Spy vs. Spy: Rumor Source Obfuscation

Peter Kairouz
University of Illinois at Urbana-Champaign

Joint work with
Giulia Fanti, Sewoong Oh, and Pramod Viswanath
Some people have important, sensitive things to say.
Personal confessions

Others have less important, but sensitive things to say.

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!

I'm a Mormon, and losing my faith.
Existing anonymous messaging apps

secret

whisper

Yik Yak
Existing anonymous messaging apps

secret

whisper

Bob

Mary

Alice
Existing anonymous messaging apps

- secret
- whisper
- Yik Yak

Diagram:
- Bob
- Mary
- Alice
Existing anonymous messaging apps

- **secret**
- **whisper**
- **Yik Yak**
Existing anonymous messaging apps

secret

whisper

Bob

Alice

Mary

Server

Yik Yak
Existing anonymous messaging apps are not truly anonymous!
Compromises in anonymity

anonymity loss extends beyond the network
Distributed messaging
Distributed messaging

Bob

Alice

Mary
Distributed messaging

what can an adversary do?

Alice

Bob

Mary
Adversarial model

- Craig
- Bob
- Alice
- Mary
- David
Adversarial model

Diagram showing connections between individuals:
- Craig
- Bob
- Alice
- Mary
- David
Adversarial model

Bob

Craig

Alice

Mary

David
the adversary can figure out who got the message
Information flow in social networks

- $G$ is the graph representing the social network
Information flow in social networks
Information flow in social networks

- Alice passes the message to her neighbors
Information flow in social networks

- her neighbors pass the message to theirs
information flow in social networks

- the message spreads in **all directions** at the **same rate**
Information flow in social networks

- the message spreads in **all directions** at the same rate
Information flow in social networks

- the message spreads in all directions at the same rate
Information flow in social networks

- this spreading model is known as the diffusion model
Adversary’s observation

can the adversary locate the message author?
Concentration around the center

- the message author is in the “center” with high probability
Rumor source identification

diffusion does not provide anonymity

[Shah, Zaman 2011]
Our goal

- $N_T$: expected number of nodes with the message at time $T$
Main result: adaptive diffusion
Main result: adaptive diffusion
Main result: adaptive diffusion
Main result: adaptive diffusion
Main result: adaptive diffusion
Main result: adaptive diffusion
Main result: adaptive diffusion
Main result: adaptive diffusion
Main result: **adaptive diffusion**

provides provable anonymity guarantees!
let's start with line graphs
Line graphs: diffusion

- the message author starts a rumor at $T = 0$
Line graphs: diffusion

- with probability $\alpha$, the left (right) node receives the message

$T = 1$
Line graphs: diffusion

- the node to the right of the author receives the message

\[ T = 1 \]
Line graphs: diffusion

- The rumor propagates in both directions at the same rate.

\[ T = 2 \]
Line graphs: **diffusion**

- the rumor propagates in **both directions** at the same rate

\[ T = 2 \]
Line graphs: **diffusion**

- $\alpha$ is **independent of time or hop distance** to message author

$T = 3$
Line graphs: diffusion

- diffusion on a line is equivalent to **two independent random walks**

\[ T = 3 \]
Adversary’s observation

$N = 5$

nodes with the message

can the adversary locate the message author?
Maximum likelihood detection

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

\[
\text{Probability of detection } \approx \frac{1}{\sqrt{N_T}}
\]
Line graphs: adaptive diffusion

- consider a line graph
Line graphs: adaptive diffusion

- node 0 starts a rumor at $T = 0$
Line graphs: adaptive diffusion

- with probability $\frac{1}{2}$, the left (right) node receives the message

$T = 1$
Line graphs: adaptive diffusion

- right node 1 receives the message

\[ T = 1 \]
Line graphs: adaptive diffusion

- probability of passing message: \( \alpha = \frac{h+1}{T+1} \)

\( T = 2 \)

hop distance to message author

elapsed time
Line graphs: adaptive diffusion

- Right node 2 receives the message

$T = 2$
Line graphs: adaptive diffusion

- Probability of passing message: $\alpha = \frac{h+1}{T+1}$
- $T = 3$
- Hop distance to message author
- Elapsed time
Line graphs: *adaptive diffusion*

- Left node 1 receives the message

\[ T = 3 \]
Adversary’s observation

$N_T = 4$

nodes with the message

can the adversary locate the message author?
Maximum likelihood detection

Likelihoods

diffusion

adaptive diffusion

$N_T/2$

$N_T$

$k$
Maximum likelihood detection

Probability of detection \( \approx \frac{1}{N_T} \)
$d$-regular trees

- what about $d$-regular trees?
\(d\)-regular trees: diffusion

- likelihoods concentrate heavily around the "center"
\textit{d}-regular trees: adaptive diffusion
$d$-regular trees: adaptive diffusion

- Initially, the source is also the "virtual source"
\(d\)-regular trees: adaptive diffusion

- at \(T = 1\), the author selects one neighbor at random
at \( T = 1 \), the author selects one neighbor at random.
\(d\)-regular trees: adaptive diffusion

- the chosen neighbor becomes the new virtual source
at $T = 2$, the virtual source passes the message to all her 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
Symmetry properties

- the graph is always symmetric around the virtual source
Keeping the virtual source token

- virtual source token is kept with probability \( \alpha = \frac{T^{T-h-1} - 1}{(d-1)^{2h+1} - 1} \)
Keeping the virtual source token

- all leaf nodes with the message pass it to their neighbors

happens in $T = 3$ and $T = 4$
Passing the virtual source token

- current virtual source selects one of its neighbors at random
Passing the virtual source token

previous virtual source passes \( h = 2 \) and \( T = 4 \) to new virtual source
Passing the virtual source token

- new virtual source passes the message to its neighbors which in turn pass it to their neighbors

happens in \( T = 3 \) and \( T = 4 \)
Adversary’s observation

can the adversary locate the message author?
Maximum likelihood detection

- All nodes except for the final virtual source are equally likely.
Main Theorem

1. We spread fast: \( N_T \approx (d - 1)^2 \)
2. All nodes except for the final virtual source are equally likely to be the source, hence

\[
P(\hat{v}_{ML} = v^*) = \frac{1}{N_T - 1}
\]

3. The expected distance between the estimated and true source is at least \( \frac{T}{2} \).
General graphs

adaptive diffusion for general graphs?
Simulation results: *Facebook graph*

- likelihoods can be *approximated* numerically
## Extensions and related work

<table>
<thead>
<tr>
<th>Theoretical</th>
<th>Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Adversaries with timing information</td>
<td>• Cyber-bullying detection</td>
</tr>
<tr>
<td>• Peer-to-peer dynamic networks</td>
<td>• Anonymous video sharing</td>
</tr>
<tr>
<td>• Hiding relays</td>
<td>• Message caching</td>
</tr>
<tr>
<td>• Multiple message sources</td>
<td>• Bootstrapping contacts</td>
</tr>
</tbody>
</table>