Overcoming the Challenges in Mobile Crowd Sensing

Nishad Aluthge
Department of Computer Science
University of Helsinki

Mobile Data Analytics seminar, 2016 Spring
Outline

• Introduction to Mobile Crowd Sensing (MCS)
• Mobile Crowd sensing Process
• Challenges in Mobile Crowd Sensing
• Solutions for the Challenges
• Conclusion
• References
Sensing with Mobile devices

• Large population: 1.86 billion smartphone users.
• Sensors embedded in mobile phones:
  – GPS, accelerometer, gyroscope, ambient light, proximity, microphone, and camera sensors
• Mobile sensing devices are pervasively available and are a rich and inexpensive source of sensor data
Mobile Crowd Sensing

Mobile crowd sensing (MCS) refers to applications that leverage consumer mobile devices (GPS, smart phones, and car sensors) to collect and share data about the user or the physical world, either interactively or autonomously, towards a common goal.
Mobile Crowd Sensing
[Cont’d]

Participatory Sensing

- Users actively engage in the data collection activity.
- Users manually determine how, when, what, where to sample.

Opportunistic Sensing

- Takes random sample which is application defined.
- Easy to gather large amount data in small time.

Filtering Data by Handling Privacy Issues & Localization.

Dataset is ready for research/ take actions.
Mobile Crowd Sensing Process
Challenges in MCS

• Privacy Threats
  Arises due to sharing of personal information/habits
  – Active privacy breach
    • Narrow tasking: Isolating the participants with conditions
    • Selective tasking: Selective task assignment
    • Local eavesdropping: Intercepting wireless communication
  – Non-active privacy breach
    • Task tracing attacks: By linking tasks
    • Location-based inference attacks: Frequent spatial tasks
Challenges in MCS [Cont’d]

• Data reliability issues
  – False data by users
  – Critical for the results

• Heterogeneity of mobile platforms
  – Different mobile platforms (Android, IOS etc.)
  – Need for separate application development

• Need for separate application installation
  – Multiple applications need to be installed
  – Reduces performance
Challenges in MCS [Cont’d]

- High network bandwidth utilization
  - Core network gets congested
  - Ex: Video sharing

- Resource limitations on mobile environment
  - Limited computation, signal processing power
  - Higher power usage
Solutions for MCS challenges

• Actions against privacy threats
  – Processing data locally (Soundsense [1])
  – Anonymity
    • Pseudonyms
      Uses set of aliases + authentication in communication
    • Connection anonymization
      The onion routing [2]
      Mix master [3]
Solutions for MCS challenges

• Actions against privacy threats
  – Policy based privacy preferences
    • Limited/ selective participation [6]
    • Cost (incentive) based task assignment [7]
Solutions for MCS challenges

- Improving Location Reliability (ILR) [8]
  - Validates data with minimum effort
  - GPS and Bluetooth scans
  - Photo tasks & sensing tasks
  - Photo selection phase
    - Graph generation
    - A set of photo tasks will be selected (node degree > x)
    - Validate photo tasks
  - Transitive trust phase:
    - Extends trust to collocated data points
Solutions for MCS challenges

- VM based crowd sensing architecture
Solutions for MCS challenges

- VM based crowd sensing architecture [9]
  - A single application in mobile side
  - Processing in cloudlets
  - MAVM aggregates data for optimization
  - A single copy of data is available for multiple MCS applications
  - Solves heterogeneity of platforms, need to install separate applications, overcoming the resource limitations in mobile devices
  - Proxy VMs reduces network bandwidth and network latency
Conclusion

• Mobile crowd sensing is a better way to gather data
• Privacy Threats, Data reliability issues, Heterogeneity of mobile platforms, Need for separate application installation, High network bandwidth utilization, Resource limitations on mobile environment
• Anonymity, Policy based task assignment, VM based MCS architecture, Improving Location reliability
• The solutions depends on the MCS application.
References


Any Questions ?
Thank you !!!
Evaluation - ILR

- Total photo tasks were 1784 and 204 with Bluetooth scans.
- All the photo tasks with Bluetooth scans were considered to be manually validated.
- 45 photos were detected to be fake.
- Among them 16 photo tasks were having Bluetooth scans with false location claims which were provided by 10 malicious users.
- These 16 photo tasks were fed in to ILR to check ILR performance.
In order to detect 40% of malicious users ILR only required validating 11% of total photos (204 out of 1784)

**TABLE I**

<table>
<thead>
<tr>
<th></th>
<th>Number of photo tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total photos</td>
<td>1784</td>
</tr>
<tr>
<td>No. of photos with Bluetooth scans (manually validated in ILR)</td>
<td>204</td>
</tr>
<tr>
<td>Trusted data points added by ILR</td>
<td>148</td>
</tr>
</tbody>
</table>

**TABLE II**

<table>
<thead>
<tr>
<th></th>
<th>Detected by ILR scheme</th>
<th>Total</th>
<th>Percentage detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks with false location claim</td>
<td>4</td>
<td>16</td>
<td>25%</td>
</tr>
<tr>
<td>Cheating people</td>
<td>4</td>
<td>10</td>
<td>40%</td>
</tr>
</tbody>
</table>