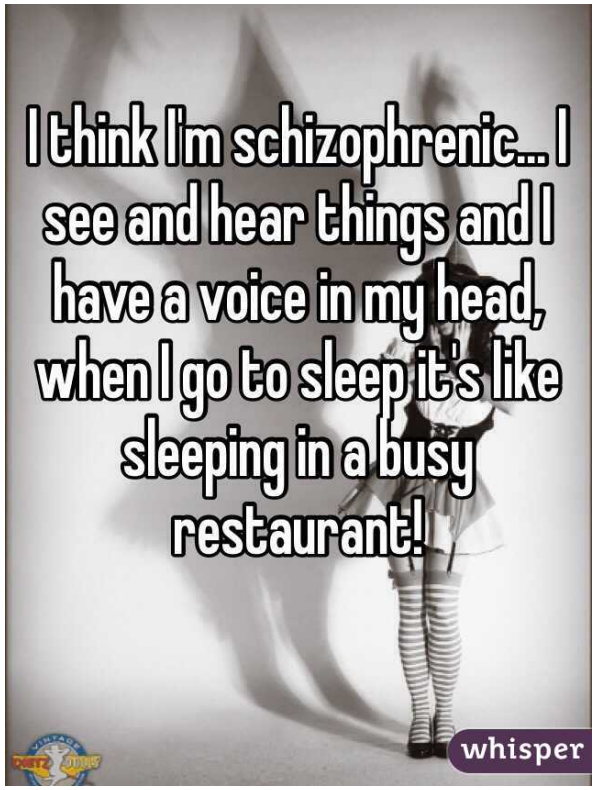
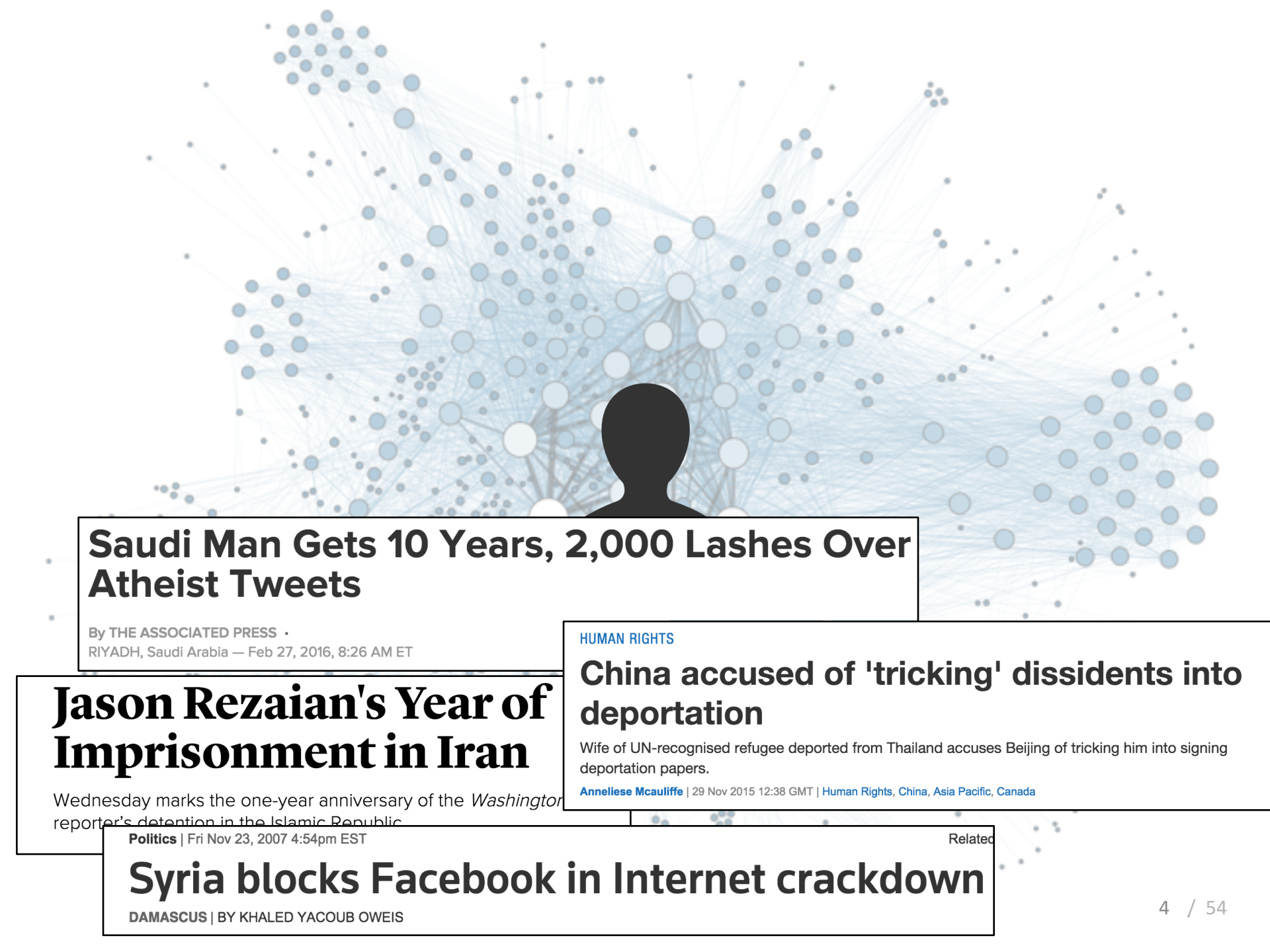
SPY VS. SPY:
ANONYMOUS MESSAGING OVER NETWORKS

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

Some people have important, sensitive things to say.

Others have less important, sensitive things to say.





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

HUMAN RIGHTS

China accused of 'tricking' dissidents into deportation

Wife of UN-recognised refugee deported from Thailand accuses Beijing of tricking him into signing deportation papers.

Anneliese Mcauliffe | 29 Nov 2015 12:38 GMT | Human Rights, China, Asia Pacific, Canada

Jason Rezaian's Year of Imprisonment in Iran

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

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

Related

Syria blocks Facebook in Internet crackdown

DAMASCUS | BY KHALED YACOUB OWEIS

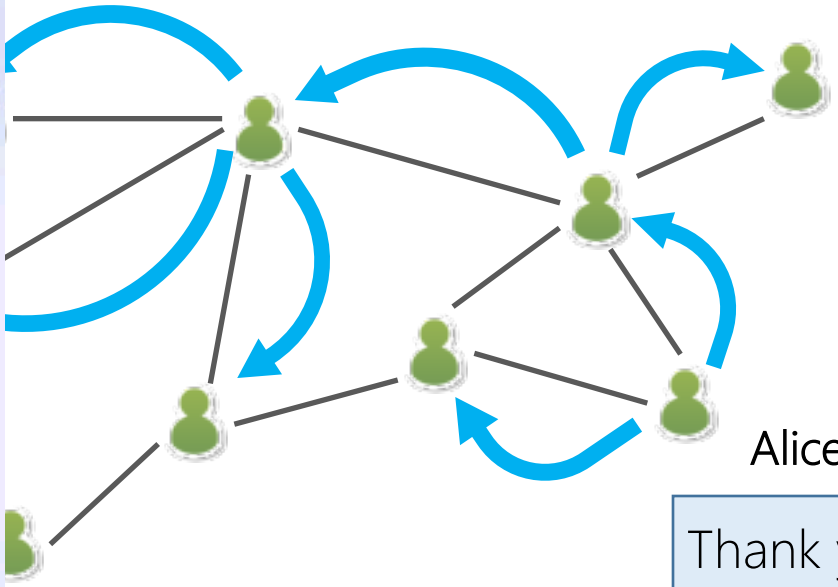
Privacy can help.

Existing anonymous messaging apps

whisper

secret

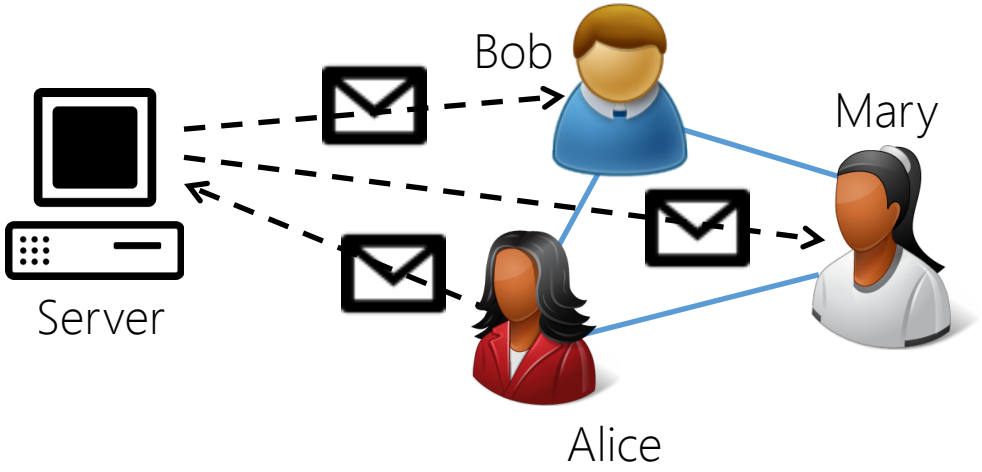
Yik Yak



Alice

Thank you to all the blood donors…

Existing anonymous messaging apps



Centralized networks are not truly anonymous!

Compromises in anonymity

Avoid trusting servers to "do the right thing"

OBJECTIVE

Design a distributed messaging mechanism that:

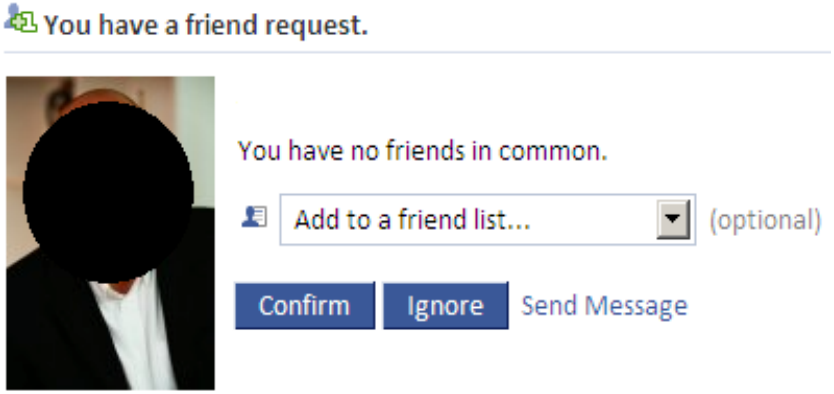
(a) spreads content fast

(b) gives authors anonymity

What can adversaries do?

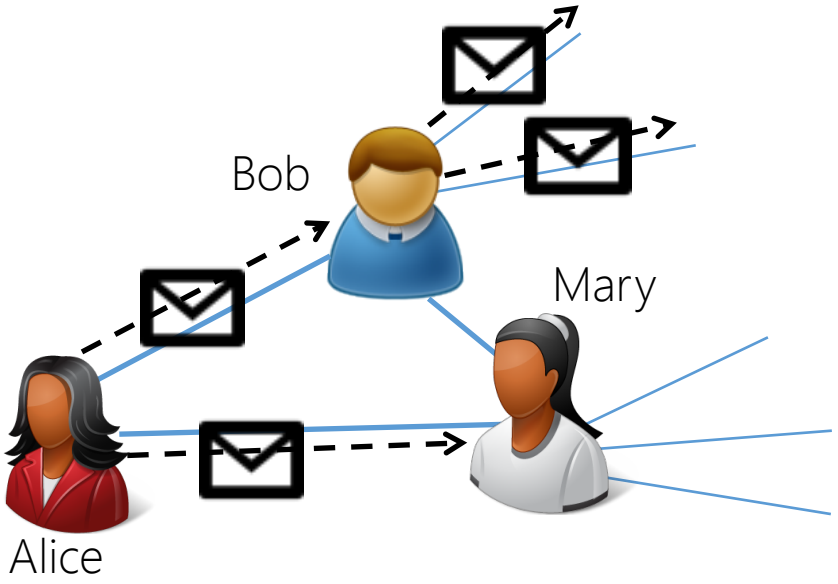
SNAPSHOT

SPY-BASED



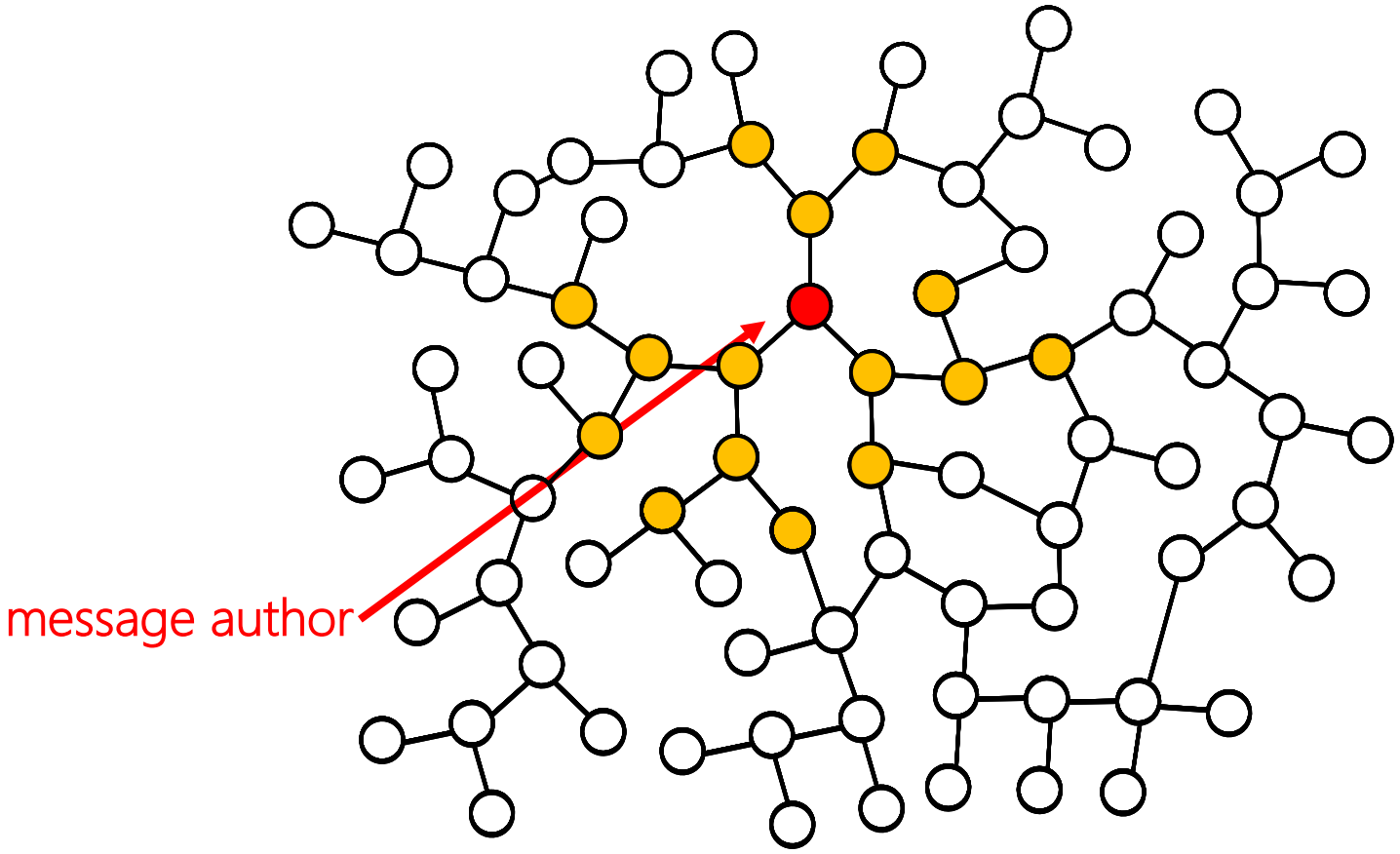
FULL OVERSIGHT

First-Order Solution: Distributed Messaging



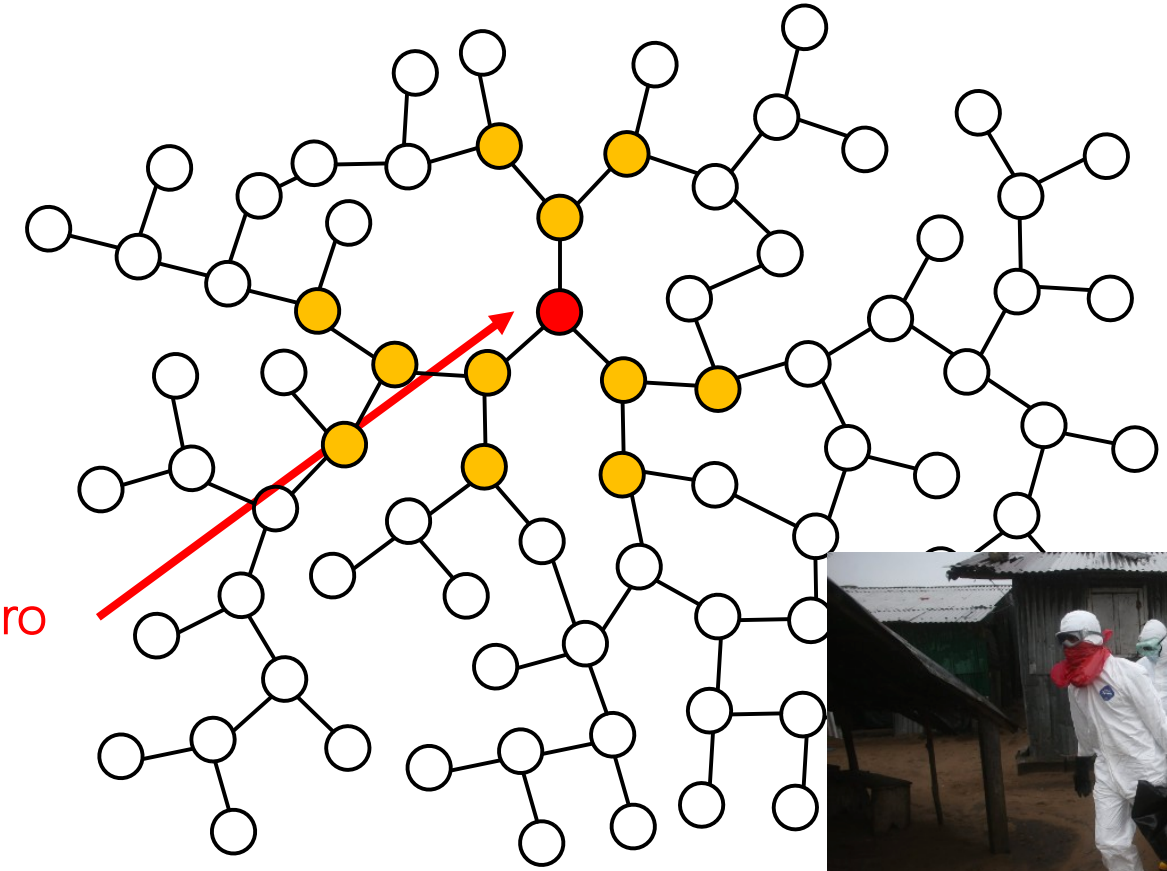
Snapshot and spy-based adversaries
can still infer the source!

Information flow in social networks



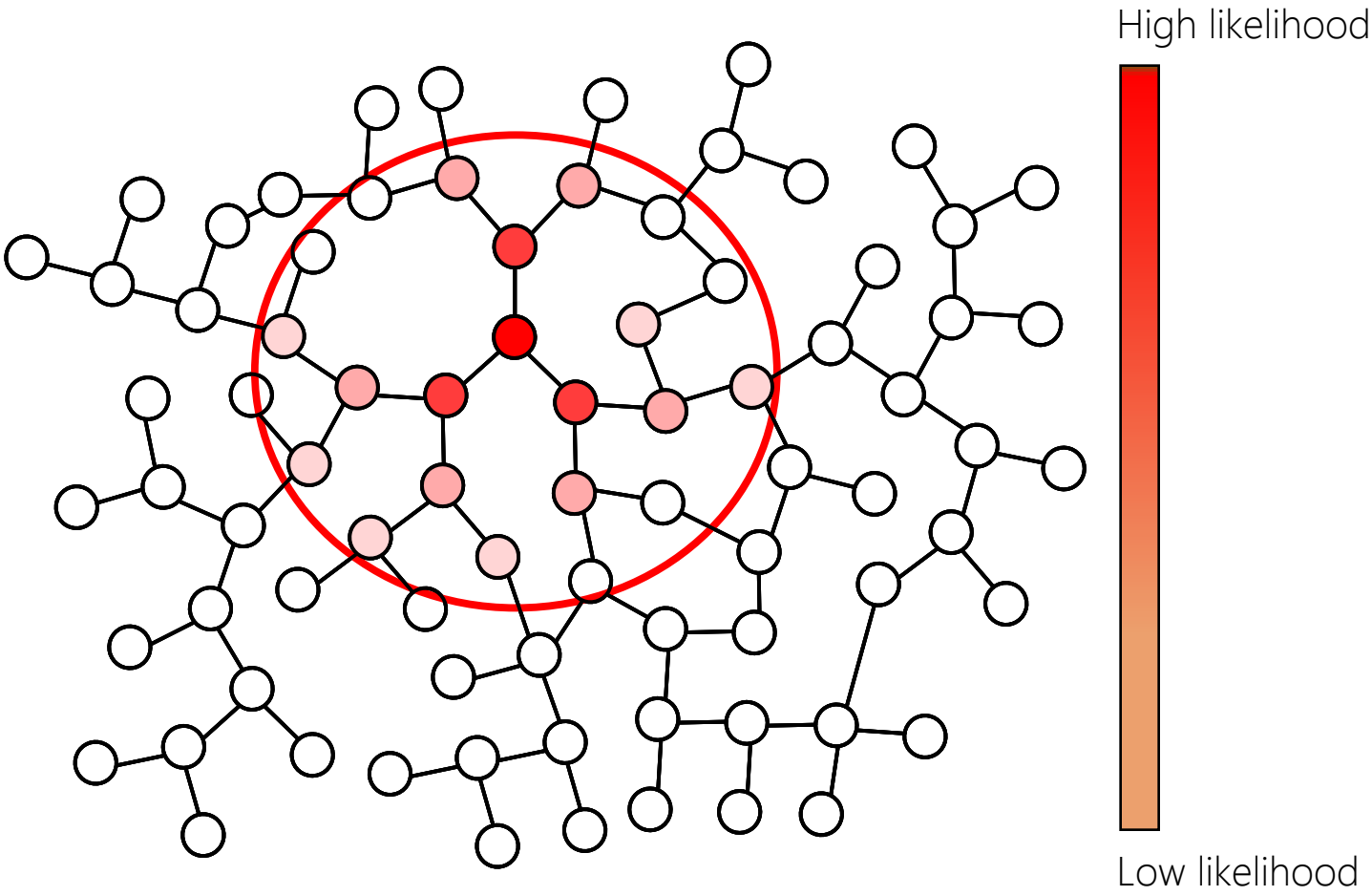
Diffusion has statistical symmetry

Disease flow in populations



[Shah and Zaman 2011, Pinto *et al.* 2012, Zhu *et al.* 2013]

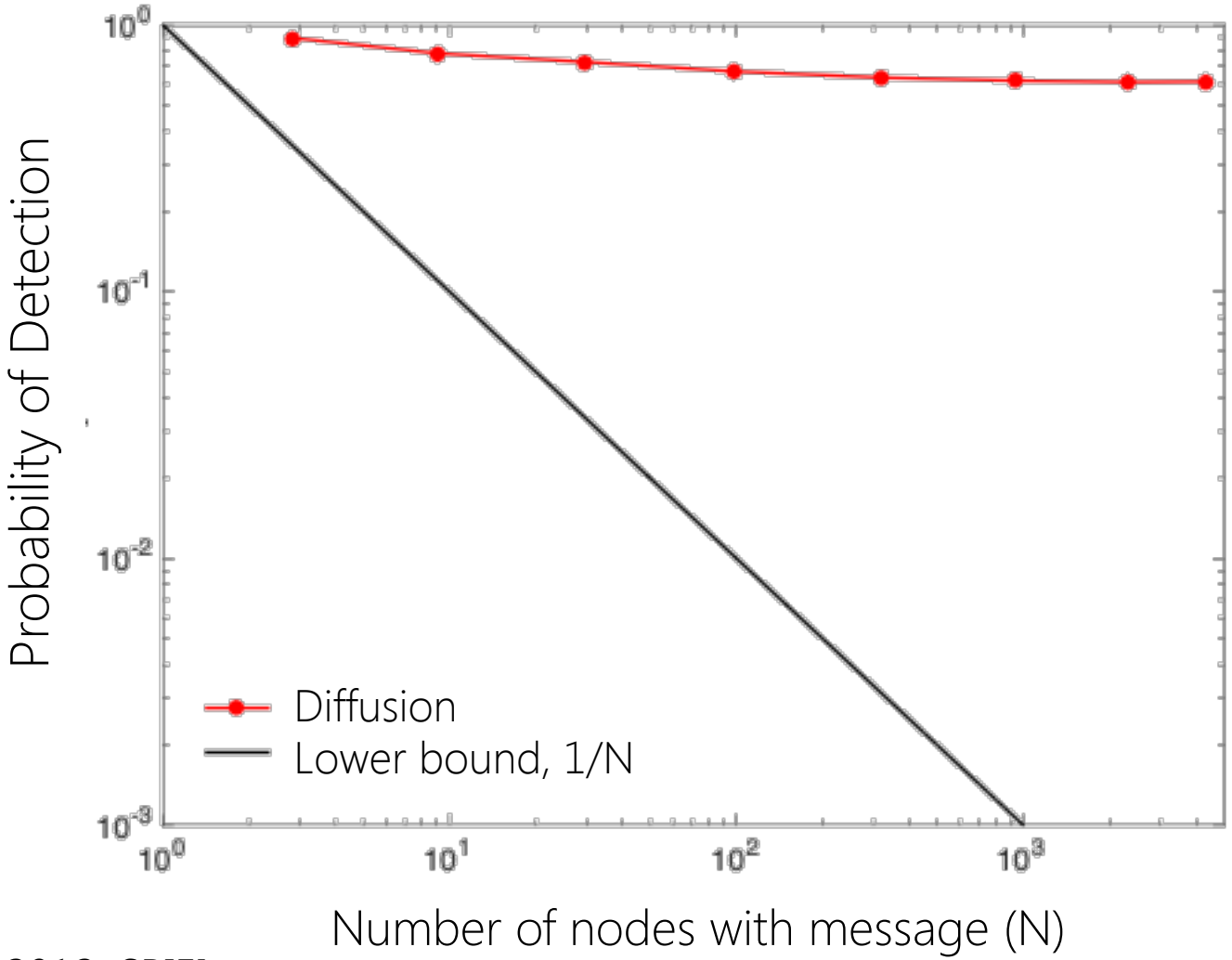
Information flow in social networks



Diffusion spreading = deanonymization

[Shah, Zaman 2011]

Deanonymization on Social Networks



[Seo et al., 2012, SPIE]

First-order solution doesn't work.

Spreads fast ☺

Bad anonymity properties ☹

LESSONS LEARNED

1) Diffusion = deanonymization

Engineer the spread to hide authorship.

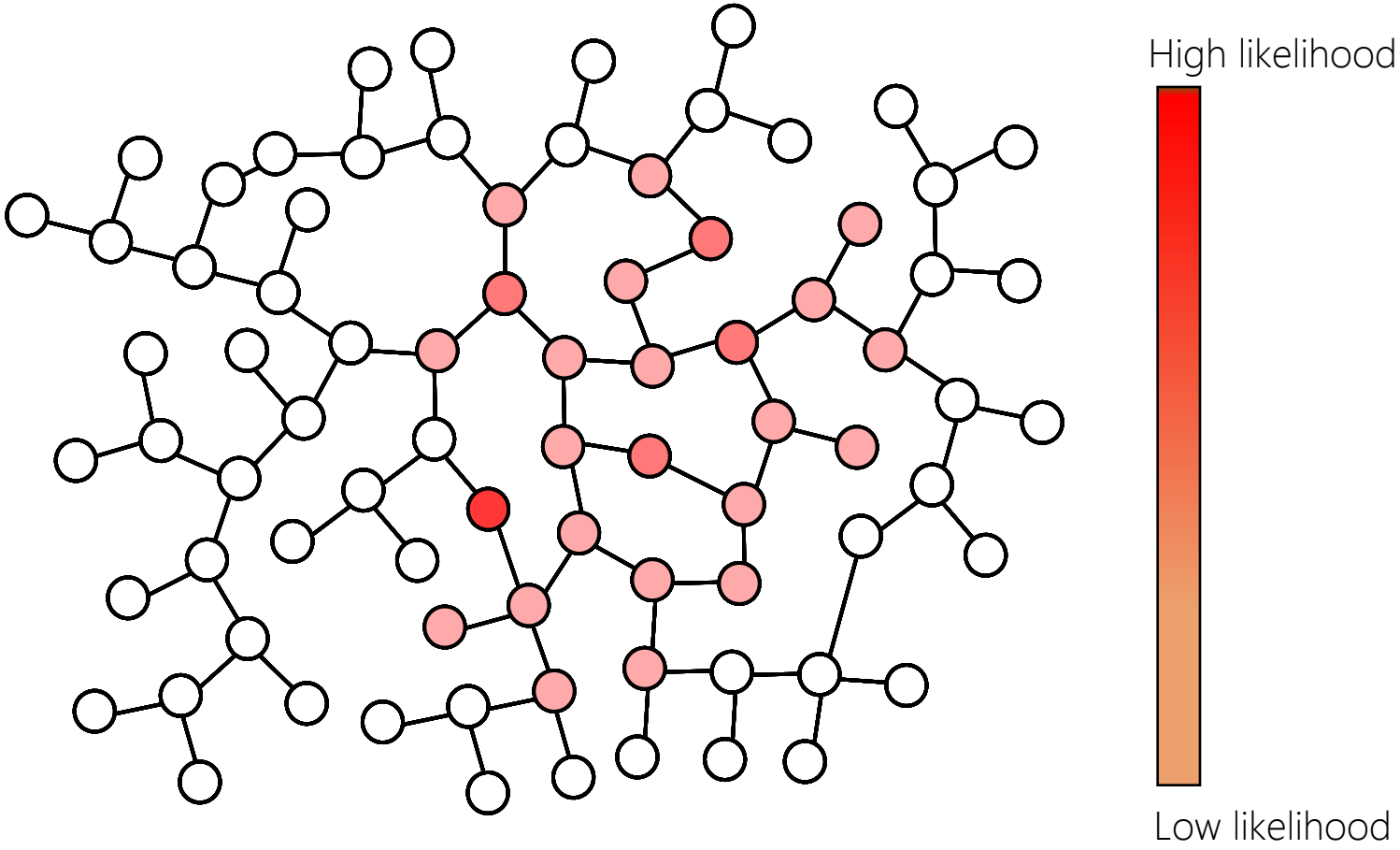
Key idea:

Break the symmetry.

Direction

Time

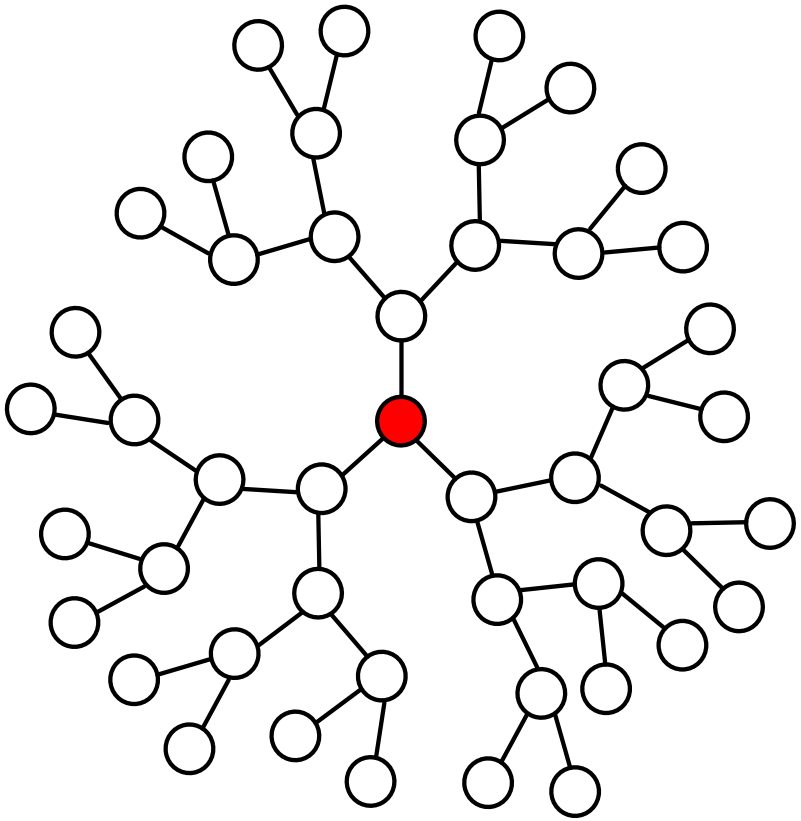
Breaking symmetry: Adaptive diffusion



Provides provable anonymity guarantees

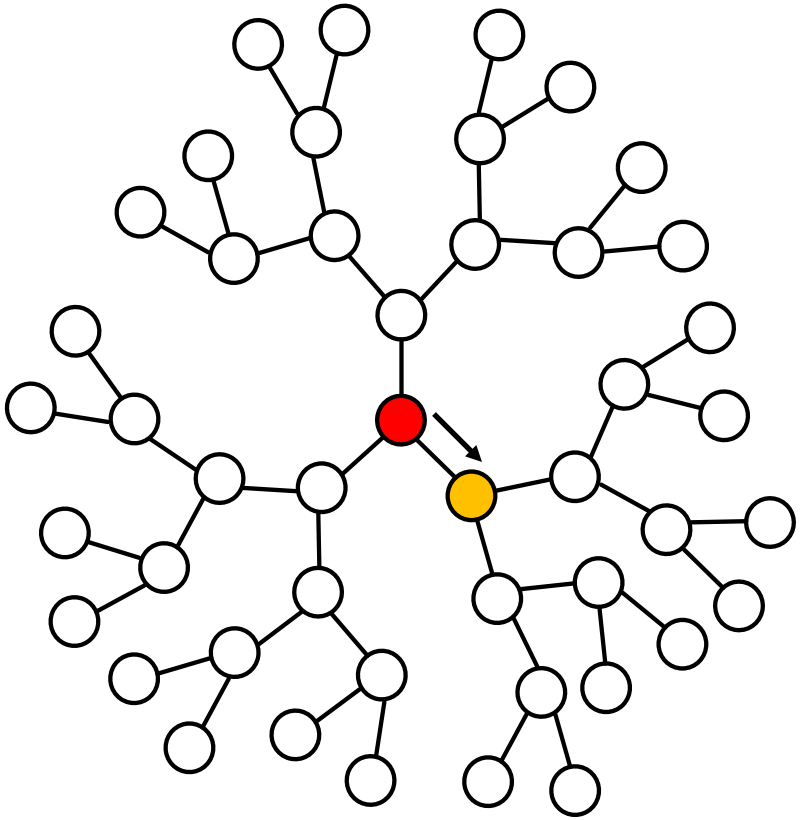
[*Spy vs. Spy: Rumor Source Obfuscation*, ACM Sigmetrics 2015]

d-regular trees: adaptive diffusion



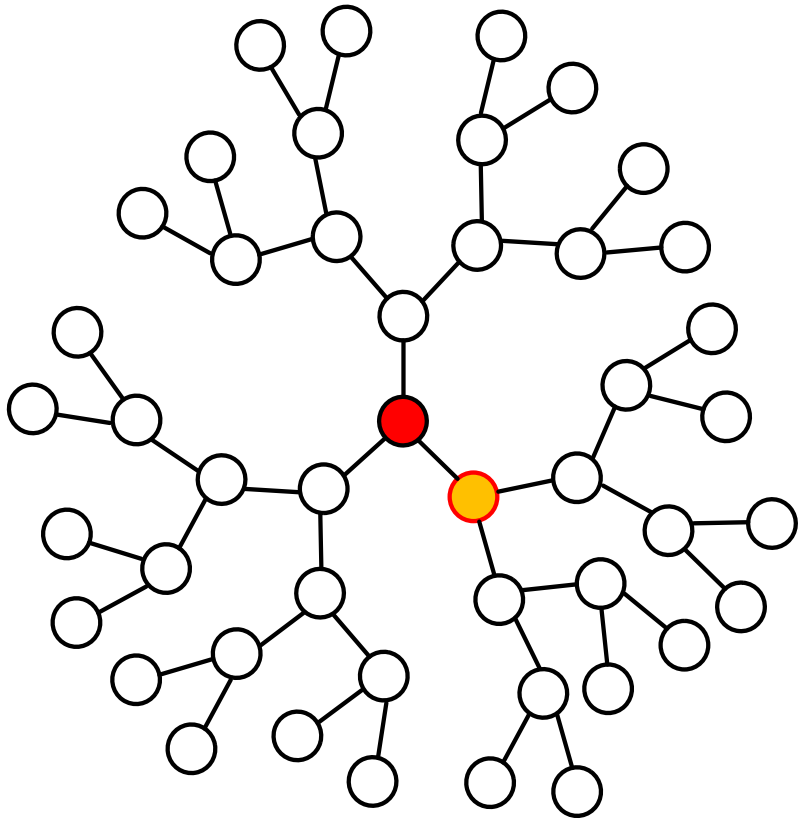
Initially, the author is also the "virtual source"

d-regular trees: adaptive diffusion



Break directional symmetry

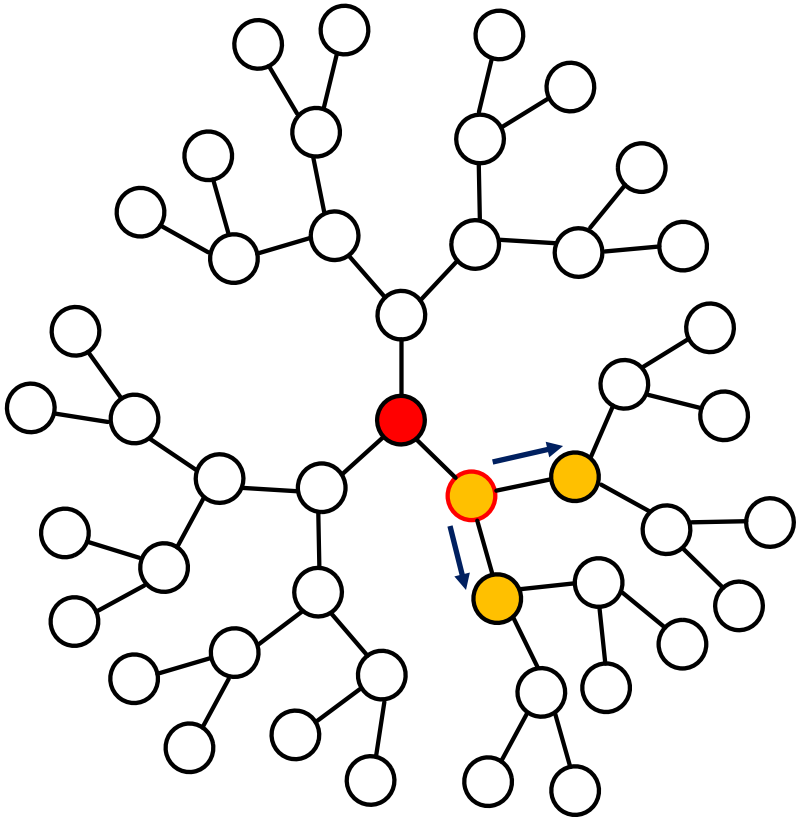
d-regular trees: adaptive diffusion



Break directional symmetry

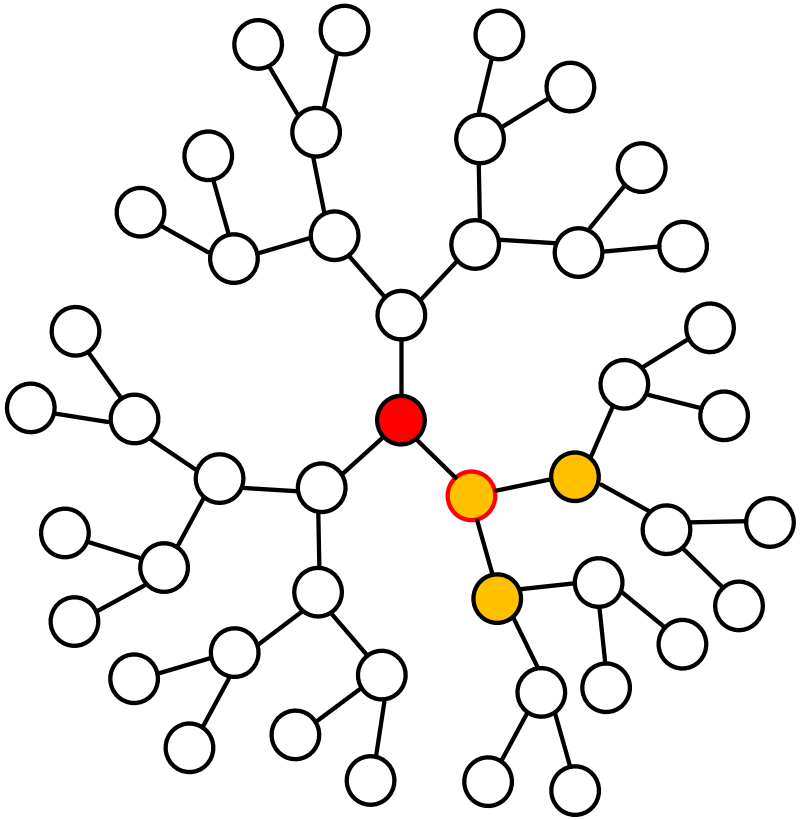
chosen neighbor = new virtual source

d-regular trees: adaptive diffusion



Break directional symmetry

d-regular trees: adaptive diffusion

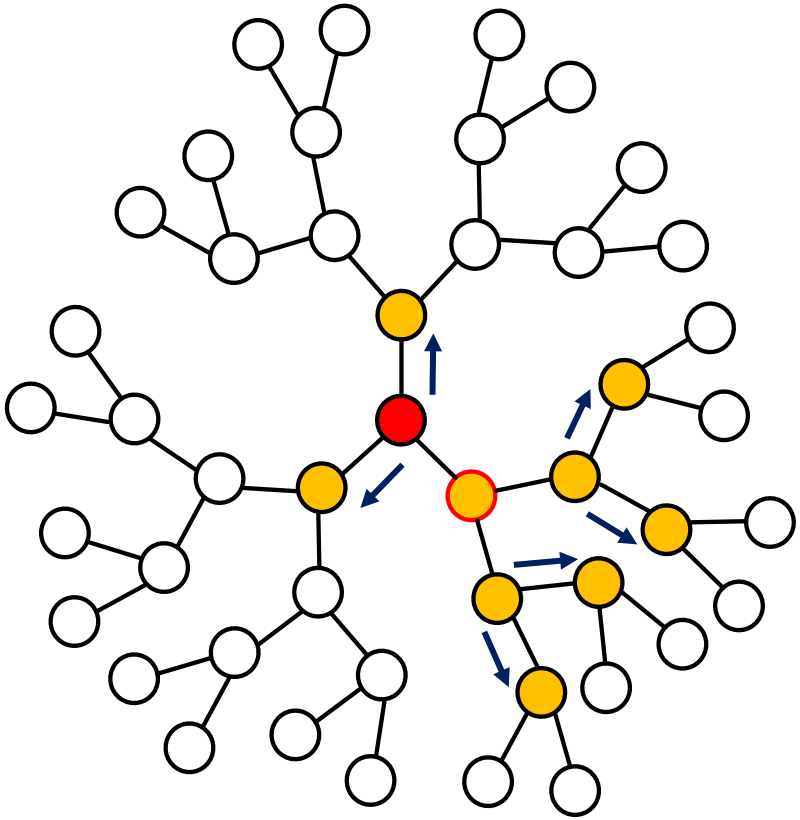


Break temporal symmetry

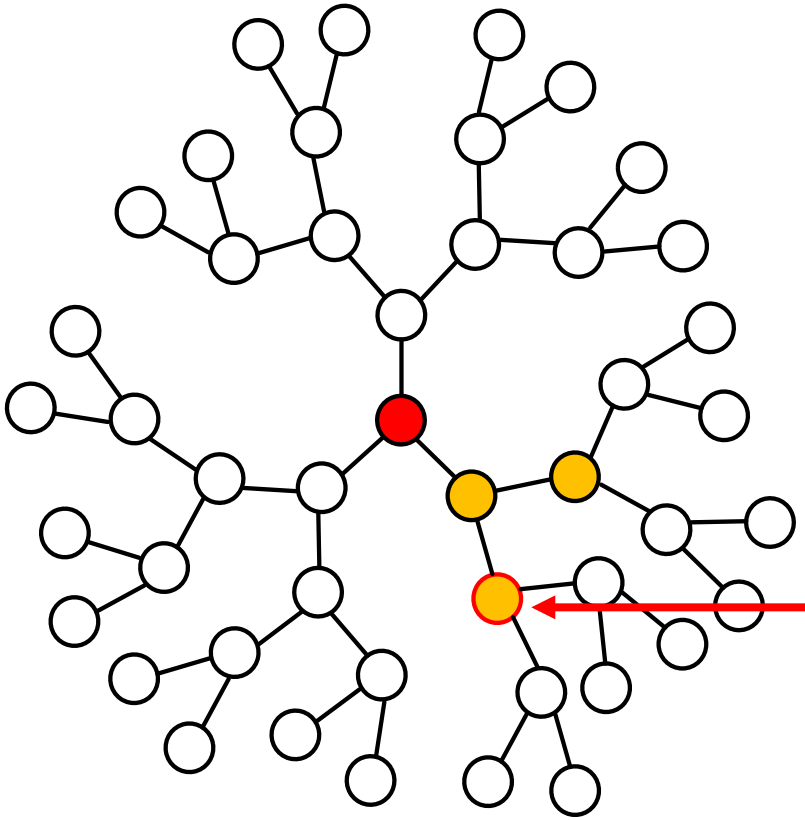
keep the virtual source token

pass the virtual source token

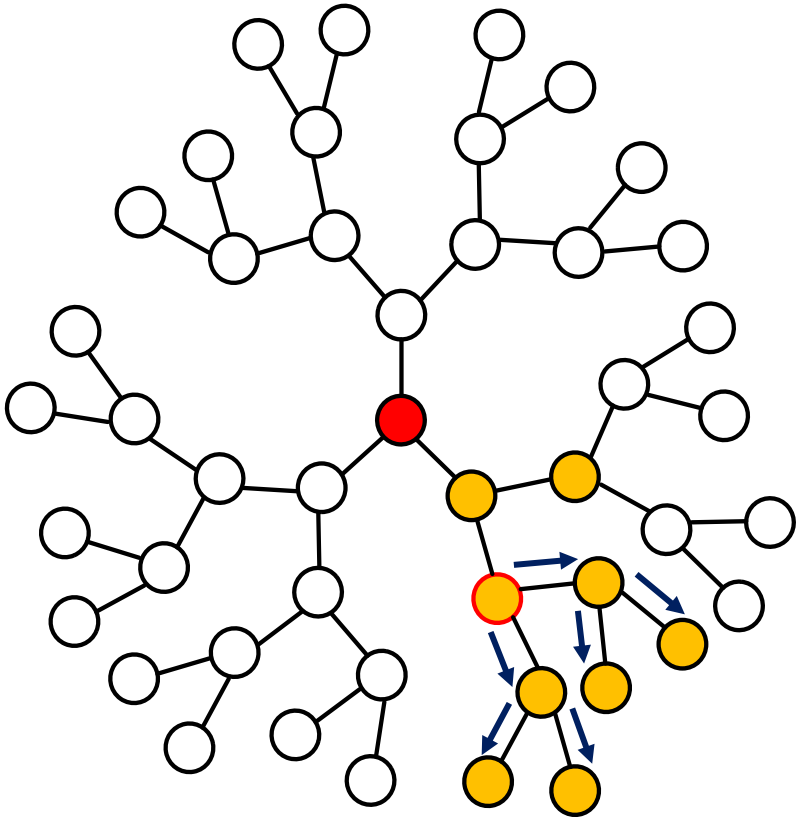
keep the virtual source token



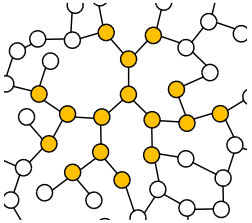
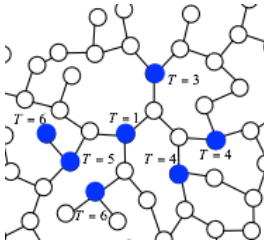
pass the virtual source token



pass the virtual source token

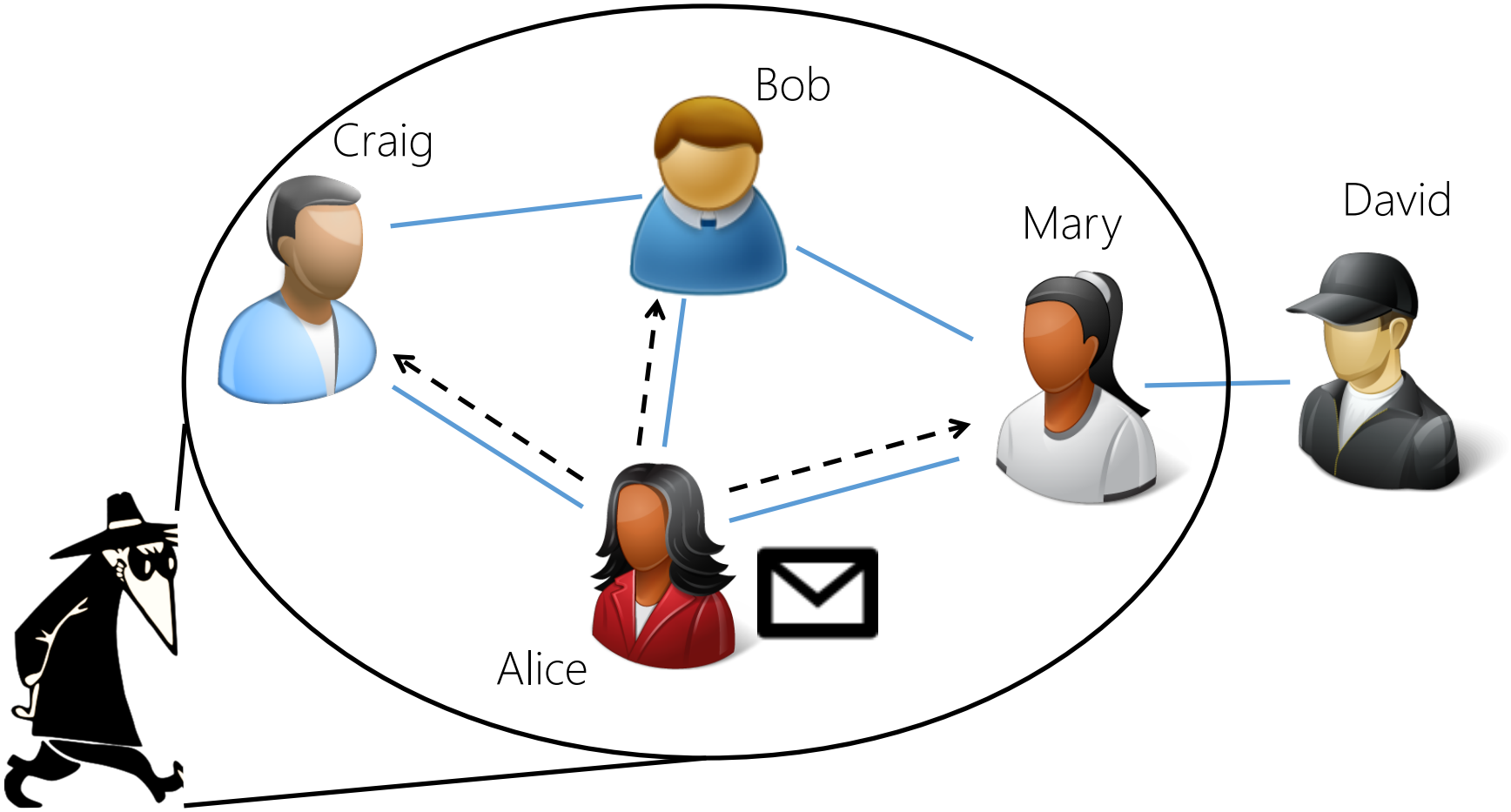


Results

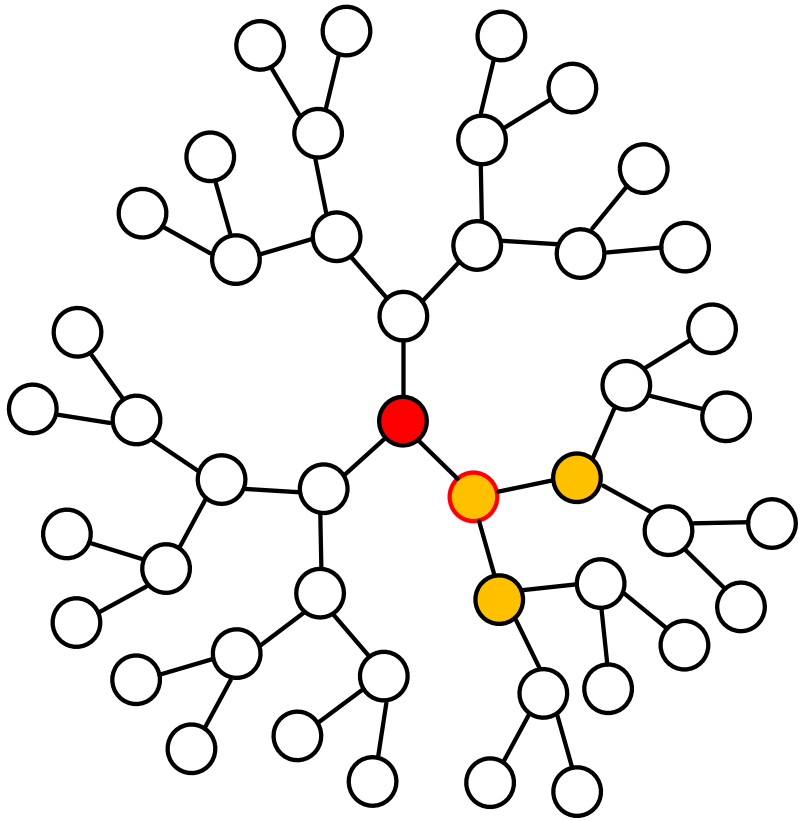
	d-Regular trees	Irregular trees	Facebook graph
Snapshot 	[1]	[2]	[1]
Spy-based 	[3]	[3]	[3]

[1] *Spy vs. Spy: Rumor Source Obfuscation*, Sigmetrics 2015
[2] *Rumor Source Obfuscation on Irregular Trees, to appear in Sigmetrics 2016*
[3] *Under review*

Snapshot adversary



When to keep the virtual source token?

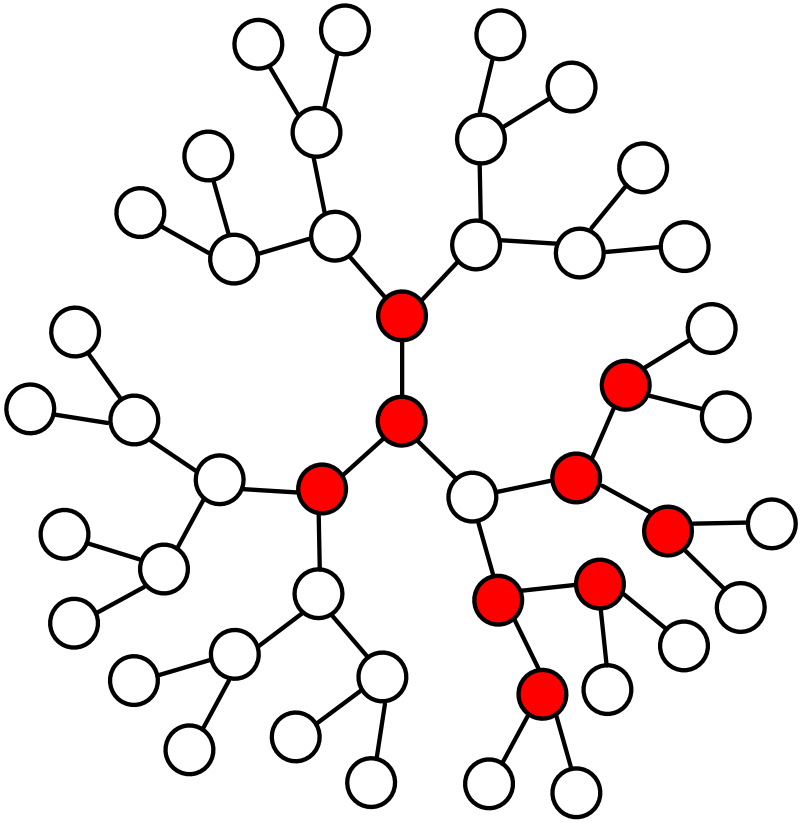


node degree

distance from source

Virtual source token is kept with probability $\boldsymbol{\alpha = (d-1)^{-h}}$

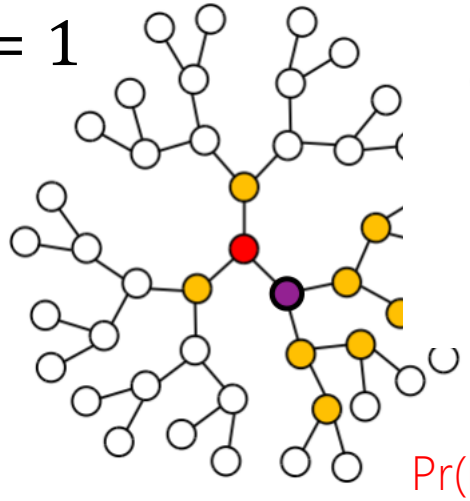
Maximum likelihood detection

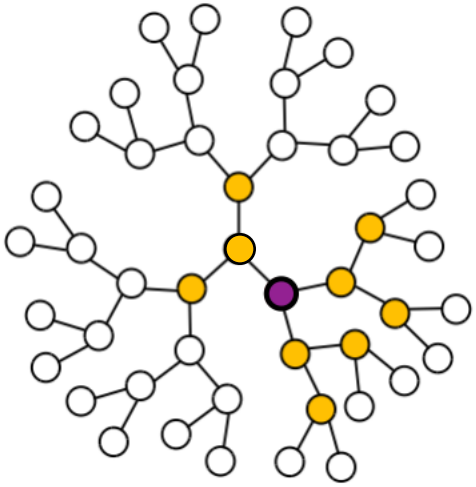


THEOREM: Probability of detection $= \frac{1}{N-1}$

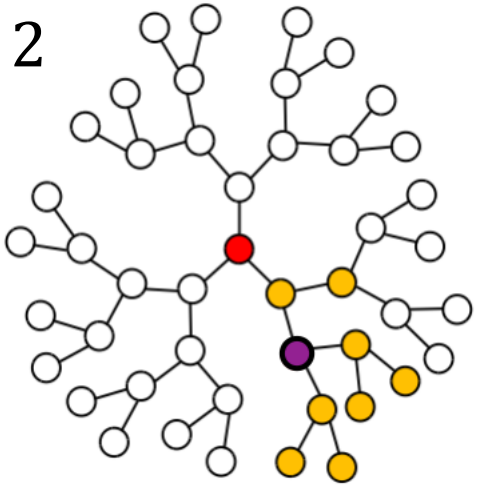
hop distance from source

$h = 1$





2



Pr(keep token)

Likelihood $= \frac{1}{d} \cdot \alpha$

Tree degree

Likelihood $= \frac{1}{d} \cdot \frac{1-\alpha}{d-1}$

Want these to be equal: $\alpha = \frac{1}{d}$

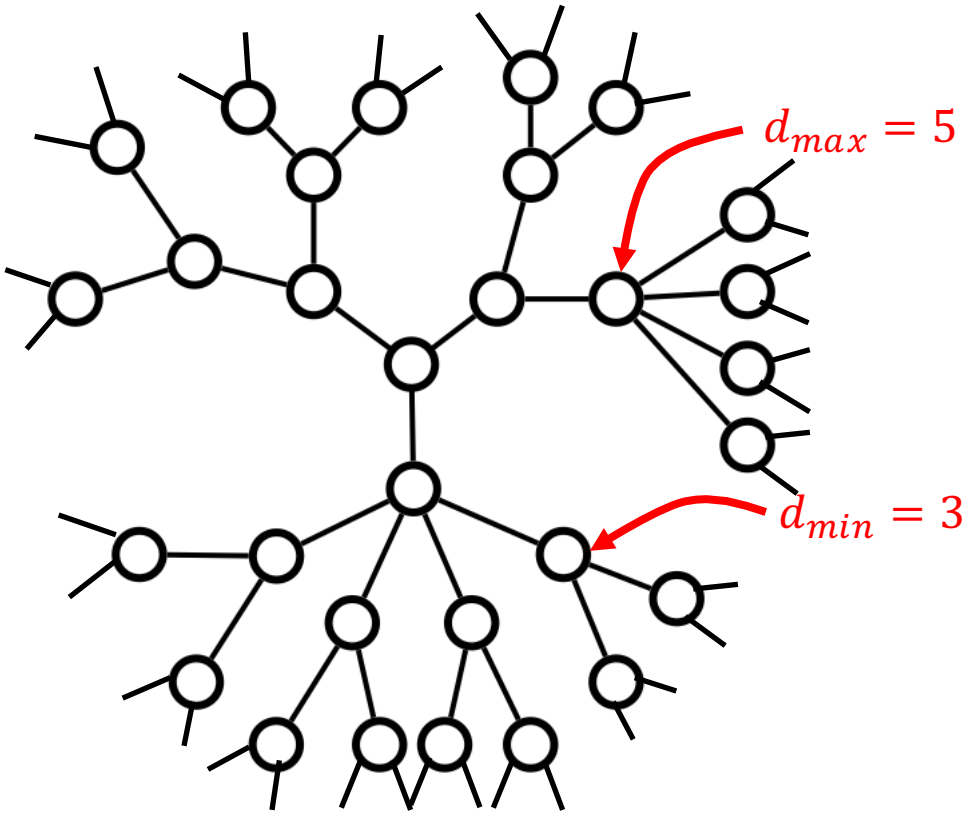
LESSONS LEARNED

1) Diffusion = deanonymization

2) For anonymity, break symmetry.

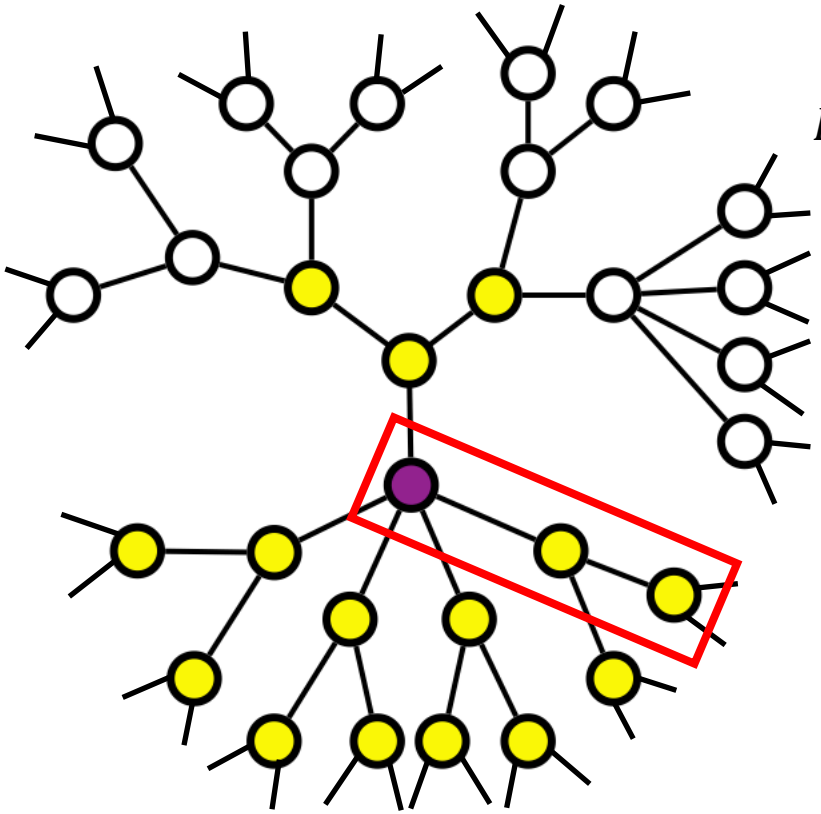
Irregular trees

$$d_v = \begin{cases} 3 & w.p. \quad 0.7 \\ 5 & w.p. \quad 0.3 \end{cases}$$



How do we analyze this?

$$d_v = \begin{cases} d_{min} & w.p. \quad p_{min} \\ d_{max} & w.p. \quad p_{max} \end{cases}$$



$$P(\text{detection} \mid \text{snapshot}) = \frac{1}{\min\limits_{v \in \text{leaves}} \prod_{v \in P(v,v_T)} d_v}$$

Path from v to virtual source

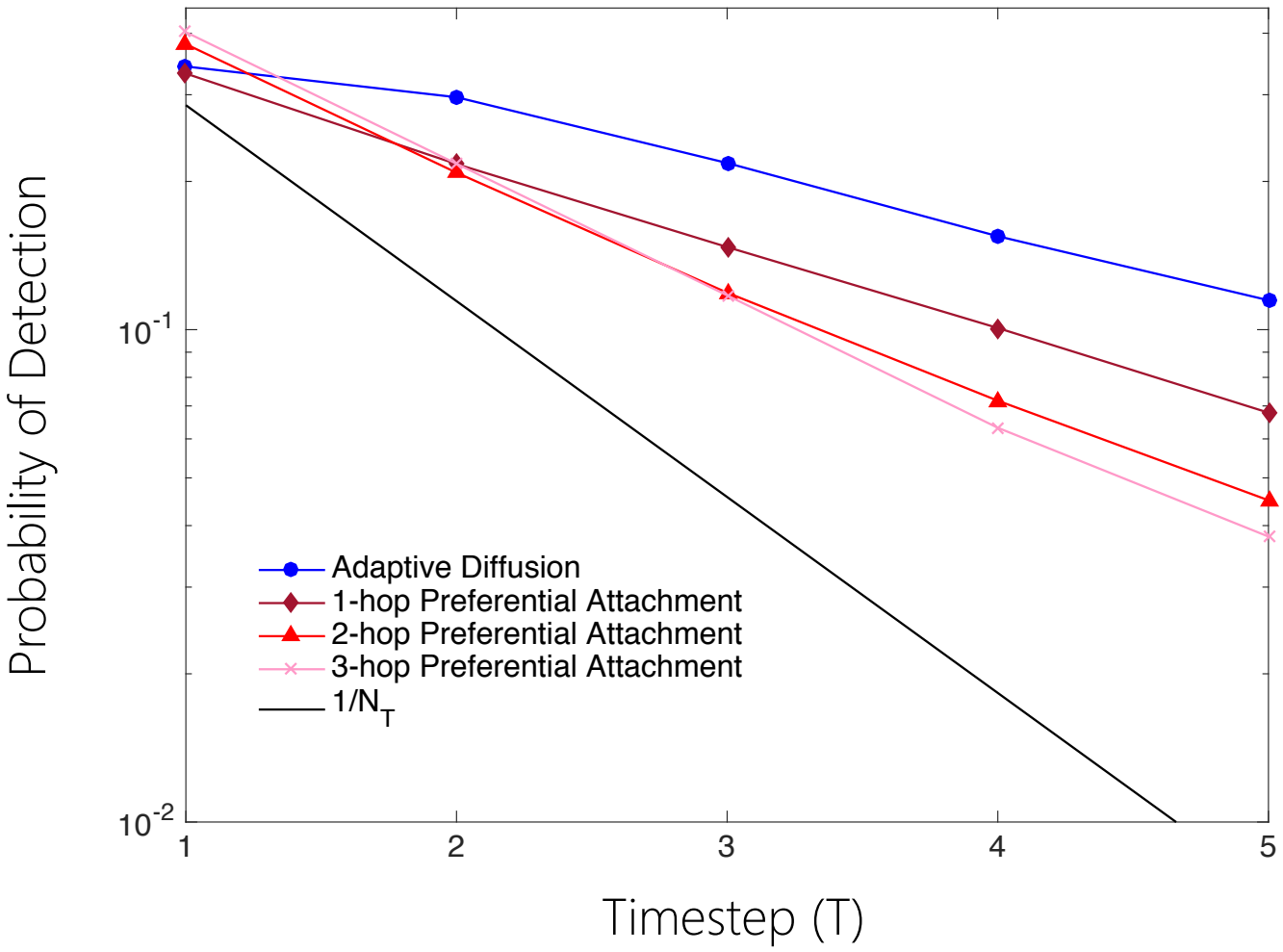
Degree of node v

If $p_{min}(d_{min} - 1) > 1$

$$\min_{v \in \text{leaves}} \prod_{v \in P(v,v_T)} d_v \approx (d_{min} - 1)^{T/2}$$

THEOREM: Probability of detection $\approx \frac{1}{(d_{min}-1)^{T/2}}$

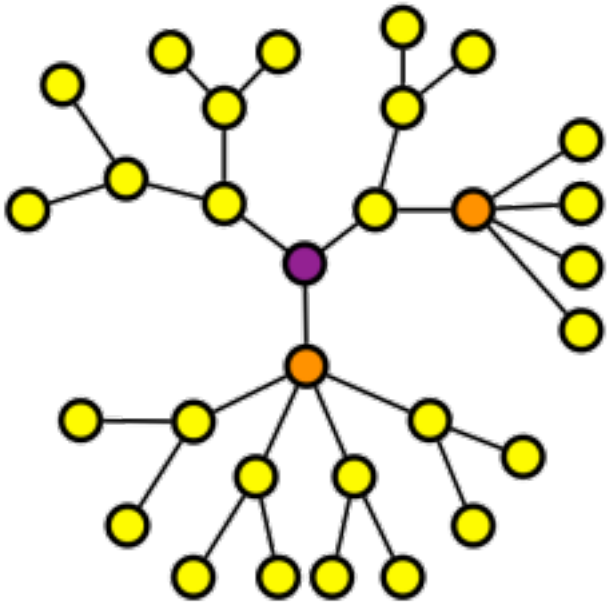
Irregular trees

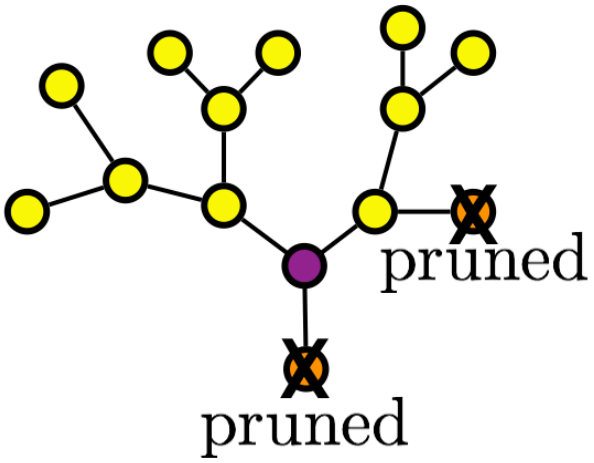


Proof sketch for $\min_{v \in \text{leaves}} \prod_{v \in P(v, v_T)} d_v \approx (d_{min} - 1)^{T/2}$

$$d_v = \begin{cases} 3 & w.p. \quad 0.7 \\ 5 & w.p. \quad 0.3 \end{cases}$$

$$d_v = \begin{cases} 3 & w.p. \quad 0.7 \\ 1 & w.p. \quad 0.3 \end{cases}$$





0.7 3

If $p_{min}(d_{min} - 1) > 1$ then the pruned process survives.

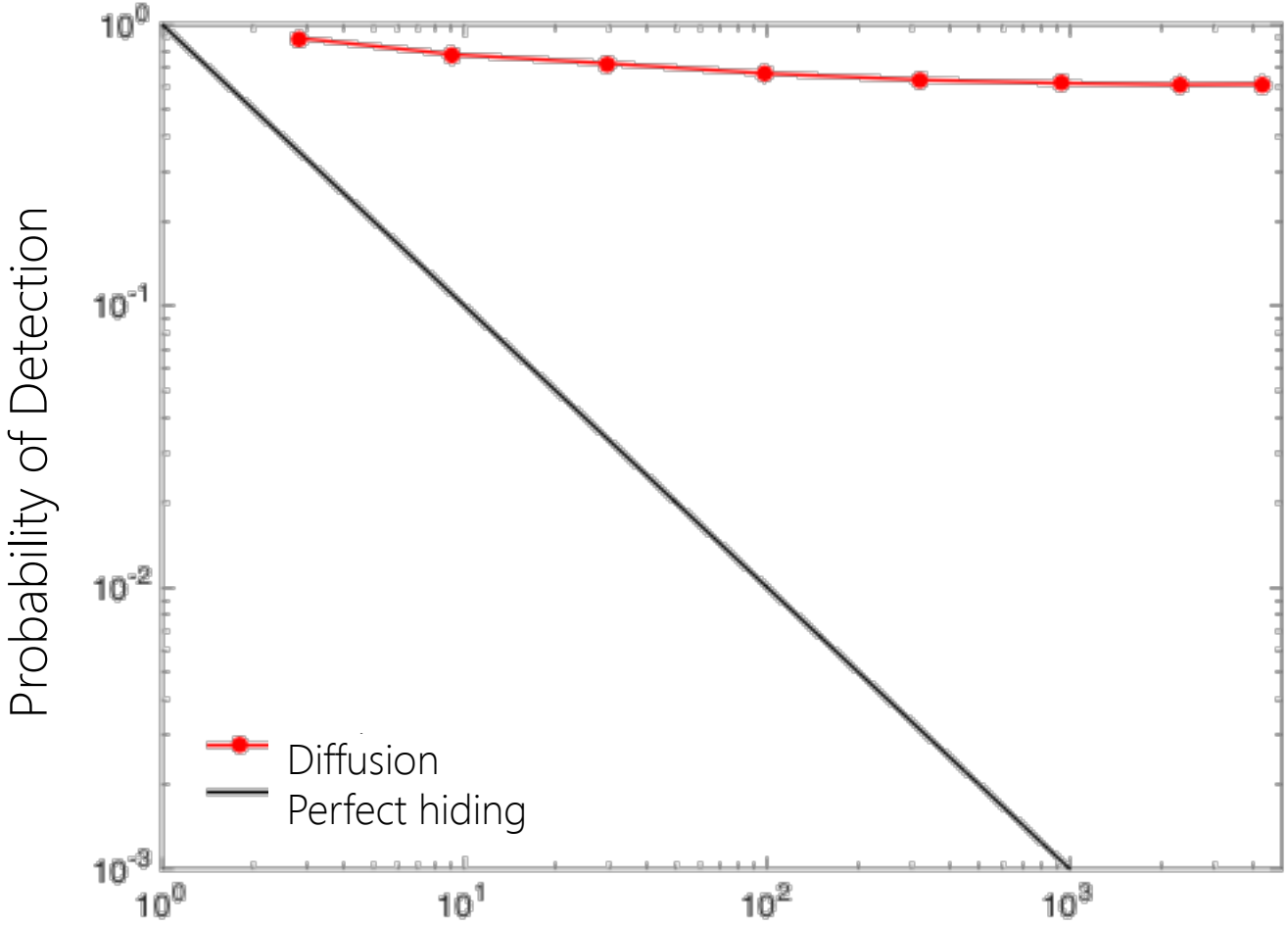
LESSONS LEARNED

1) Diffusion = deanonymization

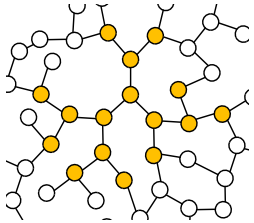
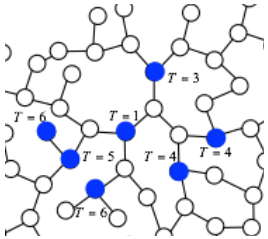
2) For anonymity, break symmetry.

3) For *more* anonymity, hide in a crowd.

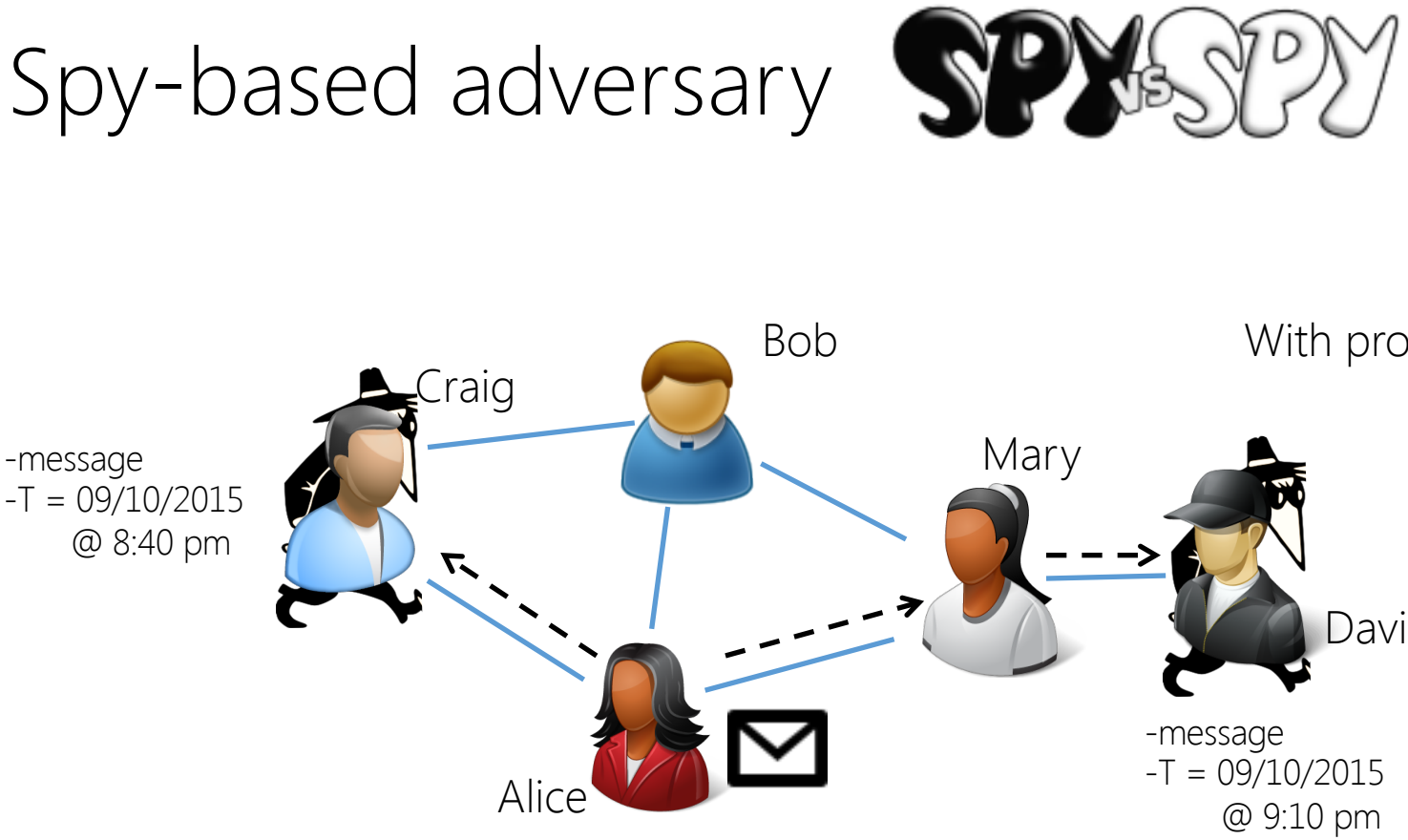
Facebook graph



Results

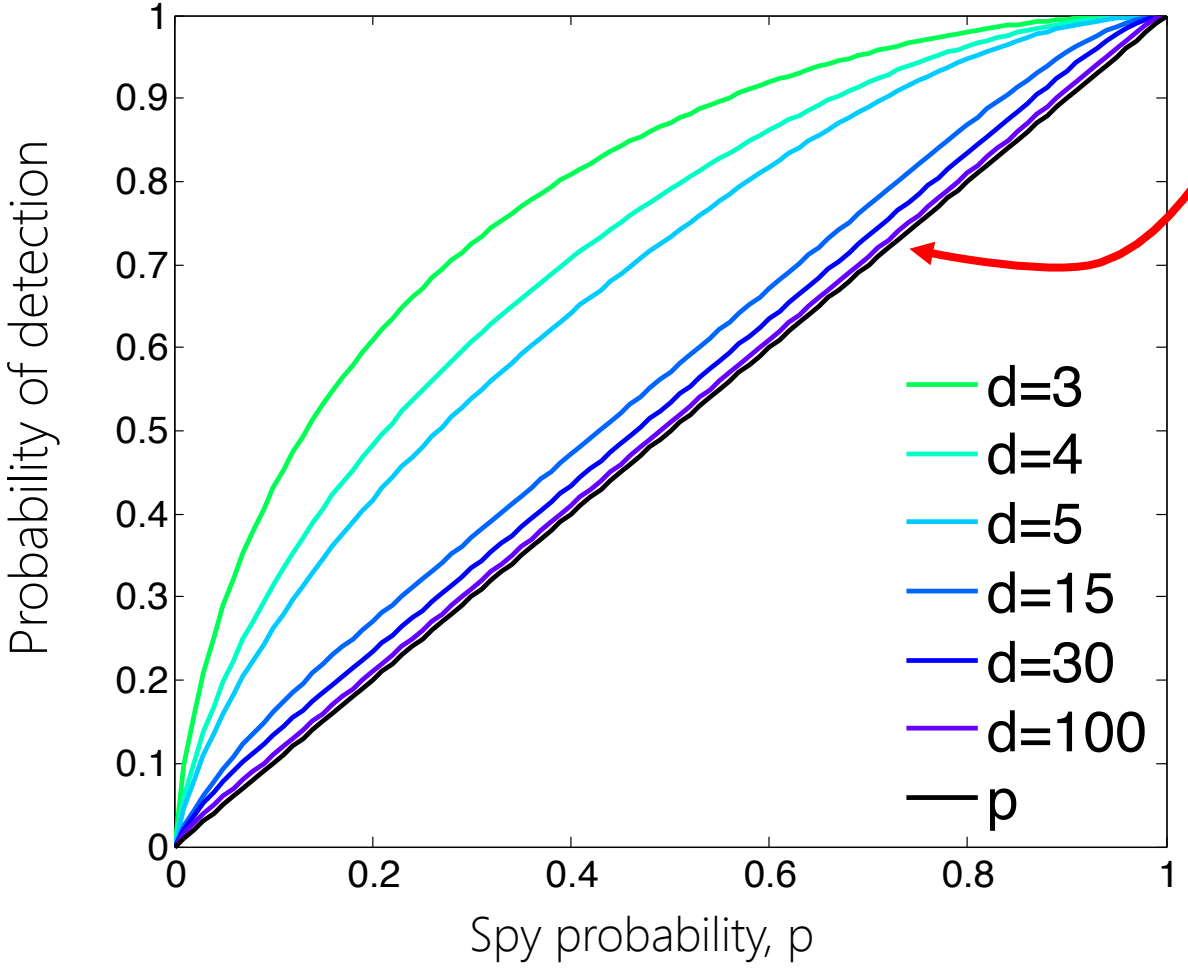
	d-Regular trees	Irregular trees	Facebook graph
Snapshot 	Optimal	Near-optimal	High anonymity
Spy-based 			

Spy-based adversary



Adversary sees metadata at spy nodes

Result on d-regular trees

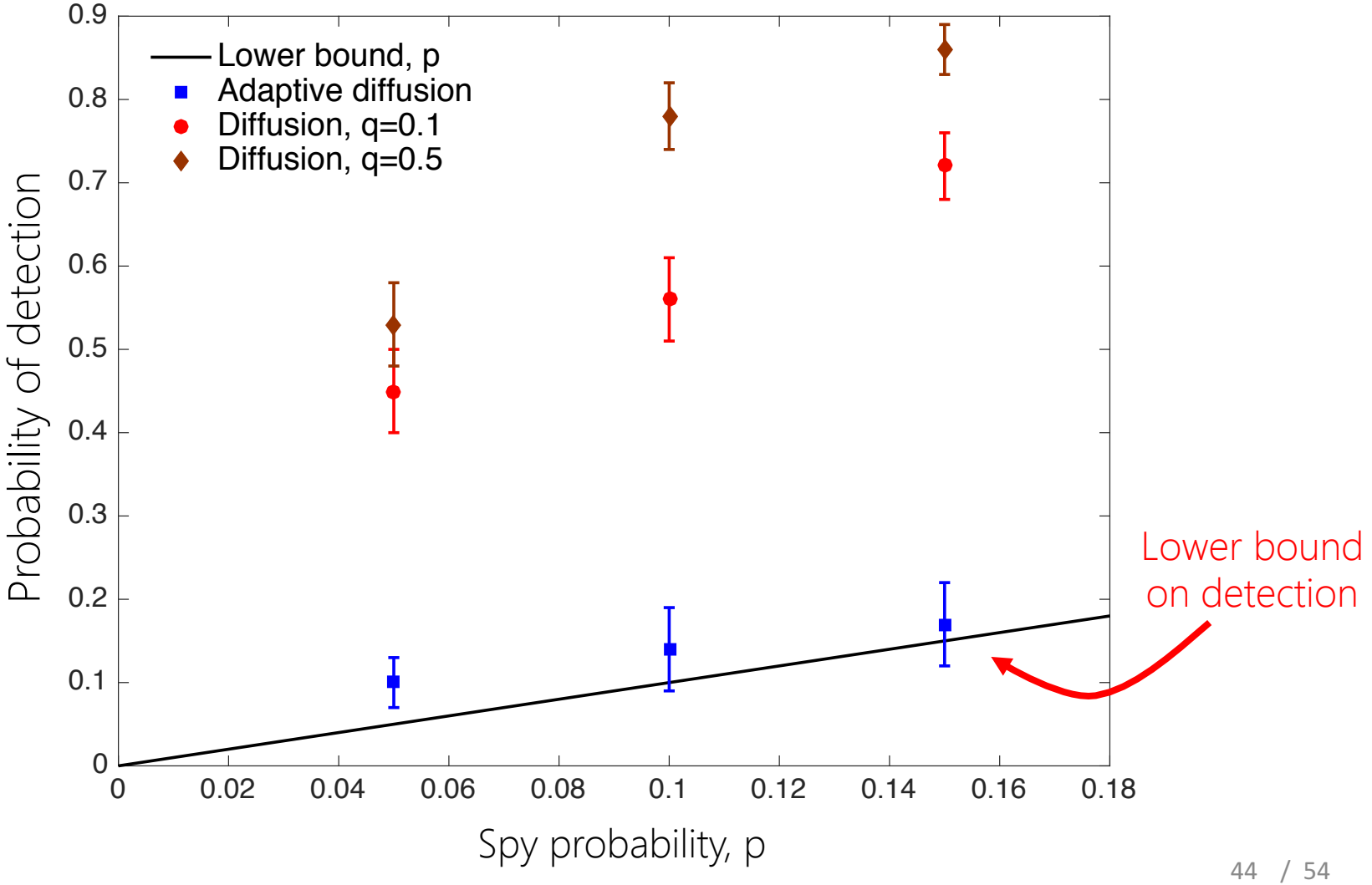


Lower bound on detection

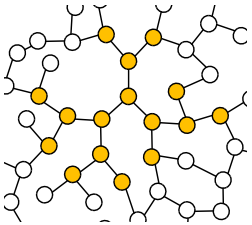
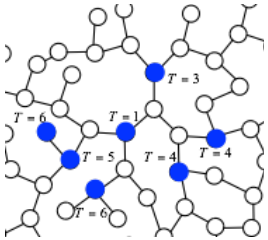
$T = \infty$

THEOREM: Probability of detection $= p + o(p)$

Facebook Graph



Results

	d-Regular trees	Irregular trees	Facebook graph
Snapshot 	Optimal	Near-optimal	High anonymity
Spy-based 	Asymptotically-Optimal	ML Estimator	High anonymity

Adaptive Diffusion

Pros

- Strong anonymity
- Fast spreading
- Distributed
- Lightweight

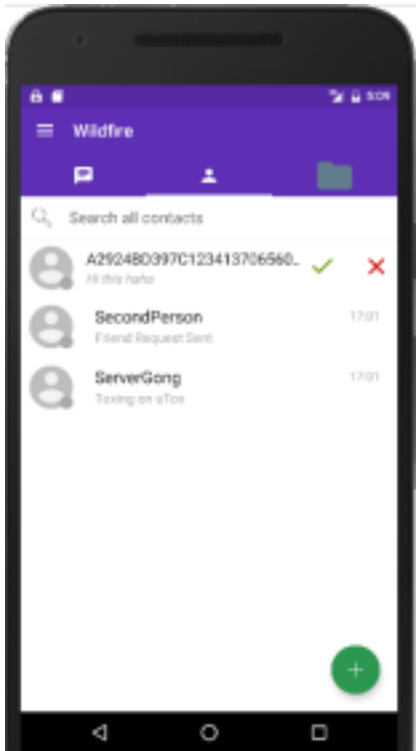
Cons

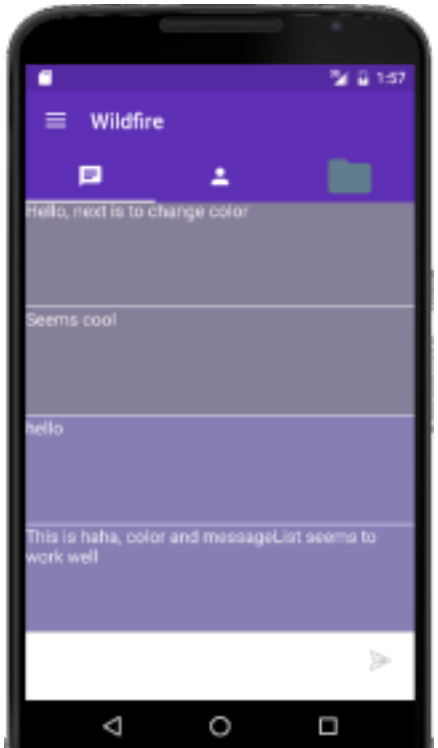
- No guarantees for general graphs
- Sub-optimal spreading
- Passes around state

Wildfire: P2P Anonymous Microblogging

TOX

https://github.com/gfanti/Wildfire

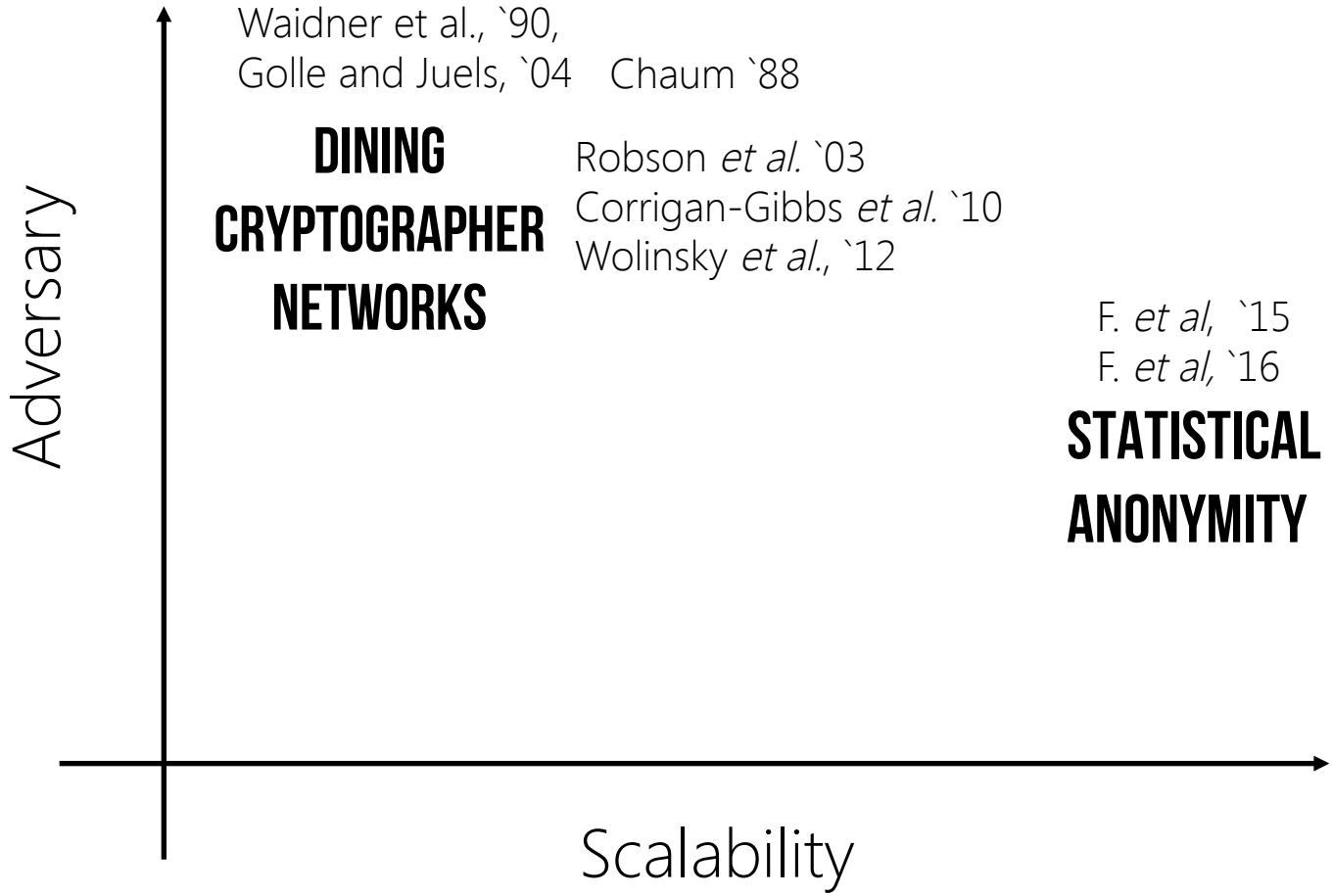




Namespace resolution

Cyberbullying

Related Work



Ongoing Work

Cellular Location Privacy

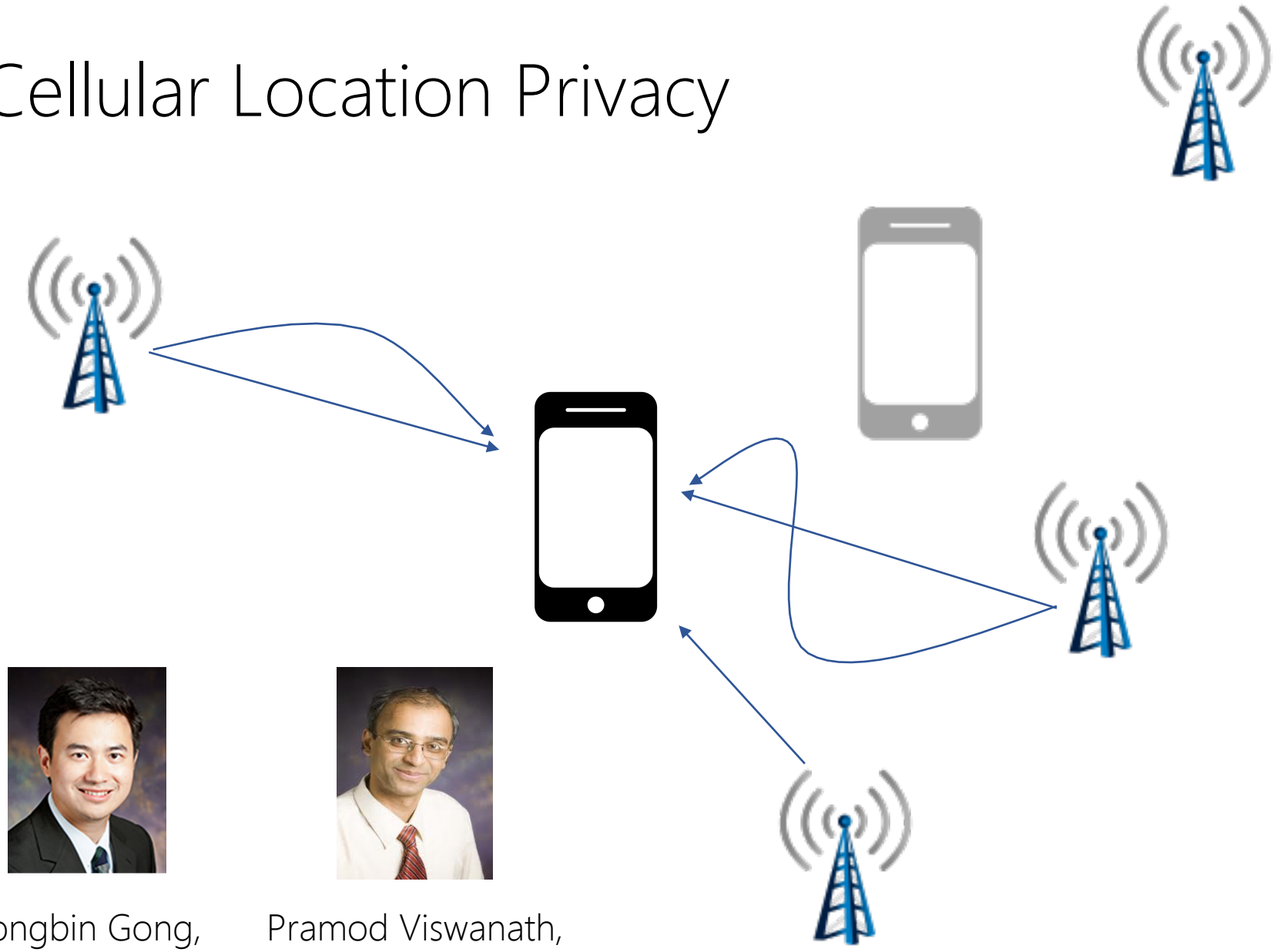
Anonymous Messaging

Cyberbullying Prevention

Vibration-based Biometrics

Anonymous P2P Networking

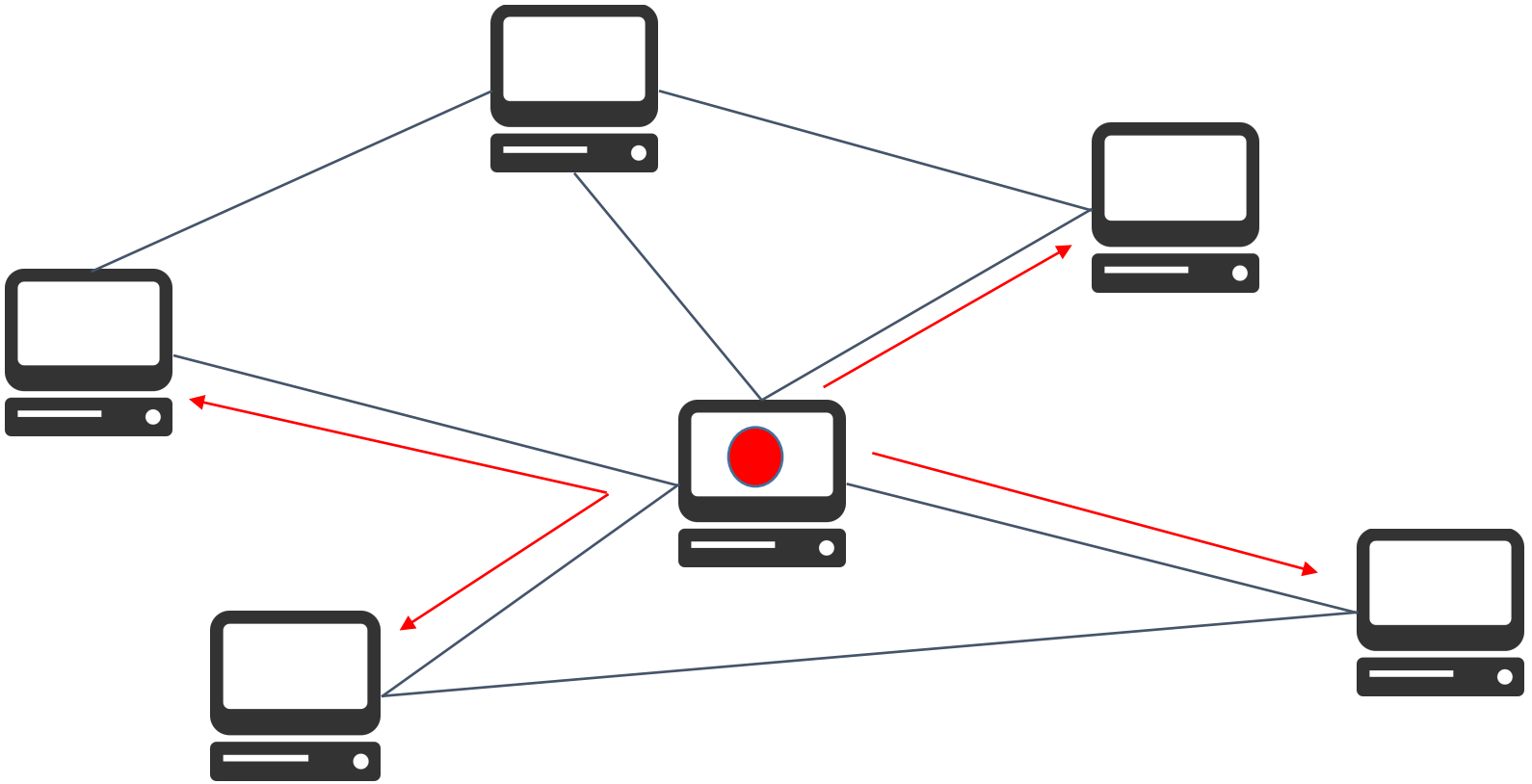
Cellular Location Privacy



Songbin Gong,
Microwave Circuits

Pramod Viswanath,
Wireless Comm.

Anonymous P2P Messaging



Cyberbullying Prevention

Suma Bhat,
NLP

Dorothy Espelage,
Educational Psychology

Ongoing Work

Cellular Location Privacy

Anonymous Messaging

Cyberbullying Prevention

Vibration-based Biometrics

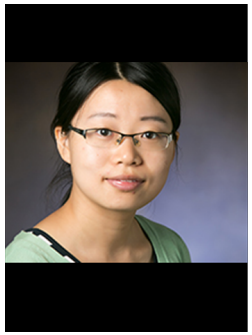
Anonymous P2P Networking

Acknowledgments

Suma Bhat

Romit Roy Choudhury

Dorothy Espelage



Hongyu Gong

Songbin Gong

Peter Kairouz

Sewoong Oh

Kannan Ramchandran

Pramod Viswanath