Anix

Anonymous Blackout-Resistant Microblogging with Message Endorsing

Sina Kamali
sinakamali@uwaterloo.ca
University of Waterloo

Diogo Barradas
diogo.barradas@uwaterloo.ca
University of Waterloo

IEEE S&P

San Francisco, CA, U.S.A.

May 13th, 2025

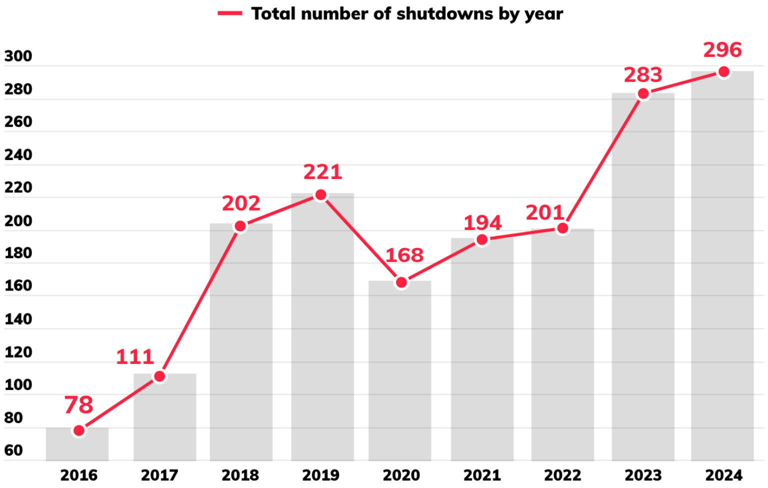
Internet Shutdowns *(a.k.a. blackouts)*

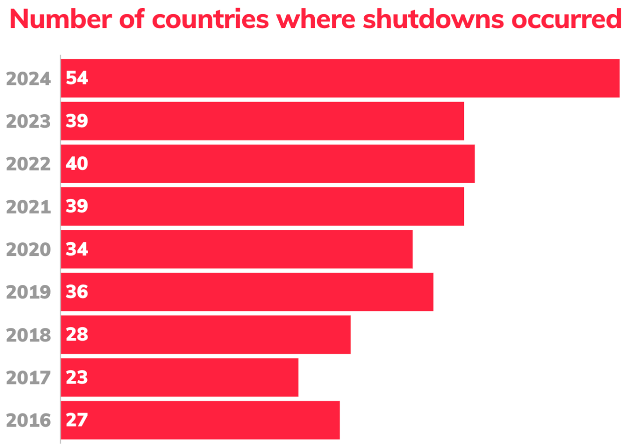
- Repressive governments often aim to control/restrict the flow of information
  - Network-level interference
  - Social media monitoring
  - Messaging filters
- Today, censors are choosing to instate region/country-wide Internet shutdowns
  - Lasting up to weeks in a row

Kashmiri journalists protest against internet blockade put by India's government in Srinagar on October 12, 2019. TAUSEEF MUSTAFA/AFP/AFP via Getty Images

https://www.cnn.com/2019/12/21/asia/internet-shutdowns-china-india-censorship-intl-hnk/index.html

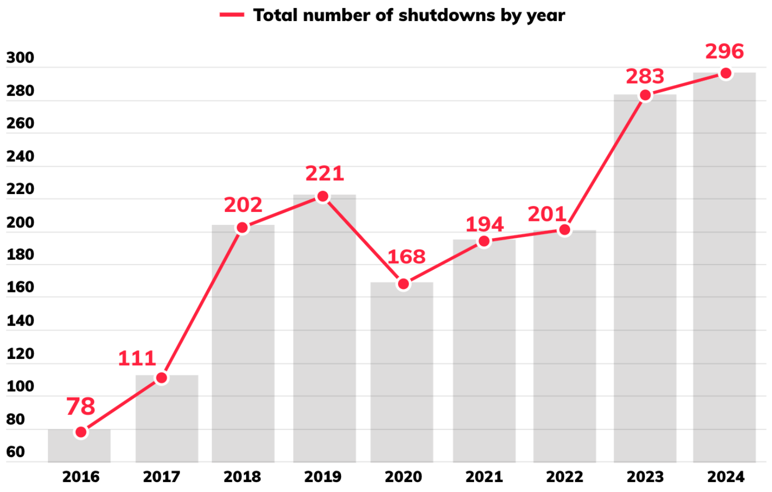
Shutdowns are on the Rise

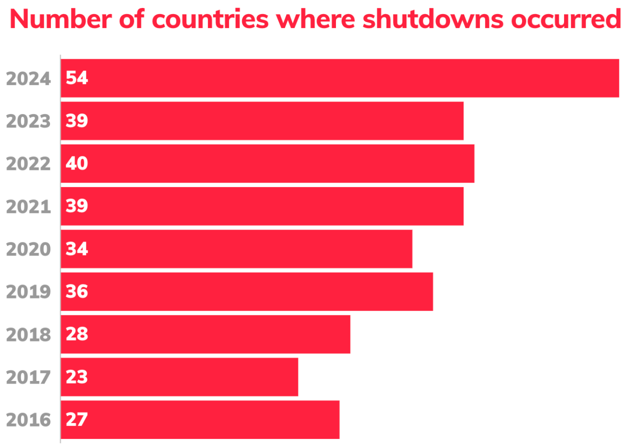




https://www.accessnow.org/internet-shutdowns-2024/

Shutdowns are on the Rise



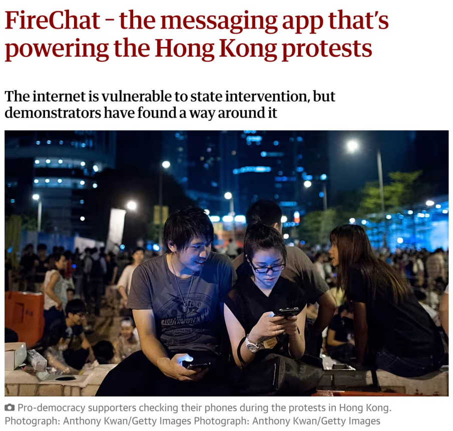


https://www.accessnow.org/internet-shutdowns-2024/

“How can we tackle these shutdowns?”

Blackout-resistant Messaging via Mobile Mesh Networks

- Allow for communication without Internet or cellular access
  - Rely on wireless capabilities (Bluetooth, WiFi Direct) of modern smartphones
  - Messages hop from phone to phone

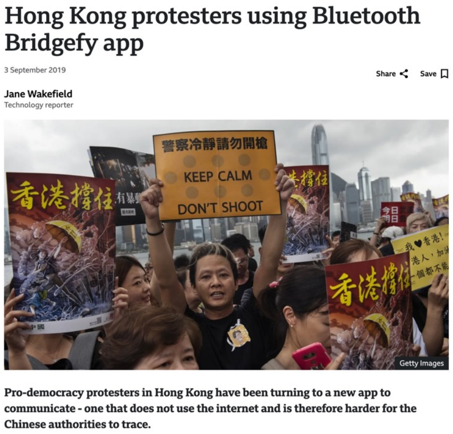


FireChat - the messaging app that's powering the Hong Kong protests

The internet is vulnerable to state intervention, but demonstrators have found a way around it

Pro-democracy supporters checking their phones during the protests in Hong Kong. Photograph: Anthony Kwan/Getty Images Photograph: Anthony Kwan/Getty Images

https://www.theguardian.com/world/2014/sep/29/firechat-messaging-app-powering-hong-kong-protests



Hong Kong protesters using Bluetooth Bridgefy app

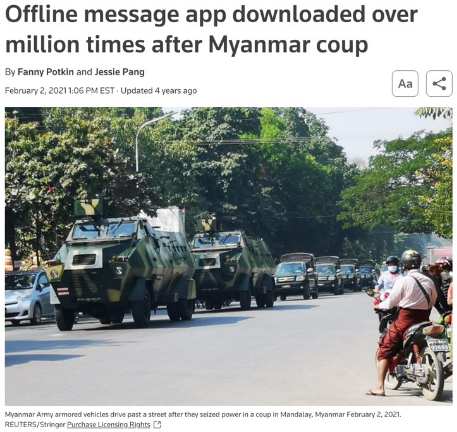
3 September 2019

Share Save

Jane Wakefield
Technology reporter

Pro-democracy protesters in Hong Kong have been turning to a new app to communicate - one that does not use the internet and is therefore harder for the Chinese authorities to trace.

https://www.bbc.com/news/technology-49565587



Offline message app downloaded over million times after Myanmar coup

By Fanny Potkin and Jessie Pang

February 2, 2021 1:06 PM EST · Updated 4 years ago

Myanmar Army armored vehicles drive past a street after they seized power in a coup in Mandalay, Myanmar February 2, 2021. REUTERS/Stringer Purchase Licensing Rights

https://www.reuters.com/article/technology/offline-message-app-downloaded-over-million-times-after-myanmar-coup-idUSKBN2A22H0/

Desirable Properties for Mesh Messaging Apps

Flexible Communication Models

- One to one
- Some to some
- One to many (broadcast)

User Anonymity

- Sender and receiver
- Forward anonymity
- Post-compromise anonymity

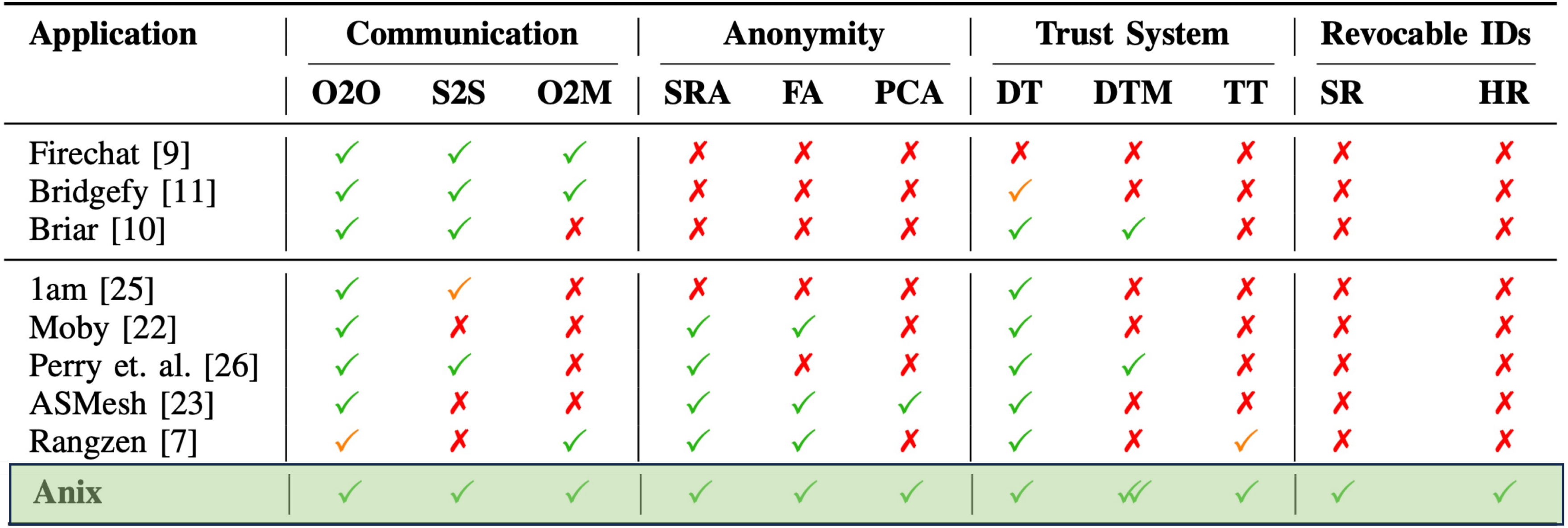
Trust Systems

- Direct Trust
- Direct Trust Mediation
- Transitive Trust

Identity Revocation

- Soft revocation
- Hard revocation

The Mesh Messaging Apps Landscape



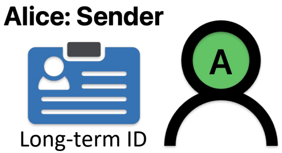
Application	Communication			Anonymity			Trust System			Revocable IDs	
	O2O	S2S	O2M	SRA	FA	PCA	DT	DTM	TT	SR	HR
Firechat [9]	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
Bridgefy [11]	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗
Briar [10]	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗
1am [25]	✓	✓	✗	✗	✗	✗	✓	✗	✗	✗	✗
Moby [22]	✓	✗	✗	✓	✓	✗	✓	✗	✗	✗	✗
Perry et. al. [26]	✓	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗
ASMesh [23]	✓	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗
Rangzen [7]	✓	✗	✓	✓	✓	✗	✓	✗	✓	✗	✗
Anix	✓	✓	✓	✓	✓	✓	✓	✓✓	✓	✓	✓

Existing apps lack desirable properties

Our Contributions

- Systematization of existing blackout-resistant mesh-messaging apps:
  - Threat models
  - Design features
- Anix: An anonymous blackout-resistant mesh messaging platform:
  - Based on selectively linkable one-time-use pseudonyms (PSUs)
  - Able to establish & manage trust relationships across the mesh
  - Able to prioritize microblogging-style messages vouched by trusted contacts via an anonymous message endorsing scheme

Anix’s Operational Workflow

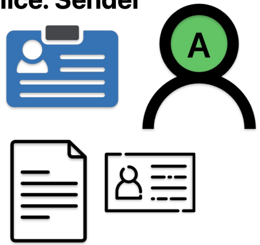


Alice: Sender

Long-term ID

Anix's Operational Workflow

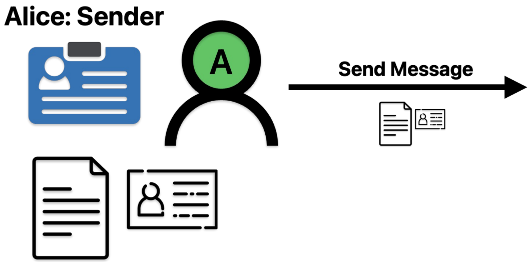
Alice: Sender



PSUs:

- One-time-use
- Unlinkable
- Anonymous
  - Unless ID is known

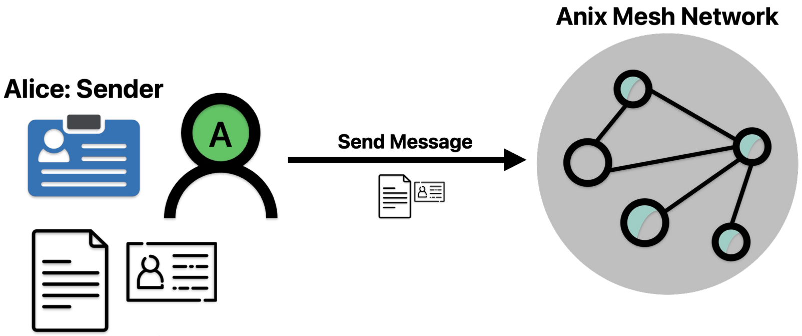
Anix’s Operational Workflow



PSUs:

- One-time-use
- Unlinkable
- Anonymous
  - Unless ID is known

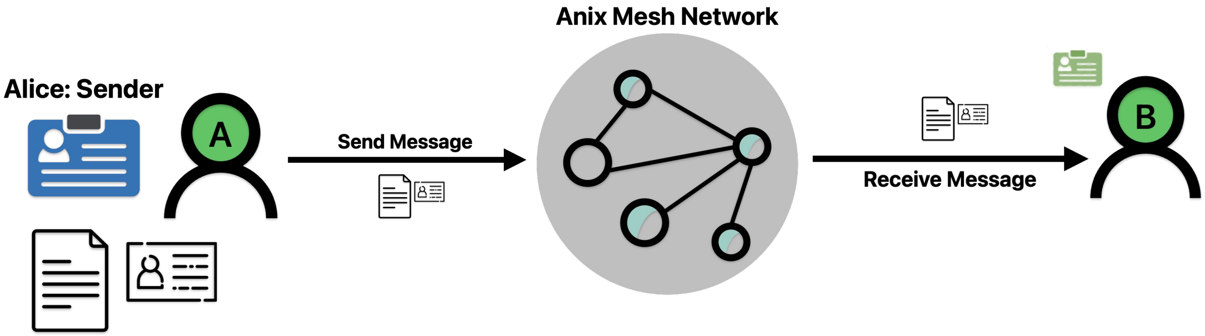
Anix's Operational Workflow



PSUs:

- One-time-use
- Unlinkable
- Anonymous
    - Unless ID is known

Anix's Operational Workflow



Alice: Sender

Send Message

Anix Mesh Network

Receive Message

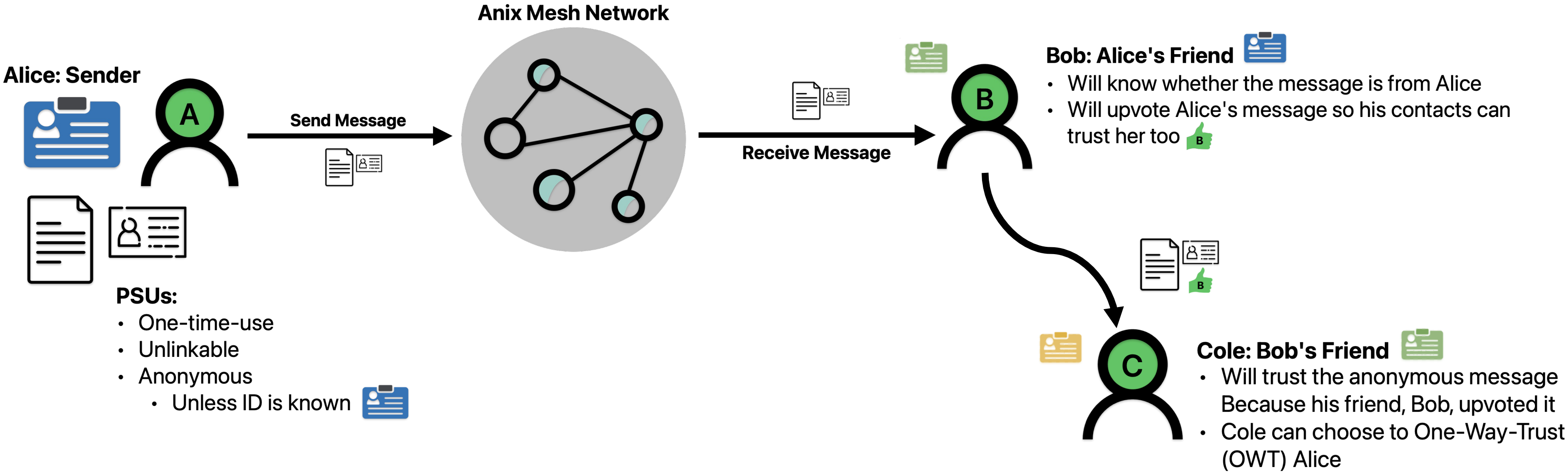
Bob: Alice's Friend

- Will know whether the message is from Alice
- Will upvote Alice's message so his contacts can trust her too

PSUs:

- One-time-use
- Unlinkable
- Anonymous
  - Unless ID is known

Anix’s Operational Workflow



Anix Mesh Network

Alice: Sender

Send Message

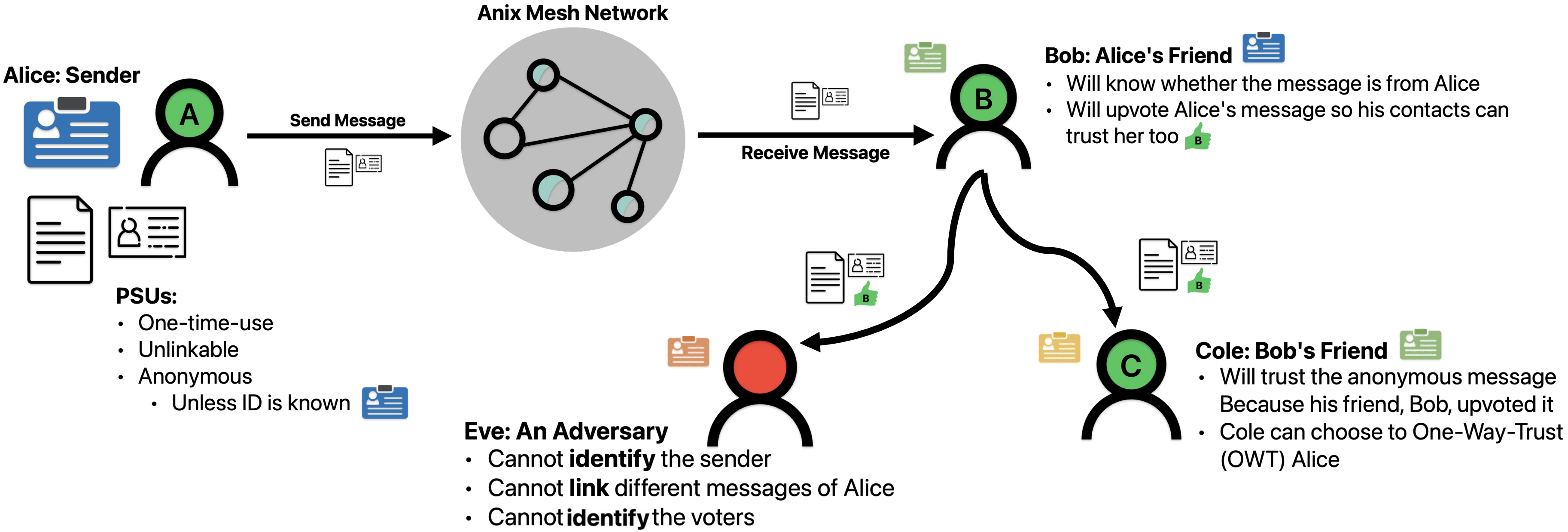
Receive Message

Bob: Alice's Friend
- Will know whether the message is from Alice
- Will upvote Alice's message so his contacts can trust her too

PSUs:
- One-time-use
- Unlinkable
- Anonymous
  - Unless ID is known

Cole: Bob's Friend
- Will trust the anonymous message Because his friend, Bob, upvoted it
- Cole can choose to One-Way-Trust (OWT) Alice

Anix's Operational Workflow



Alice: Sender

PSUs:

- One-time-use
- Unlinkable
- Anonymous
  - Unless ID is known

Bob: Alice's Friend

- Will know whether the message is from Alice
- Will upvote Alice's message so his contacts can trust her too

Cole: Bob's Friend

- Will trust the anonymous message Because his friend, Bob, upvoted it
- Cole can choose to One-Way-Trust (OWT) Alice

Eve: An Adversary

- Cannot **identify** the sender
- Cannot **link** different messages of Alice
- Cannot **identify** the voters

One-time-use Pseudonyms (PSUs)

- Each user holds two sets of key pairs:
  - Long term ID keys (kept secret)
  - One-time-use (OTU) keys

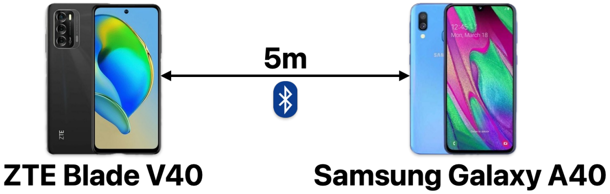
- These keys are used to generate PSUs and allow selective linking of a user's messages/votes by trusted contacts:

$$PSU = Pub_{OTU} \,||\, bSig(Priv_{ID}, Pub_{OTU})$$

, where $bSig$ is a public key-blinded signature scheme

Evaluation: Performance Micro-Benchmarks

- Implemented Anix on Android
- Avg. data exchange time: 11.58s
    - 100 messages * 10,000 votes (each)
- Avg. battery consumption: 1.5%/h

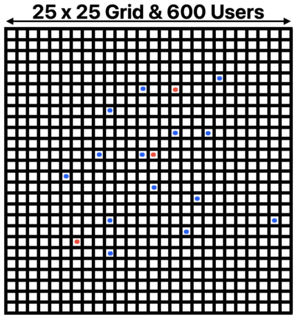


Computation time (in ms) for Anix operations

Op./Device	Gen. PSU	Create Msg.	Create Vote	Verify Sig.	BVer (Alg. 3)
Samsung A40	175.06 ± 1.05	46.30 ± 0.01	84.61 ± 1.14	61.33 ± 0.21	67.68 ± 0.21
ZTE Blade V40	64.95 ± 0.29	19.75 ± 0.01	38.76 ± 0.32	43.29 ± 0.28	47.30 ± 0.48

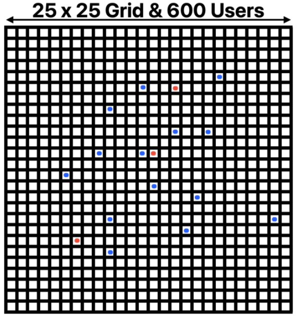
Evaluation: Simulation Testbed

- Simulated a scaled-down city environment with 600 users
- Blackout duration of 5 days (120 simulation steps)
- Most users are benign (98%), but a fraction are malicious (2%):
    - Drop benign messages
    - Attempt to gain the trust of benign users
    - Spread misinformation

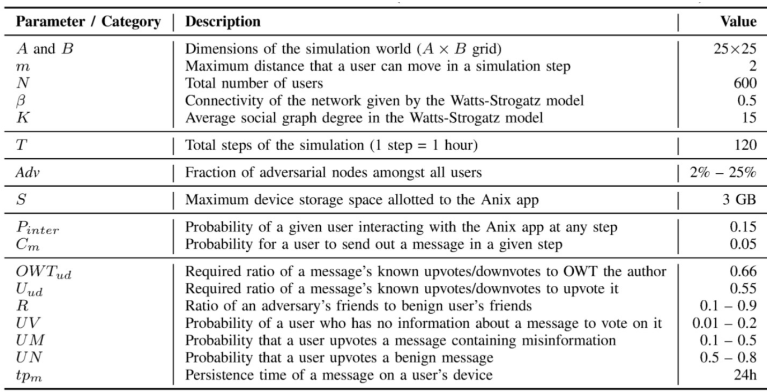


Evaluation: Simulation Testbed

- Simulated a scaled-down city environment with 600 users
- Blackout duration of 5 days (120 simulation steps)
- Most users are benign (98%), but a fraction are malicious (2%):
  - Drop benign messages
  - Attempt to gain the trust of benign users
  - Spread misinformation

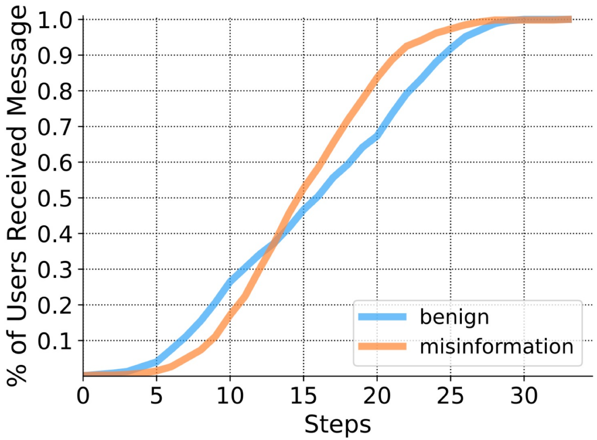


Check the paper for results under multiple settings!



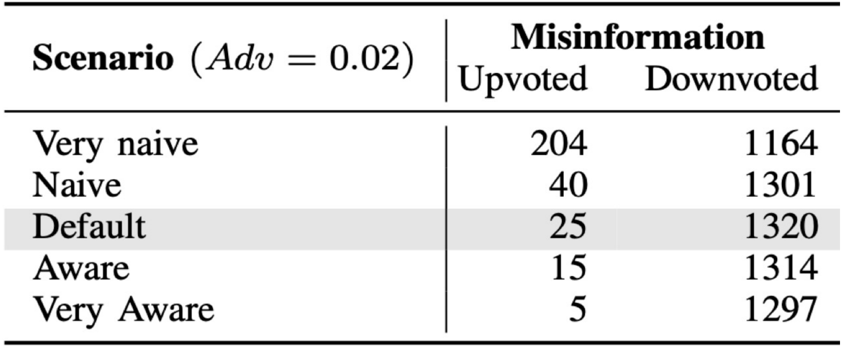
Parameter / Category	Description	Value
A and B	Dimensions of the simulation world ($A \times B$ grid)	25×25
m	Maximum distance that a user can move in a simulation step	2
N	Total number of users	600
β	Connectivity of the network given by the Watts-Strogatz model	0.5
K	Average social graph degree in the Watts-Strogatz model	15
T	Total steps of the simulation (1 step = 1 hour)	120
Adv	Fraction of adversarial nodes amongst all users	2% – 25%
S	Maximum device storage space allotted to the Anix app	3 GB
P_{inter}	Probability of a given user interacting with the Anix app at any step	0.15
C_m	Probability for a user to send out a message in a given step	0.05
OWT_{ud}	Required ratio of a message's known upvotes/downvotes to OWT the author	0.66
U_{ud}	Required ratio of a message's known upvotes/downvotes to upvote it	0.55
R	Ratio of an adversary's friends to benign user's friends	0.1 – 0.9
UV	Probability of a user who has no information about a message to vote on it	0.01 – 0.2
UM	Probability that a user upvotes a message containing misinformation	0.1 – 0.5
UN	Probability that a user upvotes a benign message	0.5 – 0.8
tp_m	Persistence time of a message on a user's device	24h

Coverage and Resilience to Misinformation



Benign messages take ~1 day to reach >90% of users

Messages up/downvoted by the majority of users



Scenario $(Adv = 0.02)$	**Misinformation**	
	Upvoted	Downvoted
Very naive	204	1164
Naive	40	1301
Default	25	1320
Aware	15	1314
Very Aware	5	1297

Anix users can weed out misinformation

Takeaways

- Internet shutdowns are becoming prevalent, and existing blackout-resistant mesh networking apps cannot sufficiently address users' needs
- We presented **Anix**, an anonymous mesh-based microblogging platform
  - Enables trusted users to exchange data while remaining anonymous to untrusted users
  - Resilient to adversaries aiming to spread misinformation
- Future work:
  - Strengthen forward anonymity; Automate identity revocation; Optimize vote exchange

Takeaways

- Internet shutdowns are becoming prevalent, and existing blackout-resistant mesh networking apps cannot sufficiently address users' needs

- We presented **Anix**, an anonymous mesh-based microblogging platform
  - Enables trusted users to exchange data while remaining anonymous to untrusted users
  - Resilient to adversaries aiming to spread misinformation

- Future work:
  - Strengthen forward anonymity; Automate identity revocation; Optimize vote exchange

Diogo Barradas
diogo.barradas@uwaterloo.ca

Thank you!