International Journal of Information Security and Privacy
Volume 20 • Issue 1 • January-December 2026

Key Method for Privacy Protection of Trajectory Data

Xiang Gong
http://orcid.org/0000-0002-0170-2982
Hebei University of Environmental Engineering, China

Qiaoqiao Wang
Hebei University of Environmental Engineering, China

Guojie Li
Hebei University of Environmental Engineering, China

Dehan Kong
Hebei University of Environmental Engineering, China
Received: December 19th, 2025 | **Accepted:** March 2nd, 2026

ABSTRACT

With the extensive proliferation of location-based services, protecting user trajectory privacy against continuous query attacks has become a critical challenge. Existing protection mechanisms often suffer from a rigid trade-off between privacy strength and service quality. To bridge this gap, this study proposes a unified demand-aware trajectory privacy protection framework. First, a fake trajectory generation algorithm is developed that ensures to resist advanced inference attacks. Second, a maximizing demand request algorithm is introduced to resolve conflicts between privacy demands and sparse historical data. Finally, two anonymous zone minimization strategies are implemented. Experimental results using real-world mobility generators demonstrate that the proposed framework improves the anonymous service success rate by more than 13% over baseline location privacy-preserving algorithms while maintaining a smaller anonymous area, balancing privacy and utility

KEYWORDS

Privacy Protection, Fake Trajectories, Service Quality, Trajectory Data

INTRODUCTION

With the widespread adoption of 5G, global positioning systems, and radio-frequency identification, location-based services (LBSs) have become ubiquitous for mobile terminal users in both indoor and outdoor environments. LBS applications have permeated daily life, enabling a smart lifestyle for users of devices such as smartwatches and smartphones. The essence of these services is smart terminals' ability to report their location to servers, enabling personalized services. Examples include navigation software (e.g., Google Maps and AutoNavi Maps), ride-hailing apps (e.g., Hailo), and lifestyle apps (e.g., Tripadvisor and Keeta). In addition, payment platforms such as Alipay and WeChat locate nearby stores for promotional discounts. These LBS-based applications have significantly enriched social activities and convenience.

DOI: 10.4018/IJISP.404386

However, the widespread use of LBS has exposed prominent issues. When mobile objects initiate LBS queries, particularly continuous requests, they disclose a large amount of their location information. Consequently, considerable user-related information is stored on servers during service requests. Chiming (2023) discussed that this information used in query computations could potentially expose sensitive user data and lead to personal information leakage. Typically, users do not want their real locations known by anyone else when using LBS. However, attackers may obtain location data from location servers and conduct unauthorized analyses of service requests from different locations. Gambs et al. (2011) reported that when such analyses are combined with known background information, attackers may deduce user attributes (e.g., home addresses, workplaces, daily routes, and interests). Guo et al. (2021) predicted user trajectories and inferred users' movement patterns and age. Qing et al. (2025) showed that leaked information could reveal user queries from locations such as bars, hospitals, or hotels, which are closely linked to personal privacy. Xie et al. (2025) further indicated that such information could enable attackers to target users with advertisements or scams. Several studies have highlighted these risks. In 2016, Uber faced a privacy crisis for tracking location data even when the app was inactive and collecting data without passenger authorization. In 2017, fitness tracker provider Strava's global heatmap of exercise activities, created from user geolocation data, revealed the movements of U.S. military personnel and outlines of sensitive military facilities. In 2020, the activity trajectory of a COVID-19 patient in Chengdu was publicized, leading to widespread dissemination of her personal information and cyberbullying. On July 21, 2022, Hailo was fined more than eight billion Yuan by Chinese authorities for illegally collecting excessive passenger information and attempting to analyze passenger travel intentions without their knowledge. From the individual to the national level, protecting the security of user trajectory information has become an important research topic.

The rest of this paper is organized as follows. Section 2 reviews related work. Section 3 details the fake trajectory generation algorithm (FTGA) and attack models. Section 4 presents the demand-aware request and zone minimization algorithms. Section 5 discusses the experimental evaluation. Section 6 provides a critical discussion of limitations and security concerns, and Section 7 concludes the paper.

LITERATURE REVIEW

To contextualize our contribution, it is essential to examine how existing research handles the tension between privacy preservation and utility. Suitable privacy protection methods for various scenarios have been researched in response to location leakage in LBS. Jing (2024), Qingyun and Wanjie (2020), Li et al. (2023), and Aloufi et al. (2025) summarized and reviewed the current state of location service privacy protection, highlighting the representative methods and their application scenarios. The most representative privacy protection methods fall into two categories: generalization and suppression.

Generalization Methods

Generalization methods are the most widely studied approach in trajectory privacy protection. Sweeney (2002) proposed k-anonymity, which assumes that each database record corresponds to an individual and that attributes are divided into identifiers and sensitive attributes. By generalizing identifier attributes, the technique ensures that each record in the published data is indistinguishable from at least k-1 other records with respect to identifiers, thereby protecting privacy. Although published data retain some utility, they remain at risk of privacy leakage due to homogeneity and background knowledge attacks. To address this issue, Rao et al. (2021) introduced l-diversity, requiring each equivalence class to contain at least one distinct sensitive value. They also proposed entropy l-diversity and recursive diversity models, both effective for protecting datasets with a single sensitive attribute. Dwork et al. (2006) developed the differential privacy model, which gained widespread academic recognition for its rigorous mathematical foundation and customizable privacy