Nomadic Communications

802.11 - PHY

UNIVERSITÀ DEGLI STUDI DI TRENTO

Renato Lo Cigno
LoCigno@disi.unitn.it - Tel: 2026

Dipartimento di Ingegneria e Scienza dell’Informazione

Home Page: http://isi.unitn.it/locigno/index.php/teaching-duties/nomadic-communications

Copyright

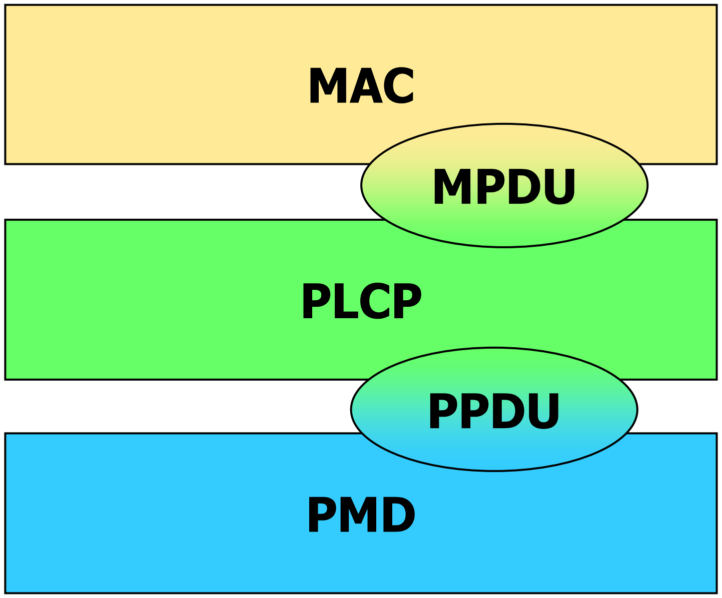
Physical Layer

A collection of different access techniques:

- Infrared (IR), never really used
- Frequency hopping spread spectrum (FHSS), 1-2 Mbit/s now obsolete
- Direct sequence spread spectrum (DSSS), 1,2,5.5 and 11 Mbit/s, the most diffused till 3-4 years ago
- Orthogonal Frequency Division Multiplexing (OFDM), nothing to do with FDM, this is a modulation technique 6 to 54 Mbit/s now the most used, and beyond
- Four different standards: 802.11; /b; /a/h/g; /n

PHY layer subdivision

- PLCP: Physical Layer Convergence Protocol
- PMD: Physical Medium Dependant
- PPDU contains the PHY layer headers stripped when the PDU is passed to the MAC
- PMD defines the specific electromagnetic characteristics used on different PHY means



- PLCP Header
  - Is actually already dependent on the PMD
  - Includes sync preambles and further info on the encoding of the remaining part of the MPDU

UNIVERSITÀ DEGLI STUDI DI TRENTO

Infrared

- Works in the regular IR LED range, i.e. 850-950 nm
- Used indoor only
- Employes diffusive transmissions, nodes can receive both scattered and line-of-sight signals
- Max output power: 2W
- Never really implemented ... tough can have "reasons" in some environments, and is very cheap
- Tx uses a LED, Rx a Photodiode
- Wavelength between 850 and 950 nm

Infrared

- Modulation is “baseband” PPM (Pulse Position Modulation), similar to on-off keying with Manchester encoding to ensure constant sync transisions
- 1 Mbit/s: 16/4 PPM
  - 0000 → 0000000000000001
  - 0001 → 0000000000000010
  - 0010 → 0000000000000100
  - 0011 → 0000000000001000
  - 0100 → 0000000000010000
  - ...
- 2 Mbit/s: 4/2 PPM
  - 00 → 0001
  - 01 → 0010
  - 10 → 0100
  - 11 → 1000
- Pulses are 250 ns

IR PLCP frame

SYNC	SFD	DR	DCLA	LENGTH	CRC	PSDU

- SYNC: variable length, synchronization and optional fields on gain control and channel quality
- SFD (Start Frame Delimiter): 4 L-PPM slots with a hex symbol of 1001. This field indicates the start of the PLCP preample and performs bit and symbol synchronization
- DR (Data Rate): 3 L-PPM slots and indicates the speed used:
  - 1 Mbps: 000; 2 Mbps: 001
- DCLA (DC Level Adjustment): used for DC level stabilization, 32 L-PPM slot and looks like this:
  - 1 Mbps: 00000000100000000000000010000000
  - 2 Mbps: 00100010001000100010001000100010
- LENGTH: number of octets transmitted in the PSDU: 16-bit integer
- CRC: header protection – 16 bits
- PSDU: actual data coming from the MAC layer; Max 2500 octets, Min 0

802.11 radios: Spread Spectrum

- All radio-based PHY layers employ Spreas Spectrum
  - **Frequency Hopping :** transmit over random sequence of frequencies
  - **Direct Sequence**: random sequence (known to both sender and receiver), called **chipping code**
  - **OFDM**: spread the signal ove many subcarriers with FFT based techniques

802.11 radios: Power

- Power radiation is limited to
  - 100mW EIRP in EU
  - 100mW EIRP in USA
  - 10mW EIRP in Japan
- NIC cards are the same all over the world: changing power is just a matter of firmware config.
- EIRP: Equivalent Isotropic Radiated Power
  - In practice defines a power density on air and not a transmitted power
- Using high gain antennas (in Tx) can be (legally) done only by reducing the transmitted power or to compensate for losses on cables/electronics

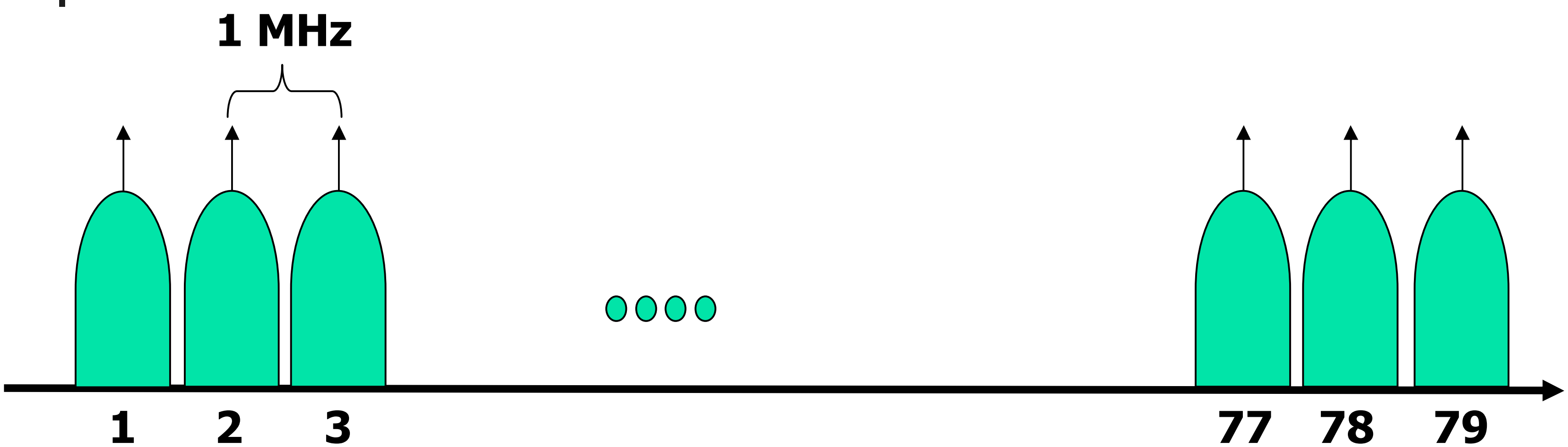
802.11 PHY evolution

st—year	Freq/Bandw	Data Rates (Mbit/s)	SS technique	Max dist in—out
- --97	2.4GHz/20MHz	1,2	FHSS	20-100
b – 99	2.4GHz/20MHz	5.5,11	DSSS	25-150
a/h – 99	5.0GHz/20MHz	6,9,12,18,24,36,48,54	OFDM	20-150
g – 03	2.4GHz/20MHz	6,9,12,18,24,36,48,54	OFDM	20-150
n – 09	2.4GHz/ 20/40MHz	15,30,45,60,90, 120,135,150 (40 MHz); divide by 2 for 20 MHz	OFDM	40-250

Band allocations

- ISM: Industrial Scientific Medical
  - Unlicenced bands for generic use
  - Normally not used for communications (cfr Cellular, TV, Radio, ...)
  - Law dictates limits in use, but do not guarantee interference-free operations
  - Similar to radio-amateurs bands ... but for the fact that those are only for study and not for commercial use
- 2.4—2.5 GHz
  - Actually 83.5 MHz of bandwidth in EU (13 channels) and 71.5 in US (11 channels)
- 4.9—5.9 GHz
  - Actual bandwidth assigned depends on countries, in US and EU there are normally 20-25 channels (about 120-150 MHz of bandwidth)

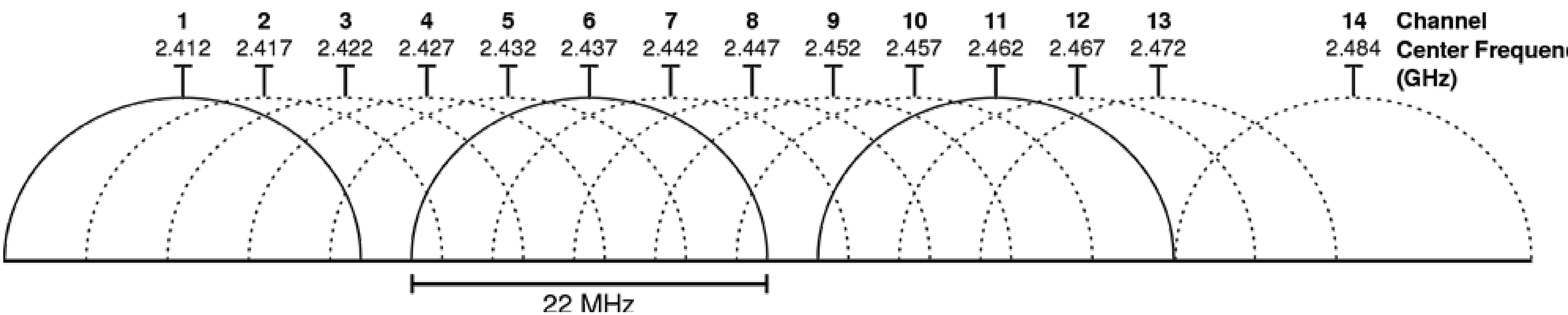
2.4 GHz channels for 802.11 FHSS



- 79 1 MHz channels
- Limits Tx speed since Tx happens on one single channel at a time

UNIVERSITÀ DEGLI STUDI DI TRENTO

2.4 GHz channels for 802.11b/g

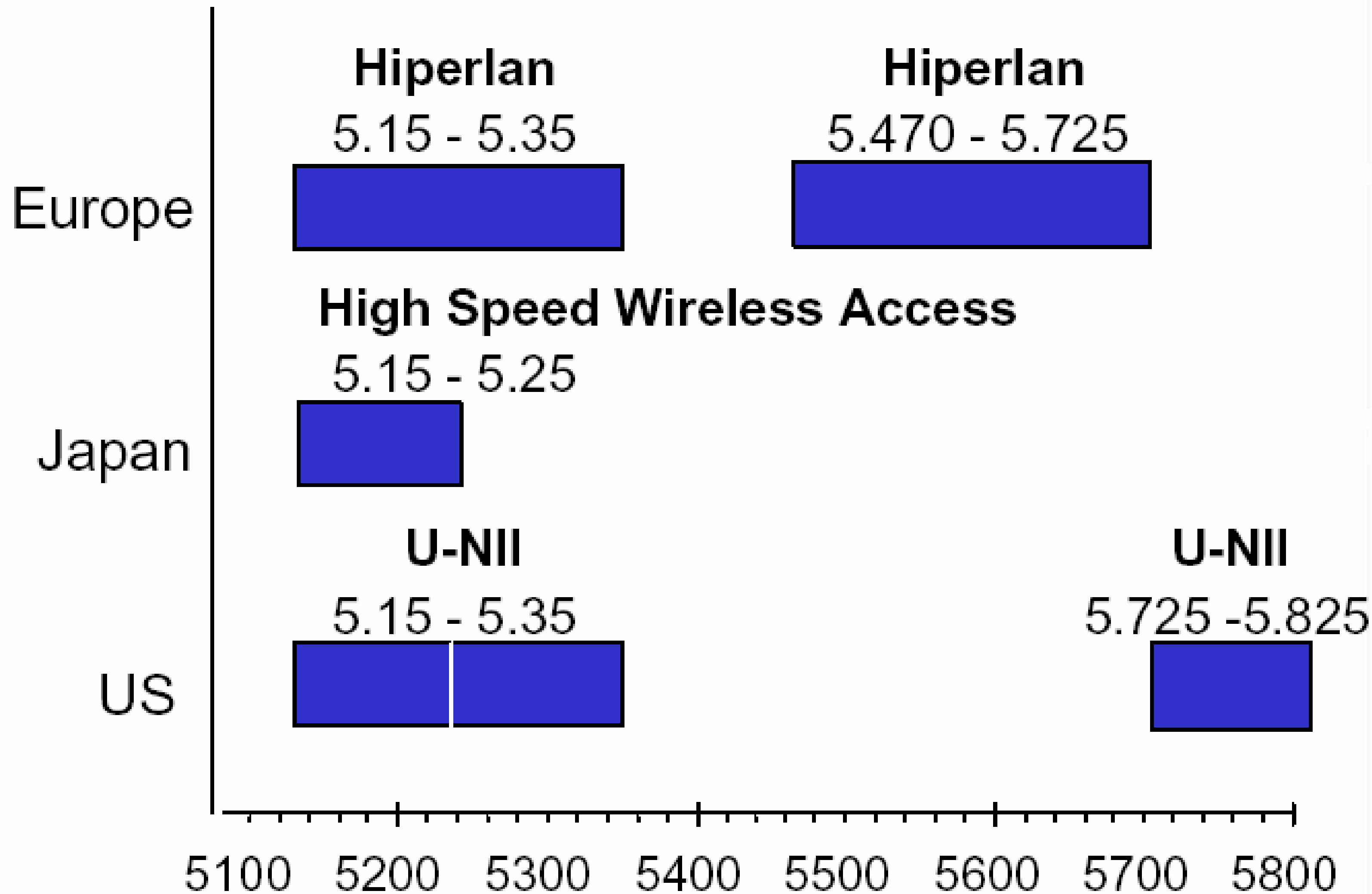


- At most 3 independet (orthogonal) FDM channels
  - 1,6,11; 1,7,12; 2,7,12; 1,7,13, ...
- Partially overlapping channels are noxious for Carrienr Sensing → exposed and hidden terminals result

5 GHz channels for 802.11a

- Overlapping channels are avoided
  - in US 12 non-overlapping channels centered at
    - 5.180, 5.200, 5.220, 5.240, 5.260, 5.280, 5.300, 5.320
    - 5.745, 5.765. 5.785, 5.805
  - in EU the frequencies above are for hyperlan2 (licensed) thus intermediate frequencies are used
    - 5.35—5.47 GHz 6 non overlapping channels

Global 5 GHz band plan



Original by Martin Johnsson: http://www.hiperlan2.com/presdocs/site/whitepaper.pdf

IEEE 802.11/b PHY

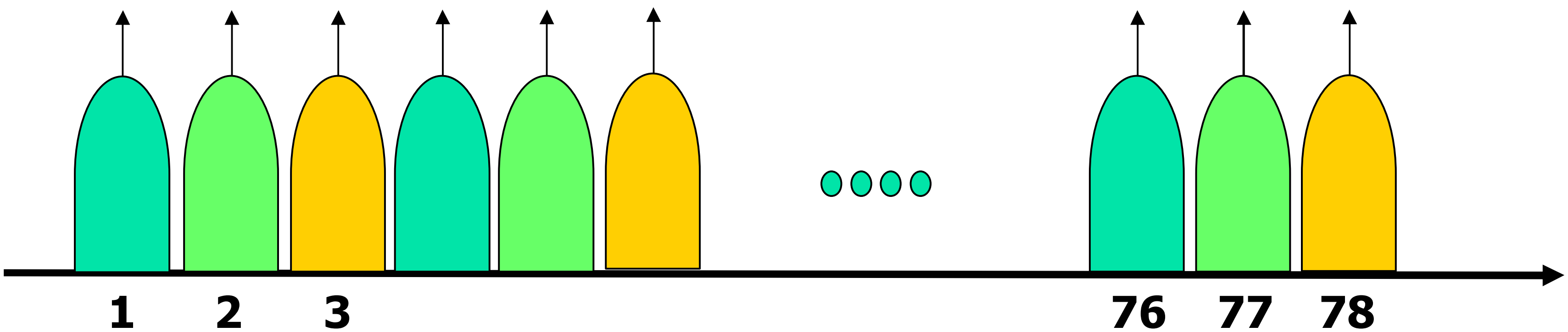
	802.11	802.11b (Wi-Fi)
Standard approval	July 1997	Sep. 1999
Bandwidth	83.5 MHz	83.5 MHz
Frequency of operation	2.4-2.4835 GHz	2.4-2.4835 GHz
Number of non-overlapping channels	3 Indoor/Outdoor	3 Indoor/Outdoor
Data rate per channel	1,2 Mbps	1,2,5.5,11 Mbps
Physical layer	FHSS, DSSS	DSSS

802.11 - FHSS

- 1 or 2 Mbit/s only @ 2.4 GHz
- GFSK modulation: base waveforms are gaussian shaped, bits are encoded shifting frequency, but the technique is such that it can also be interpreted as
  - BPSK (2GFSK → 1Mbit/s)
  - QPSK (4GFSK → 2Mbit/s)
- Slow Frequency Hopping SS
  - 20 to 400 ms dwell time ⇒ max 50 hop/s, min 2.5 hop/s

802.11 - FHSS

- 1 channel is used as guard
- 78 channels are divided into 3 orthogonal channels of 26 subchannels each



- Hopping is a PN sequence over the 26 channels
  - Tx and Rx must agree on the hopping sequence

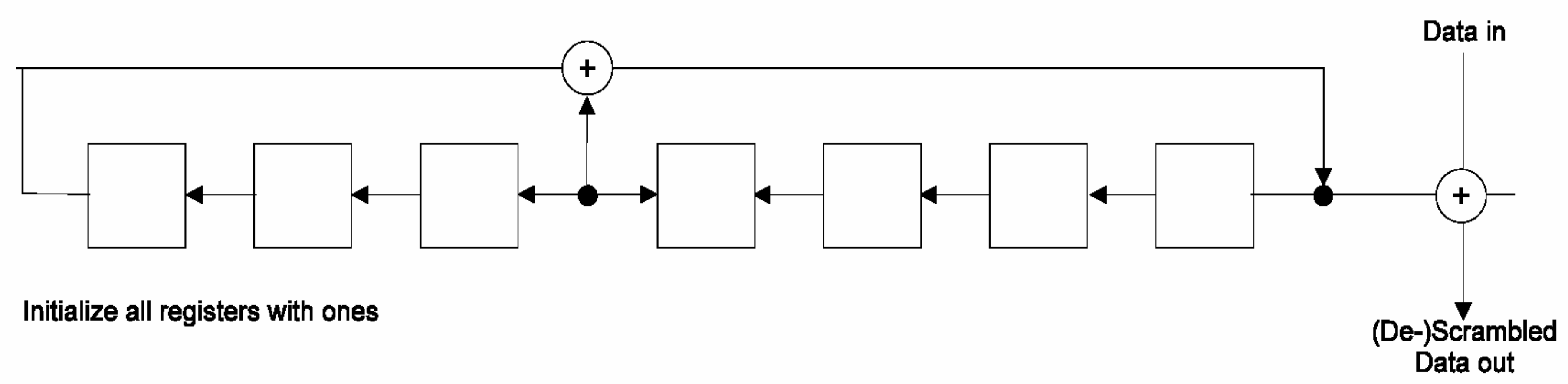
FH PLCP frame

SYNC	SFD	PLW	PSF	HEC	PSDU

- Always transmitted at 1 Mbits/s
- SYNC: 80 bits alternating 01010101 . . .
- SFD: 16 bits (0000 1100 1011 1101)
- PLW: number of octets transmitted in the PSDU: 12-bit integer
- PSF: 4 bits, indicates the rate used in the PSDU
- CRC: header protection – 16 bits
  - Generating Polinomial $G(x) = x^{16}+x^{12}+x^{5}+1$
- PSDU: actual data coming from the MAC layer; Max 4095 octets, Min 0
  - Scrambled to “whiten” it

Data scrambling (whitening)

- It is a simple feedback shift register generating a 127 bit long sequence XORed with data
  - $S(x) = x^7+x^4+1$

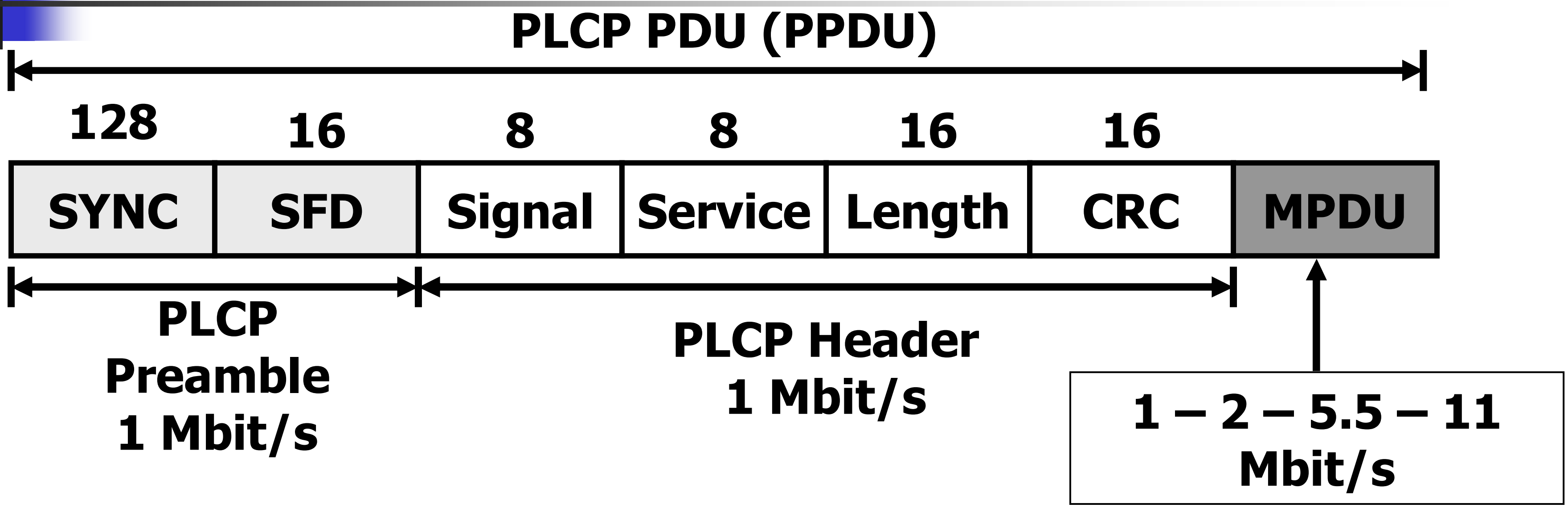


- Every 32 bits a 33-rd is inserted to suppress eventual biases

DSSS PHY

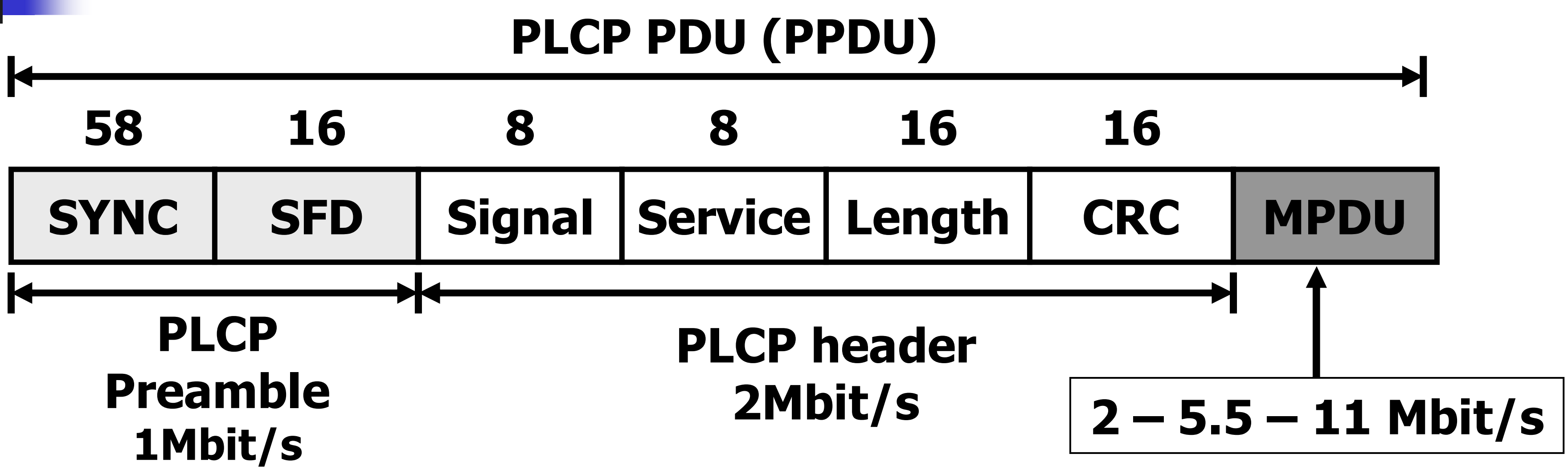
- Direct Spreading through digital multiplication with a chip sequence
- The scope is fading protection and not CDMA
- Max 3 FDM orthogonal channels
- Different specifications for the 1-2 and 5.5-11 PHY speeds
- Different headers
  - **Long** for 802.11 and 802.11b in compatibility mode
  - **Short** for 802.11b High Rates only (5.5-11)

802.11b Long Preamble PLCP PDU



- Compatible with legacy IEEE 802.11 systems
- Preamble (SYNC + Start of Frame Delimiter) allows receiver to acquire the signal and synchronize itself with the transmitter
- Signal identifies the modulation scheme, transmission rate
- Length specifies the length of the MPDU (expressed in time to transmit it)
- CRC same as HEC of FHSS

802.11b Short Preamble PLCP PDU



- Not compatible with legacy IEEE 802.11 systems
- Fields meaning is the same

Tx for 1-2 Mbit/s

- Spreading is obtained with an 11 bits Barker code
  - +1, –1, +1, +1, –1, +1, +1, +1, –1, –1, –1
- 1Mbit /s uses a binary differential PSK (DBPSK)
  - 0 → $j\omega = 0$; 1 → $j\omega = \pi$
- 2Mbit /s uses a quadrature differential PSK (DQPSK)
  - 00 → $j\omega = 0$; 01 → $j\omega = \pi/2$
  - 10 → $j\omega = \pi$; 11 → $j\omega = 3\pi/2$

Barker codes

- A sequence of +1 / -1 of length N such that

$$\left|\sum_{j=1}^{N-v} a_j a_{j+v}\right| \le 1 \qquad \text{for all } 1<v<N$$

- Has very good autocorrelation function (i.e. 11 for t=0, <1 for 1<t<11
- Improves spectrum uniformity
- Increases reflection rejection (robustness to fading) because of the autocorrelation (up to 11 bit times delays!!)

Tx for 5.5 and 11 Mbit/s

- Uses a complex modulation technique based on Hadamard Transforms and known as Complementary Code Keying CCK
- It is a sequence of 8 PSK symbols with the following formula

$$c = \{e^{j(\varphi 1 + \varphi 2 + \varphi 3 + \varphi 4)}; e^{j(\varphi 1 + \varphi 3 + \varphi 4)}; e^{j(\varphi 1 + \varphi 2 + \varphi 4)}; -e^{j(\varphi 1 + \varphi 4)}; e^{j(\varphi 1 + \varphi 2 + \varphi 3)}; e^{j(\varphi 1 + \varphi 3)}; -e^{j(\varphi 1 + \varphi 2)}; j^{\varphi 1}\}$$

φi are defined differently for 5.5 and 11 Mbit/s

- The formula defines 8 different complex symbols at 11 Mchip/s
- At 11 Mbit/s 1 bit is mapped on 1 chip,
  at 5.5 the mapping is 1→2

Tx for 5.5 and 11 Mbit/s

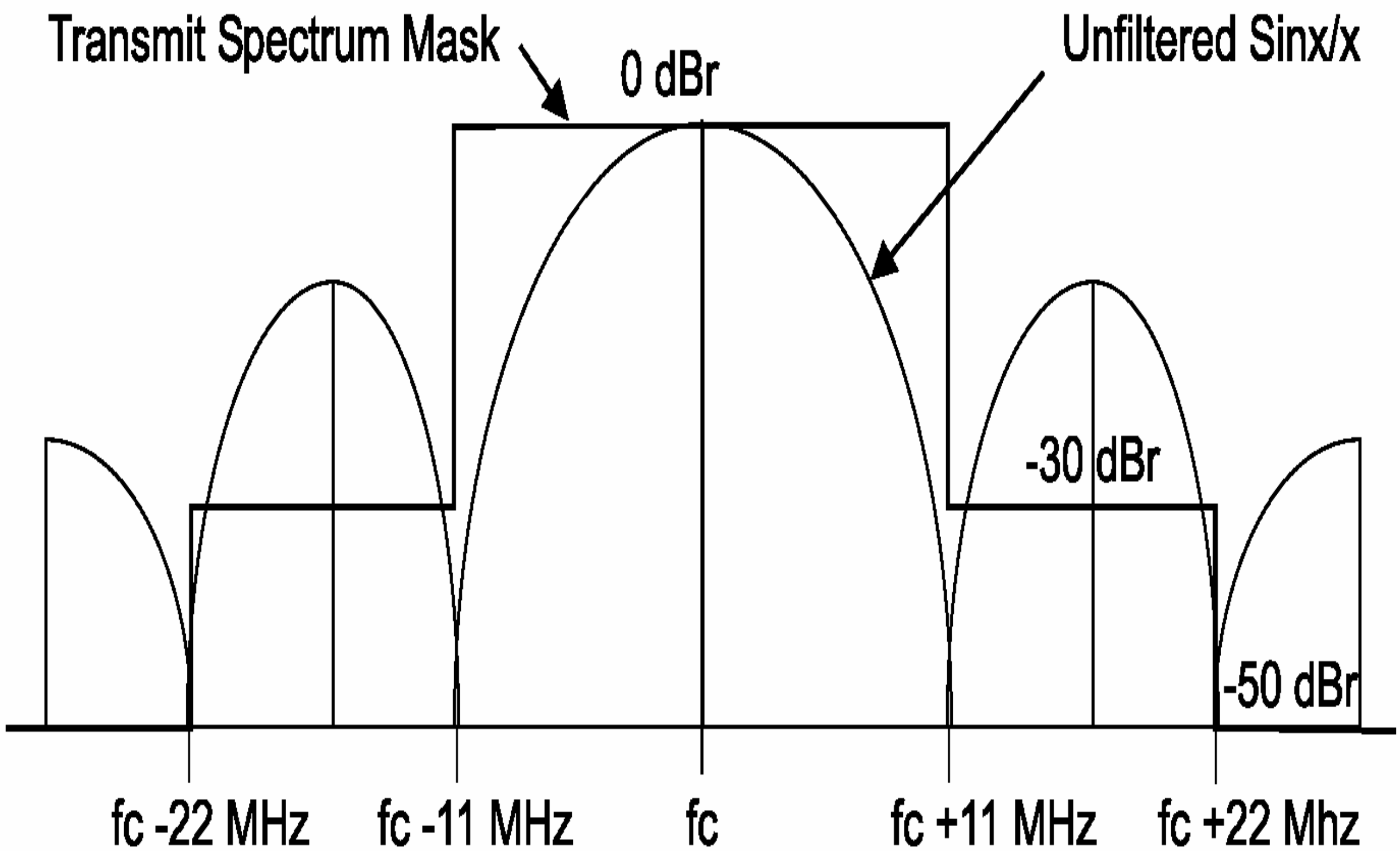
- In 5.5
  - φ1 and φ3 do not carry information
  - 4 bits are pairwise DQPSK encoded on φ2 and φ4
- In 11
  - 8 bits are pairwise DQPSK encoded on φ1, φ2, φ3 and φ4

- The resulting signal is a complex PSK modulation over single chips with correlated evolution over the CCK codes
- In practice there are 256 (2^8) possible codewords but only 32 (5.5 Mbit/s) or 64 (11 Mbit/s) are used
  - robustness to fading

Hadamard Encoding

- We can view them as extension to multiple dimensions of Barker codes
- A broad set of transformation techniques used in many fields
  - The base for the MPEG video encoding
  - Generalization of Fourier transforms
  - Quantum Computing
  - …

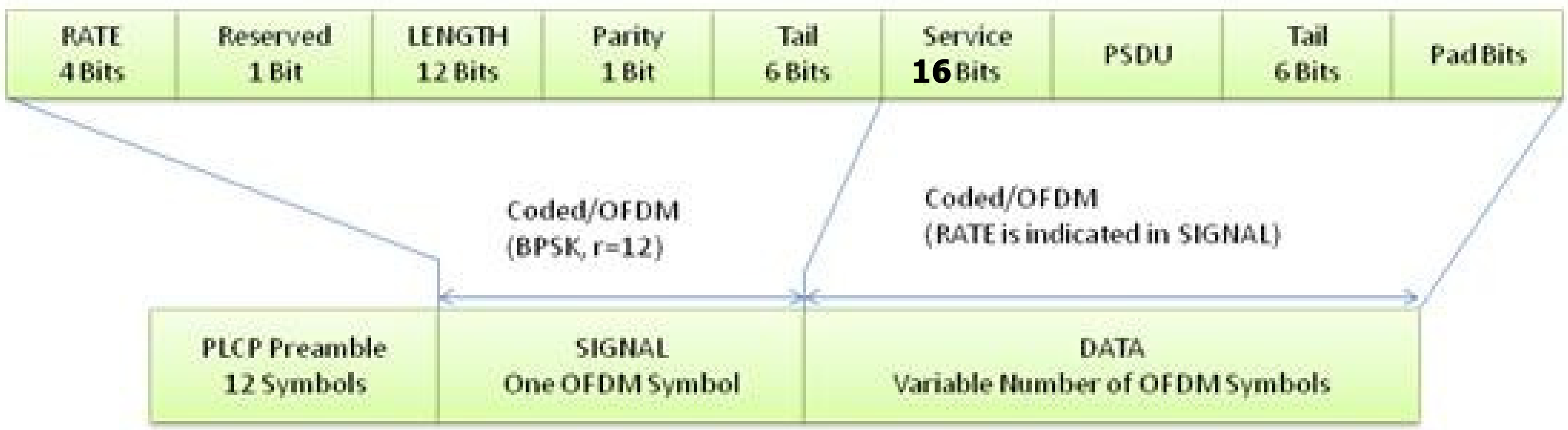
Transmission Power Mask



802.11a OFDM PHY

- 6, 9, 12, 18, 24, 36, 48, and 54 Mb/s
- 6, 12, 24 mandatory
- 52 subcarriers over 20 MHz, 312.5 kHz apart
- Adaptive BPSK, QPSK, 16-QAM, 64-QAM
- OFDM symbol duration 4 μs
- Provides also “halfed” and “quarter” over 10 and 5 MHz by doubling (X 4) the OFDM symbol time
- Convolutional encoding with different rates for error protection
  - Encoding is embedded within the OFDM MoDem

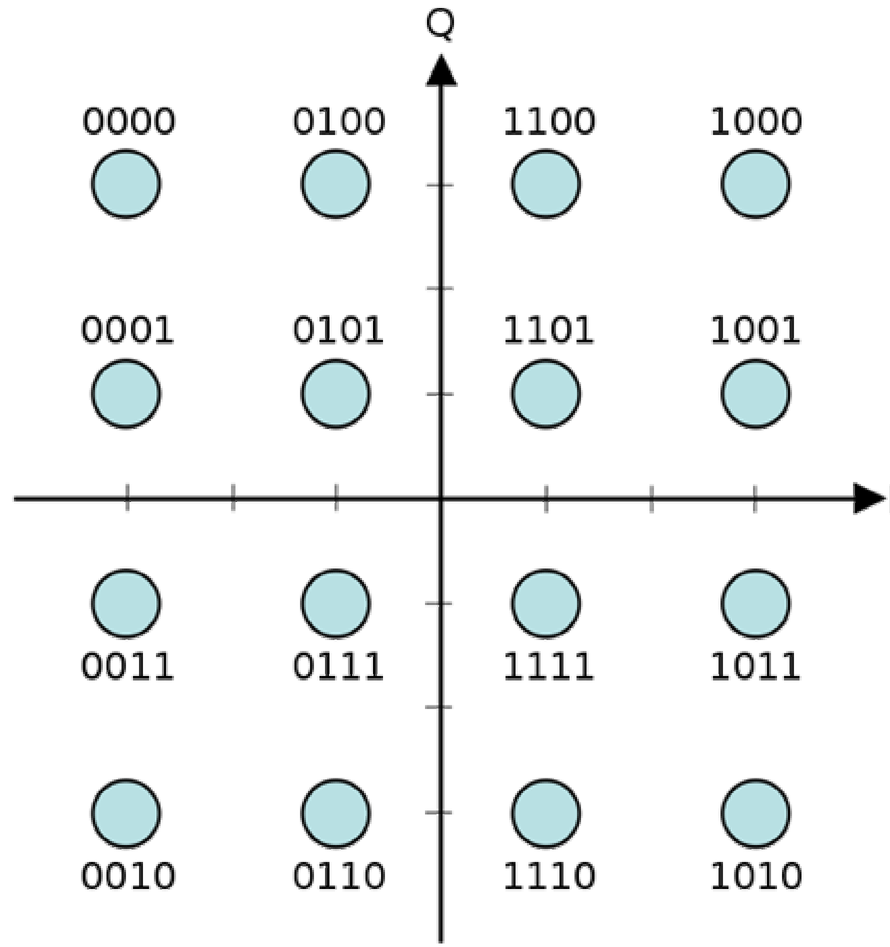
OFDM PPDU



- PLPC is 12 OFDM symbols corresponding to
- Rate defines the DATA rate
- Service is always 0 and enables scrambling synchronization
- SIGNAL is protected with a r=1/2 convolutional code

Sample 16-QAM with gray bit encoding

- Adjacent symbols differs by one bit only
- Makes multi-bit errors less probable
- Associated with interleaving and convolutional encoding greatly reduces BER and hence FER



Data rates, Slot time and BW

• 802.11a achieves data rates 6,9,12,18,24,36,48, and 54 MB/s.
• One OFDM symbol is sent every 4us, of which 0.8μs is the cyclic prefix (guard time)

BPSK example:
• 250k symbols sent every second.
• One symbol uses 48 data carriers.
• BPSK modulation with a convolutional code of rate 1/2
48 * 0.5 * 250k = 6 Mb/s

SLOT TIME
• Slot time = RX-to-TX turnaround time + MAC processing delay + CCA < 9μs where CCA = clear channel assessment

Typical times:
• RX-to-TX turnaround time < 2μs
• MAC processing delay < 2μs
• CCA < 4μs

64-QAM example:
• 250ksymbols/s, 48 data carriers.
• 64-QAM modulation = 64 = 2^6
• a convolutional code of rate 3/4
48 * 0.75 * 250k *6 = 54 Mbit/s

802.11a/g modulations

Mod.	Net (Mbit/s)	Gross (Mbit/s)	FEC rate	Efficiency (bit/sym.)	$T_{1472\ B}$ (μs)
BPSK	6	12	1/2	24	2012
BPSK	9	12	3/4	36	1344
QPSK	12	24	1/2	48	1008
QPSK	18	24	3/4	72	672
16-QAM	24	48	1/2	96	504
16-QAM	36	48	3/4	144	336
64-QAM	48	72	2/3	192	252
64-QAM	54	72	3/4	216	224

Data rates, Slot time and BW

• 802.11a achieves data rates 6,9,12,18,24,36,48, and 54 MB/s.
• One OFDM symbol is sent every 4us, of which 0.8μs is the cyclic prefix.

BPSK example:
• 250k symbols sent every second.
• One symbol uses 48 data carriers.
• BPSK modulation with a convolutional code of rate one-half.
=> 48 * 0.5 * 250k = 6 Mb/s.

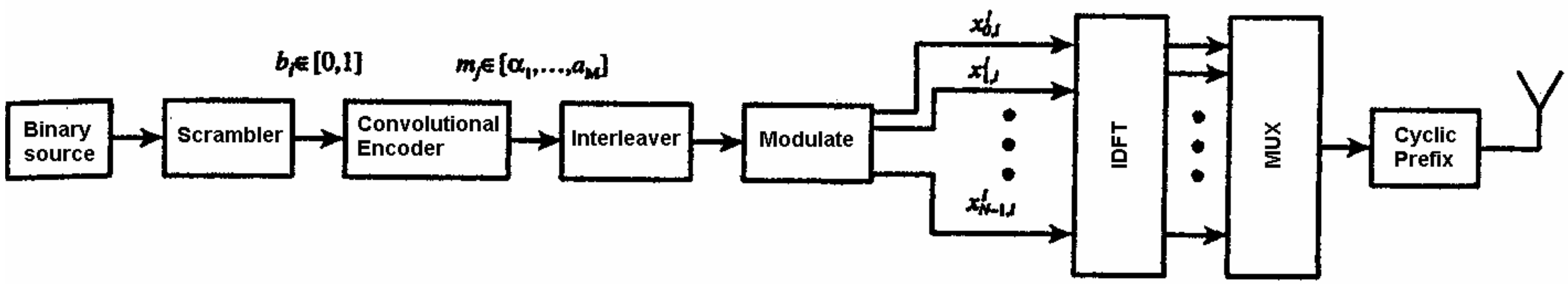
SLOT TIME
• Slot time = RX-to-TX turnaround time + MAC processing delay + CCA < 9μs.
where CCA = clear channel assessment.

Typical times:
• RX-to-TX turnaround time < 2μs
• MAC processing delay < 2μs
• CCA < 4μs.

64-QAM example:
• 250ksymbols/s, 48 data carriers.
• 64-QAM modulation = 64 = 2^6 .
• a convolutional code of rate 3/4.
=> 48 * 0.75 * 250k *6 = 54 Mb/s.

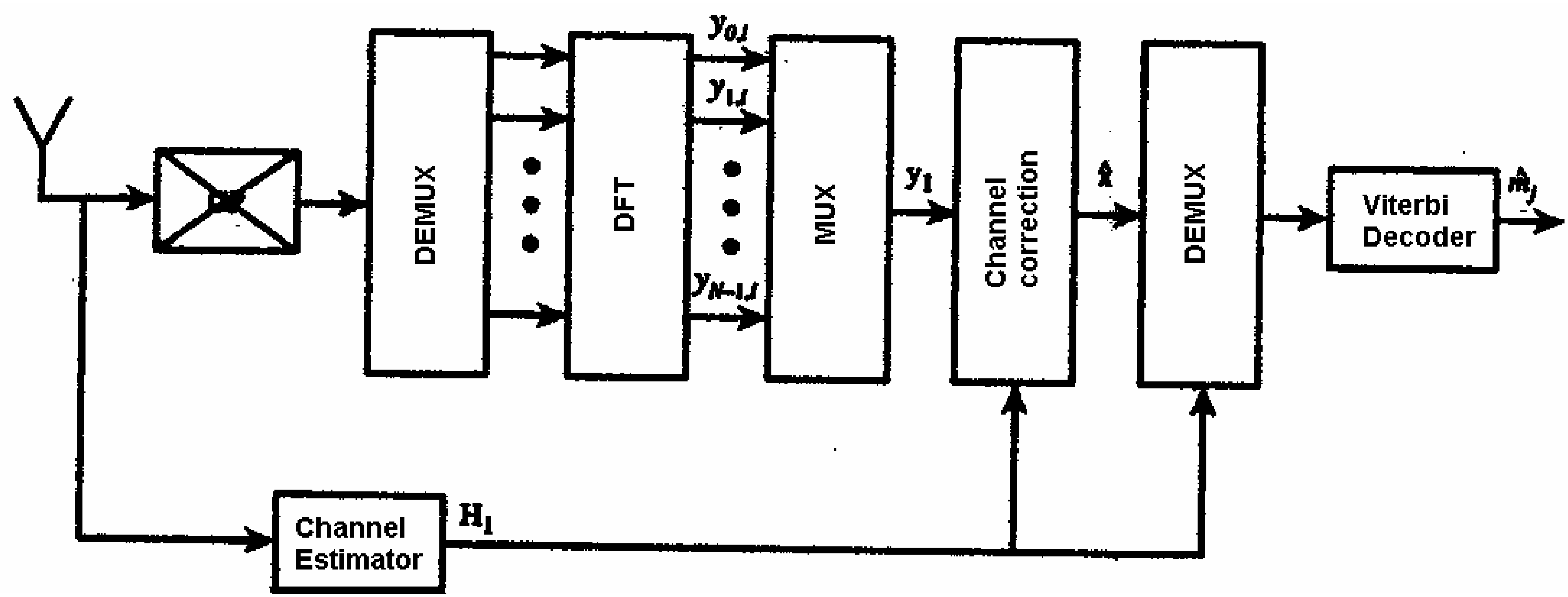
Bandwidth
• One OFDM is 20 MHz and inludes 64 carriers:
=> One carrier = 20MHz/64 = 312 kHz.

Transmission block scheme



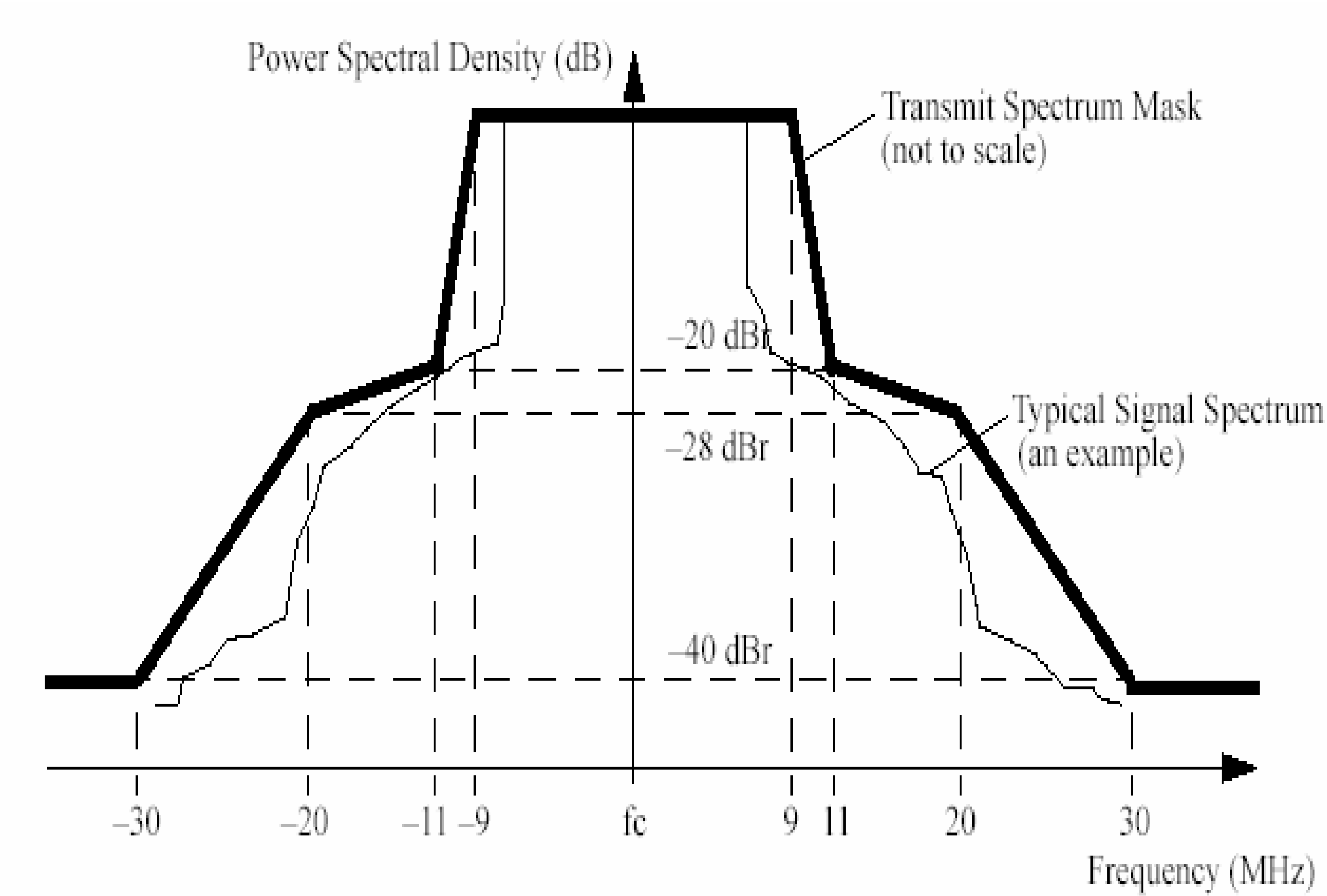
- The modulation is done in the digital domain with an IFFT
- Interleaving distributes (at the receiver) evenly errors avoiding bursts
- Convolutional coding corrects most of the “noise” errors
  - This justifies the “observation” that modern 802.11 tends to have an on-off behavior

Receiver block scheme



- Channel estimation enables distortion correction
- Viterbi decoding is an ML decoder for convolutional codes

OFDM transmission power mask



802.11g – ERP

- Extended Rate PHY (as per clause 19 of the standard!!)
- Defines the use of 802.11a OFDM techniques in the 2.4 GHz band
- Mandates backward compatibility with 802.11b
- Introduces some inefficiency for backward compatibility
- Many PPDU formats
  - Long/sort preambles
  - All OFDM (pure g) or CCK/DSSS Headers with OFDM PSDU (compatibility mode or b/g)