The New Casper: Query Processing for Location Services without Compromising Privacy

Mohamed F. Mokbel, Chi-Yin Chow
University of Minnesota

Walid G. Aref
Purdue University

Major Privacy Threats in location-based services

“New technologies can pinpoint your location at any time and place. They promise safety and convenience but threaten privacy and security.”

Cover story, IEEE Spectrum, July 2003

Service-Privacy Trade-off

Example: Where is my nearest bus?

The Location Anonymizer

- The entire system area is divided into grids.
- The Location Anonymizer incrementally keeps track the number of users residing in each grid.
- Traverse the pyramid structure from the bottom level to the top level, until a cell satisfying the user privacy profile is found.

The Casper Architecture

Users Privacy Profile

- Each user has a privacy-profile that includes:
  - K: A user wants to be k-anonymous
  - A\_max: The minimum required area of the blurred area
- Multiple instances of the above parameters to indicate different privacy profiles at different times

The Privacy-Aware Query Processor

Data Types
- Public data: Gas stations, restaurants, police cars
- Private data: Personal data records

Query Types
- Private queries over public data: What is my nearest gas station
- Public queries over private data: How many cars in the downtown area
- Private queries over private data: Where is my nearest friend

- Step 1: Locate four filters (The NN target object for each vertex)
- Step 2: Find the middle points (The furthest point on the edge to the two filters)
- Step 3: Extend the query range
- Step 4: return candidate answers

Theorem 1: Given a cloaked area A for user u located anywhere within A, Casper returns a candidate list that includes the exact answer.

Theorem 2: Given a cloaked area A for a user u and a set of filter target object t, to t, Casper issues the minimum possible range query to get the candidate list.