802.11b Wireless AP Mapping

Simon, Terry, Doug and more.

14th February 2002.

Note: this version of the slides is both incomplete and slightly out of date as they are presubmitted to make the deadline for publication. In particular there are no images.

Agenda for today

- 802.11b.
- Open Networks and Security.
- Why mapping?
- Software.
- Hardware.
- Doing it.
- Another app.
- Results, analysis.
- Business stuff.
- Future stuff.

802.11b (and other)Stuff

Wireless LAN protocol on 2.4GHz range (free, i.e. unsellable spectrum).

Base stations and cards, PCMCIA or Compact Flash.

Sexy stuff, hot next (current) big thing?

Many laptops have it built in.

Allows surfing on the toilet (female restrooms...).

Possible ISP medium, can solve last mile problem.

802.11b, More Stuff

Range, Base Station to card - 50 yards?

2.4GHz is stopped by stone, leaves, people etc (but not by tupperware).

“Security” option, WEP,

11Mbps speed, pretty fast.

Configure as access point, relay, point to point.

∃ networks in corporate buildings, smaller in homes etc.

Concrete Apps:

HSD + base station = “wired” home.

...or business

Implement the business - Arby’s, TJ, DBahn, AA.

Public space ISP.

Reaching the home.

Point to point or relay links.

Entire networks, backbone plus access.

Big ISP stuff

RBOCs dragging their feet?

CLECs going under.

Cable companies are persecuting NAT users.

Outages are common and sustained.

Bandwidth promises are not.

Satelite is one way.

Fibre, who knows.

What is happening to the BBand Revolution?

– 802.11b is in the hands of you and I –

Security

Much literature an software

End result: WEP is now next to worthless.

Open Networks

Free internet access for the people:

www.nycwireless.net (Terry Schmidt)

www.bawug.org (Bay Area)

Catchphrase: Bring down the baby bells?

“bring down” is spelt with 4 letters

Why Mapping?

- To find networks to crack into and abuse.
- Security survey (or other attributes).
- To find open networks to connect with.
- To (provide and) assess coverage of a network.
- To explore saturation of the free spectrum
- It is fun.

Software

NetStumbler (www.netstumbler.com)

Shipley's code,

Our own,

Some key features?

Note: Cards look for network themselves. You just need to be able to record what they see.

DHCP is a dangerous and wonderful thing in this domain.

Builtin 802.11b?

Hardware

Machine (palm, laptop)

802.11b Card (external antenna connection)

Antennae and spread patterns:

- omni
- panel
- dish
- yagi

GPS (with output and antenna?)

Amplifier

Transport

Location Issues

Outdoors

modern GPS (with external antenna)

compatibility?

Indoors

- Click where you are.
- Autocad generated prompts.
- Measurment protocol, plus interpolation.
- Big mouse.
- Accelerometers plus gyros.
- Deploy sensors.

Practicalities

- Weight of deployment.
- Mostly need some transport.
- Manhattan is not Nevada.
- Traffic is important.
- Sampling schemes, speed and data quality.
- Got AC?
- Repeated measures.

X10 Camera Driving

X10: Small 2.4GHz wireless cameras, advertised by annoying popunder ads.

- Hack up a base station.
- Use existing 2.4GHz antennae and amps.
- Drive and capture images with laptop via USB.
- Tag images with lat, long, time.
- Augment tags with candidate name and address data.

Leads to a fine business plan....

X10 Camera Driving cont.

The Plan:

- Web site with these annotated pictures.
- 802.11b base station at home.
- Machine in the boot of the car, boots with ign power.
- Automatic capture, annotation while driving.
- Auto-upload to web server upon getting home.
- Tagline: "You never know what you will see..."

As yet unimplemented.

Some 802.11b Results

Manhattan - 4000 APs found with Terry.

approx 964 have WEP

Less dense Metros much less found, 100s

Small towns have their fair share.

More details.....

Network Sizes

```
265 linksys
156 default
131 WaveLAN Network
127 tsunami
 93 WLAN
 78 MobileStar
 57 350 WEST 50TH (EAST SIDE)
 47 London Terrace Towers
 31 101
 27 Columbia University
 26 111e85
 19 SternOntheMove
 19 150 WEA
 18 home
 18 350 WEST 50TH (WEST SIDE)
 17 Wireless
 16 Airport
 16 740 Park Avenue
 15 Home
 15 160 EAST 65TH STREET
 13 WSR-5000
 13 ANY
  8 BusinessweekMAC1
  8 730 Park Network
  8 1065 Park Avenue
  7 nsu_universal_access
  7 micromusewireless
  7 bay1
  7 airport
  7 635 Park Network
  6 ugate
  6 CSH AirNetwork
  6 791 Park Avenue
  6 1440 Bway
  5 www.nycwireless.net
  5 voyager
  5 PRM
  5 Home Network
  5 bay3
  5 AirPort
```

“My Network...”

```
1 Aaronson’s Network
1 Angie and Scott’s Spaceship
1 Barbara Lee’s Computer Network
1 Barbara’s Airport
1 Betty Lynn’s Place
1 Bobbie’s Home Network
1 Bob’s Airport  Network
1 chel’s airport
1 Champ’s Place
1 Cubic B’s
1 dick’s powerbook
1 David’s Base Station
1 David’s Wireless Network
1 Diana’s port
1 Dick Rich’s Airport
1 ethan’s wireless 777-7F
1 Earl’s
1 f00912Amy’s Home
1 f09d29Kyle’s Airport
1 Frank’s Network
1 greg’s network
1 George’s airport
1 hil’s spaceship
1 Jessica’s AirPort Network
1 Jim’s Airport
1 liz’s airport network
1 Leslie’s Airport
1 Lipe’s Home Computer
1 Logan’s Airport Base
1 Loren’s Airport
1 Luke’s Net
1 Lu’s Appla Network
1 Lynn’s AirPort
1 Matt and Kerry’s Airport Base
1 Matt’s Airport
1 Michael’s Airport Network
1 Nina’s Network                                ***** - big!
1 Norbert’s network
```

Families

family
Family Network Base Station
Hanss Family Network
Johnson Family NYC network
Jones Family Network
Kaplan Family Foundation
Linen Family Wireless Network
Melingner Family Network
Soliman Family Airport

Addresses

100 John Street
105 WEA
1065 Park Avenue
116 Mott Street
1440 Bway
150 WEA
160 EAST 65TH STREET
176 West 87th Street
176 WEST 87TH STREET
20 EAST 74TH STREET
21 Boom
25 CPW
306 West 90th Street
350 WEST 50TH (EAST SIDE)
350 WEST 50TH (WEST SIDE)
360 east 88
4 Kims
50 E 77TH
510 PARK AVENUE
610 West End Avenue
635 Park Network
720 Park
730 Park Network
740 Park Avenue
755 WEA 9B
791 Park Avenue
845 UN Plaza 7D

Some Analyses

- Some stats on properties.

- Defaults.

- An entire multi-station network (and hence coverage).

- Locations of APs.

- Correlation with other data.

- Comparative Reach analysis.

Locating APs

Where are these base stations?

- Stupid max SNR

- Triangulation (antenna arrays?)

- Intersecting spheres (GPS problem)

- External info (phone book etc)

- The DEM?

Automatability is nice.

Consumer/Business Application

Mmmm, let us think about....

- Set up and analyse a network for use by all in some manner.

- Manage it.

- Optimise deployment.

- Target customers in footprint.

- New Products and Services?

- Phone over 802.11b?

Business Application

Suppose, we were (hypothetically) approached to consult/run a network by its owners:

Should we be able to respond by already having maps of the network?

Should we know how many street addresses appear reachable by that network?

Should we be able to find all reachable address that cannot get DSL?

Should we be able to assess the mean LD bill for an AP's reachable audience?

Conclusions?

Fun with hardware, software, getting out and about,

Lots of flexibility at this stage

Up and coming area in general.