What's on the Wireless?

14 November 2005

David Malone
Plan

1. Some 802.11 basics.
2. A little about wardriving.
3. A little about wireless in TCD.
Ethernet (802.3)

- Cable length limitations.
- CSMA/CD: Polite dinner party model.
- Now mainly switched.
- 3Mbits to 1Gbps.
- Robert Metcalfe at Xerox, mid 70s.
WiFi (802.11)

- Does back-off after every packet.
- Need acknowledgments (ACK scheme, not NAK).
- Key difference: once you speak can't hear others.
- Think old shared Ethernet without a cable.
\[ I_u(1 - I_u) \]

Bianchi Markov Model.
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, f: Faster 2.4GHz, h: modes to a, i: security, n: Faster again.

Faster again.
Association: Connecting to an access point.

Beacon: Used to advertise an access point.

mode: Infrastructure/ad-hoc (IBSS).

SSID: Network name (20 chars).

BSSID: Group of communicating individuals (MAC).

Channel: Frequency for communication (1-14).

802.11 Concepts
Interesting differences:

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

Original security mechanism: WEP.
WEP Problems

LEAP, PEAP, WPA, WPA2, ...

- Key is usually constant.
- Initial Vector is observable.
- First byte is 0xAA.
- Some IVs provide information about key.
- Has been shown to be (badly) flawed.
Wardriving

Looking for wireless networks.

Named after wardialing. Probably legal, though unauthorized access is illegal.

Cf. Port scanning.
Wireless Cards

New Chips: Atheros, Centrino, Texas Instruments,
Broadcom.

Old Chips: Lucent Hermes, InterSIl PRISM, Airone.

Some chipsets more flexible than others.

Antenna: Depends on packaging, can add omni, sector,

...&... Host AP Useful for building own networks.

Wireless: Key size and supported protocols.

WEP/WPA
Network surveying.

Now common to not provide drivers.

Networks:

- Ndiswrapper/Project Evil
- Sniffer for packets: tcpdump, Airsnort, "bsdairtools"
- Sniffer for networks: Kismet, "bsdairtools"
- NetStumbler, MacStumbler
- SwinG for networks: Kismet, "bsdairtools"

Need good driver support by/for usual suspects.

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

• No commercial hot spots in 2002, lots now.

• Community networks.

• Industrial estate.

• Public service use?

• Big network in the docks.

• IFSC and friends.
Route to work & Clontarf.

Took a bit of getting right.

antenna++, faraday-cage--;

Found MacStumbler.

War Cycling
Talking to People

Feedback.

'Guys in a car...'

Help with mapping.

Legal advice.
not just wireless problem.

dsniff

Oriano card

FreeBSD 4.7

Conference Sailing
Running Wireless Networks

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

• In first month: 488.

• Registered 200–750–1500?

• ISS: 145 APS in 50 locations, 3 services.

• Only 3 channels to go around.

• CS, ISS, Maths, Researchers.

• In TCD

4 Wireless ops.
Future

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