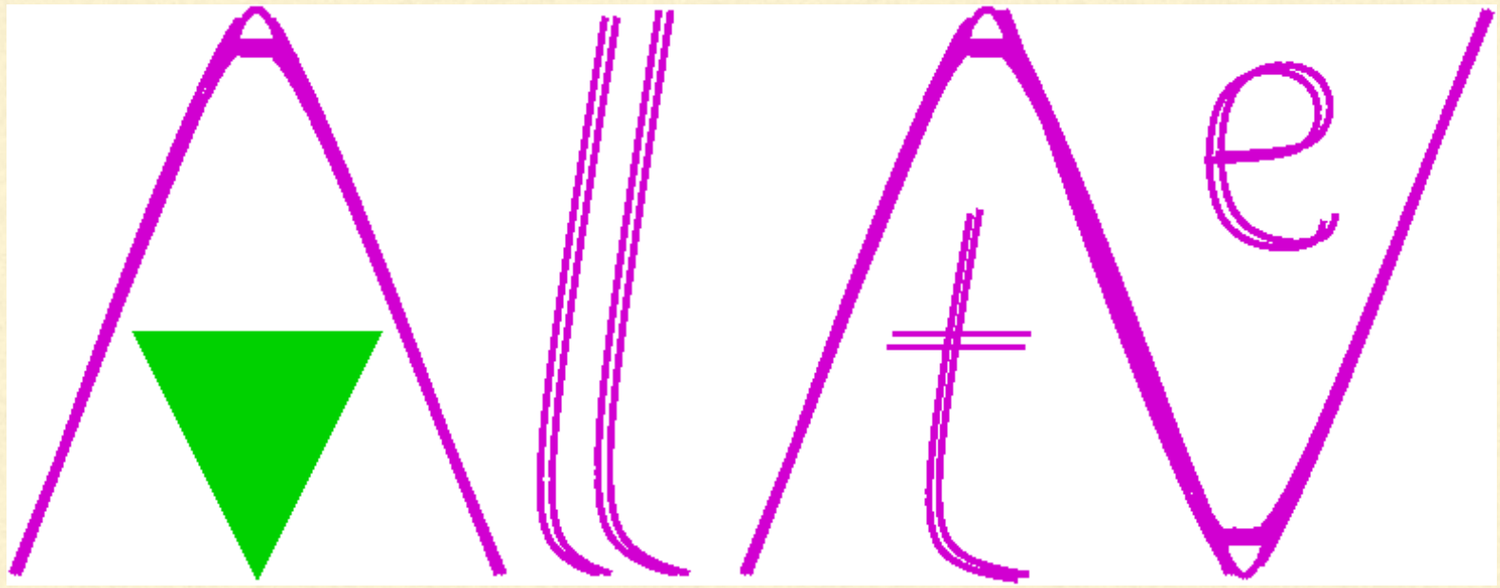
ALLNET

Ad-hoc networking for interpersonal communications



MOTIVATION FOR ALLNET

- We already have the hardware
  - every mobile device has one or more two-way radios
- where is the software?
- the infrastructure (cell towers) is great, but not always there
- but: multihop ad-hoc communication is inefficient
  - make sure can send at least text messages (e.g. for emergencies)

CROWDED FIELD

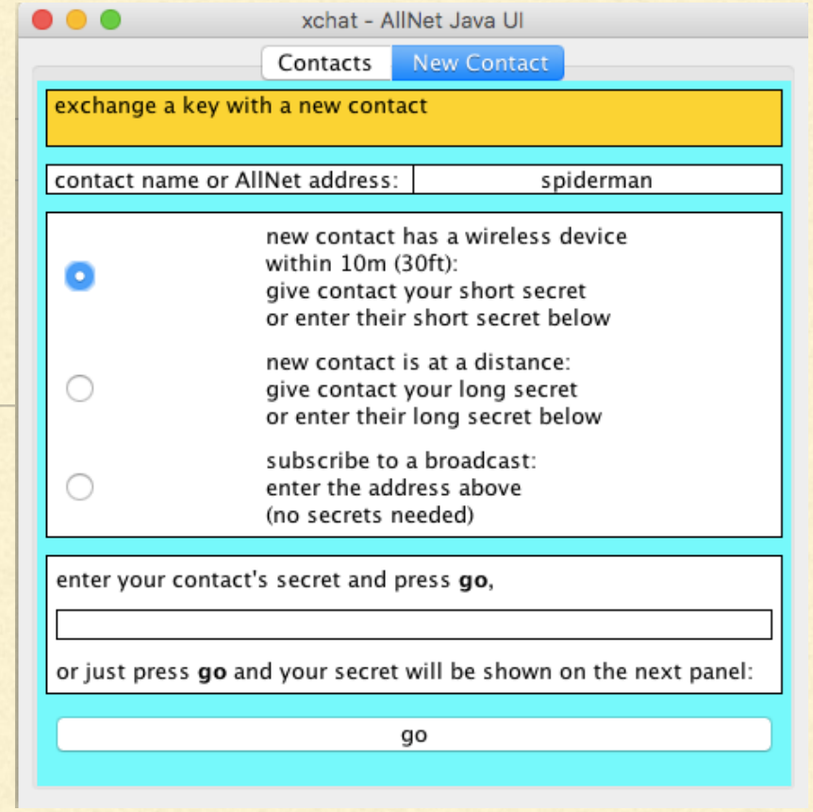
- Firechat: decentralized, but not encrypted
- Telegram: encrypted messages, centralized servers, not ad-hoc
- PGP/GPG: encrypted messages, hard to exchange keys

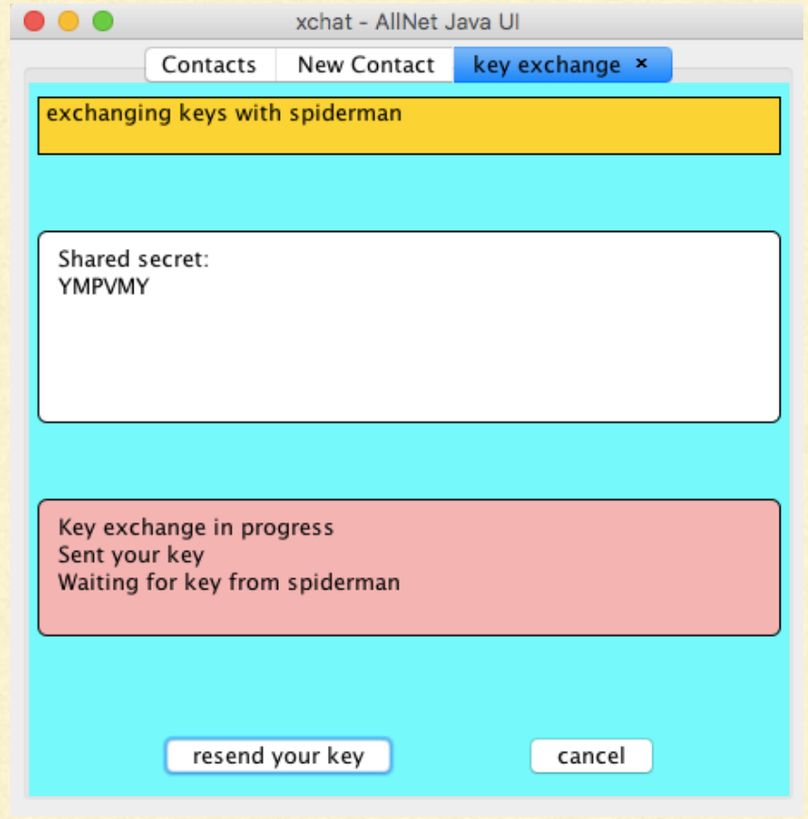
Allnet:

- encrypted messages so that forwarding devices can’t read
- straightforward key exchange
- decentralized, ad-hoc service

KEY EXCHANGE

- wireless devices carry keys
- only exchange public keys
- short string *auth* provides authentication
- *auth* is a nonce, only useful once
- 14-char *auth* for long-distance key exchange





ALLNET: OTHER FEATURES

- limit resource consumption for strangers' messages to about 1%
- prioritize own messages and messages from known senders
- anonymously track social distance
- nodes on Internet self-organize into distributed hash table (DHT)
  - allowing intermittently-connected hosts to communicate