Private & Anonymous Communication

Peter Kairouz
ECE Department
University of Illinois at Urbana-Champaign

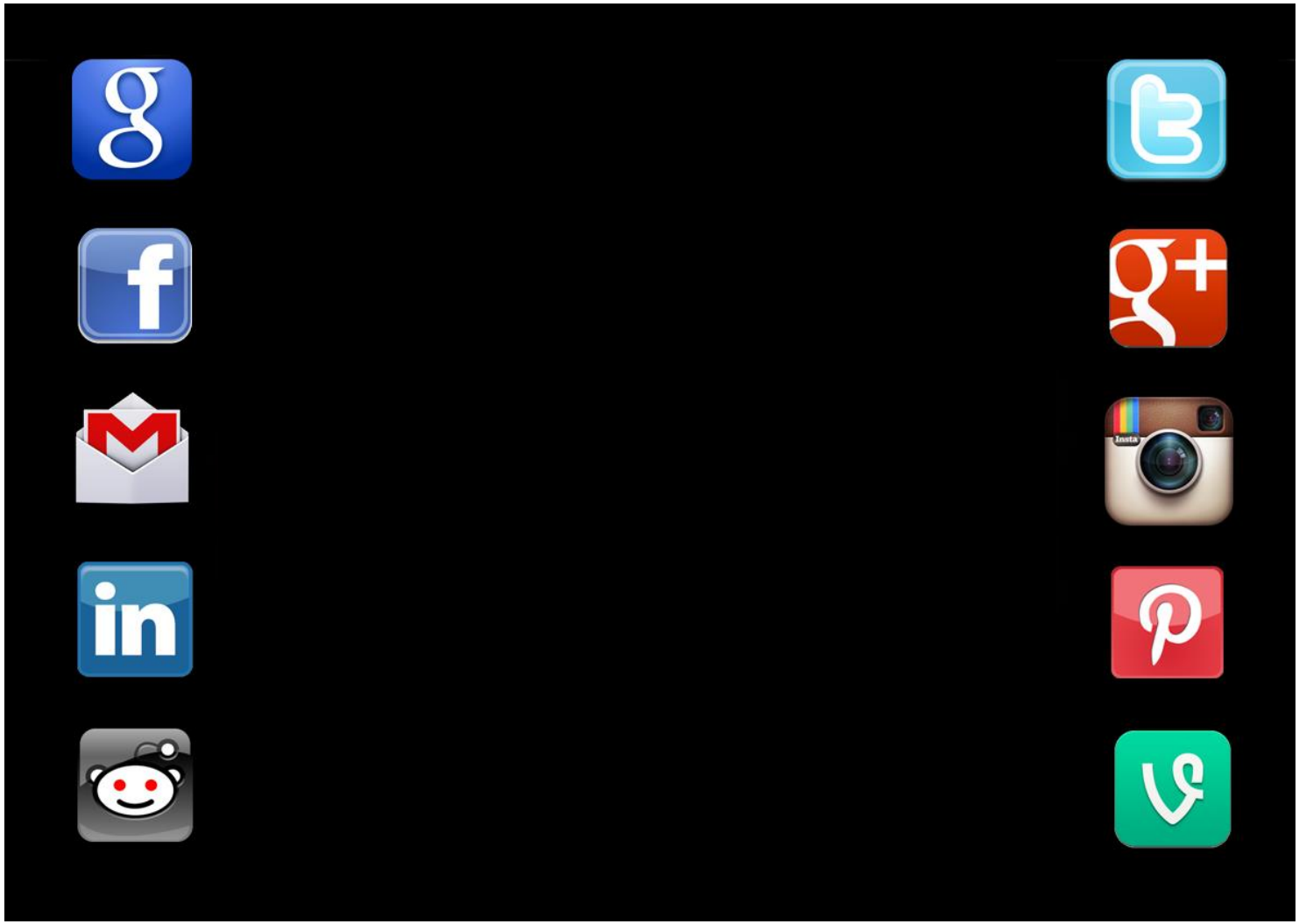
Communication

- transfer of information **from one point** in space-time **to the other**

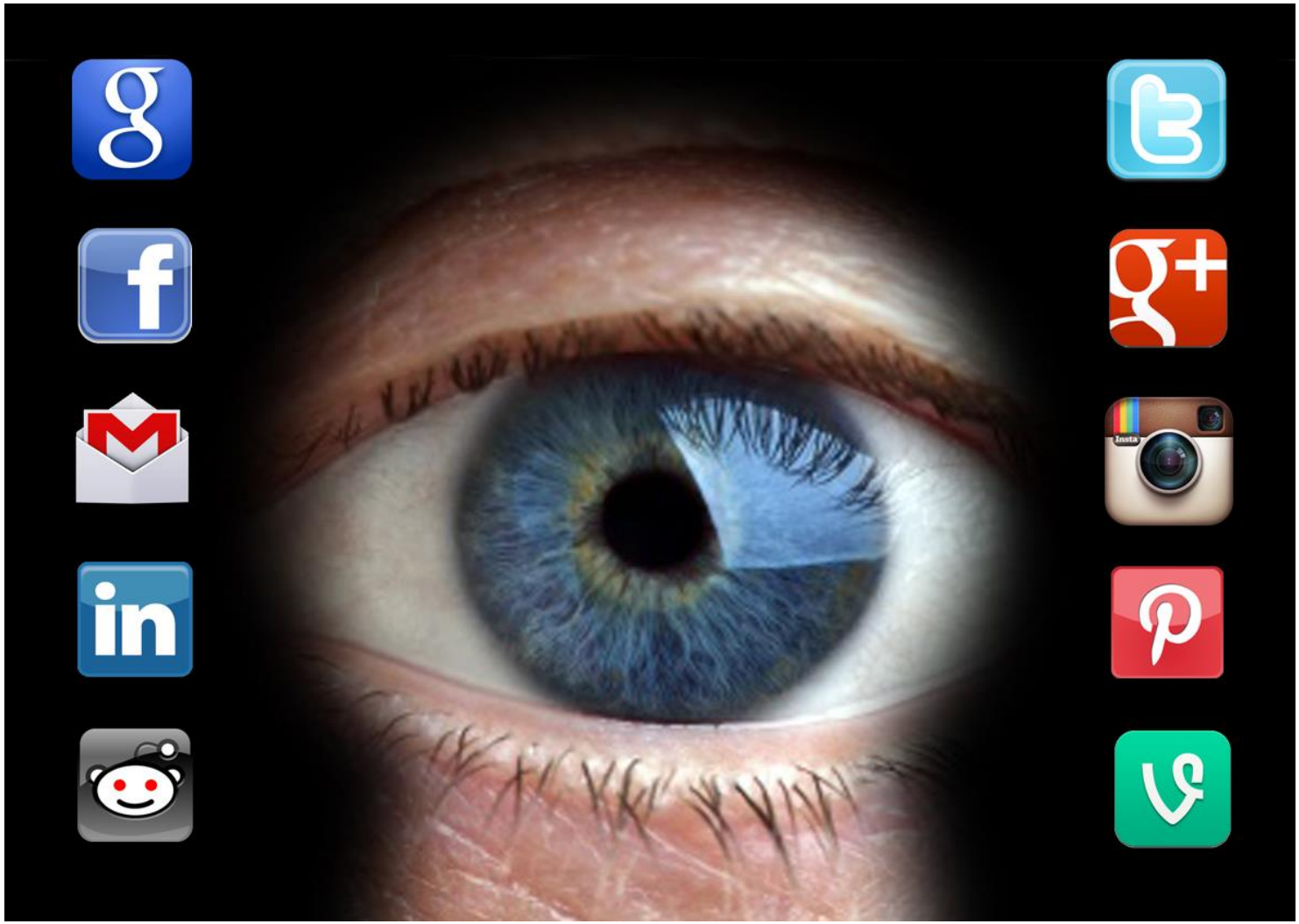
Wireless communication

- the **fundamental limits** of wireless communication are **well understood**

Rise of the planet of the apps!

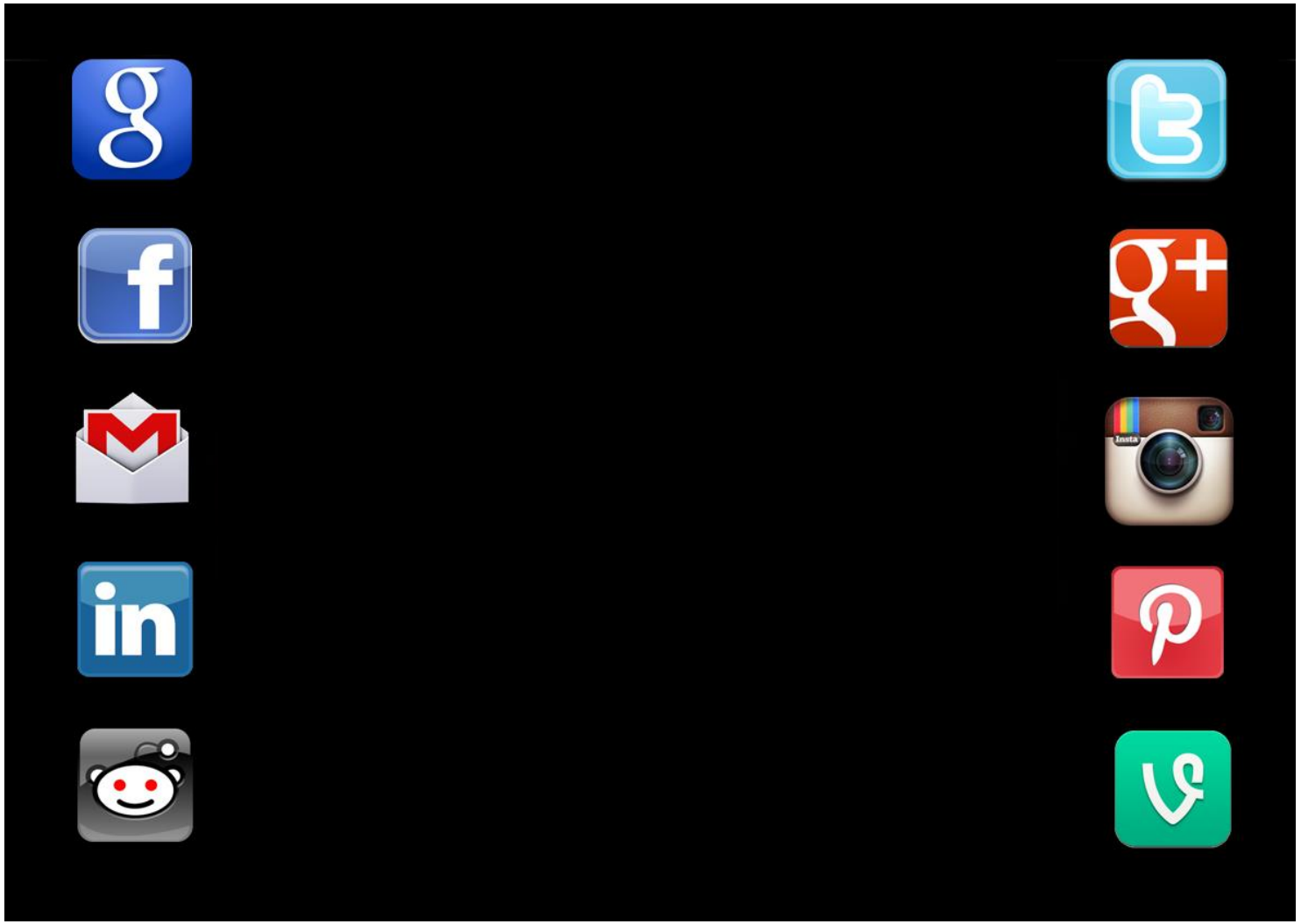


Rise of the planet of the apps!



Rise of the planet of the apps!

Rise of the planet of the apps!



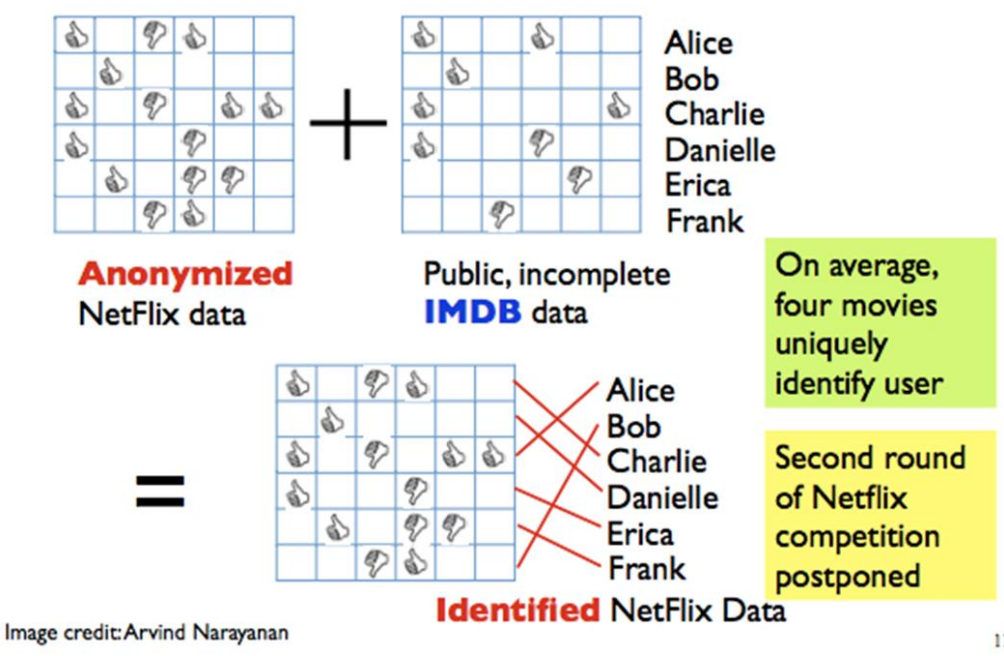
can we communicate anonymously and privately?

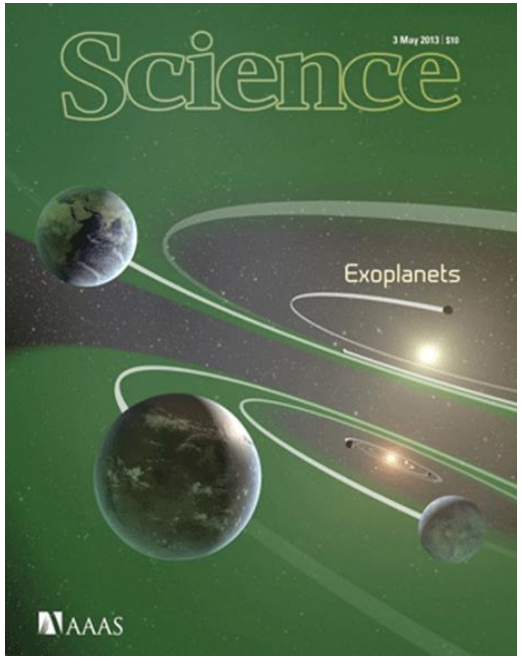
Does privacy matter?

"if you're doing something that you don't want other people to know, maybe you shouldn't be doing it in first place"

"privacy is no longer a social norm!"

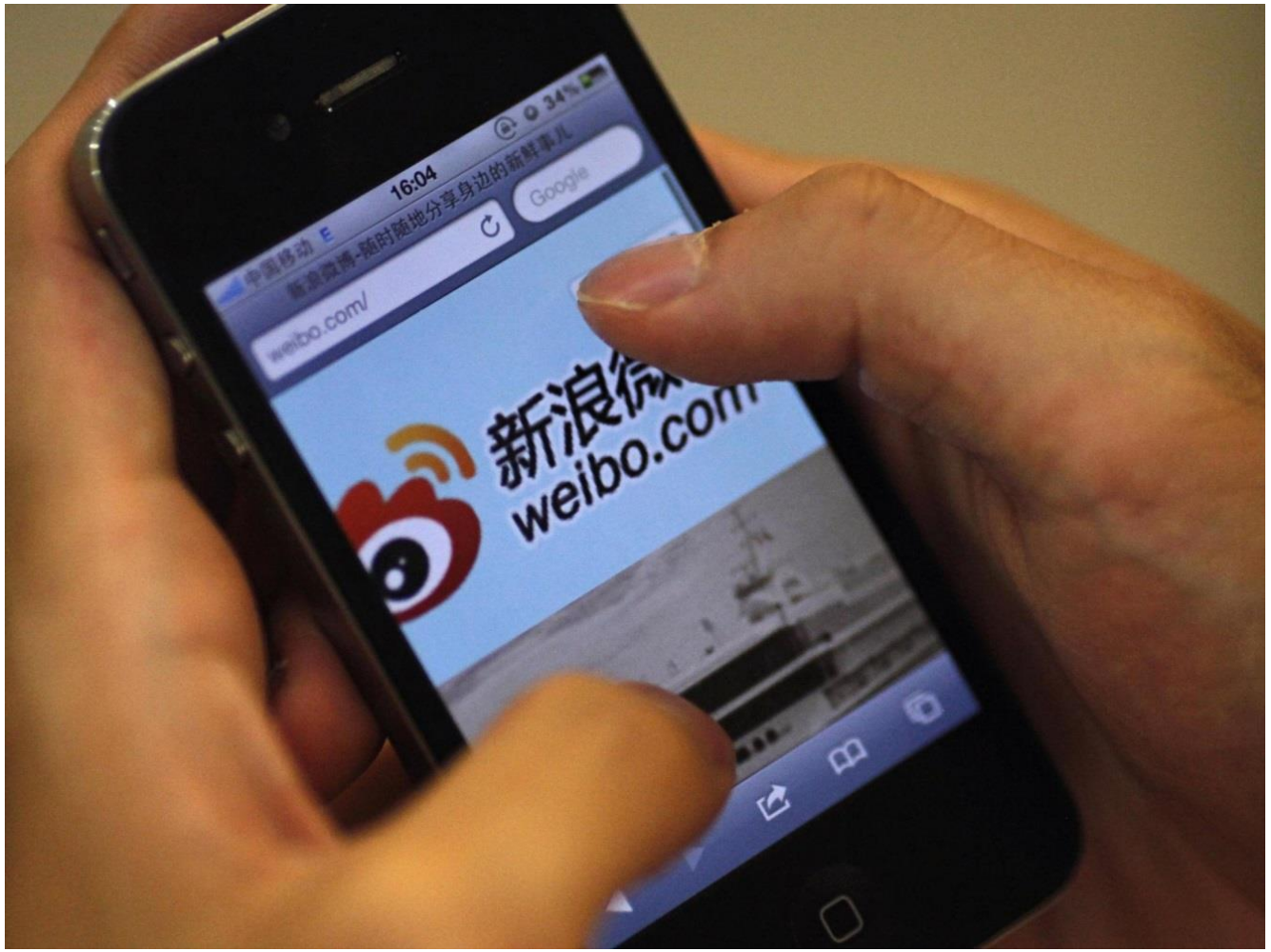
Recent privacy leaks





deanonymizing Netflix data, **identifying** personal genomes, etc.

China's crackdown on messaging apps

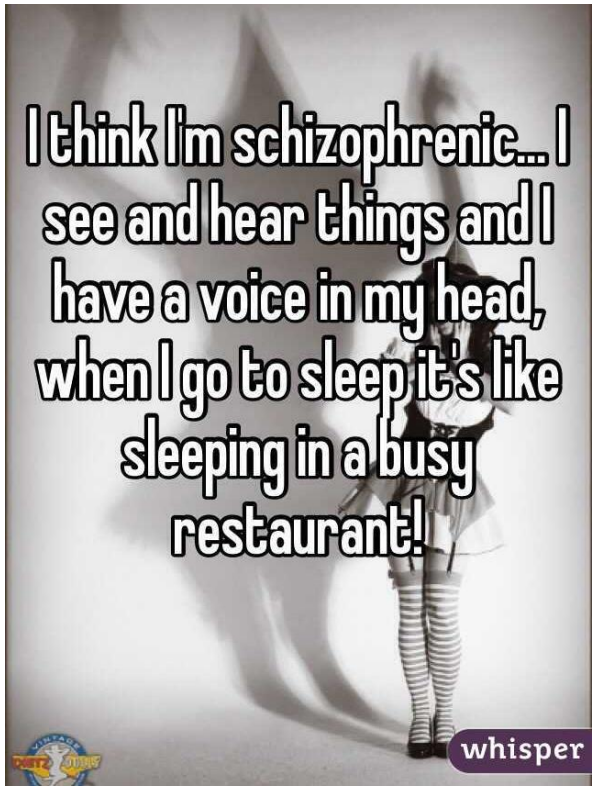


- if your message is shared 500 times, you may face **3 years in prison**

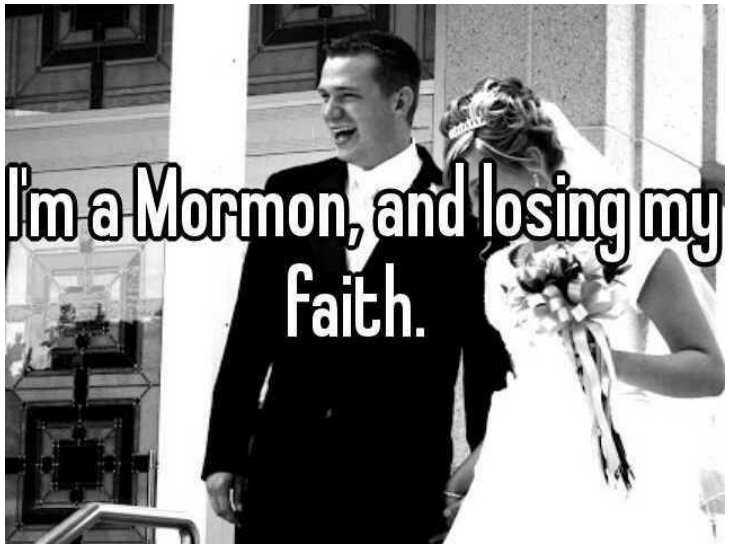
Political activism

some people have important,
sensitive things to say

Personal confessions



others have less important, but sensitive things to say



Private and anonymous communication

Bob

Alice

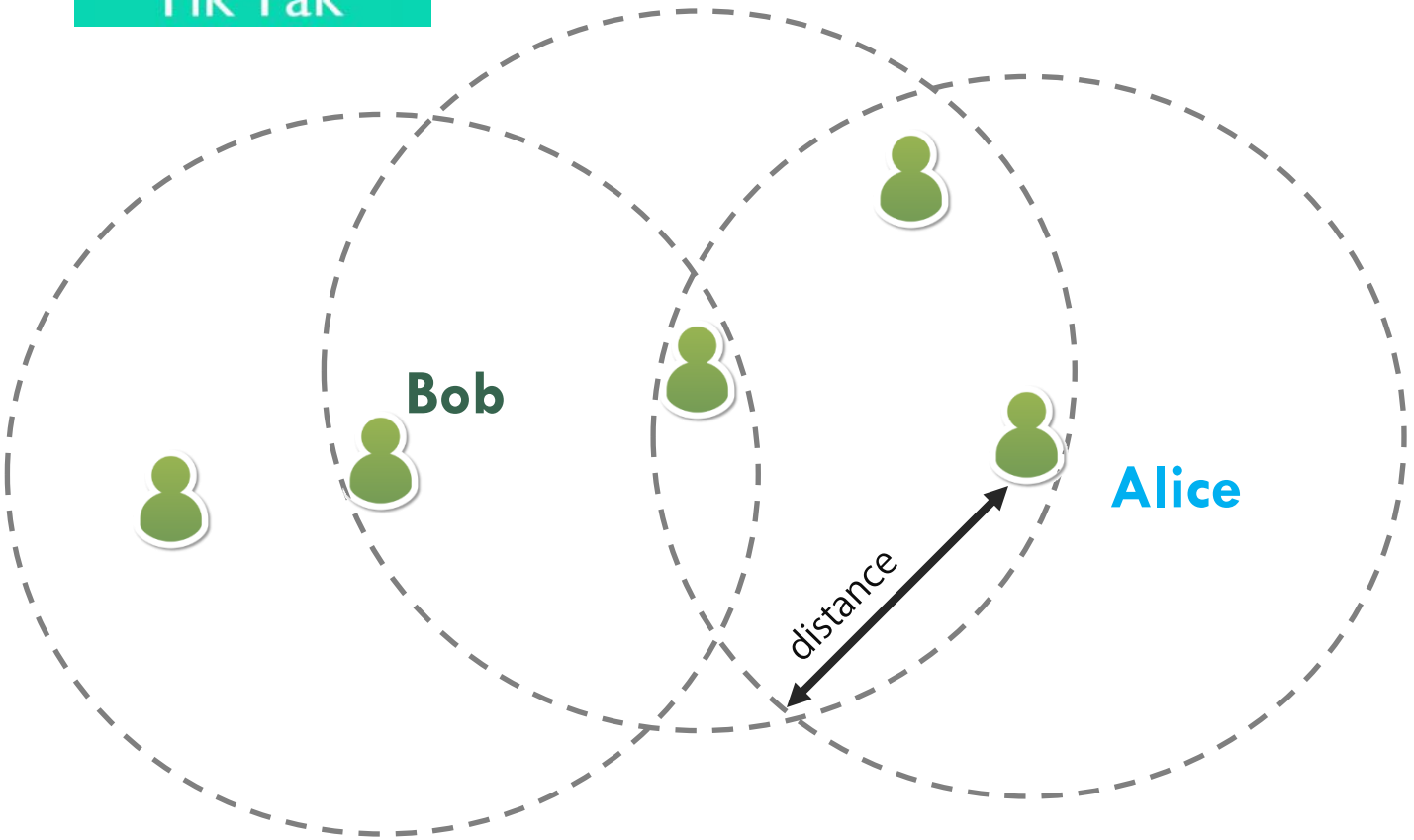
- the **data privacy** and **meta-data privacy** contexts

Part I:
Anonymous Communication

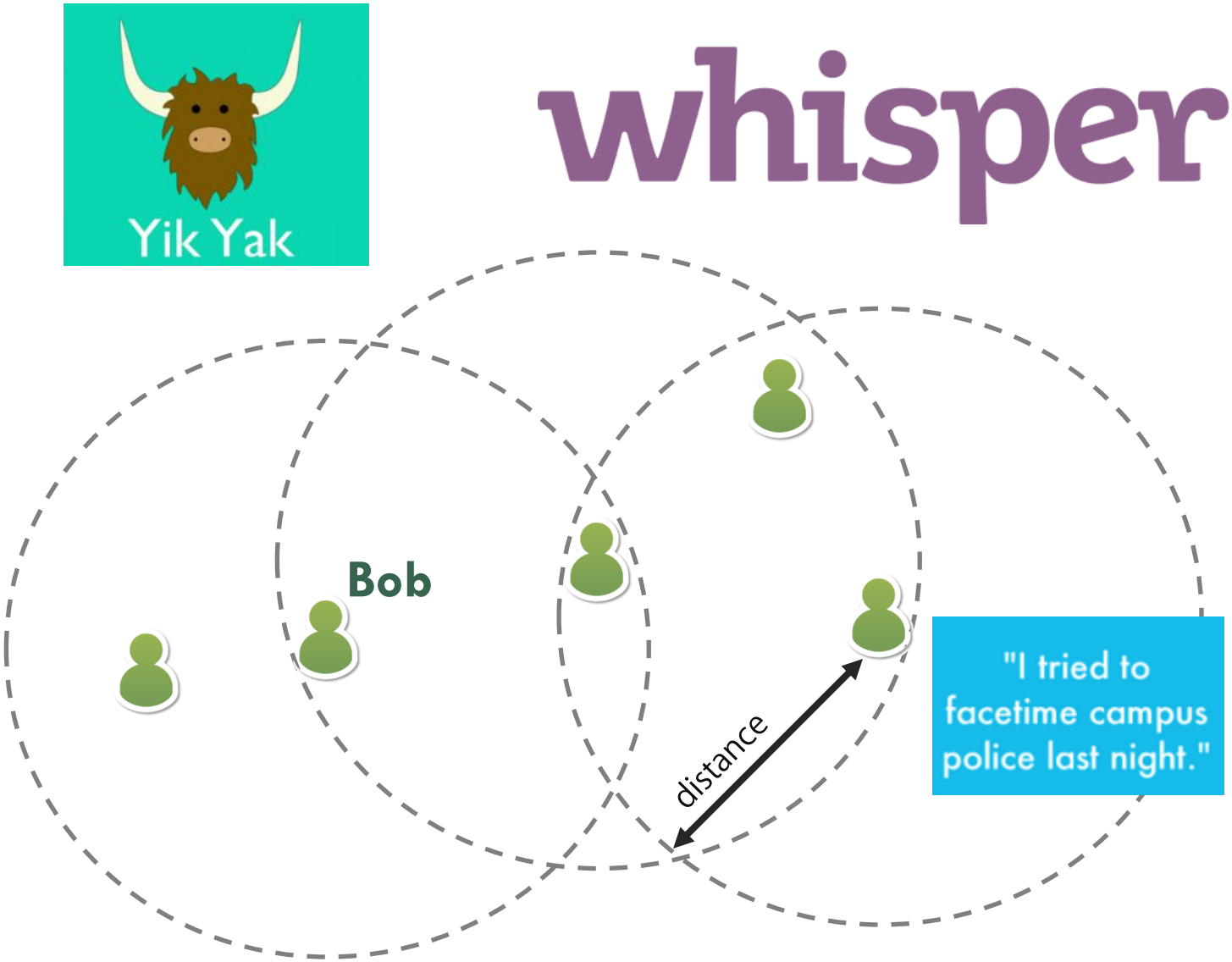
Existing anonymous messaging apps

Yik Yak

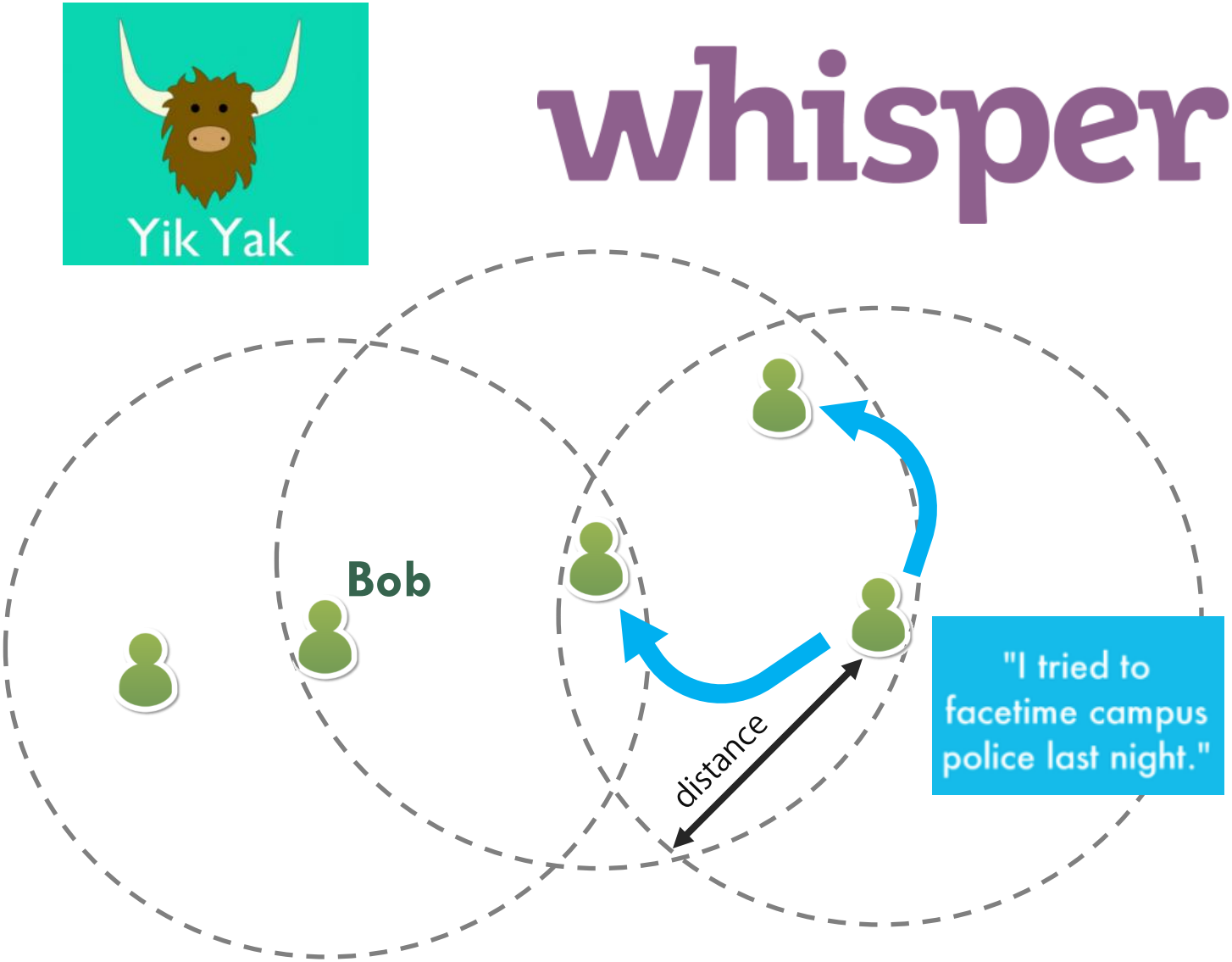
whisper



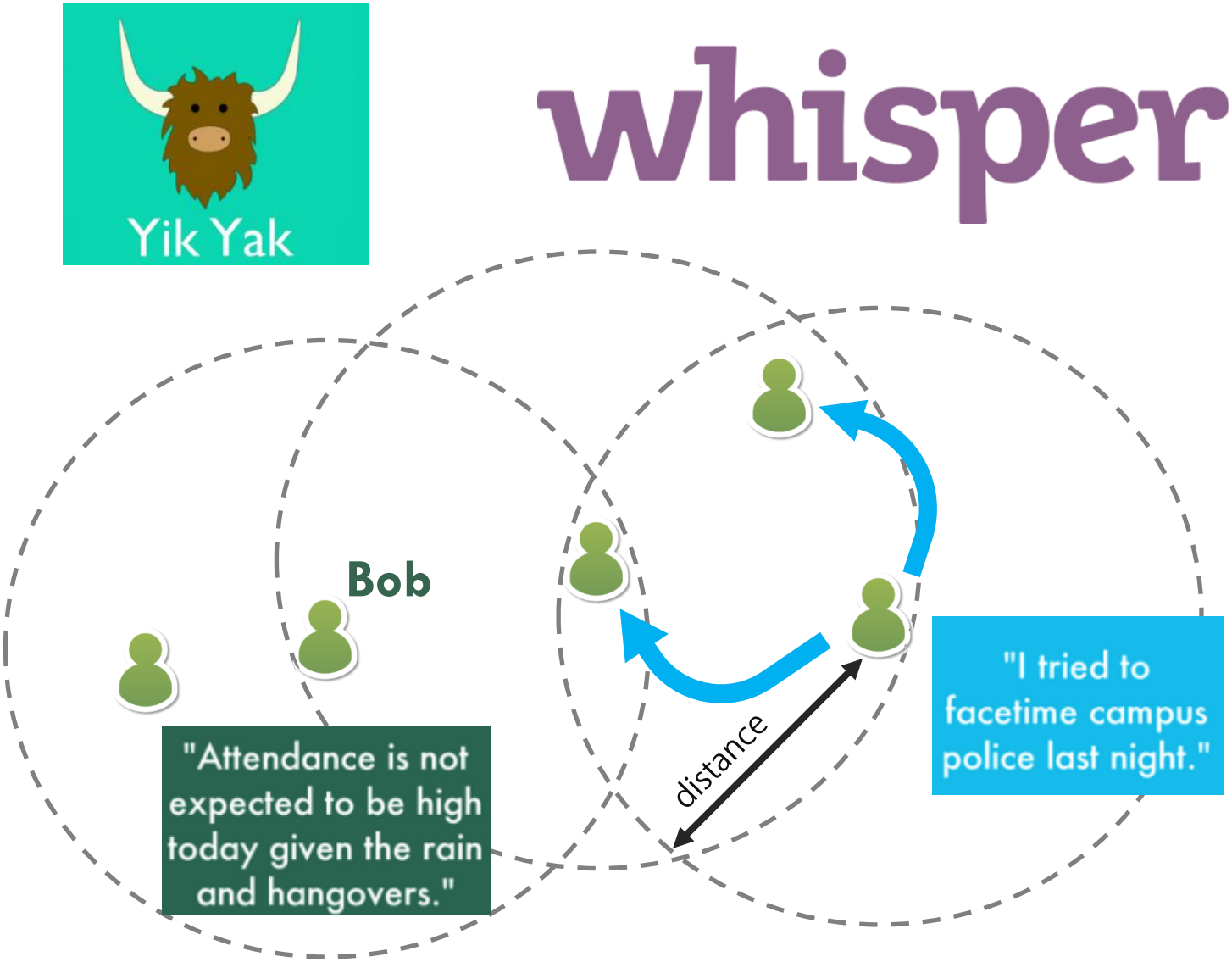
Existing anonymous messaging apps



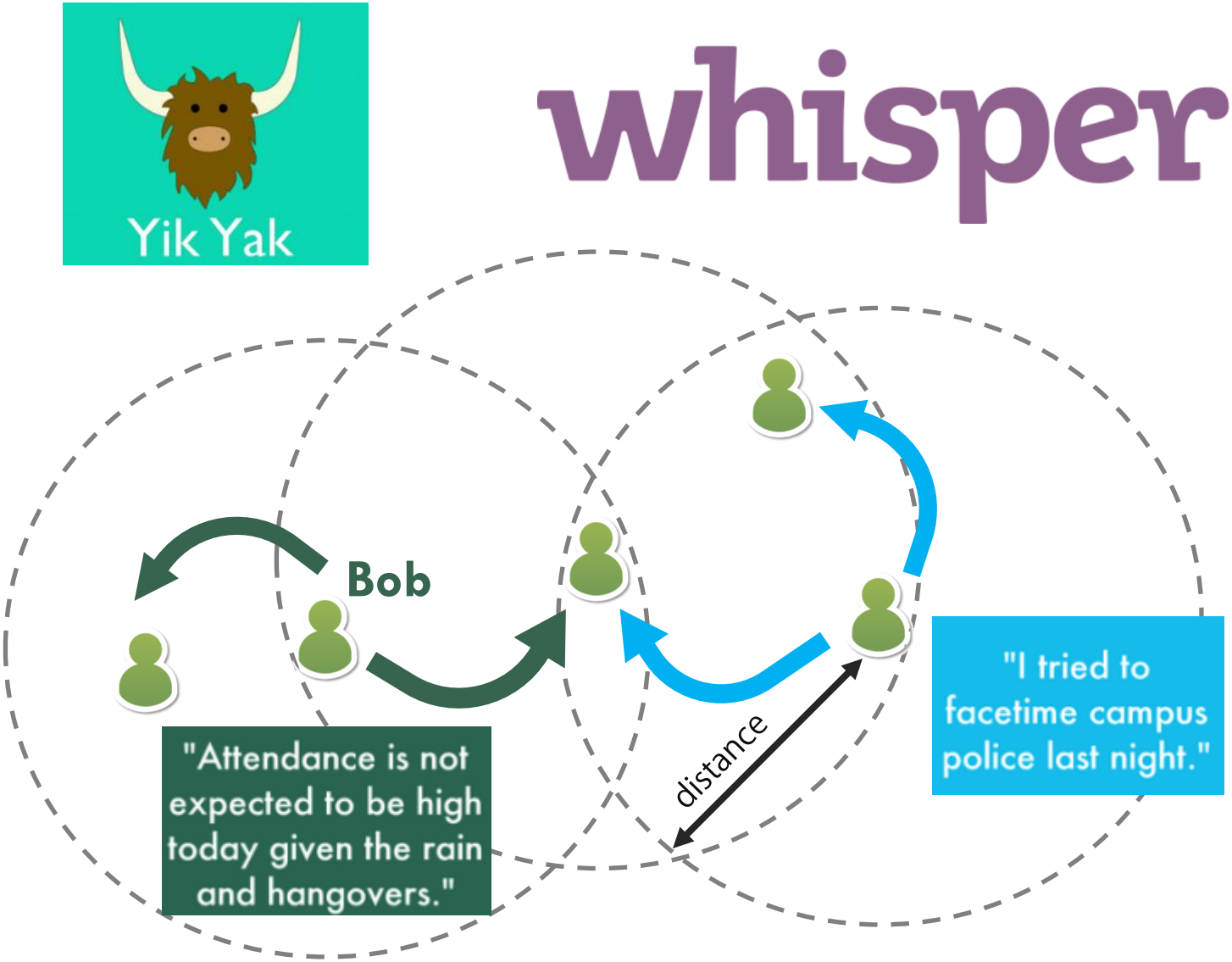
Existing anonymous messaging apps



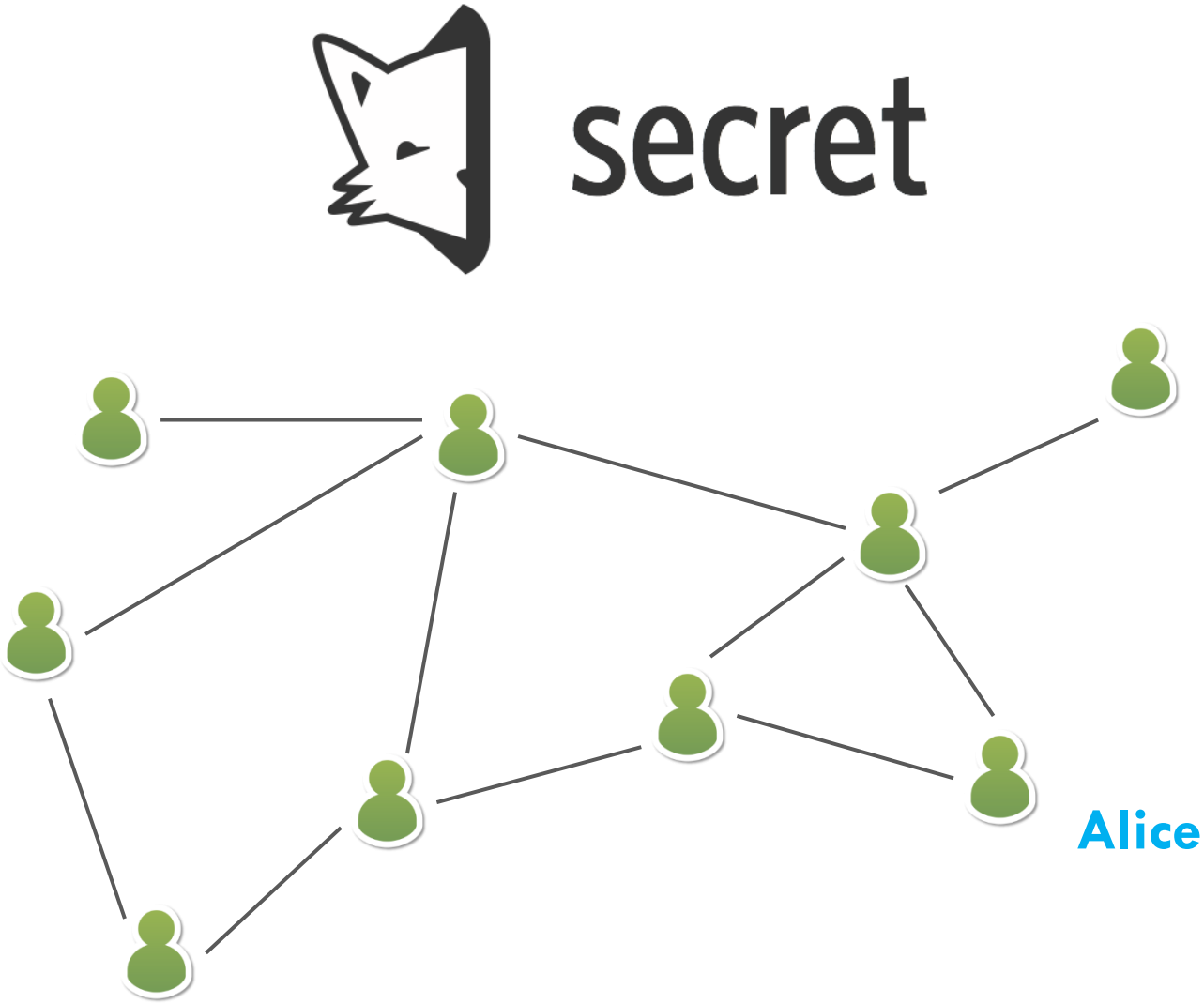
Existing anonymous messaging apps



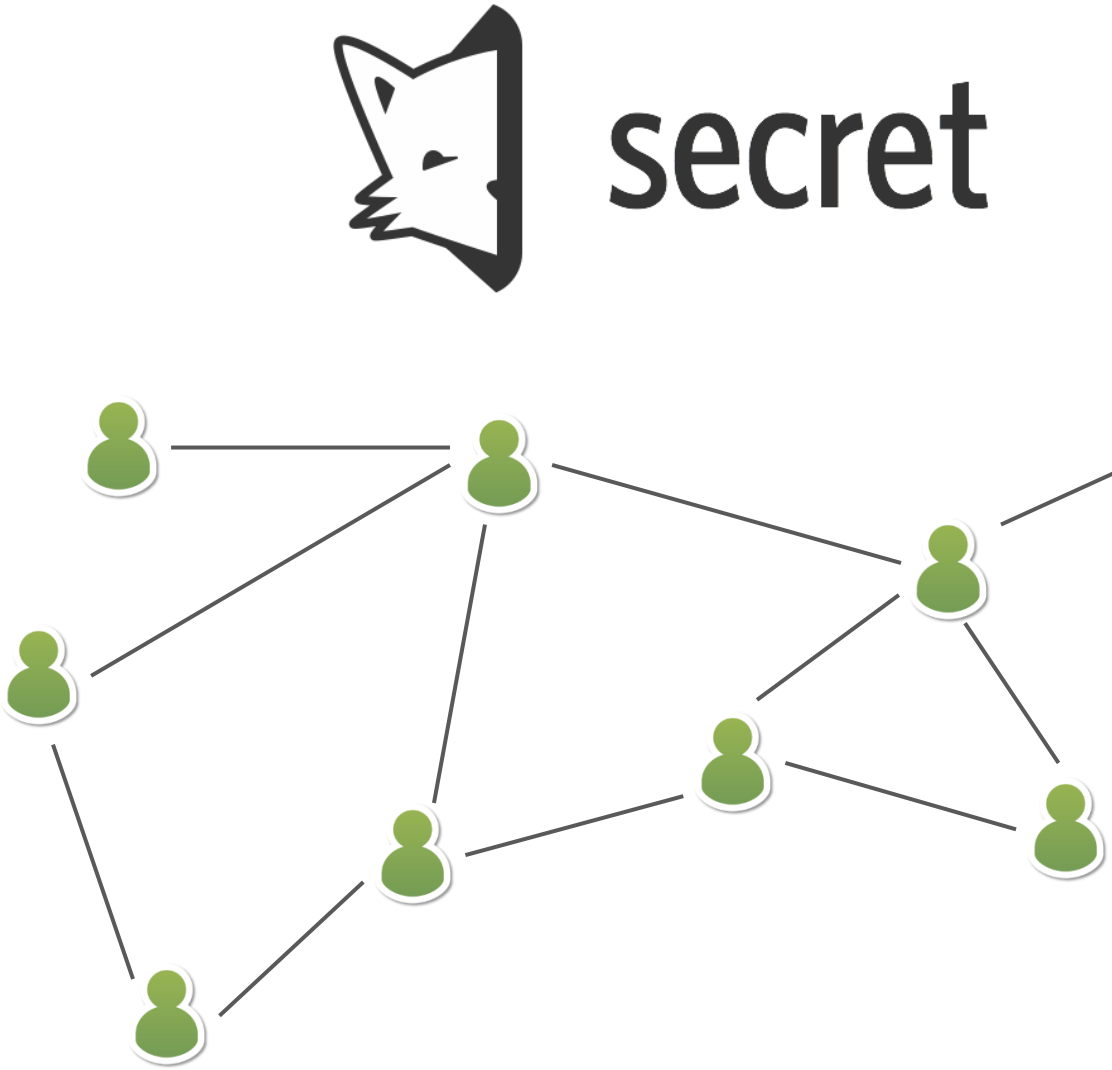
Existing anonymous messaging apps



Existing anonymous messaging apps

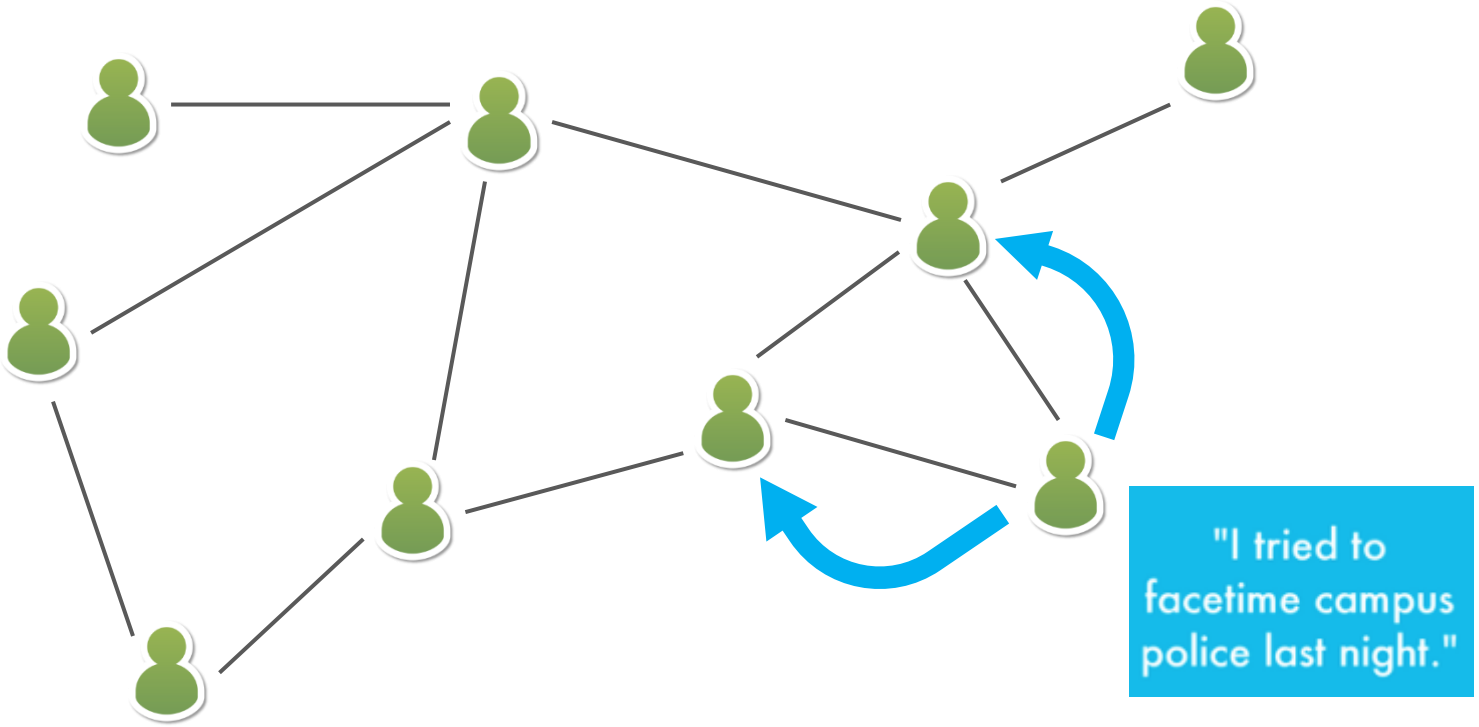


Existing anonymous messaging apps



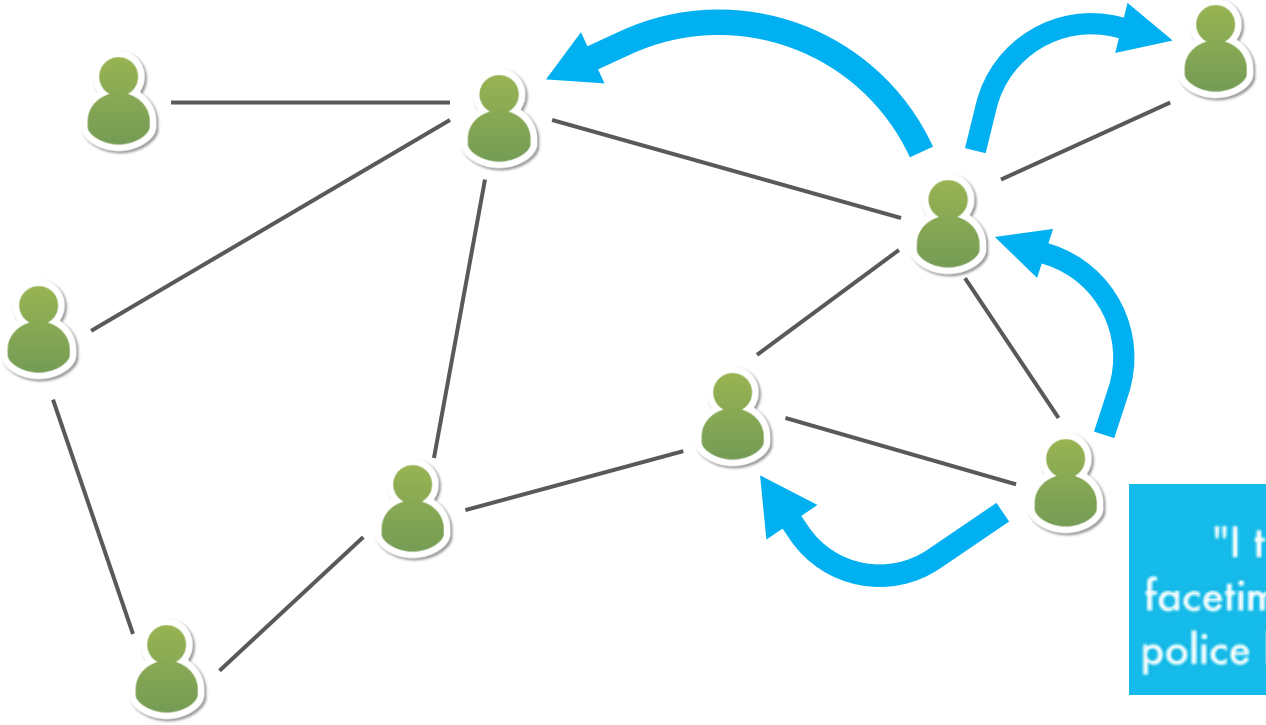
Existing anonymous messaging apps

secret

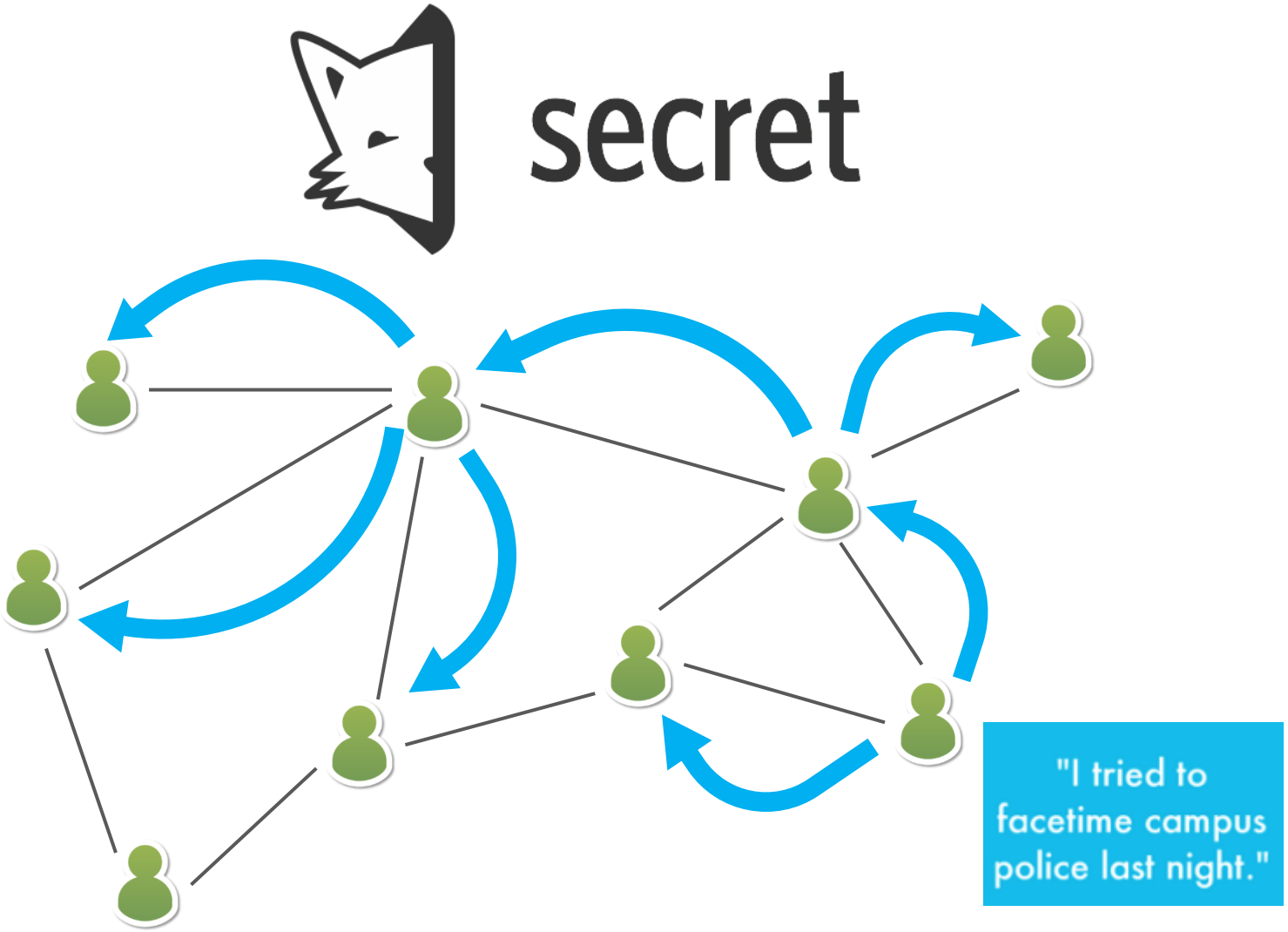


Existing anonymous messaging apps

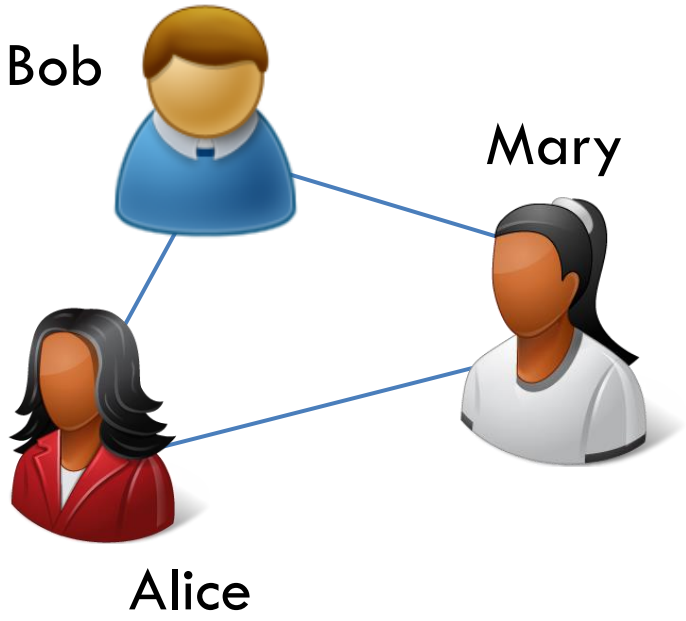
secret



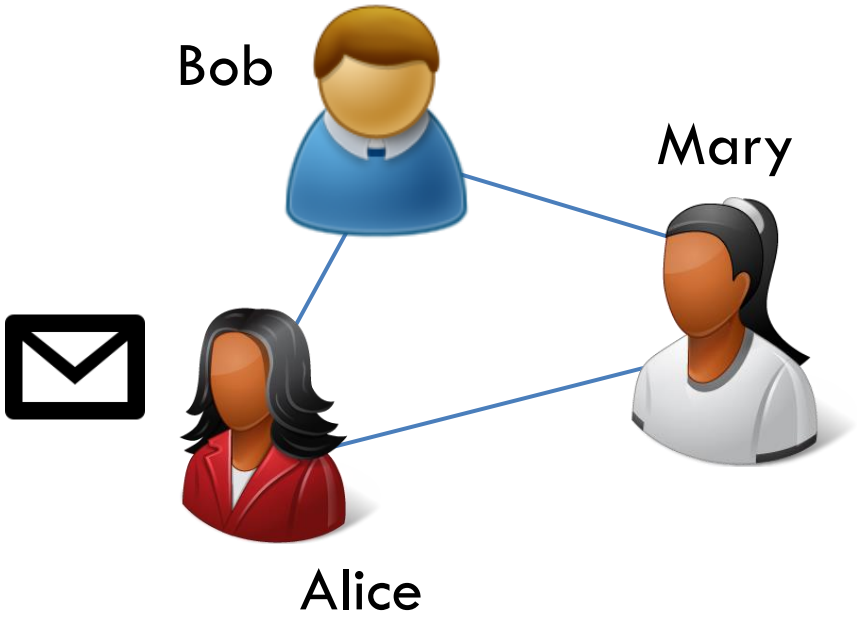
Existing anonymous messaging apps



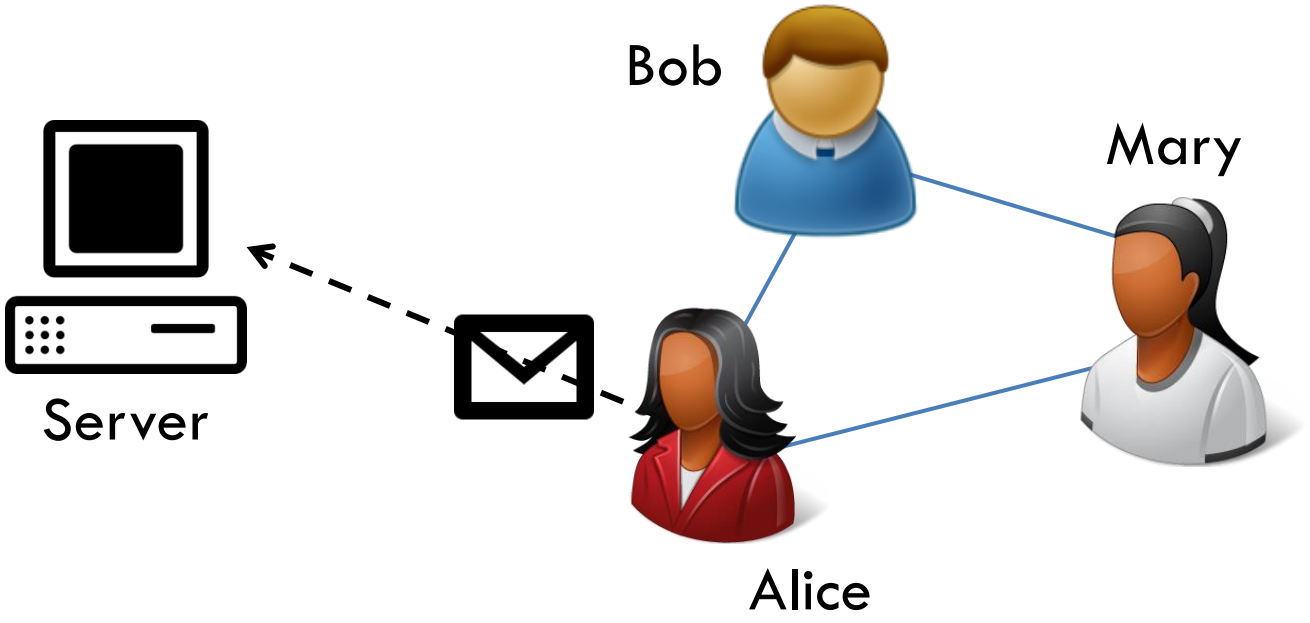
Existing anonymous messaging apps



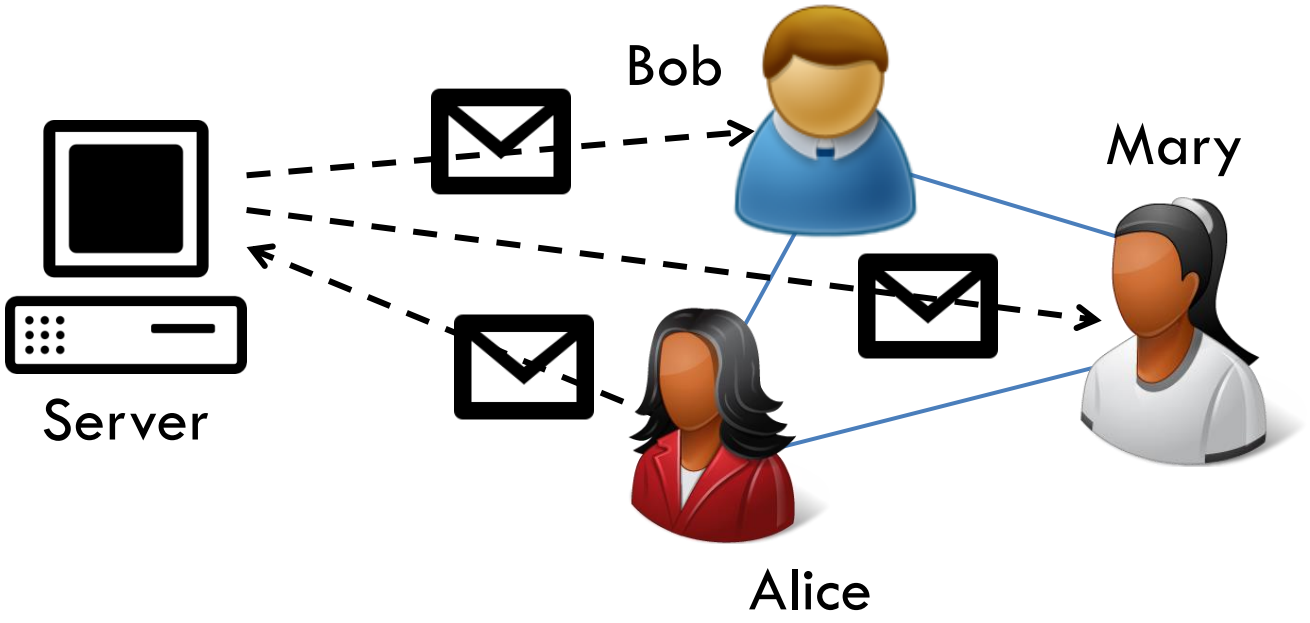
Existing anonymous messaging apps



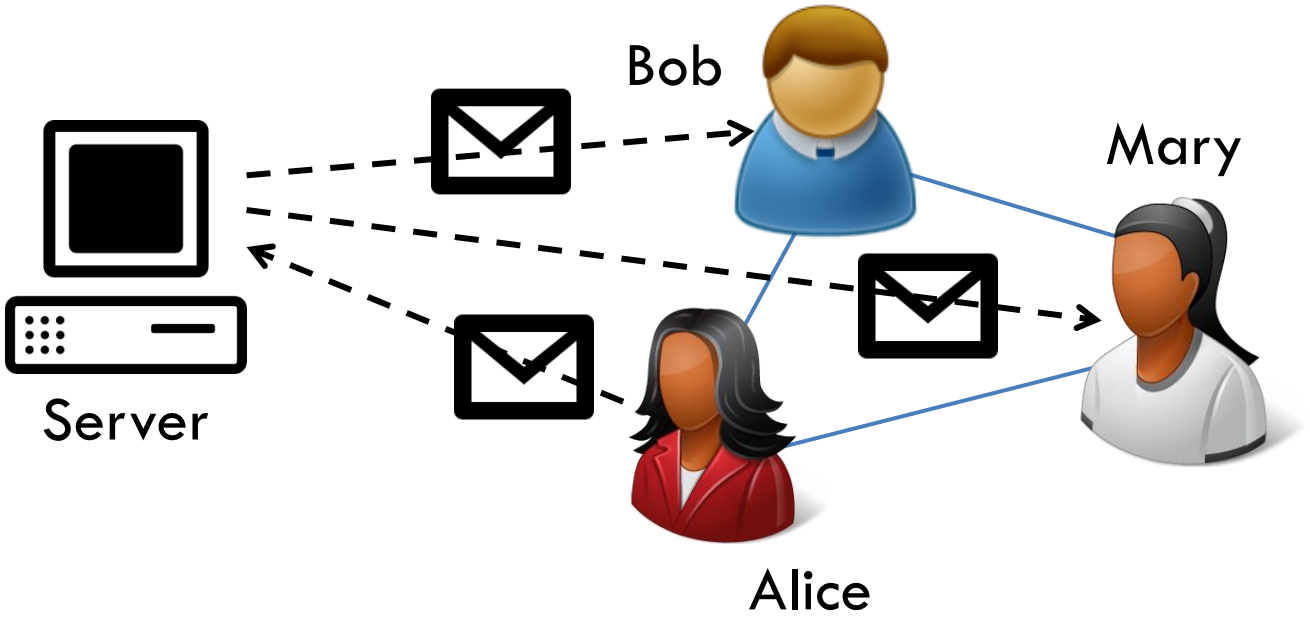
Existing anonymous messaging apps



Existing anonymous messaging apps



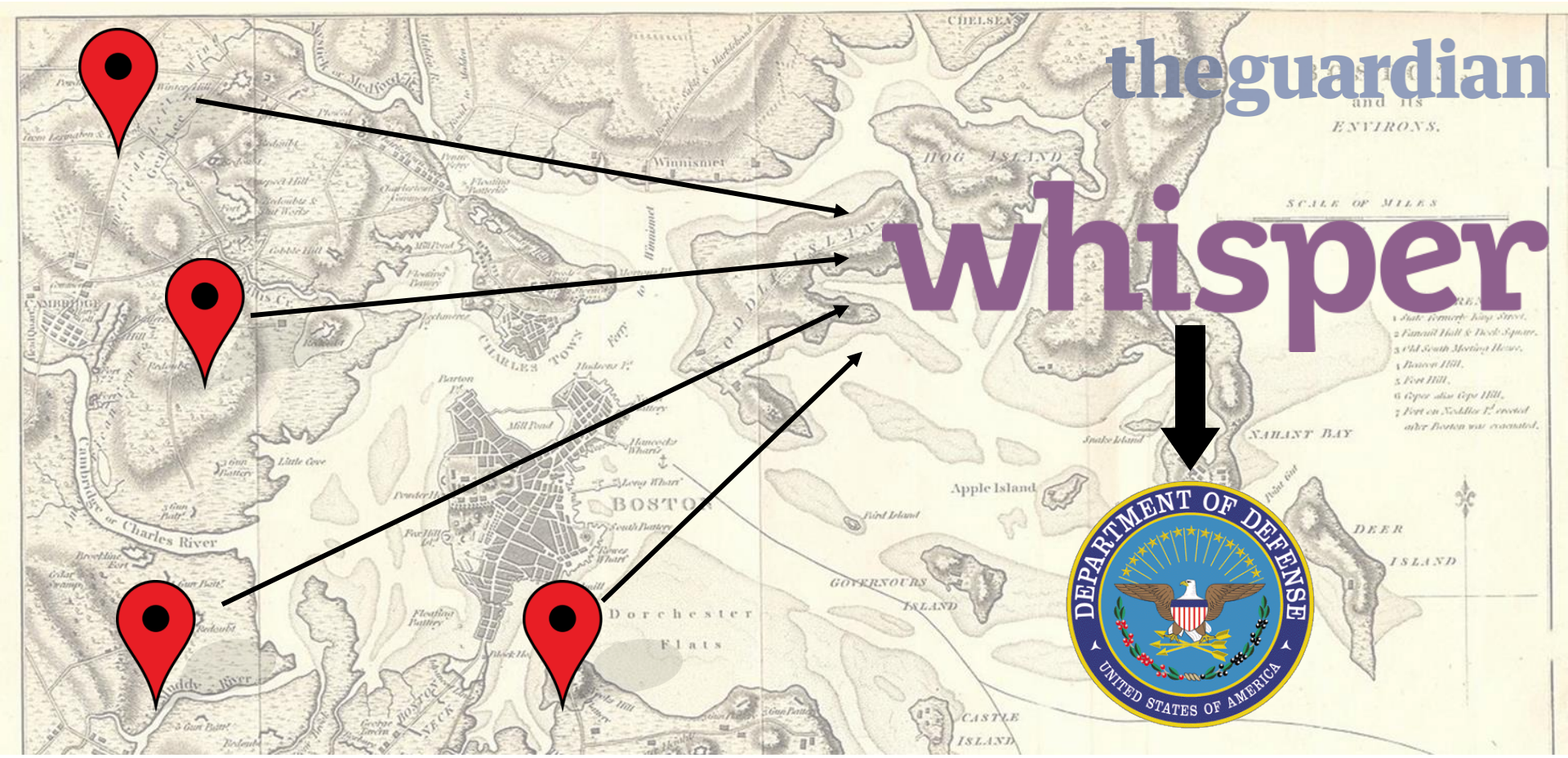
Existing anonymous messaging apps



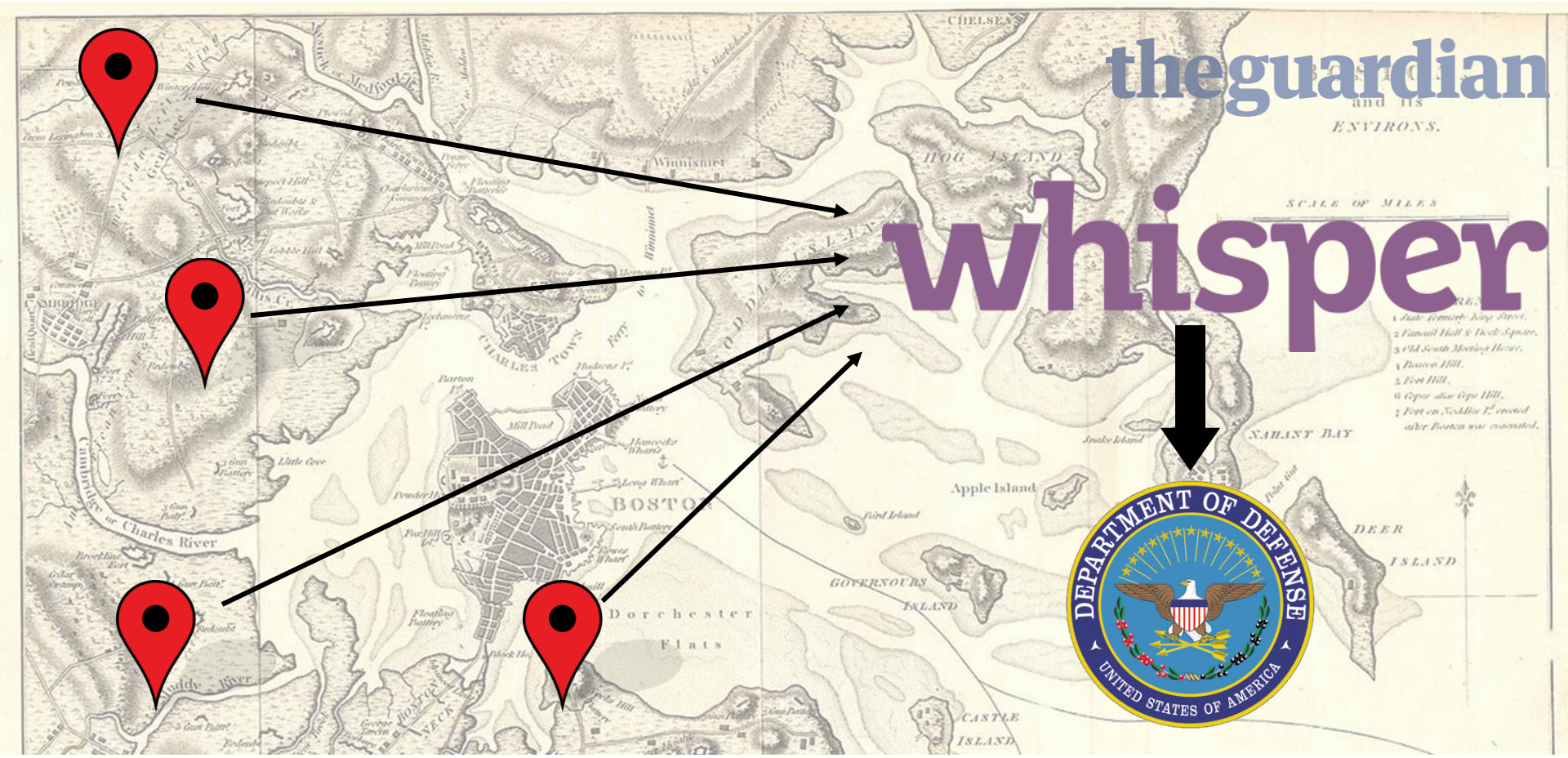
centralized networks are not truly anonymous!

Compromises in anonymity

Compromises in anonymity

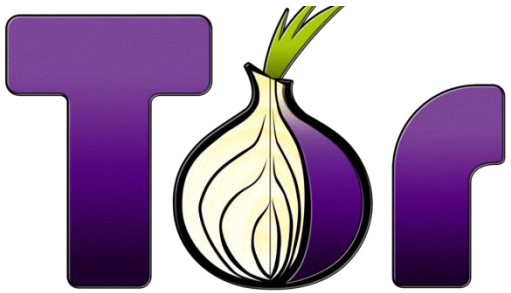


Compromises in anonymity



anonymity loss extends beyond the network

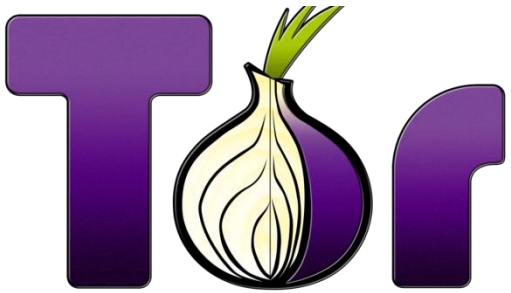
Anonymous communication



OneSwarm

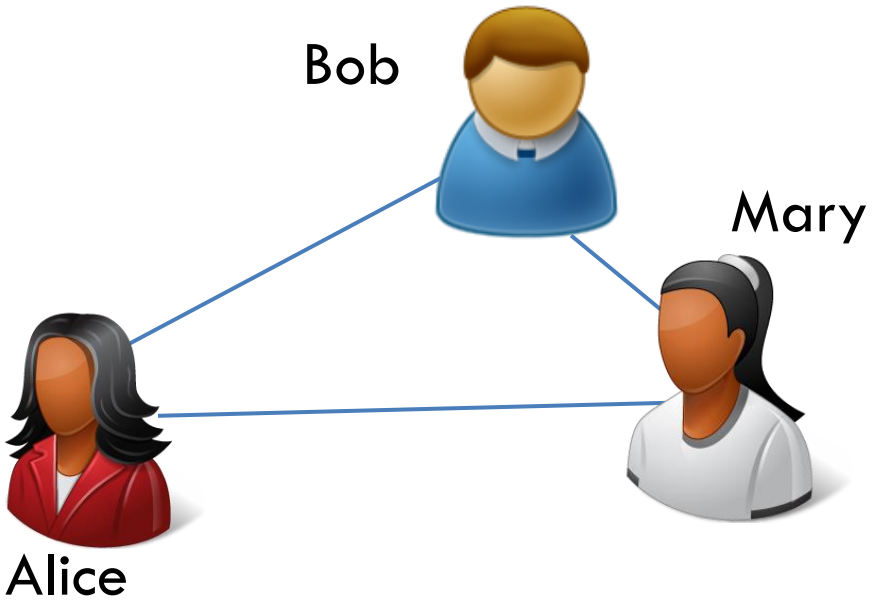
Privacy preserving peer-to-peer data sharing

Anonymous communication

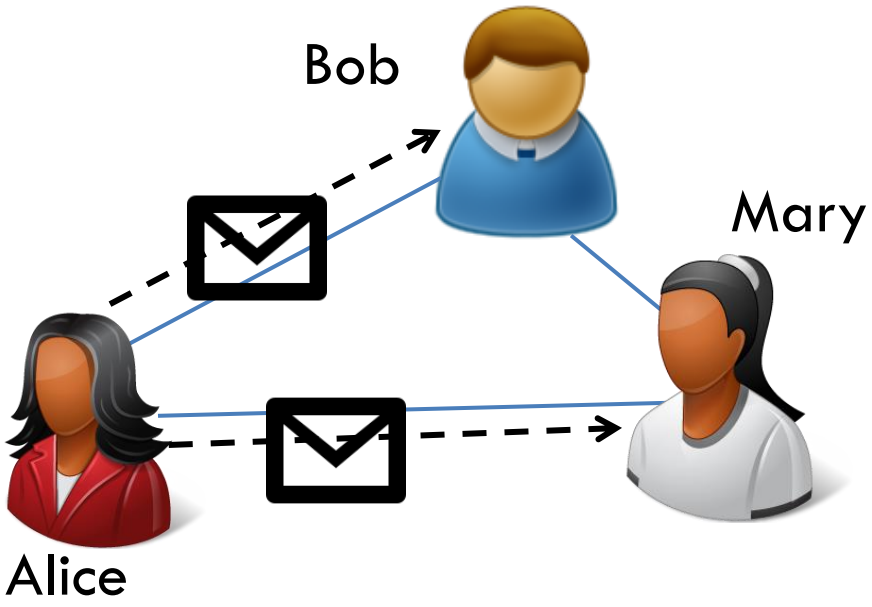


designed for point-to-point communication

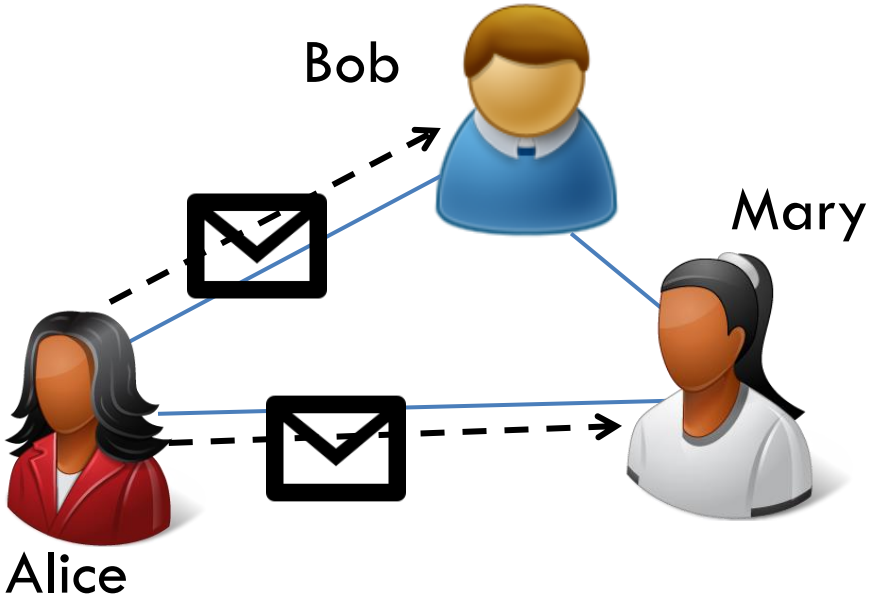
Distributed messaging



Distributed messaging

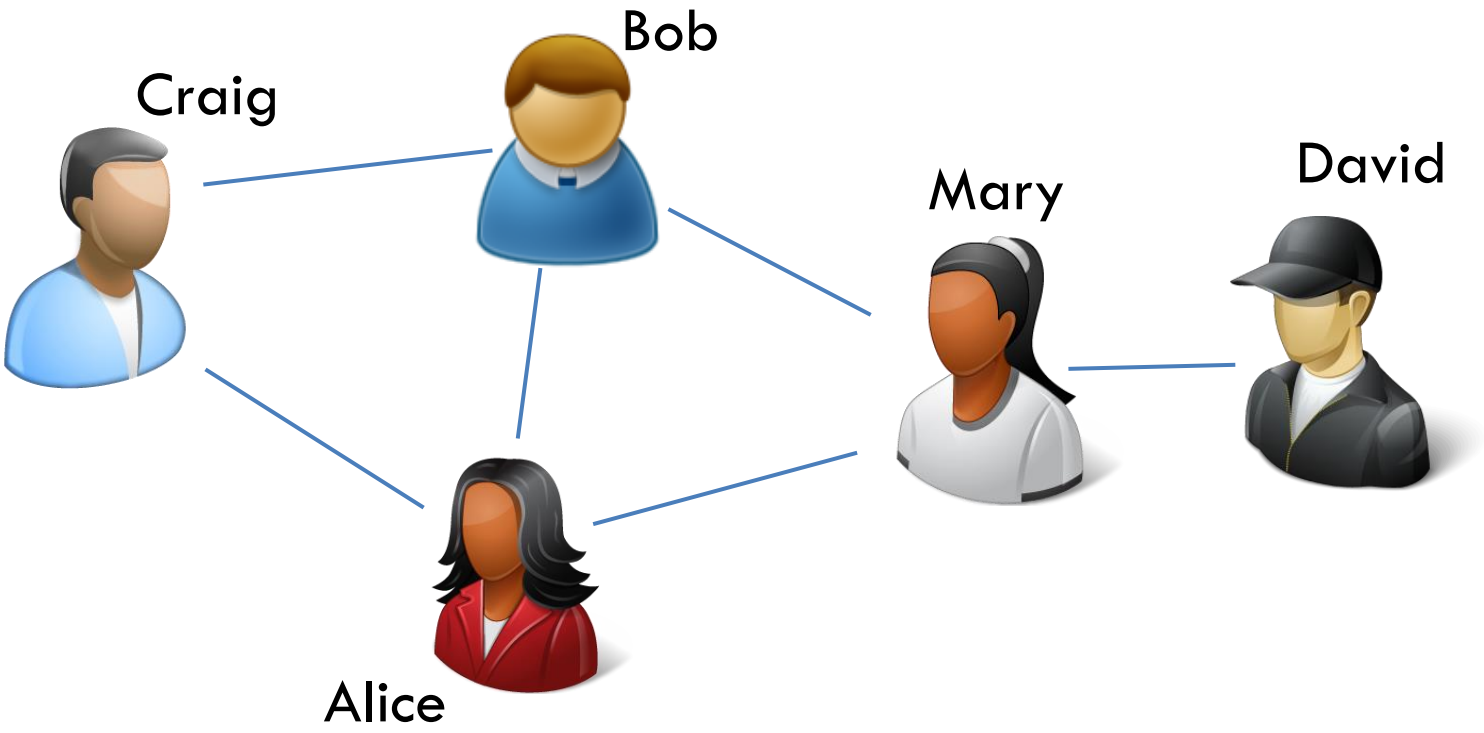


Distributed messaging

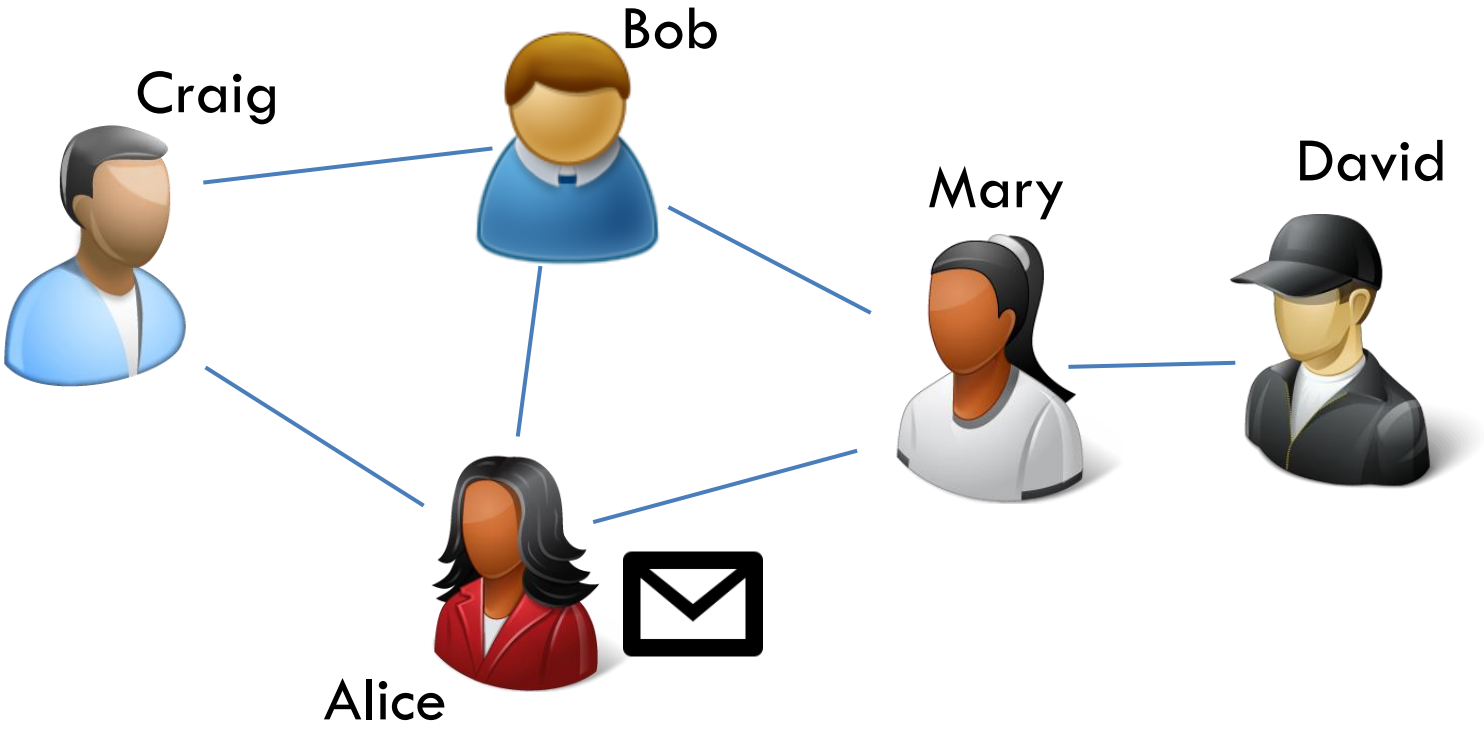


what can an adversary do?

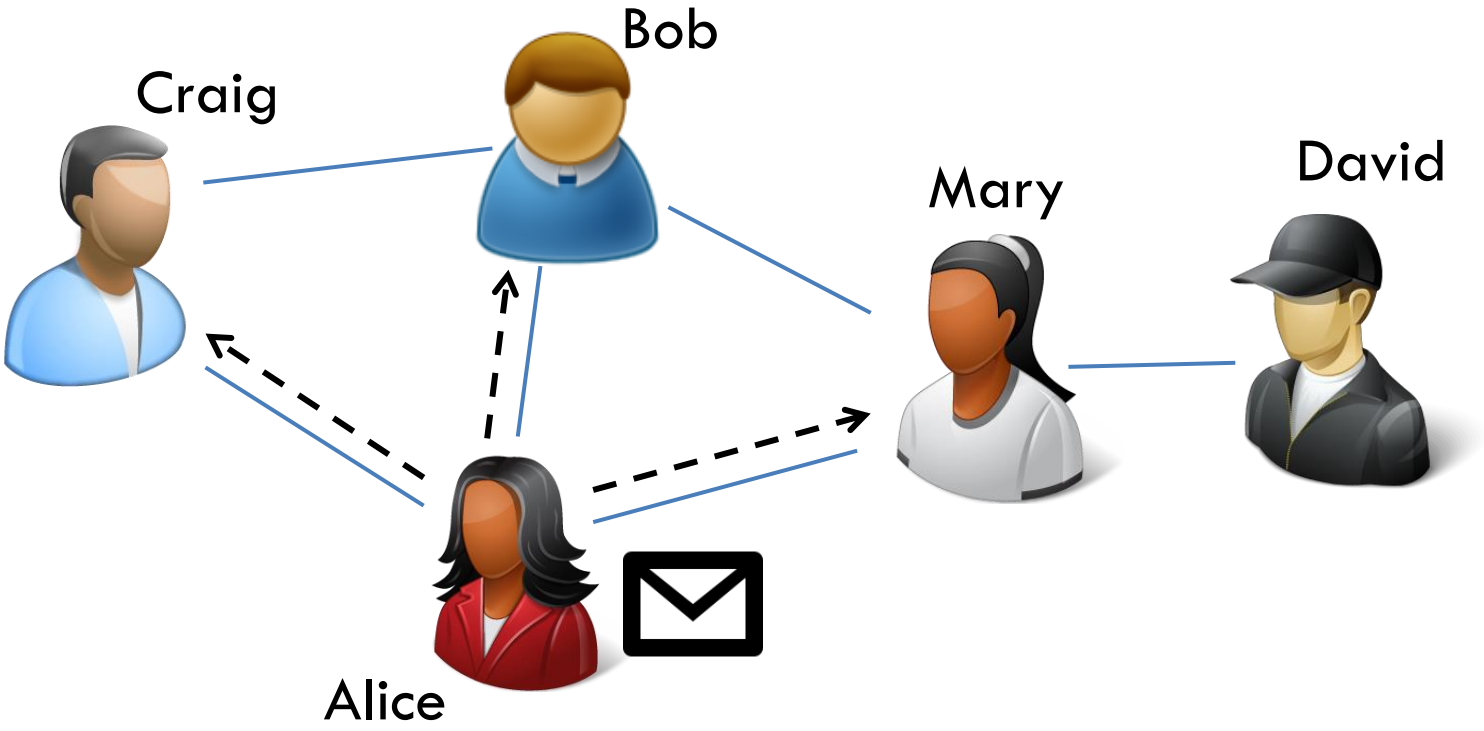
Adversary without timing



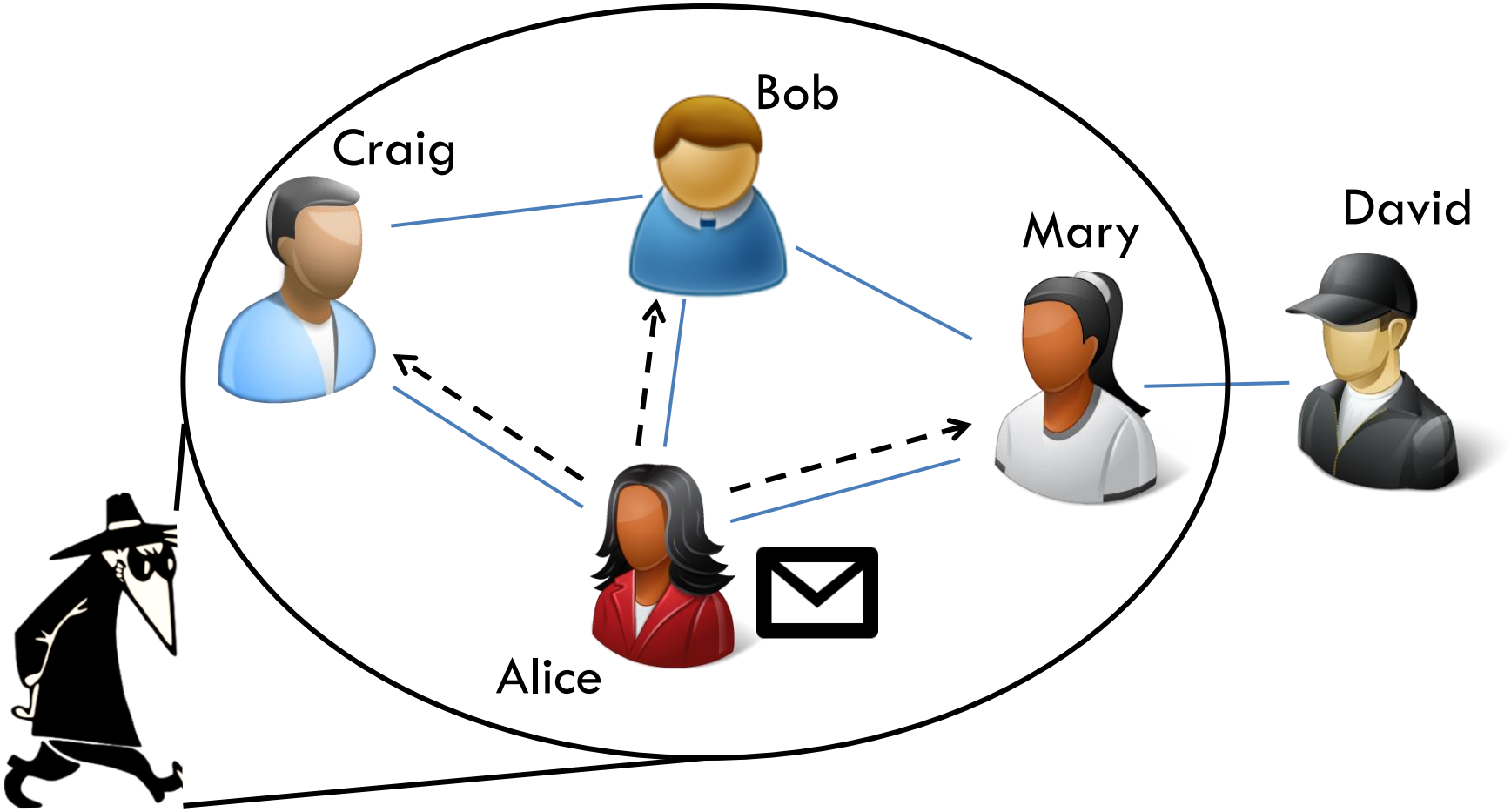
Adversary without timing



Adversary without timing

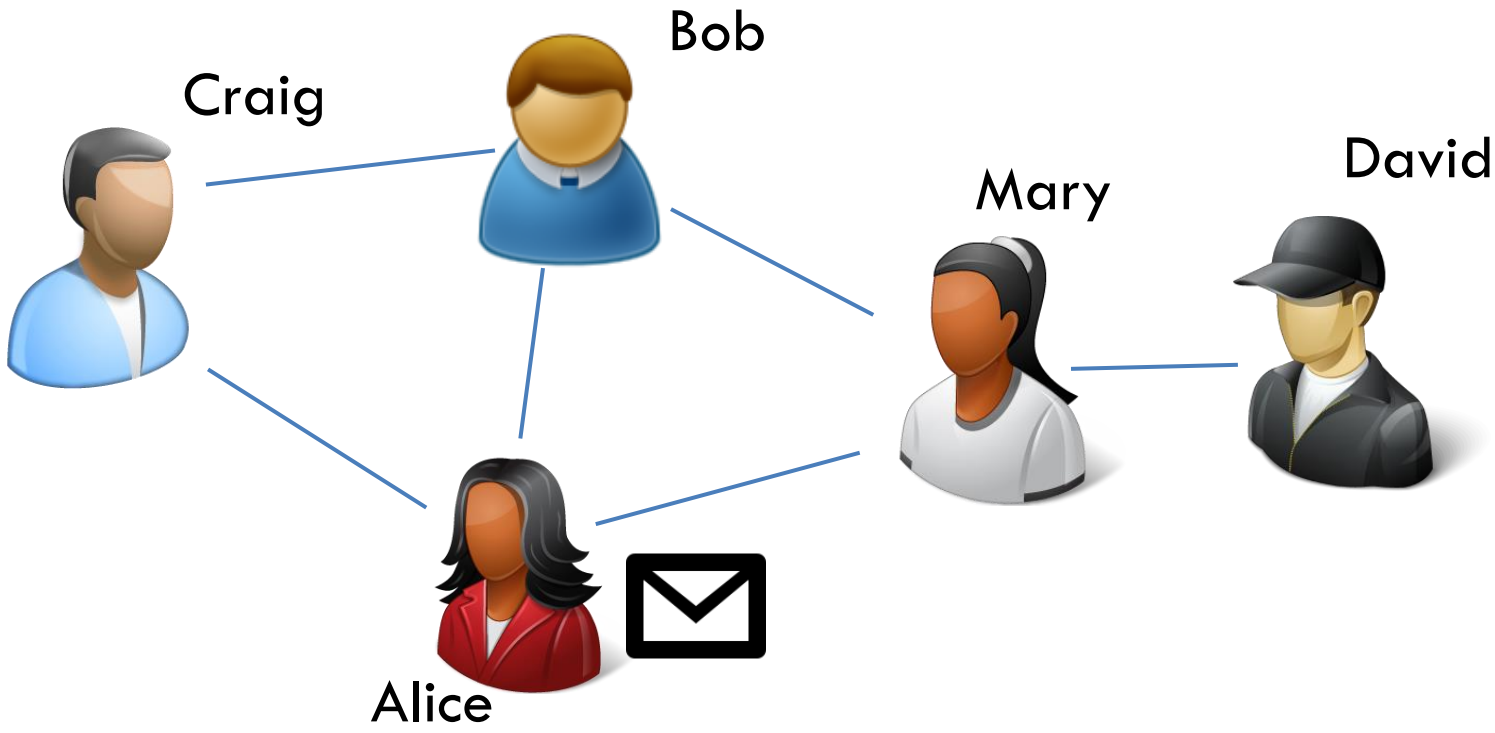


Adversary without timing

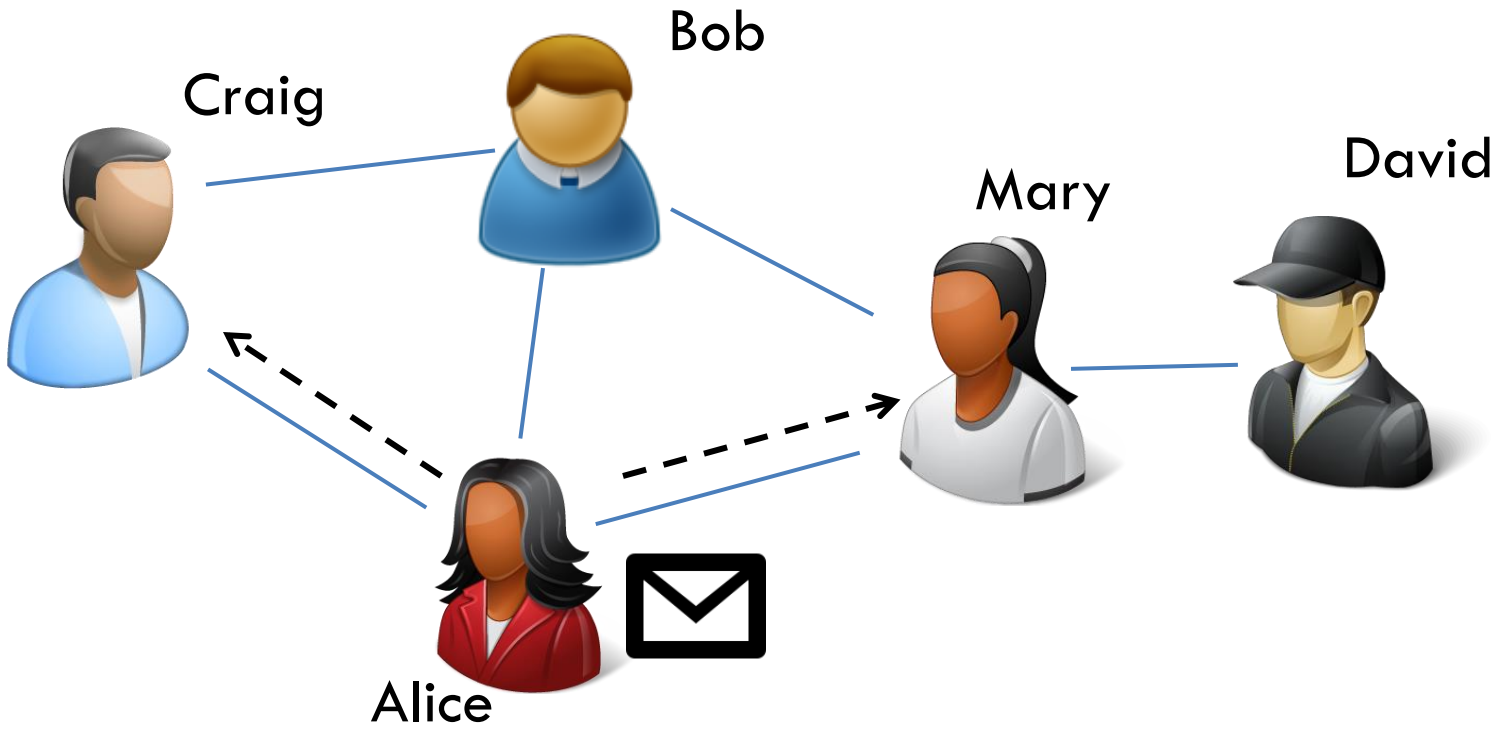


adversary can figure out who got the message

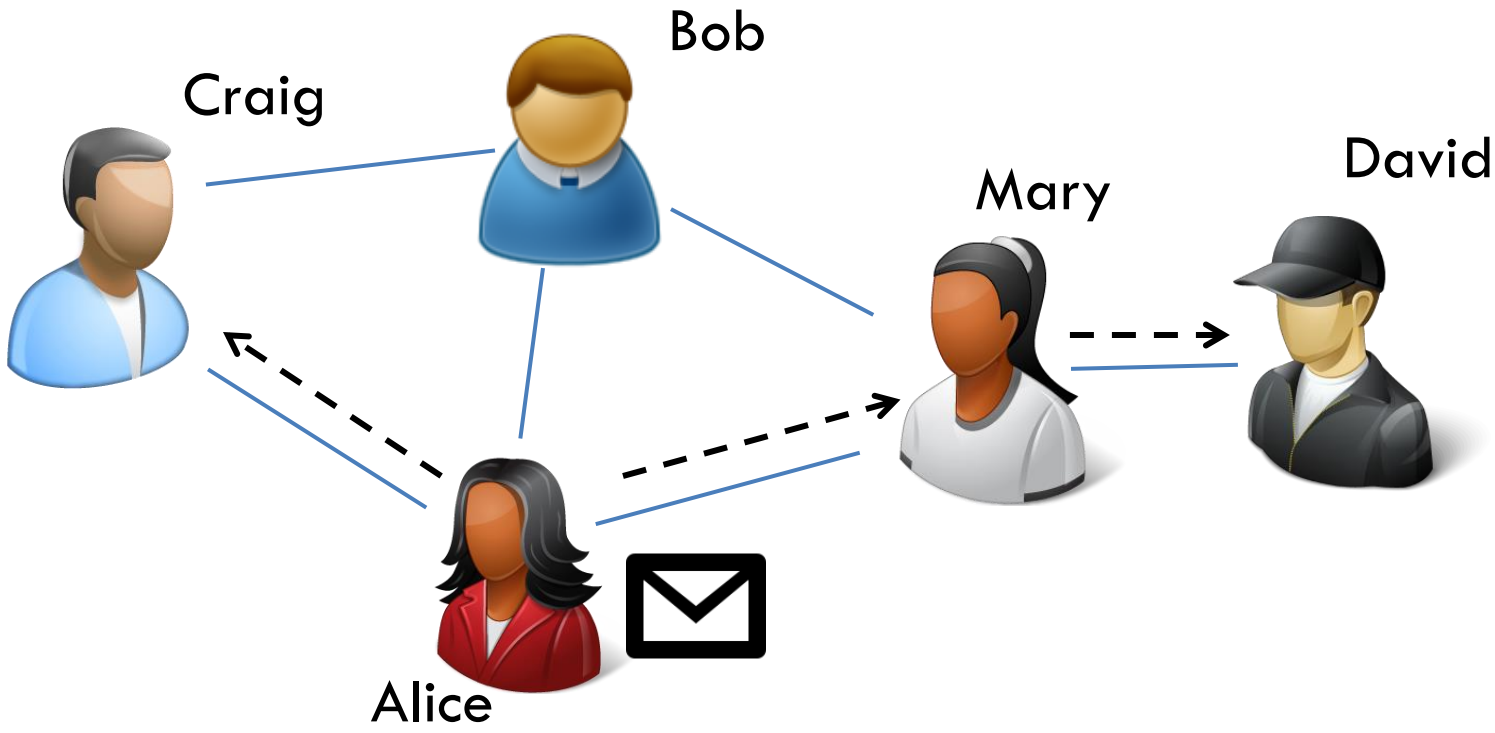
Adversary with timing



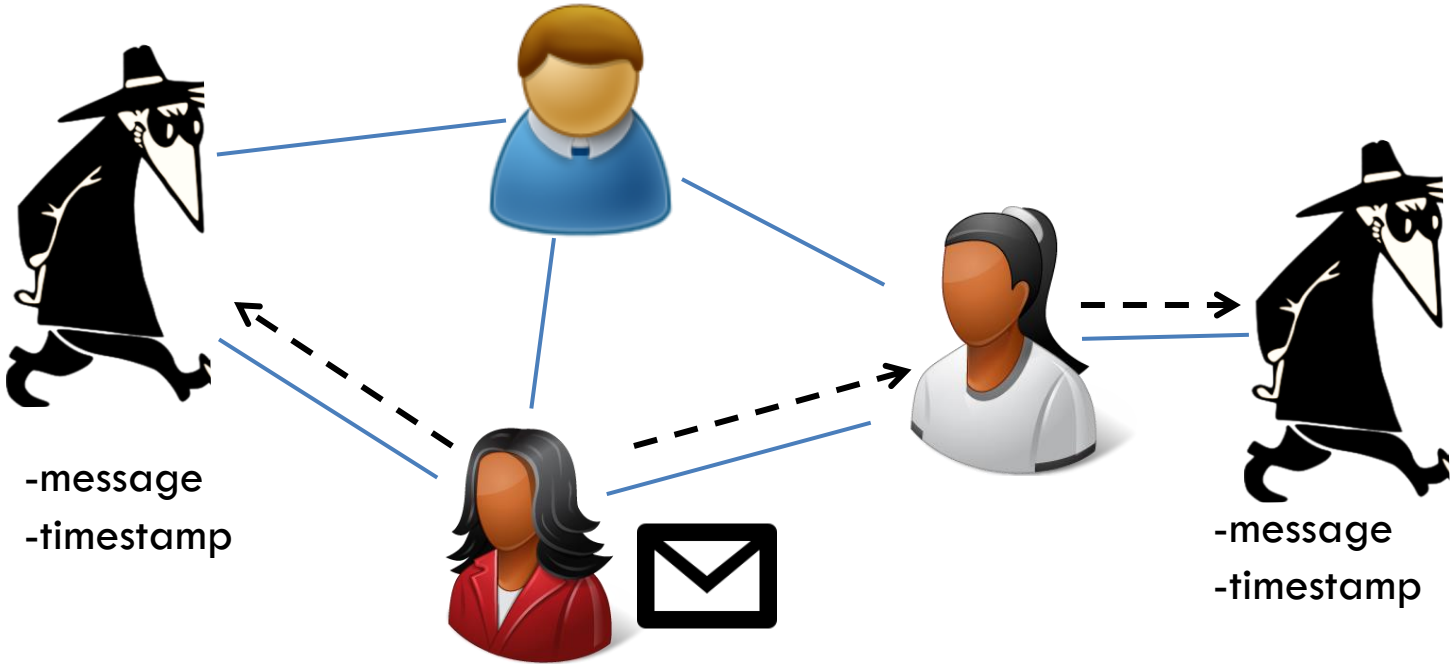
Adversary with timing



Adversary with timing

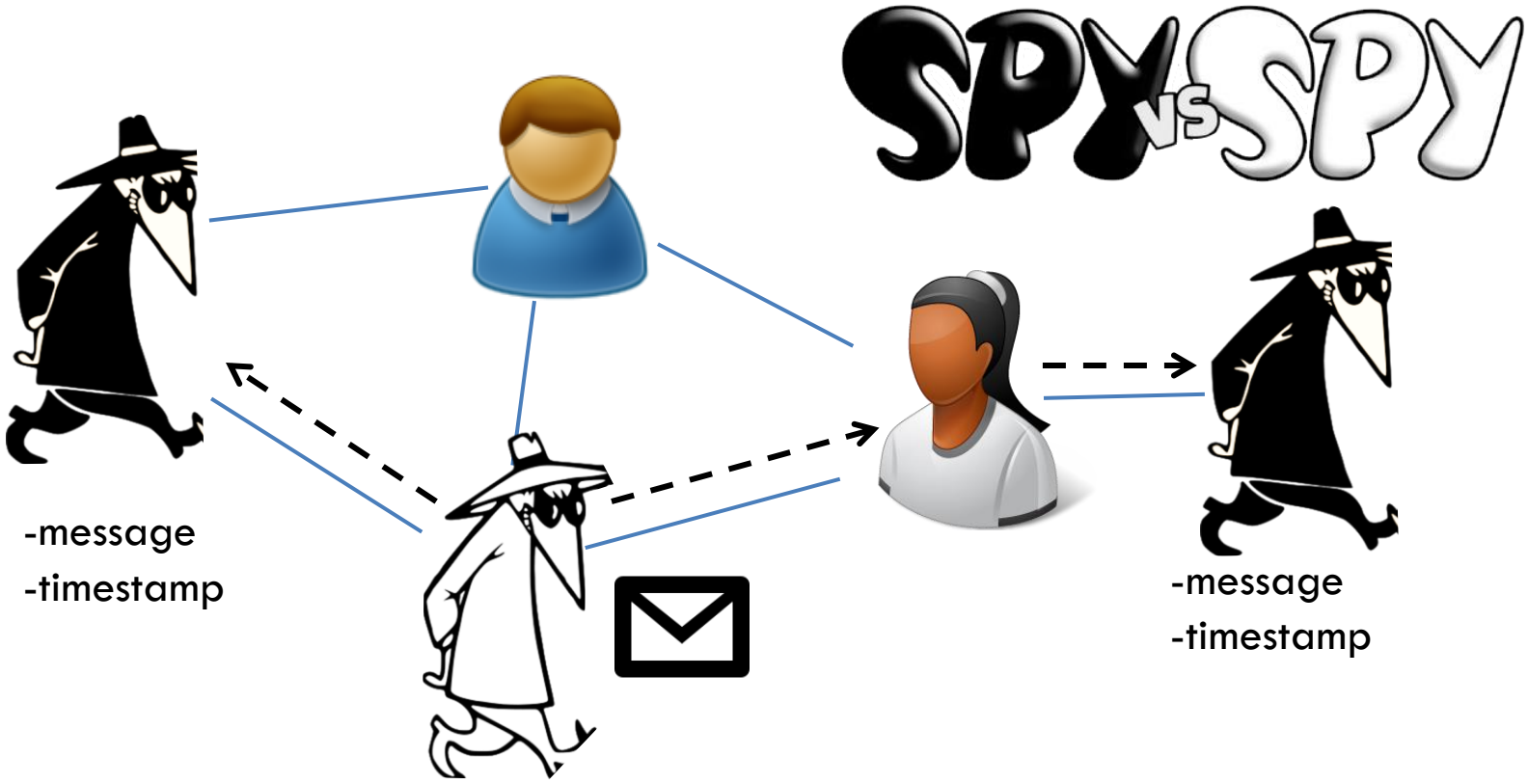


Adversary with timing



adversary can collect timing information

Adversary with timing

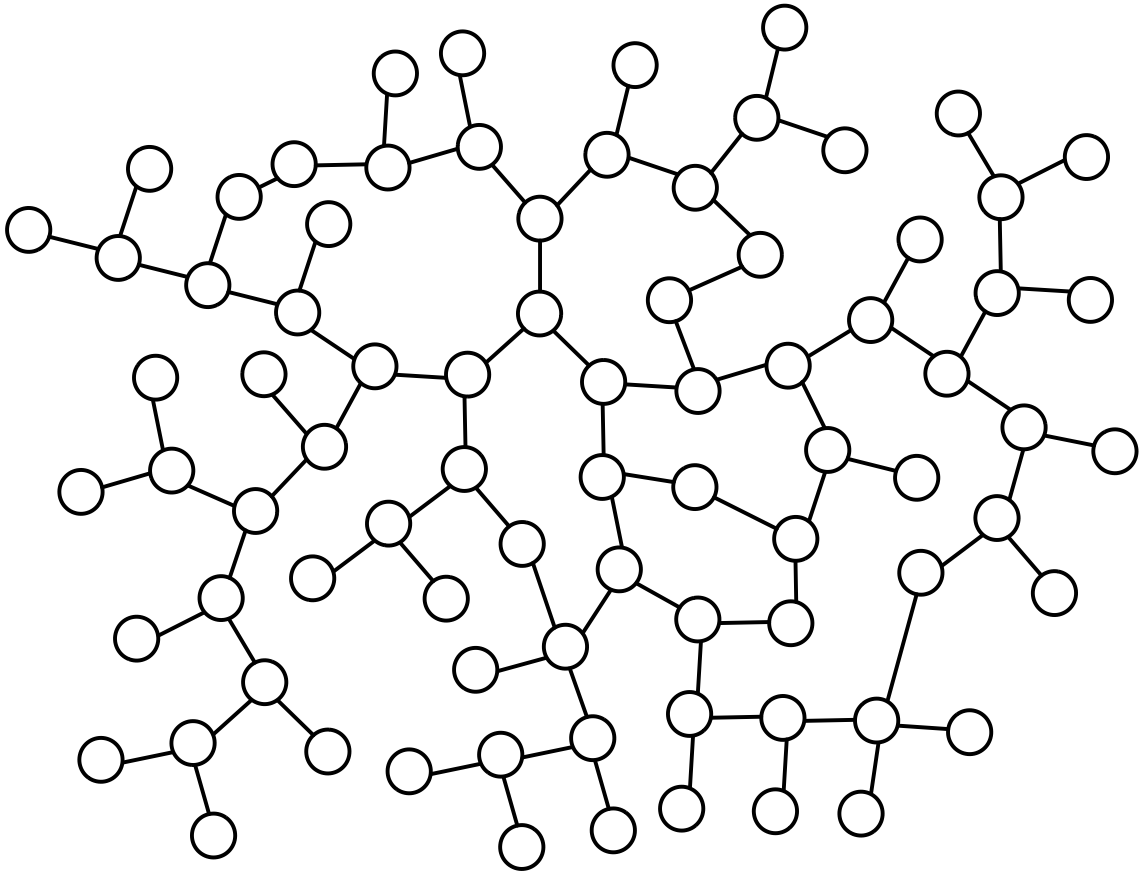


adversary can collect timing information

Distributed network forensics

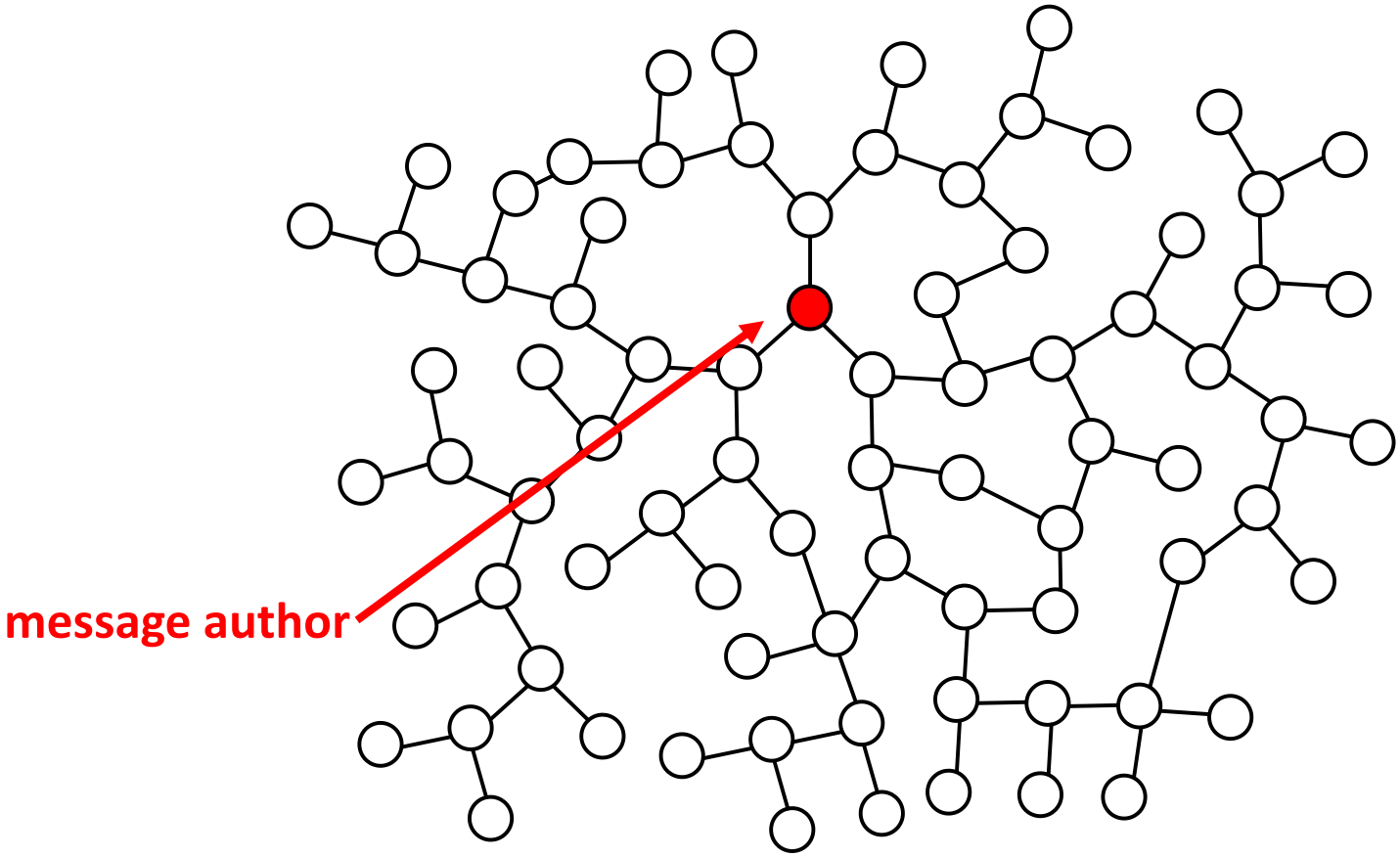
timing + who has the message = authorship

Information flow in social networks

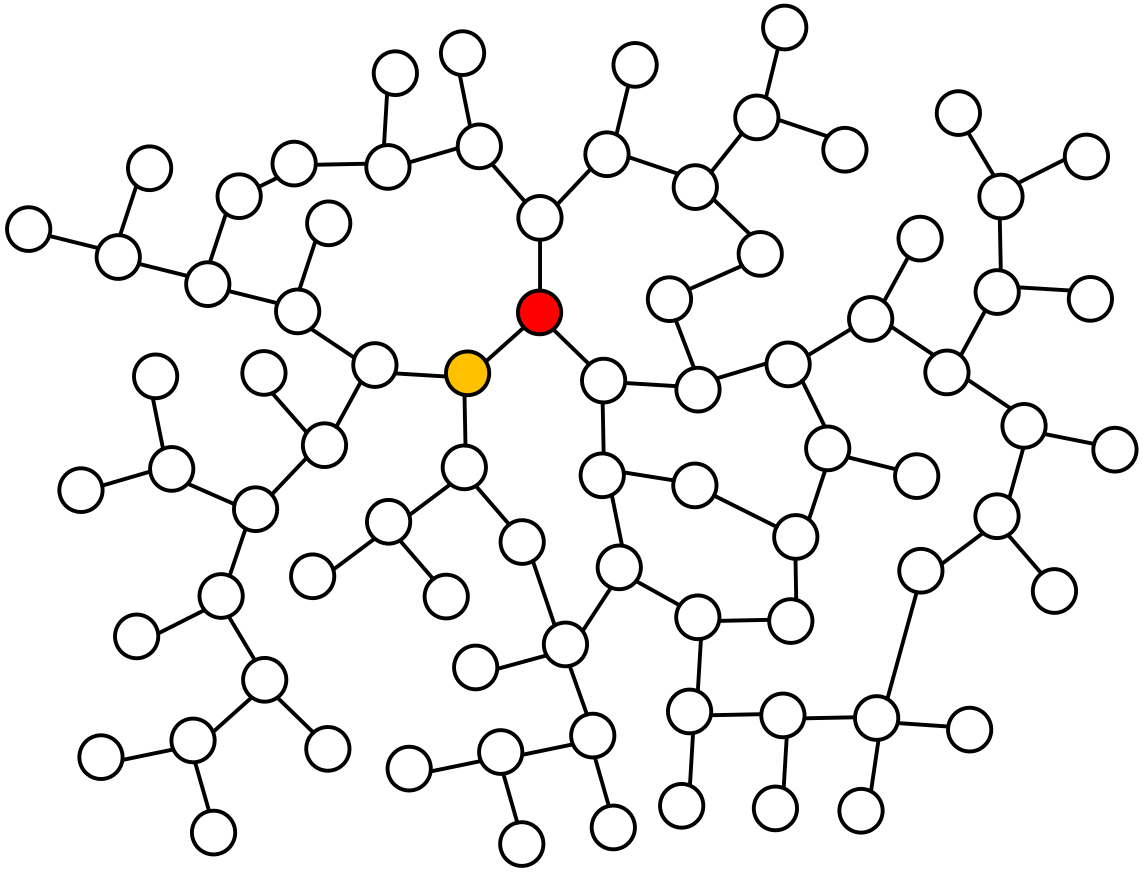


- G is the graph representing the social network

Information flow in social networks

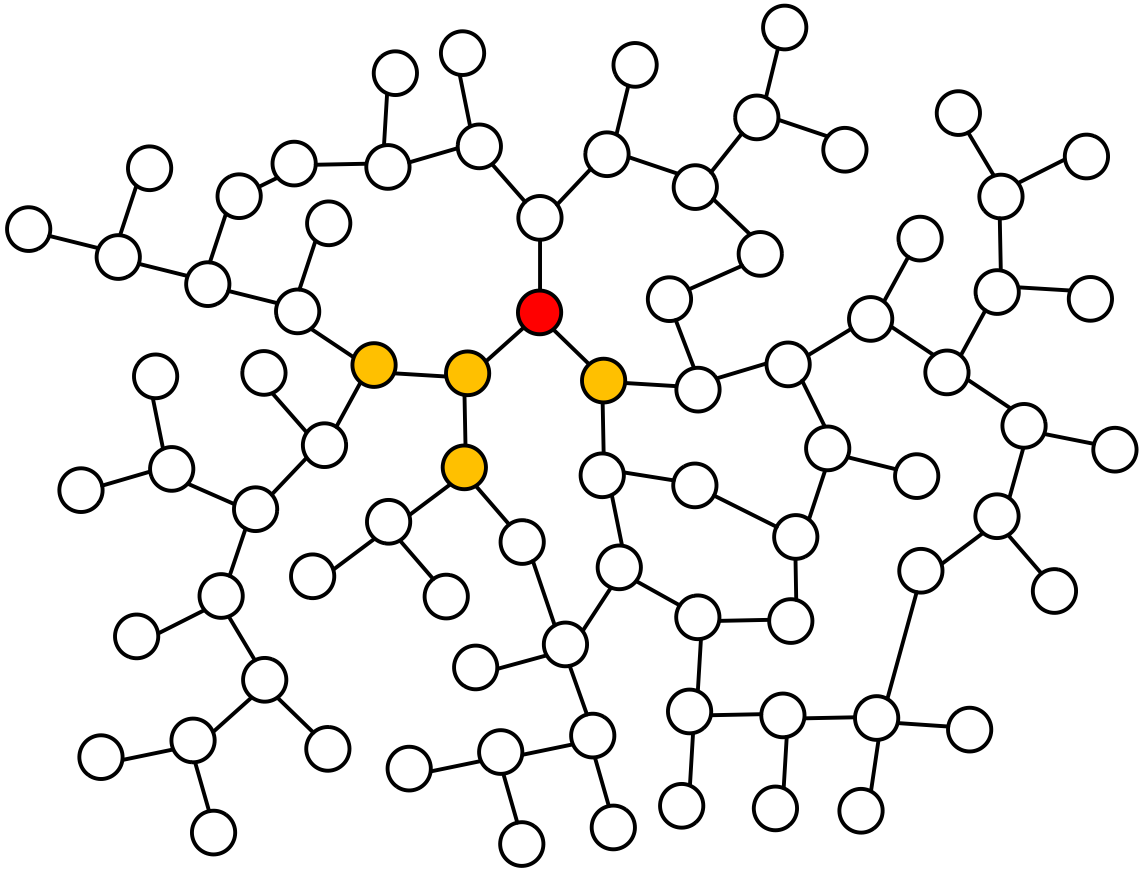


Information flow in social networks



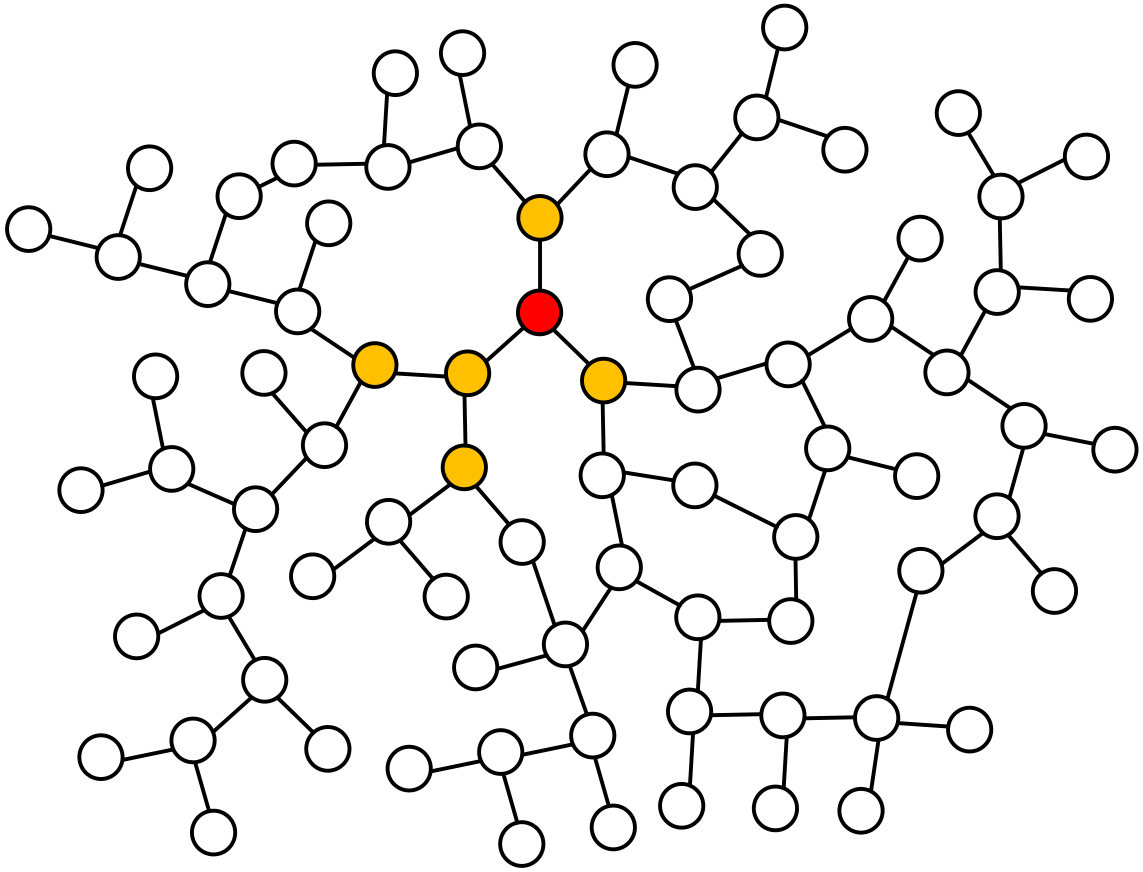
- the author passes the message to its neighbors

Information flow in social networks



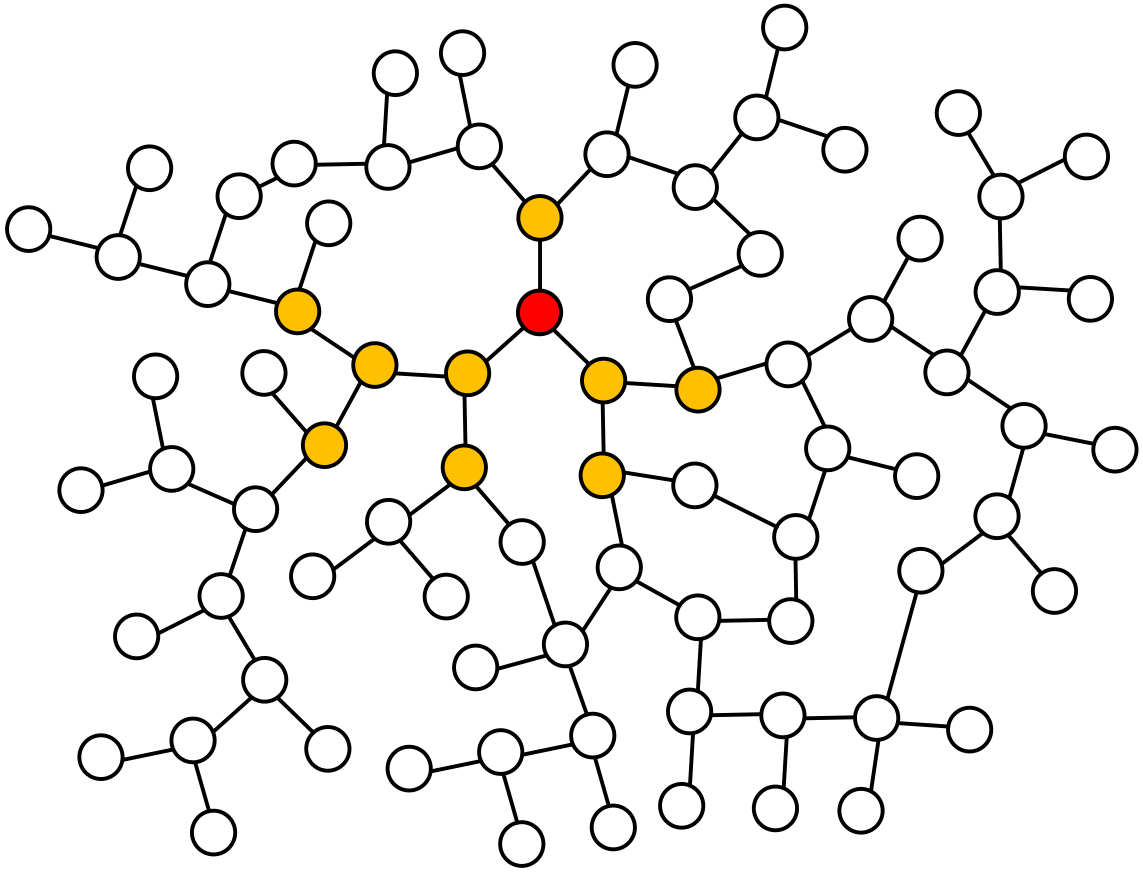
- its neighbors pass the message to theirs

Information flow in social networks



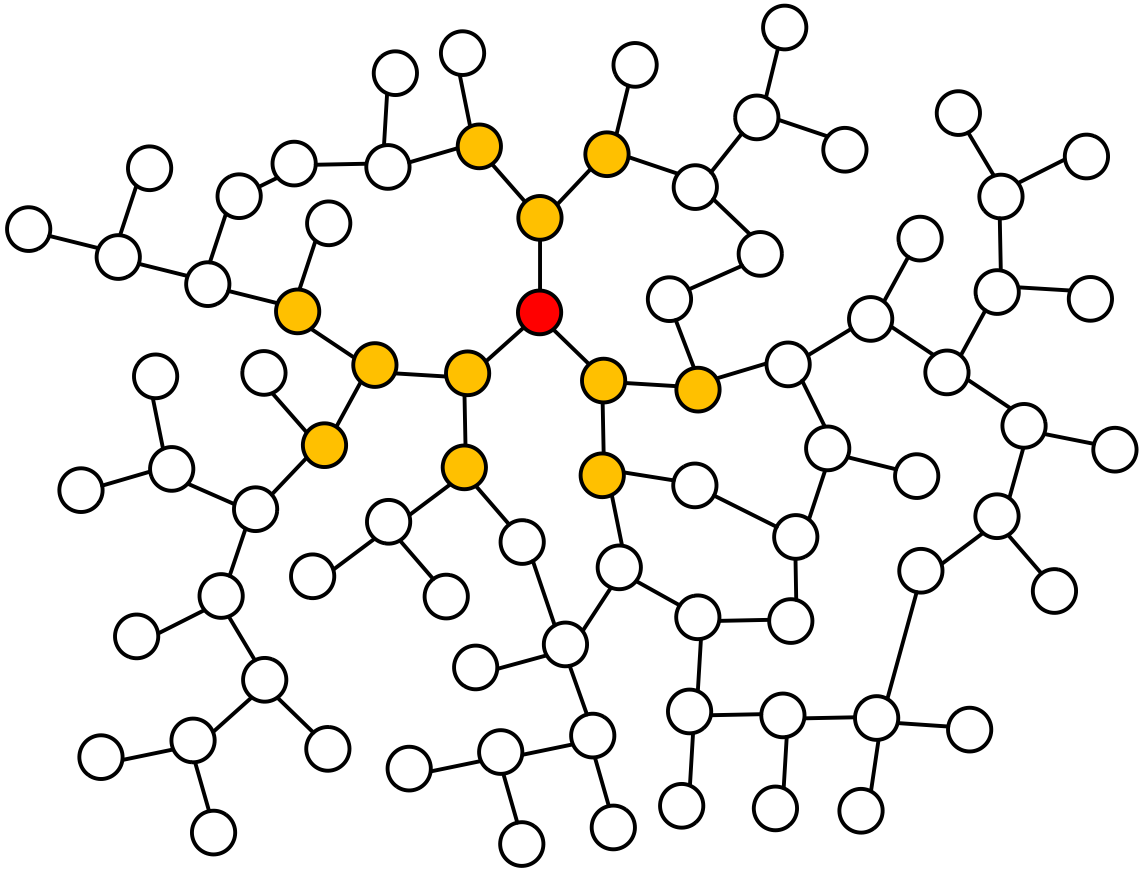
- the message spreads in **all directions** at the **same rate**

Information flow in social networks



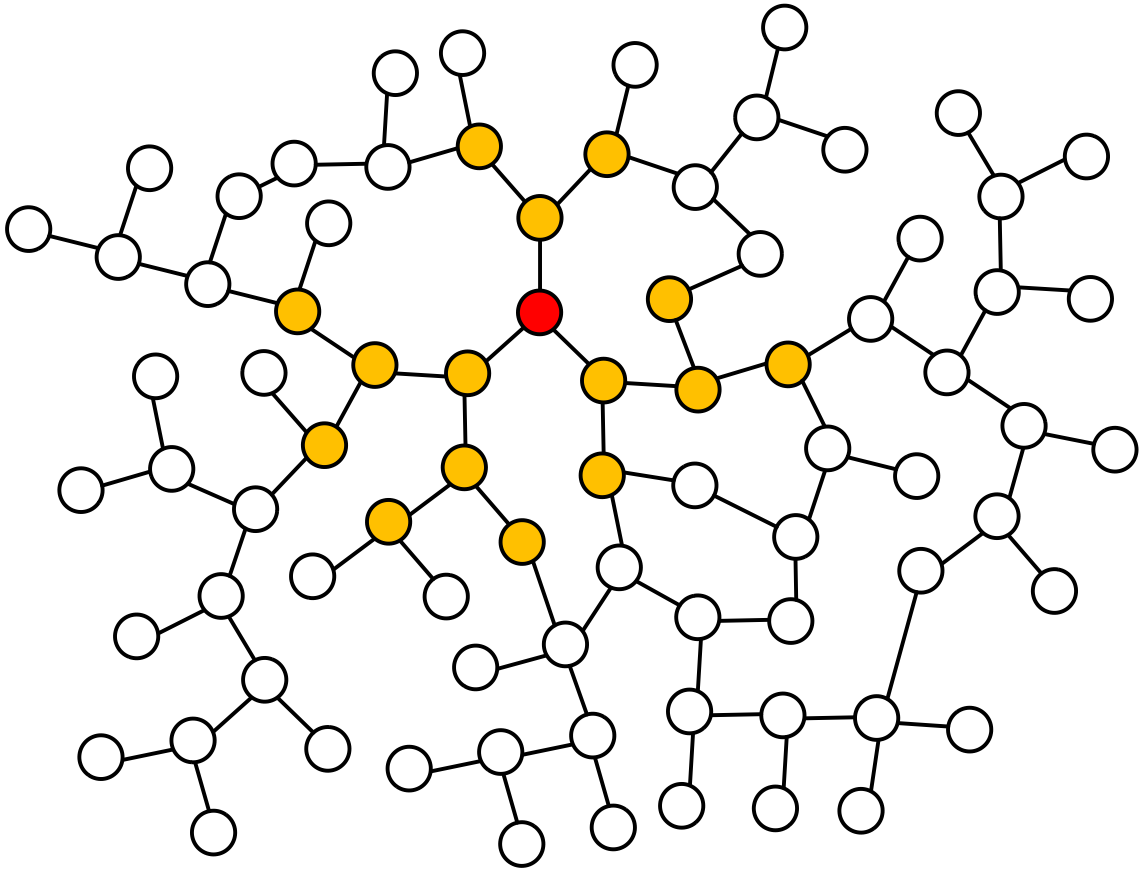
- the message spreads in **all directions** at the **same rate**

Information flow in social networks



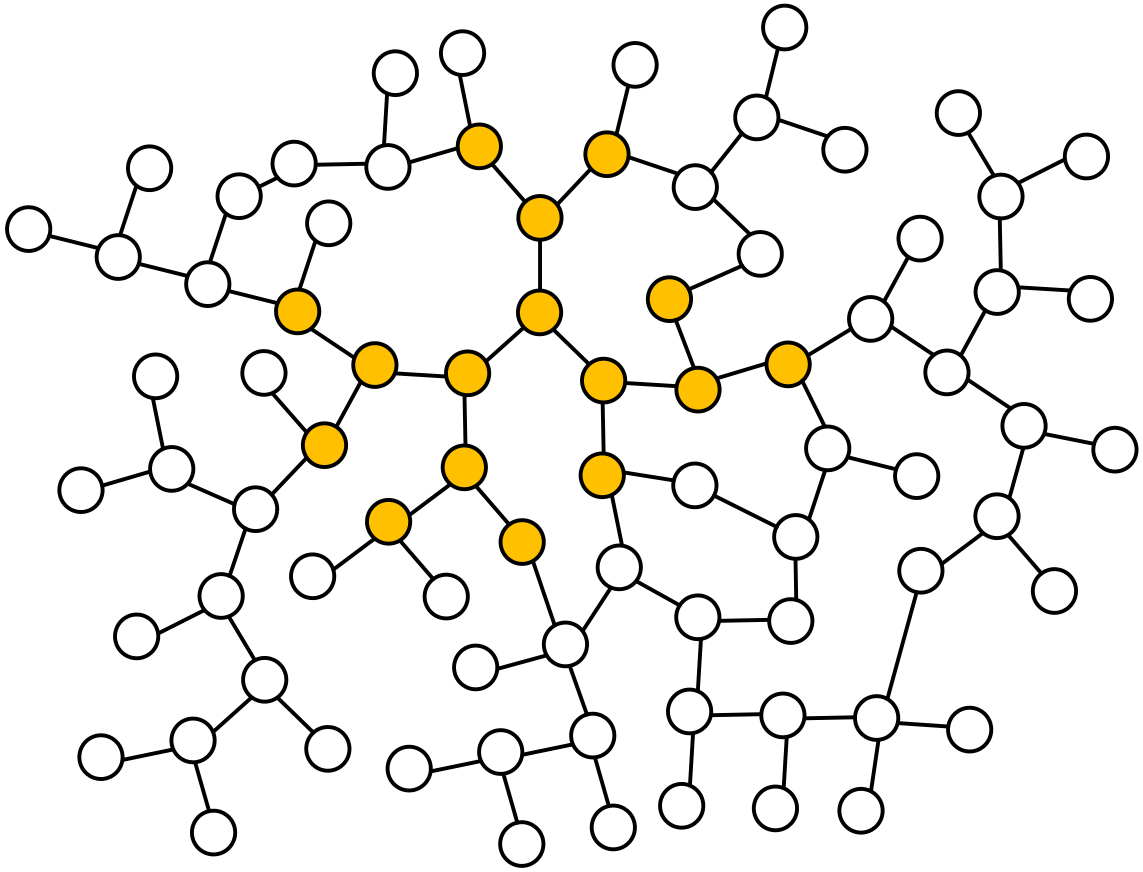
- the message spreads in **all directions** at the **same rate**

Information flow in social networks



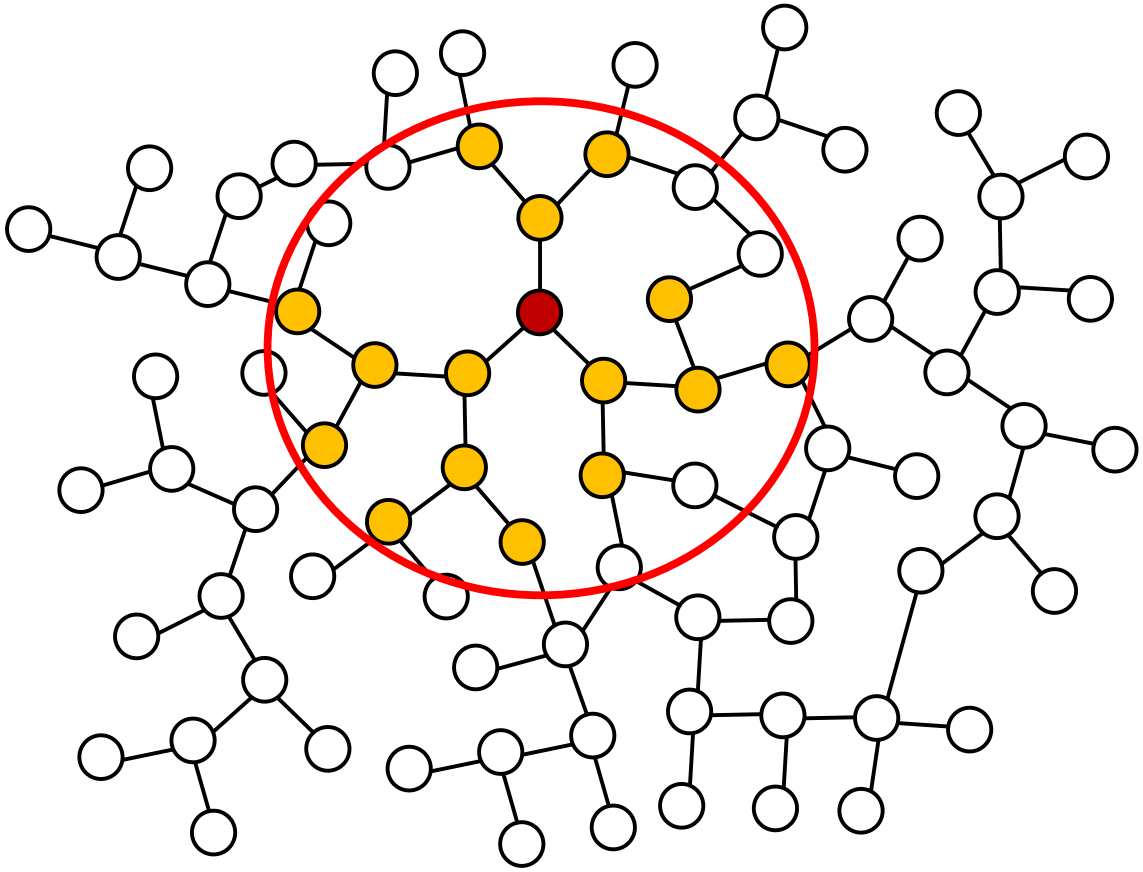
- this **spreading model** is known as the **diffusion model**

Adversary



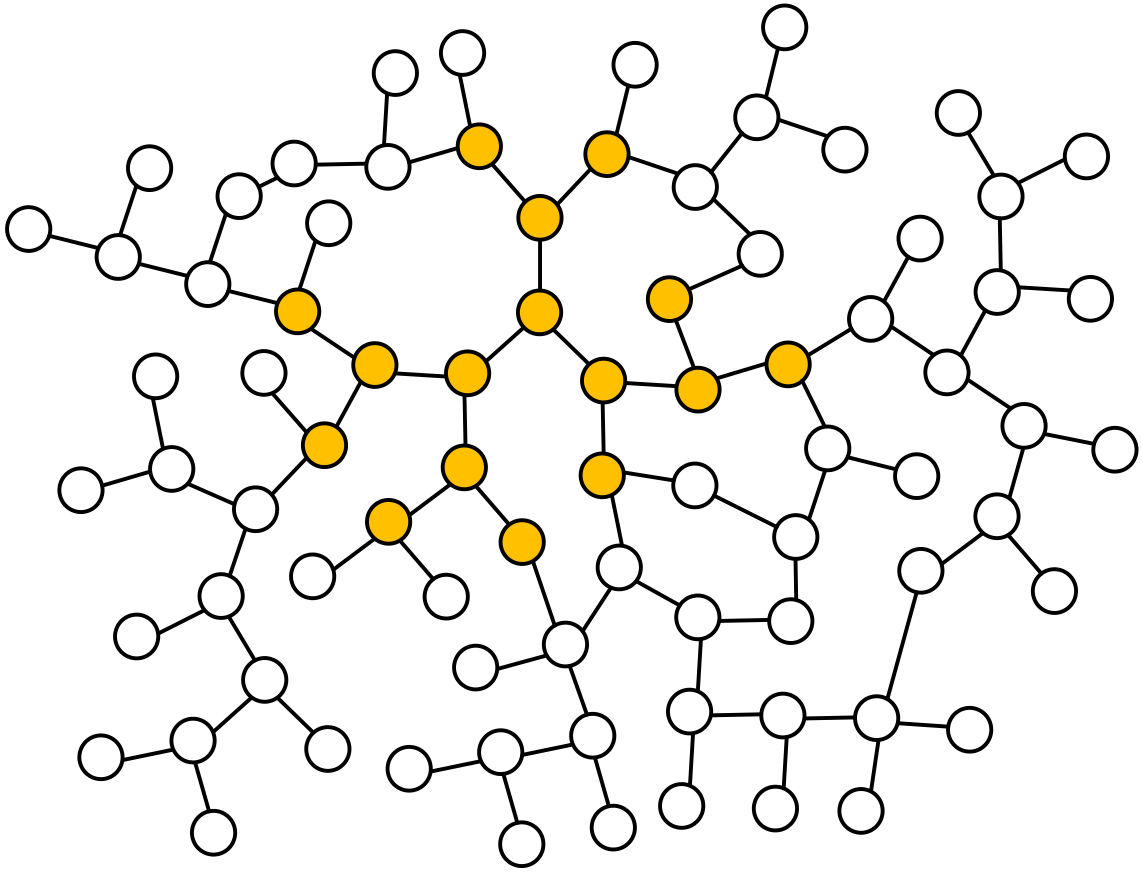
can we locate the message author?

Concentration around the center



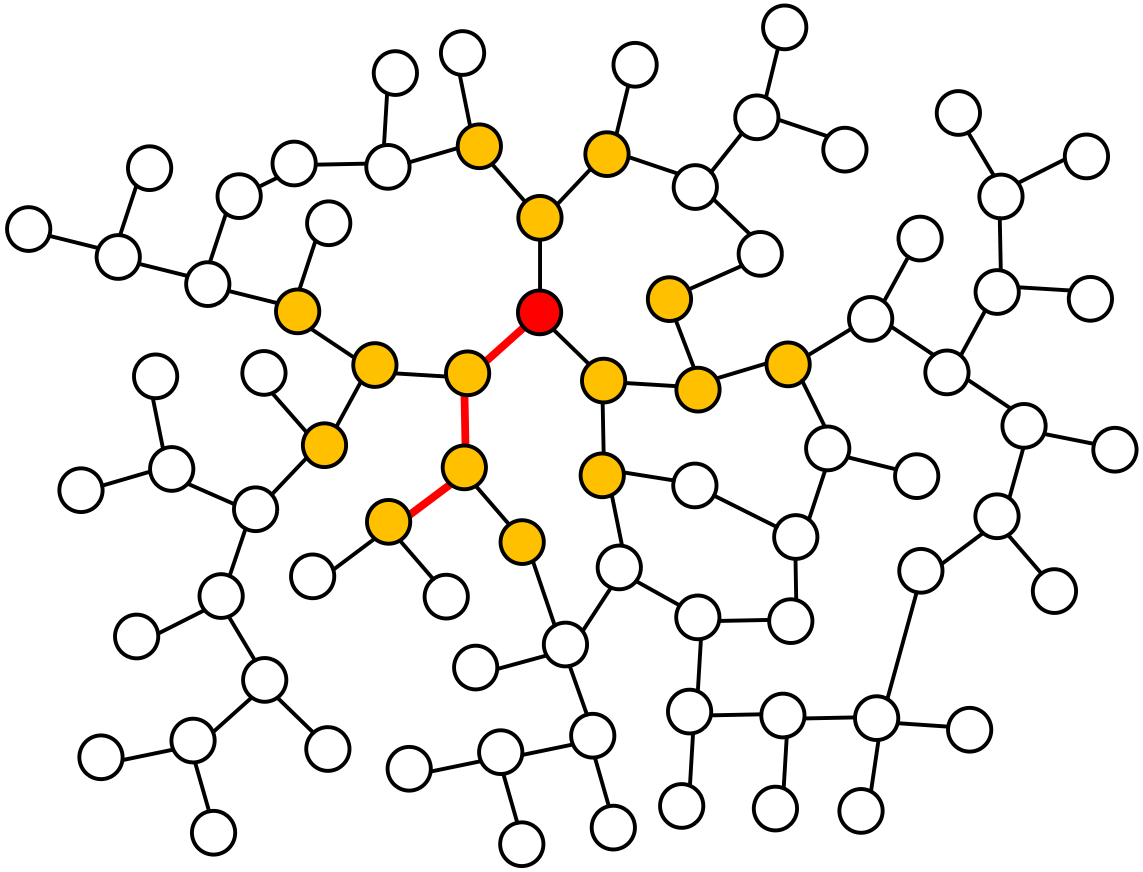
- the **message author** is in the **"center"**

Node eccentricity



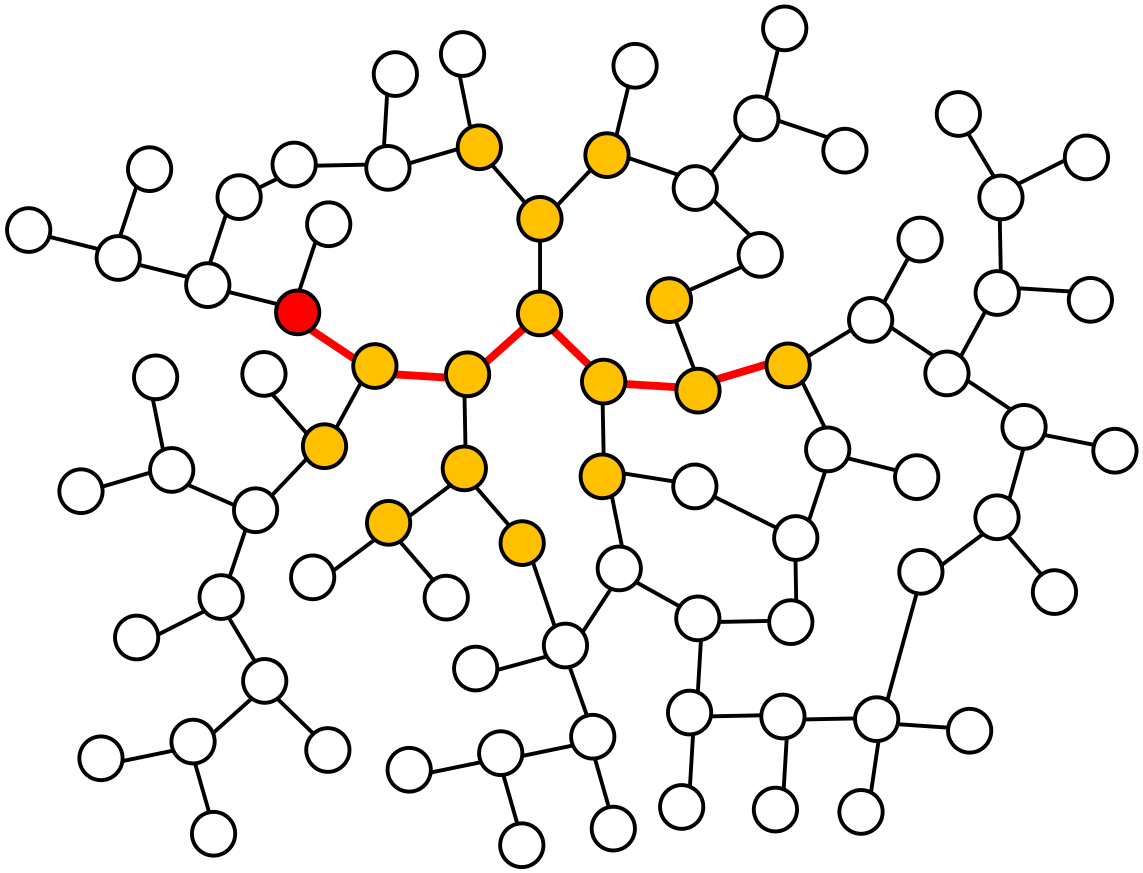
- maximum distance from a node to any other node

Node eccentricity



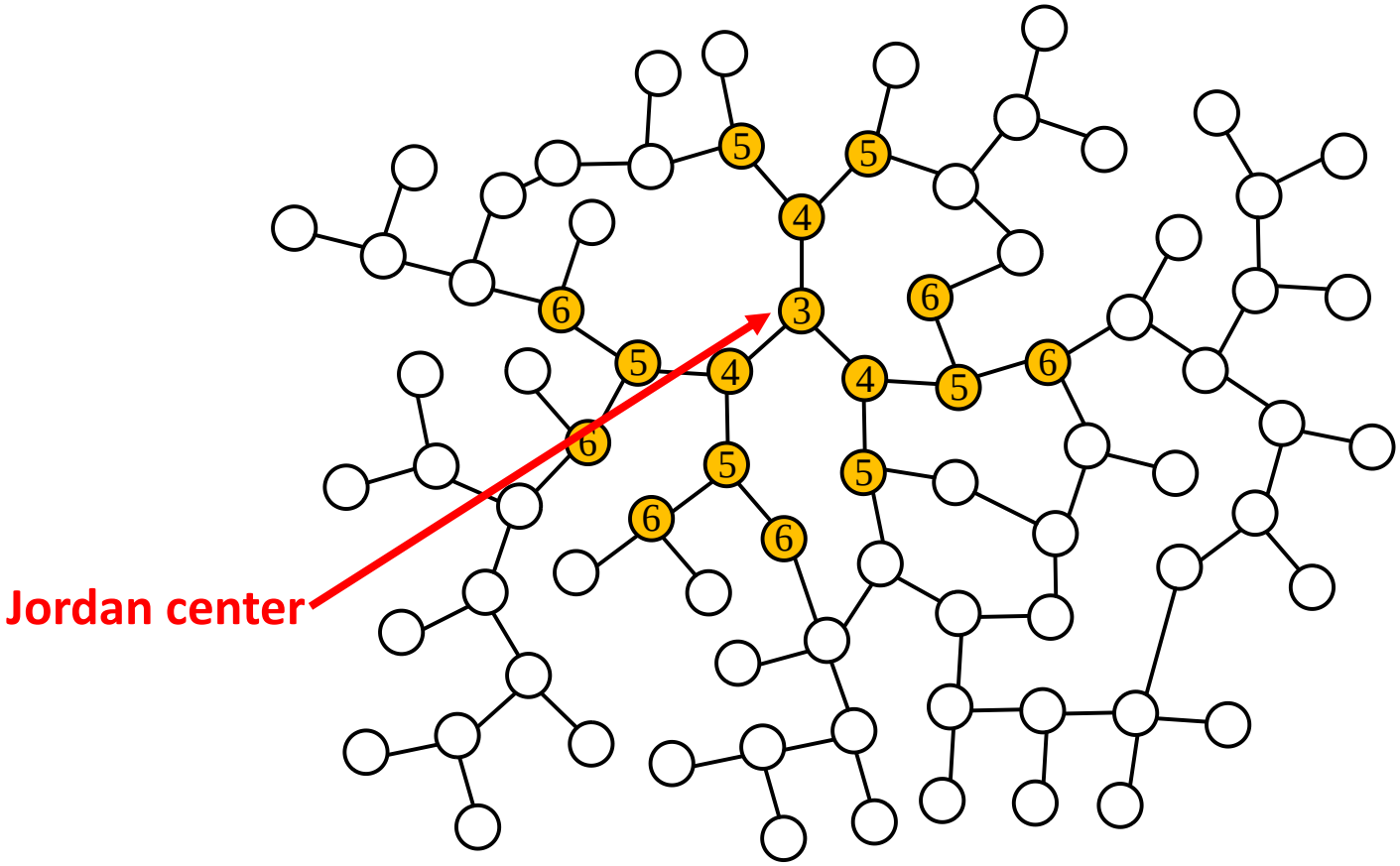
- the **message author** has an **eccentricity of 3**

Node eccentricity



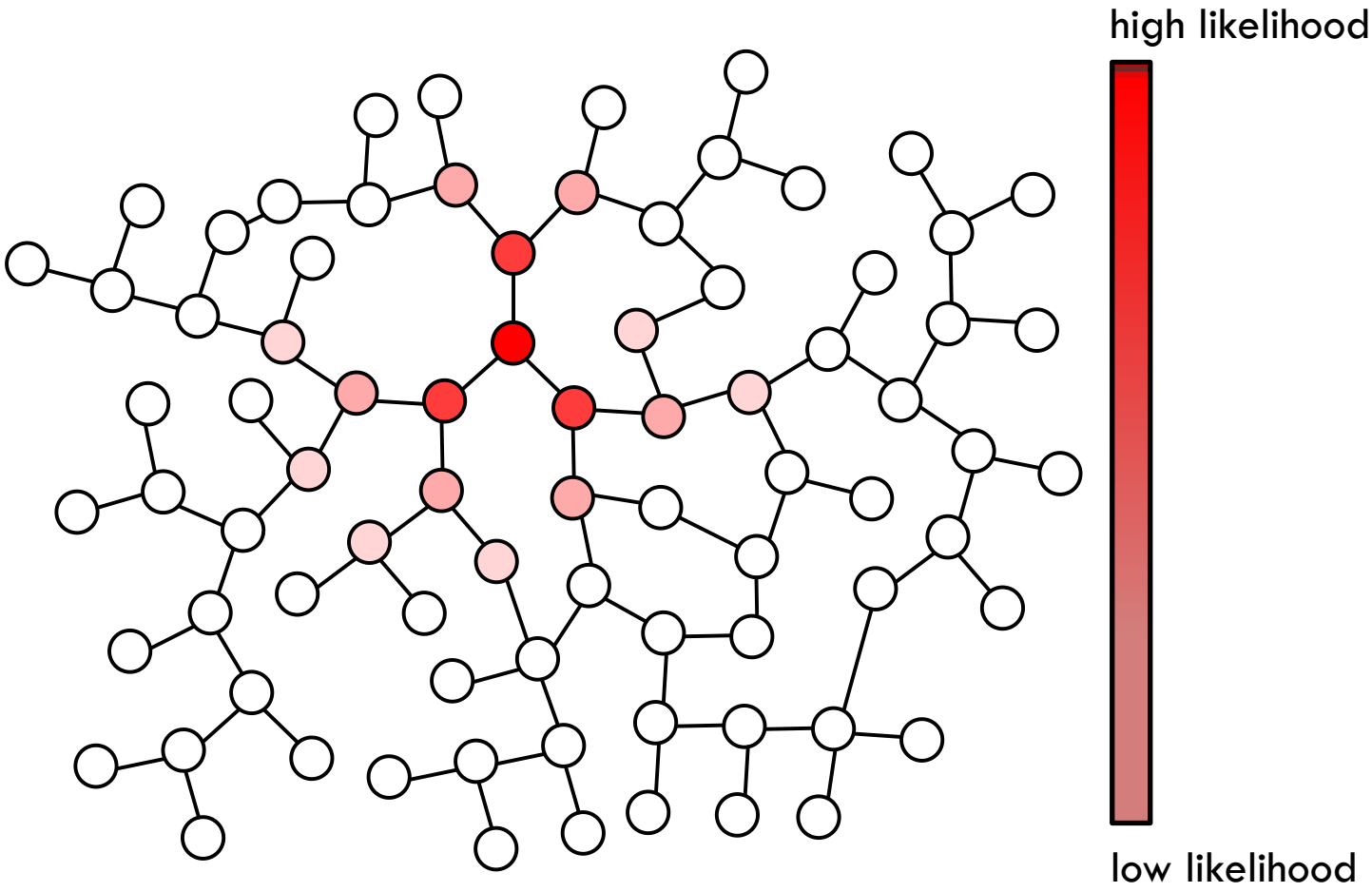
- all other nodes have larger eccentricities

Jordan centrality



- other centralities: distance centrality, rumor centrality, etc.

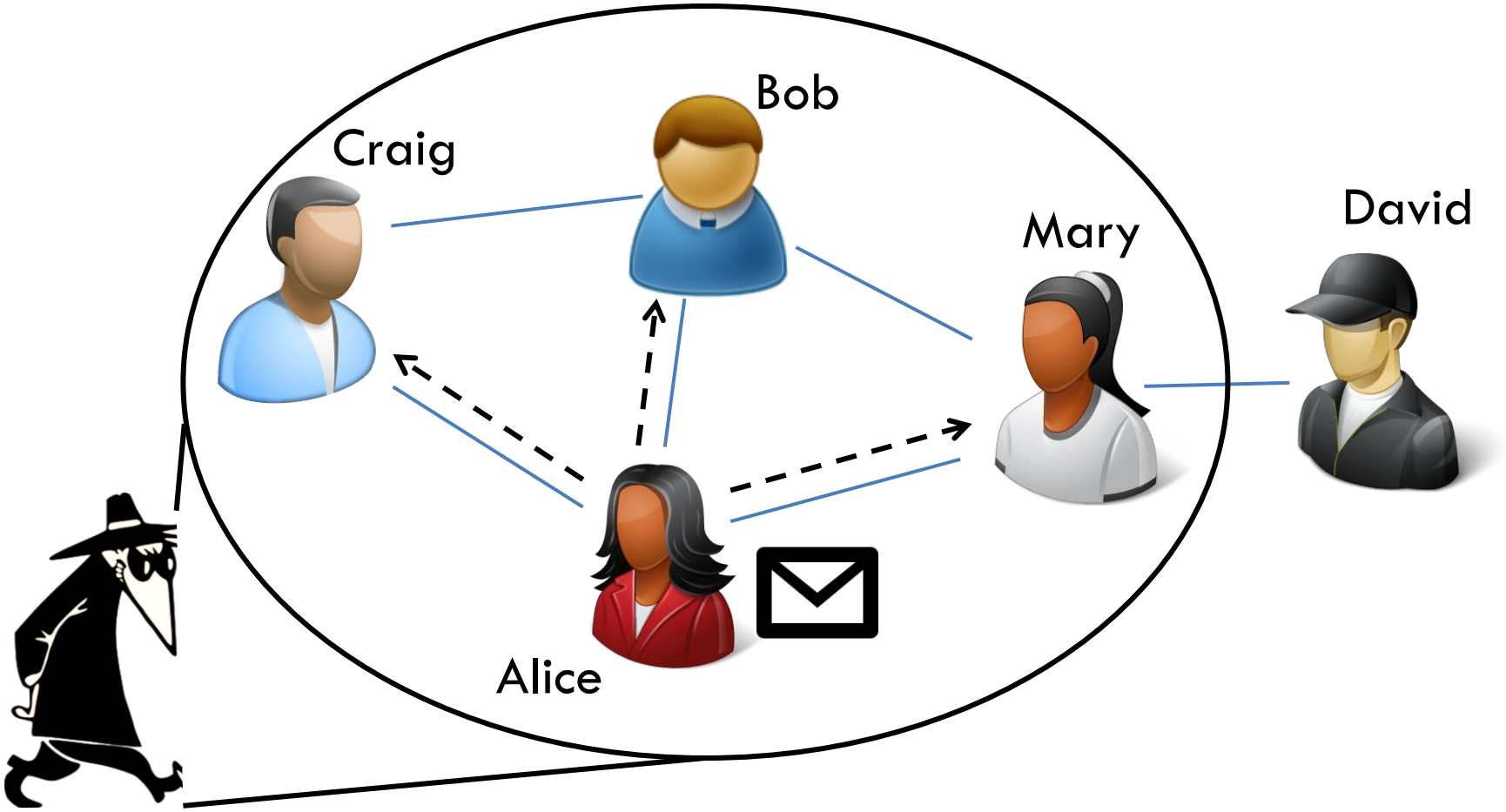
Maximum likelihood detection



diffusion spreading = deanonymization

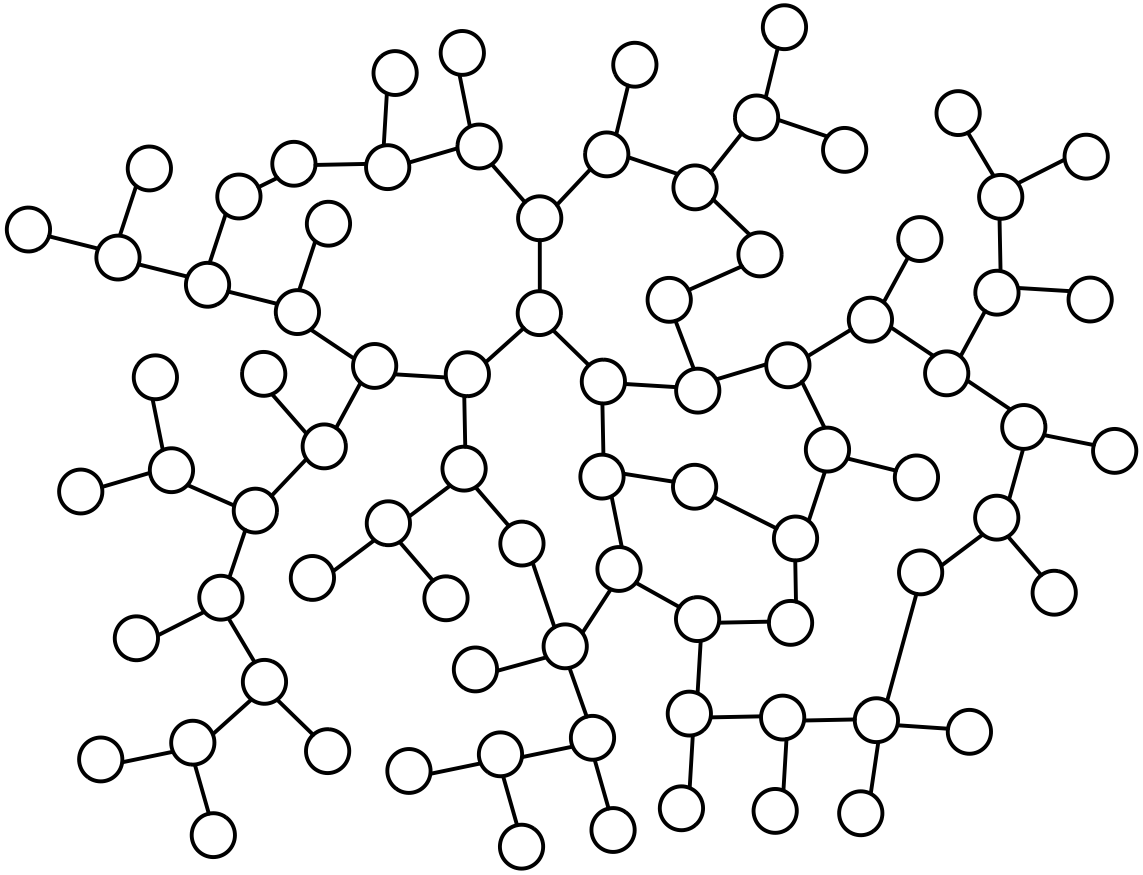
[*Shah, Zaman* 2011]

Our goal

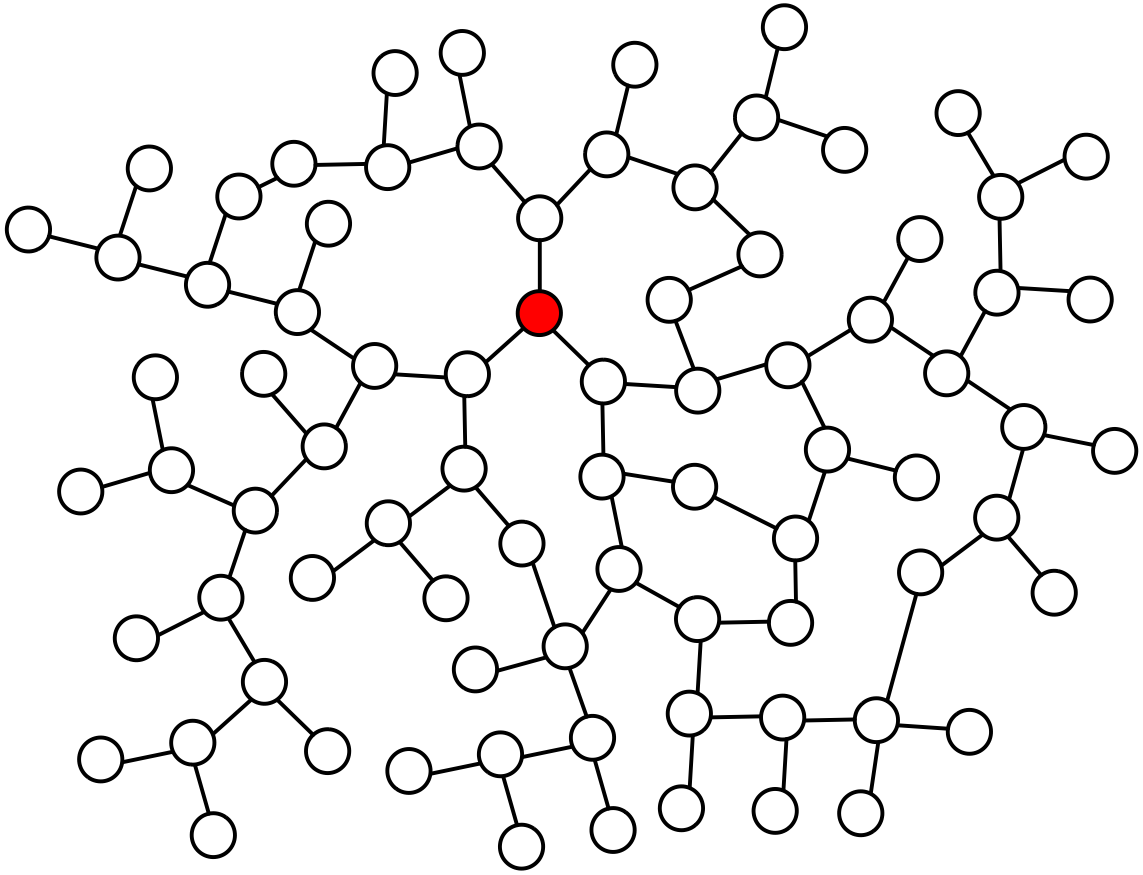


engineer the spread to hide authorship

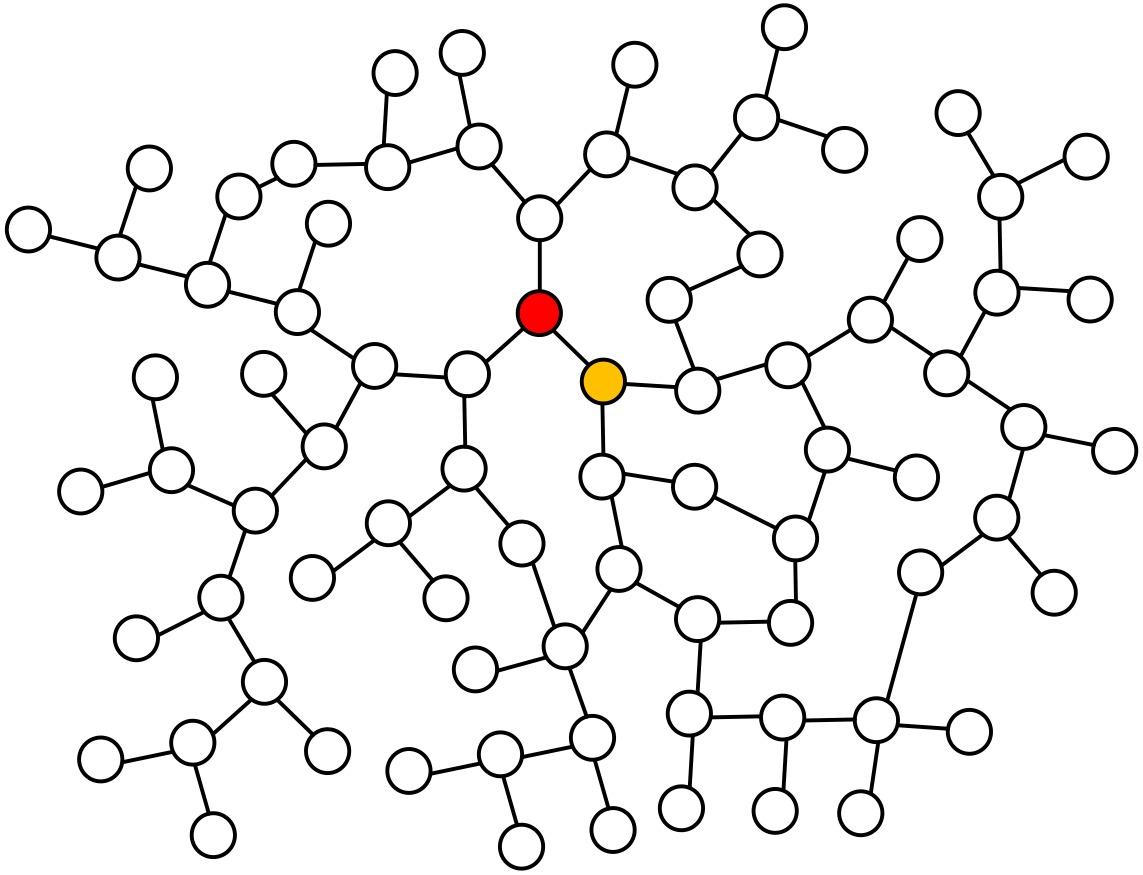
Main Result: Adaptive diffusion



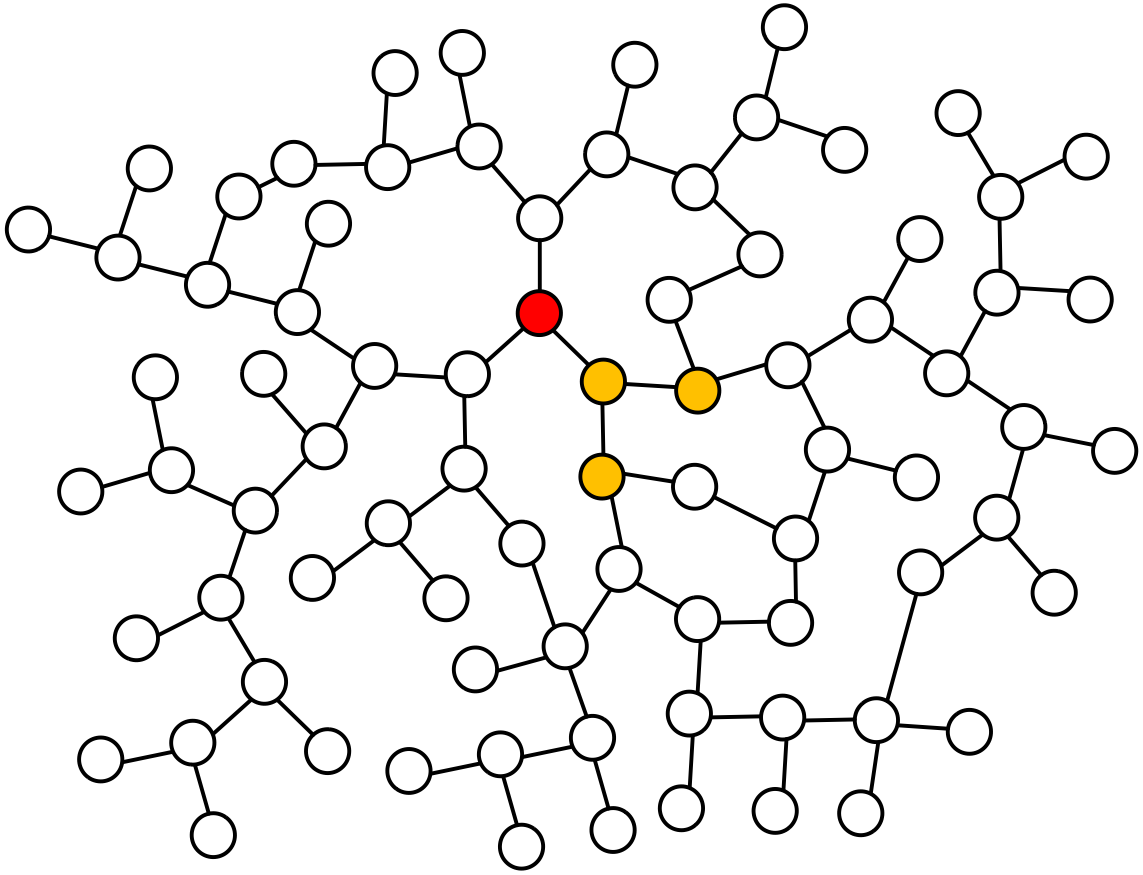
Main Result: Adaptive diffusion



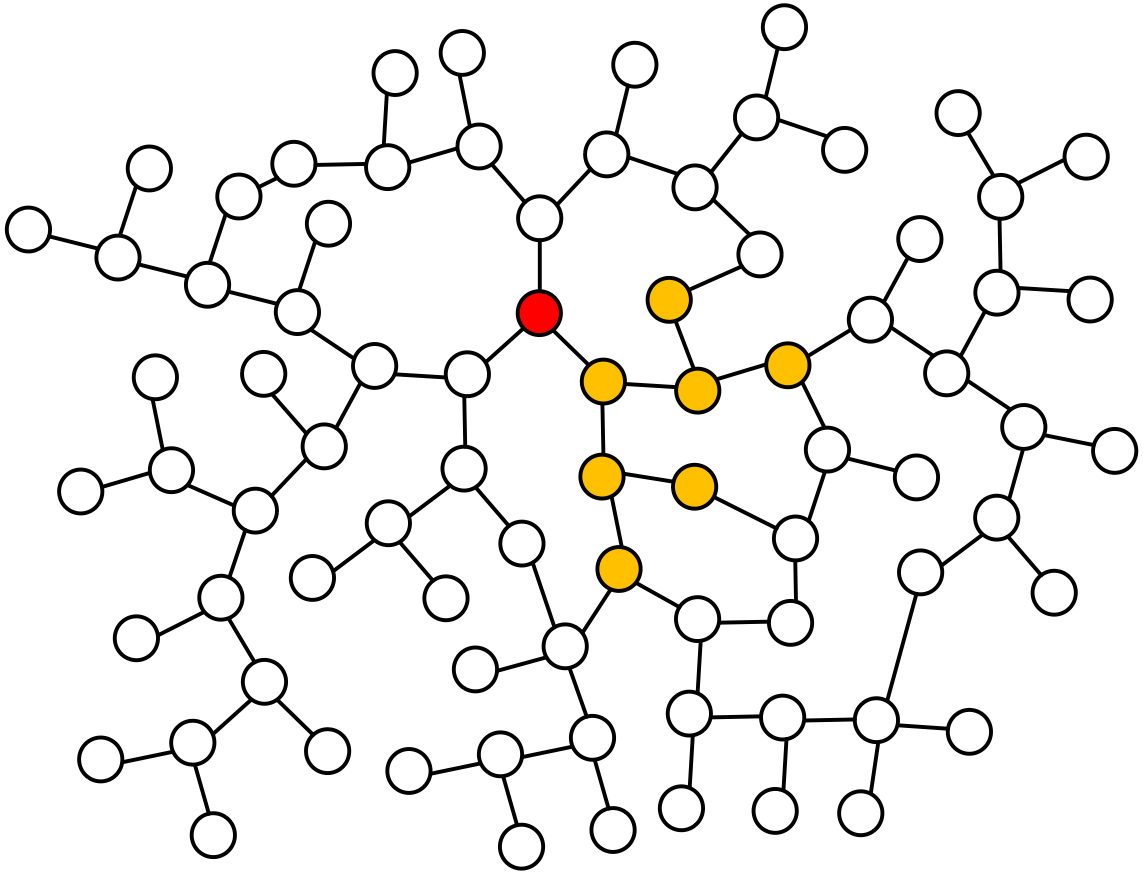
Main Result: Adaptive diffusion



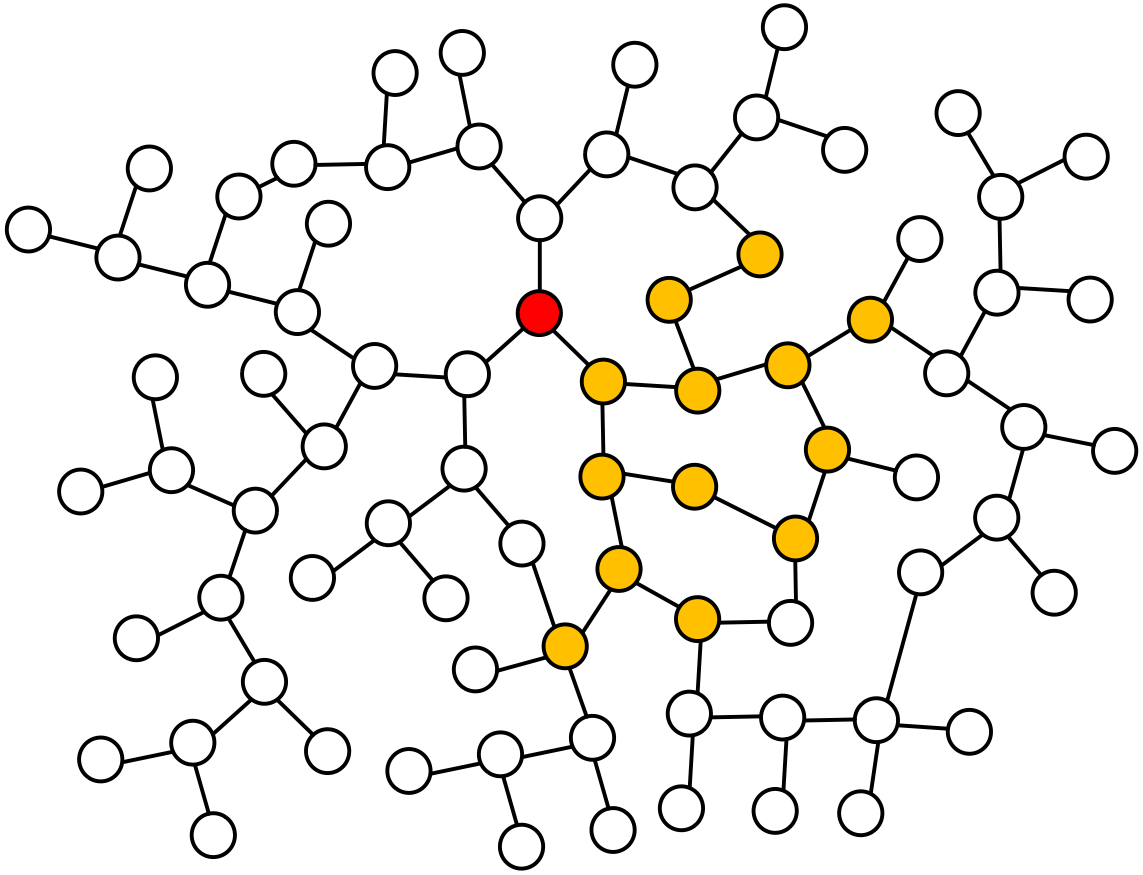
Main Result: Adaptive diffusion



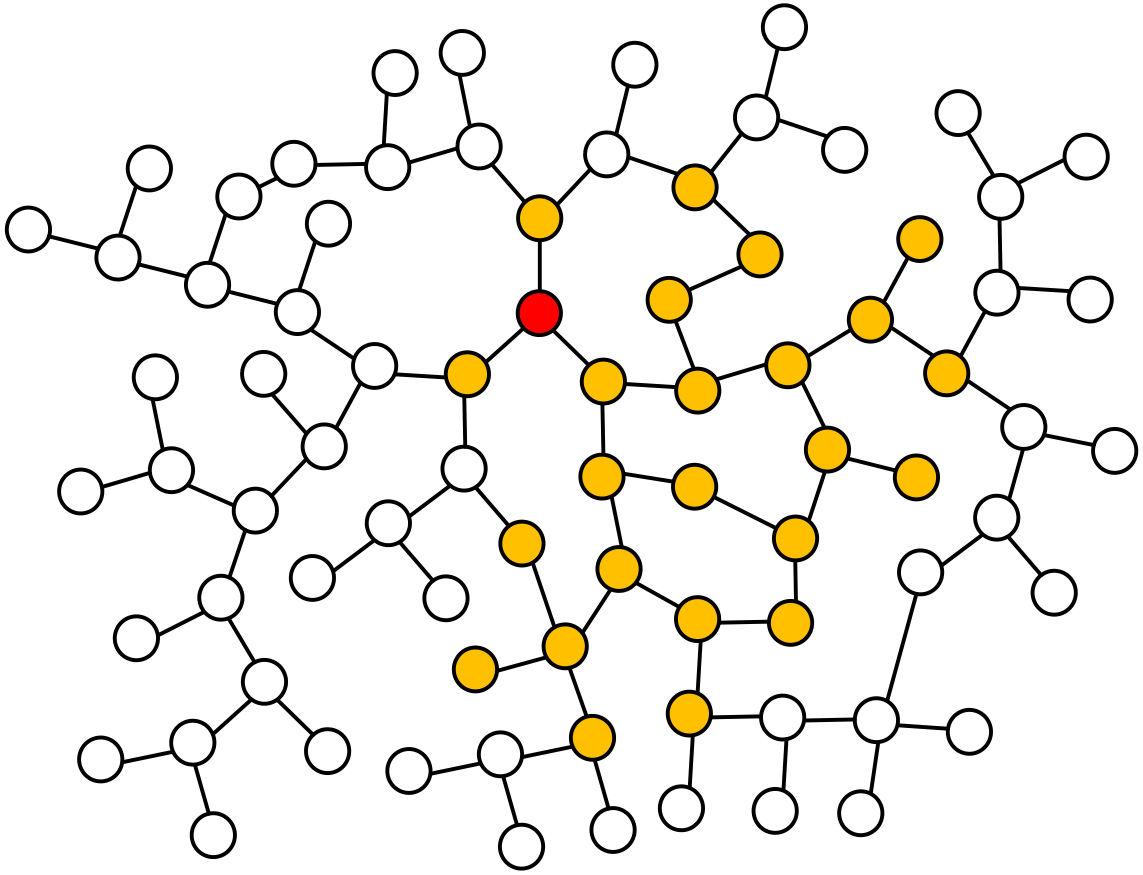
Main Result: Adaptive diffusion



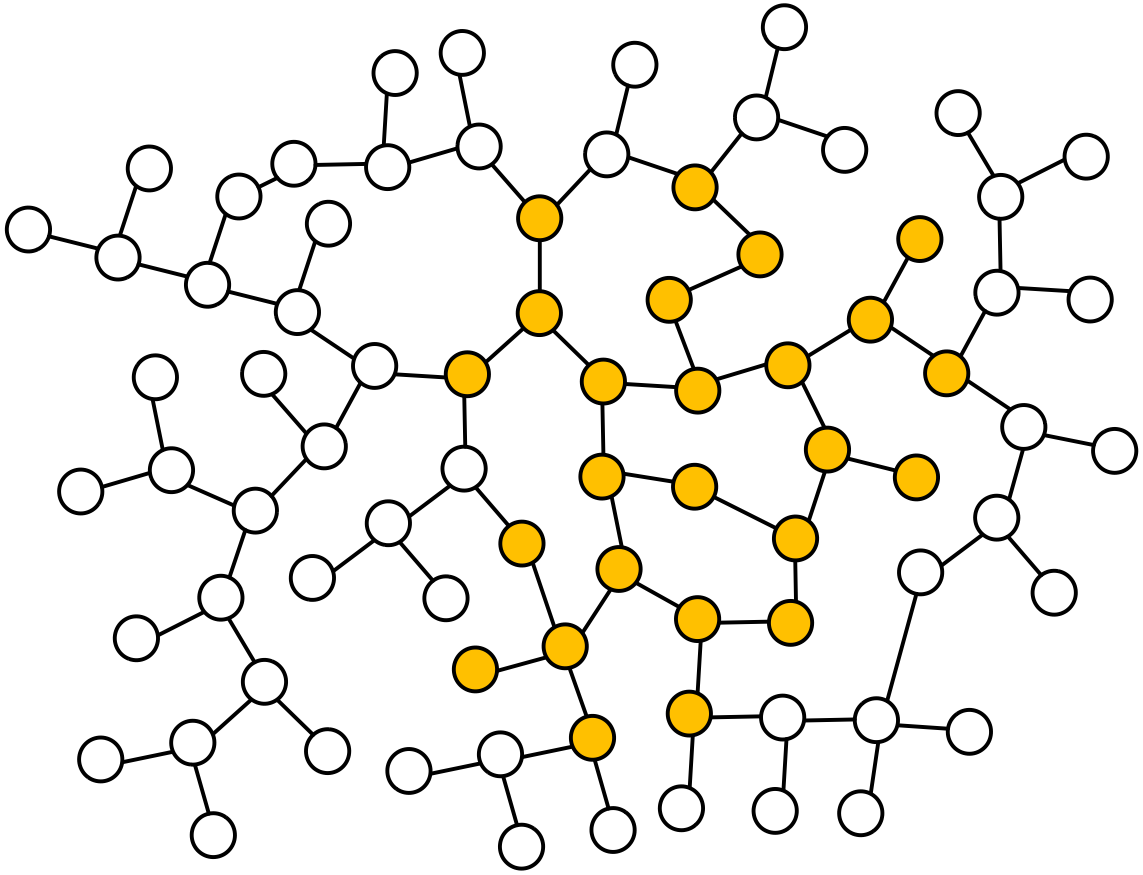
Main Result: Adaptive diffusion



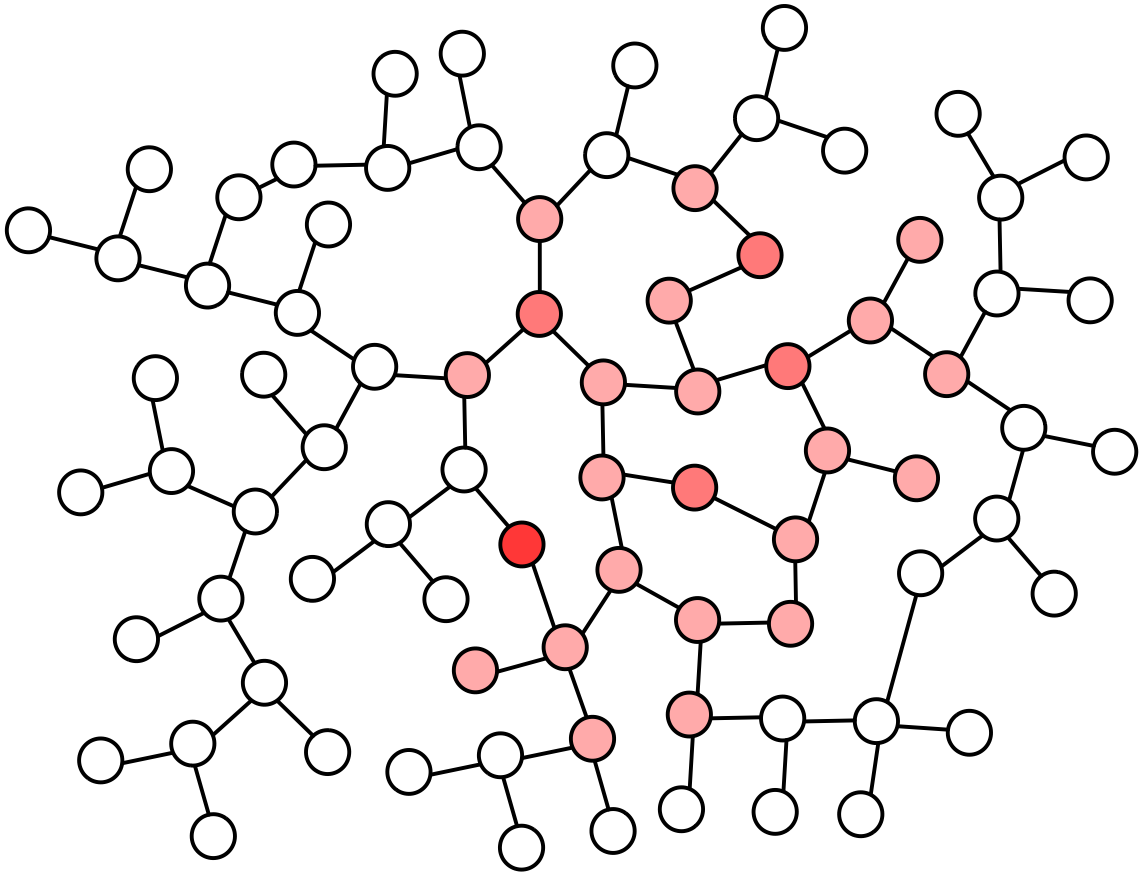
Main Result: Adaptive diffusion

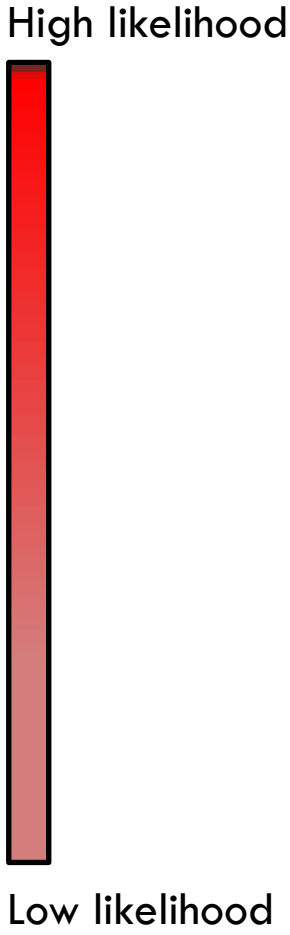


Main Result: Adaptive diffusion



Main Result: Adaptive diffusion

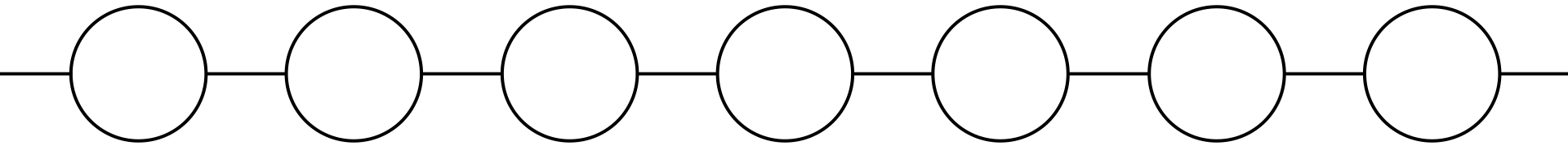




provides provable anonymity guarantees

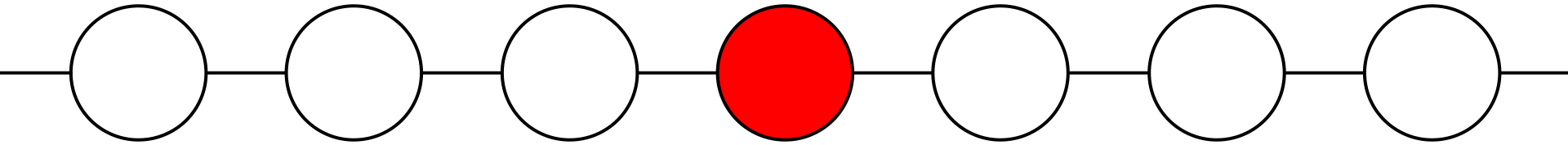
[*Spy vs. Spy: Rumor Source Obfuscation*, to appear in ACM SIGMETRICS 2015]

Line graphs



- let's start with line graphs

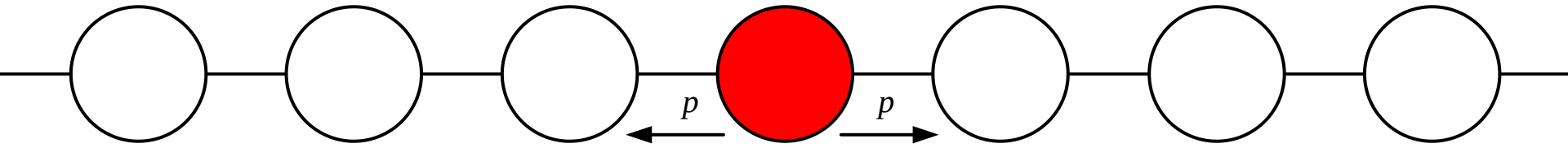
Line graphs: diffusion



$T = 0$

- the message author starts a rumor at $T = 0$

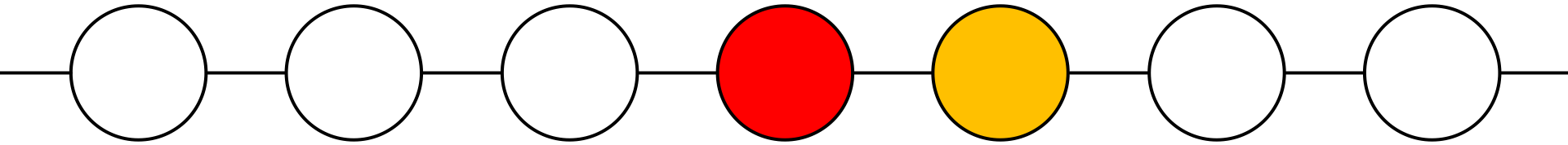
Line graphs: diffusion



$T = 1$

- with probability p, the left (right) node receives the message

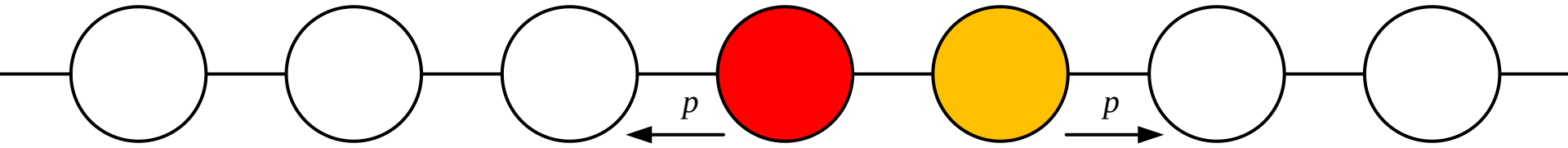
Line graphs: diffusion



$T = 1$

- the node to the right of the author receives the message

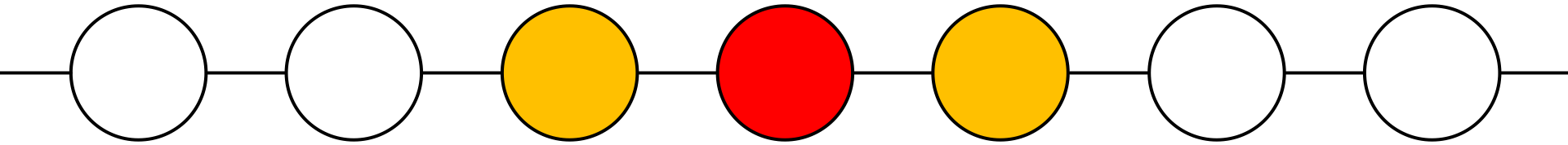
Line graphs: diffusion



$T = 2$

- the rumor propagates in both directions at the same rate

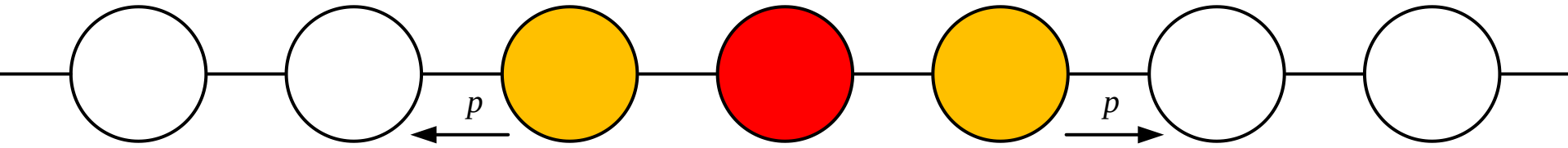
Line graphs: diffusion



$T = 2$

- the rumor propagates in **both directions** at the **same rate**

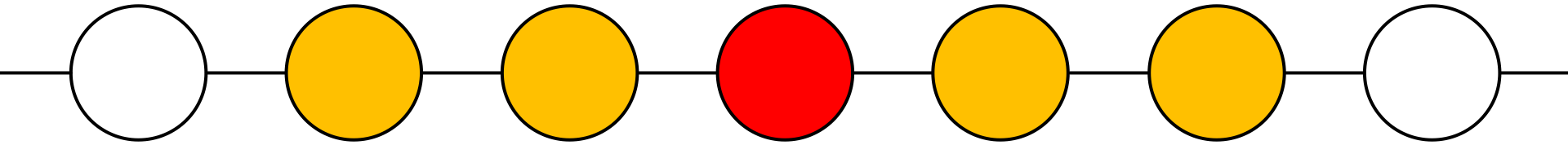
Line graphs: diffusion



$T = 3$

- p is **independent of** time or **hop distance** to message author

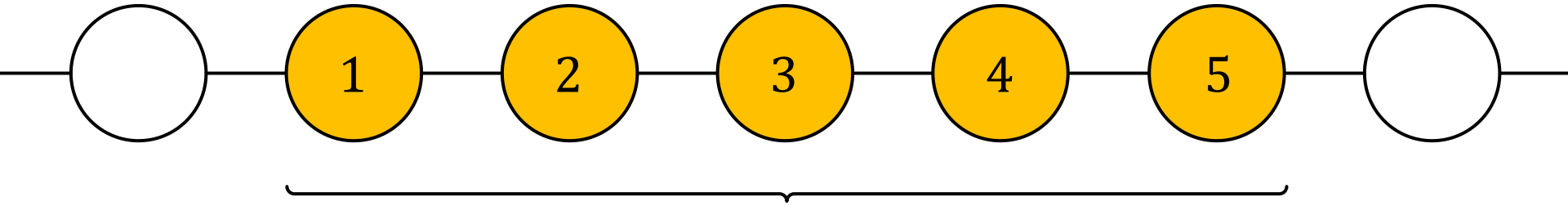
Line graphs: diffusion



$T = 3$

- diffusion on a line is equivalent to **two independent random walks**

Adversary

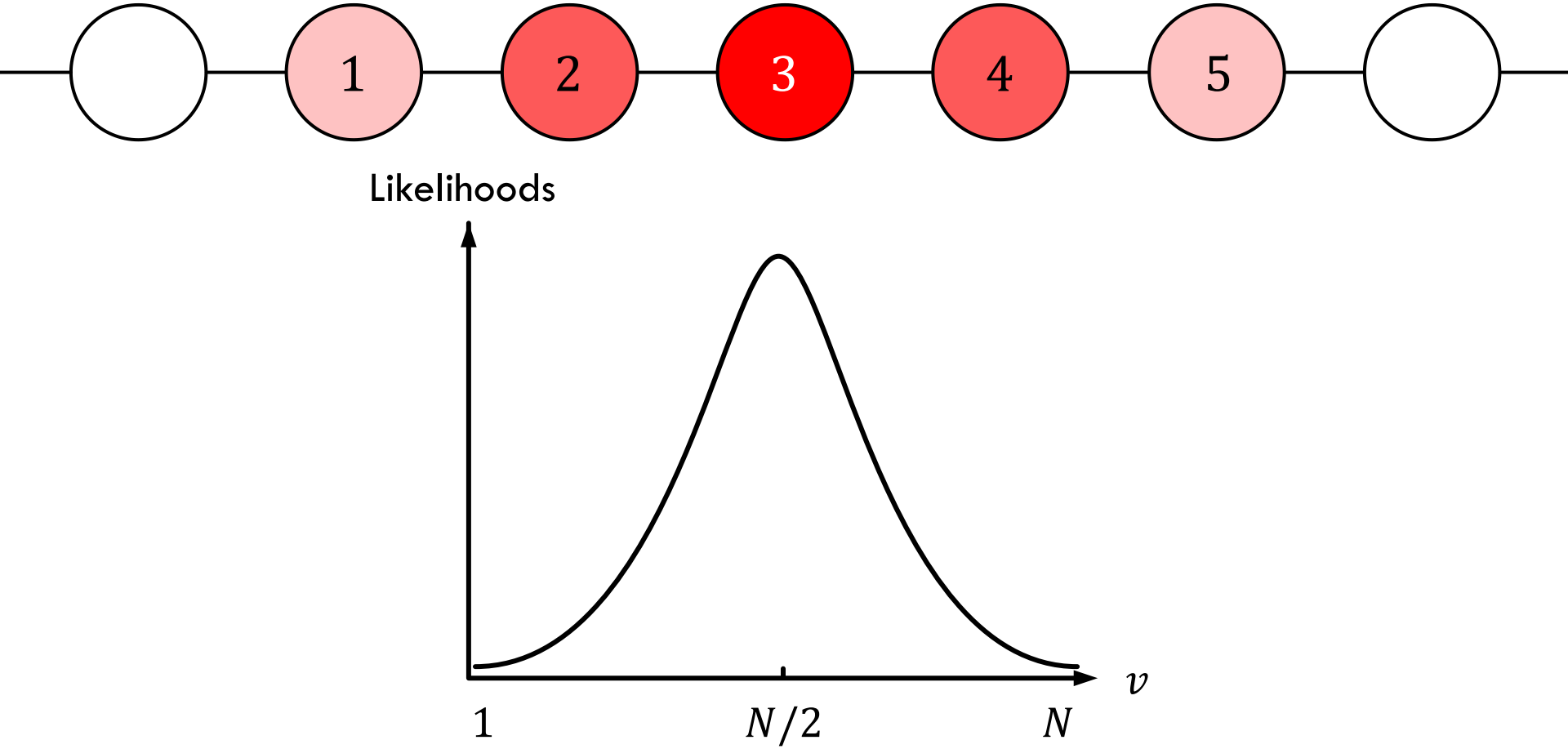


$N = 5$

nodes with the message

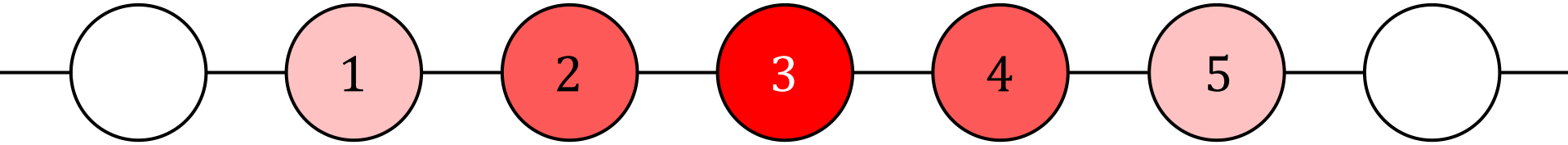
can we locate the message author?

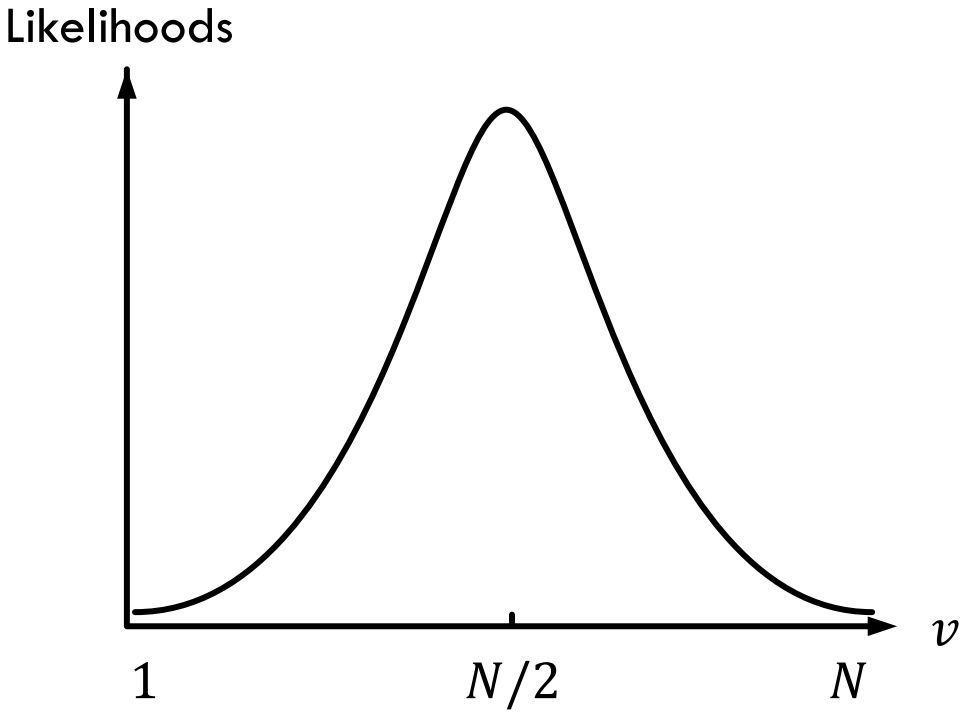
Maximum likelihood detection



- the **node in the middle** is the **mostly likely author**

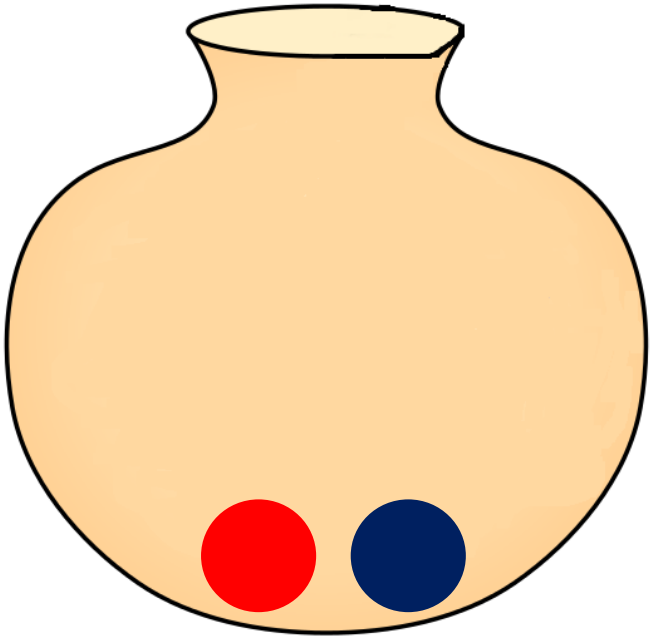
Maximum likelihood detection





Probability of detection $\approx \frac{1}{\sqrt{N}}$

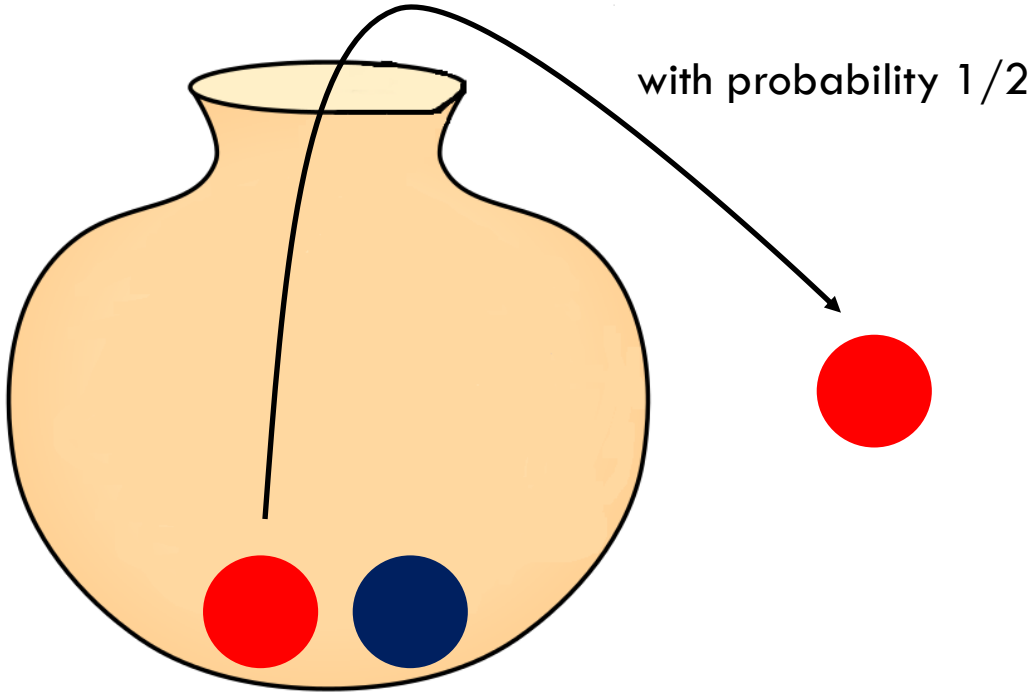
Pólya's urn process



$T = 1$

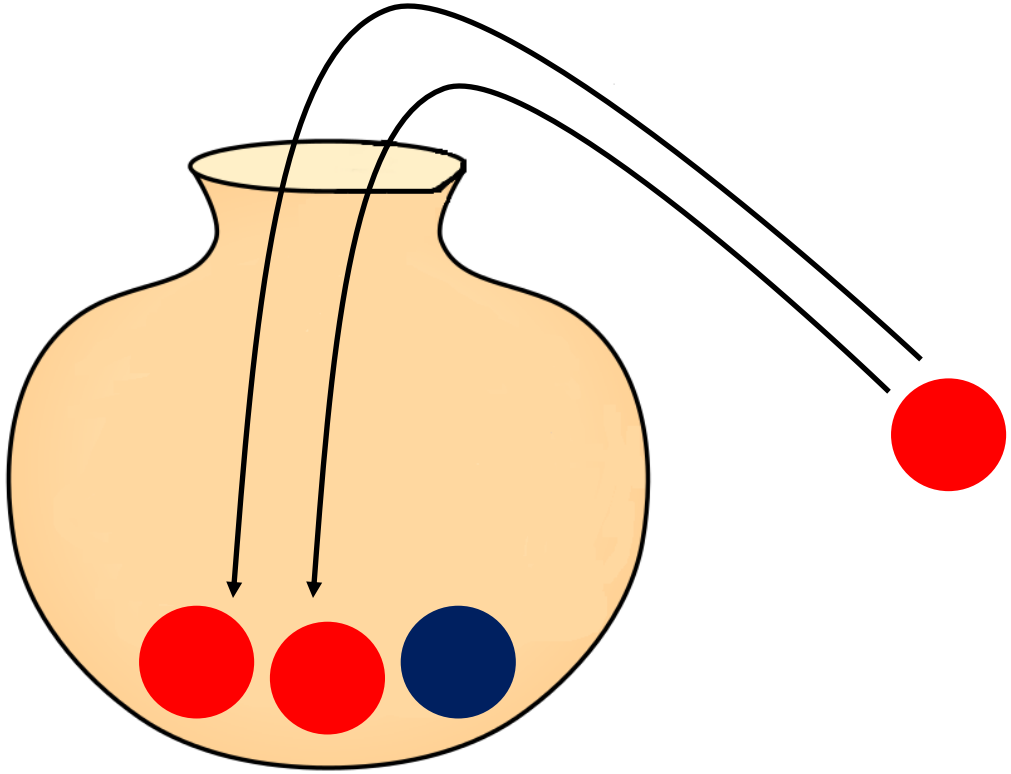
- choose a ball at random from the urn

Pólya's urn process



- choose a ball at random from the urn

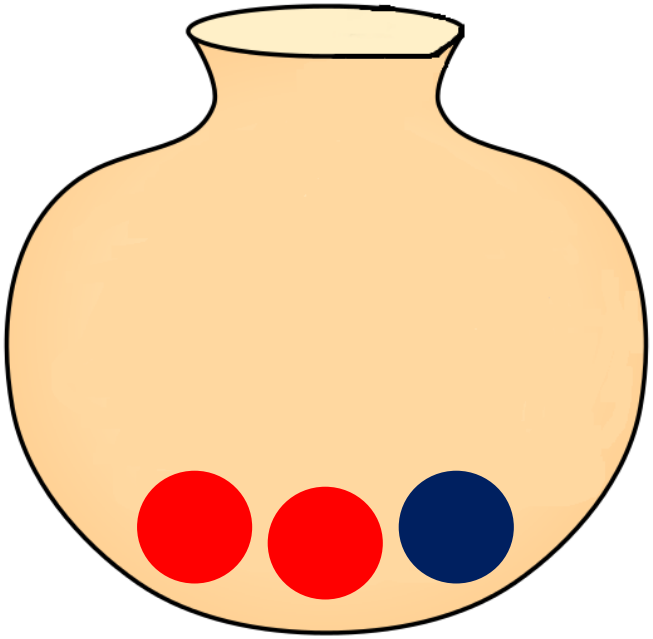
Pólya's urn process



$T = 1$

- replace the chosen ball by two balls of the same color

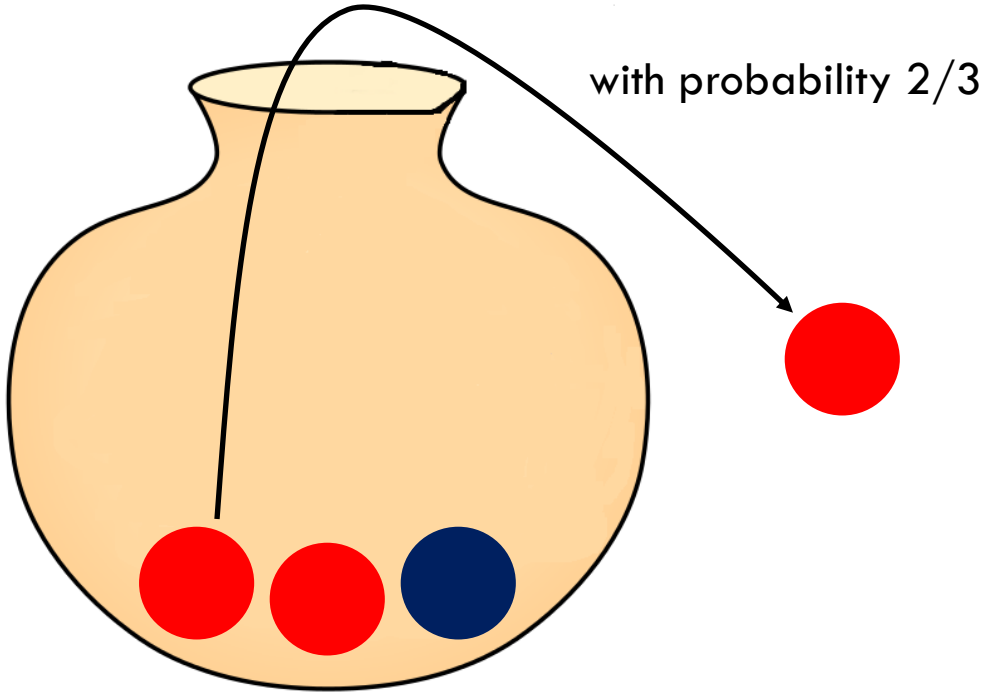
Pólya's urn process



$T = 2$

- repeat previous steps

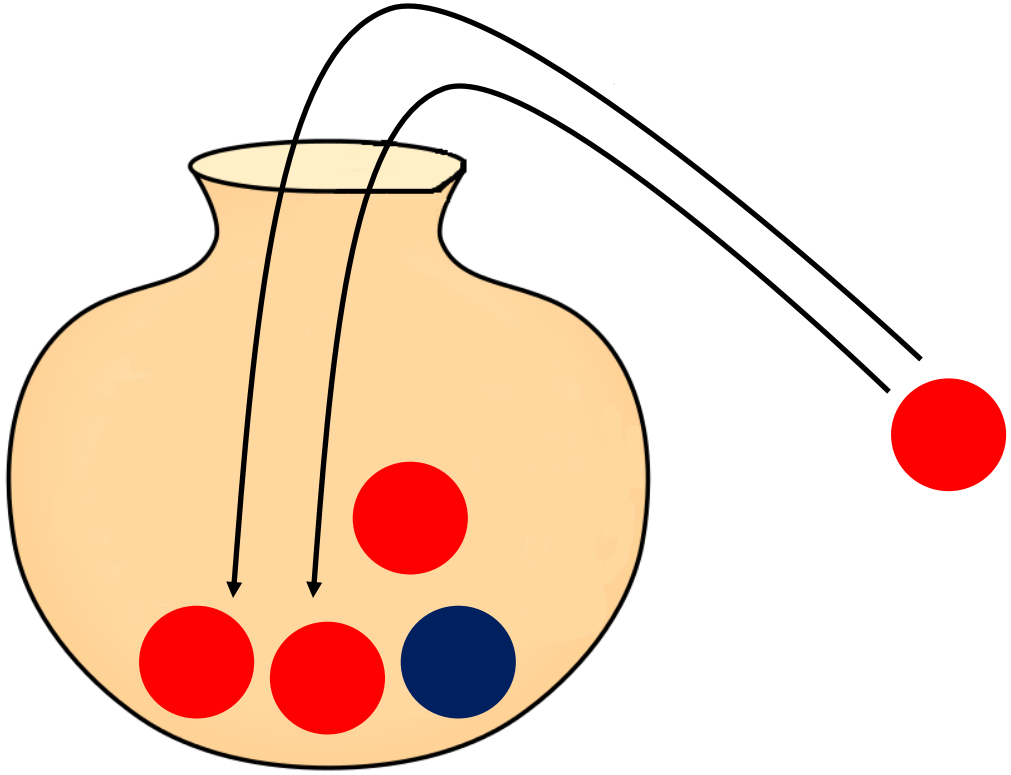
Pólya's urn process



$T = 2$

- repeat previous steps

Pólya's urn process

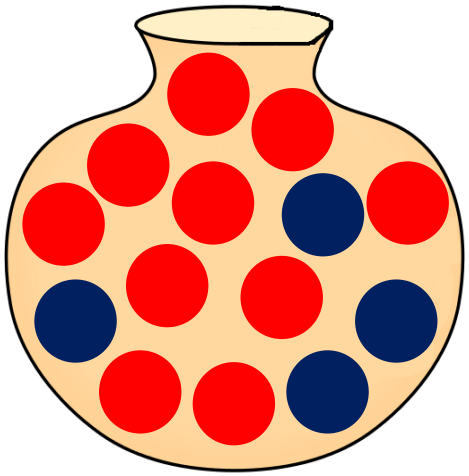


$T = 2$

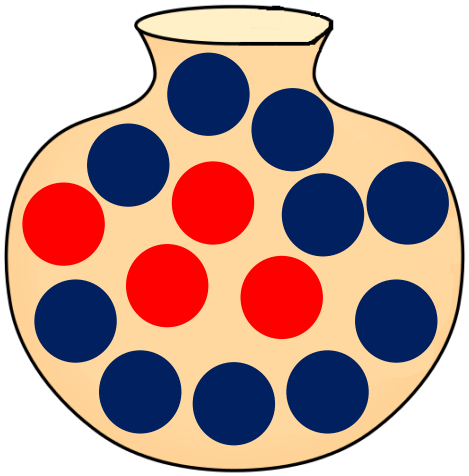
the rich get richer and poor get poorer

Pólya's urn process: anonymity properties

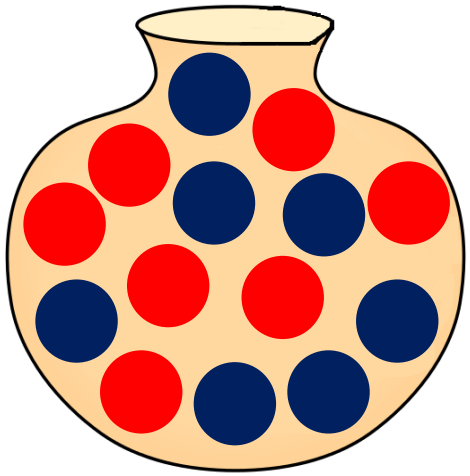
$$T = 14$$



10 red and 4 blue



4 red and 10 blue

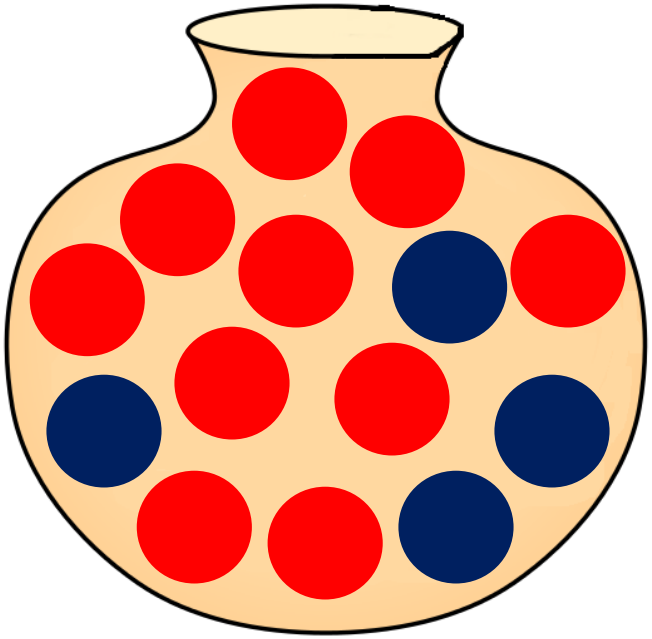


7 red and 7 blue

all events are equally likely

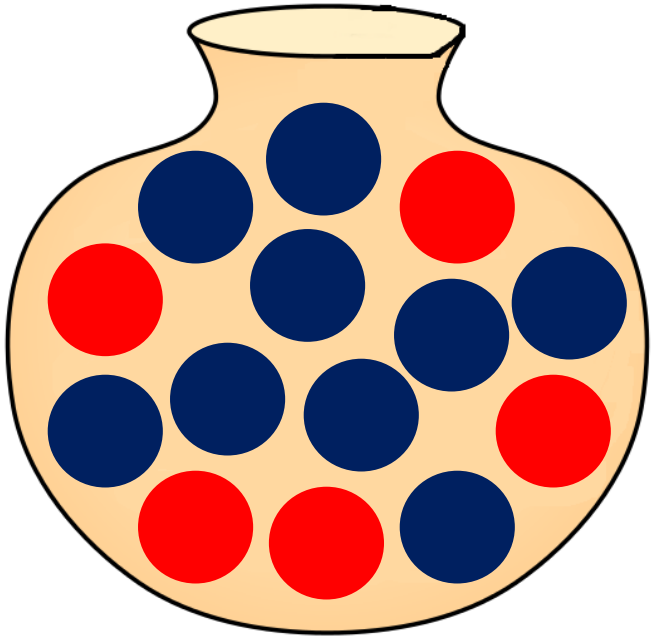
Pólya's urn process: learning

Urn 1



10 red and 4 blue

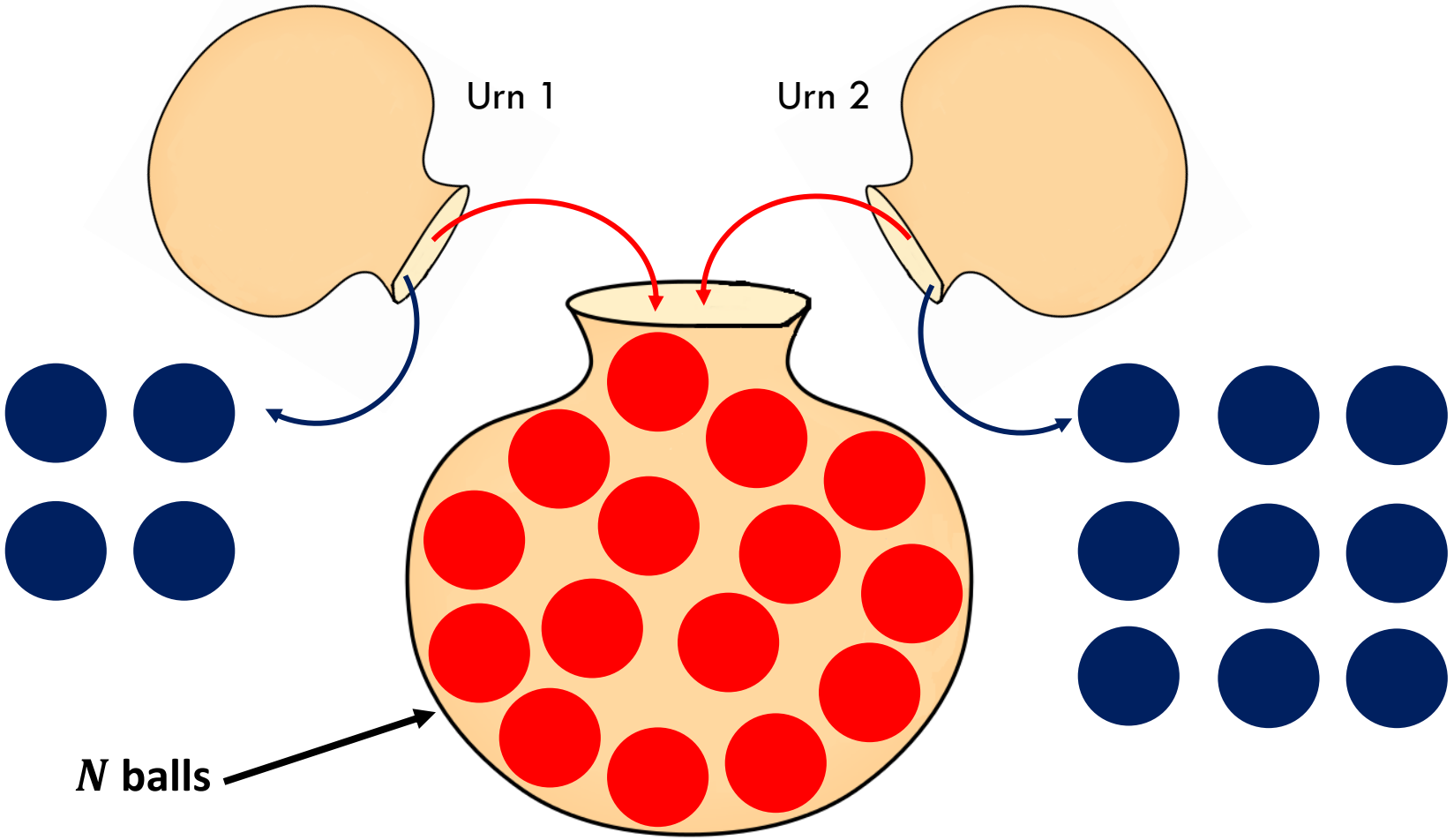
Urn 2



5 red and 9 blue

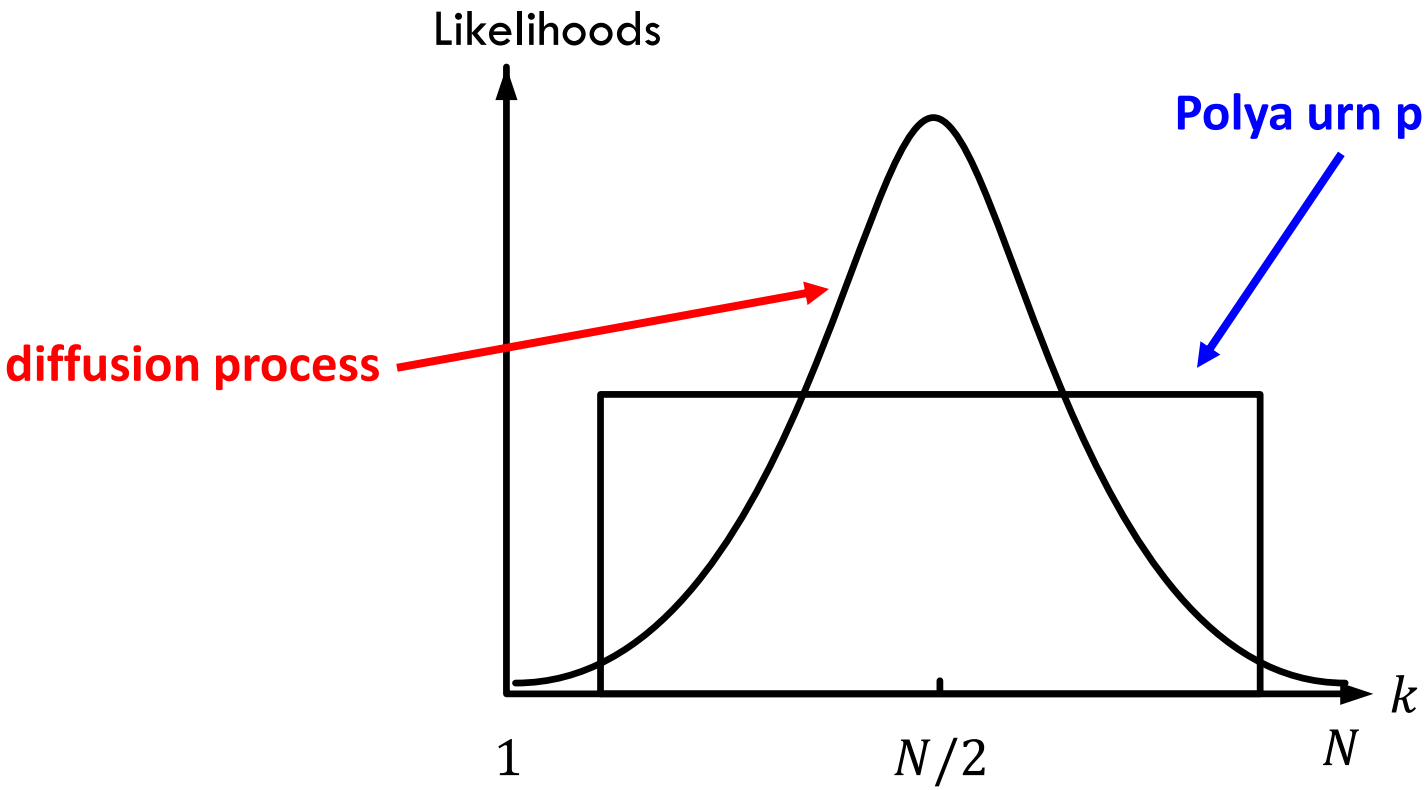
given two urns generated independently

Pólya's urn process: learning



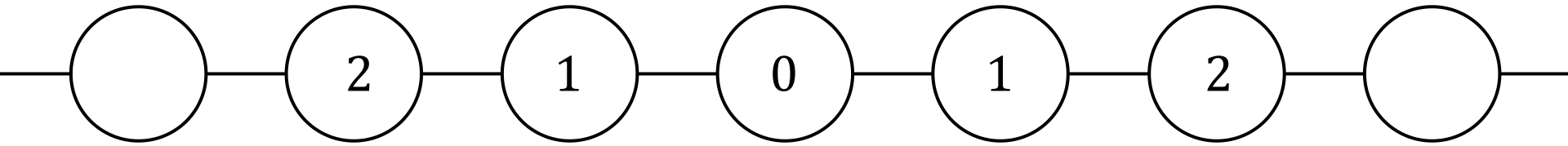
how many red balls came from urn 1?

Maximum likelihood detection



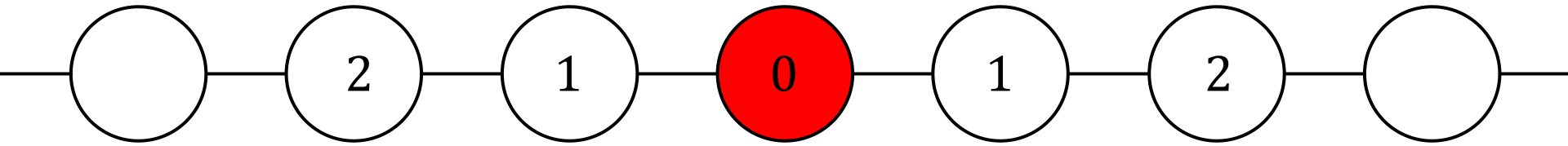
- we broke the **concentration** around $N/2$

Line graphs: adaptive diffusion



- consider a line graph

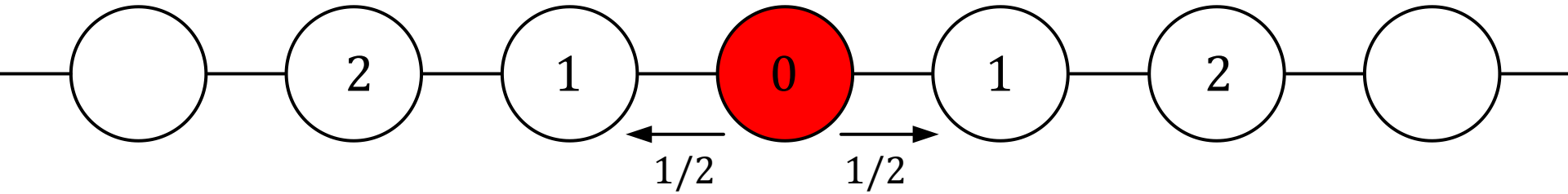
Line graphs: adaptive diffusion



$T = 0$

- node 0 starts a rumor at $T = 0$

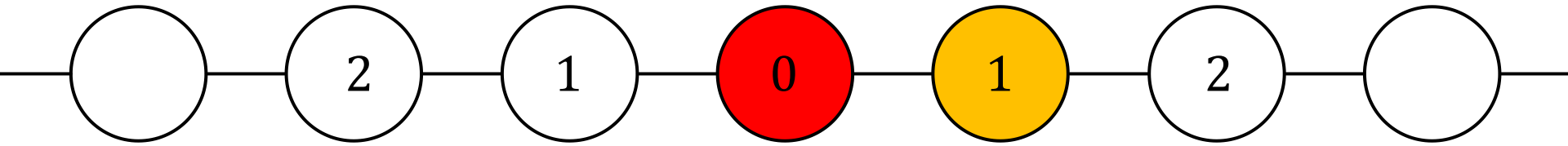
Line graphs: adaptive diffusion



$T = 1$

- with probability $1/2$, the left (right) node receives the message

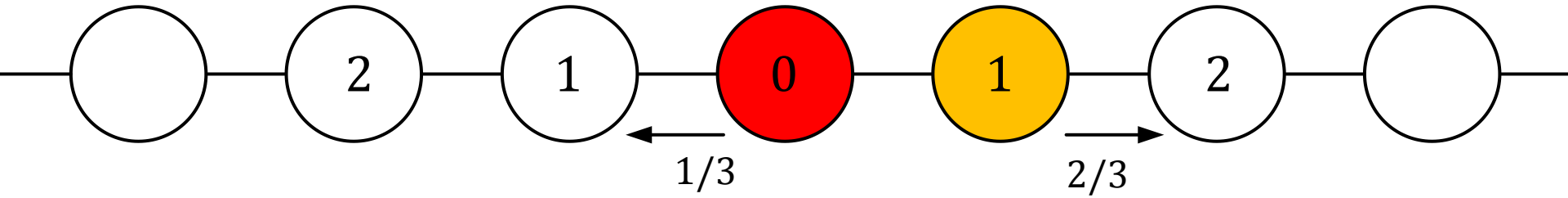
Line graphs: adaptive diffusion



$T = 1$

- right node 1 receives the message

Line graphs: adaptive diffusion



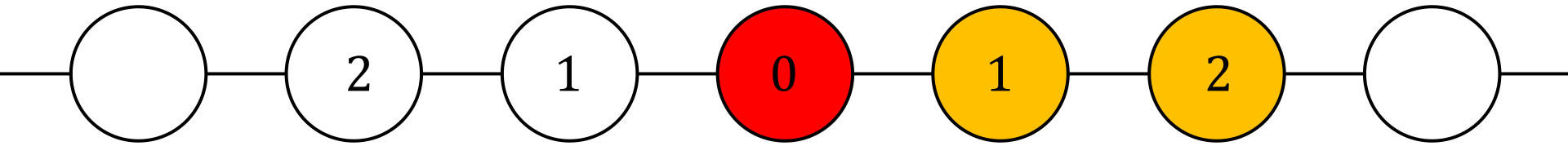
$$T = 2$$

hop distance to message author

- probability of passing message $= \frac{h+1}{T+1}$

elapsed time

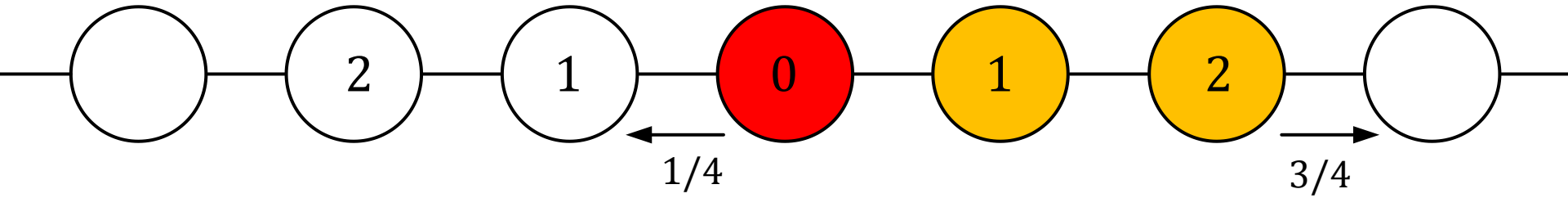
Line graphs: adaptive diffusion



$T = 2$

- right node 2 receives the message

Line graphs: adaptive diffusion



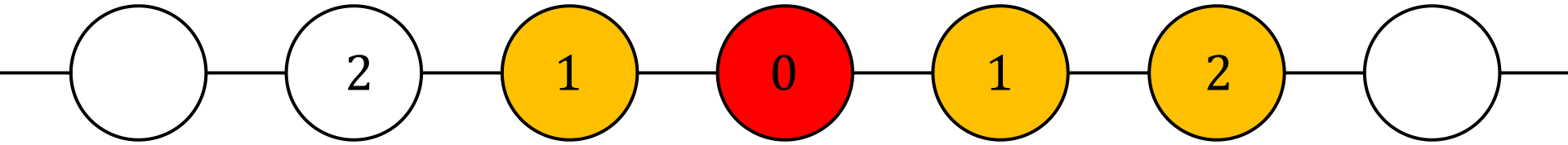
$T = 3$

hop distance to message author

- probability of passing message $= \frac{h+1}{T+1}$

elapsed time

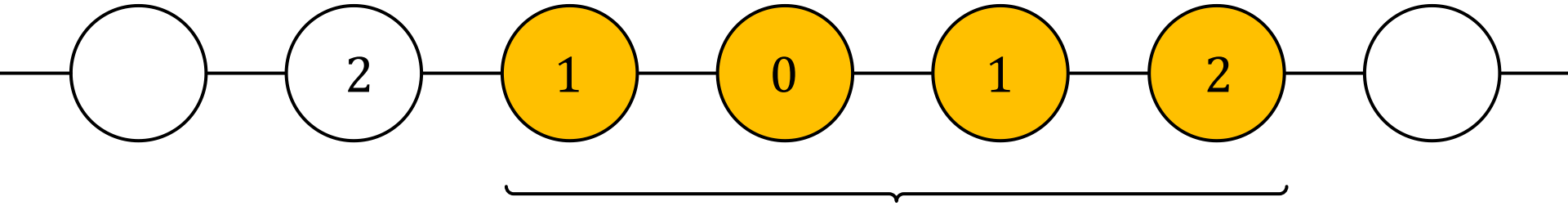
Line graphs: adaptive diffusion



$T = 3$

- left node 1 receives the message

Adversary

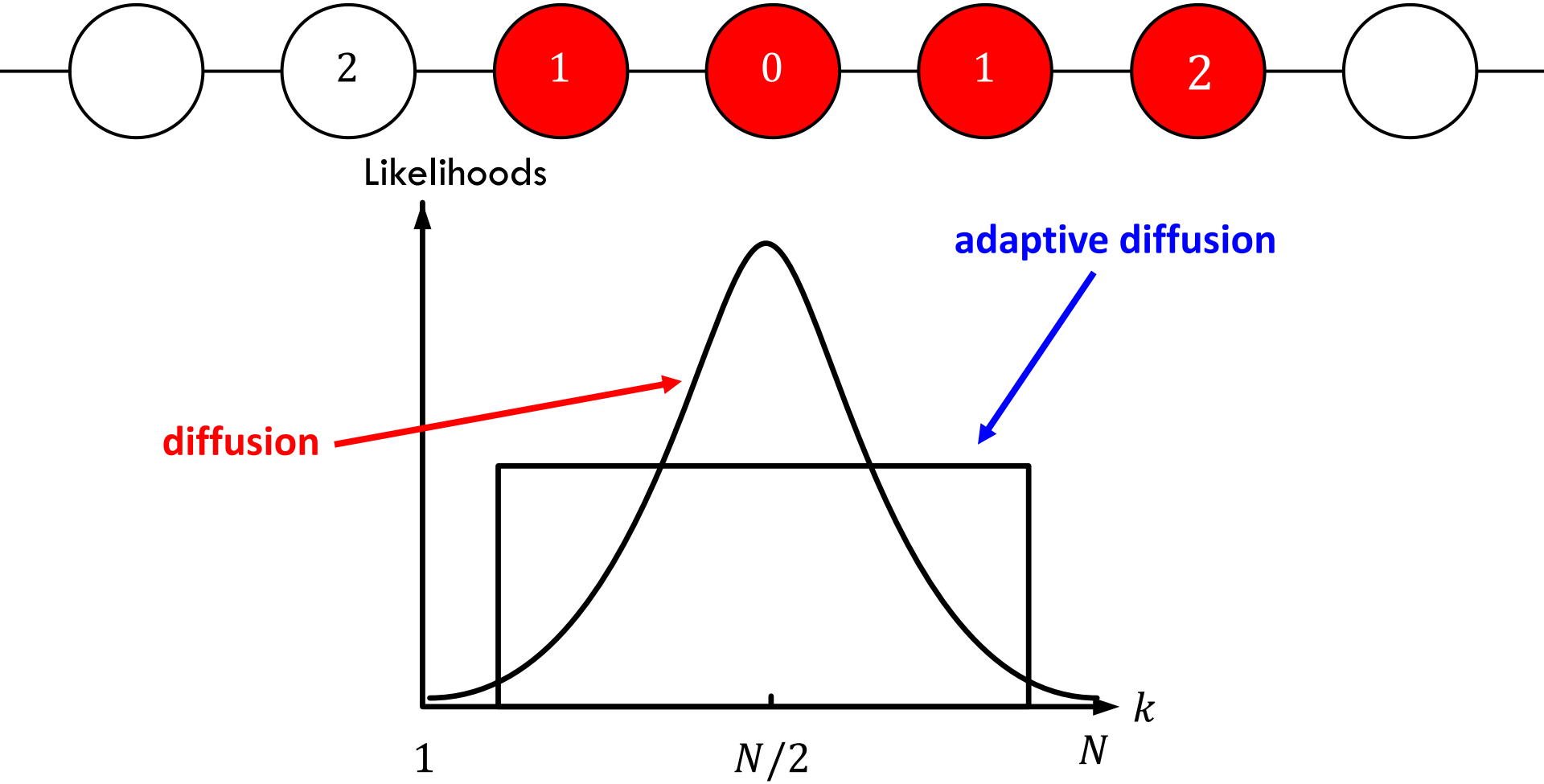


$N = 4$

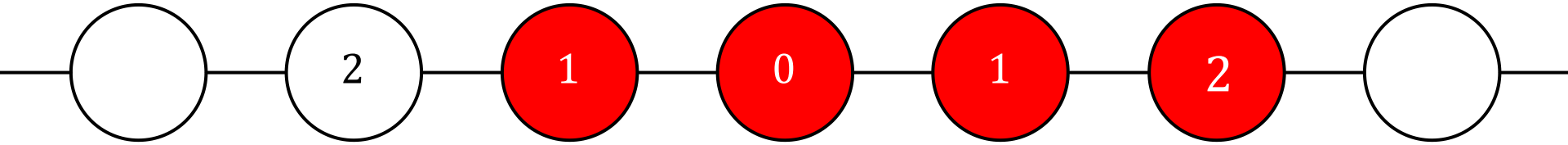
nodes with the message

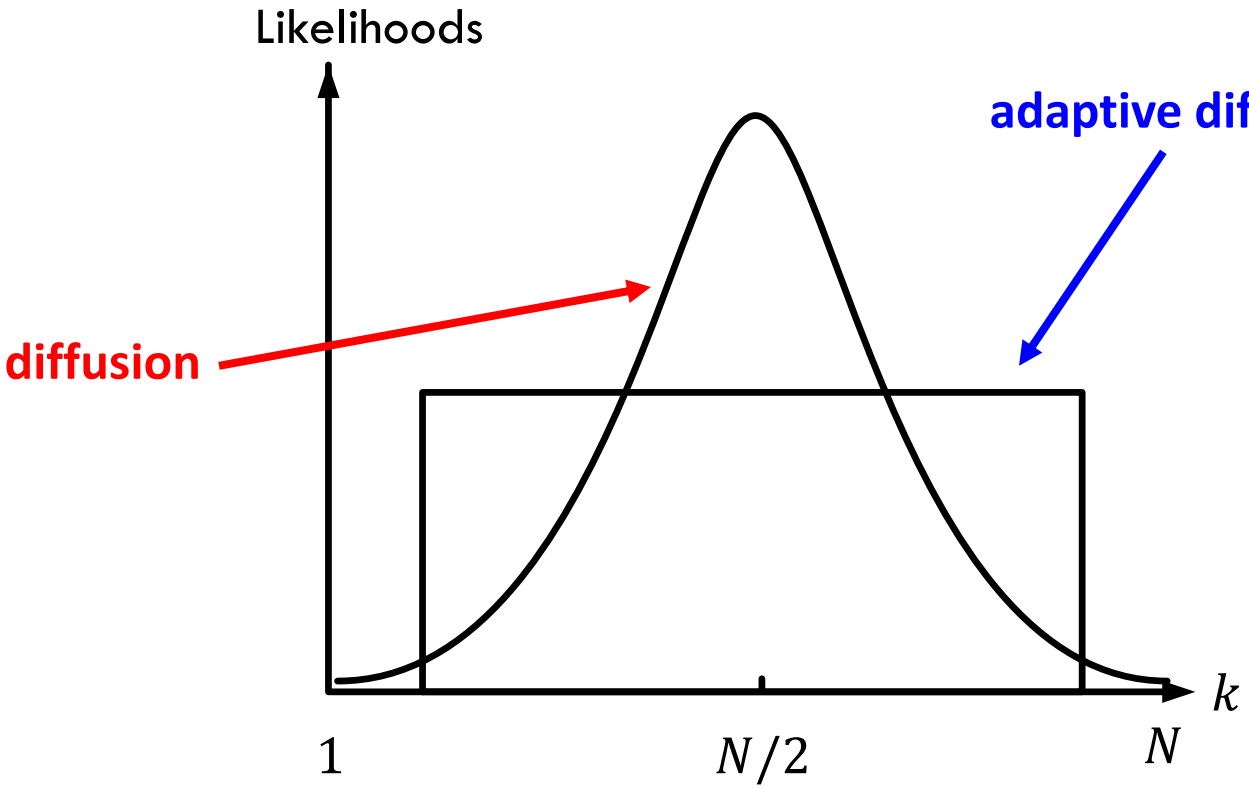
can we locate the message author?

Maximum likelihood detection



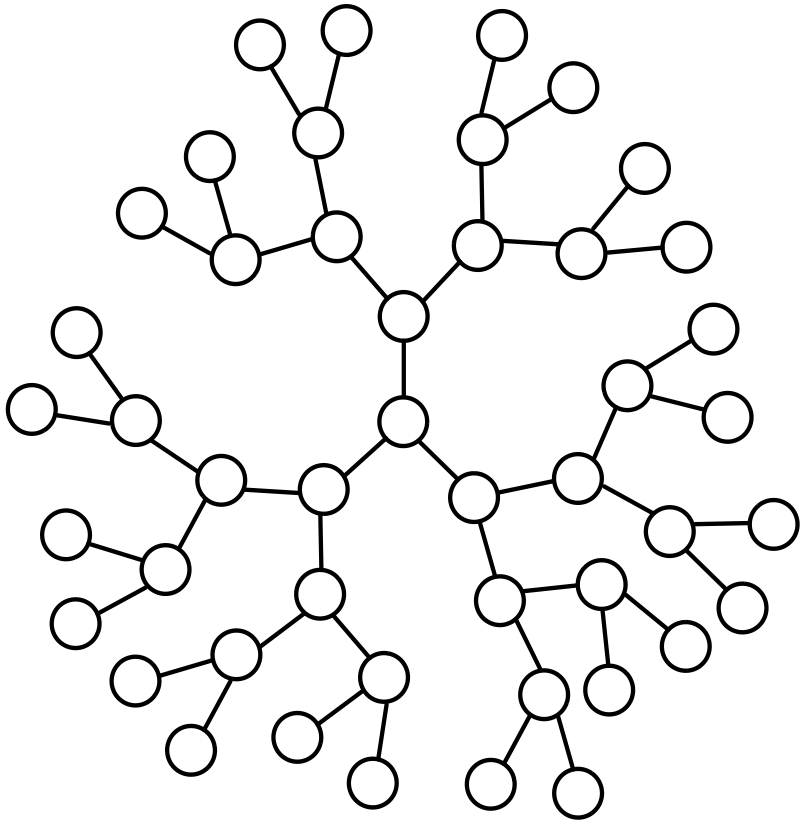
Maximum likelihood detection





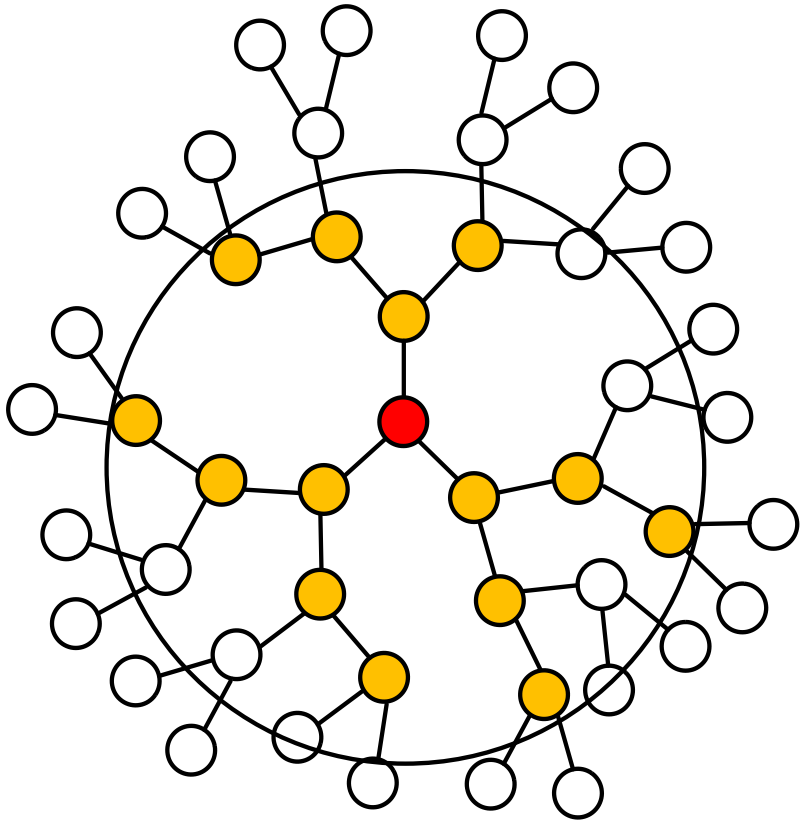
Probability of detection $\approx \frac{1}{N}$

d-regular trees



- what about d-regular trees?

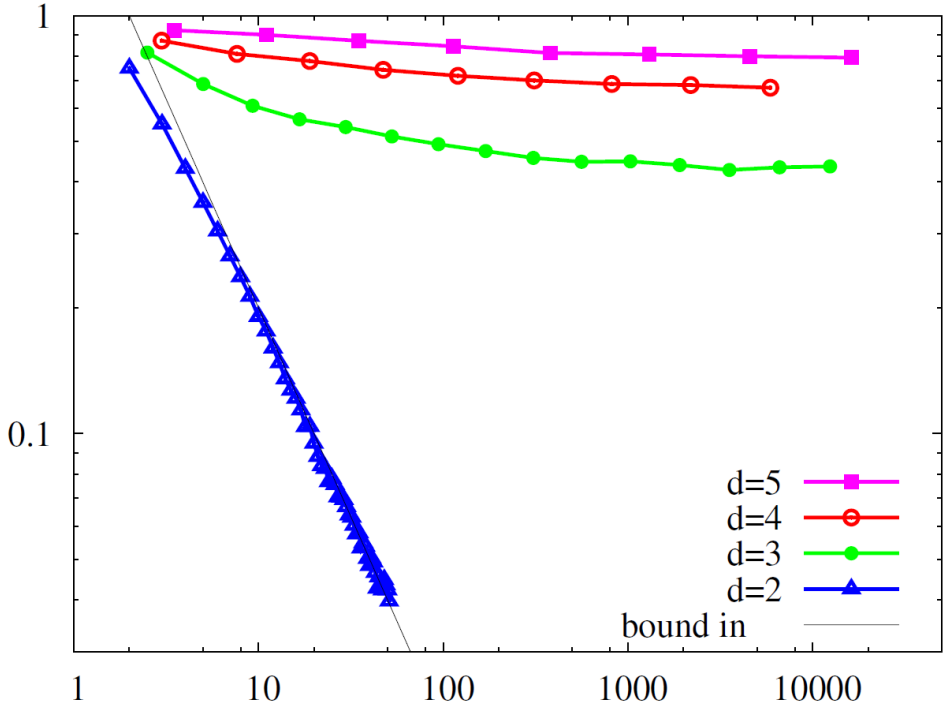
d-regular trees: diffusion



- likelihoods concentrate around the center

d-regular trees: Pólya's urn processes

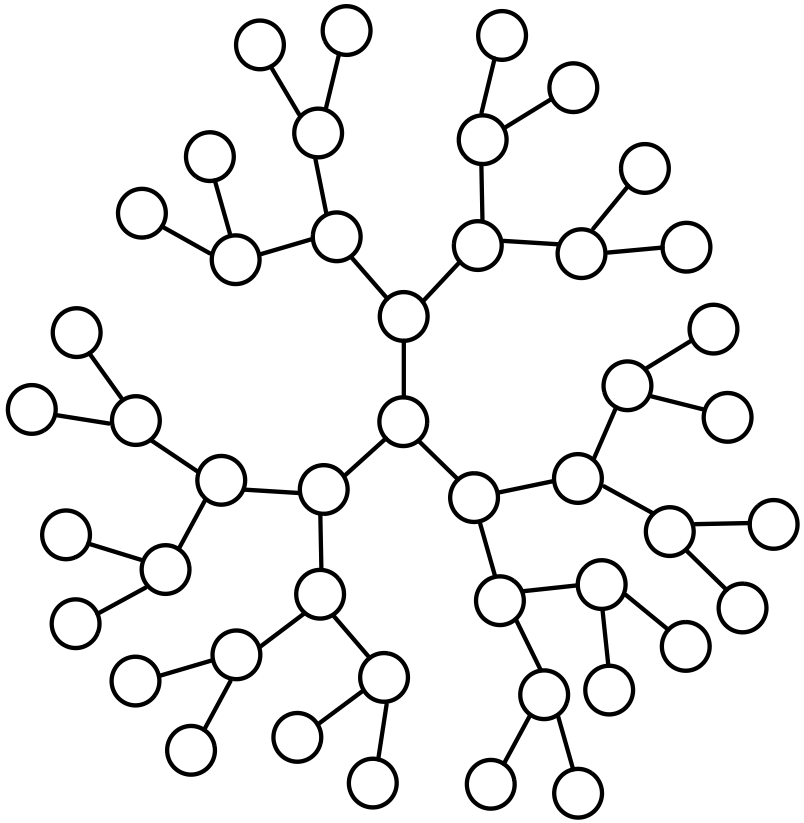
Probability of detection using Jordan centrality



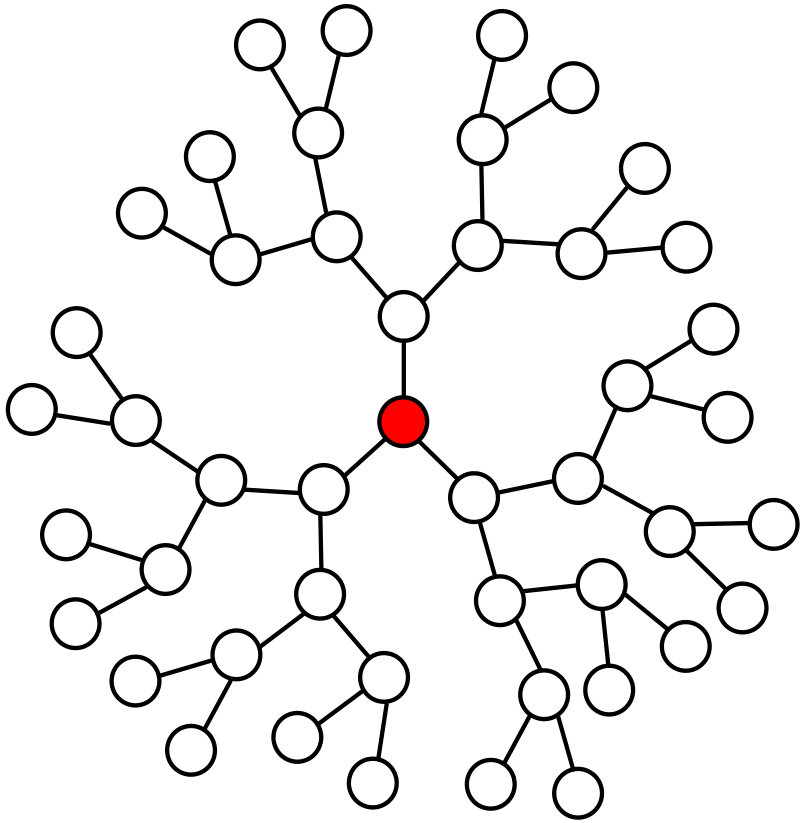
number of nodes with the message

- does not work at all!

d-regular trees : adaptive diffusion

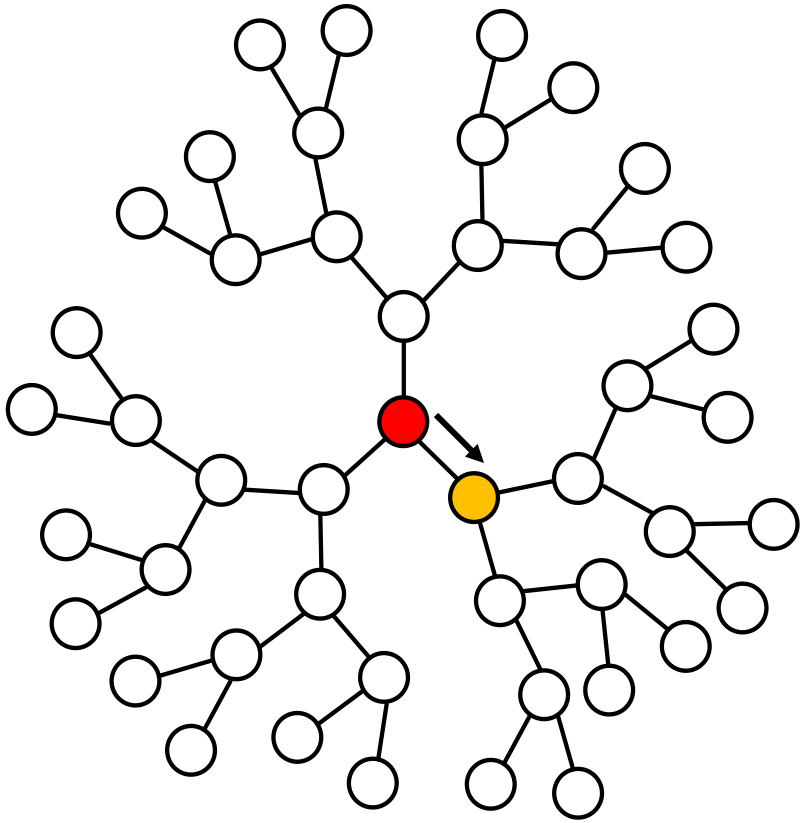


d-regular trees : adaptive diffusion



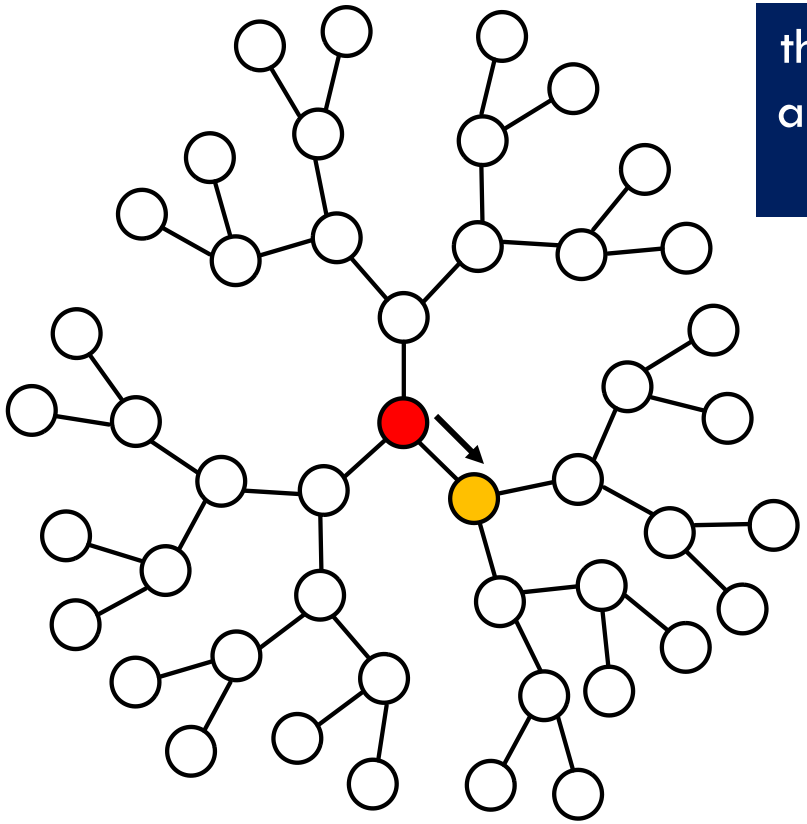
- initially, the author is also the **"virtual source"**

d-regular trees : adaptive diffusion



- at $T = 1$, the author selects one neighbor at random

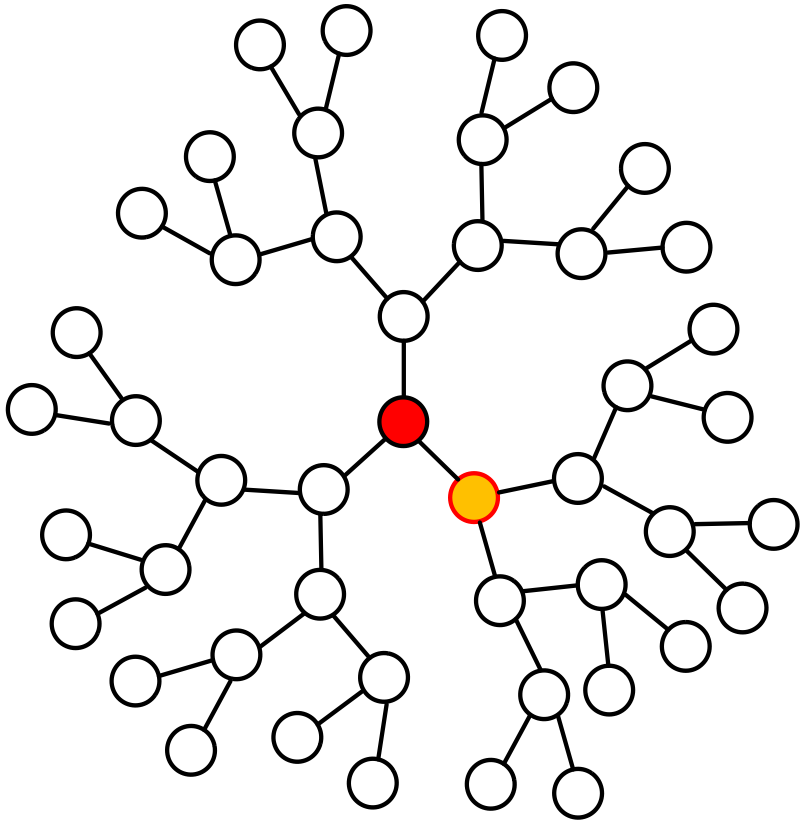
d-regular trees : adaptive diffusion



the author passes $h = 1$ and $T = 2$ to the chosen neighbor

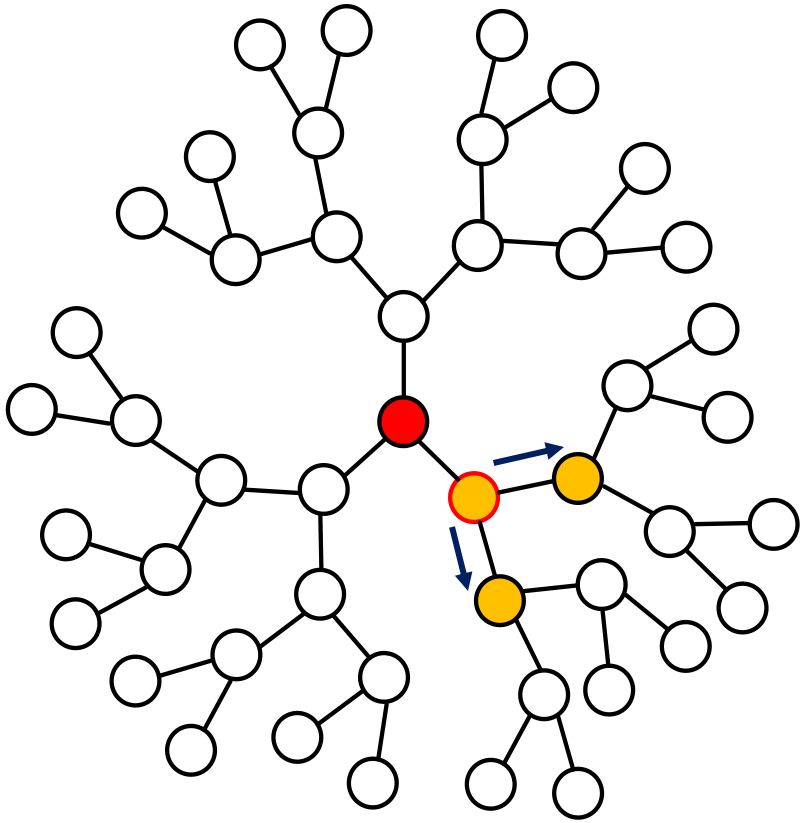
- at $T = 1$, the author selects one neighbor at random

d-regular trees : adaptive diffusion



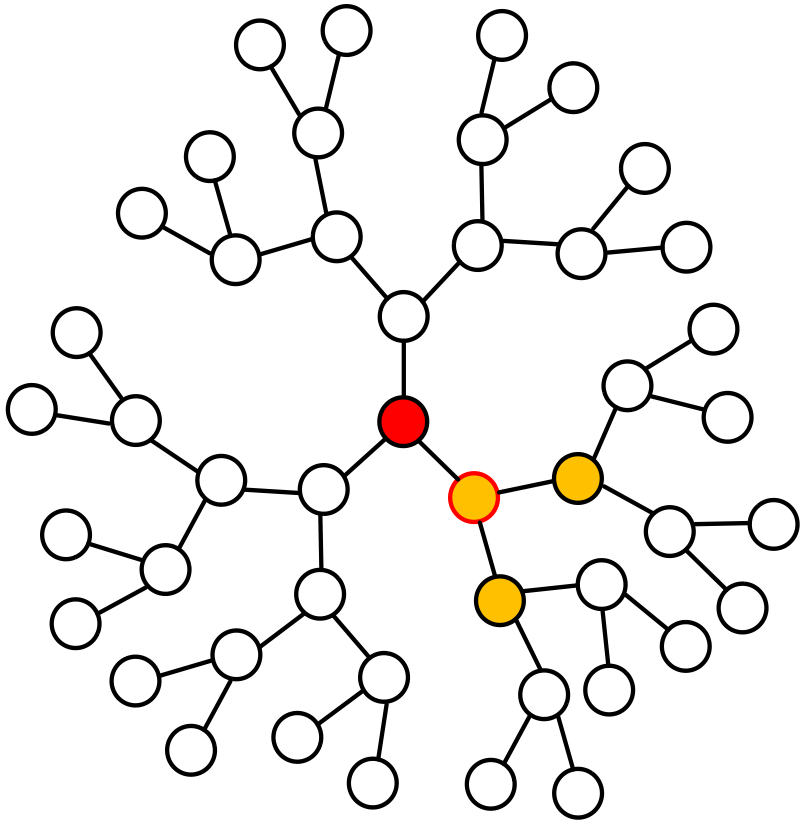
- the chosen neighbor becomes the **new virtual source**

d-regular trees : adaptive diffusion



- at $T = 2$, the **virtual source** passes the message to all its neighbors

d-regular trees : adaptive diffusion

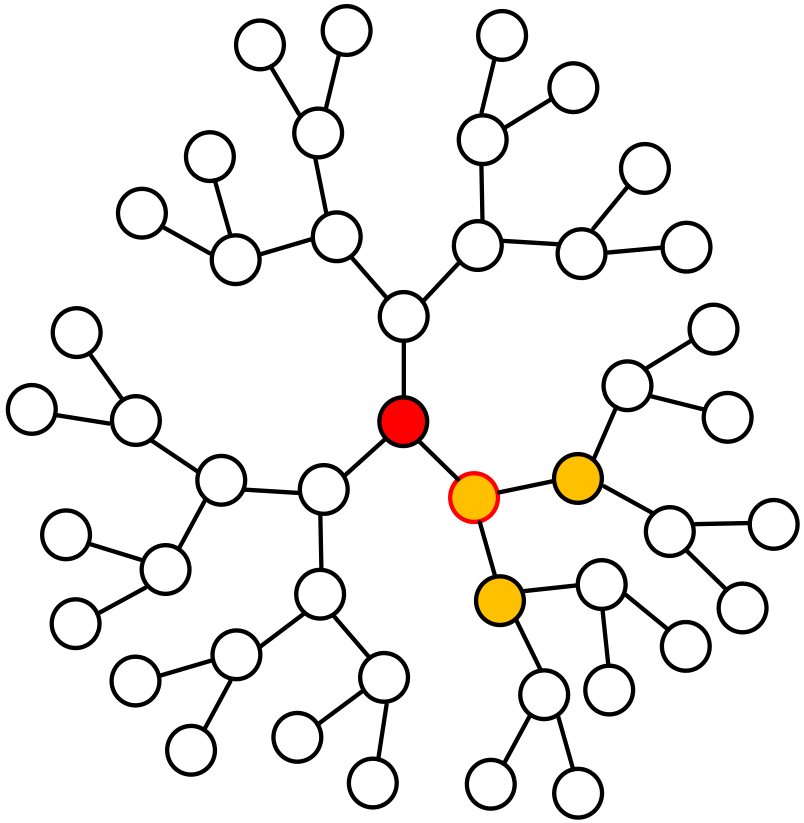


- as T transitions from even to odd, the virtual source has two options:

keeping the virtual source token

passing the virtual source token

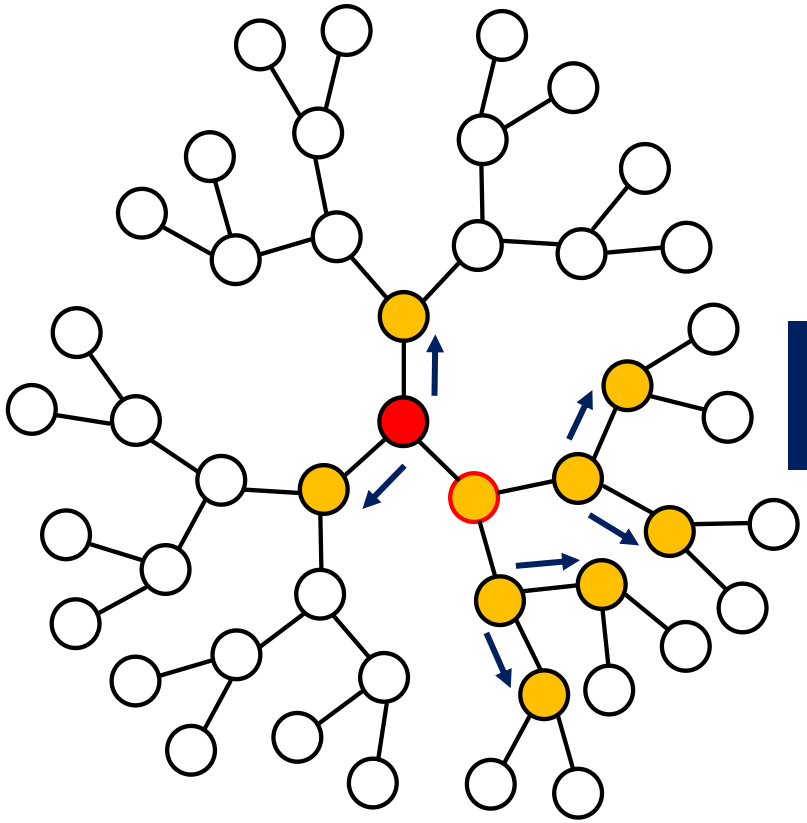
Keeping the virtual source token



adaptive rate

- virtual source token is kept with probability $\frac{(d-1)^{\frac{T}{2}-h-1}-1}{(d-1)^{\frac{T}{2}+1}-1}$

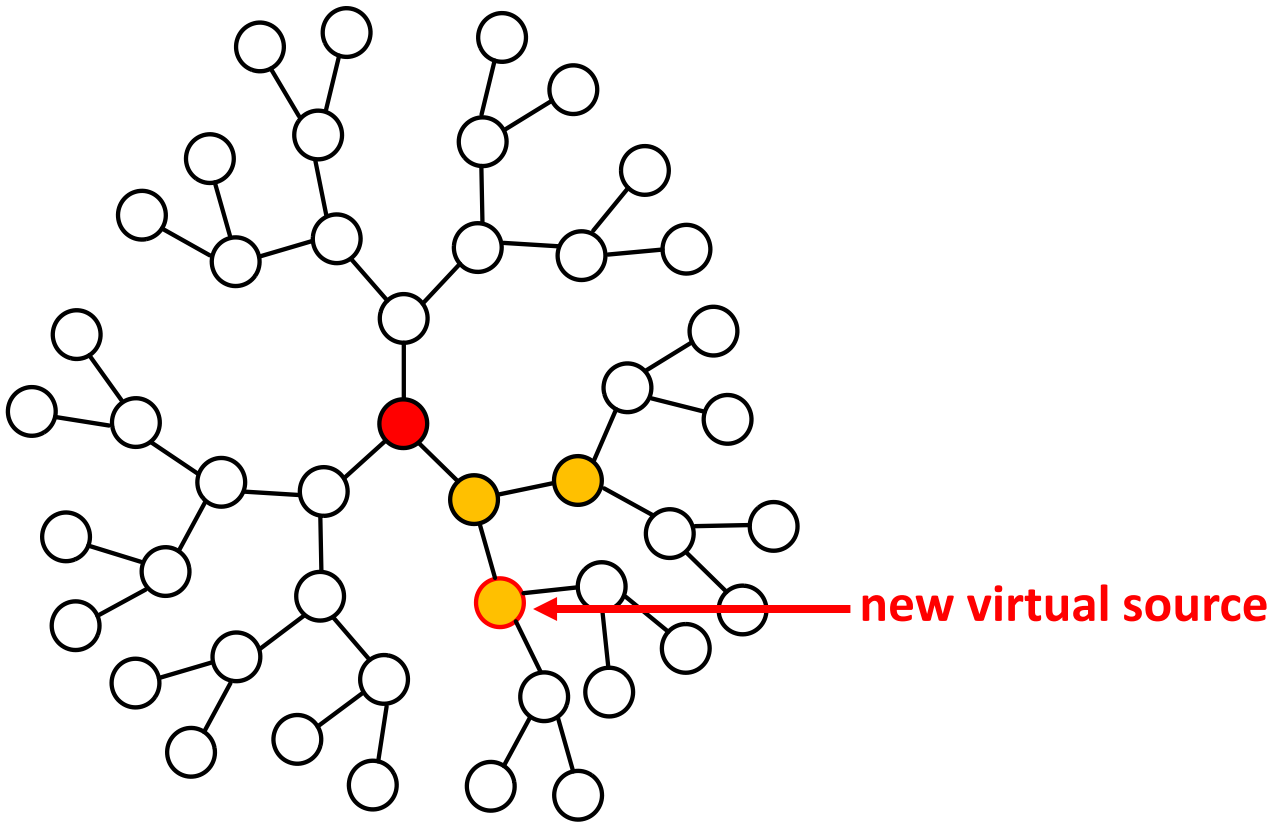
Keeping the virtual source token



happens in $T = 3$ and $T = 4$

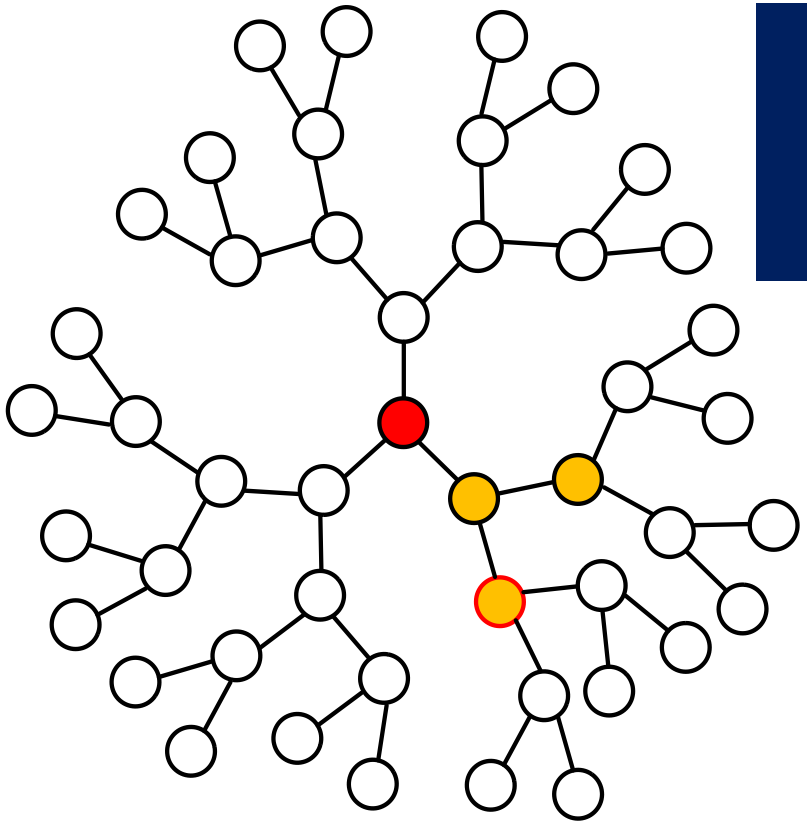
- all leaf nodes with the message pass it to their neighbors

Passing the virtual source token



- current virtual source selects one of its neighbors at random

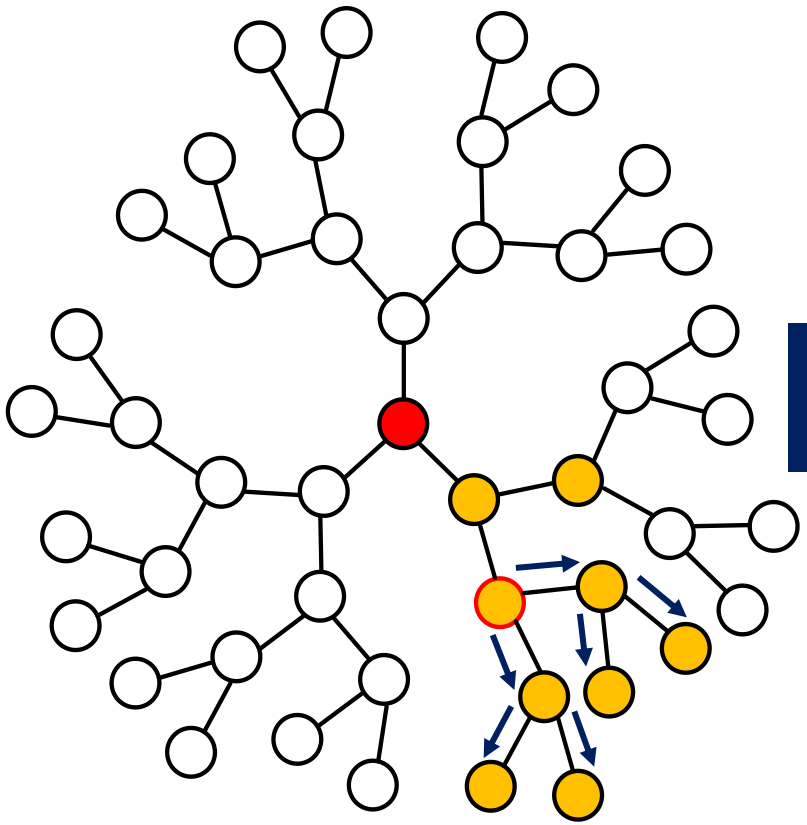
Passing the virtual source token



current virtual source passes $h = 2$ and $T = 4$ to new virtual source

- current virtual source selects one of its neighbors at random

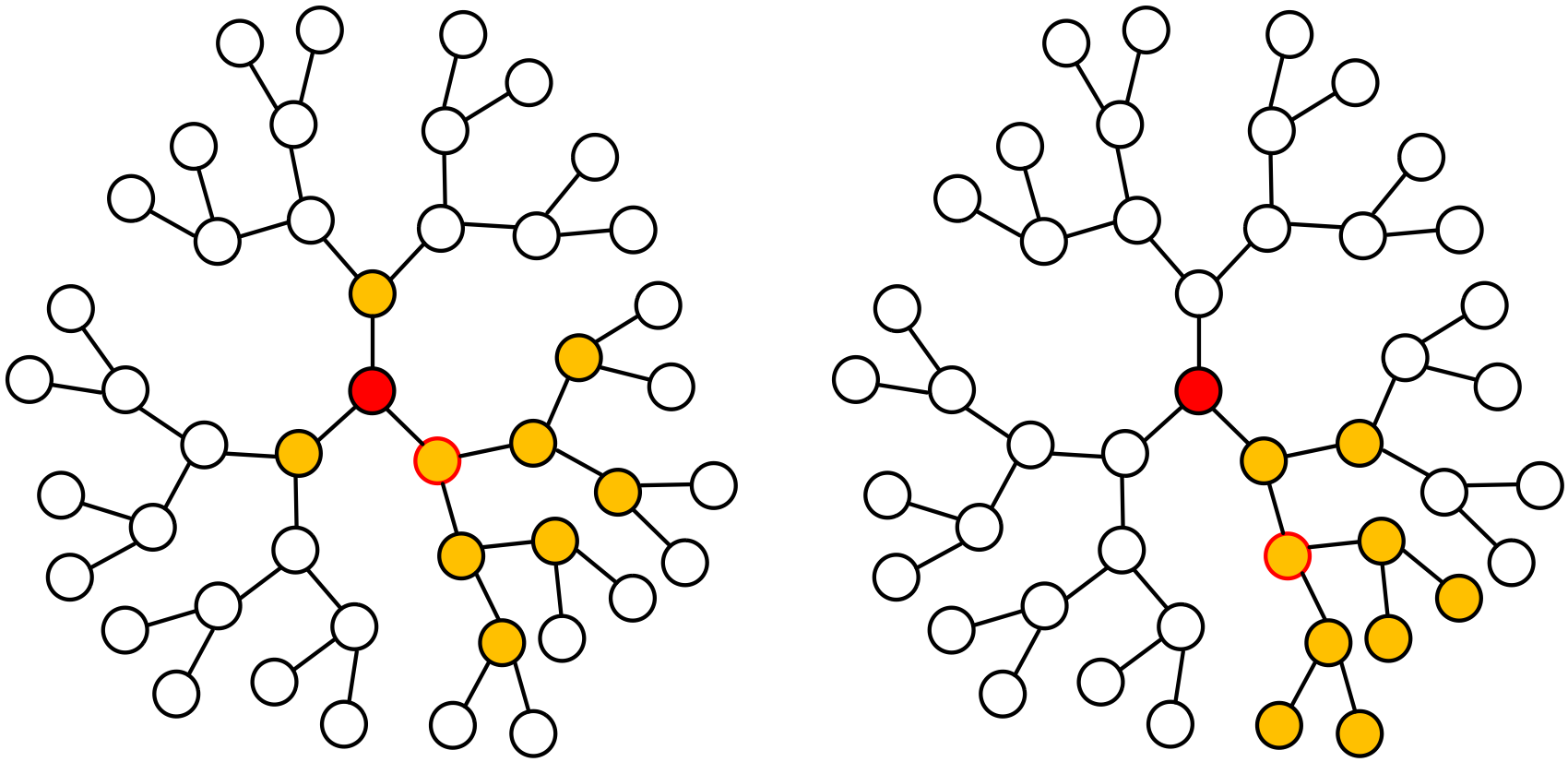
Passing the virtual source token



happens in $T = 3$ and $T = 4$

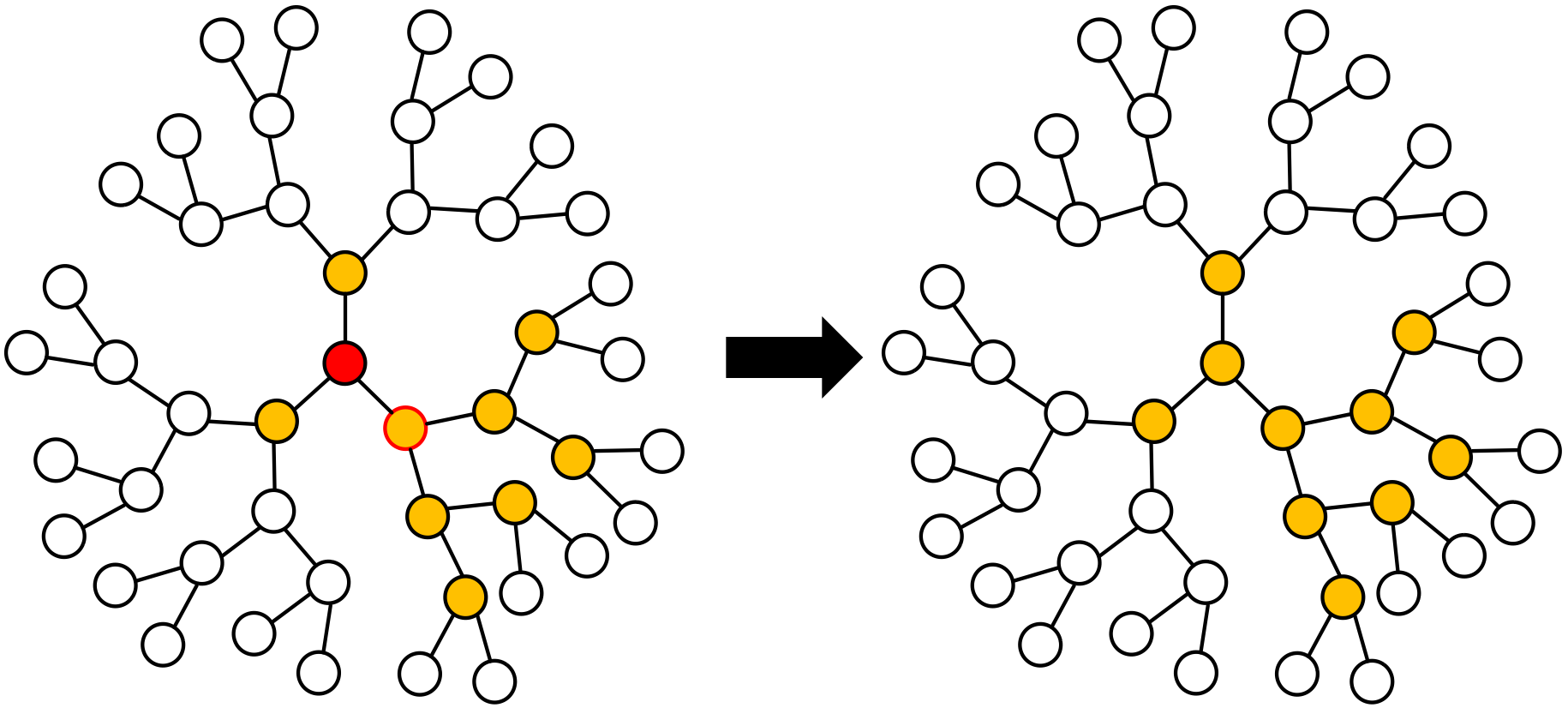
- new virtual source passes the message to its neighbors which in turn pass it to their neighbors

Symmetry properties



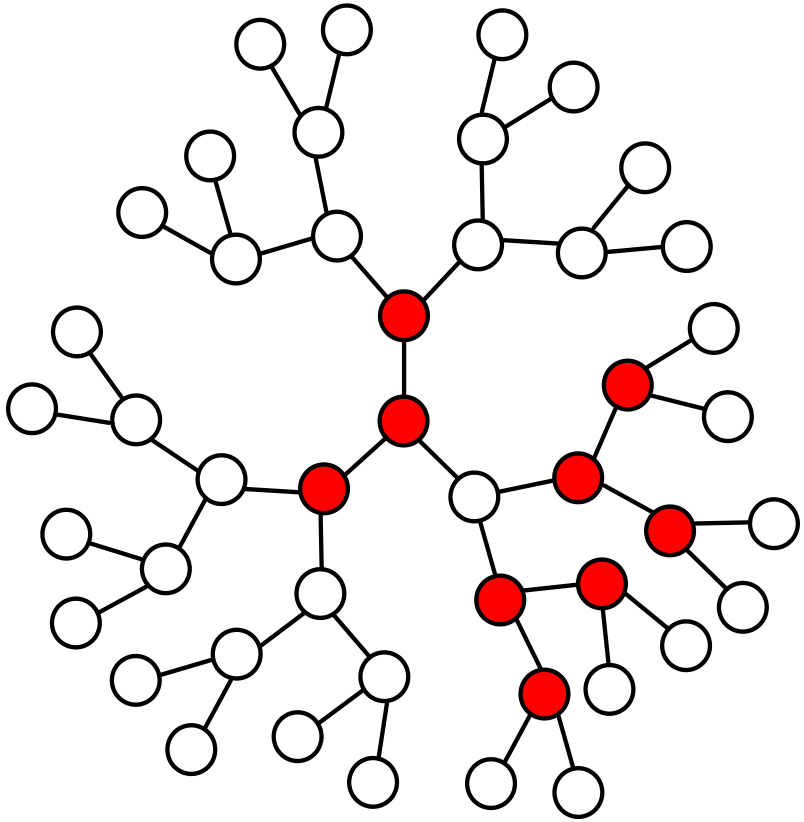
- the graph is **always symmetric** around the **virtual source**

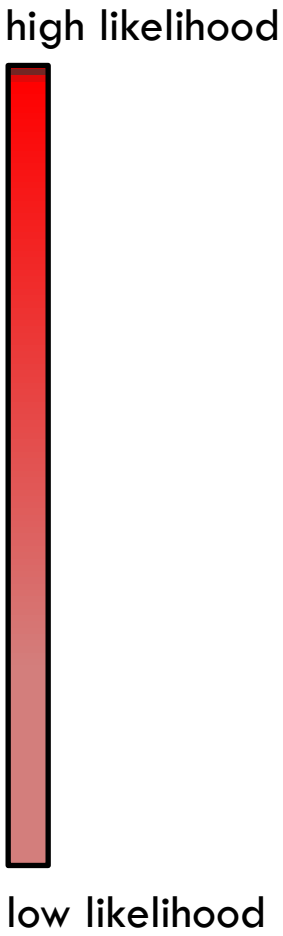
Adversary



can we locate the message author?

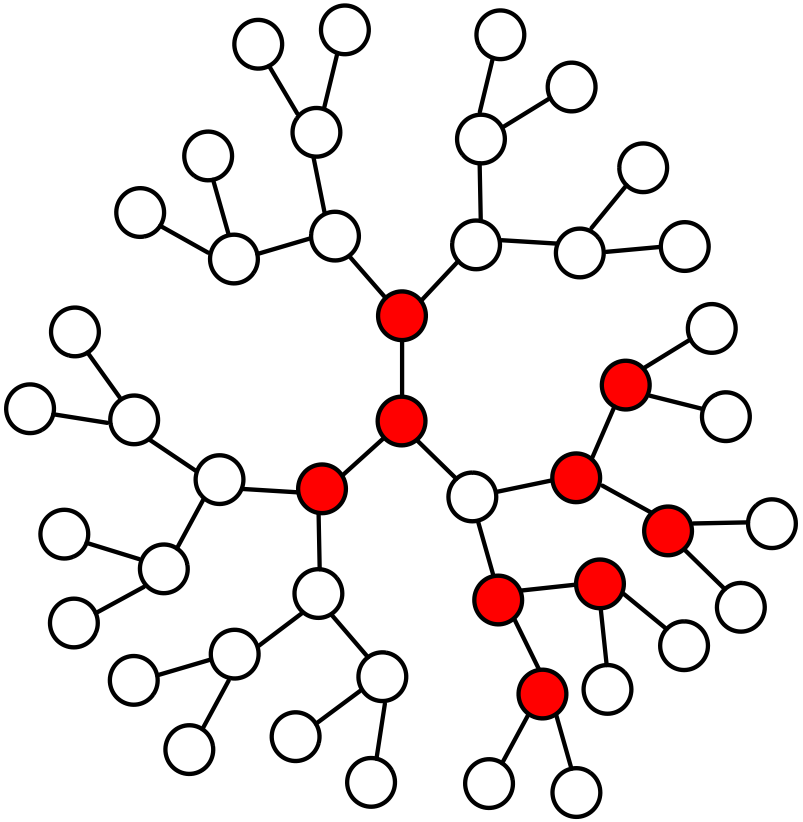
Maximum likelihood detection





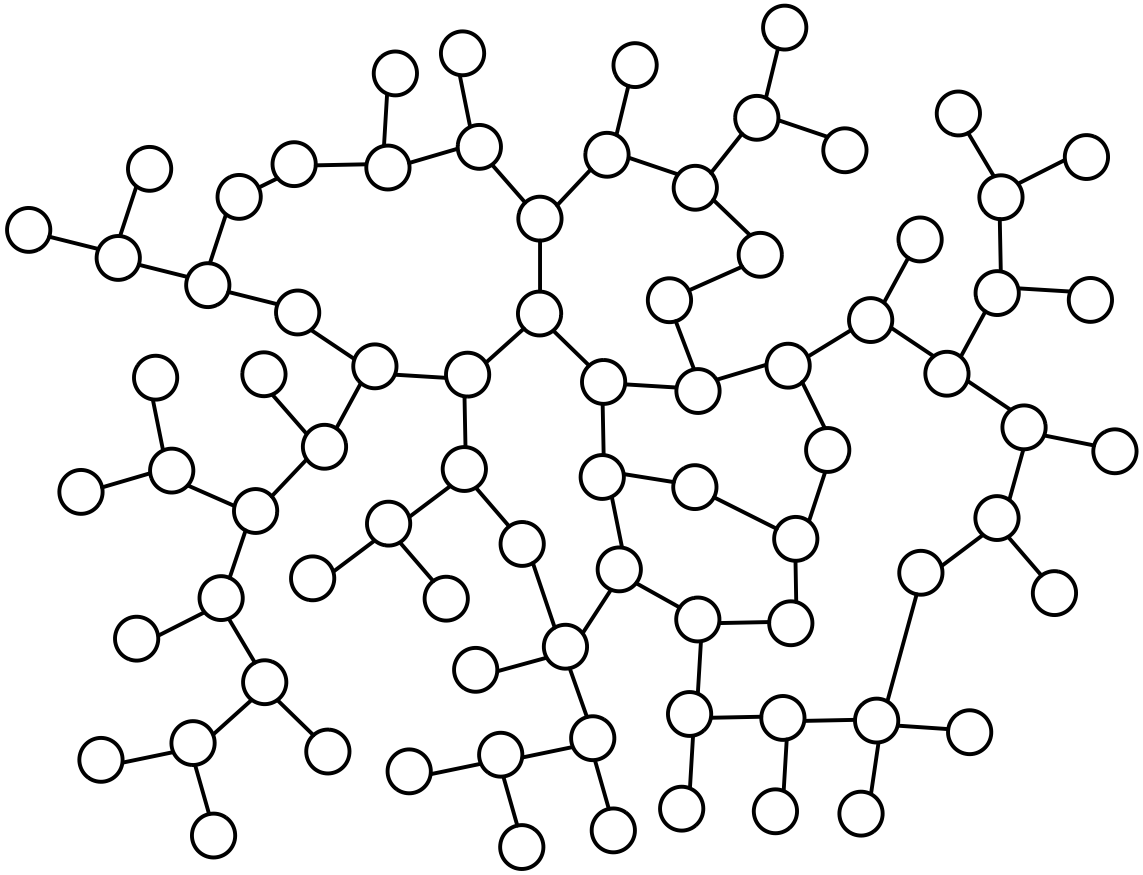
- **all nodes** except for the final virtual source **are equally likely**

Maximum likelihood detection



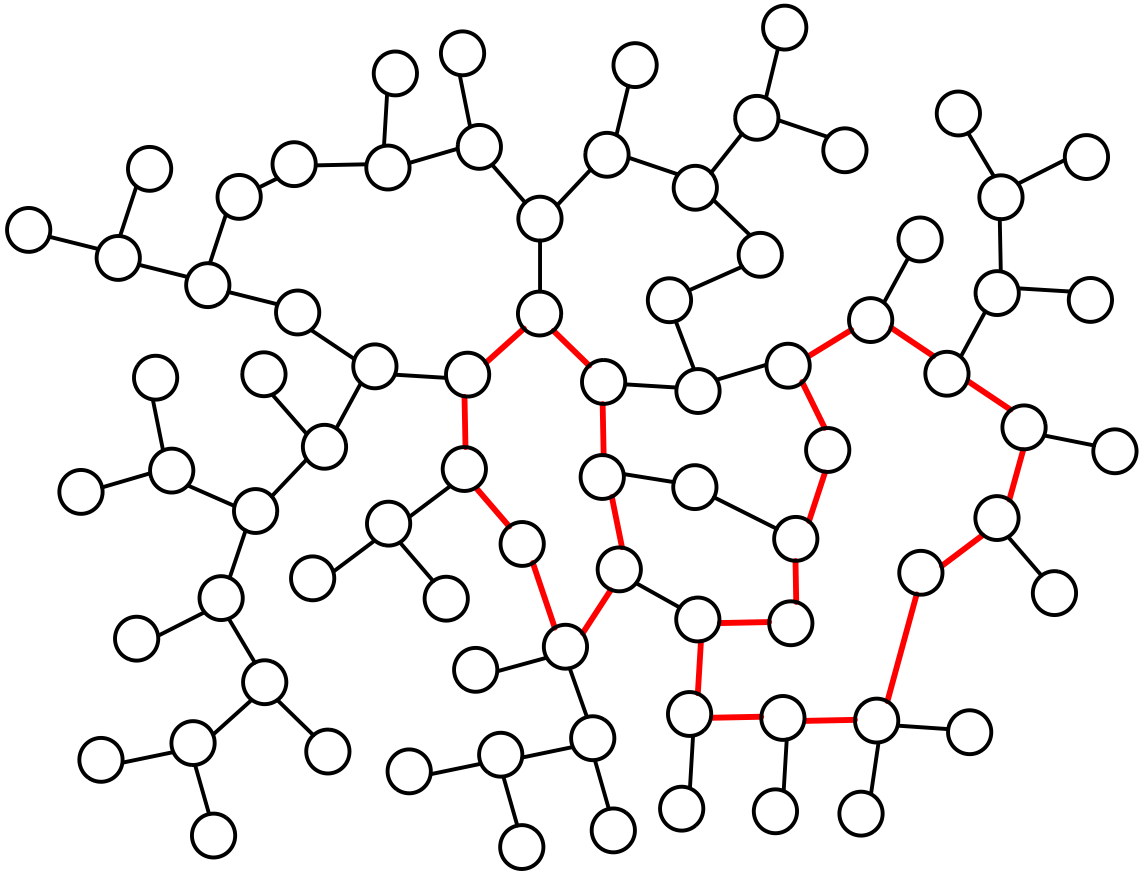
Probability of detection $= \frac{1}{N-1}$

General graphs



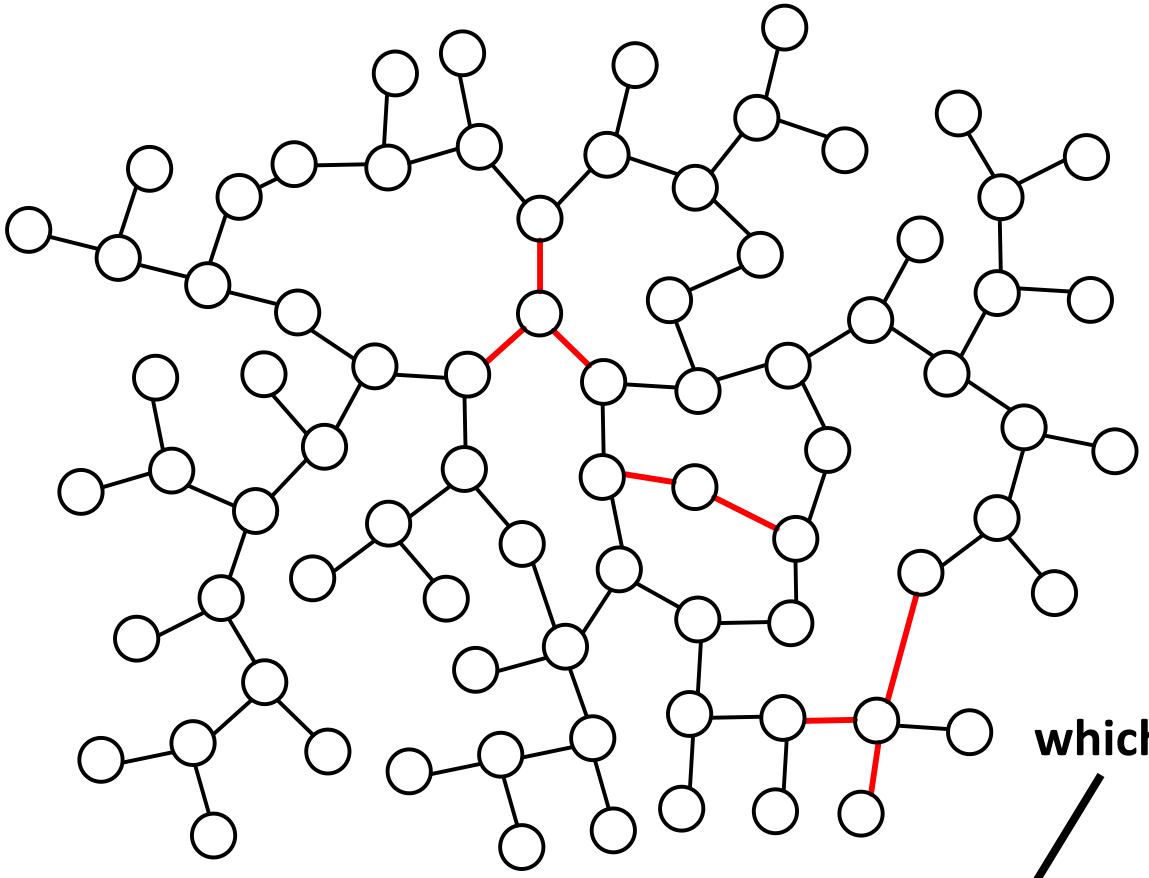
can we extend adaptive diffusion for general graphs?

General graphs: cycles



- do not pass the message to a node that already has the message

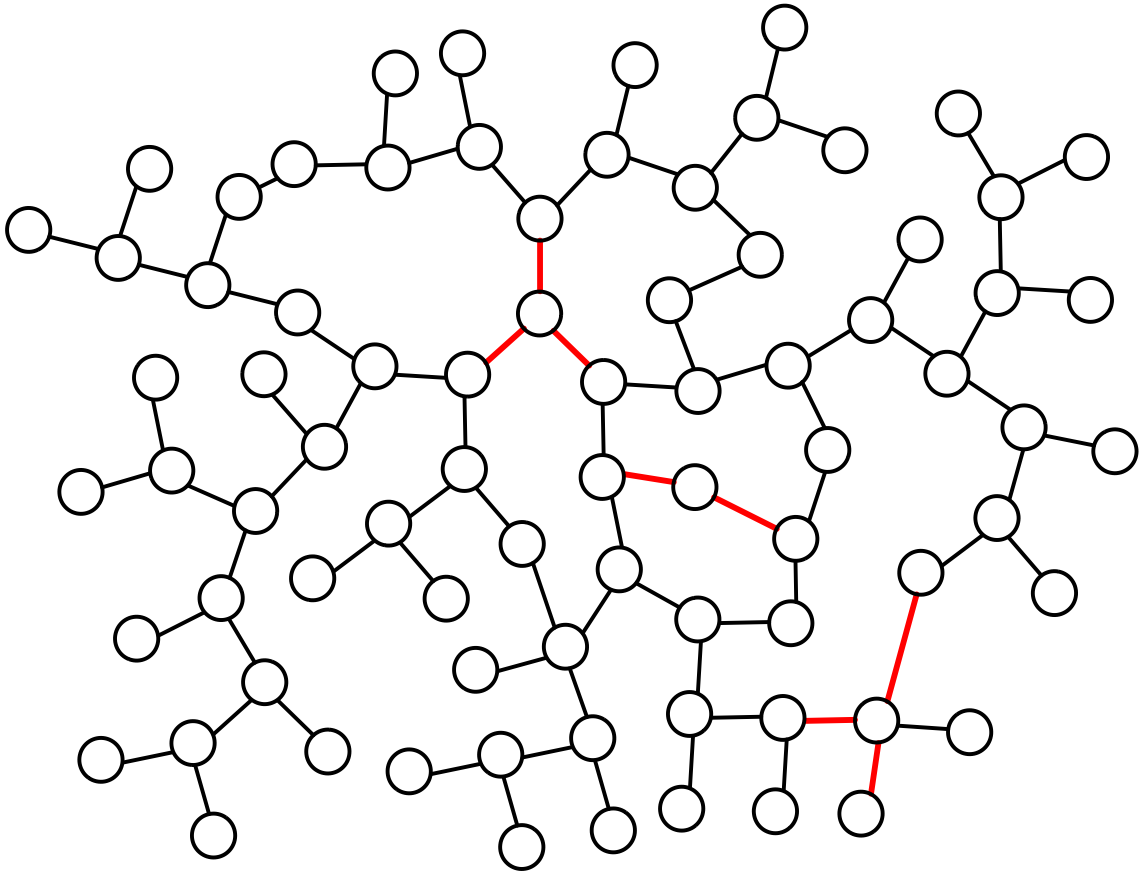
General graphs: degree irregularities



which d to choose?

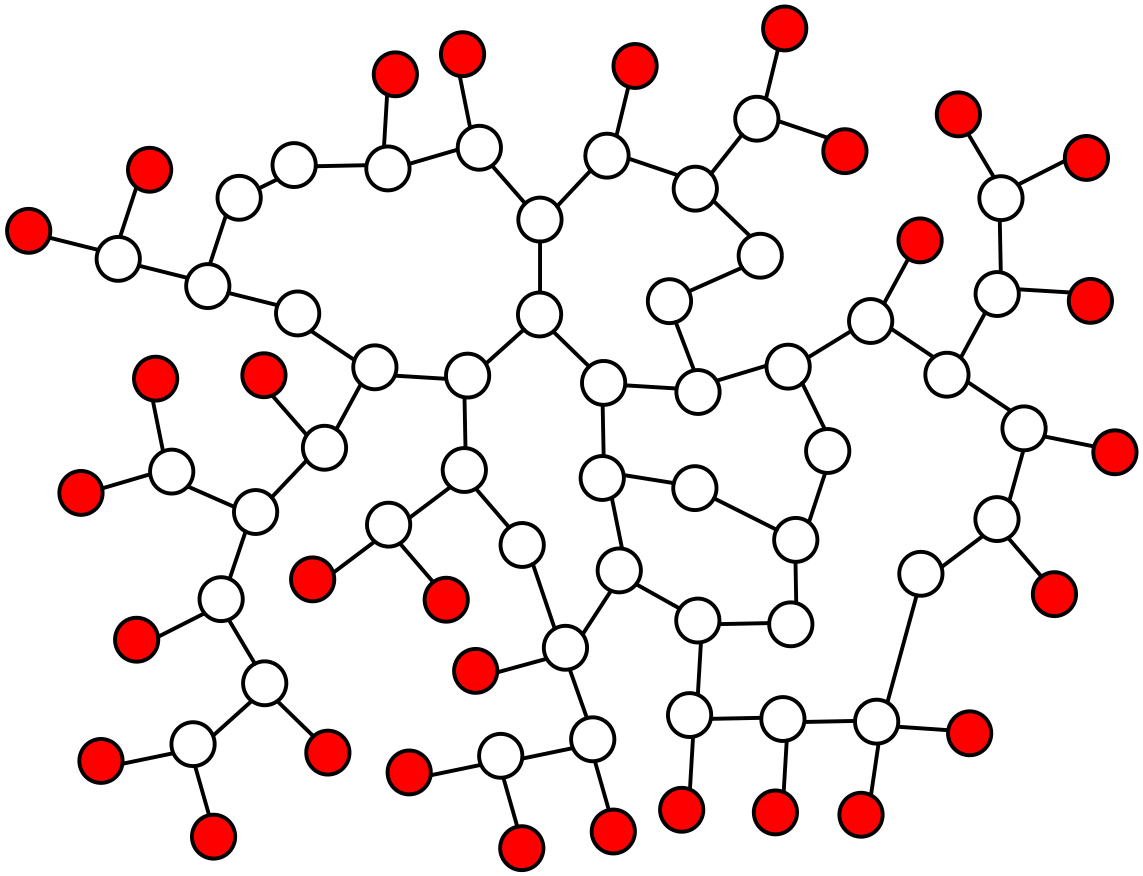
- virtual source token is kept with probability $\frac{(d-1)^{\frac{T}{2}-h-1}-1}{(d-1)^{\frac{T}{2}+1}-1}$

General graphs: degree irregularities



- any $d \geq 3$ works well in practice
- to preserve symmetry, each node talks to at most 3 neighbors

General graphs: boundary effects



- the **virtual source** is allowed to turn around when it hits the boundary

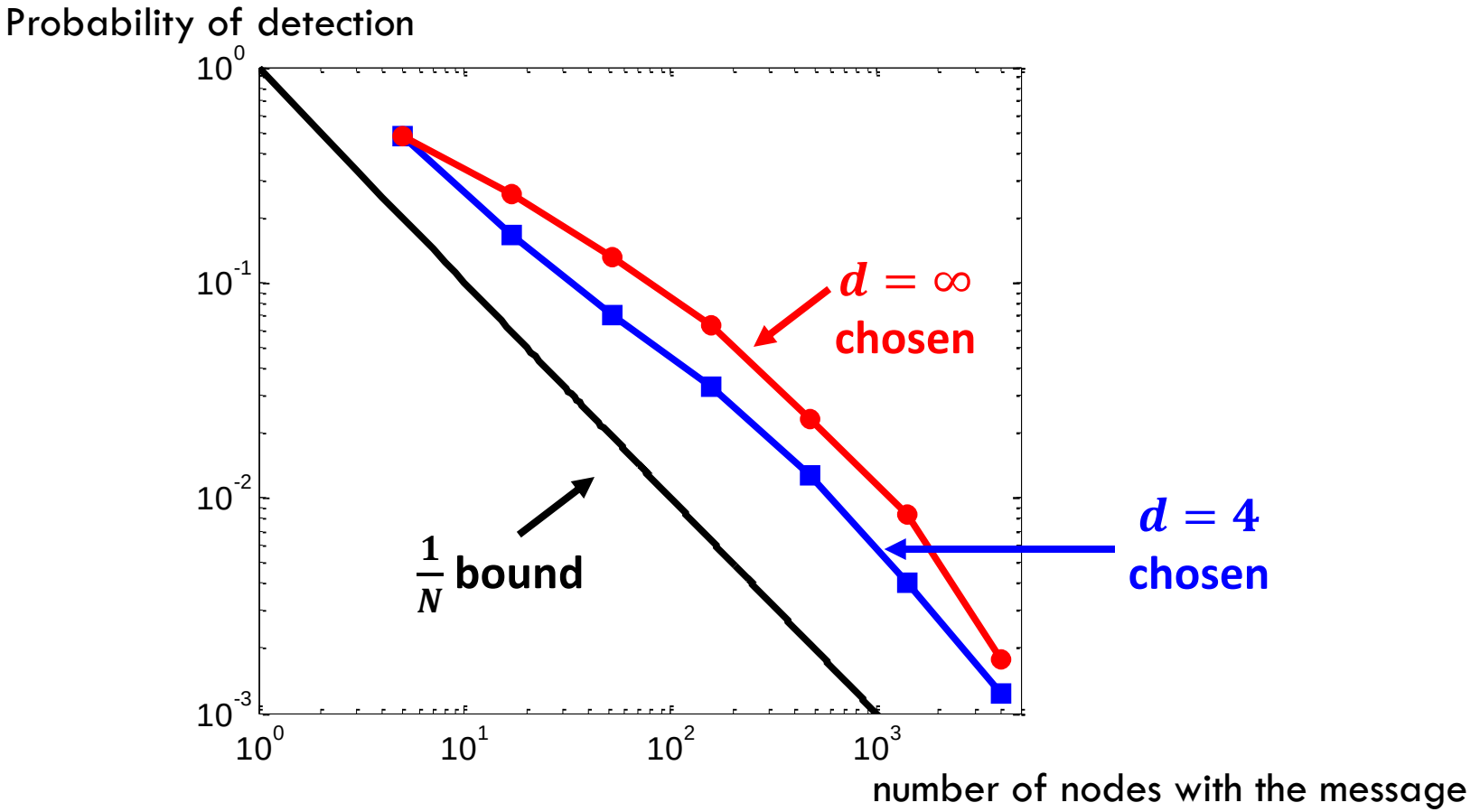
Simulation setup

- 10,000 Facebook users in New Orleans circa 2009
- all users with degree less than 3 were removed

Simulation results

- on average, 96% of users received the message within 10 time steps

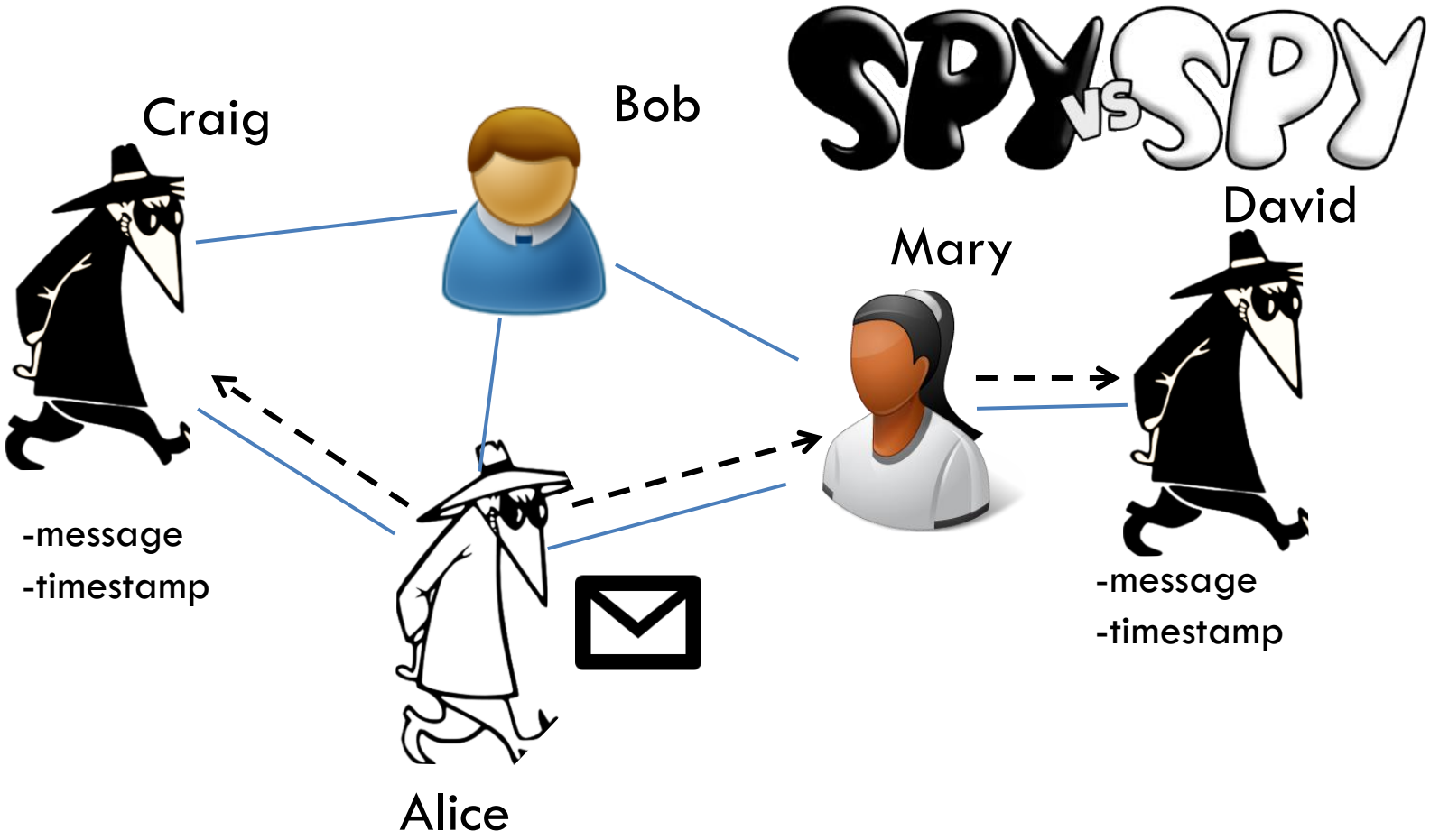
Simulation results



- likelihoods can be **approximated** numerically

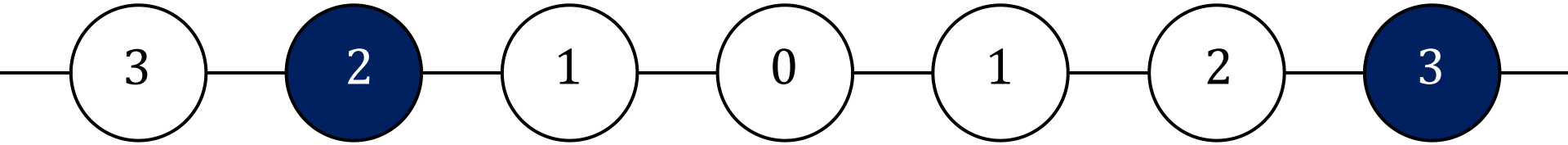
Part I:
Proposed Research

Spy adversarial model



adversary can collect timing information

Adversary with timing



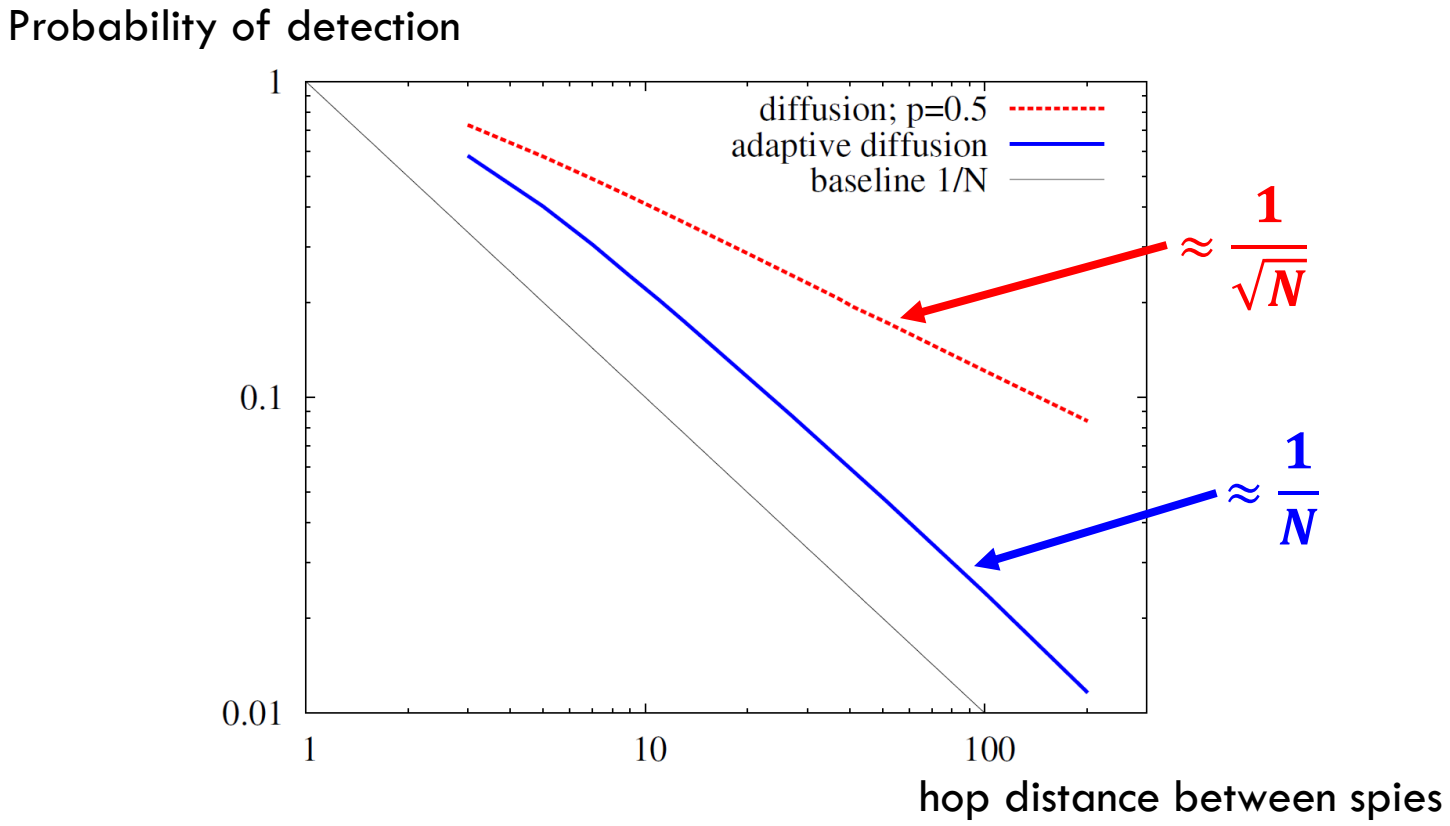
spy node 1

spy node 2

N = distance between spies

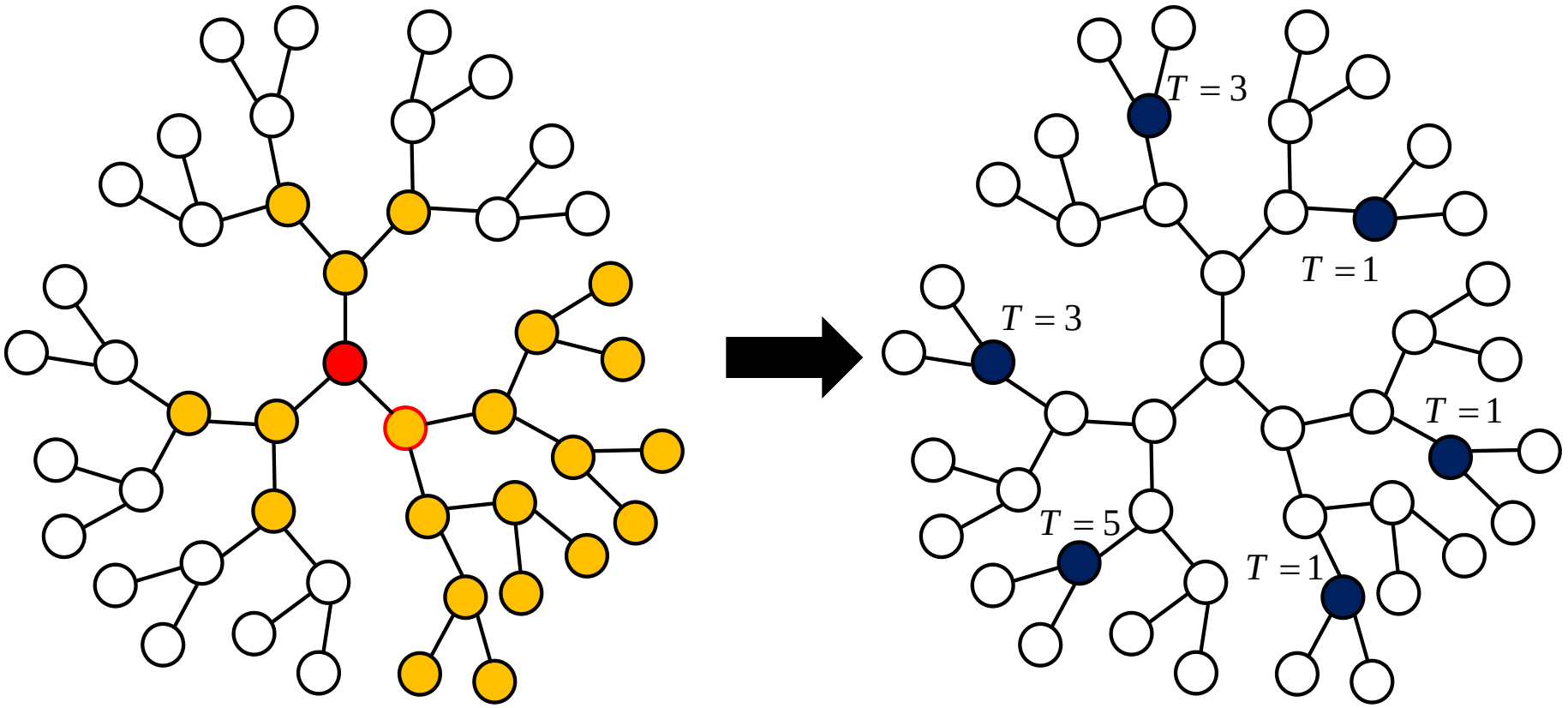
what if spies can collect timing information?

Maximum likelihood detection



Probability of detection $\approx \frac{1}{N}$

Adversary with timing

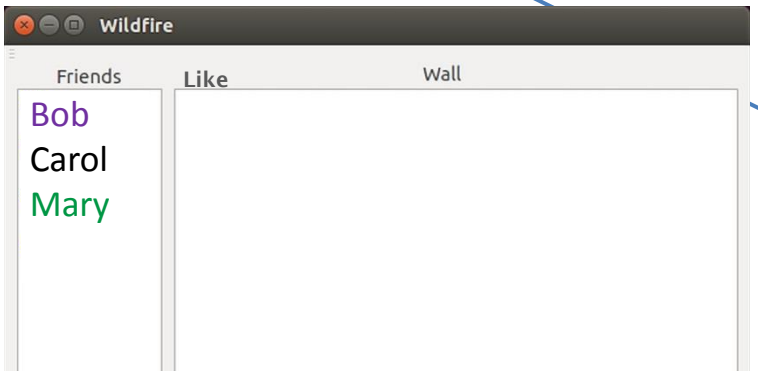


cordon of spy nodes: a work in progress

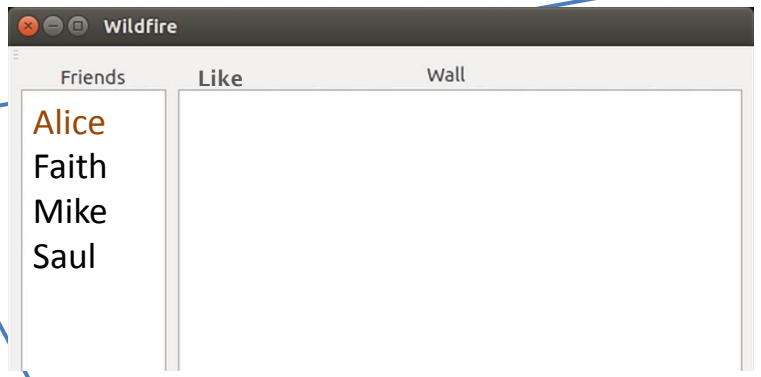
Current progress: Wildfire

Bob

Alice



Mary

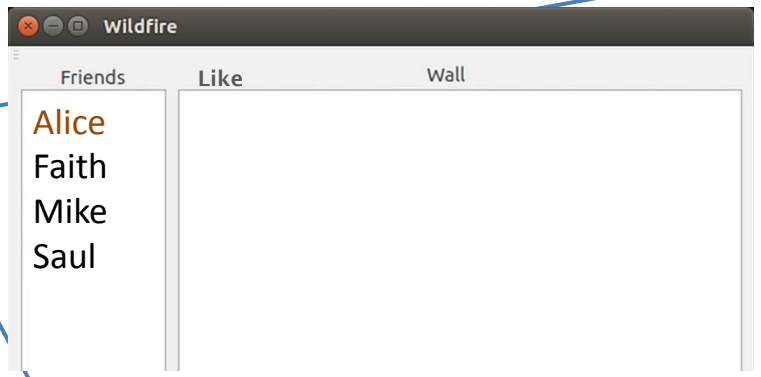


Current progress: Wildfire

Bob

Alice

Mary

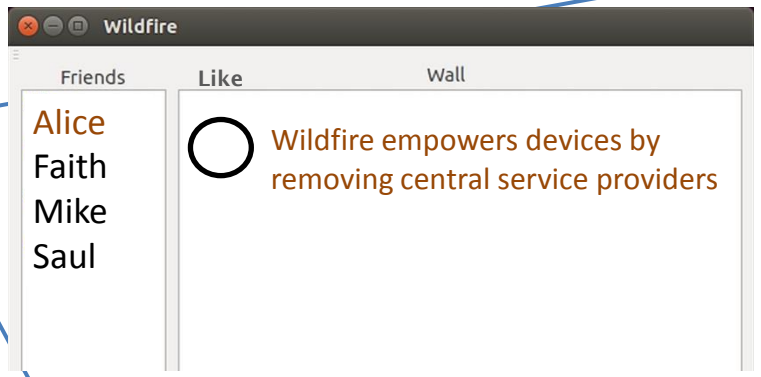


Current progress: Wildfire

Bob

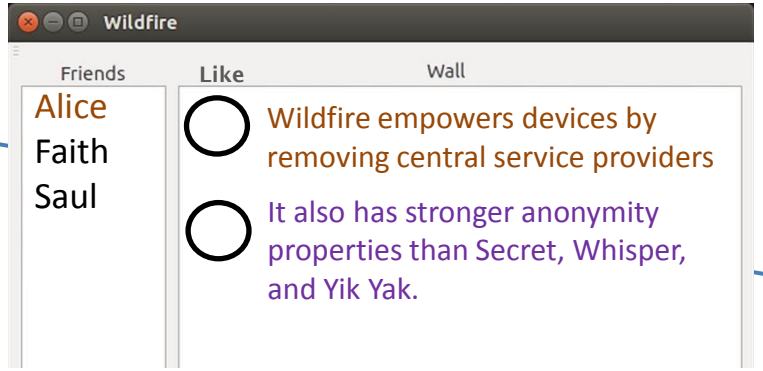
Alice

Mary



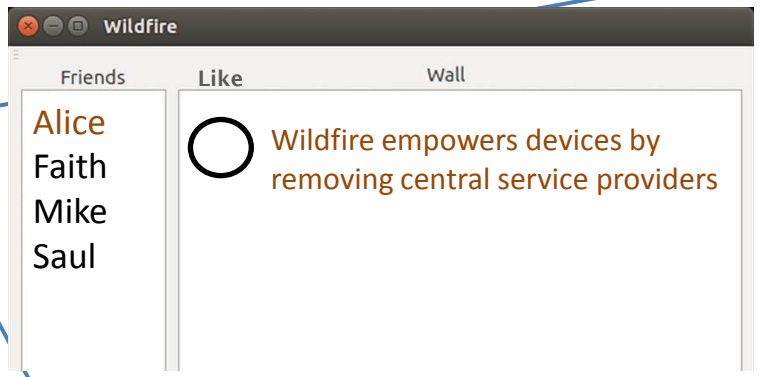
Current progress: Wildfire

Bob



Alice

Mary



Current progress: Wildfire

Bob

Wildfire

Friends
Alice
Faith
Saul

Like

Wall
Wildfire empowers devices by removing central service providers
It also has stronger anonymity properties than Secret, Whisper, and Yik Yak.

Alice

Wildfire

Friends
Bob
Carol
Mary

Like

Wall
Wildfire empowers devices by removing central service providers
It also has stronger anonymity properties than Secret, Whisper, and Yik Yak.

Mary

Wildfire

Friends
Alice
Faith
Mike
Saul

Like

Wall
Wildfire empowers devices by removing central service providers

Current progress: Wildfire

Bob

Wildfire

Friends	Like	Wall
Alice Faith Saul	○	Wildfire empowers devices by removing central service providers
	○	It also has stronger anonymity properties than Secret, Whisper, and Yik Yak.

Alice

Wildfire

Friends	Like	Wall
Bob Carol Mary	○	Wildfire empowers devices by removing central service providers
	👍	It also has stronger anonymity properties than Secret, Whisper, and Yik Yak.

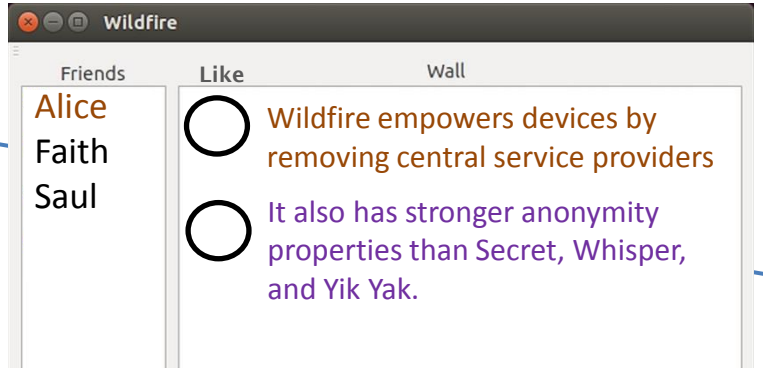
Mary

Wildfire

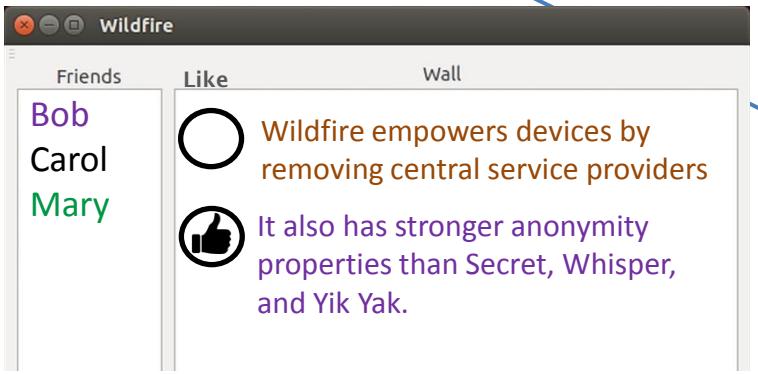
Friends	Like	Wall
Alice Faith Mike Saul	○	Wildfire empowers devices by removing central service providers

Current progress: Wildfire

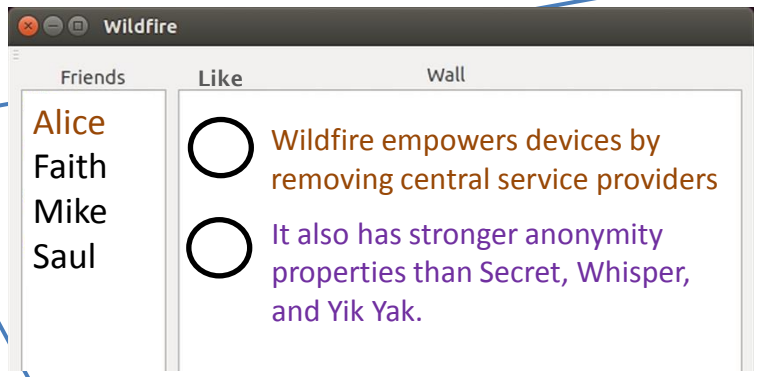
Bob



Alice

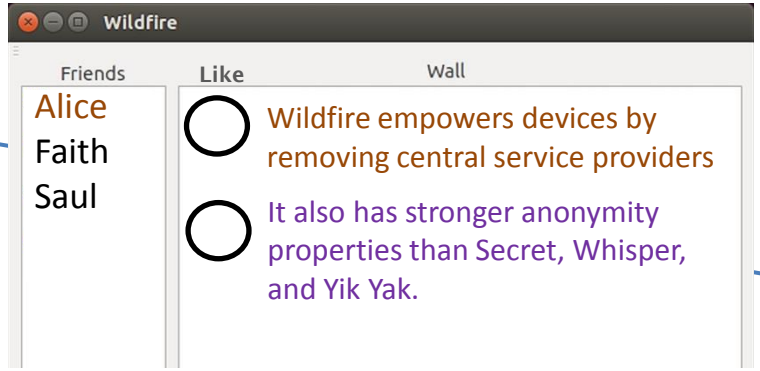


Mary

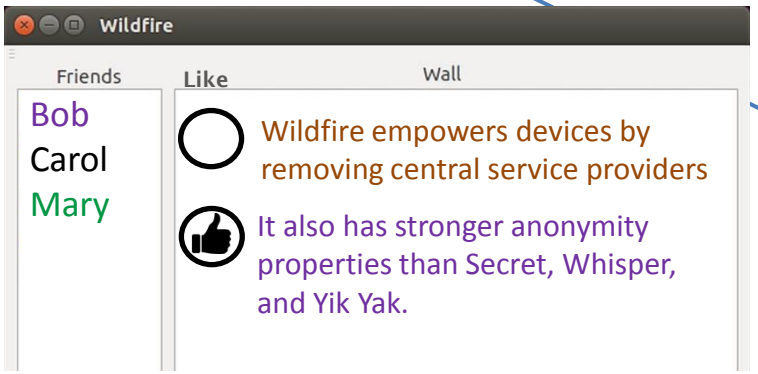


Current progress: Wildfire

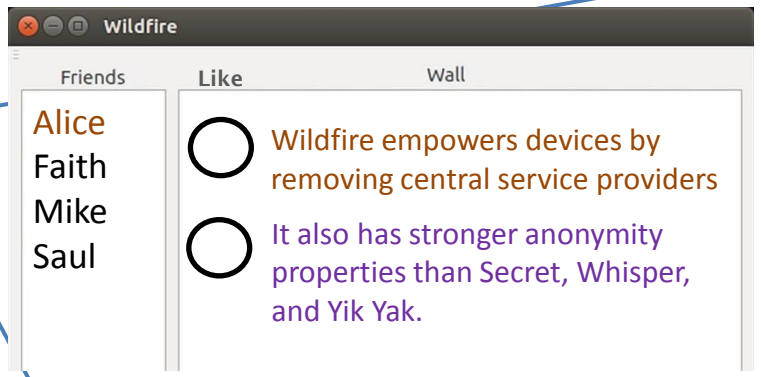
Bob



Alice



Mary



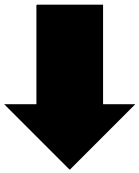
anonymous, distributed, secure implementation

Upcoming research

Theoretical — Systems

- Spy adversarial model
- Hiding relays
- Dynamic networks

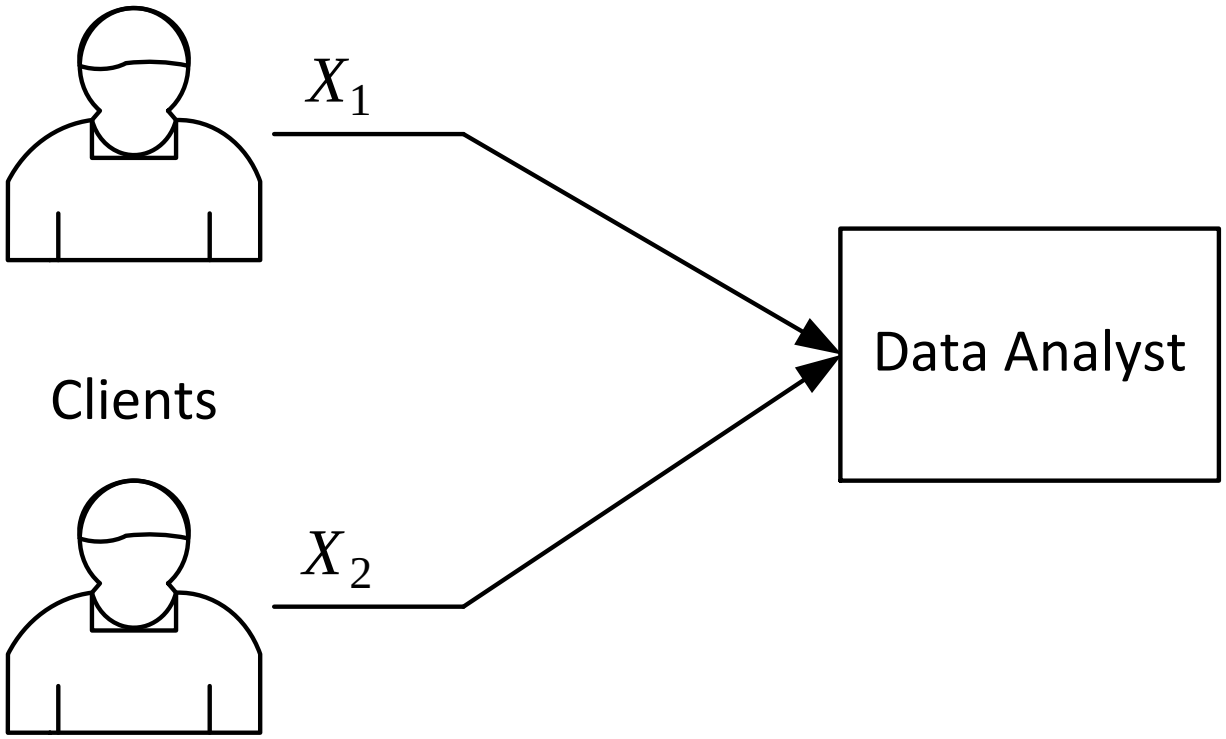
- Video sharing
- Message caching
- Bootstrapping contacts



Wildfire Release

Part II:
Private Communication

Local privacy model



- clients **receive a service** if they share their data
- clients **do not** trust data analyst

Lying is the ultimate protection

"the future of privacy is **lying**"

- **lying** = **randomizing**

Privacy via plausible deniability

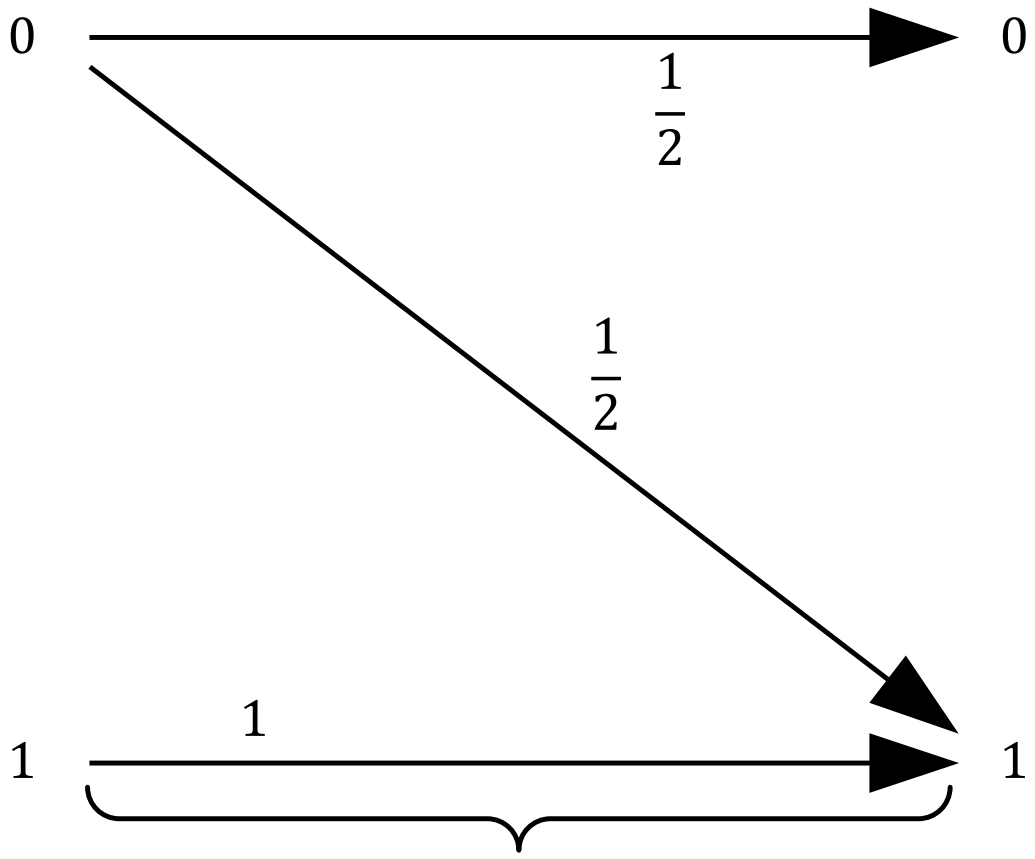
have you ever used illegal drugs?

say yes

answer truthfully

[*Warner* 1965]

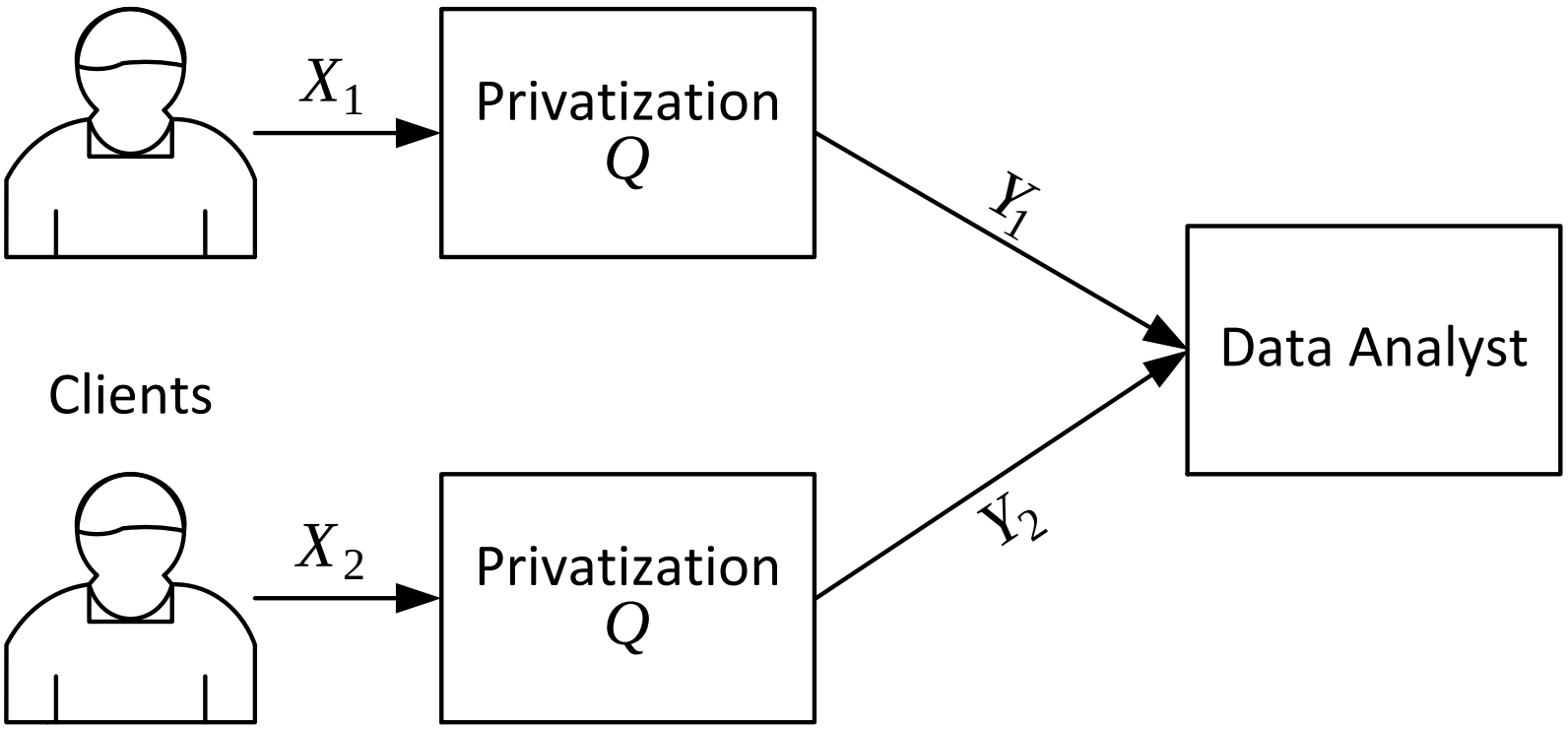
Privacy via plausible deniability



Q: **privatization mechanism**

- instead of $\boldsymbol{X = x}$, share $\boldsymbol{Y = y}$ w.p. $Q(y|x)$
- Q: $|\mathcal{X}| \times |\mathcal{Y}|$ is a stochastic mapping

Local privacy model



- each user **privatizes** her data before releasing it

[*Duchi, et. al.*, 2013]

Local differential privacy

Q is ε-locally differentially private iff **for all $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$**

$$e^{-\varepsilon} \leq \frac{Q(y|x)}{Q(y|x')} \leq e^{\varepsilon}$$

ε controls the level of privacy

large ε, low privacy

small ε, high privacy

- $\mathcal{D}_\varepsilon$: set of all ε-locally differentially private mechanisms

Privacy vs utility

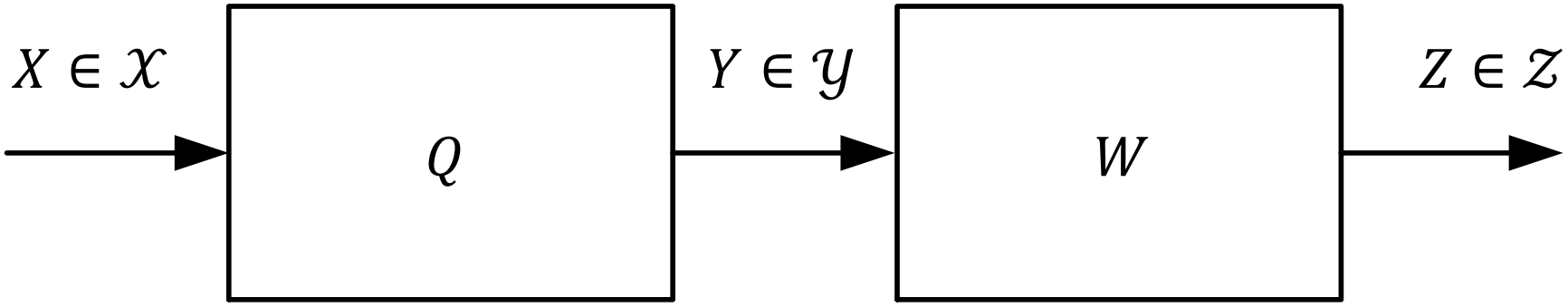
- the **more private** you want to be, the **less utility** you get
- there is a **fundamental trade-off** between **privacy** and **utility**

$$\begin{aligned} \underset{Q}{\text{maximize}} \quad & U(Q) \\ \text{subject to} \quad & Q \in \mathcal{D}_\varepsilon \end{aligned}$$

$U(Q)$: application dependent utility function

$\mathcal{D}_\varepsilon$: set of all ε-locally differentially private mechanisms

Utility functions



utility functions obeying the **data processing inequality**:

$$T = Q \circ W \Longrightarrow U(T) \leq U(Q)$$

- further randomization **can only reduce utility**
- note that if $Q \in \mathcal{D}_\varepsilon \Longrightarrow T \in \mathcal{D}_\varepsilon$

Information theoretic utility functions

- for $|\mathcal{X}| > 2$, we focus on a rich class of **convex utility functions:**

$$\underset{Q}{\text{maximize}} \quad U(Q) = \sum_{y \in \mathcal{Y}} \mu(Q_y)$$

$$\text{subject to} \quad Q \in \mathcal{D}_\varepsilon$$

Q_y: the column of Q corresponding to $Q(y|.)$

μ: any sub-linear function

includes all f-divergences and mutual information

Staircase mechanisms

Q is ε-locally differentially private if **for all $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$**

$$e^{-\varepsilon} \leq \frac{Q(y|x)}{Q(y|x')} \leq e^{\varepsilon}$$

Staircase mechanisms

Q is ε-locally differentially private if **for all $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$**

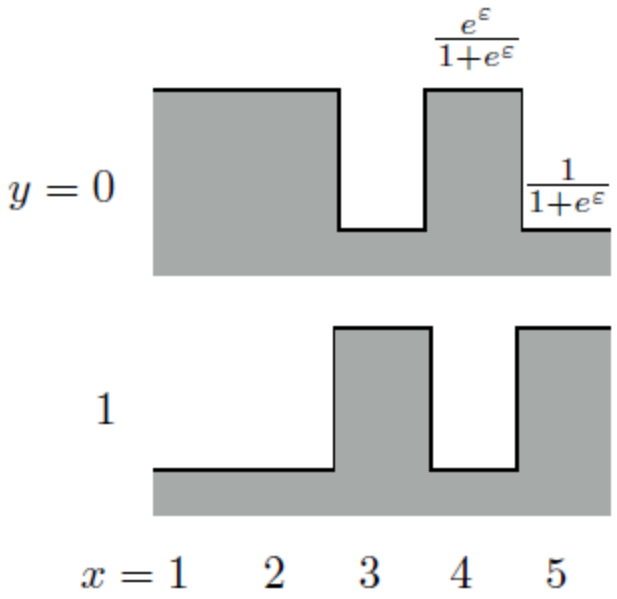
$$e^{-\varepsilon} \leq \frac{Q(y|x)}{Q(y|x')} \leq e^{\varepsilon}$$

Q is a staircase mechanism if **for all $x, x' \in \mathcal{X}$ and $y \in \mathcal{Y}$**

$$\frac{Q(y|x)}{Q(y|x')} \in \{e^{-\varepsilon}, 1, e^{\varepsilon}\}$$

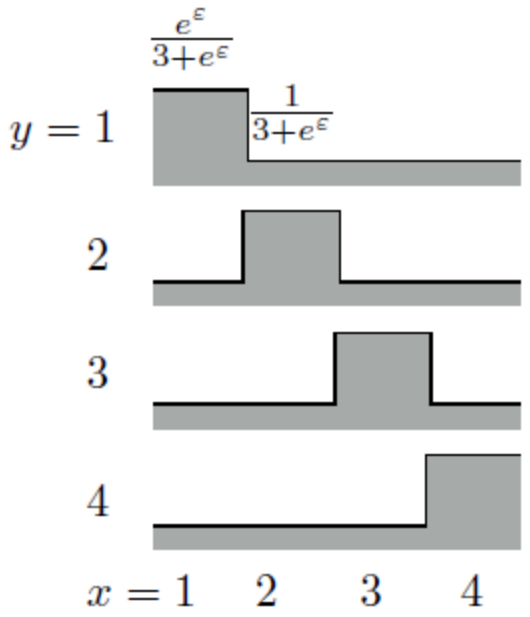
Example of staircase mechanisms

$$Q^T = \frac{1}{1+e^\varepsilon}\begin{bmatrix} e^\varepsilon & e^\varepsilon & 1 & e^\varepsilon & 1 \\ 1 & 1 & e^\varepsilon & 1 & e^\varepsilon \end{bmatrix}$$



Binary Mechanism

$$Q^T = \frac{1}{3+e^\varepsilon}\begin{bmatrix} e^\varepsilon & 1 & 1 & 1 \\ 1 & e^\varepsilon & 1 & 1 \\ 1 & 1 & e^\varepsilon & 1 \\ 1 & 1 & 1 & e^\varepsilon \end{bmatrix}$$



Randomized Response

Main result: binary data

for $|\mathcal{X}| = 2$, binary data:

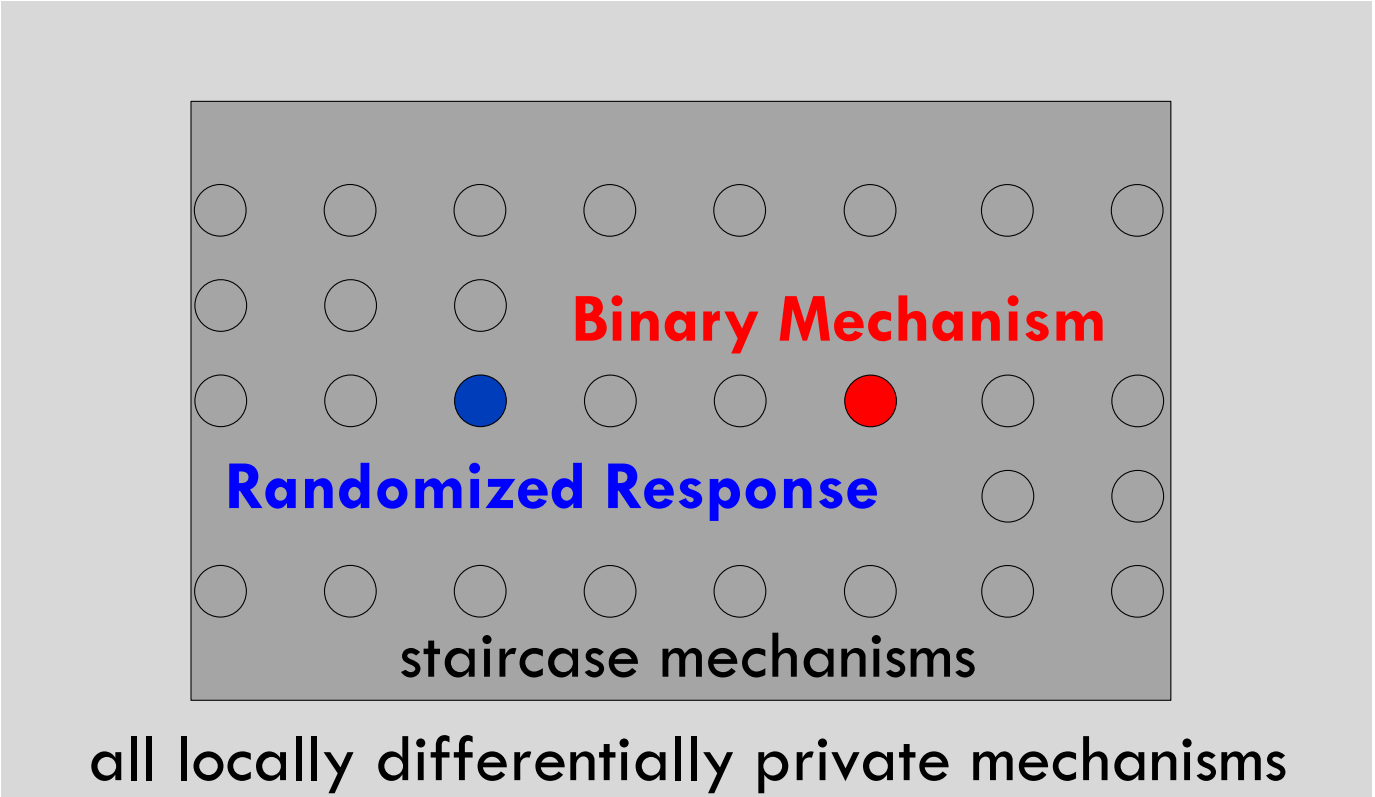
w.p. $\frac{1}{1+e^{\varepsilon}}$ lie

w.p. $\frac{e^{\varepsilon}}{1+e^{\varepsilon}}$ say the truth

- optimal for **all ε**
- optimal for **all $U(Q)$ obeying the data processing inequality**

Main result: general case

for $|\mathcal{X}| > 2$, general data:



- staircase mechanisms are optimal for **all ε**
- **BM optimal for small ε**
- **RR optimal for large ε**

Acknowledgments

Giulia Fanti

Pramod Viswanath

Sewoong Oh

Thank You!