

Internet infrastructure

Prof. dr. ir. André Mariën

Wireless networks

Wireless networks

- **WLAN: IEEE 802.11**
 - local area network
 - Office/site
 - Links computers, routers, firewalls
- **WPAN: IEEE 802.15**
 - Private area network
 - Cooperation between personal devices
 - Links devices of a computer: keyboard, headphone

802.11 a, b, g

- 802.11b
 - Used a lot up to now
 - 11 Mbps (pract: 5-7), 2.4-2.5G
- 802.11g
 - Newer network use this
 - 54 Mbps (pract: 22), 2.4-2.5G
- 802.11a
 - Next generation
 - 5G, 8 non-overlapping channels
- 802.11b & 802.11g: can coexist, 3 non-overlapping channels

- Ethernet: 10Mbps, 100 Mbps, 1000 Mbps
- ISP: < 6Mbps

Range

- 20m – 300m
- Depends on the antenna, the power, the environment
 - Power is regulated, be careful
 - Directional and dish antenna's: can capture signals from far away
 - Building material does matter

Two types of networks

- Independent configuration
 - Stations talk directly to one another
 - Basic Service Area (BSA)
- Infrastructure configuration
 - Stations talk to an access point
 - Access points may be linked into wireless networks
 - Extended Service Area (ESA)
 - Infrastructure mode

Services

- Multiple data rates are supported in both types
- Roaming is specific for infrastructure mode
- The protocol is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
 - Detection is not good enough: it is too expensive (full duplex simultaneous), and stations may not hear each other, even if the AP does
- operating in the 2 400 - 2 483.5 MHz band

Channel selection

Band 2.4-2.5 GHz

Channels:

1: 2.412

2: 2.417

...

13: 2.472

14: 2.484

Each channel: base \pm 11MHz

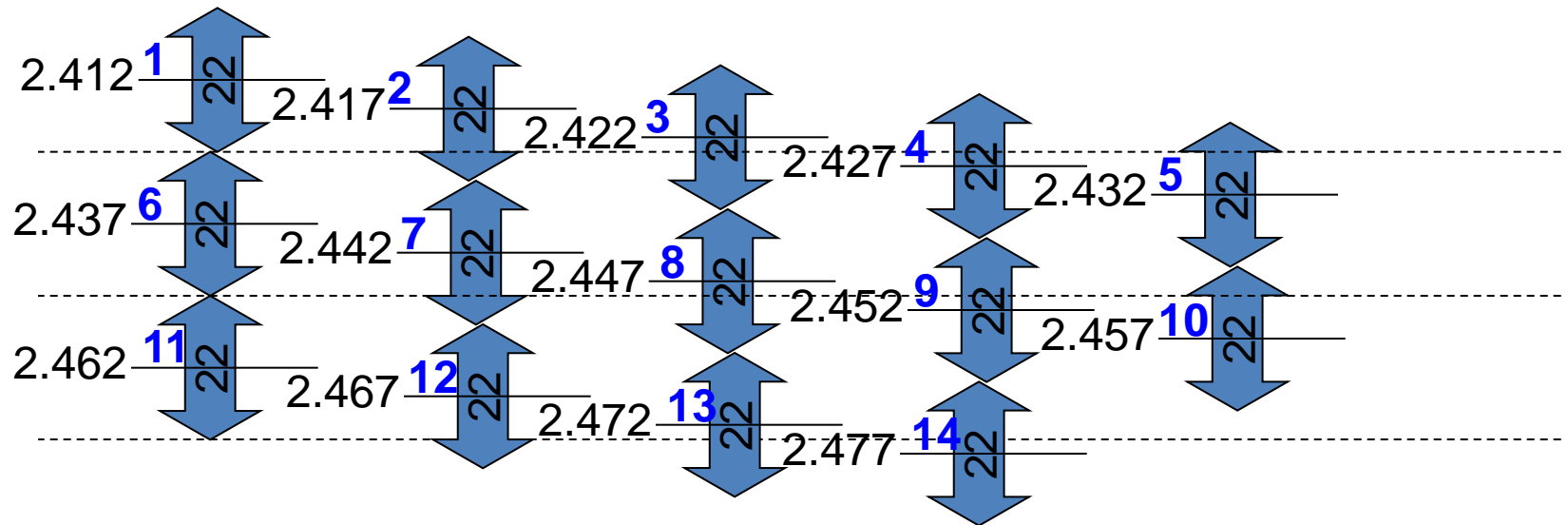
Min 5MHz between channels

Conclusion: lots of overlap

Thus: 1, 6, 11 have the least overlap

Allows for up to three network with minimal interference in the same area

Band overlap



Connection set-up

- Authentication process
 - Are you allowed on this network?
- Association process
 - Operating parameters/capabilities

Keeping connection going

- Frequency hopping
- Synchronization needed
- Roaming: switch to other/better AP

Packet types

- Management of the connection
 - Authentication/de-authentication
 - Association/re-association request/response and disassociation
 - Probe request/response
 - Beacon
- Control
 - RTS, CTS (collision avoidance)
- Data

Basic security measures

- SSID
 - Network ID
 - Broadcast: allows identification before connecting
 - Just identification
 - knowing the name suffices
 - connecting system **MUST** leak this information
- MAC address filtering
 - identification only
 - connecting systems **MUST** leak this information

Security

- Wired equivalent privacy (WEP)
 - RC4 stream cipher
 - PRNG to generate key
 - Can be implemented in Hardware/software
 - Hardware removes load from station CPU
 - One problem: broken!
- Wi-Fi Protected Access: WPA
 - a stopgap solution based on Draft 3 of the 802.11i specification
- Temporal key integrity protocol: TKIP

802.1x

- **802.1x protocol:**
 - **EAP over a wired or wireless LAN**
 - **EAP encapsulation over LANs (EAPOL).**
 - **Encapsulate EAP messages in Ethernet frames (doesn't use PPP).**
- **RFC 2284: PPP Extensible Authentication Protocol (EAP)**

802.11i

- 802.11i
 - encryption based on AES
 - meet encryption requirements for Federal Information Processing Standard 140-2 specification
 - sufficient to eliminate VPN on top of it
- Provides port-based authentication to a RADIUS server
- Streamlines WPA's key exchange process among the client, access point and authorization server by requiring fewer messages.

802.11i authentication and keys

- Authentication to RADIUS
- The authentication server creates a PMK (pair-wise master key)
 - is moved to the access point
 - exchanged with the client
 - controls both devices' access to the 802.11 channel (no matter which band)
 - used to derive the PTK (pair-wise transient key), which is actually a collection of keys that help mutually identify the devices and secure the data traffic.
- The PMK is unique to the client/AP conversation
 - Re-authentication required when roaming

Evolution of protocols

- 2001: hacker attacks on WEP had made strengthened wireless security imperative. The IEEE began work on 802.11i, an improved standard.
- 2003: the Wi-Fi Alliance created Wi-Fi Protected Access (WPA)
 - based on a subset of the then-current 802.11i draft
- 2004: WPA2

WPA

- Eye for performance
 - designed so that hardware upgrades would not be needed. The processing power of many early access points (APs) was quite limited. The RC4 cipher was chosen for WEP because it does not require a powerful CPU.
- New features
 - Kept RC4 stream cipher (cipher is not broken)
 - Use cipher correctly
 - Longer IV (48 bits, from 24)
 - Longer master key (128 bits)
 - TKIP: temporal key integrity protocol: switch keys faster
 - Add integrity checking code (move away from CRC32)
- Authentication: WPA can be used in either of two modes:
 - Personal mode:
 - This utilizes manually configured keys in the same manner as WEP
 - All clients use the same initial master key.
 - Enterprise mode:
 - Extensible Authentication Protocol (EAP): to negotiate a pair-wise master key with each client individually.
 - Verifies the identity of the client with an 802.1x server.

WPA2

- 2004: IEEE 802.11i standard
- “Counter Mode with Cipher Block Chaining Message Authentication Code Protocol” (CCMP)
- Uses Advanced Encryption Standard (AES) algorithm for authentication and data encryption.
- WPA2 also adds methods to speed the handoff as a client moves from AP to AP (roaming).

Pen-testing wireless networks

- Material
 - Pda (!), laptop
 - Wireless card + properties (prism chipset advised) + drivers
 - Antennas, amplifiers, cables & connectors
 - GPS device (link networks to locations)
- Configuration
- Software
 - Kismet (wirekismet,gkismet), ...
 - Aircrack-ng, aircrack-ng
 - WEP cracking (wepcrack)
 - 802.1x attacks (asleap-ip; MS CHAP attack)
 - Packet crafting (airjack)
- Steps
 - Footprinting
 - ESSID, WEP
 - Mitm
 - DoS

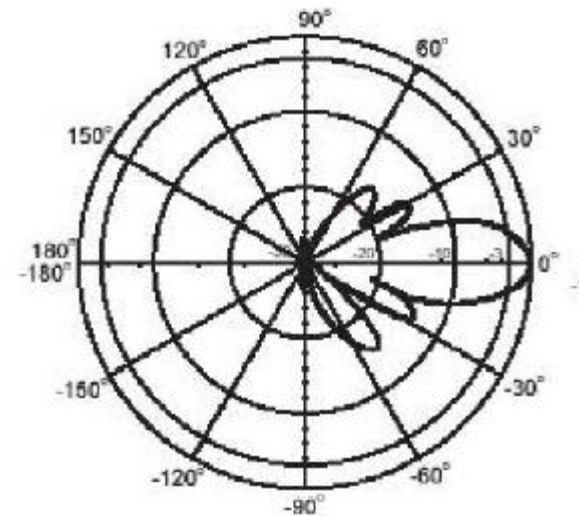
Antennas

- Omnidirectional
 - Find all networks in the neighbourhood
- Directional antennas
 - Long distance
 - Low profile

Directional antenna

The picture shows the signal's strength in all directions. Two such systems provide long range, directed connectivity.

Of course, it also means directed sniffing over long range



Horizontal

Example data: Approx. range at 2 Mbps: 26.49 miles (42.62 km). Approx. range at 11 Mbps: 20.1 miles (32.33 km). Approx. range at 54 Mbps: 4.46 miles (7.17 km).

WPAN – Bluetooth

- See: <http://www.bluetooth.com>
- Prime use: voice and data
- (unlicensed) 2.4 GHz spectrum
- Distance: 10-100 meters
- peak data rate 3 Mbps
- three modes of security
 - non-secure
 - service level enforced security
 - link level enforced security
- Low cost: chips < \$3, low power (1/5 of WiFi)
- Key concepts:
 - Discoverable – non-discoverable
 - Pairing
 - PINs

Bluejacking?

- send business cards anonymously
 - does NOT involve the removal or alteration of any data from the device.
- These business cards often have a “teaser”
- Proposed protection:
 - refuse to add the contacts to their address book.
 - Set device in non-discoverable mode

Bluebugging?

- access to the mobile phone commands
- initiate phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet.
- Vulnerable: does not affect all of the same phones as bluesnarfing.

Bluesnarfing?

- gain access to data stored on a *Bluetooth* enabled phone without alerting the phone's user of the connection made to the device.
 - Data: Phonebook, images, calendar, and IMEI (international mobile equipment identity).
 - Vulnerable: Only specific older *Bluetooth* enabled phones are susceptible to bluesnarfing.
- Proposed protection:
 - device in non-discoverable mode

References

<http://grouper.ieee.org/groups/802/11/main.html>

<http://wireless.ittoolbox.com/browse.asp?c=WirelessPeerPublishing&r=%2Fpub%2FJK052202%2Epdf>

<http://standards.ieee.org/getieee802/802.11.html>

WI-FOO The secrets of wireless hacking, A. A.

Vladimirov, K. V. Gavrilenko, A. A. Mikhailovsky

CAPWAP

- Control and provisioning of Wireless Access Points
 - RFC 3990: CAPWAP problem statement
 - RFC 4564: Objectives for CAPWAP
 - RFC 5418: CAPWAP Threat Analysis for IEEE 802.11 Deployments
 - RFC 5415: CAPWAP Protocol Specification
- Datagram Transport Layer Security: DTLS
 - RFC 4347: Datagram Transport Layer Security
 - “a datagram-compatible variant of TLS”

RFC 3990: Problem statement

- each AP is an IP-addressable device requiring management, monitoring, and control
- distributing and maintaining a consistent configuration throughout the entire set of access points in the WLAN is problematic
- dealing effectively with the dynamic nature of the WLAN medium itself is difficult
- securing access to the network and preventing installation of unauthorized access points is challenging

Session establishment

- AP joining
- Steps:
 - Discovery request
 - Discovery response
 - DTLS session establishment
 - Join request
 - Join response
 - Configuration status request
 - Configuration status response
 - Run state

Access point registration

- AP discovery
- AP joining

Reference

- Deploying and troubleshooting CISCO wireless LAN controllers, Mark Gress, CISCO press, 2009