TAPAS: Trustworthy Privacy-Aware Participatory Sensing

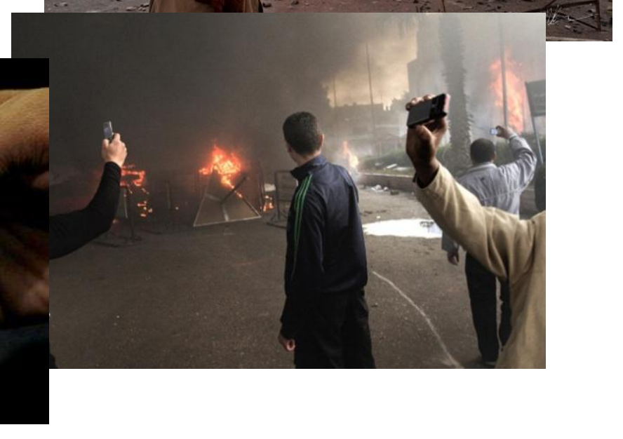
Leyla Kazemi and Cyrus Shahabi

Integrated Media Systems Center
University of Southern California

iCampus ✓iWatch CT

Introduction

- ❑ 5.3 billion mobile subscriptions by the end of 2010
  - ❑Technology advances on mobile phones
  - ❑ Network bandwidth improvements



❑ **Participatory Sensing (PS):** a new mechanism for efficient and scalable data collection

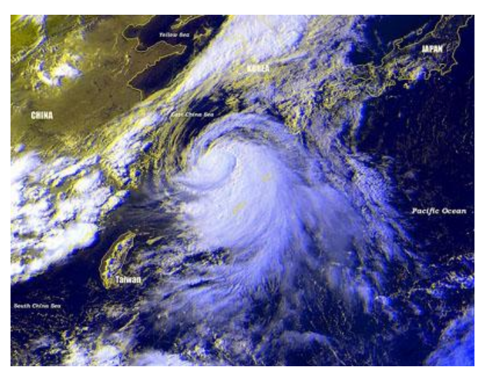
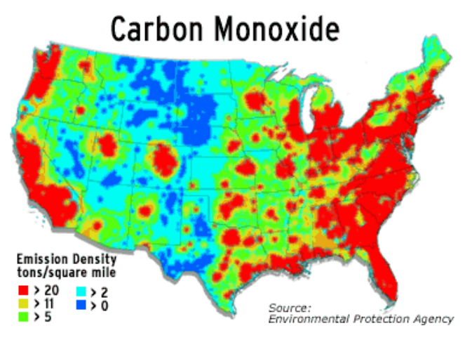
- ❑ **Privacy**: Participants may not want to associate themselves with the collected data
- ❑ **Trust:** Data contributed by participants cannot always be trusted

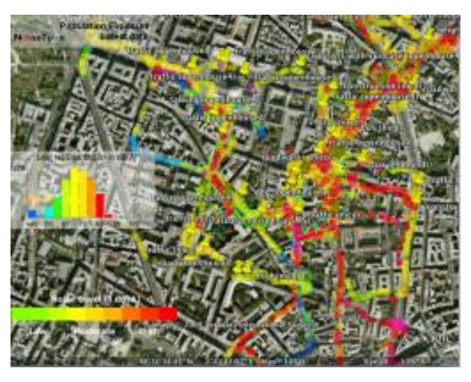
Related Work

- ❑ Privacy
  - ❑ Participatory sensing
    - ✓ Focuses on the data contribution rather than the coordination phase
    - ✓ Focuses on opportunistic data collection
    - ✓ Trust is not an issue
- ❑ Trust
  - ❑ Participatory sensing : Incorporating a trusted hardware/software (e.g., TPM) into the mobile device
    - ✓ Not designed for analog attack
  - ❑ Reputation Systems in P2P networks
    - ✓ Privacy is not usually an issue
    - ✓ Spatial dimension is not considered

Application/Project/Research

- ❑ Collect image and video, spontaneous news report
- ❑ Monitor traffic, health condition, moving patterns
- ❑ Weather, temperature, hurricane and fire watch
- ❑ Detecting chemical/hazardous materials, pollution



Problem Definition

Problem

- ❑ How to privately assign to the participants their closeby data collection points?
  - ✓ Protection from location-based attacks
  - ✓ Verification of the validity of the result

Challenges

- ❑ How to verify the validity of the data collected by anonymous user?

Idea

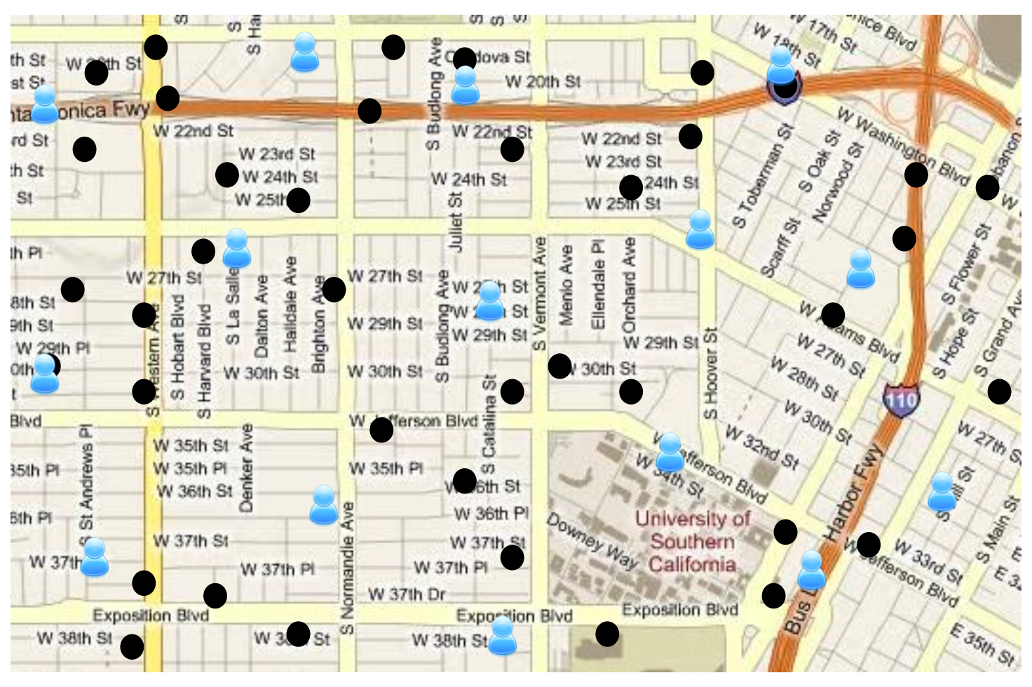
- ❑ Privacy: Following an existing approach
- ❑ Trust: Each point assigned to *k* closest users
  - ❑ Majority of users generate correct data

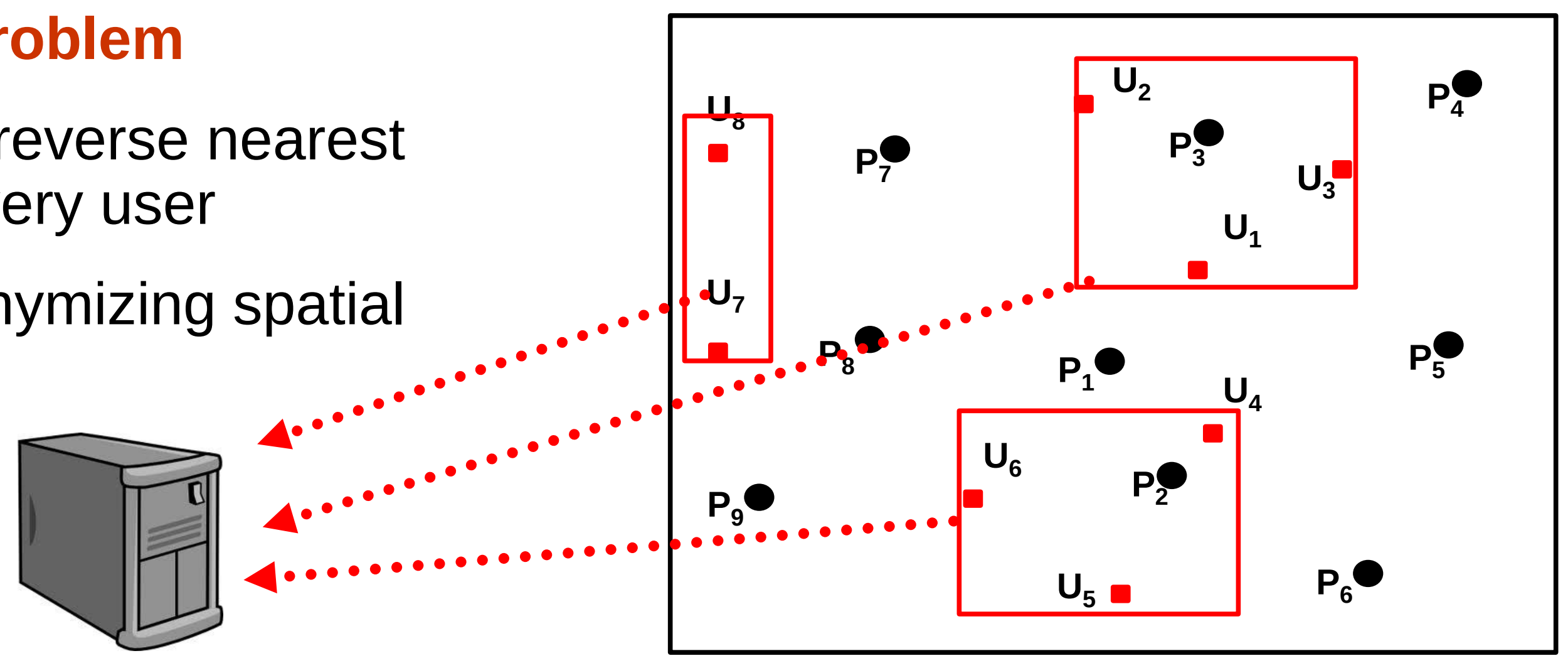
Formal Problem

- ❑ Finding the private k reverse nearest neighbor (PRkNN) of every user
  - ❑ Given a set of anonymizing spatial regions (ASR)

Possible attacks

- ❑ Malicious servers
  - ❑ Location-based attack
    - ✓ Identifying the query issuer by associating query to the query location
- ❑Malicious User
  - ❑ Intentionally collect wrong data

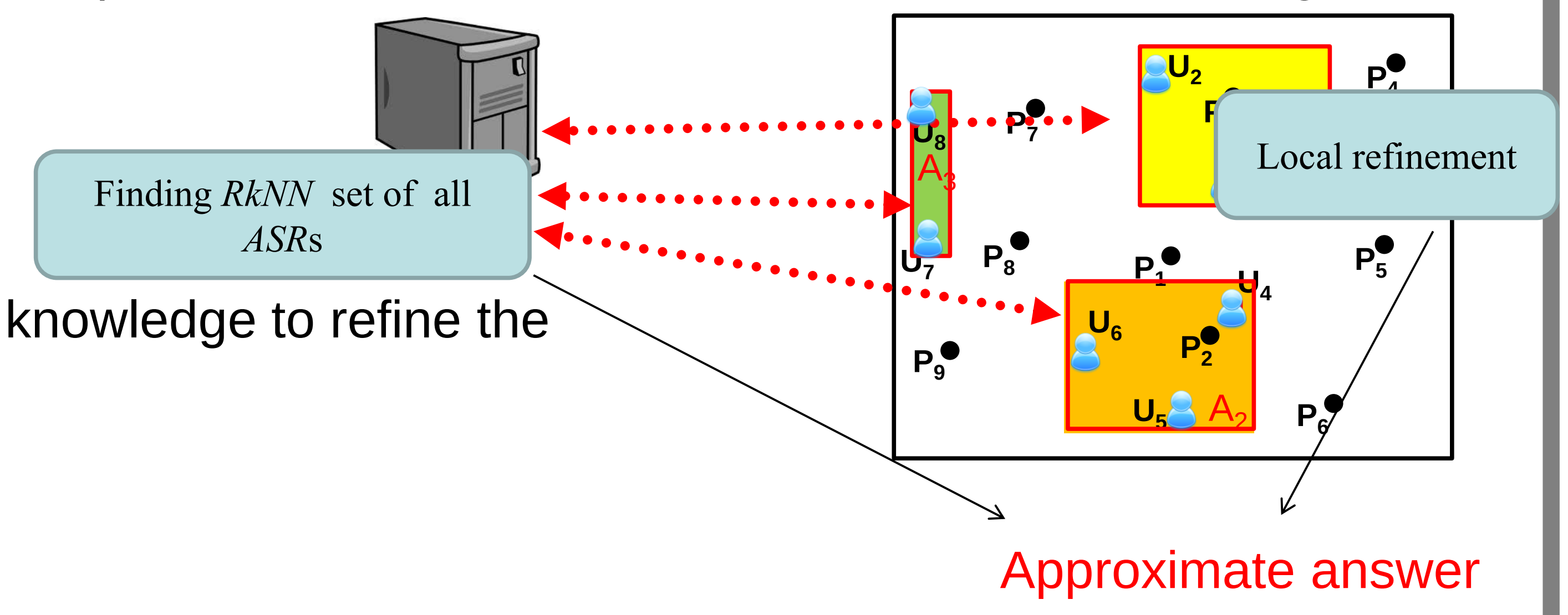




Approach/Experiments

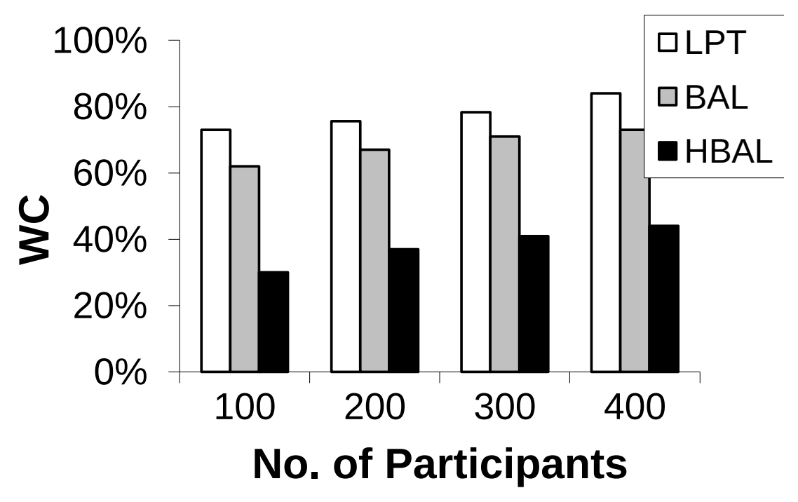
TAPAS Framework

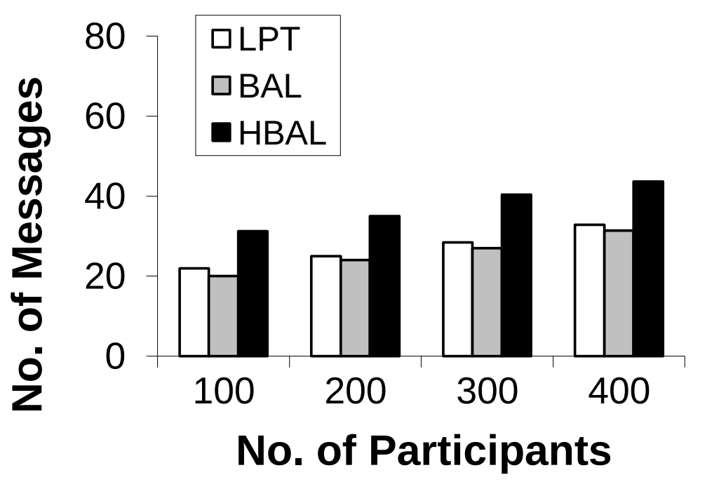
- ❑ Filter
  - ❑ Server-side
    - ✓ Limited Pruning Technique (LPT)
    - ✓ Bounded Anonymity Level (BAL)
    - ✓ Heurisic-based Bounded Anomity Level (HBAL)
  - ❑ Prune the set of points that cannot be in the *RkNN* of the users in a given *ASR*
- ❑ Refinement
  - ❑ User-side
  - ❑ Exploit local knowledge to refine the result

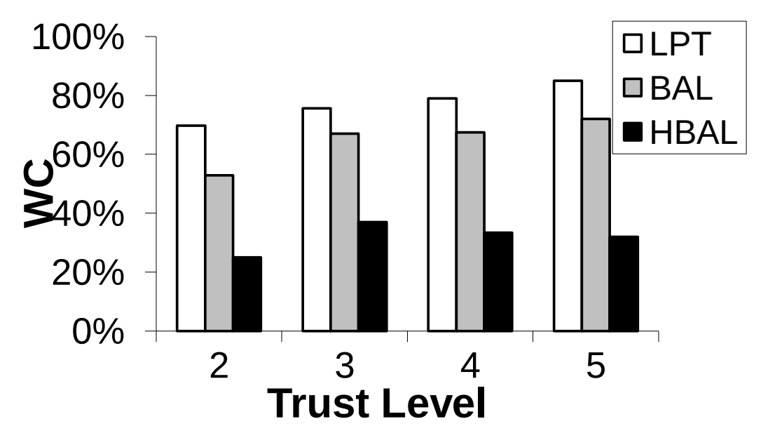


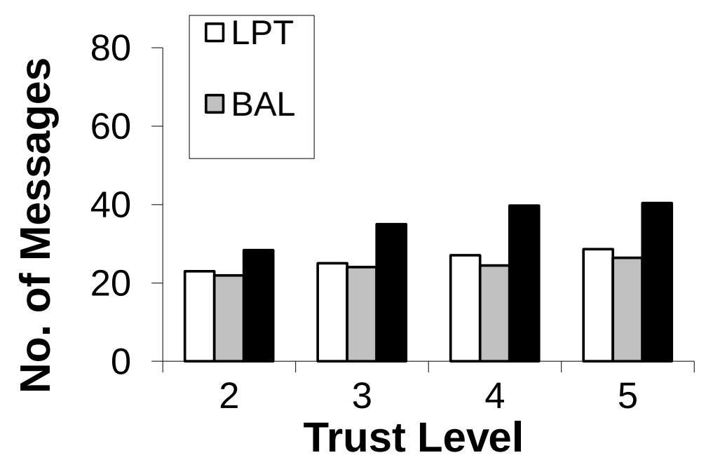
Experiments

- ❑ Methodology
  - ✓ Simulation-based experiments
  - ✓ Photo collection from 500 locations in LA area
  - ✓ Random generation of 400 users' locations
- ❑ Performance measure
  - ❑ Communication cost
  - ❑ Wasteful collection
- ❑ Evaluated approaches
  - ❑ LPT
  - ❑ BAL
  - ❑ HBAL









Conclusion and Future Work

Conclusion

- ❑ Formalized the interplay of privacy and trust in participatory sensing as a private reverse *k* nearest neighbor (*PRkNN*) problem
- ❑ Proposed *TAPAS*, a trustworthy privacy-aware framework that included three various solutions to the *PRkNN* problem

Future work

- ❑ Extend the proposed approaches to more cost-efficient and energy-efficient solutions
- ❑ Incorporating the reputation of the users in to our trust model

USC Viterbi School of Engineering

NSF

IMSC Integrated Media Systems Center