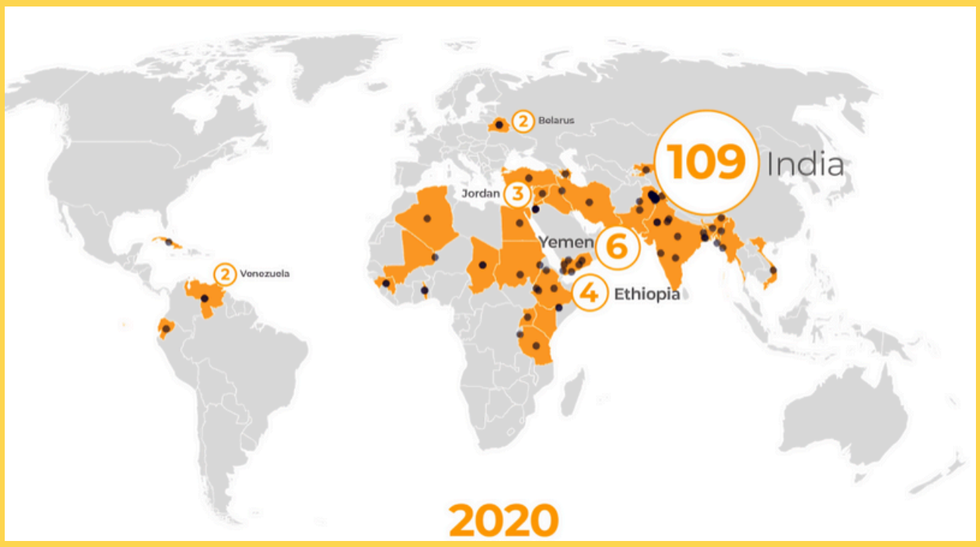
Anix: Anonymous Blackout-Resistant Microblogging with Message Endorsing

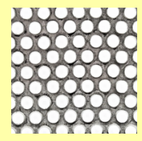
Internet Blackouts are Widespread



- A **worldwide** issue
- Many methods to circumvent censorship have been created
- Due to many reasons, such as: **political instability**, **elections**, or **protests**

Mobile Mesh Network Messaging

- Send messages using available wireless technology such as **Bluetooth** and **WiFi Direct**
- Messages **hop** from phone to phone



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]	✓	✗	✓	✓	✓	✗	✓	✗	✓	✗	✗
Nika	✓	✓	✓	✓	✓	✓	✓	✓✓	✓	✓	✓

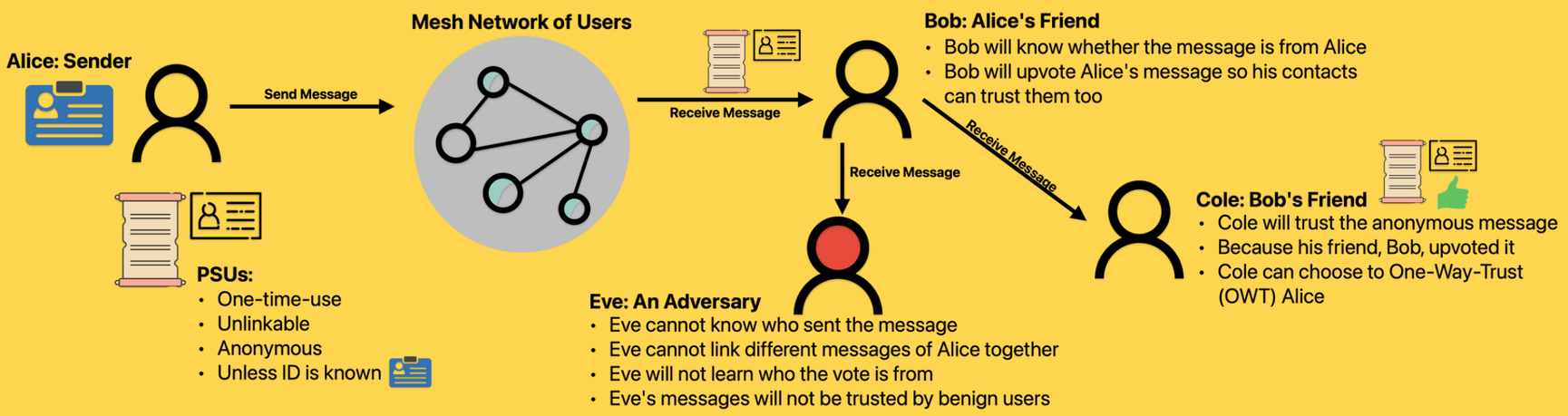
Prior solutions fail to address the practical needs of users in internet shutdowns.

How to trust anonymous messages?

PSA: Public Key Blinded Signatures

- Signatures used in Nika are **Public Key Blinded**
- They **cannot** be traced back to their signing public key
- This **preserves privacy**

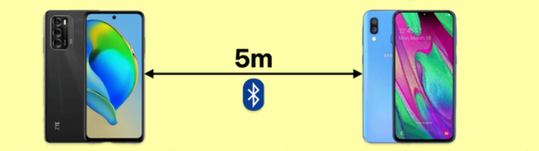
You use Nika!



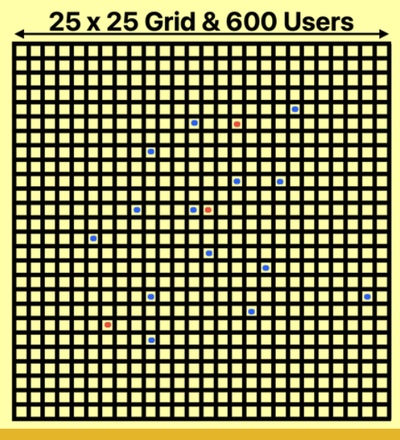
Evaluation

Experimental Testbed

- **Microbenchmarks:**



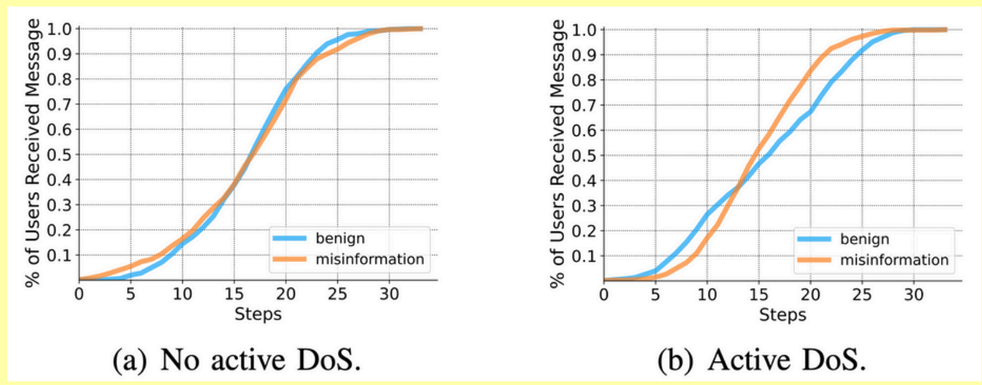
- **Simulation:**



[Micro] Benchmarks

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

Performance Under Active DoS



(a) No active DoS. (b) Active DoS.

Impact of Awareness Settings

Scenario ($Adv = 0.02$)	Parameters				Benign		Misinformation		OWTs	
	R	UV	UM	UN	Upvoted	Downvoted	Upvoted	Downvoted	Benign	Adversarial
Very naive	0.9	0.2	0.5	0.5	495	2522	204	1164	33581	106
Naive	0.7	0.1	0.4	0.55	1087	1874	40	1301	32278	43
Default	0.4	0.05	0.3	0.6	1510	1416	25	1320	31207	11
Aware	0.2	0.02	0.2	0.7	2111	704	15	1314	26115	5
Very Aware	0.1	0.01	0.1	0.8	2549	348	5	1297	15497	2

Highlights of Nika's Evaluation:

- Nika can **perform** in an **internet blackout** even under heavy **DoS**
- Nika **outperforms** competitors by upwards of **49x** in blocking **misinformation**
- Nika achieves **respectable** performance on even **lower tier** phones

Conclusion and Future Work

- We design Nika, a new *blackout-resistant messaging* app that enables users to **remotely** establish and manage trust relationships across the mesh network.
- Future work will focus on **improving network performance** and using more advanced crypto to **further secure the protocol**.

UNIVERSITY OF WATERLOO | DAVID R. CHERITON SCHOOL OF COMPUTER SCIENCE

To appear in IEEE S&P 25

Sina Kamali, Diogo Barradas
<sinakamali, diogo.barradas> @uwaterloo.ca