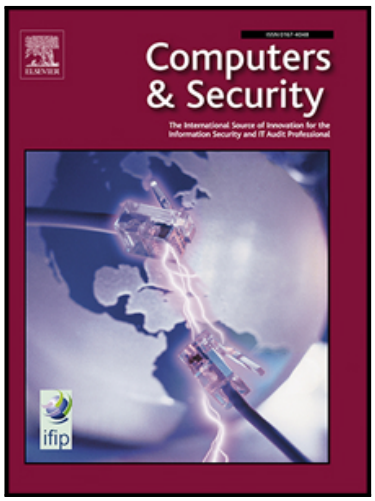


# Trajectory Privacy Protection Method Based on the Time Interval Divided

Zhaowei Hu , Jing Yang , Jianpei Zhang

PII: S0167-4048(18)30489-9
DOI: 10.1016/j.cose.2018.05.001
Reference: COSE 1338

To appear in: *Computers & Security*

Received date: 25 July 2017
Revised date: 8 April 2018
Accepted date: 2 May 2018

Please cite this article as: Zhaowei Hu , Jing Yang , Jianpei Zhang , Trajectory Privacy Protection Method Based on the Time Interval Divided, *Computers & Security* (2018), doi: 10.1016/j.cose.2018.05.001

# Trajectory Privacy Protection Method Based on the Time Interval Divided

**ZhaoweiHu[a,b], Jing Yang[a,*],JianpeiZhang[a]**

[a] Harbin Engineering University, College of Computer Science and Technology, Harbin, China,150001

[b] Jilin Normal University, College of Computer, Siping, China,136000

*Corresponding author. E-mail: lilian1024@163.com (JY)

**Abstract:** Trajectory data often provides information that is well applicable to real-world scenarios such as traffic planning and location-based advertising. Individual trajectory information may disclose sensitive personal data, thus necessitating privacy protection methods. Current methods assume and utilize the same privacy requirements for all trajectories, which can impact their protection and data utilization efficiency. This paper proposes a privacy protection method based on divided time intervals which satisfy different privacy requirements. The method works by constructing a privacy requirement matrix and running trajectory pre-processing based on the different privacy requirements for trajectories in different time points and locations. It uses trajectories that satisfy the (l, δ) -constraint to construct an undirected trajectory graph. By finding the trajectory corresponding to the edge and vertex with the minimum weight, $k_i$-anonymous sets are then constructed with trajectories which share the same or similar privacy requirements. The Manhattan distance can then be applied to calculate the space between trajectories distance, which narrows the gap between the theoretical privacy protection and the actual protective effects. Comparative experiments demonstrate that the proposed method outperforms other similar methods in regards to both privacy protection and data utilization.

**Keywords:** Trajectory privacy protection; Manhattan distance; Time interval divided; Privacy requirement matrix; Trajectory $k_i$-anonymity set

## 1 INTRODUCTION

Advancements in global positioning system (GPS) technology have resulted in a boom in location-based services (LBS).Data encompassing the number of locations and trajectories are collected by service providers to comprise a wealth of space-time information which can be analyzed to form a scientific basis for certain types of decisions. For example, a given user's trajectory information can be mined to predict places of interest in a given region; miners can then establish business circles in these locations to maximize profits. However, the disclosure of trajectory information may expose personal information which threatens the user's privacy. Therefore, the research of trajectory privacy information protection technology has become one of the important contents in information security ( Mehmet et al., 2008; Roman et al., 2009; N. Clarke et al., 2017; Zhou Fucai et al., 2014).

Most existing trajectory privacy protection methods are based on the traditional trajectories k-anonymity method( Moeinet al., 2014), wherein the user's current trajectory and at least k-1 other trajectories are combined into an anonymous region, the probability of disclosing private data is restrained to 1/k, i.e., the value of k represents the privacy requirements of the service. These methods assume that all users have the same privacy requirements and use the same k value to protect their privacy. In reality, of course, different users have different demands for privacy protection – an individual user may even have different privacy requirements across different time points and locations. Applying the same privacy parameter to all trajectories negatively impacts both privacy protection and data utilization. Using a smaller privacy protection parameter reduces its protective effects, but using a