Abstract

In the era of digital assistants, travel assistants are widely used in everyday travel to easily access route updates during the journey. On-route travel assistants requires continuous user location updates from the start of the journey, during the journey and until the end. Currently there are various approaches to protect the static user location such as location obfuscation, anonymity and perturbation but the constant location sharing increases spatio-temporal correlation amongst the adjacent points making protection more challenging. Such location correlation problem weakens the traditional as well as advanced privacy preserving mechanisms and thus the trajectory must be independent of correlation between those location points.

To address this issue, we propose using Local Differential Privacy with RAPPOR mechanism to construct a privacy-protection mechanism that is based on user locations predicted using a Markov process, rather than actual user locations. This aids ensuring the user's location privacy while also maintaining the correlation between the true trajectory location points, hence improving the utility of the system. The proposed approach has been evaluated in three different ways confirming the improvement of the privacy preserving mechanism RAPPOR when integrated with the location prediction algorithm based on Hidden Markov Model, comparing the actual trajectory and the predicted trajectory based on Markov process and finally identifying the best range of privacy budget values for a travel assistant that preserves privacy while retaining data utility.