Privacy and Trust in Participatory Sensing

Leyla Kazemi, Ling Hu and Cyrus Shahabi
Integrated Media Systems Center
University of Southern California

Introduction
- 3-4 billion mobile users in the past ten years
  - Technology advances on mobile phones
  - Network bandwidth improvements
- Participatory Sensing: a new mechanism for efficient and scalable data collection
  - Privacy: Participants may not want to associate themselves with the collected data
    - Data Collection
    - Data Contribution
  - Trust: Contributed data is not always trusted

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

Privacy data collection
- How to privately assign to the participants their close data collection points?
  
  Baseline Approach
  - Distributed Voronoi cell computation
  - Private range query

  PIRI Approach
  - Query Formation
    - Avoids range-dependency leak
    - Adjustment technique
  - Query Selection
    - Avoids all-inclusivity leak
    - Distributed voting mechanism
    - A group of participants ask queries
    - Sharing the result with the rest

Possible attacks
- Malicious servers
- Location-based attack
- Associating query to the query location

Challenges
- Range-dependency leak
- All-inclusivity leak

Private data contribution
- How to contribute information privately?
  - Location protection
  - Content ownership protection

Possible attacks
- Malicious servers
- Compromised peer mobile users
- Misuse information
- Drop message

Solution
- Data owner sends collected data (e.g. an image) to a random chosen friend
- A node sends data to one of its direct connected nodes
- Collected data hops on the network a few times (determined by a few parameters) before reaching to the server

Discussion
- Transmission overhead
- Scale free network: six degree of separation
- The originator of the data can be anyone on the network
- Communication overhead appears to be small

Experiments

Privacy data collection
- Defined a new metric for quantifying the privacy leak in participatory sensing
- Experiments on snapshot locations of 500 mobile users in USC campus
- Performance measure
  - Communication cost
- Privacy leak

Privacy data collection
- # of hops v.s. threshold
- Image loss v.s. malicious user attacks

Conclusion and Future Work

Conclusion
- Introduced a privacy-aware framework in participatory sensing
  - Data collection
  - Data contribution

Future work
- How to verify the validity of the collected data?
  - Challenge
  - Verifying data published by anonymous participants

For more information, visit http://infostlab.usc.edu/publications.php#conference

USC IMSC
Integrated Media Systems Center