Enabling Private Continuous Queries for Revealed User Locations

By
Chi-Yin Chow and Mohamed F. Mokbel

Presented by
Ove Andersen

Outline

- Introduction
- System models
- Privacy Problems
- Privacy-preserving properties
- Robust spatial cloaking algorithm
- Results
- Conclusion
- Related work & contributions
- Evaluation of paper

Introduction

- Location Based Services
- Location privacy
  - May the service know where you are?
- Query Privacy
  - May the service know you made that query?
- Courier business example
  - Company needs to know the location of the employees
  - Company must not keep track of the behaviors of the employees / what queries they make

Introduction

- *K-anonymity*
  - location indistinguishable between k users
- *Minimum spatial area*
  - location blurred into larger region
- Does not distinguish between query and location privacy
- Hides both queries and locations from service

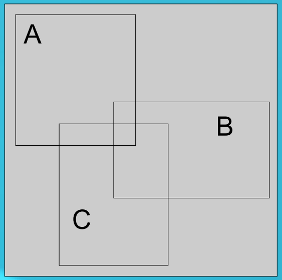
Introduction

- A robust spatial cloaking algorithm
  - Distinguishes between location and query privacy
  - Supports private LBS for public locations
  - Performs spatial cloaking on-demand rather than on every location update
  - Anonymize the link between user locations and location-based queries

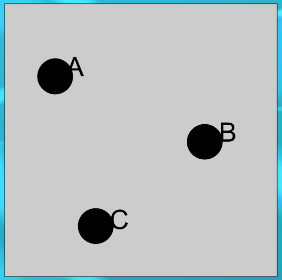
System models

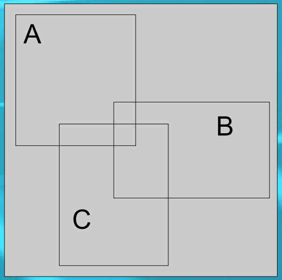
Locations | Queries

k-anonymity

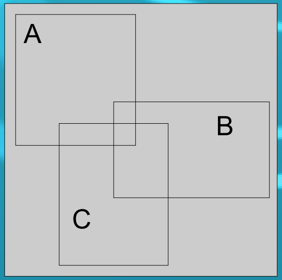


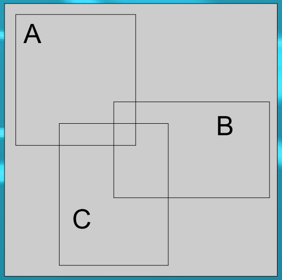
Public locations with private queries





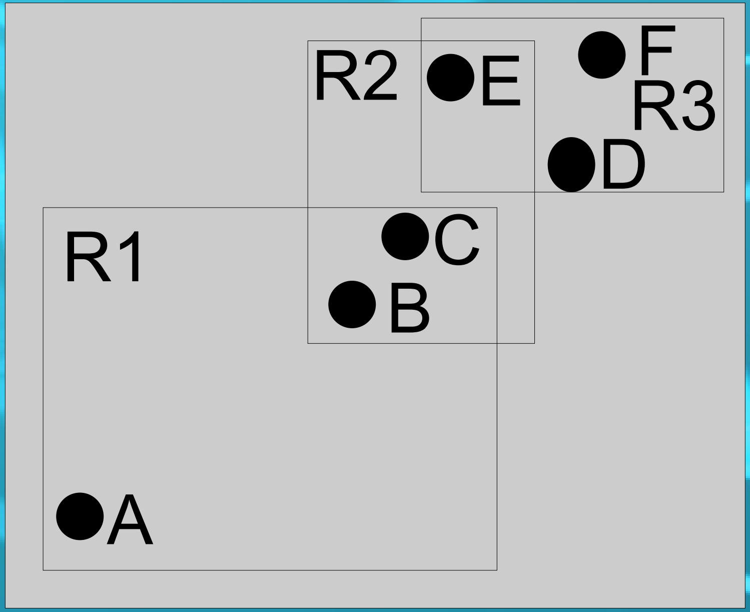
Private locations with private queries





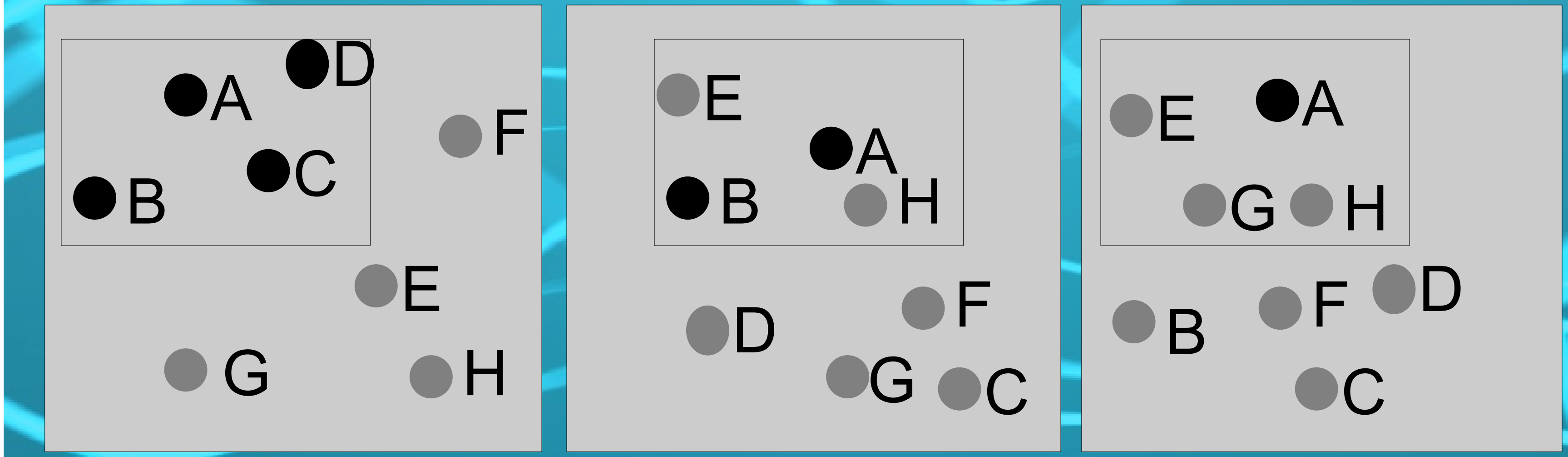
Privacy problems

- Query Sampling Attacks
  - With no distinguishing between location and query privacy, *k-anonymity* may reveal position on querying



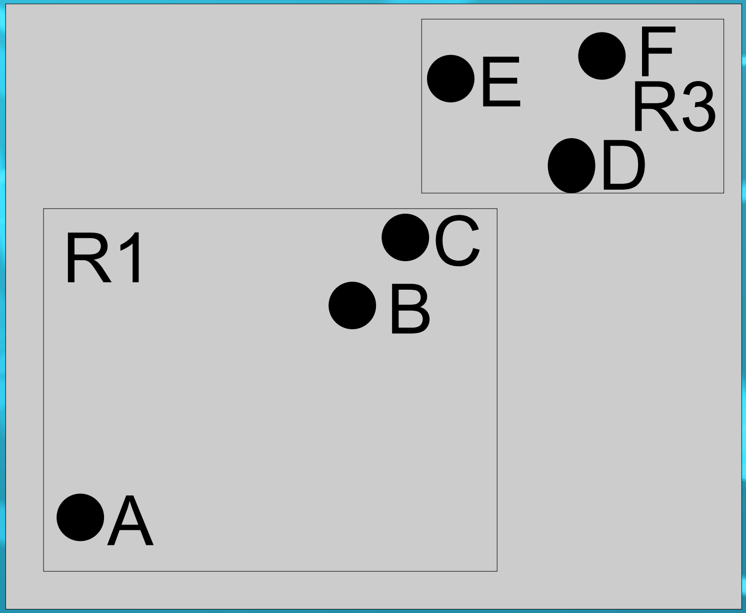
Privacy problems

- Query Tracking Attacks
  - With no distinguishing between location and query privacy, *k-anonymity* may reveal position on querying



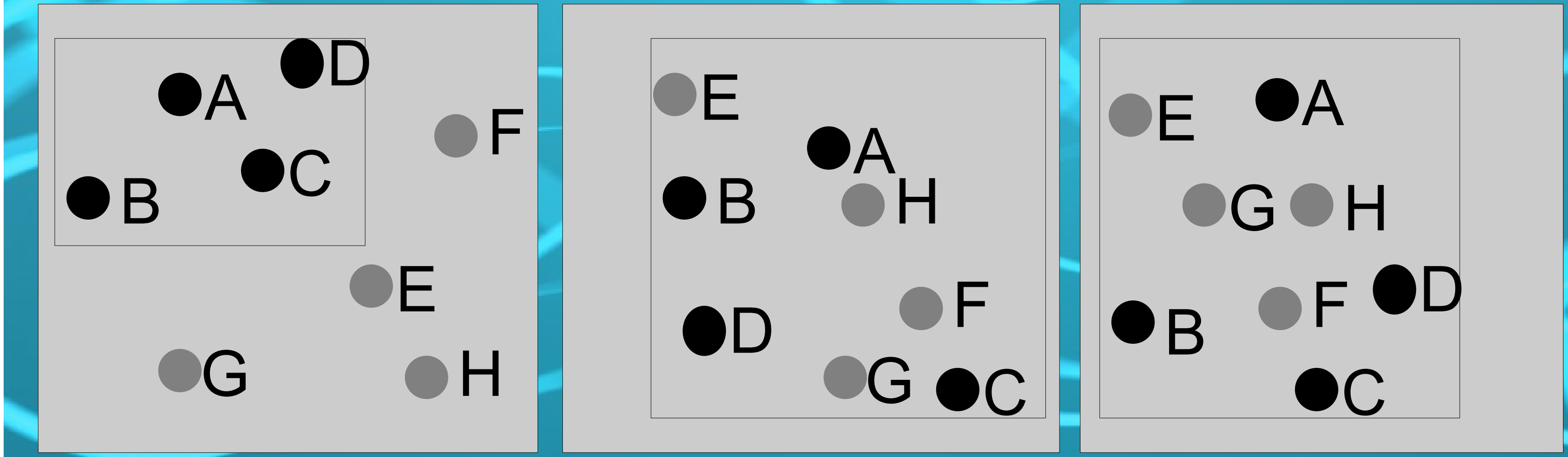
Privacy-preserving properties

- *k-sharing region*
  - A region is shared between the same users
  - Eliminates query sampling attack



Privacy-preserving properties

- *Memorization*
  - – With no memory of cloaking groups, several query snapshots may reveal position of a distinct user

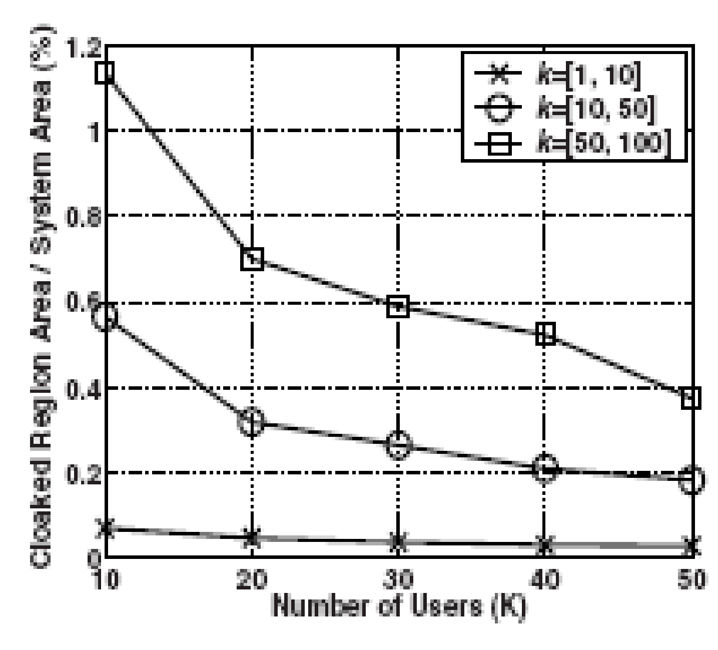


Robust spatial cloaking algorithm

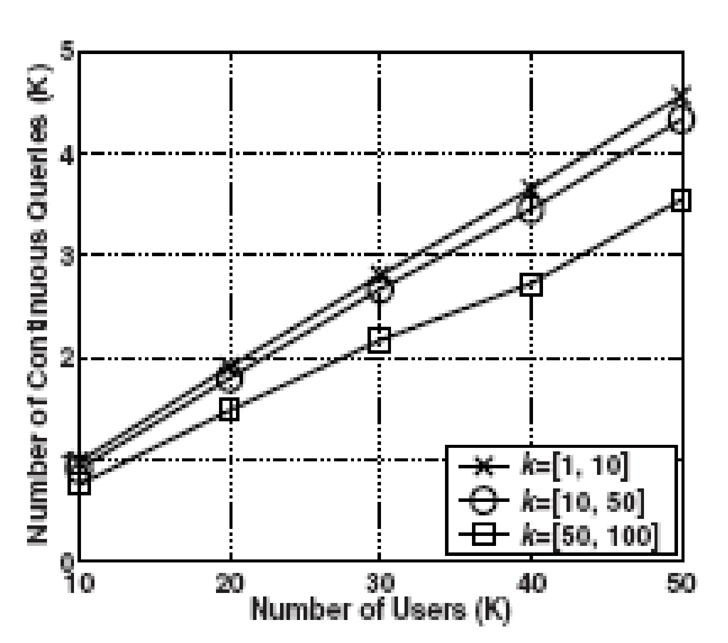
- Dynamic group concept
  - Group users together based on the users privacy requirements
  - Number of users are equal to or larger than *k-anonymity* requirements
  - All users in a group report the same cloaked spatial region as their cloaked query regions
  - If more than one user issues the same query, the query is only registered once with the database server

Results

- Scalability



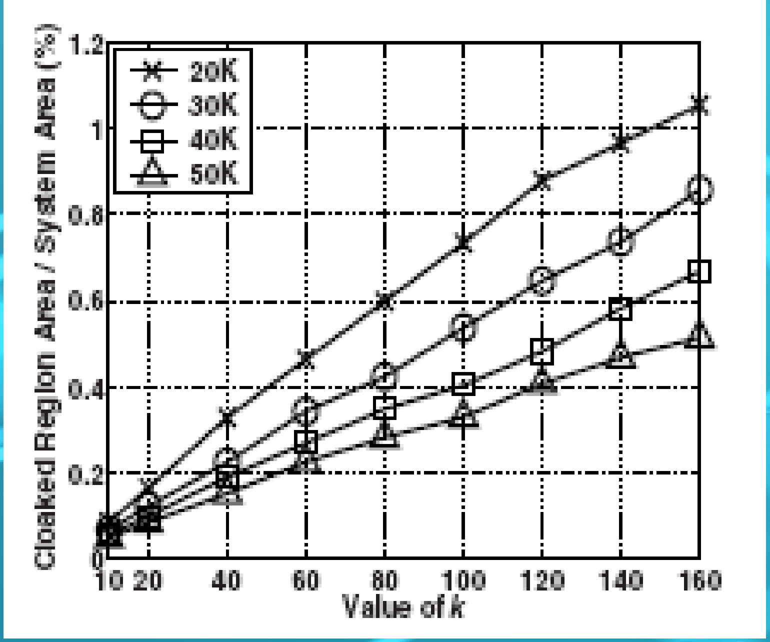
Cloaked region area



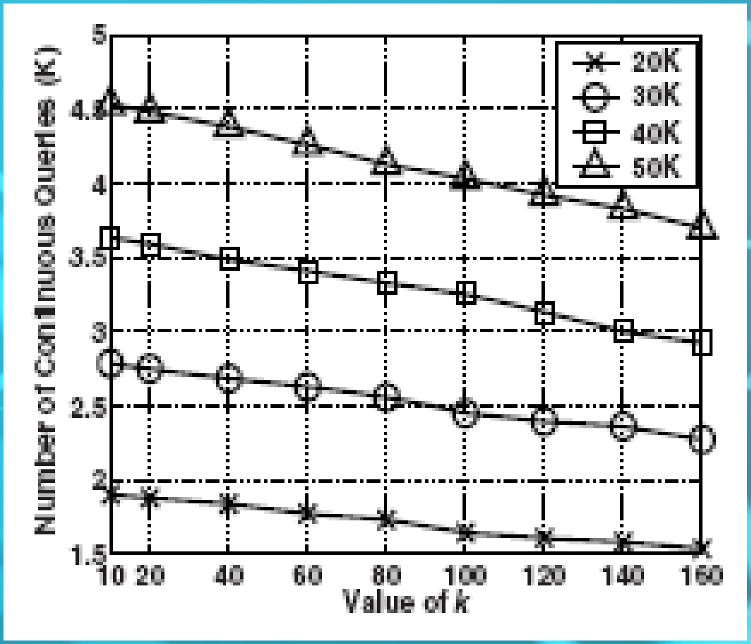
No. of Queries

Results

- Effect of query privacy requirements



Cloaked region area



No. of Queries

Conclusion

- Mobile users can protect their query privacy even if location is revealed
- Existing techniques would fail as they do not distinguish between location and query privacy
- Query sampling is eliminated by k-sharing region
- Query tracking is eliminated by memorization
- Presented robust spatial cloaking technique that distinguishes between location and query privacy, and does not suffer of the mentioned attacks
- Solution is scalable and efficient

Related work & contributions

- Dat5 project: Privacy in LBS
- Using groups and cloaked regions as well
- Contributed with a robust k-anonymity algorithm which takes query privacy into account

Evaluation of paper

- Solves some critical issues with *k-anonymity*
- Can leed in lower accuracy
- Does not solve the 'to few users' problem
- Tradeoff between performance and privacy
- Missing comparison to *k-anonymity*