Spacelab.
The City College of New York

Mesh Messaging for Large-Scale Protests: Cryptography Alone Won't Save Us

David Inyangson*, Sarah Radway*,
Tushar Jois, Nelly Fazio, James Mickens

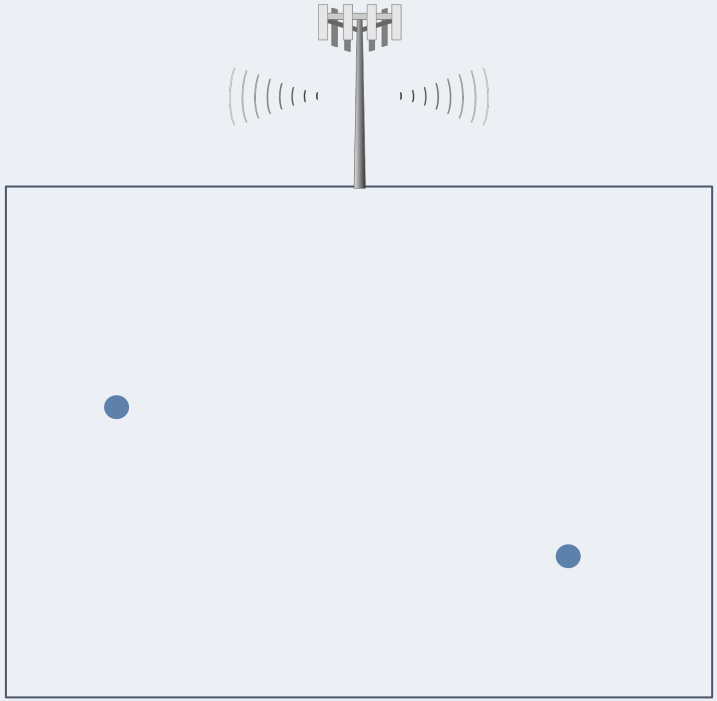
Real World Crypto Symposium (RWC) 2025
March 26, 2025

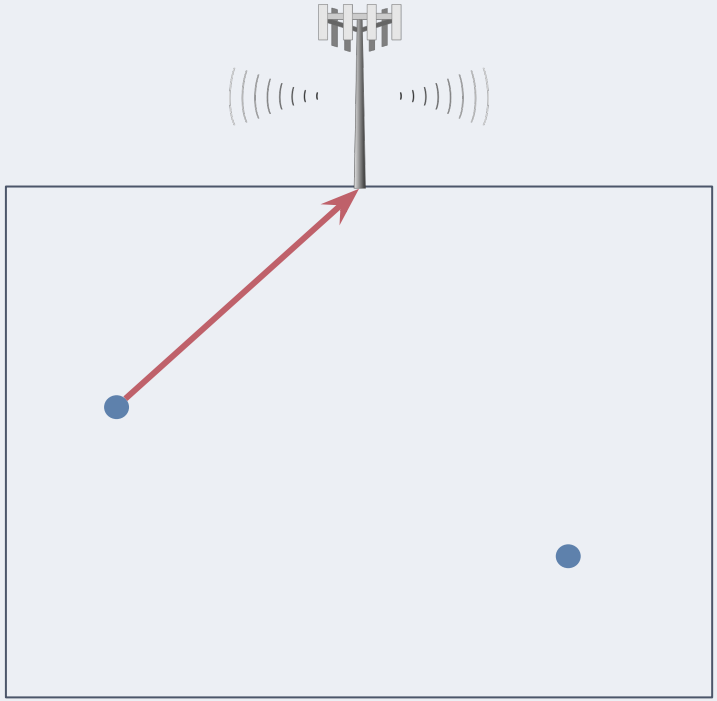
The City College of New York
Johns Hopkins University
Harvard University

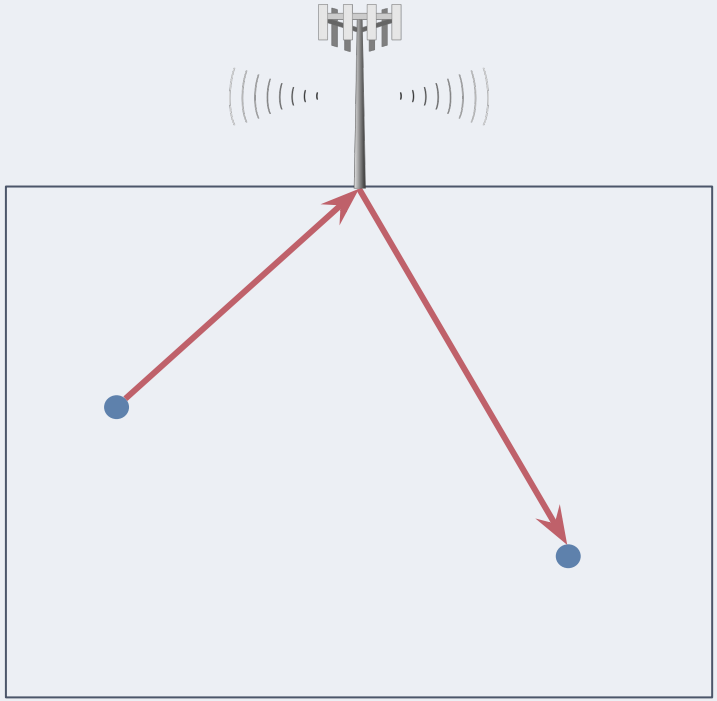
*Equal contribution.

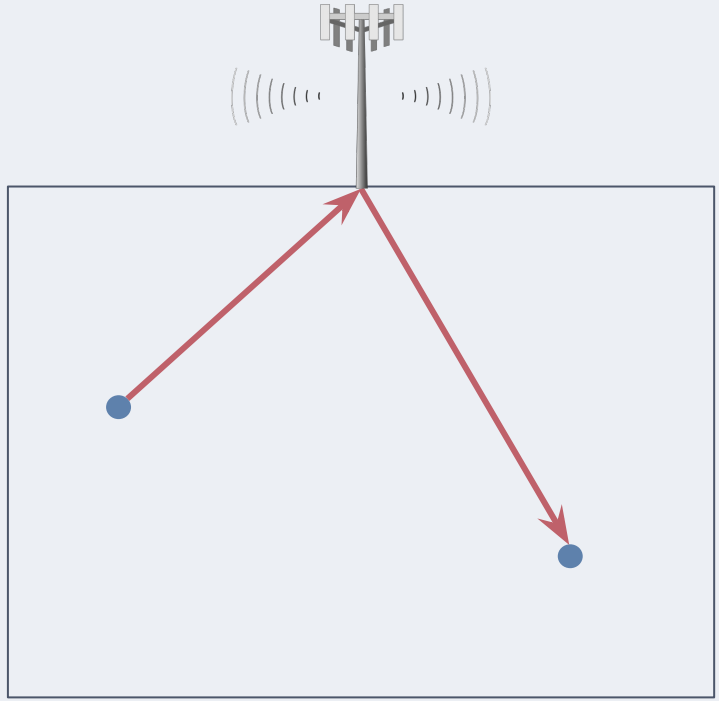

Large-scale protests


Large-scale protests
Communication is key!

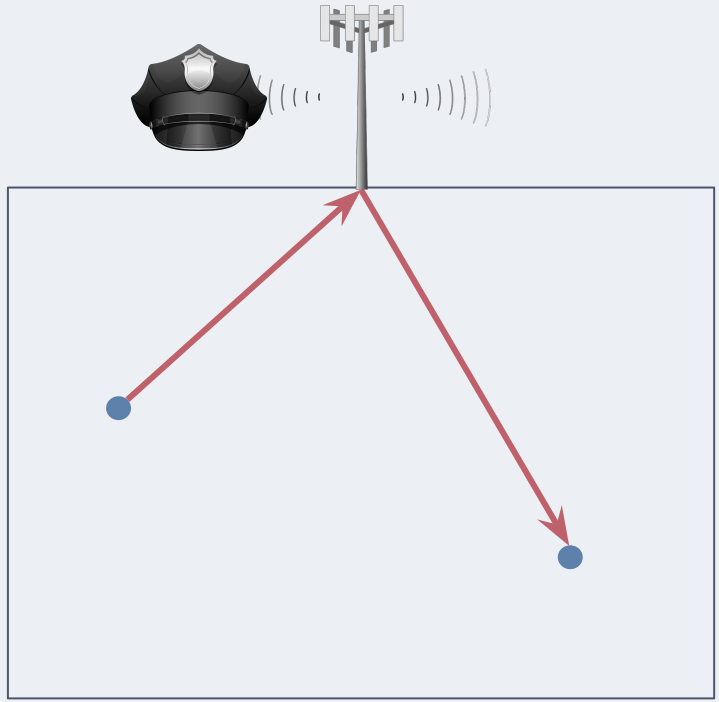




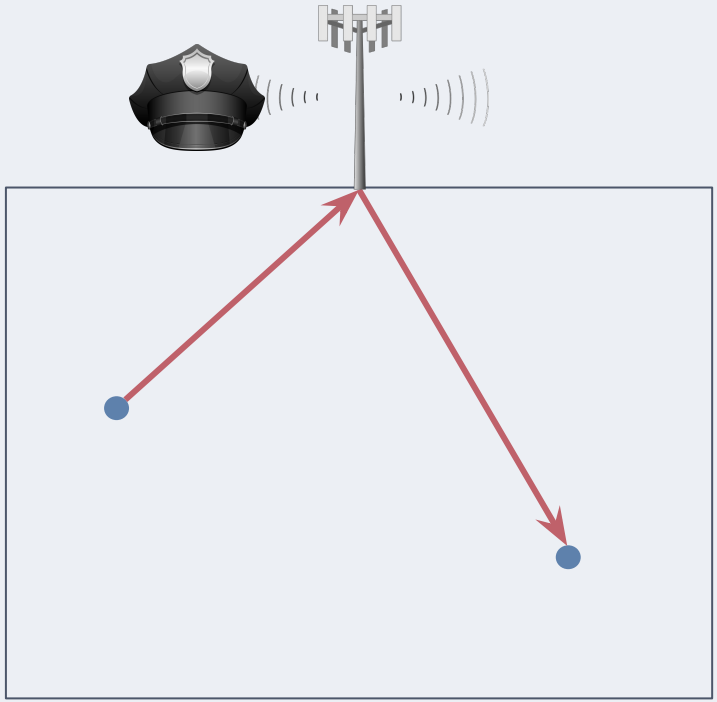




Centralized infrastructure



Centralized infrastructure



Intercepting communication

The Intercept_

HACKED DOCUMENTS: HOW IRAN CAN TRACK AND CONTROL PROTESTERS' PHONES

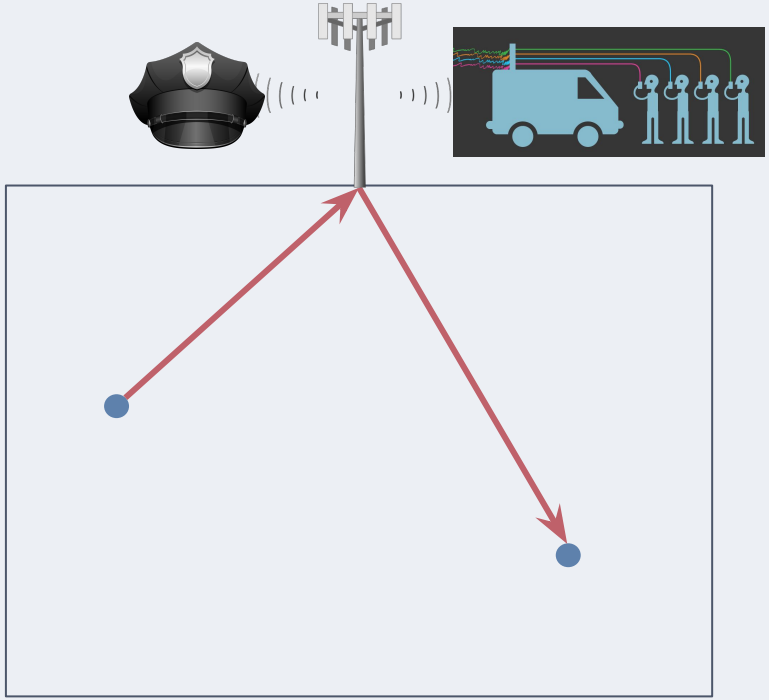
The documents provide an inside look at an Iranian government program that lets authorities monitor and manipulate people's phones.

The Marshall Project

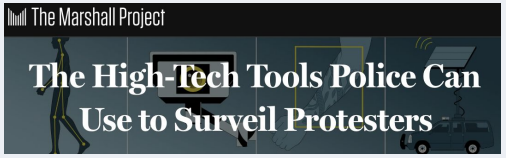
The High-Tech Tools Police Can Use to Surveil Protesters

STINGRAY TRACKING DEVICES: WHO'S GOT THEM?

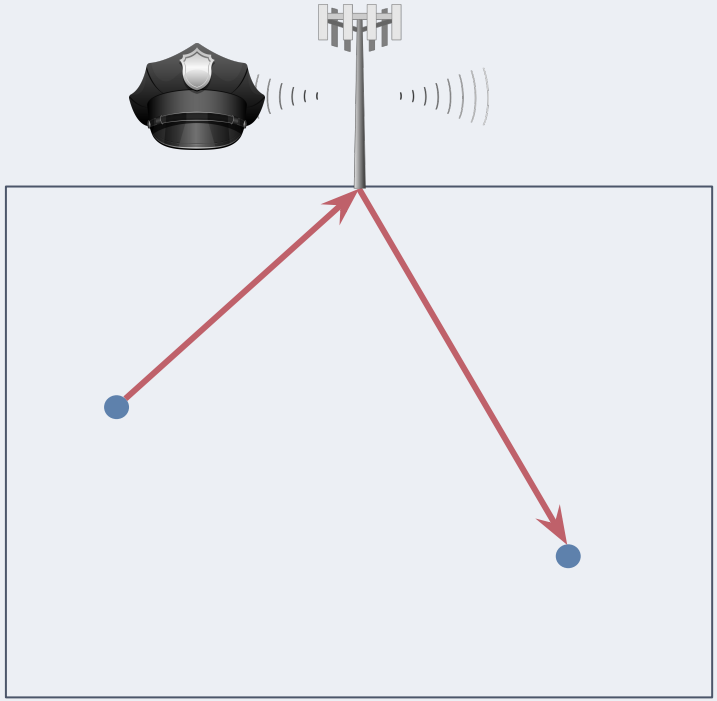
Centralized infrastructure



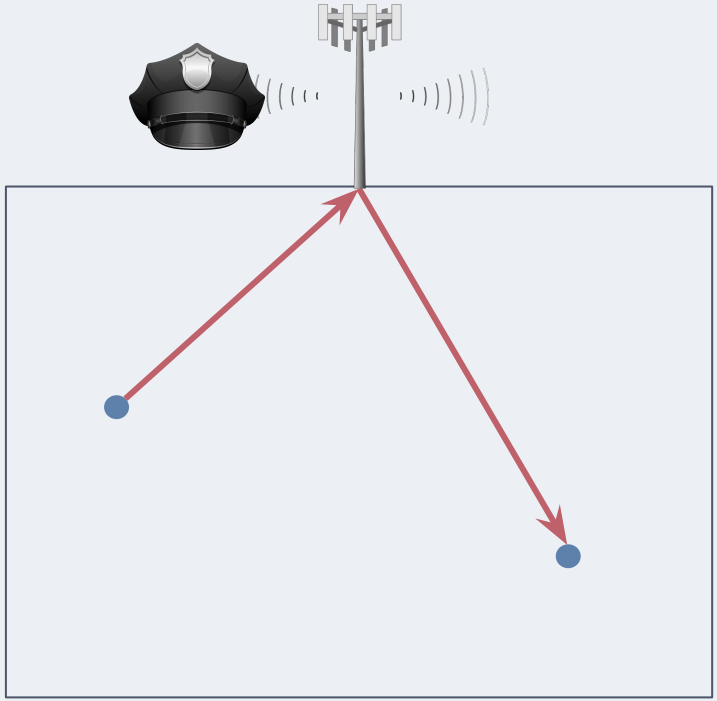
Intercepting communication



Centralized infrastructure



Centralized infrastructure



Centralized infrastructure

Preventing communication

Iran's Internet Shutdown Hides a Deadly Crackdown

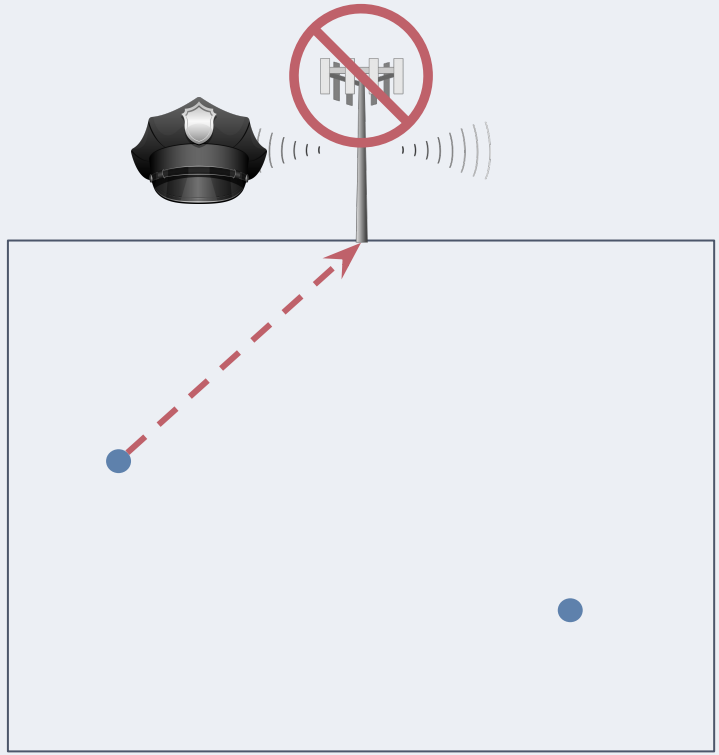
Amid protests against the killing of Mahsa Amini, authorities have cut off mobile internet, WhatsApp, and Instagram. The death toll continues to rise.

Myanmar shuts down internet and data communications

Observers say blockage might herald crackdown on freedom as popular anger rises

'No timeline' for restoring internet to Tigray: Ethiopia minister

In a ceasefire agreement signed earlier this month, Ethiopia committed to restoring basic services to the Tigray region.



Centralized infrastructure

Preventing communication

Iran's Internet Shutdown Hides a Deadly Crackdown

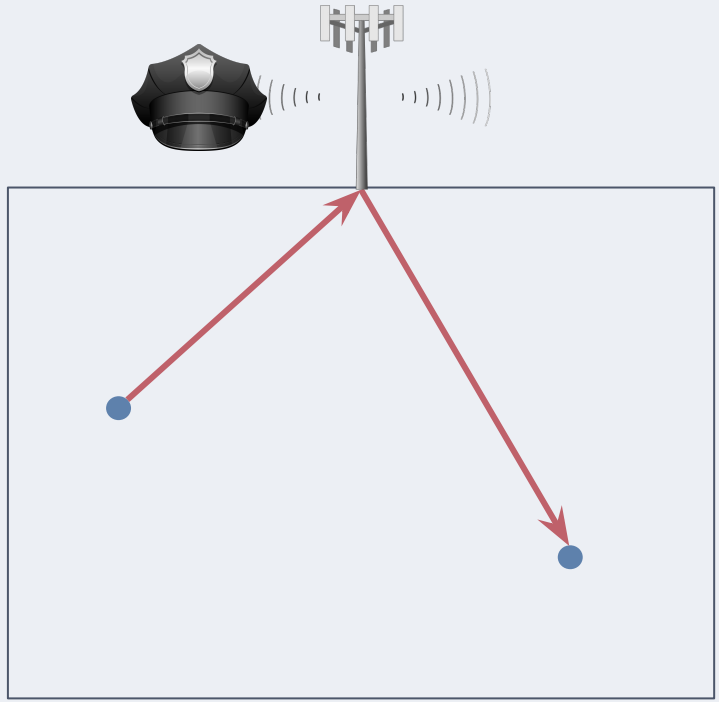
Amid protests against the killing of Mahsa Amini, authorities have cut off mobile internet, WhatsApp, and Instagram. The death toll continues to rise.

Myanmar shuts down internet and data communications

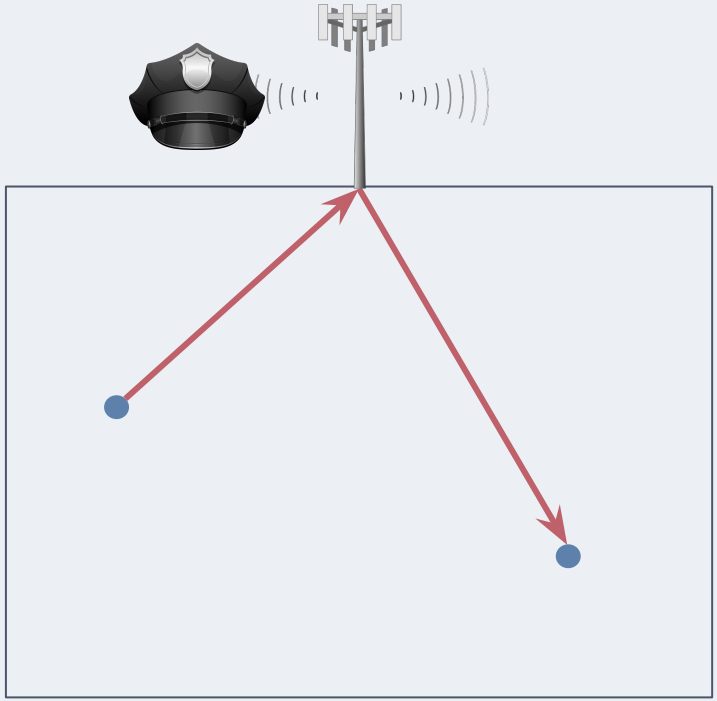
Observers say blockage might herald crackdown on freedom as popular anger rises

'No timeline' for restoring internet to Tigray: Ethiopia minister

In a ceasefire agreement signed earlier this month, Ethiopia committed to restoring basic services to the Tigray region.

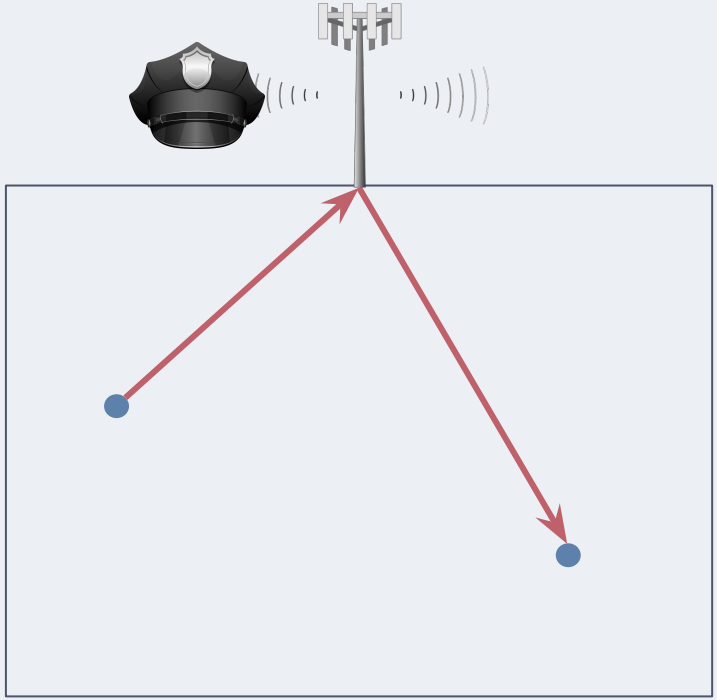


Centralized infrastructure

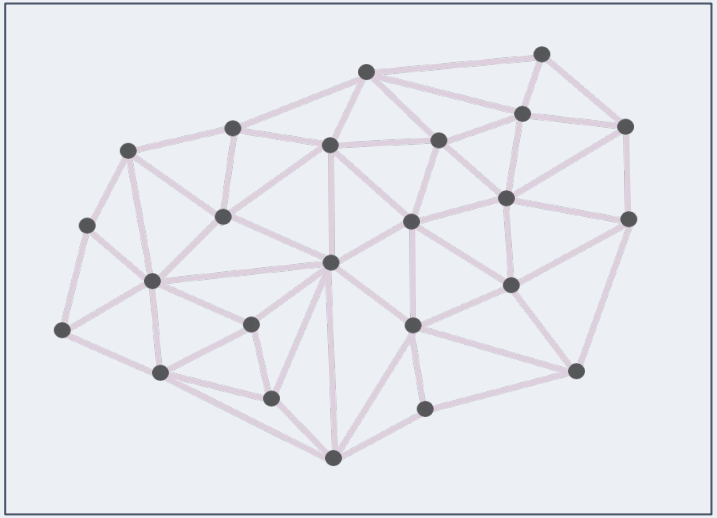


Centralized infrastructure

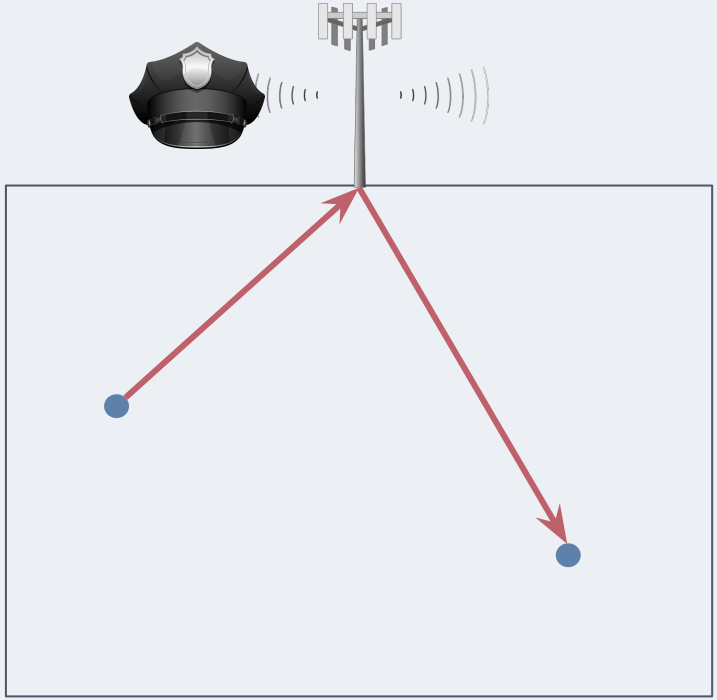
Smartphone mesh messaging



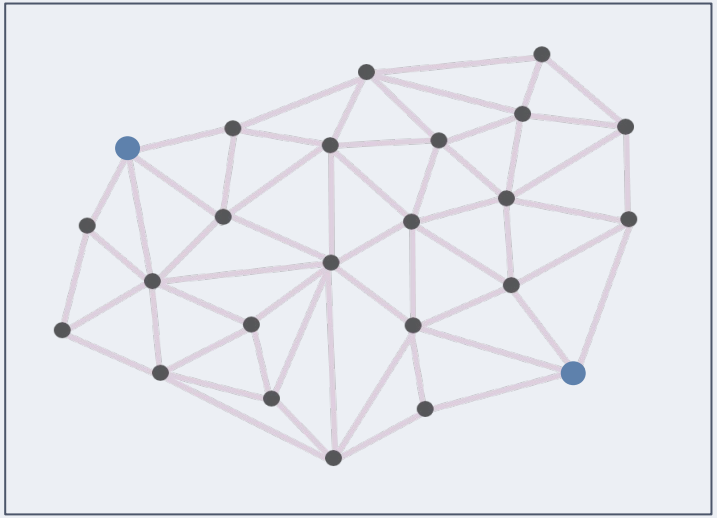
Smartphone mesh messaging



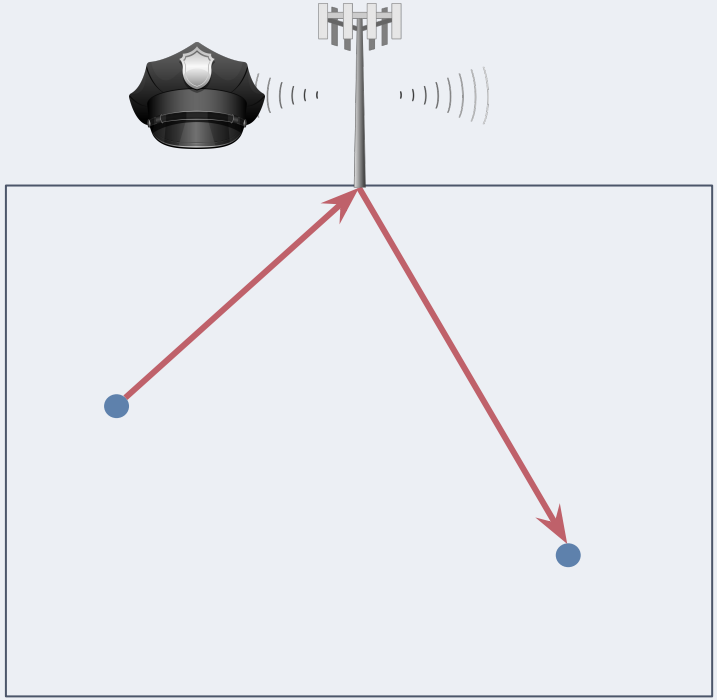
Centralized infrastructure



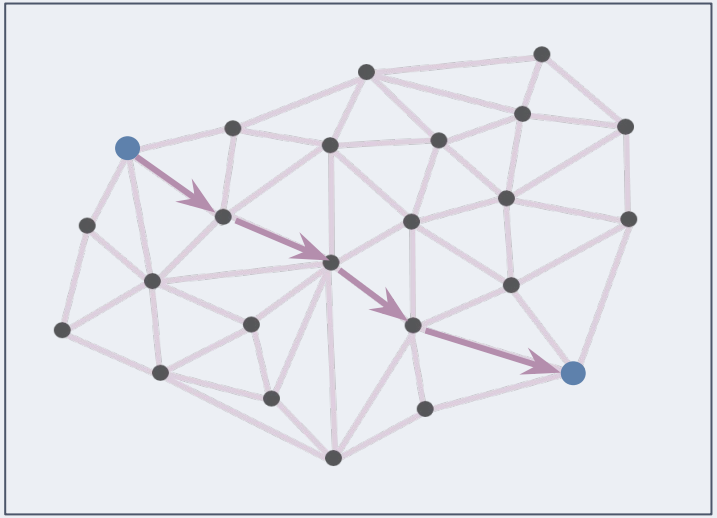
Smartphone mesh messaging



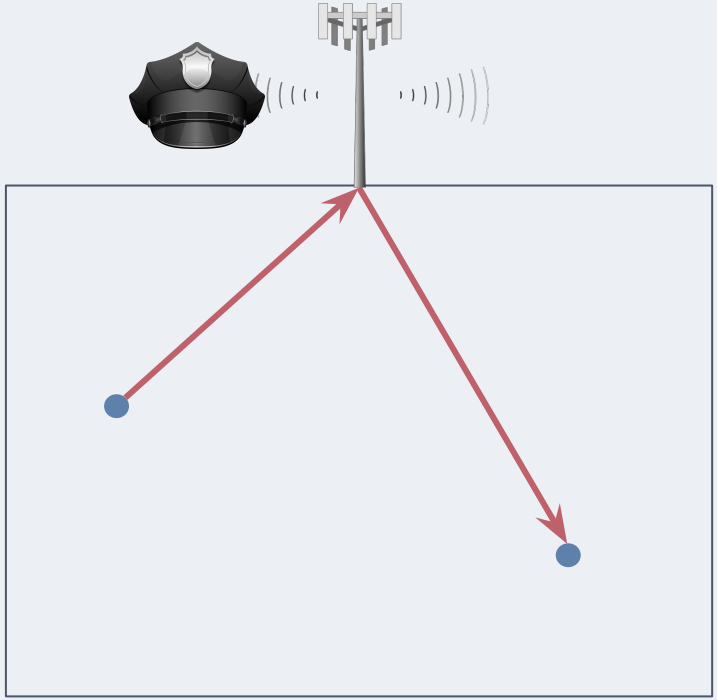
Centralized infrastructure



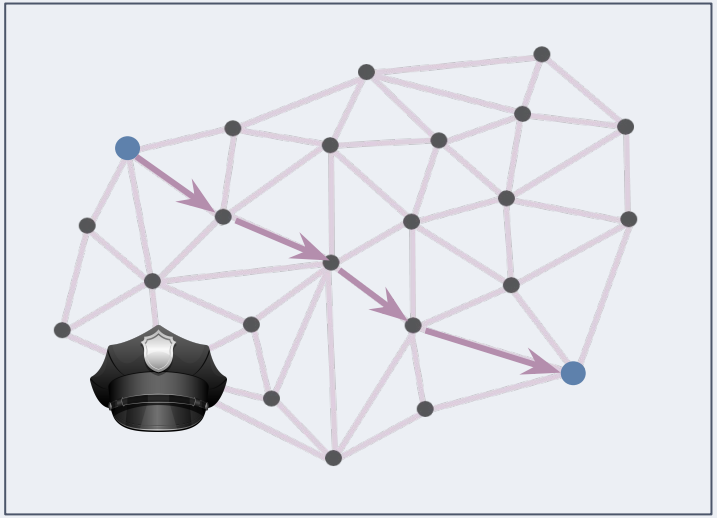
Smartphone mesh messaging



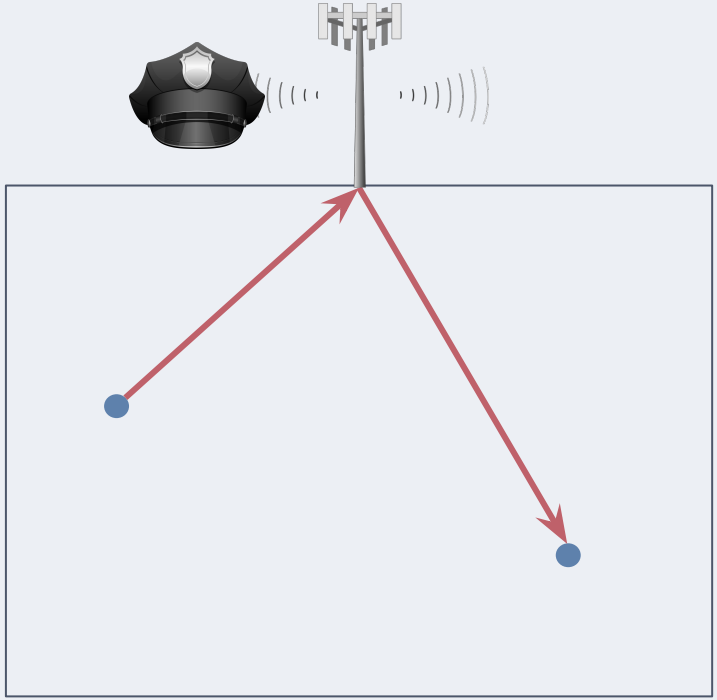
Centralized infrastructure



Smartphone mesh messaging

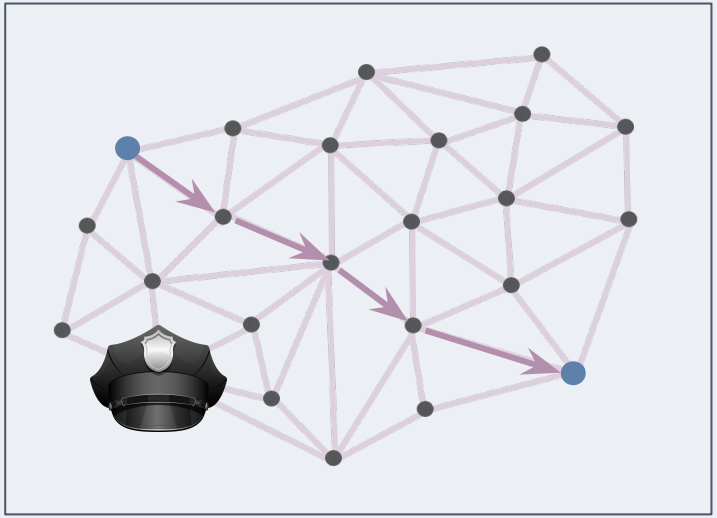


Centralized infrastructure



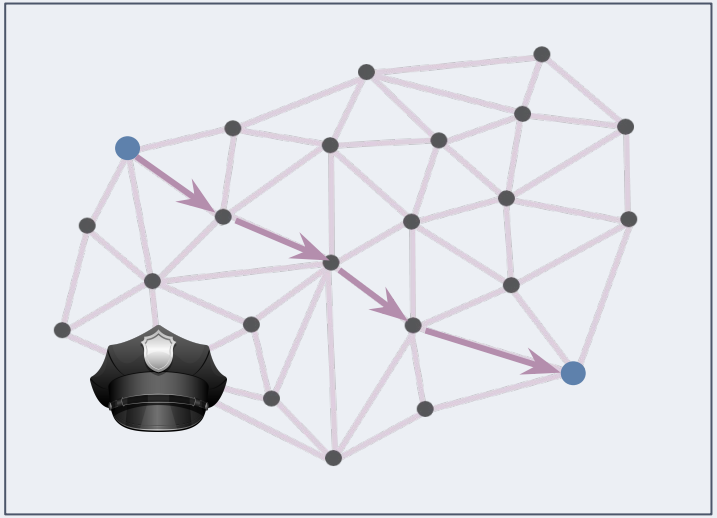
Centralized infrastructure

Smartphone mesh messaging



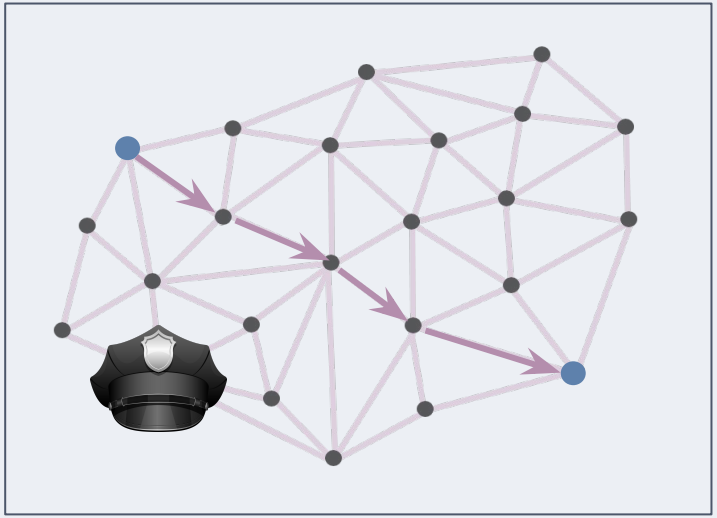
Mesh infrastructure

Smartphone mesh messaging



Mesh infrastructure

Smartphone mesh messaging



Mesh infrastructure

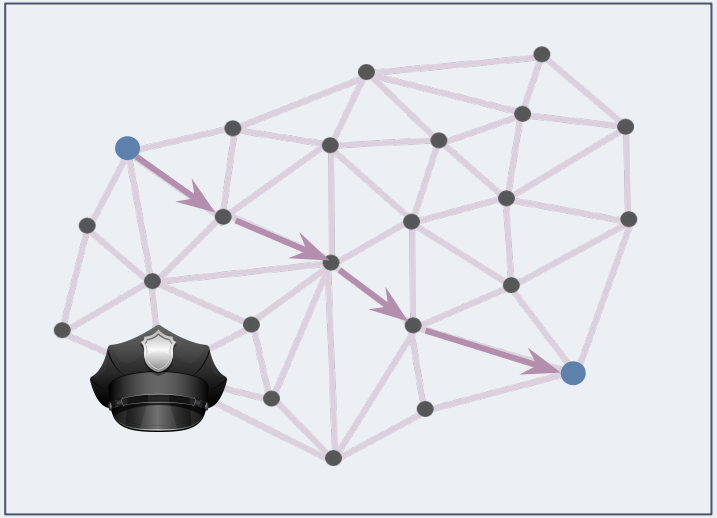
Academic work

Strong Anonymity for Mesh Messaging

Neil Perry, Stanford University
Bruce Spang, Stanford University
Saba Eskandarian, UNC Chapel Hill
Dan Boneh, Stanford University

Enhanced anonymity

Smartphone mesh messaging



Mesh infrastructure

Academic work

Strong Anonymity for Mesh Messaging

Neil Perry, Stanford University
Bruce Spang, Stanford University
Saba Eskandarian, UNC Chapel Hill
Dan Boneh, Stanford University

Enhanced anonymity

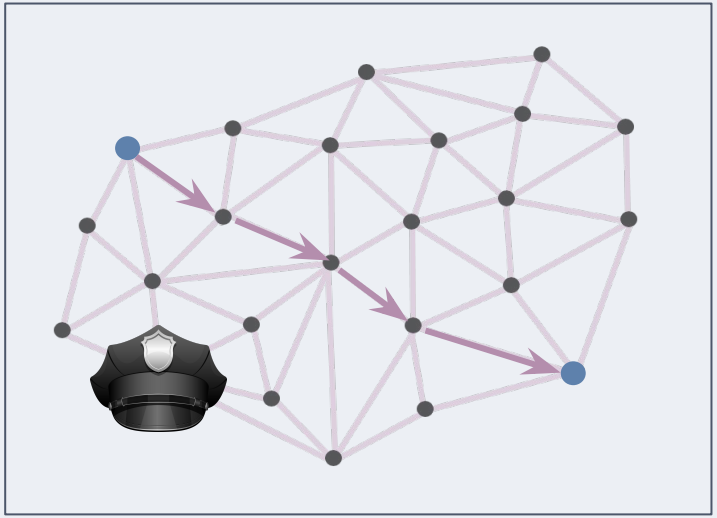
PoPETs — Proceedings on Privacy Enhancing Technologies ; 2022 (3):247–267

Amogh Pradeep*, Hira Javaid, Ryan Williams, Antoine Rault, David Choffnes, Stevens Le Blond, and Bryan Ford

Moby: A Blackout-Resistant Anonymity Network for Mobile Devices

DDoS resistance

Smartphone mesh messaging



Mesh infrastructure

Academic work

Strong Anonymity for Mesh Messaging

Neil Perry, Stanford University
Bruce Spang, Stanford University
Saba Eskandarian, UNC Chapel Hill
Dan Boneh, Stanford University

Enhanced anonymity

PoPETs — Proceedings on Privacy Enhancing Technologies ; 2022 (3):247–267

Amogh Pradeep*, Hira Javaid, Ryan Williams, Antoine Rault, David Choffnes, Stevens Le Blond, and Bryan Ford

Moby: A Blackout-Resistant Anonymity Network for Mobile Devices

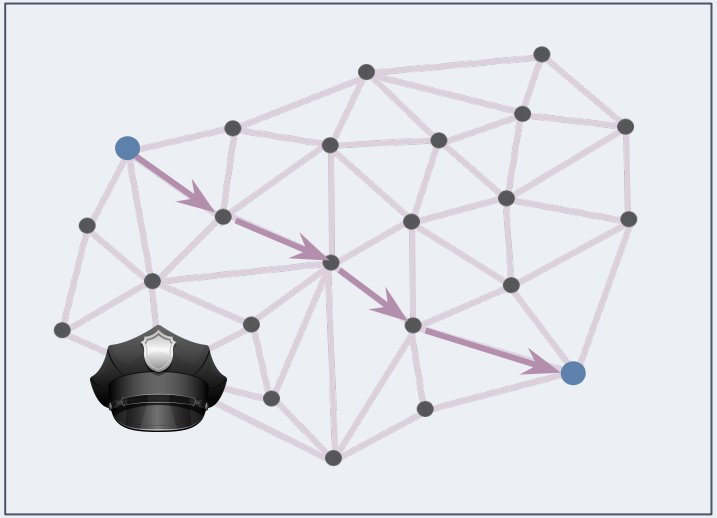
DDoS resistance

ASMesh: Anonymous and Secure Messaging in Mesh Networks Using Stronger, Anonymous Double Ratchet

Alexander Bienstock, New York University, New York, USA, abienstock@cs.nyu.edu
Paul Rösler, FAU Erlangen-Nürnberg, Nürnberg, Germany, paul.roesler@fau
Yi Tang, University of Michigan, Ann Arbor, USA

Stronger guarantees

Smartphone mesh messaging

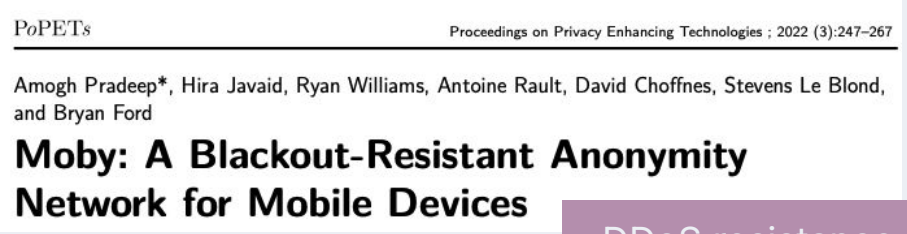


Mesh infrastructure

Academic work

Open-source apps

Enhanced anonymity



DDoS resistance

Stronger guarantees

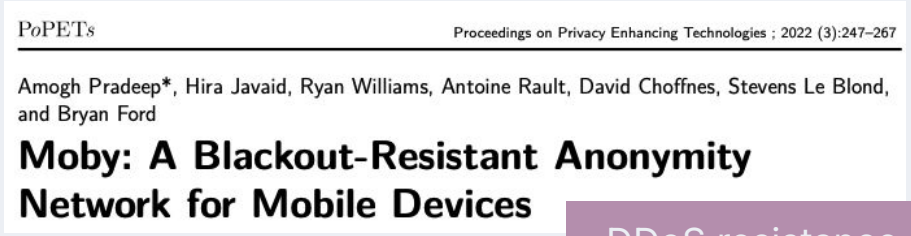
Academic work

Open-source apps

Strong Anonymity for Mesh Messaging

Neil Perry, Stanford University
Bruce Spang, Stanford University
Saba Eskandarian, UNC Chapel Hill
Dan Boneh, Stanford University

Enhanced anonymity



PoPETs Proceedings on Privacy Enhancing Technologies ; 2022 (3):247–267

Amogh Pradeep*, Hira Javaid, Ryan Williams, Antoine Rault, David Choffnes, Stevens Le Blond, and Bryan Ford

Moby: A Blackout-Resistant Anonymity Network for Mobile Devices

DDoS resistance

ASMesh: Anonymous and Secure Messaging in Mesh Networks Using Stronger, Anonymous Double Ratchet

Alexander Bienstock, New York University, New York, USA, abienstock@cs.nyu.edu
Paul Rösler, FAU Erlangen-Nürnberg, Nürnberg, Germany
Yi Tang, University of Michigan, Ann Arbor, USA

Stronger guarantees

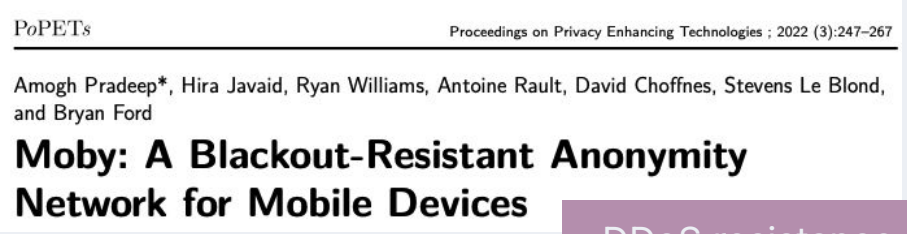
Academic work

Open-source apps

Strong Anonymity for Mesh Messaging

Neil Perry, Stanford University
Bruce Spang, Stanford University
Saba Eskandarian, UNC Chapel Hill
Dan Boneh, Stanford University

Enhanced anonymity



PoPETs Proceedings on Privacy Enhancing Technologies ; 2022 (3):247–267

Amogh Pradeep*, Hira Javaid, Ryan Williams, Antoine Rault, David Choffnes, Stevens Le Blond, and Bryan Ford

Moby: A Blackout-Resistant Anonymity Network for Mobile Devices

DDoS resistance

ASMesh: Anonymous and Secure Messaging in Mesh Networks Using Stronger, Anonymous Double Ratchet

Alexander Bienstock, New York University, New York, USA, abienstock@cs.nyu.edu
Paul Rösler, FAU Erlangen-Nürnberg, Nürnberg, Germany, paul.roesler@fau
Yi Tang, University of Michigan, Ann Arbor, USA

Stronger guarantees

FireChat

bridgefy

Academic work

Open-source apps

Strong Anonymity for Mesh Messaging

Neil Perry, Stanford University
Bruce Spang, Stanford University
Saba Eskandarian, UNC Chapel Hill
Dan Boneh, Stanford University

Enhanced anonymity

PoPETs Proceedings on Privacy Enhancing Technologies ; 2022 (3):247–267

Amogh Pradeep*, Hira Javaid, Ryan Williams, Antoine Rault, David Choffnes, Stevens Le Blond, and Bryan Ford

Moby: A Blackout-Resistant Anonymity Network for Mobile Devices

DDoS resistance

ASMesh: Anonymous and Secure Messaging in Mesh Networks Using Stronger, Anonymous Double Ratchet

Alexander Bienstock, New York University, New York, USA, abienstock@cs.nyu.edu
Paul Rösler, FAU Erlangen-Nürnberg, Nürnberg, Germany, paul.roesler@fau
Yi Tang, University of Michigan, Ann Arbor, USA

Stronger guarantees

FireChat

bridgefy

qaul قول

Academic work

Open-source apps

Strong Anonymity for Mesh Messaging

Neil Perry, Stanford University
Bruce Spang, Stanford University
Saba Eskandarian, UNC Chapel Hill
Dan Boneh, Stanford University

Enhanced anonymity

PoPETs — Proceedings on Privacy Enhancing Technologies ; 2022 (3):247–267

Amogh Pradeep*, Hira Javaid, Ryan Williams, Antoine Rault, David Choffnes, Stevens Le Blond, and Bryan Ford

Moby: A Blackout-Resistant Anonymity Network for Mobile Devices

DDoS resistance

ASMesh: Anonymous and Secure Messaging in Mesh Networks Using Stronger, Anonymous Double Ratchet

Alexander Bienstock, New York University, New York, USA, abienstock@cs.nyu.edu
Paul Rösler, FAU Erlangen-Nürnberg, Nürnberg, Germany, paul.roesler@fau
Yi Tang, University of Michigan, Ann Arbor, USA

Stronger guarantees

FireChat

Bridgefy

Not widely deployed

qaul قول

Academic work

Strong Anonymity for Mesh Messaging

Neil Perry, Stanford University
Bruce Spang, Stanford University
Saba Eskandarian, UNC Chapel Hill
Dan Boneh, Stanford University

Enhanced anonymity

PoPETs — Proceedings on Privacy Enhancing Technologies ; 2022 (3):247–267

Amogh Pradeep*, Hira Javaid, Ryan Williams, Antoine Rault, David Choffnes, Stevens Le Blond, and Bryan Ford

Moby: A Blackout-Resistant Anonymity Network for Mobile Devices

DoS resistance

ASMesh: Anonymous and Secure Messaging in Mesh Networks Using Stronger, Anonymous Double Ratchet

Alexander Bienstock, New York University, New York, USA, abienstock@cs.nyu.edu
Paul Rösler, FAU Erlangen-Nürnberg, Nürnberg, Germany, paul.roesler@fau
Yi Tang, University of Michigan, Ann Arbor, USA

Stronger guarantees

Open-source apps

FireChat

Bridgefy

Not widely deployed

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

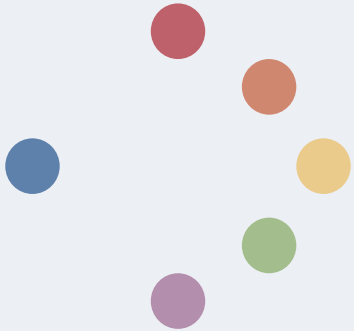
Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:



Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

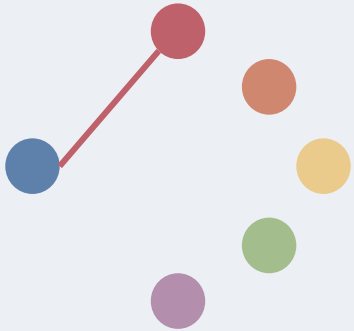
Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:



Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

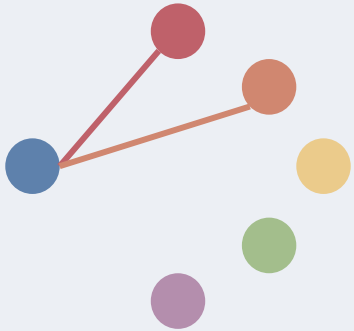
Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:



Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

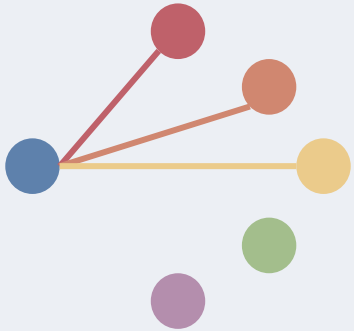
Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:



Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

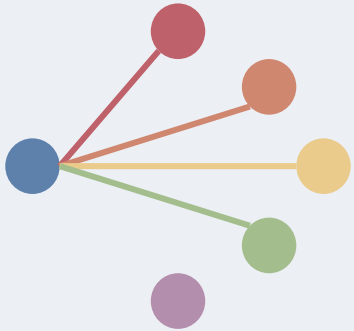
Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:



Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

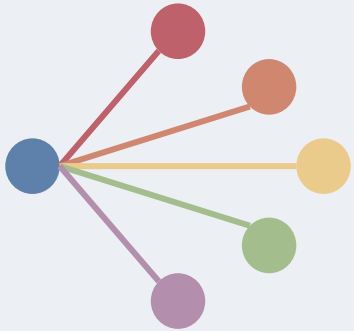
Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:



Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

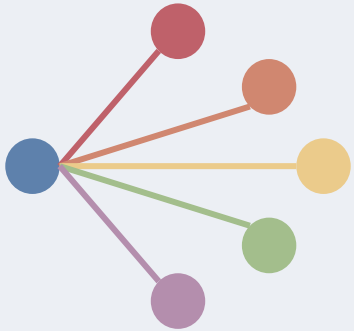
Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:



Linear

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

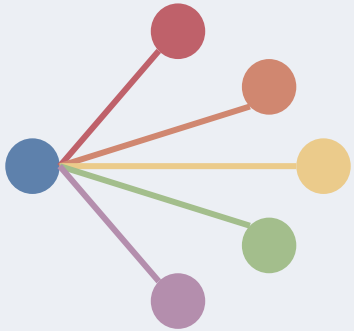
Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

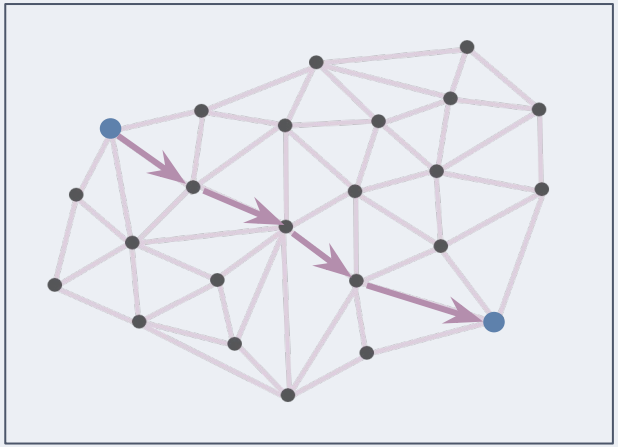
Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:



Linear



Mesh infrastructure

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

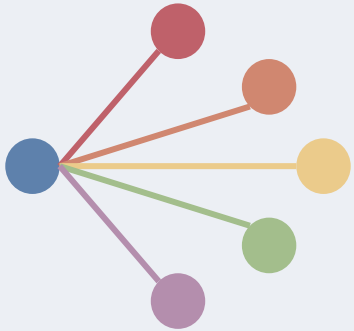
Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

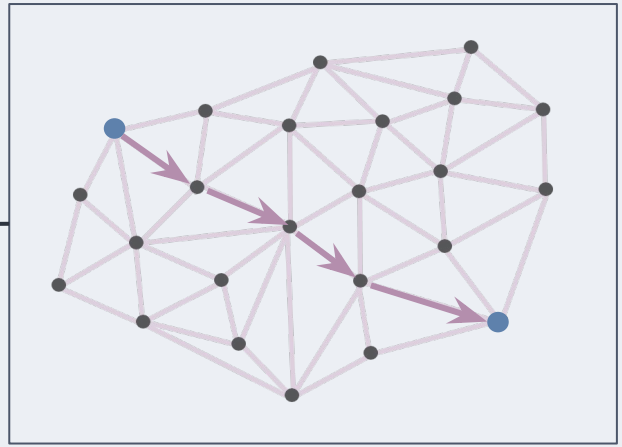
Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:



Linear



Mesh infrastructure

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

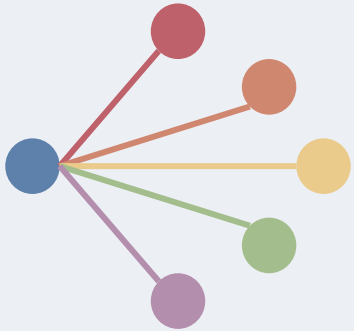
Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

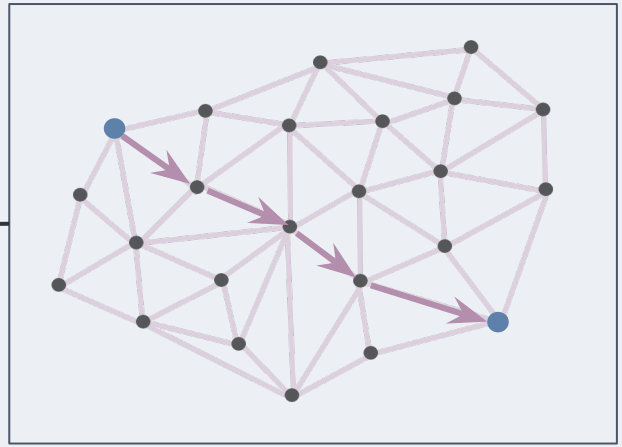
- Protesters work in groups!
- We need efficient group messaging in a mesh

Traditional group messaging:



Linear

Inefficient



Mesh infrastructure

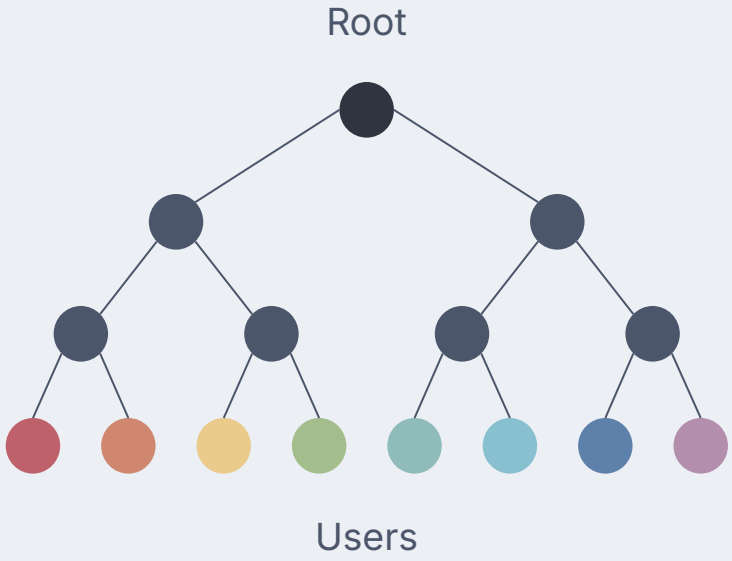
Continuous group key agreement (CGKA)

Continuous group key agreement (CGKA)

Adapted from **TreeKEM** and friends (MLS)

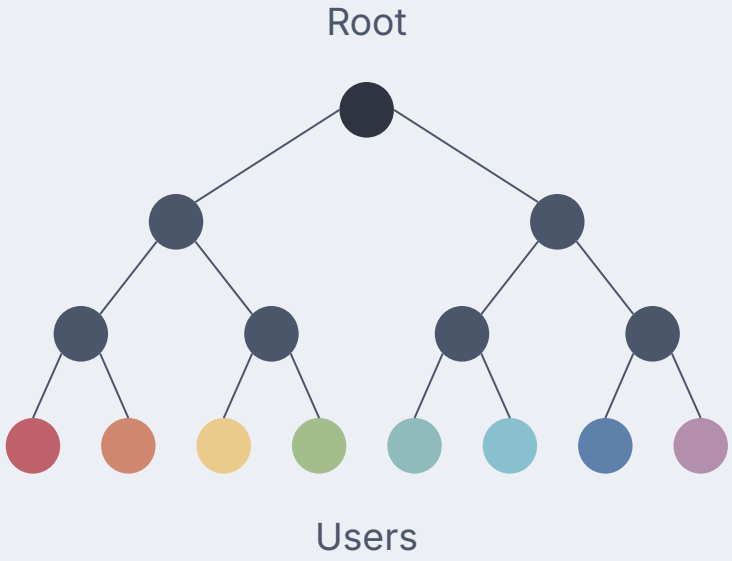
Continuous group key agreement (CGKA)

Adapted from **TreeKEM** and friends (MLS)



Continuous group key agreement (CGKA)

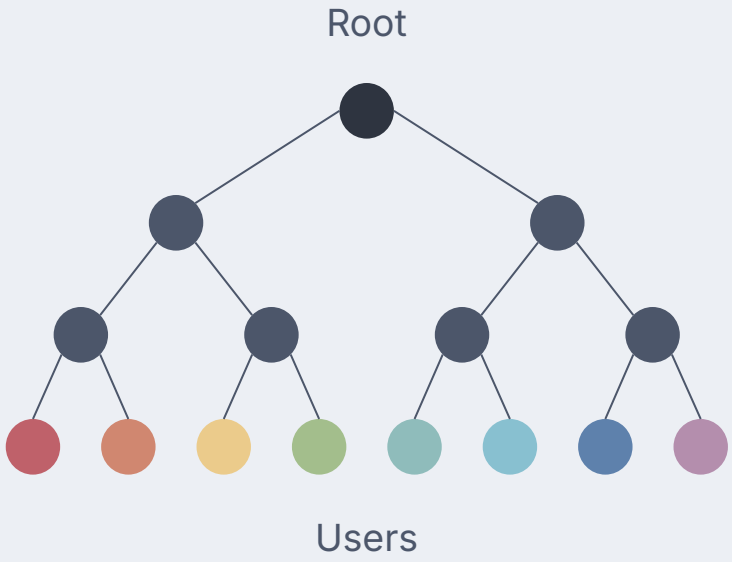
Adapted from **TreeKEM** and friends (MLS)



- Each node in the tree (users and intermediaries) has a (*pk*, *sk*) pair

Continuous group key agreement (CGKA)

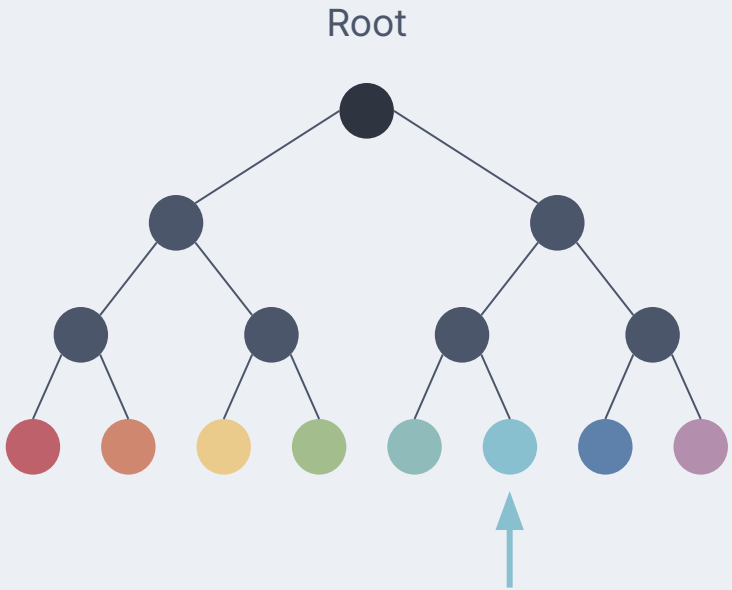
Adapted from **TreeKEM** and friends (MLS)



- Each node in the tree (users and intermediaries) has a (*pk*, *sk*) pair
- Each user only has the key material on its path to the root

Continuous group key agreement (CGKA)

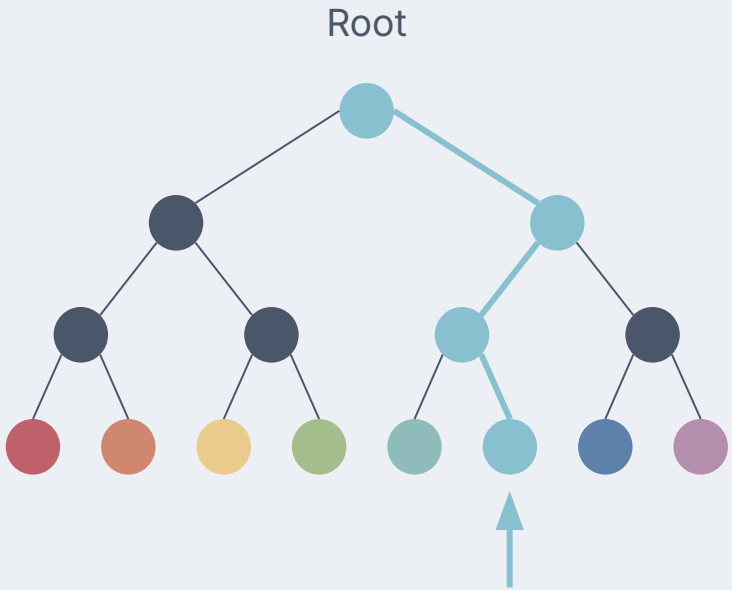
Adapted from **TreeKEM** and friends (MLS)



- Each node in the tree (users and intermediaries) has a (*pk*, *sk*) pair
- Each user only has the key material on its path to the root

Continuous group key agreement (CGKA)

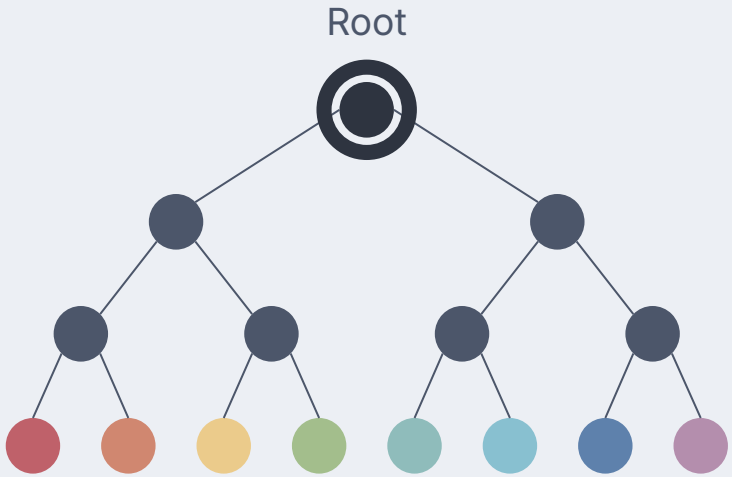
Adapted from **TreeKEM** and friends (MLS)



- Each node in the tree (users and intermediaries) has a (*pk*, *sk*) pair
- Each user only has the key material on its path to the root

Continuous group key agreement (CGKA)

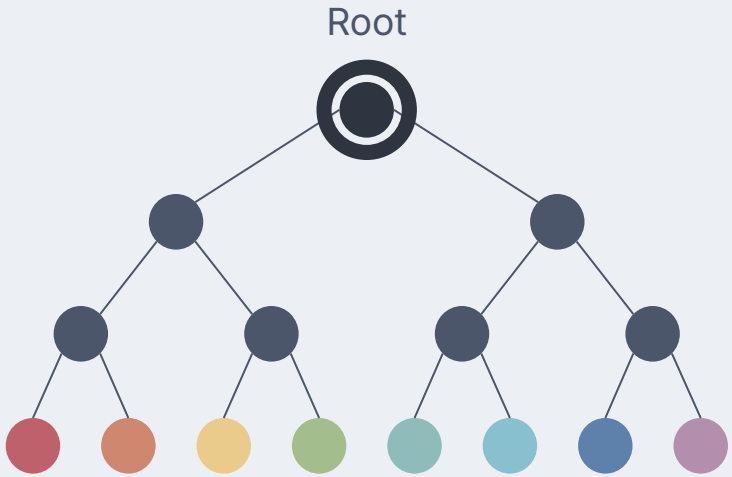
Adapted from **TreeKEM** and friends (MLS)



- Each node in the tree (users and intermediaries) has a (*pk*, *sk*) pair
- Each user only has the key material on its path to the root
- During normal communication, you can send a message to the whole group using the root

Continuous group key agreement (CGKA)

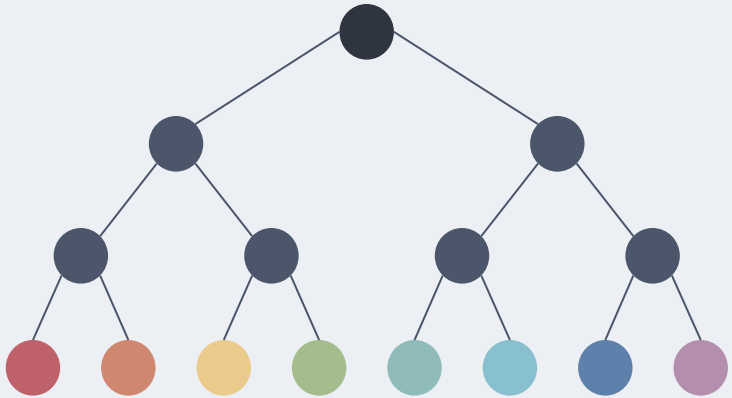
Adapted from **TreeKEM** and friends (MLS)



- Each node in the tree (users and intermediaries) has a (*pk*, *sk*) pair
- Each user only has the key material on its path to the root
- During normal communication, you can send a message to the whole group using the root
  - Conserves mesh bandwidth

Continuous group key agreement (CGKA)

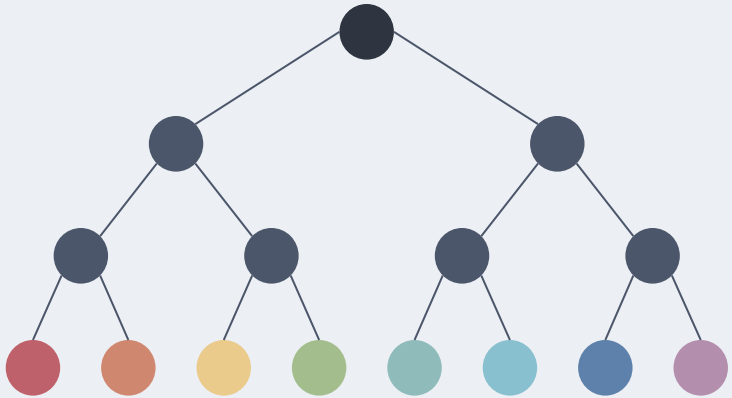
Adapted from **TreeKEM** and friends (MLS)



- Tree structure lends itself to efficient *state operations*

Continuous group key agreement (CGKA)

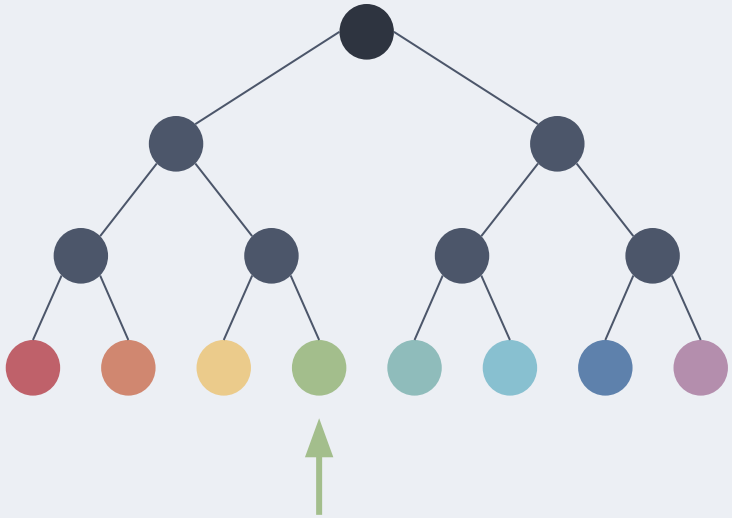
Adapted from **TreeKEM** and friends (MLS)



- Tree structure lends itself to efficient *state operations*
  - Most relevant during a protest: *revocation* from the group

Continuous group key agreement (CGKA)

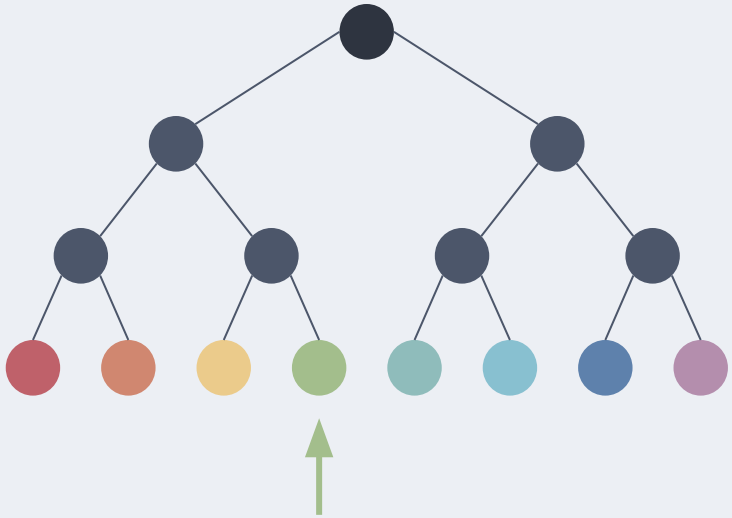
Adapted from **TreeKEM** and friends (MLS)



- Tree structure lends itself to efficient *state operations*
  - Most relevant during a protest: *revocation* from the group

Continuous group key agreement (CGKA)

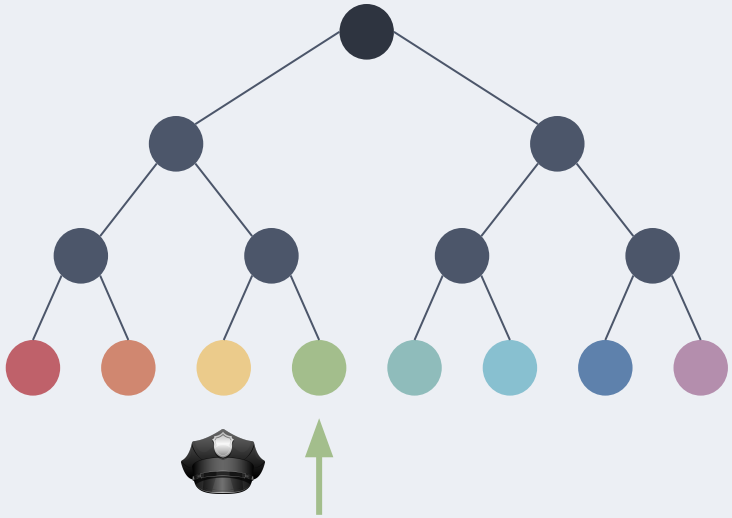
Adapted from **TreeKEM** and friends (MLS)



- Tree structure lends itself to efficient *state operations*
  - Most relevant during a protest: *revocation* from the group
- Suppose you identify that a friend has been arrested by the regime

Continuous group key agreement (CGKA)

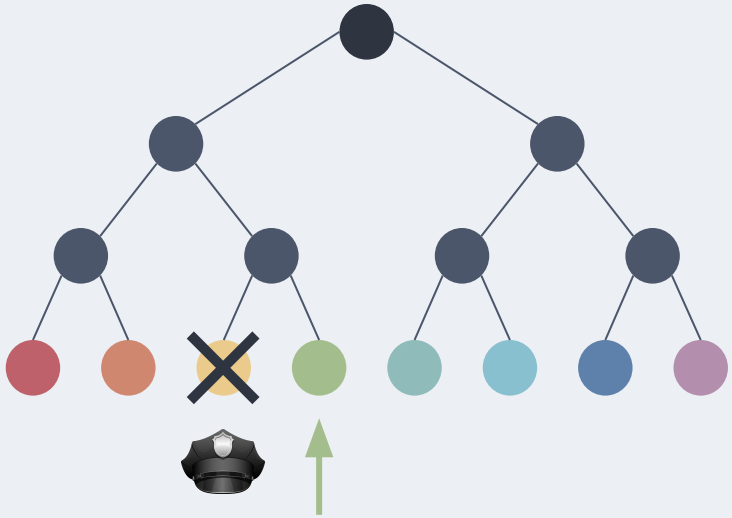
Adapted from **TreeKEM** and friends (MLS)



- Tree structure lends itself to efficient *state operations*
  - Most relevant during a protest: *revocation* from the group
- Suppose you identify that a friend has been arrested by the regime

Continuous group key agreement (CGKA)

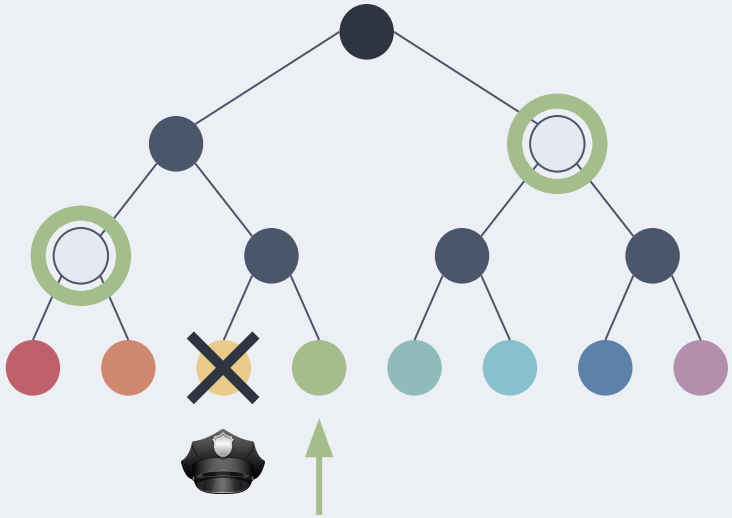
Adapted from **TreeKEM** and friends (MLS)



- Tree structure lends itself to efficient *state operations*
  - Most relevant during a protest: *revocation* from the group
- Suppose you identify that a friend has been arrested by the regime
  - Their phone is now *compromised*, including any secret state

Continuous group key agreement (CGKA)

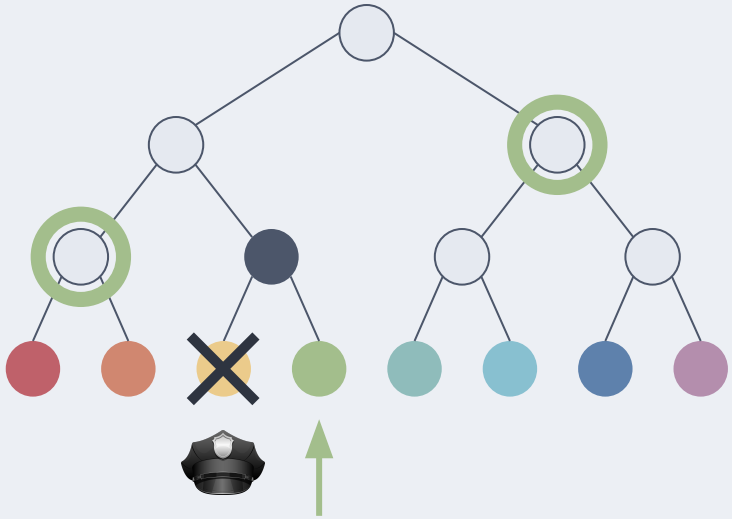
Adapted from **TreeKEM** and friends (MLS)



- Tree structure lends itself to efficient *state operations*
  - Most relevant during a protest: *revocation* from the group
- Suppose you identify that a friend has been arrested by the regime
  - Their phone is now *compromised*, including any secret state
- You can send state updates to *exclude* the compromised user

Continuous group key agreement (CGKA)

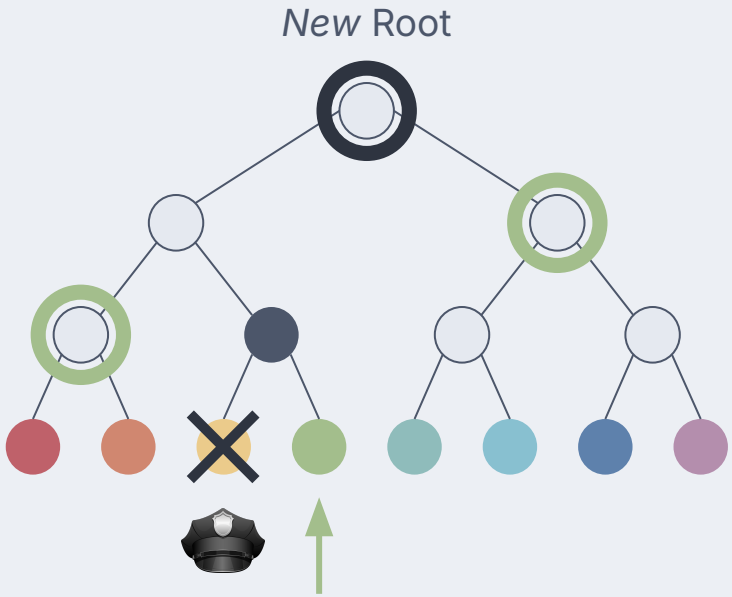
Adapted from **TreeKEM** and friends (MLS)



- Tree structure lends itself to efficient *state operations*
  - Most relevant during a protest: *revocation* from the group
- Suppose you identify that a friend has been arrested by the regime
  - Their phone is now *compromised*, including any secret state
- You can send state updates to *exclude* the compromised user
- New secret material propagates through the tree

Continuous group key agreement (CGKA)

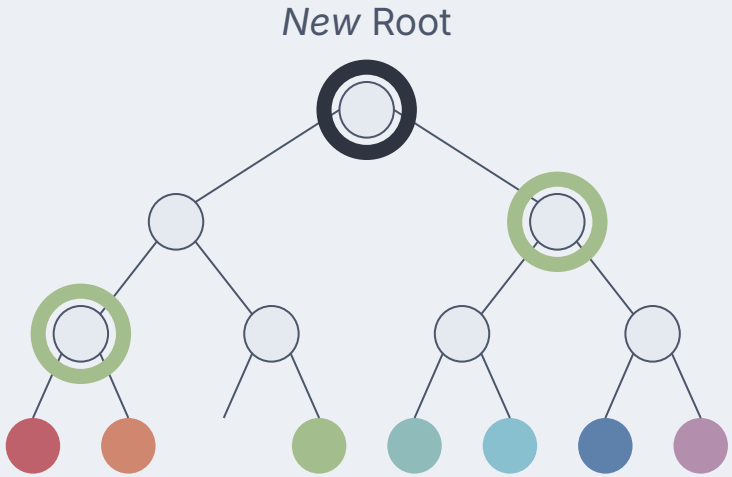
Adapted from **TreeKEM** and friends (MLS)



- Tree structure lends itself to efficient *state operations*
  - Most relevant during a protest: *revocation* from the group
- Suppose you identify that a friend has been arrested by the regime
  - Their phone is now *compromised*, including any secret state
- You can send state updates to *exclude* the compromised user
- New secret material propagates through the tree

Continuous group key agreement (CGKA)

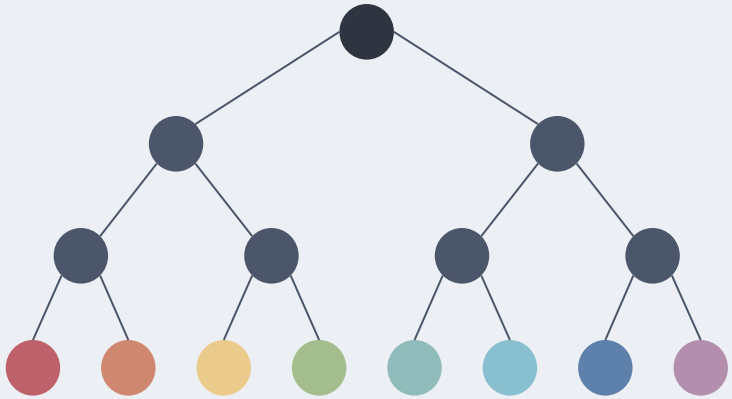
Adapted from **TreeKEM** and friends (MLS)



- Tree structure lends itself to efficient *state operations*
  - Most relevant during a protest: *revocation* from the group
- Suppose you identify that a friend has been arrested by the regime
  - Their phone is now *compromised*, including any secret state
- You can send state updates to *exclude* the compromised user
- New secret material propagates through the tree

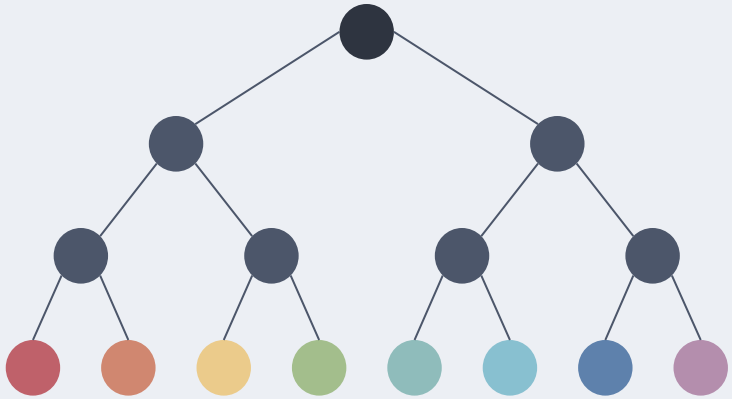
Continuous group key agreement (CGKA)

Adapted from **TreeKEM** and friends (MLS)



Continuous group key agreement (CGKA)

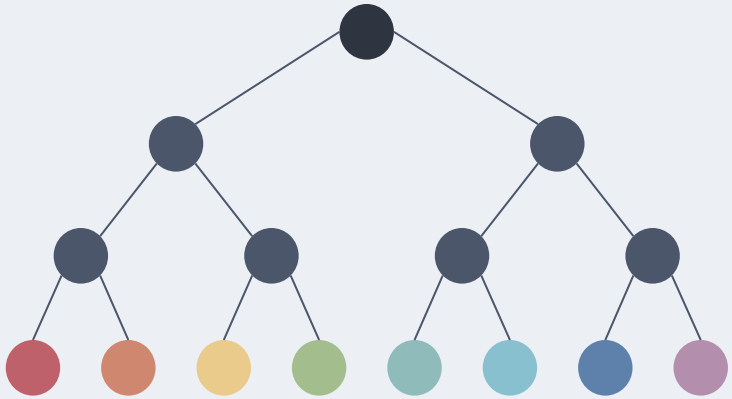
Adapted from **TreeKEM** and friends (MLS)



- Support for **concurrent state operations** on the CGKA tree

Continuous group key agreement (CGKA)

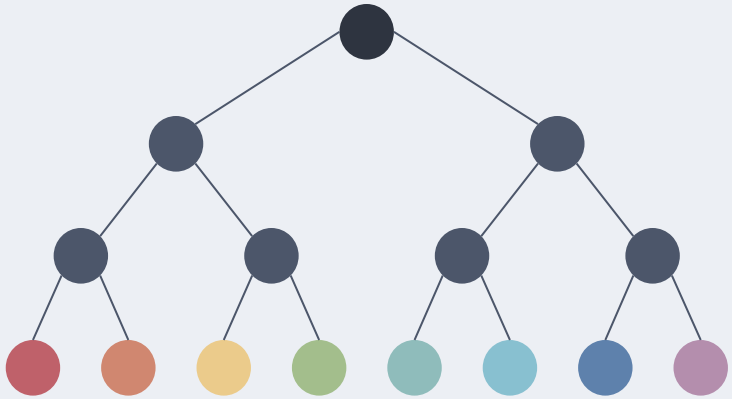
Adapted from **TreeKEM** and friends (MLS)



- Support for **concurrent state operations** on the CGKA tree
- Updatable public key encryption to provide better **forward secrecy** and **post-compromise security** guarantees

Continuous group key agreement (CGKA)

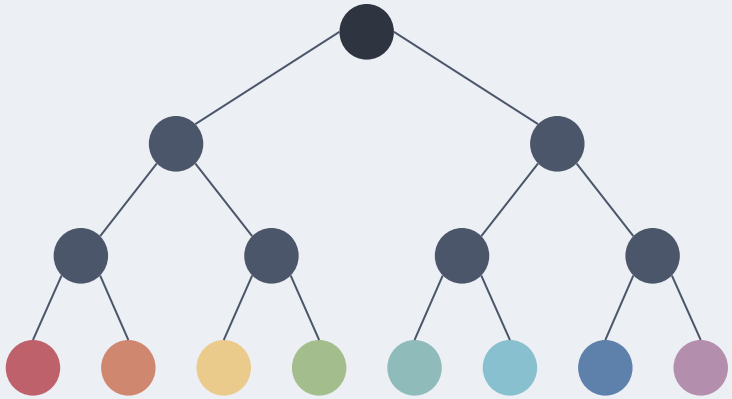
Adapted from **TreeKEM** and friends (MLS)



- Support for **concurrent state operations** on the CGKA tree
- Updatable public key encryption to provide better **forward secrecy** and **post-compromise security** guarantees
- Works in the model of **outsider anonymity** rather than full anonymity

Continuous group key agreement (CGKA)

Adapted from **TreeKEM** and friends (MLS)

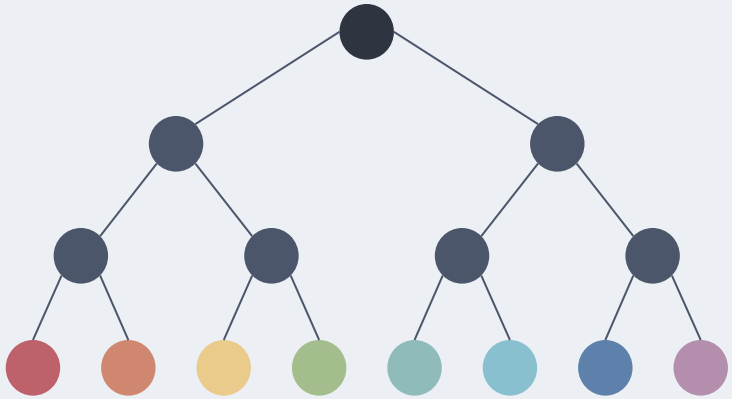


- Support for **concurrent state operations** on the CGKA tree
- Updatable public key encryption to provide better **forward secrecy** and **post-compromise security** guarantees
- Works in the model of **outsider anonymity** rather than full anonymity

Amigo

Continuous group key agreement (CGKA)

Adapted from **TreeKEM** and friends (MLS)



- Support for **concurrent state operations** on the CGKA tree
- Updatable public key encryption to provide better **forward secrecy** and **post-compromise security** guarantees
- Works in the model of **outsider anonymity** rather than full anonymity

Amigo

Read our paper for details!

Ideal world crypto


~~Ideal world crypto~~

Real world crypto

Real world crypto

How can we be sure Amigo works when deployed in the real world?

Real world crypto

How can we be sure Amigo works when deployed in the real world?

Real world crypto

How can we be sure Amigo works when deployed in the real world?

Microbenchmarks aren't enough!

Real world crypto

How can we be sure Amigo works when deployed in the real world?

Microbenchmarks aren't enough!

We can't collect protest data!

Real world crypto

How can we be sure Amigo works when deployed in the real world?

Microbenchmarks aren't enough!

We can't collect protest data!

Representative simulations

Question 1

Question 1

How do we simulate protester movements?

Question 1

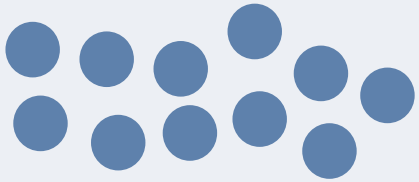
How do we simulate protester movements?

Modeling of **node dynamics** impacts mesh behavior

Question 1

How do we simulate protester movements?

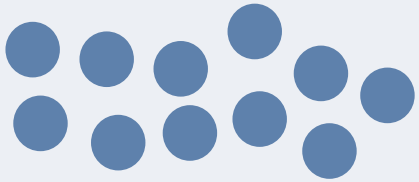
Modeling of **node dynamics** impacts mesh behavior



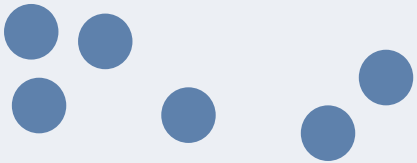
Question 1

How do we simulate protester movements?

Modeling of **node dynamics** impacts mesh behavior



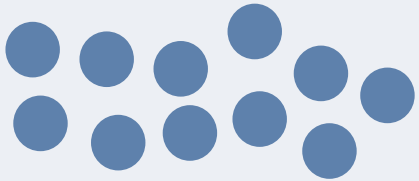
versus



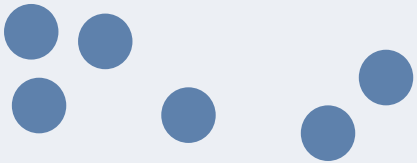
Question 1

How do we simulate protester movements?

Modeling of **node dynamics** impacts mesh behavior



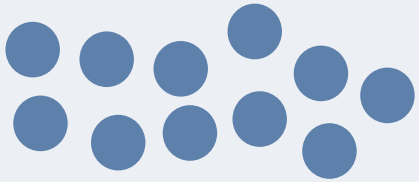
versus



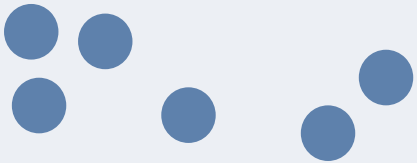
Question 1

How do we simulate protester movements?

Modeling of **node dynamics** impacts mesh behavior



versus



Search | Free Newsletters QUARTZ Editions

HOME LATEST BUSINESS NEWS MONEY & MARKETS TECH & INNOVATION A.I. LIFESTYLE LEADERSHIP

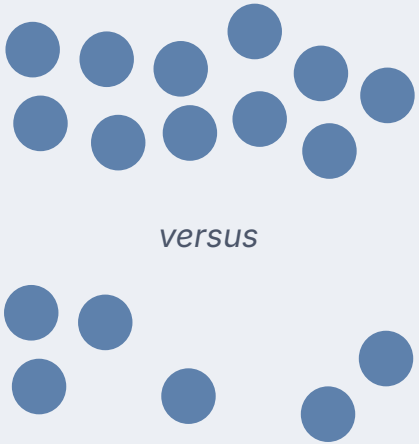
ECONOMIC INDICATORS

Hong Kongers crowdsourced a protest manual—and Myanmar's already using it

Question 1

How do we simulate protester movements?

Modeling of **node dynamics** impacts mesh behavior



versus

Search | Free Newsletters | QUARTZ | Editions

HOME LATEST BUSINESS NEWS MONEY & MARKETS TECH & INNOVATION A.I. LIFESTYLE LEADERSHIP

ECONOMIC INDICATORS

Hong Kongers crowdsourced a protest manual—and Myanmar's already using it

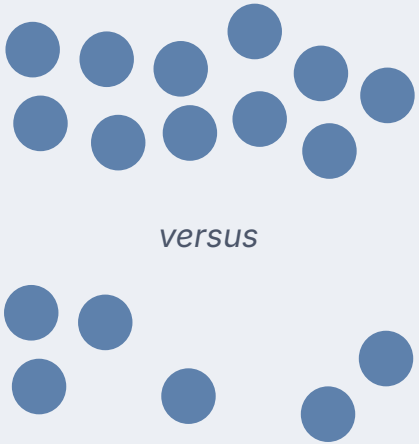
Marches on the street are visible, but not the only kind of protest possible. There can be

1. assemblies with speeches,
2. gatherings with specific focus
    a. Communal art, like preparing paper cranes or other origami
    b. Location art, like decorating Lennon Walls
    c. Music performances (with crowd participation)
3. Flash mobs
4. Human chain (the HK way, echoing the Baltic Way in the Soviet days)
5. Blockades (e.g., major highways with vehicles/objects)

Question 1

How do we simulate protester movements?

Modeling of **node dynamics** impacts mesh behavior



versus

Search | Free Newsletters | QUARTZ | Editions

HOME LATEST BUSINESS NEWS MONEY & MARKETS TECH & INNOVATION A.I. LIFESTYLE LEADERSHIP

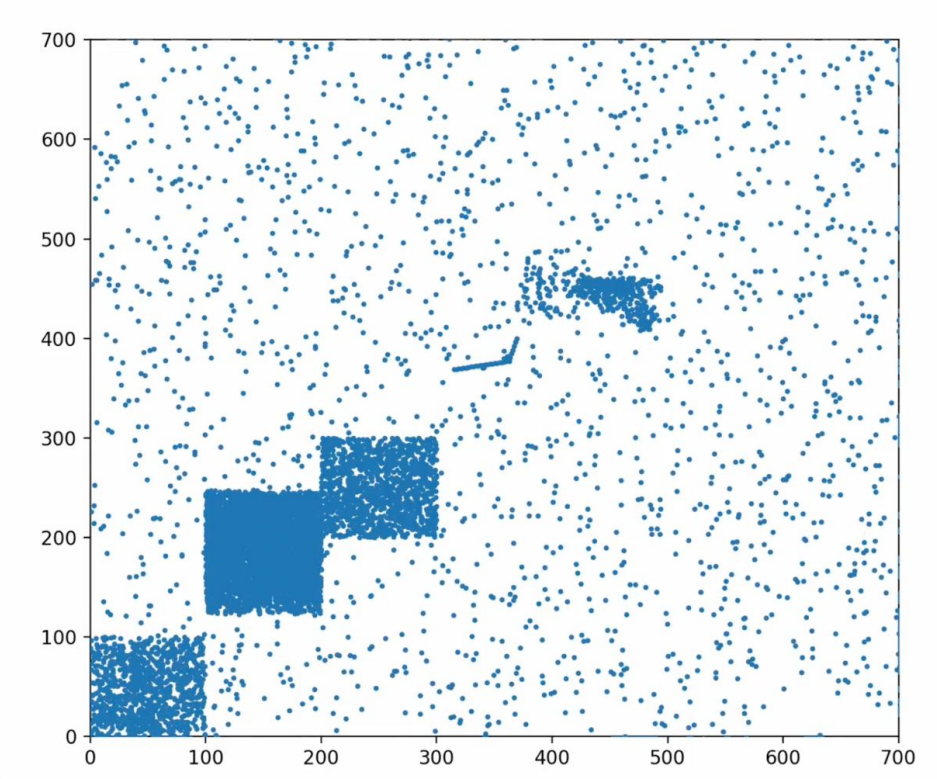
ECONOMIC INDICATORS

Hong Kongers crowdsourced a protest manual—and Myanmar's already using it

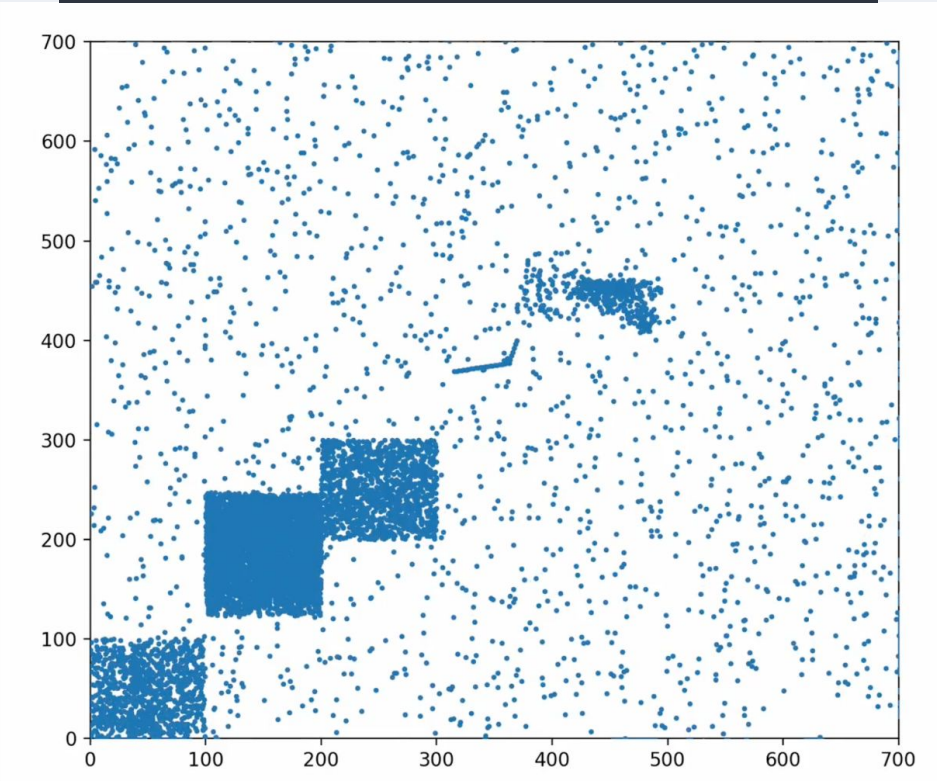
Marches on the street are visible, but not the only kind of protest possible. There can be

1. assemblies with speeches,
2. gatherings with specific focus
   a. Communal art, like preparing paper cranes or other origami
   b. Location art, like decorating Lennon Walls
   c. Music performances (with crowd participation)
3. Flash mobs
4. Human chain (the HK way, echoing the Baltic Way in the Soviet days)
5. Blockades (e.g., major highways with vehicles/objects)

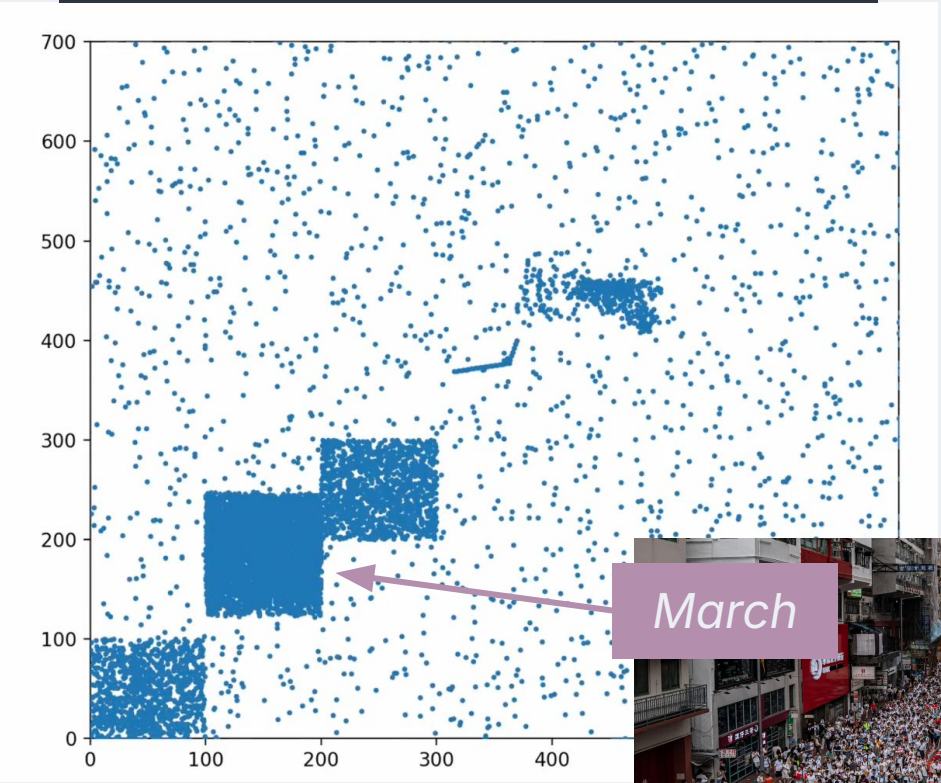
Develop **representative mobility models** based on HK19!


700
600
500
400
300
200
100
0
0
100
200
300
400
500
600
700

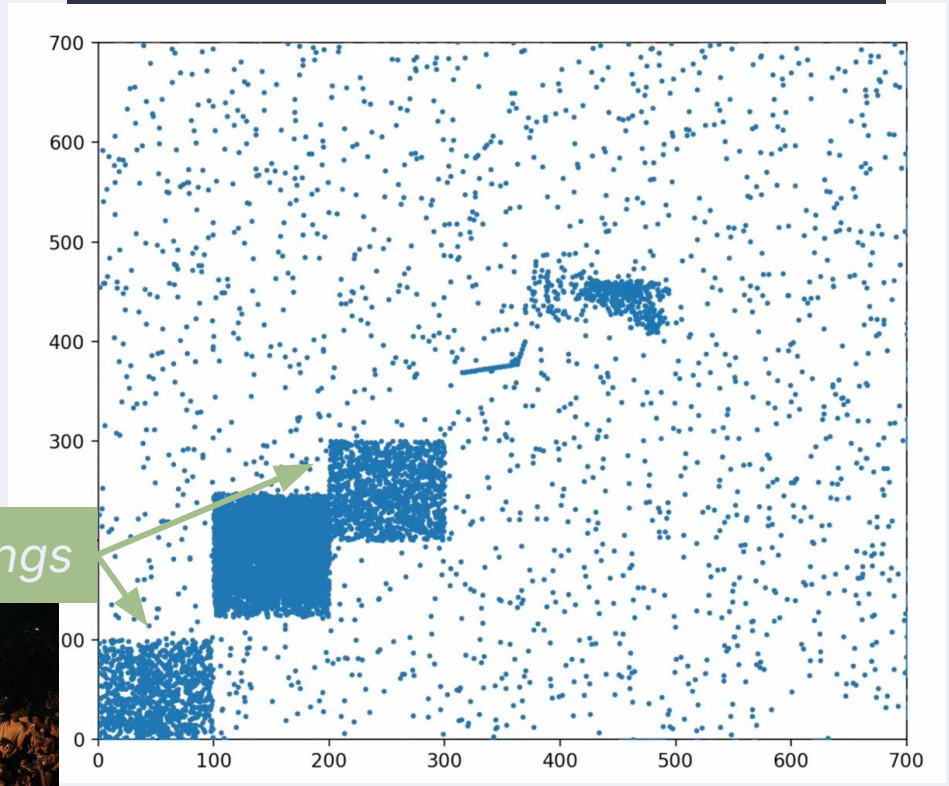
Urban protest mobility simulator



Urban protest mobility simulator

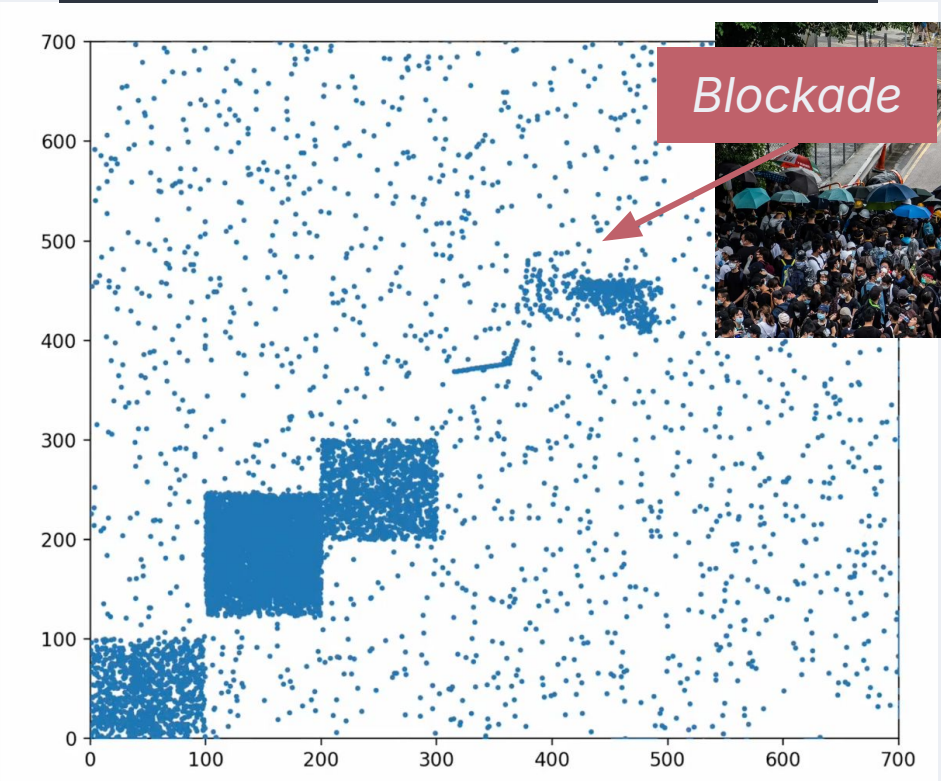


Urban protest mobility simulator



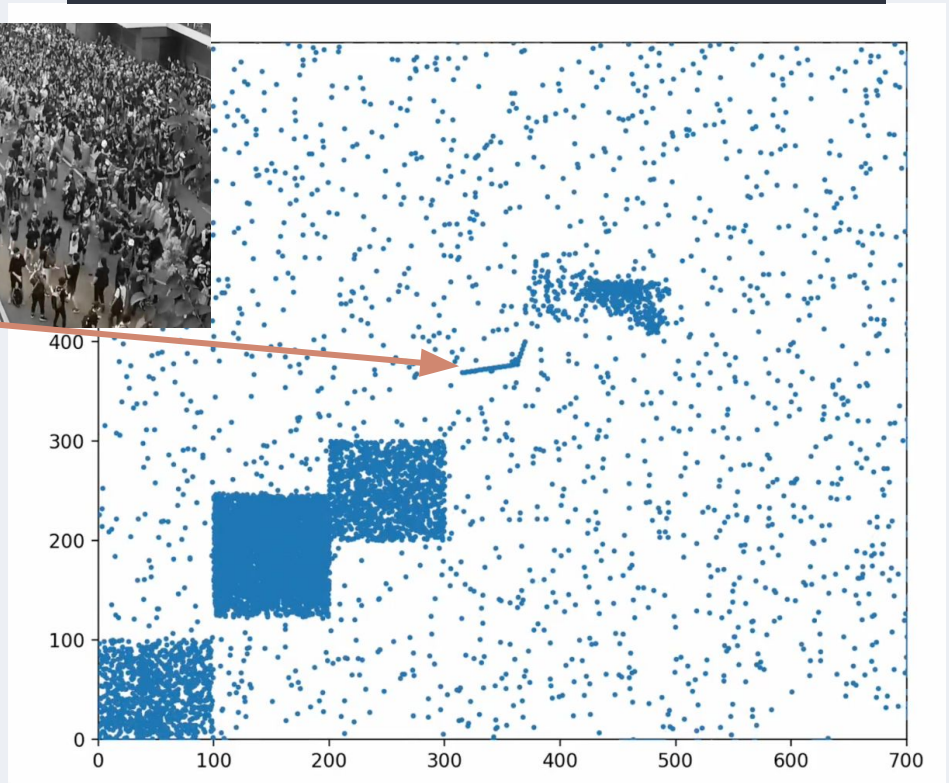
Gatherings

Urban protest mobility simulator



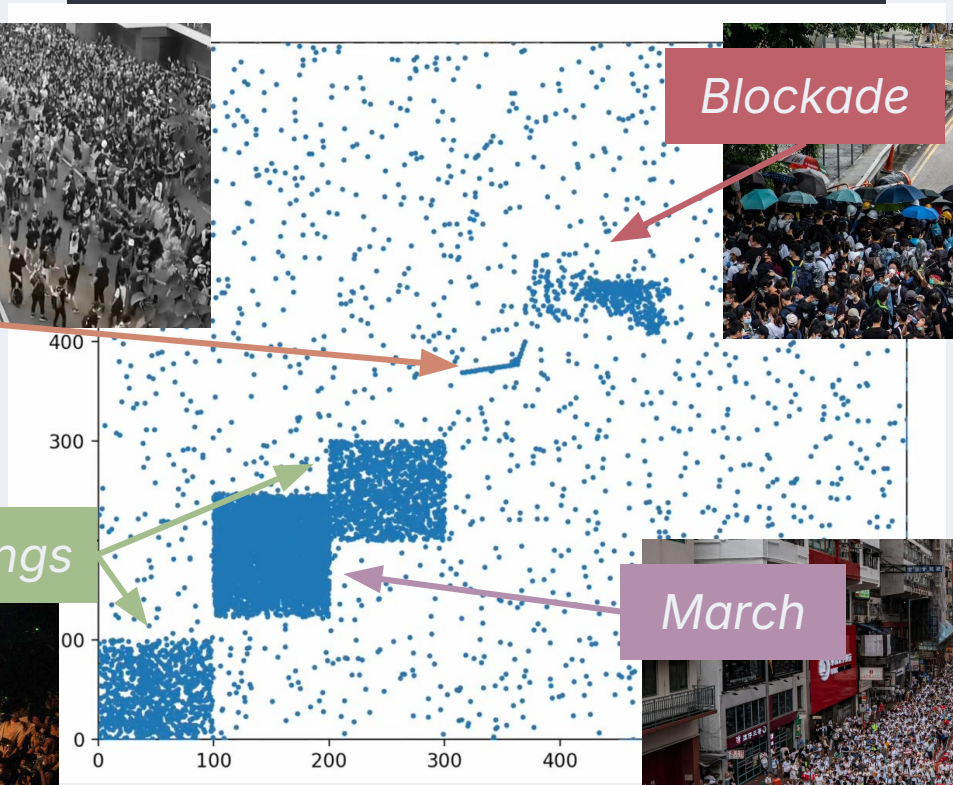
Urban protest mobility simulator

Human chain



Urban protest mobility simulator

Human chain



Blockade

Gatherings

March

Question 2

Question 2

How do we simulate mesh communication?

Question 2

How do we simulate mesh communication?

OSI reference model:

Question 2

How do we simulate mesh communication?

OSI reference model:

7. **Application** layer
6. **Presentation** layer
5. **Session** layer
4. **Transport** layer
3. **Network** layer
2. **Data link** layer
1. **Physical** layer

Question 2

How do we simulate mesh communication?

OSI reference model:

7. **Application** layer
6. **Presentation** layer
5. **Session** layer
4. **Transport** layer
3. **Network** layer
2. **Data link** layer
1. **Physical** layer

Previous mesh messaging works focus on simulating these layers ...

Question 2

How do we simulate mesh communication?

OSI reference model:

7. **Application** layer
6. **Presentation** layer
5. **Session** layer
4. **Transport** layer
3. **Network** layer
2. **Data link** layer
1. **Physical** layer

Previous mesh messaging works focus on simulating these layers ...

Question 2

How do we simulate mesh communication?

OSI reference model:

7. **Application** layer
6. **Presentation** layer
5. **Session** layer
4. **Transport** layer
3. **Network** layer
2. **Data link** layer
1. **Physical** layer

Previous mesh messaging works focus on simulating these layers ...

Question 2

How do we simulate mesh communication?

OSI reference model:

7. **Application** layer
6. **Presentation** layer
5. **Session** layer
4. **Transport** layer
3. **Network** layer
2. **Data link** layer
1. **Physical** layer

Previous mesh messaging works focus on simulating these layers ...

Question 2

How do we simulate mesh communication?

OSI reference model:

7. **Application** layer
6. **Presentation** layer
5. **Session** layer
4. **Transport** layer
3. **Network** layer
2. **Data link** layer
1. **Physical** layer

Previous mesh messaging works focus on simulating these layers ...

... so lower layers are relatively understudied!

Question 2

How do we simulate mesh communication?

OSI reference model:

7. **Application** layer
6. **Presentation** layer
5. **Session** layer
4. **Transport** layer
3. **Network** layer
2. **Data link** layer
1. **Physical** layer

Previous mesh messaging works focus on simulating these layers ...

... so lower layers are relatively understudied!

Question 2

How do we simulate mesh communication?

OSI reference model:

7. **Application** layer
6. **Presentation** layer
5. **Session** layer
4. **Transport** layer
3. **Network** layer
2. **Data link** layer
1. **Physical** layer

Previous mesh messaging works focus on simulating these layers ...

... so lower layers are relatively understudied!

Question 2

How do we simulate mesh communication?

Question 2

How do we simulate mesh communication?

Question 2

How do we simulate mesh communication?

Discrete-event simulator

Question 2

How do we simulate mesh communication?

Discrete-event simulator

- Standard for evaluations in networks/systems

Question 2

How do we simulate mesh communication?

Discrete-event simulator

- Standard for evaluations in networks/systems
- Detailed simulations of every OSI model layer

Question 2

How do we simulate mesh communication?

Discrete-event simulator

- Standard for evaluations in networks/systems
- Detailed simulations of every OSI model layer
- Approach: validate our solution and compare it to prior work

Question 2

How do we simulate mesh communication?

Discrete-event simulator

- Standard for evaluations in networks/systems
- Detailed simulations of every OSI model layer
- Approach: validate our solution and compare it to prior work
- Easy, right?

Question 2

How do we simulate mesh communication?

Discrete-event simulator

- Standard for evaluations in networks/systems
- Detailed simulations of every OSI model layer
- Approach: validate our solution and compare it to prior work
- Easy, right?

No

Question 2

How do we simulate mesh communication?

Discrete-event simulator

- Standard for evaluations in networks/systems
- Detailed simulations of every OSI model layer
- Approach: validate our solution and compare it to prior work
- Easy, right?

No

😔

- ns-3 does not support **Wi-Fi Direct**, so we need to manually implement

Question 2

How do we simulate mesh communication?

Discrete-event simulator

- Standard for evaluations in networks/systems
- Detailed simulations of every OSI model layer
- Approach: validate our solution and compare it to prior work
- Easy, right?

No

😔

- ns-3 does not support **Wi-Fi Direct**, so we need to manually implement

🤑

- Takes **one week** of wall clock time on a high-end GCP instance for one run

Question 2

How do we simulate mesh communication?

Discrete-event simulator

- Standard for evaluations in networks/systems
- Detailed simulations of every OSI model layer
- Approach: validate our solution and compare it to prior work
- Easy, right?

No

😔

- ns-3 does not support **Wi-Fi Direct**, so we need to manually implement

🤑

- Takes **one week** of wall clock time on a high-end GCP instance for one run

  $500 per day!

Question 2

How do we simulate mesh communication?

Discrete-event simulator

- Standard for evaluations in networks/systems
- Detailed simulations of every OSI model layer
- Approach: validate our solution and compare it to prior work
- Easy, right?

No

😔

- ns-3 does not support **Wi-Fi Direct**, so we need to manually implement

🤑

- Takes **one week** of wall clock time on a high-end GCP instance for one run

  $500 per day!

Probably why previous work doesn't include high-fidelity simulations of lower network layers...

Question 2

How do we simulate mesh communication?

ns-3

Discrete-event simulator

- Standard for evaluations in networks/systems
- Detailed simulations of every OSI model layer
- Approach: validate our solution and compare it to prior work
- Easy, right?

No

- ns-3 does not support **Wi-Fi Direct**, so we need to manually implement it

- Takes **one week** of wall clock time on a high-end GCP instance for one run

$500 per day!

But we did it anyway

Probably why previous work doesn't include high-fidelity simulations of lower network layers...

So what did we learn?

So what did we learn?

Existing mesh routing **does not work well** in practice

So what did we learn?

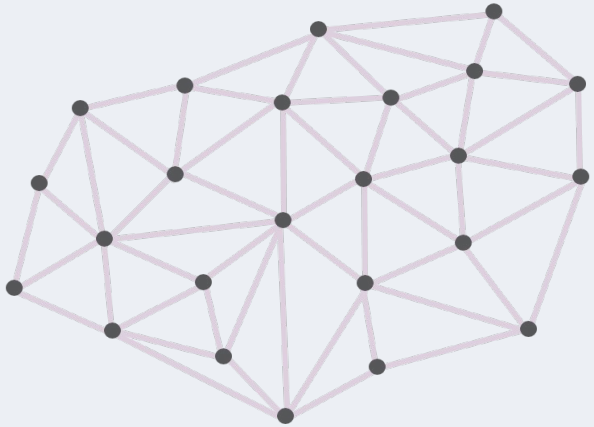
Existing mesh routing **does not work well** in practice

Default: **Epidemic flooding**

So what did we learn?

Existing mesh routing **does not work well** in practice

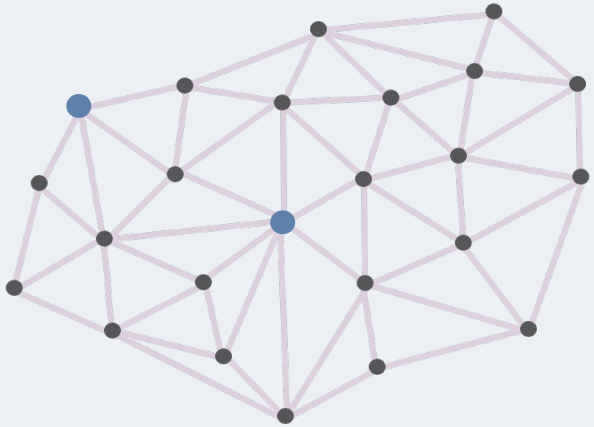
Default: **Epidemic flooding**



So what did we learn?

Existing mesh routing **does not work well** in practice

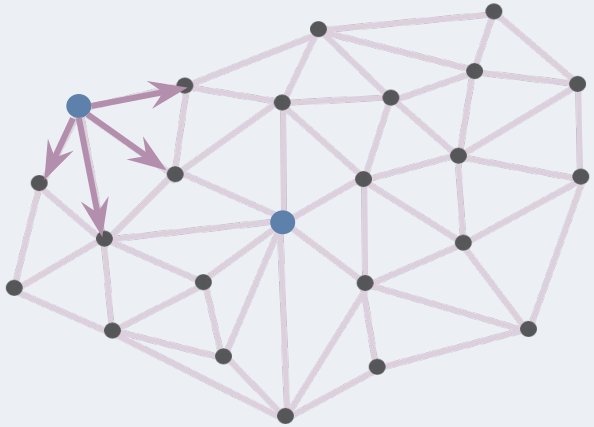
Default: **Epidemic flooding**



So what did we learn?

Existing mesh routing **does not work well** in practice

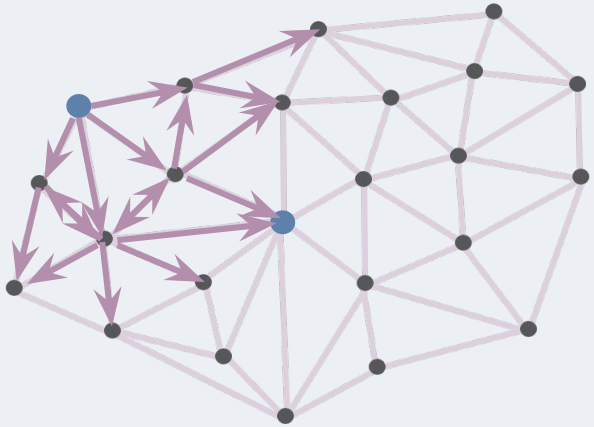
Default: **Epidemic flooding**



So what did we learn?

Existing mesh routing **does not work well** in practice

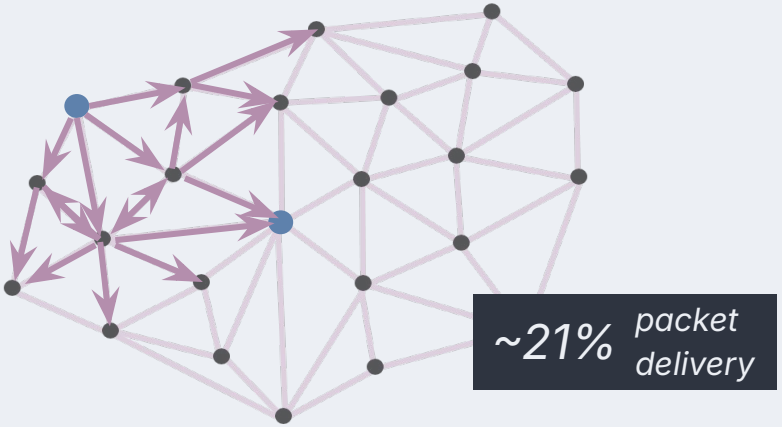
Default: **Epidemic flooding**



So what did we learn?

Existing mesh routing **does not work well** in practice

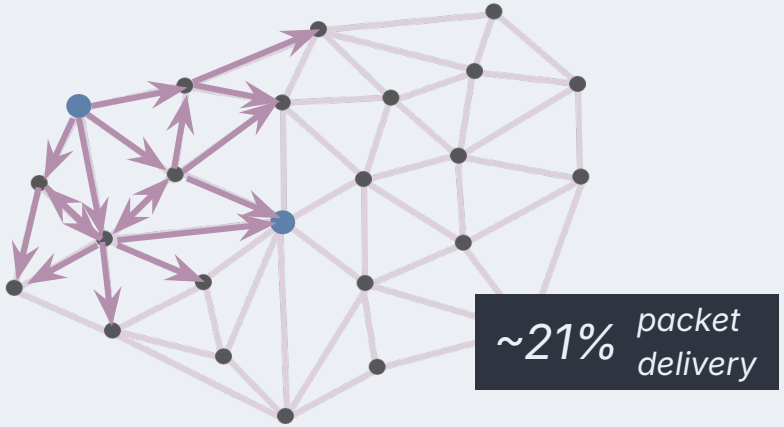
Default: **Epidemic flooding**



So what did we learn?

Existing mesh routing **does not work well** in practice

Default: **Epidemic flooding**

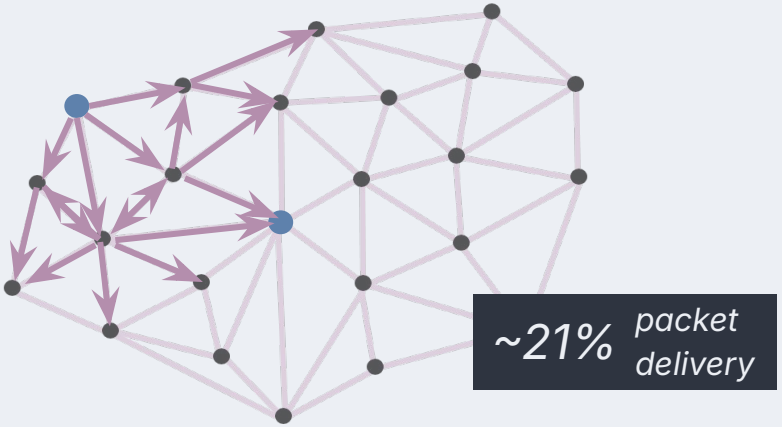


- Conflicting messages collide at Layers 1 & 2

So what did we learn?

Existing mesh routing **does not work well** in practice

Default: **Epidemic flooding**



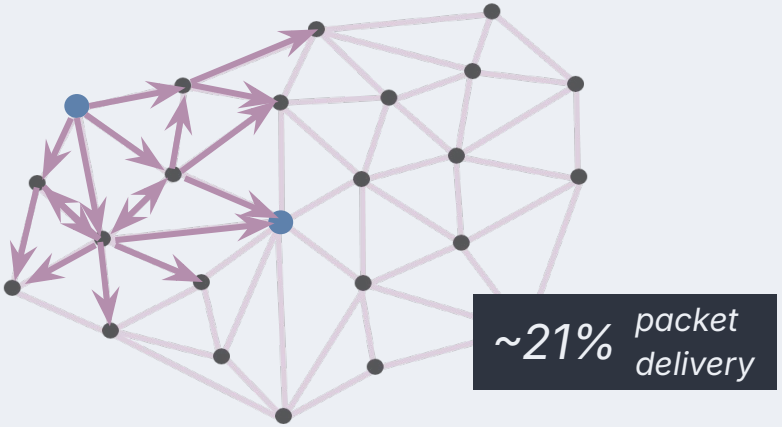
So what did we learn?

Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**

Optimization: **Digest routing**



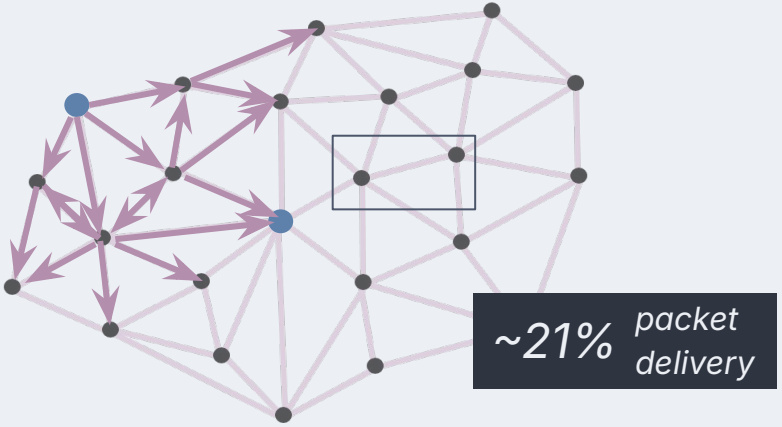
So what did we learn?

Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**

Optimization: **Digest routing**



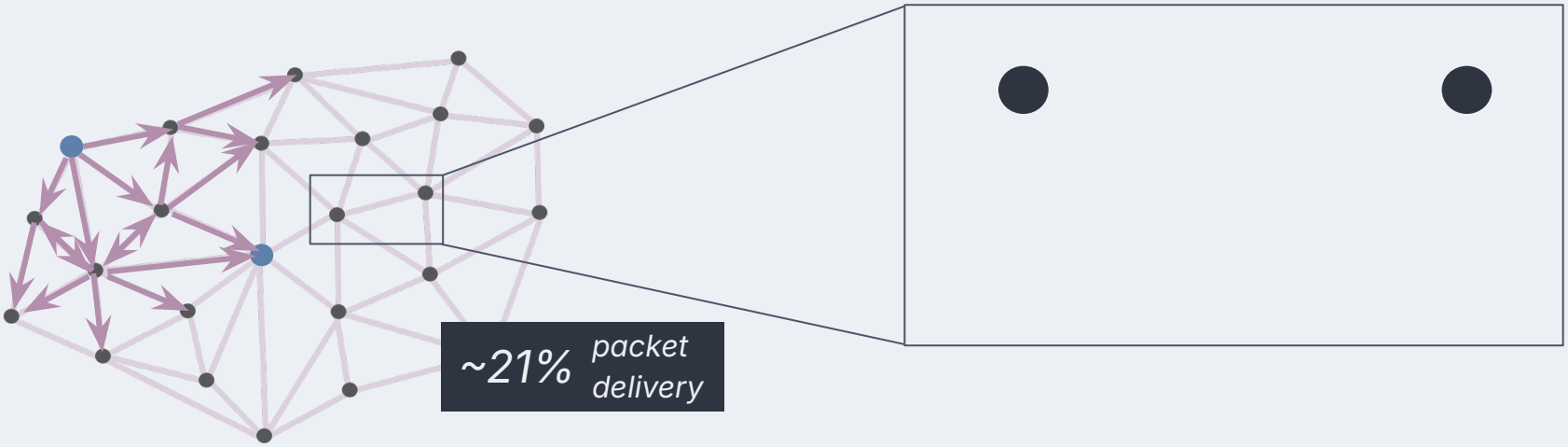
So what did we learn?

Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**

Optimization: **Digest routing**



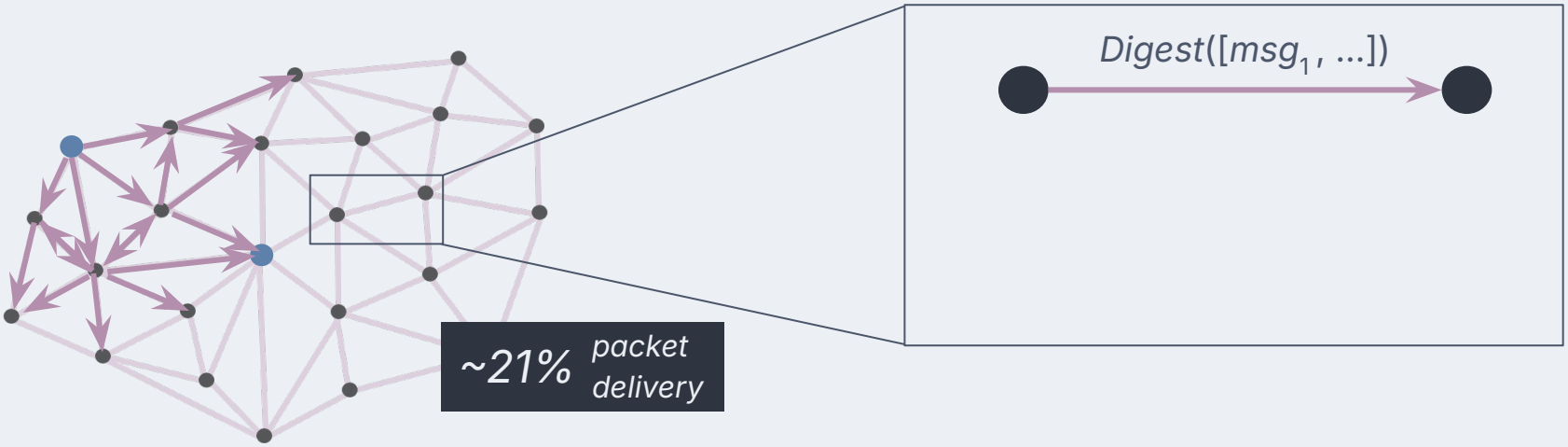
So what did we learn?

Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**

Optimization: **Digest routing**



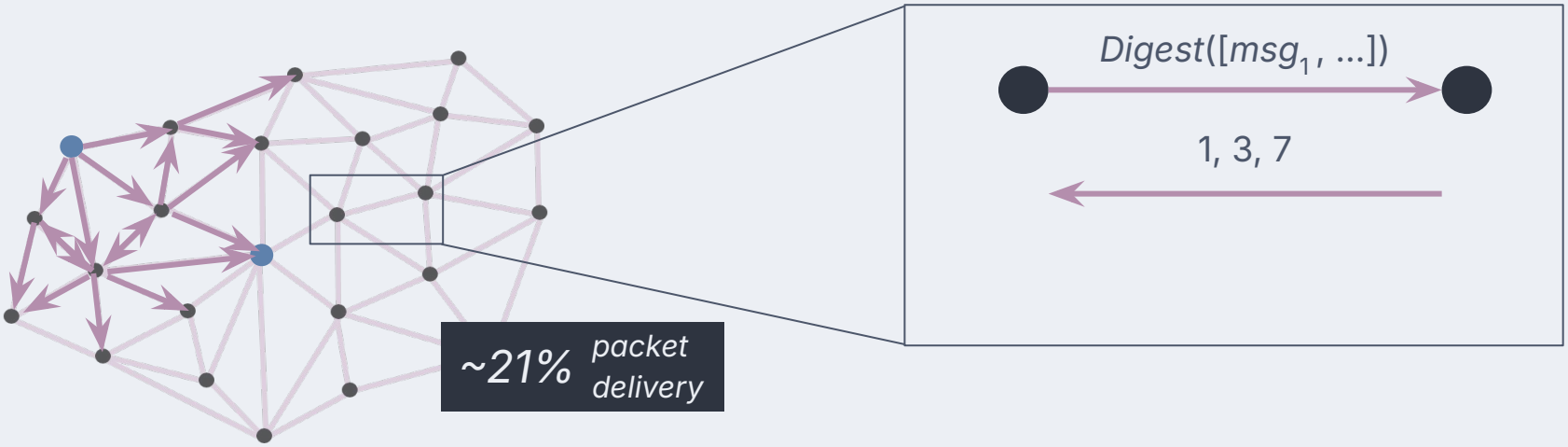
So what did we learn?

Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**

Optimization: **Digest routing**



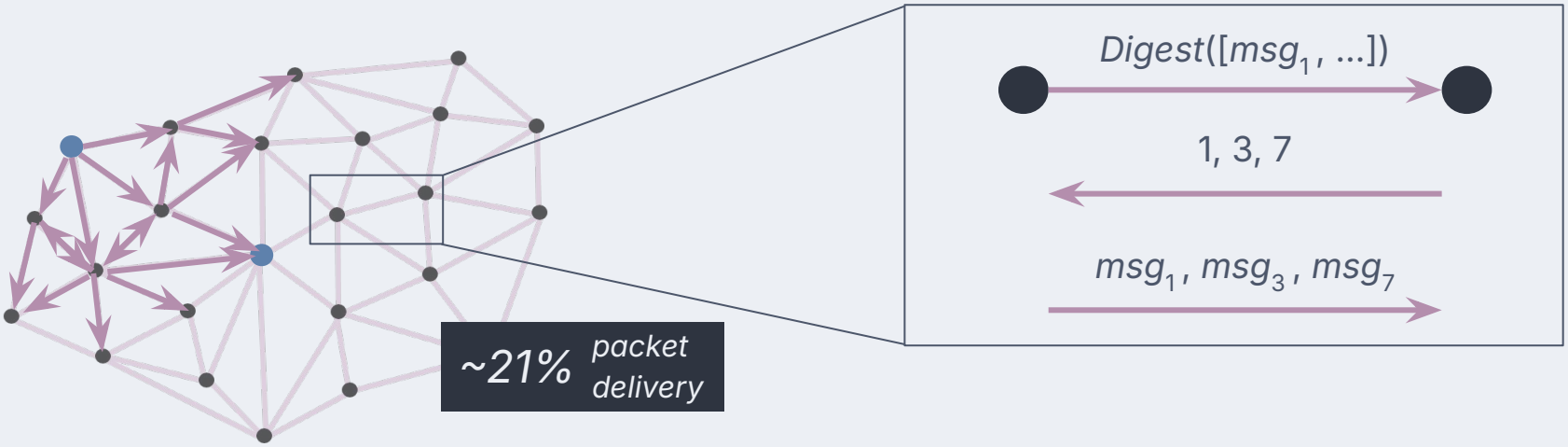
So what did we learn?

Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**

Optimization: **Digest routing**

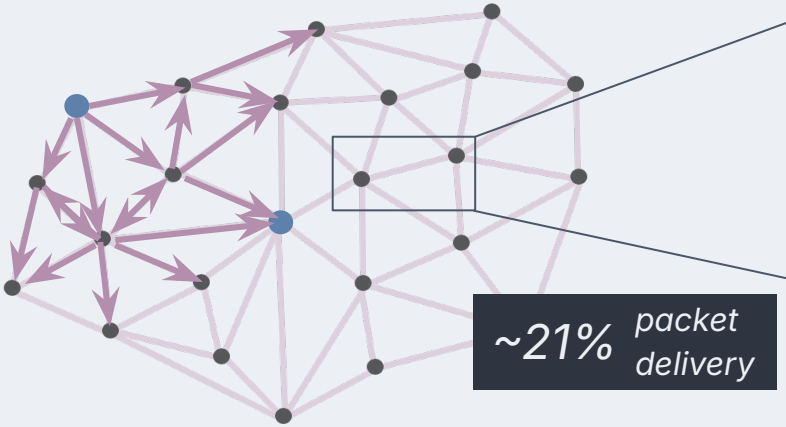


So what did we learn?

Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**



Optimization: **Digest routing**

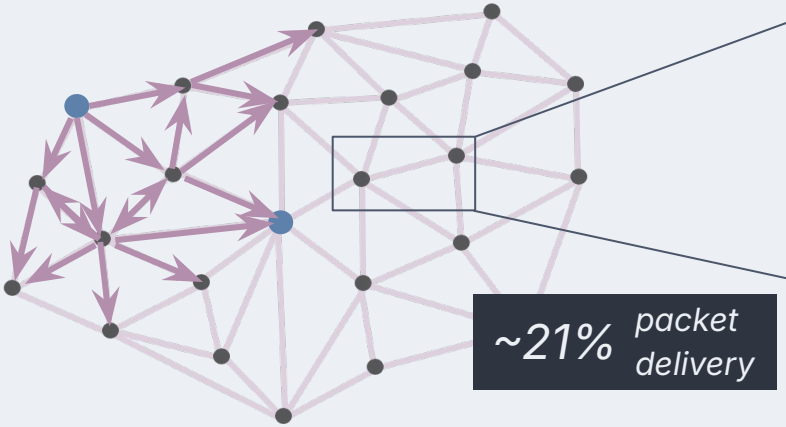
- Reduces number of messages

So what did we learn?

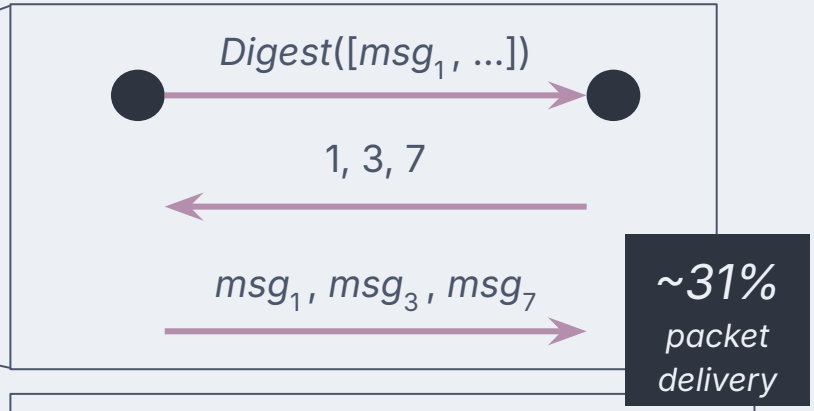
Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**



Optimization: **Digest routing**



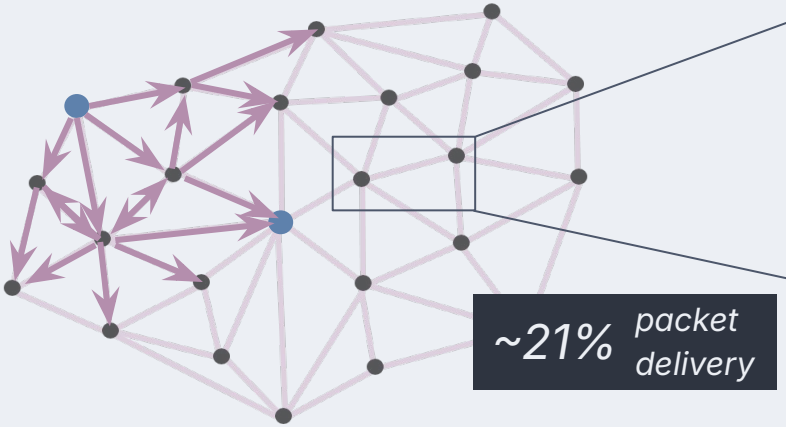
- Reduces number of messages

So what did we learn?

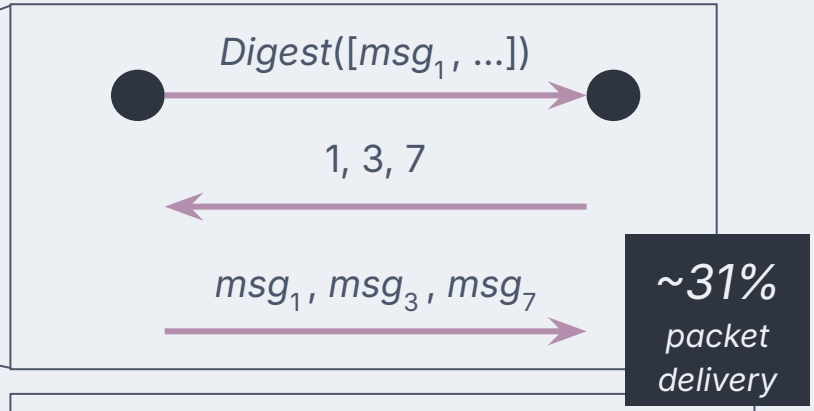
Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**



Optimization: **Digest routing**



- Reduces number of messages
- Conflicting messages *and digests* now collide at Layers 1 & 2

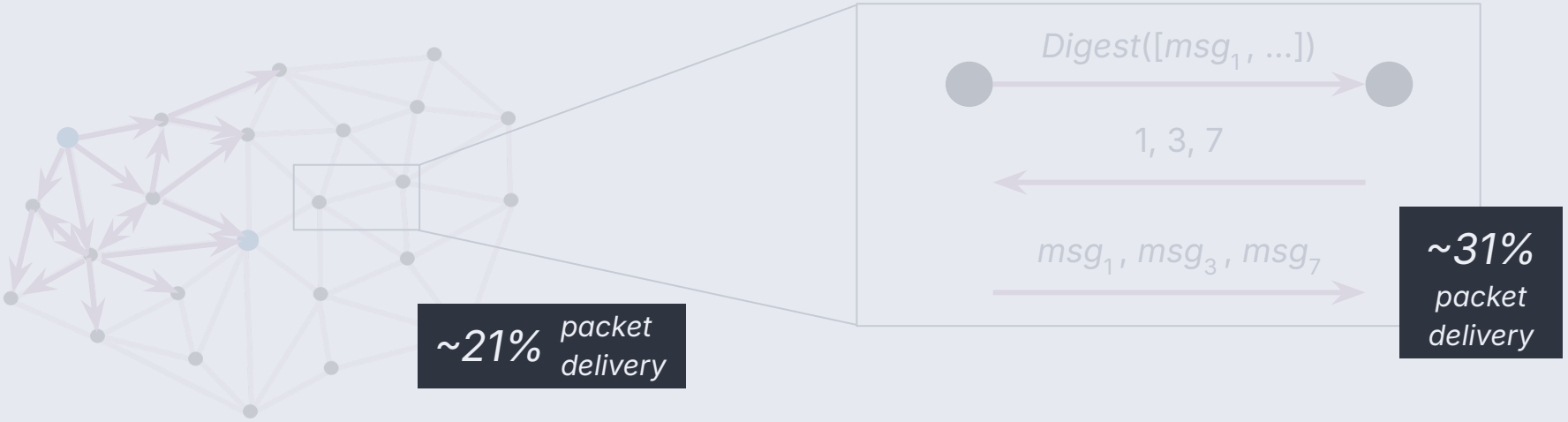
So what did we learn?

Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**

Optimization: **Digest routing**



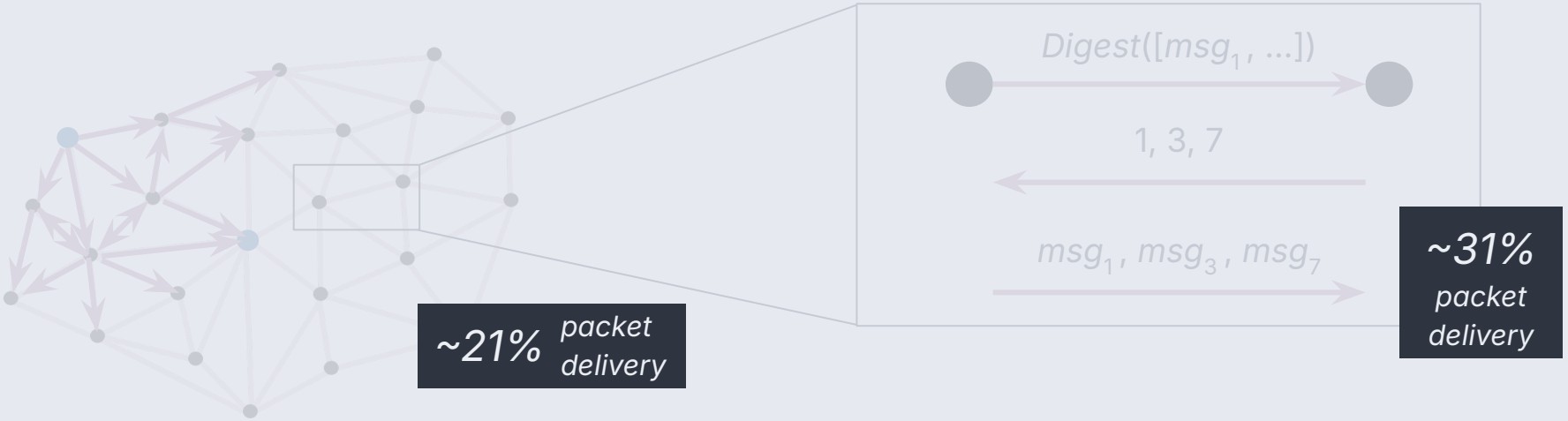
So what did we learn?

Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**

Optimization: **Digest routing**



Much lower than previously assumed!

So what did we learn?

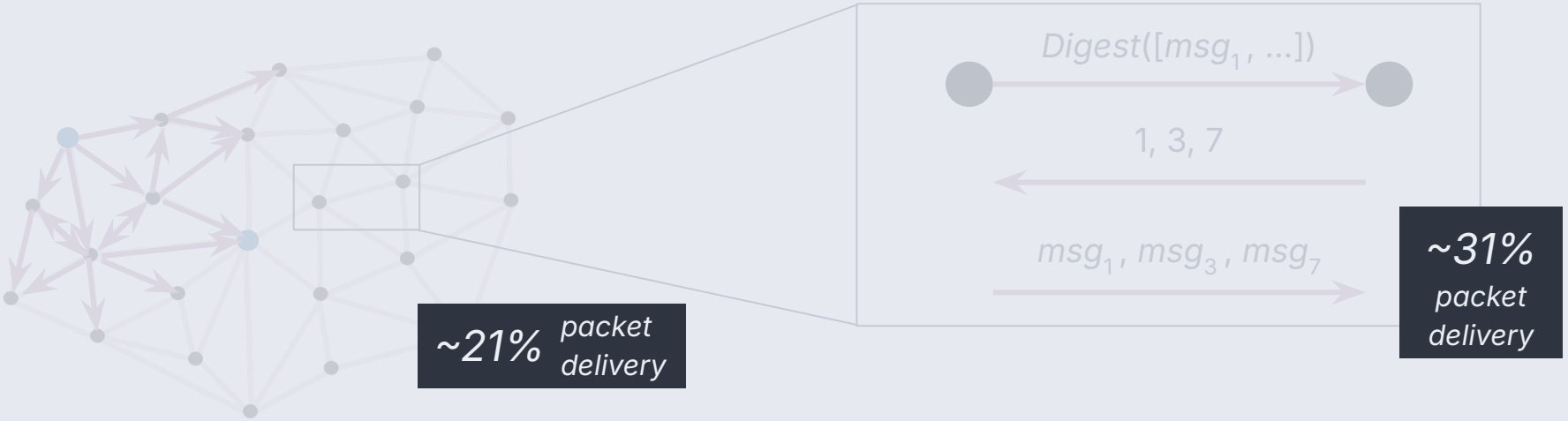
Alternative routing schemes in our paper!

Existing mesh routing **does not work well** in practice

(Perry et al.)

Default: **Epidemic flooding**

Optimization: **Digest routing**



Much lower than previously assumed!

The takeaway?

The takeaway? For mesh messaging in large-scale protests...

The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won’t save us.

The takeaway? For mesh messaging in large-scale protests...

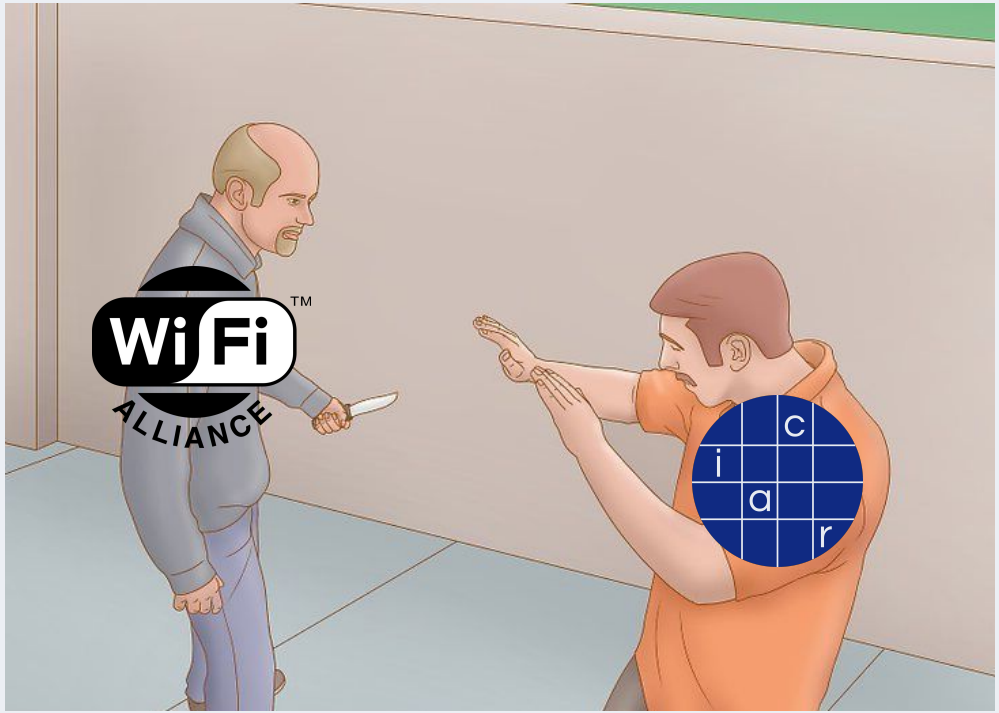
Cryptography alone won't save us.

The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won't save us.

The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won't save us.



The takeaway? For mesh messaging in large-scale protests...

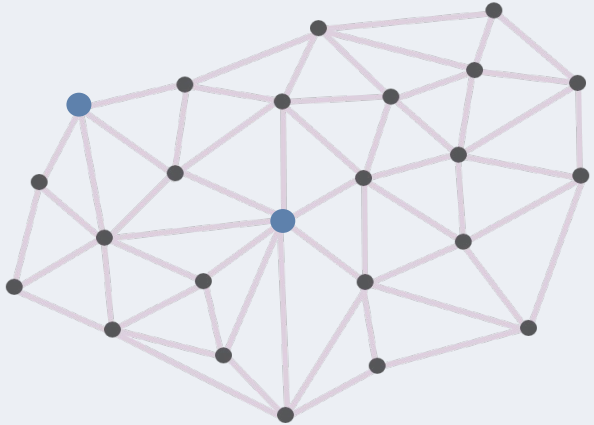
Cryptography alone won’t save us,

The takeaway? For mesh messaging in large-scale protests…

Cryptography alone won’t save us,
so we need more networks & systems research

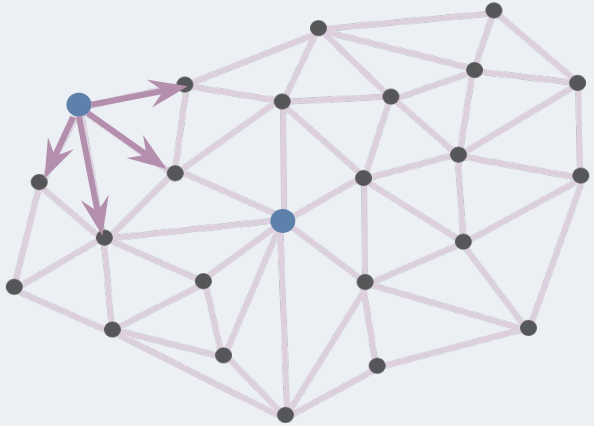
The takeaway? For mesh messaging in large-scale protests…

Cryptography alone won't save us, so we need more networks & systems research



The takeaway? For mesh messaging in large-scale protests…

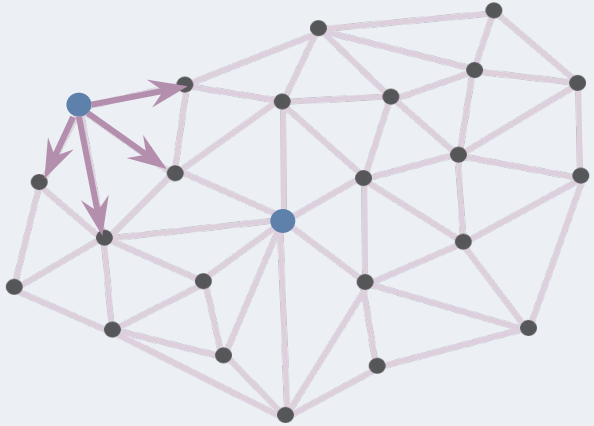
Cryptography alone won't save us, so we need more networks & systems research



- Improved mesh networking algorithms for messaging

The takeaway? For mesh messaging in large-scale protests…

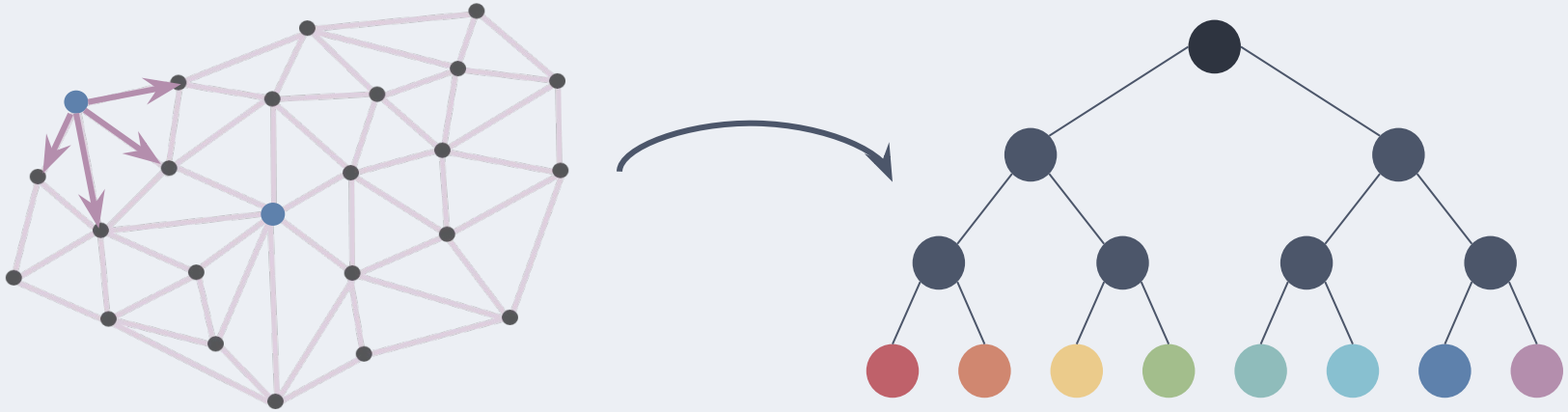
Cryptography alone won't save us, so we need more networks & systems research



- Improved mesh networking algorithms for messaging
- Co-design with cryptographic protocols

The takeaway? For mesh messaging in large-scale protests…

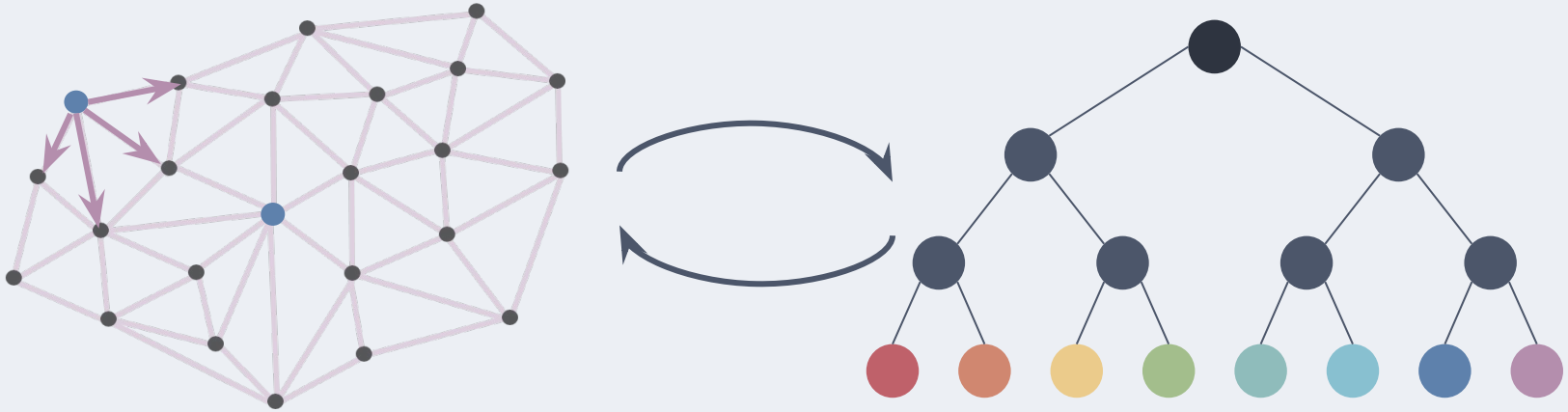
Cryptography alone won't save us, so we need more networks & systems research



- Improved mesh networking algorithms for messaging
- Co-design with cryptographic protocols

The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won't save us, so we need more networks & systems research



- Improved mesh networking algorithms for messaging
- Co-design with cryptographic protocols

The takeaway? For mesh messaging in large-scale protests...

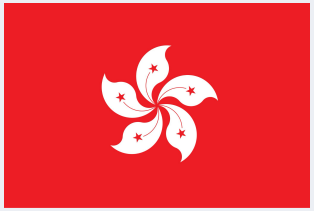
Cryptography alone won’t save us,

The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won't save us,
so we need more human factors research.

The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won't save us, so we need more human factors research.



The takeaway? For mesh messaging in large-scale protests…

Cryptography alone won't save us, so we need more human factors research.

The takeaway? For mesh messaging in large-scale protests…

Cryptography alone won't save us, so we need more human factors research.

Relatively affluent, digital society

The takeaway? For mesh messaging in large-scale protests…

Cryptography alone won't save us, so we need more human factors research.

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

Relatively affluent, digital society

The takeaway? For mesh messaging in large-scale protests…

Cryptography alone won't save us, so we need more human factors research.

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

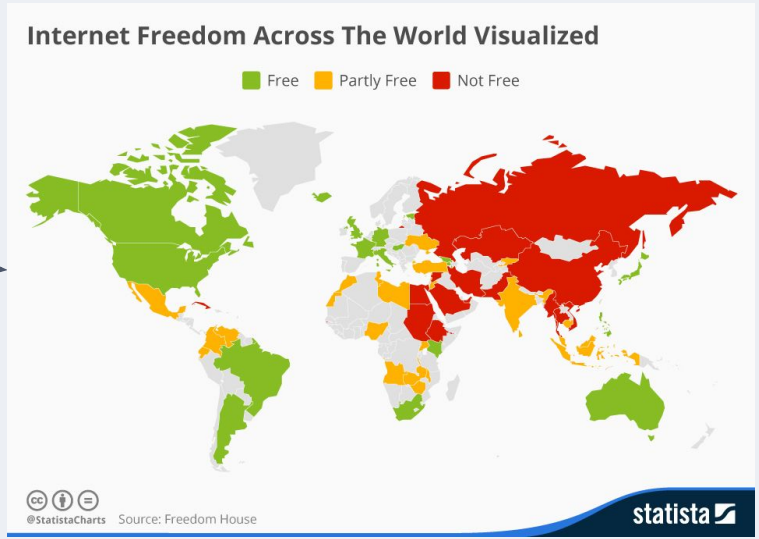
Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

Relatively affluent, digital society



The takeaway? For mesh messaging in large-scale protests…

Cryptography alone won't save us, so we need more human factors research.

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

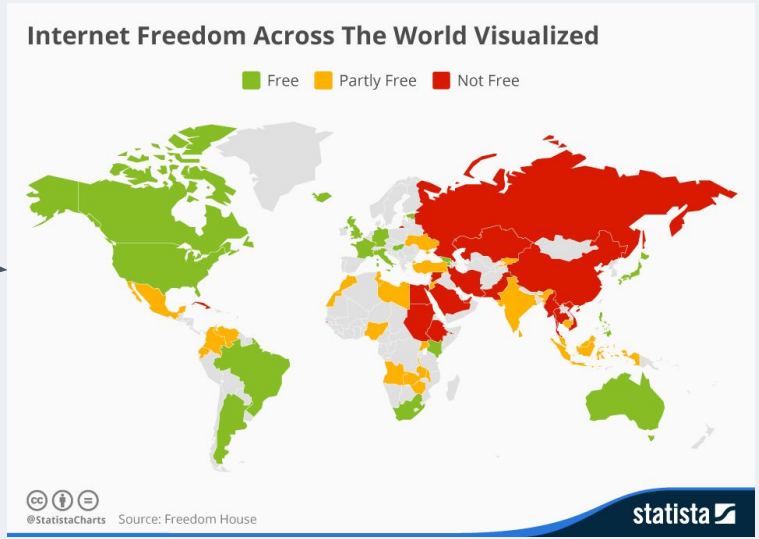
Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

Relatively affluent, digital society



- Interview studies with more activists

The takeaway? For mesh messaging in large-scale protests…

Cryptography alone won't save us, so we need more human factors research.

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

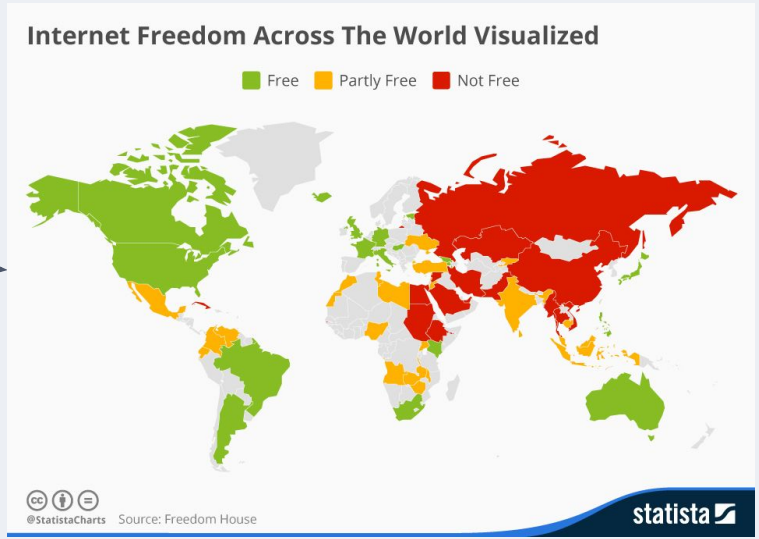
Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

Relatively affluent, digital society



- Interview studies with more activists
- User studies for better tools

The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won’t save us,

The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won't save us, but cryptography is still important.

The takeaway? For mesh messaging in large-scale protests...

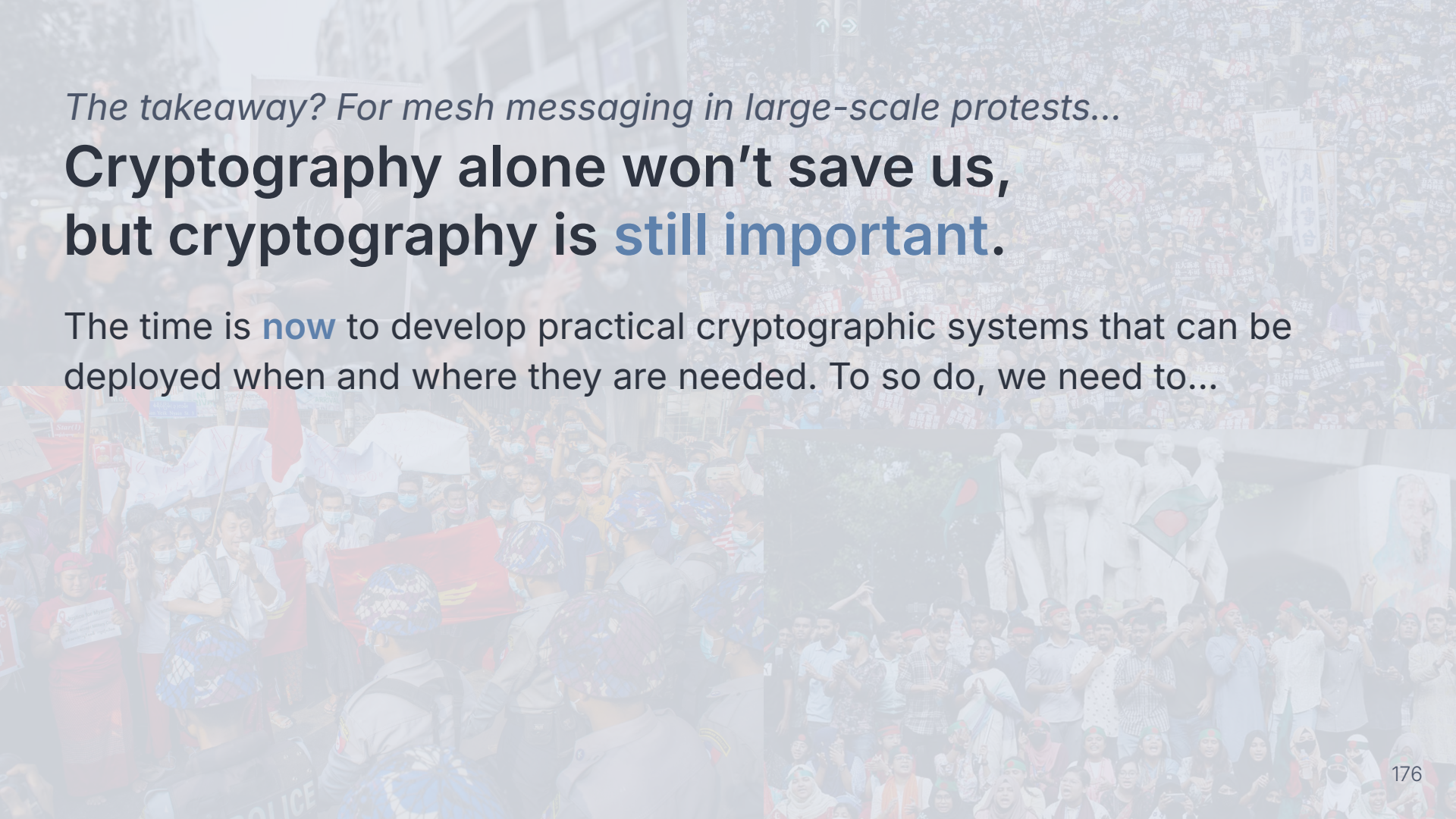
Cryptography alone won't save us, but cryptography is still important.

The time is **now** to develop practical cryptographic systems that can be deployed when and where they are needed.

The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won't save us, but cryptography is still important.

The time is **now** to develop practical cryptographic systems that can be deployed when and where they are needed. To so do, we need to...



The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won't save us, but cryptography is still important.

The time is **now** to develop practical cryptographic systems that can be deployed when and where they are needed. To so do, we need to...

- Acknowledge this is an **interdisciplinary problem** with an **interdisciplinary solution**

The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won't save us, but cryptography is still important.

The time is **now** to develop practical cryptographic systems that can be deployed when and where they are needed. To so do, we need to...

- Acknowledge this is an **interdisciplinary problem** with an **interdisciplinary solution**
- Engage with researchers in **networking**, **systems**, and **human factors** for a more holistic approach

The takeaway? For mesh messaging in large-scale protests...

Cryptography alone won't save us, but cryptography is still important.

The time is **now** to develop practical cryptographic systems that can be deployed when and where they are needed. To so do, we need to...

- Acknowledge this is an **interdisciplinary problem** with an **interdisciplinary solution**
- Engage with researchers in **networking**, **systems**, and **human factors** for a more holistic approach
- Start a broader conversation on how academics can achieve **tangible impact** on sensitive populations

Spacelab.
The City College of New York

Tushar Jois

📧 tjois@ccny.cuny.edu
💻 https://tjo.is
🦋 @tjo.is

Amigo: Secure Group Mesh Messaging in Realistic Protest Settings

David Inyangson*, Sarah Radway*, **Tushar M. Jois**, Nelly Fazio, James Mickens

Cryptology ePrint Archive, Paper 2024/1872

https://ia.cr/2024/1872

**Equal contribution.*