Bluetooth

Larry Rudolph
Feb 16, 2006

What is bluetooth?

- Wireless, short-range communication

  - about 10 meters

- Replacement for USB cables

- Low power, low cost

- Automatically hook together mobile devices

- The term covers lots of things from HW to SW

CSAIL

Barbie Bluetooth Headset

Found this on the gizmodo site:

"Some die-hard Trekkie would probably love to get his hands on this. A guy from New Zealand modeled this Barbie doll to a) look like a Star Trek crew member, and b) act as a Bluetooth handsfree headset. Yes, that's right, it's embedded with a Bluetooth headset. According to Ms. Barbie herself:"

You can use me to make and receive calls with Bluetooth 1.1 compatible mobile phones. I have no wires. I work within a 10 meter radius of your phone so you can leave your mobile in your pocket or a bag. You turn me on/off, receive calls, make calls and pair me with other devices by pressing in the small of my back.

CSAIL

Our focus

- What we don't care about

    - bluetooth headsets, keyboards, ovens

    - how to blast advertisements at users

- What we do care about

    - how to send data between bluetooth devices using python code

- Give a foundation to let you discover more

CSAIL

Programming Concepts

- Choose a communication partner

- Desired type of communication

- Connection

  - initiate outgoing or accept incoming

- Send & Receive data

CSAIL

Choosing Partner

- Every device has a bluetooth address
  - unlike TCP, same address at all layers
  - 48-bit mac address (unique)
    - could be changed by software
- Devices have bluetooth name
  - User supplied, not unique
  - "My Phone" is a common name

Common protocols

- RFCOMM

  - com port (rs232) replacement, streaming

  - only 30 ports available

  - reliable

- L2CAP

  - connection oriented, customizable reliability

  - reserved ports: 1 -- 4095 (odd numbered)

  - unreserved: 4097 -- 32765 (odd numbered)

CSAIL

Service ID

- Every service has a 128 bit (supposedly) unique identifier -- UUID

  - some reserved, developers registered

- Service class ID

- Service Description -- human readable

- Protocol Descriptor -- which prot. used

- Profile Descriptor -- which ones, e.g. mouse

Bluetooth Freq Hopping

- Designed for BT device rich environments

- Lots of radio interference

- Divide spectrum into 72 slices

- Frequency hop between slice

  - pseudo-random hopping

  - hard to track without knowing seed

- Why pairing / discovery takes so long

HCI Tools