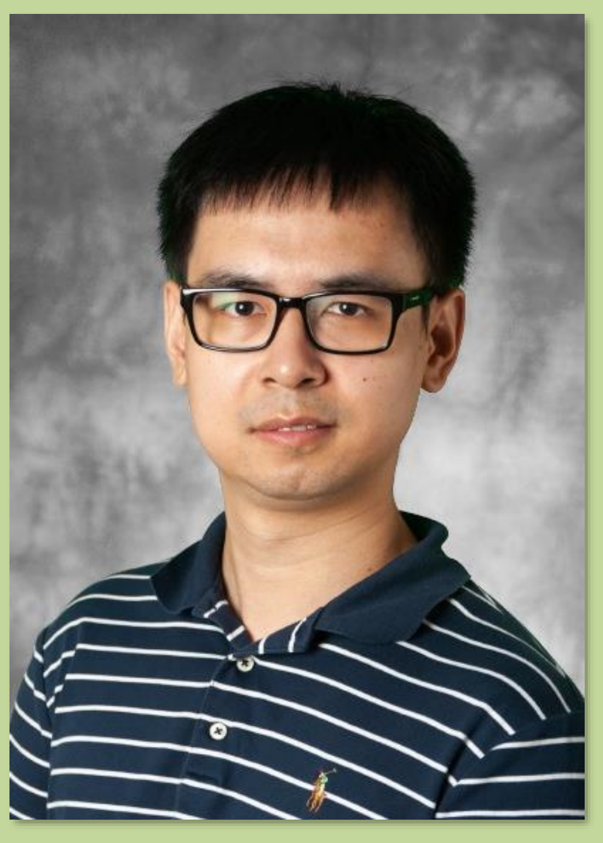
Collaborative research: SaTC: Core: Small: Privacy protection of Vehicles location in Spatial Crowdsourcing under realistic adversarial models

PI (presenter): Chenxi Qiu, University of North Texas, Award ID: CNS2029881

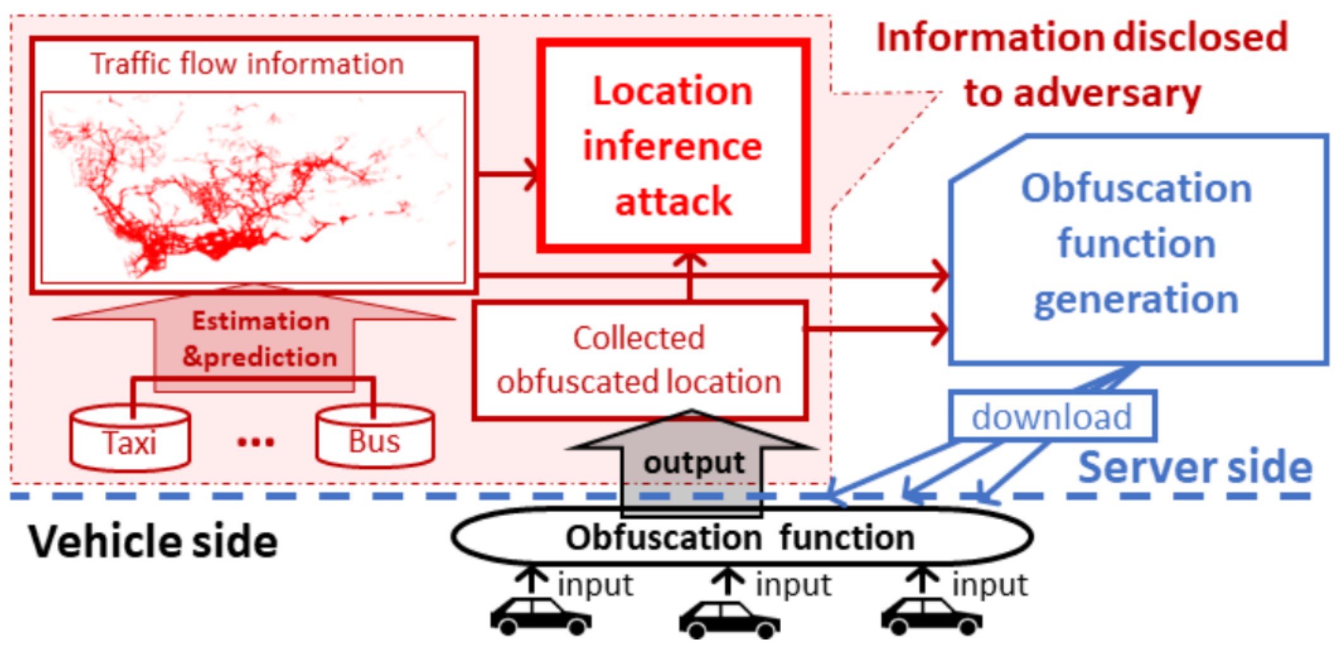
Lead PI: Anna Squicciarini, Penn State University, Award ID: CNS2029976

https://chenxiunt.github.io/projects/1_project/ email: chenxi.qiu@unt.edu



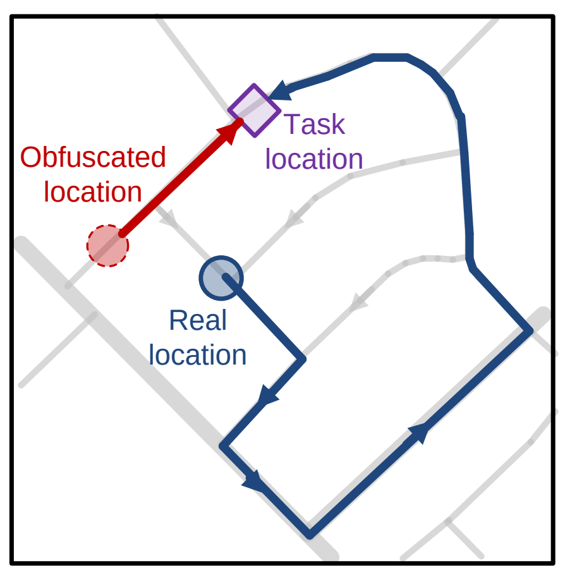
Goals

- Design time-efficient geo-obfuscation in vehicular spatial crowdsourcing by considering vehicles' mobility features.
- Develop realistic threat models using vehicles' mobility features and traffic flow information and design the countermeasures.
- Design scalable geo-obfuscation algorithm in highly dynamic vehicle systems with the consideration of diverse vehicle distribution across different regions.

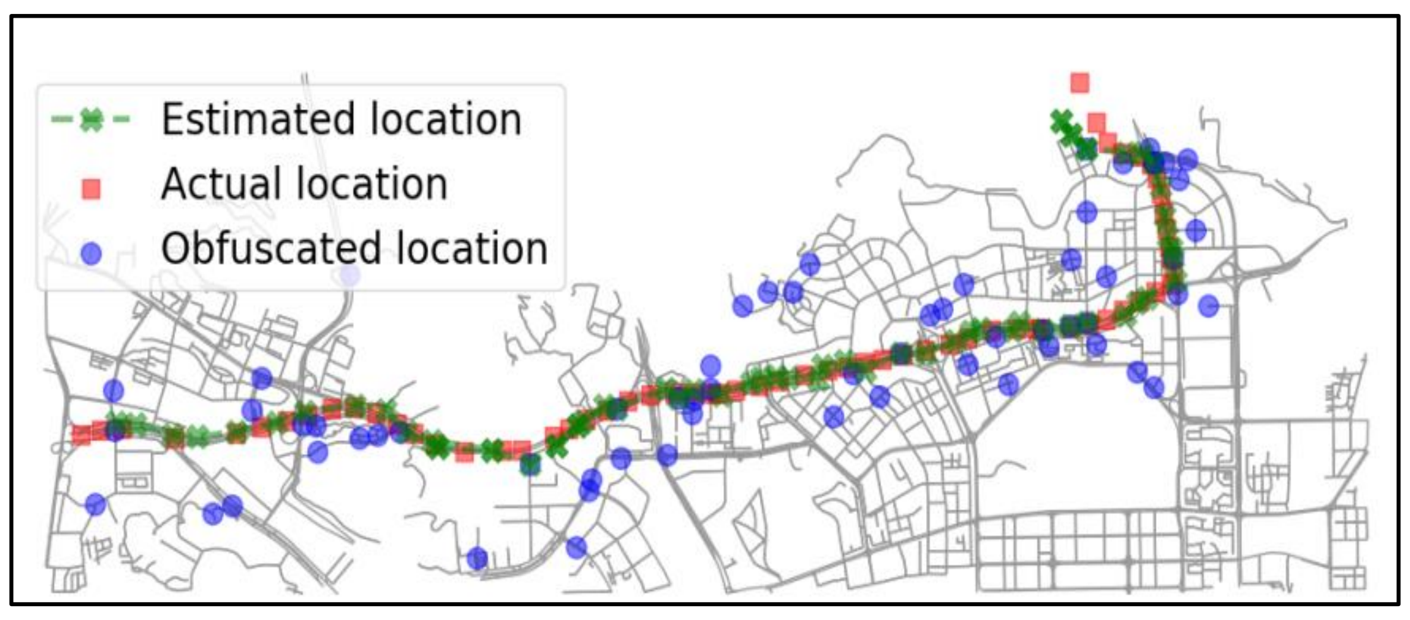


Key problems to be addressed

- How to consider vehicles' mobility features in obfuscation?
- How to protect against new inference attack using vehicles' mobility features and traffic flow information?
- How to consider personalized privacy given vehicles' distribution?



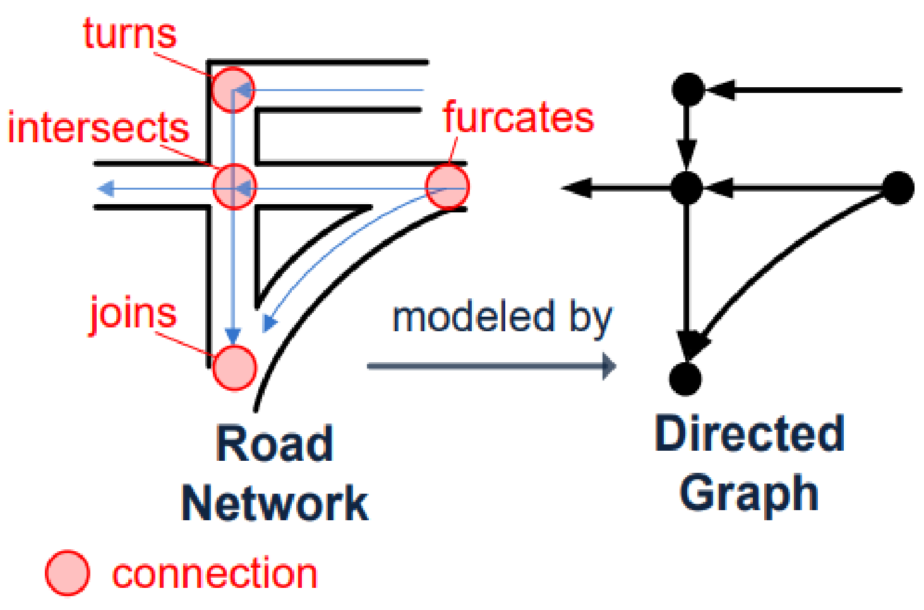
Vehicles' mobility is restricted by road network



Attacker can use traffic flow information to infer vehicles' trajectory

Scientific impact

- New geo-obfuscation based on graph-based mobility model.
- New formal adversarial model accounting for vehicles' mobility features and traffic flow information.

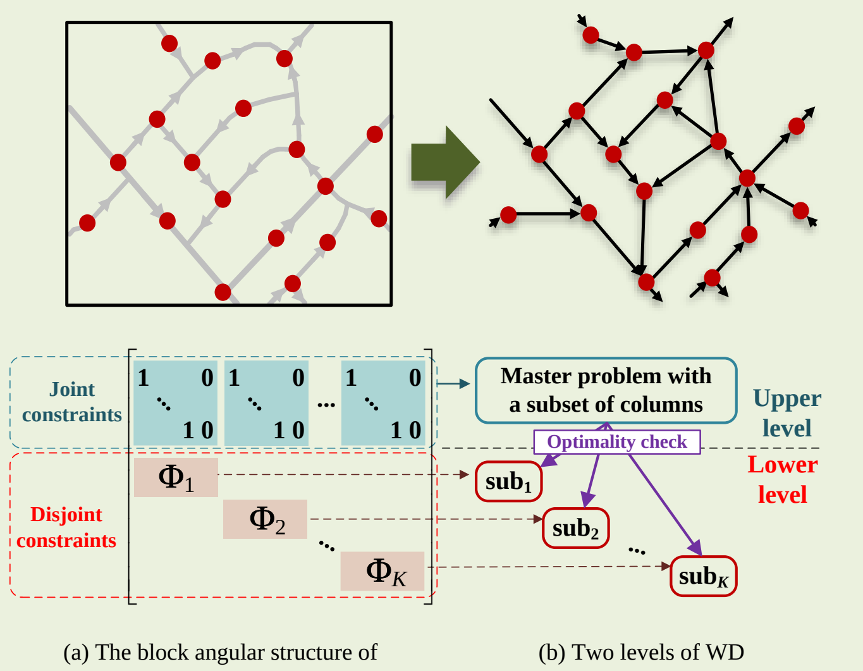


Graph-based mobility model

- Countermeasures to protect against traffic-aware inference attacks.
- Scalable implementation of geo-obfuscation via constraint reduction and optimization decomposition.

Solutions

- 1. Graph-based geo-obfuscation
  - ○ Location field is discretized to "nodes".
  - ○ Linear programming
  - ○ Challenge: high computation load
  - ○ Solutions: constraint reduction

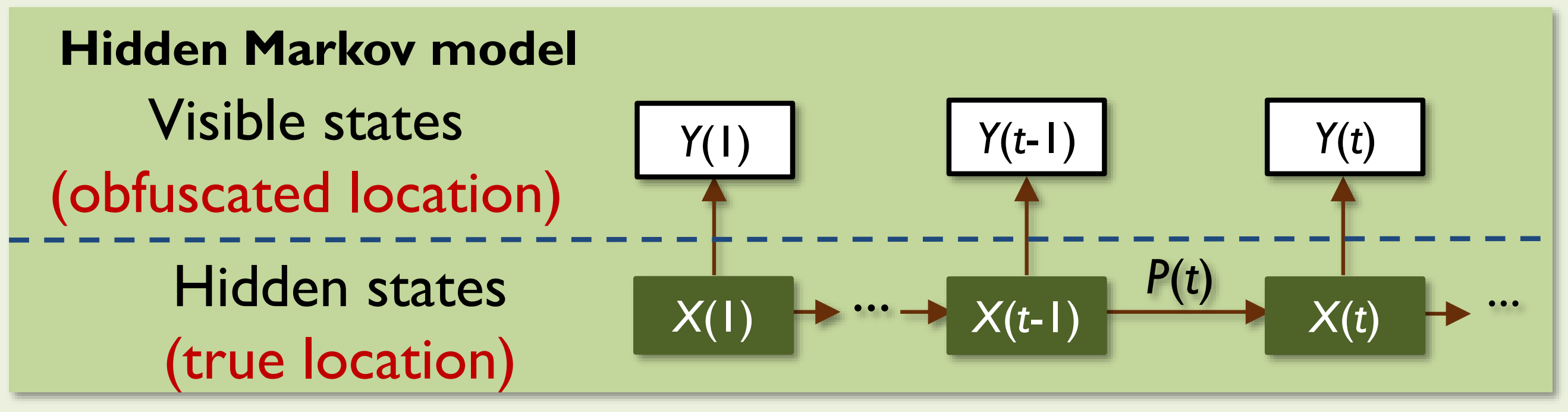


(a) The block angular structure of GMG's constraint matrix

(b) Two levels of WD decomposition

- 2. Adversarial models considering vehicle traffic flow

Model a vehicle's mobility as a Markov process.

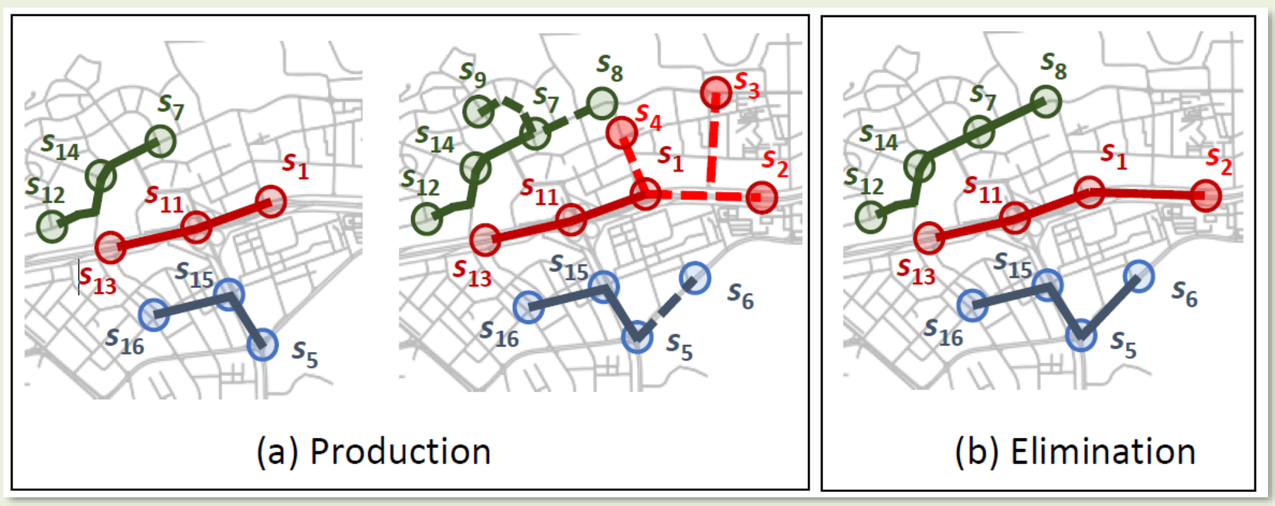


Hidden Markov model

Visible states (obfuscated location)

Hidden states (true location)

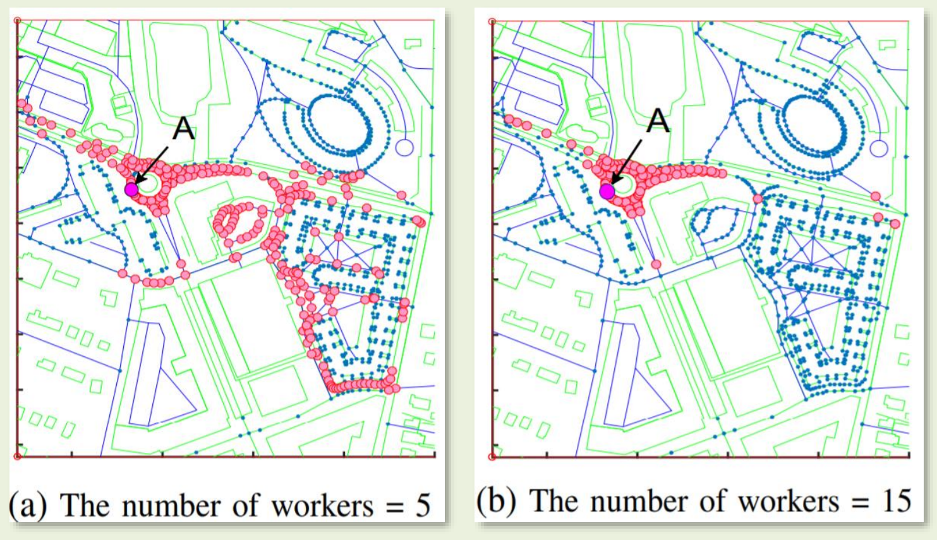
- 3. Trajectory-indistinguishability obfuscation
  - ○ Maintain a pool of fake trajectories.
  - ○ Fake trajectories are indistinguishable (differential privacy).
  - ○ Challenge: Trajectory pool maintenance.


s_1 s_2 s_3 s_4 s_5 s_6 s_7 s_8 s_9 s_{11} s_{12} s_{13} s_{14} s_{15} s_{16}

(a) Production

(b) Elimination

- 4. Elastic privacy criteria by identifying "safe region" of geo-obfuscation
  - ○ Different density leads to different privacy demand.
  - ○ Safe region of geo-obfuscation (identified by sensitivity analysis of utility to obfuscation).



(a) The number of workers = 5

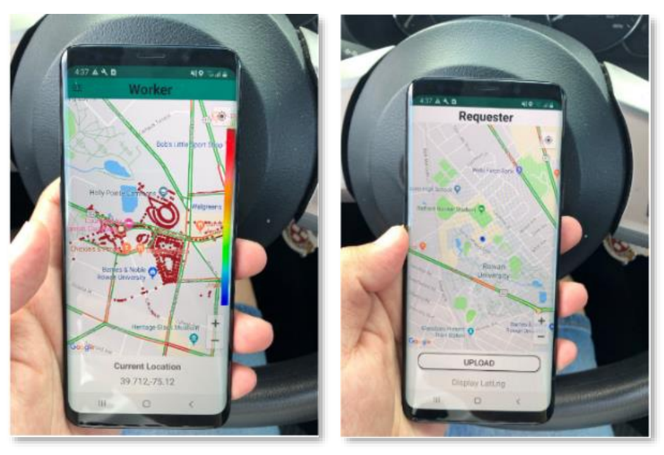
(b) The number of workers = 15

Impact on society

- Protect people's data privacy.
- Incentivize more people to participate in crowdsourcing/public services.

Examples: Transportation systems, Public health systems.

CPR volunteer location protection.



Transportation system.

Education and outreach

- Participated students

1 Ph.D. students, and 3 undergraduate students at Rowan (PI's previous institution) and UNT.

- Course development

CSE 5880 (Computer Networks) at UNT: project – crowdsourcing platform design.

- Participation from underrepresented groups

Impact on other domains

- Mobile user privacy protection in general location-based service (consider mobility restrictions).
- Fine-grained geo-obfuscation.
  - ✓ graph-based mobility models under different scenarios (e.g., high buildings).
- Applications of optimal decomposition & constraint reduction.

The 5th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2022 SaTC PI Meeting)

June 1-2, 2022 | Arlington, Virginia