Inferring Visibility: Who is (not) talking to whom?

Gonca Gürsun, Natali Ruchansky, Evimaria Terzi, and Mark Crovella
A Simple Question

• What paths pass through my network?
  – If someone at BU were to send an email to Telefonica, would it go through my network?

• Important for network planning, traffic management, security, business intelligence.
Surprisingly hard to answer!

- Routing decisions are only partially communicated to neighbors via BGP
- In general, decisions made by a remote AS are not known
Observing Traffic

• An AS can observe the traffic passing through it
  – If BU sends traffic to Telefonica through Sprint, Sprint knows it
• Traffic only provides **positive** information
  – Absence of traffic is ambiguous

If the observer does not see traffic from i to j, it is either
  – A **true zero**: the path from i to j does not go through the observer; or
  – A **false zero**: the path goes through, but i is not sending anything to j
The Visibility-Inference Problem

- For each observer there is a ground truth matrix $T$
  - $T(i, j) = 1 \implies$ path from $i$ to $j$ passes through observer

- Traffic summarized in observable matrix $M$
  - $M(i, j) = 1 \implies$ traffic was seen flowing from $i$ to $j$
  - $M(i, j) = 1 \implies T(i, j) = 1$

- Problem: label the zeros in $M$ as either true or false

\[
T = \begin{bmatrix}
0 & 1 & 0 \\
1 & 1 & 0 \\
1 & 0 & 1
\end{bmatrix} \quad M = \begin{bmatrix}
0 & 0 & 0 \\
1 & 0 & 0 \\
1 & 0 & 1
\end{bmatrix}
\]
Intuition

• Amplify knowledge obtained from traffic observation
• Empirically we observe that there are groups of sources, destinations exhibiting `similar routing’
• Observed traffic provides positive knowledge for entire group

\[
M = \begin{bmatrix}
0 & 0 & 0 \\
1 & 0 & 0 \\
1 & 0 & 1 
\end{bmatrix}
\]
General Approach

Given an observed matrix $M$, for each zero element $(i, j)$:

0. Choose sets $S_i$ and $D_j$ having similar routing to $i$ and $j$
1. Extract the descriptive submatrix $M(S_i, D_j)$ for $(i, j)$
2. Compute descriptive value $\Pi_{ij}$, e.g. sum or density of $M(S_i, D_j)$
3. If $\Pi_{ij}$ is above a threshold $\beta$, then classify $(i, j)$ as false zero, otherwise true zero.

Each step can be instantiated in various ways.
Data

• **Ground-truth matrices from BGP data**
  – Collected all active paths from 38 sources to 135,000 destinations
  – 24K observer ASes
  – For each AS, constructed 38 x 135,000 ground truth matrix \( T \)

• **Simulate traffic absence by setting some 1s to zeros**
  – Flipped at random from 1 to 0
    • 10%, 30%, 50%, 95%
  – Also studied correlated flipping patterns
Observer AS Types

• Different Ases have different patterns of 1s in their visibility matrices
  – affected by AS’s topological location.

• Core ASes : Core-100, Core-1000
  – 1-valued entries scattered relatively uniformly

• Edge ASes : Edge-1000
  – 1-valued entries clustered in a small set of rows and columns

\[ T = \]
Two Methods

- **Visibility-based Method**
  - Uses only observed visibility patterns in M

- **Proximity-based Method**
  - Uses external information (BGP paths)
Submatrix Selection : Visibility-Based Method

• Is it possible to find the group of paths routed similarly by **only** using the information in $M$?
• Select the submatrix $M(S_i, D_j)$ for zero $(i, j)$ as follows:
  $$S_i = \{ i \} \cup \{ i' | M(i', j) = 1 \} \text{ and}$$
  $$D_j = \{ j \} \cup \{ j' | M(i, j') = 1 \}$$
• $S_i$ = set of sources that are observed to send traffic to $j$
• $D_j$ = set of dest. that are observed to receive traffic from $i$

$$M = \begin{pmatrix}
  s_1 & s_2 \\
  \begin{bmatrix}
    d_1 & d_2 \\
    0 & 0 & 0 \\
    1 & 0 & 0 \\
    1 & 0 & 1 \\
  \end{bmatrix}
\end{pmatrix}$$
SUM Distributions
For Edge-1000 set

True Zeros
Threshold $\beta$ is easy to set automatically by cross-validation

False Zeros
• Good performance for edge ASes
• Need a better approach for core ASes
Measuring “Routing Similarity”

- Conceptually, imagine capturing the entire routing state of the Internet in a matrix $H$
- $H(i,j) = \text{next hop on path from } i \text{ to } j$
- Each row is actually the routing table of a single AS
Measuring “Routing Similarity”

- Conceptually, imagine capturing the entire routing state of the Internet in a matrix $H$
- $H(i,j) =$ next hop on path from $i$ to $j$
- Each row is actually the routing table of a single AS
- Now consider the columns

$$H = \begin{bmatrix} \quad \end{bmatrix}$$
Routing State Distance

- $\text{rsd}(a,b) = \# \text{ of entries that differ in columns } a \text{ and } b \text{ of } H$
- If $\text{rsd}(a,b)$ is small, most ASes think $a$ and $b$ are ‘in the same direction’
- A metric (obeys triangle inequality)
RSD in Practice

• Key observation: we don’t need all of H to obtain a useful metric

• Many (most?) nodes contribute little information to RSD
  – Nodes at edges of network have nearly-constant rows in H

• Sufficient to work with a small set of well-chosen rows of H

• Such a set is obtainable from publicly available BGP measurements
  – Note that public BGP measurements require some careful handling to use properly for computing RSD
Submatrix Selection: Proximity-based Method

- Select the submatrix $M(S_i, D_j)$ for zero $(i, j)$ as follows:

  \[ S_i = \{ i \} \cup \{ i' | rsd(i, i') < \gamma \} \]
  \[ D_j = \{ j \} \cup \{ j' | rsd(j, j') < \gamma \} \]

- **Success Rates**

<table>
<thead>
<tr>
<th></th>
<th><strong>Edge-1000</strong></th>
<th></th>
<th><strong>Core-100</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Flip Rate</td>
<td>TPR</td>
<td>FPR</td>
<td>TPR</td>
<td>FPR</td>
</tr>
<tr>
<td>10%</td>
<td>0.99</td>
<td>0.03</td>
<td>0.95</td>
<td>0.02</td>
</tr>
<tr>
<td>95%</td>
<td>0.85</td>
<td>0.08</td>
<td>0.96</td>
<td>0.06</td>
</tr>
</tbody>
</table>
Discussion

• Each method works well for its respective AS types.
  – Visibility-based method for Edge ASes
  – Proximity-based method for Core ASes

• Distribution of false zeros
  – Random false zeros
  – Correlated false zeros – all 1s to a destination are false zeros

<table>
<thead>
<tr>
<th>Edge (Visibility-based)</th>
<th>Core (Proximity-based)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPR</td>
<td>FPR</td>
</tr>
<tr>
<td>1.0</td>
<td>0.98</td>
</tr>
<tr>
<td>TPR</td>
<td>FPR</td>
</tr>
<tr>
<td>0.78</td>
<td>0.02</td>
</tr>
</tbody>
</table>
Related Work

- First time “Visibility Inference” problem is introduced.

- RSD is a generalization of BGP atoms
  - Broido et.al. NRDM 01

- Computing RSD requires understanding BGP routing
  - Mühlbauer et.al. SIGCOMM 07

- Study of zero-inflated models from other fields
  - Zero-inflated truncated generalized Pareto distribution for the analysis of radio audience data, Coutirier et.al, 10
  - Zero tolerance Ecology: Improving Ecological Inference By Modelling the Source of Zero Observations, Martin et.al, 05
Conclusion

- ASes can identify which paths go through their networks very accurately by using a nonparametric classifier.

- An AS should instantiate its classifier based on its type
  - Edge ASes: Visibility-based method
  - Core ASes: Proximity-based method

- A new metric: Routing State Distance (RSD) to measure routing similarity of prefixes.
THANKS!

Inferring Visibility: Who is (not) talking to whom?

Gonca Gürsun, Natali Ruchansky, Evimaria Terzi, and Mark Crovella
Discussion: Data Hygiene Implications

- BGP data is known to favor customer-provider links and miss peer-peer links
- Our restriction to 38 x 135000 known paths means that we are not missing any links in the scope of our experiments
- Hence accuracy for the chosen subsets of M is not affected by missing links
- However, the accuracy of our methods may be different on the full M
  - Whether better or worse, it’s not clear
  - There is some reason to believe it would be better...
RSD vs. Hop Distance

Graph showing the relationship between RSD and Hop Distance for different prefix pairs.
Application: Traffic Matrix Completion

- Estimating traffic *volumes* that are not directly measurable given a partially known matrix $V$
  - Use known elements to estimate unknowns.
  - So far, any 0-valued element of $V$ is treated as missing.
  - What if it’s not missing but just 0 (a false zero)?

- Using $V$ of a Tier-1 provider
  - Complete unknowns in $V$ with and without the knowledge of false zeros.
  - NK: Completion without any knowledge of false zeros
  - GT: Completion with the ground truth for false zeros
  - VIS: Completion with the knowledge of false zeros learned by Visibility-based Method
  - PROX: Completion with the knowledge of false zeros learned by Proximity-based Method
Application: Traffic Matrix Completion

- Cross-validation to measure success.
  - Flip some portion of the knowns to unknowns and estimate them
- Normalized Mean Squared Error (NMAE):
  \[
  \sum \frac{|V(i,j) - \hat{V}(i,j)|}{\sum V(i,j)} \text{ for all unknown } i,j
  \]

- Knowledge of false zeros improves TM Completion accuracy
- Proximity-based Method works as good as the Ground-Truth
Application: Traffic Matrix Completion

- Accuracy gain is higher for small-valued entries

- Small entries

- Large entries

- Accuracy gain is higher for small-valued entries