Traffic Localization Under Differential Privacy

Proposed by :
Dionysis Manousakas
University of Cambridge

dm754@cam.ac.uk

Abstract

Emerging intelligent transportation systems often entail end-user applications that continuously transmit geolocation information to external data aggregators performing monitoring tasks. Distributed traffic information can be collected via multiple user data streams, sent and processed in real-time, allowing scalable state estimation of the road network. Revealing sensitive location information though can result in an undesirable loss of privacy for the users in exchange of the benefits provided by the application. Motivated by this scenario, this work will aim to address reliable traffic estimation while formally protecting the privacy of users contributing their data. To this end, we rely on the cryptographically-motivated framework of differential privacy, which offers strong privacy guarantees against adversaries with arbitrary side information. Traffic is represented as a signal over the vertex-domain of a graph corresponding to the underlying road network, and estimated using the idea of trend filtering, which generalizes nonparametric lasso regression to graphs, allowing advances in localizing non-smooth signals and scalability over large datasets. Applying filtering on non-private user data and data protected with increasing levels of differential privacy, we conduct an empirical study on quantifying the tradeoff of privacy and utility on a large volume of spatio-temporal Manhattan urban data.

Keywords

differential privacy, sensor networks, graph smoothing, trend filtering, fused lasso