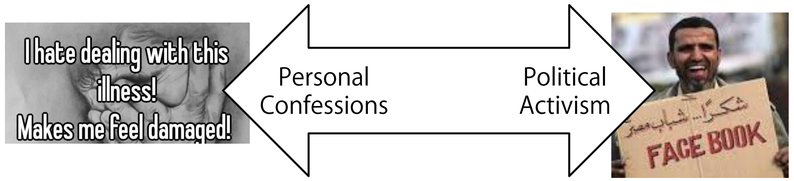
HOW TO SPREAD MESSAGES ANONYMOUSLY: SPY vs SPY

Giulia Fanti and Peter Kairouz
U.C. Berkeley and U.I. Urbana-Champaign

Anonymity matters.



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

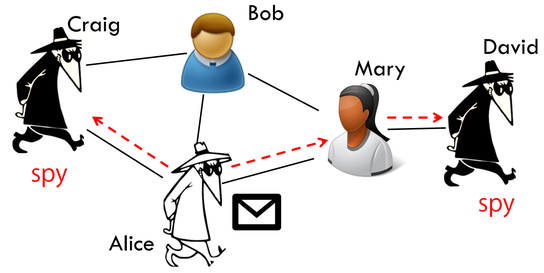
The Problem:

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 Adversary:

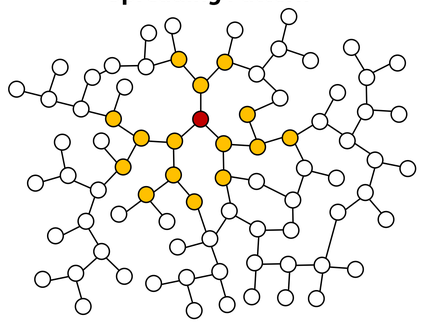


Colluding "spies" share message contents, metadata, and underlying graph structure to infer message authorship.

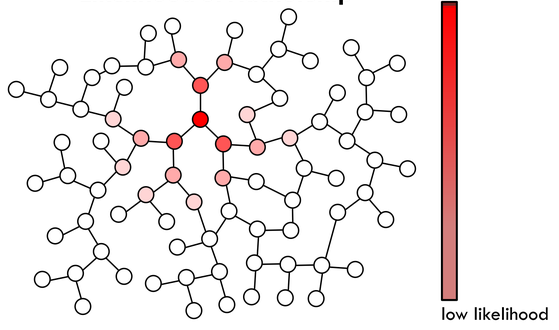
Most social networks spread content symmetrically based on user input.

(user approves message → message gets passed to friends)

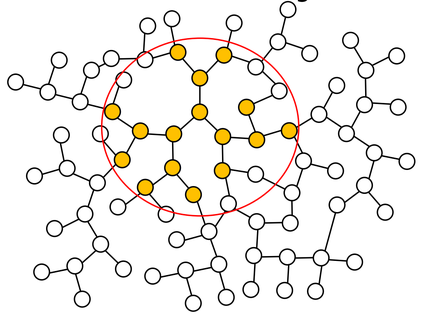
Spreading Pattern



Likelihood of Authorship



Nodes with Message



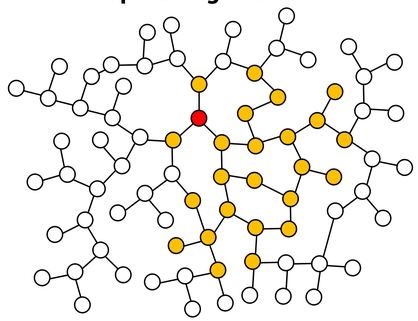
This spreading model is known as the diffusion model. Messages flow in all directions at the same rate. With high probability, diffusion places the true source in the center of the graph. This helps adversaries infer the source. [Shah & Zaman 2011]

Goal: engineer the spread to hide authorship

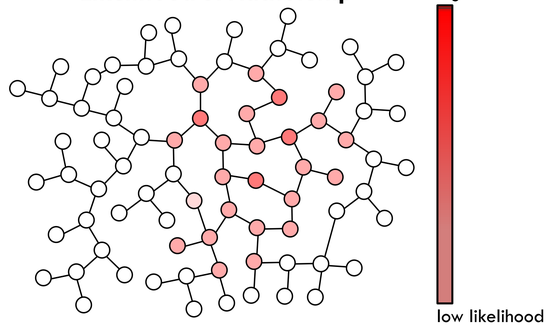
Adaptive diffusion breaks symmetry to provide strong anonymity.

Intuition: carefully adapt the information flow rate and direction

Spreading Pattern



Likelihood of Authorship

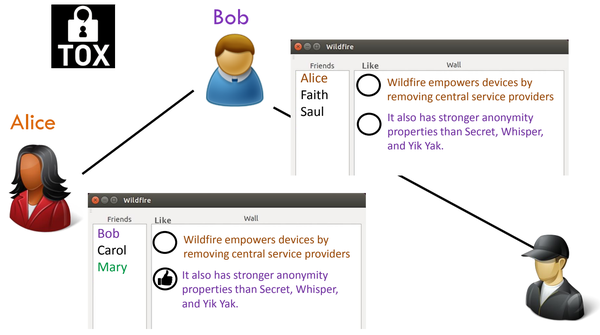


Theorem: On regular trees, adaptive diffusion lets the source hide among N-1 nodes and spreads the message exponentially quickly.

Simulation: On social graphs and irregular trees, adaptive diffusion hides the source among O(N) nodes and spreads exponentially quickly.

Provable anonymity guarantees

Wildfire is an anonymous messaging app powered by adaptive diffusion.



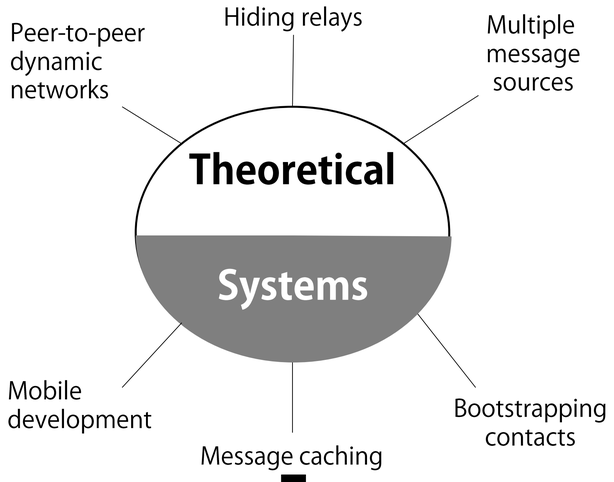
Fully-distributed implementation

Secure message transmission via Tox

Device-centric architecture

Code at github.com/cpx0rpc/wildfire.git

Remaining challenges



Wildfire Release

Advised by Professors Sewoong Oh, Kannan Ramchandran, and Pramod Viswanath