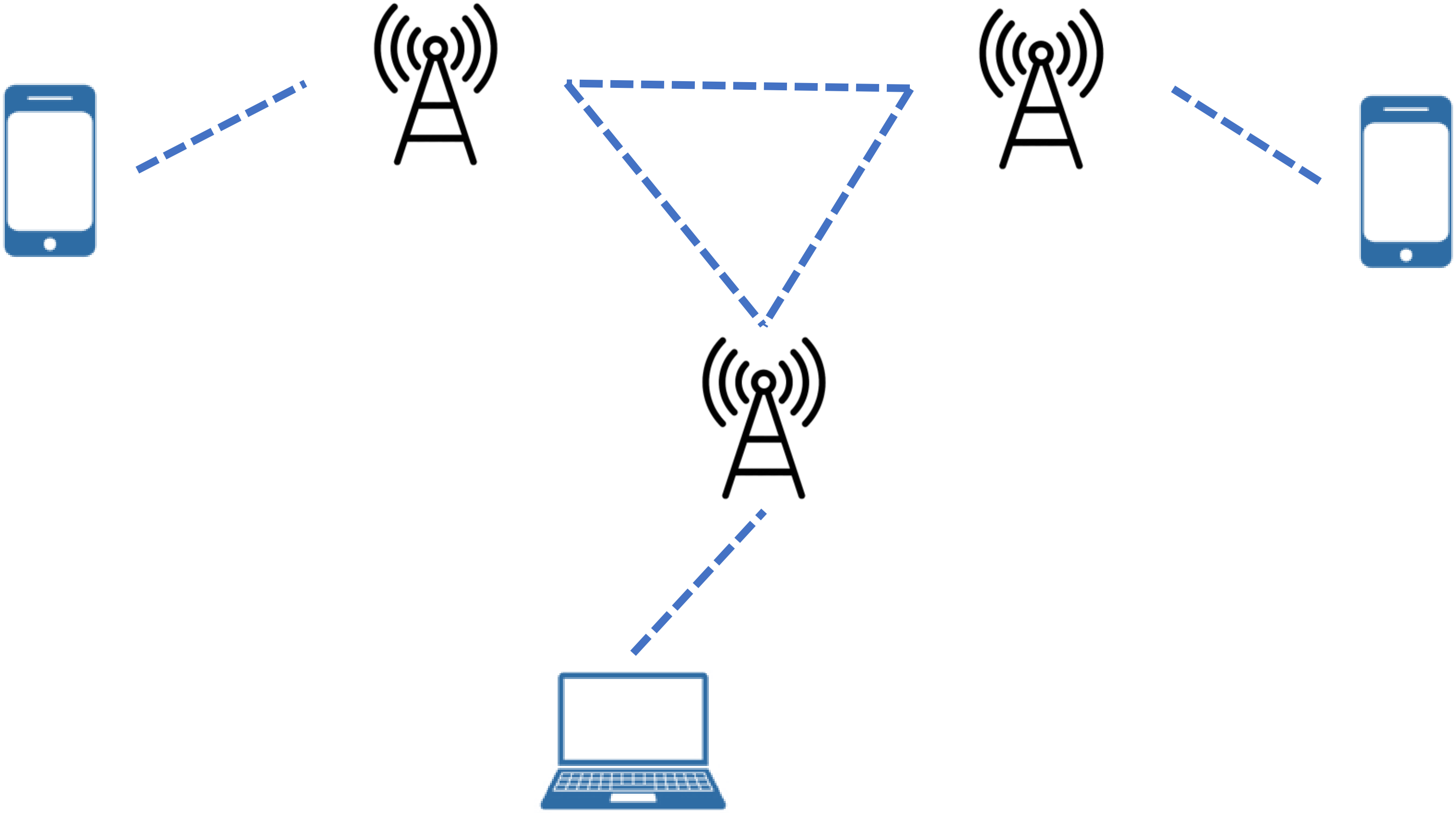
Mirage: Private Mobility-based Routing for Censorship Evasion

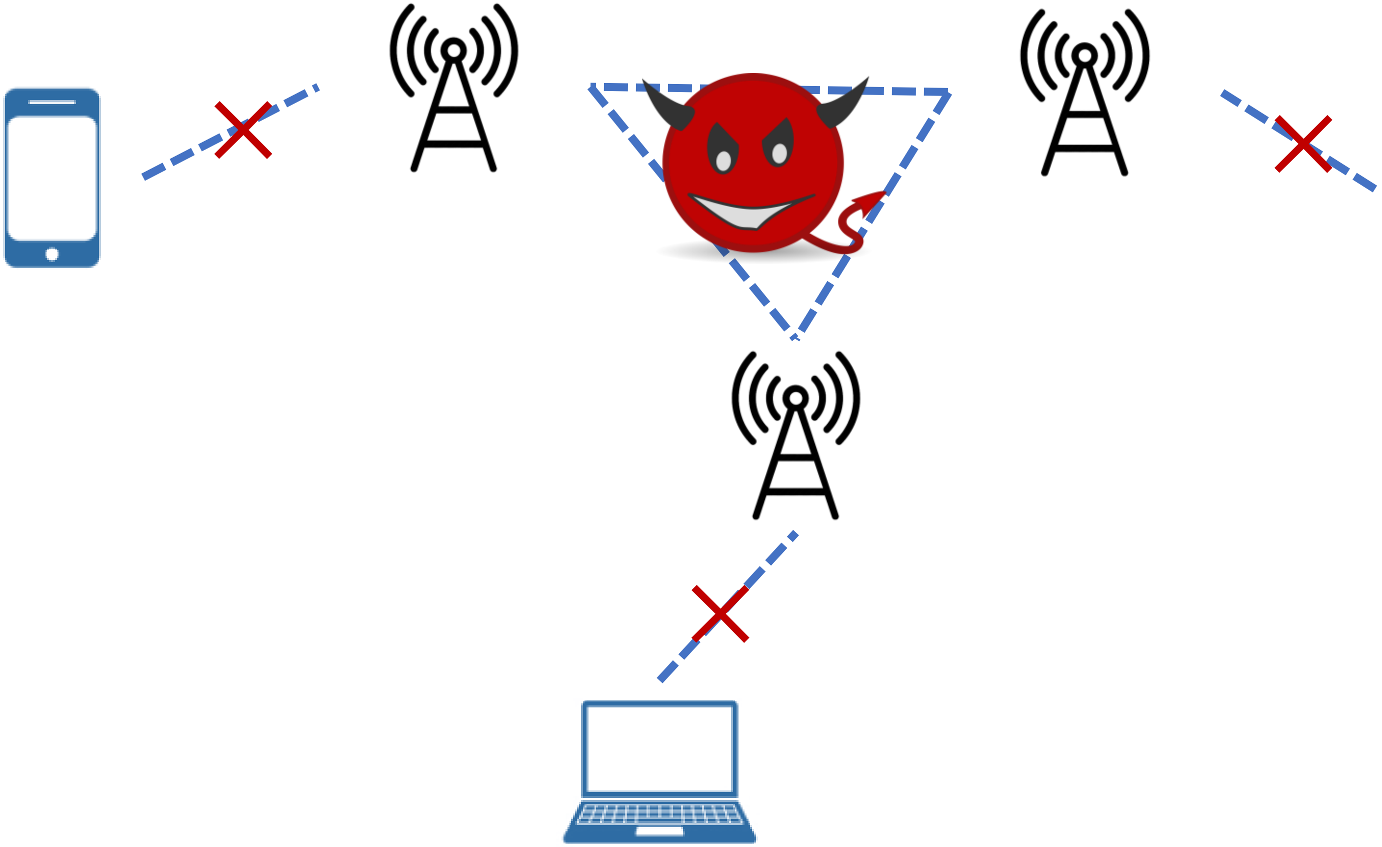
Zachary Ratliff[1] Ruoxing (David) Yang[2] Avery Bai[2]
Harel Berger[2,3] Micah Sherr[2] James Mickens[3]

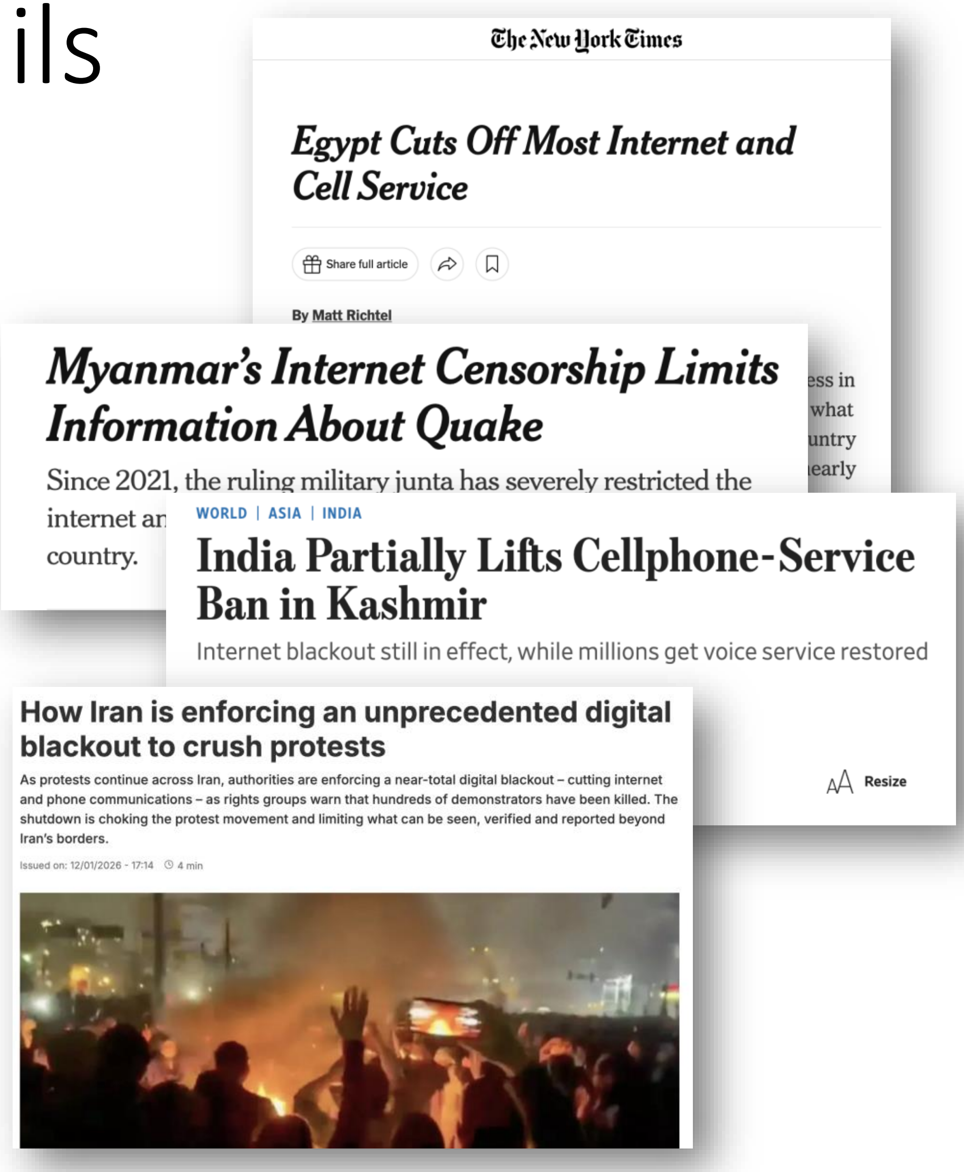
[1]Harvard University *[2]Georgetown University* *[3]Ariel University*

Motivation: When Internet Fails



Motivation: When Internet Fails





The New York Times

Egypt Cuts Off Most Internet and Cell Service

By Matt Richtel

ess in
what
untry
early

Myanmar's Internet Censorship Limits Information About Quake

Since 2021, the ruling military junta has severely restricted the internet an
country.

WORLD | ASIA | INDIA

India Partially Lifts Cellphone-Service Ban in Kashmir

Internet blackout still in effect, while millions get voice service restored

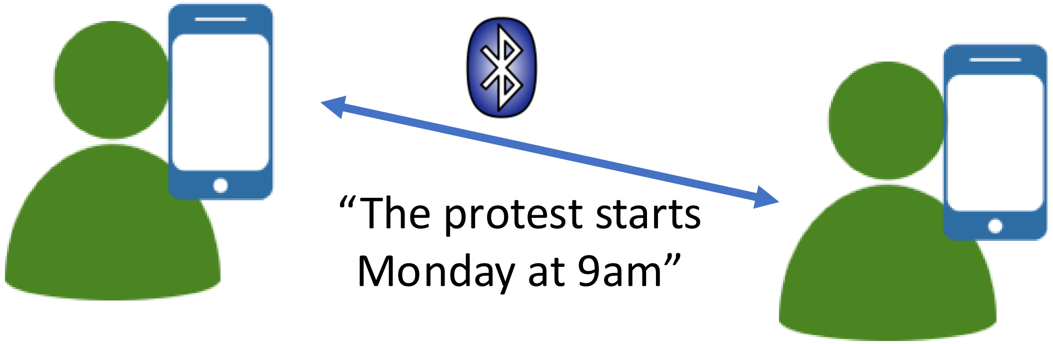
How Iran is enforcing an unprecedented digital blackout to crush protests

As protests continue across Iran, authorities are enforcing a near-total digital blackout – cutting internet and phone communications – as rights groups warn that hundreds of demonstrators have been killed. The shutdown is choking the protest movement and limiting what can be seen, verified and reported beyond Iran's borders.

Issued on: 12/01/2026 - 17:14 ⏱ 4 min

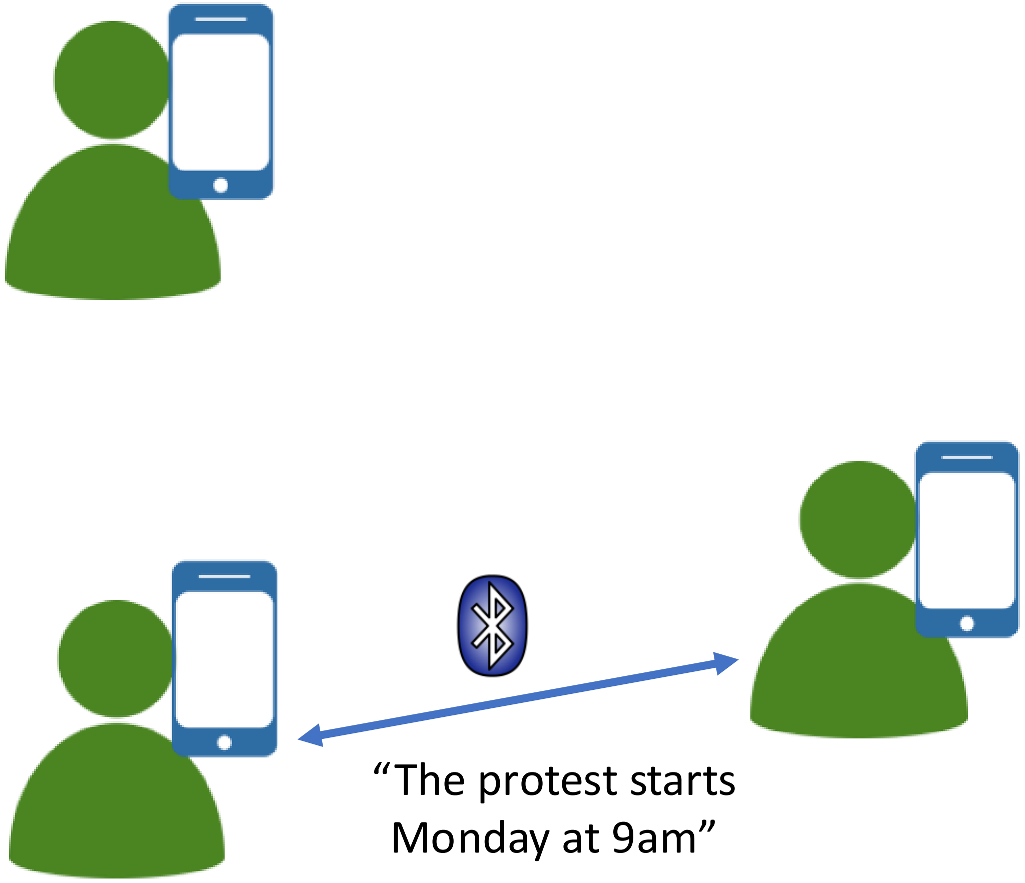
Mobile Ad Hoc Networks

Mobile Ad Hoc Networks



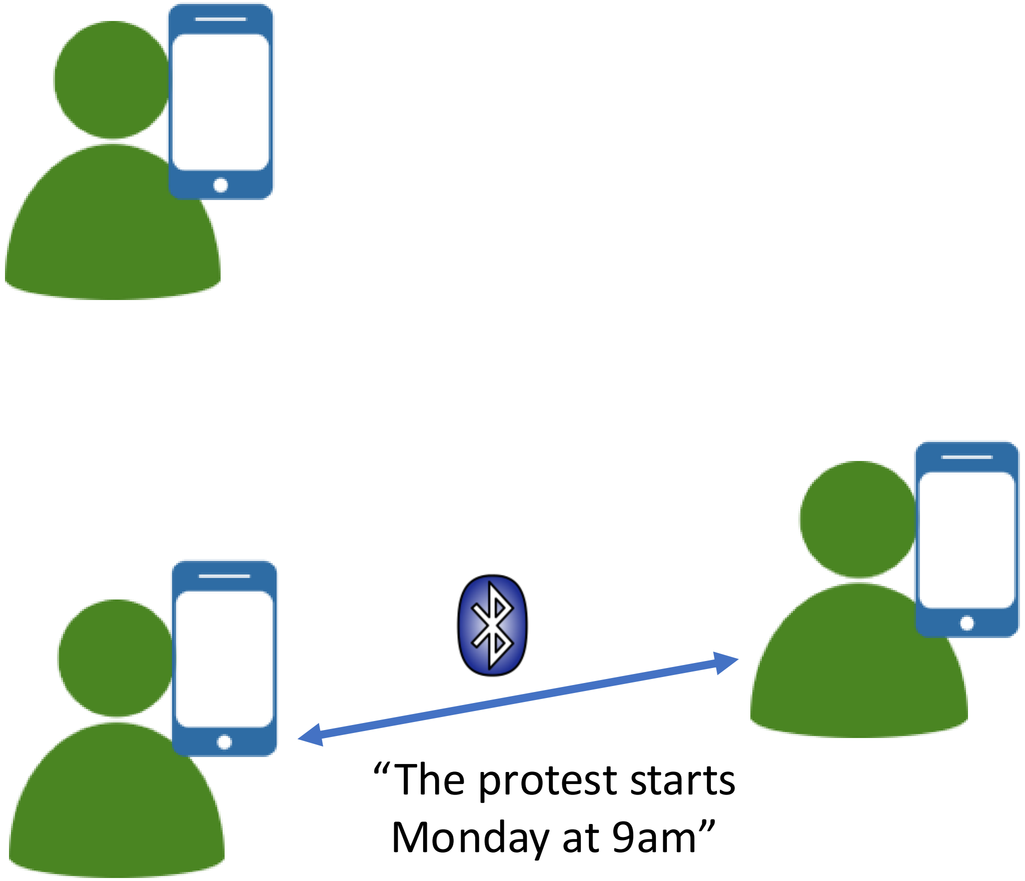
- Messages transfer upon physical encounter (e.g., over Bluetooth LE or WiFi direct)

Mobile Ad Hoc Networks



- Messages transfer upon physical encounter (e.g., over Bluetooth LE or WiFi direct)
- No centralized routers or ISP

Mobile Ad Hoc Networks

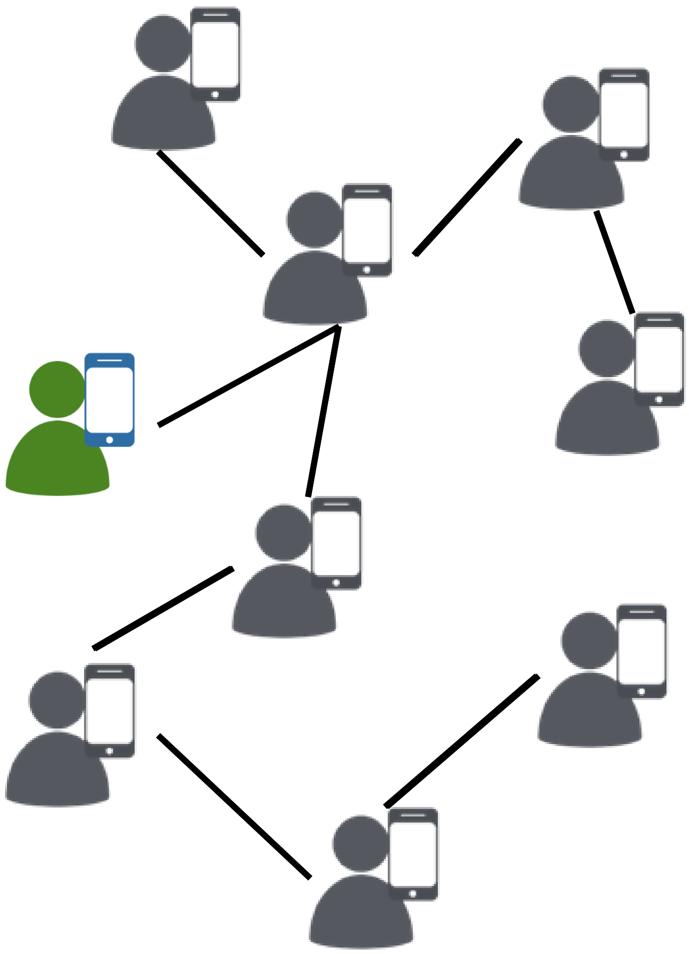


“The protest starts Monday at 9am”

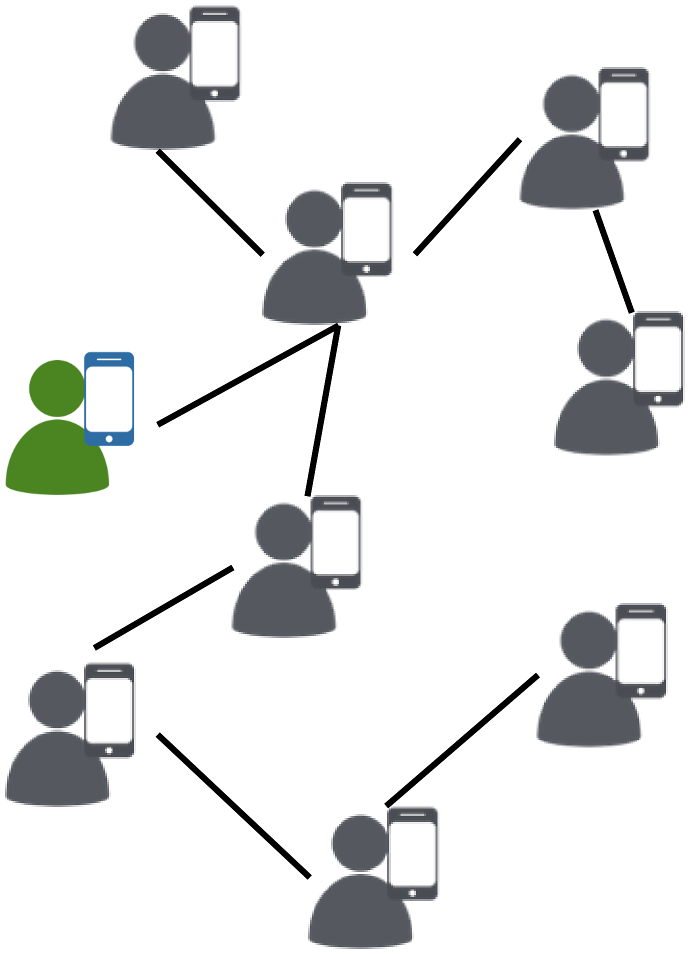
- Messages transfer upon physical encounter (e.g., over Bluetooth LE or WiFi direct)
- No centralized routers or ISP
- **Messages move where people move**

Flooding and Random Walks

Flooding

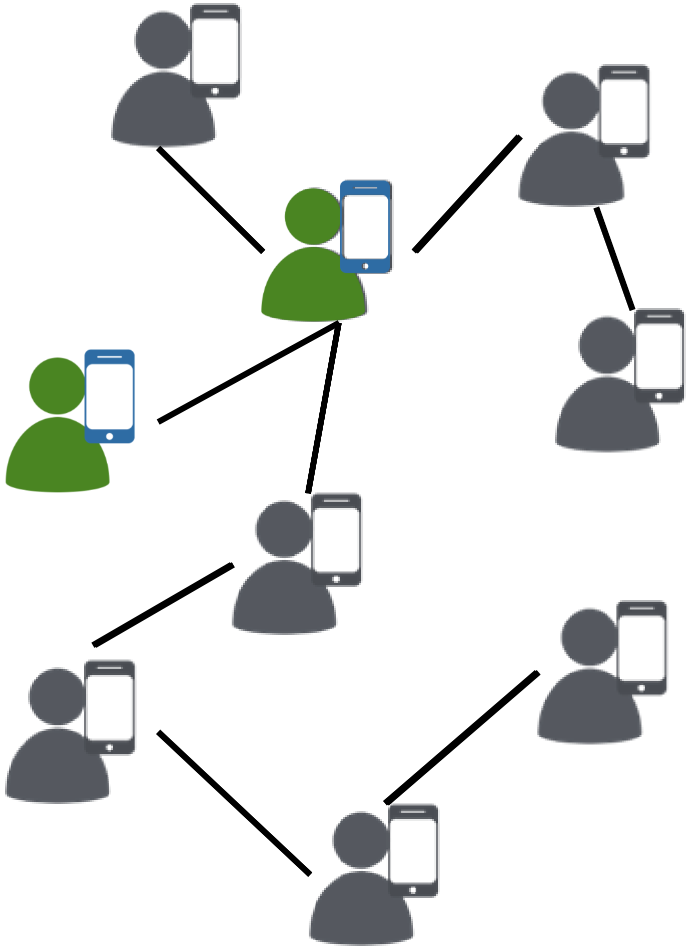


Random Walk

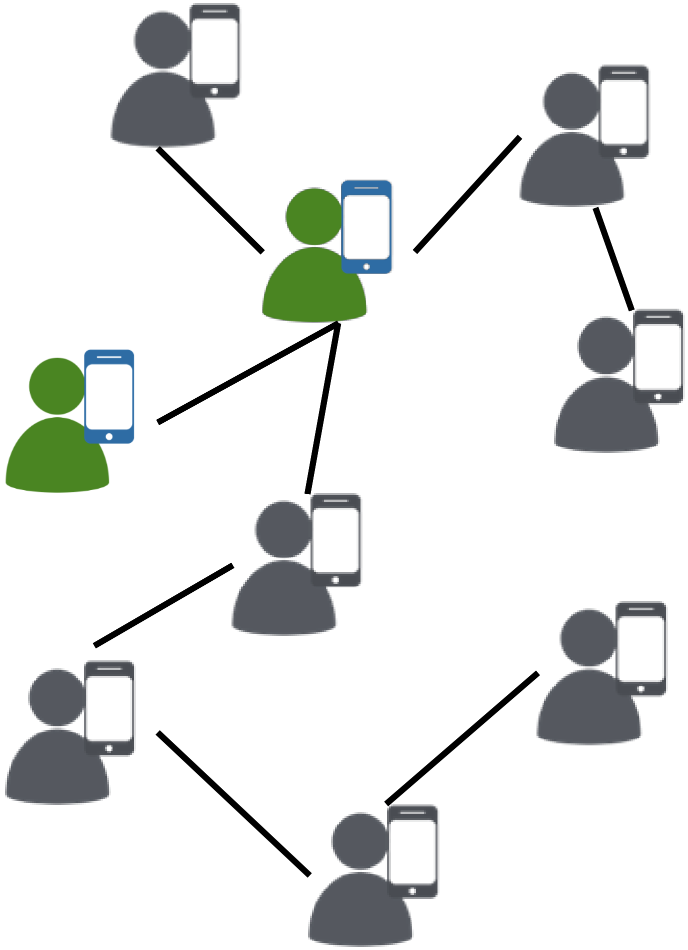


Flooding and Random Walks

Flooding

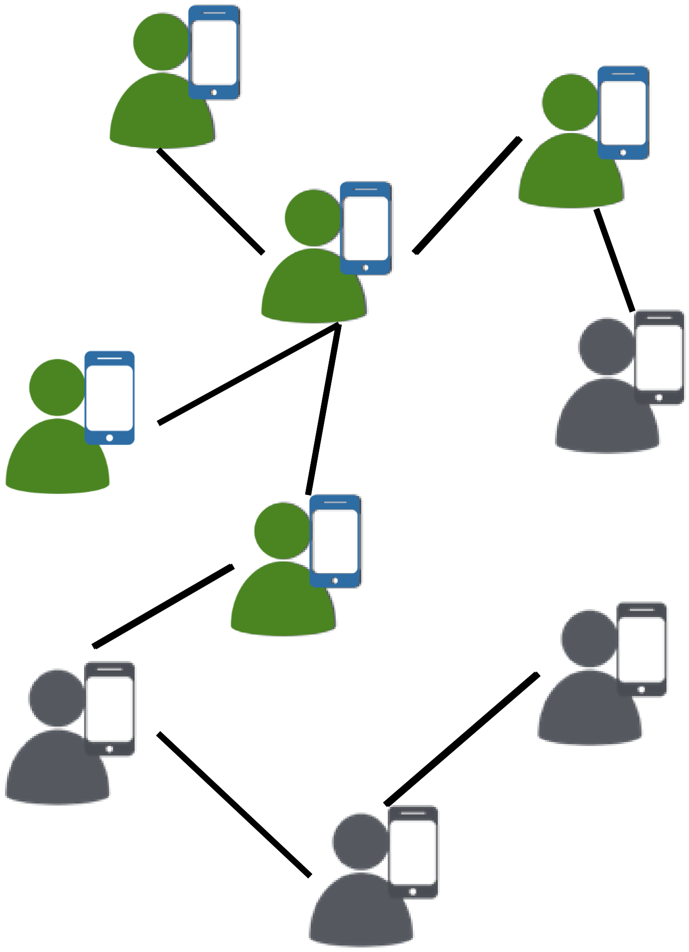


Random Walk

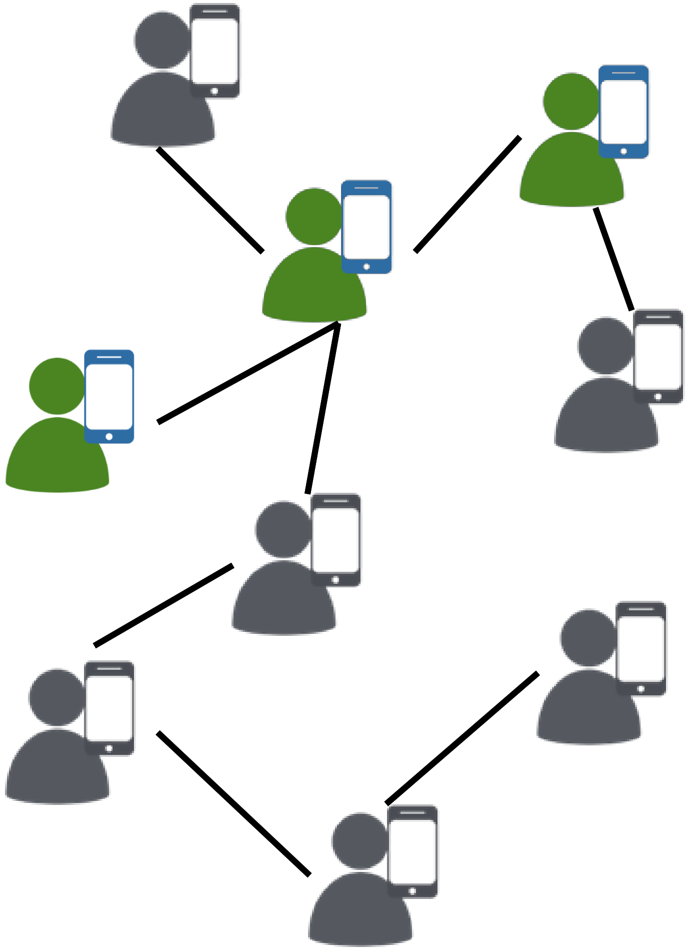


Flooding and Random Walks

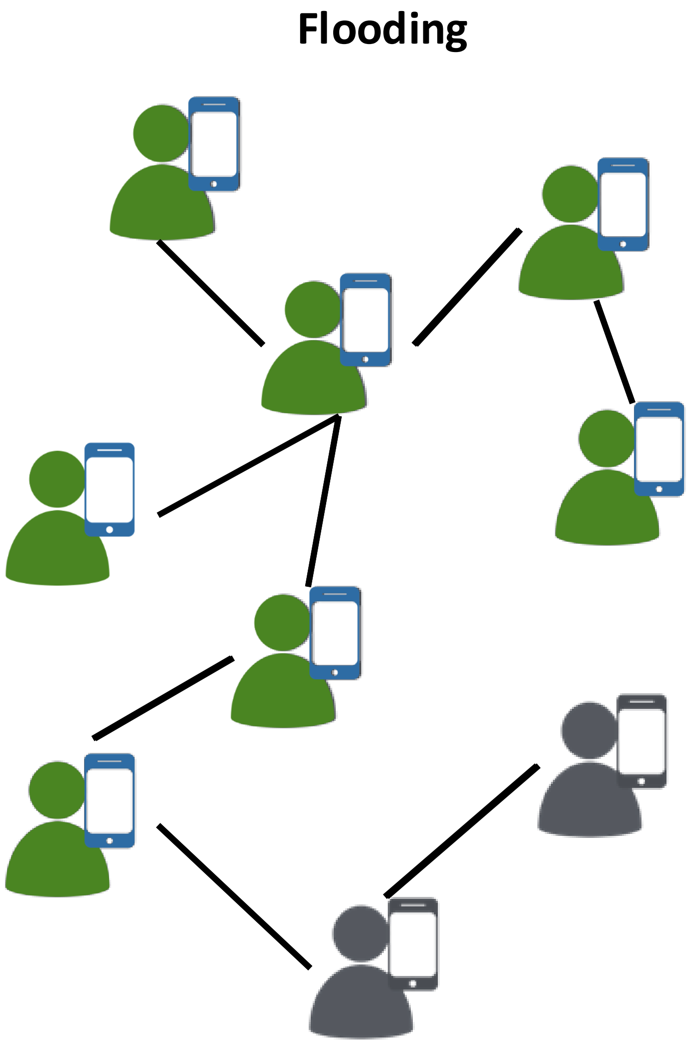
Flooding

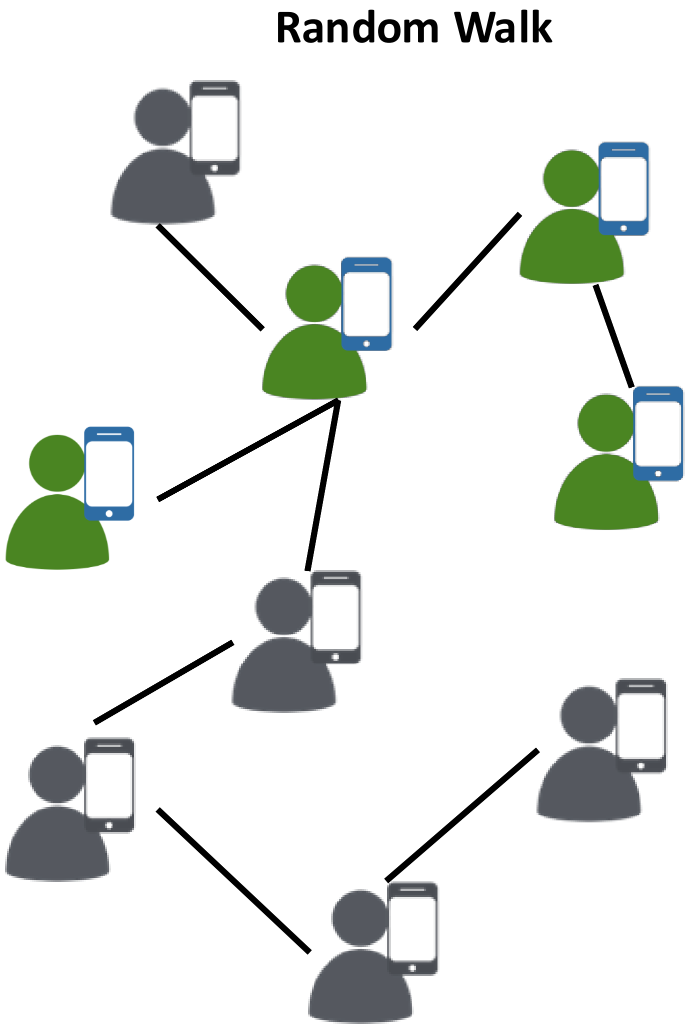


Random Walk

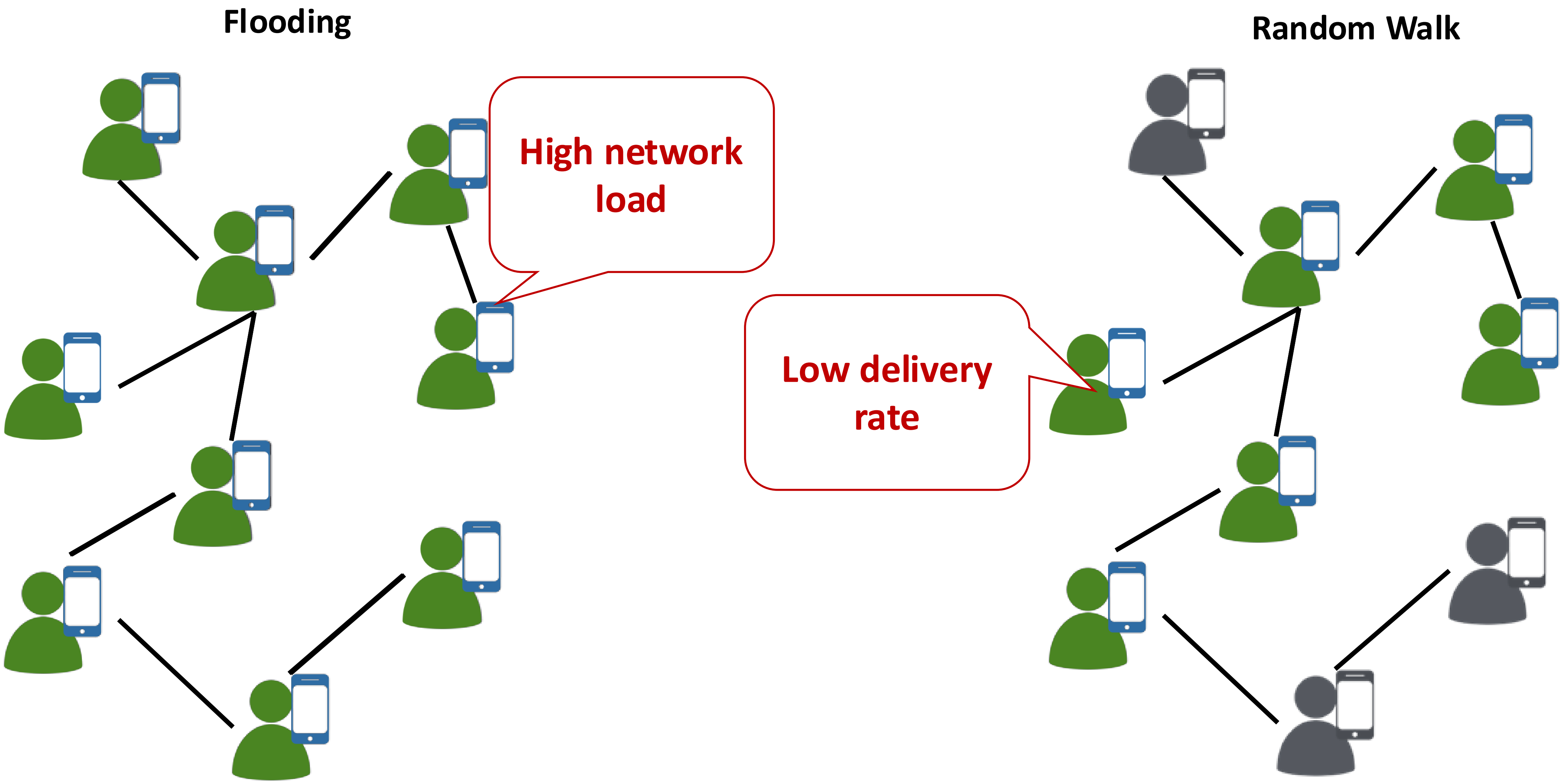


Flooding and Random Walks





Flooding and Random Walks



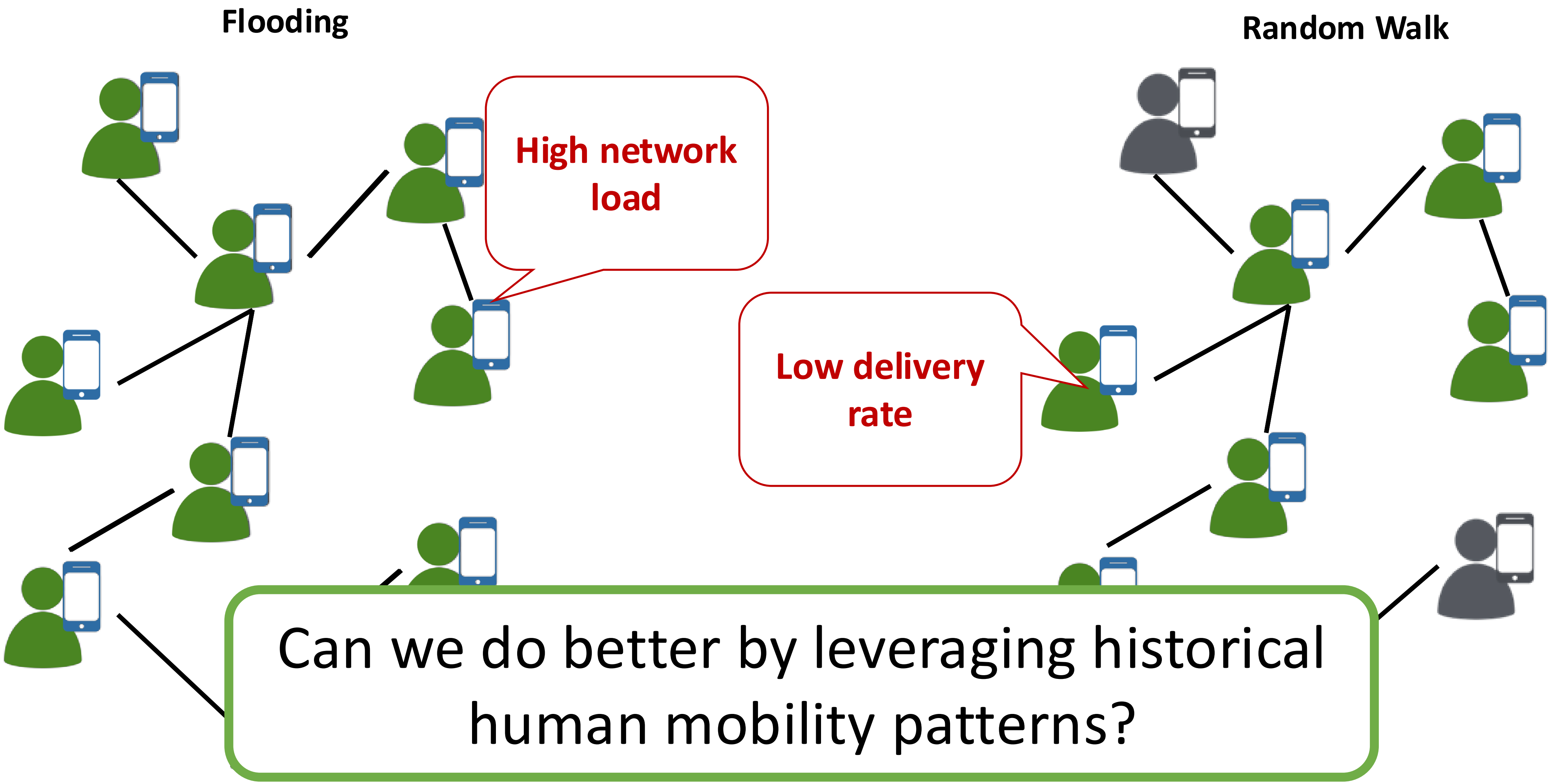
Flooding

Random Walk

High network load

Low delivery rate

Flooding and Random Walks



Flooding

Random Walk

High network load

Low delivery rate

Can we do better by leveraging historical human mobility patterns?

HumaNets

(Aviv, Sherr, Blaze, and Smith, 2010)

- Mobility-aware routing that leverages predictable movement patterns
- Messages are addressed to **districts**

Harvard Square

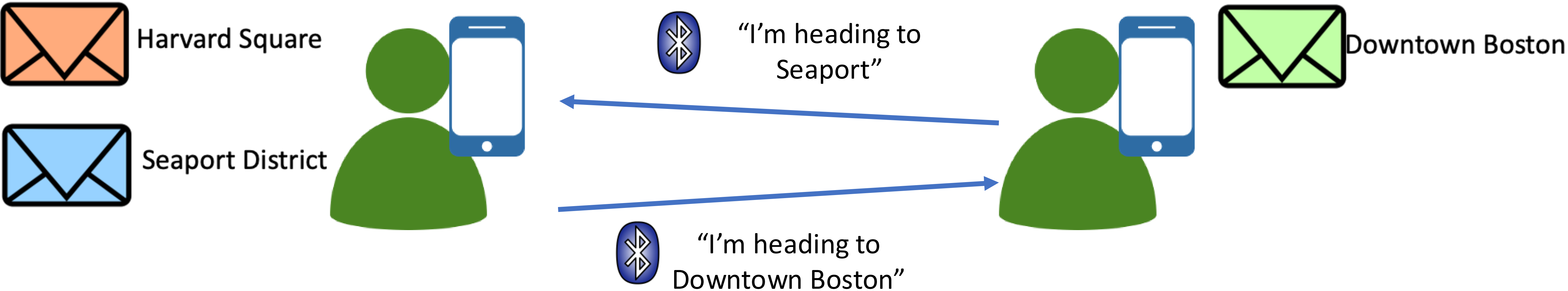
Seaport District

Downtown Boston

HumaNets

(Aviv, Sherr, Blaze, and Smith, 2010)

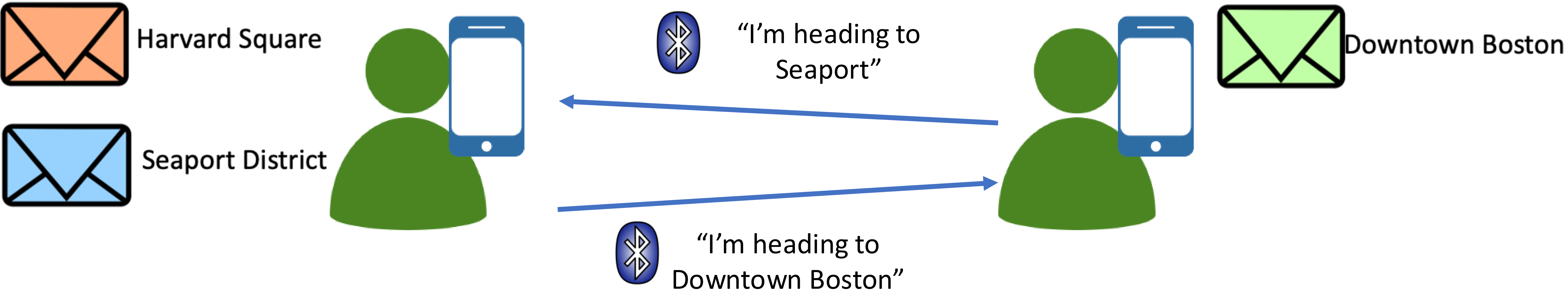
- Mobility-aware routing that leverages predictable movement patterns
- Messages are addressed to **districts**



HumaNets

(Aviv, Sherr, Blaze, and Smith, 2010)

- Mobility-aware routing that leverages predictable movement patterns
- Messages are addressed to **districts**



Routing leaks mobility information ☹

This Work: Private HumaNets

- We show that **existing privacy-preserving HumaNet protocols are vulnerable to statistical disclosure attacks**
    - Even when participants do not directly share mobility information, **routing decisions implicitly leak sensitive movement patterns**

This Work: Private HumaNets

- We show that **existing privacy-preserving HumaNet protocols are vulnerable to statistical disclosure attacks**
  - Even when participants do not directly share mobility information, **routing decisions implicitly leak sensitive movement patterns**

- We develop **Mirage: a private mobility-based routing protocol**
  - Provides **formal privacy guarantees**
  - Achieves **comparable efficiency to prior (non-private) HumaNet protocols**
  - **Evaluated on real-world city-scale mobility data**

Probabilistic Profile-based Routing (PPBR)

(Aviv, Blaze, Sherr, and Smith, 2014)

Districts

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

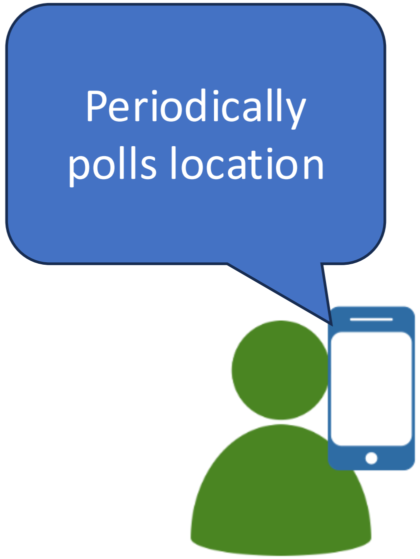
Periodically polls location

Probabilistic Profile-based Routing (PPBR)

(Aviv, Blaze, Sherr, and Smith, 2014)

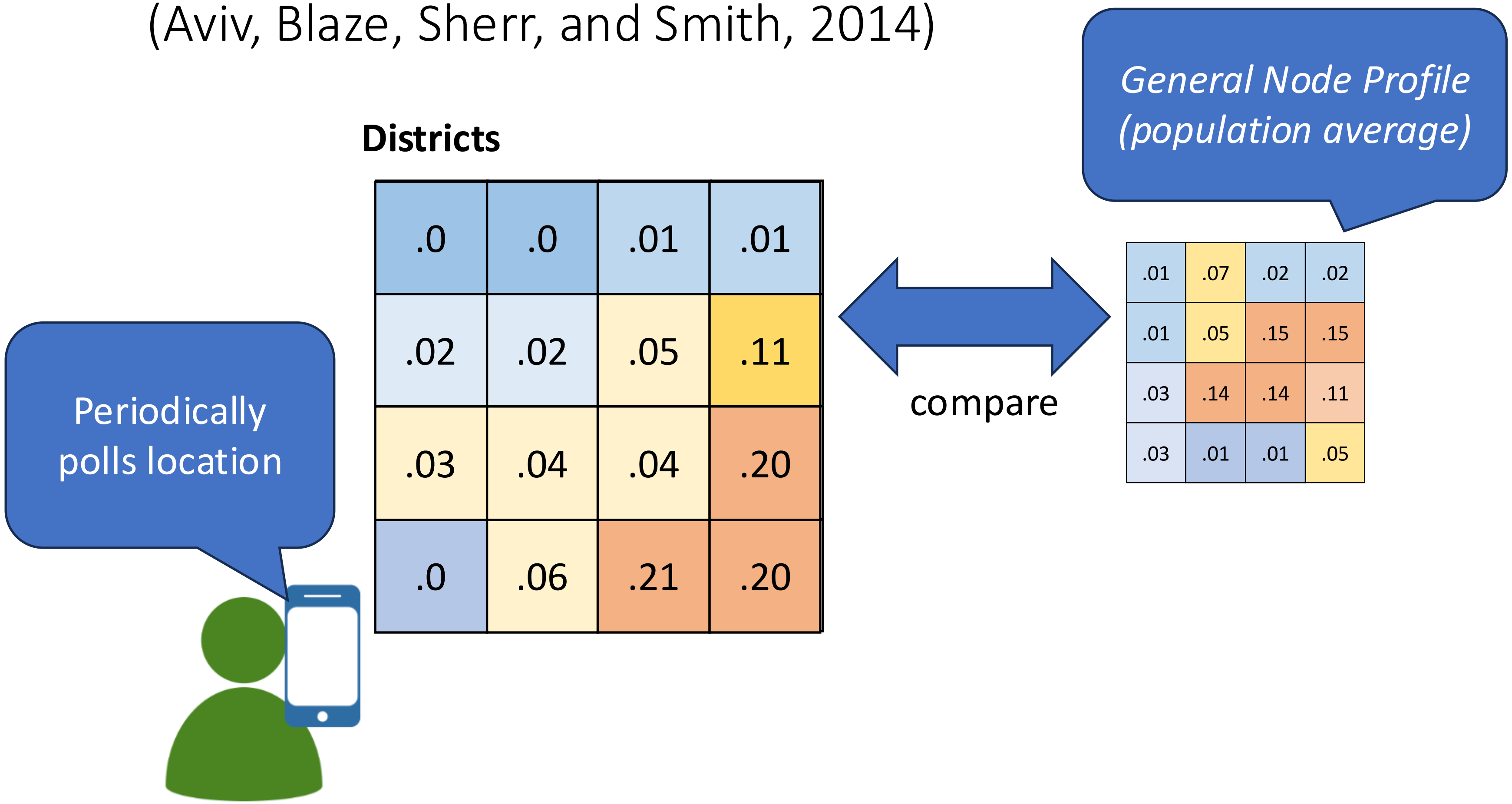
Districts

.0	.0	.01	.01
.02	.02	.05	.11
.03	.04	.04	.20
.0	.06	.21	.20



Probabilistic Profile-based Routing (PPBR)

(Aviv, Blaze, Sherr, and Smith, 2014)



Periodically polls location

Districts

.0	.0	.01	.01
.02	.02	.05	.11
.03	.04	.04	.20
.0	.06	.21	.20

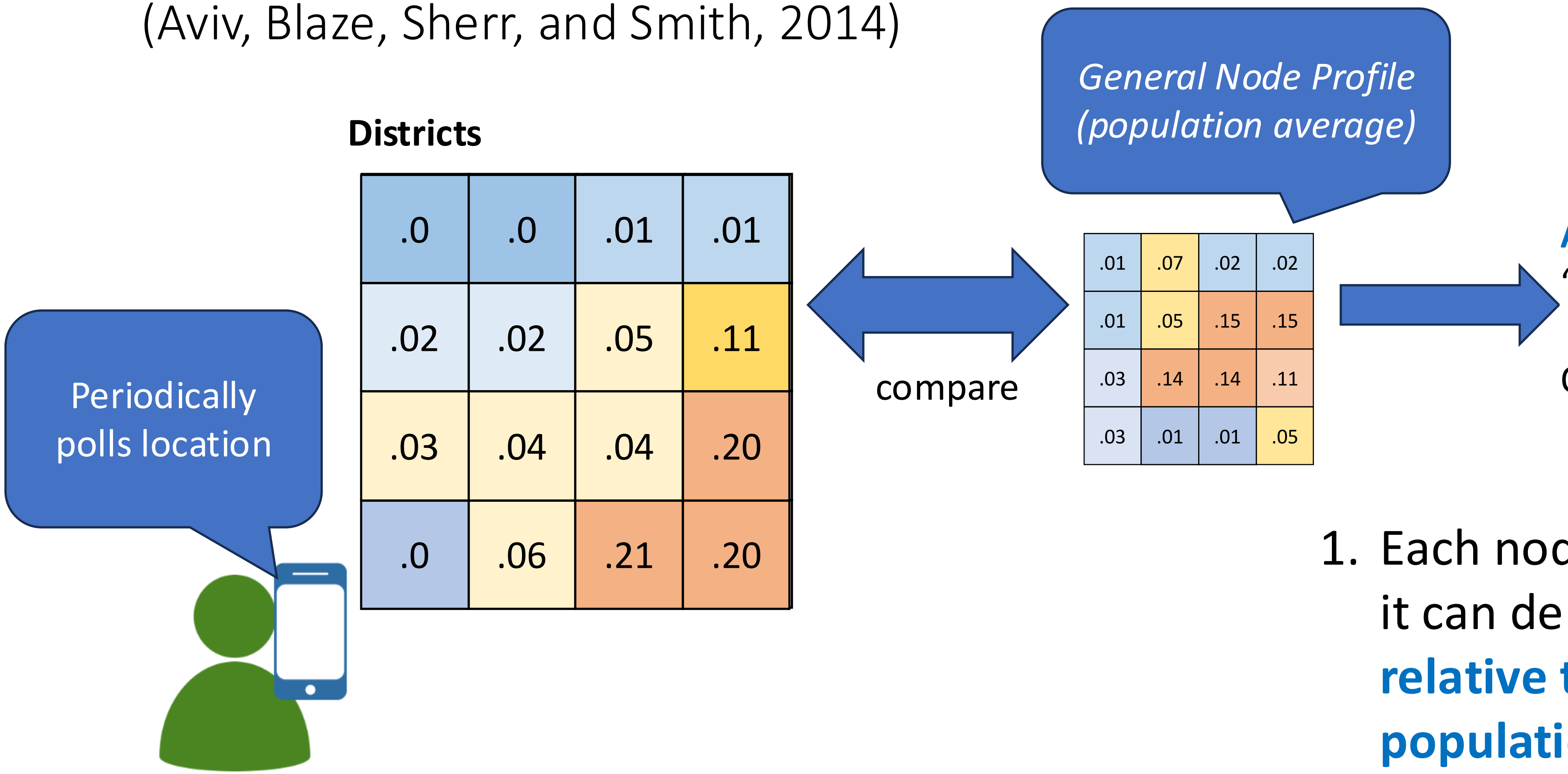
compare

General Node Profile (population average)

.01	.07	.02	.02
.01	.05	.15	.15
.03	.14	.14	.11
.03	.01	.01	.05

Probabilistic Profile-based Routing (PPBR)

(Aviv, Blaze, Sherr, and Smith, 2014)



Periodically polls location

Districts

.0	.0	.01	.01
.02	.02	.05	.11
.03	.04	.04	.20
.0	.06	.21	.20

compare

General Node Profile (population average)

.01	.07	.02	.02
.01	.05	.15	.15
.03	.14	.14	.11
.03	.01	.01	.05

Accept messages for:
"*Downtown Boston, Seaport*"

Otherwise **drop**

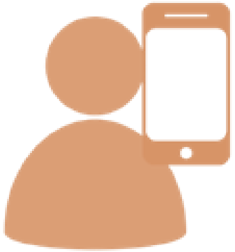
1. Each node computes how well it can deliver a message **relative to the general population**
2. **Silently accept** messages only its **top-K destinations**

Statistical Disclosure Attacks Against PPBR

Districts

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

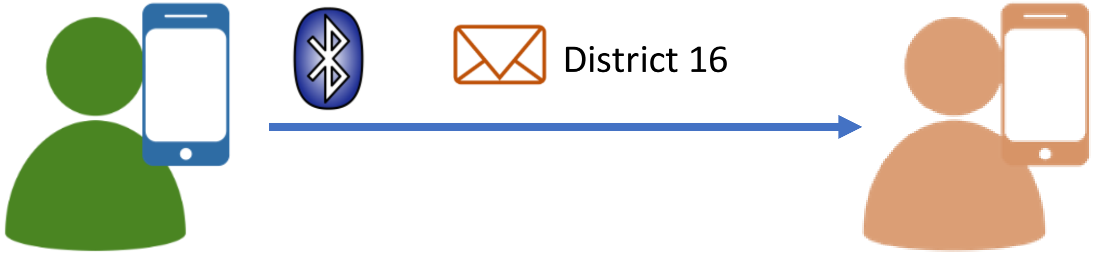
District 16



Statistical Disclosure Attacks Against PPBR

Districts

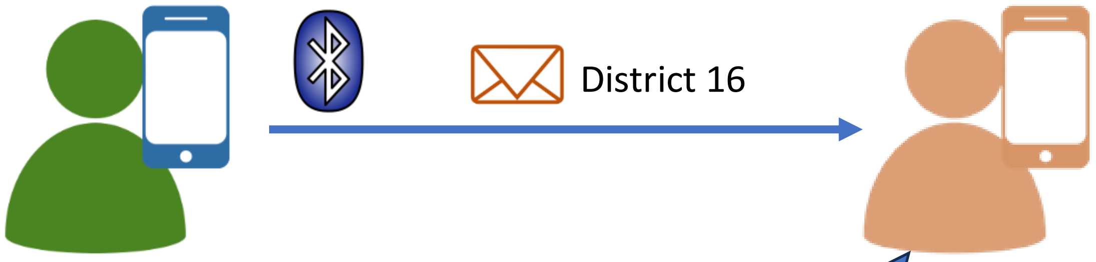
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16



Statistical Disclosure Attacks Against PPBR

Districts

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16



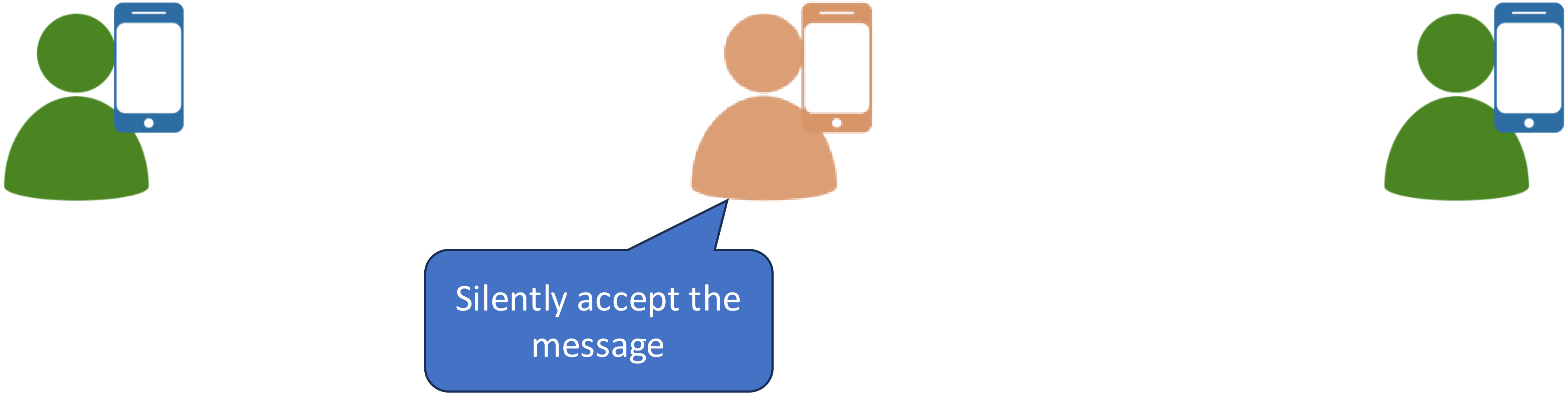
District 16

Silently accept the message

Statistical Disclosure Attacks Against PPBR

Districts

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

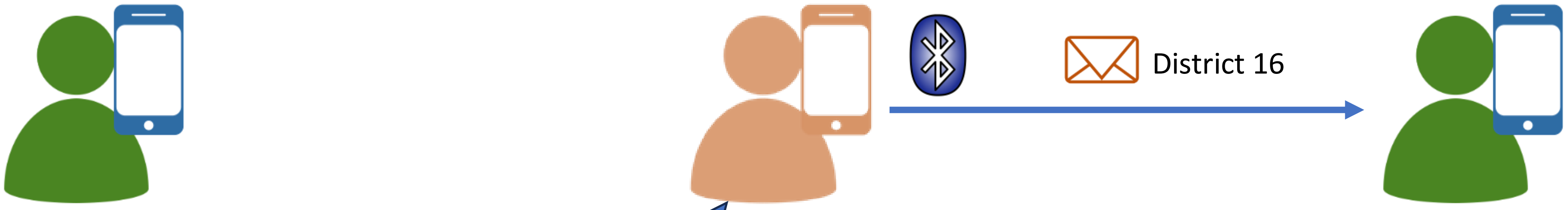


Silently accept the message

Statistical Disclosure Attacks Against PPBR

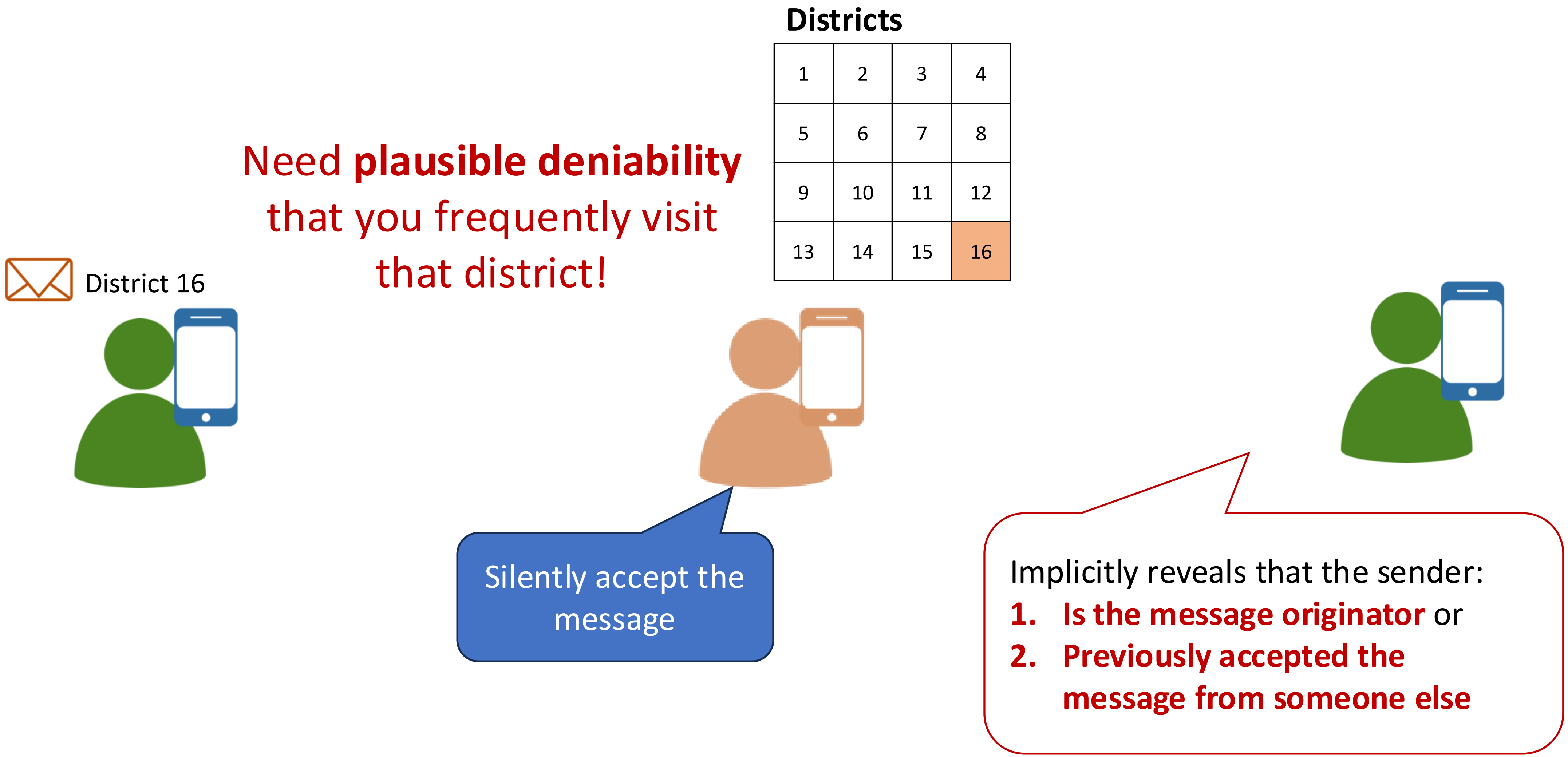
Districts

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16



Silently accept the message

Statistical Disclosure Attacks Against PPBR



Districts

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

District 16

Need **plausible deniability** that you frequently visit that district!

Silently accept the message

Implicitly reveals that the sender:

1. **Is the message originator** or
2. **Previously accepted the message from someone else**

Mirage Design

Key Idea: the average person frequently travels between a small number of locations (e.g., work, school, and home)

Privatized Mobility Graphs

Districts

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Privatized Mobility Graphs

Districts

.0	.0	.01	.01
.02	.02	.05	.11
.03	.04	.04	.20
.0	.06	.21	.20

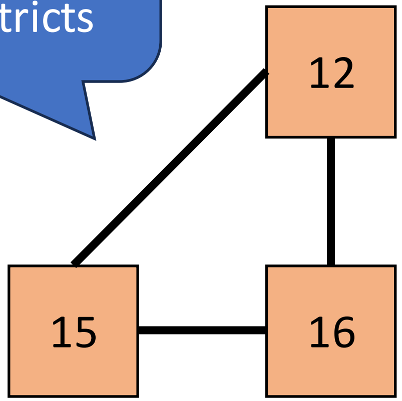
Privatized Mobility Graphs

Districts

.0	.0	.01	.01
.02	.02	.05	.11
.03	.04	.04	.20
.0	.06	.21	.20

Edges encode frequent transitions between districts

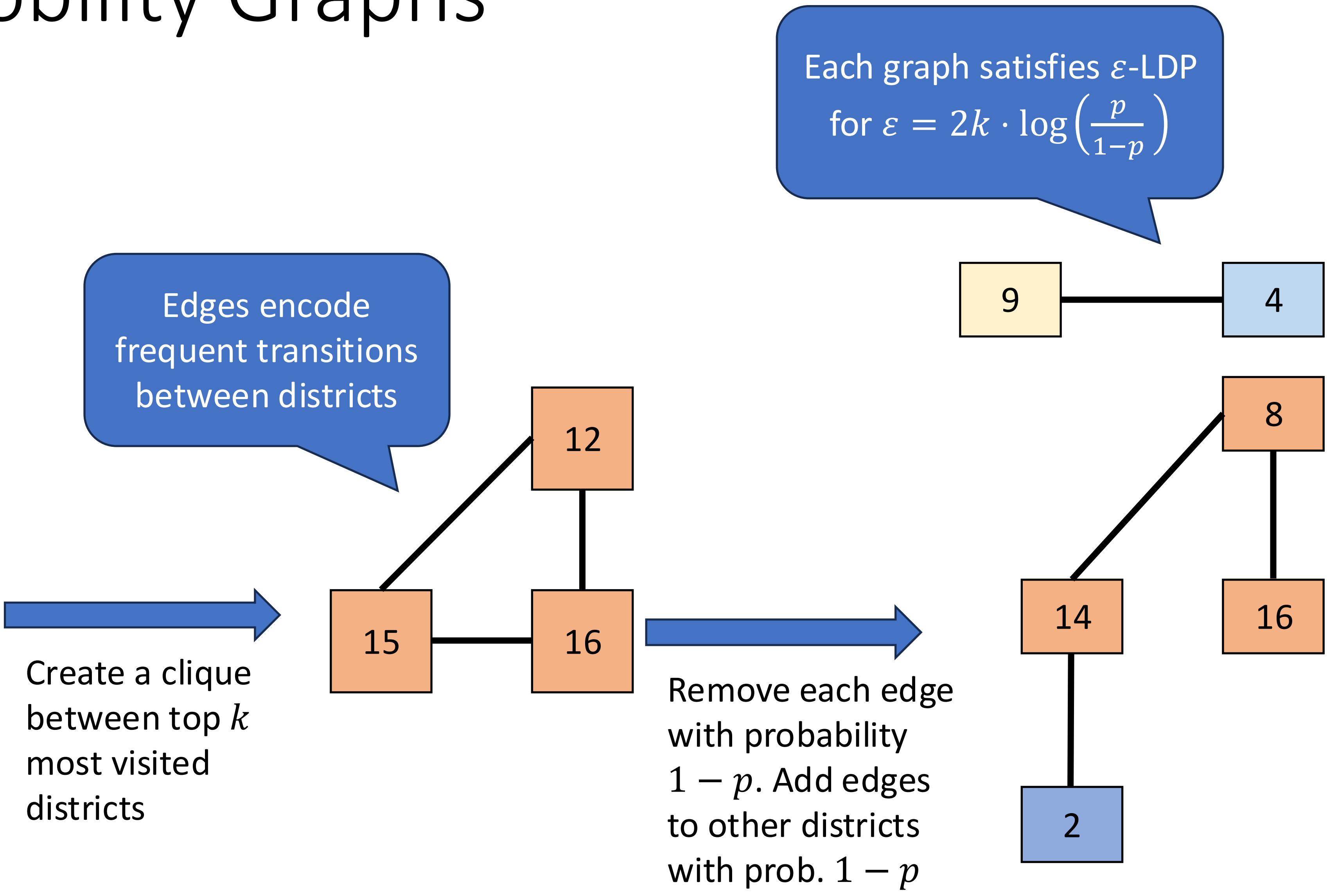
Create a clique between top k most visited districts



Privatized Mobility Graphs

Districts

.0	.0	.01	.01
.02	.02	.05	.11
.03	.04	.04	.20
.0	.06	.21	.20



Create a clique between top k most visited districts

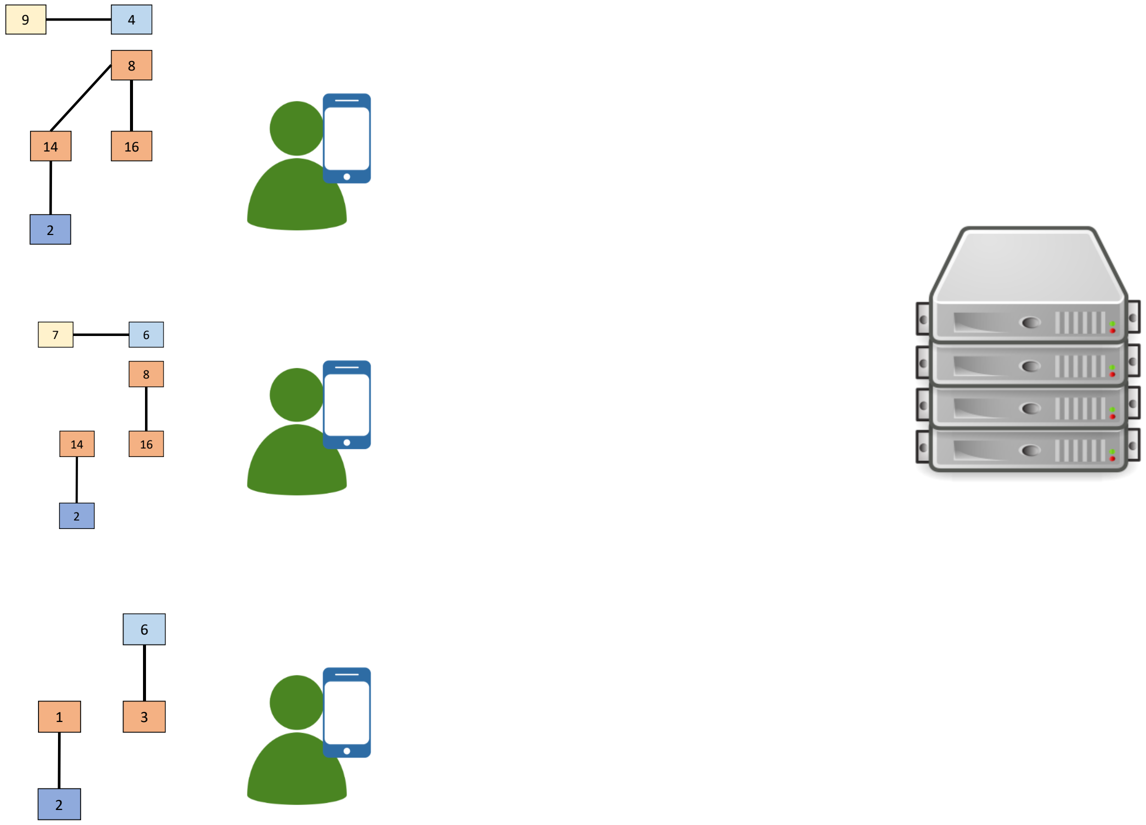
Edges encode frequent transitions between districts

Remove each edge with probability $1-p$. Add edges to other districts with prob. $1-p$

Each graph satisfies ε-LDP for $\varepsilon = 2k \cdot \log\left(\frac{p}{1-p}\right)$

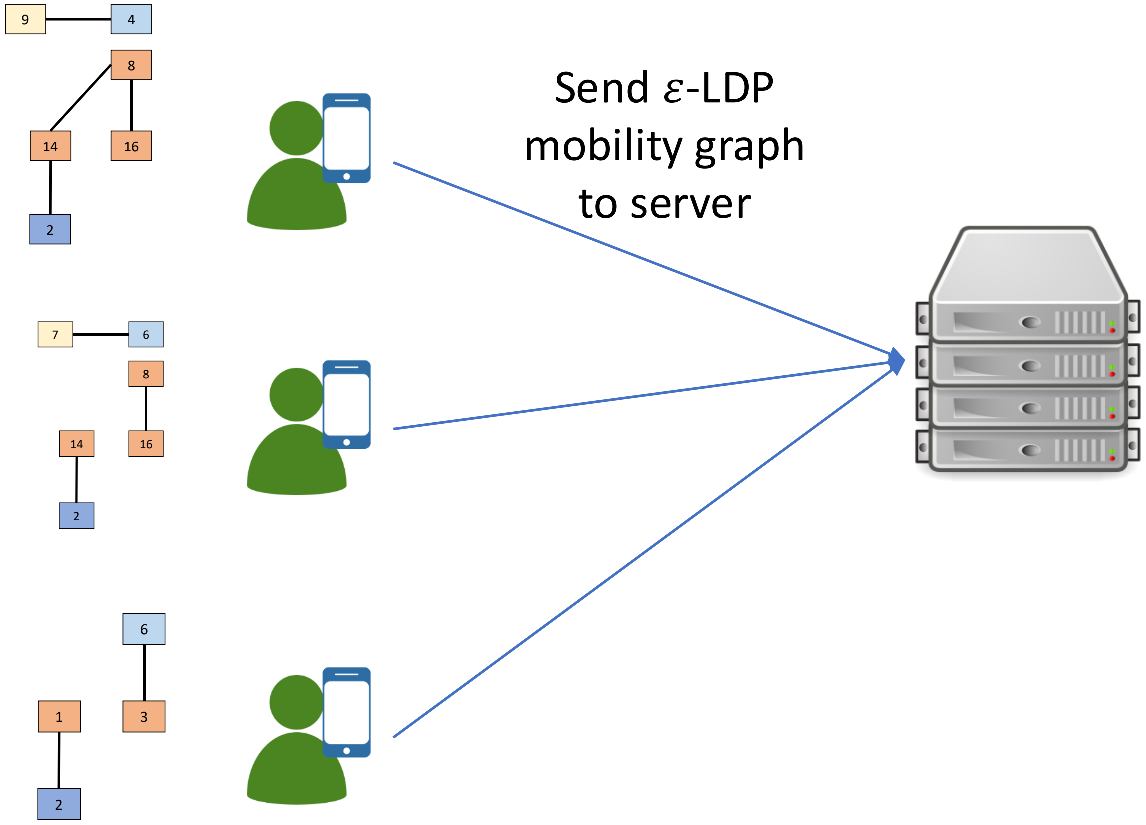
Global Mobility Profile

- Created during a setup phase (e.g., during app install)



Global Mobility Profile

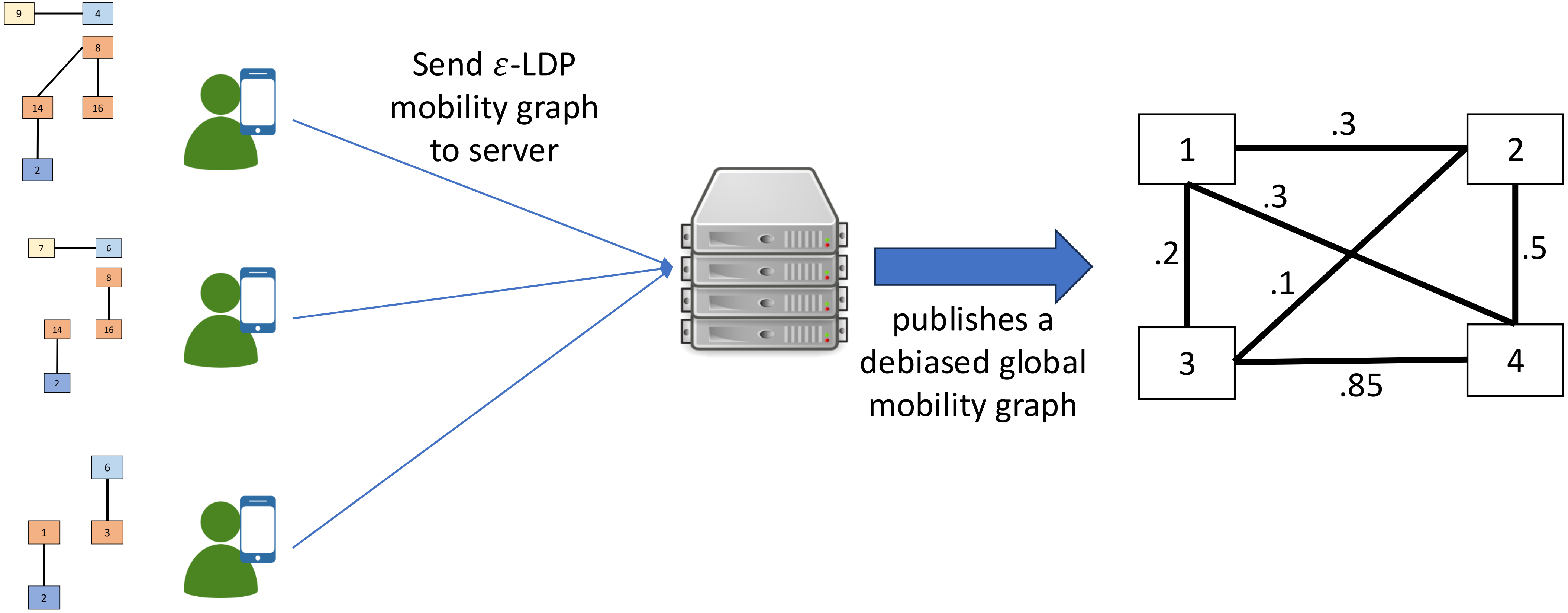
- Created during a setup phase (e.g., during app install)



Send ε-LDP mobility graph to server

Global Mobility Profile

- Created during a setup phase (e.g., during app install)

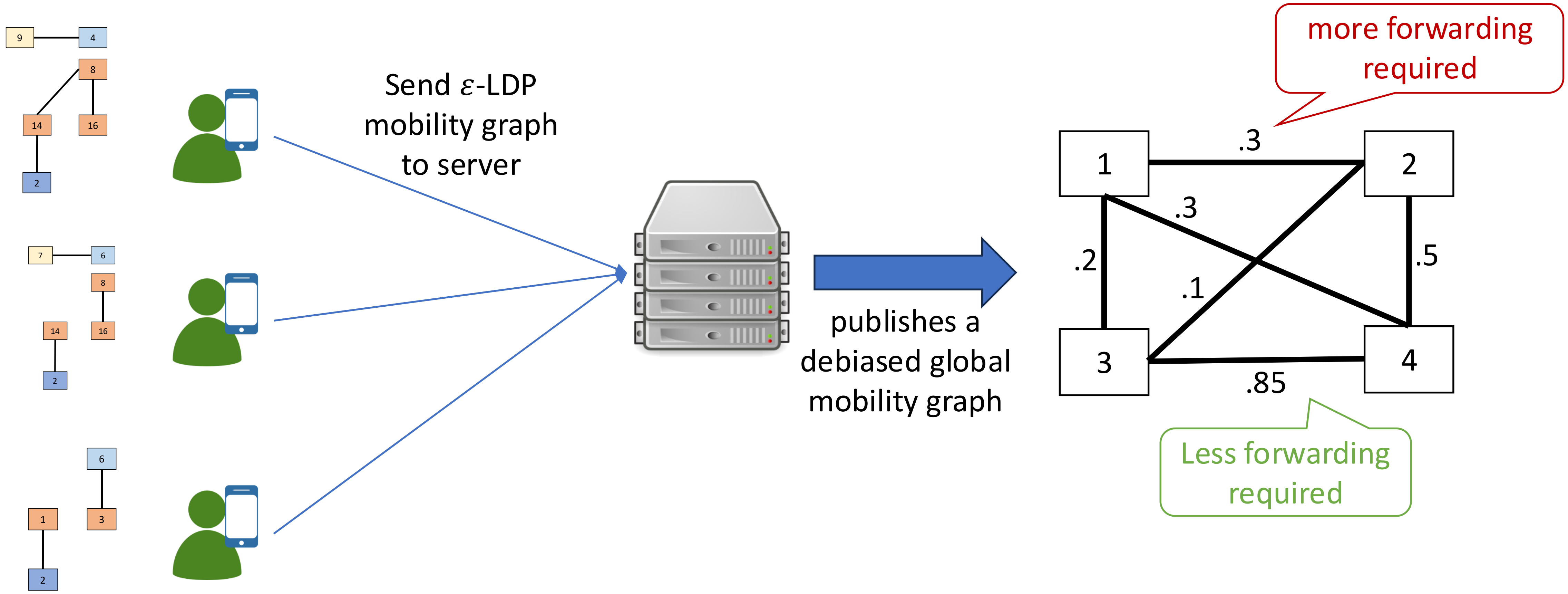


Send ε-LDP mobility graph to server

publishes a debiased global mobility graph

Global Mobility Profile

- Created during a setup phase (e.g., during app install)



Send ε-LDP mobility graph to server

publishes a debiased global mobility graph

more forwarding required

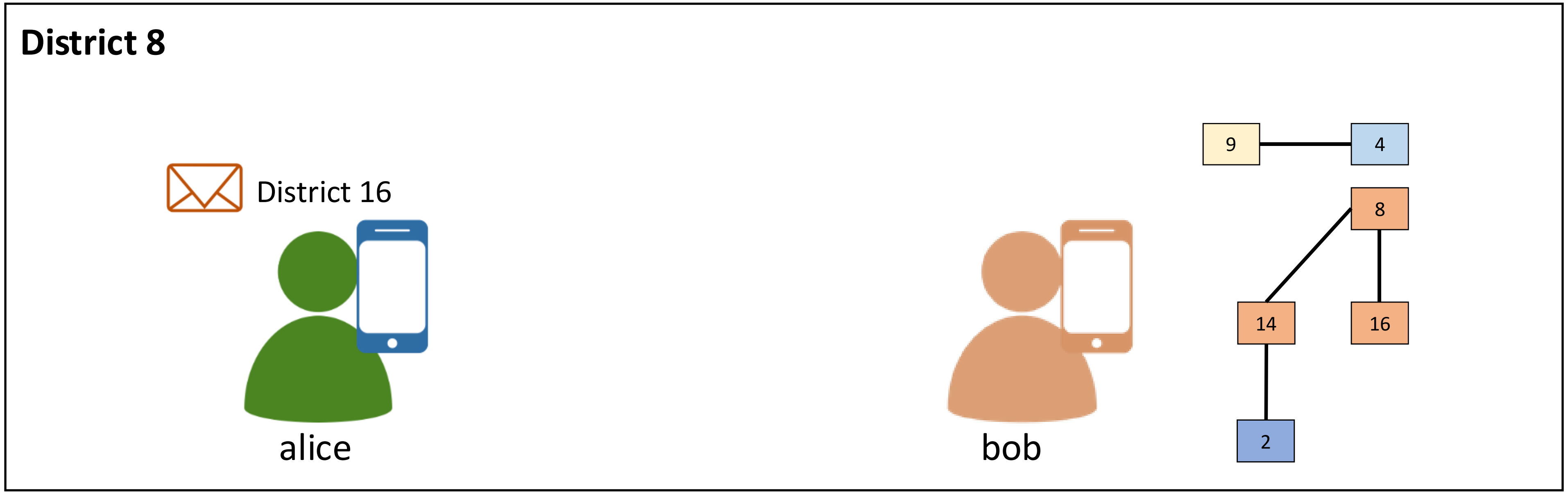
Less forwarding required

Private Routing Function

Intuition: Bob wants **plausible deniability** that he frequents a given district

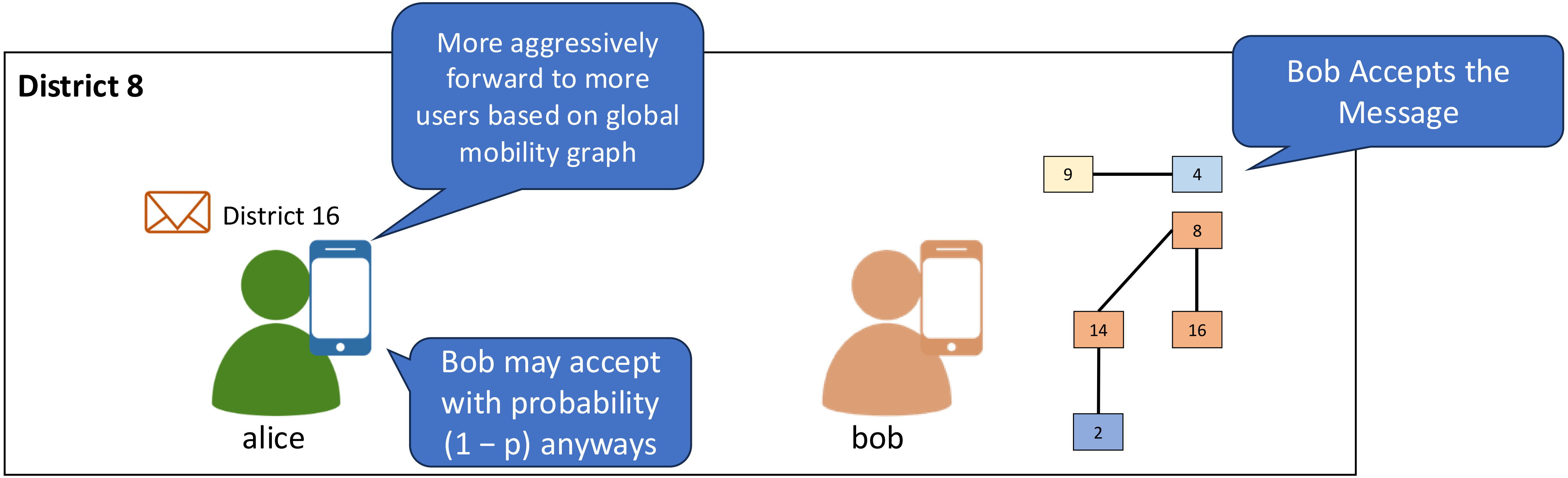
Private Routing Function

Intuition: Bob wants **plausible deniability** that he frequents a given district



Private Routing Function

Intuition: Bob wants **plausible deniability** that he frequents a given district



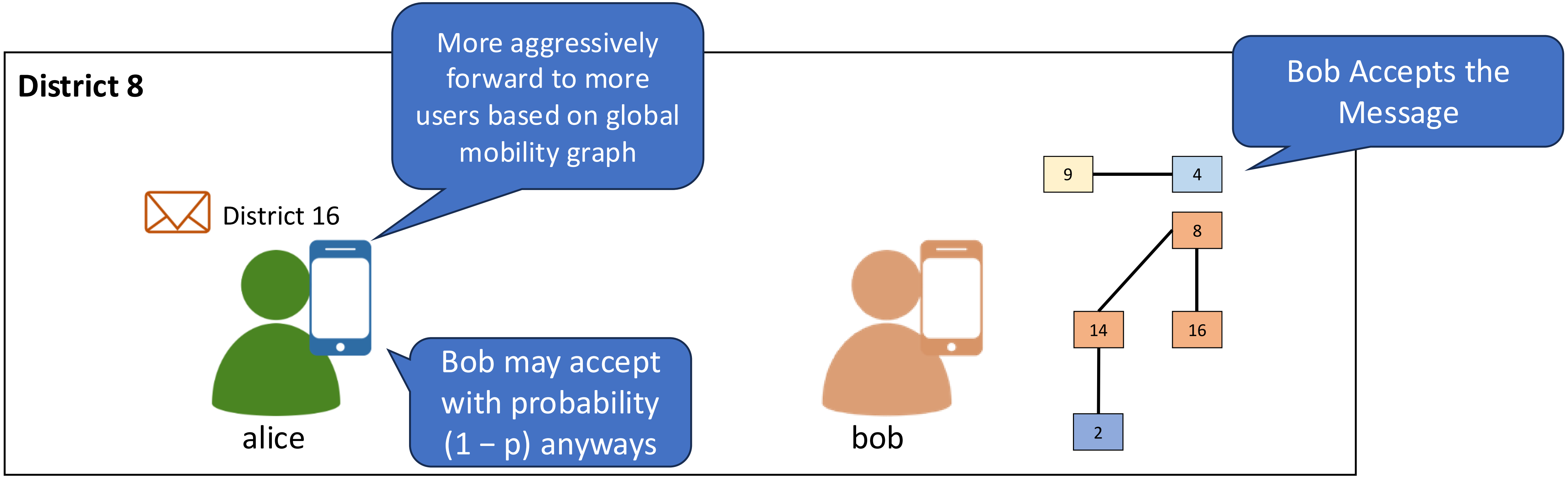
More aggressively forward to more users based on global mobility graph

Bob may accept with probability (1 – p) anyways

Bob Accepts the Message

Private Routing Function

Intuition: Bob wants **plausible deniability** that he frequents a given district



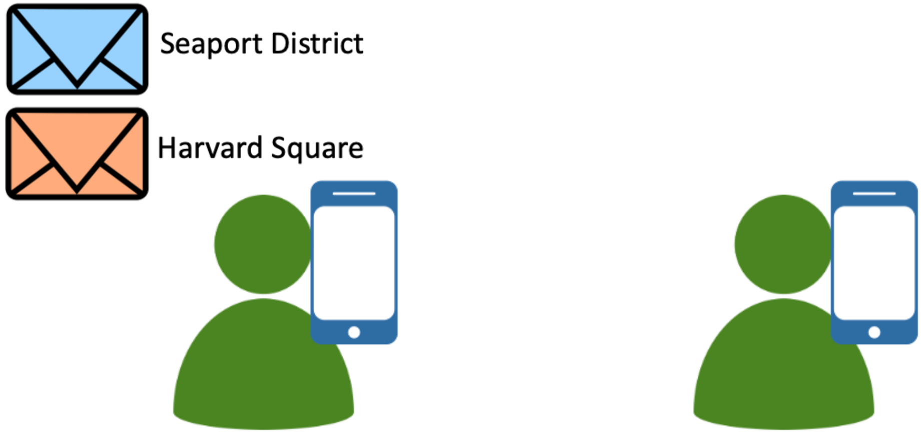
More aggressively forward to more users based on global mobility graph

Bob may accept with probability (1 – p) anyways

Bob Accepts the Message

ε-LDP Guarantee: $\Pr\left[f\left((\text{alice}, \text{bob}), m\right) = 1\right] \leq e^{\varepsilon} \cdot \Pr\left[f\left((\text{alice}, \text{charlie}), m\right) = 1\right]$

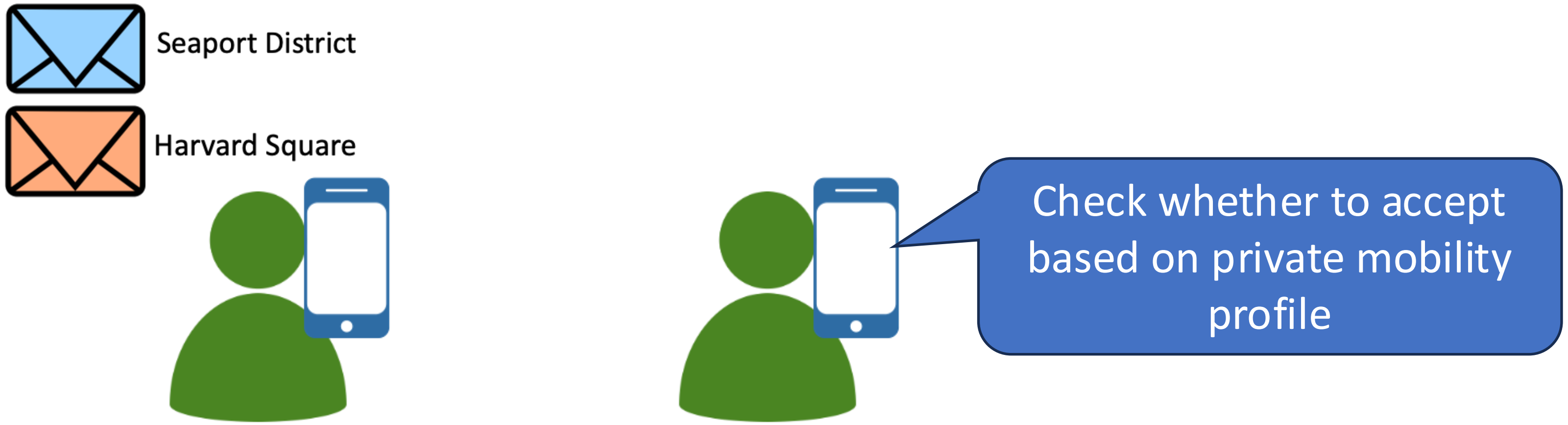
Mirage: Private Mobility-based Routing



Seaport District

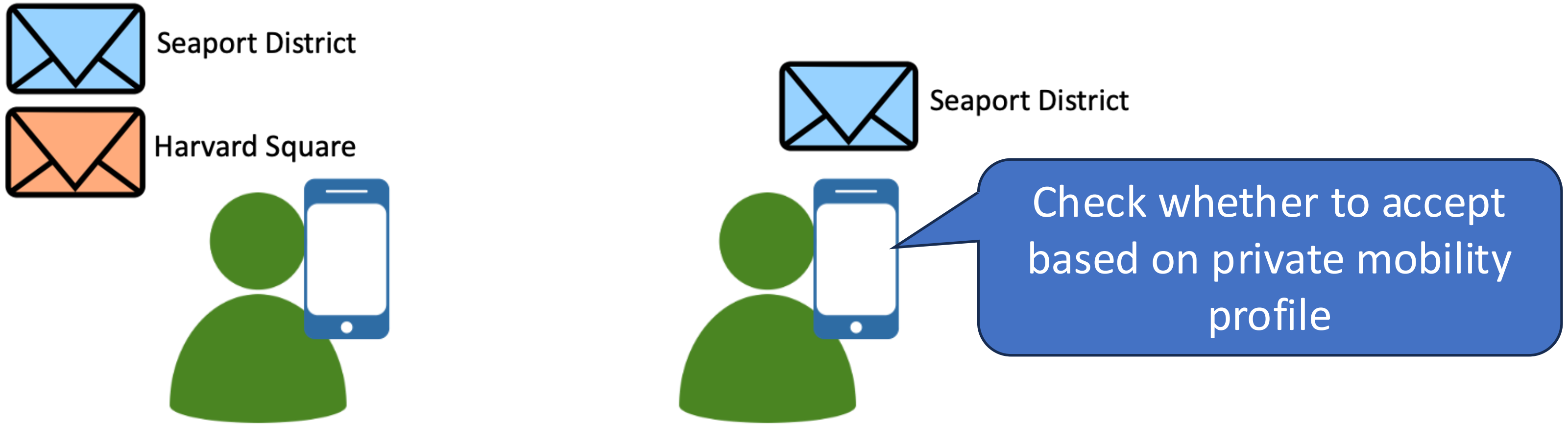
Harvard Square

Mirage: Private Mobility-based Routing



Check whether to accept based on private mobility profile

Mirage: Private Mobility-based Routing



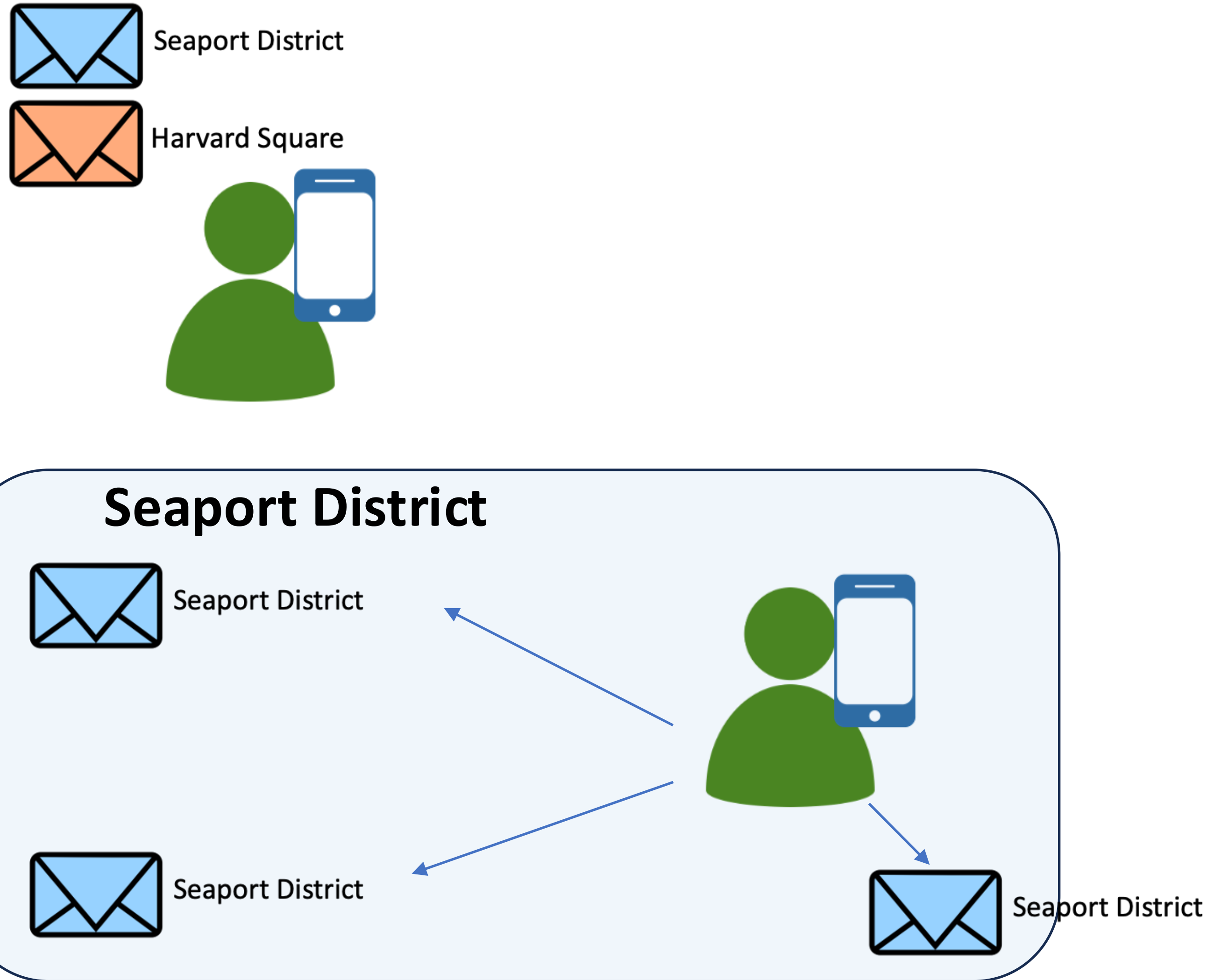
Seaport District

Harvard Square

Seaport District

Check whether to accept based on private mobility profile

Mirage: Private Mobility-based Routing



Seaport District

Harvard Square

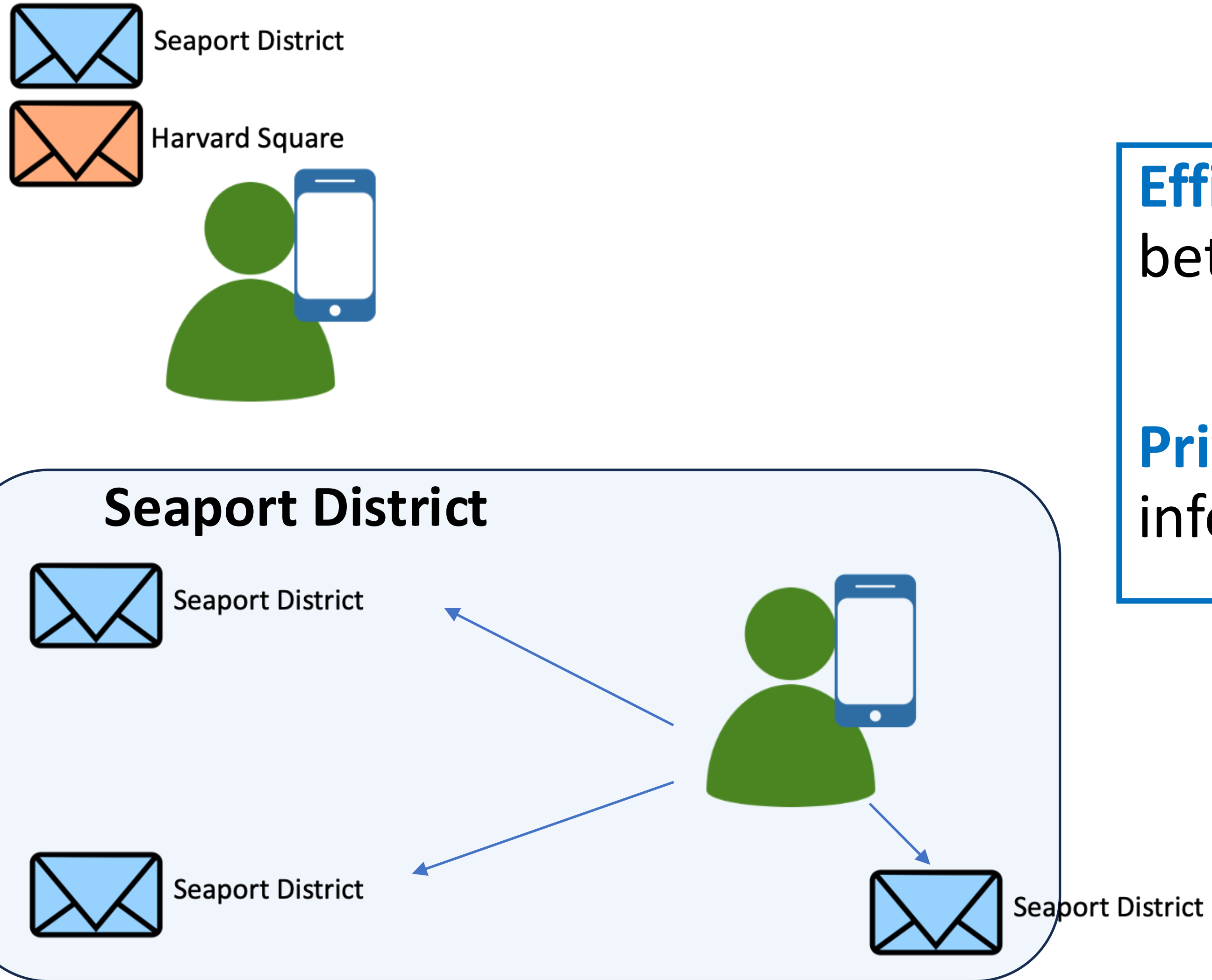
Seaport District

Seaport District

Seaport District

Seaport District

Mirage: Private Mobility-based Routing



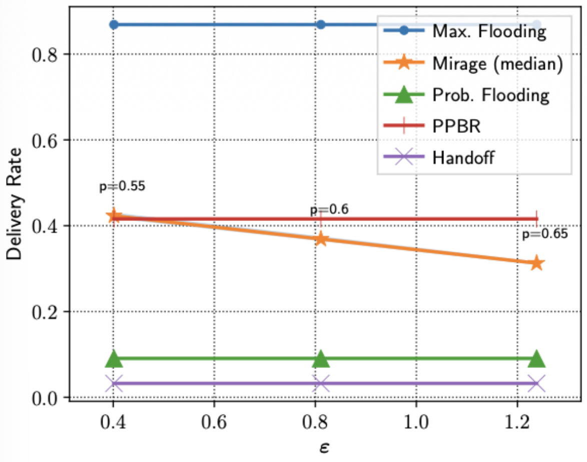
Efficiency: Reduced load vs. flooding, better delivery than random walk

Privacy: formal guarantees on how much information is leaked

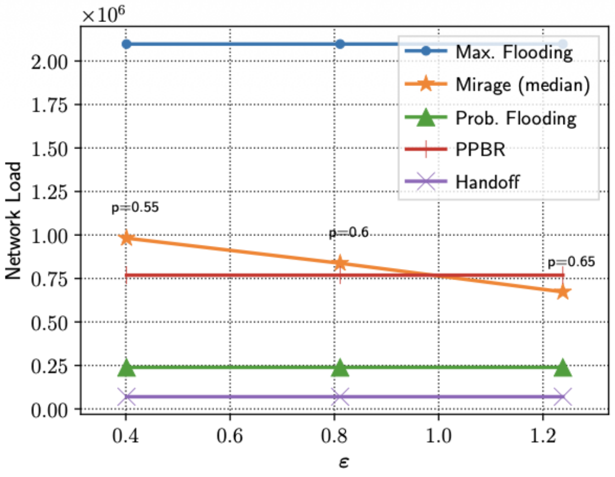
Performance Evaluation

- Evaluated within the **Cadence** Human-movement protocol sim (Berger, Sherr, Aviv, 2023)
- Used T-Drive (Beijing taxi traces) and YJMob100K (Japan metropolitan mobility) datasets

YJMob100K Dataset



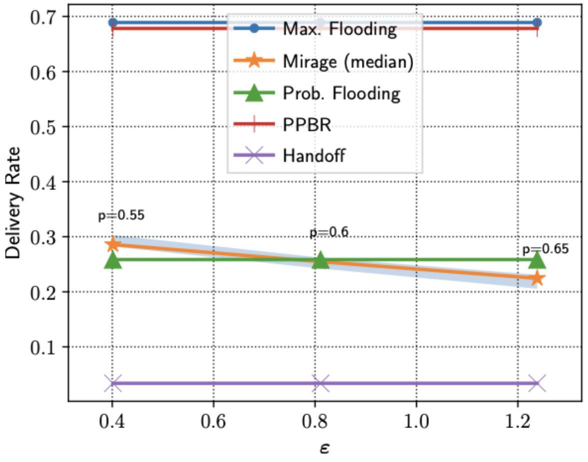
Delivery Rate



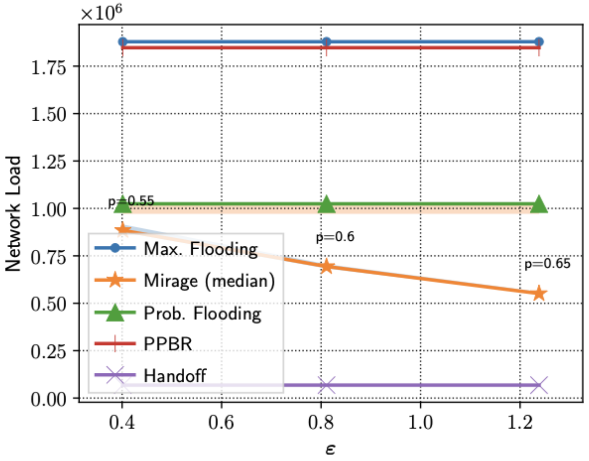
Network load

Comparable performance to PPBR!

T-Drive Dataset



Delivery Rate



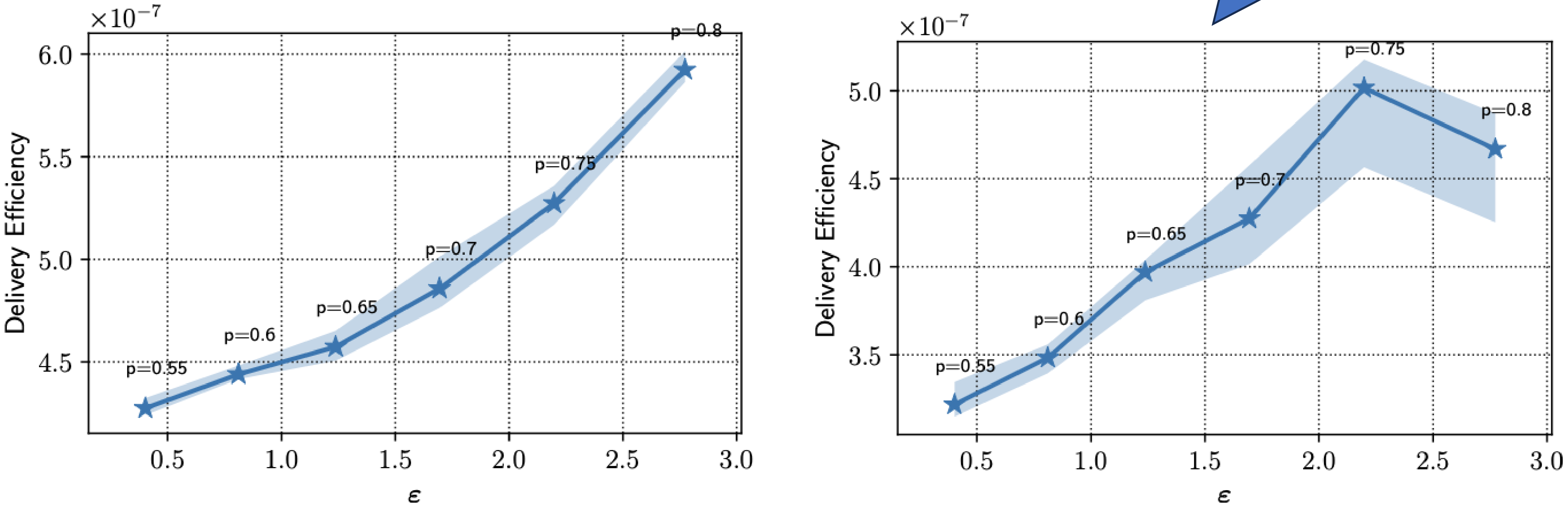
Network load

Worse on delivery rate; Better network load

Privacy Tradeoff

Delivery Efficiency Metric: $\frac{\text{Delivery Rate}}{\text{Network Load}}$

Higher ε → reduced privacy, but better delivery efficiency



(a) YJMob100K dataset

(b) T-Drive dataset

Questions?