

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

I hate dealing with this illness!

Makes me feel damaged!

Jason Rezaian's Year of Imprisonment in Iran

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

Russian Activists and Journalists Attacked at

Personal Confessions

Political Activism

FACE BOOK

Can we design social networks that protect user anonymity?

The Problem

Design a distributed messaging protocol that:

- Spreads content quickly over an underlying contact graph
- Prevents an adversary with network oversight from linking messages to their sources

Adversarial Models

Snapshot Adversary

Adversary observes:

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

Spy-based Adversary

Spies with probability p

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.

Spreading Pattern

Snapshot Adversary

Spy-based Adversary

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]

Source Likelihood: Diffusion

high

low

Solution: Break the symmetry

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

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

State

Color: ● ●

Level: $m = 0, 1, \dots$

Source picks one neighbor randomly, and infects it with state ●, $m=1$

Regular Trees: Snapshot Adversary

Snapshot collected

Likelihoods of all nodes

high

low

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 nodes with the message.

Regular Trees: Spy-based Adversary

Metadata collected

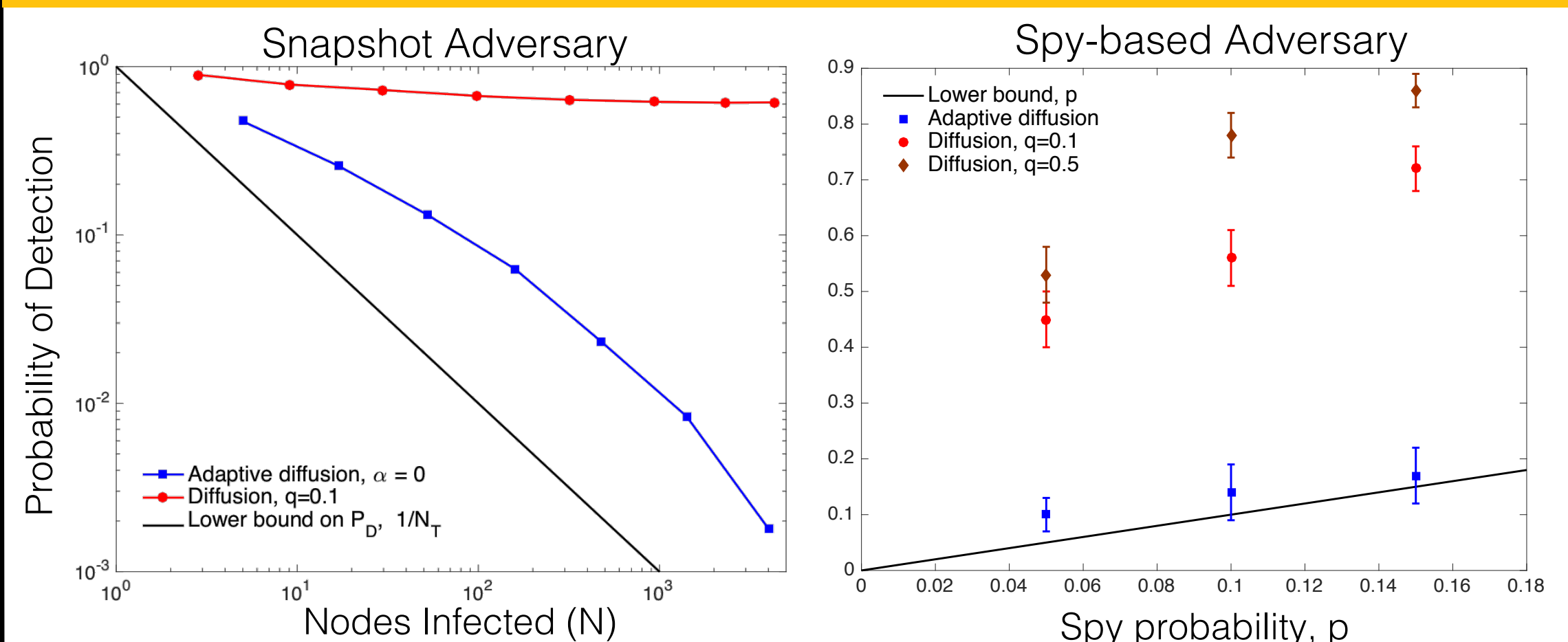
Likelihoods of all nodes

high

low

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



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



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

INFORMATION TRUST
 INSTITUTE