K.U.Leuven

Internet Infrastructure

Prof. dr. ir. André Mariën

Wireless networks

Table of contents

Wireless network types

There are a few different types of wireless networks. The two most commonly found are WiFi and Bluetooth.

Bluetooth

Bluetooth is not further discussed. It is defined in standard IEEE 802.15, Wireless Private network (WPAN). As the name says, it is supposed to be used for a private area network, more precisely for cooperation between your personal devices. It is used to connect devices, like a computer, to a keyboard, headphone, camera etc. It uses low power, short range connectivity. It is convenient for wireless communication between PDA and GSM for use as a modem, for synchronization of data (calendar, email).

WiFi

WiFi is the name given to the Wireless LAN according to IEEE 802.11. WiFi is a technology for the local area network, spanning an office, possibly a site. It can link computers, routers, firewalls, printers and other WiFi enabled devices. For WiFi, there are three variations: 802.11 a, b and g. Many of the devices in use are still 802.11b, with speeds theoretically up to 11 Mbps. Just like with regular Ethernet, a WiFi network will not achieve these maximum rates but be restrained to 5 – 7 Mbps. 802.11b uses the 2.4-2.5 Ghz band for its transmissions. This is a non-regulated band in most countries, as long as you stay under a certain power. Conflicts may arise with other equipment using the same band.

WiFi using 802.11g operates at higher speeds, up to 54 Mbps, with a realistic 22 Mbps, and operates in the same band as 802.11b. Both b and g only have three real separated bands, which is difficult when trying to cover larger areas with multiple zones.

802.11a is quickly making grounds. Its main advantage is that it operates in a wider band, 5Ghz, allowing 8 non-overlapping channels.

Just for reference, wired Ethernet uses always 10Mbps at least, but home systems start shipping with 1 Gbps connectors. On the other hand, for web surfing and similar remote activities, the ISP connection is usually below 6Mbps, so the wireless gateway is not the bottleneck.

Range

The range of a wireless network depends on a lot of factors, and is mostly in the range 20m – 300m. But surprises happen in both directions. The range depends on the antenna, the power, and the environment. The maximum power is regulated, be careful. Anyway, high power antennas may have other issues, as the continuous discussion about the risks of GSM radiation keeps going. Directional and dish antenna's can capture signals from far away. Very far away.

Building material does matter. Not just the type of material that is being used, but also other elements like the distance between the steel/iron bars, the use of metals in glass, and more than you can think of. Before deploying a costly wireless network, it is wise to measure what the signals strengths would be for the correct placing of the access points. If you expect one for each floor, but end up needing one for each room on a floor, your infrastructure picture looks very different.

Configurations

There are two types of network configurations with WiFi. The most common is infrastructure mode, the more basic mode is ad-hoc.

In an ad-hoc, or independent configuration, the stations talk directly to one another. This mode is sometimes referred to as Basic Service Area (BSA).

The more interesting, from a business perspective, is the infrastructure configuration. All stations talk to an access point. These access points may be linked together into a larger wireless network. It is also referred to as the Extended Service Area (ESA). In such a network, roaming may become a necessity: when a station moves from point A to point B, it may connect to different APs as it moves to keep the best signal strength. This move should be transparent ad fluent.

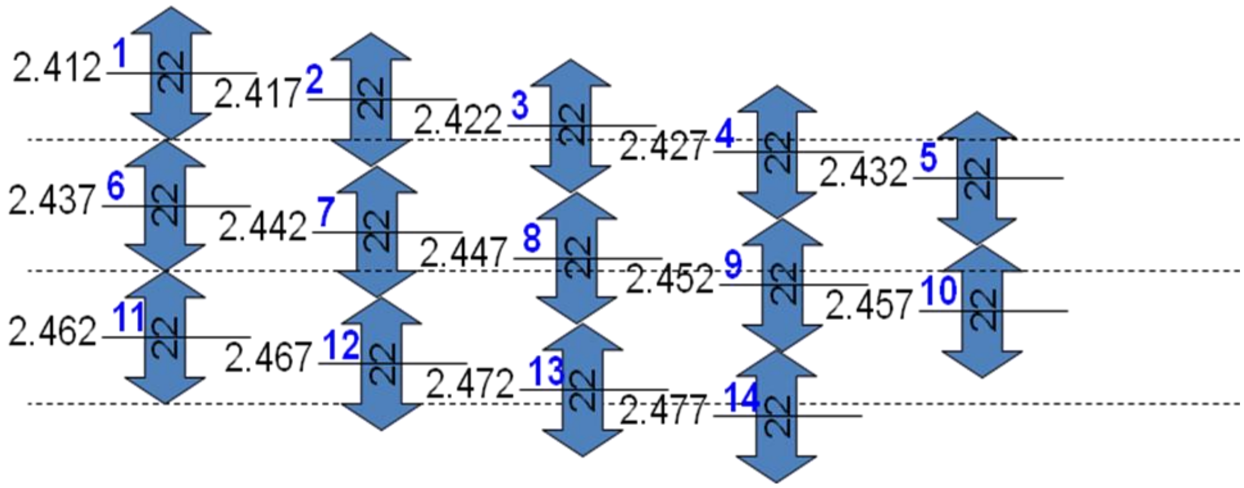
Protocol

The protocol used for WiFi 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 (other side of the AP, diametrically opposite, for instance).

Band and channels

WiFi b and g are operating in the 2 400 - 2 483.5 MHz band. There are 14 channels in this band. You have to configure the channel on which the AP is operating.

How are these channels allocated? Each channel has a base frequency, and uses that frequency +- 11MHz. There should be a minimum of 5Mhz between channels. Conclusion: with 14 cannels there are lots of overlap. The channels 1, 6, 11 have the least overlap.



This analysis shows that b and g allow for up to three network with minimal interference in the same area.

Connection

To connect to a wireless network, first the network must be found and identified, it's capabilities and operating parameters must match the capabilities of the connecting station. For open networks, you are now connected.

But most networks should be "closed": only authorized stations should be able to connect. This is the purpose of the authentication process.

The next steps are similar to a wired connection: get your configuration for IP set-up, and use the network.

Once established, the connection must be kept going. Some packets are dedicated to connection management. These handle

  - Authentication/de-authentication
  - Association/re-association request/response and disassociation
  - Probe request/response
  - Beacon (I am here): sending the SSID
    - Network ID
    - It is usually broadcast: allows identification before connecting
    - Just identification: knowing the name suffices
  - Control, like RTS, CTS (collision avoidance)

Security

WiFi networks provide security measures. The first ones are rather basic (not strong):

- Do not broadcast the SSID,
  - So it must be guessed? No, it can be found on existing connections
- Apply MAC address filtering
  - This is identification only, and connecting systems MUST leak this information

More advanced security measures provide confidentiality and stronger authentication

The first version was Wired equivalent privacy (WEP). It uses and RC4 stream cipher (good), a PRNG to generate key (may be good), can be implemented in Hardware/software (convenient). One small problem: WEP is broken!

New standards have plugged the whole, for instance Wi-Fi Protected Access: WPA. WPA is a consequence of a stopgap solution based on Draft 3 of the 802.11i specification. It incorporates the Temporal key integrity protocol: TKIP .

For use in organizations, the standard IEEE802.1x links WiFi networks with corporate authentication mechanisms. The 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).

The 802.11i provides confidentiality, via encryption based on AES. It is supposed to be strong enough to meet the encryption requirements from the Federal Information Processing Standard 140-2 specification. This should be largely enough to even to eliminate the use of (another) VPN on top of it. It Provides port-based authentication to a RADIUS server. It streamlines WPA's key exchange process among the client, access point and authorization server by requiring fewer messages.

Pen-testing wireless networks

IMPORTANT: do not do this unless you have written authorization, or you are the owner.

You need hardware equipment:

- PDA (!), laptop
- Wireless card + properties (prism chipset advised) + drivers
- Antennas, amplifiers, cables & connectors
- GPS device (link networks to locations)

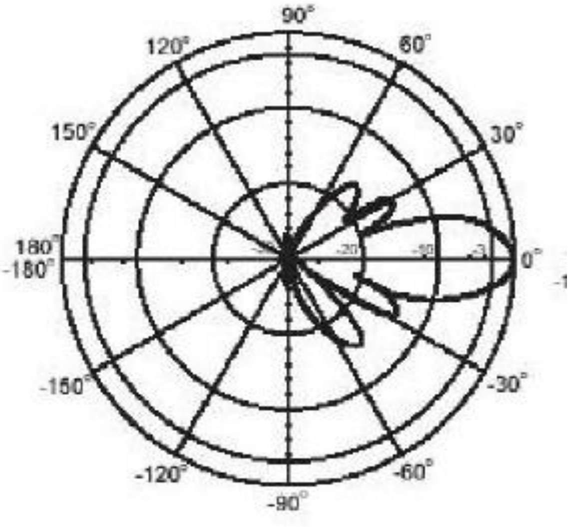
You need to be able to configure the hardware right for the intended use.

You need some software:

- Kismet (wirekismet,gkismet), …
- Airsnort, cain&abel
- WEP cracking (wepcrack)
- 802.1x attacks (asleap-ip; MS CHAP attack)
- Packet crafting (airjack)

Key hardware: Antennas

- Omni directional: to Find all networks in the neighborhood
- Directional antennas: work over Long distance, or keep low profile



Horizontal

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

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).

Silence.

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