trajGANs: Using generative adversarial networks for geo-privacy protection of trajectory data (Vision paper)

Xi Liu$^{\star 1[0000-0002-1771-3731]}$, Hanzhou Chen[1], and Clio Andris[1]

Department of Geography, The Pennsylvania State University, University Park, PA 16802, USA {xiliu,hzc176,clio}@psu.edu

Abstract. In this vision paper, we propose the trajGANs framework and address the potential of using generative adversarial networks for geo-privacy protection of trajectory data. Our goal is to provide a geo-privacy protection layer for trajectory data publication and usage by generating synthetic trajectories that can preserve the summary properties of real data and have close-to-real-data performance in analysis tasks. We summarize the trajectory types in geo-privacy protection and the possible data generation scenarios. We also provide validation metrics and address the possible challenges of implementing trajGANs.

Keywords: Geo-privacy · Trajectory data · Generative adversarial networks.

1 Introduction and motivation

People's location information in cities is tracked by various sensors and mobile devices, which produces massive trajectory data. The footprint of people's daily travel can be passively collected when their mobile phones connect to a nearby cell tower, or be recorded by the apps installed on their mobile devices based on GPS signals. Location information is also actively shared by users on social media platforms, commonly referred to as "check-ins". Trajectory data are valuable for commercial uses, such as targeted advertisements based on places users have visited. Moreover, trajectory data contain rich information about people's travel patterns and their interactions with the urban built environment, which can benefit academic research in fields such as transportation, geography, and urban planning.

However, leveraging users' detailed spatiotemporal traces in cities can easily violate their privacy [6]. For example, it is possible to infer home/work location and socioeconomic status of a user even from sparse social media check-in data. Although personal identifiers such as user IDs are often removed to anonymize trajectory data, users can still be re-identified with very little location information [3]. For instance, if a social media company such as Foursquare published an

* Corresponding author.

anonymous check-in dataset, it would be possible to re-identify a user by cross-referencing even only four or five check-ins he or she shared on Twitter.

Current research in geo-privacy protection for trajectory data has mainly focused on two scenarios: disclosing real-time locations and publishing historical trajectory data [13]. In both scenarios, the studies try to blur a user's location and add more uncertainty to reach the goal of K-anonymity and differential privacy, while still maintaining a certain level of utility for specific analysis tasks [2]. However, the trade-off between uncertainty and utility is hard to control: an algorithm may obscure the trajectory data to the extent of perfectly protecting geo-privacy, but cannot ensure the data quality for most use cases.

Rapidly-developing machine learning techniques can provide opportunities to protect geo-privacy of trajectory data from new perspectives. Generative adversarial networks (GANs [5]) are a family of neural network models that can generate high-quality synthetic data which follow the same distribution as the training data. A typical GAN contains a generator and a discriminator, which are usually both neural networks, and it learns the original data distribution by playing a minimax game. GANs do not require large input data and have been widely adopted in producing high-quality images (e.g. [9]) that looks real. GANs also provide potential solutions for some privacy issues. For example, [1] designed medGAN to generate synthetic patient records that preserve the statistical properties and achieved comparable performance in multiple tasks to real data.

In this paper, we propose the trajGANs framework to address the potential for and challenges of using GANs for geo-privacy protection when publishing people's trajectory data. The trajGANs can be used in the historical data publication scenario as a geo-privacy protection layer (Figure 1). The goal of trajGANs is to generate synthetic trajectory data that can ensure the quality of multiple summary analysis tasks.

2 Trajectory types and data generation scenarios

A users trajectory is a sequence of consecutive location points accompanied with time stamps, i.e. $l_1 \rightarrow l_2 \rightarrow \cdots \rightarrow l_n$, where $l =< x, y, t >$. Raw trajectory data are often messy and require preprocessing steps such as map matching and stay-point detection to be transformed into more interpretable formats. One unique property of human trajectories compared to movements of other animals is that human travel in cities is constrained by the urban topology of places and road networks.

Thus, we categorize processed trajectory data into two categories: **road-based trajectories** and **place-based trajectories**. Road-based trajectories are mapped to road networks and can be simplified as sequences of road segments and time stamps, i.e. $< s_1, t_1 > \rightarrow < s_2, t_2 > \rightarrow \cdots \rightarrow < s_n, t_n >$, where s_i refers to a road segment. Trajectories of bikes and Uber/Lyft are often simplified into road-based trajectories using map matching algorithms. They focus more on the geometric information of trajectories (e.g. which road segments the user took)

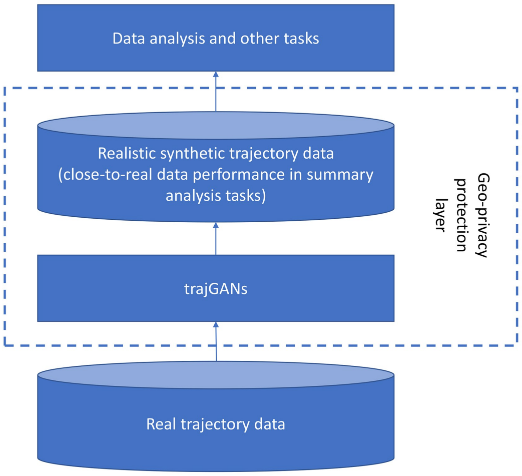
Data analysis and other tasks
Realistic synthetic trajectory data (close-to-real data performance in summary analysis tasks)
Geo-privacy protection layer
trajGANs
Real trajectory data

Fig. 1. Adding the geo-privacy protection layer in data publication using trajGANs can contribute to privacy protection by generating synthetic trajectory data that preserve summary analysis results compared to real data.

and are often used for route recommendation and transportation planning. Place-based trajectories are usually simplified into sequences of places, such as points of interest (POIs) or neighborhoods, and time stamps, i.e. $< p_1, t_1 > \rightarrow < p_2, t_2 > \rightarrow \cdots \rightarrow < p_n, t_n >$, where p_i refers to a place. They are rich in semantics: we can infer the related activities, such as work, shopping, and dining, inherent to each trip in a trajectory based on the property of the place. Social media check-in data are an example of place-based trajectories, although other trajectory data, such as mobile phone records, can also be transformed into place-based trajectories using stay-point detection.

Based on the usage of published historical trajectory data, we further divide the synthetic trajectory generation scenario into **individual trajectory generation** and **aggregated trajectory generation** (Figure 2). Individual trajectory generation aims to generate synthetic trajectories that have similar properties to each individual people. The trajectory of a person needs to be divided into multiple segments in order to train the generative model. For aggregated trajectory generation, the goal is to generate synthetic trajectories that approximate the summary statistics and analytical capabilities inherent to the original dataset.

3 The trajGANs framework

Similar to a typical GAN [5], a trajGAN consists of two main parts: a generator G and a discriminator D (Figure 3). The generator G accepts a random vector z and generates dense representation of synthetic trajectory samples, while the

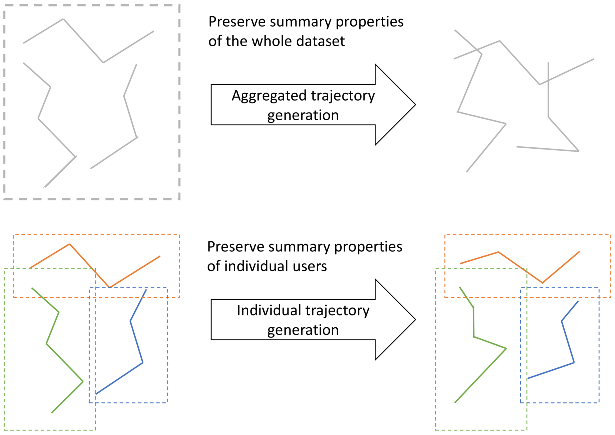
Preserve summary properties of the whole dataset
Aggregated trajectory generation
Preserve summary properties of individual users
Individual trajectory generation

Fig. 2. trajGANs can be designed to generate synthetic data that preserve properties of the whole dataset or of each user.

discriminator D classifies an input trajectory sample into "real" or "fake". G and D are both neural networks. During the training process, the discriminator D tries to maximize the probability of correctly labeling real and fake trajectories, while the generator G tries to generate indistinguishable trajectory samples for D. The G and D play a minimax game with the following objective function:

$$\min_G \max_D [\mathbb{E}_{x \sim p_{data}} \log D(\boldsymbol{x}) + \mathbb{E}_{z \sim p(\boldsymbol{z})} \log(1 - D(G_x(\boldsymbol{z}))] \tag{1}$$

where p_{data} is the distribution of the real trajectory samples and $p(\boldsymbol{z})$ is the distribution of the random prior. In other words, in the training process, G learns to map z sampled from the prior to the distribution of the original trajectory data through non-linear transformations. Thus, after the training process, we are able to use the generator to generate synthetic trajectories that share the same properties as the real samples.

For designing a trajGAN, one challenge is creating dense representations of trajectories, i.e. representing a trajectory as a fixed-length vector of numbers as input and output for the generator and discriminator. Recurrent Neural Networks (RNNs) combined with LSTM/GRU would be the ideal fundamental structure for the encoder and decoder to transform between trajectories and distributional representations [4]. Modifications are needed for different usage scenarios.

As the basic elements in a trajectory sequence, road segments and places are often pre-trained into vector representations to feed into the RNNs for learning trajectory embeddings. POI embedding is an emerging topic that could benefit place-based trajectory generation, and the spatial and/or temporal properties of POIs have been shown to improve performance [11, 12]. Some studies also discretize continuous geographical space into small areas (e.g. grids, census tracts) to reduce the complexity of place-based trajectories [8], while choosing

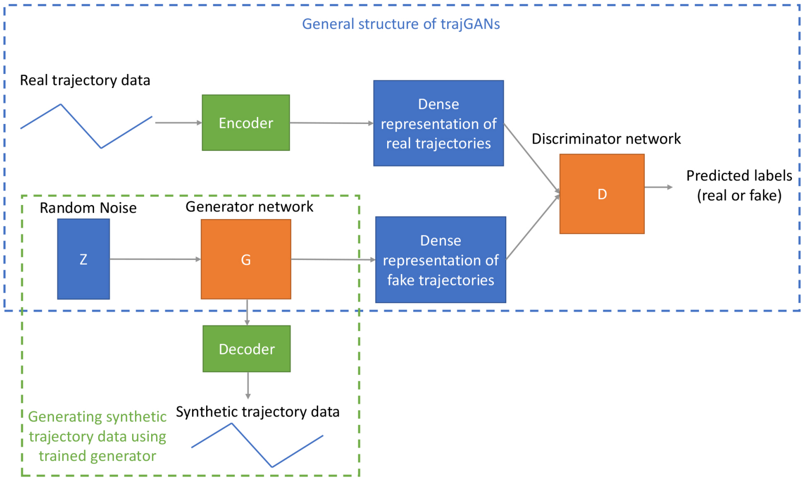
General structure of trajGANs
Real trajectory data
Encoder
Dense representation of real trajectories
Discriminator network
D
Predicted labels (real or fake)
Random Noise
Z
Generator network
G
Dense representation of fake trajectories
Decoder
Synthetic trajectory data
Generating synthetic trajectory data using trained generator

Fig. 3. The framework of trajGANs. The detailed structure would vary according to the properties of the input trajectories.

the granularity of those areas is an issue that needs attention. As for road-based trajectories, they are strictly constrained by road networks since the transition of road segments can only happen between the spatially adjacent ones. Thus, more adaptations are needed on the RNN structure for encoding/decoding road-based trajectories [10].

The representation of time-stamps in trajectory sequences is also poorly addressed in the current literature since most related work focuses on predicting the next location of a trajectory, which does not require a specific time-stamp. Besides incorporating random process models, one possible solution for place-based trajectories is dividing time stamps into slots and learning embeddings for the slots such as hour of the day and day of the week. The learned time-stamp vectors can be concatenated with place vectors and fed into the RNN based encoder. In the decoding process, we can add random deviations to generate more realistic time stamps based on the slots. For road-based trajectories, generating time-stamps based on travel speed sampled from real data may be helpful.

As mentioned, travel patterns in cities are repetitive and often have anchor points such as work and home places. Thus, for place-based trajectories, modifying the trajGANs framework based on the conditional generative adversarial network (CGAN) [7] may generate synthetic trajectories that are conditioned on certain home and work locations sampled from residential and commercial areas, allowing trajGANs to preserve more properties of the real trajectories while not revealing home and work locations of individuals.

4 Validation metrics

Based on trajectory types and data-generation scenarios, we propose multiple validation metrics (Table 1) to measure the performance of a trajGAN. These metrics cover different perspectives of trajectory-related analysis, and it may be difficult for a model to perform well on all metrics. Thus, the tasks that are commonly used for research and analysis of published datasets should be emphasized and prioritized.

Table 1. Metrics for measuring the performance of trajGANs

	Road-based trajectory	Place-based trajectory
Individual trajectory generation	segment usage distribution segment usage temporality transportation mode comparison speed distribution time in transit	activity space radius of gyration tortuosity mobility motifs
Aggregated trajectory generation	segment usage distribution segment usage temporality average speed distribution user distribution driving behavior	temporal semantics of POIs trip-length distribution trip-angle distribution network-based urban structure OD matrix comparison

5 Conclusions and Discussion

In this vision paper, we proposed the trajGANs framework, which aims to protect geo-privacy of trajectory data by generating synthetic trajectories that preserve the summary statistical properties of real data and offer competitive performance in important tasks. Different from simulations, trajGANs directly sample from the complex distribution of trajectory data through training samples instead of generating trajectories with explicit functions based on pre-calculated statistical metrics. Simulation models require a deep understanding of how and why people travel, while trajGANs have the potential to preserve more properties of original data in a more straightforward approach.

However, implementing trajGANs presents major challenges. Aside from aforementioned trajectory embedding and time-stamp issues, we may also face problems such as failing to identify the occasional inter-city travels of people. Moreover, training GANs itself has many engineering challenges. We need to prevent the model from overfitting or converging to a local optimum. If the model simply copies the training data instead of generalizing high-level patterns in trajectories, we may risk of violating privacy. Despite these challenges, efforts to solve trajectory related geo-privacy issues are likely to pay-off in the future, as these data have already revealed many interesting patterns about human behavior in the built environment, and need to be safeguarded to ensure their continued use for planning and policy.

References

1. Choi, E., Biswal, S., Malin, B., Duke, J., Stewart, W.F., Sun, J.: Generating multi-label discrete patient records using generative adversarial networks. In: Machine Learning for Healthcare Conference. pp. 286–305 (2017)
2. Chow, C.Y., Mokbel, M.F.: Trajectory privacy in location-based services and data publication. ACM SIGKDD Explorations Newsletter **13**(1), 19–29 (2011)
3. De Montjoye, Y.A., Hidalgo, C.A., Verleysen, M., Blondel, V.D.: Unique in the crowd: The privacy bounds of human mobility. Scientific reports **3**, 1376 (2013)
4. Gao, Q., Zhou, F., Zhang, K., Trajcevski, G., Luo, X., Zhang, F.: Identifying human mobility via trajectory embeddings. In: IJCAI (2017)
5. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y.: Generative adversarial nets. In: Advances in neural information processing systems. pp. 2672–2680 (2014)
6. Keßler, C., McKenzie, G.: A geoprivacy manifesto. Transactions in GIS **22**(1), 3–19 (2018)
7. Mirza, M., Osindero, S.: Conditional generative adversarial nets. arXiv preprint arXiv:1411.1784 (2014)
8. Ouyang, K., Shokri, R., Rosenblum, D.S., Yang, W.: A non-parametric generative model for human trajectories. In: IJCAI (2018)
9. Radford, A., Metz, L., Chintala, S.: Unsupervised representation learning with deep convolutional generative adversarial networks. arXiv preprint arXiv:1511.06434 (2015)
10. Wu, H., Chen, Z., Sun, W., Zheng, B., Wang, W.: Modeling trajectories with recurrent neural networks. In: IJCAI (2017)
11. Xie, M., Yin, H., Wang, H., Xu, F., Chen, W., Wang, S.: Learning graph-based poi embedding for location-based recommendation. In: CIKM (2016)
12. Zhao, S., Zhao, T., King, I., Lyu, M.R.: Geo-teaser: Geo-temporal sequential embedding rank for point-of-interest recommendation. In: WWW (2017)
13. Zheng, Y.: Trajectory data mining: an overview. ACM Transactions on Intelligent Systems and Technology (TIST) **6**(3), 29 (2015)