AllNet: ubiquitous interpersonal communications

Edoardo Biagioni
Information and Computer Sciences
University of Hawai’i at Mānoa

Limitations of cellular service

- Not always available
- Sometimes too expensive
- One size may not fit all
- Inefficient for communication among nearby mobile devices

Free improvement
(no additional hardware needed)

- Ad-hoc communication between nearby devices
  - wifi, bluetooth, opportunistic networking
- Forwarded by others:
  - messages are seen by many, so encryption is required
  - key exchange authenticated by interpersonal communications
  - prioritize messages to and from friends
    - as long as we can recognize our friends’ messages
- Internet when available
  - Distributed Hash Table is decentralized, resilient

about this talk

- Introduction
  - slides 1-4
- Challenges: technical, security, human
  - slides 5-11
- Project contributions
  - slides 12-15
- Future work
  - slide 16

Technical Challenges

- Low-overhead universal P2P communication is not widely supported on mobile devices
  - Android blocks Wifi P2P (ad-hoc) mode unless rooted
  - iOS has true P2P, that only works with other iOS devices!
  - Bluetooth takes time to establish connections
  - other mechanisms require extra hardware or are experimental
  - working on the fringes, so properties are often buggy or not well documented
- Reliable communicaton over ad-hoc networks
  - don't want to send all the time (that would be spam)
  - but messages are important, so must be sent
- Picking appropriate levels and details of security
  - design, operations

Security Challenges

- Security and usability often conflict
- goal: secure and usable in a high-school setting
- assume that the device is secure

  (often not a correct assumption)
- choose sensible defaults, give users options
  - save messages on the device, let users export them

    (importing is more challenging)
  - save keys on the device
    - not very secure
    - maybe provide forward secrecy?

Security Example

- Each device generates its own keys
- to exchange keys, you and I have to authenticate the keys with a secret string
  - example: DFDLKKCPAFGBYL
  - could also use QR codes or other methods
- once keys are exchanged, encrypt everything
- equivalent to https?
  - better: no central points of failure
  - worse: not completely automatic

Network Effect

- I benefit if you use the same communication technology as I do
- I benefit more if everyone uses the same communication technology
  - example: telephones
  - mobile phones are different from landlines
  - but the two are compatible
  - making adoption easier

Network Effect: P2P

- ad-hoc P2P communication depends on others carrying my messages
  - may I borrow your phone?
  - automatically and without having to ask?
- good if everyone uses it
  - especially when the infrastructure is not available
  - e.g. in emergencies
  - e.g. when I can't afford the infrastructure

P2P costs

- my message sits on your device
  - takes up space
- your device must forward my messages
  - ok, doesn't have to, but then the network breaks
  - costs you battery, bandwidth, perhaps $$

Automatic Prioritization

- my messages come first
- then my friends' messages
- then maybe their friends' messages?
- and finally, background messages
  - each time, with fewer resources
  - and likely, with more messages!

Contributions so far

- automatic and convenient security
  - authentication relies on personal connection
- improve service in the local area
- anonymous computation of social distance
- ack is hash of message ID
  - recognizable by all, only destination can issue
- addresses suitable for mobility, wireless networks
- priority forwarding with resource management

Anonymous Social Networks

- Each device has a pseudonym P (or more than one)
- I give my friends the modified pseudonym P' for each of my friends
  - easy to compute P' from P, but not P from P'
  - for example, P’ is a prefix of P, or a hash of P
- I also give them P'' for my friends' friends (f^2)
- if a stranger gives me P'' for their f and f^2, I can compute their social distance if it is less than 4
- if so, I may be willing to prioritize their messages

Status

- works well on Linux
  - implementations for iOS, MacOS, Windows
  - Android implementation in progress
  - anonymous social network is not implemented
- supports Wifi (ad-hoc mode) and Internet

Summary

Device-to-Device communication can be useful for interpersonal communication

Re-examine assumptions from wired networks

Encryption, addressing, limited broadcasts

Future projects related to AllNet

- http://alnt.org/
  - continuing design and software development
- motivating participation:
  - the connectivity game
  - monthly awards for “the most helpful device”
    - how could people cheat?
- anonymous social networks
  - we can tell which friends we have in common
  - maybe not always good?
  - how much information is it OK to share?