Metadata Conscious Anonymous Messaging

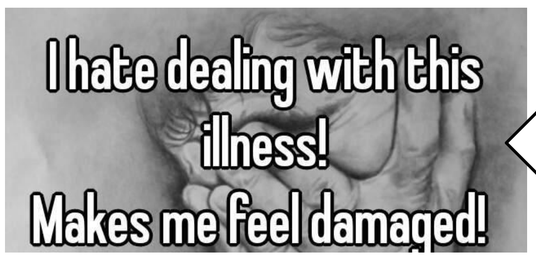
PI: Pramod Viswanath

Postdoc: Giulia Fanti

Collaborators: Peter Kairouz, Sewoong Oh, and Kannan Ramchandran

e-mails: {fanti, kairouz2, swoh, pramodv}@illinois.edu and kannanr@eecs.berkeley.edu

Anonymity matters



Personal Confessions → Political Activism

Jason Rezaian's Year of Imprisonment in Iran

Wednesday marks the one-year anniversary of the *Washington Post* reporter's detention in the Islamic Republic.

Russian Activists and Journalists Attacked at Chechen Border

Saudi Man Gets 10 Years, 2,000 Lashes Over Atheist Tweets

By THE ASSOCIATED PRESS
RIYADH, Saudi Arabia — Feb 27, 2016, 8:26 AM ET

Politics | Fri Nov 23, 2007 4:54pm EST Related

Syria blocks Facebook in Internet crackdown

DAMASCUS | BY KHALED YACOUB OWEIS

How can we empower people to speak without fear of social or political retribution?

The problem

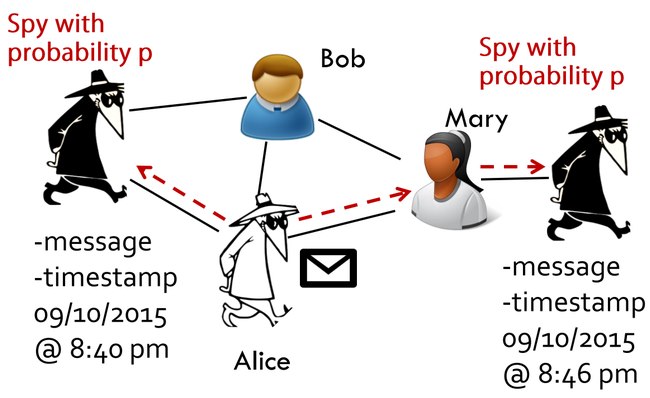
Design a distributed messaging algorithm that:

a) Prevents a powerful adversary from identifying the true message source,

b) Spreads content quickly over contact graphs.

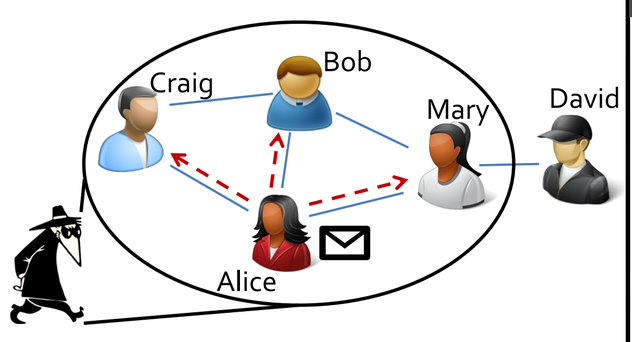
The adversaries

Spy-based Adversary



Colluding "spies" share message contents, metadata, and underlying graph structure to infer message authorship.

Snapshot Adversary



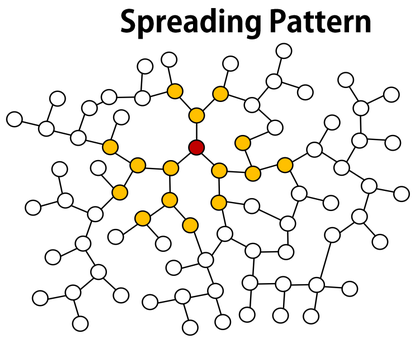
Adversary knows the underlying graph and can con collect a snapshot containing information about who got the message.

Information flow in social networks

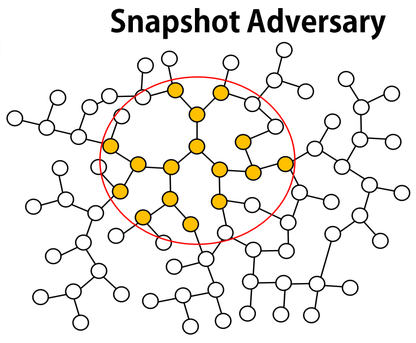
Most social networks spread content symmetrically based on user input.

(user approves message → message gets passed to friends)

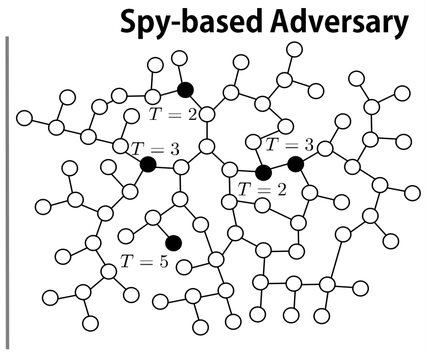
Spreading Pattern



Snapshot Adversary

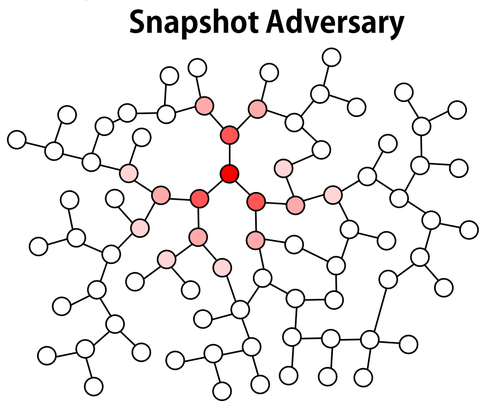


Spy-based Adversary



This spreading model is known as the diffusion model. Messages flow in all directions at the same rate. With high probability, diffusion places the true source in the center of the graph. This helps adversaries infer the source. [Shah & Zaman 2011, Pinto et. al. 2012]

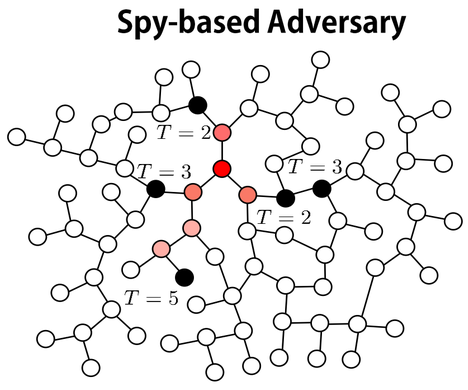
Snapshot Adversary

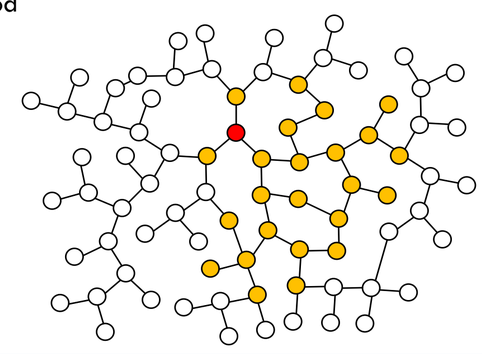


high likelihood

low likelihood

Spy-based Adversary





Intuition: Break the symmetry around the center. Spread in a way such that the source is always on the boundary of the information spread.

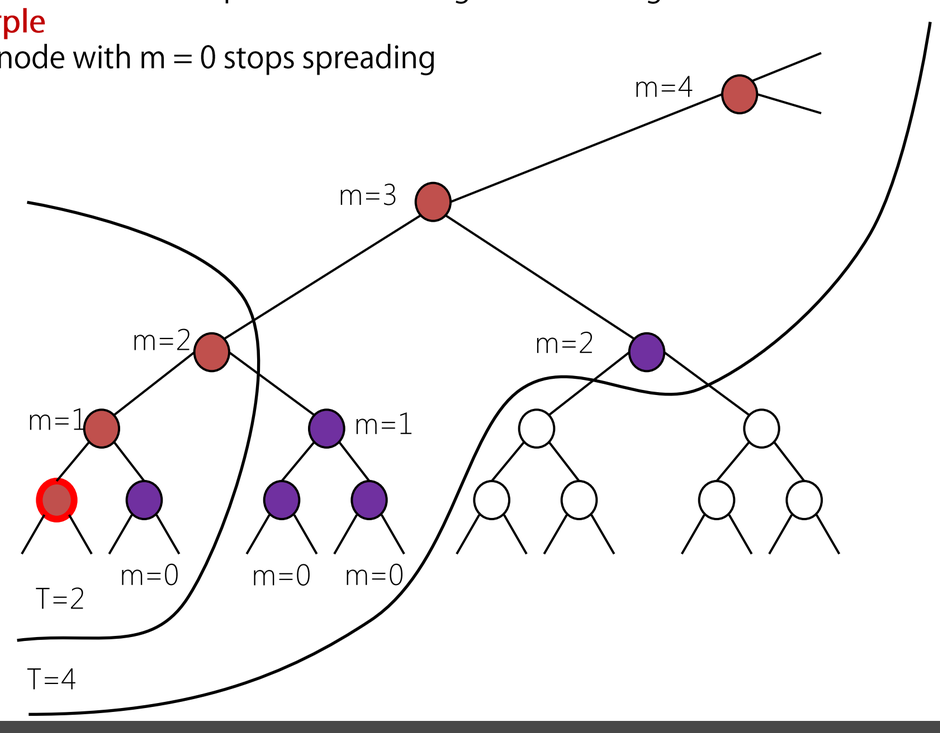
Adaptive diffusion

Adaptive diffusion breaks symmetry to provide strong anonymity.

Intuition: carefully adapt the information flow rate and direction

Adaptive diffusion protocol:

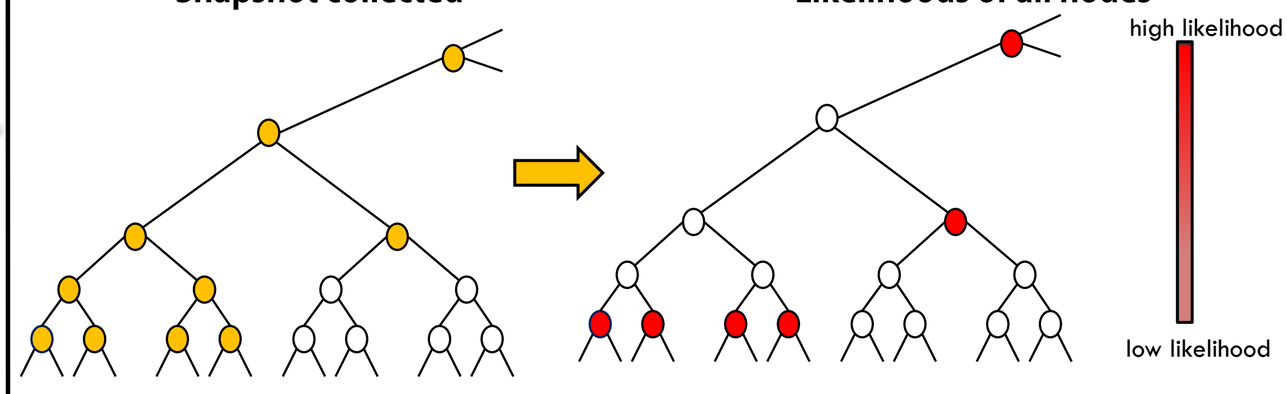
1. The source node chooses a neighbor at random, and passes the message to it with m = 1 & color = orange
2. An orange node
   1. passes the message to a randomly chosen neighbor with an incremented m & color = orange,
   2. and then to all other neighbors with a decremented m & color = purple.
3. A purple node with m > 1 passes the message to all its neighbors with a decremented m & color = purple
4. A purple node with m = 0 stops spreading



Regular trees: snapshot adversary

Snapshot collected

Likelihoods of all nodes

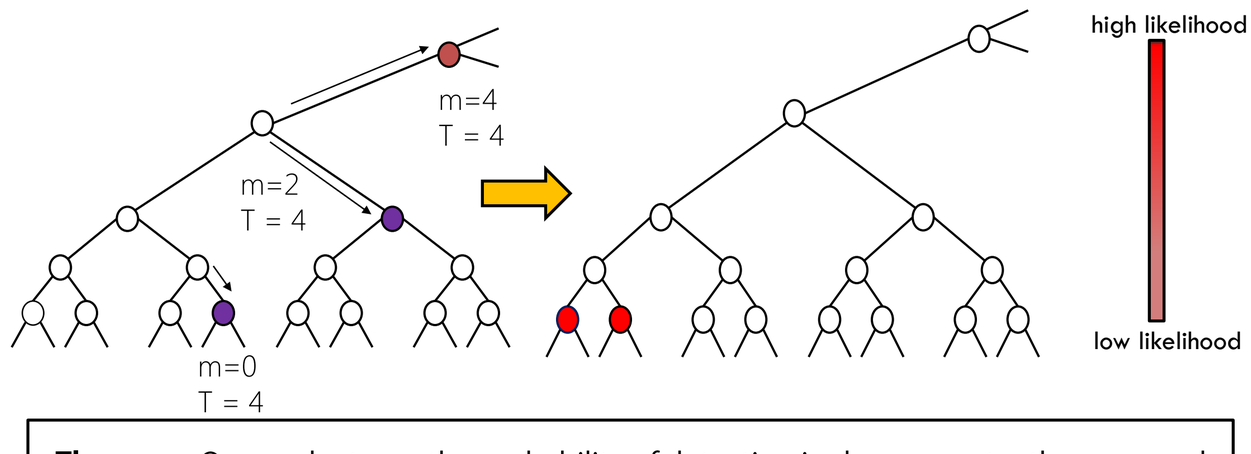


Theorem: On regular trees, adaptive diffusion hides the source in all the leaf nodes and spreads the message exponentially quickly. Therefore, the probability of rumor source detection is inversely proportional to the number of noes with the message.

Regular trees: spy-based adversary

Metadata collected

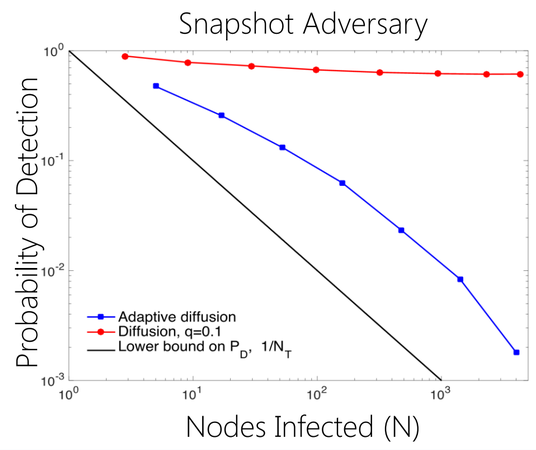
Likelihoods of all nodes



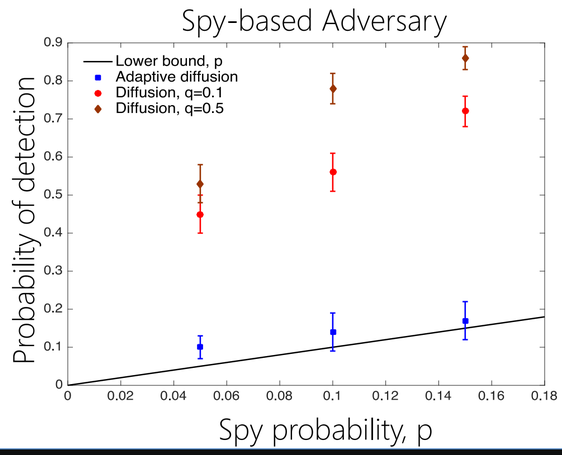
Theorem: On regular trees, the probability of detection is always greater than or equal to p. Moreover, the probability of detection under adaptive diffusion is p + o(p). The limit of the probability of detection, as the degree of the tree goes to infinity, is equal to p.

Adaptive diffusion on real graphs

Snapshot Adversary



Spy-based Adversary



SCIENCE OF SECURITY
VIRTUAL ORGANIZATION
Funded by the National Security Agency.

INFORMATIONTRUST INSTITUTE