Challenge: Privacy

Tarek Abdelzaher
University of Illinois at Urbana Champaign

Trusted Aggregator?

- Yes:
  - Trust the aggregation node with not violating privacy (most of today’s applications, such as gmail, dropbox, Facebook, etc)
  - How to support new and unknown applications?
- Model: Honest but curious
  - Application is trusted to perform aggregation correctly but not trusted with private data
Enabling Community Sensing

- The privacy dilemma:
  - Individuals do not want to share private data (e.g., GPS trajectories)
  - Useful applications can be built if enough data is shared (e.g., real-time traffic maps)

- Two types of solutions:
  - Anonymity: reveal data, hide owner
  - Data perturbation: reveal owner, hide data
Anonymity

- Share data (e.g., GPS trajectory), but not user ID
- Problems?

Perturbation

- Example: Compute the average family income of people in this class
  - Each person adds a random number in the range +/- $1,000,000 to their family income and shares the result
  - Aggregator averages the results. Given enough people, the added “noise” cancels out
Perturbation and Repeated Experiments

- What if we perform the previous process every day?
  - Aggregator can average the responses from the same person over time to remove the noise and find out family income
- Solution?
Perturbation and Time Series Data

- User shares a slow-changing variable such as weight every day
  - How to prevent aggregator from averaging same user answers to find weight?

- How to prevent aggregator from funding out weight trend?
An Example

- Dieters want to share weight information to find efficacy of the given diet, without revealing their true weight, average, trend (loss or gain of weight), etc...

Perturb data? Add Noise?

- Weight curve perturbed by adding independent random noise
- Estimation using PCA to breach privacy of user
Add Noise and Random Offset?

Weight curve perturbed by adding independent random noise and a random offset

Estimation using PCA to estimate the data of the user

Challenge

- Develop perturbation that preserves privacy of individuals
  - Cannot infer individuals’ data without large error
  - Reconstruction of community distribution can be achieved within proven accuracy bounds
  - Perturbation can be applied by non-expert users
Intuitive Approach

- Client adds noise time-series with co-variance that largely mimics covariance of actual data (overlap in frequency domain)

Add virtual user curve to real curve

Can’t reconstruct
Intuitive Approach

- Client adds noise time-series with co-variance that largely mimics covariance of actual data (overlap in frequency domain)
- Users send their perturbed data to aggregation server

![Diagram](image1)

Intuitive Approach

- Client adds noise time-series with co-variance that largely mimics covariance of actual data (overlap in frequency domain)
- Users send their perturbed data to aggregation server
- Given perturbed community distribution and noise, server uses deconvolution to reconstruct original data distribution at any point in time

![Diagram](image2)
Perturbing Speed of Traffic

![Graph showing perturbed speeds compared to original and reconstruction using PCA.]

Reconstruction of Average Speed

![Graph showing real community average and reconstructed community average speeds.]

10/26/2015
Reconstruction of Community Speed Distribution

Real community distribution of speed  
Reconstructed community distribution of speed

Perturbing Speed and Location

- Clients lie about both location and speed
Reconstruction Accuracy

- Real versus reconstructed speed

![Real community distribution of speed](image1)

![Reconstructed community distribution of speed](image2)

More on Reconstruction Accuracy

- Real versus reconstructed speed on Washington St., Champaign

![Real community distribution of speed](image3)

![Reconstructed community distribution of speed](image4)
How Many are Speeding?

- Real versus estimated percentage of speeding vehicles on different streets (from data of users who “lie” about both speed and location)

<table>
<thead>
<tr>
<th>Street</th>
<th>Real % Speeding</th>
<th>Estimated % Speeding</th>
</tr>
</thead>
<tbody>
<tr>
<td>University Ave</td>
<td>15.6%</td>
<td>17.8%</td>
</tr>
<tr>
<td>Neil Street</td>
<td>21.4%</td>
<td>23.7%</td>
</tr>
<tr>
<td>Washington Street</td>
<td>0.5%</td>
<td>0.15%</td>
</tr>
<tr>
<td>Elm Street</td>
<td>6.9%</td>
<td>8.6%</td>
</tr>
</tbody>
</table>

Privacy and Optimal Perturbation

- Is there an optimal perturbation scheme?
- What is the measure the privacy?
- How can we generate the optimal perturbation?
Privacy Measure

- We use the mutual information $I(X; Y)$ to measure the information about $X$ contained in $Y$.
- Minimal information leak under noise power constraint

$$P_X^* = \min_{Z} I(X, X + Z),$$
subject to $P_Z \leq P_0$

- $X$ is the original data
- $Y$ is the perturbed data
- $Z$ is the noise
- $P_Z$ is the power of $Z$

Upper Bound on Privacy

- Lemma (Ihara, 78)
- The noise that minimizes the upper bound on information leak is a Gaussian noise

$$I(X; Y) \leq I(X_G, X_G + Z_G) = \frac{1}{2} \frac{\det(K_X + K_Z)}{\det(K_Z)}$$
Finding the Optimal Noise

- Solving for the optimal noise’s covariance matrix

\[
K_Z^* = \arg \min_{K_Z} \frac{1}{2n} \log \frac{\det(K_X + K_Z)}{\det(K_Z)}
\]

subject to

\[
\frac{1}{n} \text{trace}(K_Z) \leq P_0
\]

\[
K_Z > 0
\]

\[
K_Z \text{ is Symmetric Toeplitz}
\]

Optimal Noise

- The noise generation method can be seen as the optimal allocation of noise energy in the frequency domain
Recollection Error vs. Privacy Trade-off

- A third party (or modeling server) may attempt to reconstruct participant data traces.
- **Reconstruction Error**: The difference between the reconstructed data and the original data.
- **Modeling Error**: The accuracy or constructed community-wide model.
Privacy and Model Construction

- **Goals:**
  - **Minimize the modeling error:**
    - The same modeling accuracy as not employing any data alterations.
  - **Maximize the reconstruction (breach) error:**
    - The higher reconstruction error means more privacy assurance.
- **A perfect privacy-enabling data sharing scheme:**
  - **Perfect modeling:**
    - Shared data produce exactly the same model as the original private data.
  - **Perfect neutrality:**
    - Reconstruction of private user data from shared data yields the same error as if no additional information was available.

Pre-aggregation

- **Linear Regression Modeling Goal:** Find coefficients for
  - $\hat{Y} = W\eta$
  - $w_{ij} = g_j(x_{i1}, ..., x_{id}), 1 \leq j \leq k$

- **Correlation matrices contain enough information for modeling while hiding the data trace values**
  - $\rho_u = Y_u^T Y_u$
  - $\nu_u = W_u^T Y_u$
  - $\Theta_u = W_u^T W_u$
Regression Modeling

- Compute aggregate matrix values by adding all feature matrices from all users
  - $\rho = Y^T Y = \sum_{i=1}^{n} \rho u_i$
  - $v = W^T Y = \sum_{i=1}^{n} v u_i$
  - $\Theta = W^T W = \sum_{i=1}^{n} \Theta u_i$

- Compute regression coefficients and error exactly as if the private data were accessible:
  - $\eta = (W^T W)^{-1} W^T Y = \Theta^{-1} v$
  - Error $= (Y - W\eta)^T (Y - W\eta) = \eta^T v - v^T \eta + \eta^T \Theta \eta$

Privacy-aware Properties

- Empirical results for reconstructing random data tuples from shared features.

Correlation among attributes

![Graph showing correlation among attributes](image)

Correlation among tuples

![Graph showing correlation among tuples](image)
Comparing with Perturbation

- Perturbation noise increases the reconstruction error and prediction error at the same time.

![Graph showing prediction error vs. noise energy](image)

Case Study: Prediction Error

- The modeling error introduced by perturbation in the GreenGPS service.

<table>
<thead>
<tr>
<th>Car Make</th>
<th>Car Model</th>
<th>Car Year</th>
<th>Our Approach % Error</th>
<th>Perturbation % Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Honda</td>
<td>Accord</td>
<td>2003</td>
<td>0.46</td>
<td>7.86</td>
</tr>
<tr>
<td>Ford</td>
<td>Contour</td>
<td>1999</td>
<td>0.58</td>
<td>2.12</td>
</tr>
<tr>
<td>Toyota</td>
<td>Corolla</td>
<td>2009</td>
<td>0.36</td>
<td>6.52</td>
</tr>
<tr>
<td>Ford</td>
<td>Focus</td>
<td>2009</td>
<td>0.11</td>
<td>2.25</td>
</tr>
<tr>
<td>Hyundai</td>
<td>Santa Fe</td>
<td>2008</td>
<td>0.39</td>
<td>2.43</td>
</tr>
<tr>
<td>Ford</td>
<td>Taurus</td>
<td>2001</td>
<td>0.18</td>
<td>1.75</td>
</tr>
</tbody>
</table>