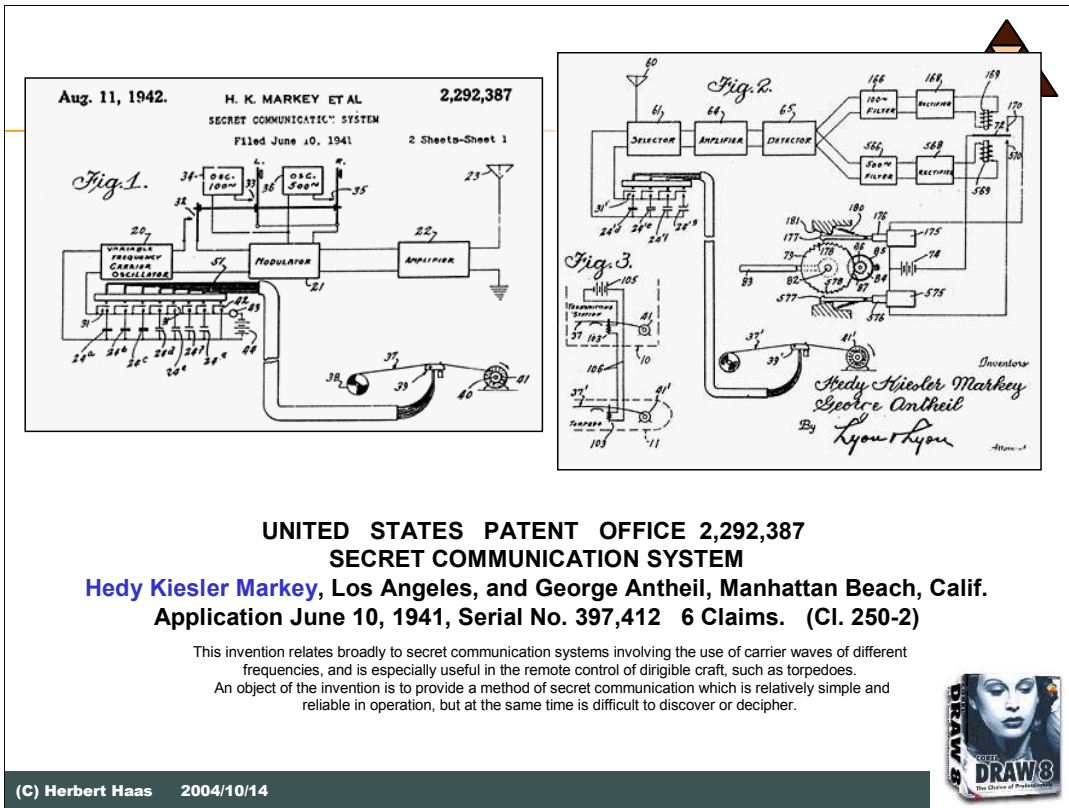




# **Modulation Techniques**

**Spread Spectrum Basics  
FHSS vs. DSSS  
QAM Variants and CCK  
OFDM**



Hedy Lamarr was honored with the Viktor Kaplan Medal of the Austrian Association of Patent Holders and Inventors on October 16, 1998. The medal, considered the highest award which can be bestowed upon inventors in Austria, was presented to Miss Lamarr for her pioneering contribution to enabling radio communications to be made secure from interference and eavesdropping. Miss Lamarr was proposed for the medal by Dr. Peter Paul Sint of the Austrian Academy of Sciences. In support of the nomination, Dr. Sint stated that her invention was decades ahead of its time and anticipated "essential elements of digital logic." Hedy Lamarr was the recipient of a number of technology prizes in the US during 1997. The presentation of the Viktor Kaplan Medal is the first such recognition of her achievement in her homeland Austria. As with prior awards, Miss Lamarr did not personally attend the Kaplan Medal presentation ceremony in Esterhazy Palace in Eisenstadt, Austria. She was represented by her son, Anthony Loder.

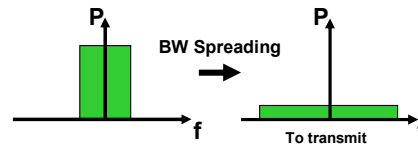
BTW: The tremendous fame of the movie "Ecstasy" is due above all to a single scene in which the audience sees Hedy Lamarr swimming nude in a lake and then running through a nearby forest. This sequence - lasting several minutes - is considered the first nude scene in cinematic history and caused a worldwide scandal in the 1930s. "Ecstasy" was then banned in many countries of the world - most notably in the US - or only a radically expurgated version of it was permitted to be shown.

# Why Bandwidth Spreading?

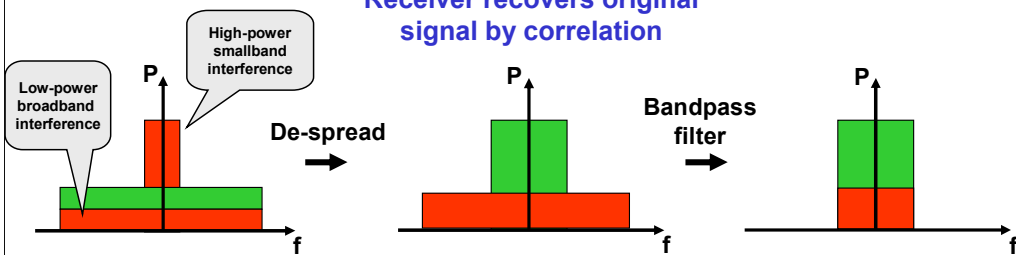


- If input power is spread over a large band: hard to intercept
- The noise is reduced (compared to the noise in the total bandwidth used) by the spreading gain  $\gamma_c = \frac{T}{T_c}$
- To synchronize, we multiply with all possible shifted versions of the PN sequence
- Fast auto-correlation needed

Sender reduces spectral power density but conserves total energy:



Receiver recovers original signal by correlation



(C) Herbert Haas 2004/10/14

3

While transmission small- and broadband interferences add to the user signal. Power density could be smaller than in the smallband signal. It is also possible that the power density is smaller than the ambient noise.

# Bandwidth Spreading Methods



- **Direct Sequence Spread Spectrum (DSSS)**
  - ♦ 802.11b/g: 14 possible channels – 3 channels can be used simultaneously
  - ♦ Can operate with SNR of 12dB
  - ♦ Throughput up to 11 Mbit/s (and more)
  - ♦ Range up to 40 km (and more)
- **Frequency Hopping Spread Spectrum (FHSS)**
  - ♦ 802.11: 79 possible channels – 15 channels can be used simultaneously
  - ♦ Can operate with SNR of 18dB
  - ♦ Interference tolerant
  - ♦ Less multipath problems
  - ♦ Technically limited up to 2 Mbit/s
- **OFDM (Multicarrier Modulation)**
  - ♦ Actually used to minimize the required bandwidth but often referred as spreading technique in the WLAN context

DSSS defines a set of channels spaced across the whole radio bandwidth. There are 14 of these channels, but channel 14 is reserved for Japan. DSSS modulates the data with a spreading code (chipping) and transmits the result on only one of these channels. There has to be 30MHz between the carrier frequencies for multiple access points to operate within the same area without interference. Since the entire bandwidth is 83.5MHz, only a maximum of 3 DSSS access points can operate within the same area. The limited available total bandwidth is also the methods vulnerability. If narrow band interference occurs in the used channel, one can only wait until it disappears before communications can be resumed. In return DSSS gives a longer range. The modulation technique can operate with a signal to noise ratio (SNR) of 12dB where FHSS operates with SNR of 18dB.

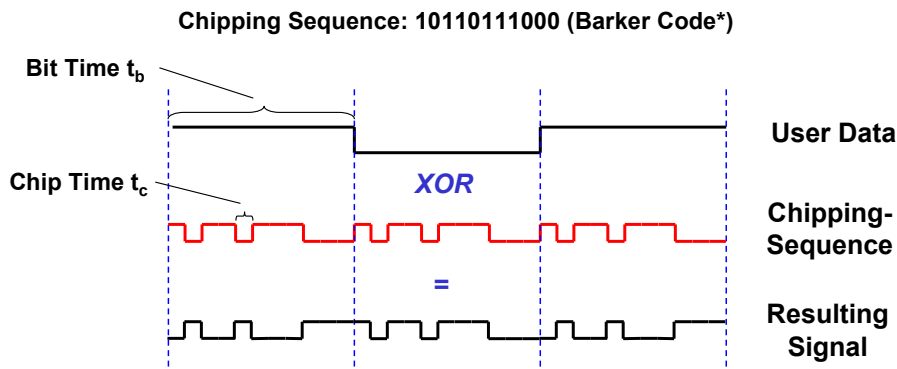
FHSS defines a set of channels spaced across the whole radio bandwidth. Here in Norway, there are 79 such channels. When transmitting, FHSS uses only one channel at a time in a predetermined sequence and dwell time between hops. There are 78 such sequences and they are orthogonal so that they do not interfere with each other. This enables as many as approx. 15 access points belonging to different systems, to coexist. Because the whole bandwidth is available and the signal is sent/received on only a small part of it at a time, this is the method most tolerant to narrow band interference. This would not block the communication entirely but only when the hopping pattern happens to hit the interfering frequency and only for the duration of the dwell time, often set to 128ms. All band interference would of course stop FHSS also. FHSS also has lowest power consumption.

Orthogonal Frequency Division Multiplexing (OFDM) is a multicarrier transmission method and actually tries to reduce the required bandwidth. Using OFDM together with QAM (see later) very high data rates can be achieved, therefore a given bandwidth (20-22 MHz with WLANs) is optimally utilized.

# DSSS



- **User bit-pattern is modulated (substituted) with chipping-sequence (“Barker code“)**
  - ◆ Each bit of data is encoded by 11 bits of the chipping sequence
  - ◆ 802.11b: 22 MHz modulation bandwidth



(C) Herbert Haas 2004/10/14

5

In 802.11, the chipping sequence is known as the Barker code, which is an 11-bit sequence (10110111000) that has certain mathematical properties making it ideal for modulating radio waves. The basic data stream is XORed with the Barker code to generate a series of data objects called chips. Each bit is "encoded" by the 11 bit Barker code, and each group of 11 chips encodes one bit of data.

Direct Sequence Spread Spectrum (DSSS) uses a XOR – Chipping Sequence on the userdata to spread the signal (digital modulation). The spreaded signal is modulated to a carrier (analog modulation).

Userdata bit  $\rightarrow$  bit length of  $t_b$

Chipping Sequence  $\rightarrow$  smaller bit length of  $t_c$  (chips)

Spreading Factor:  $s = t_b/t_c$

Bandwidth of spreaded signal  $\rightarrow s*w$

Civil uses  $\rightarrow$  spread factor of 10-100 (Barker-Code has factor 11), Military  $\rightarrow$  spread factor up to 10000

## Codes Used



Data Rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11 (Barker)	DBPSK	1 MSps	1
2 Mbps	11 (Barker)	DQPSK	1 MSps	2
5.5 Mbps	8 (CCK)	DQPSK	1.375 MSps	4
11 Mbps	8 (CCK)	DQPSK	1.375 MSps	8

- **For 5.5 and 11 Mbps data rates, Barker sequences are not used**
- **Instead Complementary Code Keying (CCK) is used (64 8-bit code words)**

By regulations, a DSSS system in the ISM band must have a minimum of 10 dB processing gain

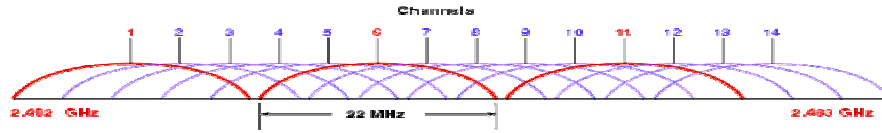
1 Mbps 11 bit Barker code processing gain = 10.4 dB

11 Mbps CCK processing gain = 11 dB

Any highrate modulation is more susceptible to jamming, multipath interference and filter distortion than lower rate modulation because of the higher required SNR ( $E_s/N_0$ )

Processing gain is the reason why DS is relatively jamming resistant provided that the WLAN hardware is designed well (which is often not the case with cheap hardware).

# 802.11b DSSS Channels



Channel	Frequency	Americas	EMEA	Israel	Japan
1	2412	X	X	-	X
2	2417	X	X	-	X
3	2422	X	X	X	X
4	2427	X	X	X	X
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	-	X
11	2462	X	X	-	X
12	2467	-	X	-	X
13	2472	-	X	-	X
14	2484	-	-	-	X

Fourteen channels are defined in the IEEE 802.11b Direct Sequence (DS) channel set. Each DS channel as transmitted is 22 MHz wide, however the channel center separation is only 5 MHz. This leads to channel overlap such that signals from neighboring channels can interfere with each other. In a 14-channel DS system (11 usable in the US), only three non-overlapping (and hence, non-interfering) channels, 25 MHz apart are possible (for example, Channels 1, 6, and 11).

This channel spacing governs the use and allocation of channels in a multi-access points environment such as an office or campus. Access points are usually deployed in "cellular" fashion within an enterprise where adjacent access points are allocated non-overlapping channels. Alternatively, access points can be collocated using Channels 1, 6, and 11 to deliver 33 Mbps bandwidth to a single area (but only 11 Mbps to a single client).

# FHSS



- Available bandwidth split into several smaller channels with smaller bandwidth
- Sender and receiver uses one of this smaller channels for a part of time, then jump to next one
  - ♦ Pseudo-random jump sequence
  - ♦ Avoids being stuck in a bad frequency band
  - ♦ Slow hopping: multiple bits before frequency hop
  - ♦ Fast hopping: multiple frequency hops per bit
- On multi-access media, collisions are only rare
- ISM bandwidth (2.4 GHz) = 83 MHz is divided into 1 MHz channels for FHSS
- FCC requires that any FHSS radio must visit at least 79 of the channels at least once in 30 seconds
  - ♦ Minimum hop rate: 2.5 hops/second

Note: The original 802.11 implementations only used FHSS, but it is **still used** in critical environments today (airports etc)



(C) Herbert Haas 2004/10/14

Frequency Hopping Spread Spectrum (FHSS) uses a radio that moves or hops from one frequency to another at predetermined times and channels. The hopping pattern is specified in the WLAN beacons.

The regulations require that the maximum time spent on any one channel is 400mS. For the 1- and 2-Mb FH systems, the hopping pattern must include 75 different channels, and must use every channel before reusing any one.

For the Wide Band Frequency Hopping (WBFH) systems, that permit up to 10-Mb data rates, the rules require use of at least 15 channels, and they cannot overlap. With only 83MHz of spectrum, it limits the systems to 15 channels, thereby causing scalability issues.

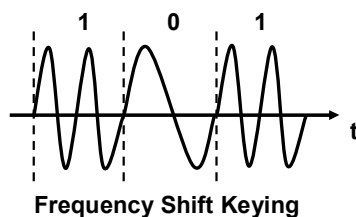
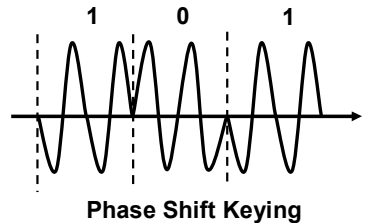
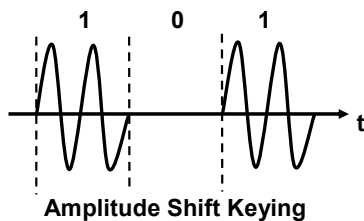
GFSK is used for the modulation process.

FHSS was used for the initial IEEE 802.11 standard, providing up to 2 Mbit/s but it is still available today, manufactured by certain vendors, to allow wireless data transmission in difficult environments such as airports etc.

# Modulation – Basics



$$g(t) = A_t * \cos(2\pi f_t t + \varphi_t)$$



The illustrated ASK method is simple OOK.  
FSK and PSK are angle-modulation methods.  
(nonlinear=>spectrum shape is changed)  
The BER of BPSK is 3 dB better than OOK.

(C) Herbert Haas 2004/10/14

9

The slide shows a general modulation equation. The 3 parameters of the equation describe the 3 basic modulation types. All 3 parameters, the amplitude  $A_t$ , the frequency  $f_t$  and the phase  $\varphi_t$  can be varied, even simultaneously. In nature, there is no real digital transmission; the binary data stream needs to be converted into an analog signal. As first step, the digital data will be “directly” transformed into a analog signal (0 or 1), which is called a baseband signal. In order to utilize transmission media such as free space (or cables and fibers) the base signal must be mixed with a carrier signal. This analog modulation shifts the center frequency of the baseband signal to the carrier frequency to optimize the transmission for a given attenuation/propagation characteristic.

## Amplitude Shift Keying

A binary 1 or 0 is represented through different amplitudes of a sinus oscillation. Amplitude Shift Keying (ASK) requires less bandwidth than FSK or PSK since *natura non facit saltus*. However ASK is interference prone. This modulation type also used with infrared-based WLAN.

## Frequency Shift Keying

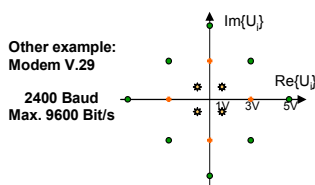
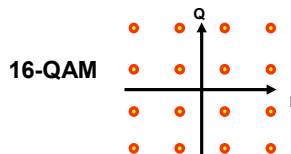
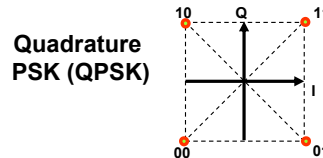
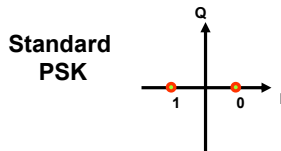
Frequency Shift Keying (FSK) is often used for wireless communication. Different logical signals are represented by different frequencies. This method needs more bandwidth but is more robust against interferences. To avoid phase jumps, FSK uses advanced frequency modulators (Continuous Phase Modulation, CPM).

## Phase Shift Keying

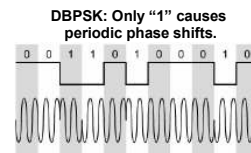
The 3rd basic modulation method is the Phase Shift Keying (PSK). The digital signal is coding through phase skipping. In the picture above you see the simplest variation of PSK, using phase jumps of 180°. In practice, to reduce BW, phase jumps must be minimized, and therefore PSK is implemented using advanced phase modulators (e. g. Gaussian Minimum Shift Keying, etc). The receiver must use same frequency and must be perfectly synchronized with the sender using a Phase Locked Loop (PLL) circuit. PSK is more robust as FSK against interferences, but needs complex devices.

After understanding these modulation methods QAM shall be introduced, which is the most important modulation scheme today – for both wired and wireless transmission lines.

# QAM



- **802.11a and Hiperlan**
  - Wireless Medium: OFDM
  - BPSK @ 6 and 9 Mbps
  - QPSK @ 12 and 18 Mbps
  - 16-QAM @ 24 and 36 Mbps
  - 64-QAM @ 48 and 54 Mbps
- **802.11b**
  - Wireless Medium: DSSS
  - DBPSK @ 1 Mbps
  - DQPSK @ 2 Mbps
  - 16 CCK @ 5.5 Mbps
  - 256 CCK @ 11 Mbps



It is important to understand that spread spectrum (or OFDM) techniques are always combined with a symbol modulation scheme. Quadrature Amplitude Modulation (QAM) is a general method where practical methods such as BPSK, QPSK, etc are derived from.

The main idea of QAM is to combine phase and amplitude shift keying. Since orthogonal functions (sine and cosine) are used as carriers, they can be modulated separately, combined into a single signal, and (due to the orthogonality property) de-combined by the receiver.

And since  $A \cdot \cos(\omega t + \phi) = A/2 \{ \cos(\omega t) \cos(\phi) - \sin(\omega t) \sin(\phi) \}$  QAM can be easily represented in the complex domain as  $\text{Real} \{ A \cdot \exp(i \cdot \phi) \cdot \exp(i \cdot \omega t) \}$ .

The standard PSK method only use phase jumps of  $0^\circ$  or  $180^\circ$  to describe a binary 0 or 1. In the right picture above you see an enhanced PSK method, the Quadrature PSK (QPSK) method. While using Quadrature PSK each condition (phase shift) represent 2 bits instead of 1. Now it is possible to transfer the same data rate by halved bandwidth.

The QSK signal uses (relative to reference signal)

- $45^\circ$  for a data value of 11
- $135^\circ$  for a data value of 10
- $225^\circ$  for a data value of 00
- $315^\circ$  for a data value of 01

To reconstruct the original data stream the receiver need to compare the incoming signal with the reference signal. The synchronization is very important.

### Why not coding more bits per phase jump ?

Especially in the mobile communication there are too many interferences and noise to encode right. As more bits you use per phase jump, the signal gets more "closer". It is getting impossible to reconstruct the original data stream. In the wireless communication the QPSK method has proven as a robust and efficient technique.

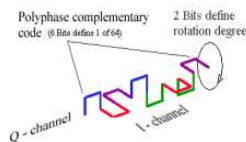
# CCK



- **Based on Marcel J. E. Golay (1951) polyphase complementary codes**
  - ♦ Has ideal AKF properties
- **Complex codes**
  - ♦ 6 bits of each byte select one of 64 unique orthogonal eight chips long polyphase complementary codes
  - ♦ The other two bits rotate the whole code word (0, 90, 180 or 270 degrees)
- **8 chips => 1 symbol hence 1,375 Mbaud => 11 Mchips/s**
- **Symbol is a 8-dimensional vector with complex components:**



- ♦ Data bits encode component phases using DQPSK
  - ♦  $\Phi_1$  is contained in all 8 chips => rotates the vector
- **Same spectrum shape as with Barker code words**



## Example:

Assuming that the bits of a 8-bit word control the phase components according

d1	d0	→	$\phi_1$
d3	d2	→	$\phi_2$
d5	d4	→	$\phi_3$
d7	d6	→	$\phi_4$

and the following QPSK specification is true

0	0	→	0
0	1	→	$\pi$
1	0	→	$\pi/2$
1	1	→	$-\pi/2$

then the codeword

**10110101**

transforms into

**{1, -1, j, j, -j, j, -1, -1}**

Based on Marcel J. E. Golay, 1951, spectrometer application. The Walsh transform is a special case of the Fourier transform and used for the correlation. The eight components of the 8-dimensional vector are complex chips, as shown in the example on the right (1, -1, j, j, -j, j, -1, -1).

CCK is a variation on M-ary Orthogonal Keying modulation, which uses I/Q modulation architecture with complex symbol structures. CCK allows the 802.11b for multi-channel operation in the 2.4 GHz band using the existing 802.11 DSSS channel structure scheme. The spreading employs the same chipping rate and spectrum shape as the 802.11 Barker's code word. The spread function for CCK in 802.11b is chosen from a set of M nearly orthogonal vectors by the data word. CCK uses one vector from a set of 64 complex (QPSK) vectors for the symbol and thereby modulates 6 bits (one of 64) on each 8 chips spreading code symbol. In the 802.11b, the formula that defines the CCK codewords has 4 phase terms. The first of them modulates all of the chips and this is used for the QPSK rotation of the whole code vector. The second modulates every odd chip, the third modulates every odd pair of chips and the fourth modulates every odd quad of chips.

# OFDM



- **Orthogonal Frequency Division Multiplexing (OFDM)**
  - ♦ Avoids multipath-induced interferences that always occur at higher symbol rates
  - ♦ 1966: Chang (Bell Labs) issued OFDM paper and patent
  - ♦ 1993: Morris implemented first experimental OFDM WLAN at 150 Mbit/s
- **Basic idea:**
  - ♦ 1) Split data stream in multiple lower-rate streams
  - ♦ 2) Convert  $n$  bits into  $m$  QAM symbols
  - ♦ 3) Regard the  $m$  QAM symbols as discrete complex spectrum and convert it into the time domain via FFT<sup>-1</sup>
    - The  $m$  complex QAM symbols must be "mirrored" appropriately in order to get real-valued time-domain values (hint: amplitudes even, phase odd)
  - ♦ Each element of the "QAM-vector" can be interpreted as a subchannel
- **Subchannels overlap!**
  - ♦ Approx. 50% less total bandwidth necessary than FDM
  - ♦ ISI is minimized because of orthogonal sub-bands
  - ♦ Equivalent to Nyquist-pulses in time domain

In Europe a special modulation type for digital radio, called Digital Audio Broadcast (DAB) is used. This modulation method uses many frequencies at the same time (Multicarrier Modulation (MCM)). The big advantage is the robustness against ISI. As higher the symbol rate as higher the ISI effect. Because of this reason MCM splits the symbol rate into more stream with lower rate on a own carrier.

For example:

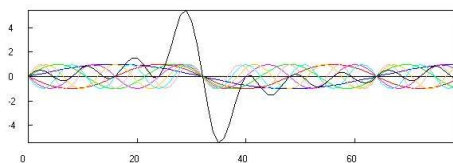
$n$  Symbols per second uses  $c$  new carrier. Then only  $n/c$  symbols per second need to be transferred, and each symbol represent 2 bits (like QPSK). Only small parts of the signal will be destroyed while strong interferences.

The DAB standard can use 192-1536 carrier at the same time.

# OFDM – 802.11a Details (1)



- **Channel BW is 20 MHz (occupied BW is 16.6 MHz)**
  - ♦ 52 subcarriers are used per channel
  - ♦ 48 subcarriers carry the data
  - ♦ 4 subcarriers are pilots which facilitate phase tracking for coherent demodulation
  - ♦ Subcarrier separation: 312,5 kHz (20 MHz/64)
- **Each of these subcarriers can be a BPSK, QPSK, 16-QAM or 64-QAM coded signal**



TIME DOMAIN construction of an OFDM signal from its constituent carriers

(C) Herbert Haas 2004/10/14

13

OFDM is efficiently realized by the use of effective signal processing, fast-fourier transform, in the transmitter and receiver. This significantly reduces the amount of required hardware compared to earlier FDM-systems. One of the benefits of OFDM is the robustness against the adverse effects of multipath propagation with respect to intersymbol interference. It is also spectrally efficient because the subcarriers are packed maximally close together. OFDM also admits great flexibility considering the choice of and realization of different modulation alternatives.

OFDM, Orthogonal Frequency Division Multiplex, is a special form of multicarrier modulation. The basic idea is to transmit broadband, high data rate information by dividing the data into several interleaved, parallel bit streams, and let each one of these bit streams modulate a separate subcarrier. In this way the channel spectrum is passed into a number of independent non-selective frequency subchannels. These sub channels are used for one transmission link between the AP and the MNs.

The time domain construction of an OFDM signal from its constituent carriers is shown above. The data values can be adjusted. For some data combinations the peak power is much higher than for others and this can complicate analog amplifier design in OFDM systems. In multipath channels, the delays can cause symbol overlap, destroying the perfect sum of sinusoids. This is easily fixed by cyclicly extending the signal by a length longer than the channel delay.

## OFDM – 802.11a Details (2)



- **Symbol duration is 4 microseconds (250 symbols/sec)**
  - ♦ With a guard interval of 800 ns
  - ♦ Optional shorter guard interval of 400 ns may be used in small indoor environments
- **Generation of orthogonal components is done in baseband (via DSPs) which is then upconverted to 5 GHz at the transmitter**
  - ♦ Each subcarrier can be represented as complex number
  - ♦ The time domain signal is generated by IFFT
- **The receiver downconverts, samples at 20 MHz and does an FFT to retrieve the original complex coefficients**

The guard interval is needed to achieve the desired spectral shape.

# OFDM – Pros and Cons



- **Advantages**
  - ♦ High spectrum efficiency
  - ♦ High multipath resistance
  - ♦ General better interference resistance
  - ♦ All this results in longer distances
- **Drawbacks**
  - ♦ More expensive circuits
  - ♦ Higher power consumption (compared to 802.11b)
  - ♦ Envelope of Multi-carrier modulation results in high Crest factors (peak to average power)
    - Nonlinear effects in analog devices and ADCs
    - Results in BW spreading (higher order signals)
    - Four-Wave Mixing
    - Neighbor channel interference degrades receiver sensitivity
  - ♦ **Therefore 30 mW EIRP limitation**

Note: OFDM was originally only planned for 802.11a in the "clean" 5 GHz band since the QAM used here is relatively noise-sensitive, much more compared to DSSS. Considering this, how will 802.11g really perform in noisy 2,4 GHz environments?

**Appendix**

**Code Division Multiple Access**

# CDMA (1) – Basic Concept

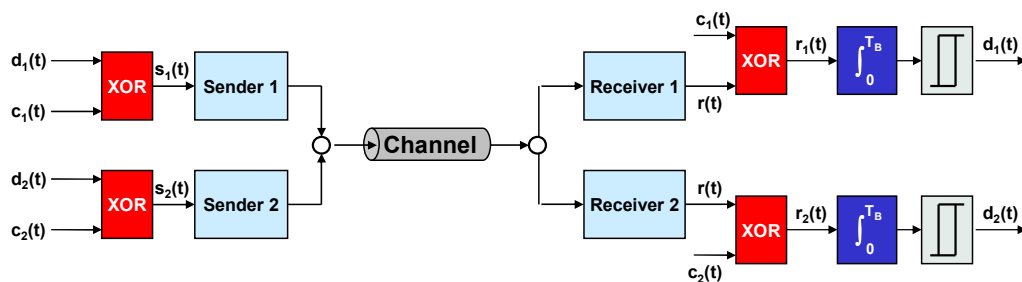


- Code multiplex allows multiple utilization of same frequency channel (without TDM)
- Multiple senders may transmit simultaneously using a different set of **orthogonal code words**
  - ♦ Aka Direct Sequence CDMA (DS-CDMA)
- Each receiver sees the sum of all signals but can extract any particular signal using the sender's code word set
- Number of connections per channel = number of available (orthogonal) codes
  - ♦ Much higher capacities possible compared to time slot techniques (TDMA)
- Alternative method: Frequency Hopping
  - ♦ Requires different ("orthogonal") hopping pattern
  - ♦ Very robust but does not scale to high data rates (< 1-2 Mbit/s with much efforts)

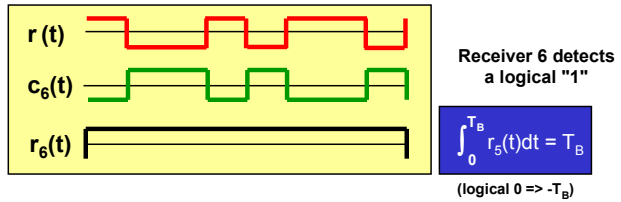
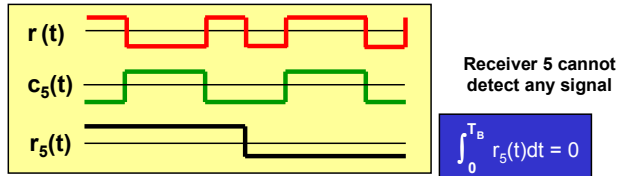
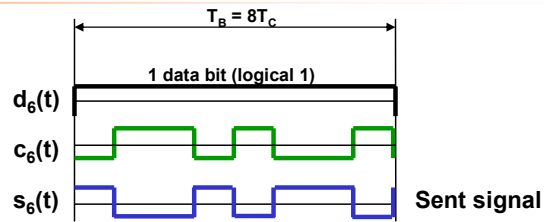
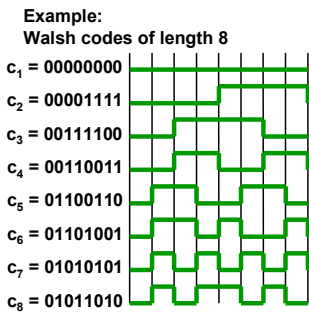
# CDMA (2) – Technical Realization



- Transmitter XORs each data bit with a binary code word (CW)
  - Using orthogonal codes, e. g. Walsh codes ("chipping sequence")
  - Results in a BW spreading with a spreading factor  $SF=length(CW)$
- Receiver performs "despreading"
  - 1) XORs received signal with this CW
  - 2) and integrates the result over one bit duration  $T_B$
- For each  $T_B$  the orthogonality relation results to
  - Zero if sender and receiver used different CWs
  - One if sender and receiver used same CWs
- Extraction of particular signals works because
  - Spreading, summation of signals, and despreading are *linear* operations



# CDMA (3) – Code Example



## CDMA (4) – Note



- Walsh codes only work if sent **phase synchronized**
  - ♦ Only works downstream
- **Upstream** CDMA communication would require better codes
  - ♦ Whose cross-correlation function is nearly zero for all possible time (=phase) shifts
- A **separate code** set could be used for spreading and channel separation in order to gain an optimal spectral power distribution
- Practical CWs are not 100% orthogonal and cause **additional noise** (reduced SNR at receiver)
  - ♦ SNR does NOT depend on number of CWs!
  - ♦ Only the power levels of other senders are critical
- Therefore each sender should **control its TX power**:
  - ♦ All uplink channels should have same level at base station then the SNR is equal in all channels
  - ♦ The power levels of any downlink channel should be reduced to a minimum (just about receivable) to optimize the SNR in each mobile station