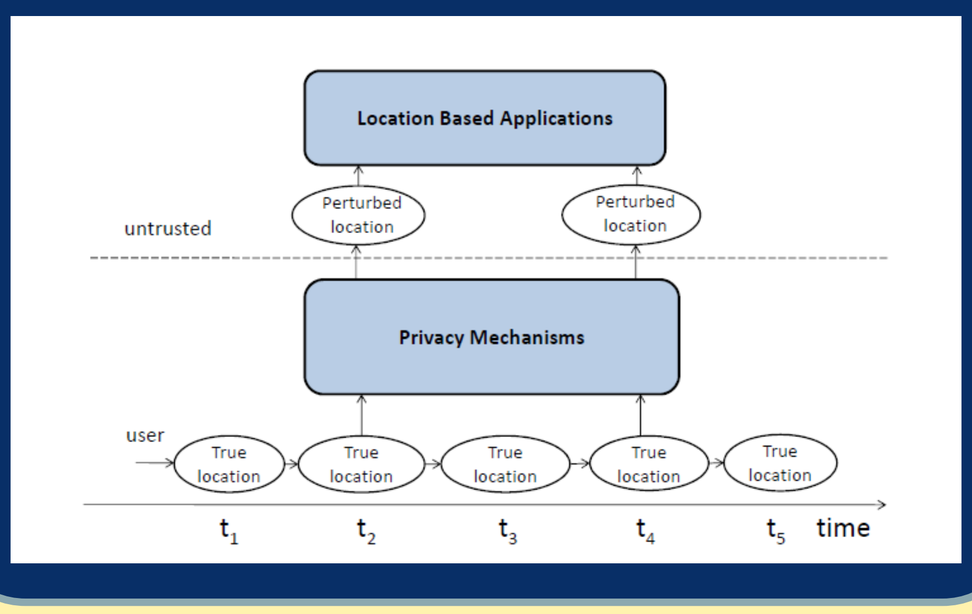
Spatiotemporal Privacy for Location Based Applications

PI: Li Xiong, Emory University http://www.mathcs.emory.edu/aims/stprivacy

The objective of this project is to develop rigorous and customizable privacy notions and location perturbation mechanisms for individual location sharing in location based applications, and study their impact in the context of location based queries and geospatial crowdsourcing.

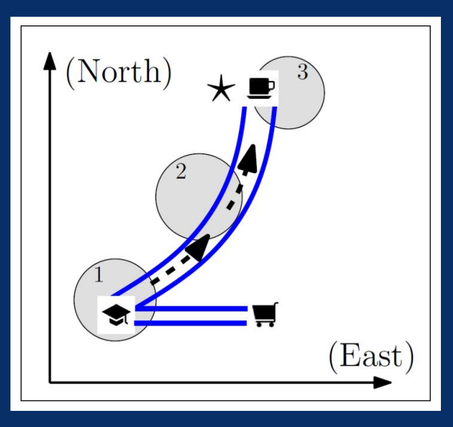
Problem

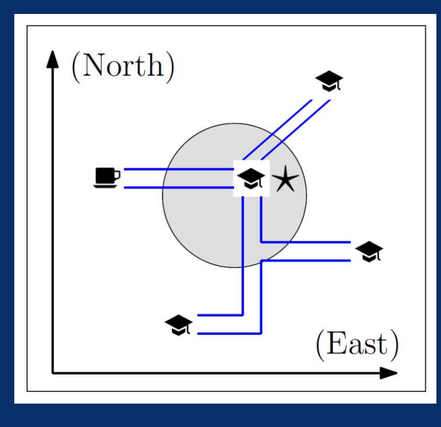
- Preserving privacy of location and trajectories
- Enabling location based applications



Challenges

- Temporal correlations in locations (road networks, moving patterns)
- Personalized privacy requirements (sensitive locations, spatiotemporal semantics)
- Varying application requirements (kNN queries, geospatial crowdsourcing)





Objectives and Approach

Extended and customizable privacy notions

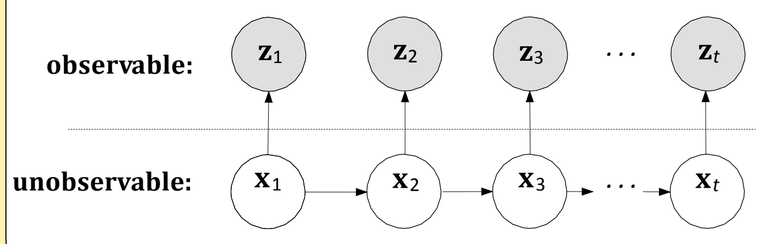
- Location (coordinate) protection accounting for temporal correlations
- Trajectory and spatiotemporal event protection with semantics
- Customizable privacy for both location and trajectory protection via policy graphs

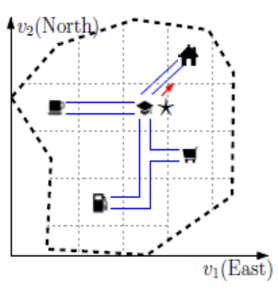
Perturbation mechanisms

- Optimal mechanisms with maximized utility while guaranteeing privacy (distance between perturbed and true location, application driven utility metrics)
- Efficient heuristic mechanisms for high dimensional problem (trajectory perturbation)

Extended differential privacy*

- Hide true location within **possible** locations due to temporal correlations (Markov model) – constrained indistinguishability set
- Ensure each pair of locations in the set is indistinguishable

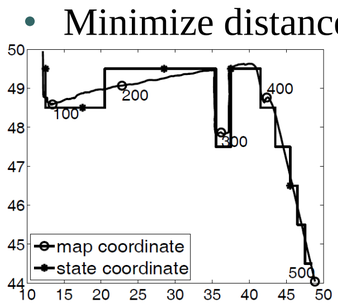




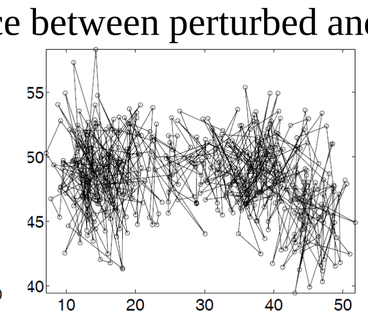
* Y. Xiao, L. Xiong. Protecting Locations with Differential Privacy under Temporal Correlations. ACM CCS 2015

Optimal perturbation mechanism

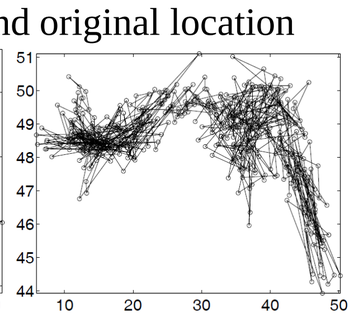
- Based on sensitivity hull of constrained indistinguishability set
- Minimize distance between perturbed and original location



(a) Original trace



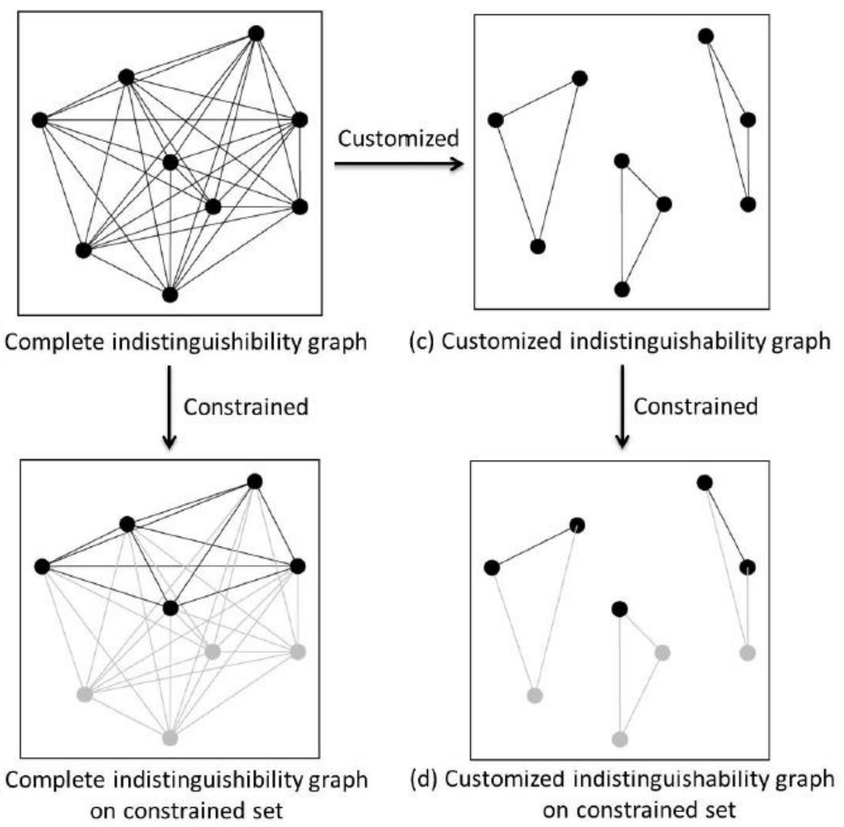
(b) LM Perturbed



(c) PIM perturbed

Customizable privacy via policy graphs

- Extended blowfish privacy on dynamically computed constrained set accounting for temporal correlations
- Challenge: need to ensure customized/constrained graph still guarantees privacy



(a) Complete indistinguishability graph

(c) Customized indistinguishability graph

(b) Complete indistinguishability graph on constrained set

(d) Customized indistinguishability graph on constrained set

Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN

EMORY UNIVERSITY