Indoor WLAN Design

Part X: Existing Physical Layers and the Future of 802.11

Kjell Jørgen Hole
UiB

Last updated 16.02.09

Mail: `Kjell.Hole@ii.uib.no`
URL: `www.kjhole.com`

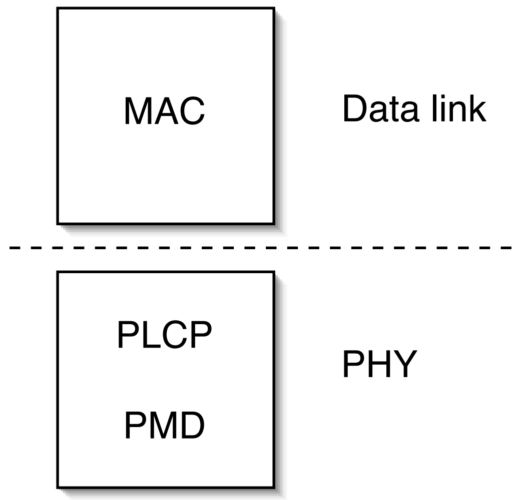
Outline

- 802.11 physical-layer architecture
- Types of spread spectrum signalling techniques
- Standardized 802.11 spread spectrum physical (**PHY**) layers
  - 802.11a vs. 802.11b
- The 802.11g PHY
  - high-speed layers: 802.11g vs. 802.11a
- Predictions and key challenges

Physical-Layer Architecture

- The physical layer is divided into two sublayers:
  - **Physical Layer Convergence Procedure** (PLCP) Upper component of PHY. Each PHY has its own PLCP, which provides auxiliary framing to the MAC. Normally, frames include a preamble for synchronization of incoming transmissions
  - **Physical Medium Dependent** (PMD) Lower component of PHY, responsible for transmitting RF signals
- The physical layer also implements a *Clear Channel Assessment* (CCA) function to indicate to the MAC when a signal is detected

MAC and PHY Components



Spread Spectrum

Spread Spectrum Signalling technique. Transmitter utilizes mathematical functions to diffuse signal power over a large range of frequencies. Receiver performs inverse operation

Spreading the transmission over a wide band makes transmission look like noise to a traditional narrowband receiver

Types of Spread Spectrum

Frequency-Hopping (FH) systems jump from one frequency to another in a random pattern, transmitting a short burst at each subchannel

Direct-Sequence (DS) systems spread the power out over a wider frequency band using mathematical coding functions

Orthogonal Frequency Division Multiplexing (OFDM) divides an available channel into many subchannels and encodes a portion of the signal across each subchannel in parallel

Standardized PHY Layers (1)

Three PHY layers were standardized in 1997:

- **FH** spread-spectrum radio PHY, low-rate 1- and 2 Mbps layer
- **DS** spread-spectrum radio PHY, low-speed 1- and 2 Mbps layer used in 802.11b
- **Infrared Light** (IR) PHY, no products use IR PHY

Standardized PHY Layers (2)

Two more layers were published in 1999:

- 802.11b: **High-Rate Direct Sequence** (HR/DS) PHY, 5.5 and 11 Mbps
- 802.11a: **OFDM** PHY, up to 54Mbps

All radio PHYs, except 802.11a OFDM PHY, transmit in the microwave ISM band at 2.4GHz

802.11a Details

- Each 20MHz OFDM channel consists of 52 subcarriers. Four subcarriers are used for *pilot symbols*. The 48 remaining subcarriers transmit data

- The 48 subcarriers provide transmissions of 6, 9, 12, 18, 24, 36, 48, or 54Mbps of which 6, 12, and 24Mbps are mandatory for all products

- There is an inverse relationship between data rate and range

More on 802.11a

- Twelve OFDM channels divided into three different bands, each band with a different output power limit

- Some 802.11a devices support a "Turbo Mode" that provides for 72 or even 108Mbps data rates. The benefit is limited because:
  - Two OFDM channels are combined to achieve the increased data rate, reducing the number of available OFDM channels
  - Channel binding is *not* part of the 802.11a specification
  - The MAC was not designed to support these data rates

HiperLAN2

- *European Telecommunications Standards Institute* (ETSI) standard utilizing OFDM in the 5GHz frequency range

- HiperLAN2 provides data rates up to 54 Mbps at the physical level for short-range communications in indoor and outdoor environments

- The core parts of the specification were finalized in 1999. HiperLAN2 is *nearly* identical to the competing IEEE 802.11a standard at the physical level

HiperLAN2 vs. 802.11a

- 802.11a and HiperLAN2 have very different MAC layers. The HiperLAN2 MAC supports traffic classes and is much more sophisticated than the 802.11 MAC

- HiperLAN2 is based in large part on ATM. For this reason, it is more difficult to implement than 802.11a

- HiperLAN2 has no support from the wireless LAN community and is DEAD

802.11a vs. 802.11b (1)

802.11a transmits in the 5GHz band. Compared to 802.11b transmitting in the 2.4GHz ISM band, this leads to:

- Higher path losses, i.e., more BSs are needed to cover a given area
- Higher transmit power, i.e., 802.11a may not be well-suited for battery-powered MSs
- Less interference from other devices in the 5GHz band since it currently does not have much traffic. This advantage will diminish over time

802.11a vs. 802.11b (2)

More spectrum space at 5GHz than at 2.4GHz leads to:

- Higher speed. 802.11a supports data rates up to 54 Mbps at the physical level, while 802.11b only supports 11 Mbps

- More channels. 802.11a supports *twelve* separate non-overlapping OFDM channels (eight for indoor use and four for outdoor), while 802.11b has only *three* such channels

802.11g

- The 802.11g standard was ratified on 12 June, 2003

- It combines some of the best aspects of the 802.11b and 802.11a standards:
  - utilizes OFDM to offer 802.11a data rates in the 2.4GHz band
  - mandatory implementation of 802.11b modes, i.e., backwards compatibility with MSs utilizing 802.11b PCMCIA cards

802.11g vs. 802.11a (1)

802.11g transmits in the 2.4GHz ISM band, while 802.11a transmits on 5GHz band. Because of this 802.11g has:

- Lower path losses, i.e., less BSs are needed to cover a given area
- Lower transmit power, i.e., 802.11g is well-suited for battery-powered MSs
- More interference. The 2.4GHz band is more crowded than the 5GHz band

802.11g vs. 802.11a (2)

Less spectrum space at 2.4GHz than at 5GHz leads to:

- Less channels. 802.11g supports only *three* separate non-overlapping channels, while 802.11a has *twelve* channels

Does 802.11a Still Have a Real Mission?

- Wireless consumers are primarily price-driven; power usage, range, and data rates are less important. This has given *g* a decisive edge over *a* at the retail level

- Many BSs have dual-mode or even tri-mode radios, including a 802.11a radio (see next slide)

Dual-Band Solutions

802.11a/802.11b dual-band, dual-mode radios 54Mbps maximum data rate multiplied by 8 (indoor) channels equals a capacity of 432Mbps, and 11Mbps maximum data rate multiplied by 3 channels equals 33Mbps for a combined capacity of 465Mbps

802.11b/802.11a/802.11g dual-band, tri-mode radios 54Mbps maximum data rate multiplied by 11 channels equals a capacity of 594Mbps

802.11g Products

- Apple was one of the first companies to introduce 802.11g devices. 802.11g *AirPort Extreme* BS supports
  - transmission power control
  - wireless bridging of BSs
  - bridging is available with both internal and external antennas

Transmission Power Control

- Possible to adjust the range of network by increasing or decreasing the amount of power the BS is transmitting

- Some people claim that power control helps ensure network security
  - this is complete nonsense

Wireless Bridging

- Wireless bridging, also referred to as *Wireless Distribution System* (WDS), enables a BS to connect to another BS and use its Internet access

- One BS is the primary station and is connected directly to the wired network. A second BS is the remote and uses the Internet connection of the primary

- The primary and remote combine to create a larger wireless network that uses the primary's physical network connection

Predictions

- 802.11 will help establish broadband Internet access for the general population

- Wi-Fi hotspots will offer easy and cheap broadband access to anyone with a laptop or PDA

- Wi-Fi hotspots will enable “suspend and go, open and resume” experience

Key Challenges

1. Network planning
2. Network management
3. Ease of use
4. Security
5. Mobility

1. Planning an Enterprise Network

- A well functioning enterprise-class network requires planning:
  - users have come accustomed to high-performance Ethernet connections. To avoid frustrating users, it is therefore important to provide sufficiently large bandwidth when designing the wireless network
  - integrating a wireless network into an existing wired infrastructure will increase networking costs initially, but a phased approach can keep the cost manageable

The Dreaded Walkabout

- The process of determining RF signal strength and propagation in the intended coverage area is costly and time consuming
  - the accuracy of this site survey is often short-lived

- Experience shows the walkabouts do not significantly reduce the trial and error associated with placing BSs within the intended coverage area

! Some new BSs can adjust signal strengths and select suitable channels on their own

Capacity vs. Coverage

- It is important to distinguishing between designing merely for RF coverage versus designing for network capacity

- The wireless network provides shared, not switched, connections. This makes it difficult to design a wireless network with large enough capacity

- The traditional site survey followed by the calculation of BS placements and channel selections do not allow us to build networks that scale

2. Network Management

- It is difficult to manage large Wi-Fi networks because
  - the physical layer, i.e. the wireless links, are vulnerable to many sources of interference, such as nearby Wi-Fi networks under management of other organizations

! There is a great need for powerful physical-layer management tools

Rougue BSs

- Employees with novice experience from deployment of a BS at home feel empowered to set up their own BSs at work, with no consideration for IT policies and security

- SOHO BSs may be programmed with a default setting of no security, and the limited built in security may not be sufficient in the enterprise

! There exist management tools that discover rougue BSs

3. Ease of Use

- Simpler and more robust configuration of BSs and MSs are needed

- Universal "plug and play" operation is needed, must include security features

- Commercial hotspots must make it simple
  - for one-time users to pay on site
  - for first-time users to sign up
  - for returning users to be authorized

4. Security

- Wi-Fi networks with WEP are vulnerable to eavesdroppers and other hackers

- Two approaches have been developed to improve the security
  - VPN on top of the insecure wireless links and backbone network
  - WPA2 standard to protect the air link between MS and BS

Problems

- WPA does not support mobility between different subnets

- Client VPNs do not scale easily because of the cryptographic load they place on the VPN server and the significant client configuration required

! Need wireless security technique that scales and supports roaming

5. Mobility

- The following options are used to add mobility to current wireless networks:
  - put all wireless users on the same subnet, and force all wireless users to be routed to their resources
  - use the Mobile IP protocol, which requires a new routing protocol on all edge routers and a special proxy service in the BSs
- Unfortunately, these techniques have a large impact on configuration and deployment of the existing wired backbone structure

Future Mobility

- Mobility more akin to the global roaming capability of cellular systems is needed

- Global roaming requires uniform mechanism for handling
  - authentication
  - authorization
  - accounting

- Mobile IP is needed for always-on Wi-Fi mobility

The End

- In the future, more and more computers will access networks through wireless links
- 802.11g is much more popular than 802.11a
- 802.11n is likely to take over in the long run
- While 802.11i has solved some of the most pressing security problems, more efficient security techniques are needed to handle the security in large networks