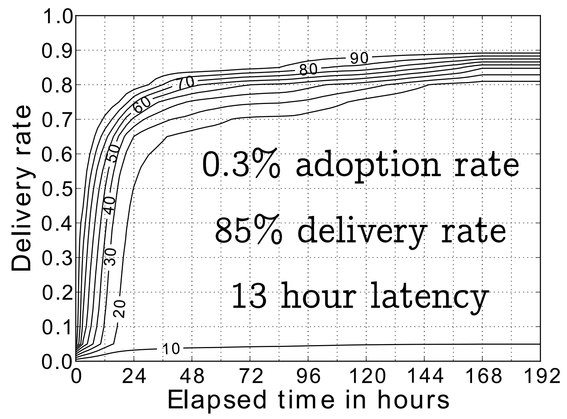
A Mobile Path to Censorship Resistance and Privacy

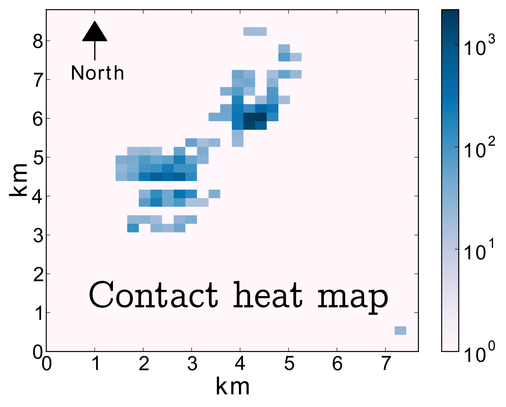
Yue Liu, David Bild, David Adrian, Gulshan Singh, Robert Dick, Dan Wallach, and Z. Morley Mao

This work was supported, in part, by NSF under award TC-0964545.

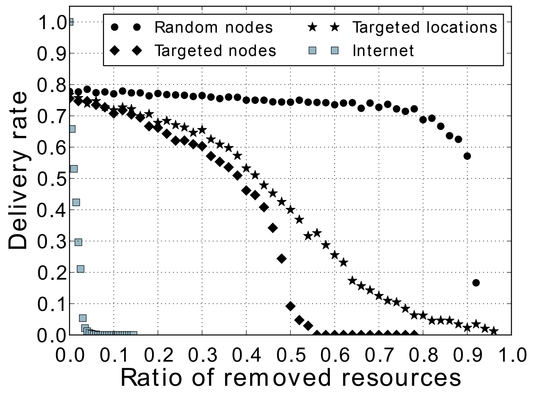
1am microblogging app
released on campus.



Phone-to-phone contacts happen throughout campus.



Twice the observed contact rate of prior user studies.



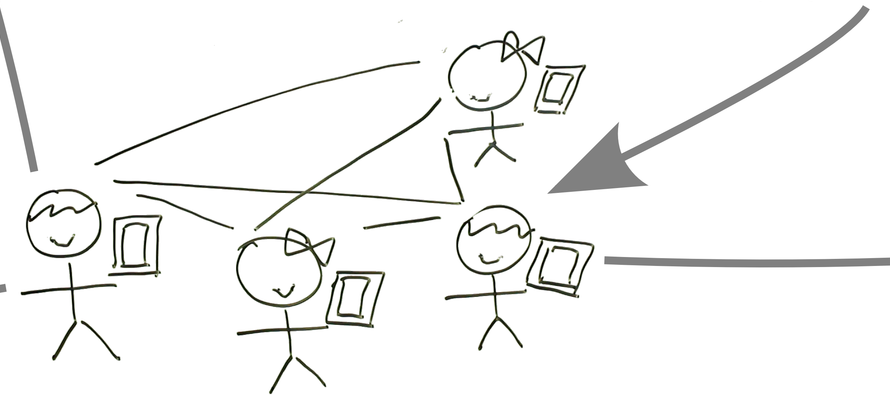
Works with most important half of participants disabled.

The Alternative

Commodity smartphones.
App install.
Peer-to-peer WiFi.
Fully distributed architecture.

What about **delay**, required **adoption rate**, and implications of **human motion** patterns?

What about **reliability** in the presence of **denial of service** attacks, **Sybil** attacks, and **spam/propaganda**?

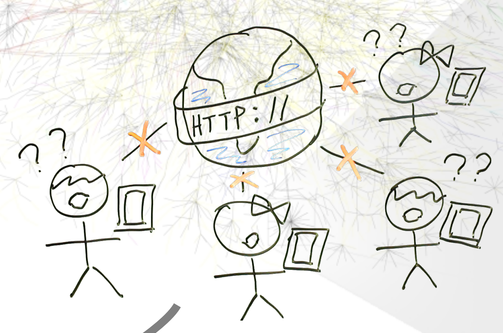


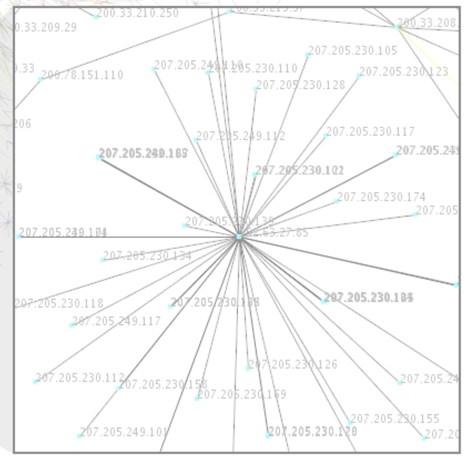
The Internet

Opened content access and creation,
Hierarchical.
Easy to shut down, censor, and spy on.

Can we create a **blocking-, censorship-, and surveillance-resistant** network that is practical for normal smartphone users?

How would that work?





What about **spam/propaganda** in this fully decentralized network?

No central authority.
What can be done with local information?

Use transitive rebroadcast graph instead of followers graph.

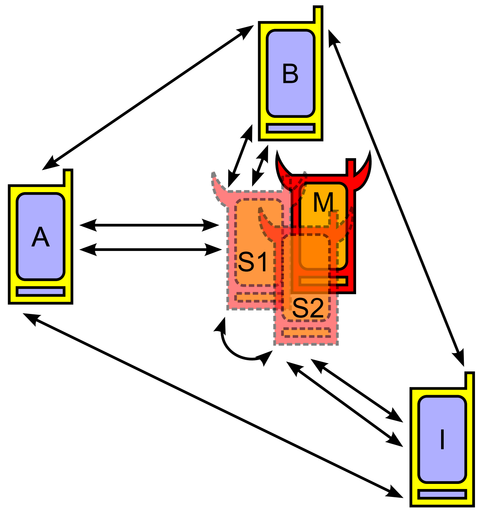
Less disassortive and more clustered, like non-digital social networks.

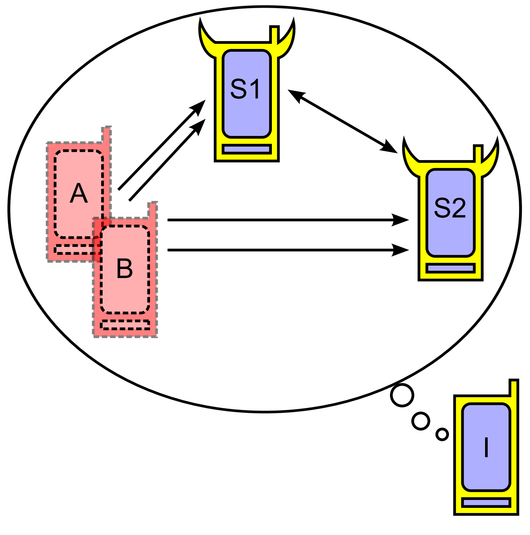
Use graph structure to find spammers.

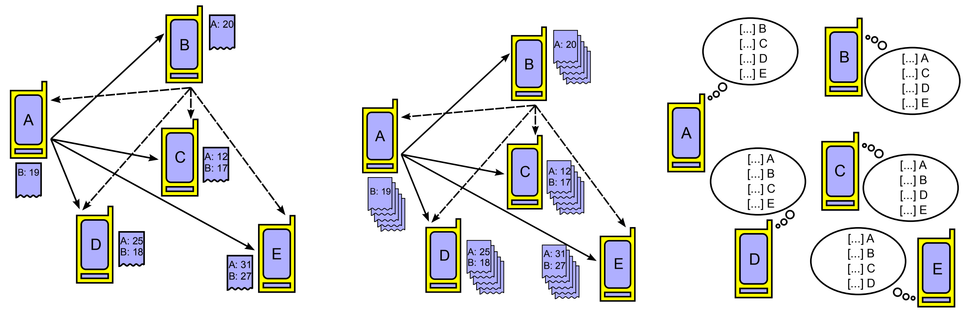
Challenges: Can't change hardware.
No trusted authorities. Participants move.

Insight: Can determine true worldview **without trusting any participant.**

Sybil attack: A single physical entity can pretend to be multiple participants, gaining unfair influence at low cost.







Identities transmit and record signal strengths.
Exchange observations.
Nodes form internally consistent world views.

Tested on HTC Magic smartphones with 11 users.

Eliminates 91%-100% of Sybil identities, depending on environment.