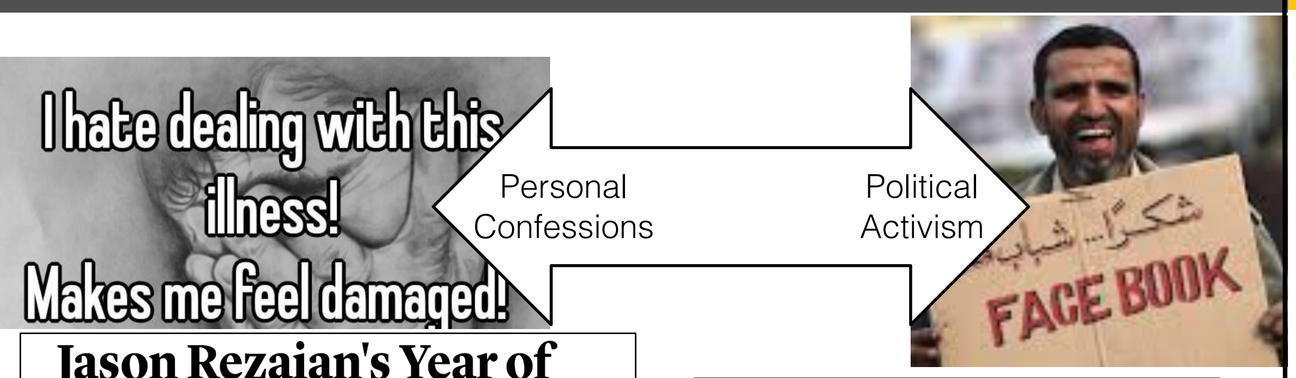
Spy vs. Spy:
Anonymous Broadcasting over Networks

Giulia Fanti*, Peter Kairouz*, Sewoong Oh*, Kannan Ramchandran†, Pramod Viswanath*
* University of Illinois at Urbana-Champaign † University of California, Berkeley

Anonymity in Social Networks



Can we design social networks that protect user anonymity?

The Problem

Design a distributed messaging protocol that:

a) Spreads content quickly over an underlying contact graph

b) Prevents an adversary with network oversight from linking messages to their sources

Proposed Solution: Adaptive Diffusion

Adaptive diffusion breaks the symmetry of random diffusion to provide strong, provable anonymity guarantees.

Idea: *Build a d-regular tree with the source at one of the leaves.*

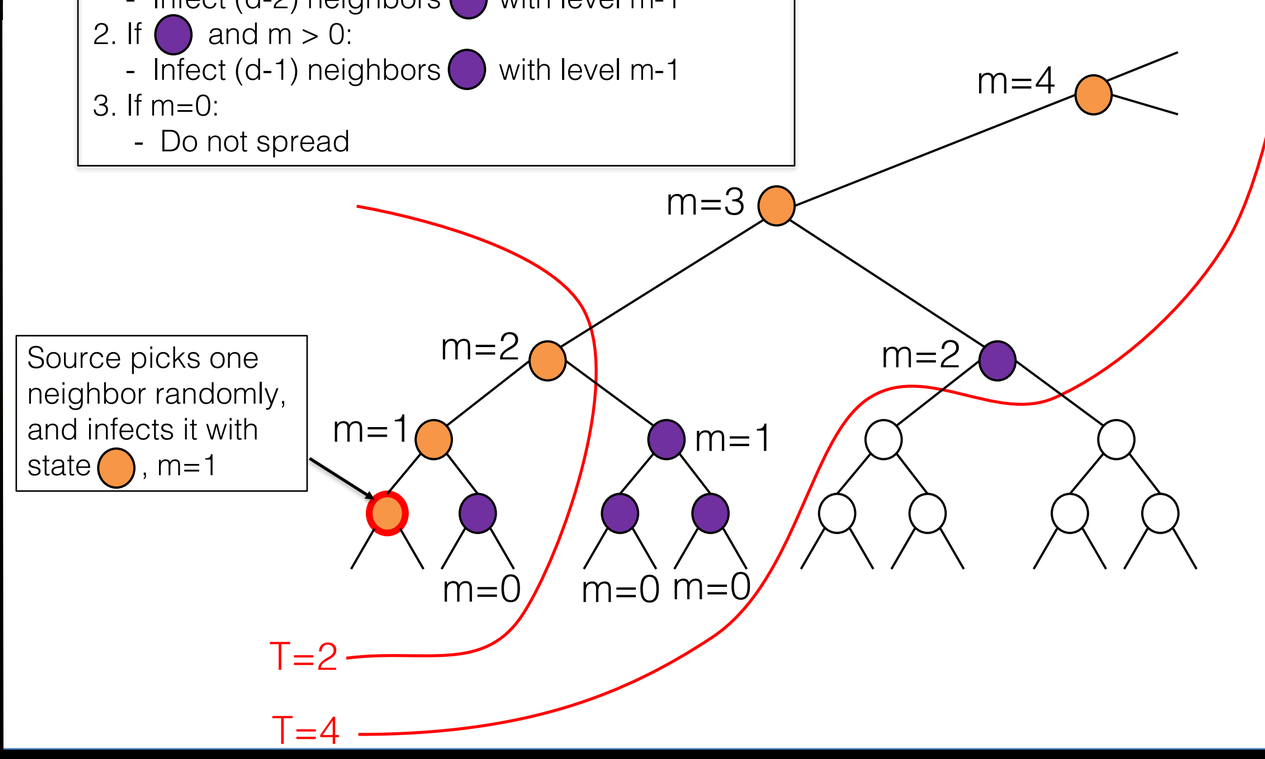
Rules

1. If ● and m>0:
   - Infect one neighbor ● with level m+1
   - Infect (d-2) neighbors ● with level m-1
2. If ● and m > 0:
   - Infect (d-1) neighbors ● with level m-1
3. If m=0:
   - Do not spread

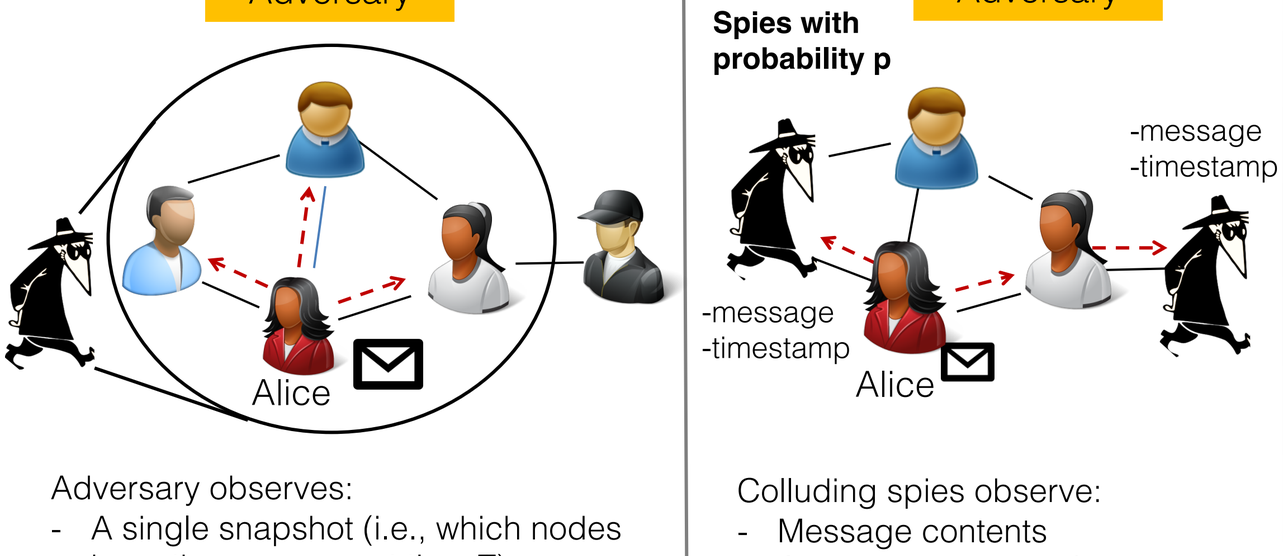
State

Color: ● ●

Level: m = 0, 1, …



Adversarial Models

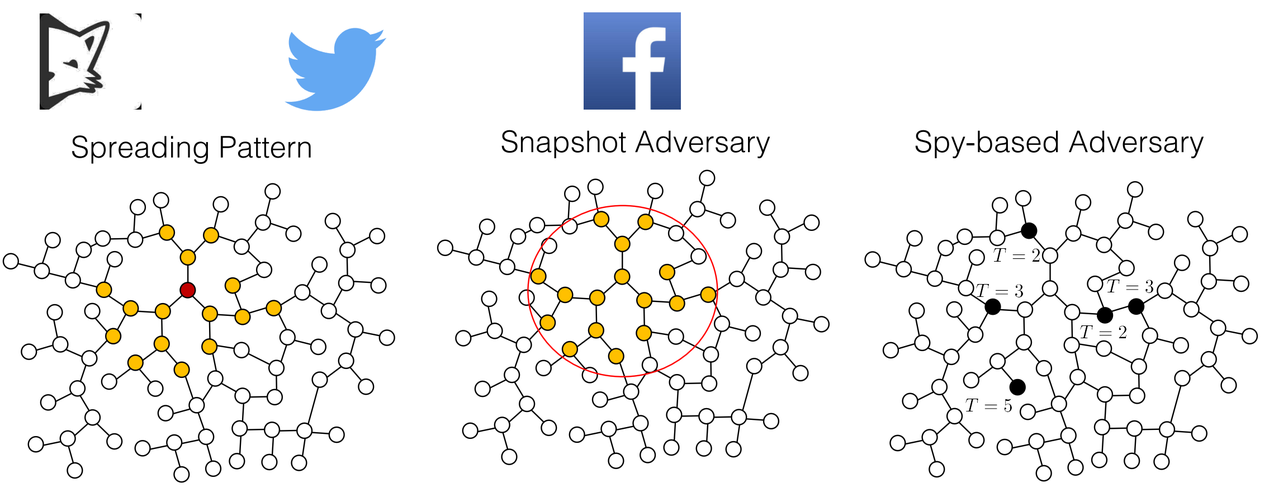


Adversary observes:
- A single snapshot (i.e., which nodes have the message at time T)
- The underlying graph

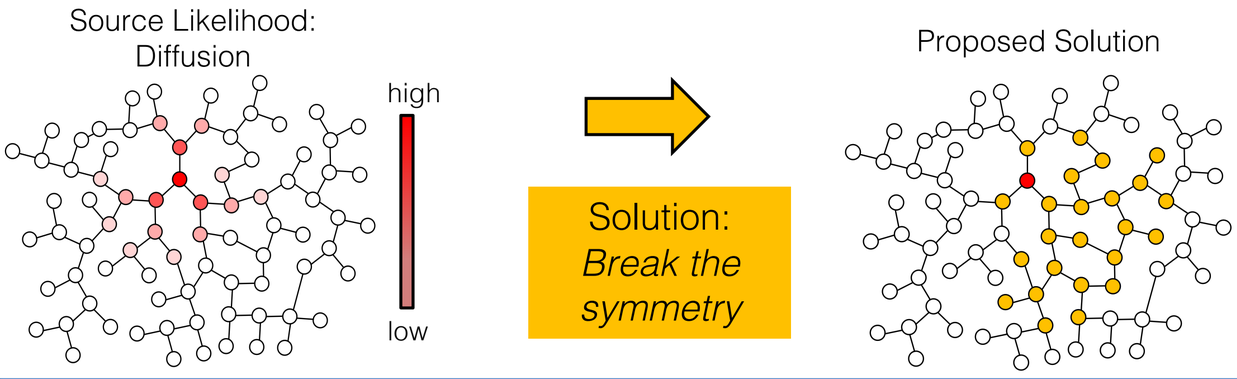
Colluding spies observe:
- Message contents
- Any message metadata
- The underlying graph

Information Flow in Networks

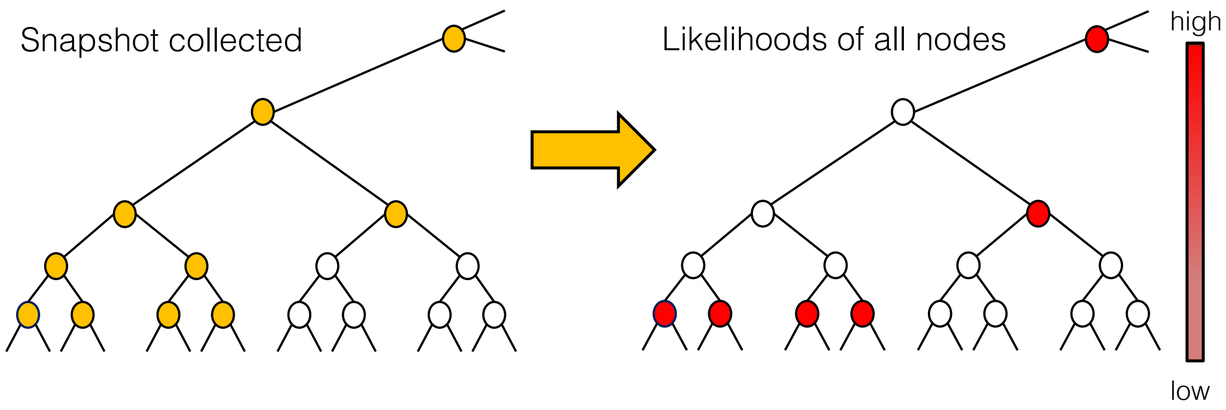
Most social networks spread content symmetrically based on user input.



This spreading can be modeled by random diffusion. 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]

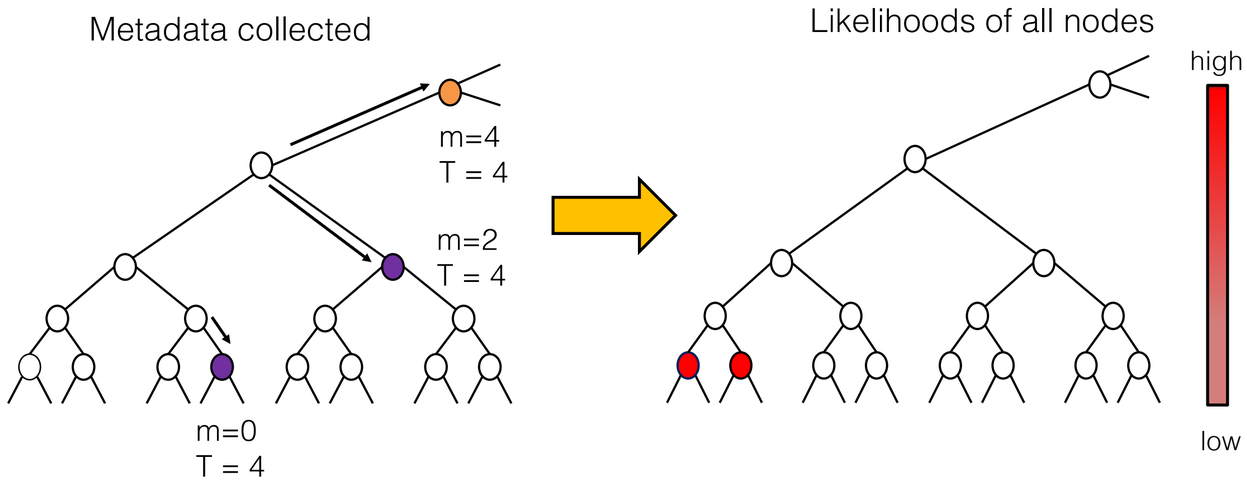


Regular Trees: Snapshot Adversary



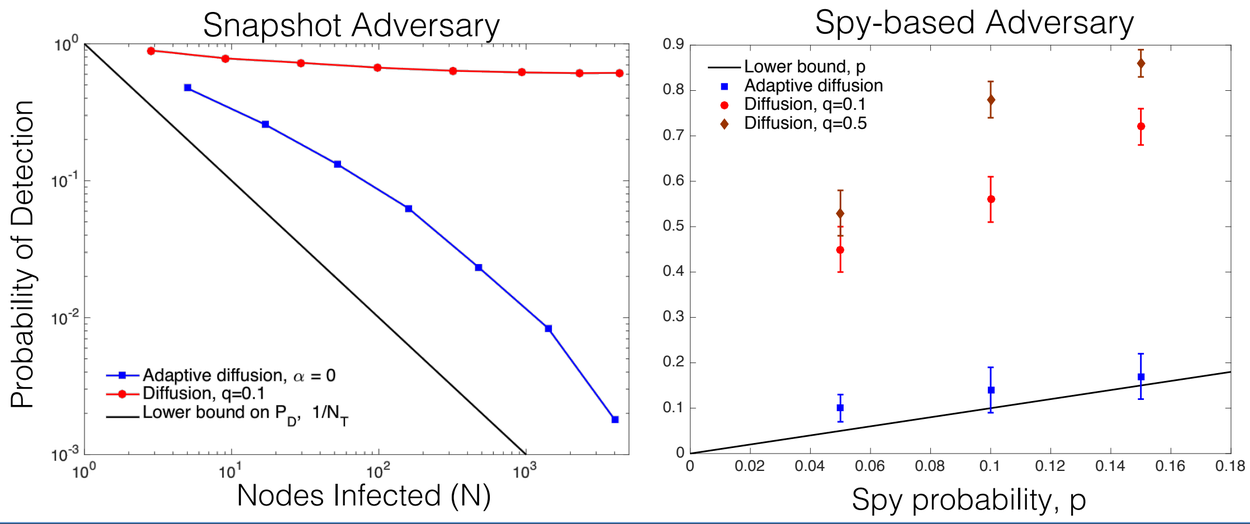
Theorem: On regular trees, adaptive diffusion hides the source in all the leaf nodes and spreads the message exponentially fast. The probability of source detection (P_D) is inversely proportional to the number of noes with the message.

Regular Trees: Spy-based Adversary



Theorem: On regular trees, no scheme can achieve P_D (probability of detection) lower than p. Moreover, P_D under adaptive diffusion is p + o(p).

Adaptive Diffusion on Real Graphs



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

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141

INFORMATIONTRUST INSTITUTE