Towards Plausible Graph Anonymization

Yang Zhang, Mathias Humbert, Bartlomiej Surma, Praveen Manoharan, Jilles Vreeken, Michael Backes
Graph sharing

**Netflix Prize data**
Dataset from Netflix's competition to improve their recommendation algorithm
Netflix • updated 3 months ago (Version 2)

**Twitch Social Networks**
Andrea Garritano • updated 3 months ago (Version 1)

**IJCNN Social Network Challenge**
This competition requires participants to predict edges in an online social network. The winner will receive free registration and the opportunity to present their solution at IJCNN 2011.

$950 • 117 teams • 9 years ago
Graph anonymization
Graph anonymization
Graph anonymization

id 1

id 2

id 3

id 4

id 5

id 6

id 7

id 8
Graph anonymization
Graph anonymization
Our work

- Find a fundamental flaw in graph anonymization designs
Our work

- Find a fundamental flaw in graph anonymization designs
- Exploit it to recover original graph
Our work

- Find a fundamental flaw in graph anonymization designs
- Exploit it to recover original graph
- Use our findings to enhance anonymization designs
Our work

- Find a fundamental flaw in graph anonymization designs
- Exploit it to recover original graph
- Use our findings to enhance anonymization designs
- Evaluate privacy and usability of enhanced techniques on 3 real life datasets:
  - Enron, NO, Snap
Graph anonymization methods

- ’08 Liu et al. - k-anonymity (k-DA)
- ’08 Zhou et al. - k-anonymity (k-NA)
- ’10 Cheng et al. - k-anonymity (k-iso)
- ’11 Sala et al. - differential privacy
- ’12 Mittal et al. - random walk privacy
- ’14 Xiao et al. - differential privacy
k-DA algorithm
k-DA algorithm
k-DA algorithm
k-DA algorithm

### Node Degree Distribution

<table>
<thead>
<tr>
<th>Node Degree</th>
<th># Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

2-DA

### Node Degree Distribution

<table>
<thead>
<tr>
<th>Node Degree</th>
<th># Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

2-DA
SalaDP algorithm

dK-2 series

ε-DP

perturbed dK-2 series
Social network graph properties
Social network graph properties
Social network graph properties
Social network graph properties
Graph recovery attack - overview

A: [1.2, 5.7, -3.2, 0.9]
B: [0.8, -3.4, 5.2, 1.3]
C: [0.9, -1.2, 0.2, 4.3]
D: [-3.2, 0.4, 0.7, 1.1]
E: [7.7, 2.4, -0.2, 0.3]
F: [3.8, -9.3, 0.3, 3.2]
Graph recovery attack - graph embedding

- Node embeddings with node2vec ’16 Grover and Leskovec
- Mapping users into continuous vector space
- User’s vector reflects structural properties
Graph recovery attack - graph embedding

Plausibility is cosine similarity between embeddings

![Graph representation](image)

- A [1.2, 5.7, -3.2, 0.9]
- B [0.8, -3.4, 5.2, 1.3]
- C [0.9, -1.2, 0.2, 4.3]
- D [-3.2, 0.4, 0.7, 1.1]
- E [7.7, 2.4, -0.2, 0.3]
- F [3.8, -9.3, 0.3, 3.2]

- \( s_A(A, B) \)
- \( s_A(A, C) \)
- \( s_A(A, D) \)
- \( s_A(A, F) \)
- \( s_A(B, E) \)
- \( s_A(C, E) \)
- \( s_A(C, F) \)
- \( s_A(D, E) \)
- \( s_A(D, F) \)
Graph recovery attack - graph embedding

Plausibility is cosine similarity between embeddings
Graph recovery attack - graph embedding

Find a cutoff point and remove non-plausible edges

<table>
<thead>
<tr>
<th></th>
<th>Enron</th>
<th>NO</th>
<th>SNAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k$-DA ($k = 50$)</td>
<td>0.792</td>
<td>0.642</td>
<td>0.857</td>
</tr>
<tr>
<td>$k$-DA ($k = 75$)</td>
<td>0.796</td>
<td>0.710</td>
<td>0.869</td>
</tr>
<tr>
<td>$k$-DA ($k = 100$)</td>
<td>0.812</td>
<td>0.761</td>
<td>0.881</td>
</tr>
<tr>
<td>SalaDP ($\epsilon = 100$)</td>
<td>0.672</td>
<td>0.712</td>
<td>0.853</td>
</tr>
<tr>
<td>SalaDP ($\epsilon = 50$)</td>
<td>0.750</td>
<td>0.723</td>
<td>0.835</td>
</tr>
<tr>
<td>SalaDP ($\epsilon = 10$)</td>
<td>0.819</td>
<td>0.876</td>
<td>0.802</td>
</tr>
</tbody>
</table>

F1 score
Enhancing anonymization

- get fake edges with highest plausibility?
  - the distribution will look unnatural
Enhancing anonymization

- get fake edges with highest plausibility?
  - the distribution will look unnatural
- draw fake edges from same plausibility distribution?
Enhancing anonymization

- get fake edges with highest plausibility?
  - the distribution will look unnatural
- draw fake edges from same plausibility distribution?

![k-DA (k=100)](image1.png)

![Enhanced k-DA (k=100)](image2.png)
Resilience to graph recovery attack

- F1 score for original anonymizations

<table>
<thead>
<tr>
<th></th>
<th>Enron</th>
<th>NO</th>
<th>SNAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k$-DA ($k = 50$)</td>
<td>0.792</td>
<td>0.642</td>
<td>0.857</td>
</tr>
<tr>
<td>$k$-DA ($k = 75$)</td>
<td>0.796</td>
<td>0.710</td>
<td>0.869</td>
</tr>
<tr>
<td>$k$-DA ($k = 100$)</td>
<td>0.812</td>
<td>0.761</td>
<td>0.881</td>
</tr>
<tr>
<td>SalaDP ($\epsilon = 100$)</td>
<td>0.672</td>
<td>0.712</td>
<td>0.853</td>
</tr>
<tr>
<td>SalaDP ($\epsilon = 50$)</td>
<td>0.750</td>
<td>0.723</td>
<td>0.835</td>
</tr>
<tr>
<td>SalaDP ($\epsilon = 10$)</td>
<td>0.819</td>
<td>0.876</td>
<td>0.802</td>
</tr>
</tbody>
</table>

- F1 score for enhanced anonymizations

<table>
<thead>
<tr>
<th></th>
<th>Enron</th>
<th>NO</th>
<th>SNAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k$-DA ($k = 50$)</td>
<td>0.531</td>
<td>0.391</td>
<td>0.632</td>
</tr>
<tr>
<td>$k$-DA ($k = 75$)</td>
<td>0.428</td>
<td>0.433</td>
<td>0.609</td>
</tr>
<tr>
<td>$k$-DA ($k = 100$)</td>
<td>0.510</td>
<td>0.501</td>
<td>0.597</td>
</tr>
<tr>
<td>SalaDP ($\epsilon = 100$)</td>
<td>0.422</td>
<td>0.370</td>
<td>0.515</td>
</tr>
<tr>
<td>SalaDP ($\epsilon = 50$)</td>
<td>0.390</td>
<td>0.411</td>
<td>0.522</td>
</tr>
<tr>
<td>SalaDP ($\epsilon = 10$)</td>
<td>0.439</td>
<td>0.527</td>
<td>0.490</td>
</tr>
</tbody>
</table>

- $k$-DA drops by: 26~51%
- SalaDP drops by: 37~48%
Utility of Enhanced anonymization

- Eigencentrality (Enron)
- Eigencentrality (NO)
- Eigencentrality (SNAP)
- Degree distribution (Enron)
- Degree distribution (NO)
- Degree distribution (SNAP)
- Triangle count (Enron)
- Triangle count (NO)
- Triangle count (SNAP)
Resilience to deanonymization attack

Anonymity gain (%)

- $k$-DA ($k = 50$)
- $k$-DA ($k = 75$)
- $k$-DA ($k = 100$)
- SalaDP ($\epsilon = 100$)
- SalaDP ($\epsilon = 50$)
- SalaDP ($\epsilon = 10$)
Conclusion

We find flaws in current graph anonymizations
Conclusion

We find flaws in current graph anonymizations

We recover the original, pre-anonymized graph
Conclusion

We find flaws in current graph anonymizations

We enhance the anonymization techniques

We recover the original, pre-anonymized graph
Conclusion

We find flaws in current graph anonymizations

We enhance the anonymization techniques

We recover the original, pre-anonymized graph

We evaluate privacy and utility of enhanced anonymization