

**RobLoP: Towards Robust Privacy Preserving Against Location Dependent Attacks in Continuous LBS Queries**

**Abstract:**

With the increasing popularity of location-based services (LBS), how to preserve one’s location privacy has become a key issue to be concerned. The commonly used approach *k*-anonymity, originally designed for protecting a user’s *snapshot* location privacy, inherently fails to preserve the user from location-dependent attacks (LDA) that include the maximum movement boundary (MMB) attacks and maximum arrival boundary (MAB) attacks, when the user *continuously* requests LBS. This paper presents RobLoP, a robust location privacy preserving algorithm against LDA in continuous LBS queries. The key insight of RobLoP is to theoretically derive the constraints of both MMB and MAB in a uniform way. It provides a necessary condition of the pairwise user to be safely cloaked against LDA. On top of that, RobLoP first identifies those candidate users who can be cloaked with the requesting user. RobLoP then searches for a so-called strict point set including the candidate set and other auxiliary points, as a sufficient condition under which RobLoP can finally generate the cloaked region successfully. To the best of our knowledge, RobLoP is the first work that can preserve location privacy against LDA thoroughly and closely with a theoretical guarantee. The effectiveness and superiority of RobLoP to state-of-the-art studies are validated via extensive simulations on the real trucks data, the synthetic data, as well as the measured data collected by ourselves.

**Existing System:**

Location-based services (LBS) have been enjoying growing popularity in recent years where mobile users can enjoy context-aware features (e.g., finding nearby restaurants from yelp, or monitoring real-time traffic from Google Maps) at all time and places, with their locations provided to the LBS server. On the downside, the location disclosure when LBS are provided often implies sensitive personal information such as one’s life style or visited places, thereby

raising severe privacy concerns. Therefore, how to preserve location privacy has become a key issue in LBS.

LDA is referred to as, in a narrow sense, the spatio-temporal correlation attacks when location *k*-anonymity is used in continuous LBS as in the existing work

**Proposed System:**

We focus on how to preserve location privacy against, when continuous LBS queries are issued with *k*-anonymity technique, the so-called location dependent attacks (LDA). In the following, we first briefly introduce *k*-anonymity and LDA, and then review existing *k*-anonymitybased privacy preserving methods against LDA, followed by our contributions.