Spy vs Spy: Anonymous Messaging

Sewoong Oh
University of Illinois at Urbana-Champaign

Joint work with
Giulia Fanti, Peter Kairouz and Pramod Viswanath
Anonymous Social Media provide meta-data privacy
Anonymous Messaging Apps

I think I'm schizophrenic... I see and hear things and I have a voice in my head, when I go to sleep it's like sleeping in a busy restaurant!

Sometimes I type "Sent from my iPhone" at the end of an email when I'm really at my computer so that I can get away with a short reply.
Anonymous messaging over networks
Centralized protocols are not truly anonymous
Messaging App: **Wildfire**

- Alice
- Bob
- Mary
- Carol
- Faith
- Saul
- Mike

**Wildfire** empowers devices by removing central service providers.

- It also has stronger anonymity properties than Secret, Whisper, and Yik Yak.

**Anonymous, distributed, secure implementation**
Diffusion of rumor/contagion

Social network/contact network
Diffusion of rumor/contagion

message author
Diffusion of rumor/contagion
Diffusion of rumor/contagion
Diffusion of rumor/contagion
Diffusion of rumor/contagion
Diffusion of rumor/contagion
Diffusion of rumor/contagion
Rumor source detection

can we locate the message author?
Snapshot reveals the source

- message author is likely to be in the “center”
Node eccentricity

- maximum distance from a node to any other node
Jordan centrality [Zhu, Ying ‘13]
Rumor Centrality [Shah, Zaman ’11]

Diagram showing a network with nodes of varying colors indicating high and low likelihood.
Diffusion over d-regular trees

Probability of detection

- image credit: [Shah & Zaman ’11]
Our Goal

\[ \log \mathbb{P}(\text{detection}) = \log N_T \]

\[ \mathbb{P}(\text{Detection}) = \frac{1}{N_T} \]
- If we know when the adversary is going to attack,
- Go straight in a line for T/2
If we know when the adversary is going to attack,

- Go straight in a line for $T/2$
- Then, diffusion for $T/2$
Line graph
Line graph: diffusion

$T = 0$
Line graph: diffusion

$p$ $p$

$T = 1$
Line graph: diffusion

\[ T = 1 \]
Line graph: diffusion

\[ T = 2 \]
Line graph: diffusion

\[ T = 2 \]
Line graph: diffusion

$T = 3$
Line graph: diffusion

- Probability of spread is constant
- spreads at the same rate in all directions
- equivalent to **two independent random walks**

\[ T = 3 \]
Adversary with snapshot

nodes with the message

can we locate the message author?
Maximum likelihood detection

- node in the middle is the mostly likely author
Maximum likelihood detection

Likelihoods

Probability of detection $\approx \frac{1}{\sqrt{N}}$
Pólya’s urn process is good for privacy

- choose a ball at random from the urn

with probability $1/2$

$T = 1$
Pólya’s urn process

- replace chosen ball by two balls of the same color

$T = 1$
Pólya’s urn process

- repeat previous steps

$T = 2$

with probability $2/3$
Pólya’s urn process

$T = 2$

rich get richer and poor get poorer
Anonymity Property

all events are equally likely

T = 12

10 red and 4 blue w.p. 1/13

4 red and 10 blue w.p. 1/13

7 red and 7 blue w.p. 1/13
Pólya’s urn process for spreading messages

Urn 1
8 red and 6 blue

Urn 2
5 red and 9 blue
Source detection from snapshot

How many balls came from urn 1?
Maximum likelihood detection

Likelihoods

diffusion process

Polya urn process

1

\( \frac{N}{2} \)

\( N \)
Maximum likelihood detection

Likelihoods

diffusion process

Polya urn process

Probability of detection $\approx \frac{1}{N}$
Line graph: adaptive diffusion

- consider a line graph
Line graph: adaptive diffusion

- Node 0 starts rumor at $T = 0$
- every time, one more node is infected
Line graph: adaptive diffusion

one of the neighbor is infected w.p. 1/2

$T = 1$
Line graph: adaptive diffusion

$T = 1$

Node 1 receives message at $T = 1$
Line graph: **adaptive diffusion**

- Hop distance to message author
- Elapsed time

In addition to the message, the author passes $h = 1$ and $T = 2$ to node 1.
Line graph: **adaptive diffusion**

-2  -1  0  1  2

-\frac{1}{3} \quad \frac{2}{3}

\[ T = 2 \]

- probability of passing message = \frac{h+1}{T+1}
Line graph: adaptive diffusion

- node 2 receives the message

$T = 2$
Line graph: adaptive diffusion

-2 | -1 | 0 | 1 | 2

in addition to the message, node 1 passes $h = 2$ and $T = 3$ to node 2

hop distance to message author
elapsed time
Line graph: adaptive diffusion

$T = 3$

- probability of passing message $= \frac{h+1}{T+1}$
Line graph: adaptive diffusion

- left node 1 receives the rumor

\[ T = 3 \]
Line graph: **adaptive diffusion**

-2 -1 0 1 2

- **in addition to the message, node 0 passes**
  \[h = 1 \text{ and } T = 4\]
  to node 1

- **hop distance to message author**
- **elapsed time**
Given snapshot

can we locate the message author?
Maximum likelihood detection

probability of detection $\sim \frac{1}{N}$
Maximum likelihood detection

Probability of detection

number of nodes with the message

probability of detection $\sim \frac{1}{N}$
$d$-regular trees
Probability of detection using Rumor Centrality

spread with fixed probability $p$

- [Shah & Zaman ’11]
Probability of detection using Jordan centrality

spread with probability

\[ p(h, t) = \frac{h + 1}{t + 1} \]
$d$-regular trees: adaptive diffusion
$d$-regular trees: adaptive diffusion

- initially, the author is also the "virtual source"
$d$-regular trees: adaptive diffusion

- at $T = 1$, node $v^*$ selects one neighbor at random
- the chosen node becomes the new virtual source

in addition to the message, $v^*$ passes $h = 1$ and $T = 1$ to the chosen neighbor

$h = \# \text{ of hops away from true source}$
$d$-regular trees: adaptive diffusion

- the chosen neighbor becomes the new virtual source
\(d\)-regular trees: adaptive diffusion

- At \(T = 2\), the virtual source passes the message to all its neighbors.
$d$-regular trees: adaptive diffusion

- as $T$ transitions from even to odd, the virtual source has two options:
  - keeping the virtual source token
  - passing the virtual source token
Keeping the virtual source token

- virtual source token is kept with probability \( \frac{T}{(d-1)^2 h-1 - 1} \)
- nodes that received message faster, spreads faster
Keeping the virtual source token

- all leaf nodes with the message pass it to their neighbors
balanced tree rooted at the virtual source

keeping the virtual source token

w.p. \( \frac{(d - 1)^{t/2} - h - 1}{(d - 1)^{t/2} + 1} - 1 \)

passing the virtual source token

w.p. \( 1 - \frac{(d - 1)^{t/2} - h - 1}{(d - 1)^{t/2} + 1} - 1 \)
Adversary with snapshot

can we locate the message author?
Maximum likelihood detection

Theorem. [Fanti, Kairouz, Oh, Viswanath 2015]
1. All nodes except for the virtual source is equally likely, such that

$$P(\text{Detection}) = \frac{1}{N - 1}$$

2. The expected distance between the estimated and the true source is

$$\frac{T}{2}$$
Timing

<table>
<thead>
<tr>
<th>time</th>
<th>from</th>
<th>to</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:12</td>
<td>Alice</td>
<td>Spy1</td>
</tr>
<tr>
<td>10:25</td>
<td>Bob</td>
<td>Spy2</td>
</tr>
<tr>
<td>11:01</td>
<td>Mary</td>
<td>Spy3</td>
</tr>
</tbody>
</table>
Adversary with timing

what if spies collect meta-data?
what about the control packets?

State information reveals the source location.

<table>
<thead>
<tr>
<th>time</th>
<th>from</th>
<th>to</th>
<th>state</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1=8</td>
<td>1</td>
<td>Spy1</td>
<td>h=2, t=3</td>
</tr>
<tr>
<td>T2=10</td>
<td>4</td>
<td>Spy2</td>
<td>h=3, t=5</td>
</tr>
</tbody>
</table>
Suppose the state is hidden

\[ N = 101 \text{ and } T_2 = T_1 + 25 \]
Hiding state variables by sending only the sampling paths

along with message, pass the entire sample path
Hiding state variables by sending only the sampling paths

\[ T = 2 \]

node 1 waits 1 unit of time and passes message
Hiding state variables by sending only the sampling paths

\[ T = 4 \]

spies observe both meta-data and control packet
Hiding state variables by sending only the sampling paths

<table>
<thead>
<tr>
<th>time</th>
<th>from</th>
<th>to</th>
<th>state</th>
</tr>
</thead>
<tbody>
<tr>
<td>(T_1=8)</td>
<td>1</td>
<td>Spy1</td>
<td>left sample path after (T=8)</td>
</tr>
<tr>
<td>(T_2=10)</td>
<td>4</td>
<td>Spy2</td>
<td>right sample path after (T=10)</td>
</tr>
</tbody>
</table>
Pólya’s urn process

Sampling with (double) replacement

\[ \theta \sim U[0, 1] \]
\[ X_t \sim \text{i.i.d. Bern}(\theta) \]

Sampling without replacement with hidden parameter
Pólya’s urn process on a line

\[ \theta_L \sim U[0, 1] \]

\[ L_t \sim \text{i.i.d. Bern}(\theta_L) \]

\[ \theta_R \sim U[0, 1] \]

\[ R_t \sim \text{i.i.d. Bern}(\theta_R) \]

Spy nodes can figure out \( \theta_L \) and \( \theta_R \) exactly from control packets, and only \( \theta_L \) and \( \theta_R \)

<table>
<thead>
<tr>
<th>time</th>
<th>from</th>
<th>to</th>
<th>state</th>
</tr>
</thead>
<tbody>
<tr>
<td>( T1=8 )</td>
<td>1</td>
<td>Spy1</td>
<td>( \theta_L )</td>
</tr>
<tr>
<td>( T2=10 )</td>
<td>4</td>
<td>Spy2</td>
<td>( \theta_R )</td>
</tr>
</tbody>
</table>
Adaptive diffusion on a tree

<table>
<thead>
<tr>
<th>time</th>
<th>from</th>
<th>to</th>
<th>state</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Alice</td>
<td>Spy1</td>
<td>sample paths for the descendants of the spy</td>
</tr>
<tr>
<td>10</td>
<td>Bob</td>
<td>Spy2</td>
<td>sample paths for the descendants of the spy</td>
</tr>
</tbody>
</table>
Adaptive diffusion on a tree

infinite $d$-regular tree, with spies i.i.d. chosen with probability $p$

$\mathbb{P}(\text{detection})$
Collaborators

Giulia Fanti  Peter Kairouz  Pramod Viswanath

 Discussions: Kannan Ramchandran