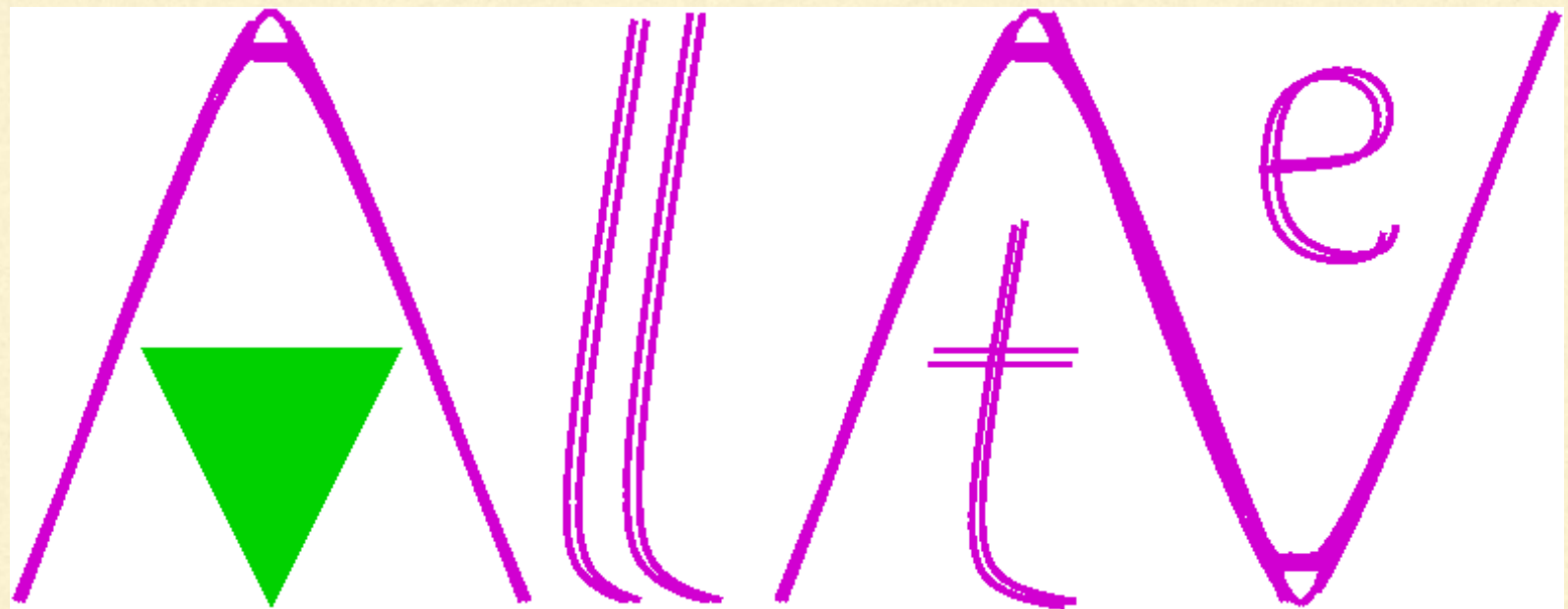

ALLNET

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

The screenshot shows a window titled "xchat - AllNet Java UI" with two tabs: "Contacts" and "New Contact". The "New Contact" tab is active, displaying a yellow header bar with the text "exchange a key with a new contact". Below this is a form with a label "contact name or AllNet address:" and a text input field containing "spiderman". There are three radio button options: the first is selected and labeled "new contact has a wireless device within 10m (30ft): give contact your short secret or enter their short secret below"; the second is labeled "new contact is at a distance: give contact your long secret or enter their long secret below"; and the third is labeled "subscribe to a broadcast: enter the address above (no secrets needed)". Below the radio buttons is a text input field with the placeholder text "enter your contact's secret and press go,". At the bottom, there is a text input field with the placeholder text "or just press go and your secret will be shown on the next panel:" and a "go" button.

The screenshot shows the same window with the "key exchange" tab active. The header bar is yellow and says "exchanging keys with spiderman". The main area is light blue. It contains a white box with the text "Shared secret: YMPVMY". Below this is a pink box with the text "Key exchange in progress", "Sent your key", and "Waiting for key from spiderman". At the bottom, there are two buttons: "resend your key" and "cancel".

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
-