What's on the Wireless?

David Malone

14 November 2005

Plan

1. Some 802.11 basics.
2. A little about wardriving.
3. A little about wireless in TCD.

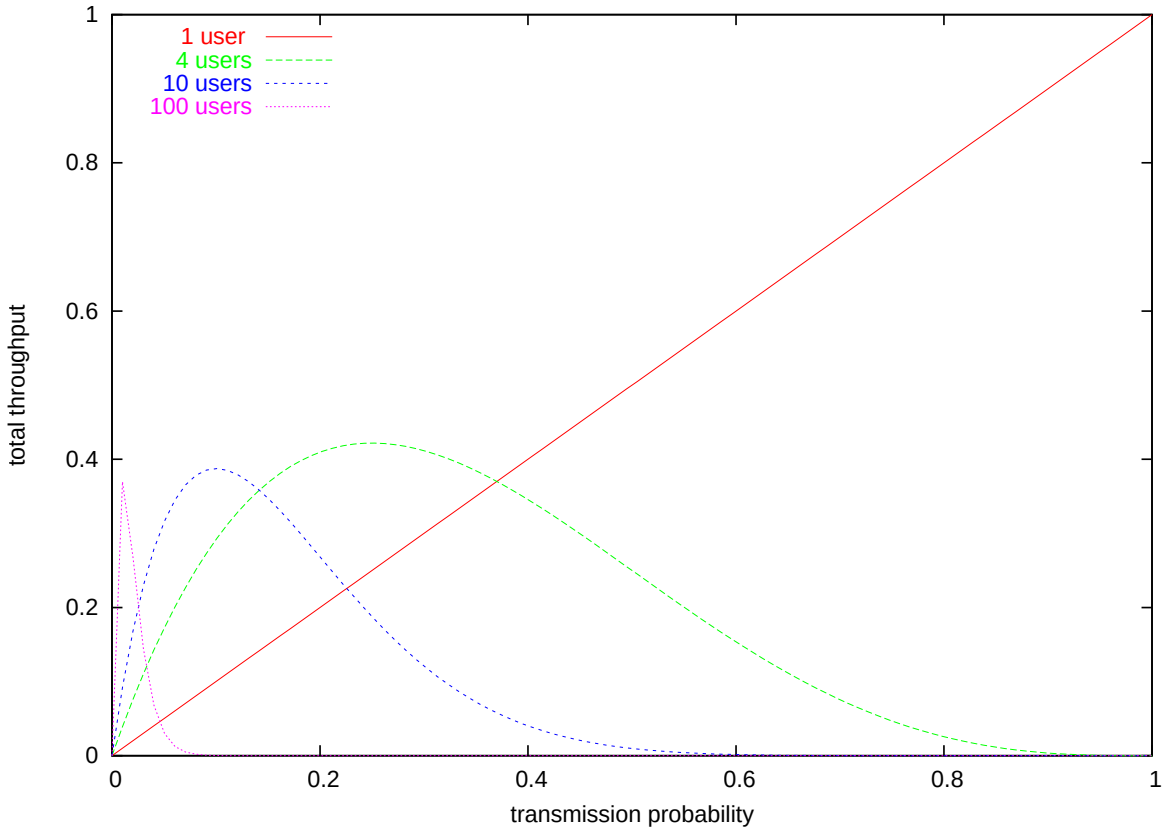
Ethernet (802.3)

- Robert Metcalfe at Xerox, mid 70s.
- 3Mbps to 100Gbps.
- Now mainly switched.
- CSMA/CD: Polite dinner party model.
- Cable length limitations.

WiFi (802.11)

- Think old shared Ethernet without a cable.
- Key difference: once you speak can't hear others.
- Need acknowledgments (ACK scheme, not NAK).
- Does back-off after every packet.

$$n\tau(1-\tau)^{n-1}$$



Bianchi Markov Modle.

Common variants

802.11b Most common variant. 2.4GHz, 11Mbps, 100m.

802.11g Most common variant. 2.4GHz, 54Mbps, 100m.

802.11a Fast variant in different band 5GHz, 54Mbps, 50m.

802.1x EAP based authentication.

e: QoS, g: faster 2.4GHz, h: mods to a, i: security, n: Faster again.

802.11 Concepts

Channel Frequency for communication (1–14).

BSSID Group of communicating individuals (MAC).

SSID Network name (20 chars).

mode Infrastructure/ad-hoc (IBSS).

Beacon Used to advertise an access point.

Association Connecting to an access point.

Other interesting differences

Original security mechanism: WEP.

- Encrypts the body of frames.
- 40 (104) bit keys.
- Default or per-station.
- No key management.

WEP Problems

Has been shown to be (badly) flawed.

- Key is usually constant.
- First byte is `0xAA`.
- Initial Vector is observable.
- Some IVs provide information about key.
- LEAP, PEAP, WPA, WPA2, ...

Wardriving

- Looking for wireless networks.
- Named after wardialing.
- Probably legal, though unauthorized access is illegal.
- Cf. Port scanning.

Wireless Cards

Old Chips Lucent Hermes, Intersil PRISM, Aironet.

New Chips Atheros, Centrino, Texas Instruments, Broadcom.

Sniffing Some chip sets more flexible than others.

Host AP Useful for building own networks.

Antenna Depends on packaging, can add omni, sector, yagi, ...

WEP/WPA Key size and supported protocols.

Software

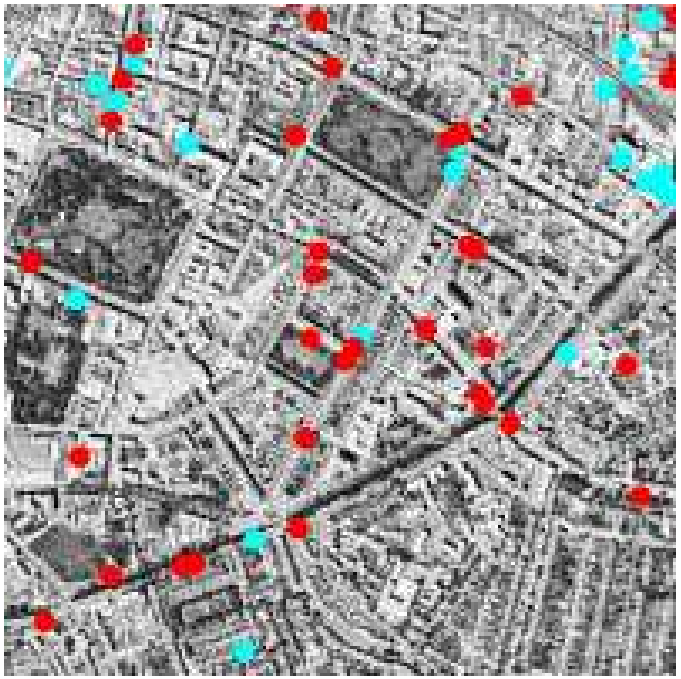
- Need good driver support by/for usual suspects.
- Now common to not provide drivers: Ndiswrapper/Project Evil.
- Sniffing for networks: kismet, bsdairtools, NetStumbler, MacStumbler,...
- Sniffing for packets: tcpdump, AirSnort, bsdairtools,...
- Network surveying.

- Dry run around TCD.
- Expand to around town.
- Industrial Estates.
- Results.

Interesting Finds

- IFSC and friends.
- Big network in the docks.
- Public service use?
- Industrial estate.
- Community networks.
- No commercial hot spots in 2002, lots now.

Before



After

War Cycling

- Found MacStumbler.
- `antenna++, farady_cage--;`
- Took a bit of getting right.
- Route to work & Clontarf.


iBook

Talking to People

- Legal advice.
- Help with mapping.
- 'Guys in a car. . . '
- Feedback.

Conference Sniffing

- FreeBSD 4.7,
- Orinoco card,
- dsniff,
- *not just wireless problem.*

Running Wireless Networks

- Have to run something.
- Dirty wireless.
- LEAP/PEAP/WPA/....
- Authenticate to gateway/IPsec.
- Captive portal (IP over DNS).

In TCD

- 4 Wireless ops.
- CS, ISS, Maths, *Researchers*.
- Only 3 channels to go around!
- ISS: 145 APs in 50 locations, 3 services.
- Registered 200→750→1500?
- In first month: 488.
- Coverage in Goldsmith to improve.

Future

- City crawling with wireless.
- 802.11n, MIMO, using 802.11e.
- WiMax, 802.16, connectivity everywhere.
- Next Gen Mobile 1Gbps, 100Mbps.