

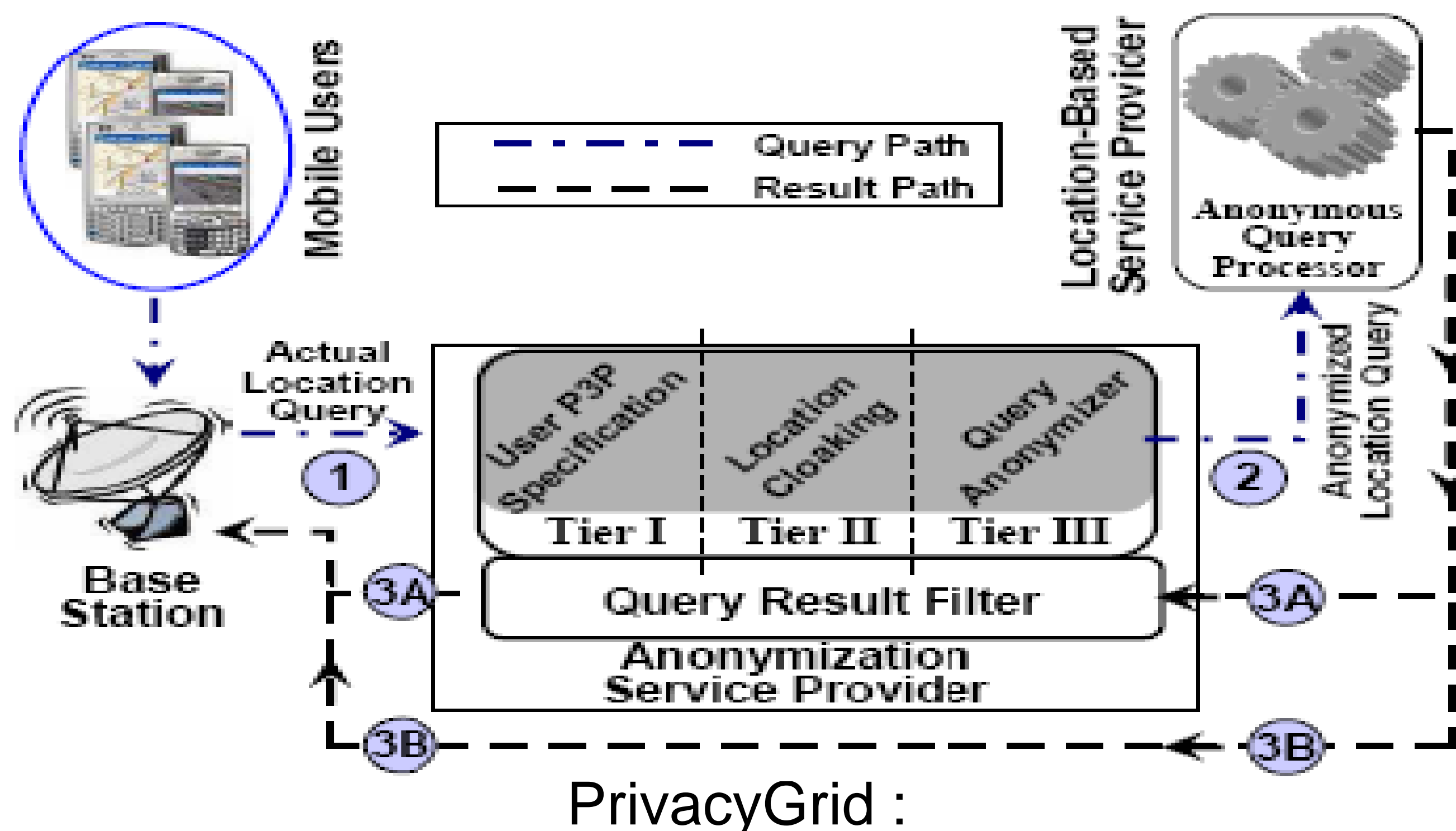
Protecting Location Privacy in Location-Aware Computing Architectures and Algorithms

(NSF Grant CNS-0627474)

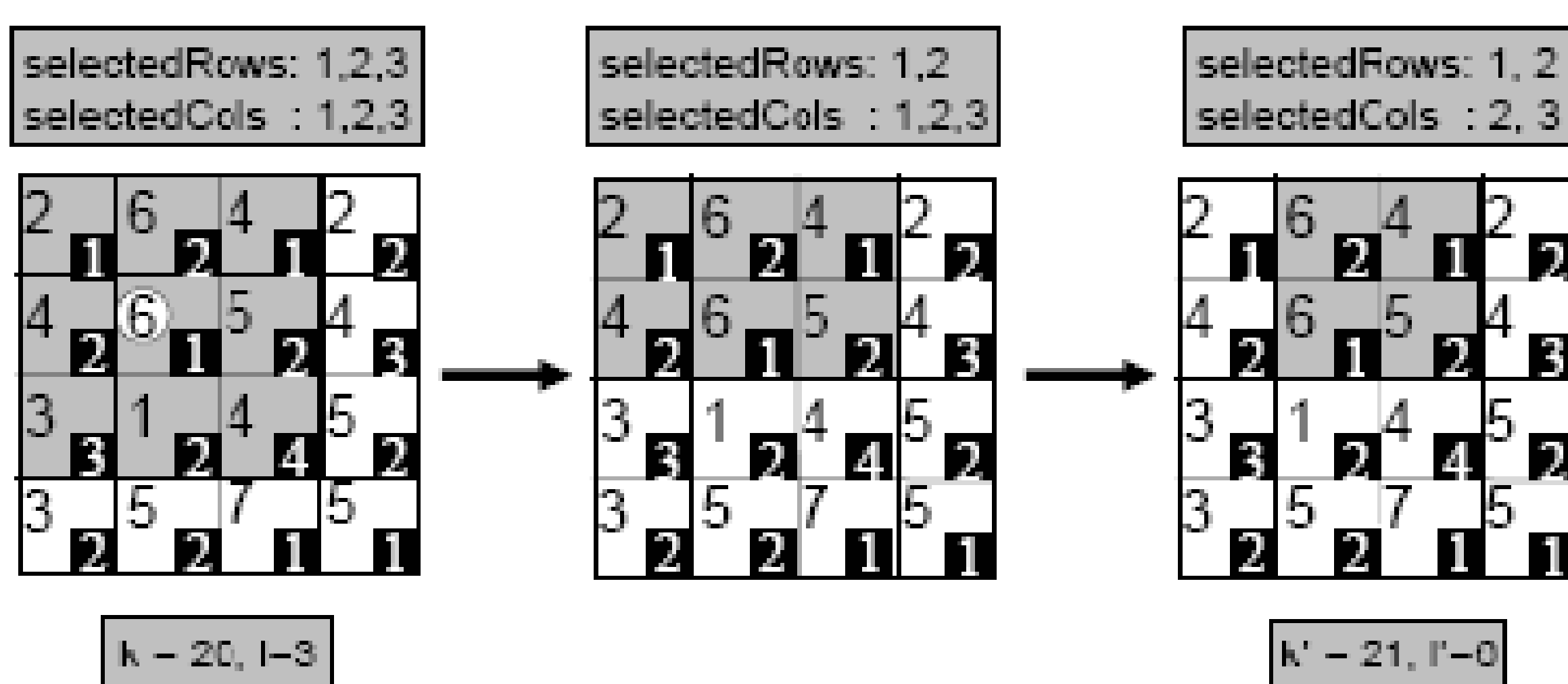


Ling Liu, Georgia Institute of Technology (www.cc.gatech.edu/projects/dis/LocationPrivacy/)

- Investigate alternative architecture designs for providing personalized location privacy guarantee, while maintaining desirable quality of service requirements
- Exploits the intrinsic relationships between policy-based location privacy model and location-anonymity based privacy protection mechanisms
- Finding an optimal balance between location privacy and location service quality and Introducing uncertainty on location-identity associations
- Scalable and attack resilient location cloaking algorithms

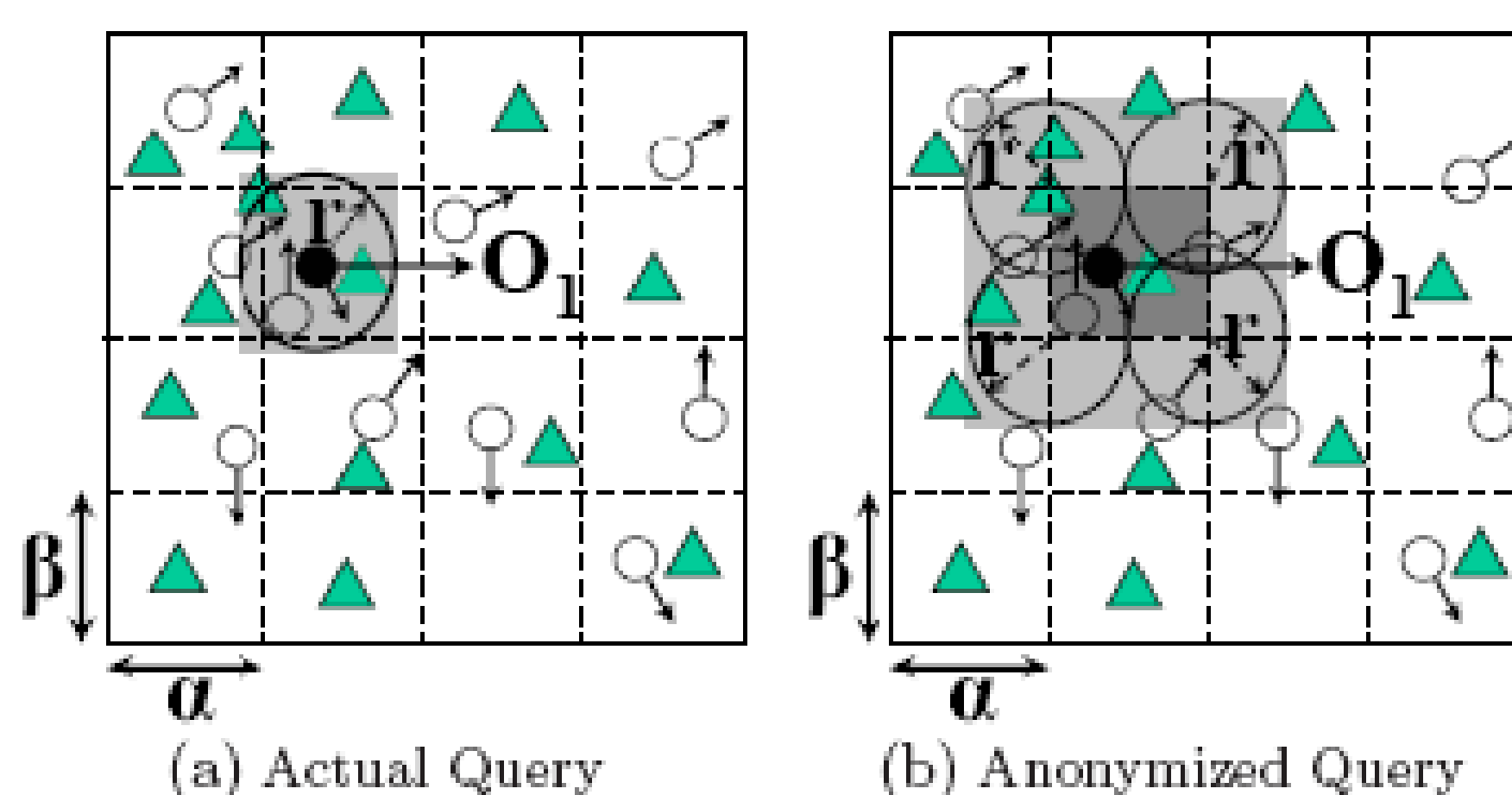


PrivacyGrid :
A Three-Tier Location Anonymization Framework



PrivacyGrid Top-Down Location Anonymization, ensuring location k -anonymity and location l -diversity.

Anonymous Location Query Processing



Personalized Location Anonymization

Usage Model:

Privacy Requirements serve as constraints for location cloaking
 Location k -anonymity with variable k
 Location l -diversity with variable l
 Personalized maximum Spatial/Temporal Resolution

Three Alternative Location Anonymization Models

Centralized corporate,
 Decentralized non-corporate,
 Device based.

Design Goals

Optimal Anonymization: cloaking as many messages as possible; minimizing dropped service requests due to location anonymization requirements given in the usage model.

Technical Challenges

- How to balance location privacy and service quality?
- How to provide personalized location privacy? variable k + variable l + personalized constraint box \rightarrow maximum temporal and spatial location resolution
- What is the most scalable and yet effective architecture for supporting personalized location anonymity model?