

Connecting the Unconnected

free is good

Edoardo Biagioni
University of Hawaii at Manoa
Information and Computer Sciences

AllNet project

Ad-Hoc Networking

- old idea (1990s)
- Alice's device talks to Bob's device talks to Charlie's device talks to
- until we build a useful network

In 2017 we all carry two-way radios!!!!

Conventional vs. Free

- can mobilize large capital investments
- incentives for reliability
- central planning
- fixed infrastructure
- **very successful**
- follows money
- can serve the underserved
- incentives to contribute
- well-understood need
- flexible deployment
- some success
- **follows people**

problems with free

- **relies on network effect**
 - works best when many people use it
- “tragedy of the commons”
 - most people prefer to use more, contribute less
- no large investments
 - hard to build infrastructure
 - cannot use for long-distance high-volume communications
- all responsible, nobody responsible
 - can others see my messages?

advantages of free

- free!
- decentralized decision-making
 - end-users make decisions
 - end-to-end architecture
- portable infrastructure
 - **end-users bring devices where needed**

Devices follow People

- still works when infrastructure is down
- as long as devices can be powered
- **supports emergency communication**

Ad-Hoc and Delay Tolerant

- messages are stored and forwarded by intermediate devices
- forwarding may be immediate or delayed
- devices may carry messages: **sneakernet**
 - inefficient – multiple message retransmissions
 - but acceptable for low-rate communication:
text messages!
- infrastructure not required

P2P networking

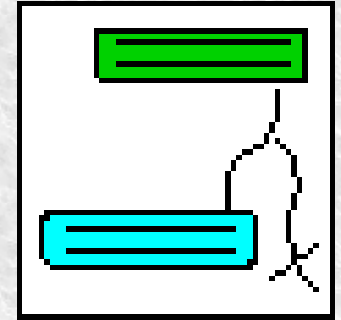
Real-Life challenges

- WiFi has an ad-hoc mode
 - but ad-hoc Wifi **not supported on iOS or Android**
 - unless the device is rooted!
- so bluetooth where possible, other technologies in the future
- can use WiFi network *not connected to the Internet*
 - local infrastructure

Leveraging the Internet

- needs to work well without the Internet
- needs to work better when there is Internet!
- distributed implementation: **internet-connected devices self-organize** so my device knows where it can pick up its messages
 - similar to email, but self-organizing
 - Distributed Hash Table

AllNet status



- works well on Linux, including ad-hoc WiFi mode and Internet
- works on Internet-connected Apple and Windows desktops
- works on iOS, including multipeer (peer-to-peer) and Internet

`allnet-xchat`

<http://allnt.org/>

- preliminary implementation for Android

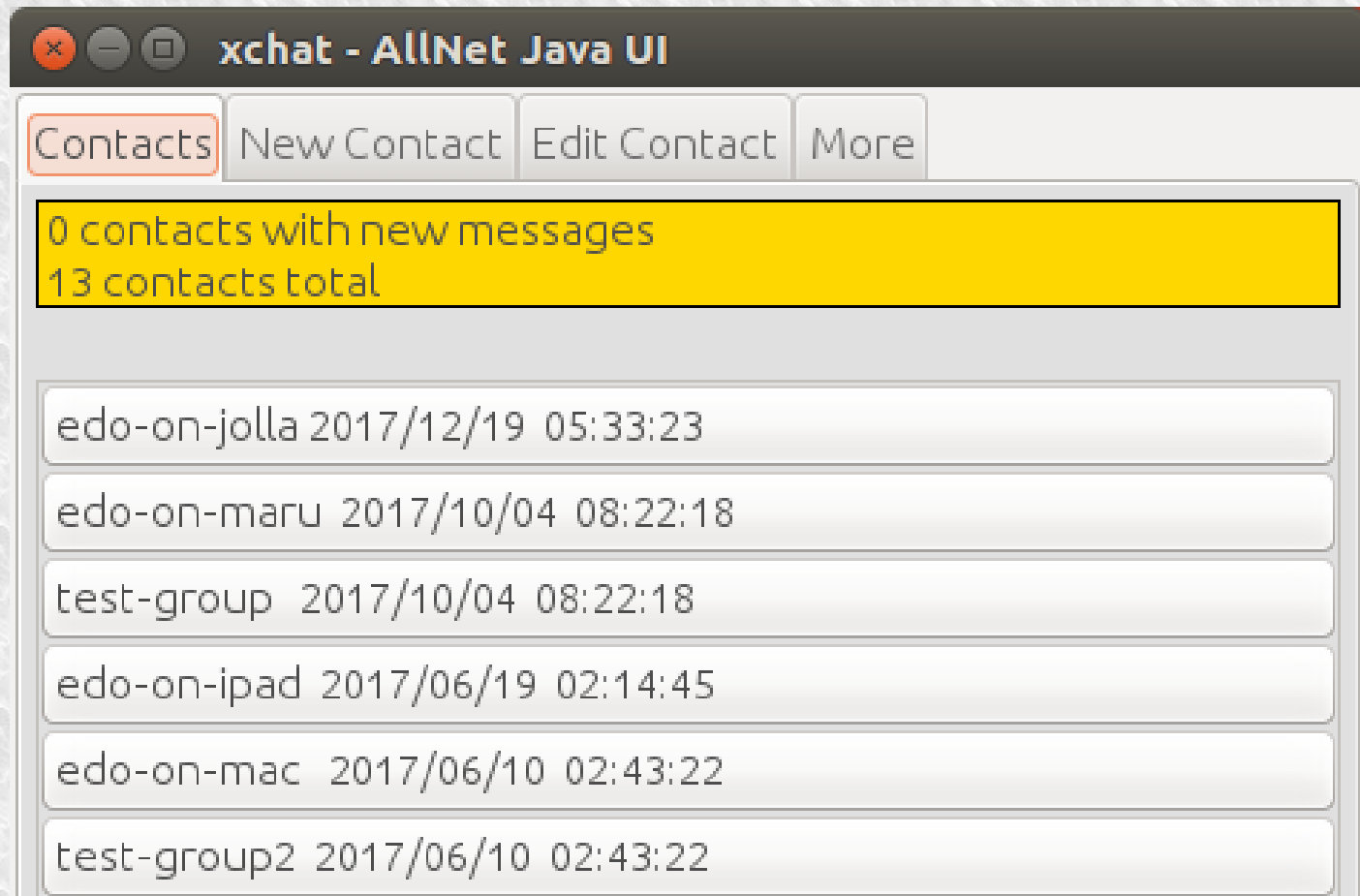
Challenges and **Solutions**

- distributed identification
- anyone may snoop
- resource depletion
 - battery
 - storage
 - bandwidth
- unreliable
- use a shared secret for initial ID
- encrypt messages
- prioritize traffic
 - my own first
 - my friends' next
 - then others'
- meaningful packets

Experience

- Internet messaging used daily over the Internet
 - by a small group
- so far, P2P mostly used for testing
- mobile devices run apps for short periods only
 - fetch data when run, not when convenient
- **mostly delivers messages reliably**

in a distributed setting
it is easy to create test accounts!



Contact Creation

- distributed
 - I could claim to be Justin Bieber!
- **we meet through a secret known only to us**
- secret chosen by system
- secret only used once
 - ok if compromised after key exchange

AllNet Technology

- messages encrypted, authenticated
- sender-based message prioritization
- self-selected, non-unique, location-independent device identifiers (“addresses”)
- anonymous acks
- distributed, anonymous social network
- **mobile differs from wired networking!**

Anonymous Acks 1/2

- each personal message has an unencrypted header, or “envelope”, and encrypted content
- unencrypted header includes a **message ID**
- encrypted content includes the **ack**

Anonymous Acks 2/2

- (encrypted) ack hashes to (unencrypted) message ID
- anyone receiving ack hashes it, to compare it to received message IDs
- **only receiver can ack**
- anyone can match ack to message

Incentives to Contribute

- could have competitive **games** for “who contributes more to others' transmissions”
 - a distributed currency
- **games** could leverage the anonymous social network
 - the network effect used to incentivize
- must be free to choose how much to contribute
- default is to contribute at least a little
 - e.g. 1%

Future Work

2018/01/01

- better evaluate multihop and delayed ad-hoc
- **collaboration with Pacific Disaster Center**
- complete Android implementation
- add ad-hoc wherever and however possible
- cellphone walkie-talkie

free is good

- but needs minimal support from OS authors
 - Android is Linux, but no API for P2P wifi
 - iOS Multipeer is restricted to iOS devices
- distributed decision-making
- **network follows people**

`http://alnt.org/`