Trajectory Data Publication Based on Differential Privacy

Zhen Gu, Harbin Engineering University, China*

https://orcid.org/0000-0003-1480-458X

Guoyin Zhang, Harbin Engineering University, China

ABSTRACT

Analyzing trajectory data can provide people with a higher quality of life. However, publishing trajectory data directly will leak privacy. The authors propose a trajectory data publication method based on differential privacy (TDDP). TDDP method consists of two stages. In the location generalization stage, firstly, the locations at each timestamp are clustered into classes by k-means++ algorithm, and then the representative location of each class is selected by using the exponential mechanism. In the generalized trajectory data publication stage, the authors design a sampling mechanism to form the generalized trajectories. The locations are sampled from the representative locations under different timestamps to form the generalized trajectories. The TDDP method can avoid the generation of non-semantic representative locations and ensure that the generalized trajectories can resist filtering attacks. The experimental results show that the trajectory data released by TDDP method can achieve a good balance between privacy protection and data availability.

KEYWORDS

Data Publication, Differential Privacy, Exponential Mechanism, Filtering Attacks, Generalized Trajectory, Privacy Leakage, Representative Location, Trajectory Data

INTRODUCTION

In the era of big data, location-aware technologies such as mobile communications and sensing devices digitize the geographic locations of people and objects, and subsequently generate a large amount of trajectory data. Location data contains characteristics of human behavior, by analyzing and mining trajectory data, better services can be provided to people (Yang et al., 2019). For example, urban traffic can be reasonably planned to avoid traffic congestion by analyzing trajectory data (Yuan et al., 2012, & Yuan et al., 2013). However, trajectory data contain a lot of sensitive personal information, such as the home address, work address, physical health status. If the location or trajectory data are directly released, it will lead to privacy leakage (Wernke et al., 2014, Gursoy et al., 2019, & Ding et al., 2020),
seriously, it will even threaten people’s personal safety and property safety. The researches on trajectory
data privacy protection are mainly divided into two types. One is the trajectory data privacy protection
in offline mode. A specific organization collects trajectory data for analysis and mining to provide
useful information to specific customers (Abul et al., 2008, Hua et al., 2015, Li et al., 2017, & Ma et
al., 2021). The other type is online trajectory data privacy protection, such as location-based services.
The real-time trajectory data of moving objects needs to be uploaded to the service provider, in this
case, privacy protection of trajectory data is also required (Zhang et al., 2017, Zhang et al., 2018). In
this paper, the authors mainly study the privacy protection of trajectory data in offline mode.

The existing trajectory data privacy protection methods mainly include \( k \)-anonymity method
(Sweeney et al., 2002), encryption method and random disturbance method. The \( k \)-anonymity
method is vulnerable to attacks with background knowledge. The encryption method is not a commonly
used method due to its high computational cost. Among the random perturbation methods, the
trajectory data publishing based on differential privacy has become a more popular research (Hua et
al., 2015, & Liu et al., 2021). Differential privacy technology (Dwork et al., 2017) is the strongest
unconditional privacy protection technology currently known, differential privacy can resist attacks
from any background knowledge. However, some current researches on trajectory data publishing
based on differential privacy also have some aspects that need to be improved.

(a) Some current researches require that the start and end times of any two trajectories must be the
same or assume that the raw trajectories need to contain the same prefix or a common subsequence.
However, it is difficult for the actual collected trajectory data to have these characteristics.
(b) Some current methods are to cluster the locations of all trajectories at each timestamp, and then
use the cluster center of each class as a representative of all locations within the same class,
at last, they use the cluster centers to generate the generalized trajectory. However, the cluster
centers sometimes do not have semantic information, even, non-semantic representative locations
can appear in multiple clusters, which will make the published trajectories to be identified and
filtered by the adversary.

For the above aspects, the authors propose a trajectory data publishing method based on differential
privacy (TDDP), and the contributions are as follows:

(a) The authors propose a trajectory data publishing method based on differential privacy. The TDDP
method consists of two stages. In the first stage, the locations of each timestamp are clustered
into \( K \) classes, and then the representative location of each class at each timestamp is selected
by the exponential mechanism. In the second stage, locations are sampled from representative
locations of different timestamps to form the generalized trajectories, which can avoid generating
non-semantic locations and resist filtering attacks.
(b) In order to improve the utility of the trajectory data published, in the second stage, the TDDP
method make the generalized trajectory data set is partly composed of the generalized trajectories
which containing the raw trajectories.
(c) The authors conduct experiments on real data set. Hausdorff distance and spatial range queries
are used for measuring the utility of the published trajectory data, mutual information is used to
measure the total privacy loss, the results show that the published trajectory data can maintain
good utility.

RELATED WORK

Abul et al. (2008) proposed the NWA (Never walk alone) algorithm which uses the inherent uncertainty
of the motion trajectory to make the \( k \) trajectories in the trajectory cylinder indistinguishable and
Related Content

Binary Classification of Network-Generated Flow Data Using a Machine Learning Algorithm

Application of Cyber Security in Emerging C4ISR Systems
[www.irma-international.org/chapter/application-cyber-security-emerging-c4isr/56304](www.irma-international.org/chapter/application-cyber-security-emerging-c4isr/56304)

Cyberbullying Among Malaysian Children Based on Research Evidence
[www.irma-international.org/chapter/cyberbullying-among-malaysian-children-based-on-research-evidence/213645](www.irma-international.org/chapter/cyberbullying-among-malaysian-children-based-on-research-evidence/213645)

Designing an Early Warning System for Stock Market Crashes by Using ANFIS
[www.irma-international.org/chapter/designing-early-warning-system-stock/46807](www.irma-international.org/chapter/designing-early-warning-system-stock/46807)

The Role of Mutual Benefit in Informal Risk Management
[www.irma-international.org/article/the-role-of-mutual-benefit-in-informal-risk-management/303105](www.irma-international.org/article/the-role-of-mutual-benefit-in-informal-risk-management/303105)