AllNet

A secure network to connect (mobile) devices for interpersonal communication

without relying on infrastructure

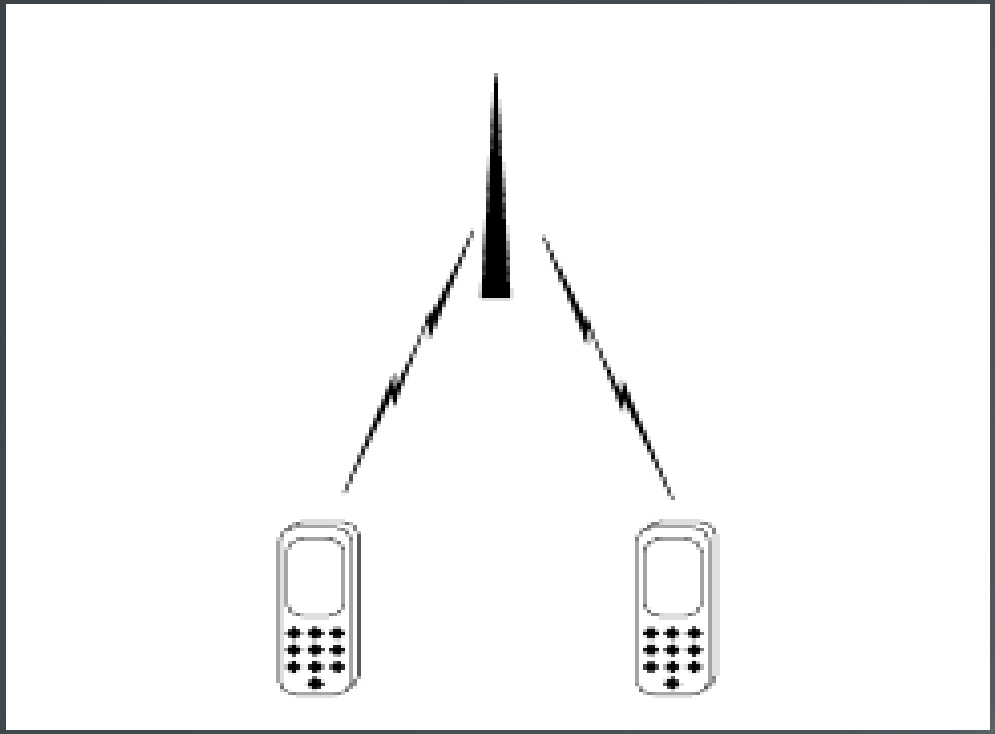
Edoardo Biagioni

Department of Information and Computer Sciences

University of Hawaii at Manoa

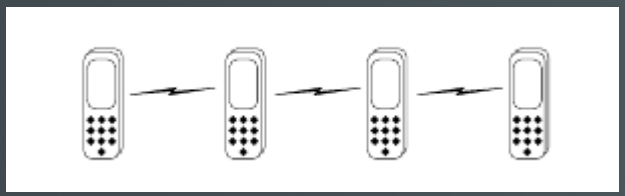
Motivation

- Why can’t my cellphone talk to your cellphone?
  - not a hardware limitation



Motivation II

- Cellphone infrastructure is pretty good in emergencies, but sometimes fails
- Very little resources needed for text
  - 140 characters for twitter, SMS
- A p2p network can support this using few resources
  - and be available in emergencies
  - and other occasions



Motivation III

- If your cellphone is connected to the Internet,

  could I use some of your bandwidth?
- Some very expensive services available at some U.S. airports, at some hotels
- Useful sometimes, but overpriced for email
- Poor people sometimes excluded from Internet
  - Iphone personal hotspot: a step in the right direction

Motivation IV

- Privacy issues in current email, social networks
- People surprised when I tell them email not secure
- PGP more effective if key exchange is improved
- Mobile devices in range of each other can securely exchange keys, as for Bluetooth setup
- Personal exchange provides keys and identity

Benefits of AllNet

- Private interpersonal communication
- P2P social network
- Free low bandwidth internet access in more places
- More choice about whether to use the infrastructure

- AllNet provides always-on networking for low-resources, secure communications

Applications of AllNet

- Chat
  - Distributed, secure social network
- Text-based or low bandwidth Internet access
- Distributed authentication system
- When desired, multimedia and full Internet access
- Emergency communications
- Off-the-grid communications
  - Hiking, on vessels, on the road...

Allnet design

- Secure network: traffic encrypted by default
- Interpersonal communication: low traffic rates
- Infrastructure-free: P2P system
    - but use the Internet when available
- Low overhead lets people support AllNet ”for free”
- Forwarding messages based on individual priority
- Priority computed from message itself

Secure Communication in AllNet

- Parties find out each other's public key
  - Everything is encrypted
- Destination can be limited broadcast or unicast
  - Address has configurable number of bits, so
  - All matching nodes can attempt to decrypt
  - Addresses giving more bits are more selective, so
    - more bits can mean higher priority
  - Small number of bits discourages traffic analysis

Delay-Tolerant Communication in AllNet

- I am often in range of my friends' devices
- Data that cannot be transferred any other way, can be stored for later delivery
- Multimedia and especially images and videos can be shared this way when there is no alternative

Security note

- If everyone's computer and mobile device stores one or more public keys for the user, and
  - If these keys are reliably backed up
- I can use the same kind of key on the WWW
  - I don't have to remember as many passwords
  - my device(s) become part of my key
  - again, backups become essential

Emergency Communication in AllNet

- Daily usage can train people to use a secure system that is almost always available
- The system can then be available in emergencies
- Priority for uses that consume fewer resources

- There could be an ”natural disaster mode” where I accept messages from strangers
- Local authorities should be able to sign messages

AllNet: P2P social network

- Easy to establish group keys to support groups
  - Group key can change when membership changes
- Higher-resource multimedia available when connected to the infrastructure
- Low-resource text only at other times
- My computer can store what is of interest to me

- I may give more resources to my friends' friends

Similar work

- TERA: Trylogy Emergency Response Application (emergency infrastructure, e.g. set up for the Red Cross/Red Crescent)
  - Effective but expensive, and only after deployment
- Maniac: motivating people to participate in P2P
- Byzantium: emergency mesh networking
  - Babel: ad-hoc network routing
- ...and much more

AllNet Status

- Very preliminary implementation (version 0)
- Allnet daemon forwards messages
  - keeps track of peers
  - limits resource usage for non-local messages
- Allnet client(s) generate and consume messages
  - Chat client
  - End-to-end encryption

AllNet summary

Secure, highly available interpersonal communication

Low resource usage

Social network model of security

esb @ hawaii.edu

http://www2.hawaii.edu/~esb/allnet/