Network Privacy

Networks out of Control

Matthias Grossglauser
AOL search log release (2006)

4417749 care packages 2006-03-02 09:19:32
4417749 movies for dogs 2006-03-02 09:24:14
4417749 blue book 2006-03-03 11:48:52
4417749 best dog for older owner 2006-03-06 11:48:24
4417749 best dog for older owner 2006-03-06 11:48:24
4417749 rescue of older dogs 2006-03-06 11:55:25
4417749 school supplies for the iraq children 2006-03-06 13:36:33
4417749 school supplies for the iraq children 2006-03-06 13:36:33
4417749 pine straw lilburn delivery 2006-03-06 18:35:02
4417749 pine straw delivery in gwinnett county 2006-03-06 18:36:35
4417749 landscapers in lilburn ga. 2006-03-06 18:37:26
4417749 pine straw in lilburn ga. 2006-03-06 18:38:19
4417749 pine straw in lilburn ga. 2006-03-06 18:38:27
4417749 gwinnett county yellow pages 2006-03-06 18:42:08

...
User 4417749 uncovered by New York Times

- **Searches:**
  - “landscapers in Lilburn, Ga”
  - “homes sold in shadow lake subdivision gwinnett county georgia”
  - “jarrett t. arnold”, “jack t. arnold”

- **4417749=Thelma Arnold**
  - 62 years old widow and dog owner
  - home: Lilburn, GA

- **AOL press release:**
  - “There was no personally identifiable data provided by AOL with those records, but search queries themselves can sometimes include such information.”

- **Heads had to roll...**
  - AOL CTO Maureen Govern (+2 others) fired
Privacy: hard to define

- Personally identifiable information (PII):
  - “information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual” (wikipedia)
Privacy of Networks

- **Adversary has:**
  - Anonymized network: unlabeled graph
  - Side information: subgraph; statistics on certain nodes; noisy version of whole network; ...

![Diagram of matching nodes by structure only]
**Taxonomy of network privacy attacks**

**Active:** attacker can create nodes/links

**Passive:** attacker can only observe

**Targeted:** de-anonymize a small subgraph

**Global:** de-anonymize the whole network

**Internal:** attacker(s) part of network

**External:** attacker not in network

**Scope of attack**
- targeted, internal
- global, external

**Access of adversary**
- active
- passive

**References**
- [Backstrom, Dwork, Kleinberg]
- [Hay, Miklau, Jensen, Towsley, Li]
- [Narayanan, Shmatikov]
- [Pedarsani, MG]
Automorphism: Asymmetric vs Symmetric

Asymmetric

Symmetric

aug = 1

aug = 12

aug = size of automorphism group
Targeted & active attack

This happens before the network is released... $H$ will be anonymized along with the rest.

$H = G(k, \frac{1}{2})$ over $k$ dummy nodes

$b$ nodes in $G$ attacked

[Backstrom, Dwork, Kleinberg]
Targeted & active attack (2)

Attack works if $H$ is unique in $G$...

i.e., $\text{aug}(H) = 1$ and $H \subset G$ only once

...and if set of attack nodes for each attacked node is unique
Targeted & active attack

- **Two different scalings / attacks**
  - “walk-based attack”
    - \( k = \log n, \ b = k^2 = (\log n)^2 \)
    - Pros: efficient recovery algorithm, hard to detect
    - Cons: requires larger \( H \) than theoretically possible
  - “cut-based attack”
    - \( k = b = (\log n)^{1/2} \)
    - Pros: smallest possible \( H \)
    - Cons: smaller “yield” in revealed nodes, easier to detect, computationally more demanding

- **Remarkable feature:**
  - Success does not depend on \( G \! \)
  - Success with high prob. is w.r.t. to randomness in construction of \( H \)
Targeted & passive attacks

- **Model:**
  - Adversary sees $k$-hop neighborhood of selected nodes
  - E.g.: db access; knowledge about own social circle; facebook privacy policy

$H_0$: 0-hop subgraph

$H_1$: 1-hop subgraph

$H_2$: 2-hop subgraph

$H_3$: 3-hop subgraph

[Hay, Miklau, Jensen, Towsley, Li]
Targeted & passive attacks (2)

\[ G(n, p), n \to \infty \]

<table>
<thead>
<tr>
<th>( H_1 ): 1-hop subgraph</th>
<th>Sparse ( p = c/n )</th>
<th>Dense ( p = c \log n / n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>anon</td>
<td>anon</td>
<td>fail</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( H_2 ): 2-hop subgraph</th>
<th>anon</th>
<th>fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>( H_3 ): 3-hop subgraph</td>
<td>anon</td>
<td>fail</td>
</tr>
</tbody>
</table>

Proof technique: focus on degree sequence within \( H_i \); compute \( P(\text{sequence unique}) \)

Sharp transition from perfectly anonymous to very fragile!
Global de-anonymization

[Narayanan, Shmatikov]
[Pedarsani, MG]
Heuristics for network de-anonymization

Try mapping high-degree nodes first

But how to map them correctly?

What if the two graphs are not isomorphic, just “similar”?
Neighborhood overlap metric

Similarity metric:

\[ \text{sim} \left( A, B \right) = \frac{|A \cap B|}{\sqrt{|A||B|}} \]

\[ \text{sim}(u,v) = \frac{2}{2} = 1 \]

\[ \text{sim}(u,v) = \frac{1}{\sqrt{3}} < 1 \]
Map propagation

Select a random $u$ on left

Find max $\text{sim}(u,v)$ on the right

Check that $u$ is max $\text{sim}(u,v)$ on the left

Continue until done or blocked
Insights from de-anonymization experiments

- **Remarkable result**
  - Fairly simple & efficient algorithm de-anonymizes millions of nodes

- **Open questions**
  - When does it work? Seems to rely on:
    - Very compact graph $\rightarrow$ for propagation to continue
    - Strong clustering $\rightarrow$ for cosine similarity metric
    - Skewed degree distribution $\rightarrow$ to identify seed set
  - Dependence on:
    - Tuning parameters?
    - Seed set identification?
    - Error propagation behavior?
  - **When can an infinitely powerful adversary de-anonymize?**
    - Information-theoretic: non computational limitation
**$G(n, p; s)$ Sampling Model**

Generator $G = G(n, p)$
- ** sampled ($s$)
-  not sampled ($1 - s$)

“real” social ties
phone calls
emails

$s$ measures similarity

[Narayanan, Shmatikov]
[Pedarsani, MG]
Mappings and Edge Mismatch

\[ \Delta(\pi_0) = 0 \]

\[ \Delta(\pi) = 2 \]
Adversary model

▪ **Assumption:**
  ▪ Attacker has infinite computational power
  ▪ Can try all possible mappings $\pi$ and compute edge mismatch function $\Delta(\pi)$

▪ **Question:**
  ▪ Are there conditions on $p, s$ such that
    
    $$ P \left\{ \pi_0 \text{ unique} \min \Delta(\pi) \right\} \rightarrow 1 $$

▪ If yes: adversary would be able to match vertex sets only through the structure of the two networks!

▪ **Note:**
  ▪ $G(n, p; s)$ model: statistically uniform, low clustering, degree distribution not skewed $\rightarrow$ conjecture: harder than real networks
Theorem:
For the $G(n, p; s)$ matching problem, if

\[
\frac{s^2}{2 - s} \leq \frac{E[\text{degree}]_{G_{1,2}}}{8 \log n + \omega(1)}
\]

then $G_{1,2}$ can be perfectly matched w.h.p.

Interpretation:
- Surprisingly weak condition:
  - Degree growing faster than $\sim \log n$ enough to break anonymity
  - Decrease with $s$ only quadratic

threshold for $\text{aug}(G) = 1$
Proof sketch (1)

- Define the number of order-$k$ mappings that beat the identity mapping

\[ S_k = \sum_{\pi \in \Pi_k} 1_{\{\Delta_\pi \leq \Delta_0\}} \]

- Want to show that total number of mappings giving lower error than identity

\[ \mathbb{E}[S] \leq \sum_{k=2}^{\infty} n^k \max_{\pi \in \Pi_k} \mathbb{P}\{\Delta_\pi - \Delta_0 \leq 0\} \rightarrow 0 \]

Bound on # of order-$k$ permutations

Set of order-$k$ permutations

Worst-case prob. of error for any order-$k$ map

First-Moment Method: to show $P(S = 0) \rightarrow 1$
Proof sketch (2)

- Fix a particular map $\pi$

$V_\pi$: set of mismatched nodes under $\pi$

$\pi \in \Pi_{11}$

Transposition $\Rightarrow$ invariant edge
Proof sketch (3)

\[ E_\pi = V \times V_\pi: \text{all the edges modified under } \pi \]

\[ n - k \text{ nodes} \]

\[ V_\pi: k \text{ nodes} \]

\[ \Delta_0: \text{each edge contributes } Ber(2ps(1 - s)): \text{ sampling errors} \]

\[ \Delta_\pi: \text{each pair of edges contributes } Ber(2ps(1 - ps)): \text{ matching errors} \]
Proof sketch (4)

- Distribution of sampling and matching errors

\( X_\pi \) and \( Y_\pi \) are dependent, because functions of same random sets

\[
\begin{align*}
\text{Number of matching errors} & \quad \text{under } \pi \text{ within } E_\pi \\
\text{Number of sampling errors} & \quad \text{(i.e., under identity) within } E_\pi \\
\text{Upper bound on } \# \text{ of invariant edges} & \\
\text{Size of set of edges that get changed by } \pi
\end{align*}
\]

\[
\begin{align*}
\text{(stoch.)} \quad X_\pi & \geq Y_\pi \\
\begin{cases}
\text{Bi} (e_k, 2ps(1 - ps)) \\
\text{Bi} (e_k - \left\lceil k/2 \right\rceil, 2ps(1 - s))
\end{cases}
\end{align*}
\]
Proof sketch (5)

- Dependence $\Rightarrow$ crude bound
  \[ P \{ X_2 - X_1 \leq 0 \} \leq P \{ X_1 \geq x \} + P \{ X_2 \leq x \} \]

- Appropriate choice of $x$
- Chernoff bounds for left/right tails of binomial
- If
  \[ ps \frac{s^2}{2 - s} = 8 \frac{\log n}{n} + \omega(n^{-1}) \]
  then identity permutation minimizes error function a.a.s.
Conclusion

Random graph models:
- Rigorous statements, but sacrificing “realism”
- More “uniform” than real networks → corner case
- Salient features, parsimonious
- Guide where to focus heuristics, algorithms

Key takeaway:
- Graph anonymity is harder than it may seem!
  - Active: \((\log n)^{1/2}\) dummy nodes
  - Passive: \(\log n\) degree growth (local+exact, global+noise)
- Evidence that networks densify with size \((\text{deg} \propto n^{\alpha-1}, \alpha>1)\)
  → large nets always go over the privacy threshold

How to share network data?
- Focus on applications: what do we really need to reveal?
  - E.g.: community structures, distance function, ...?
- Privacy guarantees vs value of information?
The End

Thanks for your interest!

Networks out of Control

Matthias Grossglauser
Patrick Thiran