보다 정확하고 현실적인 경로 모델링이 가능하다. 또한 정점간의 공간 관계를 더 잘 포착할 수 있다. 예를 들어, TAP-GAN이 사용하는 경로 데이터는 정점의 속성을 나타내는 카테고리 값이 포함되어 있기 때문에 지리적 특징이 포함되어 있다고 할 수 있다. 이러한 경우 Attention Layer를 통해 특정 정점이 가지는 카테고리 값에 집중을 할 수 있으므로 더욱 효과적으로 민감 정점을 숨길 수 있게 된다. 마지막으로 Regression/Classification Layer은 Attention Layer의 출력을 합성 경로 데이터로 디코딩하는 작업을 한다. 위치 특징의 경우 tanh 활성화 함수를 통해 디코딩 되며, 나머지 특징들은 softmax를 통해 디코딩 된다.



(그림 2) Generator 아키텍쳐

Generator가 생성한 합성 경로 데이터는 Discriminator의 입력으로 사용된다. 그림 3은 Discriminator의 아키텍쳐를 보여준다. Discriminator는 Embedding Layer, Feature fusion Layer, LSTM Layer, Classification Layer로 이루어져있다. 전체적인 작업은 Generator와 동일하다. 하지만 Discriminator는 경로 데이터의 진위를 판별하고, 클래스를 예측하는 역할을 하기 때문에 Embedding Layer의 출력에 Noise를 추가하지 않으며, Attention Layer가 아닌 LSTM Layer만 사용한다.



(그림 3) Discriminator 아키텍쳐

4. 실험

TAP-GAN의 성능 평가를 위해 Hausdorff distance와 TUL(Trajectory User Linking) Test를 사용한다. 성능 비교를 위해 선행 연구 모델인 LSTM-TrajGAN과 TCAC-GAN의 점수를 함께 비교한다. Hausdorff distance는 두 집합간의 유사도를 측정하는 방법이다. 표 1은 세 모델의 Hausdorff distance 점수를 나타낸다. 모든 점수에서 TAP-GAN의 점수가 낮은 것을 확인할 수 있다. 이는 원본 경로 데이터와 합성 경로 데이터간의 거리 차이가 작다는 것을 의미하며, TAP-GAN의 유용성이 가장 높음을 나타낸다.

<표 1> Hausdorff distance 점수 비교

	LSTM-TrajGAN	TCAC-GAN	Proposed
MIN	0.006839	0.004439	**0.002554**
MAX	0.062886	0.052982	**0.051066**
AVG	0.020647	0.017155	**0.015668**
MEAN	0.019752	0.015978	**0.015228**

표 2는 세 가지 모델의 TUL 정확도를 보여준다. TUL Test는 ACC@1, ACC@5, Macro-Precision, Macro-Recall, Macro-F1 score로 이루어져 있으며, 경로 분석을 통한 사용자 식별의 정확도를 측정하는 방법이다. 따라서 TUL 정확도가 낮을수록 사용자를 식별할 수 없음을 나타내며, 익명성이 높음을 의미한다. TAP-GAN은 Macro-P를 제외한 모든 점수에서 높은 익명성을 보여준다. Macro-P의 결과는 레이블을 이용한 카테고리 값의 조건부 생성과 attention mechanism의 결합으로 인해 평균 정밀도가 조금 떨어졌다는 것을 의미한다. 하지만 이를 제외한 모든 측면에서는 TAP-GAN이 사용자가 식별되는 것을 효과적으로 방지할 수 있음을 보여준다.

<표 2> TUL 정확도

	LSTM-TrajGAN	TCAC-GAN	Proposed
ACC@1	0.406037	0.308666	**0.256086**
ACC@5	0.651412	0.587147	**0.515093**
Macro-P	0.345144	0.230609	**0.251950**
Macro-R	0.390910	0.256103	**0.243969**
Macro-F1	0.374779	0.293933	**0.206121**

5. 결론

위치 기반 서비스로 인해 경로 데이터가 기하급수적으로 증가하고 있다. 경로 데이터는 많은 분야에서 유용하게 사용될 수 있다. 하지만 경로 데이터를 통해 사용자의 집 주소와 같은 민감 정보를 유추해 낼 수 있다. 따라서 본 논문에서는 경로 데이터의 유용성을 보존하고, 민감 정점을 보호할 수 있는 합성 경로 생성 모델 TAP-GAN을 제안하였다. 또한 선행 연구 모델인 LSTM-TrajGAN, TCAC-GAN과의 성능 비교를 통해 TAP-GAN의 유용성과 익명성의 향상을 입증하였다. 이를 통해 TAP-GAN이 생성한 경로 데이터를 분석 가능한 자료로 유용하게 사용할 수 있음을 기대한다. 차후 연구로는 TAP-GAN의 출력에 차분 프라이버시를 도입함으로써 경로 데이터를 질의할 때, 사용자의 프라이버시를 강화하는 연구를 진행하려 한다.

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, 50%)과 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2021R1F1A1054739, 50%).

참고문헌

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

[2] Odena, A., Olah, C., and Shlens. J, "Conditional Image Synthesis with Auxiliary Classifier GANs", ICML, Sydney, 2017, pp. 2642-2651

[3] Rao, J., Gao, S., Kang, Y., and Huang, Q., "LSTM-TrajGAN: A Deep Learning Approach to Trajectory Privacy Protection", GIScience'21, Poznań, 2021, pp. 17

[4] 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", BigComp, Jeju, 2023, pp. 314-315

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