Metadata-Conscious Anonymous Messaging

Giulia Fanti, Peter Kairouz, Sewoong Oh,
Kannan Ramchandran, and Pramod Viswanath

Anonymity matters

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

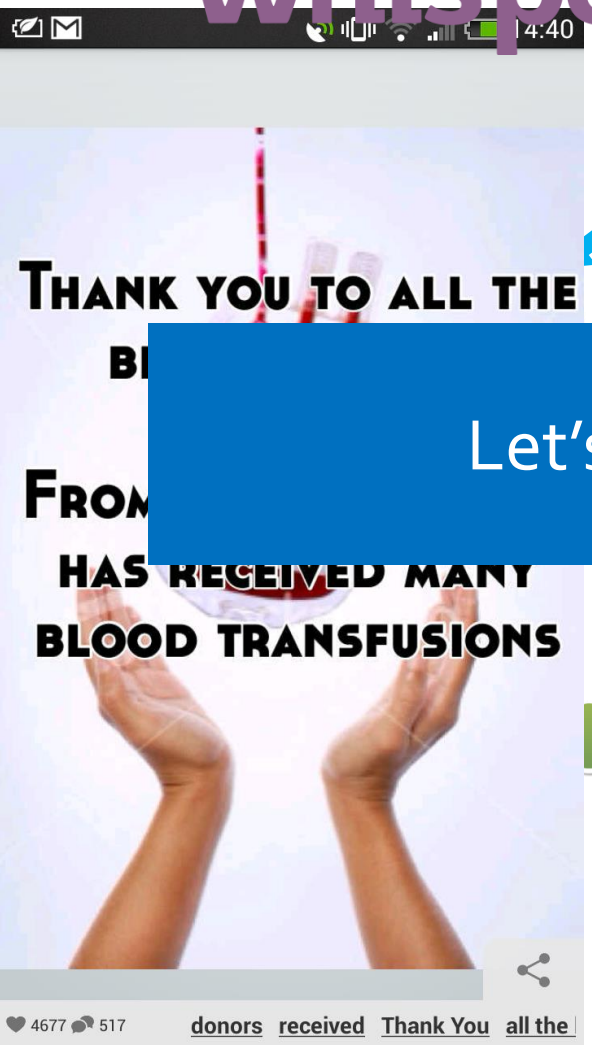
Related

Syria blocks Facebook in Internet crackdown

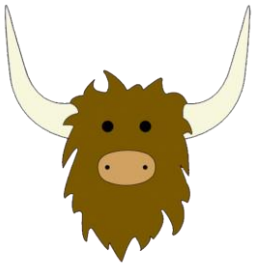
DAMASCUS | BY KHALED YACOUB OWEIS

Existing anonymous messaging apps

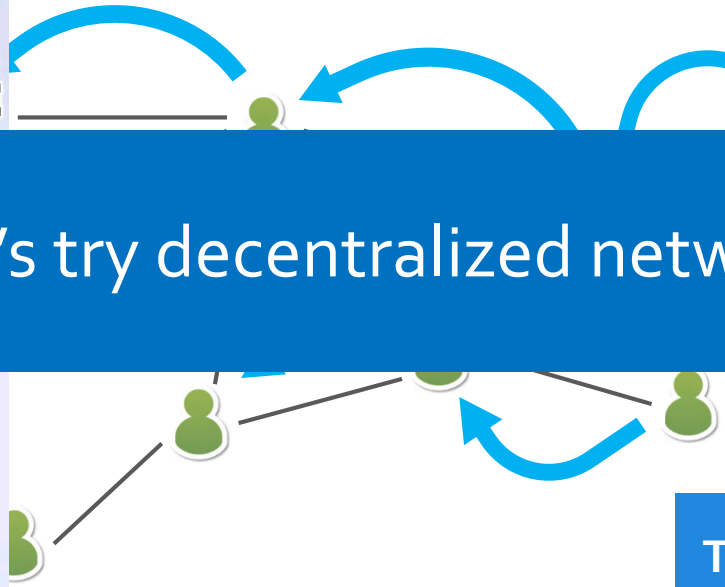
whisper



secret



Yik Yak

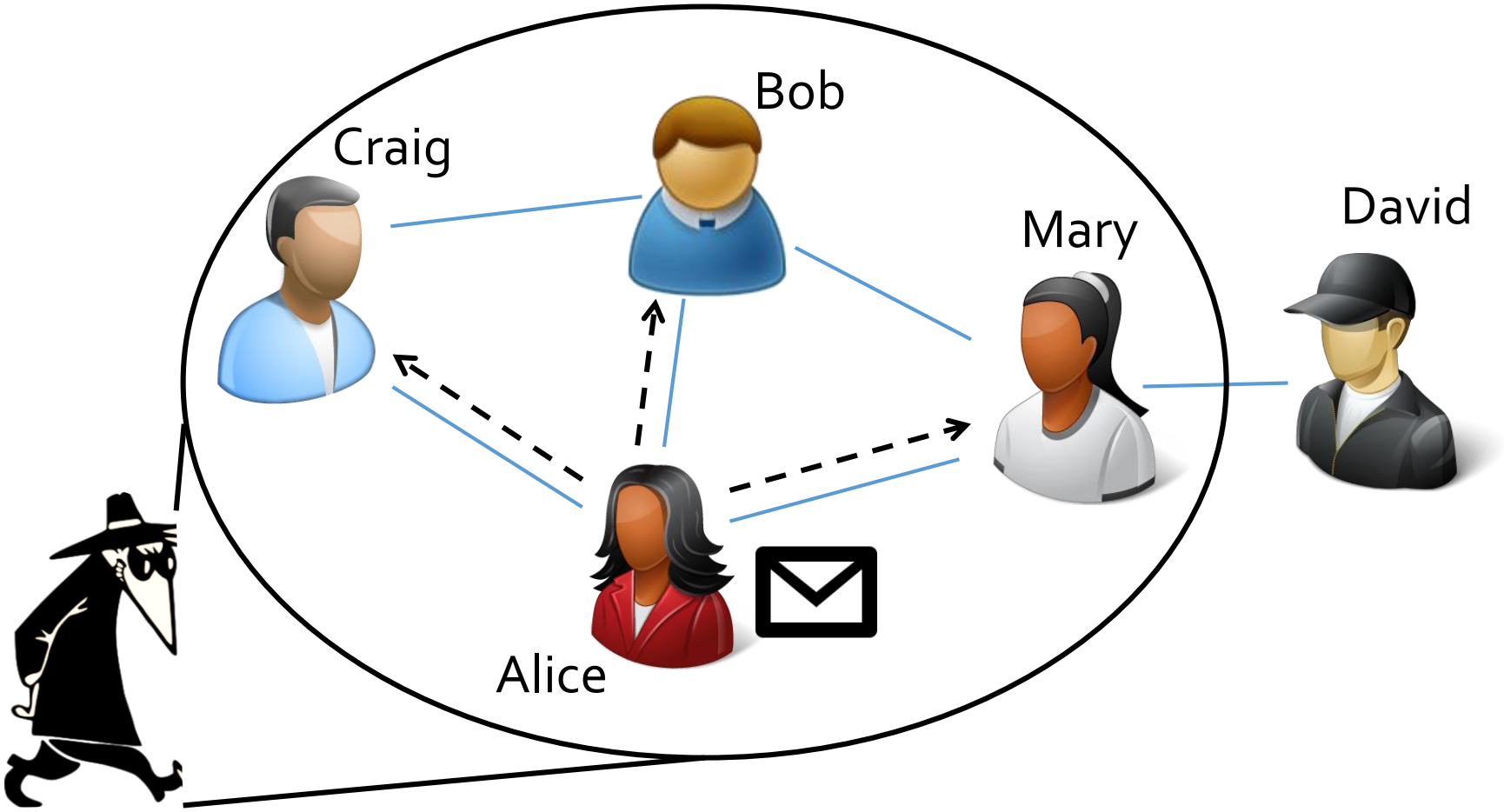


Let's try decentralized networks!

Alice

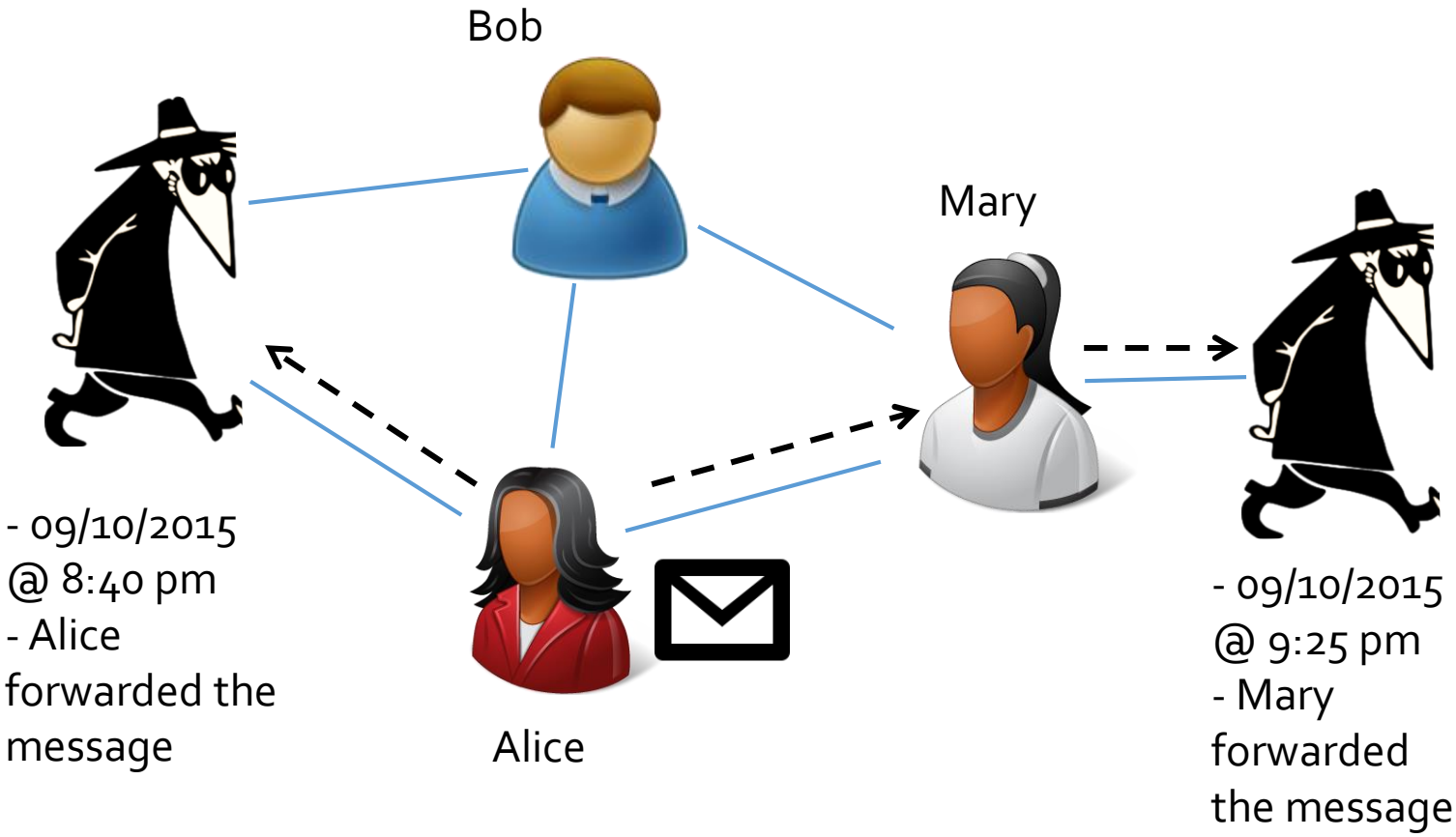
Thank you to all the blood donors…

Snapshot Adversary



adversary can figure out **who got the message**

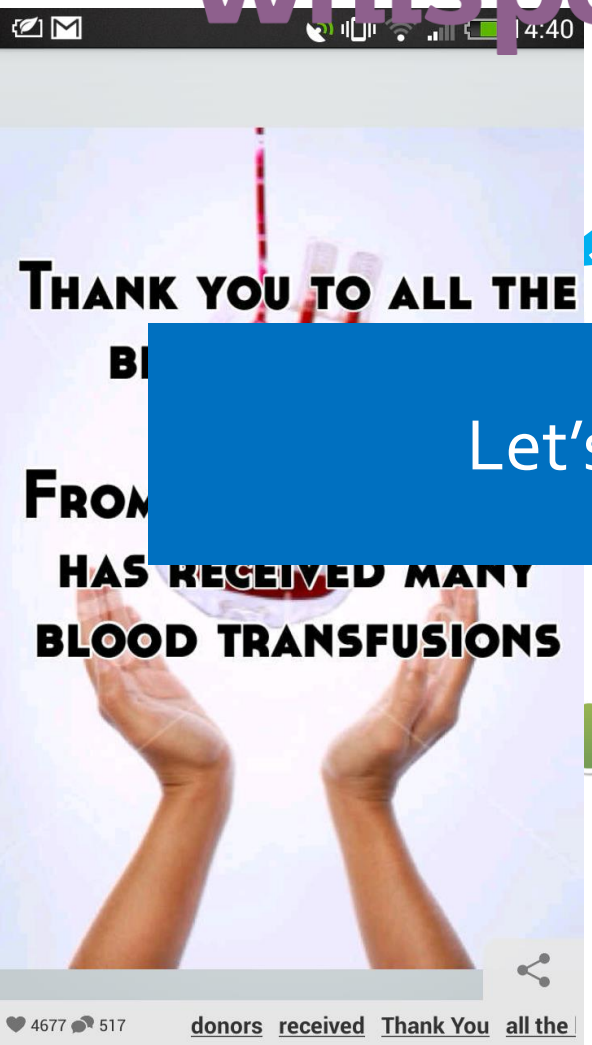
Spy-based adversary



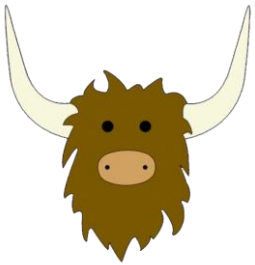
adversary can **collect timing information**

Existing anonymous messaging apps

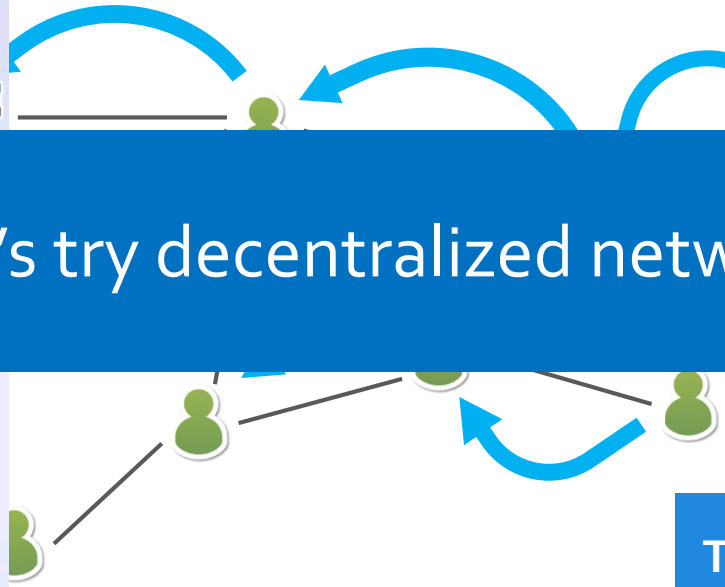
whisper



secret



Yik Yak

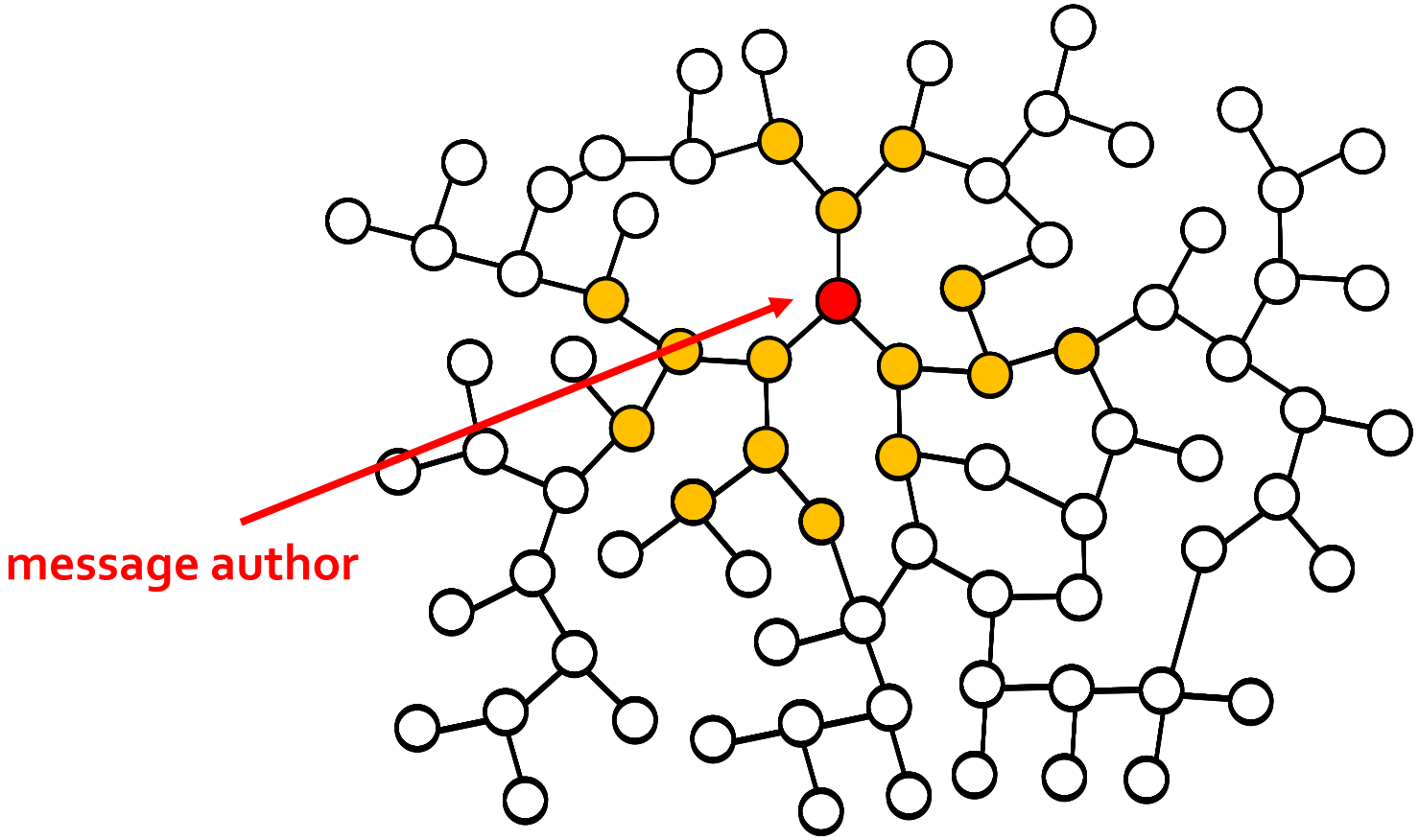


Let's try decentralized networks!

Alice

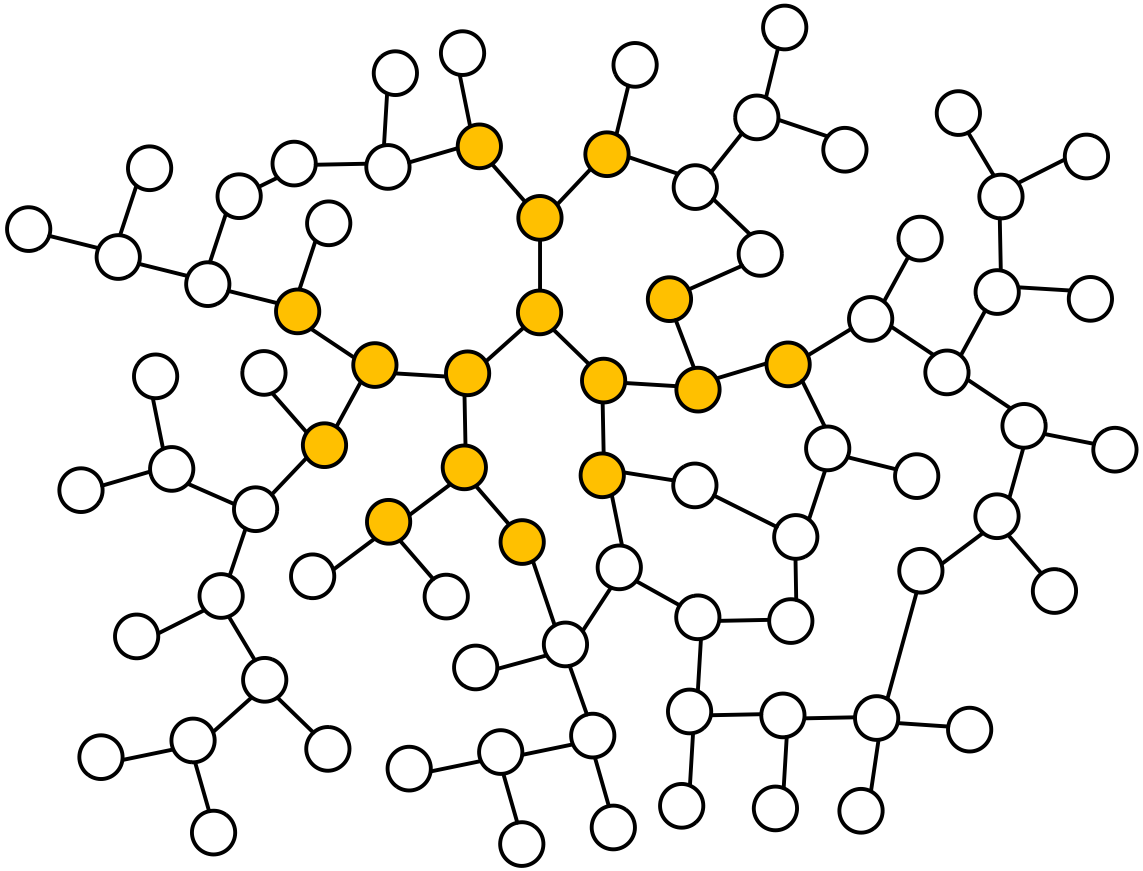
Thank you to all the blood donors…

Information flow in social networks



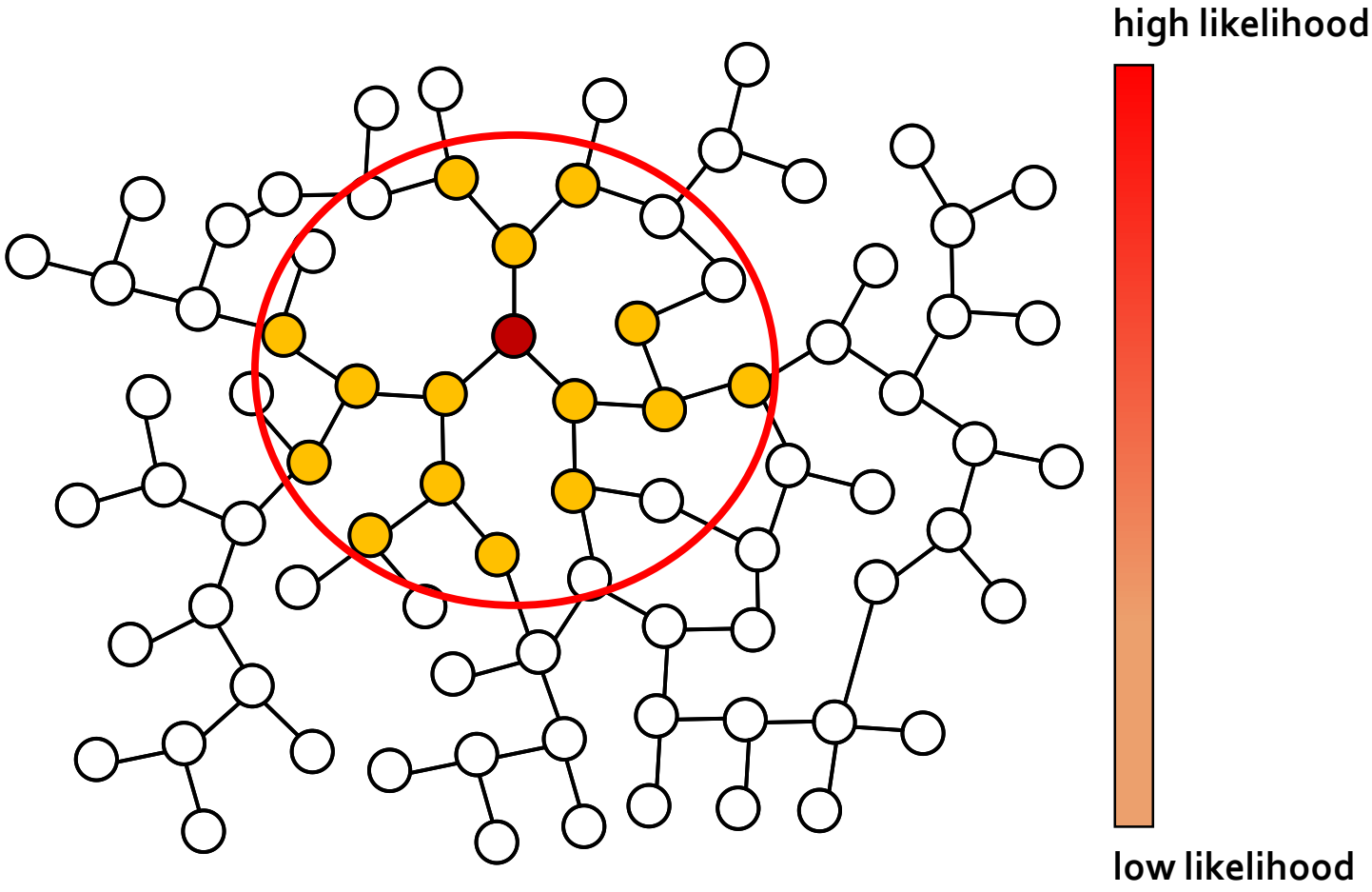
information spreads at the **same rate** in **all direction**

Can you find the source?



[*Shah et al. 2011, Zhu et al. 2013*]

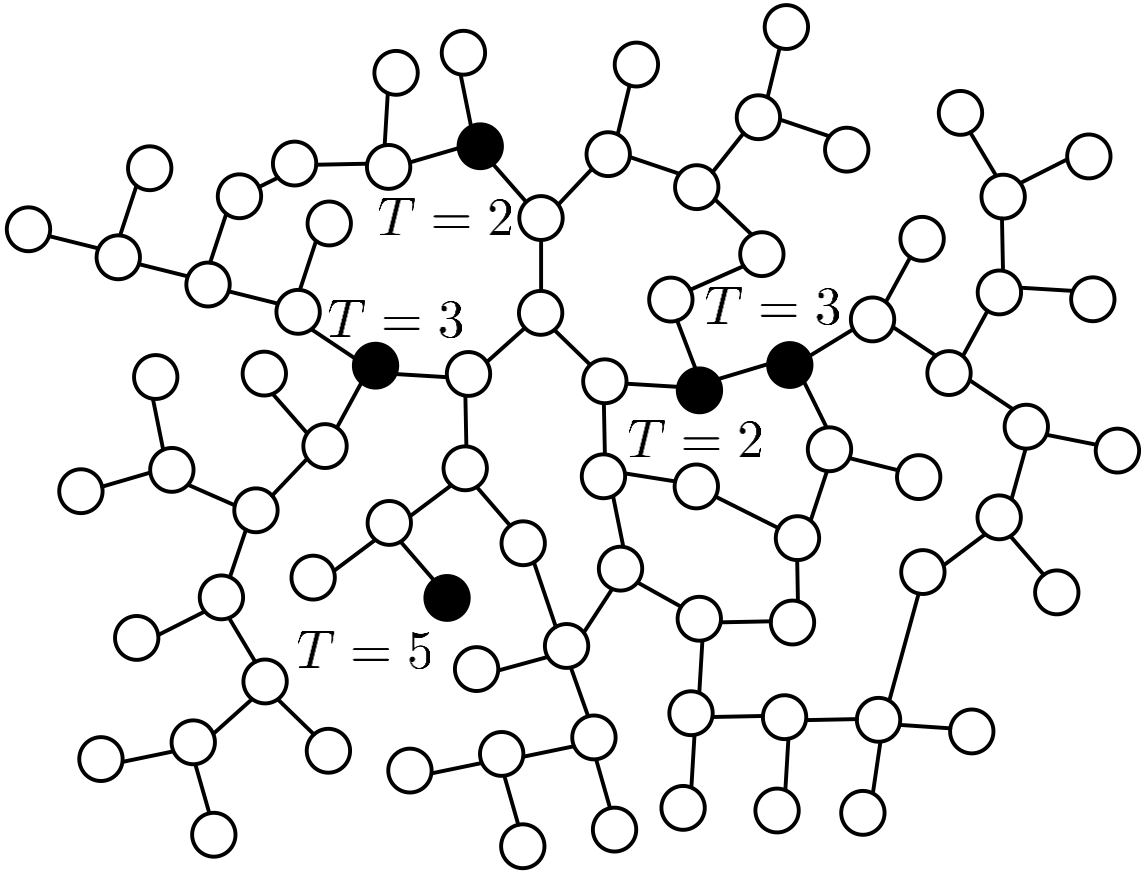
Concentration around the center



diffusion spreading = **de-anonymization**

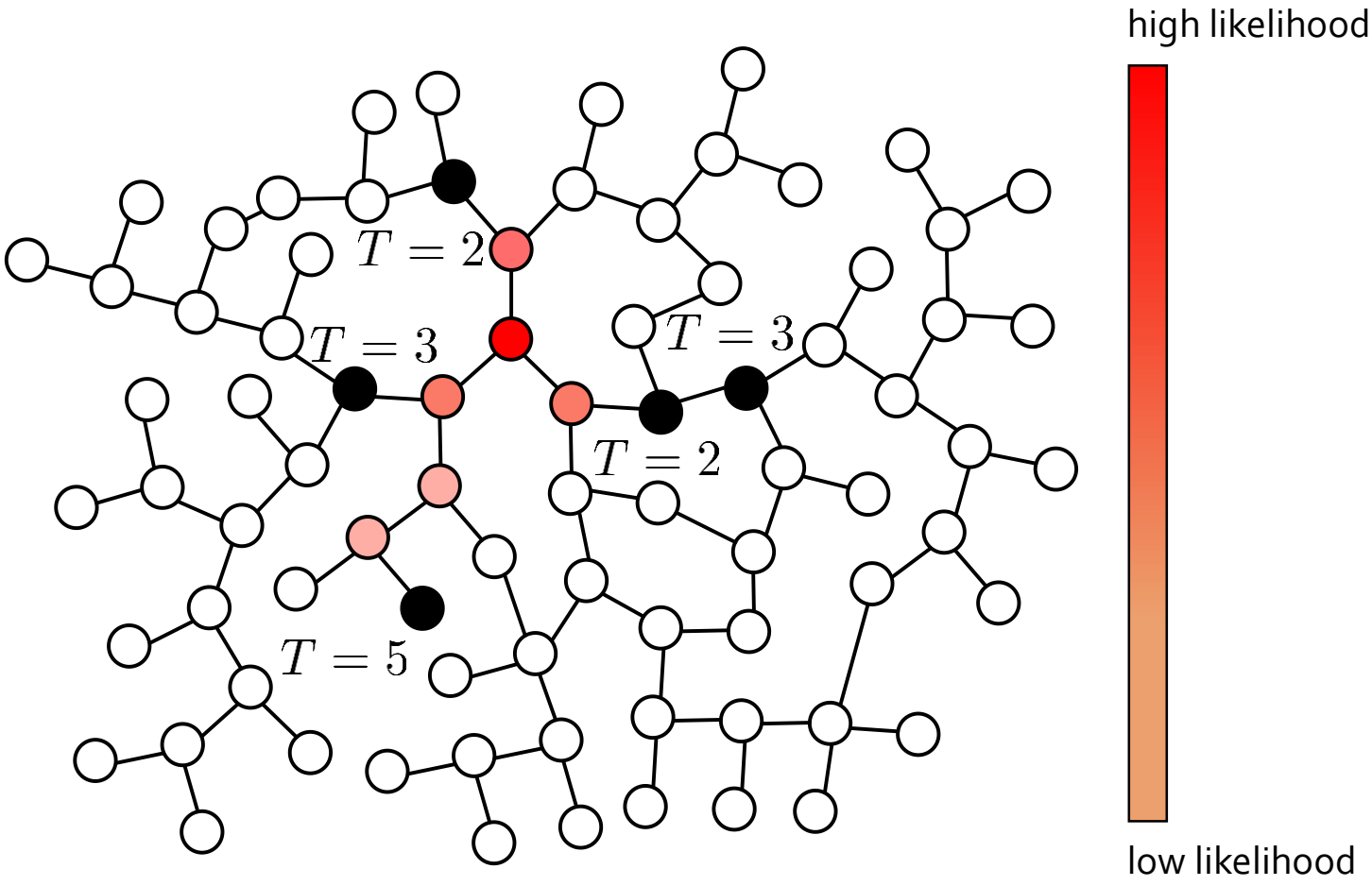
[*Shah et al. 2011, Zhu et al. 2013*]

Can you find the source?



[*Pinto et al. 2012*]

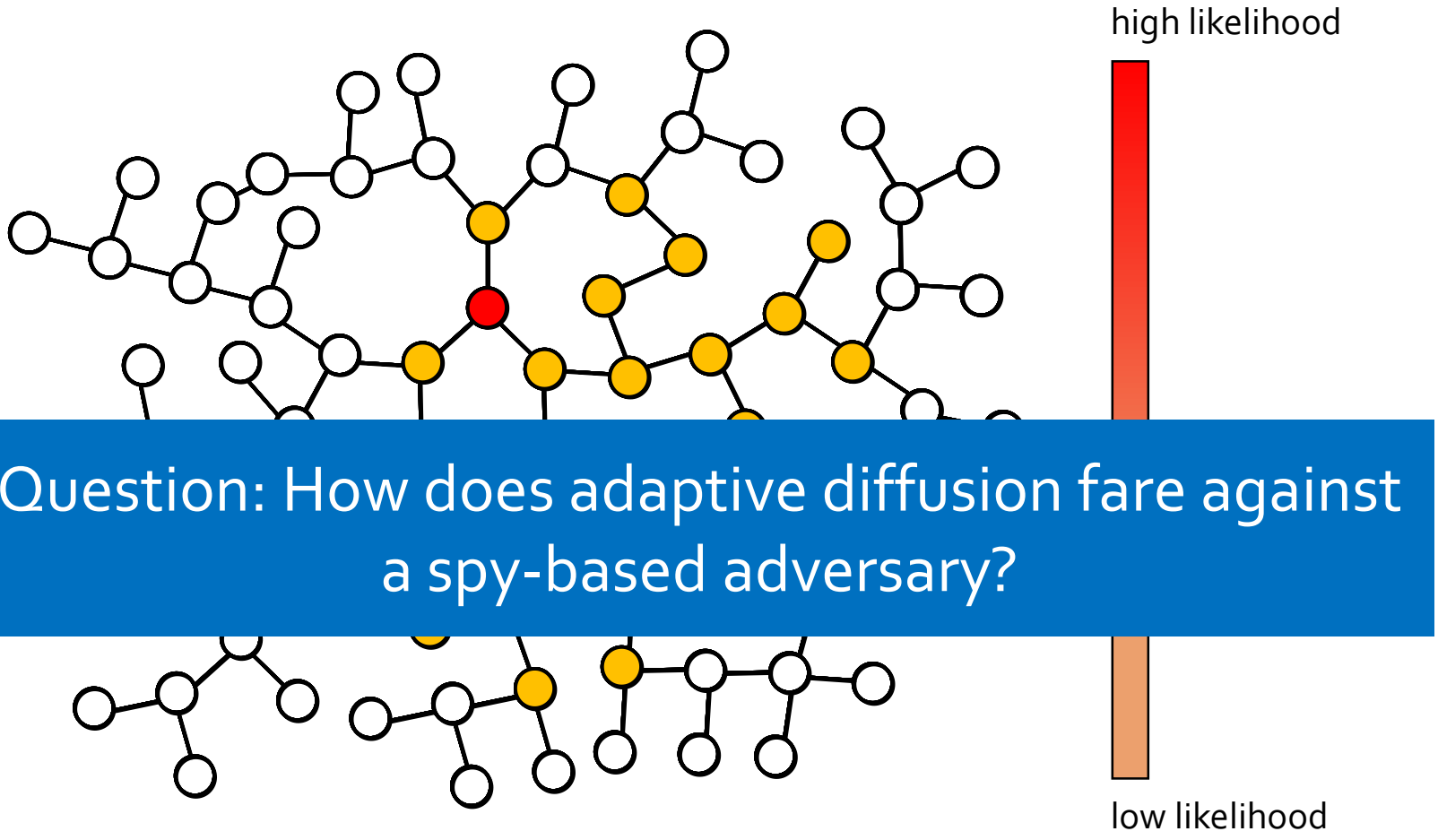
Maximum likelihood detection



diffusion spreading = **de-anonymization**

[*Pinto et al. 2012*]

Prior work: adaptive diffusion

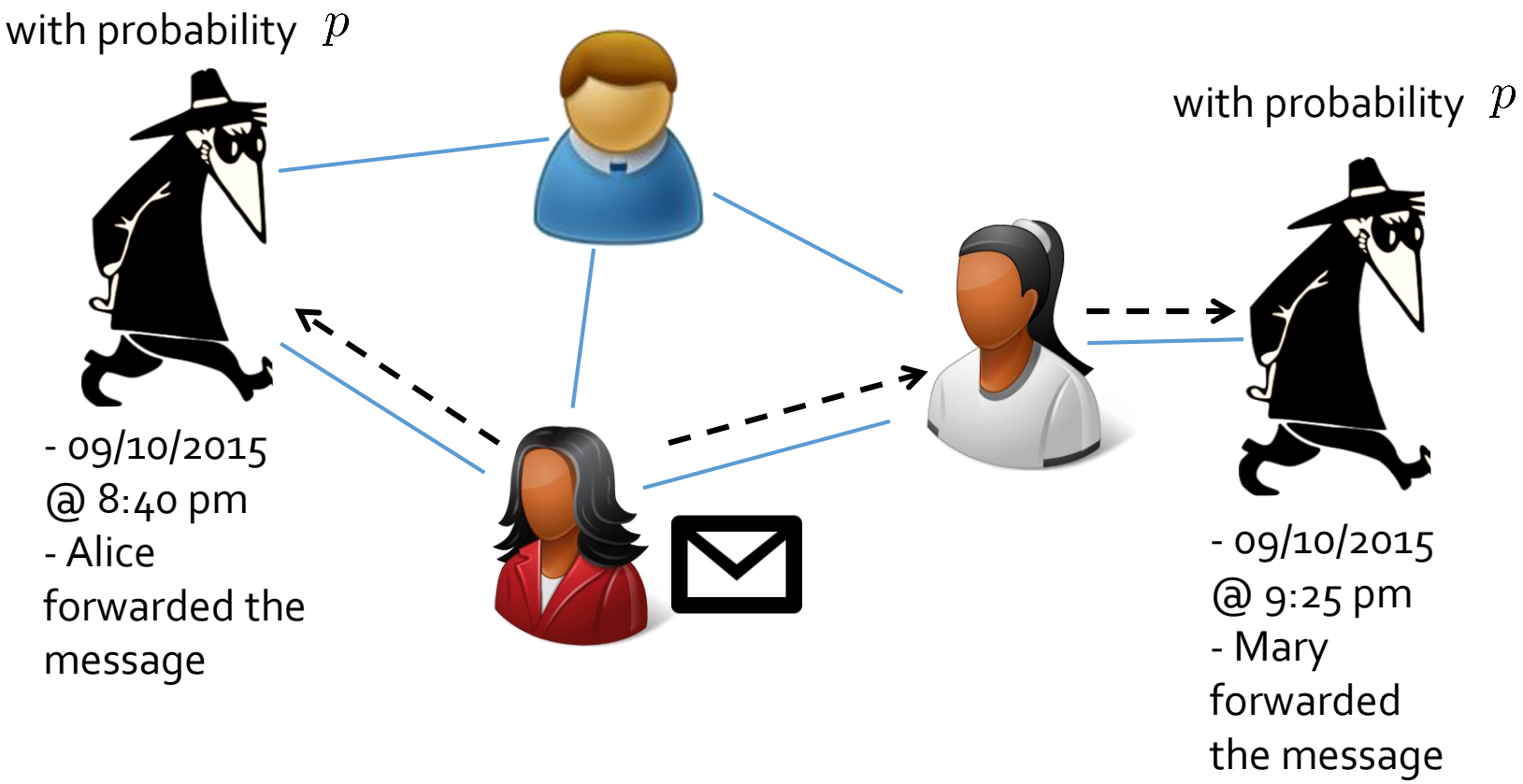


Question: How does adaptive diffusion fare against a spy-based adversary?

provable anonymity guarantees—*for a snapshot adversary*

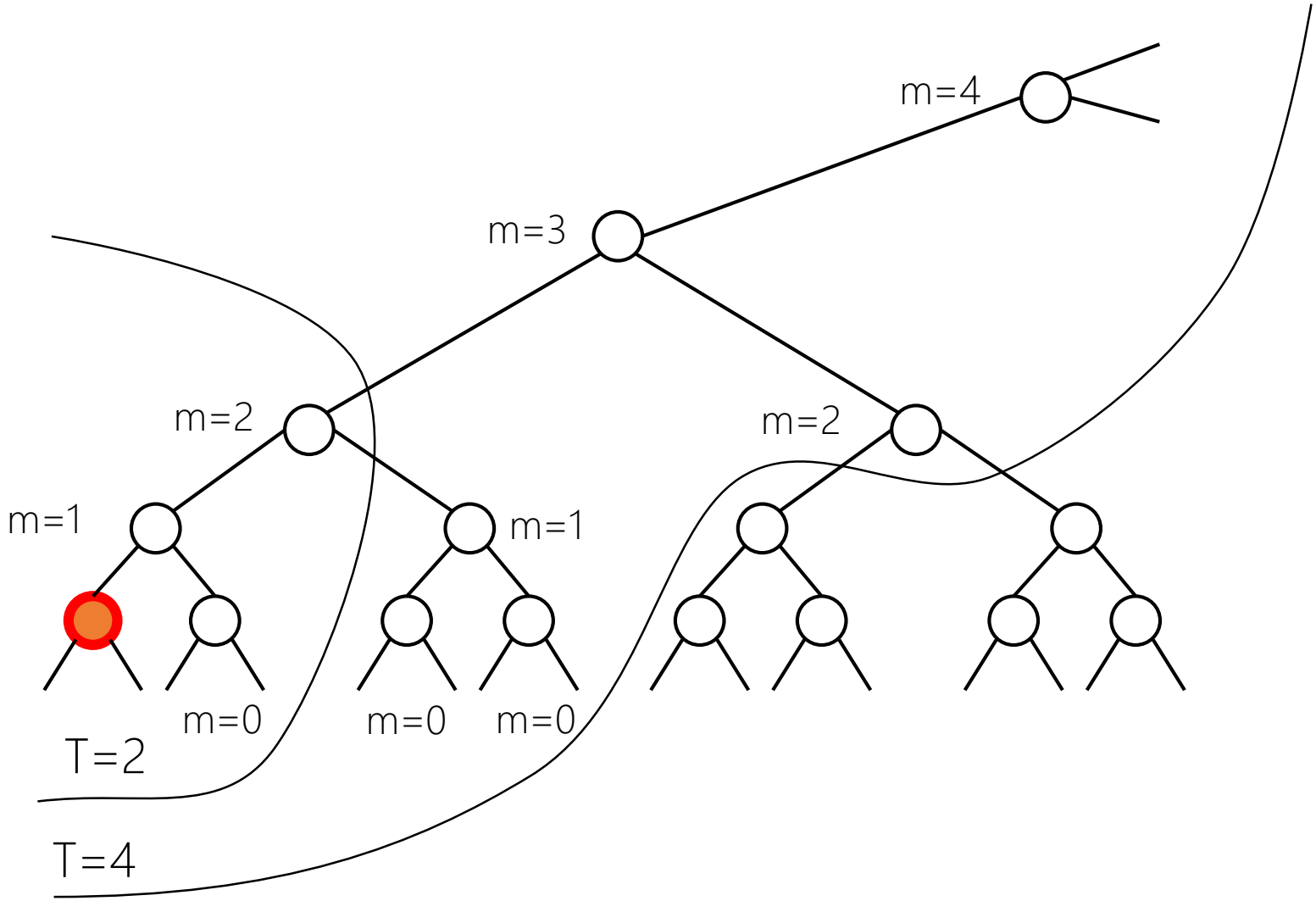
[*Spy vs. Spy: Rumor Source Obfuscation*, ACM SIGMETRICS 2015]

Our objective

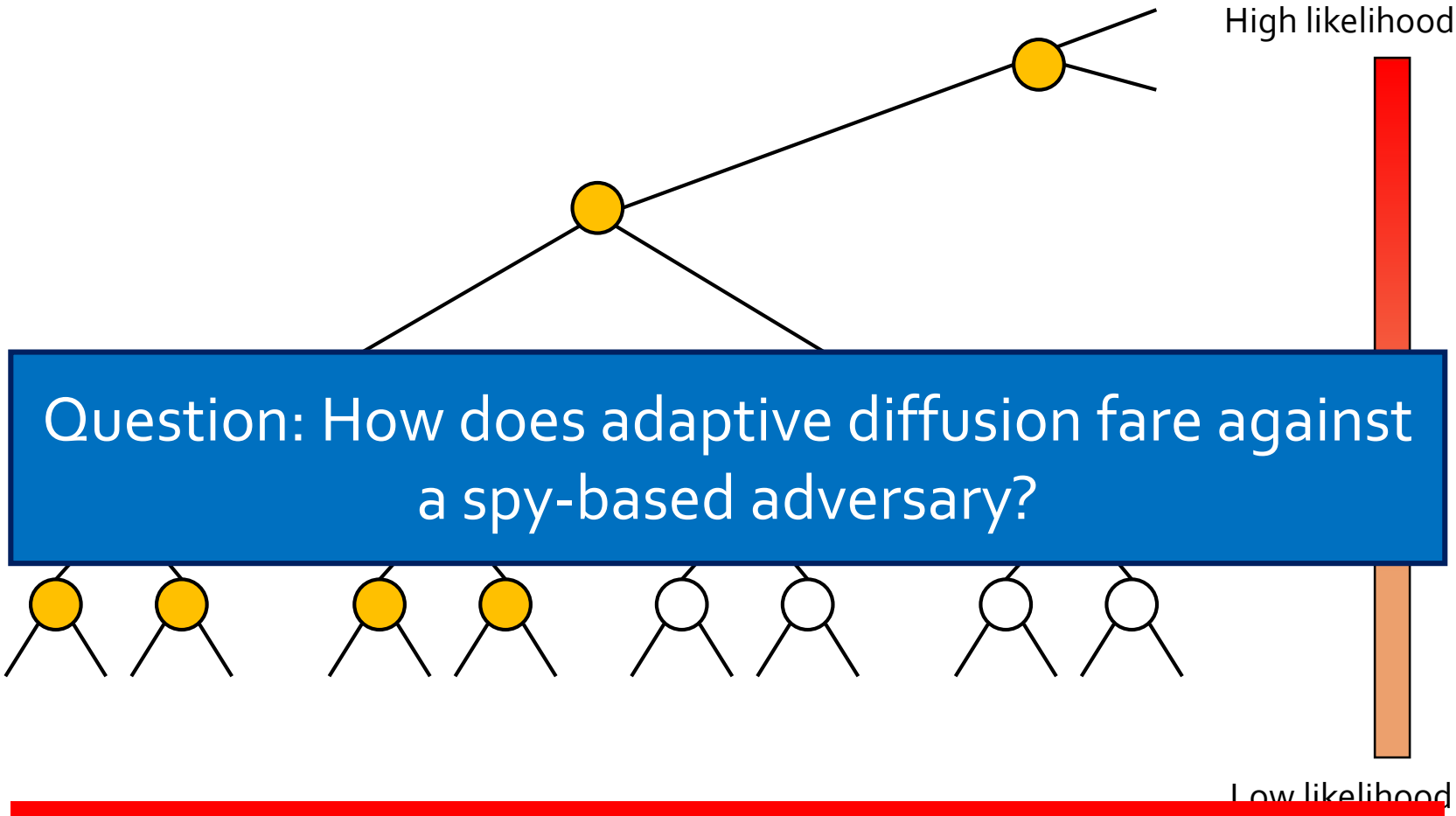


engineer the spread to hide authorship

Adaptive diffusion over d-regular trees



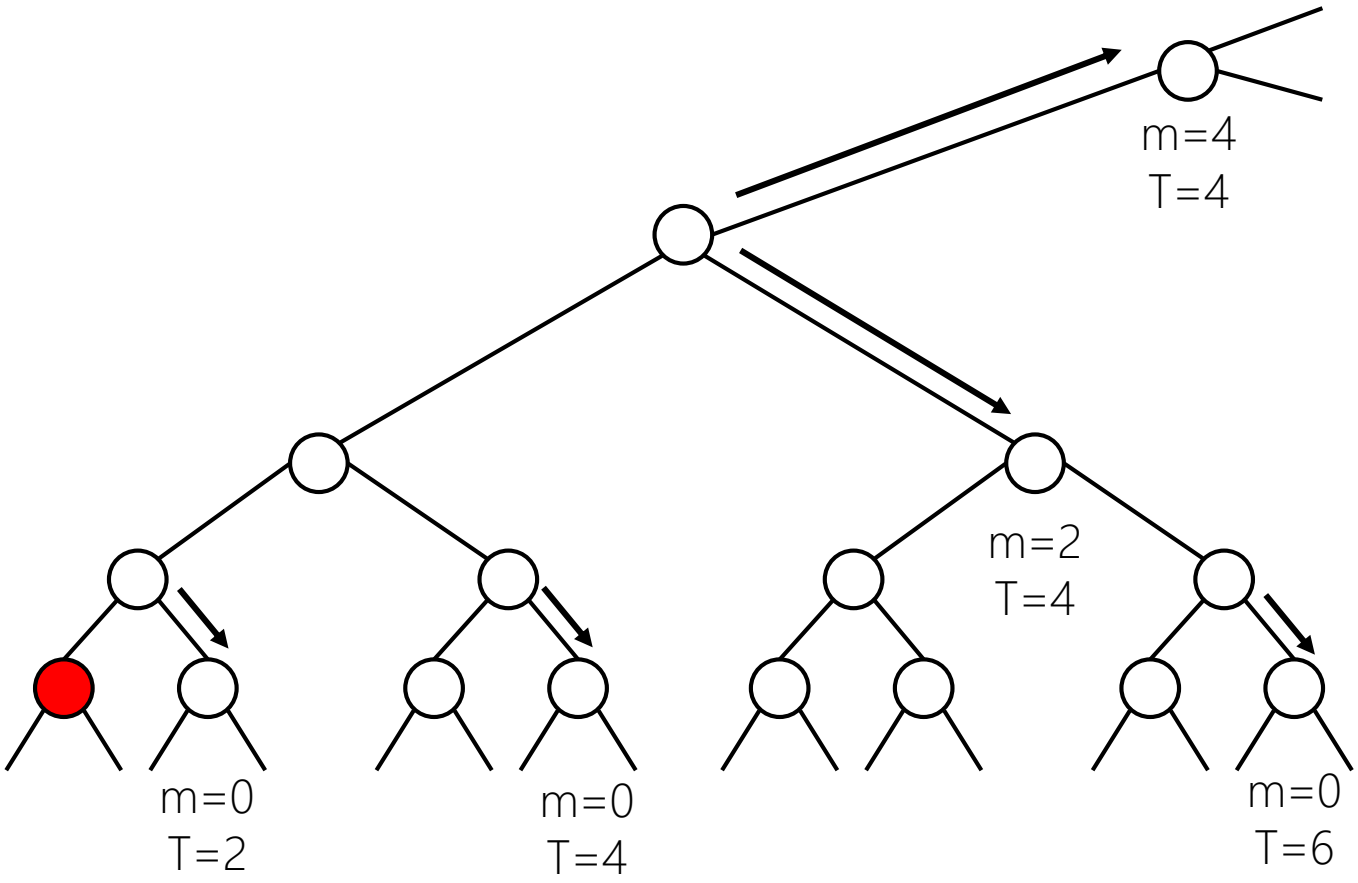
Snapshot adversary



Question: How does adaptive diffusion fare against a spy-based adversary?

THEOREM: Probability of detection $= O(\frac{1}{N})$

Spy-based adversary



Main Theorem

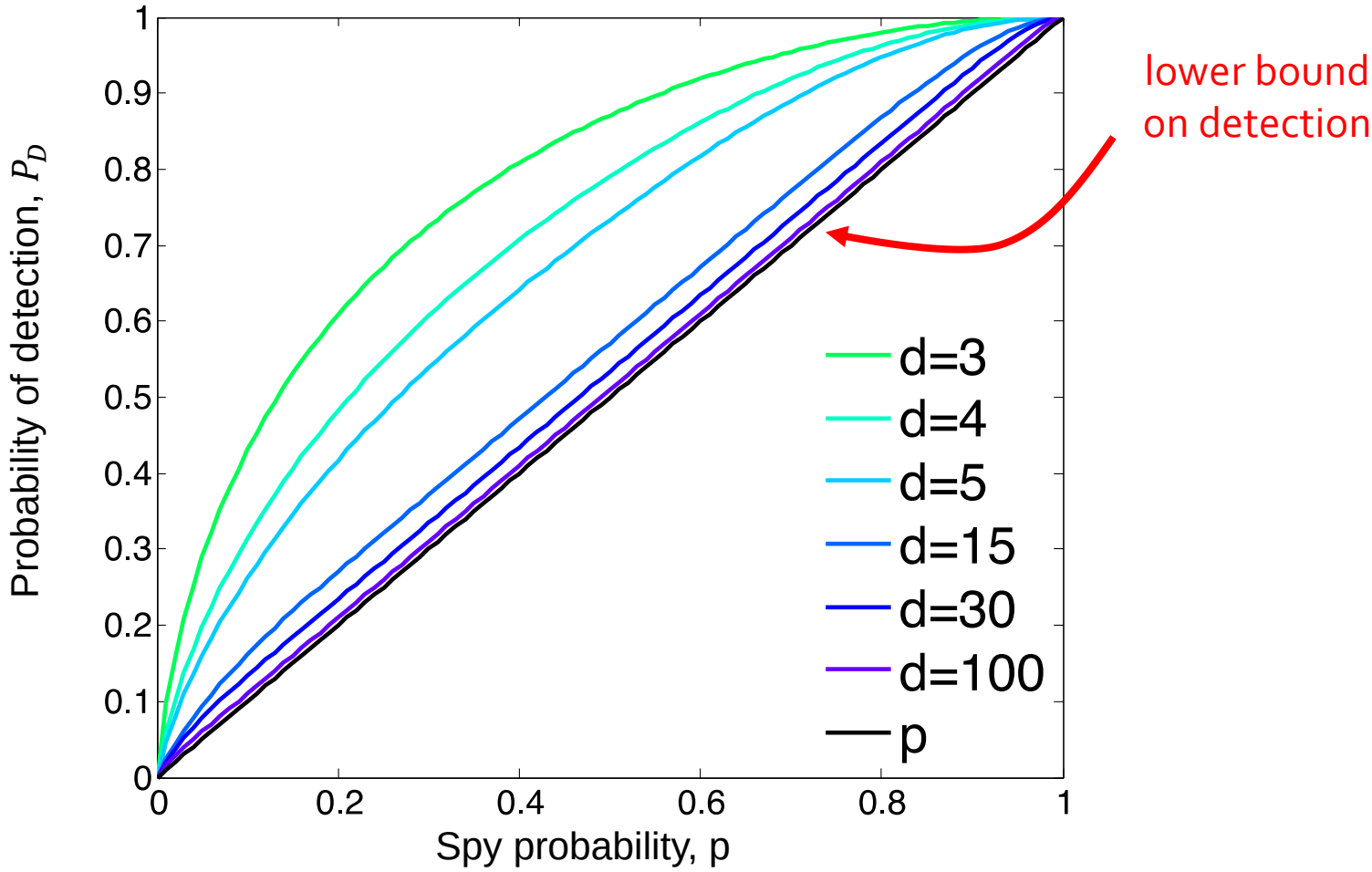
1. For any network and any protocol that passes the message to at least once node, we have that:

$$\min_{\text{protocol}} \max_{\hat{v}} \mathbb{P}(\hat{v} = v^*) \geq p\,.$$

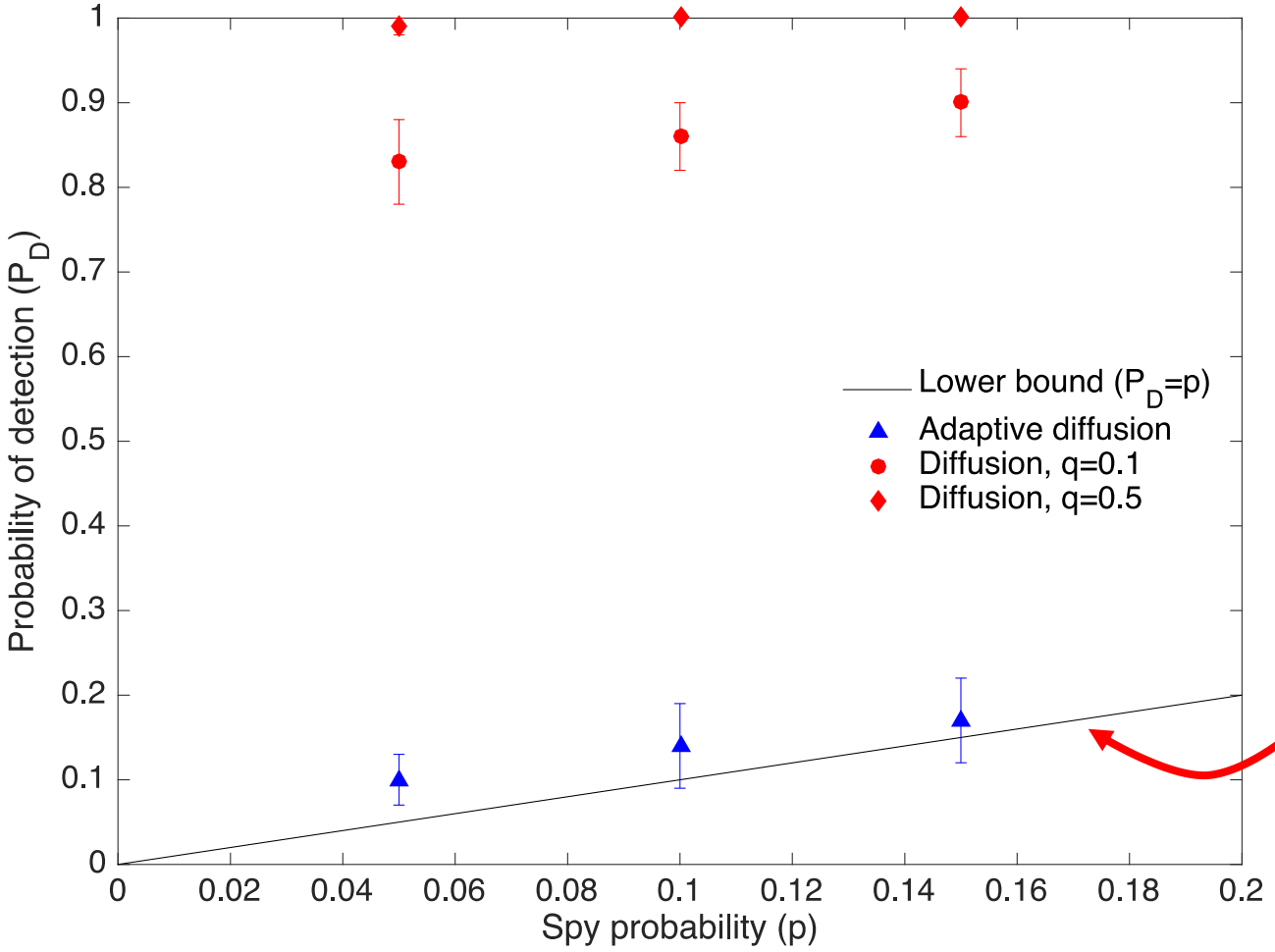
2. On d-regular trees, the probability of detection under adaptive diffusion is given by

$$\mathbb{P}(\hat{v}_{\mathrm{ML}} = v^*) = p + o(p).$$

Results on d-regular trees



Facebook graph



Acknowledgments

Giulia Fanti

Sewoong Oh

Kannan Ramchandran

Pramod Viswanath