Wireless Networking and Mobile Computing

8. Cellular Networking Basics (LTE, 5G, Internet-of-Things)

Stefan Mangold

Course Outline

1. Introduction
2. Wireless Communication Basics
3. IEEE 802.11 Wireless LAN (Wi-Fi)
4. IEEE 802.15 Wireless PAN (ZigBee & Bluetooth)
5. Mobile Computing Algorithm Basics: Control and Game Theory
6. Visible Light Communication
7. Audio Communication
8. Cellular Networking Basics (LTE, 5G, Internet-of-Things)
9. Mobile Computing for Automated Medicine Delivery
10. Cognitive Radio, Delay Tolerant Networking, Radio Spectrum Sharing

Literature

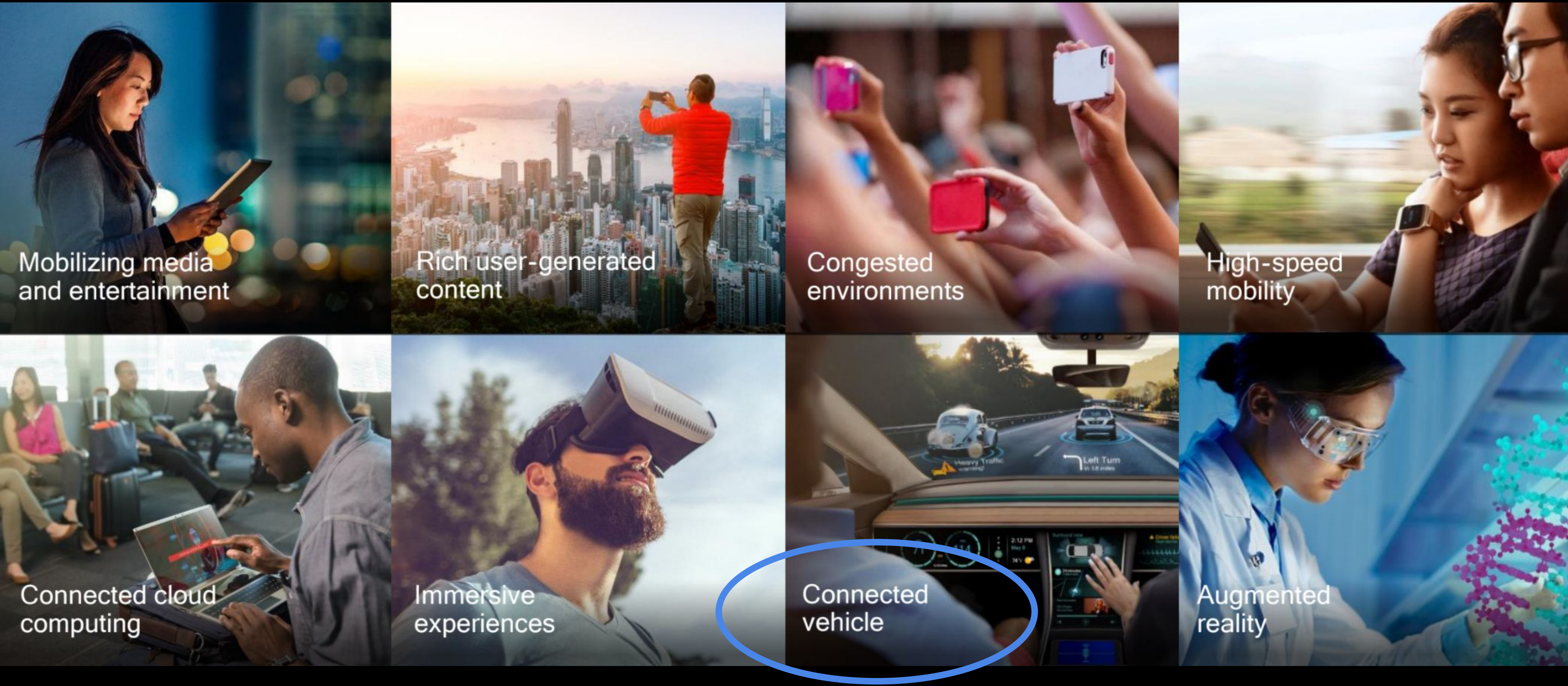
- This document contains illustrations and charts from Swisscom, Ericsson, Huawei, and Qualcomm
- sites.google.com/site/lteencyclopedia/home
- 5G Cellular

operator co-location
(tower in FL, USA)

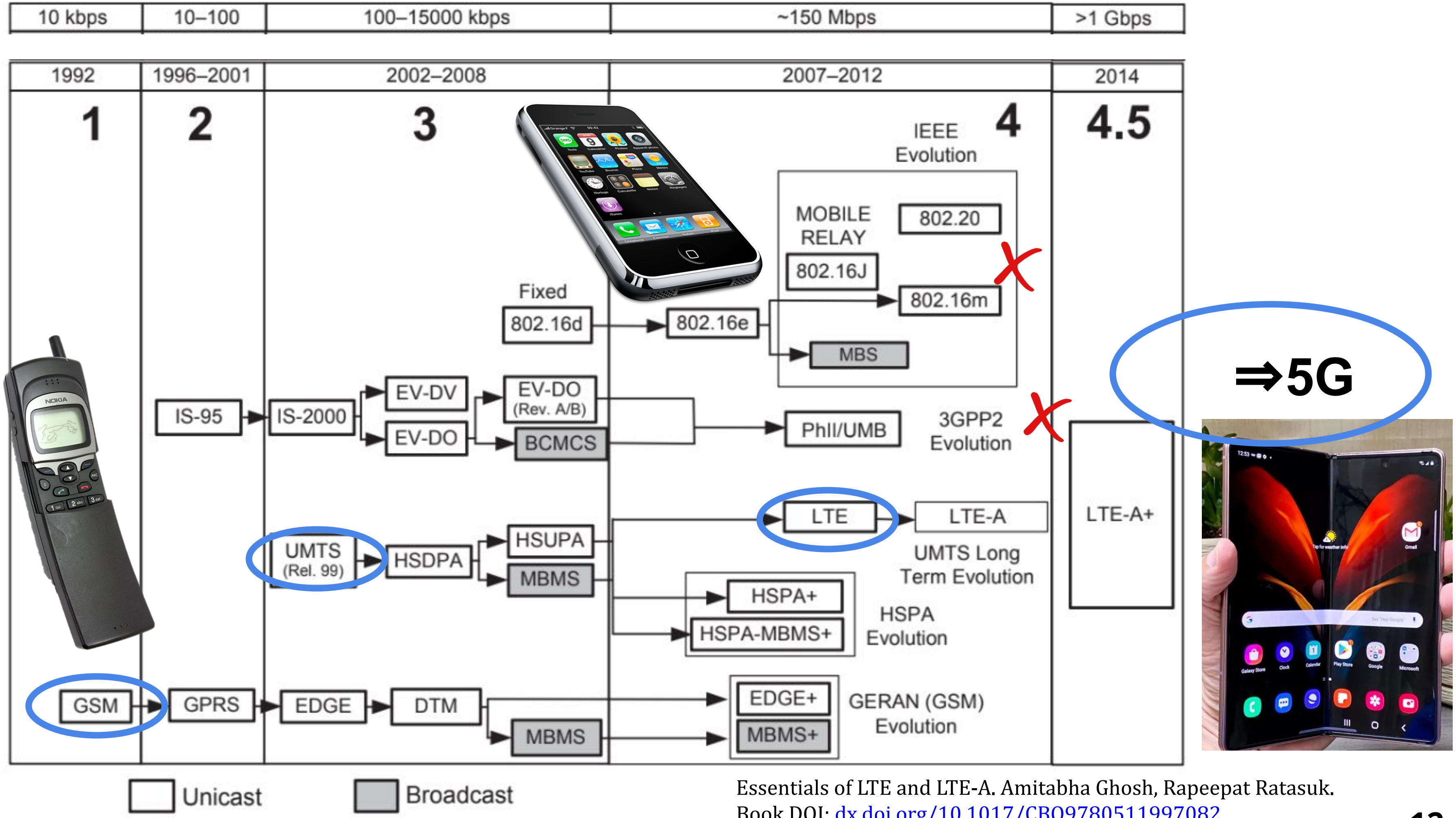
Overview of the 3GPP Cellular Standard

- The original study item on Long Term Evolution (LTE) of 3GPP Radio Access Technology (RAT) was initiated with the aim to ensure that 3GPP RAT is competitive in the future.
  - Focus has been on enhancement of the radio-access technology and optimization of the core network.
- The key driving factors for 4G LTE have been:
  - Higher data rate with reduced latency
  - Reduced cost for the operator
  - Efficient & flexible spectrum utilization
  - Improved system capacity and coverage
- 5G improves all this, and additionally will offer very reliable low-latency services (industry 4.0, vehicles, AR/VR & games)

Vertical Markets, 5G as Enabling Technology (QUALCOMM)

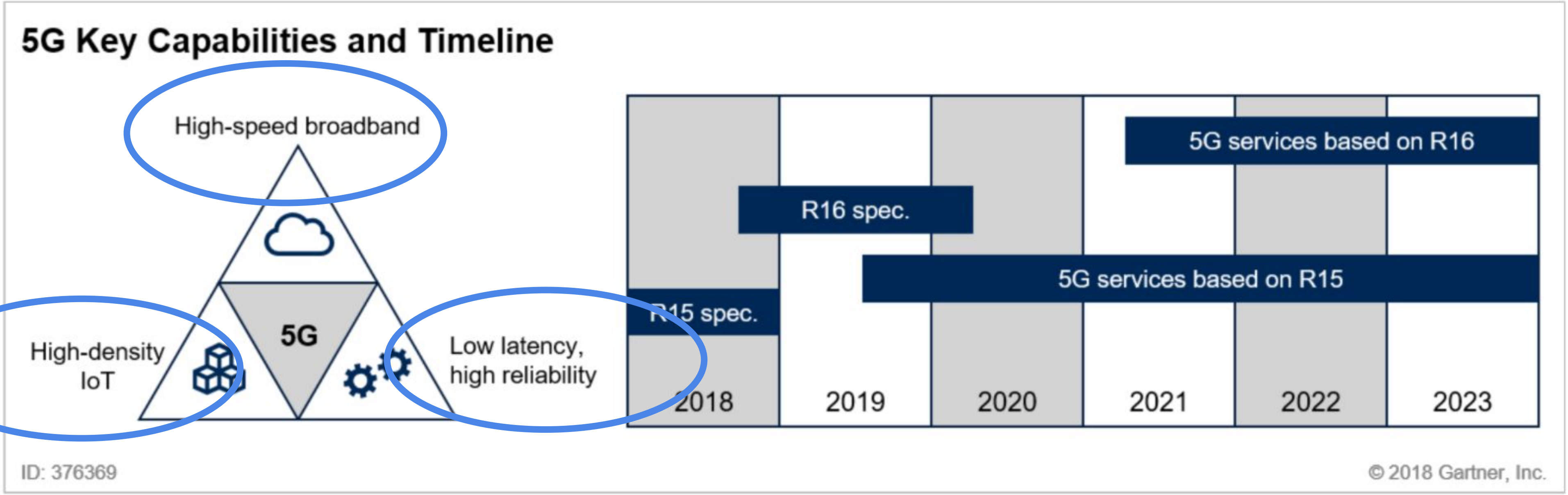


Vertical Markets, 5G as Enabling Technology (QUALCOMM)



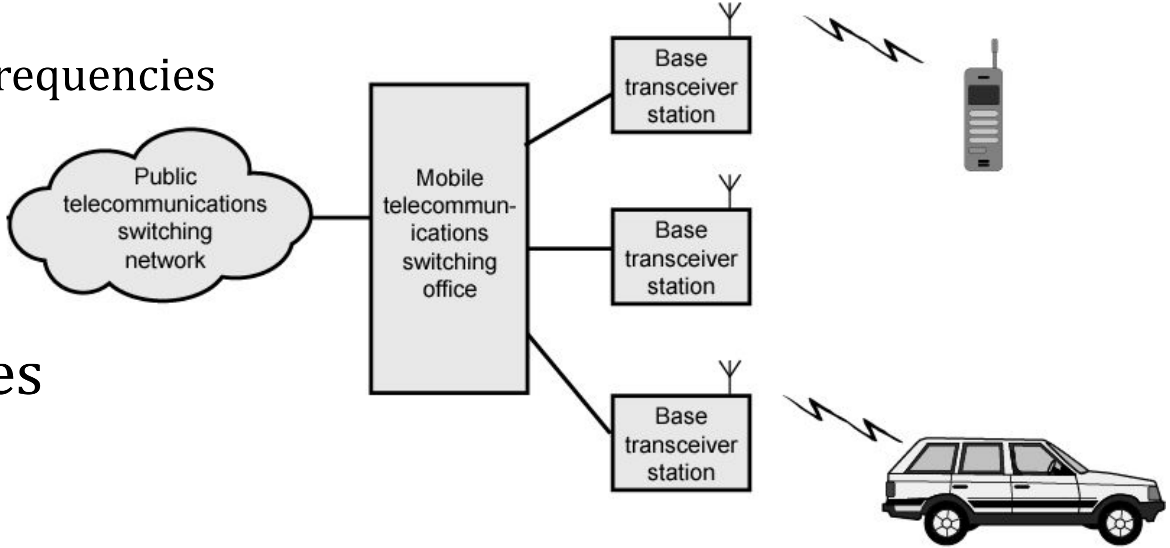
Essentials of LTE and LTE-A. Amitabha Ghosh, Rapeepat Ratasuk.
Book DOI: dx.doi.org/10.1017/CBO9780511997082

2018, Gartner

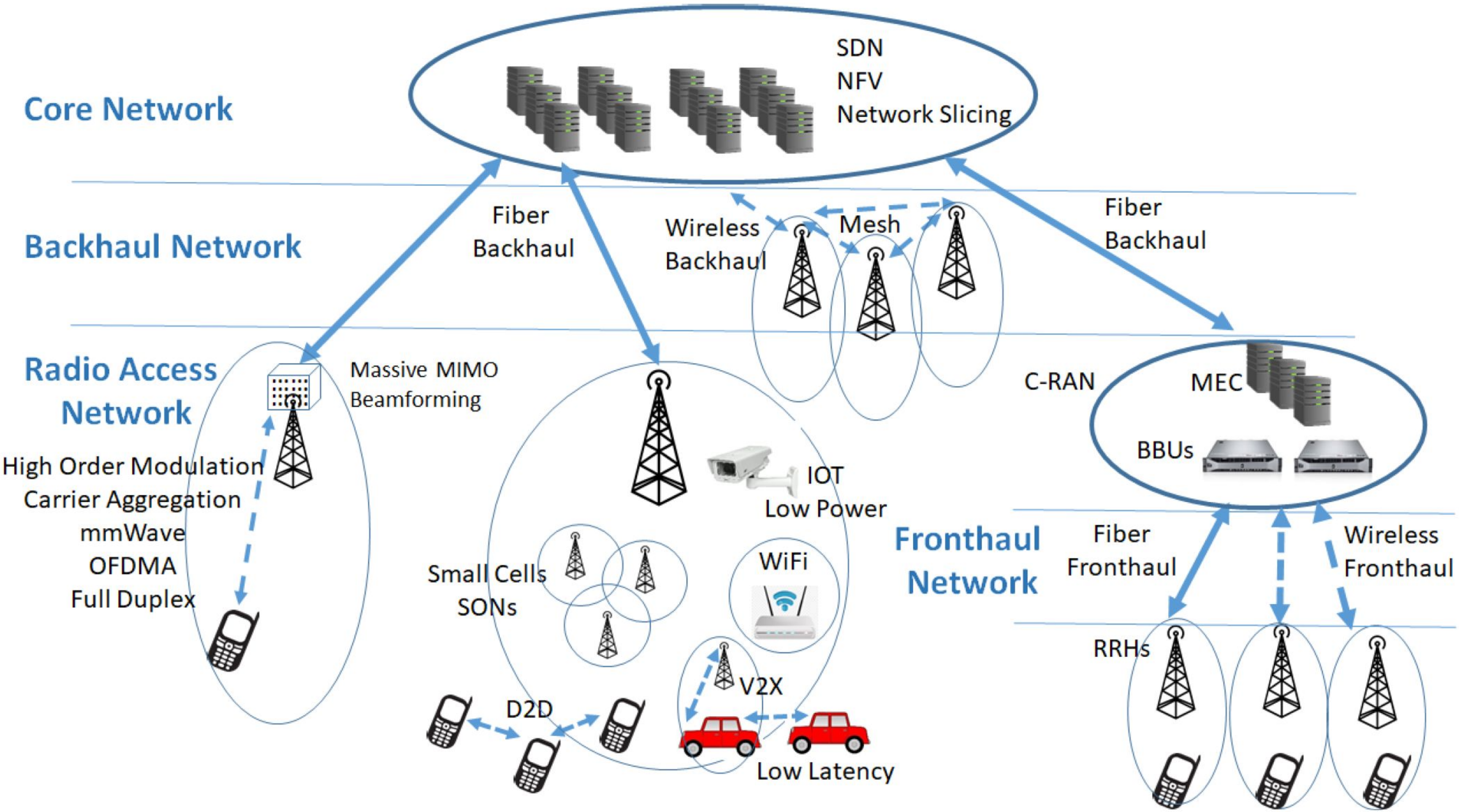


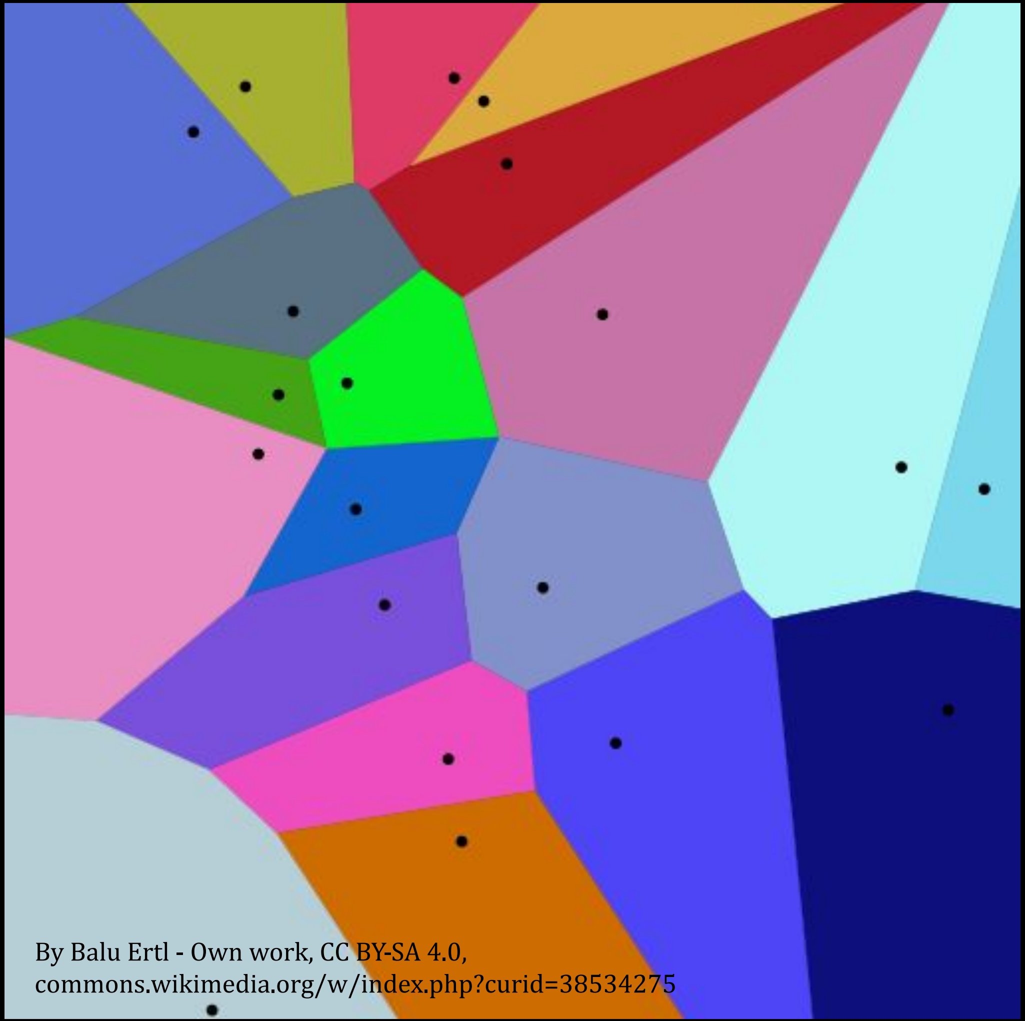
Cellular Networks

- Multiple low power transmitters
  - 10 Watt or less
- Coverage area is divided into cells
  - Each with own antenna
  - Each with own range of frequencies
  - Served by base station: Transceiver, control unit
- Adjacent cells operate on different frequencies to avoid crosstalk

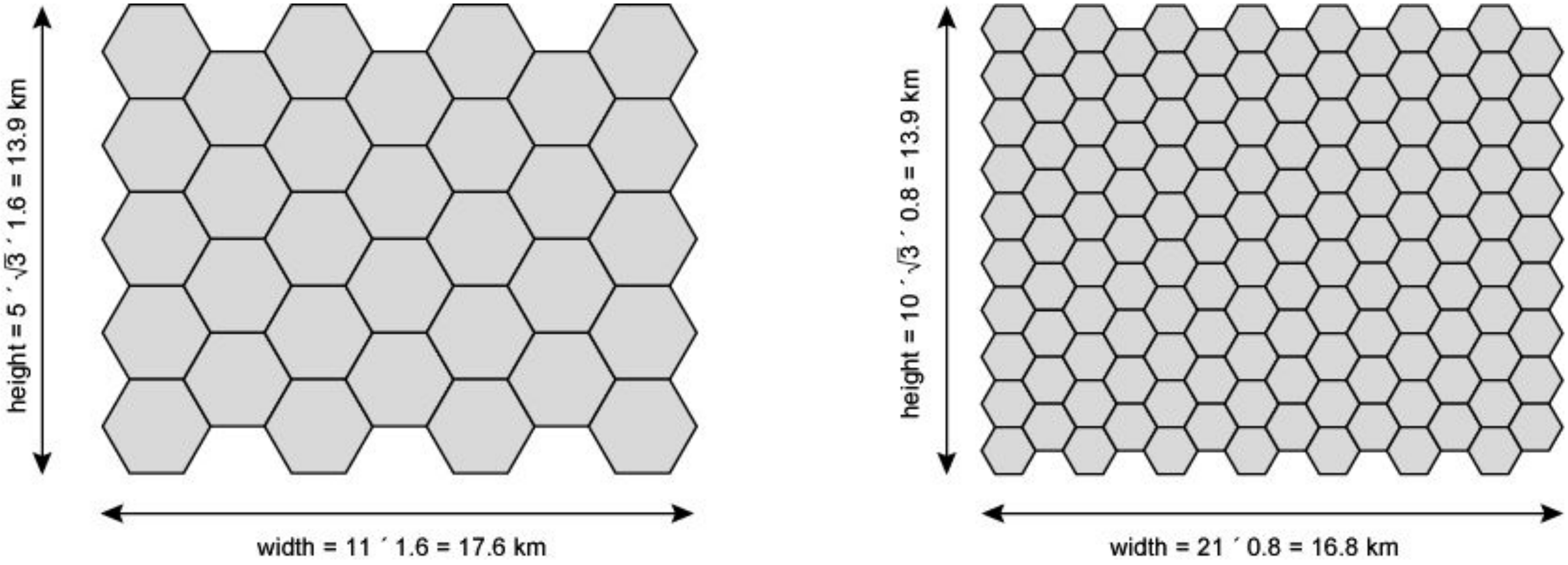


Cellular Infrastructure





Radio Cells



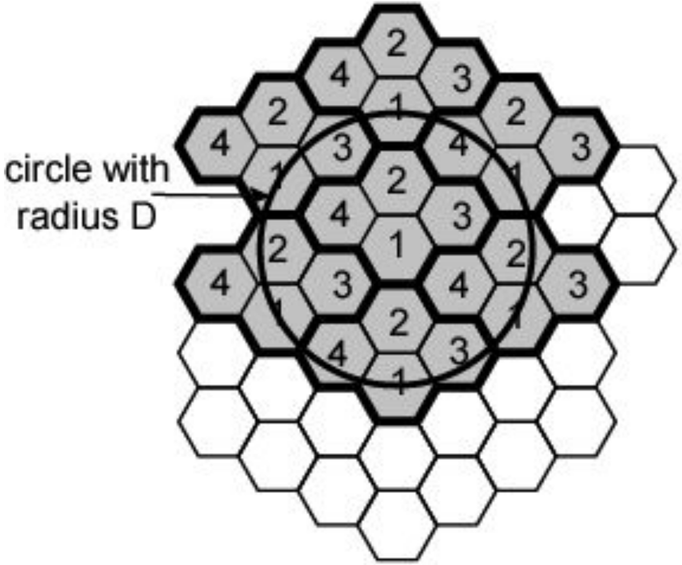
(a) Cell radius = 1.6 km

(b) Cell radius = 0.8 km

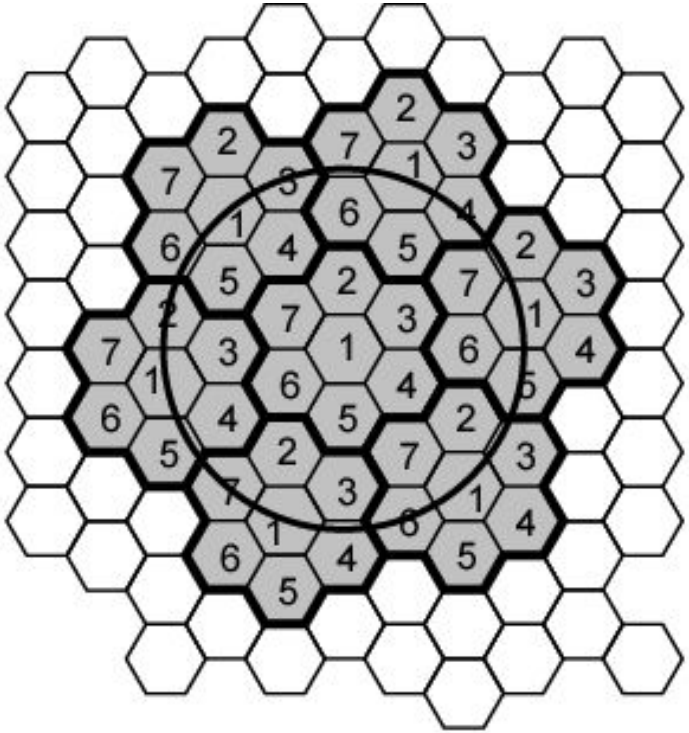
Basic Principle: Reuse of Radio Resources

- Communication within one cell on a given frequency
- Re-use of this frequency in a nearby cell
- Use the same frequency for multiple data streams, but at different locations
- Typically, 10 – 50 frequencies per base station
- For example:
    - N cells all using same number of frequencies
    - K total number of frequencies used in systems
    - Each cell operates with K/N frequencies

Reuse Pattern (1)

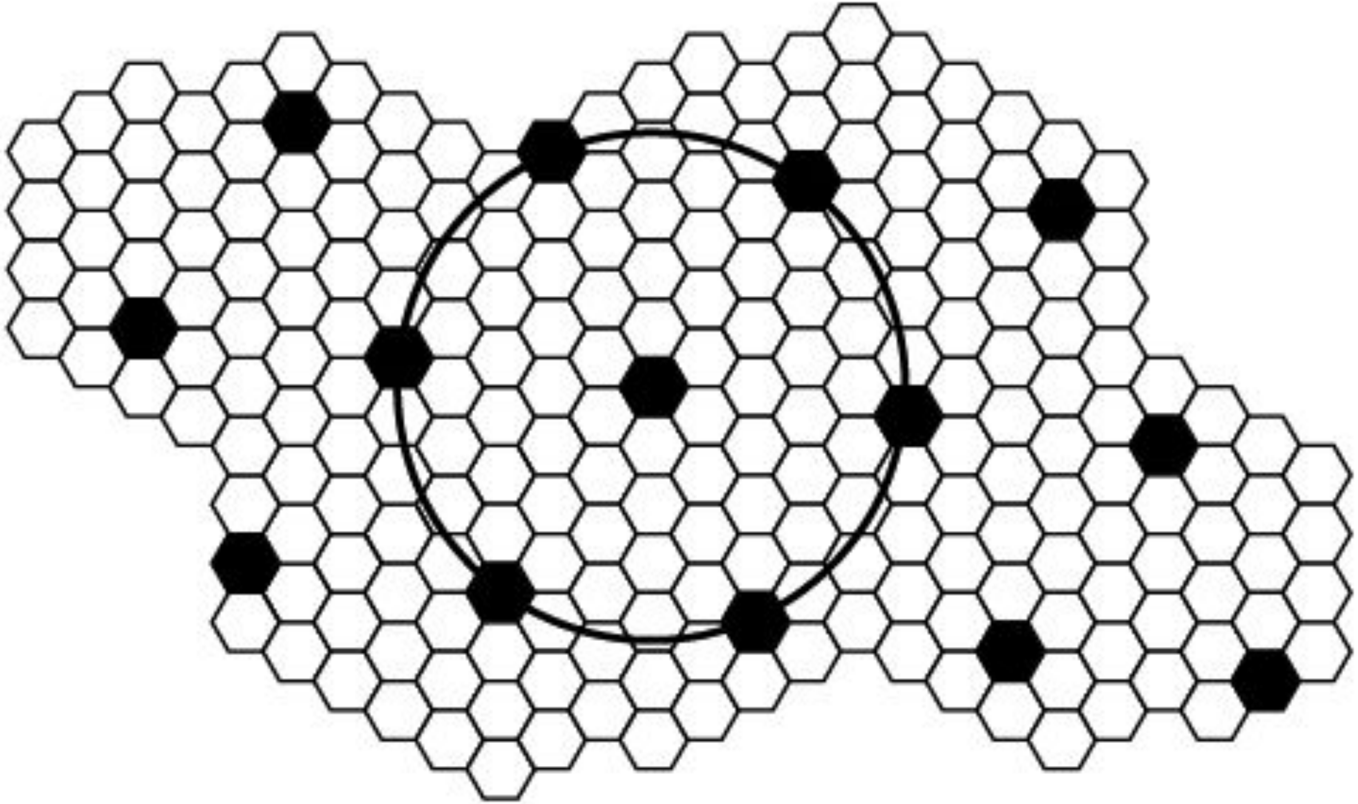


(a) Frequency reuse pattern for N = 4



(b) Frequency reuse pattern for N = 7

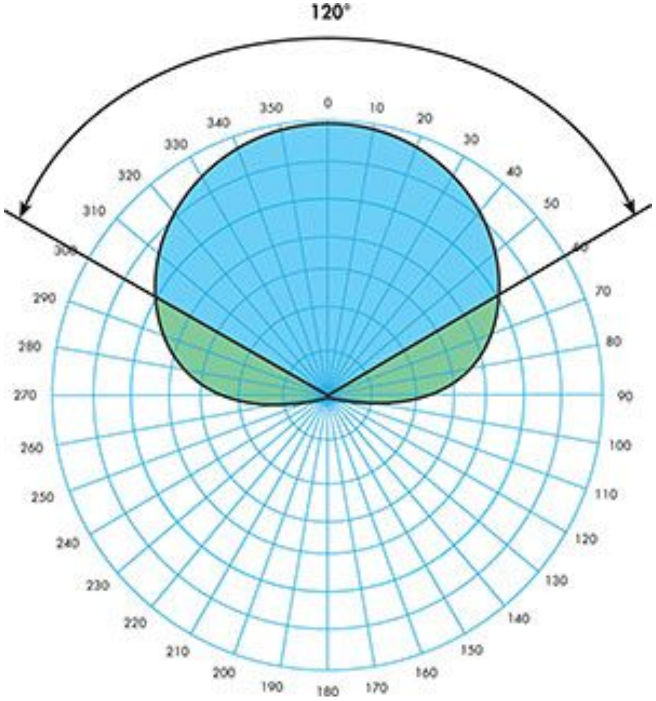
Reuse Pattern (2)



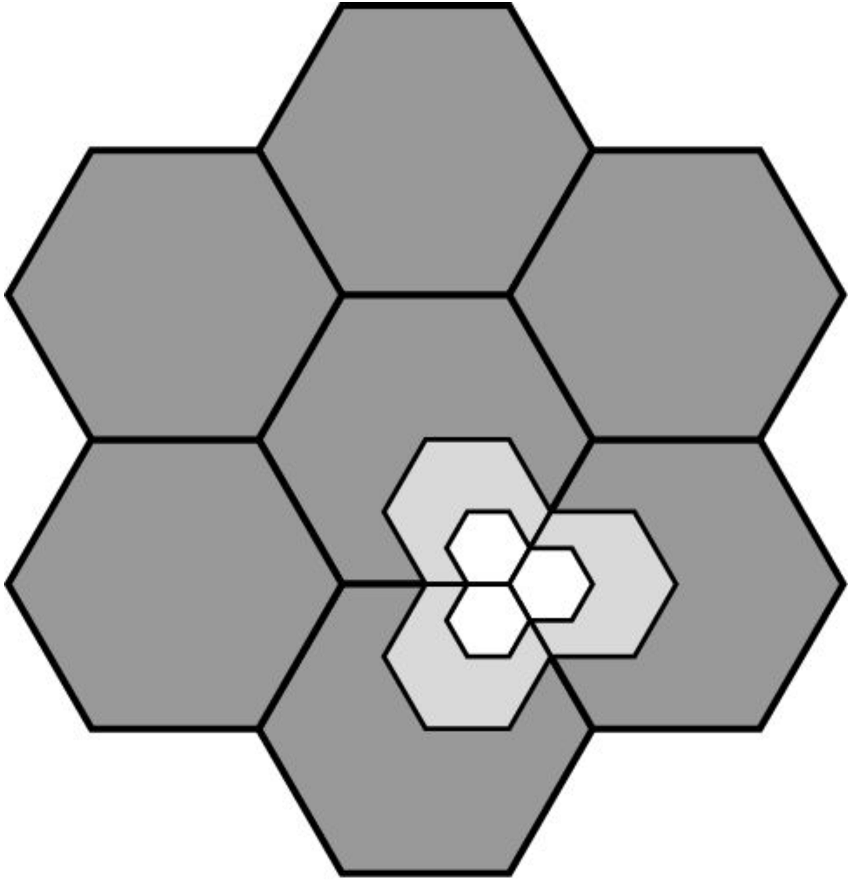
(c) Black cells indicate a frequency reuse for N = 19

How to Increase the Network Capacity (bit/s/Hz/m^2)

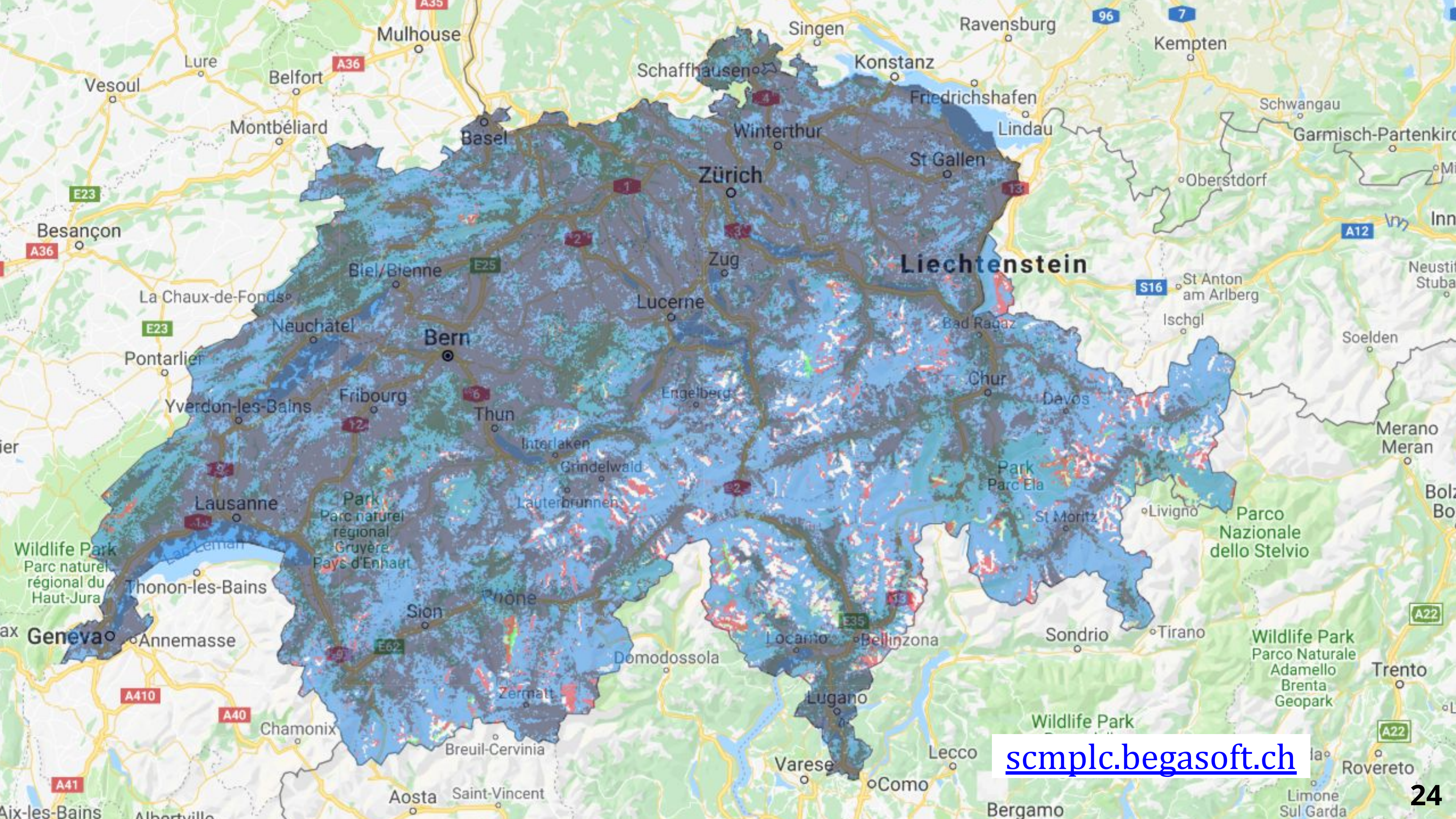
- Add new frequency channels, new radio spectrum
- Increase number of cells
- Cell Sectorization
  - Cell divided into sectors
  - 3 – 6 sectors per cell
  - Sectorized (directional) antennas
- Dynamic frequency borrowing
  - Take frequencies from other cells when possible
  - Even across telco operators
- Microcells (see next page)



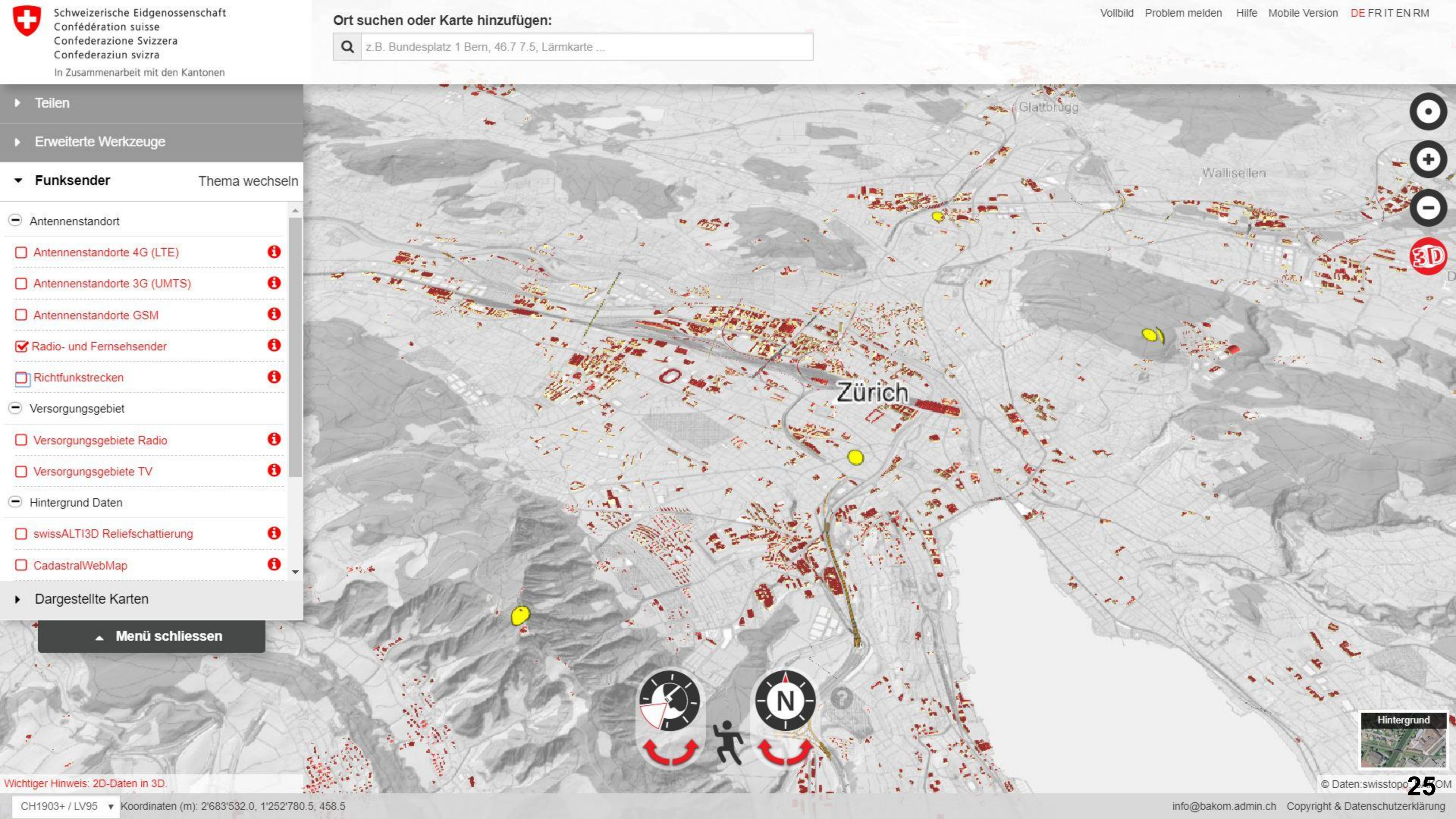
Cell Splitting with Micro Cells

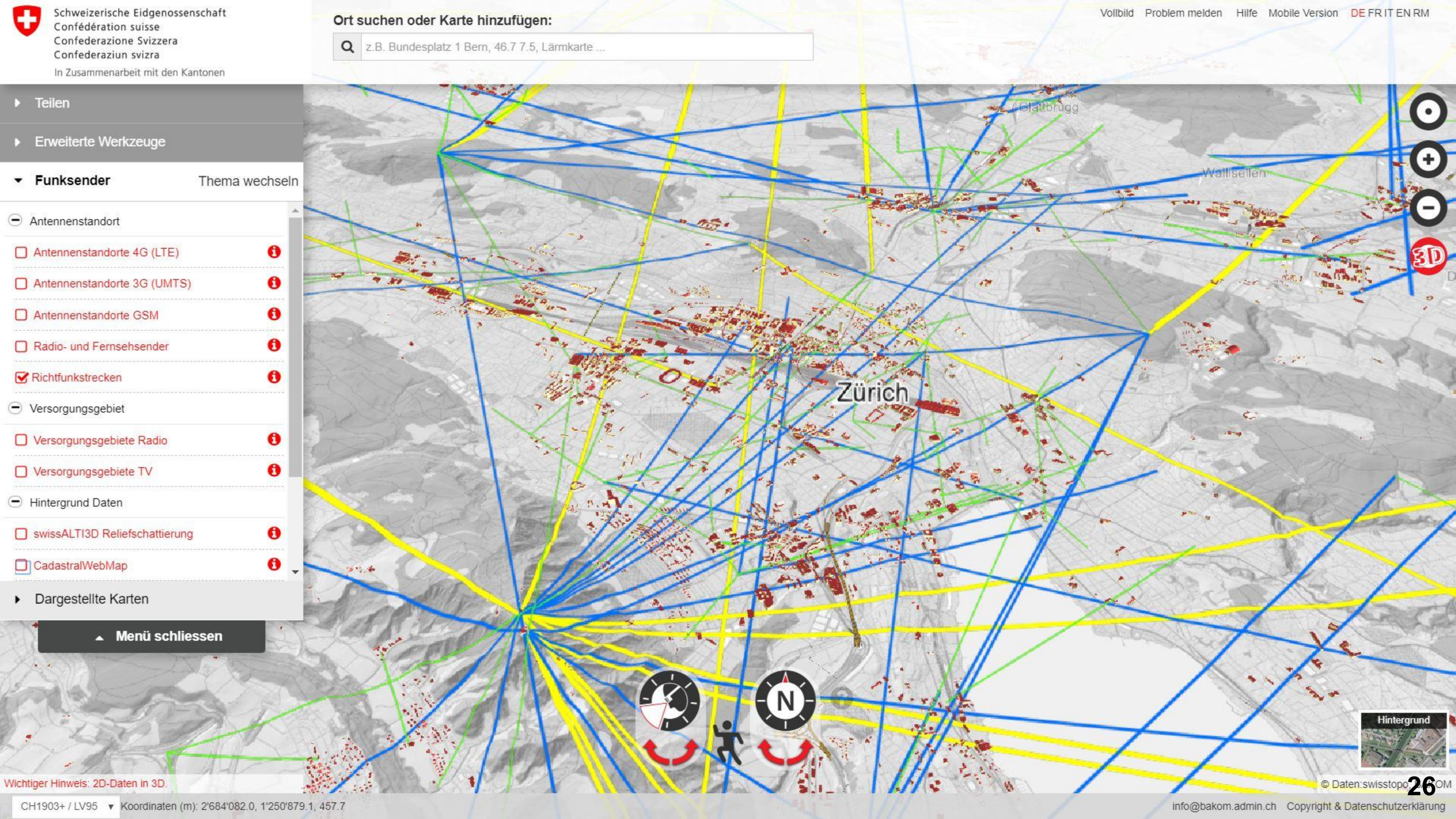


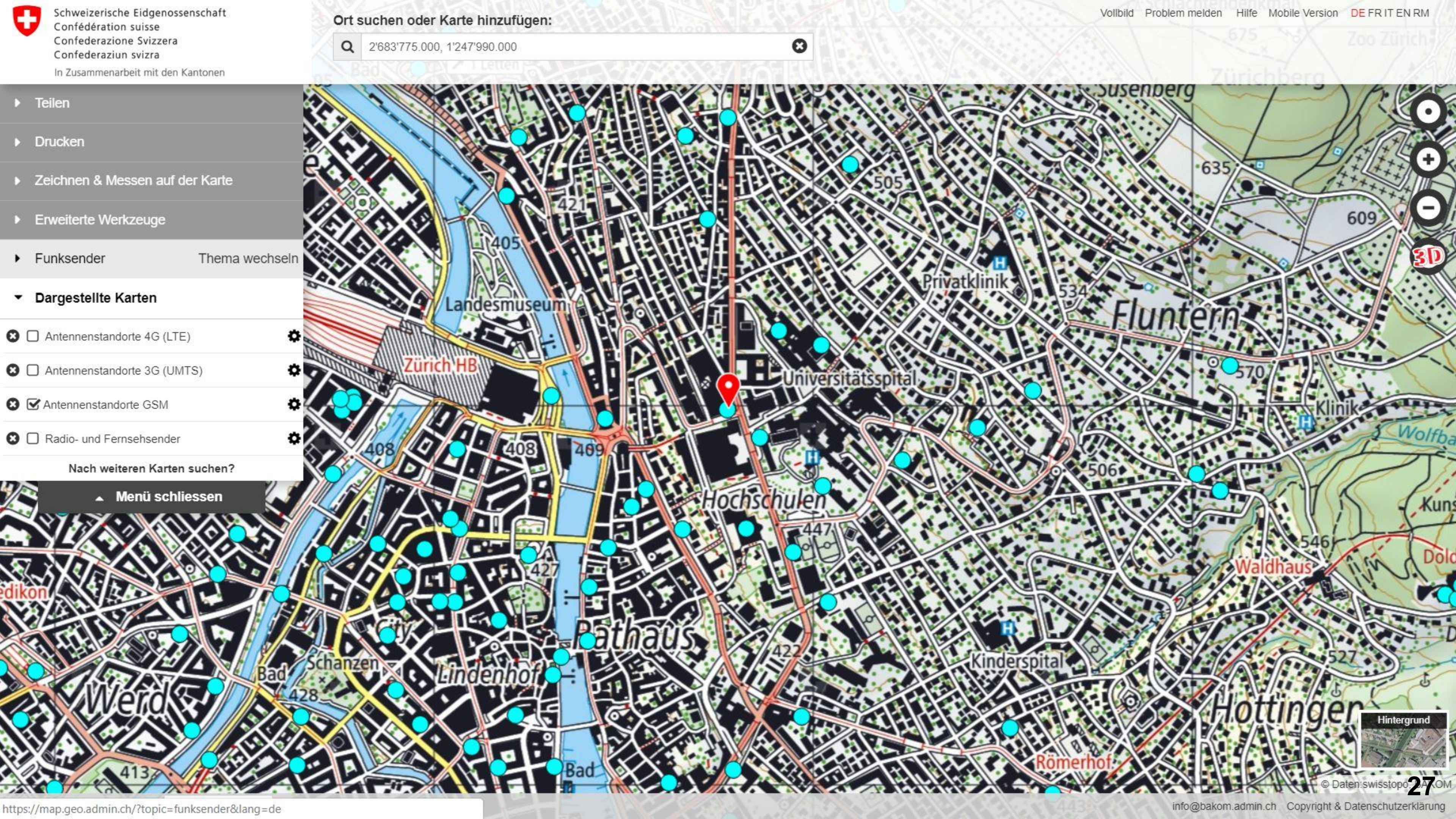
Ericsson's "Multi-Operator Dot"

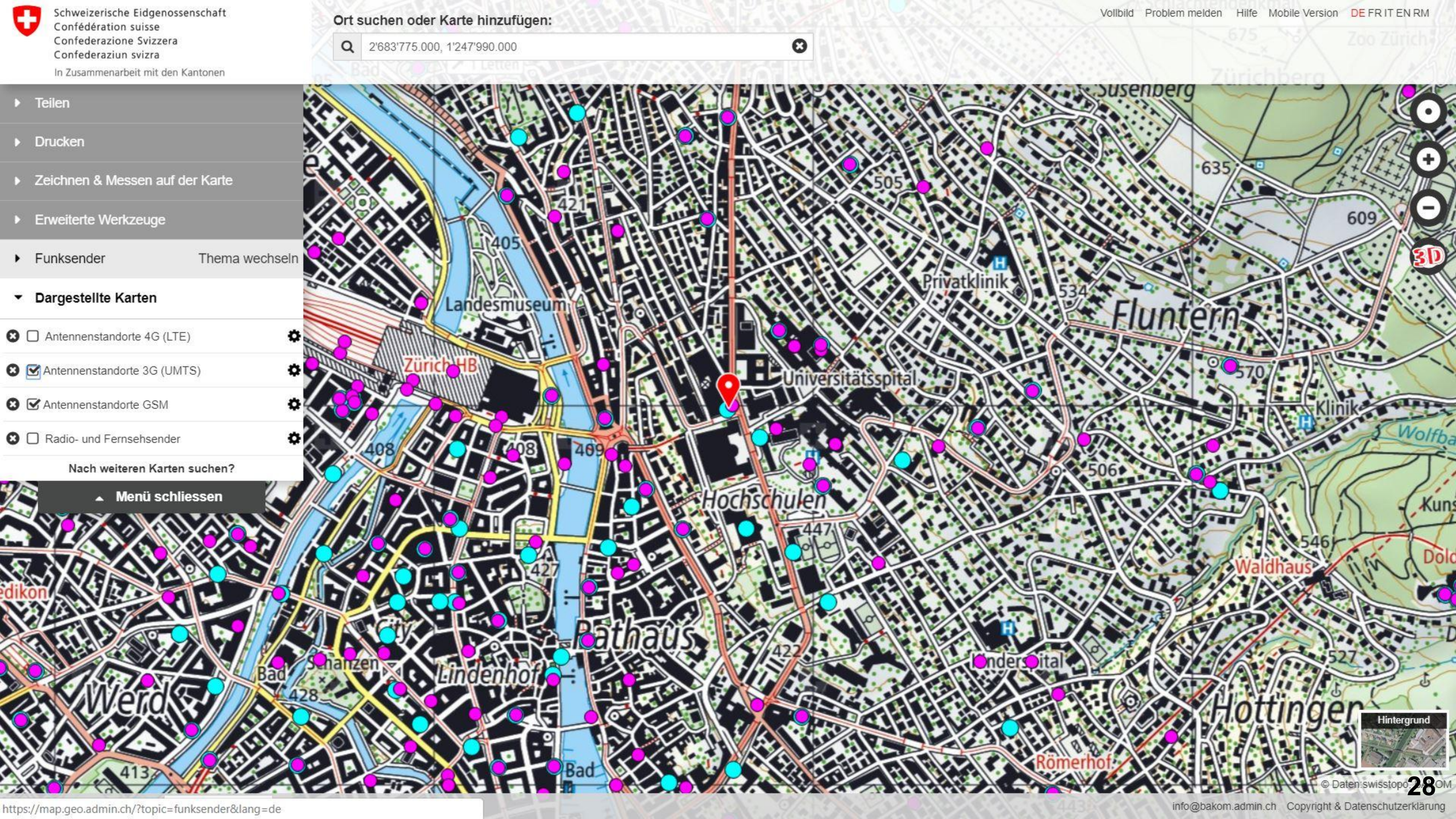


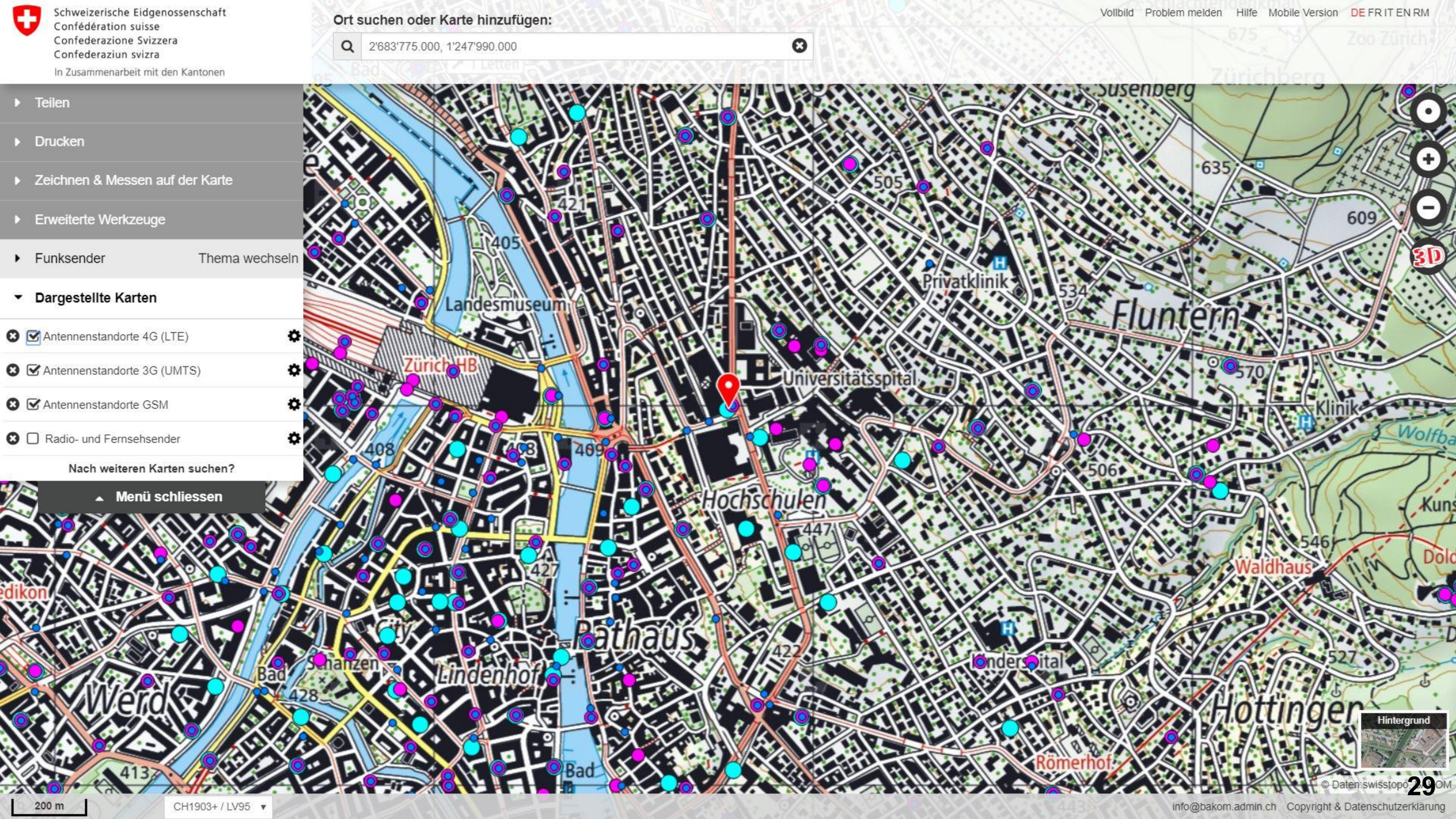
scmplc.begasoft.ch


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
In Zusammenarbeit mit den Kantonen
Ort suchen oder Karte hinzufügen:
z.B. Bundesplatz 1 Bern, 46.7 7.5, Lärmkarte ...
Vollbild
Problem melden
Hilfe
Mobile Version
DE FR IT EN RM
Teilen
Erweiterte Werkzeuge
Funksender
Thema wechseln
Antennenstandort
Antennenstandorte 4G (LTE)
Antennenstandorte 3G (UMTS)
Antennenstandorte GSM
Radio- und Fernsehsender
Richtfunkstrecken
Versorgungsgebiet
Versorgungsgebiete Radio
Versorgungsgebiete TV
Hintergrund Daten
swissALTI3D Reliefschattierung
CadastralWebMap
Dargestellte Karten
Menü schliessen
Glattbrugg
Wallisellen
Zürich
3D
N
Hintergrund
Wichtiger Hinweis: 2D-Daten in 3D.
CH1903+ / LV95
Koordinaten (m): 2'683'532.0, 1'252'780.5, 458.5
info@bakom.admin.ch
Copyright & Datenschutzerklärung


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
In Zusammenarbeit mit den Kantonen
Ort suchen oder Karte hinzufügen:
z.B. Bundesplatz 1 Bern, 46.7 7.5, Lärmkarte ...
Vollbild
Problem melden
Hilfe
Mobile Version
DE FR IT EN RM
Teilen
Erweiterte Werkzeuge
Funksender
Thema wechseln
Antennenstandort
Antennenstandorte 4G (LTE)
Antennenstandorte 3G (UMTS)
Antennenstandorte GSM
Radio- und Fernsehsender
Richtfunkstrecken
Versorgungsgebiet
Versorgungsgebiete Radio
Versorgungsgebiete TV
Hintergrund Daten
swissALTI3D Reliefschattierung
CadastralWebMap
Dargestellte Karten
Menü schliessen
Glattbrugg
Wallisellen
Zürich
3D
N
Hintergrund
Wichtiger Hinweis: 2D-Daten in 3D.
CH1903+ / LV95
Koordinaten (m): 2'684'082.0, 1'250'879.1, 457.7
© Daten:swisstopo
info@bakom.admin.ch
Copyright & Datenschutzerklärung

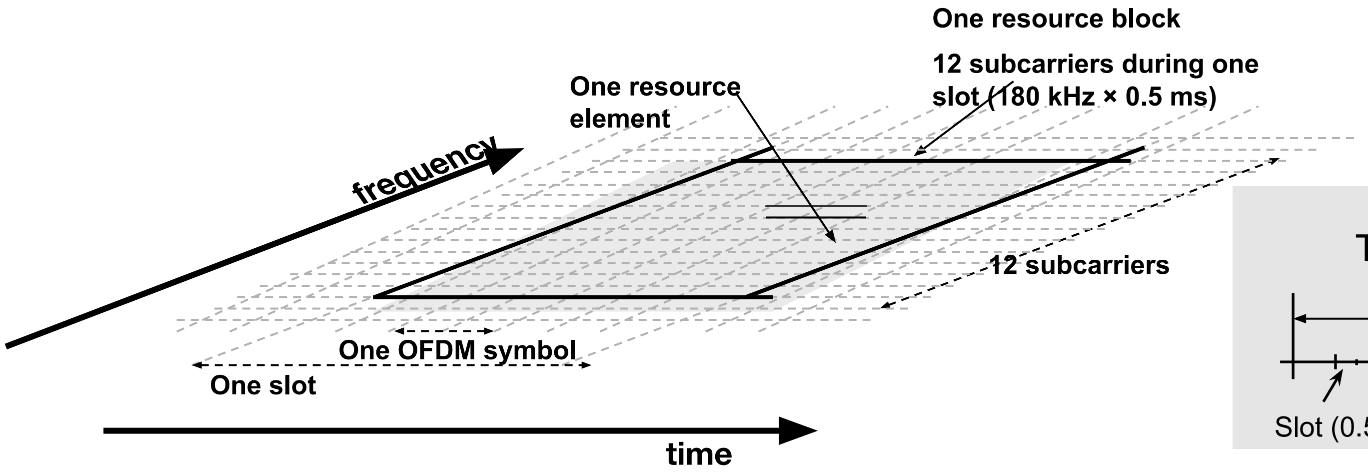

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
In Zusammenarbeit mit den Kantonen
Ort suchen oder Karte hinzufügen:
2'683'775.000, 1'247'990.000
Vollbild
Problem melden
Hilfe
Mobile Version
DE FR IT EN RM
Teilen
Drucken
Zeichnen & Messen auf der Karte
Erweiterte Werkzeuge
Funksender
Thema wechseln
Dargestellte Karten
Antennenstandorte 4G (LTE)
Antennenstandorte 3G (UMTS)
Antennenstandorte GSM
Radio- und Fernsehsender
Nach weiteren Karten suchen?
Menü schliessen
Susenberg
Zürichberg
Landesmuseum
Zürich HB
Privatklinik
Fluntern
Universitätsspital
Klinik
Hochschulen
Waldhaus
City
Rathaus
Schanzen
Lindenhof
Werd
Kinderspital
Hottingen
Römerhof
Bad
Hintergrund
© Daten: swisstopo
https://map.geo.admin.ch/?topic=funksender&lang=de
info@bakom.admin.ch
Copyright & Datenschutzerklärung

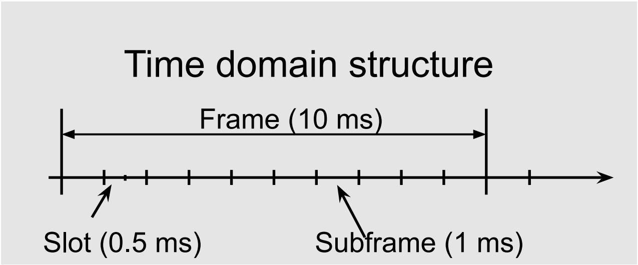

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
In Zusammenarbeit mit den Kantonen
Ort suchen oder Karte hinzufügen:
2'683'775.000, 1'247'990.000
Vollbild
Problem melden
Hilfe
Mobile Version
DE FR IT EN RM
Teilen
Drucken
Zeichnen & Messen auf der Karte
Erweiterte Werkzeuge
Funksender
Thema wechseln
Dargestellte Karten
Antennenstandorte 4G (LTE)
Antennenstandorte 3G (UMTS)
Antennenstandorte GSM
Radio- und Fernsehsender
Nach weiteren Karten suchen?
Menü schliessen
Landesmuseum
Zürich HB
Universitätsspital
Privatklinik
Fluntern
Hochschulen
Rathaus
Lindenhof
Werd
Hottingen
Waldhaus
Römerhof
Susenberg
Klinik
Hintergrund
© Daten: swisstopo
https://map.geo.admin.ch/?topic=funksender&lang=de
info@bakom.admin.ch
Copyright & Datenschutzerklärung


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
In Zusammenarbeit mit den Kantonen
Ort suchen oder Karte hinzufügen:
2'683'775.000, 1'247'990.000
Vollbild
Problem melden
Hilfe
Mobile Version
DE FR IT EN RM
Teilen
Drucken
Zeichnen & Messen auf der Karte
Erweiterte Werkzeuge
Funksender
Thema wechseln
Dargestellte Karten
Antennenstandorte 4G (LTE)
Antennenstandorte 3G (UMTS)
Antennenstandorte GSM
Radio- und Fernsehsender
Nach weiteren Karten suchen?
Menü schliessen
Landesmuseum
Zürich HB
Universitätsspital
Privatklinik
Fluntern
Hochschulen
Rathaus
Lindenhof
Werd
Waldhaus
Hottingen
Römerhof
Klinik
Susenberg
Hintergrund
© Daten: swisstopo
200 m
CH1903+ / LV95
info@bakom.admin.ch
Copyright & Datenschutzerklärung

LTE Air Interface

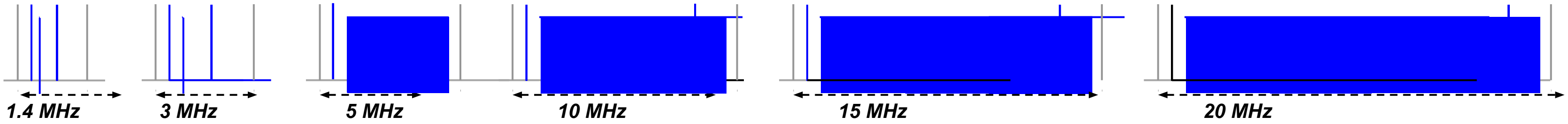
- The key improvement in LTE radio is the use of OFDM
- Orthogonal Frequency Division Multiplexing
- Just like Wi-Fi !





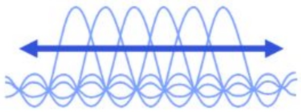
LTE Air Interface

- OFDM(A), deviating from spread spectrum / CDMA
- Real-time functions performed in base stations
  - No need for a central Radio Network Controller (RNC)
  - No real-time signalling network network core entities
- Packet oriented
  - Supports bursty traffic and statistical multiplexing by default
  - No specific support for circuit switched traffic (voice)
- Scalable spectrum use:



5G “New Radio” Air Interface

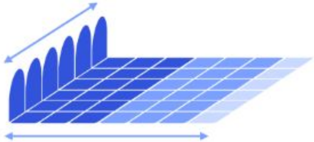
Scalable OFDM-based air interface



Scalable OFDM numerology

Efficiently address diverse spectrum, deployments/services

Flexible slot-based framework



Self-contained slot structure

Key enabler to low latency, URLLC and forward compatibility

Advanced channel coding

Multi-Edge LDPC and CRC-Aided Polar

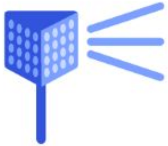
Efficiently support large data blocks and a reliable control channel

Massive MIMO

Reciprocity-based MU-MIMO

Efficiently utilize a large number of antennas to increase coverage/capacity

Mobile mmWave



Beamforming and beam-tracking

Enables wide mmWave bandwidths for extreme capacity and throughput

Source: Qualcomm

5G Challenges

huawei.com/minisite/5g/img/Huawei%205G%20Overview.pdf

5G “New Radio” - 3GPP Release 16

Source: Qualcomm

1. New Rel-16 SI; 2. Rel-15 SI converting to Rel-16 WI; 3. Also include UE power consumption, network interference management, mobility, and NOMA; 4. Rel-16 WI to enable LTE IoT in-band with 5G NR; 5. Enhancing LTE enTV in Rel-14 to meet 5G requirements; 6. Non-terrestrial networks, 5G NR SON/MDT and more... 9

SDN and NFV

Software Defined Networking, Network Functionality Virtualization

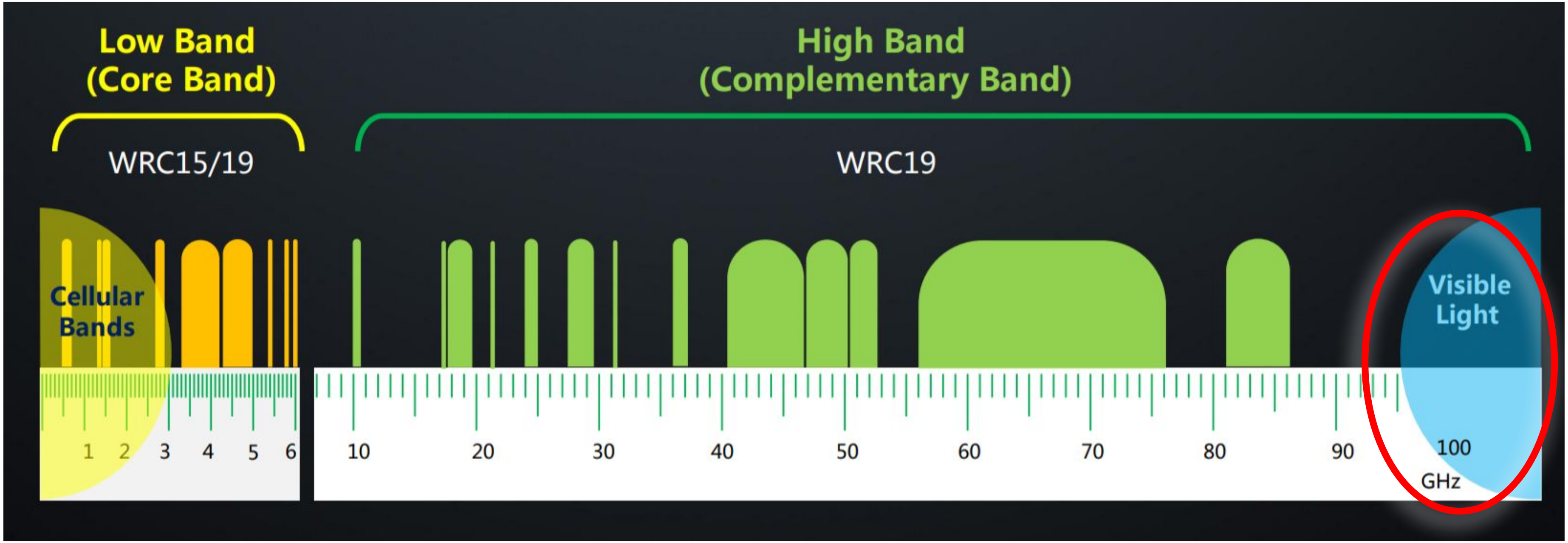
- Virtualization separates the hardware and software functions of network elements such as IP packet routers.
  - Networks contain routers and switches for data forwarding and network control. SDN, centralizes the network control functions in a single software-based SDN controller.
  - Then, routers/switches only perform forwarding
- The SDN controller oversees a large part of the network and determines the routes for packets
  - Claimed to be especially useful when network is congested or unreachable
- Main opportunity: Separate infrastructure from operator, lower entry level for newcomers

Huawei: Unified Standard

huawei.com/minisite/5g/img/Huawei%205G%20Overview.pdf

Visible Light Communication might be used too!

- VLC might be considered in the future
  - WRC = World Radio Conference



Wireless Networking and Mobile Computing

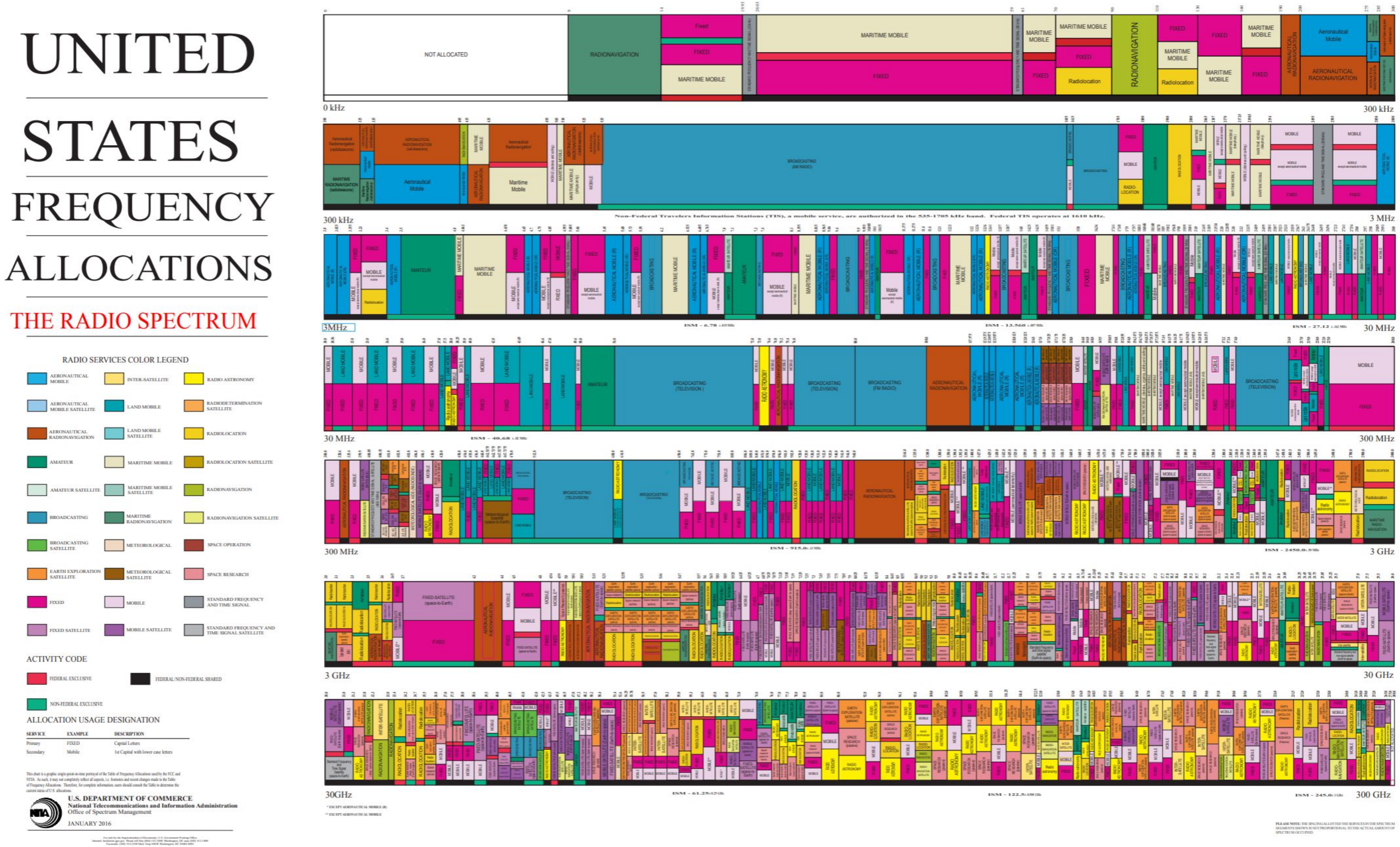
10. Cognitive Radio and Spectrum Sharing, Delay Tolerant Networking

Stefan Mangold

Course Outline

1. Introduction
2. Wireless Communication Basics
3. IEEE 802.11 Wireless LAN (Wi-Fi)
4. IEEE 802.15 Wireless PAN (ZigBee & Bluetooth)
5. Mobile Computing Algorithm Basics: Control and Game Theory
6. Visible Light Communication
7. Audio Communication
8. Cellular Networking Basics (LTE, 5G, Internet-of-Things)
9. Mobile Computing for Automated Medicine Delivery
10. Cognitive Radio, Delay Tolerant Networking, Radio Spectrum Sharing

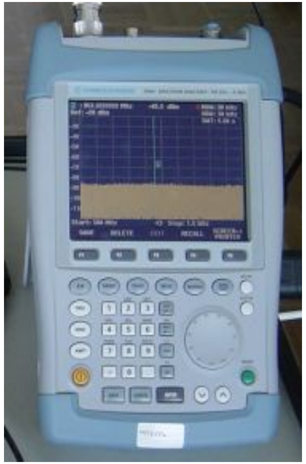
FCC Radio Spectrum

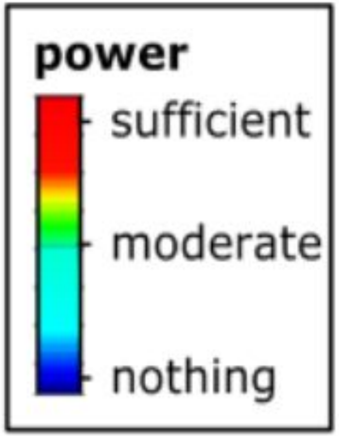


https://www.ntia.doc.gov/files/ntia/publications/january_2016_spectrum_wall_chart.pdf

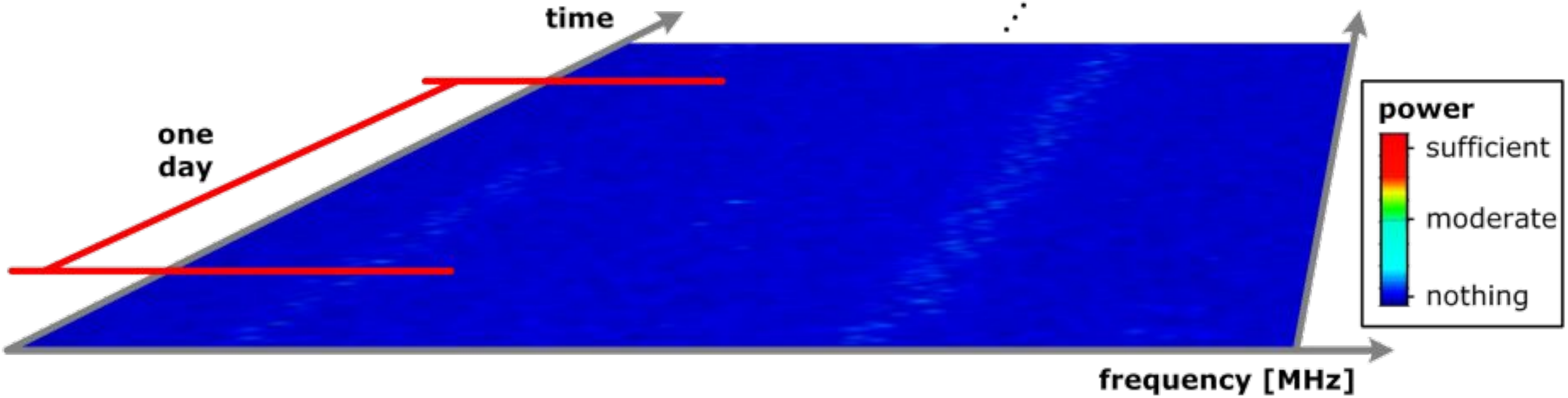
Let’s find out what’s going on in the Radio Spectrum

- Let us measure how overloaded it is!
- We use a simple omni-antenna and a spectrum scanner
- We measure in all directions, for a long time

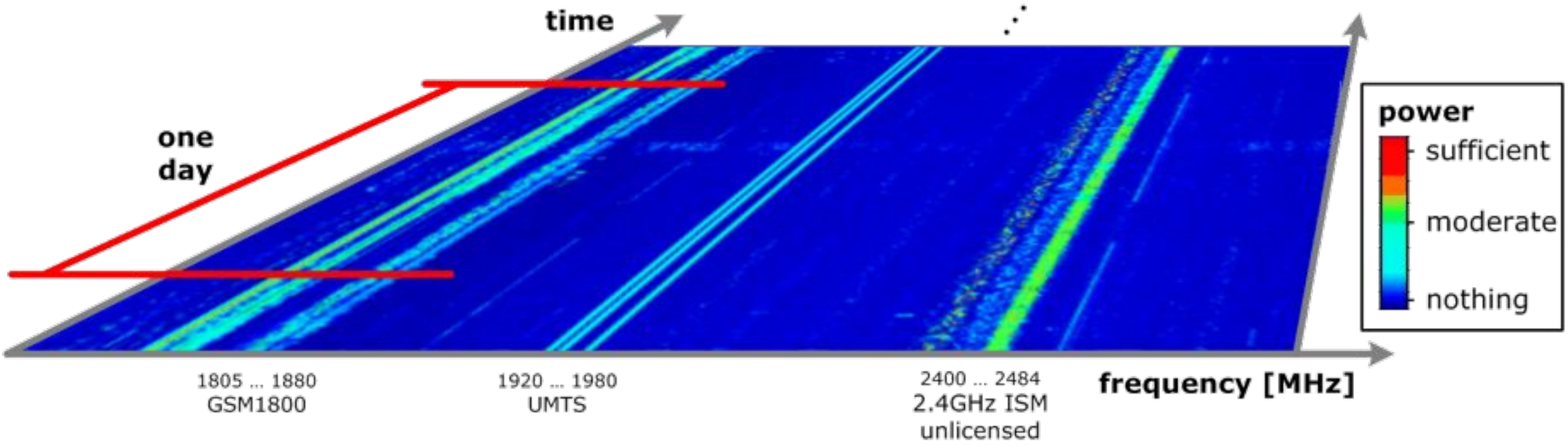




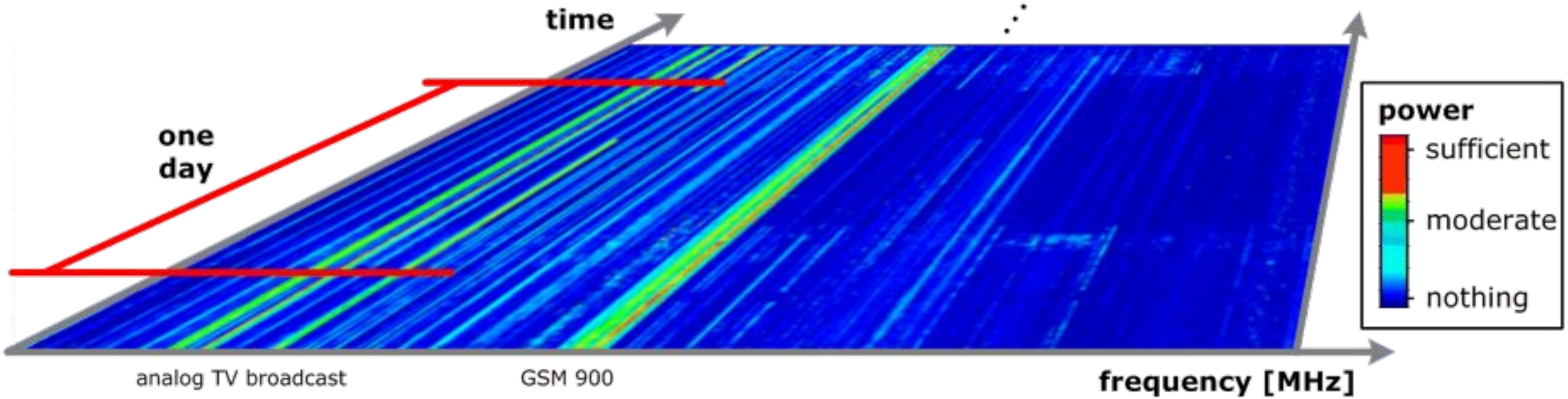
In a Closed Shelter in Berne, Switzerland



Office Space 1.5 GHz … 3 GHz



Office Space, 0.5 GHz … 1.5 GHz



DARPA NeXt Generation (XG) Program

- XG was a (not entirely successful) attempt for a technology development project
  - sponsored by DARPA's Strategic Technology Office
- Objective:
  - “To develop both the enabling technologies and system concepts to dynamically redistribute allocated spectrum along with novel waveforms ...”
  - “... to provide [...] improvements in assured military communications in support of a full range of worldwide deployments."
- XG might have been too ambitious (at its time, before 2010)

DARPA XG Reasoning Engine

- A mechanism to create previously unknown assertions, and to demonstrate their truth
  - The reasoner creates an assertion upon stimulus
  - Starts with premises (the existing knowledge, spectrum regulation)
  - Uses valid inference rules (the arguments)
  - Infers a conclusion (the actual action)
- Reasoning engines
  - Realized with languages such as web ontology language OWL
  - Exploit first order predicate logic
- BENEFITS: Traceable decision making and patent infringement detection

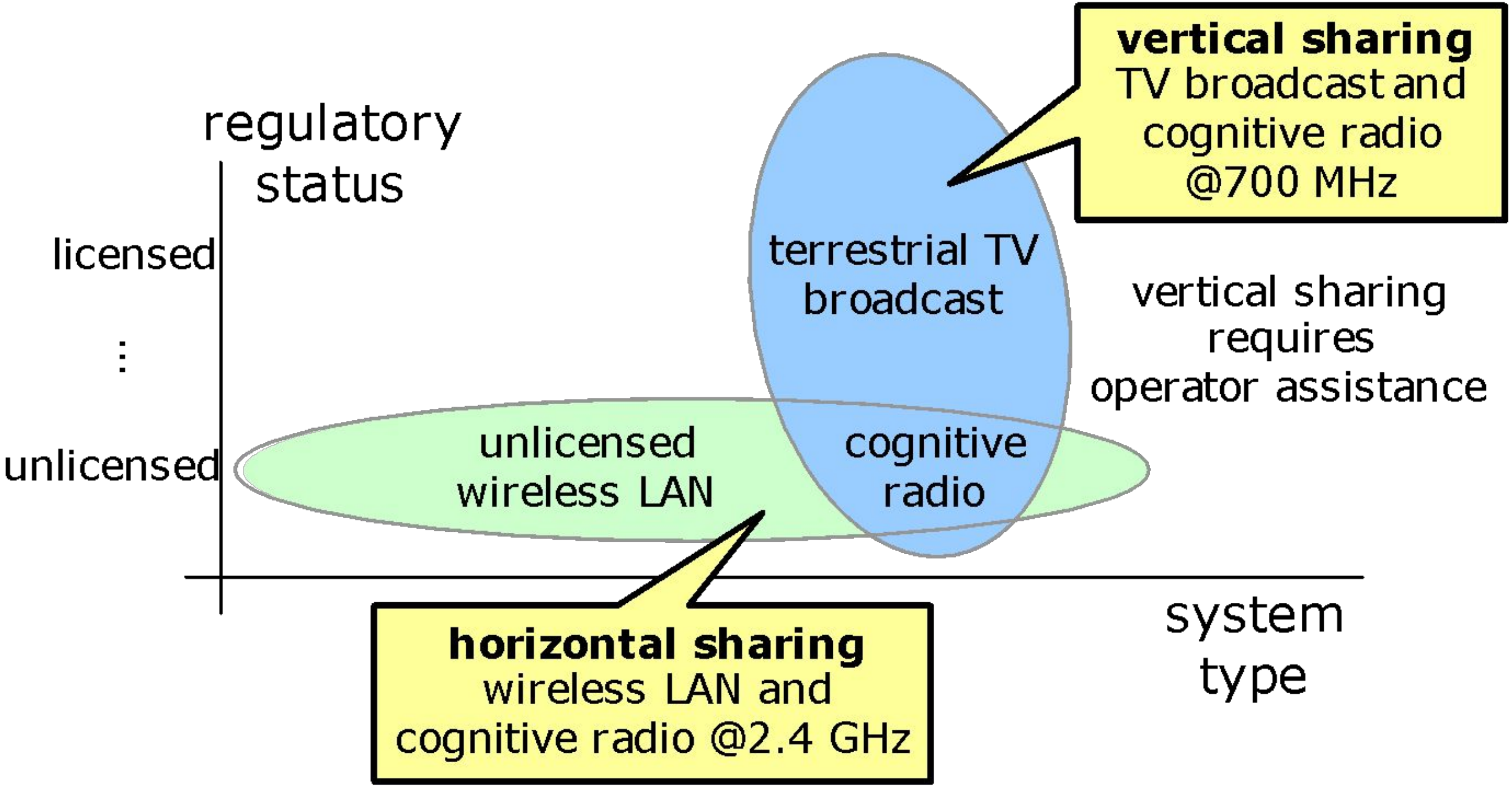
Example

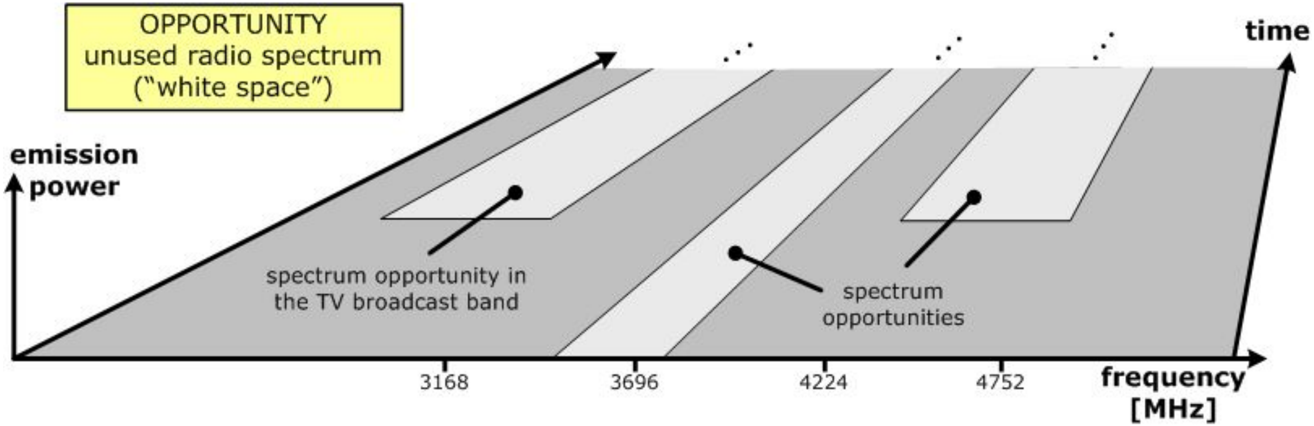
- Reasoner demonstrates truth of assertion Q based on existing premises
- By using this valid inference rule

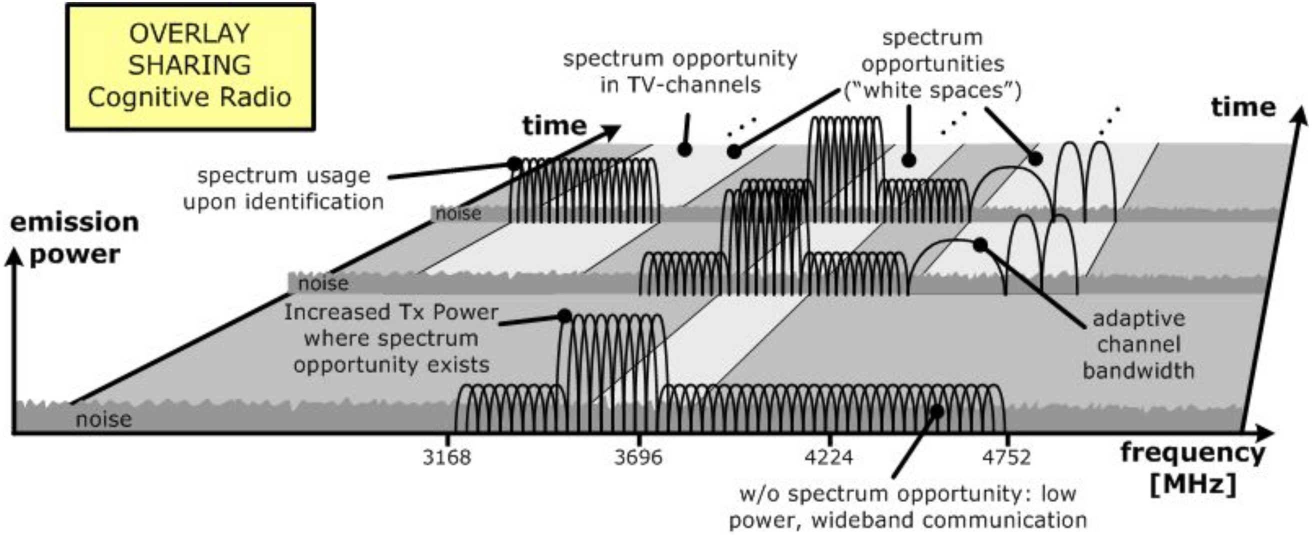
predicate P assigned to individual x:	$P(x)$
premises:	$\forall x, P(x) \rightarrow Q(x)$
	$P(y)$
conclusion:	$\vdash Q(y)$

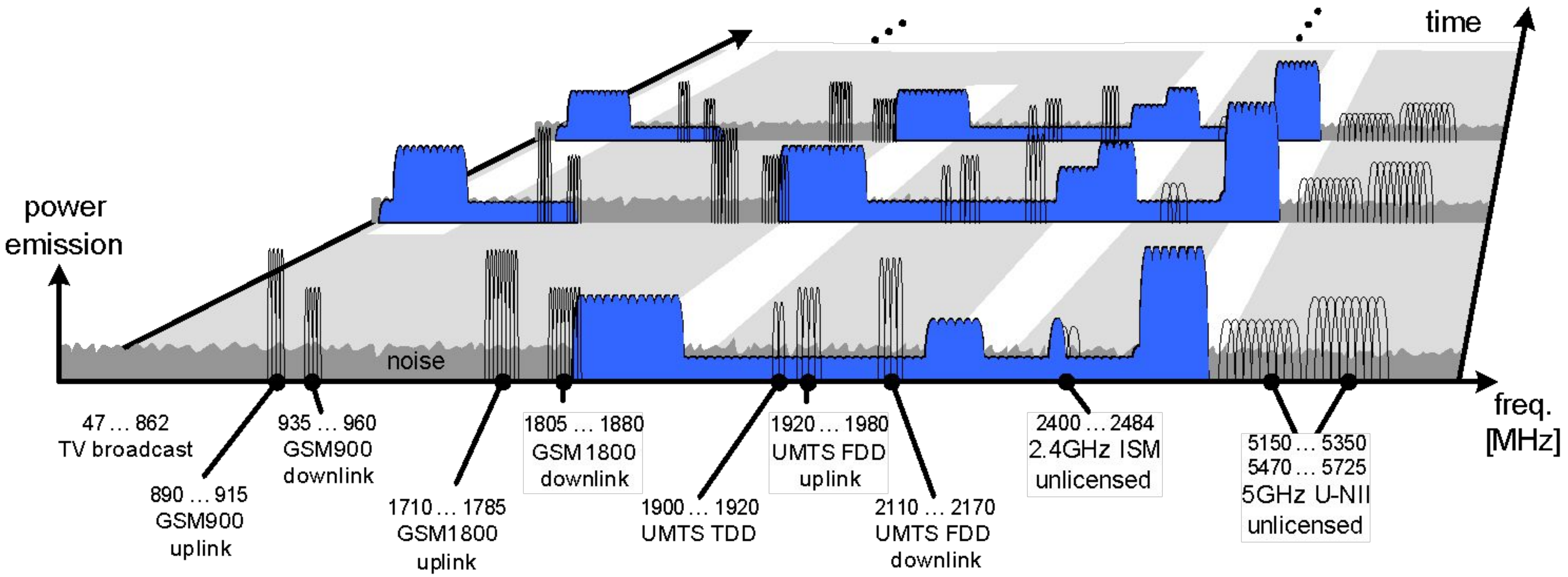
- As result, the cognitive radio judges Q as true and the related action will be executed

Spectrum Sharing




OPPORTUNITY
unused radio spectrum
("white space")
emission power
time
spectrum opportunity in the TV broadcast band
spectrum opportunities
3168
3696
4224
4752
frequency [MHz]


OVERLAY
SHARING
Cognitive Radio
emission power
time
spectrum opportunity in TV-channels
spectrum opportunities ("white spaces")
spectrum usage upon identification
noise
Increased Tx Power where spectrum opportunity exists
adaptive channel bandwidth
3168
3696
4224
4752
frequency [MHz]
w/o spectrum opportunity: low power, wideband communication



time
power
emission
noise
freq.
[MHz]
47 … 862
TV broadcast
890 … 915
GSM900
uplink
935 … 960
GSM900
downlink
1710 … 1785
GSM1800
uplink
1805 … 1880
GSM 1800
downlink
1900 … 1920
UMTS TDD
1920 … 1980
UMTS FDD
uplink
2110 … 2170
UMTS FDD
downlink
2400 … 2484
2.4GHz ISM
unlicensed
5150 … 5350
5470 … 5725
5GHz U-NII
unlicensed

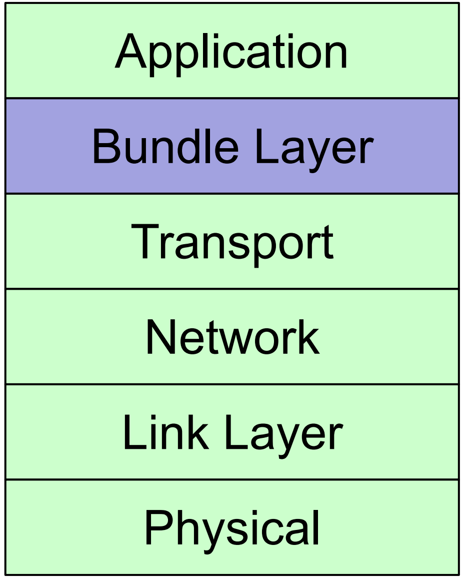
Delay Tolerant Networking

Delay Tolerant Networking, DTN

- The DTN idea originated from the Interplanetary Networking Special Interest Group (IPNSIG)
  - Deep space networks and spacecraft communications
- Use Cases in Wireless Communication Networks
  - Challenged Networks
  - Military Battlefield Networks
  - Mobile routers with intermittent connectivity
- Can tolerate delay/disruption/disconnection
- Date is traveling through the network by exploiting the mobility of devices

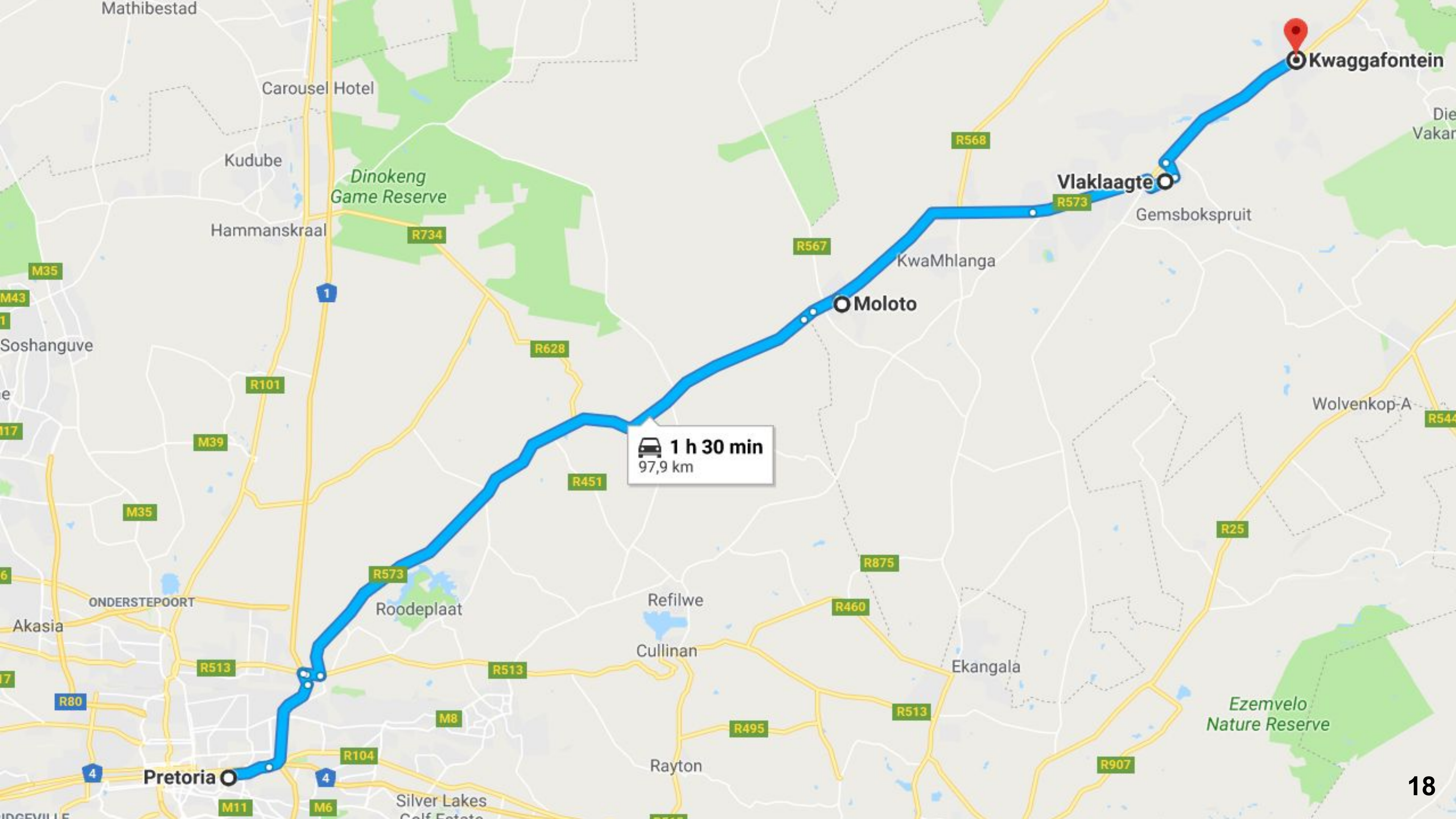
DTN Layer in the Protocol Stack

- Creates bundles (data units)
  - Open for different DTN routing schemes
  - Supports TCP and UDP convergence layer
- IETF Standards:
  - rfc 4838: Delay-Tolerant Network Architecture
  - rfc 5050: Bundle Protocol Specification
- A few disadvantages of DTN:
  - Very large delays
  - Unpredictable link error rates
  - Unpredictable network capacity (could be low with a small number of mobile devices, but also be very high with a large number of mobile devices)

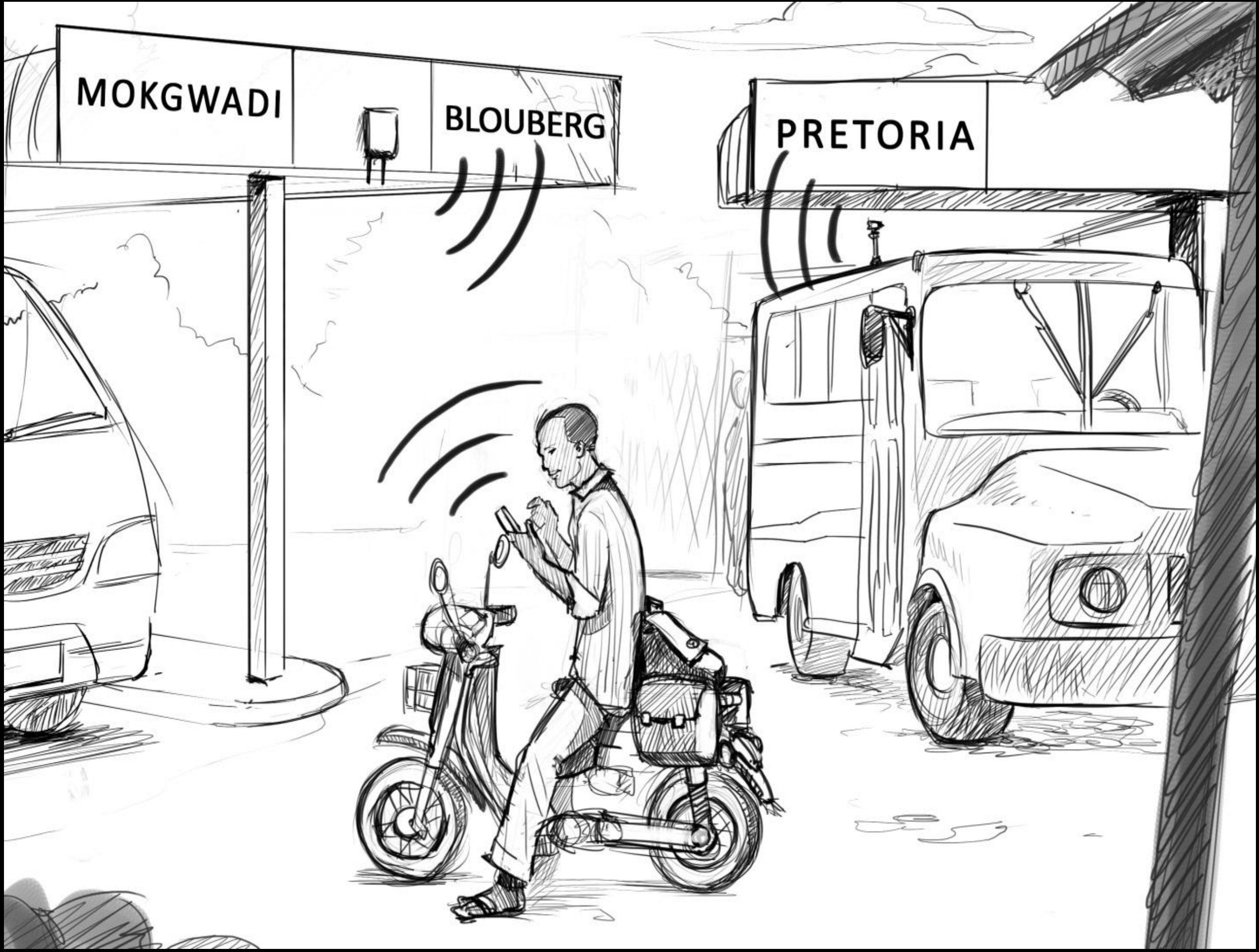


Test Case: From Pretoria to Rural South Africa

- Villages: Moloto, Vlaklaagte, Kwaggafontein


Mathibestad
Carousel Hotel
Kudube
Dinokeng Game Reserve
Hammanskraal
R734
M35
M43
Soshanguve
R628
R101
1
R568
R567
R573
Kwaggafontein
Vlaklaagte
Gemsbokspruit
KwaMhlanga
Moloto
1 h 30 min
97,9 km
M39
R451
M35
R573
Roodeplaat
ONDERSTEPOORT
Akasia
Refilwe
Cullinan
R513
R513
R80
Pretoria
4
4
R104
M8
R495
Rayton
M11
M6
Silver Lakes
R875
R460
Ekangala
R513
Wolvenkop-A
R25
R907
Ezemvelo Nature Reserve

Bus Stations


MOKGWADI
BLOUBERG
PRETORIA

Wireless Networking and Mobile Computing

6. Visible Light Communication

Stefan Mangold

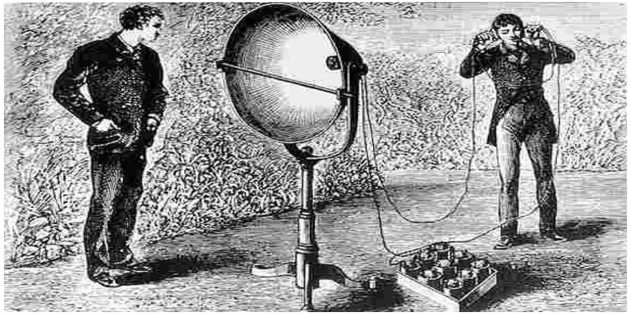
Course Outline

1. Introduction
2. Wireless Communication Basics
3. IEEE 802.11 Wireless LAN (Wi-Fi)
4. IEEE 802.15 Wireless PAN (ZigBee & Bluetooth)
5. Mobile Computing Algorithm Basics: Control and Game Theory
6. Visible Light Communication
7. Audio Communication
8. Cellular Networking Basics (LTE, 5G, Internet-of-Things)
9. Mobile Computing for Automated Medicine Delivery
10. Cognitive Radio, Delay Tolerant Networking, Radio Spectrum Sharing

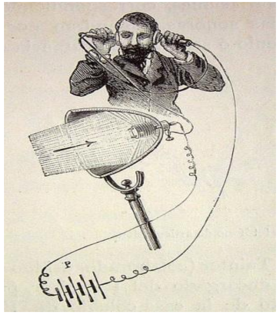
VLC History - Photophone

Source: Wikipedia

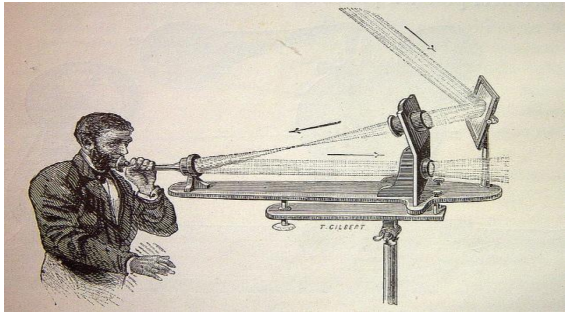
- First dated application of VLC
- Invented by Alexander Graham Bell, 1880
- World’s first wireless telephone message
- transmitted over >200 meters, using modulated sunlight



Bell’s receiver, a parabolic mirror collecting the light which is later interpreted by a photoresistor.



Schematic of the receiver.



The transmitter is collecting sunlight and projecting it on a mirror which modulates the light. (Focusing or dispersing of the light beam)

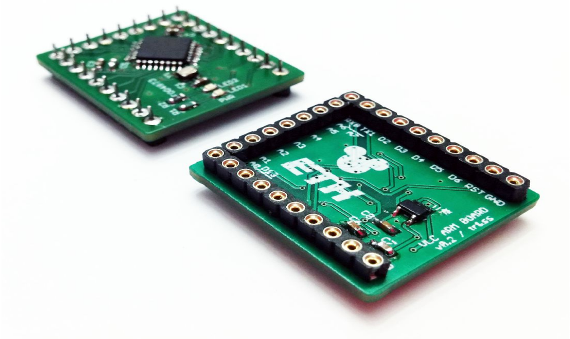
Why Visible Light?

- The visible light spectrum is a broad (400 THz) and **unlicensed** spectrum
- Visible light is **not perceived as** radio wave, or harmful
- LEDs are **already embedded** in many consumer electronics devices, and (of course) in lights
- **Underwater communication** works best with visible light
- VLC is considered for next generation cellular (“6G”) standards, and for future Wi-Fi generations (“Li-Fi”)

LEDs as Receivers

- Any photodiode is an LED, specialized in light reception
- LEDs can be used as light receivers, like photodiodes, but with less sensitivity
  - P. Dietz, W. Yerazunis, and D. Leigh: "Very low-cost sensing and communication using bidirectional LEDs," UbiComp 2003.
  - Photons create an electric current that is proportional to the intensity of the incoming light
  - This approach reduces the complexity of a device
- Only one single LED is required to transmit and receive data
  - Protocol to control the LED is required
  - Tradeoff: low sensitivity, shorter distances, low data rates

Low-Cost Software-Defined VLC

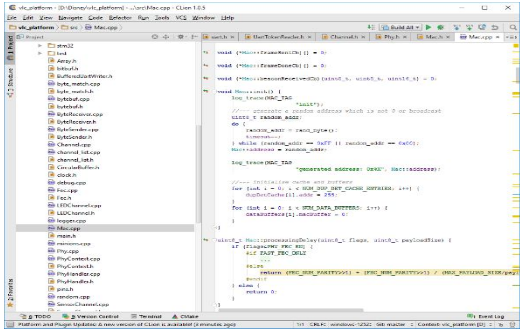


Microcontroller

+

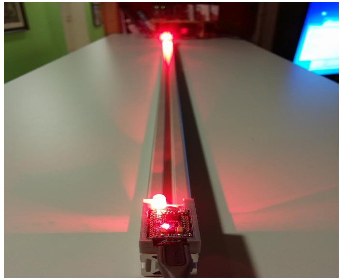
Sender/Receiver

+



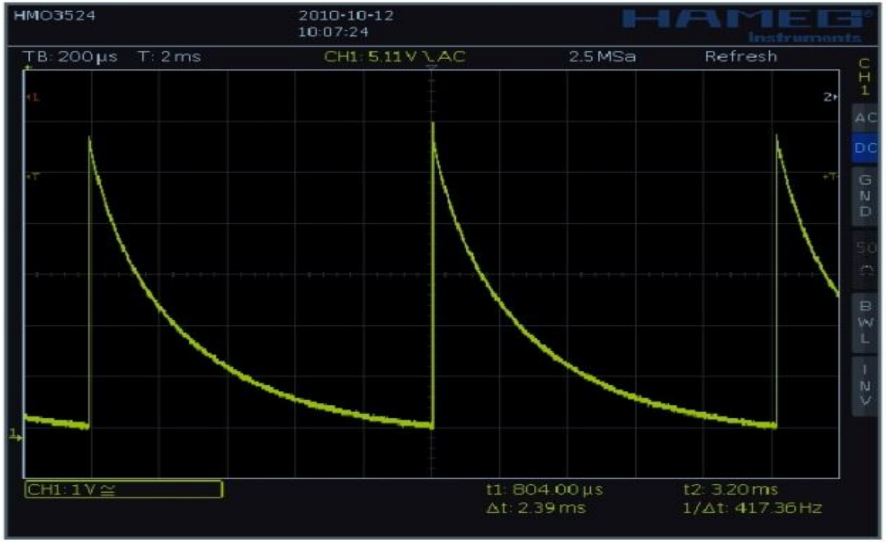
Embedded Software

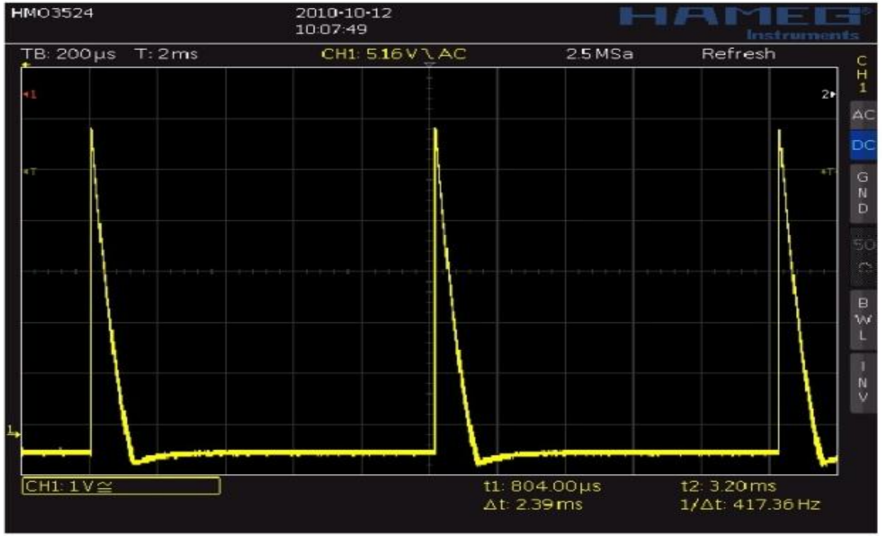
=



VLC communication link:
1 kb/s over 2 meters

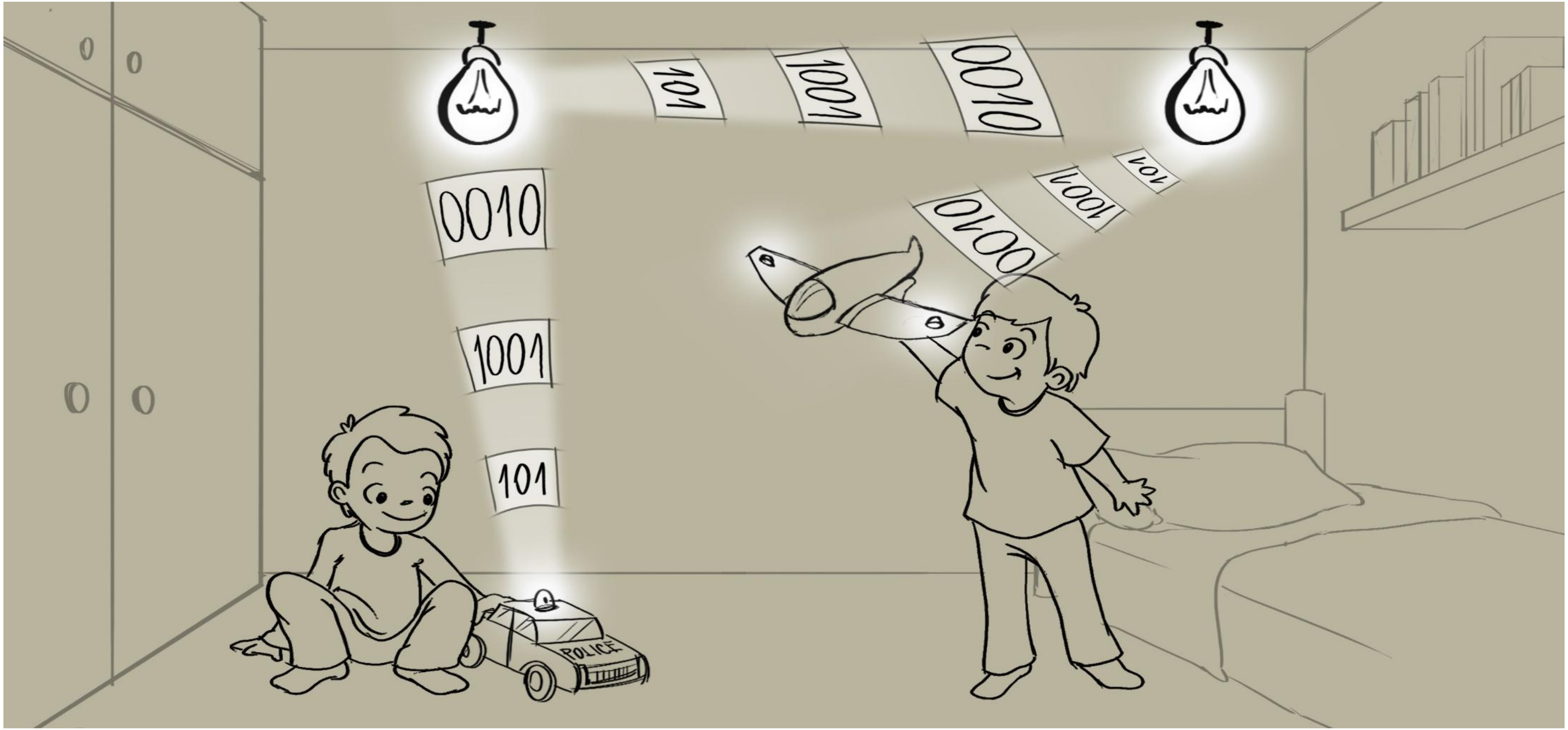
Light Sensing with LEDs



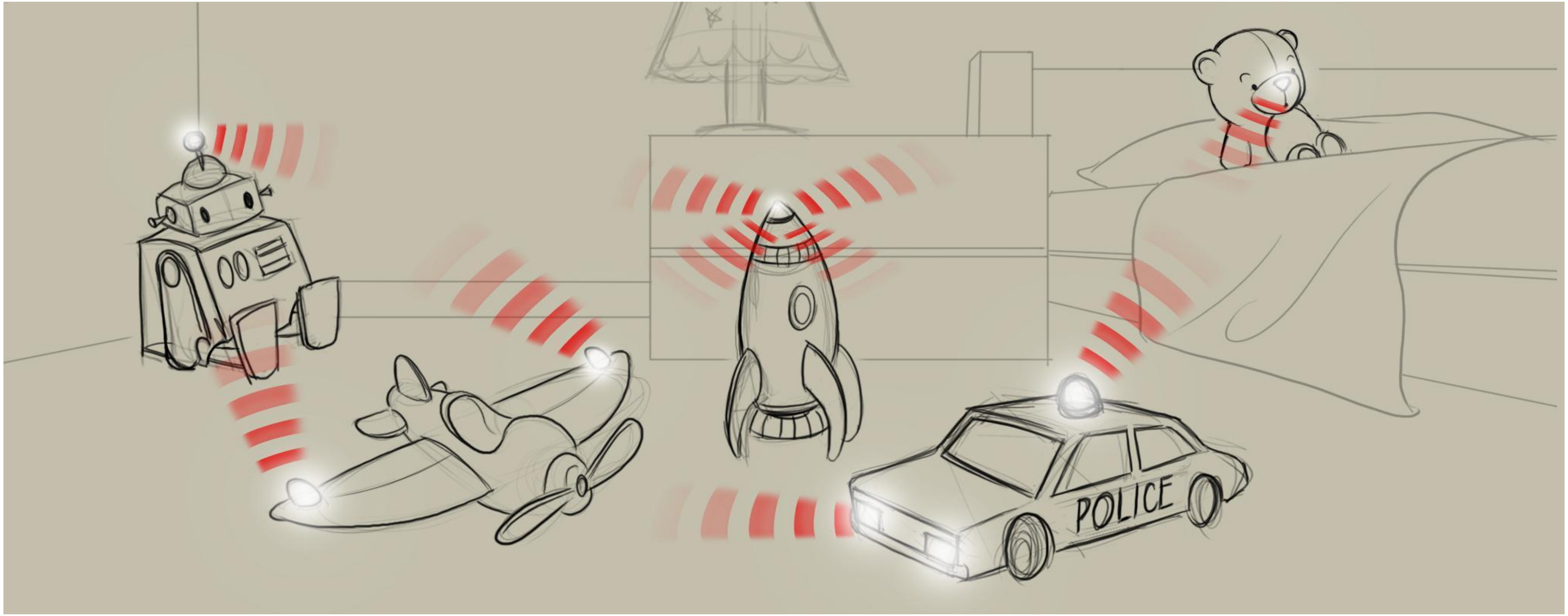


Applications

Home Networks

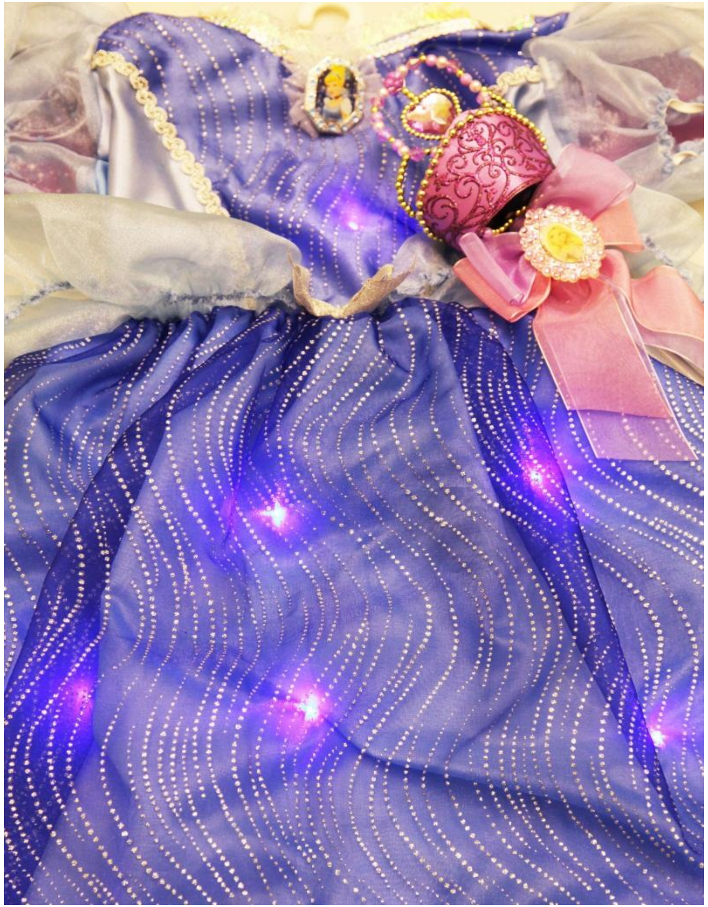


Toy Networks



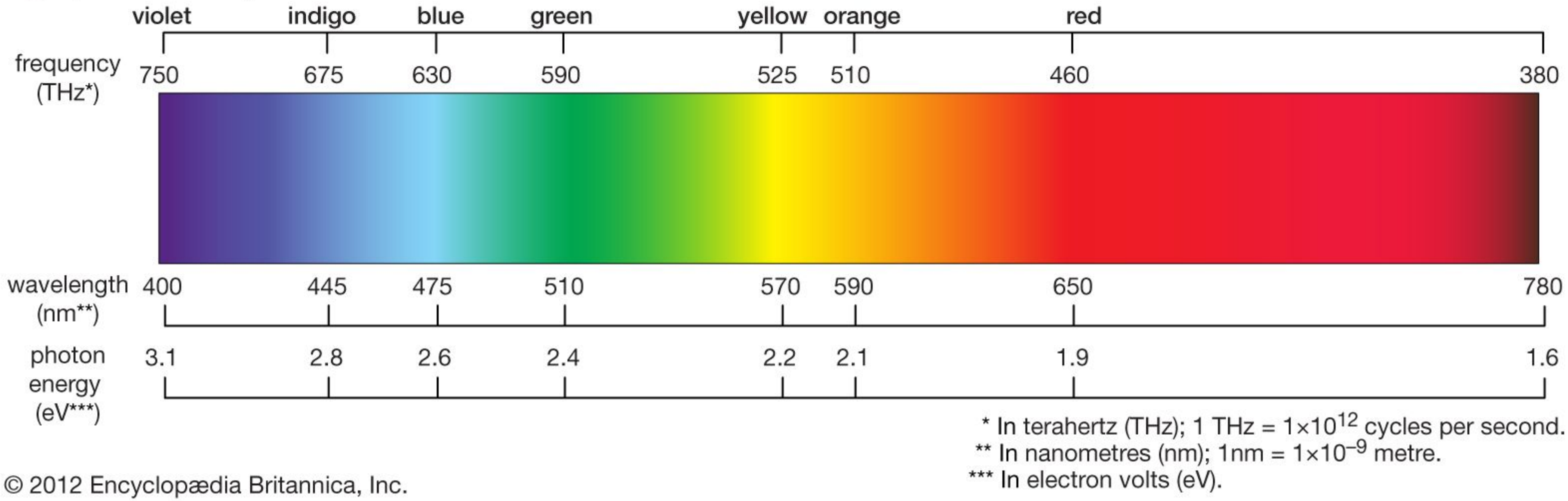
Toys

Fashion and Fabrics - Princess Dress



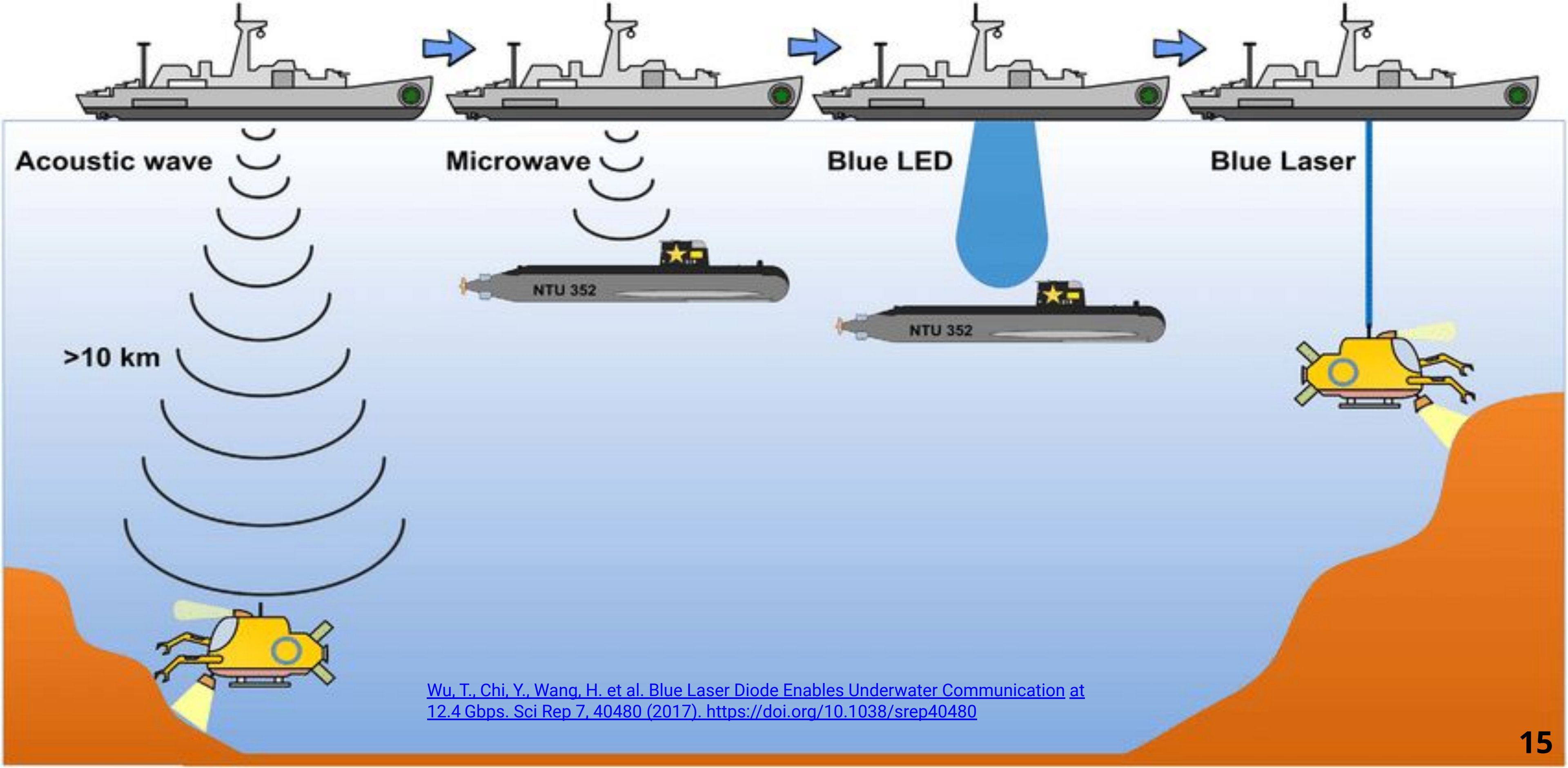
VLC-enabled Toys

Visible Light Spectrum



https://www.britannica.com/science/light

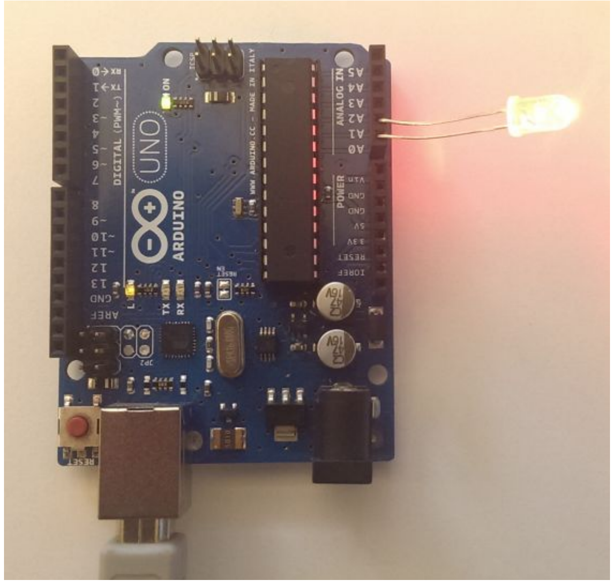
Underwater Communication



Wu, T., Chi, Y., Wang, H. et al. Blue Laser Diode Enables Underwater Communication at 12.4 Gbps. Sci Rep 7, 40480 (2017). https://doi.org/10.1038/srep40480

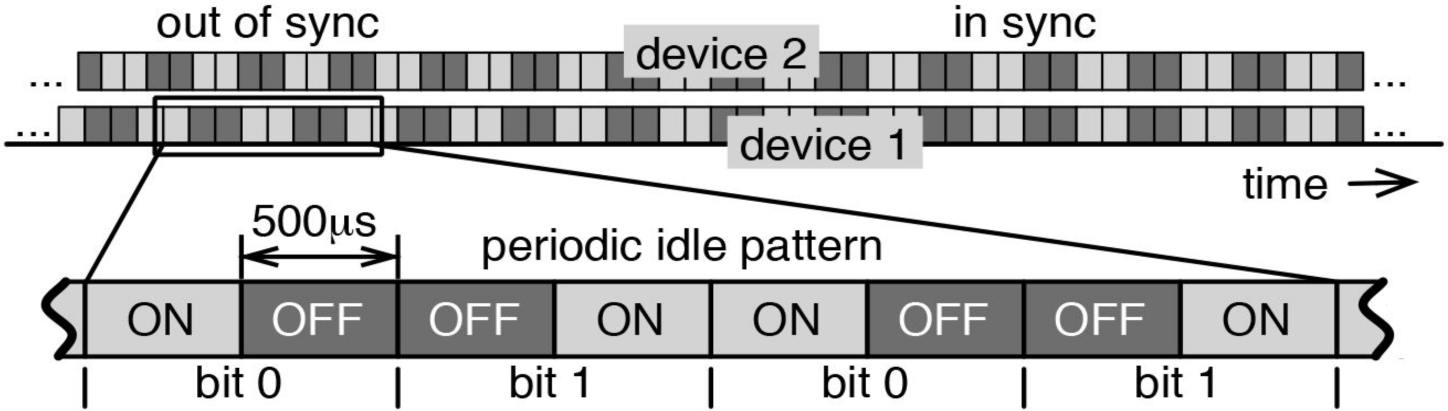
Software-Defined PHY-Layer

- Responsible for:
  - Frame delivery over free-space optical medium
  - Synchronization
  - Medium idle/busy sensing
- Hardware parts:
  - Low-cost 8-bit microcontroller (µC)
  - Standard LED
  - PHY-layer is part of the µC’s firmware
- LED is used to sense/emit light (directly connected to µC)



Idle Mode

- LED appears to be always on
  - Required for all communication modes (idle, receiving, transmitting)
  - Necessary to provide constant brightness (illumination, toys)
- Periodic idle pattern

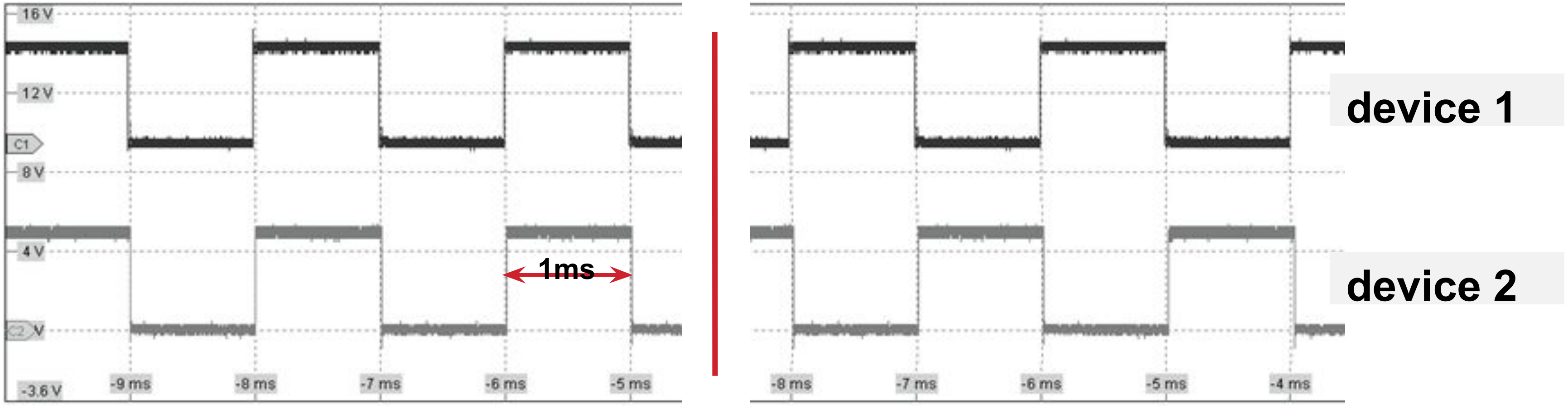


ON: emit light, OFF: sense light

Synchronization During Idle Mode

- Communication requires synchronization
  - Devices have to synchronize to idle pattern, continuously
  - Synchronize so that OFF-slots are aligned
- Enables CSMA/CA MAC protocol

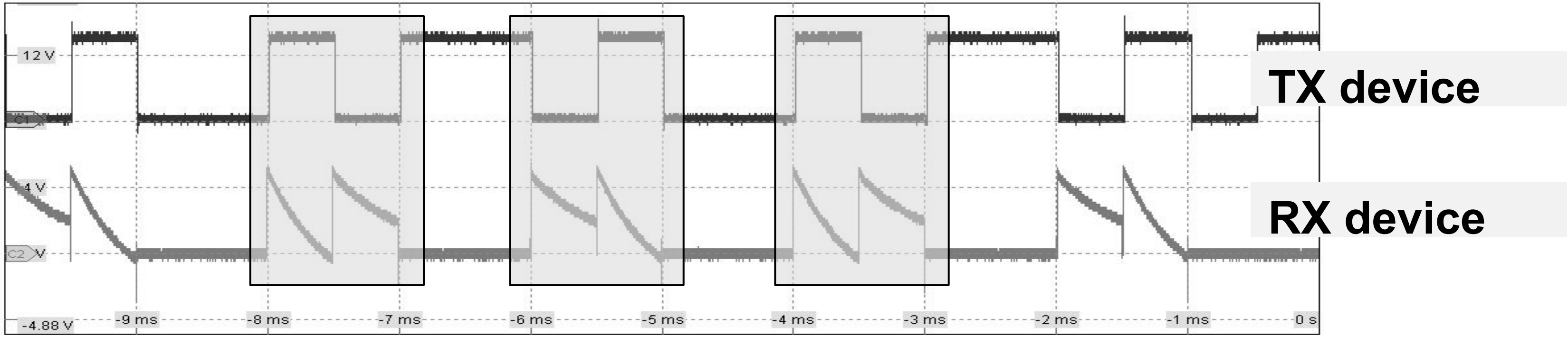
in-sync: aligned OFF-slots **out of sync: OFF aligned with ON slots**



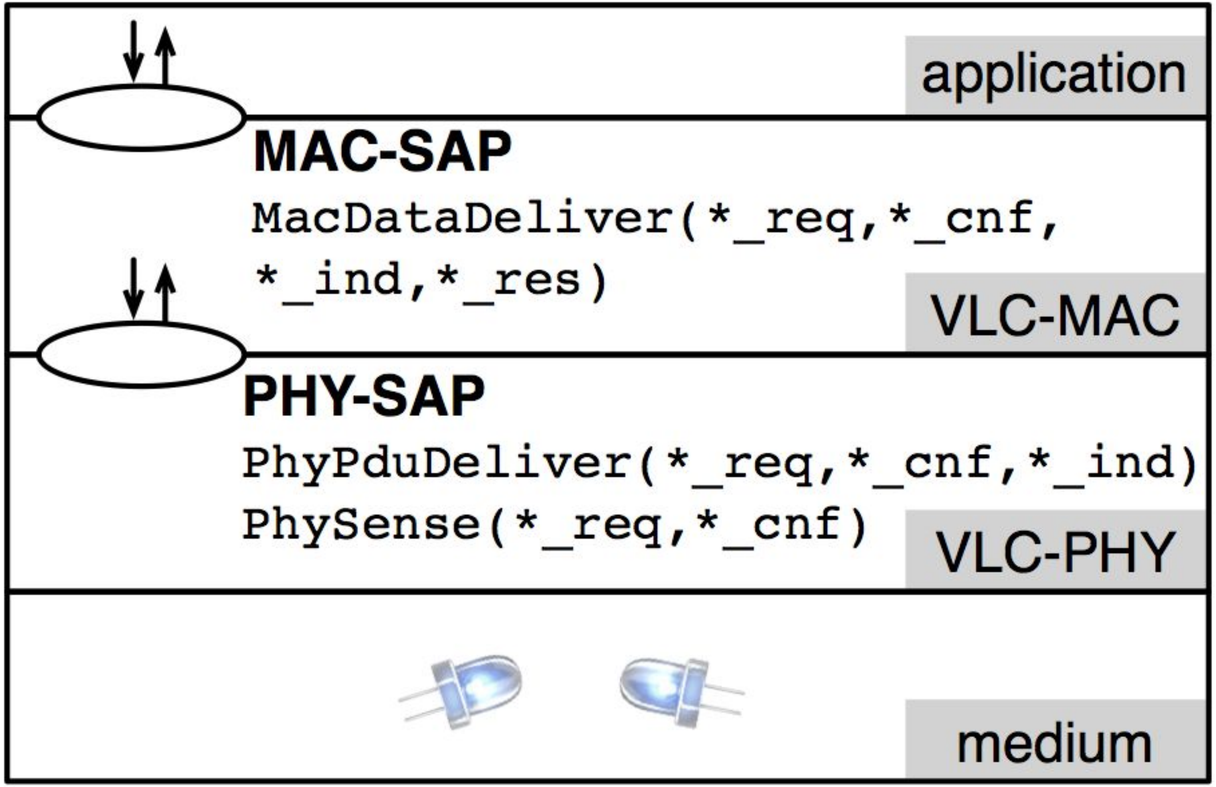
Transmitting (TX) / Receiving (RX) Mode

bit	first symbol	second symbol
0	ON	OFF
1	OFF	ON

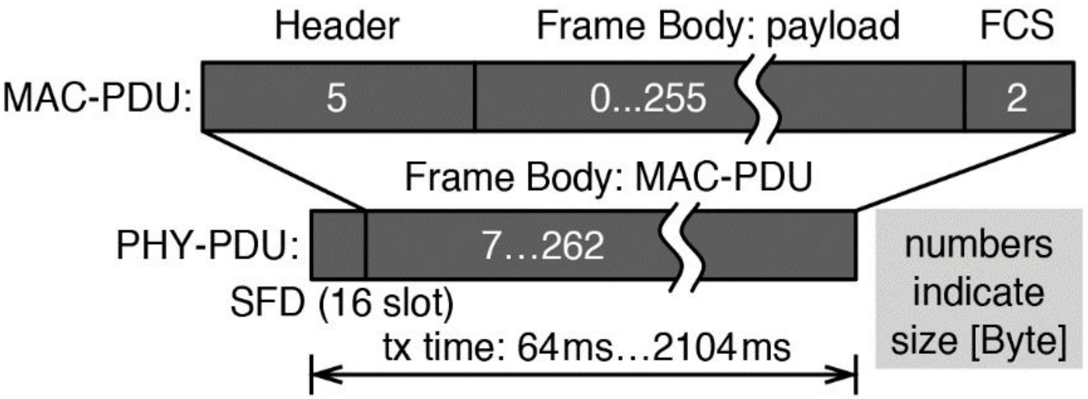
- TX mode:
  - 2-pulse position modulation (2-PPM)
  - Same number of ON and OFF slots during transmission
- RX mode:
  - Reverse-biased LED, measuring cathode voltage with a microcontroller‘s Analog-to-Digital Converter (ADC), at the end of the slot



VLC Reference Model



MAC Protocol Data Unit



MAC- and PHY-PDU definition

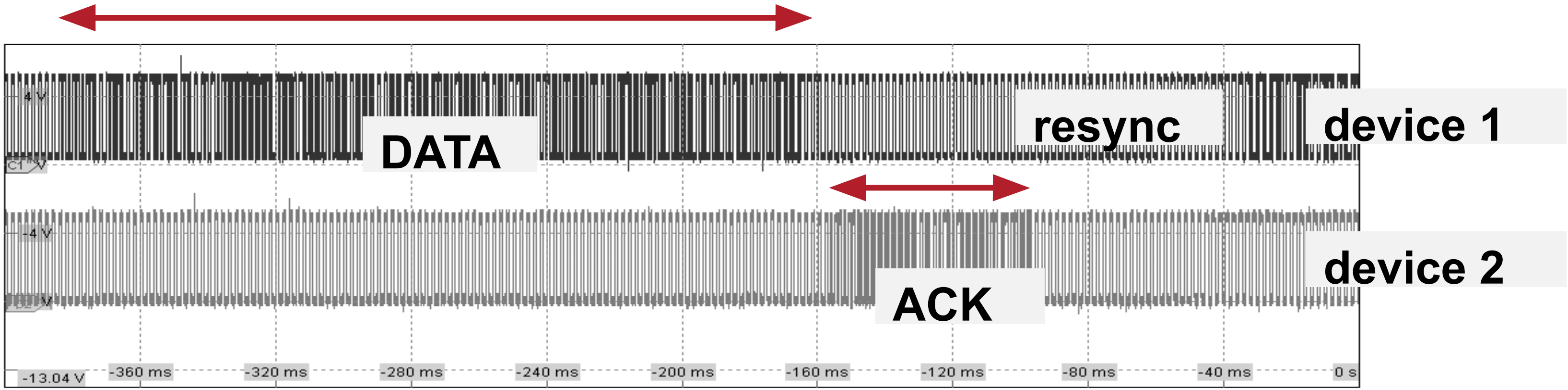
Element	Bytes (Slots)
Header	5 (80)
Body (DATA)	0-255 (0-4080)
Body (ACK)	0 (0)
FCS	2 (32)

Element	Bytes (Slots)
Body size	1 (16)
Control	1 (16)
Destination	1 (16)
Source	1 (16)
Sequence	1 (16)

MAC frame structure

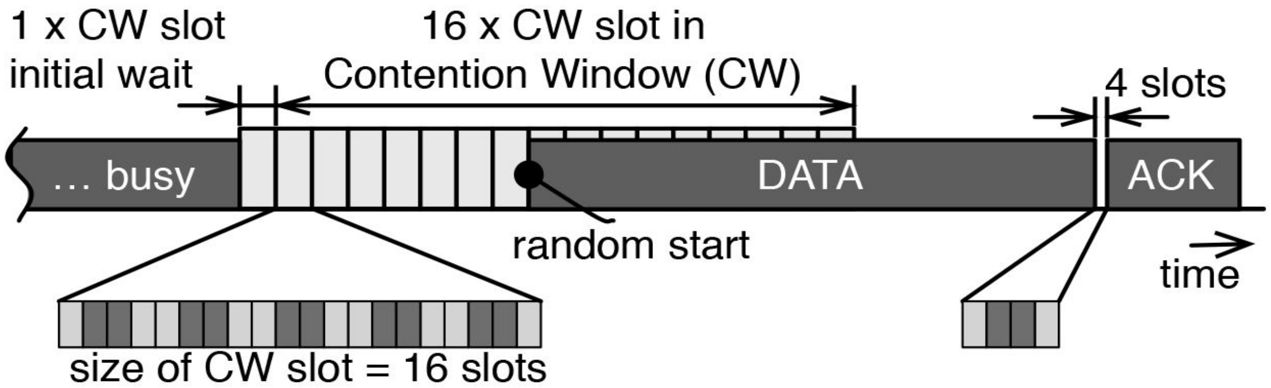
DATA/ACK Frame Exchange

- Device 1 sends a DATA frame to device 2
- Device 2 replies with an ACK (if FCS correct)
- Device 1 continues with the next DATA frame (if available)
- Resynchronizing in IDLE mode between DATA frames



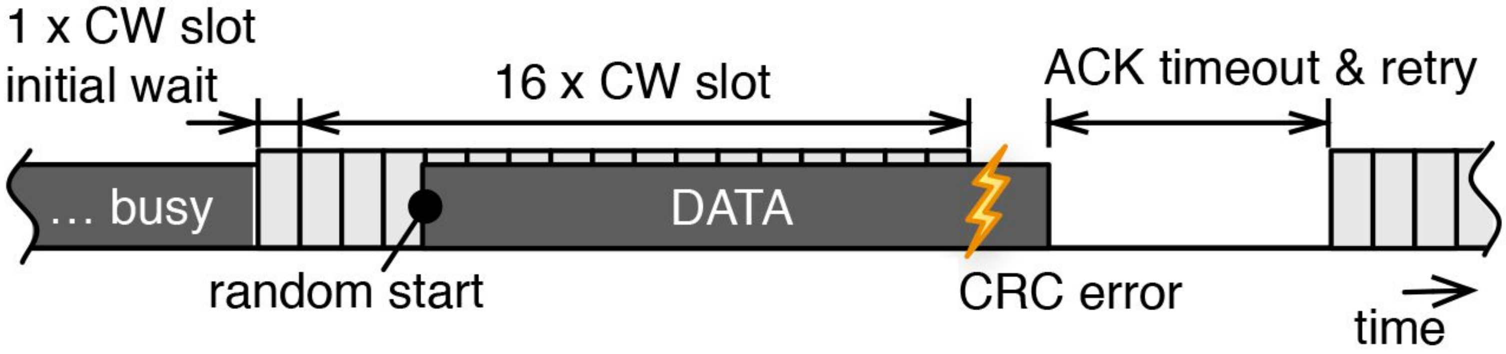
CSMA / CA Medium Access

- ACK has priority, minimum contention windows: 1 CW slot
  - Packet transmission starts after random number of CW slots
- When SFD is successfully decoded (preamble detection):
  - Switch to RX mode, prohibit switching to TX mode
- When no frame is decoded, or an SFD is missed:
  - No or small variation in recent measurements → idle channel (else: busy)



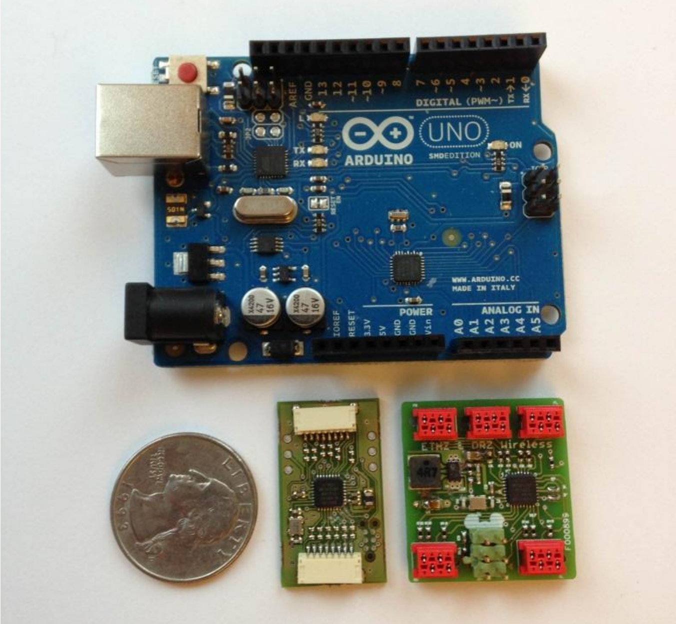
Retransmissions

- On collision or bad reception: CRC error
- Receiver: No ACK is generated
- Transmitter: Retransmit frame after ACK timeout



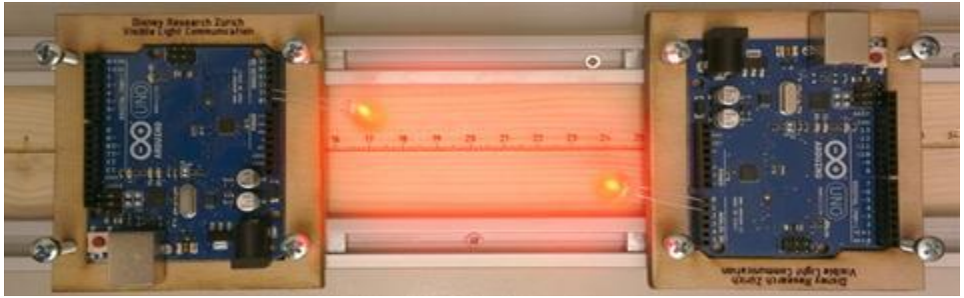
Microcontroller Testbed

- Various Arduino boards for prototyping
- ATmega 328P microcontroller
- 8 bit, 32K program storage
- 2K RAM
- 8 ADC pins (multiplexed)



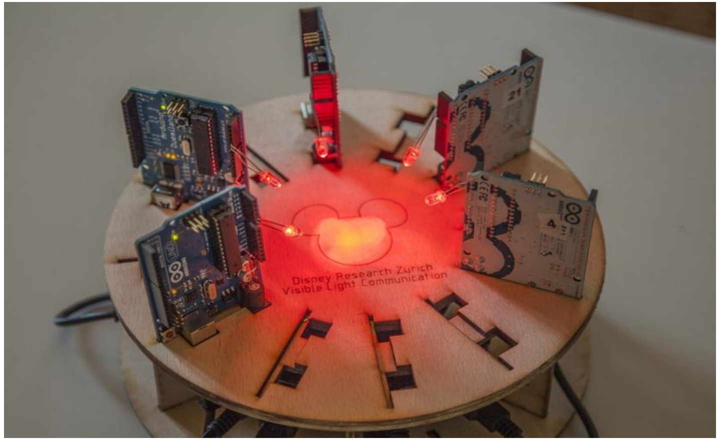
Testbed

- ATmega328P evaluation boards (Arduino)
- 5mm red LED (640 nm, 20°, 12000 mcd)

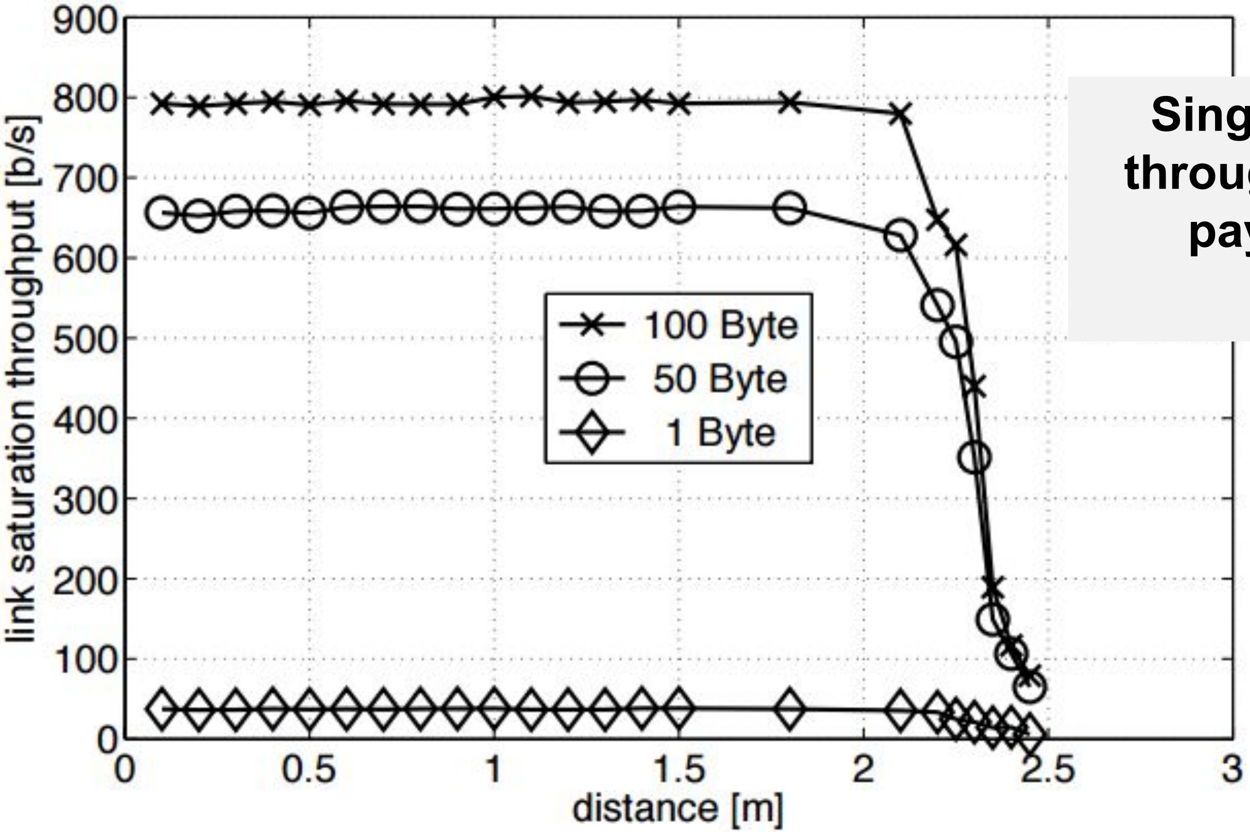


Network measurements testbed with boards and LEDs

Distance measurements testbed with boards and LEDs



Single Link Throughput (I)

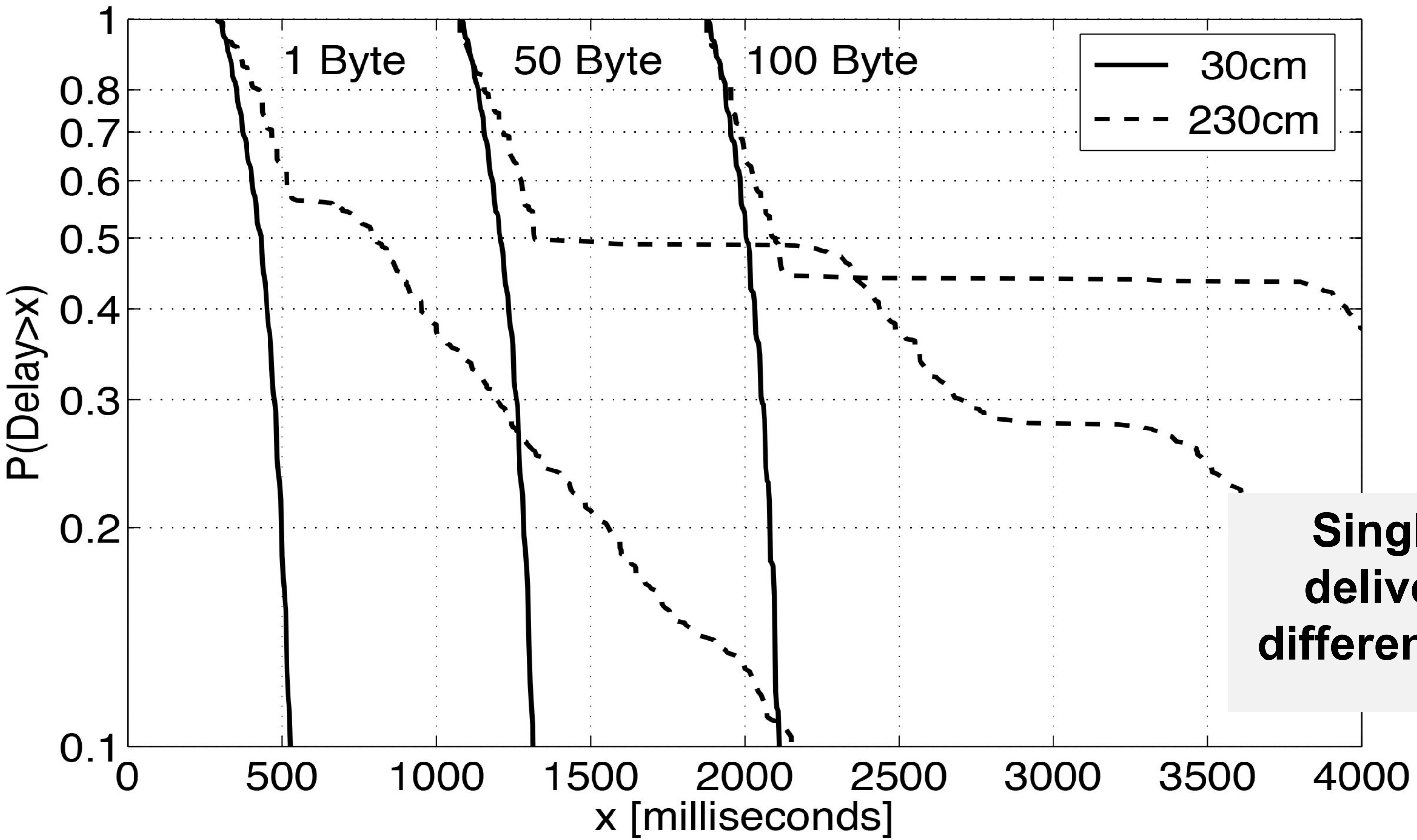


Single link saturation throughput for different payload sizes and distances

Single Link Throughput (II)

- Distance <= 2 m: Constant throughput for all packet sizes
- Distance > 2 m: Throughput collapses because of increased error probability due to bad reception
- Achieved maximum throughput: 800 b/s (bit per second) for 100 B (100 Byte) packets

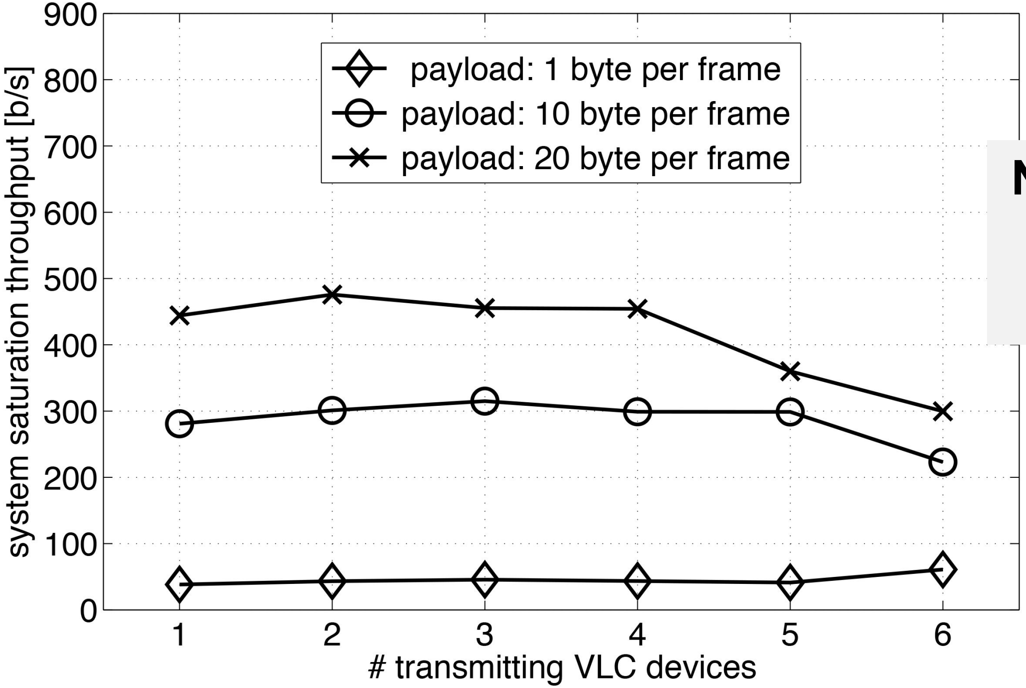
Single Link Delays (I)



Single link packet delivery delays for different payload sizes

Network Throughput (I)

- N devices transmit data to a sink and compete for the medium
- All devices can see each other (no hidden stations)

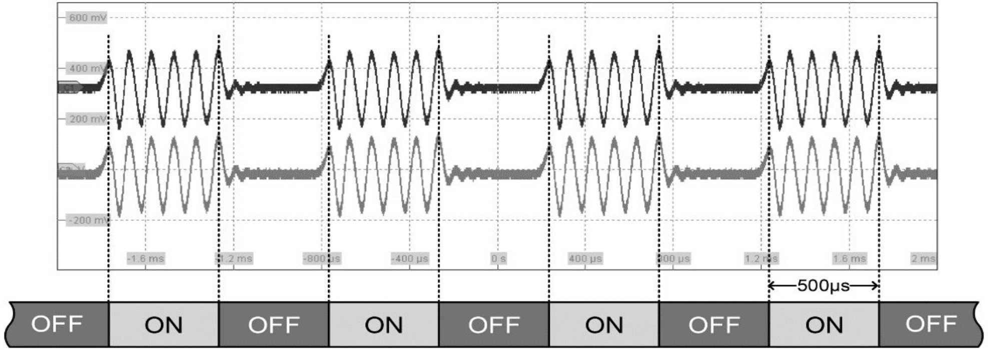


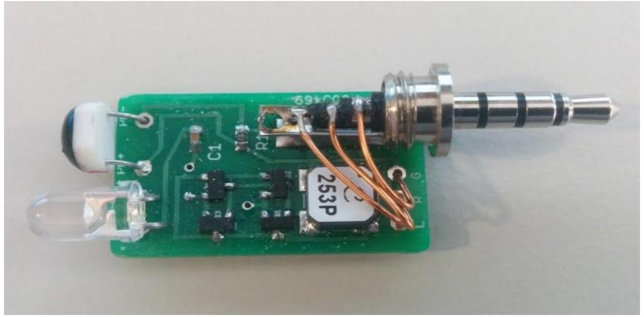
Network throughput for 1 to 6 transmitting devices and different payload sizes

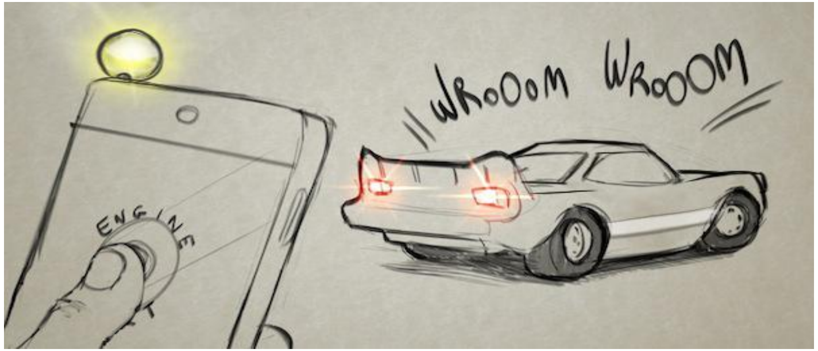
Network Throughput (II)

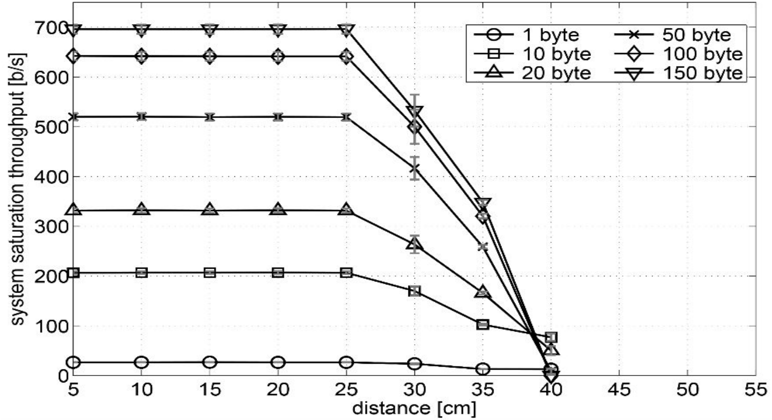
- Smaller packet sizes due to increased error probability
- Less than five transmitting devices: Constant throughput, medium access handled sufficiently by MAC protocol
- More than five transmitting devices: Reduced throughput because of retransmissions due to less stable synchronization
- Network throughput: 500 b/s (bit per second)

From Sound to Sight









Video: VLC Toys

Student Project (Carl Friess)

- I really liked the VLC assignment from your Wireless Networking class. It's a fun and interesting way of communicating. I wanted to know more about how to implement the firmware used in the assignment and decided to try to implement a more basic version myself.
- I thought it could also be interesting to try to use a phone screen to transmit data. This way any toy or gadget with some LED that doesn't have any other means of communication could still be connected to a smartphone (at least uni-directionally) without extra hardware.
- The firmware I came up with isn't nearly as nice as the firmware you provided but it actually works reasonably well. There is a small web app you can open on a computer or a phone that flashes the screen to send messages. The Arduino firmware receives the data and prints it to serial.
- I uploaded the code and a short demo here: https://github.com/carlfriess/LED_Receiver
- There's still a lot of room for improvement: The data rate is very low (~2B/s). I found the timing of the transmitter was very difficult to do accurately in the browser, so this is a big limiting factor. I think by implementing a native app this could be improved up to the refresh rate of the display. Furthermore, the data is encoded using a very basic scheme compared to the firmware you provided and there is no real MAC layer.
- Thought you might find this interesting.

Wireless Networking and Mobile Computing

7. Audio Communication

Stefan Mangold

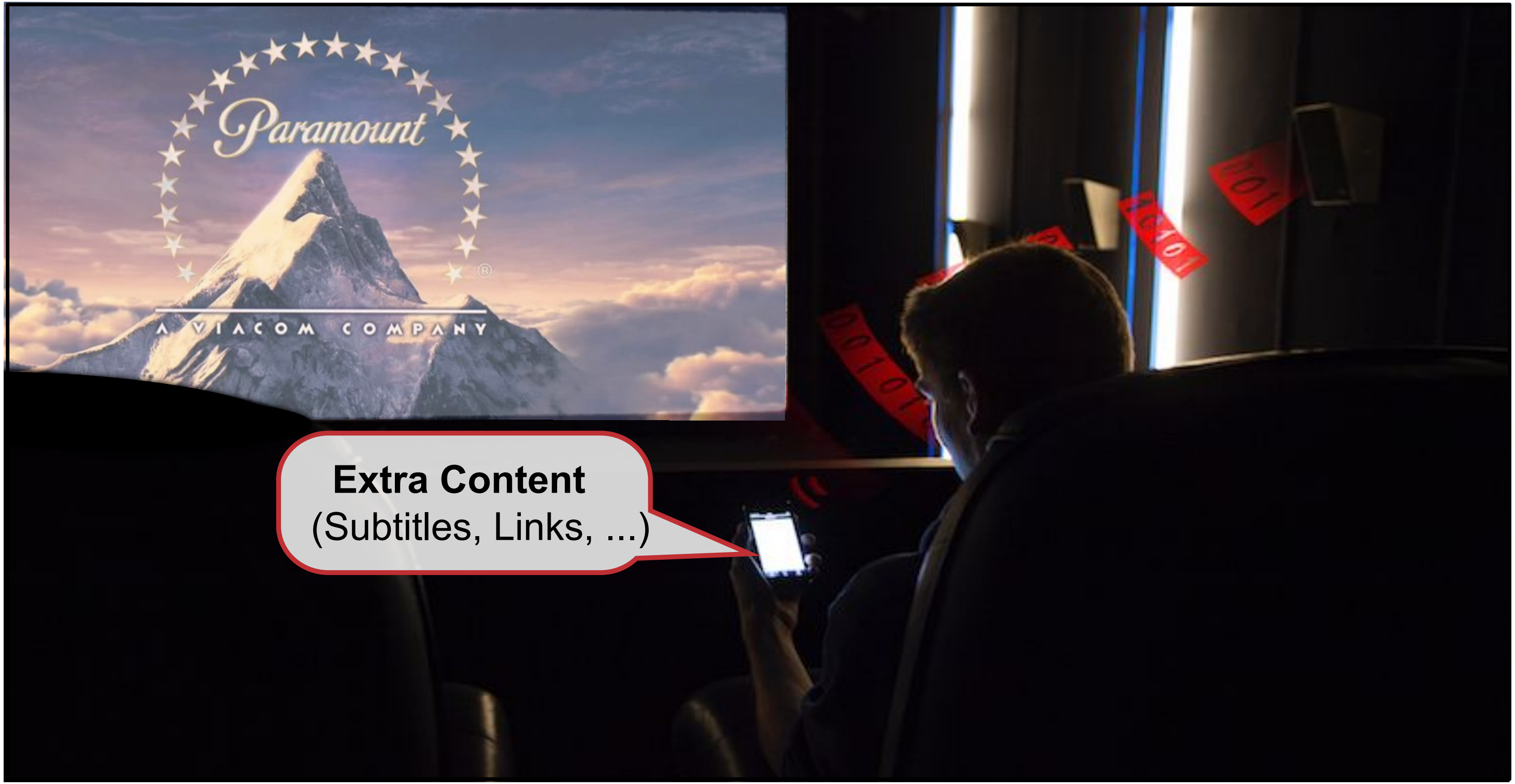
Course Outline

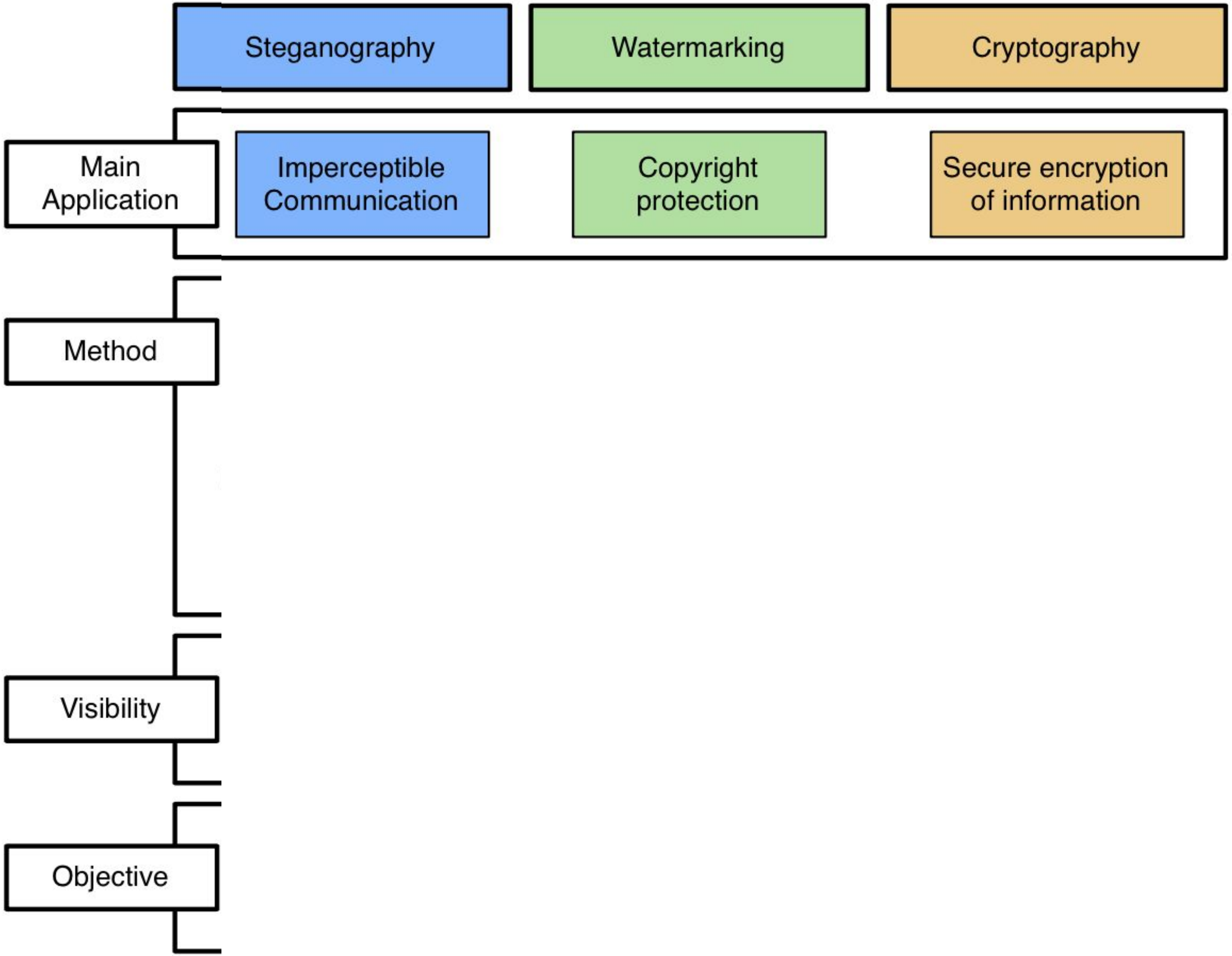
1. Introduction
2. Wireless Communication Basics
3. IEEE 802.11 Wireless LAN (Wi-Fi)
4. IEEE 802.15 Wireless PAN (ZigBee & Bluetooth)
5. Mobile Computing Algorithm Basics: Control and Game Theory
6. Visible Light Communication
7. Audio Communication
8. Cellular Networking Basics (LTE, 5G, Internet-of-Things)
9. Mobile Computing for Automated Medicine Delivery
10. Cognitive Radio, Delay Tolerant Networking, Radio Spectrum Sharing

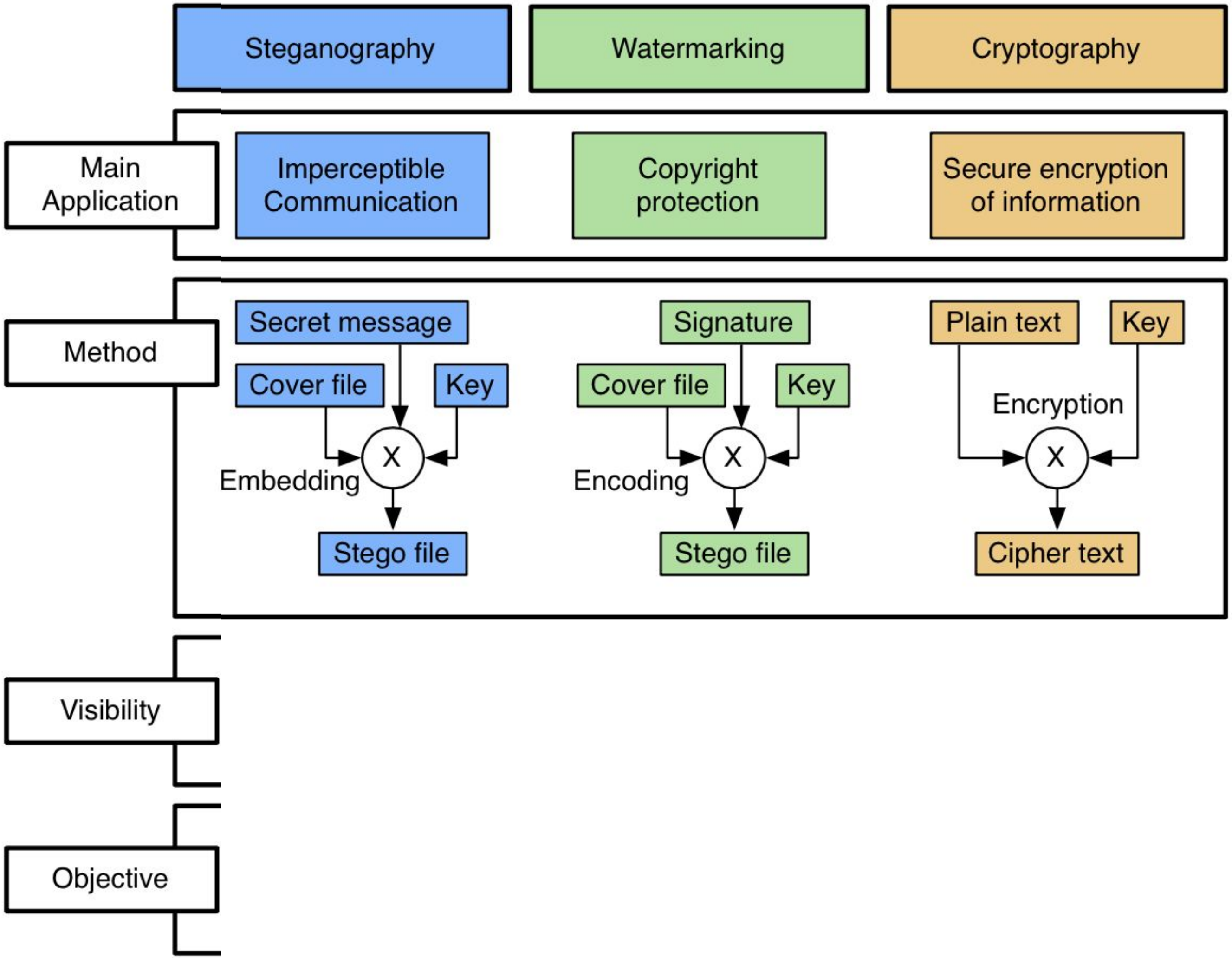
Remarks

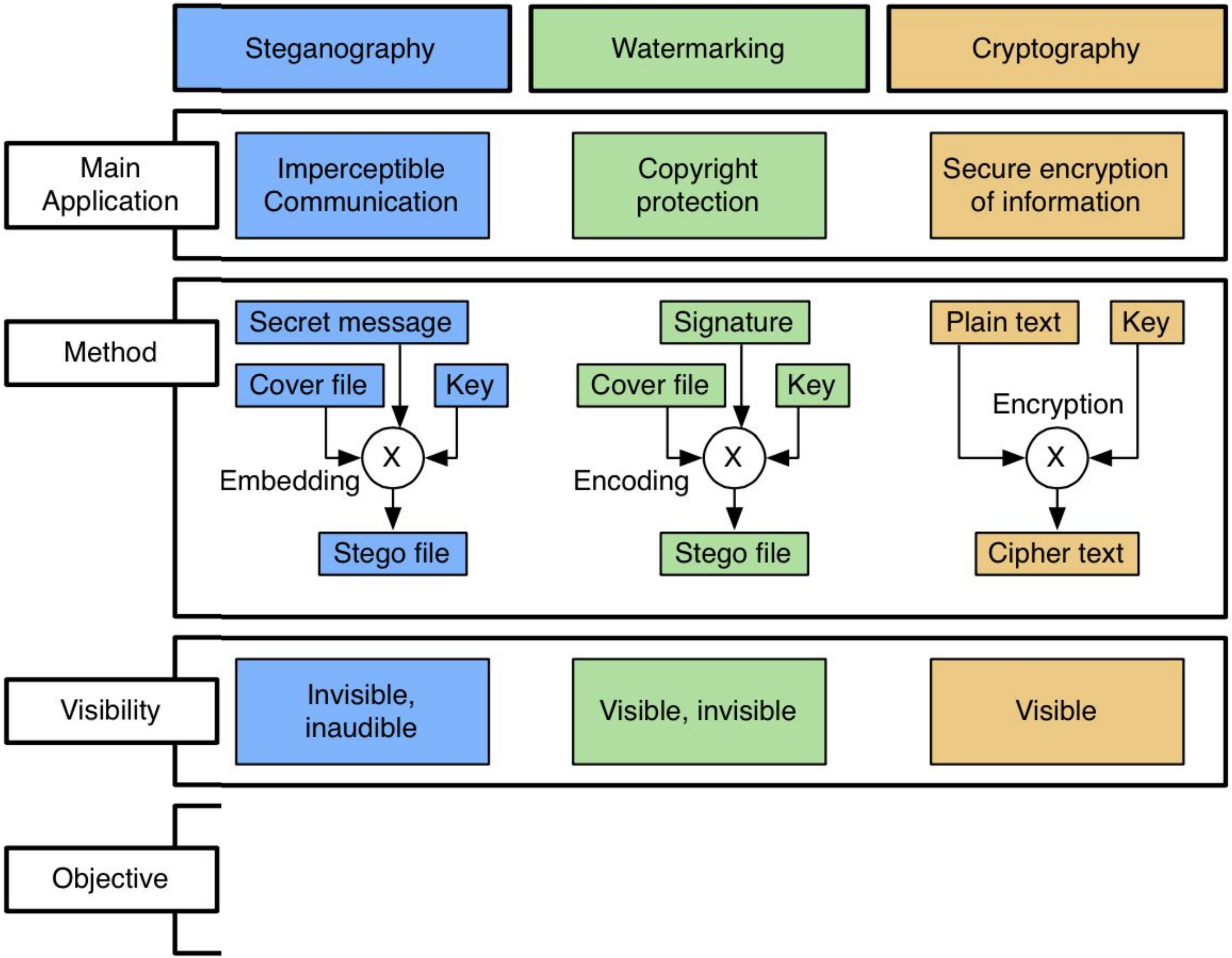
- Audio signals are not electromagnetic signals, and are therefore not radio signals.
- Common audio signals have a bandwidth, which is measured in Hertz (Hz).
- A human voice communicates between 100 and 1’000 Hz.
- The human audible frequency range extends up to ∼15’000 Hz, and up to ∼20’000 Hz for younger adults and children.
- Elephants can communicate at low frequencies, at ∼1 … 20 Hz, and over a couple of kilometers.

2nd Screen Application

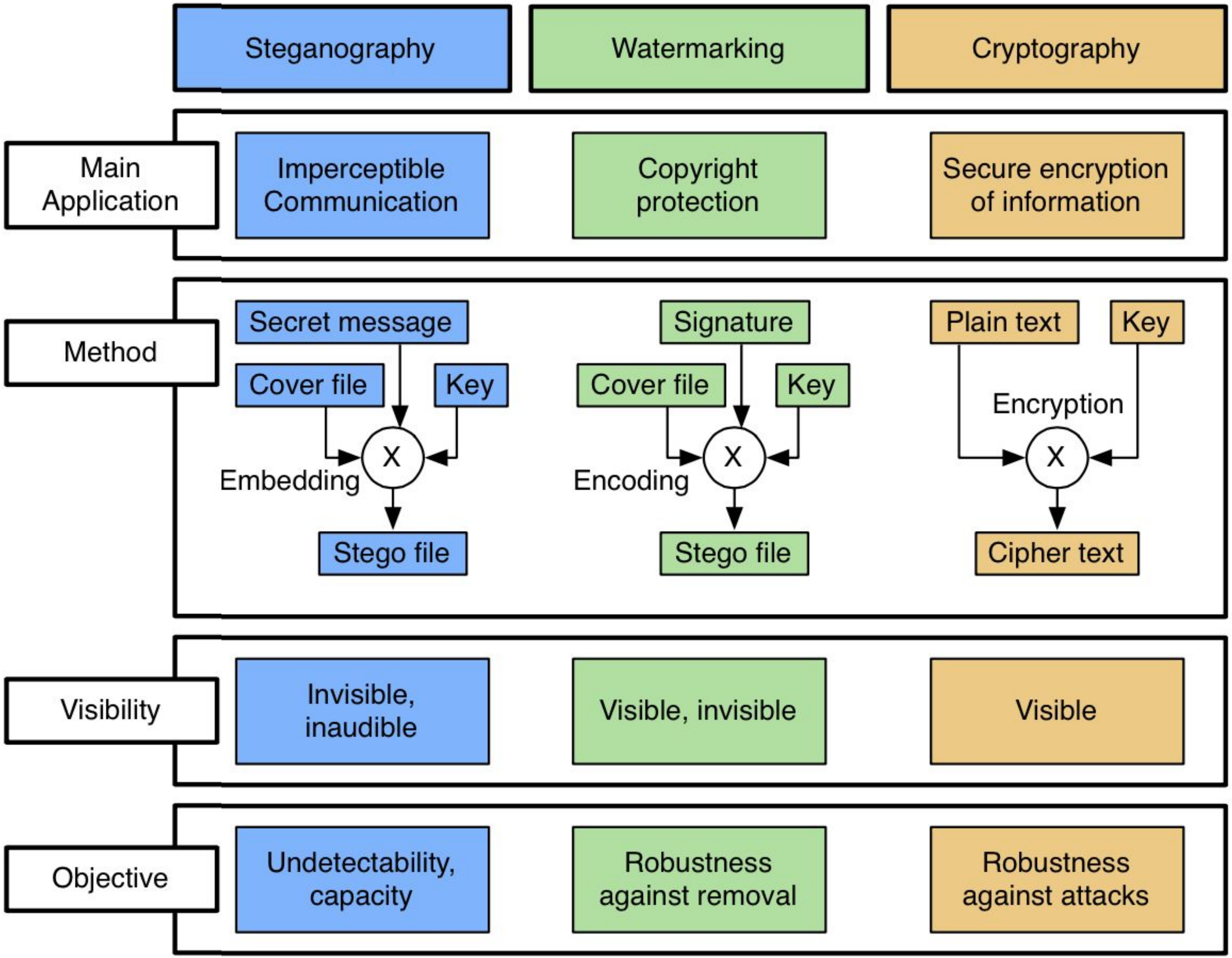



Steganography
Watermarking
Cryptography
Main Application
Imperceptible Communication
Copyright protection
Secure encryption of information
Method
Visibility
Objective


Steganography
Watermarking
Cryptography
Main Application
Imperceptible Communication
Copyright protection
Secure encryption of information
Method
Secret message
Cover file
Key
X
Embedding
Stego file
Signature
Cover file
Key
X
Encoding
Stego file
Plain text
Key
Encryption
X
Cipher text
Visibility
Objective

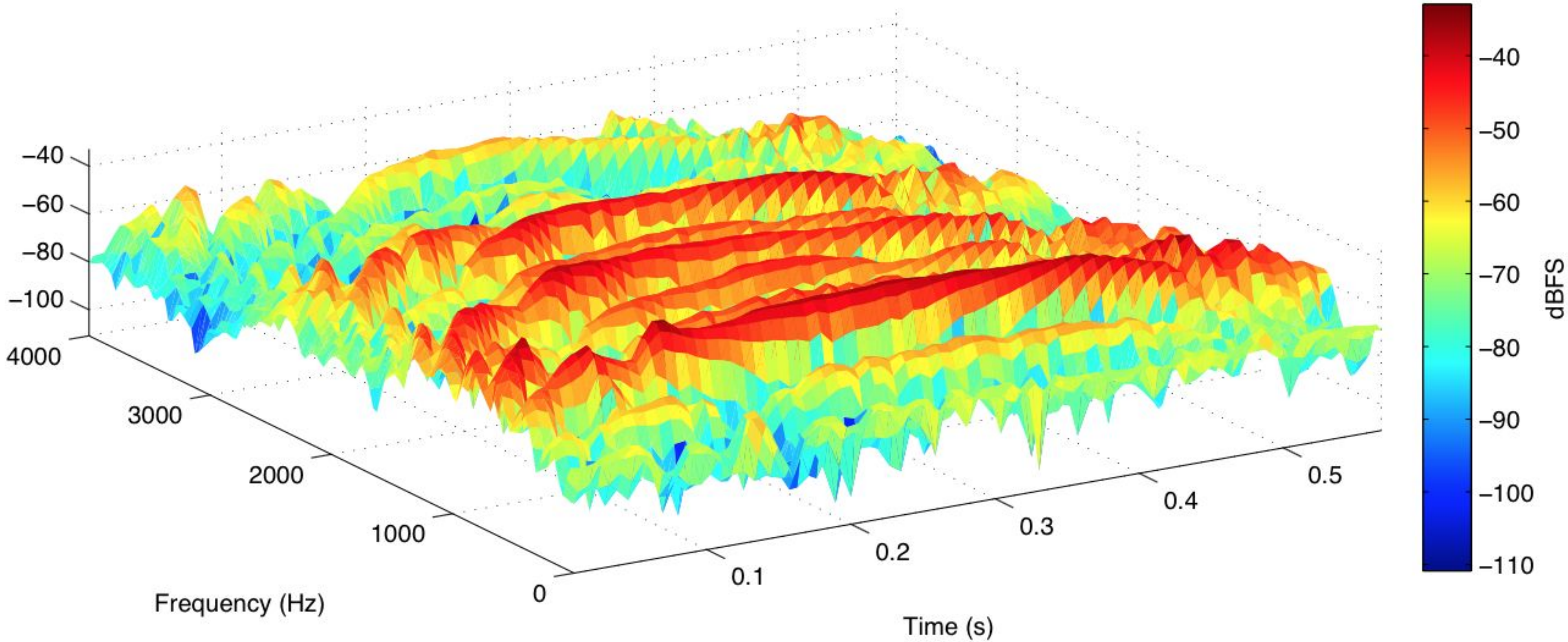


Steganography
Watermarking
Cryptography
Main Application
Imperceptible Communication
Copyright protection
Secure encryption of information
Method
Secret message
Cover file
Key
X
Embedding
Stego file
Signature
Cover file
Key
X
Encoding
Stego file
Plain text
Key
Encryption
X
Cipher text
Visibility
Invisible, inaudible
Visible, invisible
Visible
Objective

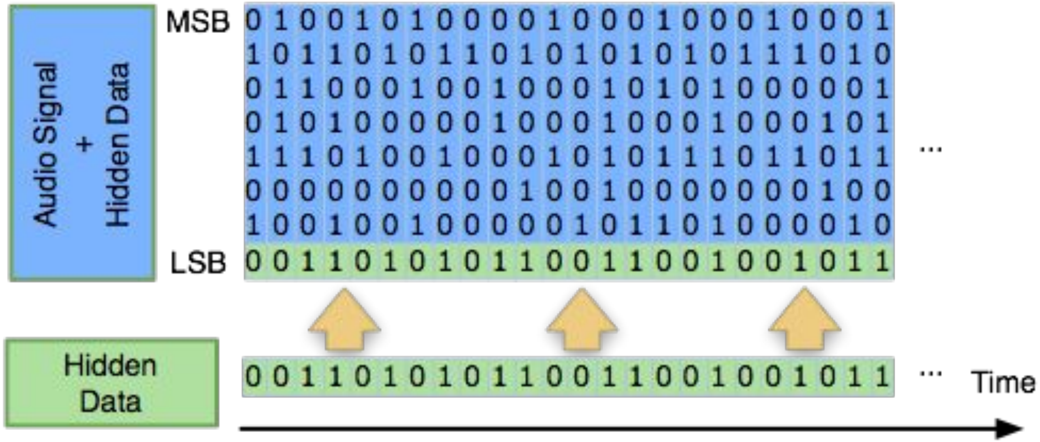

Steganography
Watermarking
Cryptography
Main Application
Imperceptible Communication
Copyright protection
Secure encryption of information
Method
Secret message
Cover file
Key
X
Embedding
Stego file
Signature
Cover file
Key
X
Encoding
Stego file
Plain text
Key
Encryption
X
Cipher text
Visibility
Invisible, inaudible
Visible, invisible
Visible
Objective
Undetectability, capacity
Robustness against removal
Robustness against attacks

Audio-Spectrogram of the Spoken Word "Hello"

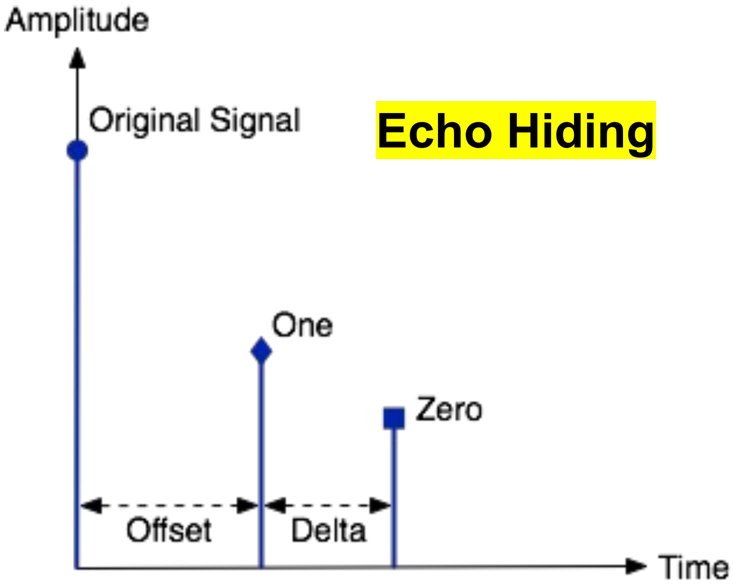
- Levels given in deciBels relative to Full Scale (dBFS)



Methods for Information Hiding within Audio-Signal

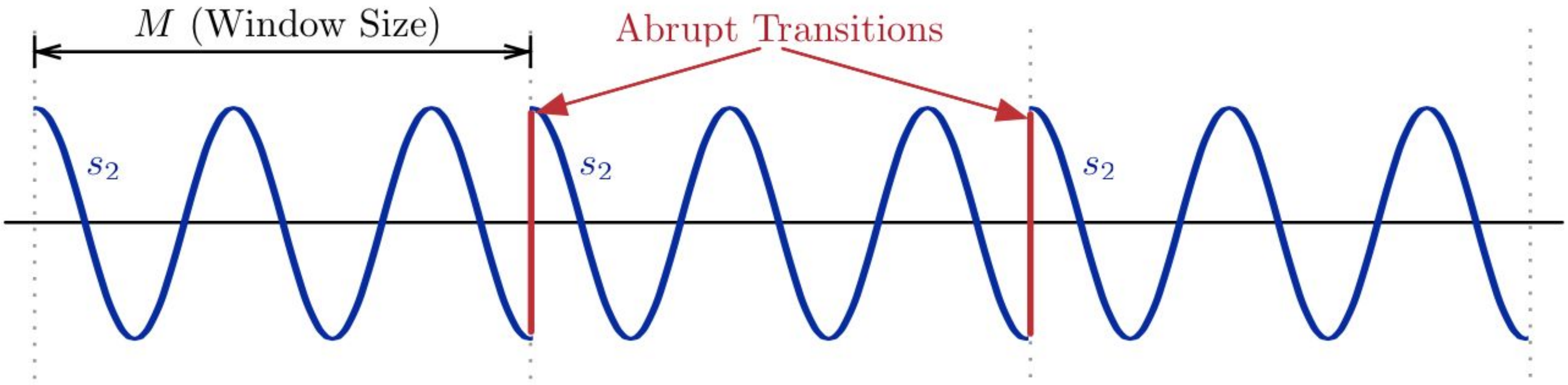


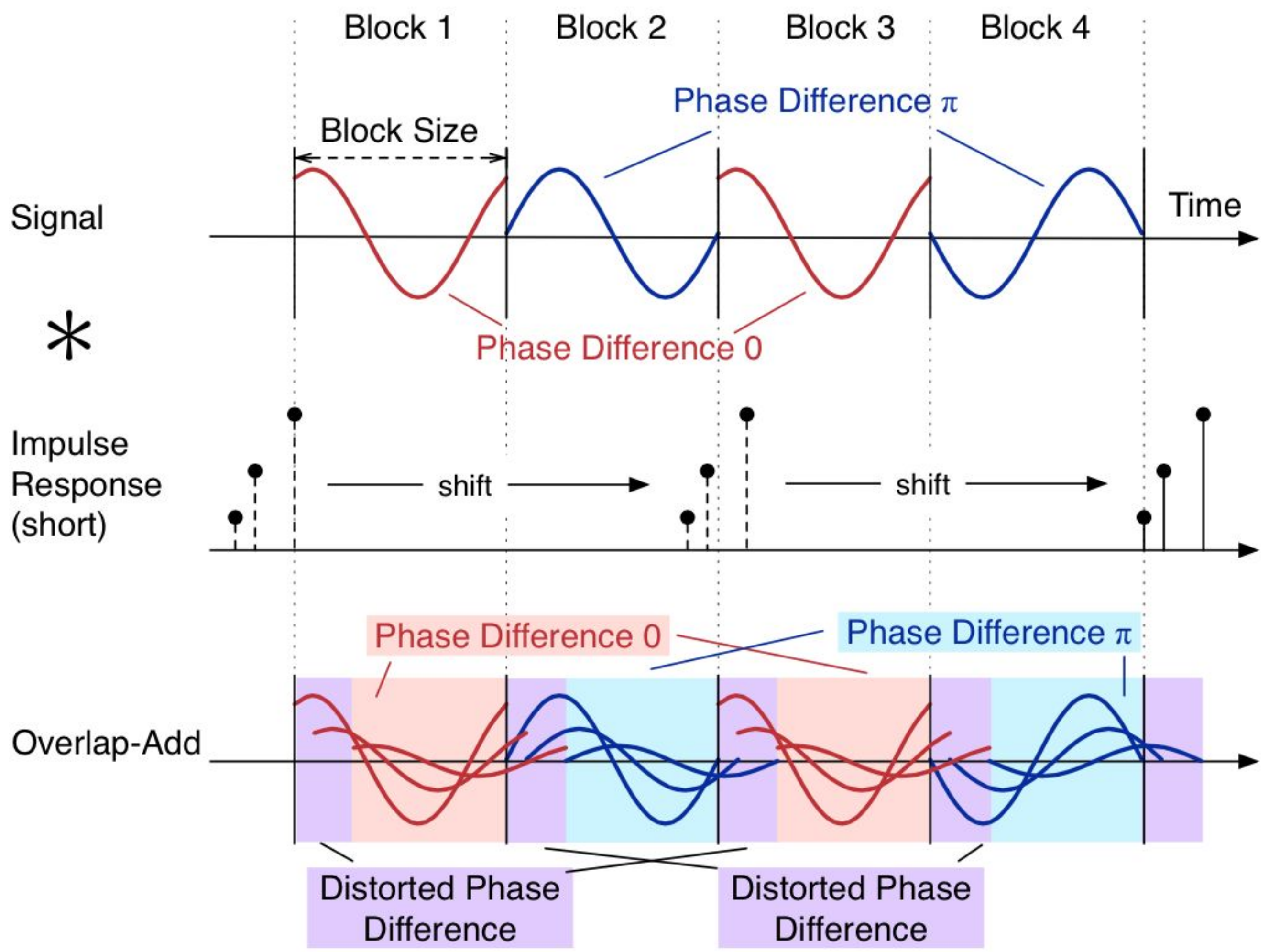
Least Significant Bit (LSB) Coding



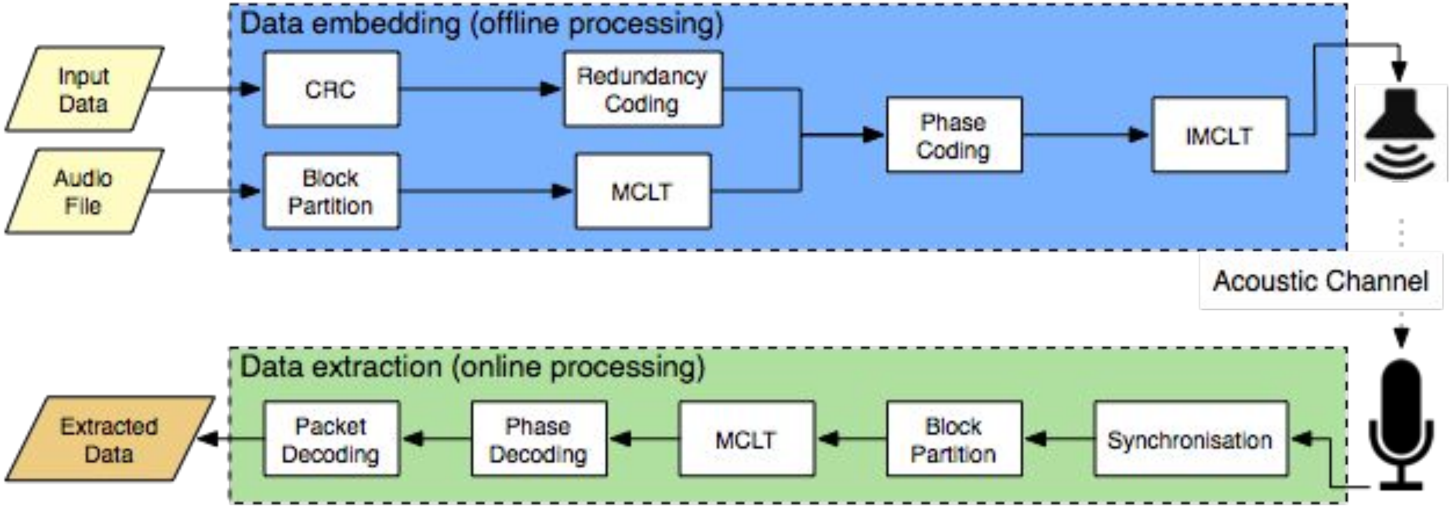
- (1) LSB Coding (left)
- (2) Echo Hiding (right)
- (3) Spread Spectrum
- (4) Phase Coding (next page)

Phase Encoding



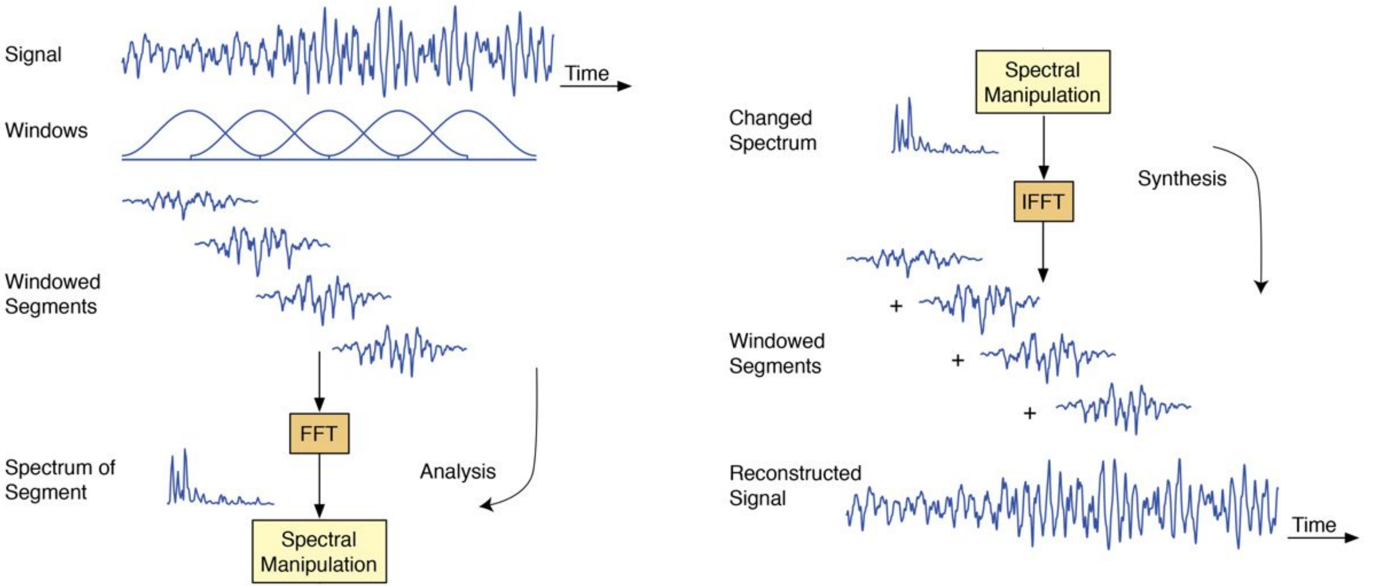

Block 1
Block 2
Block 3
Block 4
Block Size
Phase Difference π
Signal
Time
*
Phase Difference 0
Impulse Response (short)
shift
shift
Phase Difference 0
Phase Difference π
Overlap-Add
Distorted Phase Difference
Distorted Phase Difference

System Overview



- MCLT = Modulated Complex Lapped Transform
- Phase coding has advantages over alternative solutions
  - Shazam fingerprinting: no data communication, needs training
  - Ultrasound: increased audio signal energy (not desirable for TV broadcast)
  - Spread spectrum: creates noise (undesirable in cinemas)

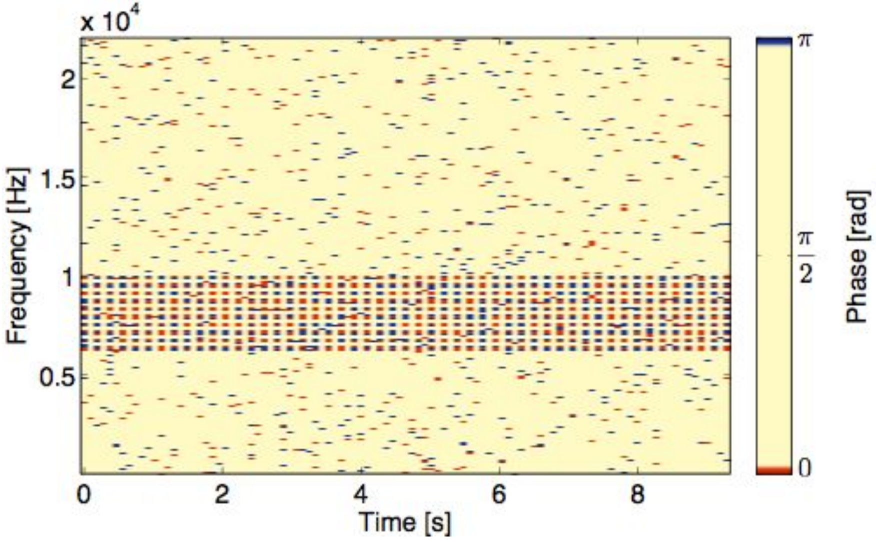
Signal (Re-) Construction



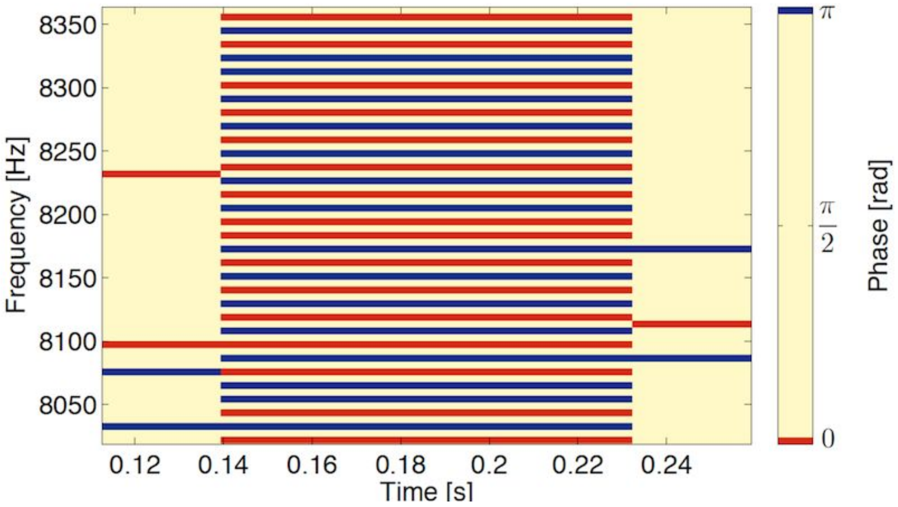
- Construction can be offline, or immediately in real-time
- Here: MCLT instead of Fast Fourier Transform (FFT)

Resulting Phases after Signal Construction

- Signal Construction = embedding message = modulation
- Signal Reconstruction = demodulation at receiver

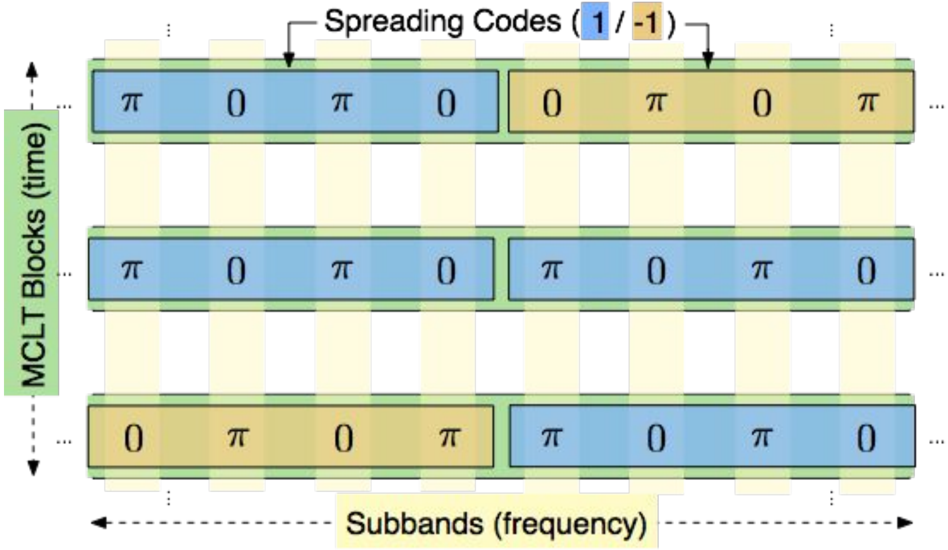


Overview



Zoom

Phase Coding

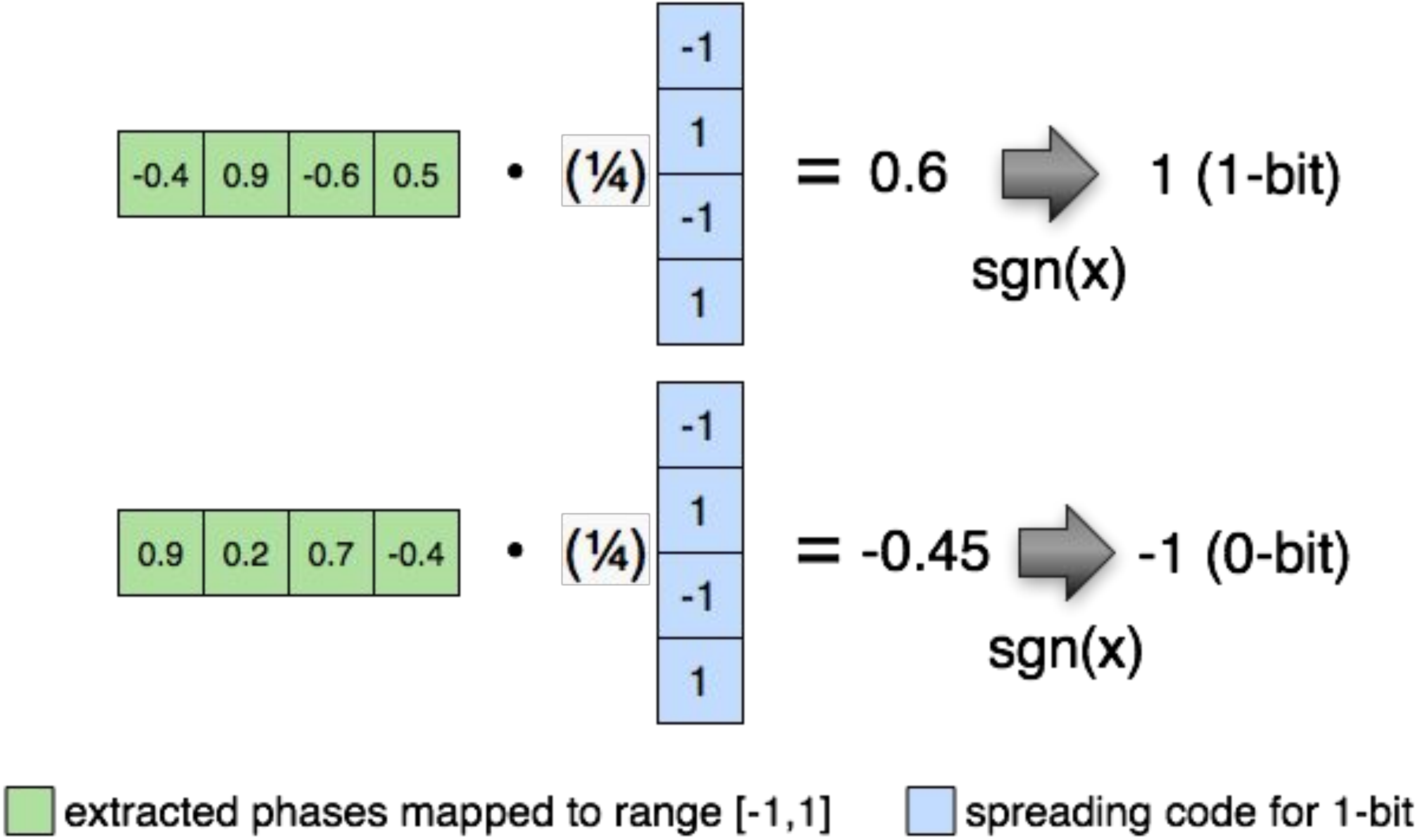


- Use frequency representation to alter phases (here: MCLT)
- Bits translated to spreading codes:

$$1 \rightarrow [-1\ 1\ -1\ 1] \rightarrow [\pi\ 0\ \pi\ 0]$$

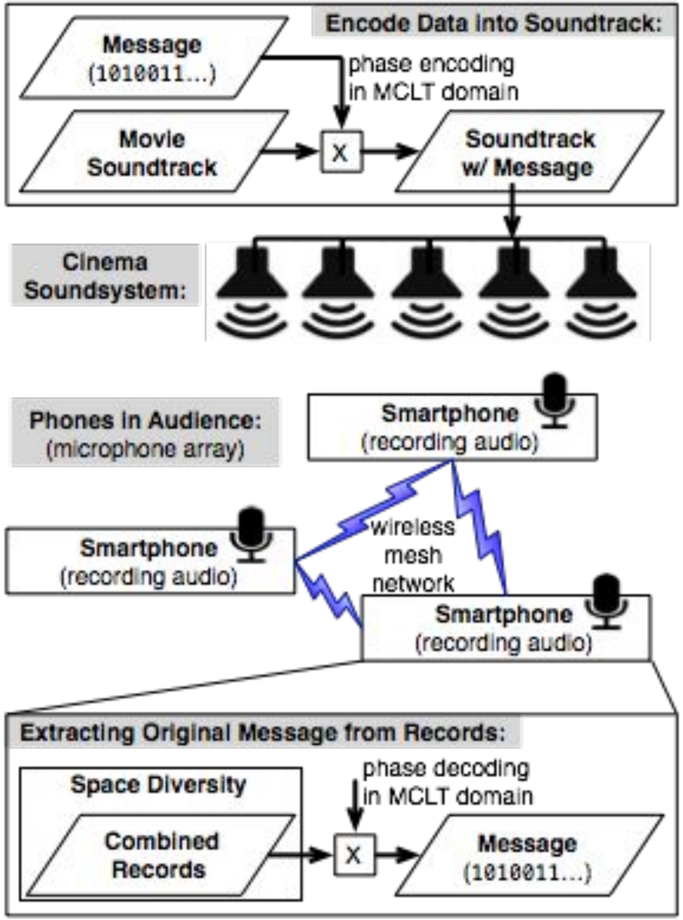
$$-1 \rightarrow [1\ -1\ 1\ -1] \rightarrow [0\ \pi\ 0\ \pi]$$

Phase Decoding (Correlation)



Receiver Diversity (Use of Multiple Phones)

Prototype

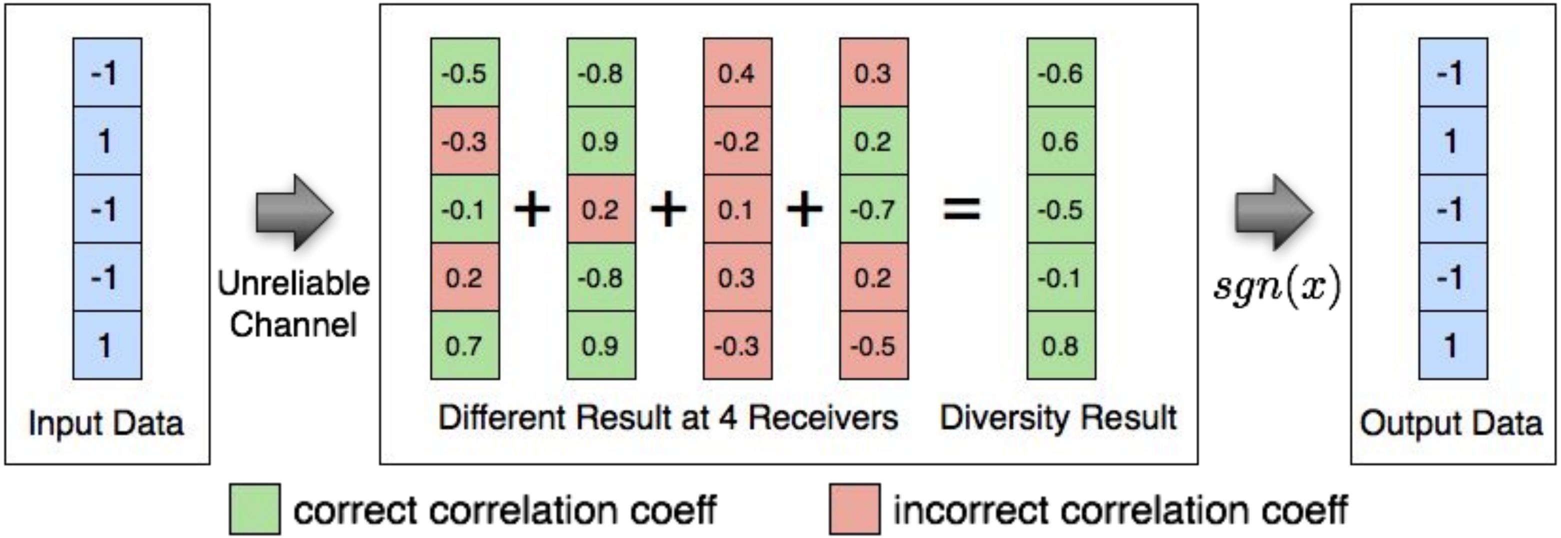


- Matlab prototype for embedding of messages
- iOS app as receiver/extractor
- Personal Hotspot for ad-hoc network (Wi-Fi)
- Single server combines all receivers' sequences

Receiver Diversity

Diversity Result: $$\hat{\rho}(n) = \frac{1}{L}\sum_{l=0}^{L-1}\rho_l(n)$$

$\rho_l(n)$: Sequence of correlation coefficients decoded at receiver l




ETH
Disney Research

Test Campaign in Cinema

- Arena Cinemas Zurich
- 200 square meter cinema (10m x 20m)
- Left, center, right speakers
- 4 receivers
  - Carrier signal: Pop song
- Metrics:
  - Bit Error Rate (BER)

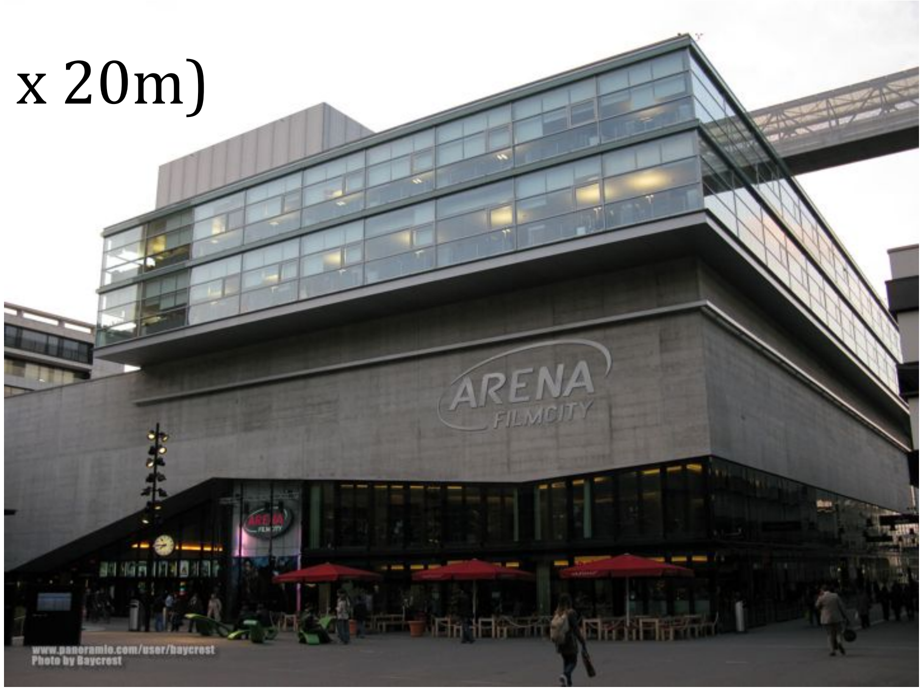
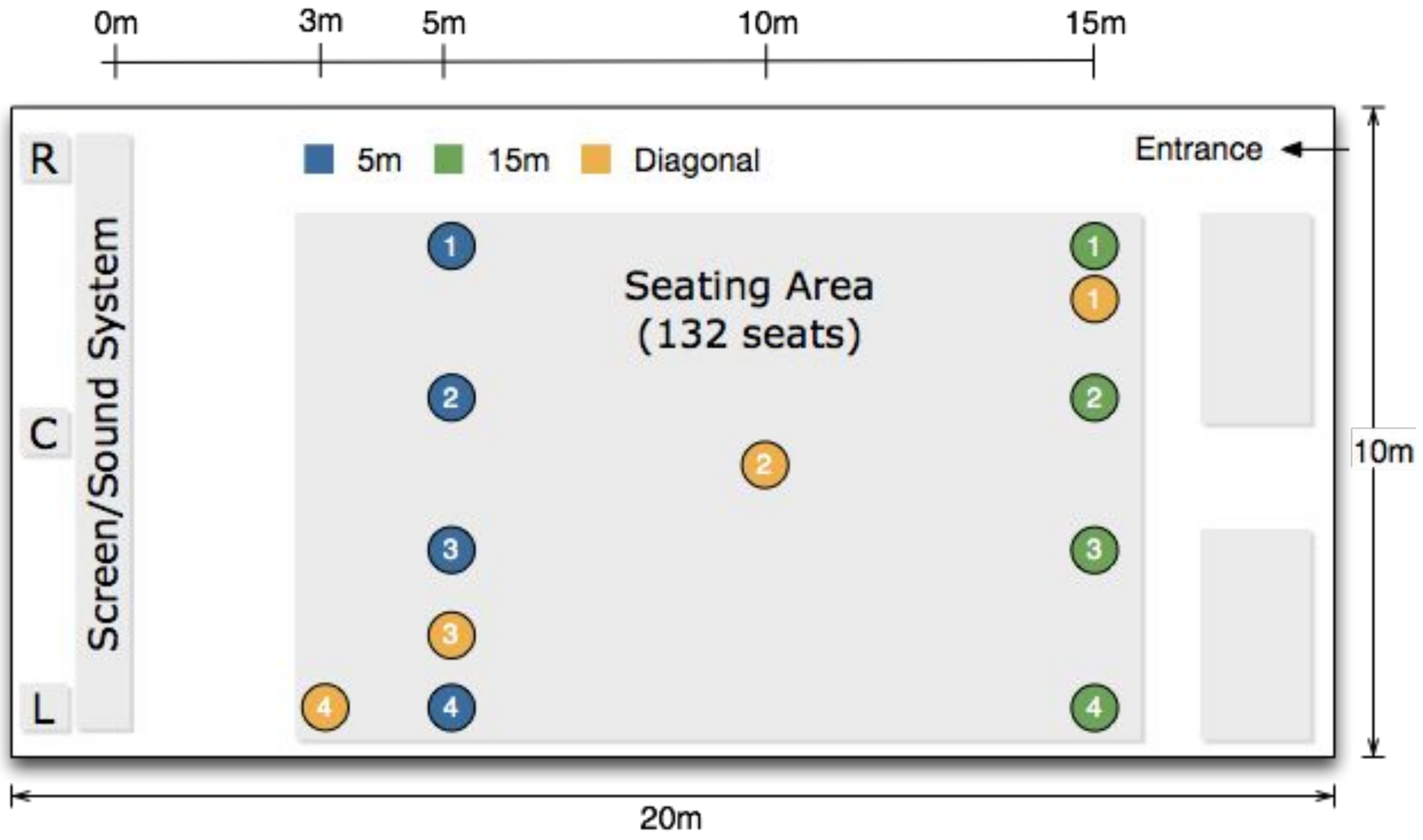


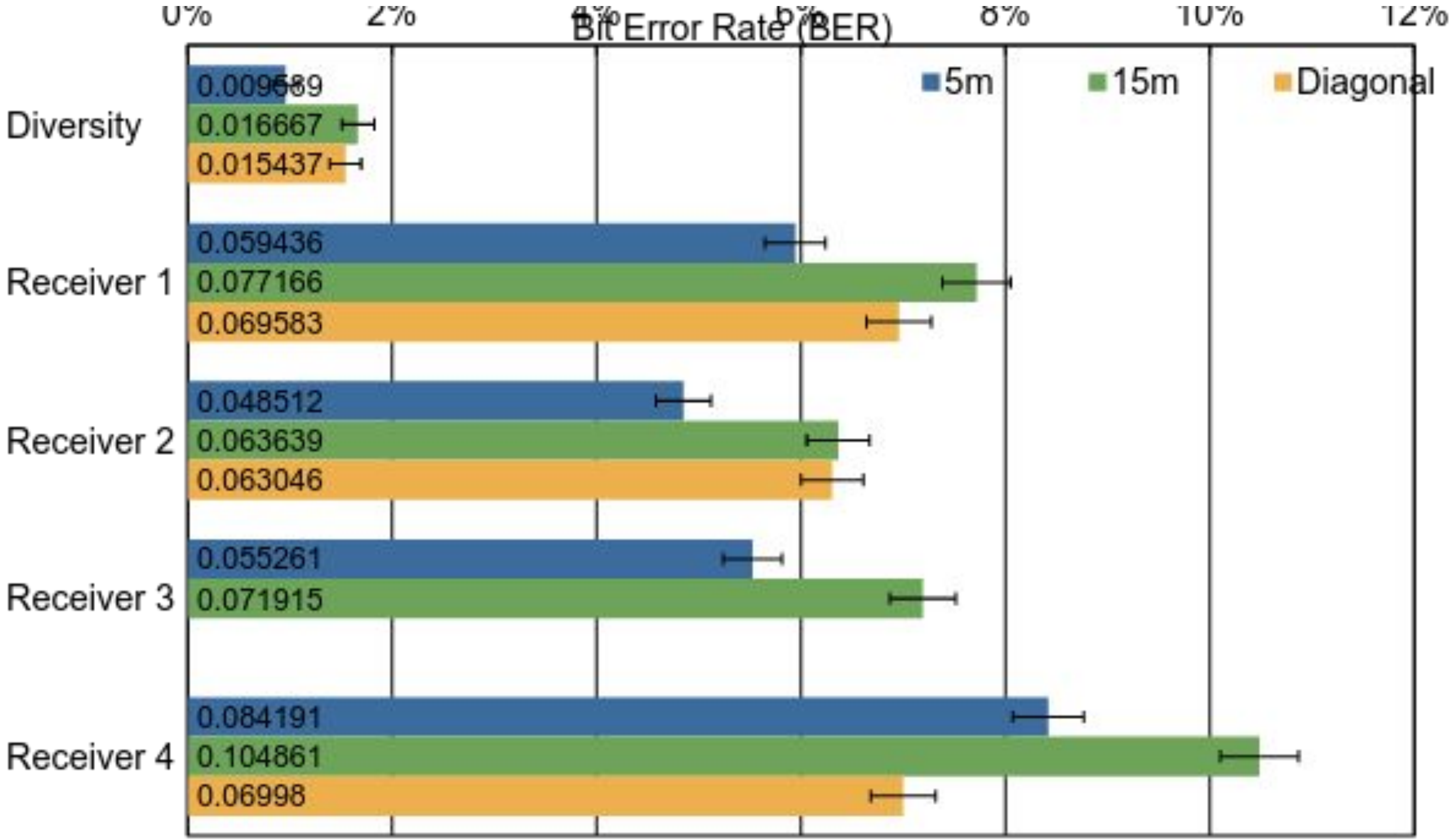
Photo: Baycrest (www.panoramio.com/user/Baycrest)


ARENA
CINEMAS

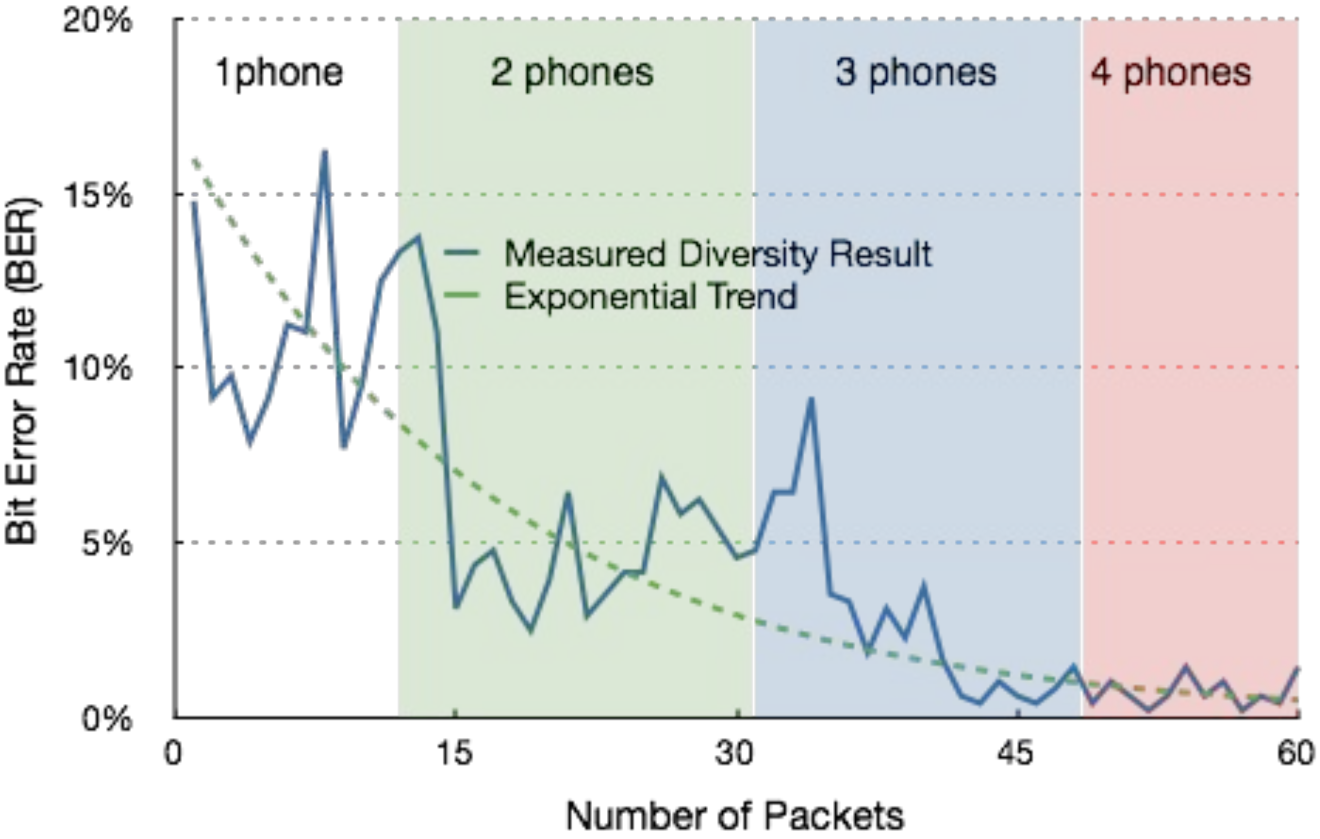
Cinema Field Test: Receiver Arrangement



Cinema Field Test: Results (1)



Cinema Field Test: Results (2)



Wireless Networking and Mobile Computing

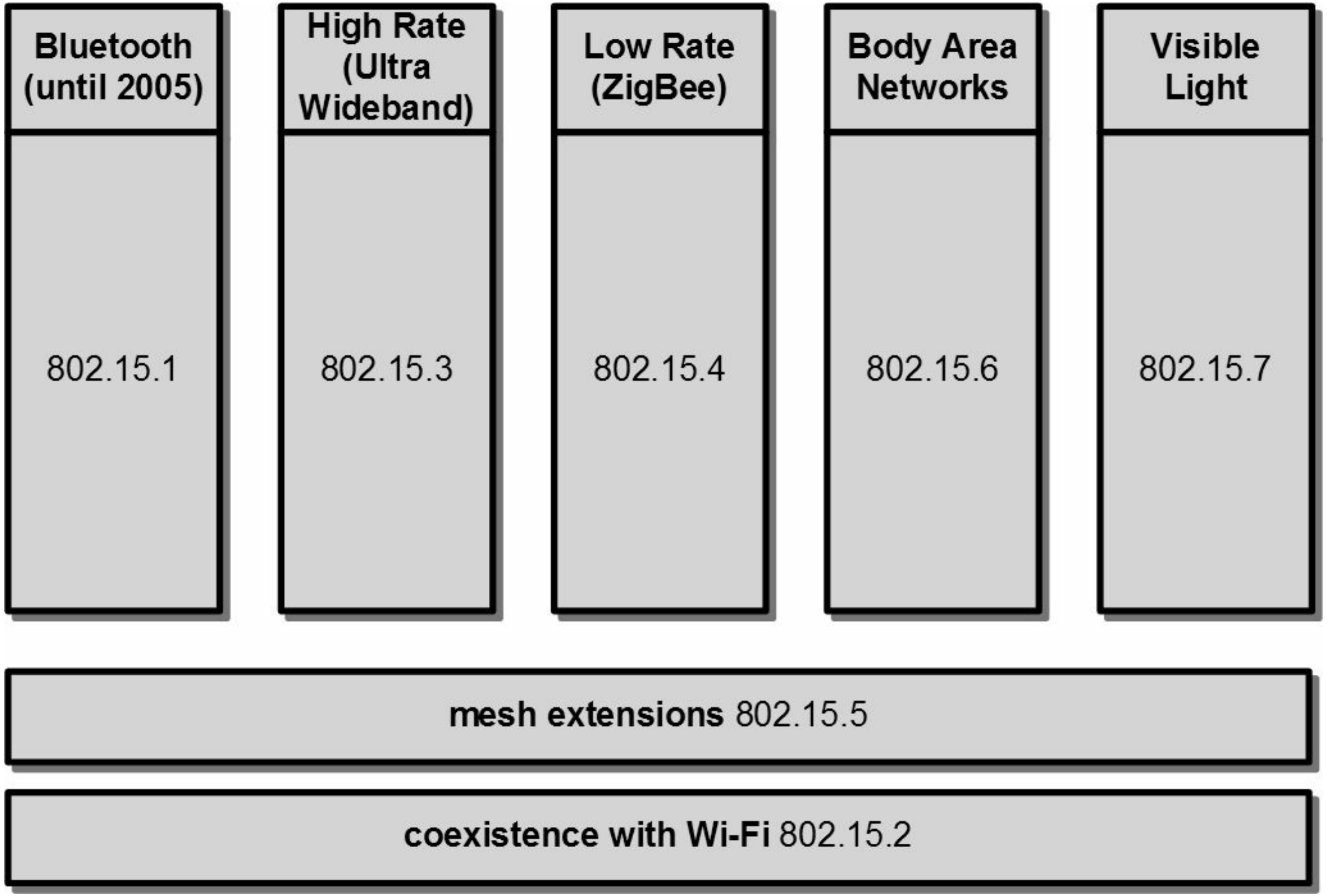
4. IEEE 802.15 Wireless Personal Area Networks (WPANs)

Stefan Mangold

Course Outline

1. Introduction
2. Wireless Communication Basics
3. IEEE 802.11 Wireless LAN (Wi-Fi)
4. IEEE 802.15 Wireless PAN (ZigBee & Bluetooth)
5. Mobile Computing Algorithm Basics: Control and Game Theory
6. Visible Light Communication
7. Audio Communication
8. Cellular Networking Basics (LTE, 5G, Internet-of-Things)
9. Mobile Computing for Automated Medicine Delivery
10. Cognitive Radio, Delay Tolerant Networking, Radio Spectrum Sharing

IEEE 802.15 Wireless Personal Area Networks



IEEE 802.15 Overview "Personal Area Networks" (1 of 2)

- 802.15.1: Bluetooth v1.1
- 802.15.2: Coexistence Mechanisms
- 802.15.3: High Rate WPAN
  - .3a: High Rate Alternative PHY (MB-OFDM vs. DS-UWB)
  - .3b: MAC Amendment
  - .3c: Millimeter Wave Alternative PHY

(continues on next page)

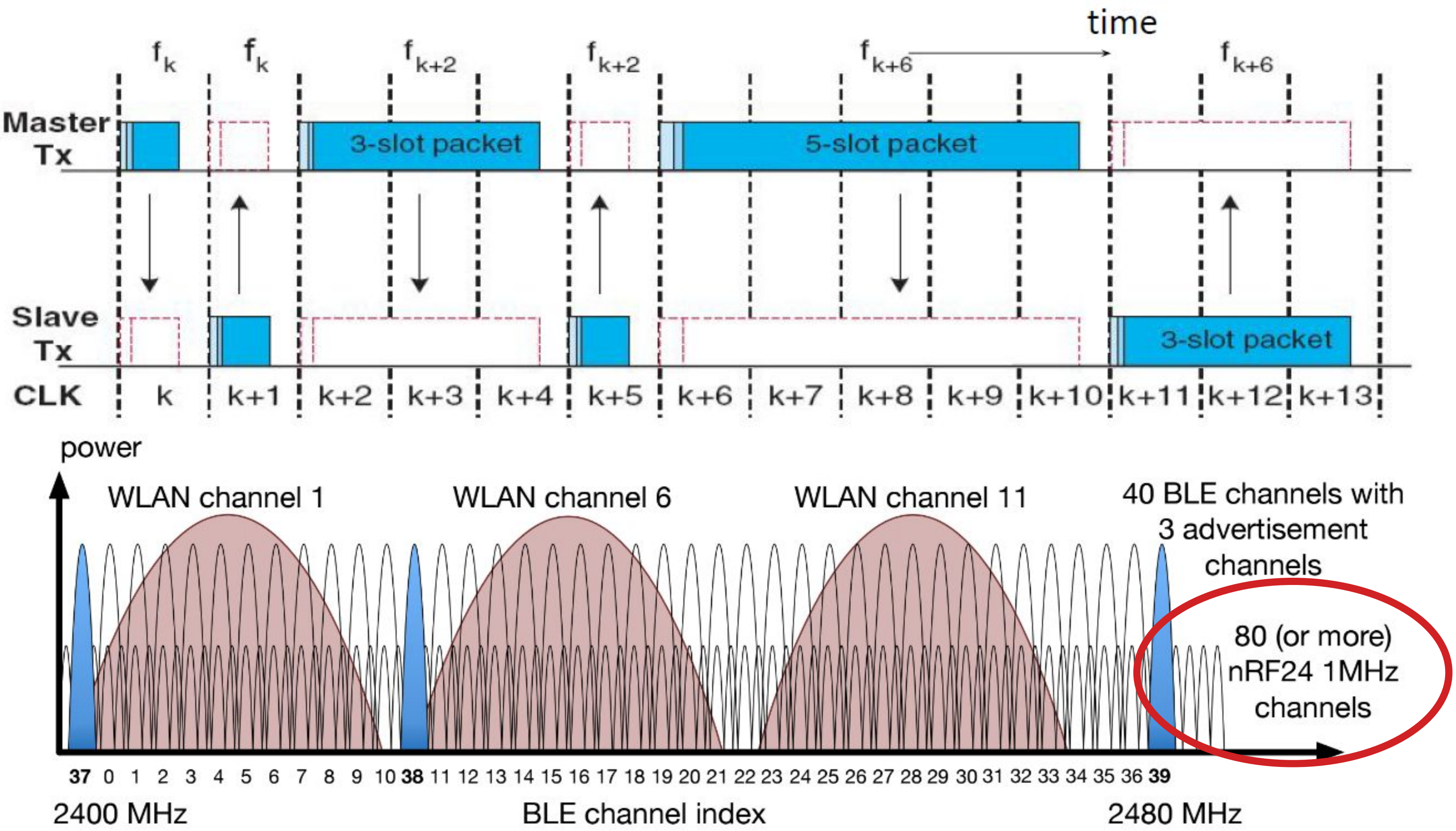
IEEE 802.15 Overview “Personal Area Networks” (2 of 2)

- 802.15.4: Low Rate WPAN → ZigBee
  - .4a: Low Rate Alternative PHY
  - .4b: Revisions and Enhancements
  - .4c: Alternative PHY for China
  - .4d: Alternative PHY for Japan
  - .4e: MAC for Industrial
  - .4f: Active RFID
  - .4g: Smart Utility Network
- 802.15.5: Mesh
- 802.15.6: Body Area Networks (medical)
- 802.15.7: VLC
- 802.15.8 … 15.10: supporting topics, security

802.15.1 Bluetooth

- Short range communication, operates mainly in ISM bands at 2.4 GHz
  - Same as WLAN 802.11b/g
  - Supports up to 8 devices in a piconet (1 master and 7 slaves), up to 7 connections
- Piconets can combine, to form scatternets
  - Linking of co-located piconets by sharing common master or slave devices
- Frequency Hopping Spread Spectrum (FHSS)
  - Polling based Time Division Duplex (TDD)
  - 2.402 GHz … 2.480 GHz divided into 79 channels with 1 MHz each
  - Bluetooth devices hop from one channel to another, pseudo-random
  - Up to 1600 hops per second

802.15.1: MAC illustrated



802.15.1 Bluetooth Protocol Stack

- Link Controller (LC)
  - Connection establishment, addressing
  - Packet formatting
  - Timing and power control
- Link Manager Protocol (LMP)
  - Link setup and link management
  - Encryption, authentication
- Logical Link Control and Adaptation Protocol (L2CAP)
  - Adapts upper layer protocols to baseband layer
  - Provides connectionless and connection oriented services

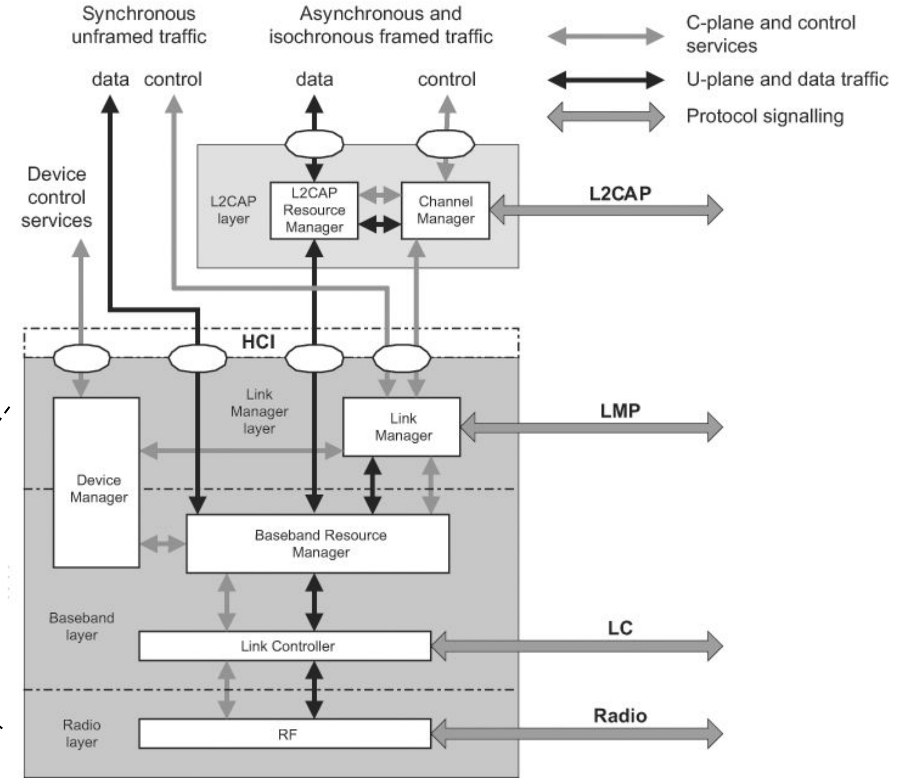
Bluetooth Stack Illustrated

ISO/OSI Reference Model

Application
Presentation
Session
Transport
Network
Data Link
Physical

802 Scope

Medium Access
Physical



802.15.1 Medium Access Control

- Time division duplex, TDD, time slot length 625 us
  - synchronized clock signals are needed
- Packets are sent on single-hop carrier
  - Frequency remains constant for packet transmission duration
- Frequency Hopping Synchronization (FHS)
  - Fixed and Multi-slot packets (3-slot and 5-slot)
- Master polls slaves according to polling scheme
  - Master schedules UL and DL traffic (UL=uplink, DL=downlink)
  - Slave transmits only after it has been polled
  - Often it is stated that an “intelligent algorithm is required”

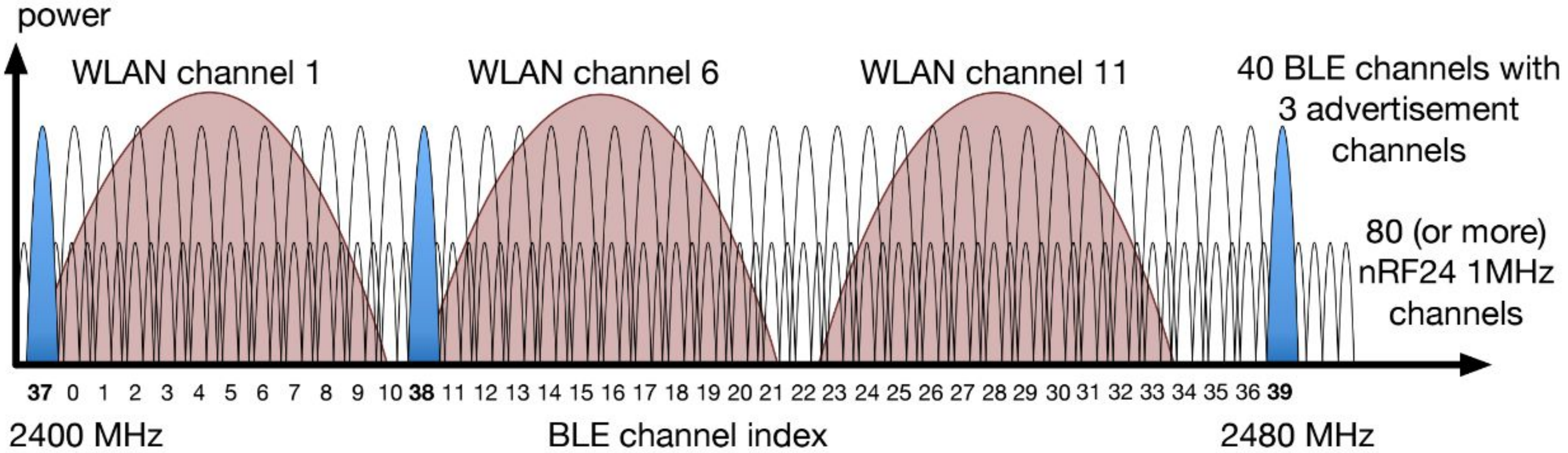
Bluetooth Versions

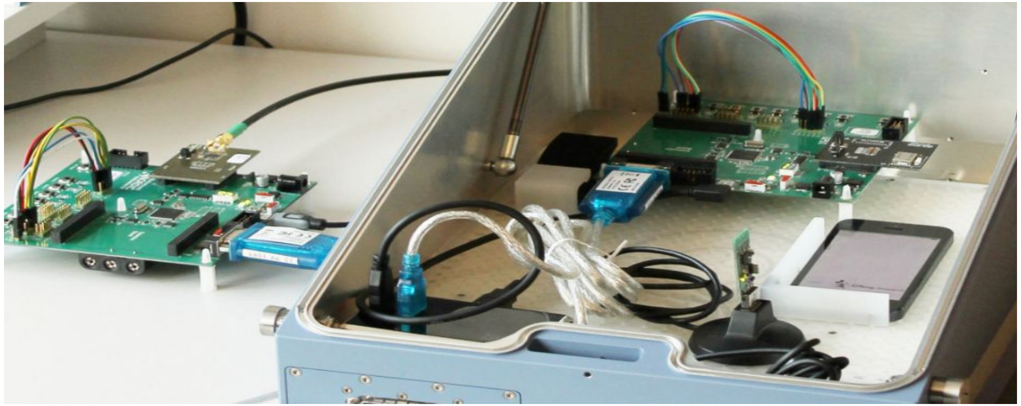
- The 2017 Bluetooth 5 is backward compatible with previous Bluetooth versions such as v1.2, v2, v2.1, v3, v4, v4.1 and v4.2.
- Bluetooth 5 addresses the need for IoT (low power, longer range and higher speed)
  - Bluetooth 4.2 offers already limited power consumption with Bluetooth Low Energy (BLE)
  - Connectionless broadcasting (new: 255 Byte packets) is advantageous for applications like local advertising, guides in shopping mall, for parking
- 1...2 MHz bandwidth, GFSK and QPSK modulation
- Centralized TDMA MAC protocol

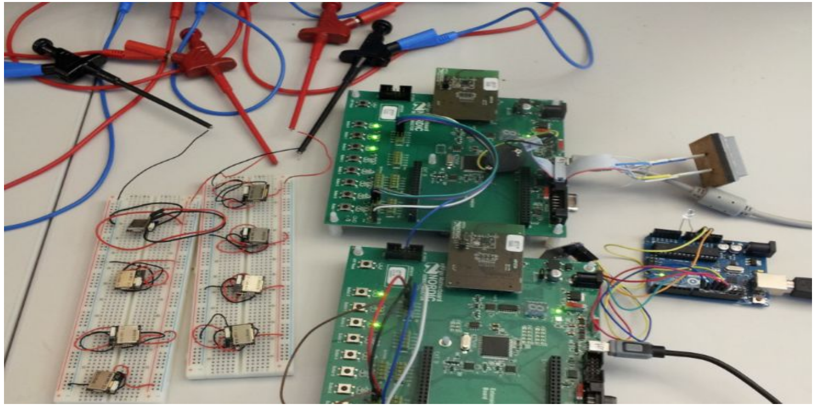
BLE

	BLE	Classic BT
Frequency Band	2.4GHz ISM Band	2.4GHz ISM Band
Frequency Channels	3 advertising and 37 data channels, 2 MHz spacing	79 channels, 1 MHz spacing
Freq. Channel Usage	Static on the three advertisement channels, optional adaptive FHSS for data exchange.	Static during advertisement, adaptive FHSS during data exchange
Modulation	GFSK	GFSK, π/4 DQPSK, 8DPSK
Energy Consumption	~0.01x to 0.5x of reference	1 (reference value)
Max Data Rate	125 Kb/s … 2 Mb/s	1 Mb/s … 3 Mb/s
Max Tx Power	1mW (0 dBm) … 100 mW (+20 dBm)	1mW (0 dBm) … 100 mW (+20 dBm)
Network Topologies	Point-to-Point (piconet), Broadcast, Mesh	Point-to-Point (piconet)

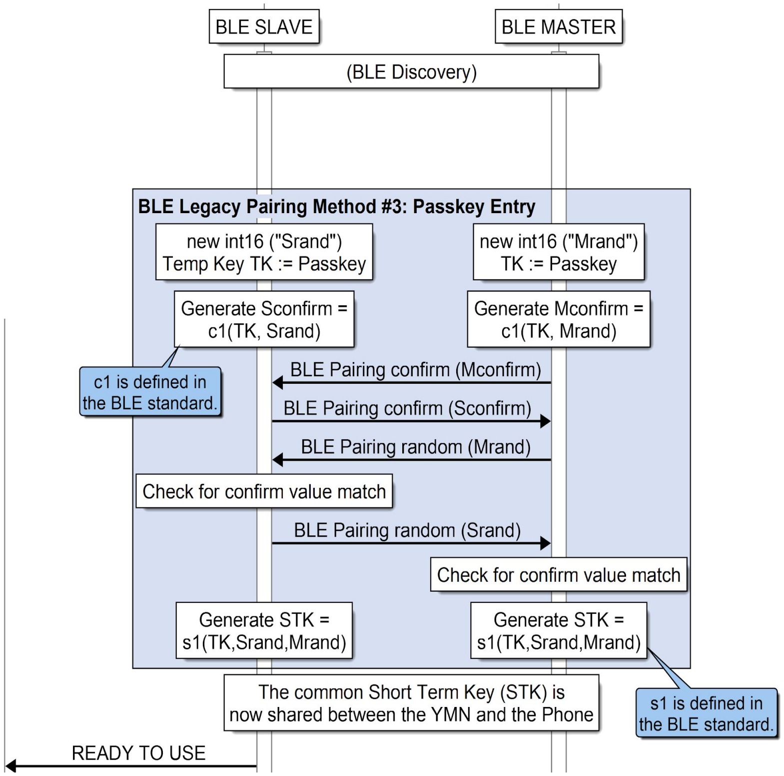
Bluetooth Low Energy (BLE) & commercial Nordic NRF24

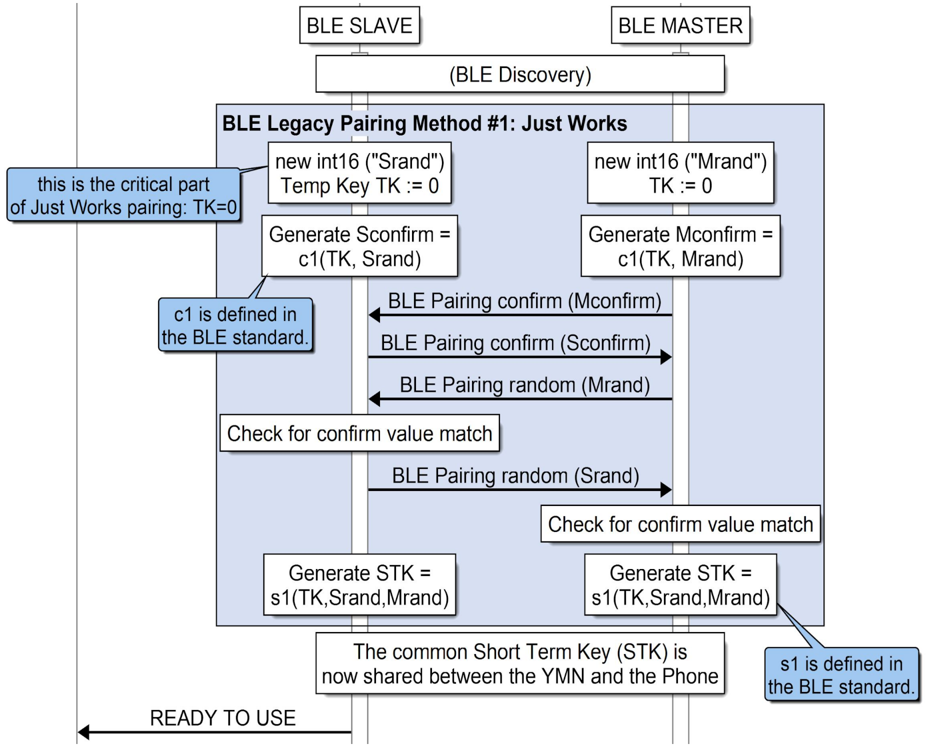




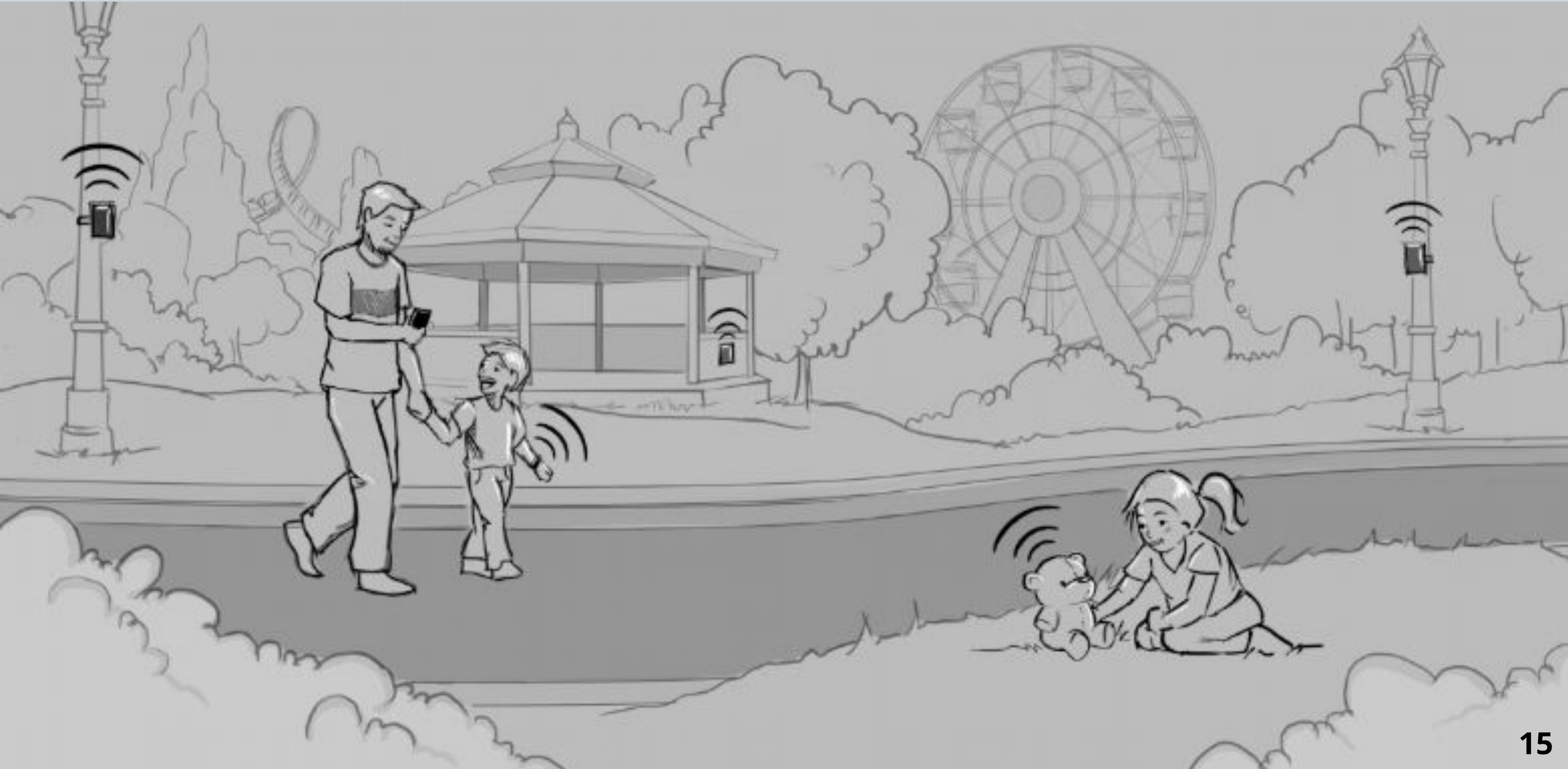


Pairing ("Passkey" and "Just Works")

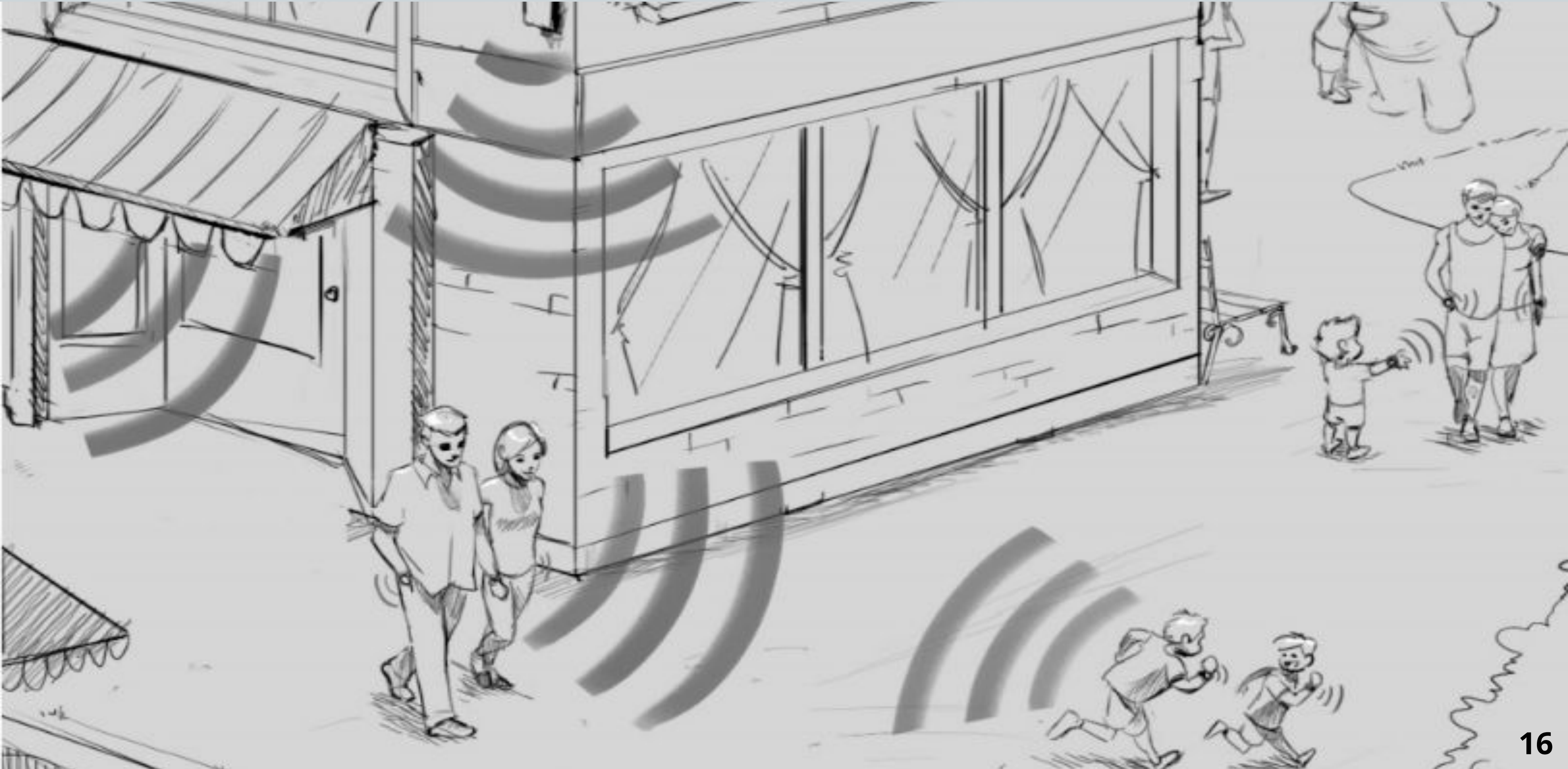




Beacons



Beacons & Mesh Network



Exposure Notification Mobile App

During the Bluetooth broadcast, advertisements are to be non-connectable undirected. The advertiser address type shall be random non-resolvable.

On platforms supporting the BT Random Private Address with a randomized rotation timeout interval, the **advertiser address rotation** period is random.

The advertiser address, Rolling Proximity Identifier, and Associated Encrypted Metadata shall be changed synchronously so that they cannot be linked.

The **broadcasting interval is currently recommended to be 200-270 milliseconds**.

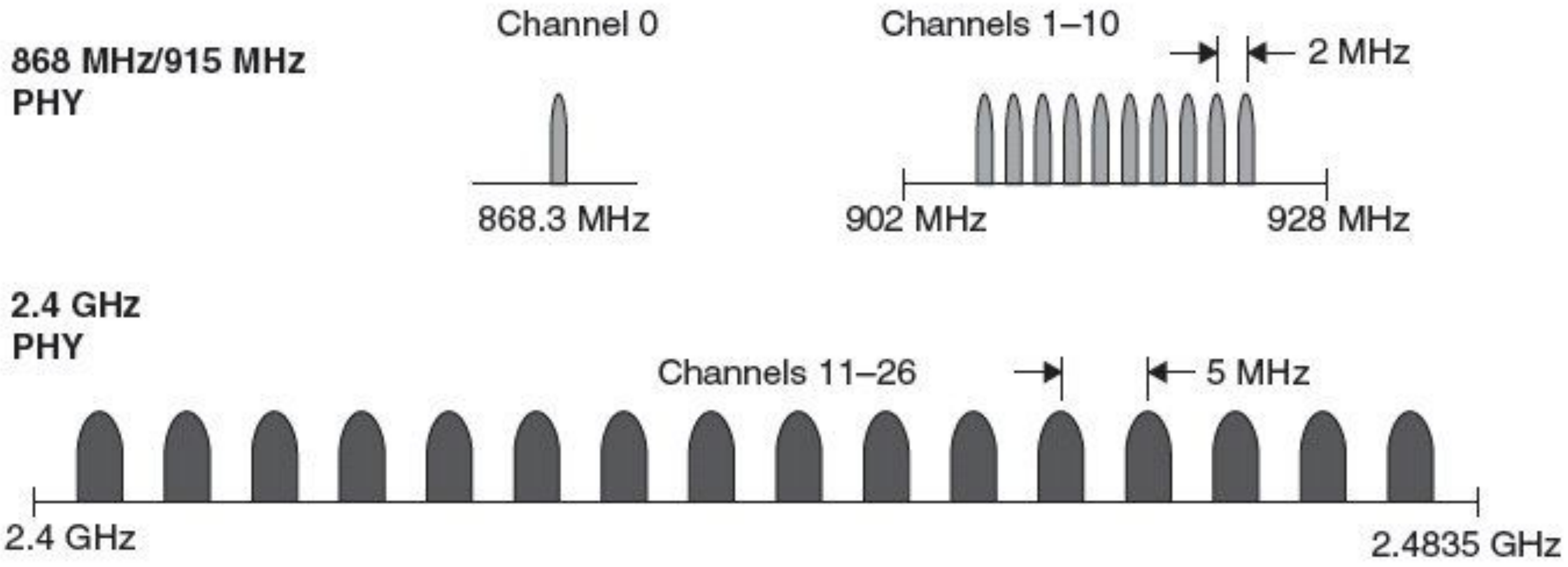
The Exposure Notification Bluetooth Specification does **not use location** for proximity detection. It strictly uses Bluetooth beaconing to detect proximity.

802.15.4 ZigBee

- IEEE Std 802.15.4-2004 published (2006 updated)
  - Conforms to the IEEE 802.15.4-2003
  - Networks “form by themselves, scale to large sizes and operate for years without manual intervention”

- Long battery life (months on AA cell)
  - low cost: low device / setup costs, small complexity and small size
- Technical features
  - Up to 65536 nodes, max. data rate 250 kb/s
  - 27 channels over 2 bands (16 @ 2.4 GHz, 10 @ 915/868 MHz)
  - Limited data rate and QoS, optimized for timing-critical applications and power management, mesh support

ZigBee Radio Channels



802.15.4 ZigBee Network Topology

- PAN coordinator (ZigBee coordinator)
  - Forms root of network tree and might bridge to other networks
  - Introduces basic parameters and stores information about network
  - Only one per network allowed
- Full function device (ZigBee router)
  - Intermediate router for multi-hop data transmission from other devices
- Reduced function device (ZigBee end device)
  - Functionality limited to connect to parent node
  - Allows node to be asleep a significant amount of time

802.15.4 ZigBee PHY

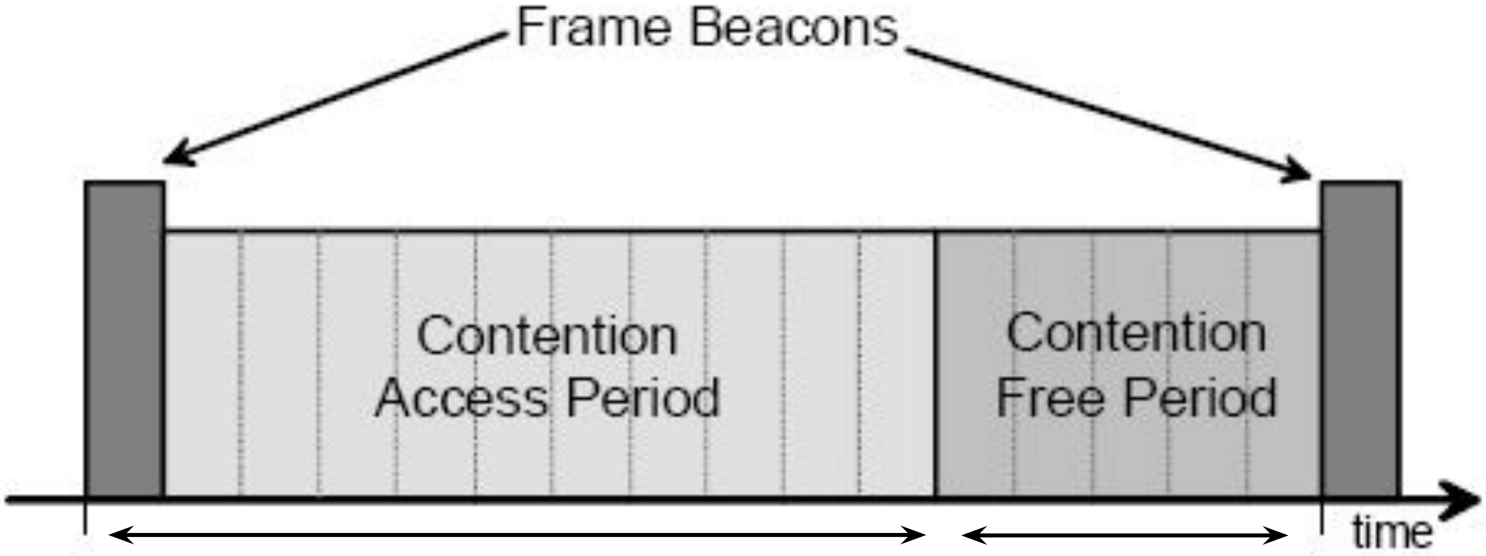
- Direct Sequence Spread Spectrum (DSSS)
- Transmission power up to 1W

PHY [MHz]	Freq. [MHz]	Chip rate [kchip/s]	Modulation	Bit rate [kb/s]	Symbol rate [ksymbol/s]	Symbols	Beacon Interval
868/915	868–868.6	300	BPSK	20	20	Binary	48ms – 786s
868/915	902–928	600	BPSK	40	40	Binary	24ms – 393s
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS	15.36ms – 251s
868/915 (optional)	902–928	1600	ASK	250	50	5-bit PSSS	15.36ms – 251s
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal	?
868/915 (optional)	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal	15.36ms – 251s
2450	2400 – 2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal	15.36ms – 251s

802.15.4 ZigBee MAC

- Variant #1: non-beacon enabled network
  - Contention Access Period (CAP)
  - Unslotted CSMA / CA based channel access
  - Positive acknowledgement for successfully received packets
- Variant #2: beacon-enabled network
  - CAP + Contention Free Period
  - Superframe structure-network coordinator transmits beacons at predetermined intervals, introduces time slots
  - Slotted CSMA-CA based channel access
  - Nodes transmit periodic beacons to confirm their presence
  - Guaranteed Time Slots (GTS) for low latency real-time requirements
  - Nodes may sleep between beacons → extended battery life

802.15.4 ZigBee MAC illustrated



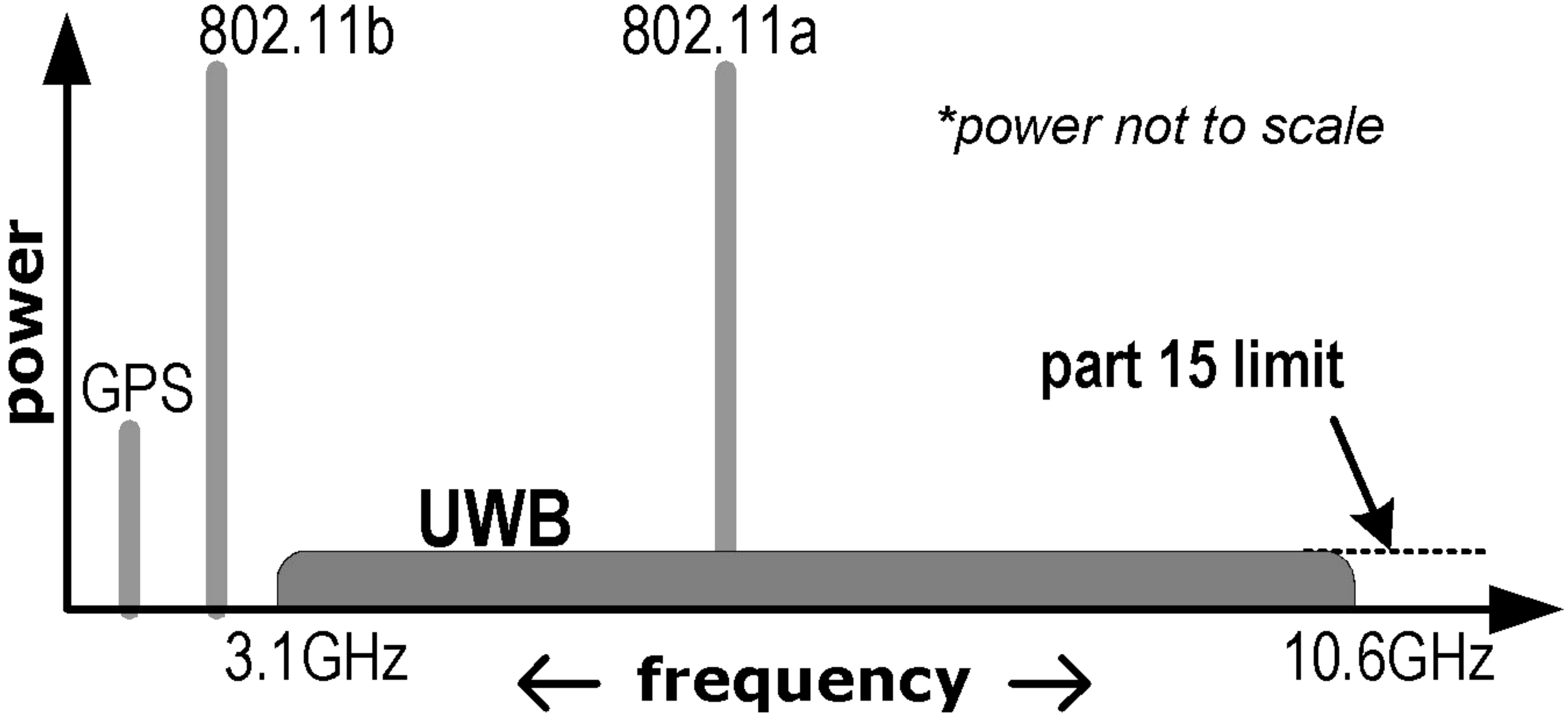
channel access under competition
slotted CSMA / CA

Guaranteed
Time Slots

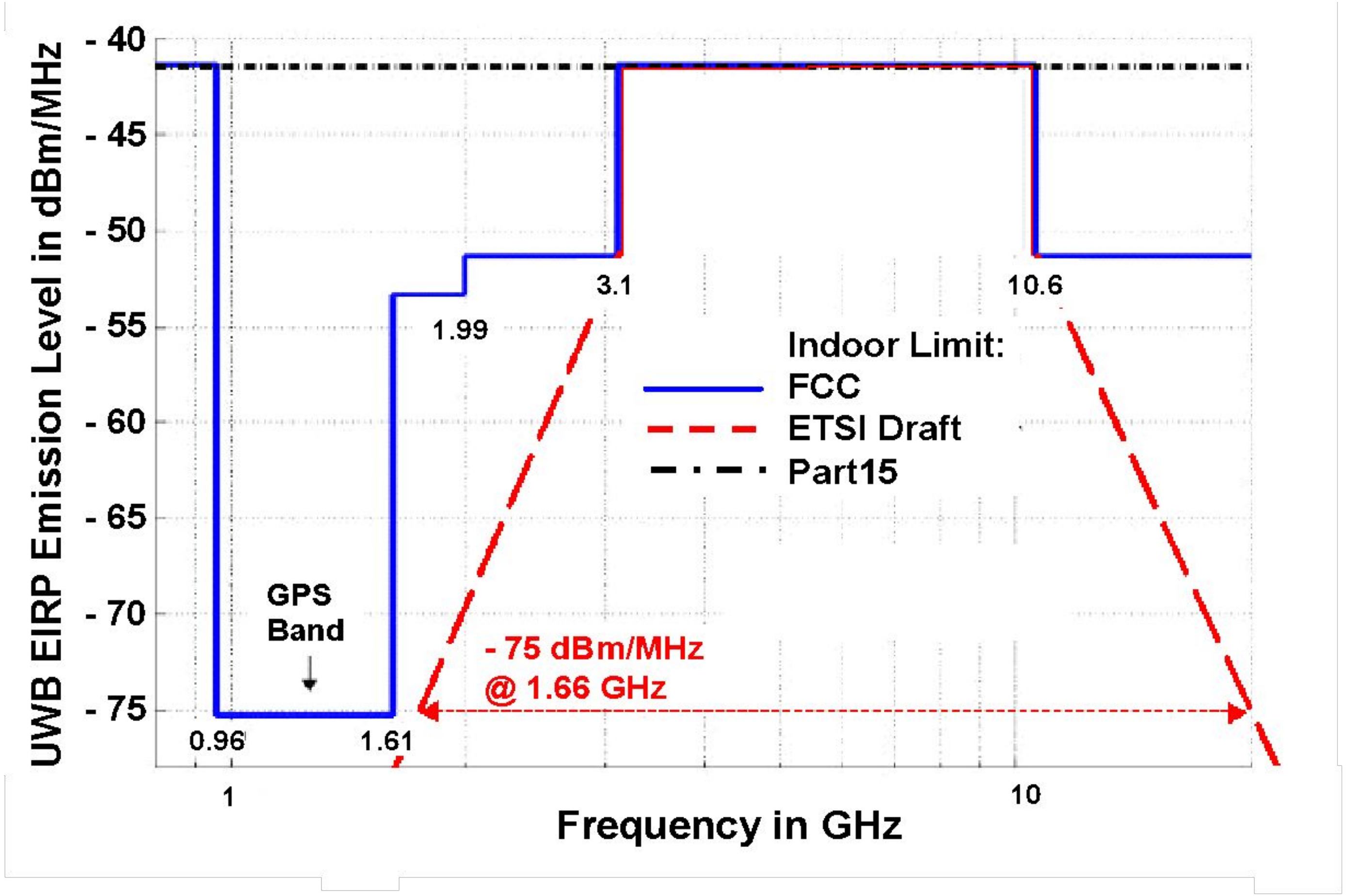
ZigBee vs. Bluetooth

	Bluetooth v1.1	ZigBee
IEEE standard	802.15.1	802.15.4
Modulation	FHSS	DSSS
Protocol stack size (estimate)	250 kB	28 kB
Max. throughput	< 1Gb/s	250 kb/s
Range	1-100m	<70m
Battery (marketing focus)	Frequent recharging	Not rechargeable
Network join time	3s	30 ms
Price for chipset	2006: 3$ 2010: <1$	1998: 4-6 2006: 3$
Enhancements	Bluetooth 2.0 / 3.0 / 4.0 Bluetooth Low Energy	802.15.4a 802.15.4b
Main applications	audio, data transfer	sensors, control automation

Underlay Spectrum Usage: Ultra Wideband Comm.



European Regulation: CEPT SE24/ ETSI TG31a Draft

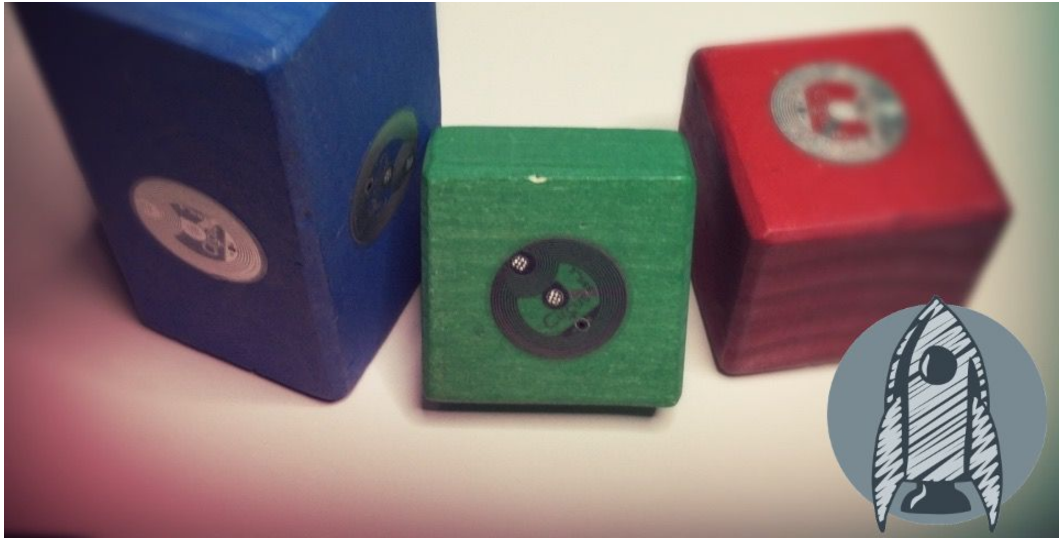


802.15.3a: Ultra Wideband Communication

	DS-UWB	MB-OFDM
PHY technique	Single-carrier direct sequence spreading	Multiband-OFDM
Frequency management	Two bands (lower band: 3.1 ~ 4.85 GHz Higher band: 6.2 ~ 9.7 GHz)	Four frequency band groups. (three bands of each in group 1, 2, 3 and 4, two in group 5) Each band covers 528 MHz.
Data rates	28, 55, 110, 220, 500, 660, 1000 and 1320 Mb/s	53.3, 80, 106.7, 160, 200, 320, 400 and 480 Mb/s
Typical Modulation	BPSK	QPSK
Channel coding	Convolutional coding with interleaving	Convolutional coding with interleaving
Logical Channels	Total 12 channels (6 in lower band and 6 in higher band)	Total 18 channels through Mulitplexing

Near Field Communications

- Secure communication within a few centimeters
- No batteries required (similar to RFID, but short range)
- Often used in logistics, for toys, and consumer products



NFC Technology

- Unlicensed radio frequency ISM band of 13.56 MHz
  - ±7 kHz bandwidth
- Data rates: 106 ... 424 kb/s at up to 10 cm distance
- There are NFC devices and passive NFC tags
  - Devices read from (and write to) tags, and can operate as tags for peer-to-peer communication
  - Tags store a small amount of data (<10kB)
- Standard: ISO/IEC 18000-3 protocols

Internet of Things

- Wi-Fi HaLow, Bluetooth, ZigBee
- IEEE 802.15.4g - Utility Industry
  - invented mainly by Itron Inc.
- Sigfox
  - includes higher layers and applications for data analytics and visualization
- LoRa
  - consortium, backed by Telcos, mainly from Semtech
- NB IoT - cellular 5G
  - backed by big telco players and the 3GPP community, Huawei, Ericsson

Wireless Networking and Mobile Computing

5. Mobile Computing Algorithm Basics: System / Control / Game Theory: PID Controller

Stefan Mangold

Course Outline

1. Introduction
2. Wireless Communication Basics
3. IEEE 802.11 Wireless LAN (Wi-Fi)
4. IEEE 802.15 Wireless PAN (ZigBee & Bluetooth)
5. Mobile Computing Algorithm Basics: Control and Game Theory
6. Visible Light Communication
7. Audio Communication
8. Cellular Networking Basics (LTE, 5G, Internet-of-Things)
9. Mobile Computing for Automated Medicine Delivery
10. Cognitive Radio, Delay Tolerant Networking, Radio Spectrum Sharing

Time-Discrete Controller: Method “compute()”

```java
public void compute() {
    message("---------------------------", 10);
    message("I am station " + this.dot11MACAddress.toString() +". My algorithm is called '" + this.algorithmName + "'.", 10);

    // observe outcome:
    Integer AIFSN_AC01 = theBackoffEntityAC01.getDot11EDCAAIFSN();
    Integer CWmin_AC01 = theBackoffEntityAC01.getDot11EDCACWmin();

    theBackoffEntityAC01.getQueueSize();
    theBackoffEntityAC01.getCurrentQueueSize();

    message("with the following contention window parameters ...", 10);
    message("    AIFSN[AC01] = " + AIFSN_AC01.toString(), 10);
    message("    CWmin[AC01] = " + CWmin_AC01.toString(), 10);

    // infer decision: (note, we just change the values arbitrarily

    // AIFSN_AC02 = 10;
    // CWmin_AC02 = 5;

    // act:
    theBackoffEntityAC01.setDot11EDCAAIFSN(AIFSN_AC01);
    theBackoffEntityAC01.setDot11EDCACWmin(CWmin_AC01);
}
```

Y (n=1,2,3,...)

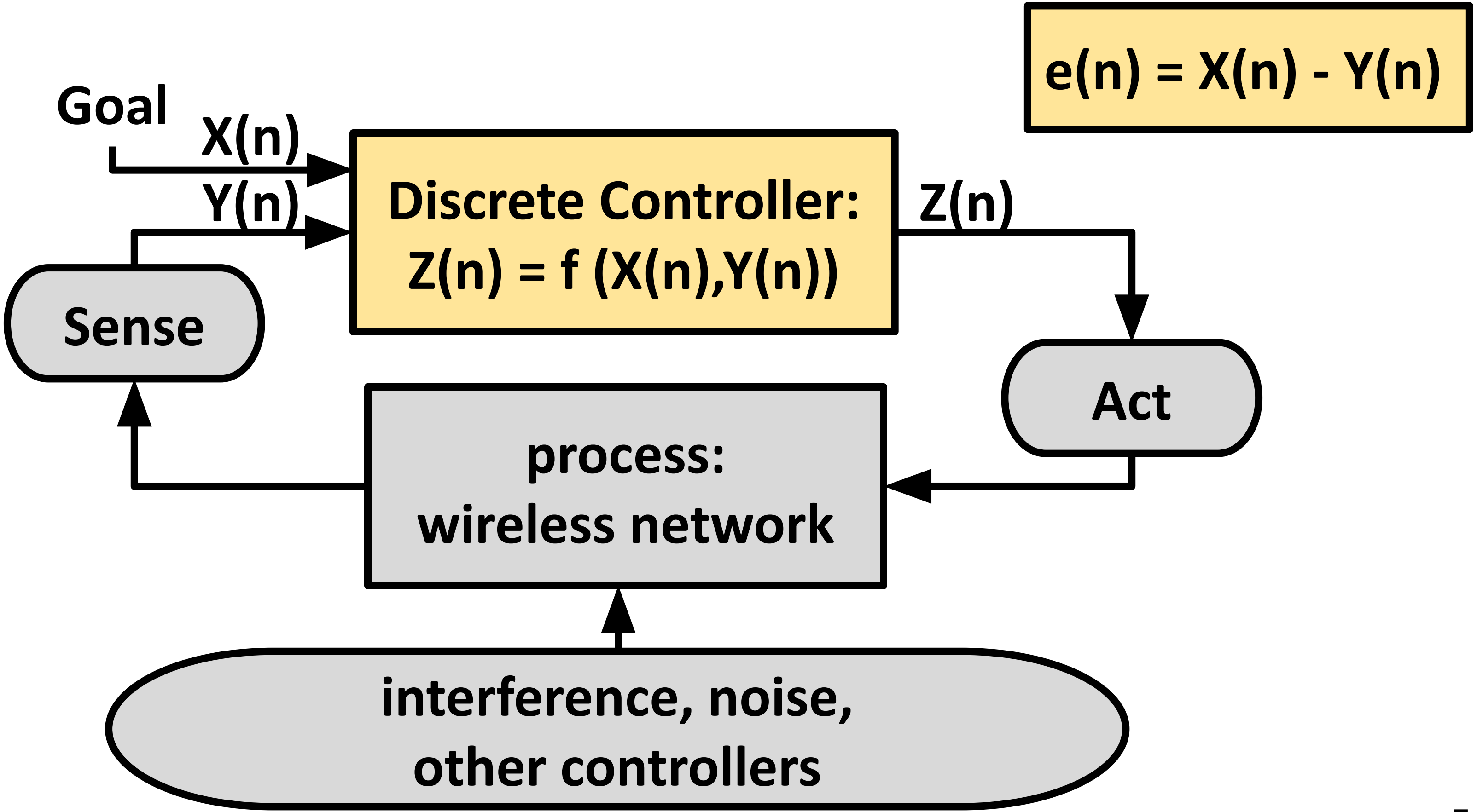
error e(n) = target X(n) - Y(n)

Z (n=1,2,3,...)

Reflexes and Control

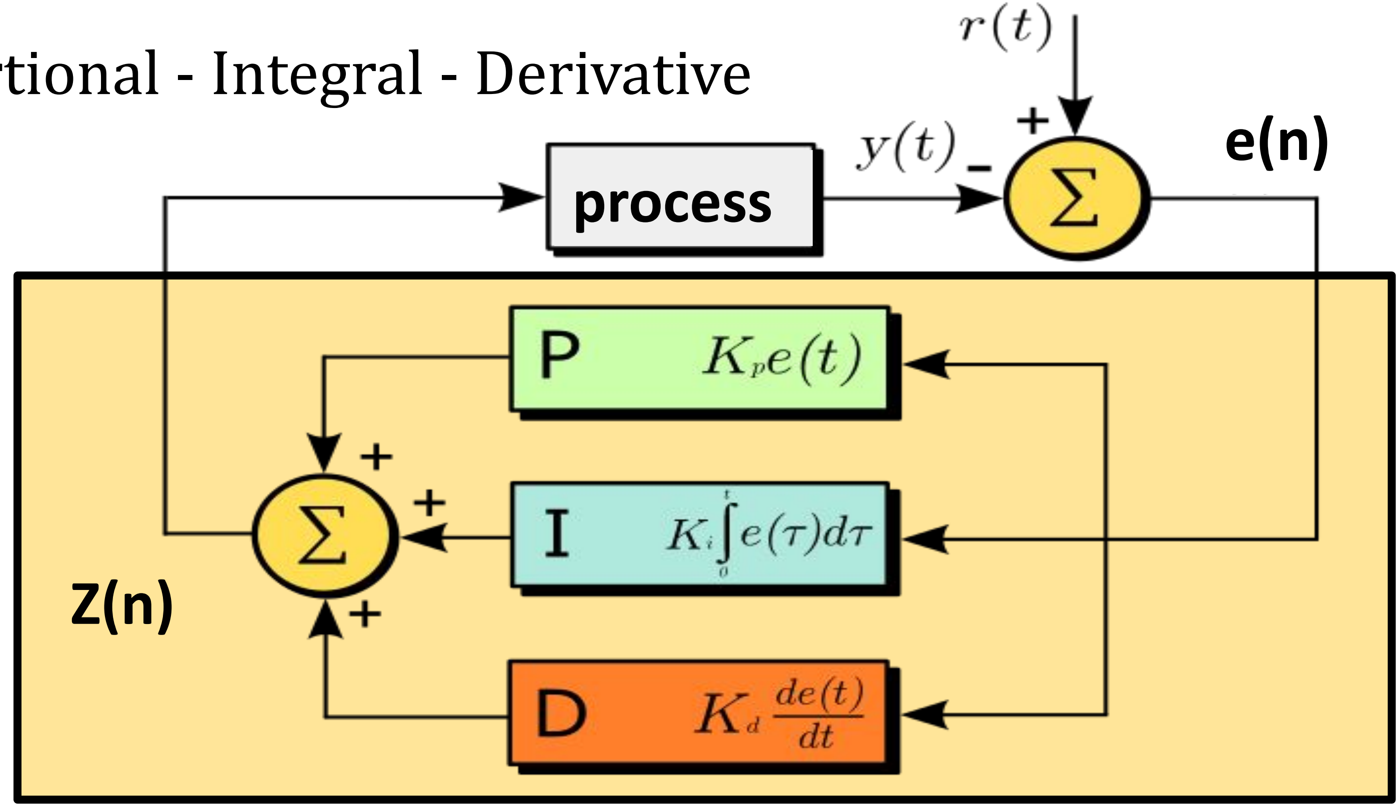
- Reflexes are (automatic) reactions without conscious control
    - Mapping from input to output
    - No decision making, just reaction
    - Might involve buffering of inputs and outputs (storage)
- Open-loop reflexes issue commands without feedback
- Closed-loop control processes use feedback to bring a system to a defined set-point and keep it there (if possible)
- Nonlinear systems are approximated to linear systems
- If multiple control processes attempt to control the same system, complicated competition scenarios might occur (game theory)

(Discrete Time) Control Systems



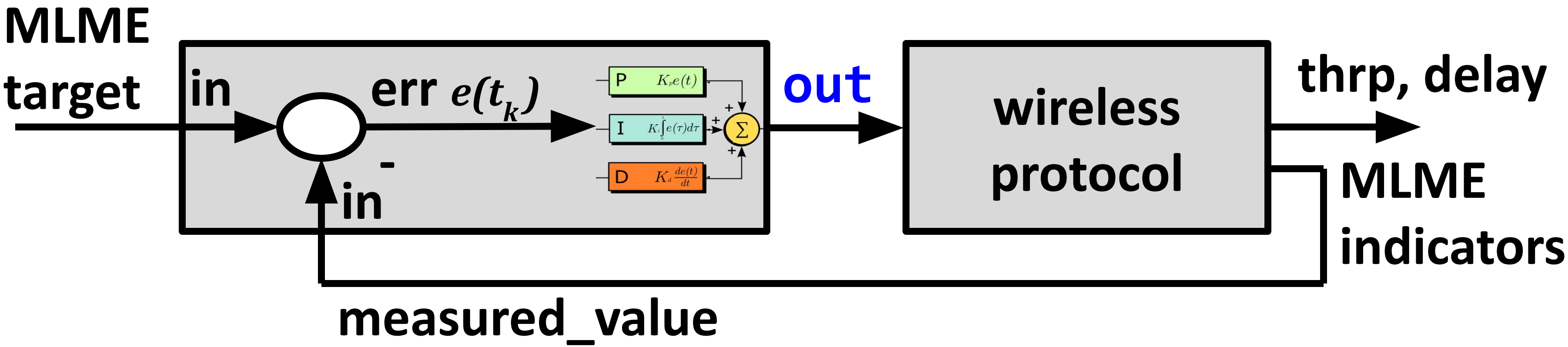
PID Controller

Proportional - Integral - Derivative



"TravTigerEE - Own work. Licensed under CC BY-SA 3.0 via Commons - wikimedia.org/wiki/File:PID_en_updated_feedback.svg#/media/File:PID_en_updated_feedback.svg

PID Controller for Mobile Computing Algorithm



$$\int_0^{t_k} e(\tau)\,d\tau = \sum_{i=1}^{k} e(t_i)\Delta t$$

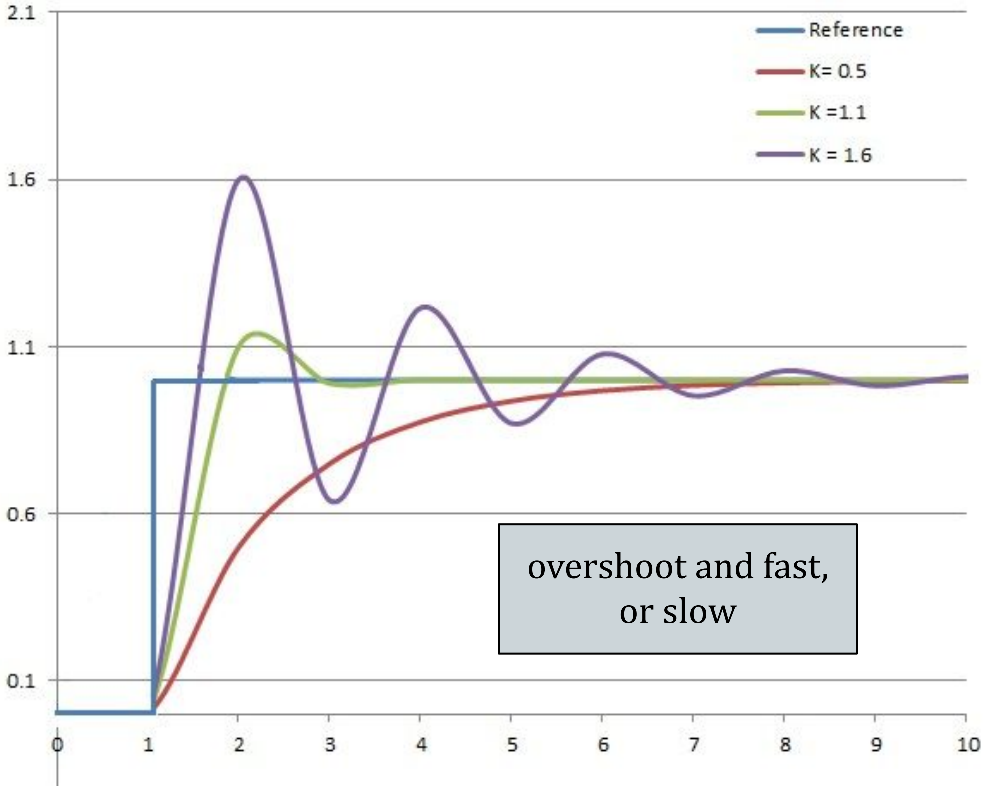
$$\frac{de(t_k)}{dt} = \frac{e(t_k) - e(t_{k-1})}{\Delta t}$$

PID Pseudo Code (Continuous Time)

```
previous_error = 0
integral = 0
start:
   error =  MAC_target - measured_value
   integral = integral + error * dt
   derivative = (error - previous_error) / dt
   out = Kp*error + Ki*integral + Kd*derivative
   previous_error = error
   wait(dt)
goto start
```

Proportional Gain Kp

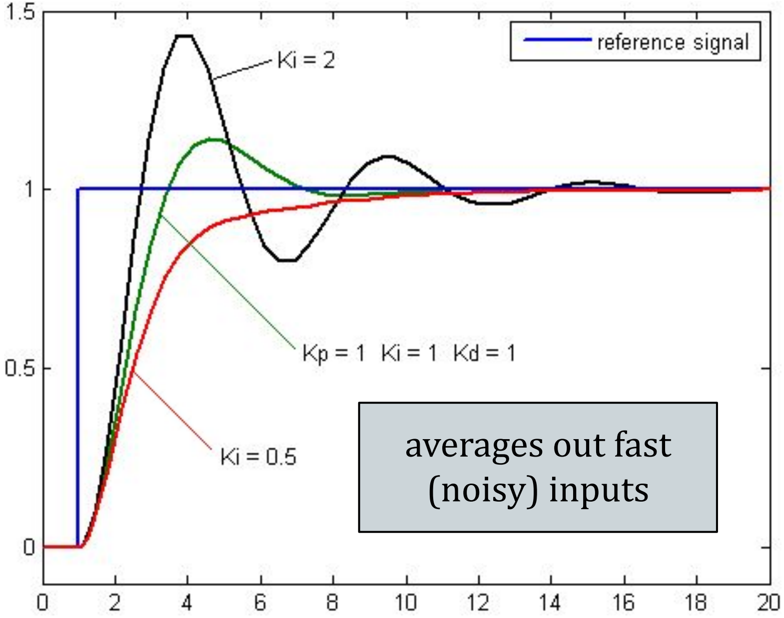
- Kp is proportional to the current error value
- Typical plot of measured value Y(n) for 3 values of Kp
  - Ki and Kd remain constant



https://en.wikipedia.org/wiki/PID_controller#/media/File:PID_varyingP.jpg

Integral Gain Ki

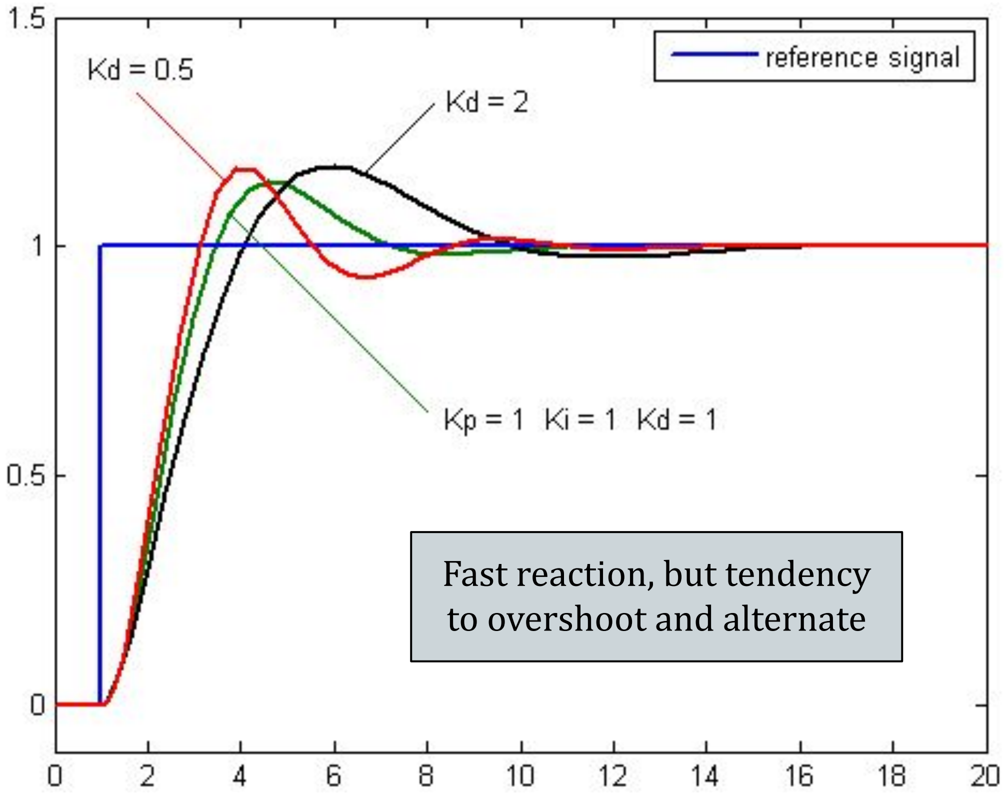
- Integral control is used to add long-term precision to a control loop.
- Example plot of measured value over time, for three values of Ki
- (Kp and Kd constant)
- It is almost always used in conjunction with proportional control.



https://en.wikipedia.org/wiki/PID_controller#/media/File:Change_with_Ki.png

Derivative Gain Kd

- Plot of measured value over time, for three values of Kd
- (Kp and Ki constant)



Fast reaction, but tendency to overshoot and alternate

https://en.wikipedia.org/wiki/PID_controller#/media/File:Change_with_Kd.png

Intuitive Understanding of the Gains

- Kp determines how fast the controller tracks the error indicator
    - The system can get unstable with too large gains.
- Kd enables fast reaction on error changes, and might be helpful in case of delayed measurements (lagged sensor information).
    - However, it might amplify noise, which can be addressed with low pass filtering of the measured data.
- Ki can be used to remove the proportional offset.
    - It might introduce either oscillations, or error accumulations.

Controller Quality and Stability

- How responsive is the controller to changes in the set-point?
- How far does the system overshoot?
- How long does it take to settle down to an acceptable error level?
  - Does it settle down or does it oscillate?
- Remark: Slowing down transitions between set-points (change in goals) can be desirable when controlling wireless networks.
  - Dynamics might lead to instability.

Sampling Rate (Rate = 1 / Time)

- Low control performance if sampling rate is too low
  - because of the added delay of the sampling
- Too high sampling rate will create problems
  - noise in the differentiator
  - overflow of the integrator
- Rule of thumb for digital control systems:
  Sample time should be between 1/10th and 1/100th of the desired system settling time

Noise

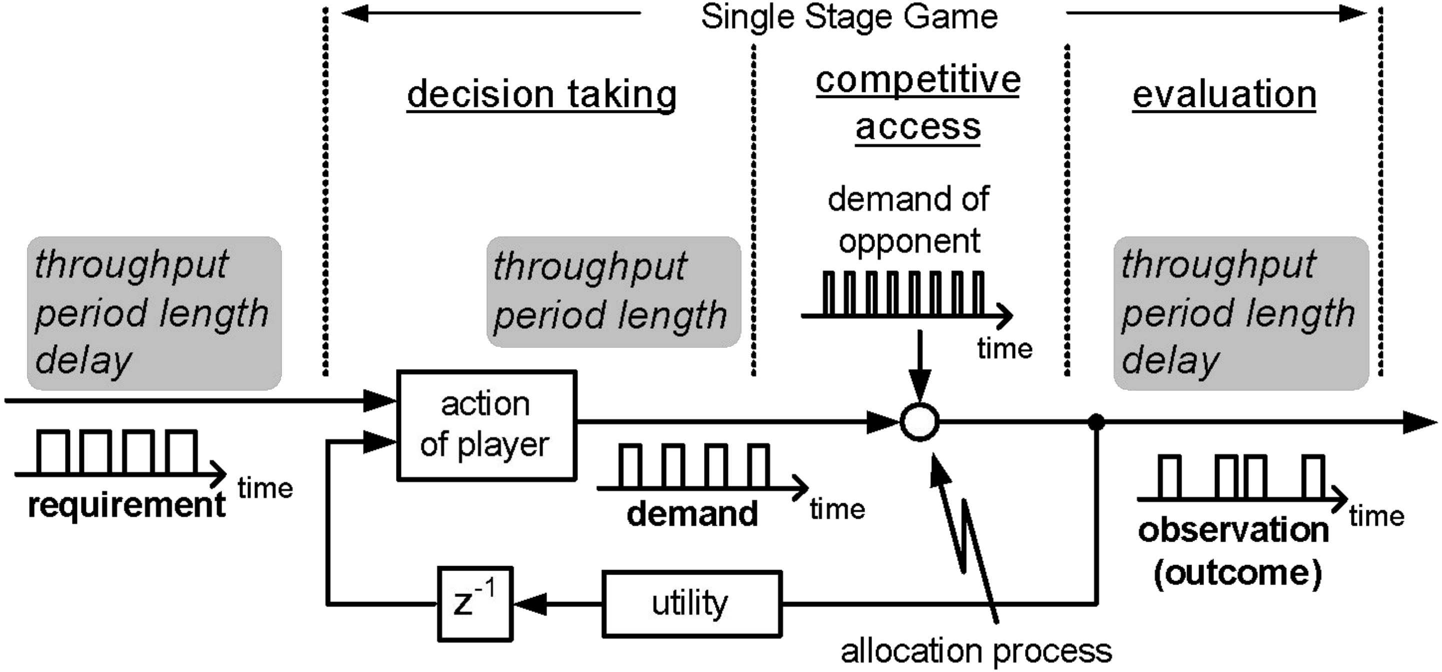
- Sources of noise are uneven and too short sampling times
- Differential control suffers from noise problems
  - Noise is usually spread evenly across the frequency spectrum
  - Control commands are at lower frequencies
  - Differential control enhances high frequency signals and the noise energy
- Proportional control passes noise energy through
- Integral control averages the noise input signal over time, which tends to reduce it

PID References

1. Aidan O'Dwyer. Handbook of PI and PID controller tuning rules. London: Imperial College Press, 3rd edition, 2009. Online-resource available in ETH Zurich library.
2. Wikipedia: https://en.wikipedia.org/wiki/PID_controller#References
3. Intuitive Description: https://www.youtube.com/watch?v=XfAt6hNV8XM
4. Jemula802 controller: https://bitbucket.org/lfield/jemula802/src/9d53667d119f/src/layer2_802Algorithms

Spectrum Sharing Games

- Repetitive competitive access to shared spectrum
- Observed QoS as outcomes of a single stage game

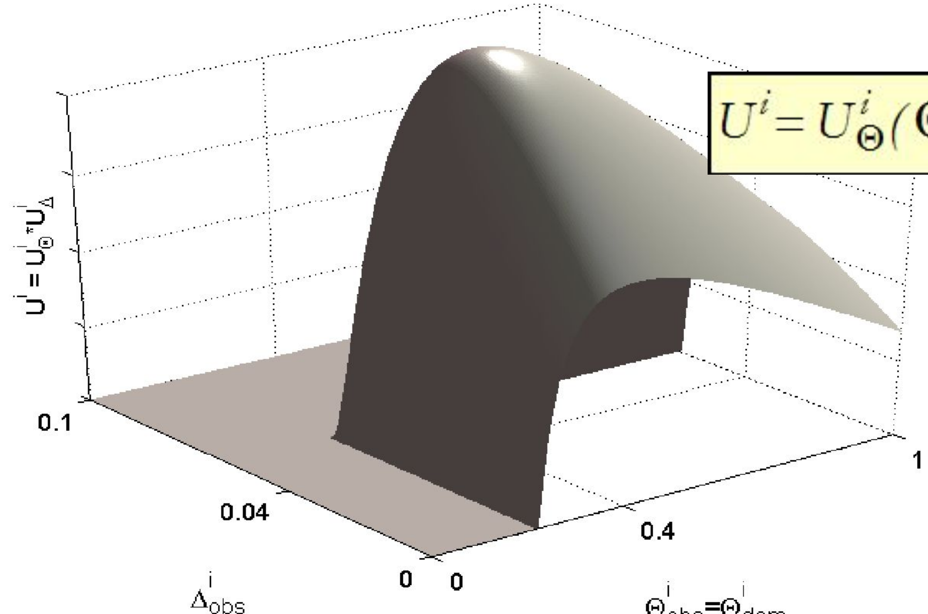


Games Theory in Mobile Computing

- Game concepts can help to analyze a competition scenario
  - Rational behavior and predictability
  - Self interest (payoff and utility function)
  - Nash Equilibrium
  - Pareto Efficiency
  - Cooperation and Fairness
- In network systems, it is not necessarily the most desirable approach to try to achieve fairness among players.
- Networks are optimized for multiple indicators, not fairness:
  - Examples: service support, regulatory requirements, infrastructure & operational cost, energy consumption, spectrum efficiency, complexity, revenue, reliability

Utility Function

- Player (index "***i***") attempts to meet its requirement
  - Therefore, players attempt to maximize the observed payoff (outcome)
  - The current payoff is high when the observation meets (or exceeds) the utility



$$U^i = U^i_\Theta(\Theta^i_{dem}, \Theta^i_{obs}, \Theta^i_{req}) \cdot U^i_\Delta(\Delta^i_{obs}, \Delta^i_{req}), \quad U^i \in \mathbb{R}^+$$

demand = f (t)

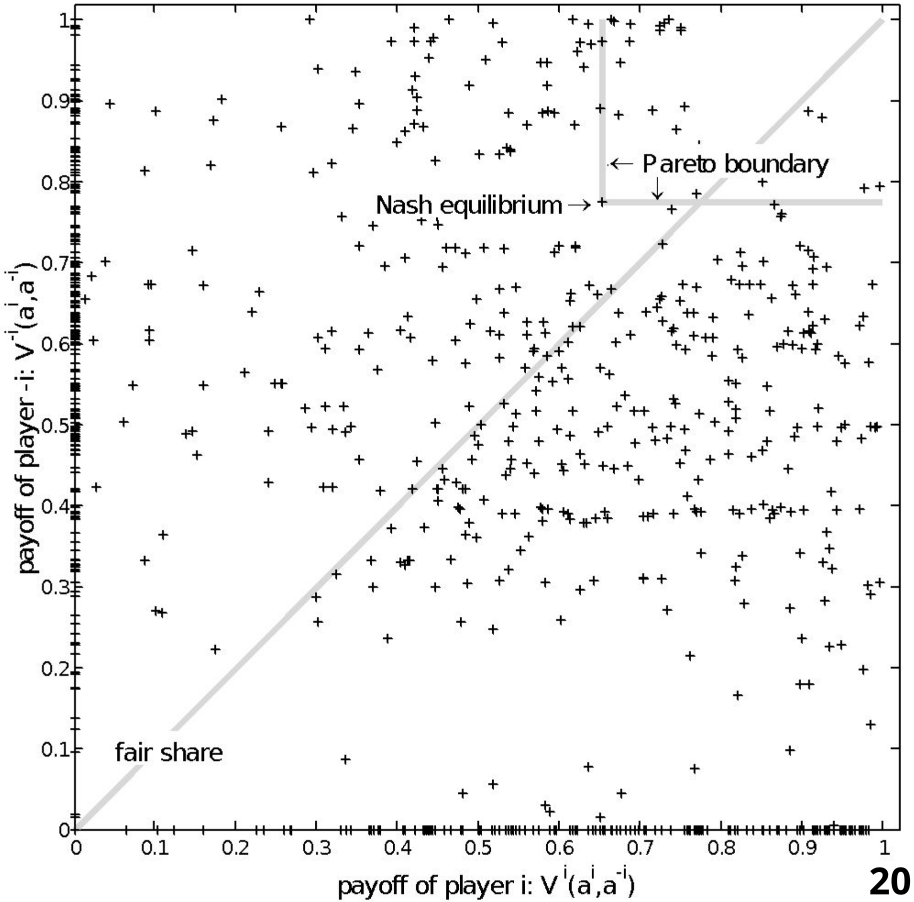
requirement = time invariant

observation = f (n)

throughput **Θ** and delay **Δ**

Pareto Efficiency and Bargaining Domain

- Players that make rational decisions might lead an repeated interaction into a Nash Equilibrium, NE
    - An action profile that is not changed by one player alone, once achieved
- Action profiles with higher payoffs may exist
- If not, then the NE is Pareto efficient



Interaction in a Single Stage Game [source]

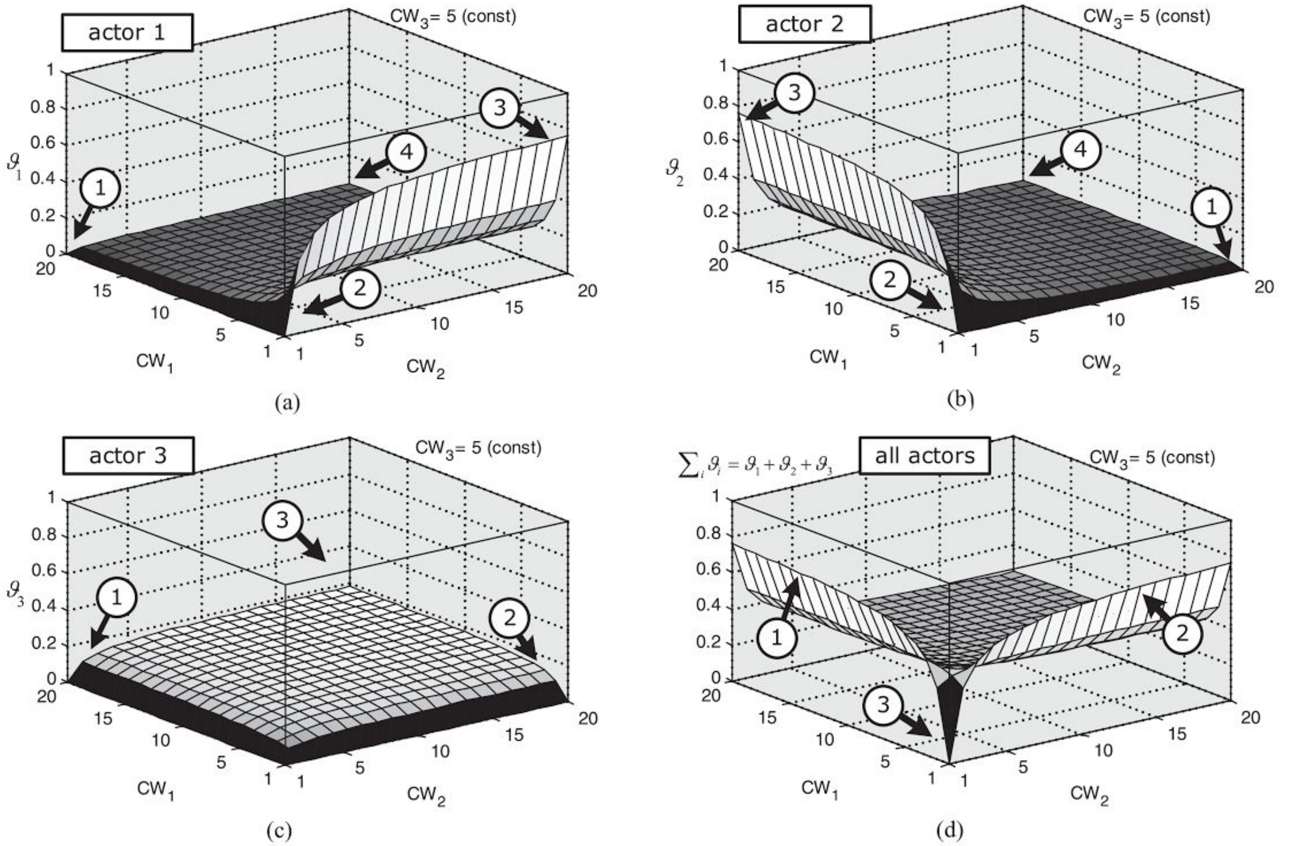
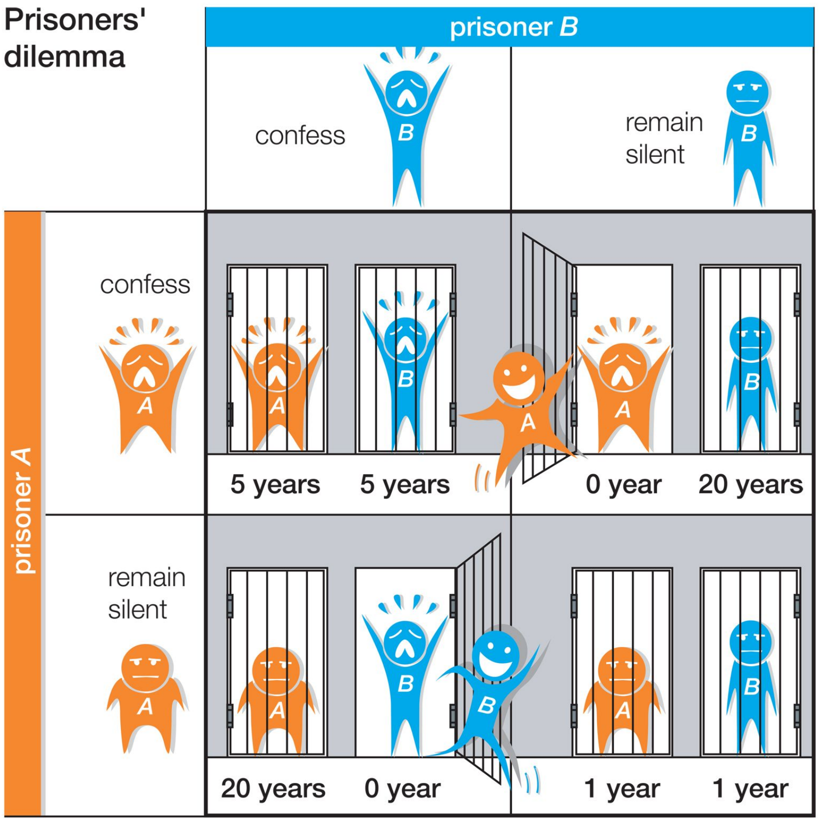


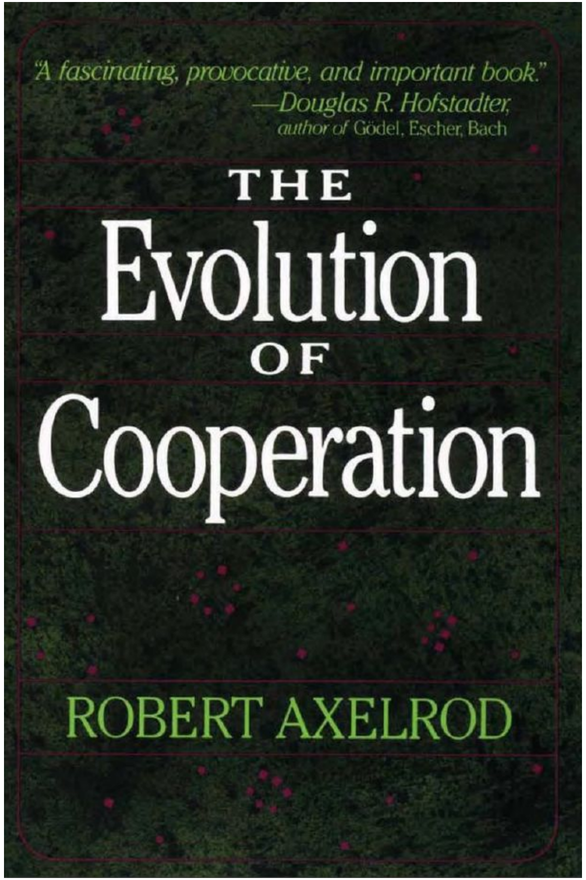
Figure 2. Observed shares of capacity ϑ_i and $\Sigma\vartheta_i$ for the three actors, with varying contention window sizes for actor 1 and actor 2. (a) observed share of actor 1; (b) observed share of actor 1; (c) observed share of actor 3 with CW_3 = const = 5; (d) sum of all actor's shares.

Multi-Stage Games and The Evolution of Cooperation

- Repeated interaction of rational players might end in long-term cooperation.
    - Even with pure self-interest of players.
- A “non-cooperative” game is a game where cooperation is achieved through self-interest, not through bargaining.
- Cooperation might not lead to the most efficient outcome, but often to a balanced result.



The Evolution of Cooperation [Axelrod, Michor & Nowak]



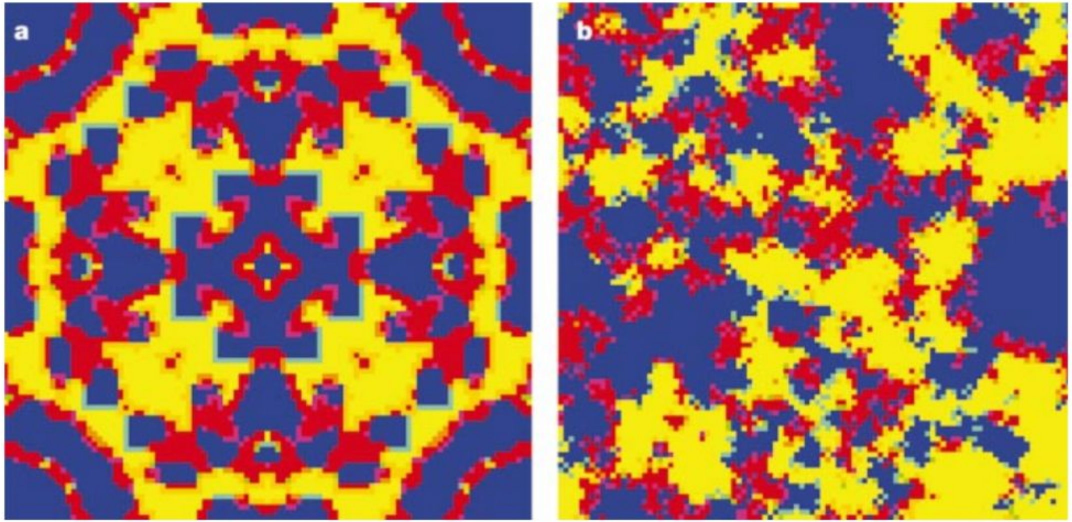


Figure 1 **Evolutionary kaleidoscope.** a, **Players in a public-goods game are represented as cells distributed spatially on a grid. Cooperators are shown in blue, defectors in red and loners in yellow. Players may change their strategy in each round of the game. For this simulation, all strategy updates are synchronous. Intermediate colours indicate players who have updated their strategies in the last round of the game.** b, **Another simulation shows the effects of asynchronous strategy updating and small amounts of noise in the system. In both cases, there is coexistence between cooperators, defectors and loners. Szabó and Hauert[5] show that the dynamics of such systems have much in common with models in statistical physics.**

NATURE | VOL 419 | 17 OCTOBER 2002 | www.nature.com/nature

Types of Social Actions

- Weber’s basic classification defines four types of motivation for social action
- From Max Weber: Wirtschaft Und Gesellschaft. 2, Verm. Aufl. ed. Vol. Abt. 3, Ed. 2. Tübingen: Mohr, 1925. Print. Grundriss Der Sozialökonomik
  - Affective social action (based on emotional state)
  - Traditional social action (guided by custom)
  - Technocratic rational social action ("zweckrational")
  - Value-oriented rational social action ("wertrational")
- Value-oriented actors limit need for regulation

References

- A collection of relevant publications can be found here.

Wireless Networking and Mobile Computing

Course ID: 252-0293

1. Introduction

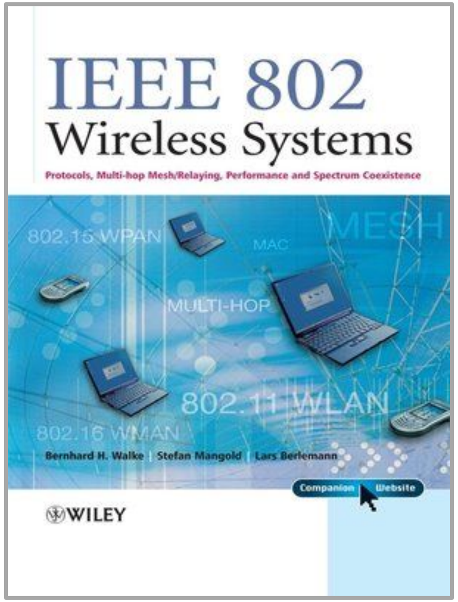
Stefan Mangold

Lecturer: Stefan Mangold

- 2020 … today: Ypsomed AG, Burgdorf BE (MedTech, Wireless)
- 2015 … today: Lovefield Wireless GmbH, Berne, (Wireless)
- 2009 … 2015: Disney Research, Zurich (Toys, Wireless)
- 2005 … 2009: Swisscom, Switzerland (Telecommunications)
- 2003 … 2005: Philips Research, USA (Wireless, Wi-Fi)
- 2003: Graduated in E.Eng. from RWTH Aachen, Germany

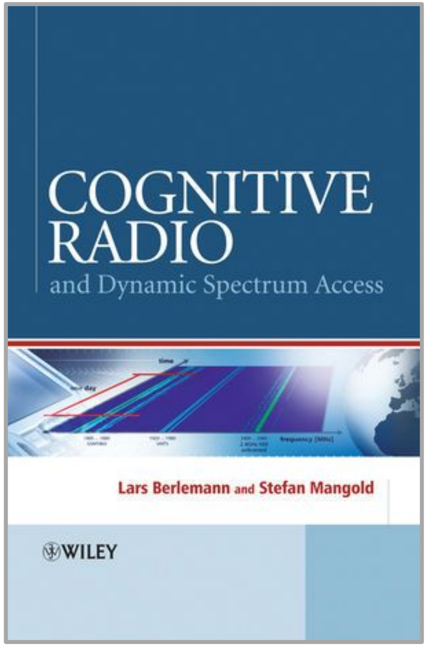
Textbook (1/2)

- Bernhard Walke, Stefan Mangold, Lars Berlemann (2006) IEEE 802 Wireless Systems – Protocols, Multi-Hop Mesh / Relaying, Performance and Spectrum Coexistence
  - wiley.com/WileyCDA
  - November 2006, 402 pages. John Wiley & Sons
- Available at ETH library



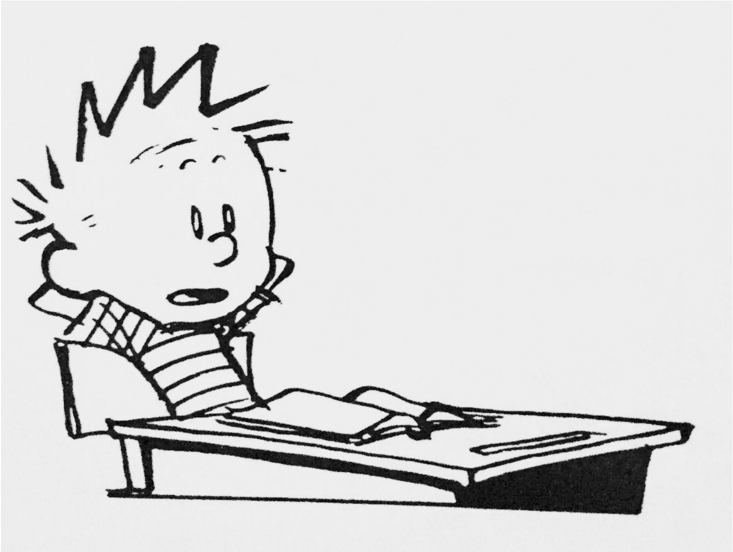
Textbook (2/2)

- Lars Berlemann, Stefan Mangold (2009)
  Cognitive Radio and Dynamic Spectrum Access
  - wiley-vch.de/publish/en/books
  - January 2009, 256 pages. John Wiley & Sons
- Available at ETH library



For Efficient Participation

- Take the course seriously: interact, ask questions, remain persistent
- (Show up and) participate
- Take the homework assignments very seriously
- Focus on the objectives of the assignments, and start early



- Criticize what can be improved: give constructive feedback
- Make appointments with me when needed (remote)

Simulator

- System emulation software, available from Bitbucket
- JAVA 10 required
- Eclipse SDK recommended
- Bitbucket: Jemula802++ and Jemula++
- Other helpful tools: Scripting (bash / Python), Matlab, GNU Octave

Course Objectives

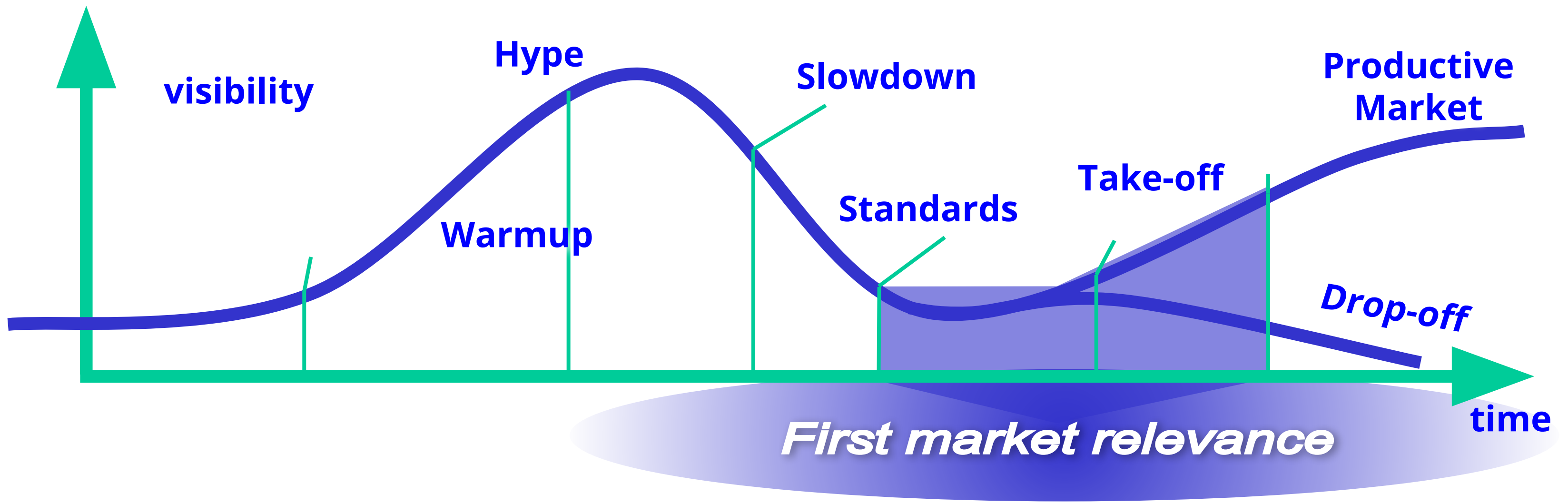
- Understand the basics of wireless communications
  - Including wireless propagation, frequencies, modulation and coding
- Get introduced to IEEE 802 wireless standards
  - with focus on IEEE 802.11 Wi-Fi and Radio Spectrum Management
- Understand free space optical communication
  - Visible Light Communication
- Get industrial insights (Telecom, Entertainment, MedTech)
- Understand cellular networks such as LTE and 5G
- Understand standards, protocols, algorithms, spectrum regulation

Course Outline

1. Introduction
2. Wireless Communication Basics
3. IEEE 802.11 Wireless LAN (Wi-Fi)
4. IEEE 802.15 Wireless PAN (ZigBee & Bluetooth)
5. Mobile Computing Algorithm Basics: Control and Game Theory
6. Visible Light Communication
7. Audio Communication
8. Cellular Networking Basics (LTE, 5G, Internet-of-Things)
9. Mobile Computing for Automated Medicine Delivery
10. Cognitive Radio, Delay Tolerant Networking, Radio Spectrum Sharing

Life-Cycle of Technology

- In this course we will look at technology that …
  - … took off towards successful markets → Wi-Fi, 60GHz
  - … or, is at its hype → Internet of Things, 5G
  - … or, is warming up → Visible Light Communication, Wi-Fi 6, Bluetooth 5, 6G



Wi-Fi and 3GPP Standards

("G"=Generation)

- Wi-Fi: wireless LAN
  - 1999: 802.11b products (11 Mb/s)
  - 2000: Wi-Fi certification program
  - 2001: 802.11a products (54 Mb/s)
  - 2005: 802.11a/b/g products
  - 2005: 802.11e QoS
  - 2008: 802.11n MIMO
  - 2010: 802.11af TV White Space
  - 2010: 802.11ad 60GHz
  - 2016: 802.11ah IoT
  - 2017: 80211ax Multi-User MIMO
  - 2019: Wi-Fi 6
- 3GPP: Cellular networks
  - 1G (early 1980) analog cellular
  - 2G (early 1990) digital cellular
  - DECT & PHS, GSM T/FDMA
  - GPRS & EDGE
  - 3G UMTS 384kb/s
  - HSDPA/HSUPA 1800/800kb/s
  - 4G LTE: End-to-end IP
  - Unlicensed LTE (LTE-U)
  - Internet-of-Things, LoRa, Sigfox
  - 5G
  - Beyond 5G, edge comp., verticals

Please Take Note of the Terminology

- 1 Mb/s = 1 Megabit per second
  - not: Mbit/s ... Mbits/s ... Mbps
- 1 MB/s = 1 Megabyte per second
  - not: MByte/s ... MBytes/s ... MBps ...
- same for kilo, Giga, …
  - kilobyte = kB
  - kilobit = kb
  - Gigabit = Gb
- 1 second = 1 s
  - not: sec ... secs

ITU-IMT Wireless System Framework

- ITU = organization “International Telecommunications Unit”
- IMT = standard family “International Mobile Telecommunication”
- IMT-2000 (UMTS / EDGE / DECT / …)
  - 144 kb/s @high mobility, 2048 kb/s @low mobility
  - deployment started in 2000
- IMT-Advanced
  - 100 Mb/s @high mobility, 1 Gb/s @low mobility
  - LTE and 802.11 standards
- IMT-2020
  - 3GPP 5th Generation

From Research to Commercialization

- Academic and industry research
- Standardization (IEEE, 3GPP, ETSI…)
- Certification (Wi-Fi Alliance, WiMAX forum …)
- Spectrum regulation (FCC, BAKOM, OFCOM, ERO, ITU…)
- Manufacturing and development of devices (chipmakers)
- Deployment (roll-out, network operators, consumer market)

5 … 20 Years Process

Standardization

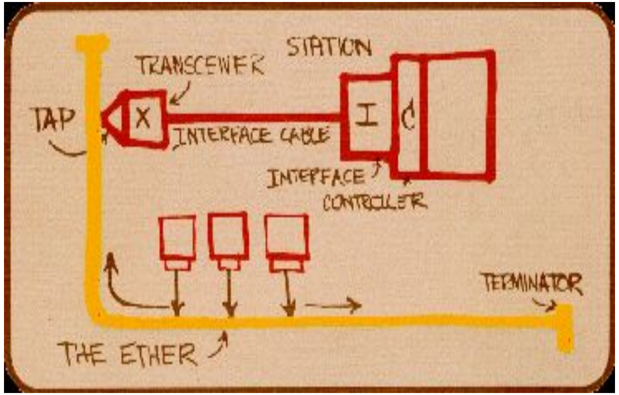
- Standardization enables competing commercial and industrial players to develop new technology together
  - to achieve interoperability, which increases value of product
  - often, used to shorten the time-to-market
- Relevant standardization bodies
  - Institute of Electrical and Electronics Engineers (IEEE)
  - 3rd Generation Partnership Project (3GPP)
  - European Telecommunications Standards Institute (ETSI)
- International Telecommunication Union (ITU)
  - defines global mobile standard → IMT-2000 family

The IEEE

- Institute of Electrical and Electronics Engineers
- Non-profit organization, >350k members in >150 countries
- Organization for various industrial sectors
  - Aerospace
  - Biomedical
  - Consumer electronics
  - Computers, Telecommunication
  - Electric power
- Academic publication platform
  - publishes transactions, journals and magazines
  - organizer of conferences

The Standardization Project IEEE 802

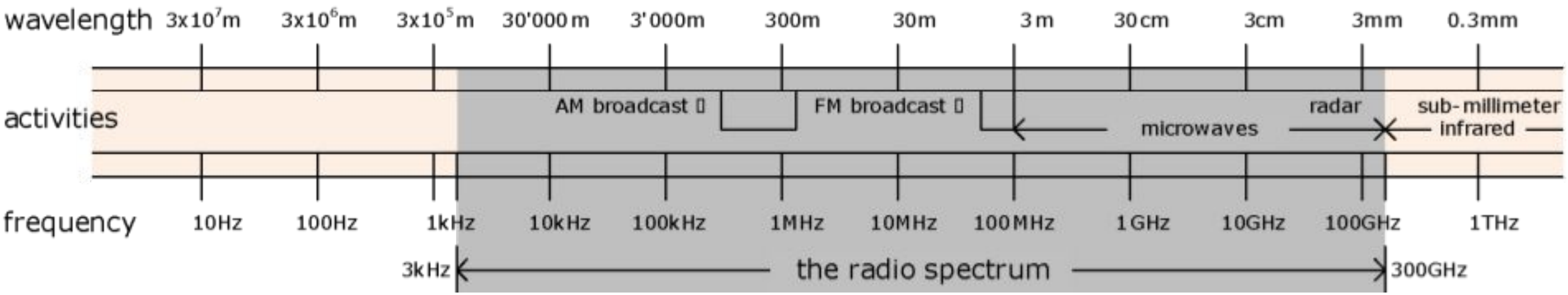
- LAN/MAN Standards Committee (LMSC)
- Focus is mainly on lower two of the OSI-ISO layers
  - Layer 1 (PHY) and Layer 2 (DLC)
- Organized in Working Groups (WGs)
  - 802.1 Higher Layer Local Area Network (LAN)
  - 802.3 Ethernet
  - **802.11 Wireless Local Area Networks (WLAN)**
  - **802.15 Wireless Personal Area Networks (WPAN)**
  - ~~802.16 Wireless Metropolitan Area Networks (WMAN)~~ (no more relevant)
  - **802.18 Radio Regulatory Technical Advisory Group (TAG)**
  - 802.22 Wireless Regional Area Networks (WRAN)



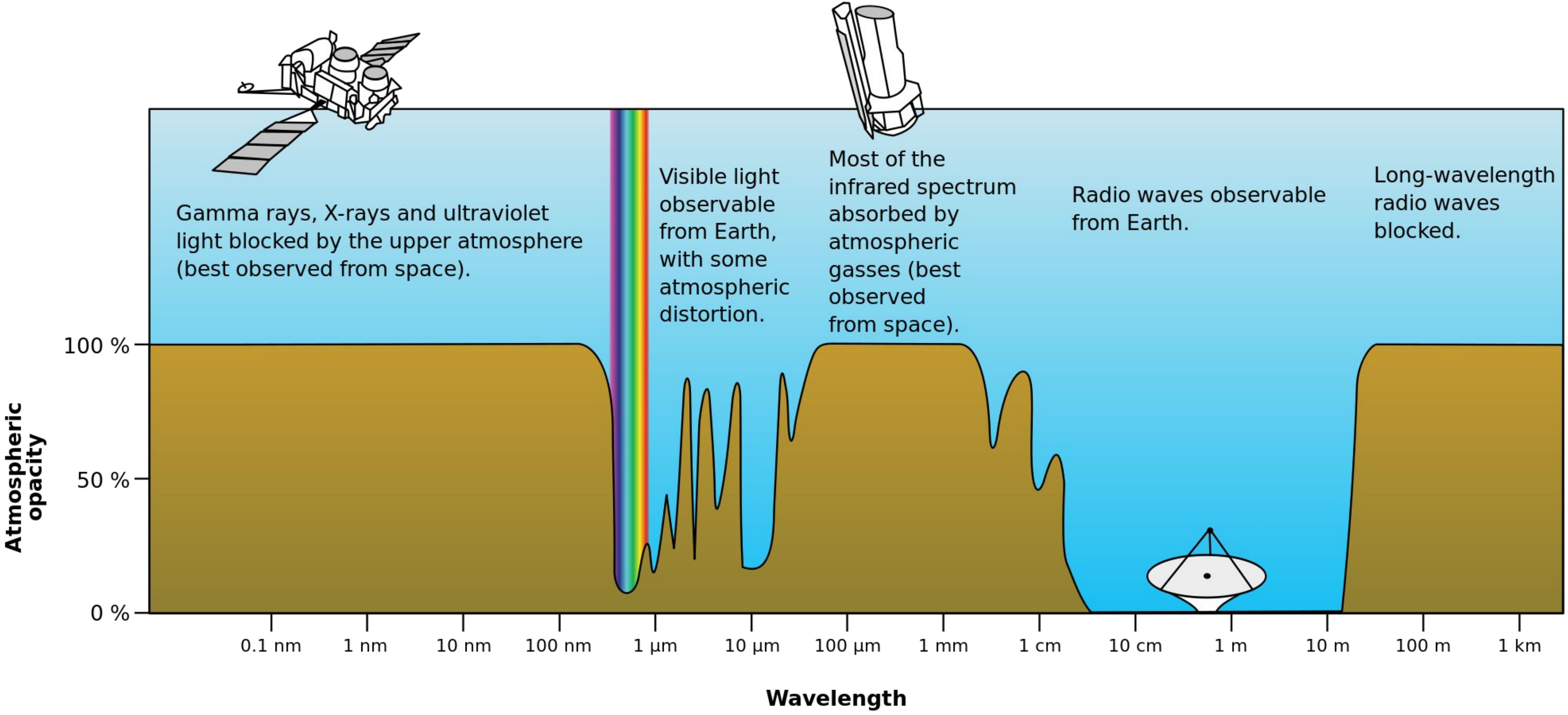
Source: Robert M. Metcalfe, 1976

Spectrum Regulation

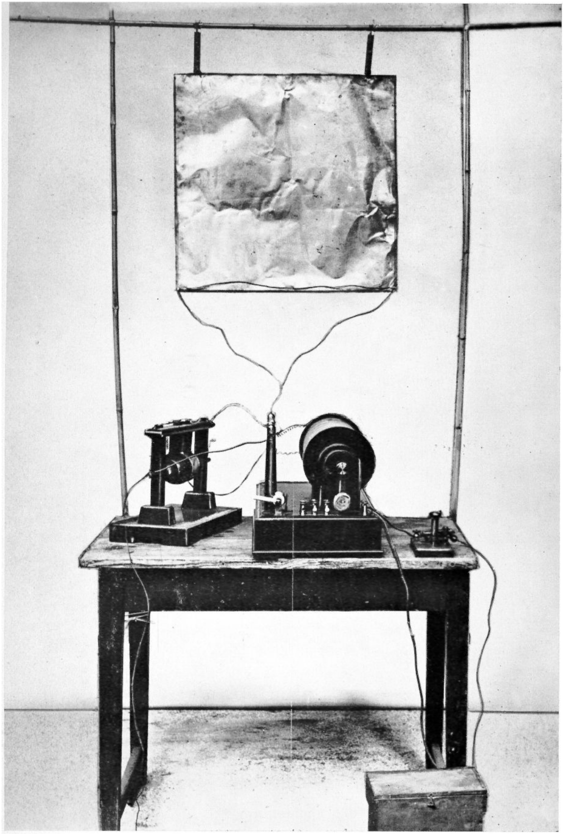
- Electromagnetic frequencies between 3 kHz and 300 GHz are commonly referred to as “radio” frequencies
- Frequency (f) and wavelength (ƛ) are inversely proportional to each other. The wave with the highest frequency has the shortest wavelength: **ƛ = c / f**



Atmospheric Opacity



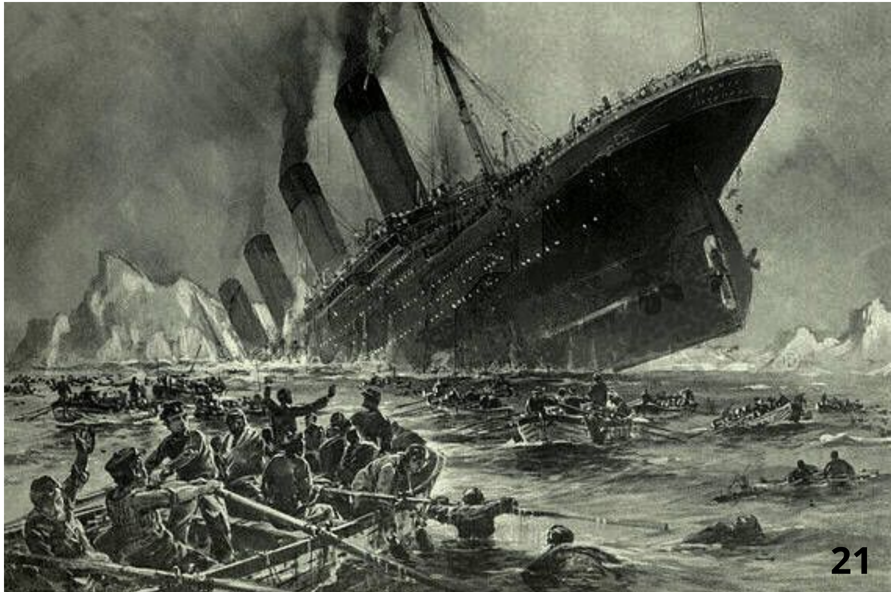
Guglielmo Marconi 1895, Bologna



https://upload.wikimedia.org/wikipedia/commons/e/e2/Post_Office_Engineers.jpg
https://en.wikipedia.org/wiki/Guglielmo_Marconi#/media/File:Marconi's_first_radio_transmitter.jpg

Radio Regulations

- Radio Regulations regulates <u>on law</u> radiocommunication services and the utilisation of radio frequencies
  - Determines how, where, when radio emissions are permitted
  - Provides spectrum access rights to licensees or unlicensed users
- 1912 Titanic tragedy
  - There was unreliable radio operation at the nearest ship, <u>it was not regulated</u>
  - The 1912 “Radio Act” was created as result of the sinking of the Titanic
  - International coordination, licensing of radio operators, a separate frequency for emergency calls



Regulatory Bodies (Government Agencies)

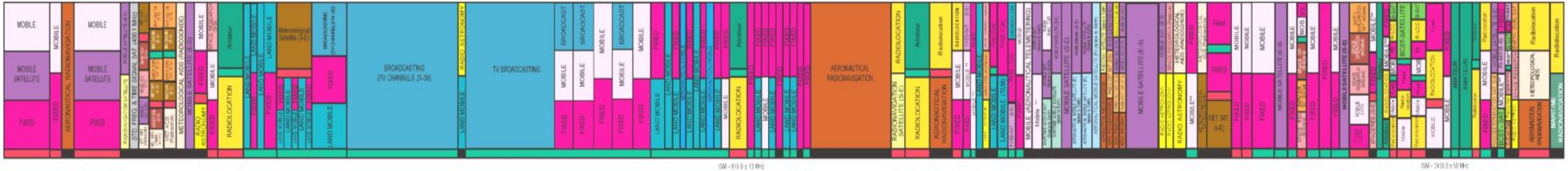
- Global
  - International Telecommunication Union (ITU)
- United States
  - National Telecommunications and Information Administration (NTIA): spectrum use by Federal Government
  - Federal Communications Commission (FCC): spectrum use by individuals, private companies and state and local government
- Europe
  - European Conference of Postal and Telecommunications Administrations
- Switzerland
  - Federal Office of Communications, OFCOM/BAKOM

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

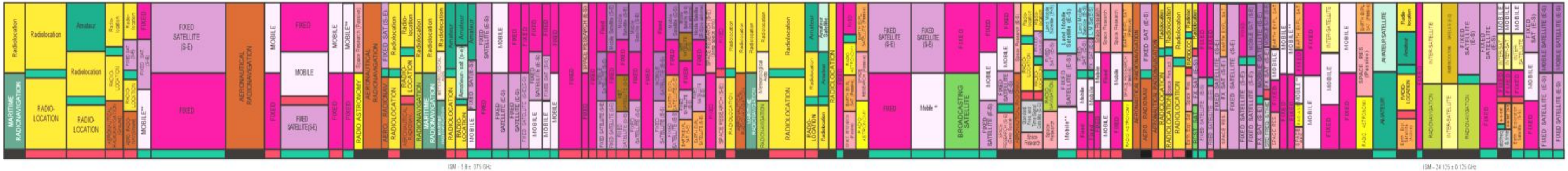
Radio Spectrum Allocation

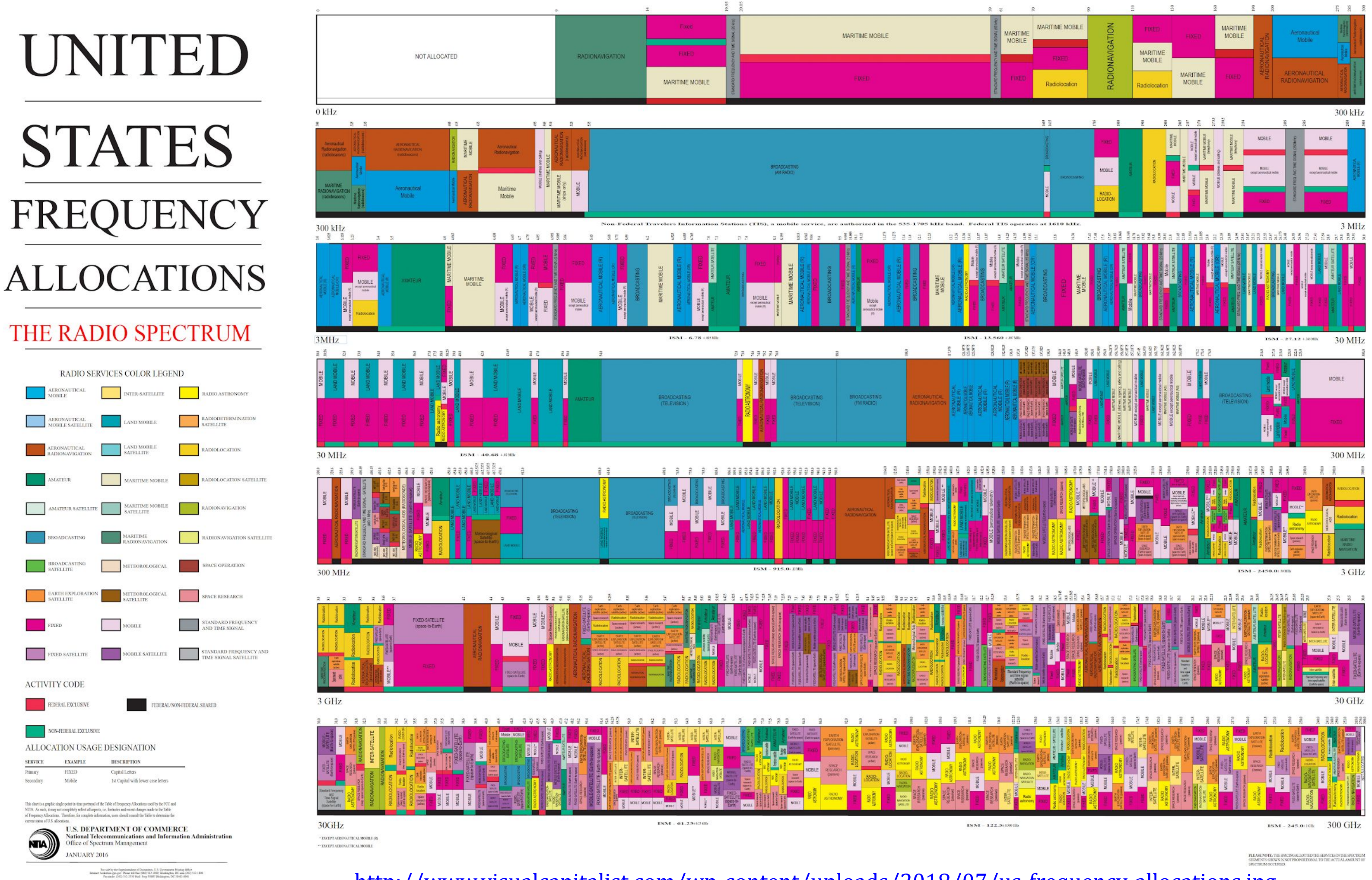
30 MHz … → **→ … 0.3 GHz**

0.3 GHz … → **→ … 3 GHz**



3 GHz … → **→ … 30 GHz**

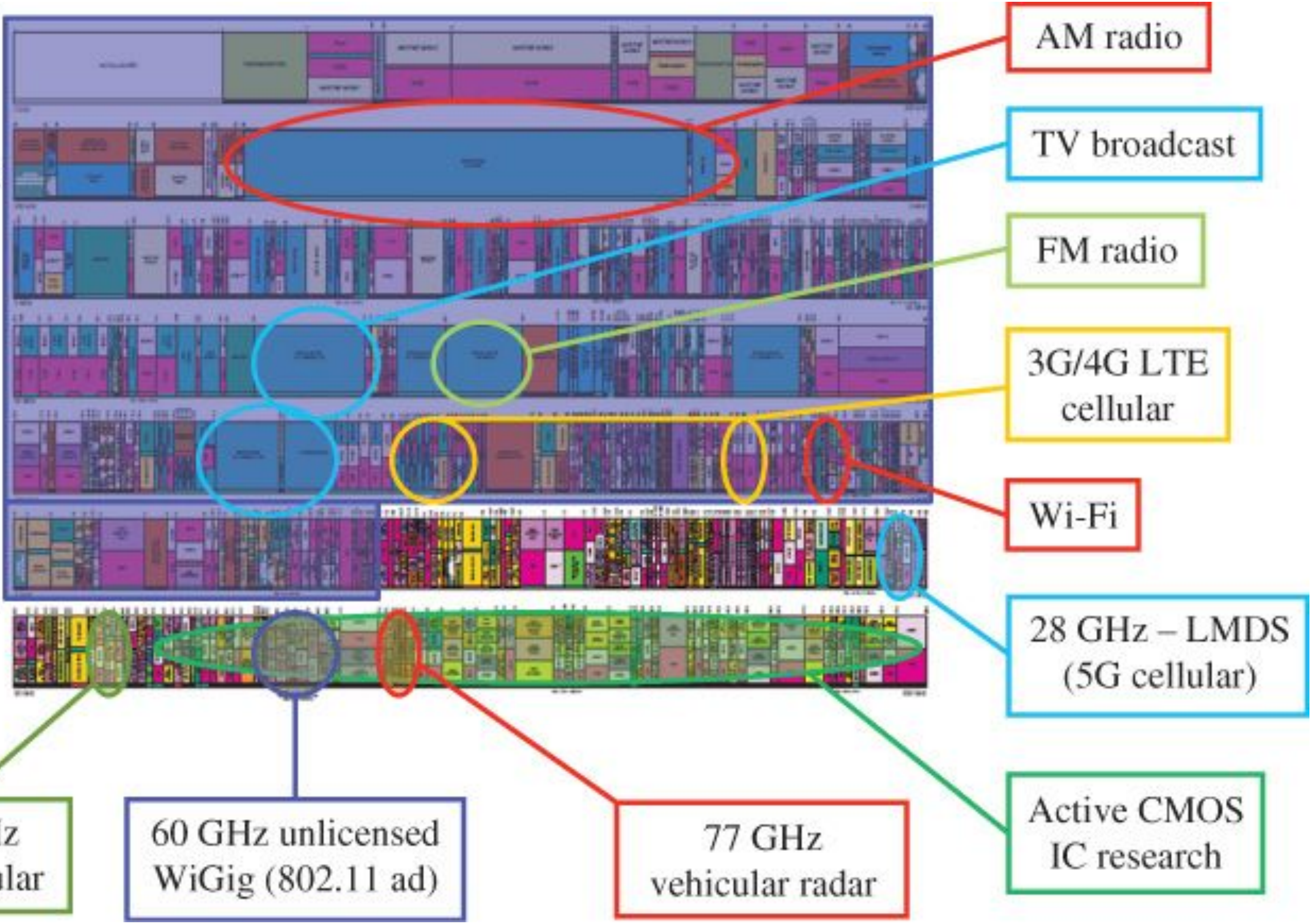




http://www.visualcapitalist.com/wp-content/uploads/2018/07/us-frequency-allocations.jpg

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

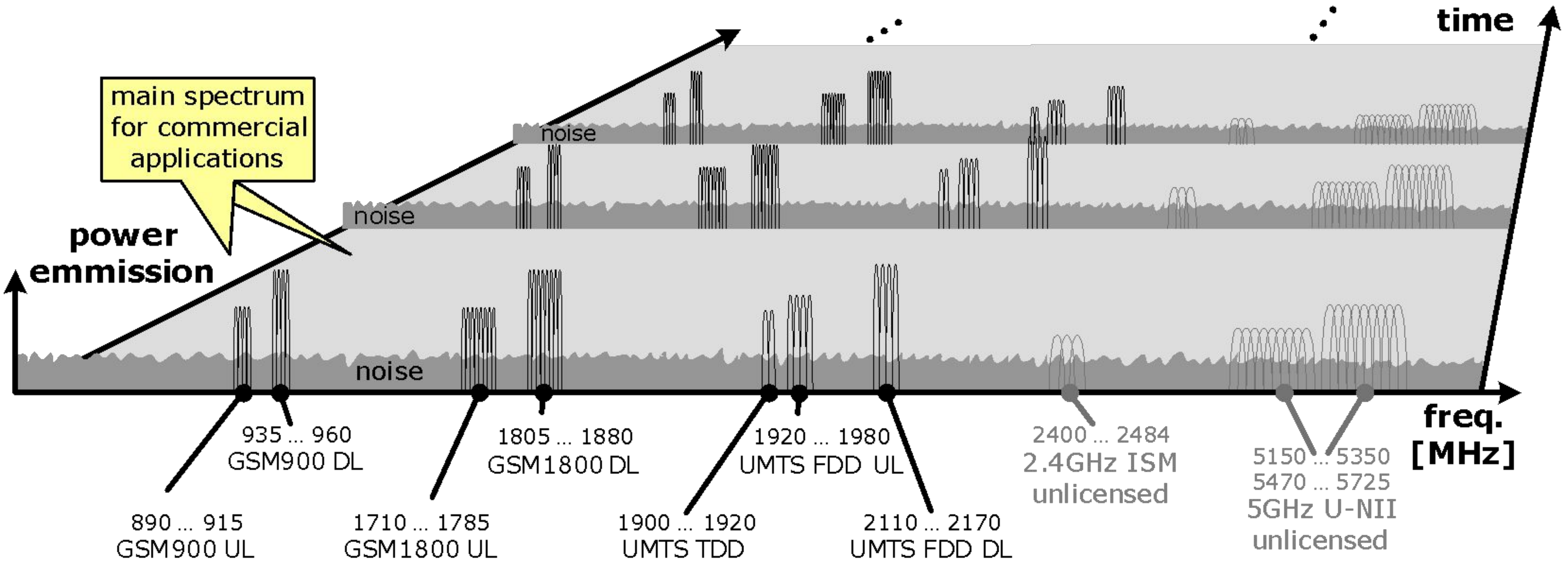


http://www.informit.com/articles/article.aspx?p=2249780

Licensed Radio Spectrum

- Most part of the radio spectrum is licensed
    - Exclusive access to spectrum, license holder pays a fee to own this privilege
    - No interference, reliable communication
- Often issued based on auctions
    - Licensing takes time and is complicated
    - The duration of licenses are typically up to decades (10-25 years)
    - Exclusive usage rights often leads to inefficient spectrum use (it is allocated, but not really used for commercial reasons)

Original Cellular Licensed Radio Spectrum



Unlicensed Radio Spectrum

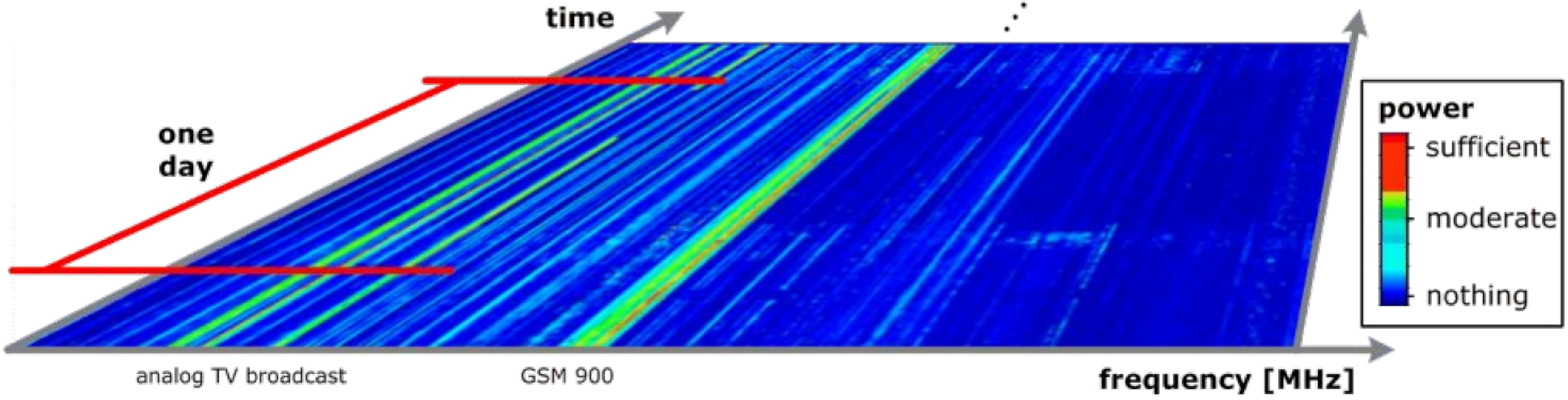
- Open access but controlled usage
  - Radio systems comply with technical rules of spectrum access, or standards, to keep the potential radio interference limited
  - Radio regulation does not impose detailed requirements about how to access spectrum, and what technology to use; instead stakeholders (users, industry) agree on common standards
- Limitations
  - The unlicensed spectrum can be overcrowded, neighbors might interfere with each other
  - The unlicensed spectrum is a shared resource: The quality of communication cannot be guaranteed

Unlicensed Radio Spectrum – FCC Part 15 Rules

- Technical rules under which a transmitter may be operated without requiring an individual license
- Three basic principles:
  - (i) listen before talk
  - (ii) when talking, make frequent pauses and listen again
  - (iii) do not talk too loud
- Typically, when detecting a busy channel, another unused frequency channel will be used
  - or the radio device has to wait until the channel has become idle again
- Rules do not require information exchange between devices

Secondary Radio Spectrum Usage

- Ultra Wideband (UWB), below noise
- White Space communication, above noise, opportunistic usage
- Cognitive Radio



Mobile Computing Algorithms – System Controllers

- Standards are mainly based on intellectual property
  - Developed in consensus between manufacturers and users
  - Stakeholders have often commercial interest
- Algorithms are not necessarily developed in consensus, or shared, but instead independently by each manufacturer
- Algorithms enable systems to outperform each other with or without violating standards and/or regulation
  - Ignoring (violating) standards: proprietary solutions when there is a larger market and no need for interoperability, for example in medical applications (wireless patient monitors), or wireless toys (devices communicate only with each other)
  - Ignoring (violating) regulation:E xceptional cases (defense scenarios)

Wireless Networking and Mobile Computing

2. Wireless Communication Basics

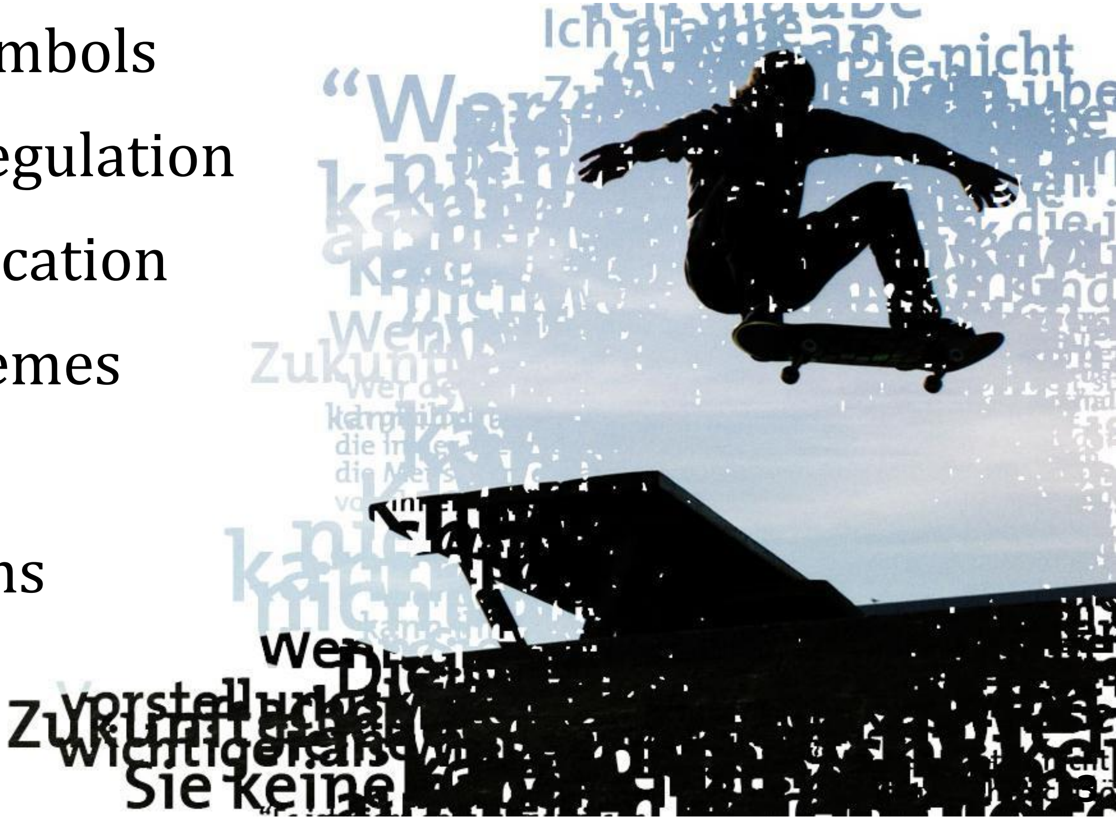
Stefan Mangold

Course Outline

1. Introduction
2. Wireless Communication Basics
3. IEEE 802.11 Wireless LAN (Wi-Fi)
4. IEEE 802.15 Wireless PAN (ZigBee & Bluetooth)
5. Mobile Computing Algorithm Basics: Control and Game Theory
6. Visible Light Communication
7. Audio Communication
8. Cellular Networking Basics (LTE, 5G, Internet-of-Things)
9. Mobile Computing for Automated Medicine Delivery
10. Cognitive Radio, Delay Tolerant Networking, Radio Spectrum Sharing

Overview of Topics

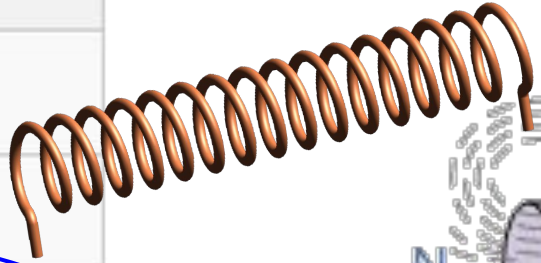
- Radio signal transmission, attenuation, multipath
- Digital modulation and symbols
- Channel bandwidth and regulation
- Optical vs. radio communication
- Duplex and multiplex schemes
- Forward error correction
- Automated retransmissions
- Slotted ALOHA, CSMA

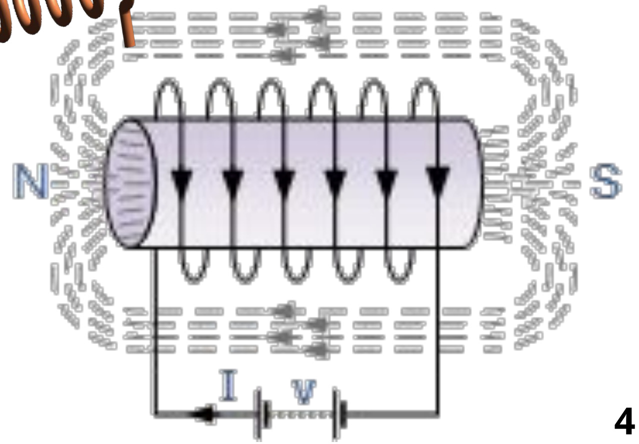


Creating an Electromagnetic Wave

- **Alternating** electrical current, flowing through inducting coil (I·R) induces magnetic field B
- This induces electric field E, which induces magnetic field, which in return induces another electric field, and so on ...

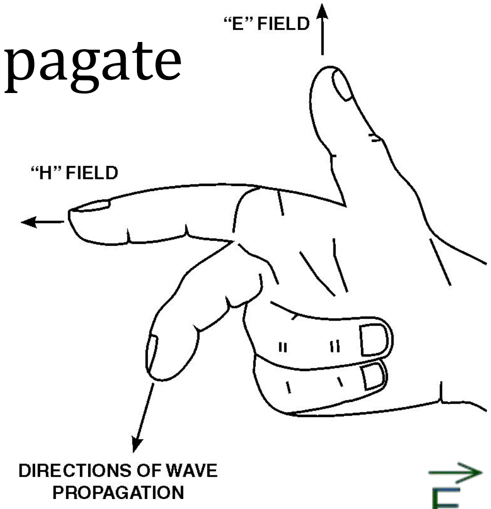
Name	Integral form
Gauss's law	$\oiint_{\partial V} \mathbf{E} \cdot \mathrm{d}\mathbf{A} = \frac{Q(V)}{\varepsilon_0}$
Gauss's law for magnetism	$\oiint_{\partial V} \mathbf{B} \cdot \mathrm{d}\mathbf{A} = 0$
Maxwell–Faraday equation (Faraday's law of induction)	$\oint_{\partial S} \mathbf{E} \cdot \mathrm{d}\mathbf{l} = -\frac{\partial \Phi_{B,S}}{\partial t}$
Ampère's circuital law (with Maxwell's correction)	$\oint_{\partial S} \mathbf{B} \cdot \mathrm{d}\mathbf{l} = \mu_0 I_S + \mu_0 \varepsilon_0 \frac{\partial \Phi_{E,S}}{\partial t}$

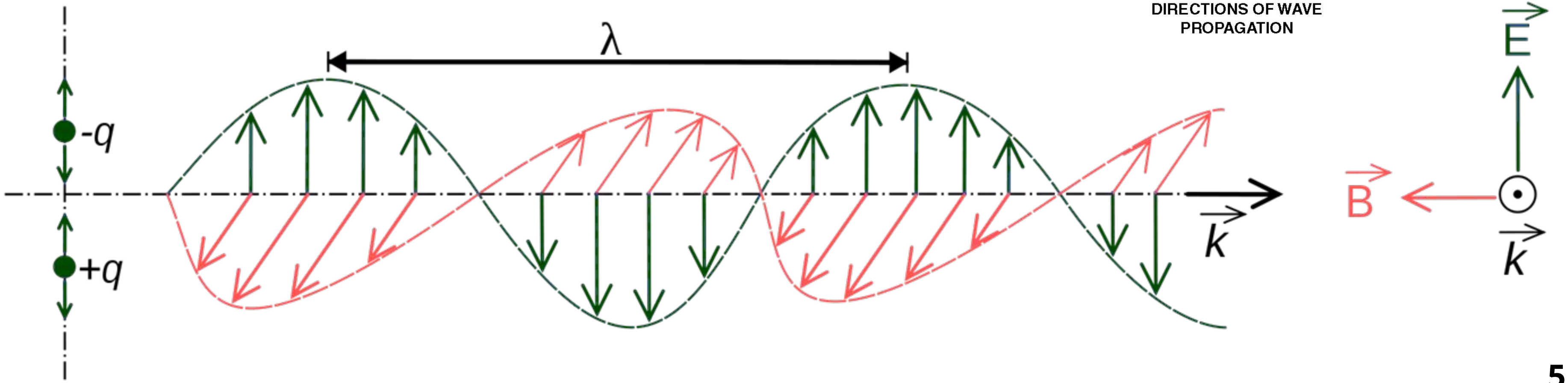




Radiation and Wave Propagation

- At high frequencies, electro-magnetic waves propagate through the medium (typically, air or vacuum)

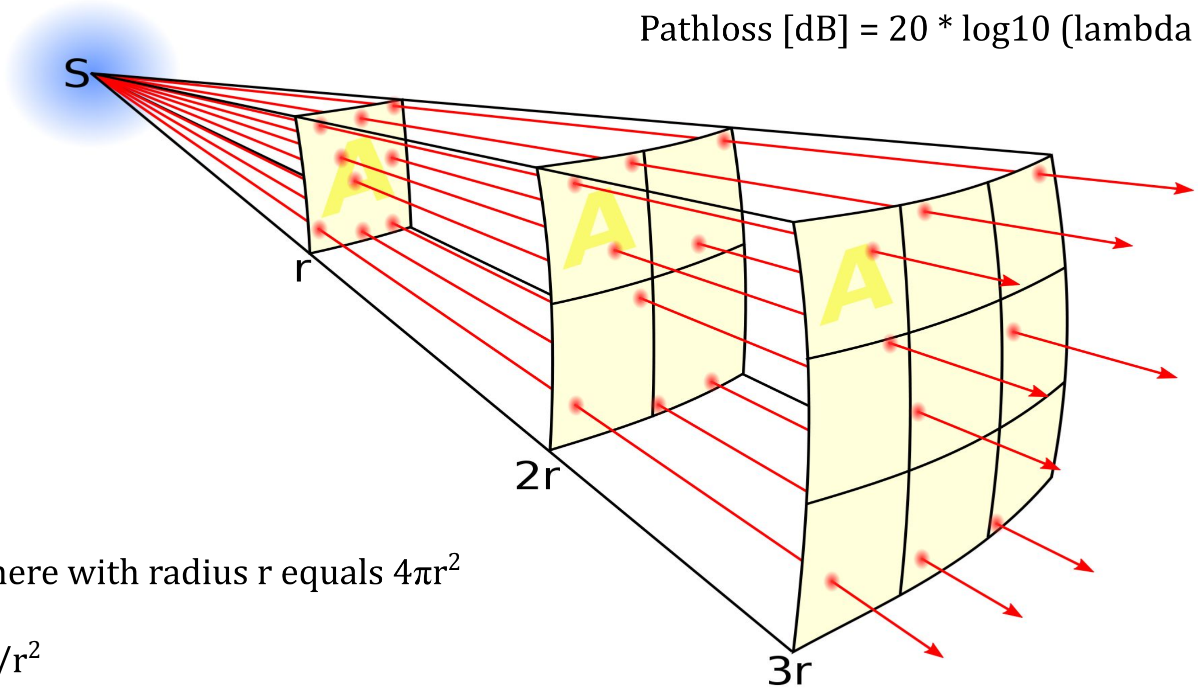




Path Loss and Free Space Propagation / Attenuation

Inverse-Square Loss of Signal Strength:

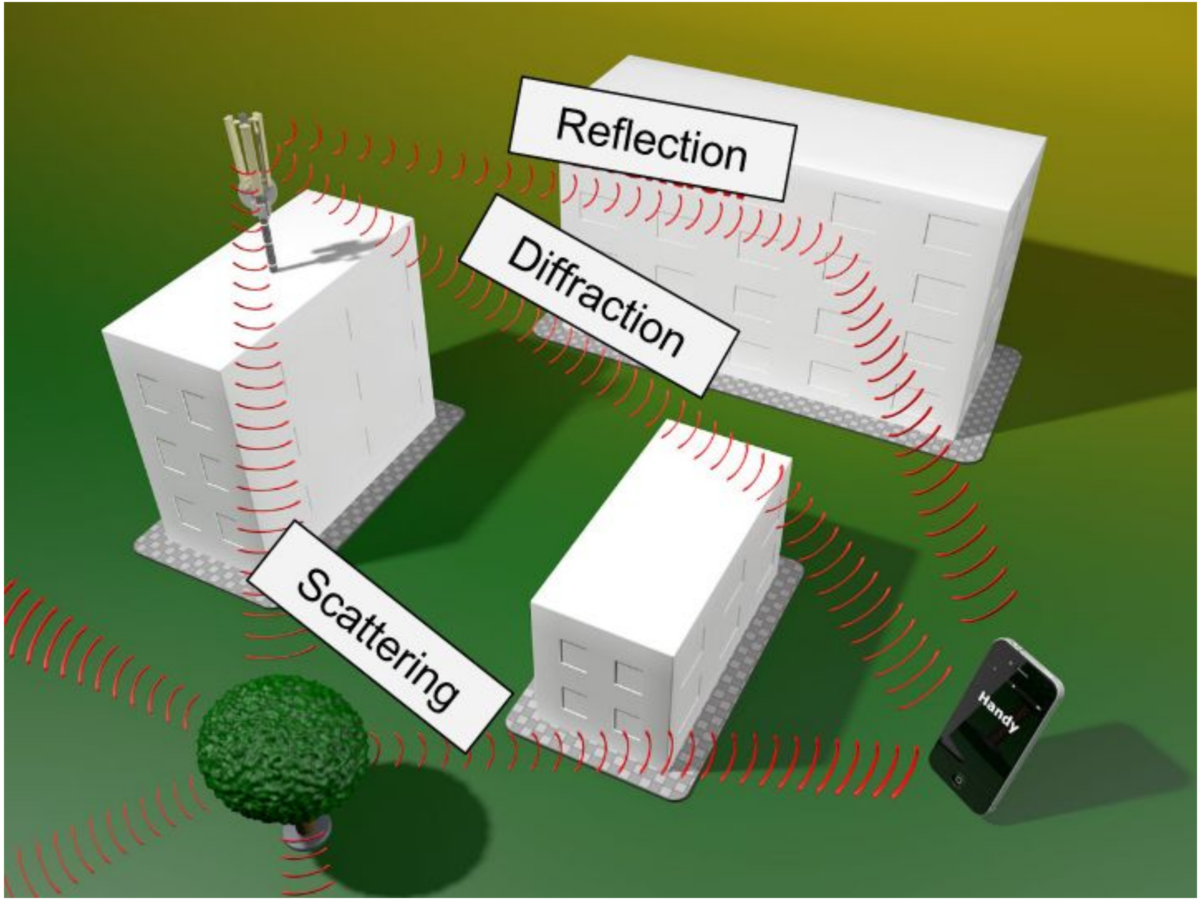
With antennas:
Pathloss [dB] = 20 * log10 (lambda ./ (4 .* pi .* r))

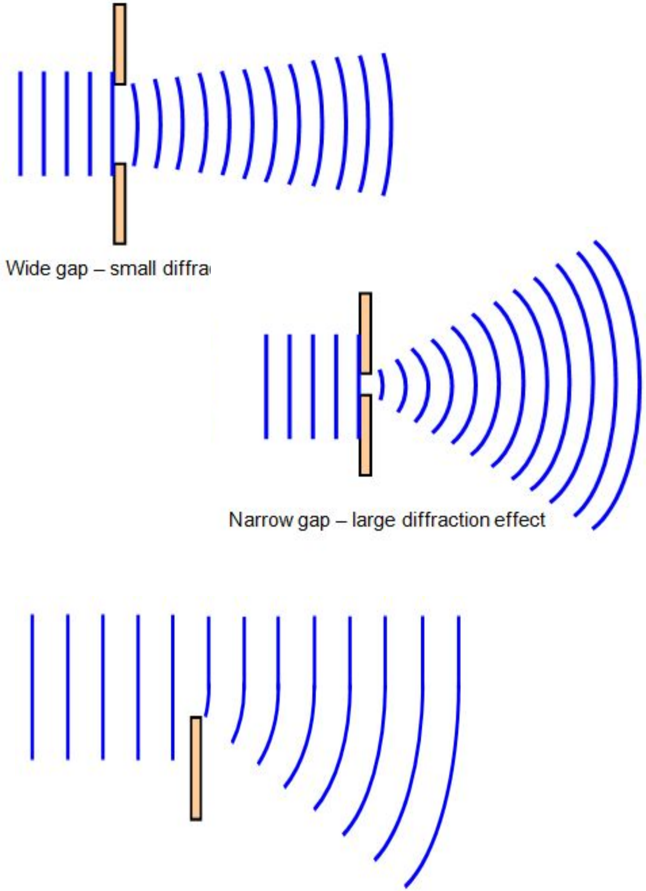


Surface area of a sphere with radius r equals $4\pi r^2$

Signal level $S(r) \sim 1/r^2$

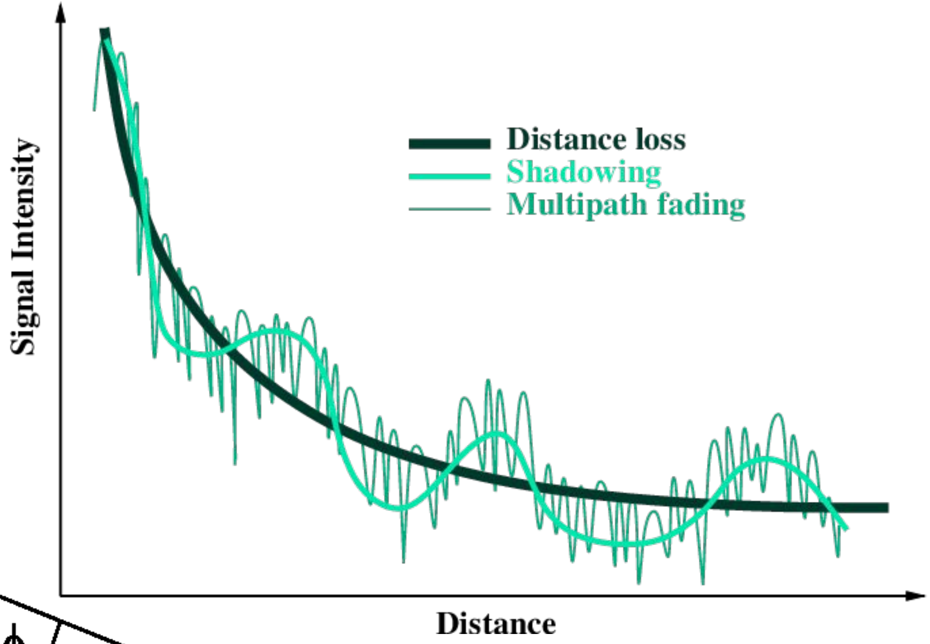
Diffraction, Reflection, Scattering

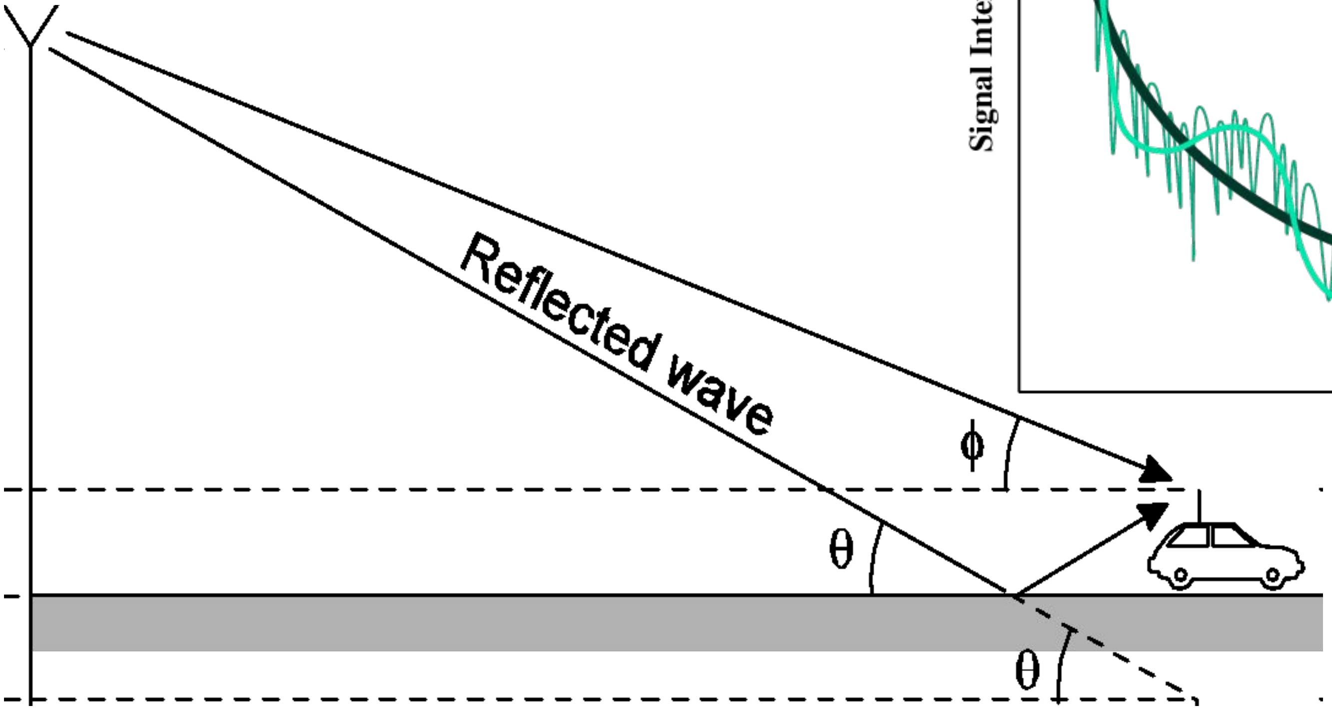




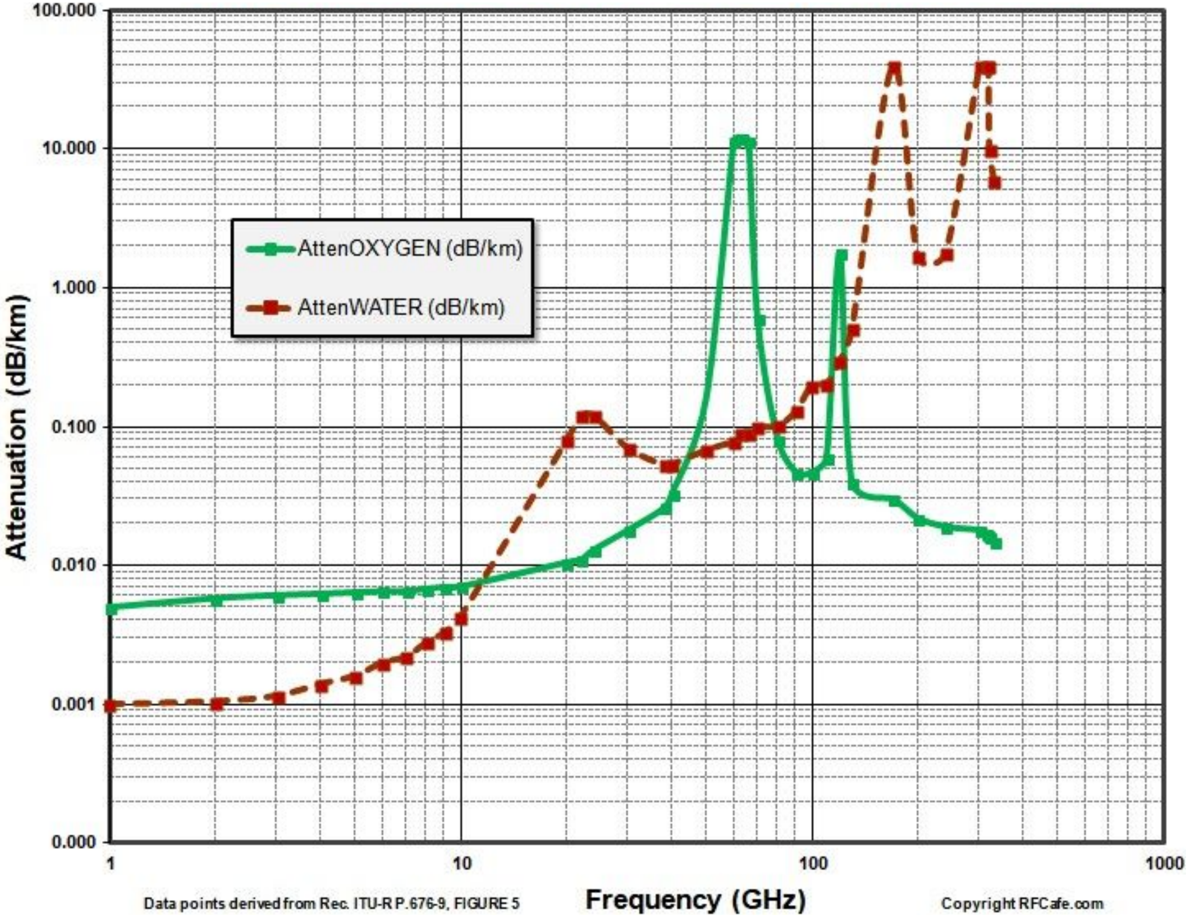
Multi-Path Propagation

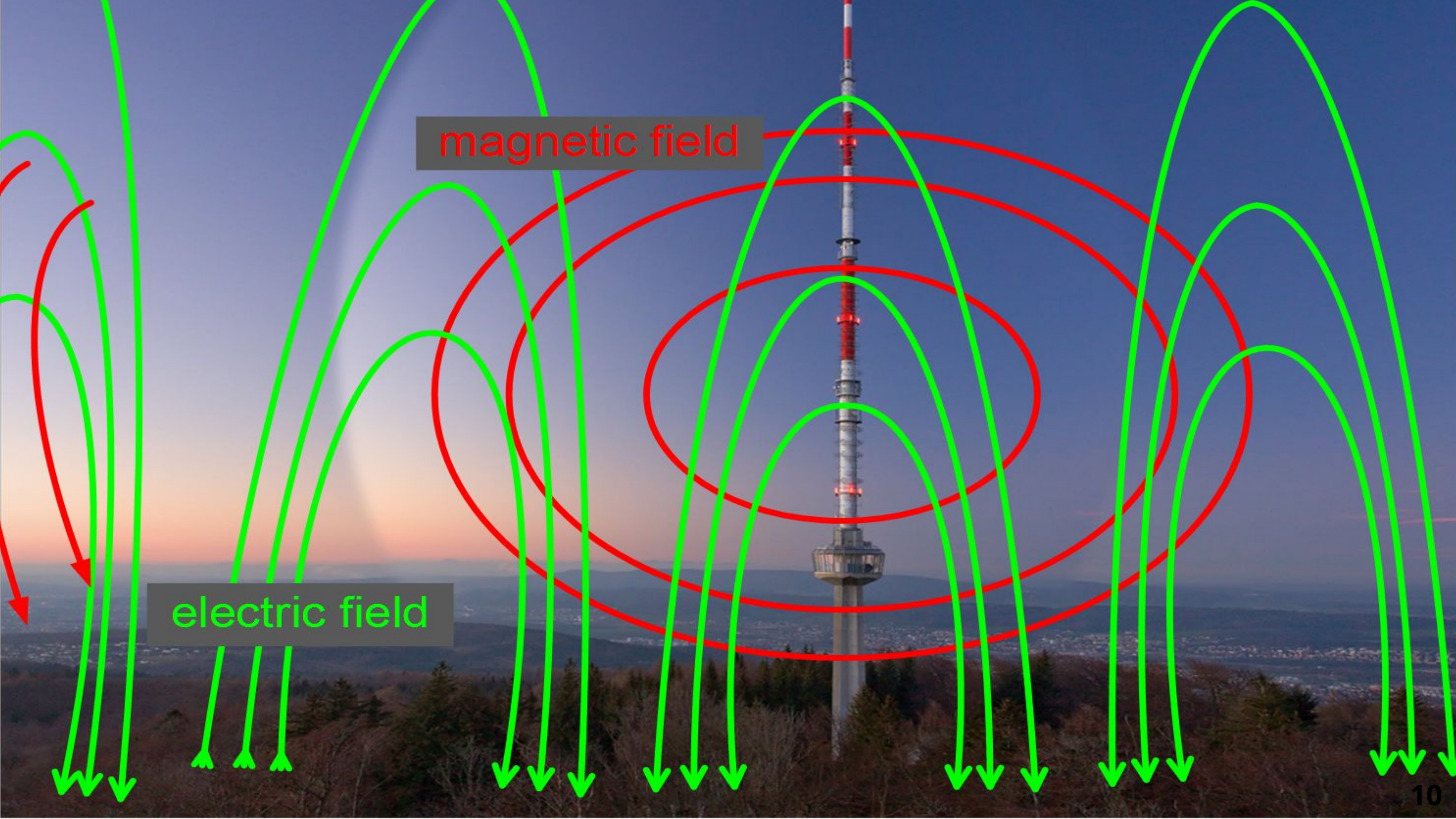
- Wireless communication with one reflection

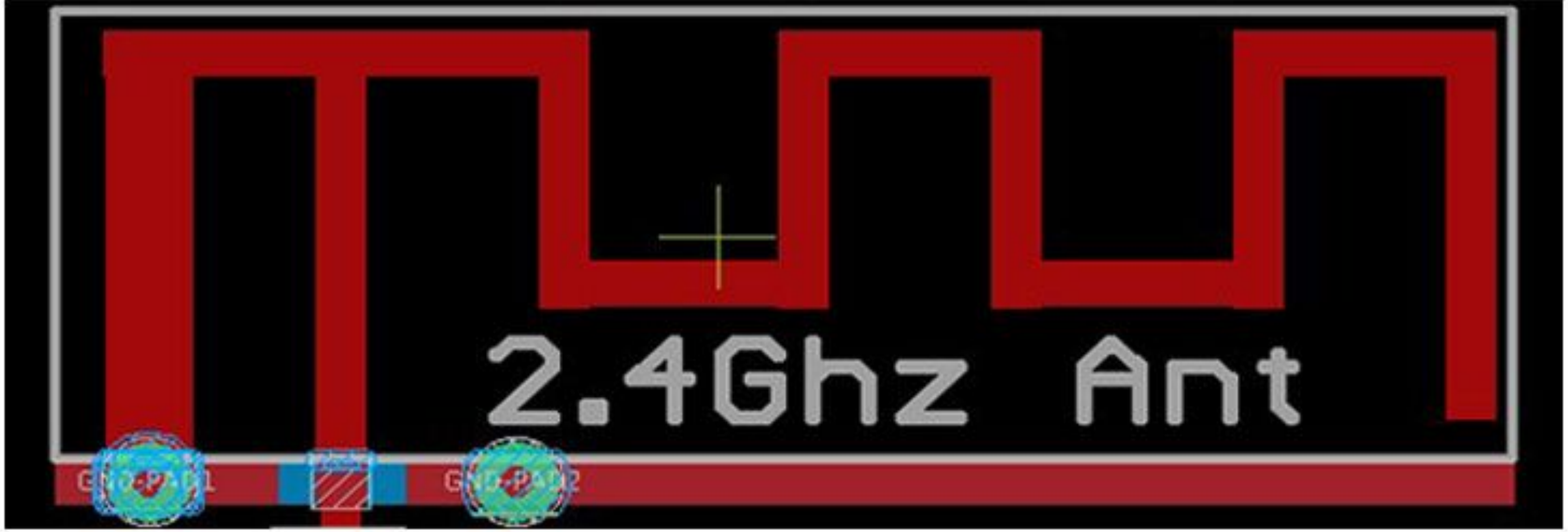




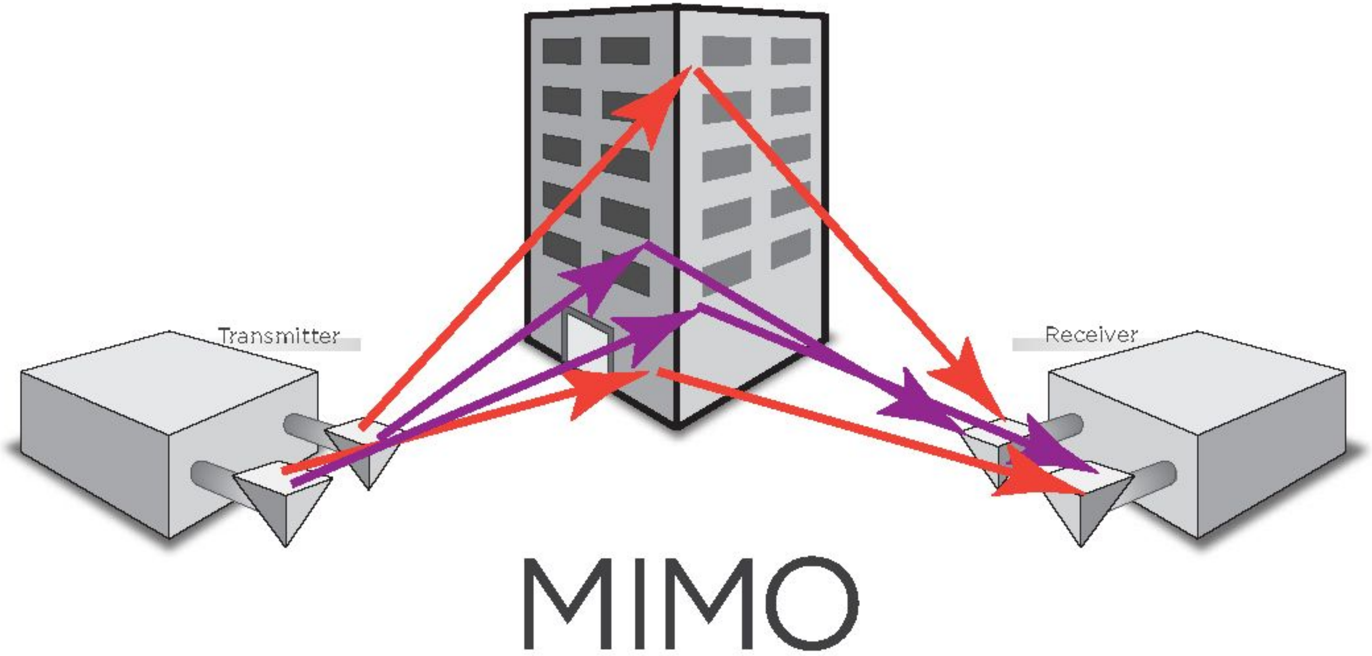
Attenuation through Atmosphere



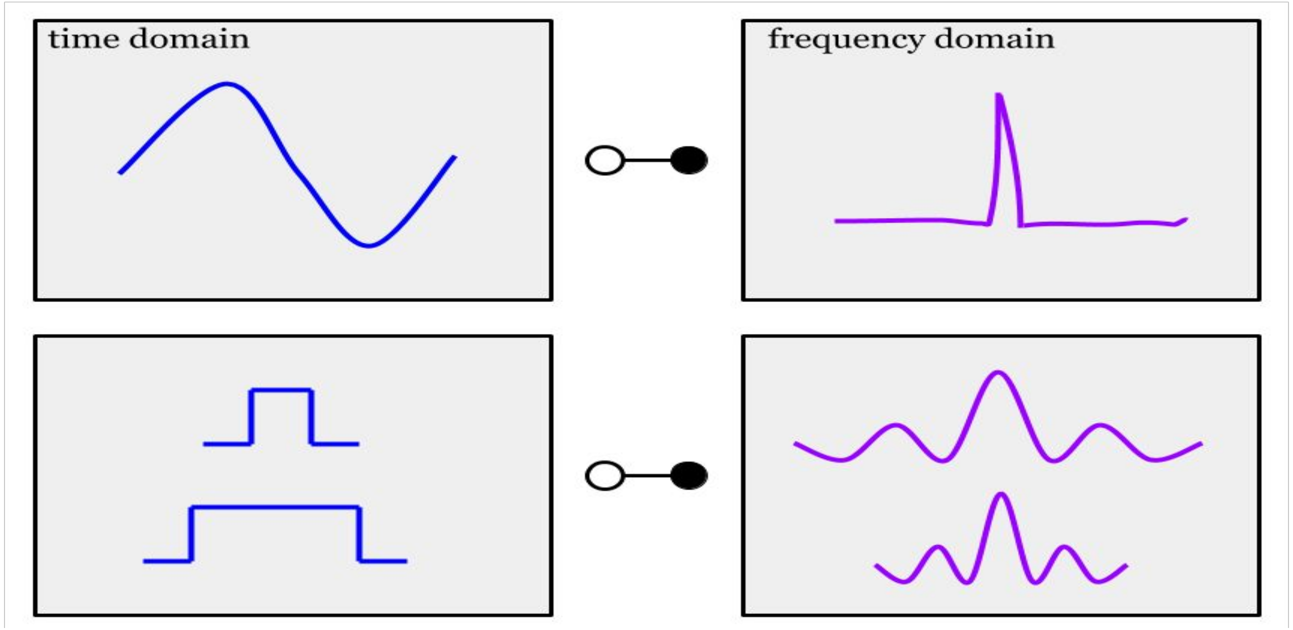

magnetic field
electric field


2.4Ghz Ant

MIMO (Multiple-Input Multiple Output)

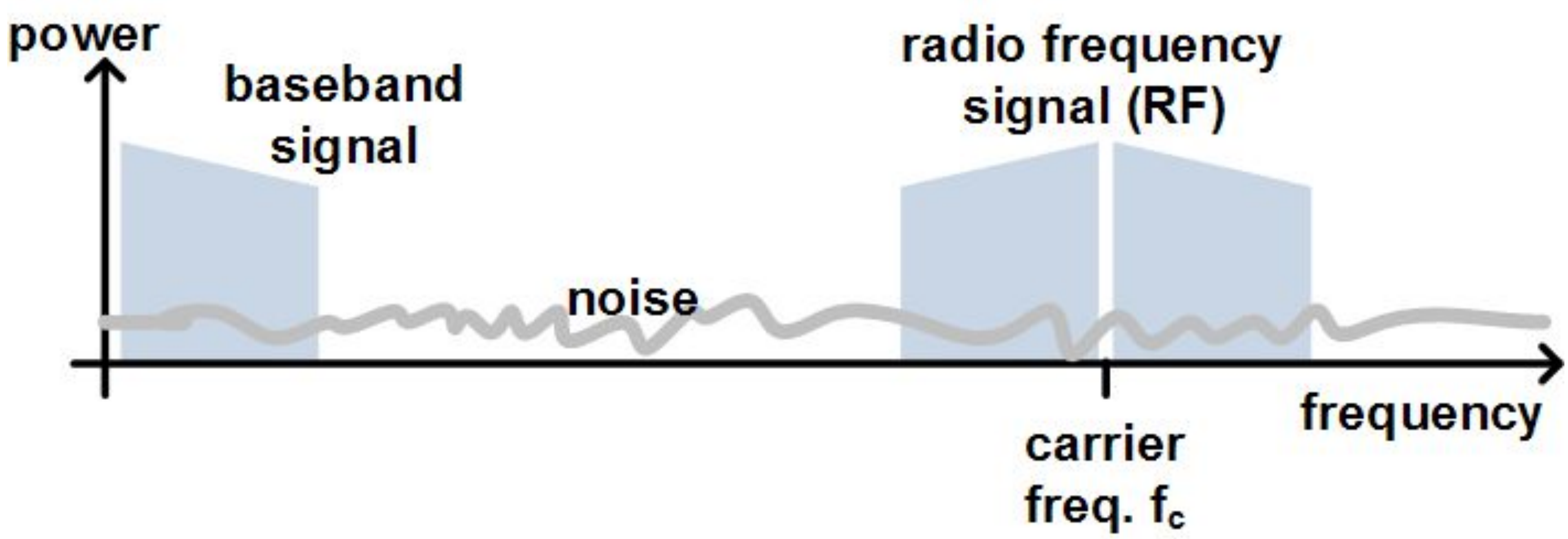


Fourier Time-Frequency Analysis



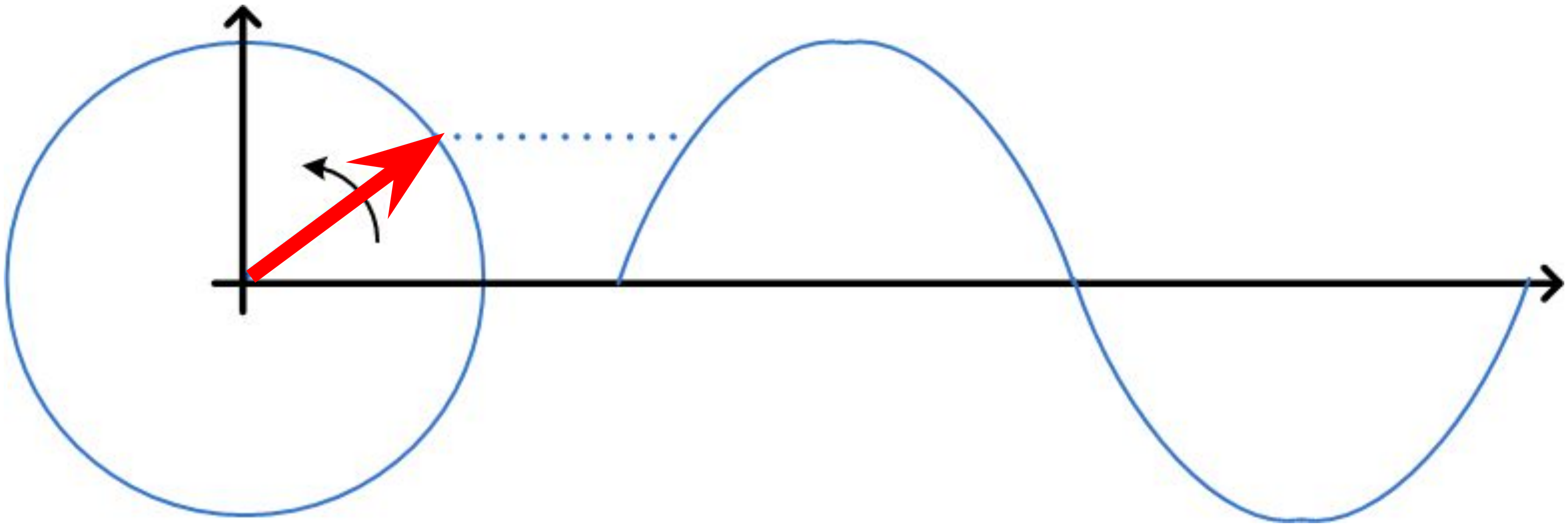
Radio-Frequency and Baseband Signal

- The high radio frequency signal propagates through the medium
- The low frequency baseband signal is modulated with the data



Illustrating Harmonic Waves with Vectors

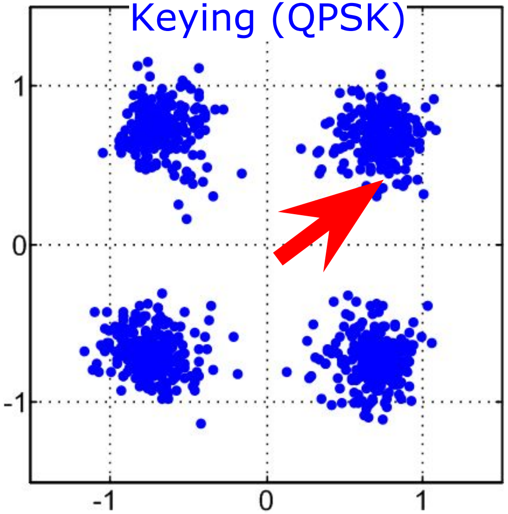
- Instead of sinus waves, harmonic waves are now illustrated with a simple vector
  - Phase and amplitude describe the baseband signal, relative to some reference
  - We ignore the speed of the vector, i.e., the frequency



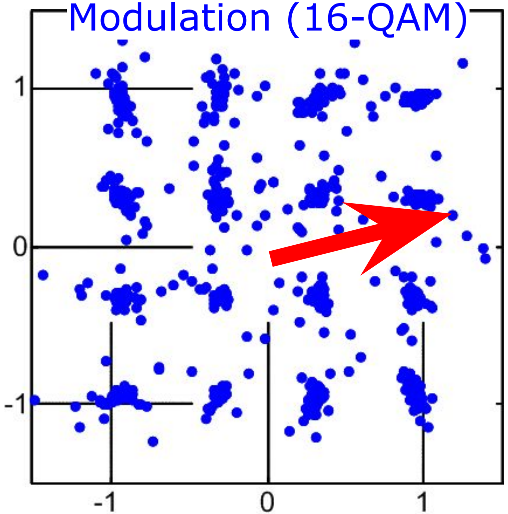
Modulation of Radio Signals

- A symbol modulated at QPSK carries 2 bit
  - 16-QAM carries 4 bit, and 64-QAM carries 6 bit
- Higher modulation is more sensitive to interference
  - For example: 64-QAM is more sensitive than 16-QAM

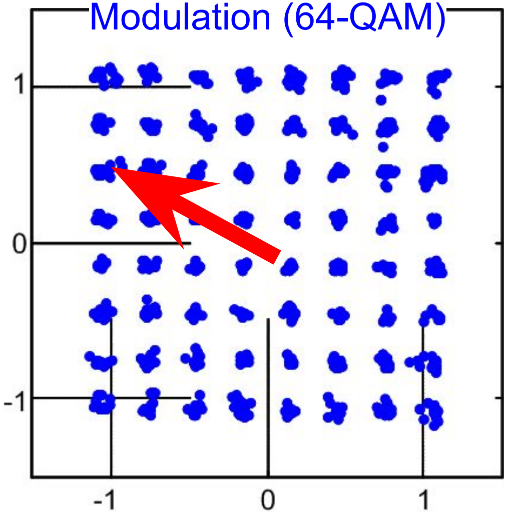
Quadrature Phase Shift Keying (QPSK)



16 Quadrature Amplitude Modulation (16-QAM)

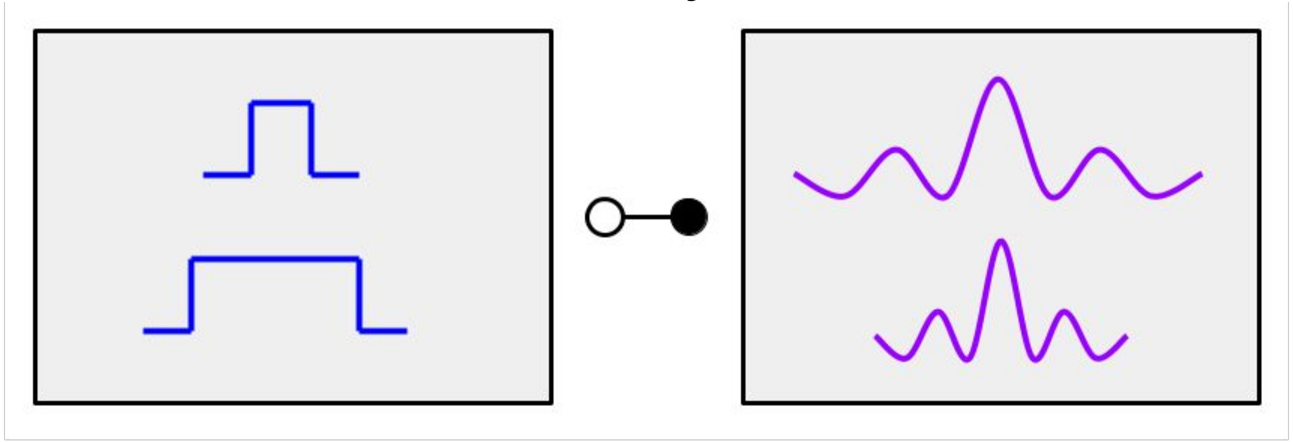


64 Quadrature Amplitude Modulation (64-QAM)



Channel Bandwidth 1/2

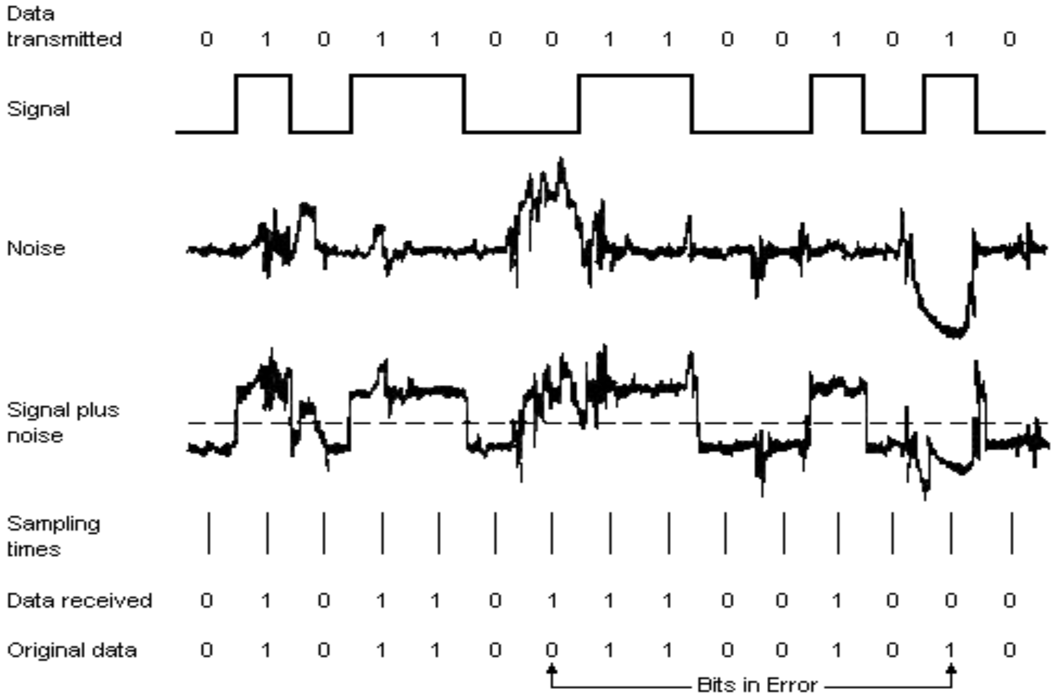
- The resulting bandwidth of a channel (in Hertz) depends on the symbol duration, not necessarily the bit rate.



- Network operators want to transmit more data, and request more spectrum bandwidth.
- Regulators struggle to assign enough spectrum to operators.

Channel Bandwidth 2/2

- The possible number of bit per symbol (in b/s) depends on the noise floor and the interference at the receiver antenna



Error Management: Forward Error Detection/Correction

- Source (transmitter) sends redundant data
- Destination (receiver) recognizes only the portion of the data that contains no errors
  - Simple example: send everything twice (repetition)
- Very relevant when there is no backchannel and the receiver cannot request a retransmission
  - Example: Broadcast
- 10% … 50% of the transmitted digital bitstream is redundant code
- Different codes can be used for different types of error patterns

(continued:) Forward Error Correction, FEC

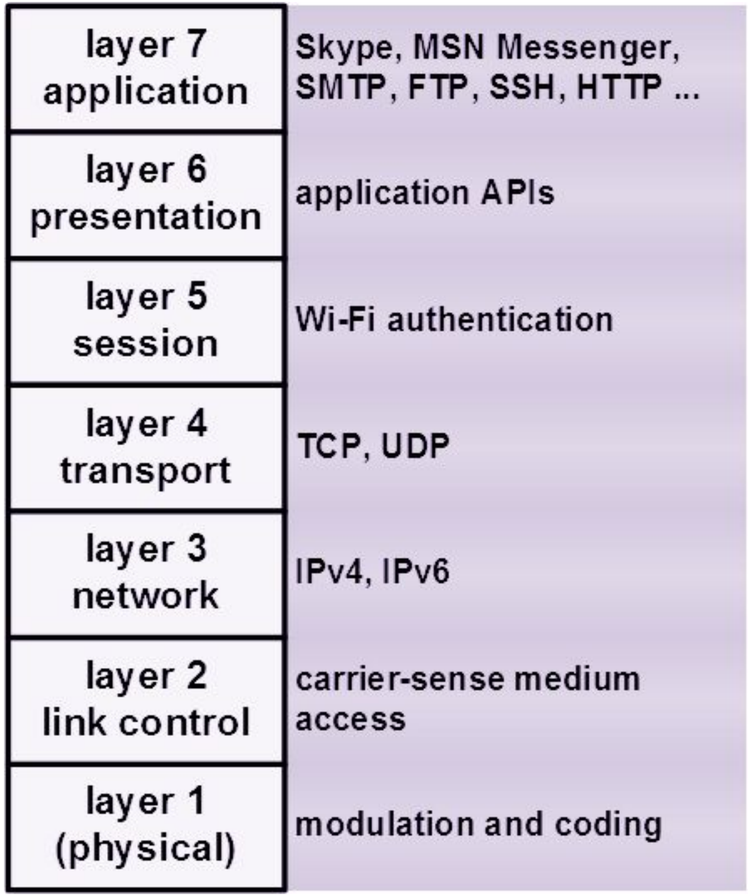
- Transmitter adds redundancy, checksum
  - using a predetermined scheme, known to transmitter and receiver
- Receiver uses redundancy to reconstruct data
  - Block by block, or continuously, as convolutional coding
- Block codes work on fixed-size blocks (packets) of bits or symbols of predetermined size
- Convolutional codes like the well-known “Viterbi” work on bit or symbol streams of arbitrary length

Optical vs. Radio

- The optical medium is not regulated by service, but for safety.
- The available bandwidth in infrared and visible light spectrum is very large (1000 x GHz).
- License-free long-range operation, in contrast with radio communication, is easier to achieve
  - Example: RONJA (Reasonable Optical Near Joint Access)
- There is no negative light
  - The signal intensity is modulated between zero and some maximum power
  - Fourier transform still applies, but the signal has only half the spectrum efficiency
  - Direct detection with photo-sensors is used instead of antennas

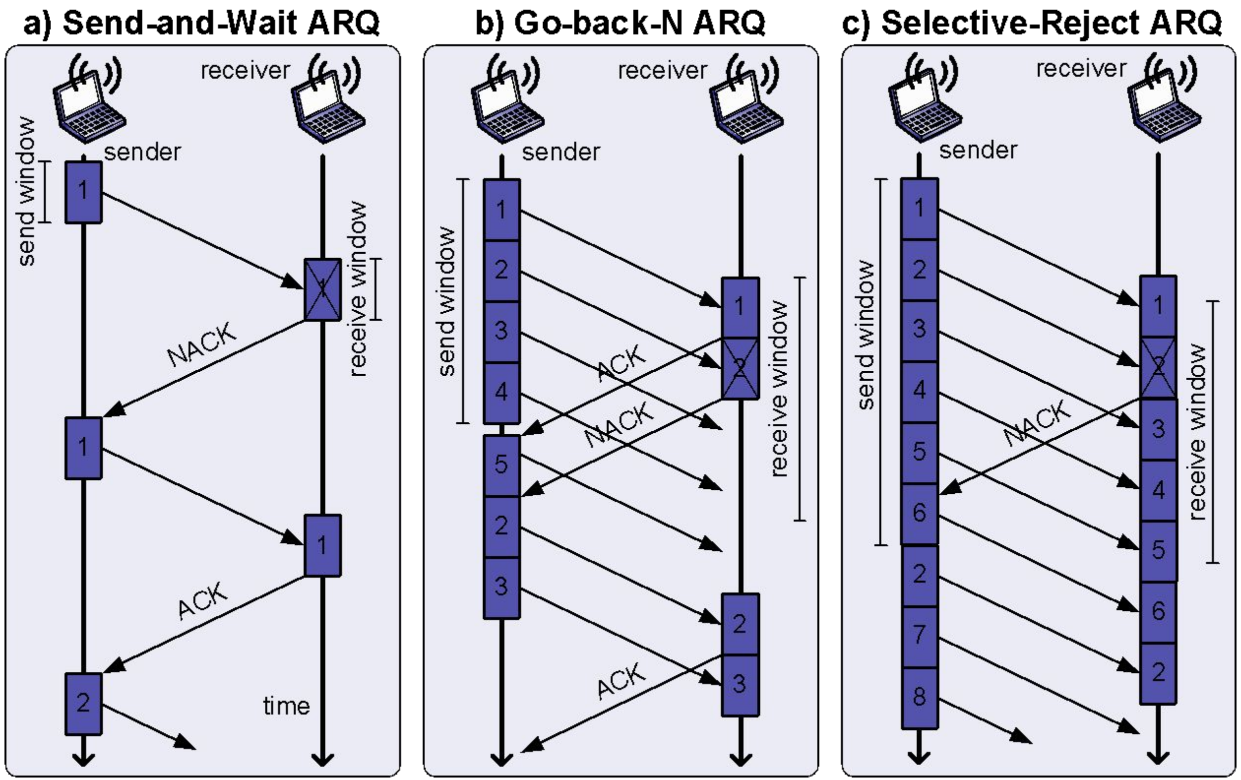
ISO/OSI Reference Model - Layer 1 and Layer 2

- Everything discussed so far was Related to the layer 1 of the seven Layer ISO/OSI reference model
- In the following, layer 2 aspects will be discussed
  - ISO: International Standardizations Organization
  - OSI: Open Systems Interconnection



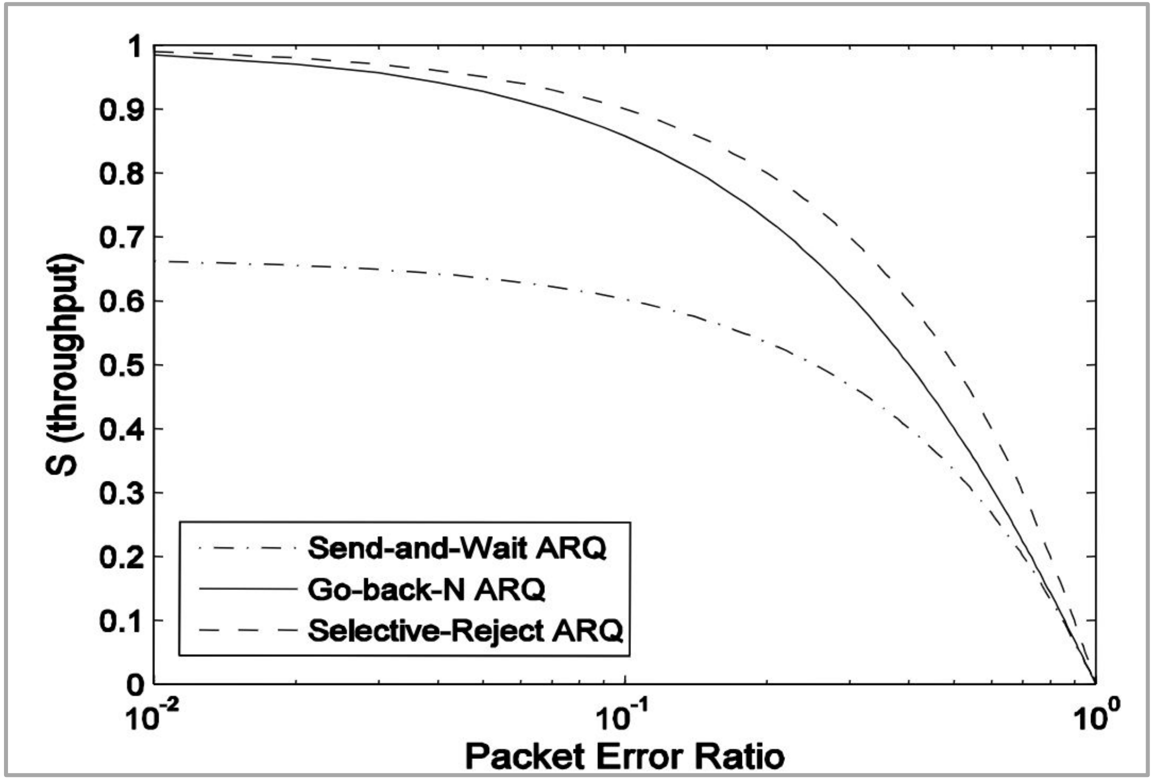
Error Management: Automatic Repeat Request, ARQ

- Also referred to as “Backward Error Detection/Correction”



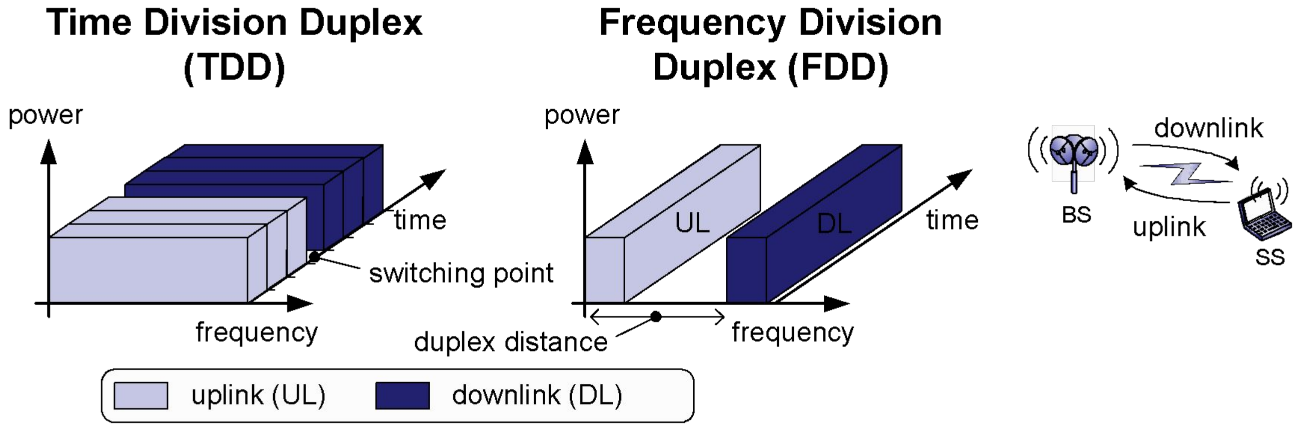
Automatic Repeat Request Throughput

- Packet size 1514 B (=1514 Byte), channel capacity of 6 Mb/s (=6 Mbps)

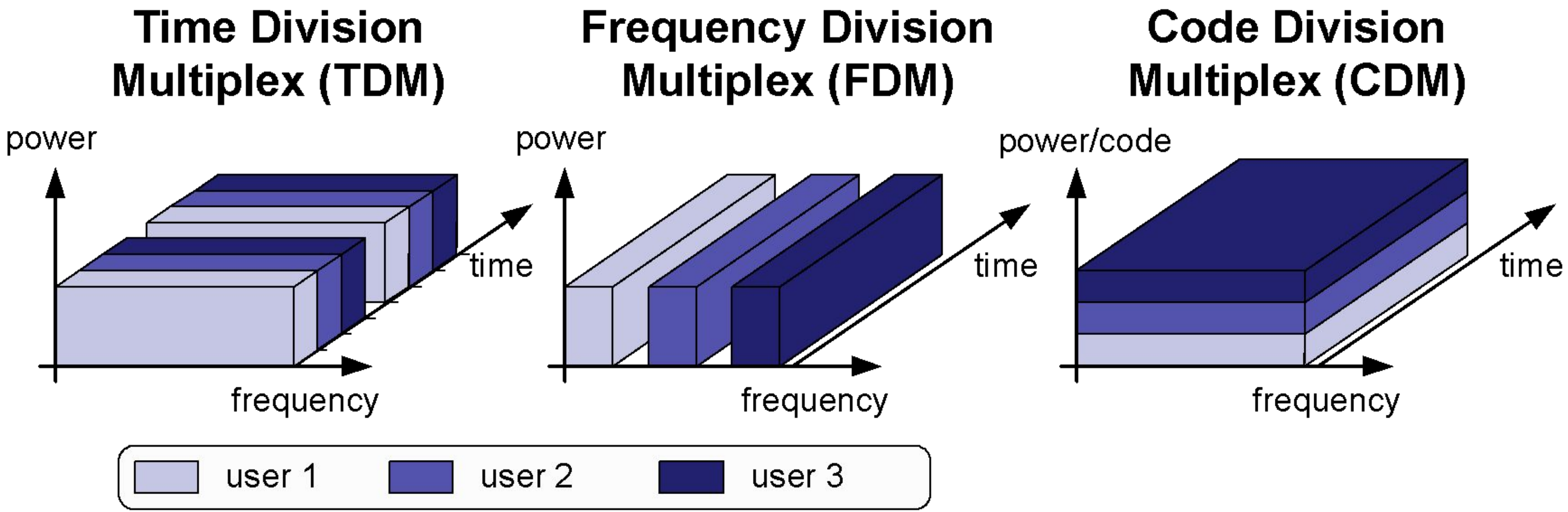


Duplexing Scheme

- Time Division Duplex
  - Switching between transmitters separates a single frequency channel, repeatedly, into uplink (UL) and downlink (DL) period - Ideal for asymmetric services
- Frequency Division Duplex
  - Downlink (DL) and uplink (UL) use different frequency channels of the same bandwidth
  - Suitable for symmetric services, but requires paired frequency bands.



Channel Multiplexing Scheme

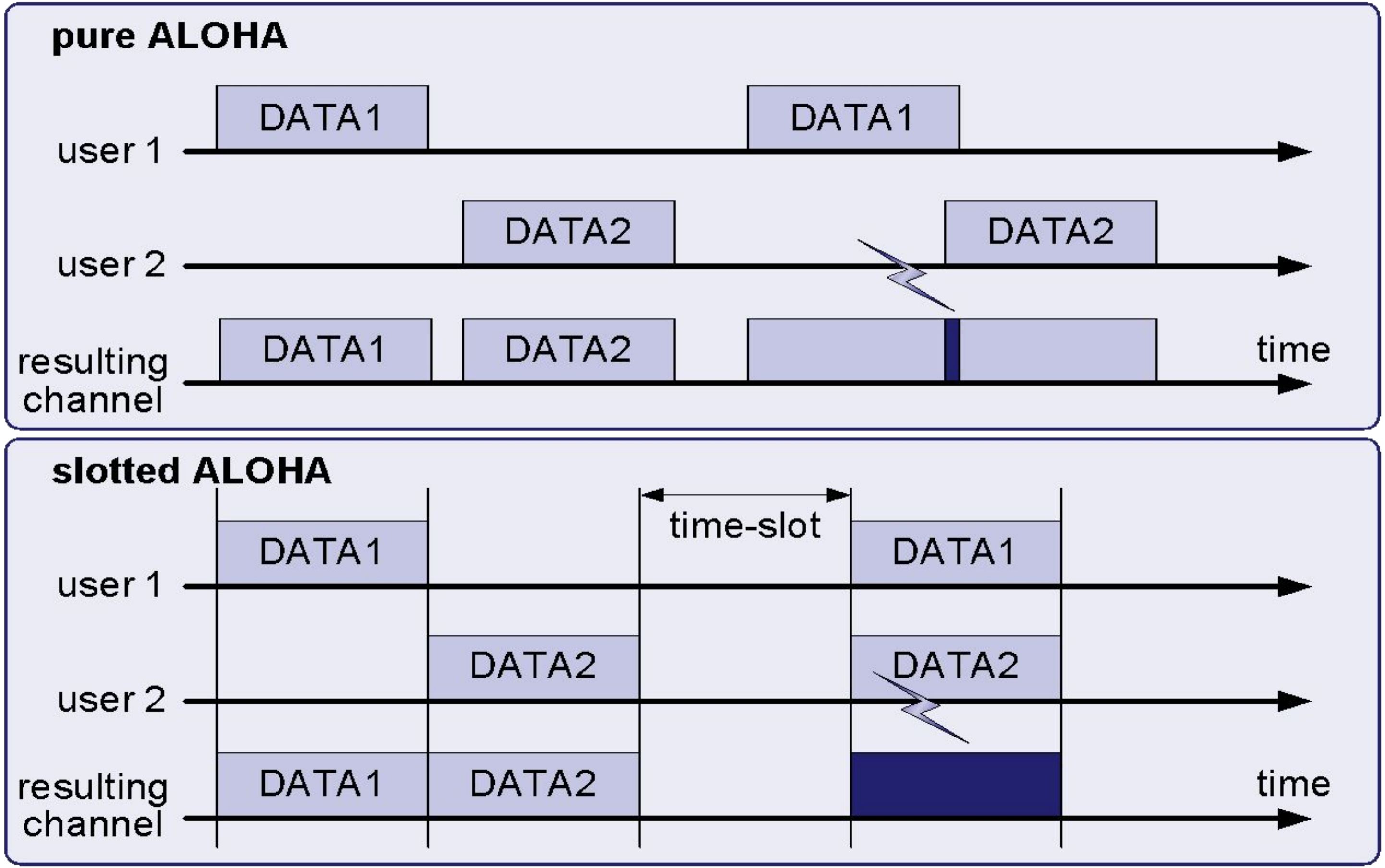


1968: ALOHA at University of Hawaii

https://citris.sites.ucsc.edu/alohanet/

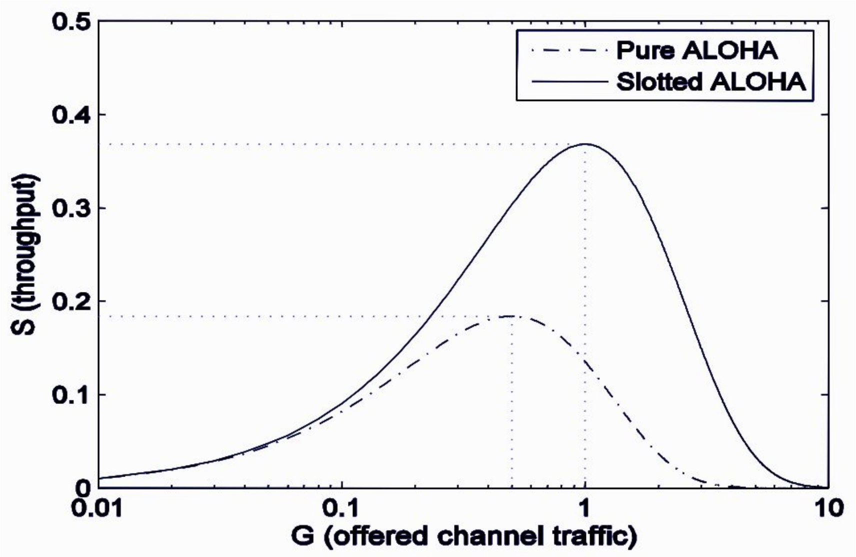
> “The essence of the ALOHA channel is to transmit at will – if the transmitter is unsuccessful then it will retransmit at some random time in the future.
>
> This simplicity, the elegance of the analytical model describing the behavior of the ALOHA channel, and the groundbreaking demonstration of a wireless packet-switching network based on it launched a revolution on packet switching over wireless links.
>
> The ongoing impact and influence of the ALOHA system project has been vast. The ALOHA channel and subsequent modifications are utilized in all major mobile networks and in almost all two-way satellite data networks.
>
> In a way, all mobile phones used today >say ALOHA< every time they are used, as the very first packet transmitted is sent via an ALOHA random access channel.”

ALOHA and slotted ALOHA



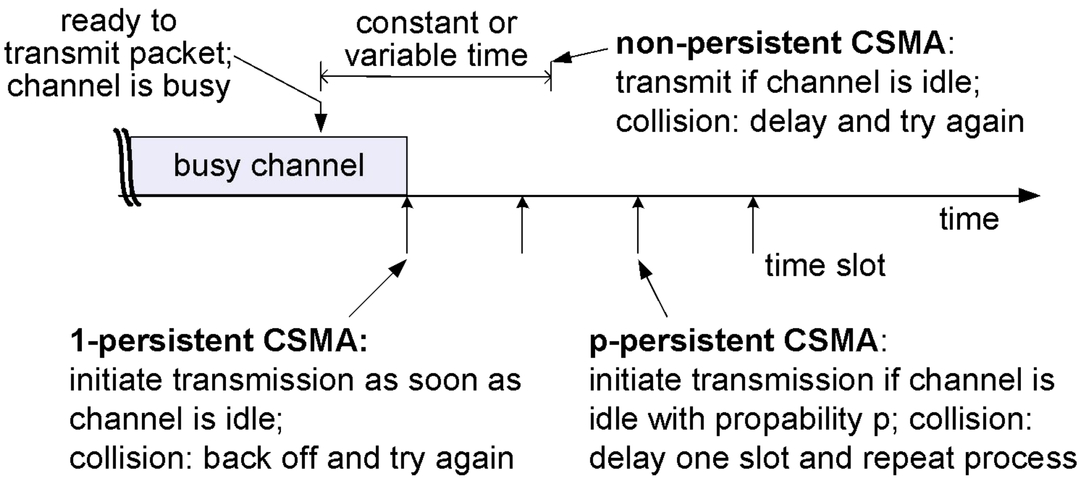
ALOHA and Slotted ALOHA Throughput

- Maximum system throughput in slotted ALOHA is twice that of pure ALOHA
  - ALOHA max. throughput of ALOHA is 18% of medium capacity (for G=0.5)
  - Slotted ALOHA max. throughput is 37% of medium capacity (for G=1)



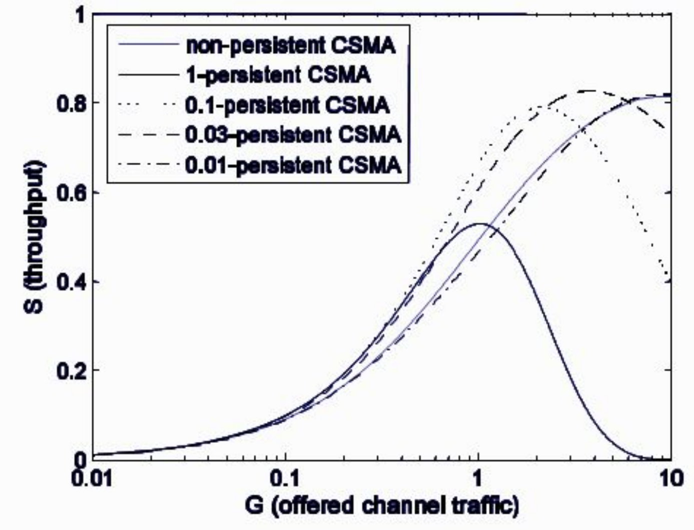
Carrier Sense Multiple Access (CSMA)

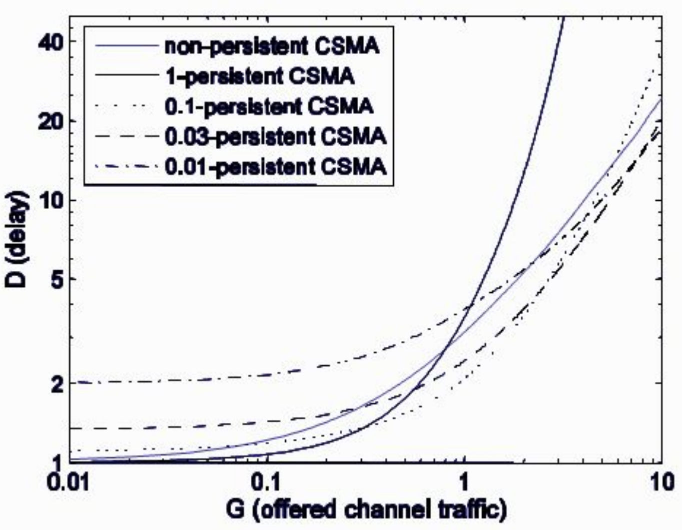
- CSMA with Collision Detection (CSMA/CD) -- **Ethernet**
  - jamming signal sent after collision detection, transmission is terminated (IEEE 802.3 Ethernet)
- CSMA with Collision Avoidance (CSMA/CA) -- **Wi-Fi**
  - stations defer from medium access when notified about transmissions



Carrier Sense Multiple Access (CSMA) Throughput

- CSMA increases efficiency of channel utilization towards 80% tradeoff between achievable throughput and delay
- Delay increases exponentially with increasing offered traffic





Wireless Networking and Mobile Computing

3. IEEE 802.11 Wireless LAN (Wi-Fi)

(a) Physical Layer 1

Stefan Mangold

Course Outline

1. Introduction
2. Wireless Communication Basics
3. **IEEE 802.11 Wireless LAN (Wi-Fi) -** (a) Physical Layer 1
4. IEEE 802.15 Wireless PAN (ZigBee & Bluetooth)
5. Mobile Computing Algorithm Basics: Control and Game Theory
6. Visible Light Communication
7. Audio Communication
8. Cellular Networking Basics (LTE, 5G, Internet-of-Things)
9. Mobile Computing for Automated Medicine Delivery
10. Cognitive Radio, Delay Tolerant Networking, Radio Spectrum Sharing

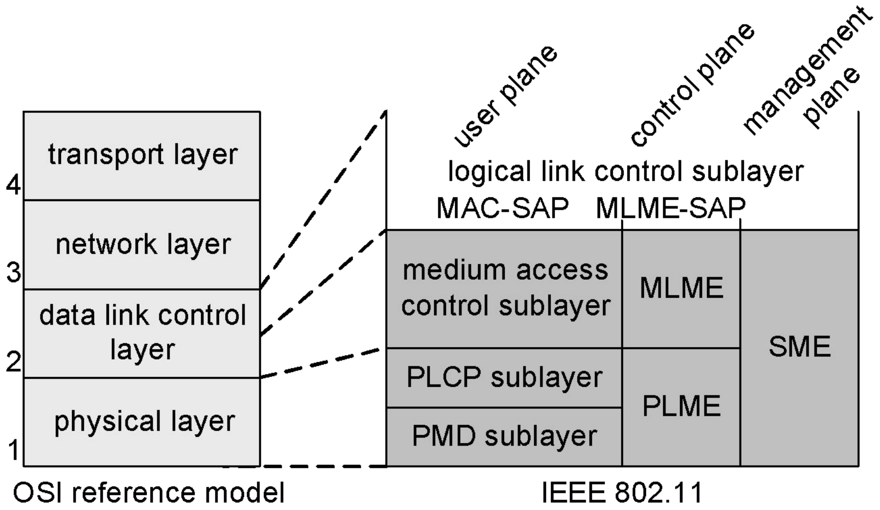
ISO/OSI Reference Model - Layer 1 and Layer 2

- ISO: International Organization for Standardization
- OSI: Open Systems Interconnection

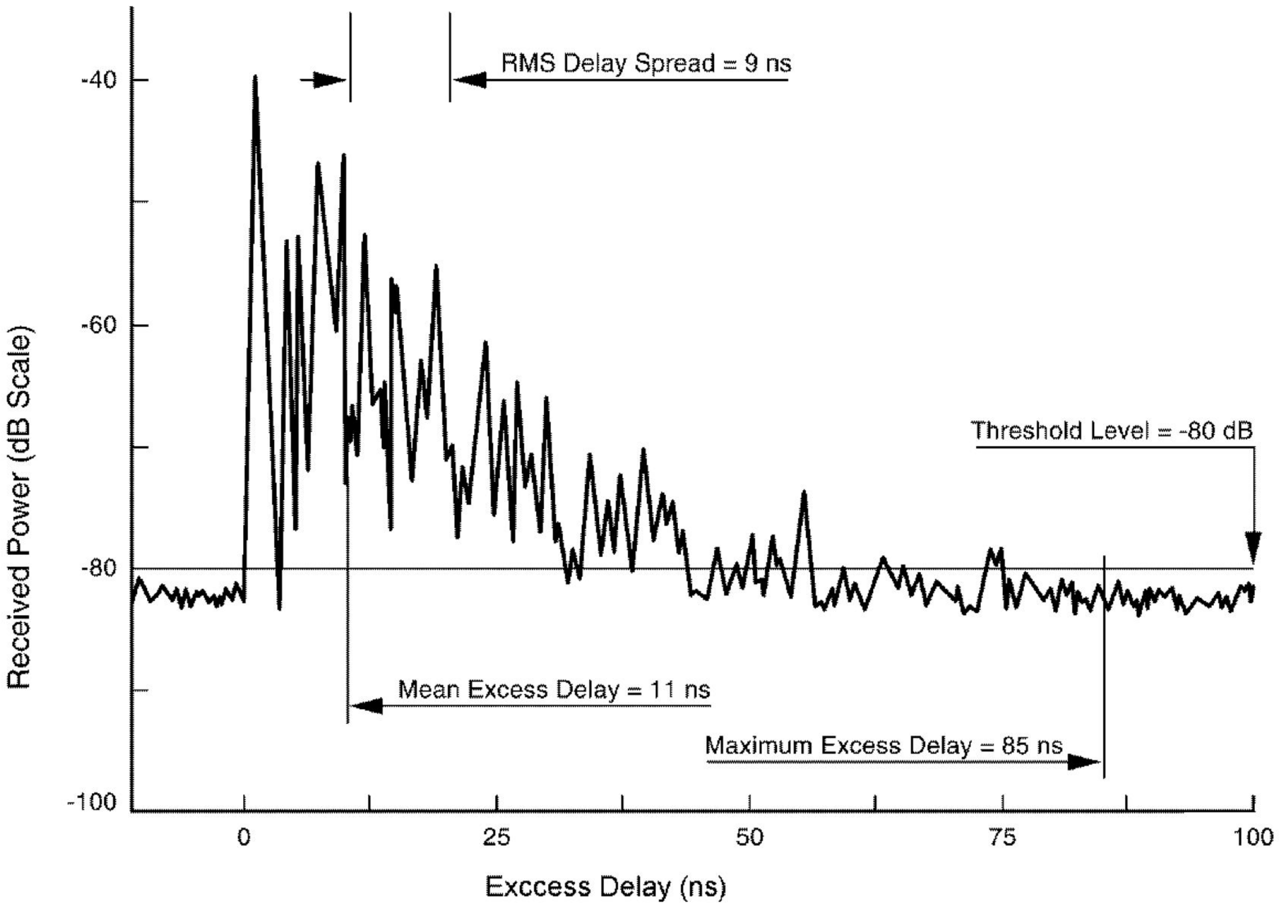
layer 7 application	Skype, MSN Messenger, SMTP, FTP, SSH, HTTP ...
layer 6 presentation	application APIs
layer 5 session	Wi-Fi authentication
layer 4 transport	TCP, UDP
layer 3 network	IPv4, IPv6
layer 2 link control	carrier-sense medium access
layer 1 (physical)	modulation and coding

IEEE 802.11 Reference Model

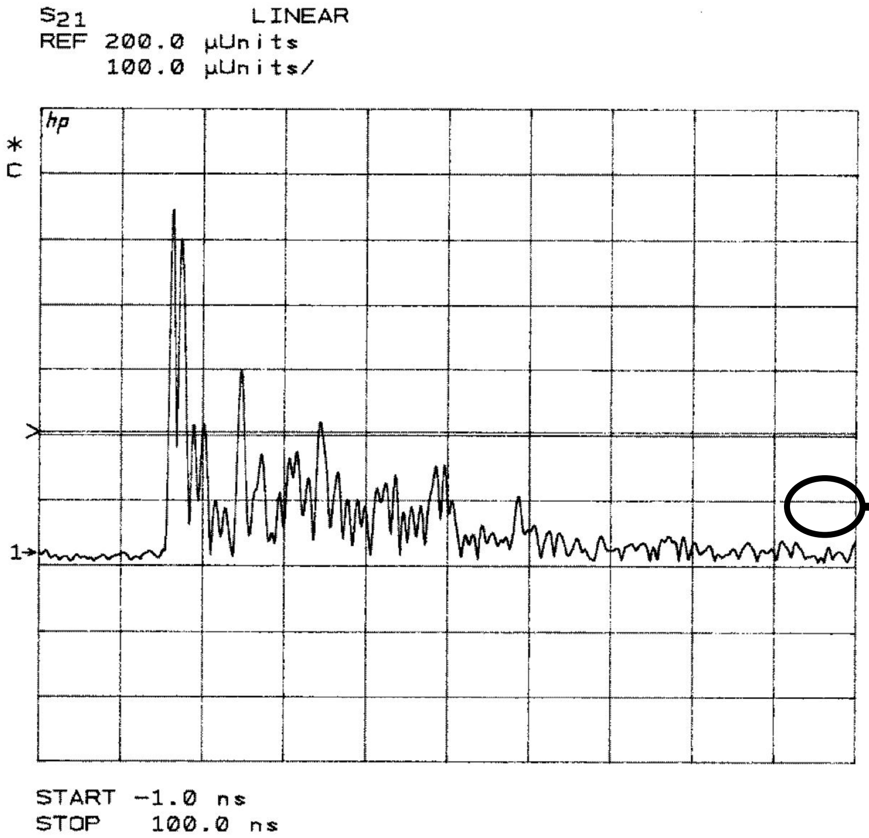
- Layer 1: PHY transmission schemes
- Layer 2: MAC protocols, MAC Layer Management Entity (MLME)
- Layer 1 & 2: Station Management Entity (SME)
- Interface to higher layers: Service Access Points (SAPs)

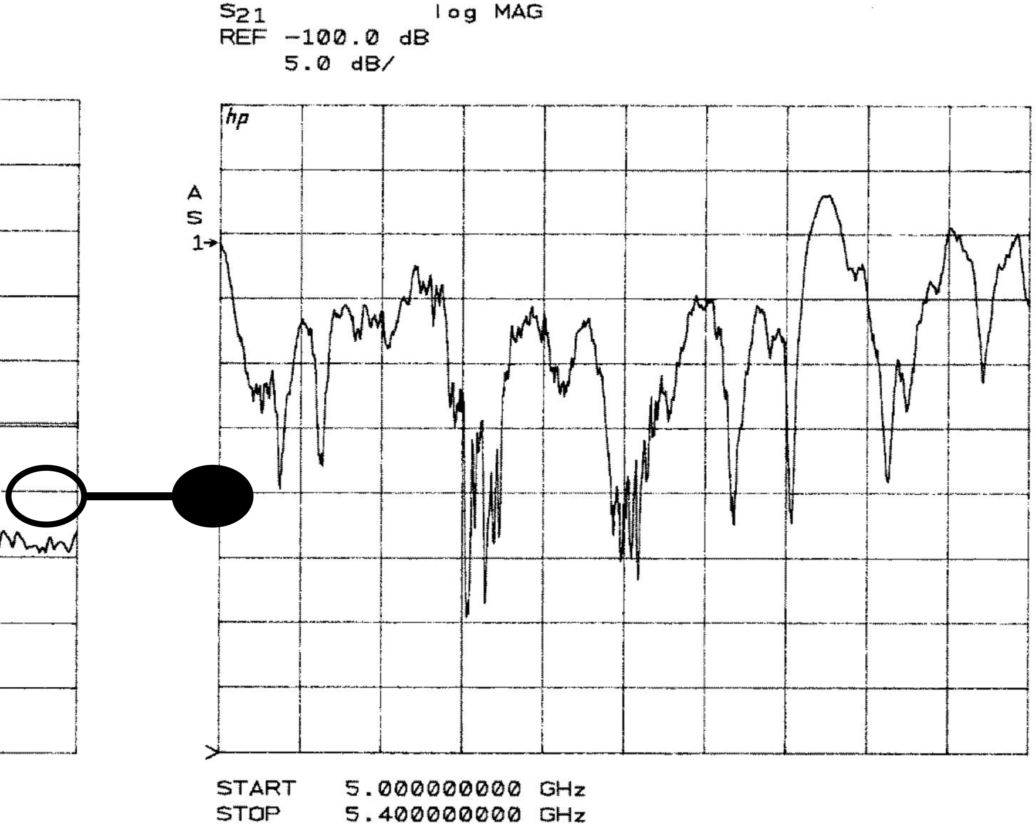


Indoor Radio Channel

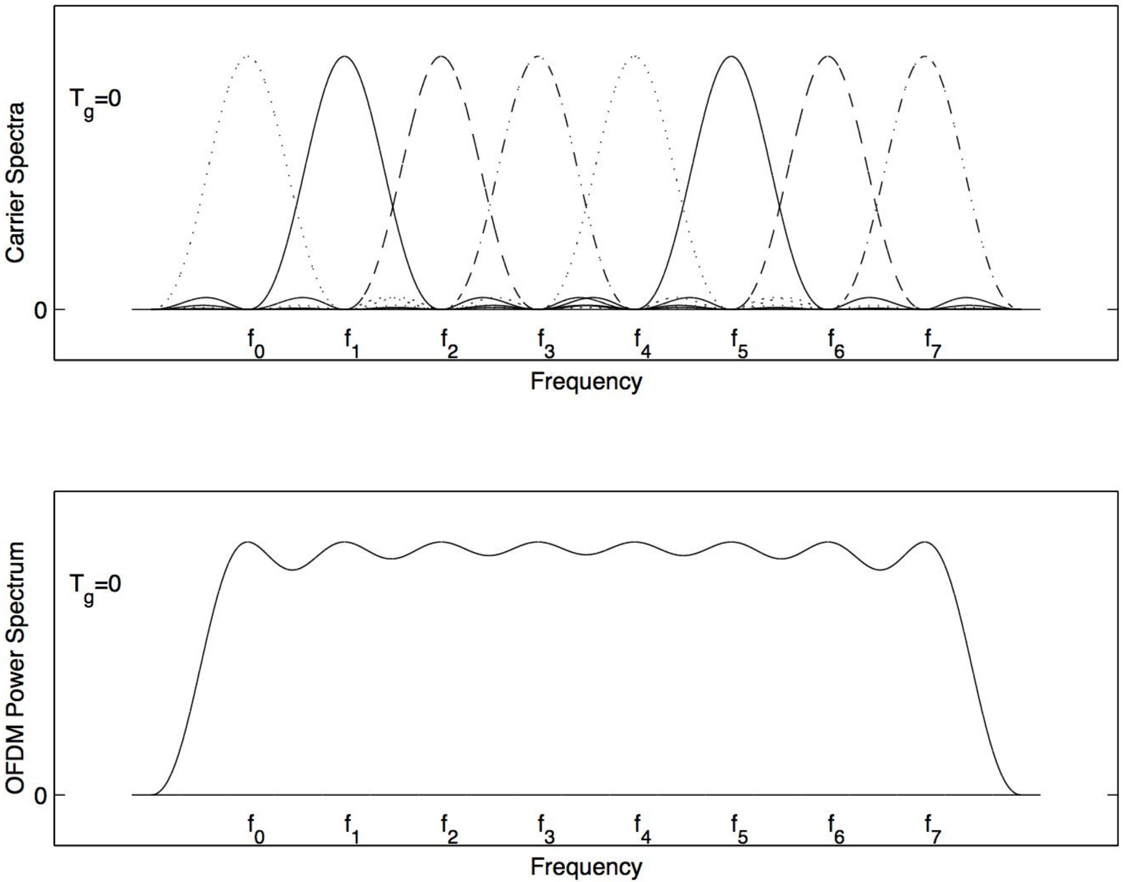


Time Domain and Frequency Domain

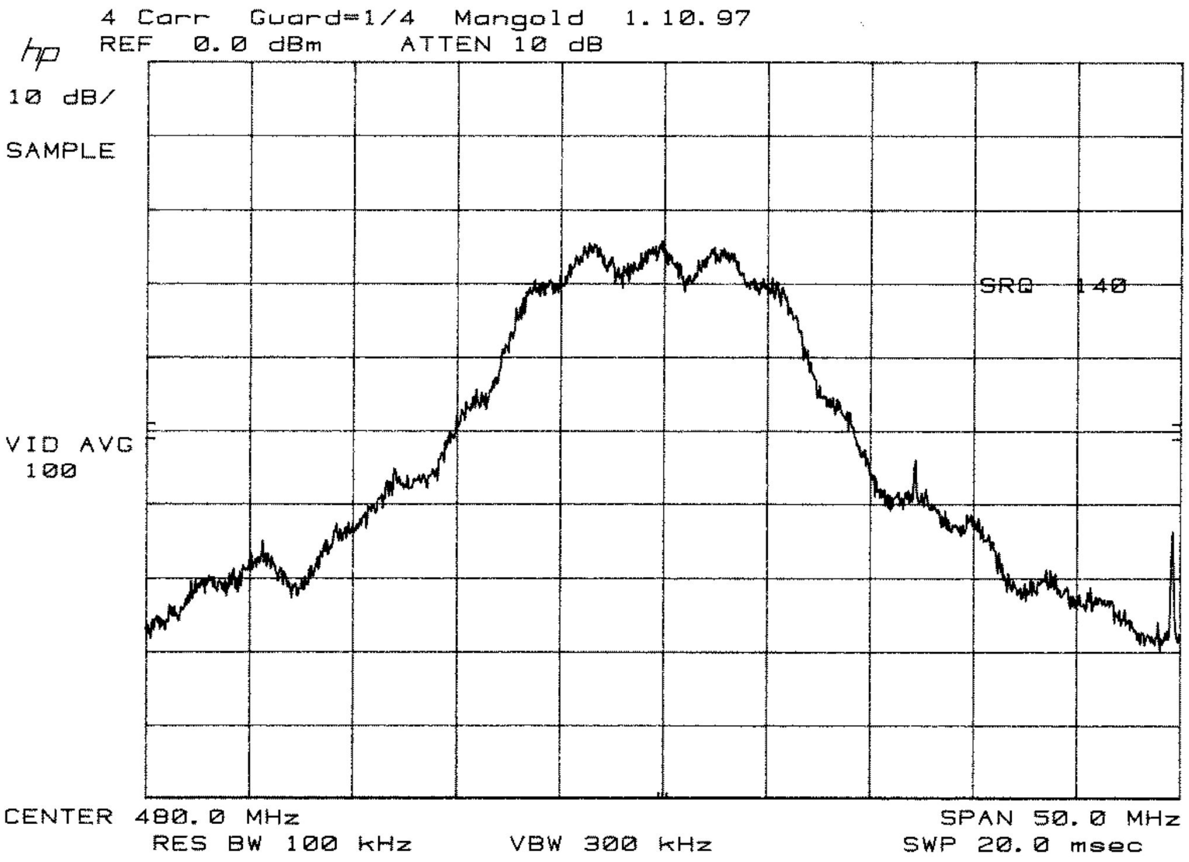




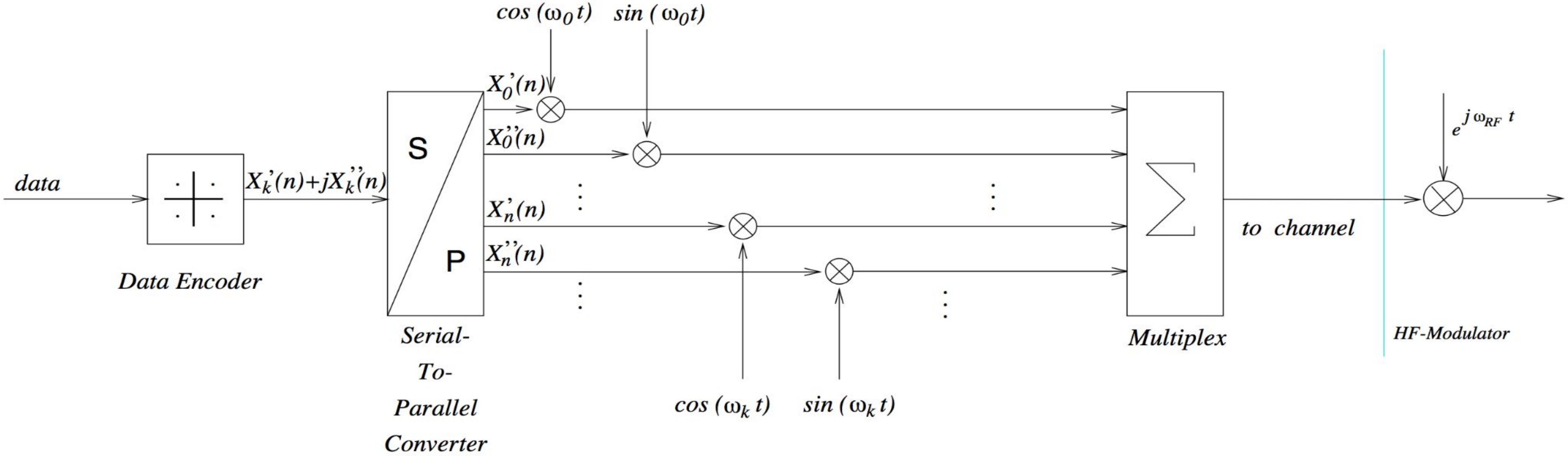
Multi-Carrier Approach



Multi-Carrier Spectrum

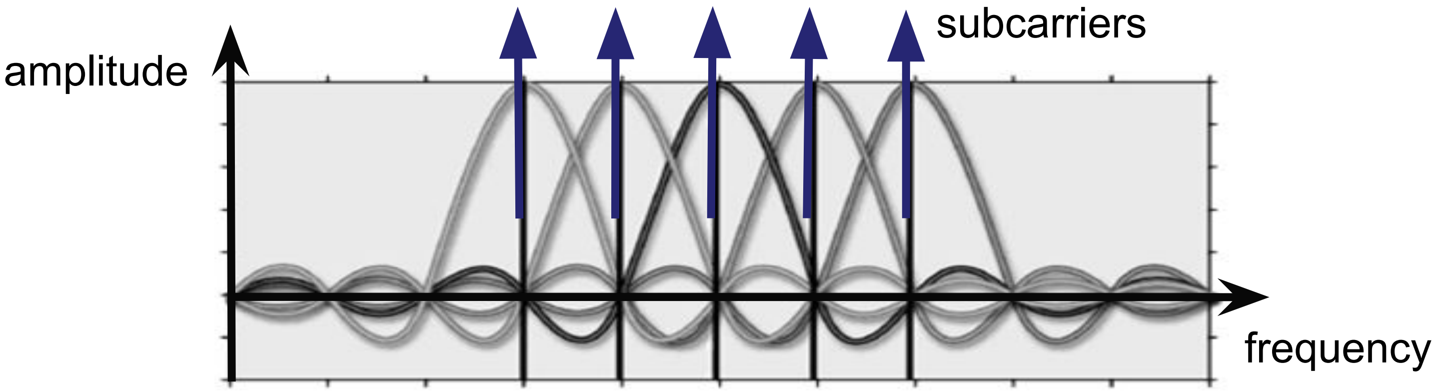


Multi-Carrier Transmitter



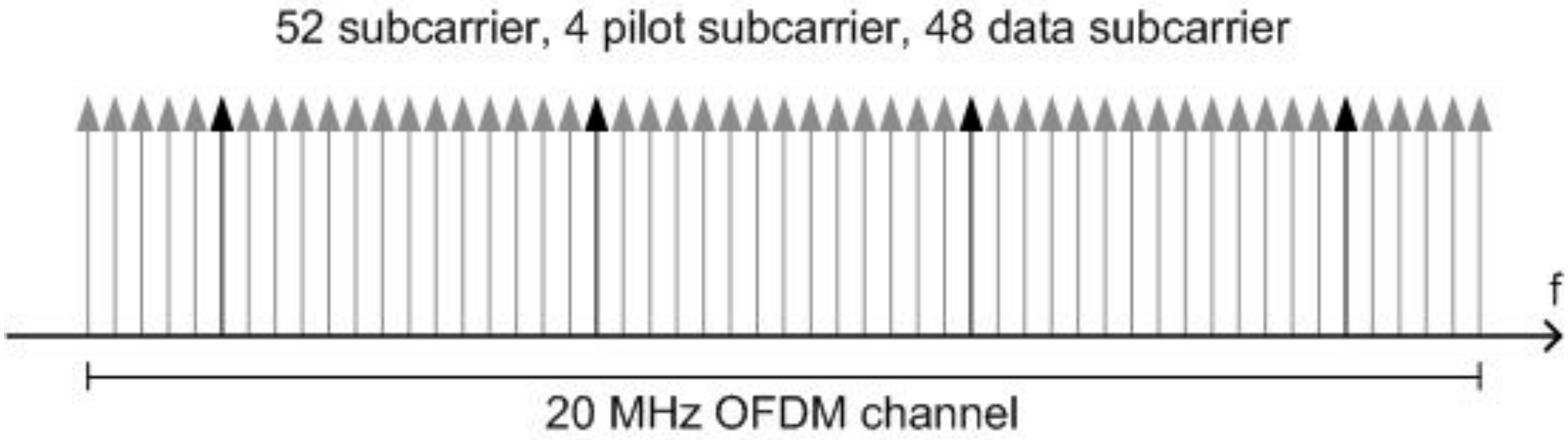
OFDM - Overview

- Orthogonal Frequency Division Multiplex
    - bandwidth is divided into subcarriers, subcarriers overlap but remain orthogonal
- High spectral efficiency, easy implementation using (I)FFTs



OFDM in IEEE 802.11a & 11g

- Data subcarriers are used for data transmission
- Pilot subcarriers are used for synchronization



OFDM - Overview

- OFDM Subcarriers
  - **Pilot** subcarriers: monitoring path shifts and ICI
  - **Data** subcarriers: data transmission
  - **Guard** subcarriers: nothing transmitted
- Design Challenge: Inter-Symbol Interference (ISI)
  - Multipath propagation: received signal arrives as an unpredictable set of reflected and direct radio waves → reason: signal delay spread
- “Inter-Channel” Subcarrier Interference (ICI)
  - Signals received from multiple indirect paths added to the direct path do not meet the condition of orthogonality between subcarriers → reason: frequency shift

IEEE 802.11a/g Parameters (1/2)

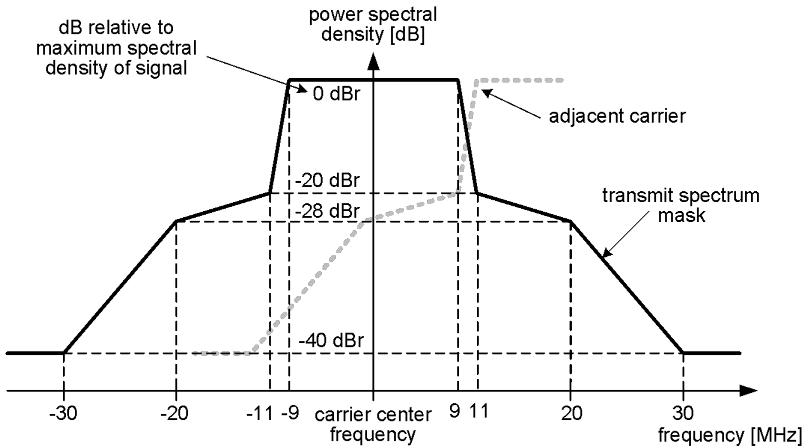
data rate [Mb/s]	modulation	coded bits per sub-carrier	coded bits per OFDM symbol	data bits per OFDM symbol
6	BPSK ½	1	48	24
9	BPSK ¾	1	48	36
12	QPSK ½	2	96	48
18	QPSK ¾	2	96	72
24	16-QAM ½	4	192	96
36	16-QAM¾	4	192	144
48	64-QAM 2/3	6	288	192
54	64-QAM¾	6	288	216

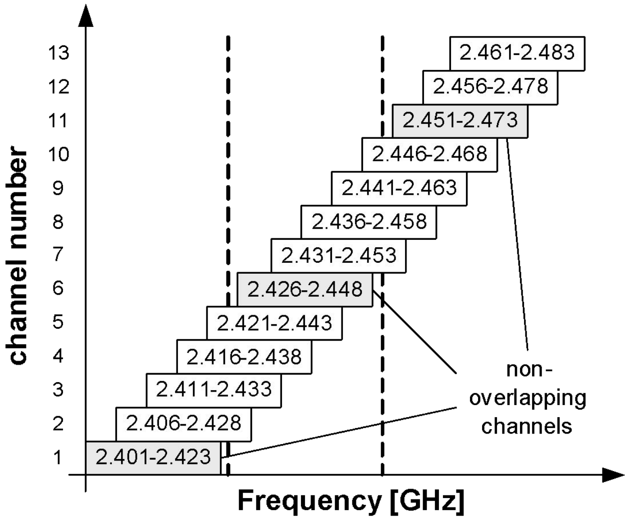
IEEE 802.11a/g Parameters (2/2)

parameter	value
Sampling rate 1/T	20 MHz
OFDM block duration Tb	64*T = 3.2 us
Guard interval duration Tg	16*T = 0.8 us
OFDM symbol duration Tb'=Tg+Tb	80*T = 4 us
Number of data sub-carriers	48
Number of pilot sub-carriers	4
Sub-carrier spacing Df	1/Tb = 0.3125 MHz
Spacing between the outmost sub-carriers	(Ntotal-1)* Df = 15.9375 MHz

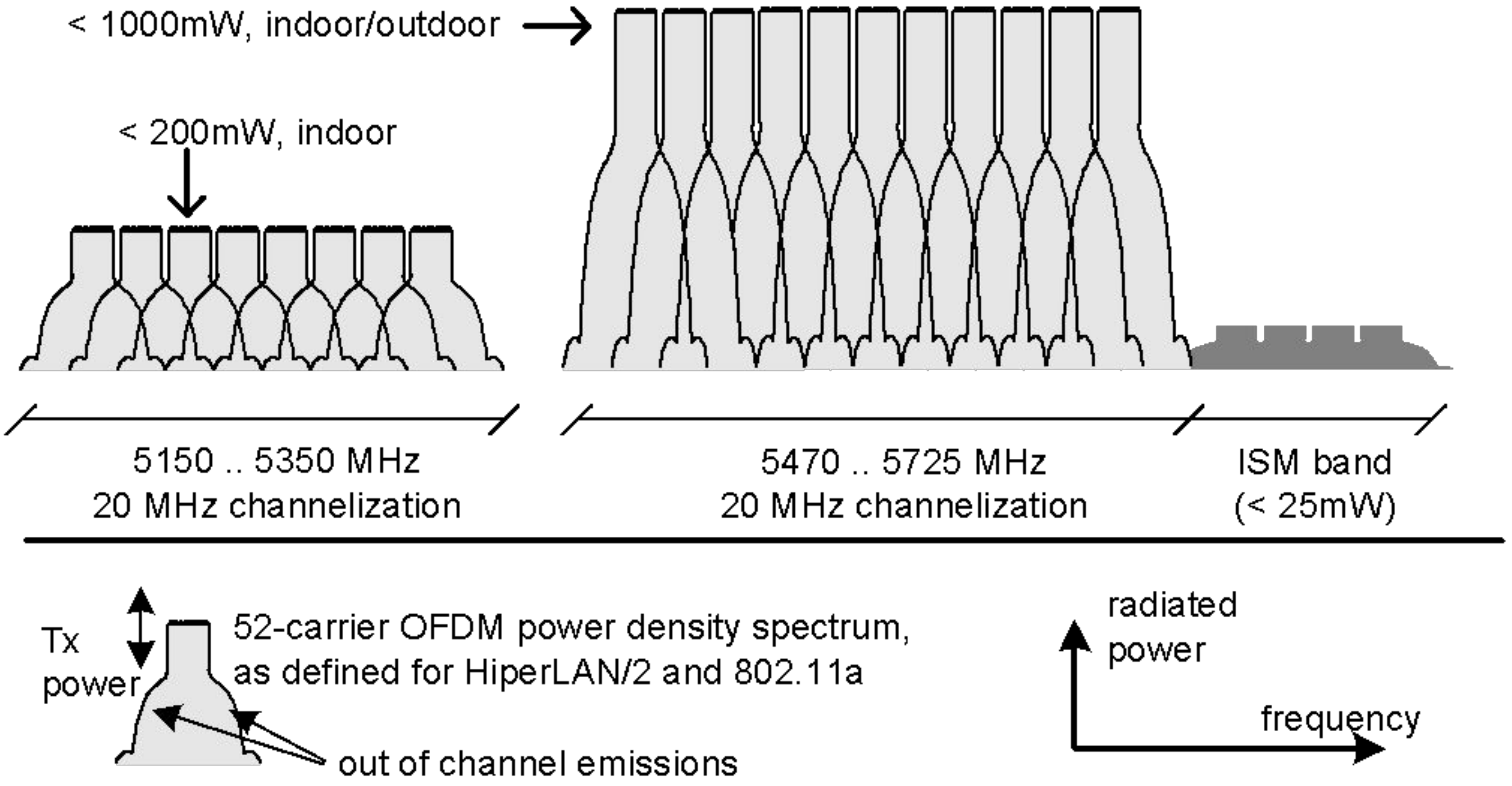
IEEE 802.11 Spectrum @ 2.4 GHz

- Transmit spectrum mask of 802.11a: limiting transmission power in frequency range
- Adjacent channels interfere with each other
  - Up to 13 channels, 3 are non-overlapping
-

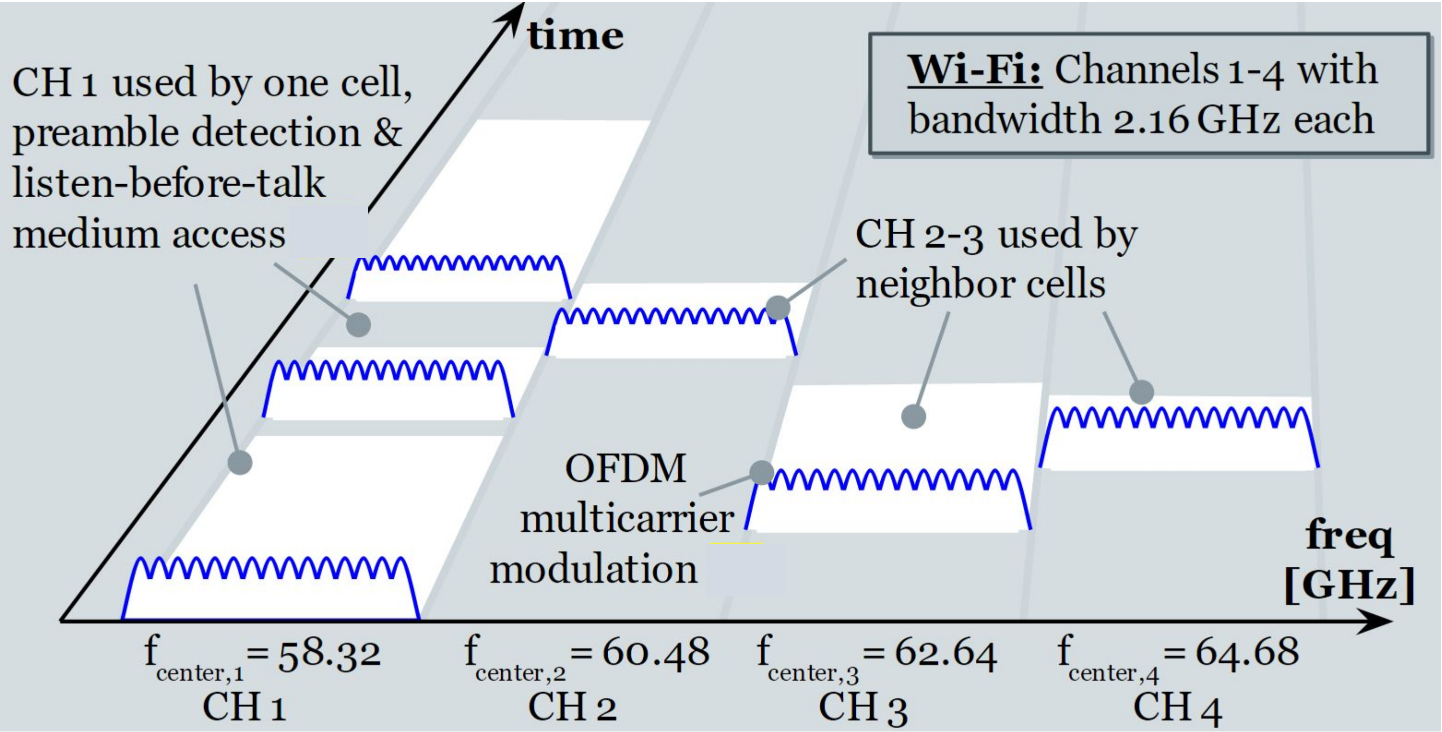




IEEE 802.11 Spectrum @ 5 GHz

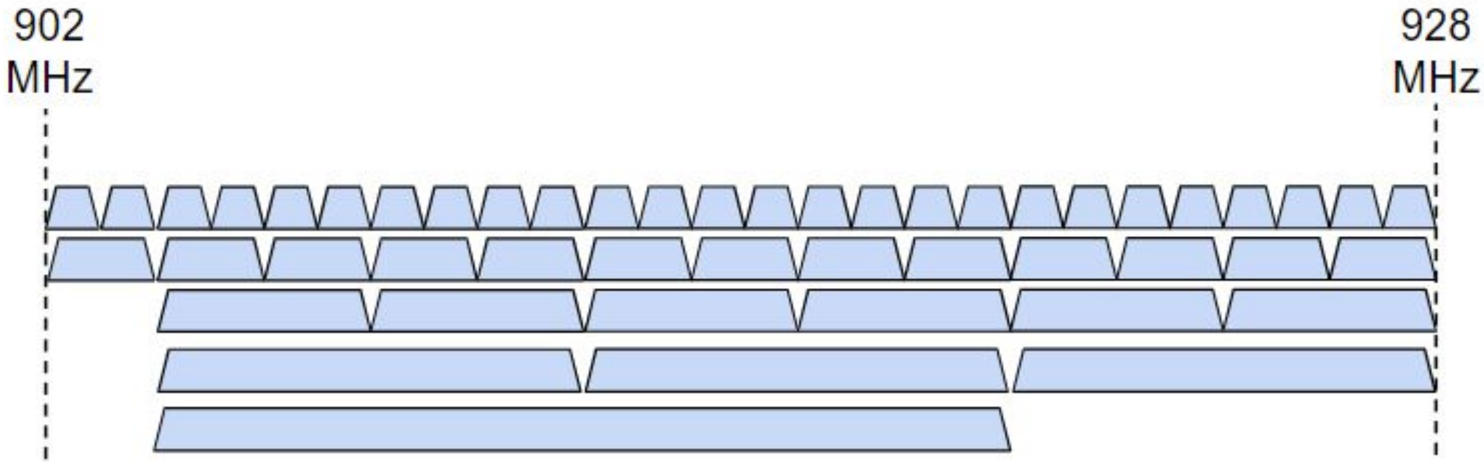


IEEE 802.11 Spectrum @ 60 GHz (OFDM, beyond Wi-Fi 6)



IEEE 802.11 Spectrum @ Sub 1 GHz

Wi-Fi Halow (explained later in this chapter)



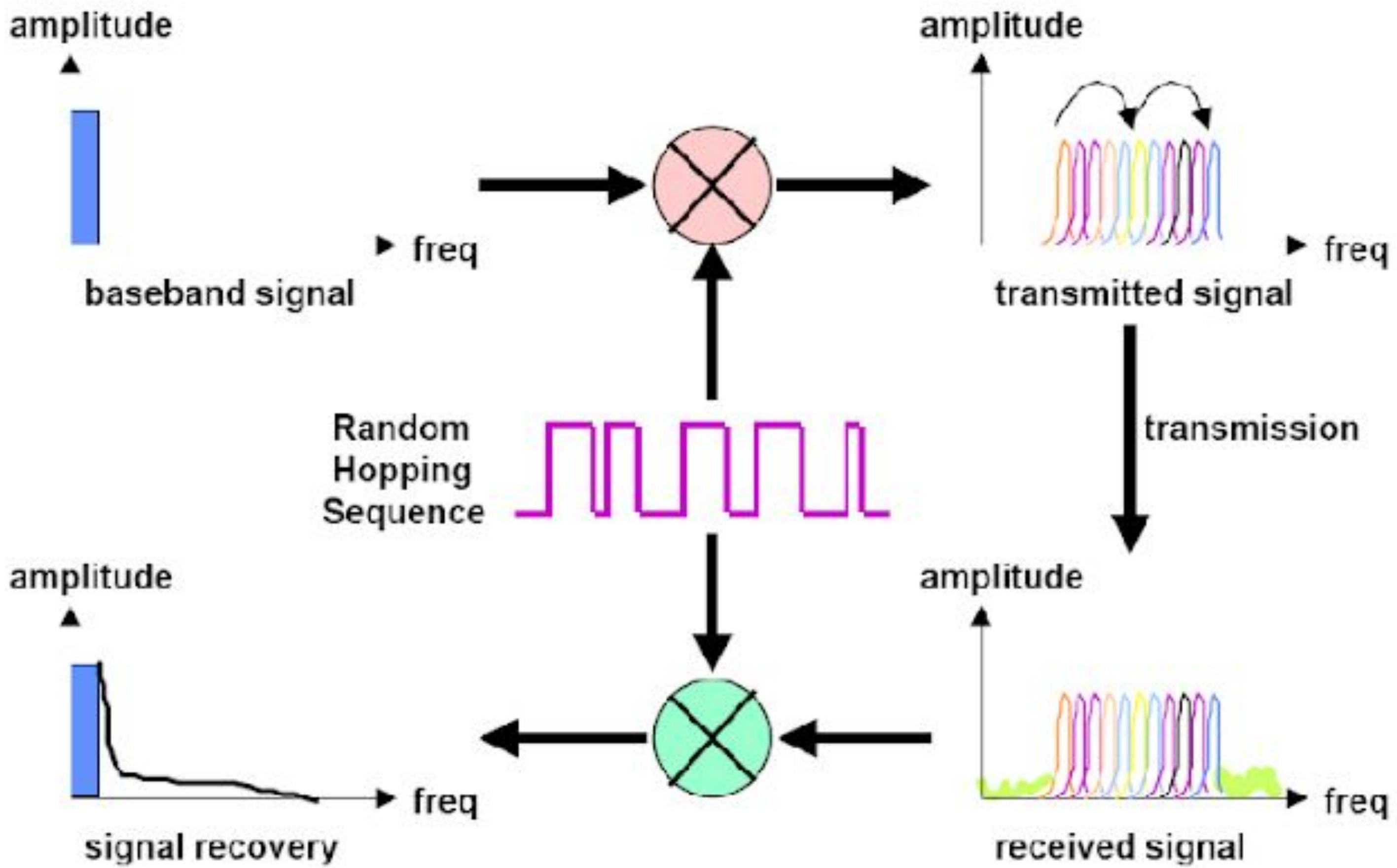
Examples of OFDM Usage

- Fixed line transmission technologies:
    - ADSL and VDSL broadband access via copper wiring
    - Power line communication (PLC), optical fiber communications
- Wireless:
    - IEEE 802.11a/g/n/ac/ah ... Wi-Fi Wireless LANs
    - IEEE 802.15.3a WiMedia Alliance's Ultra wideband (UWB) implementation
    - **Wi-Fi 6**
    - DAB systems, DVB terrestrial digital TV systems like DVB-T and DVB-H
    - IEEE 802.16 or WiMAX Wireless MANs
- 3GPP cellular, 4G Long Term Evolution (LTE) and 5G

Early / Basic Physical Layers of IEEE 802.11

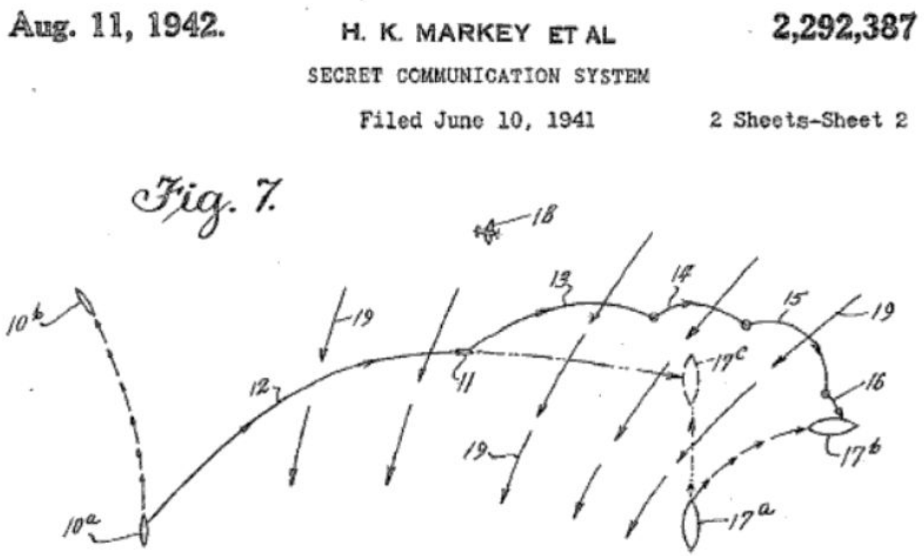
- Data rates of 1 Mb/s or 2 Mb/s
- Frequency Hopping Spread Spectrum (FHSS)
  - After short time intervals, operating frequency channel is periodically changed
  - List of selected frequencies is pseudo-random
- Direct Sequence Spread Spectrum (DSSS)
  - All stations operate at same center frequency
  - Transmitted signal is spread over full bandwidth
  - This is not CDMA: all stations operate with same code sequence!
- Infrared (IR)
  - So far no commercial success but attractive for future (light vs. radio)

Frequency Hopping Spread Spectrum FHSS

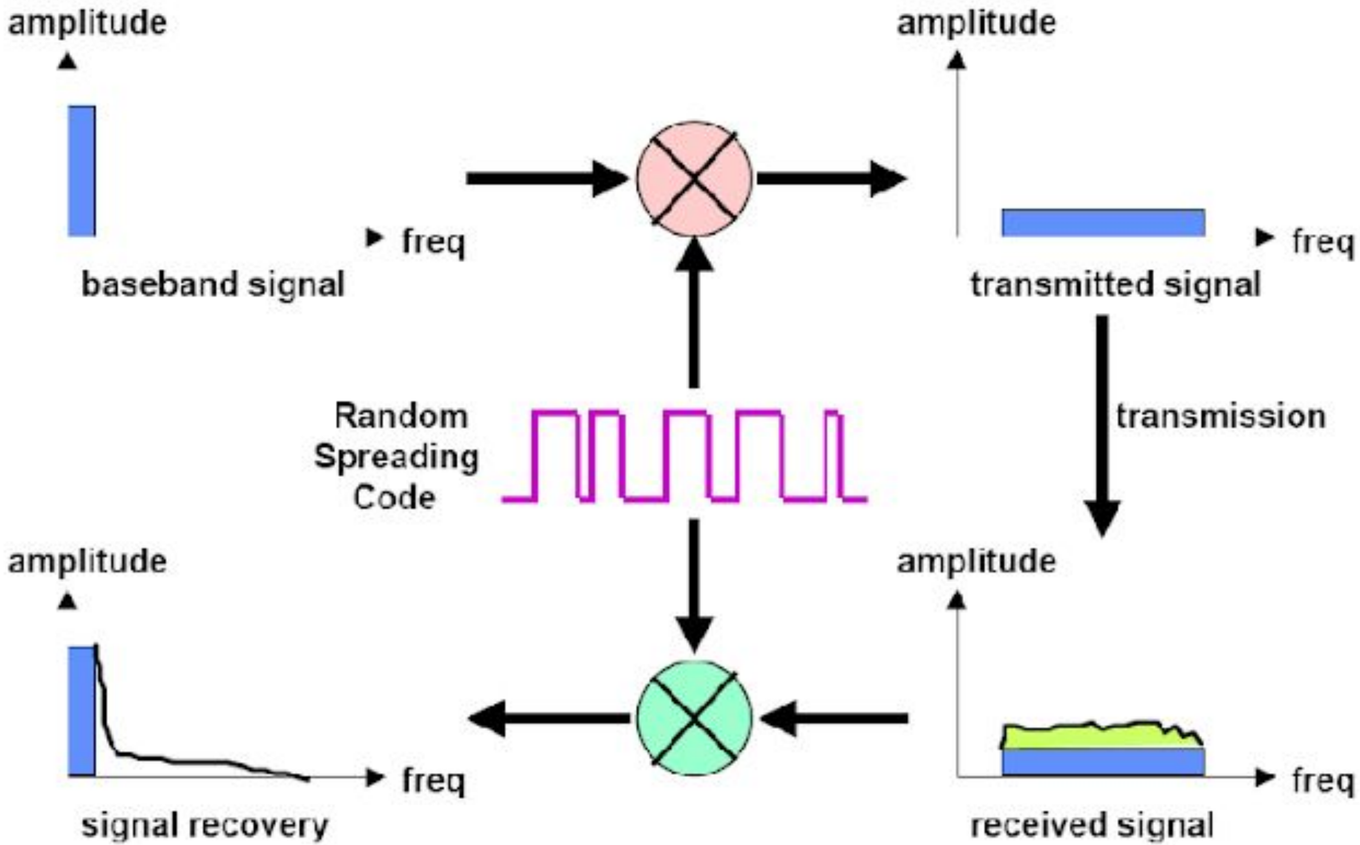


Patent on “Secret Communication System“, 1942

- Co-inventor: Hedy Lamar, famous Hollywood actress



Direct Sequence Spread Spectrum DSSS



11 Mb/s Physical layer: IEEE 802.11b

- Extension of 802.11 @2.4GHz, in 1999
- Raw data rates of 5.5 Mb/s or 11 Mb/s
- “High Rate“ Direct Sequence Spread Spectrum
  - HR/DSSS, channel bandwidth and channelization scheme equal to DSSS
- 8-chip Complementary Code Keying (CCK) modulation
  - CCK works only in conjunction with DSSS
  - Permits codes to represent greater volume of information
- IEEE 802.11b standard extension was
  - The first known under the acronym Wireless Fidelity (Wi-Fi)
  - The first 802.11 standard with significant commercial success

54 Mb/s Physical Layer: IEEE 802.11a

- OFDM operation @ 5GHz, 20 MHz channel bandwidth, 52 subcarriers
    - Uses 802.11 core protocol as original standard, in 1999
    - Not compatible to 802.11b

Data Rate [Mb/s]	modulation	coded bits per subcarrier	coded bits per OFDM symbol	Data bits per OFDM sysmbol	1472 byte transfer duration (µs)
6	BPSK ½	1	48	24	2012
9	BPSK ¾	1	48	36	1344
12	QPSK ½	2	96	48	1008
18	QPSK ¾	2	96	72	672
24	16-QAM ½	4	192	96	504
36	16-QAM¾	4	192	144	336
48	64-QAM 2/3	6	288	192	252
54	64-QAM¾	6	288	216	224

54Mb/s Physical Layer: IEEE 802.11g at 2.4GHz

- OFDM operation @ 2.4 GHz (same as 802.11b)
- Data rates: 6, 9, 12, 18, 24, 36, 48, and 54 Mb/s
  - Like 802.11a except some additional legacy overhead
- Backward compatible to non-OFDM
  - CCK for 5.5 and 11 Mb/s (802.11b)
  - DBPSK/DQPSK+DSSS for 1 and 2 Mb/s (802.11 legacy)
- 802.11b stations reduce the capacity of an 802.11g network
- Radio coverage range of 802.11g devices @2.4GHz is larger than that of 802.11a @ 5GHz

Operation @ Higher vs. Lower Frequencies

- Advantages @ 2.4 GHz
  - License-exempt (unlicensed) ISM band, good indoor radio signal penetration
  - High device penetration and low device costs
- Disadvantages @ 2.4 GHz
  - Only 3 non-overlapping channels, heavily used even by dissimilar radio systems (e.g. Bluetooth, microwave oven)
- Advantages @ 5 GHz
  - 19 non-overlapping channels, higher transmission power (100mW vs. 1W/4W)
- Disadvantages @ 5 GHz
  - Higher frequencies have higher path losses, reduced range → more dense deployment of APs

IEEE 802.11n MIMO with Multiple Antennas

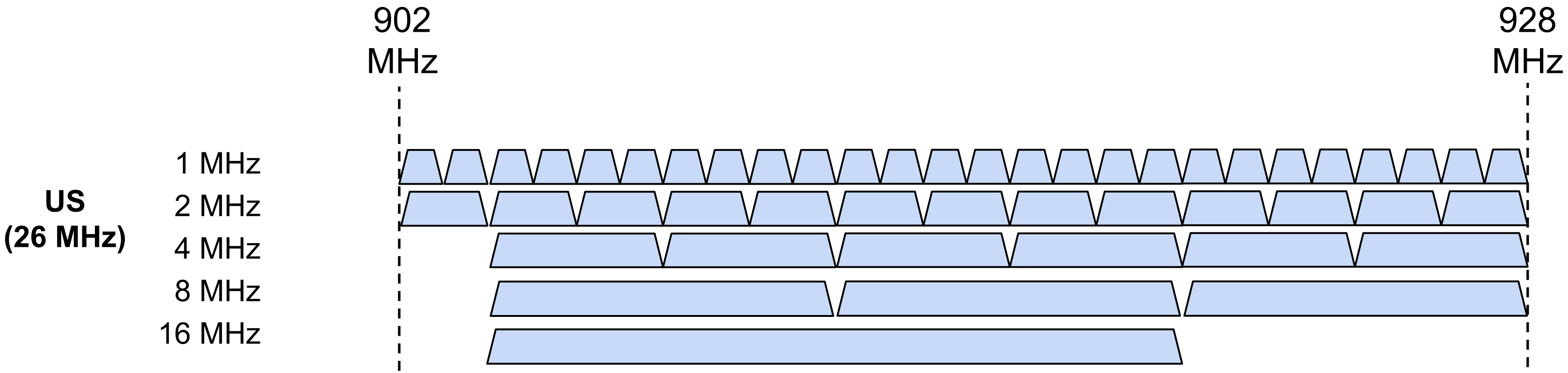
- High-Speed WLAN extension with up to 600 Mb/s
- Based on Multiple Input Multiple Output (MIMO)
- Quality-of-service management
- Channel bonding (= channel bundling) of two 20 MHz channels to one 40 MHz
- Operates at 2.4 GHz and 5 GHz band
  - 802.11n is compatible to 802.11b and 802.11g
- This is extended to multi-user MIMO in IEEE 802.11ac

Summary of the Basic Modes

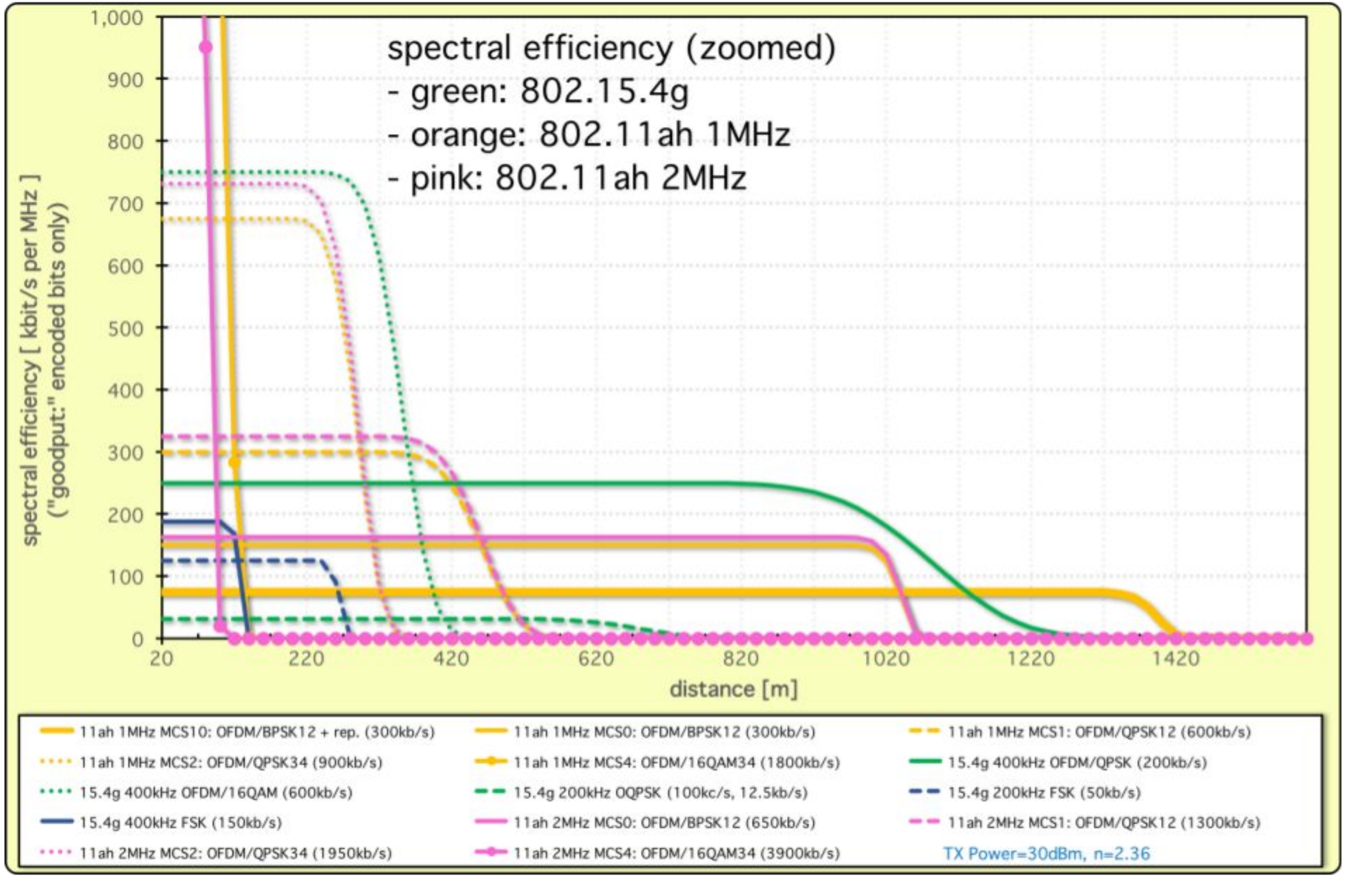
Physical Layer	Released	Frequency Band	Data Rate (max.)	Data Rate (typ.)	Range (indoor)	Range (outdoor)
Legacy	1997	2.4-2.5 GHz	2 Mb/s	0.7 Mb/s	~20 m	~75 m
802.11a	1999	5.15-5.825 GHz	54 Mb/s	23 Mb/s	~30 m	~100 m
802.11b	1999	2.4-2.5 GHz	11 Mb/s	4 Mb/s	~35 m	~110 m
802.11g	2003	2.4-2.5 GHz	54 Mb/s	19 Mb/s	~35 m	~110 m
802.11n	2007	2008.2.4 GHz and/or 5 GHz	248 Mb/s = 2x2 ant	74 Mb/s = 2x2 ant	~70 m	~160 m

- Further: 60GHz Wi-Gig, multi-user MIMO 802.11ac, TV White Space 802.11af, Internet-of-Things Wi-Fi Halow 802.11ah

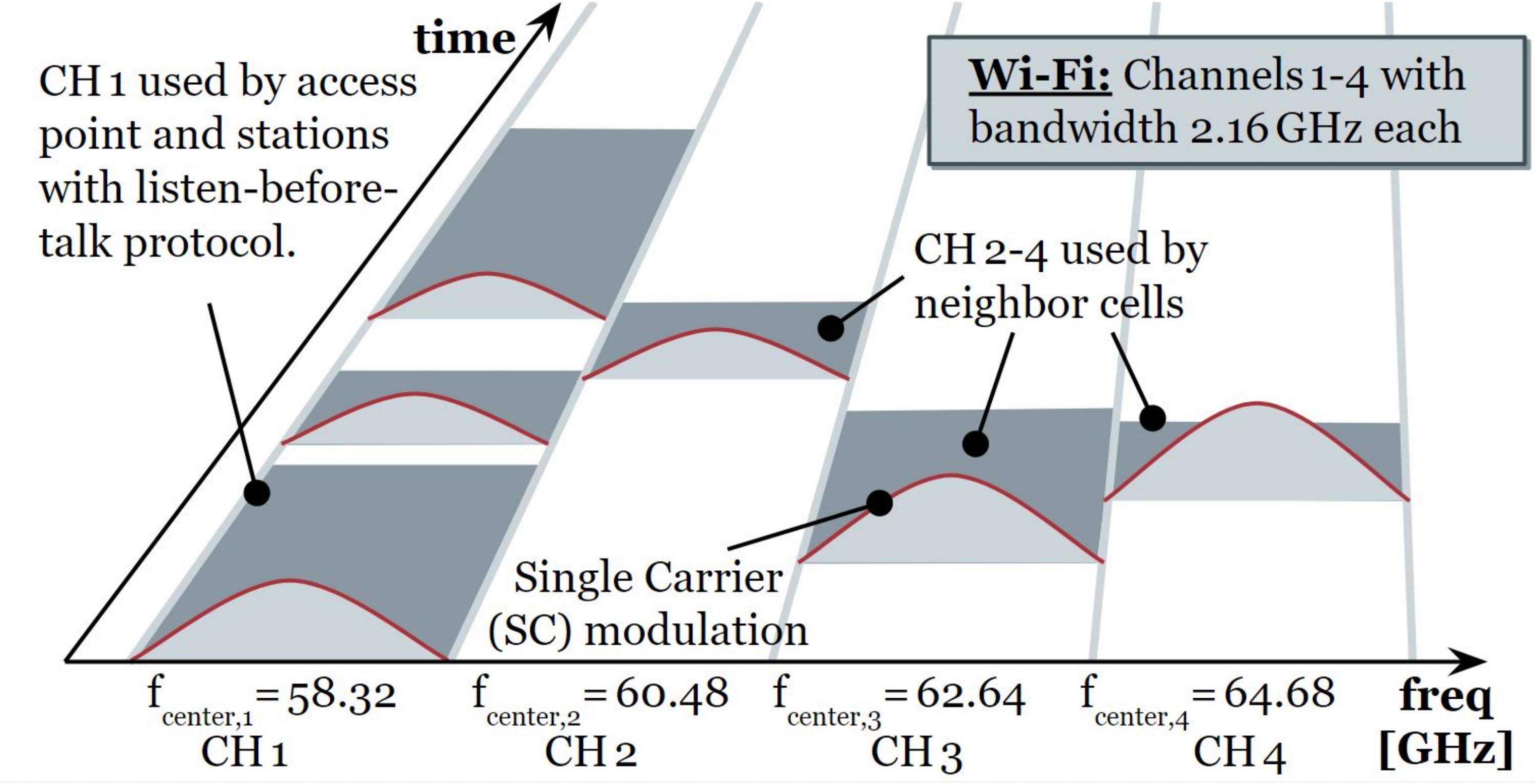
Internet-of-Things: Wi-Fi HaLow™ IEEE 802.11ah



Wi-Fi HaLow™ IEEE 802.11ah Performance



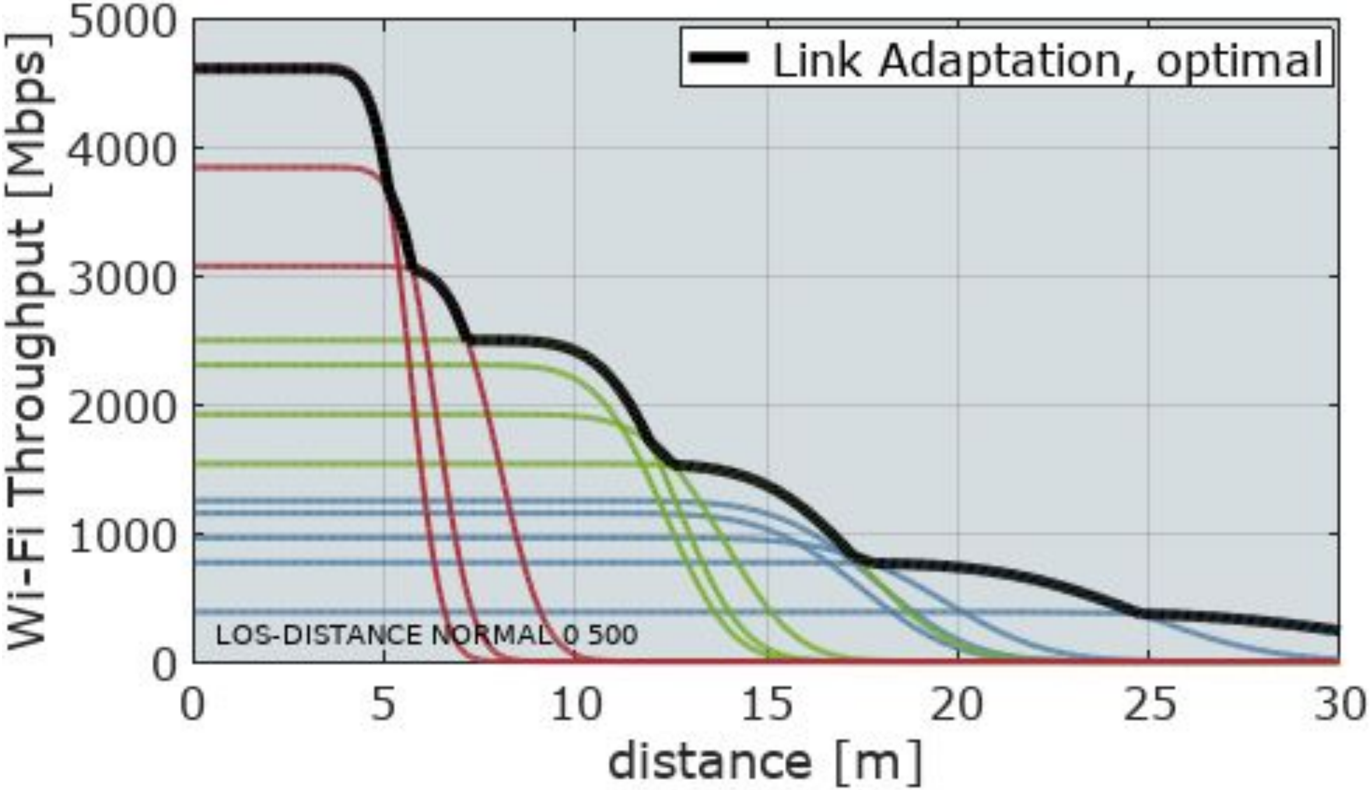
Very High Throughput at 60 GHz: IEEE 802.11ad



IEEE 802.11ad Single Carrier Modulation - Details

Channel bandwidth and center frequency	2160 MHz | 60.48 GHz
Signal bandwidth (-17 dBr transmit mask)	1880 MHz
Symbol rate (“SC chip rate” in 802.11ad)	1760 MHz
Symbol duration (“SC chip time” in 802.11ad)	1/1760 MHz = 0.56818 ns
Modulation	**π/2-BPSK | π/2-QPSK | π/2-16QAM**
Physical layer bitrate (modulated, no coding)	1760.0 Mbps | 3520.0 Mbps | 7040.0 Mbps
LDPC code rate MCS 1	1/4 **(repetition, with code rate 1/2)**
LDPC code rate MCS 2 … 12	1/2, 5/8, 3/4, 13/16
LDPC code word size	672 bit
LDPC coding gain (approx.)	**Rate 1/4:** 8.0 dB | **1/2:** 6.0 dB | **5/8:** 4.0 dB **Rate 3/4:** 3.0 dB | **13/16:** 3.2 dB
Physical layer bitrate (LDPC encoded data)	440.0 Mbps **(MCS1)** … 5280.0 Mbps **(MCS12)**
Block size (BPSK | QPSK | 16-QAM)	448 bit | 896 bit | 1792 bit
Block duration (encoded data only)	254.55 ns
Golay sequence preceding each block	64 BPSK symbols (64 bit) | **duration:** 36.364 ns
Block duration (LDPC encoded data + Golay)	290.91 ns
Physical layer bitrate (LDPC encoded data + Golay)	385.0 Mbps **(MCS1)** … 4620.0 Mbps **(MCS12)**

IEEE 802.11ad Single Carrier Performance



Wireless Networking and Mobile Computing

3. IEEE 802.11 Wireless LAN (Wi-Fi)

(b) Medium Access Control Layer 2

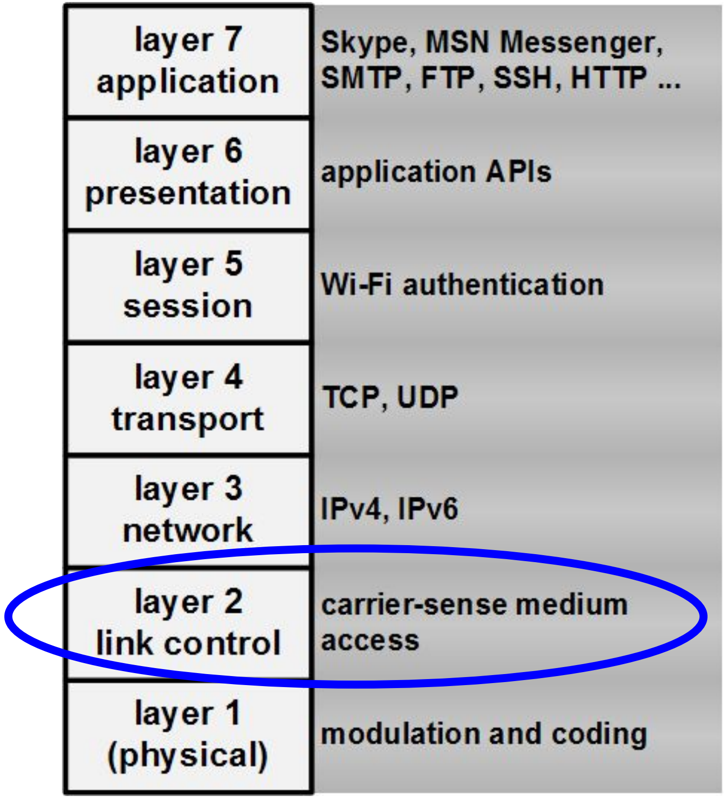
Stefan Mangold

Course Outline

1. **Introduction**
2. **Wireless Communication Basics**
3. **IEEE 802.11 Wireless LAN (Wi-Fi) -** (b) Medium Access Control Layer 2
4. **IEEE 802.15 Wireless PAN (ZigBee & Bluetooth)**
5. **Mobile Computing Algorithm Basics: Control and Game Theory**
6. **Visible Light Communication**
7. **Audio Communication**
8. **Cellular Networking Basics (LTE, 5G, Internet-of-Things)**
9. **Mobile Computing for Automated Medicine Delivery**
10. **Cognitive Radio, Delay Tolerant Networking, Radio Spectrum Sharing**

ISO/OSI Reference Model - Layer 1 and Layer 2

- ISO: International Organization for Standardization
- OSI: Open Systems Interconnection

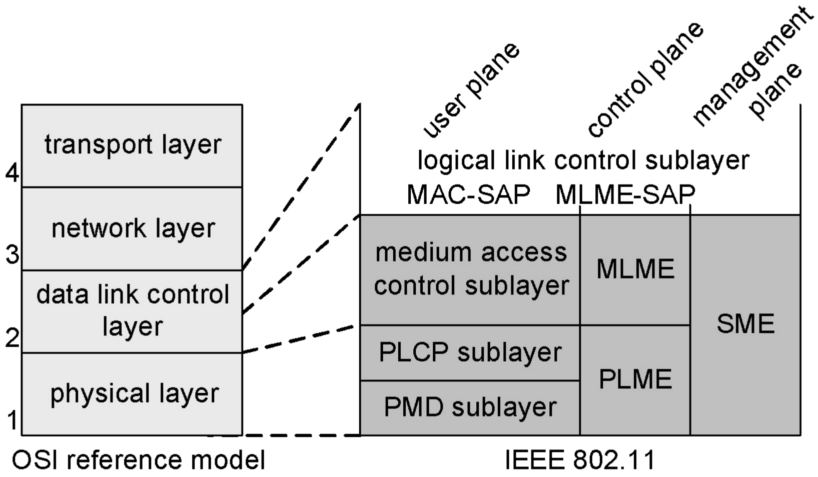


IEEE 802.11™ Overview

- Root document: IEEE 802.11 approved 1997
  - Amendments: extensions & refinements of IEEE 802.11
  - IEEE Std 802.11-2007: replacing IEEE 802.11 a/b/d/g/h…
  - IEEE Std 802.11™ -2020, was published in February, 2021
- Wi-Fi Alliance
  - Global, non-profit organization
  - Goal: Driving the adoption of a single worldwide standard
  - Test plans, interoperability & certification
  - “Wi-Fi certified” is a trademarked brand

IEEE 802.11 Reference Model

- Layer 1: PHY transmission schemes
- Layer 2: MAC protocols, MAC Layer Management Entity (MLME)
- Layer 1 & 2: Station Management Entity (SME)
- Interface to higher layers: Service Access Points (SAPs)



IEEE 802.11 List of Extensions (1/2)

document	content	status
IEEE 802.11	1 Mb/s and 2 Mb/s, @ 2.4 GHz, RF and IR	1997
IEEE 802.11a	54 Mb/s @ 5 GHz	1999
IEEE 802.11b	Enhancements to 802.11 to support 5.5 and 11 Mb/s	1999
IEEE 802.11c	Bridge operation procedures; included in IEEE 802.1D	2001
IEEE 802.11d	International (country-to-country) roaming extensions	2001
IEEE 802.11e	Quality-of-Service enhancements	2005
IEEE 802.11g	54 Mb/s, @ 2.4 GHz (backwards compatible with b)	2003
IEEE 802.11h	Spectrum managed 802.11a (5 GHz)	2004
IEEE 802.11i	Enhanced security	2004
IEEE 802.11j	Extensions for Japan	2004
IEEE 802.11k	Radio resource measurement enhancements	2007
IEEE 802.11m	Maintenance of the standard	always ongoing

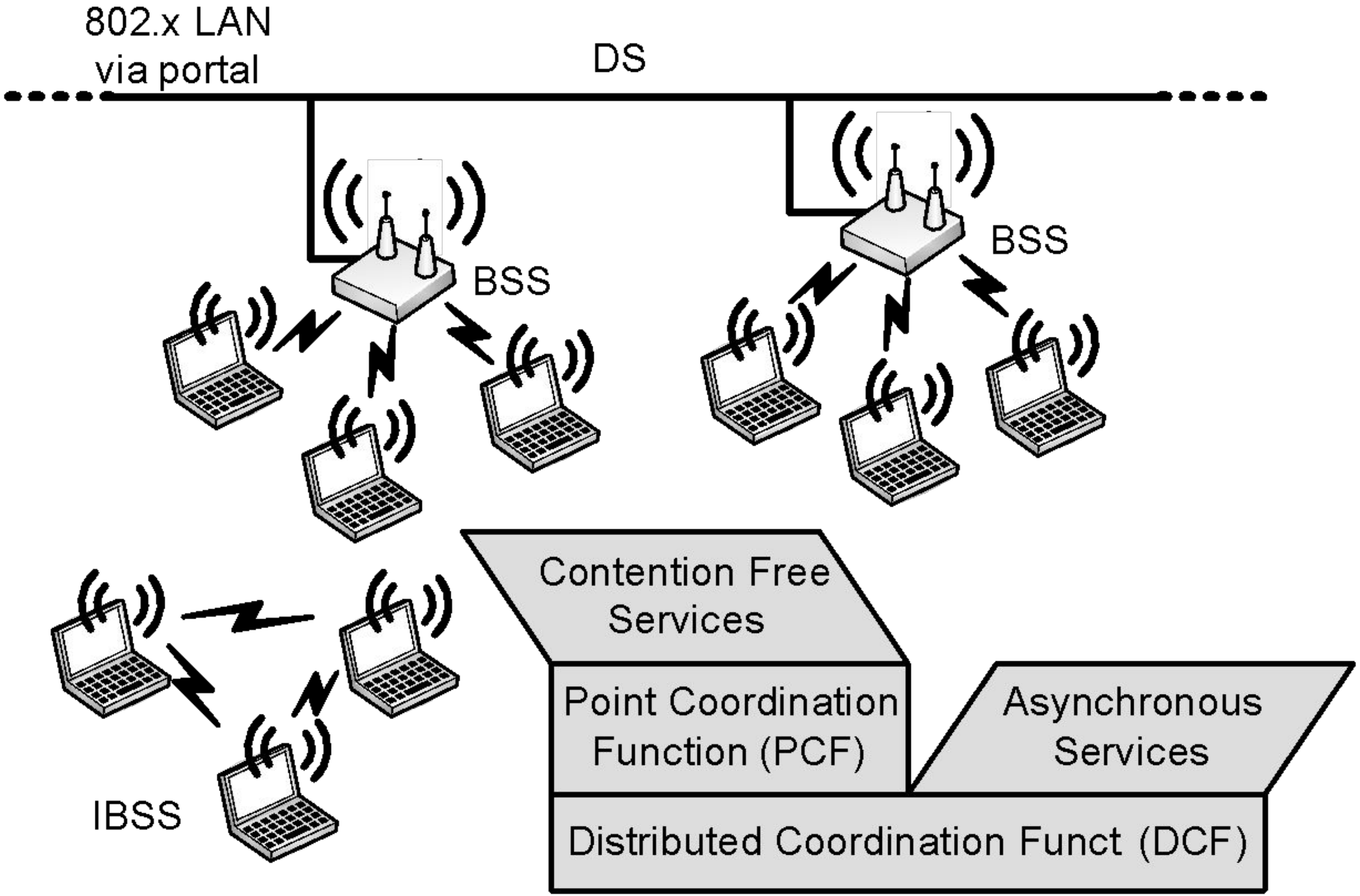
IEEE 802.11 List of Extensions (2/2)

document	content	status
IEEE 802.11n	Higher throughput improvements using MIMO	2008
IEEE 802.11p	WAVE - Wireless Access for Vehicular Environment	2009
IEEE 802.11r	Fast roaming	2007
IEEE 802.11s	ESS Extended Service Set Mesh Networking	2008
IEEE 802.11u	Interworking with non-802 networks (cellular)	2009
IEEE 802.11v	Wireless network management	2012
IEEE 802.11w	Protected Management Frames	2012
IEEE 802.11y	3650-3700 MHz Operation in U.S.	2009
IEEE 802.11z	**Direct Link Setup**	**2010**
…	… more extensions exist	…
IEEE 802.11ad	60GHz	2018, ongoing
IEEE 802.11af	TV White Space	2016
IEEE 802.11ah	Sub 1GHz, Internet of Things	2018
IEEE 802.11ax	**Wi-Fi 6: all of the above, plus higher modulation, OFDMA, power mgmt**	**2019, ongoing**

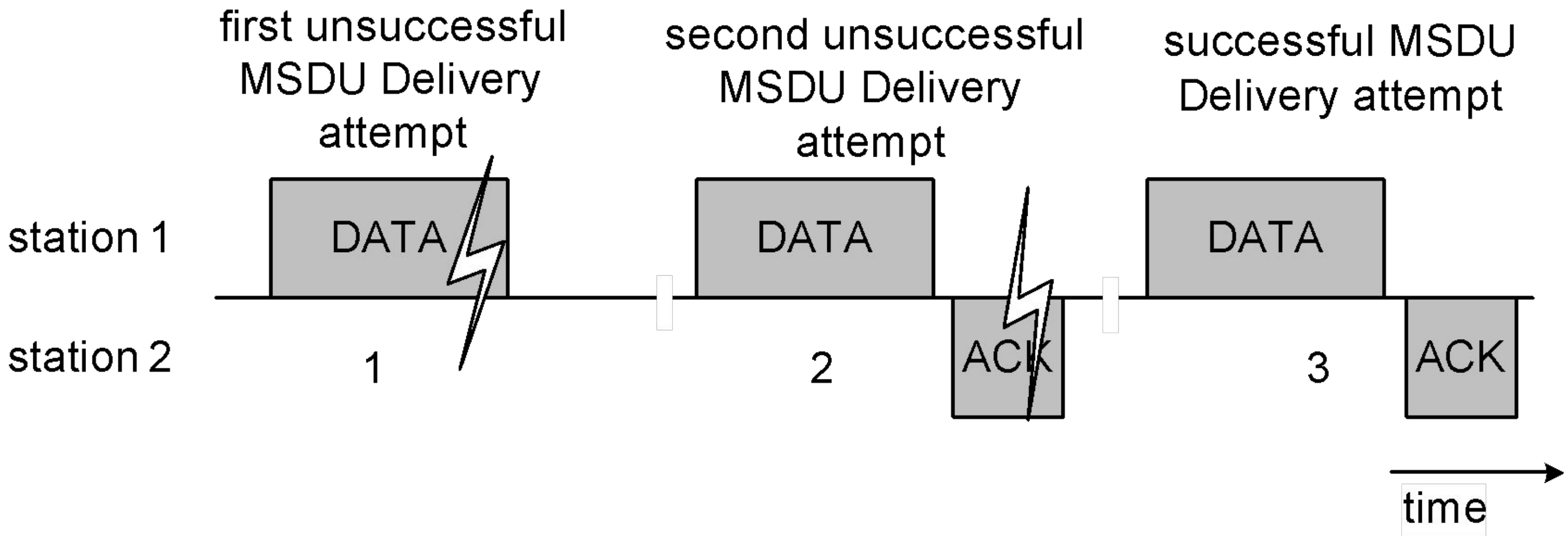
IEEE 802.11 Architecture

- BSS = Basic Service Set, with access point
- IBSS = Independent BSS, for ad hoc networks
- DS = Distribution System
- Distributed Coordination Function (DCF) = distributed control
- Point Coordination Function (PCF) = centralized control
    - PCF is not implemented in today's commercial products

IEEE 802.11 Architecture Illustrated

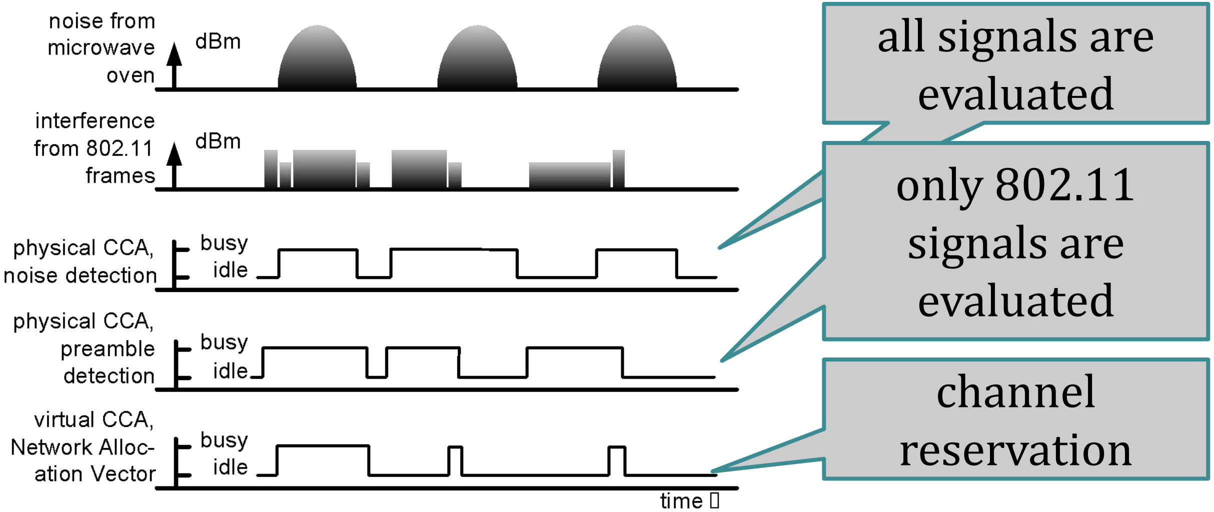


802.11 Example Frame Exchange



- First attempt: DATA frame from station 1 is not received, no ACK
- Second attempt: DATA is successfully received, ACK is sent but missed by station 1 (might be because of interference)
- Third and successful attempt: DATA and ACK are received

Carrier Sensing ("listen before talk")



- Channel sensing function: Clear Channel Assessment (CCA)
  - Fixed power threshold of -82dm (implementation dependent)
  - Channel is determined as busy when the detected power is larger than threshold
  - Network Allocation Vector (NAV): timer for reserving channel, defines duration of following frame exchange. No transmissions are allowed until timer is expired.

MAC Frames (Mac Service Data Units, MSDUs)

Management frame (beacon, association, authentication)

bytes:	2	2	6	6	6	2	0-2304 (2312 w/ WEP)	4
fields:	frame contr.	Dur./ID	DA	SA	BSS ID	seq. control	frame body	FCS

MAC header

Data frame (DATA)

bytes:	2	2	6	6	6	2	6	0-2304 (2312 w/ WEP)	4
fields:	frame contr.	Dur./ID	addr1	addr2	addr3	seq. control	addr4	frame body	FCS

MAC header

Control frame (RTS)

bytes:	2	2	6	6	4
fields:	frame contr.	Dur./ID	RA	TA	FCS

MAC header

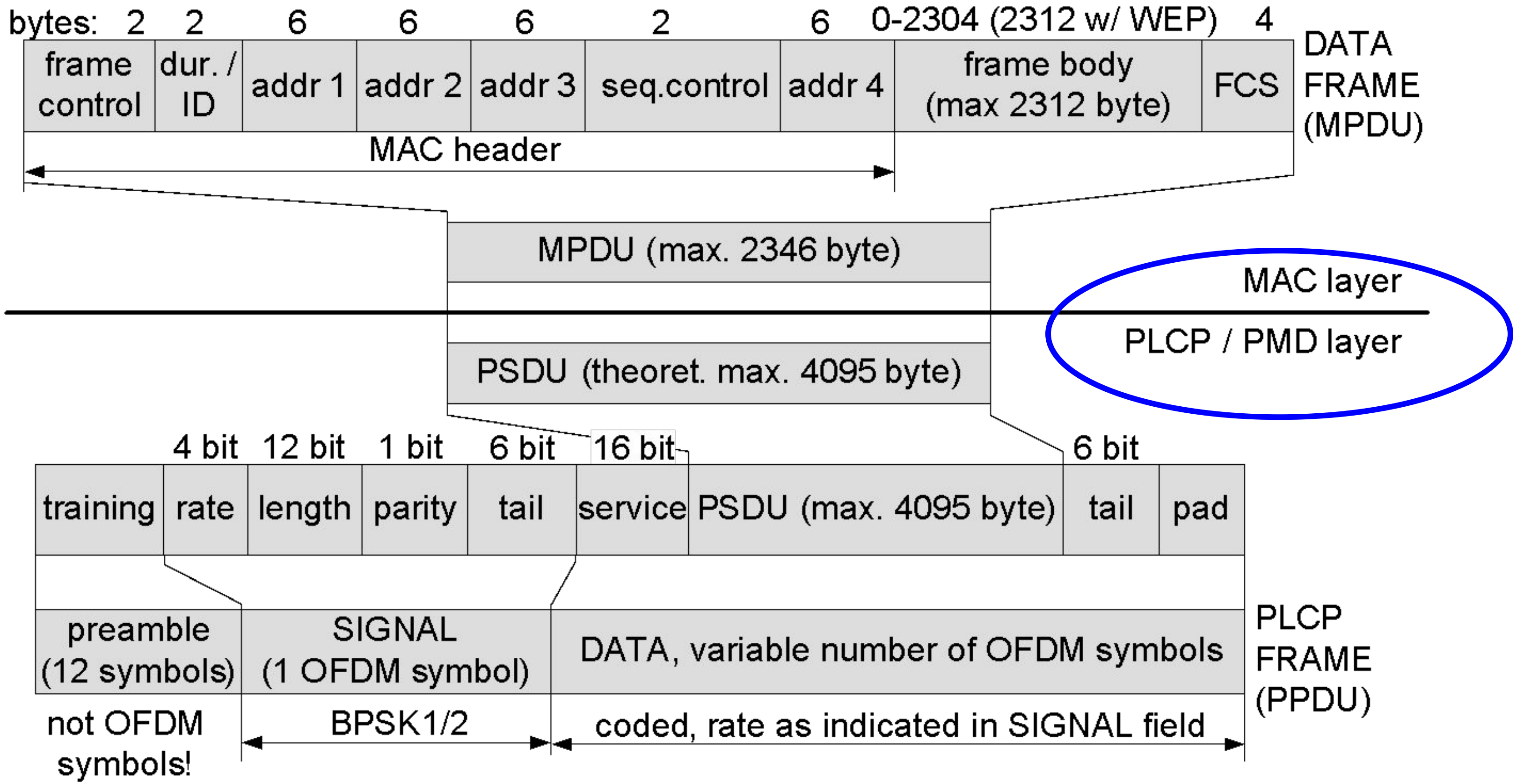
Control frame (CTS, ACK)

bytes:	2	2	6	4
fields:	frame contr.	Dur./ID	RA	FCS

MAC header

DA/SA: Destination / Source Address
RA/TA: Receiving station / Transmitting station Address

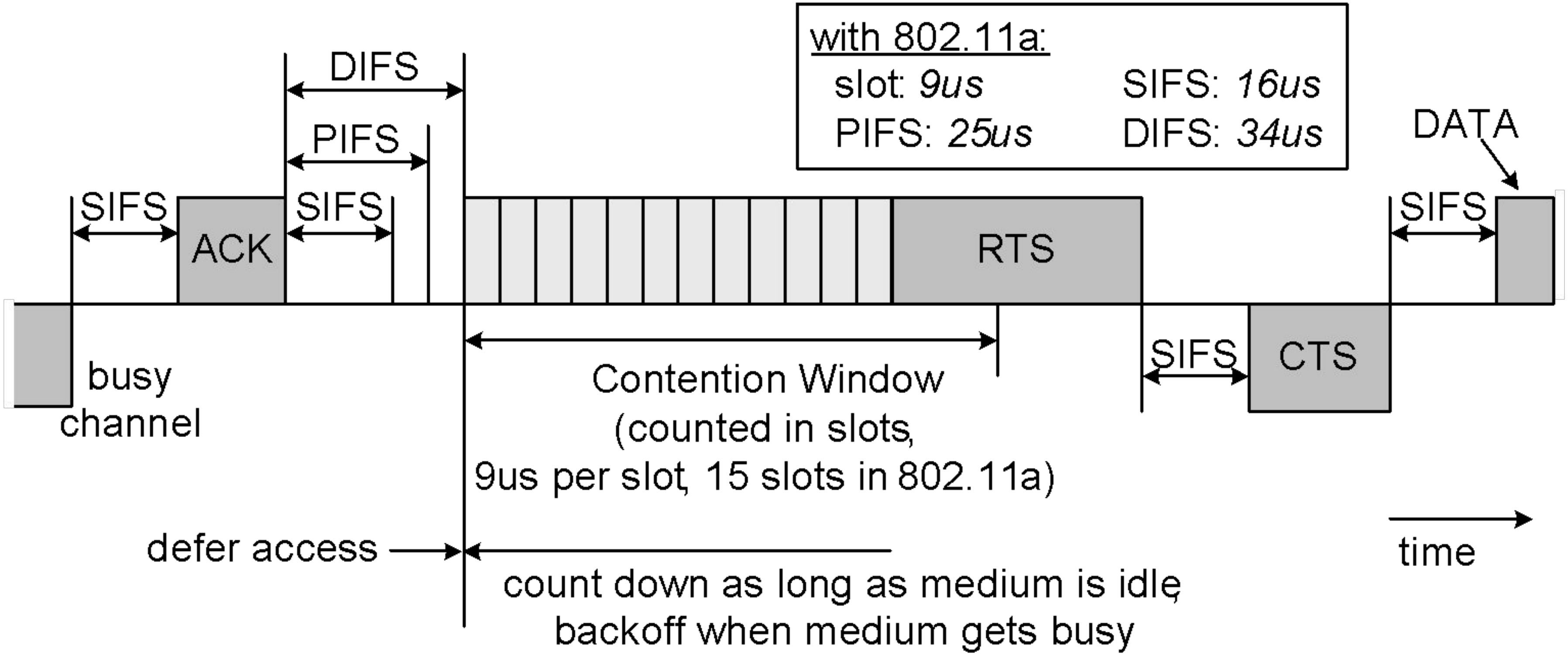
802.11 Frame Mapping MAC <-> PHY



Distributed Coordination Function (DCF)

- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - listen-before-talk principle and backoff procedure
- CCA carrier sensing is used to detect idle channel
  - CCA = Clear Channel Assessment
  - collision avoidance (not: Collision Detection)
- Packet transmission is initiated after certain idle time:
  - SIFS = Short Interframe Space (no CCA carrier sensing)
  - PIFS = PCF Interframe Space = SIFS + aSlotTime (with CCA)
  - DIFS = DCF Interframe Space = PIFS + aSlotTime (with CCA)
- SIFS is needed for transceiver turnaround

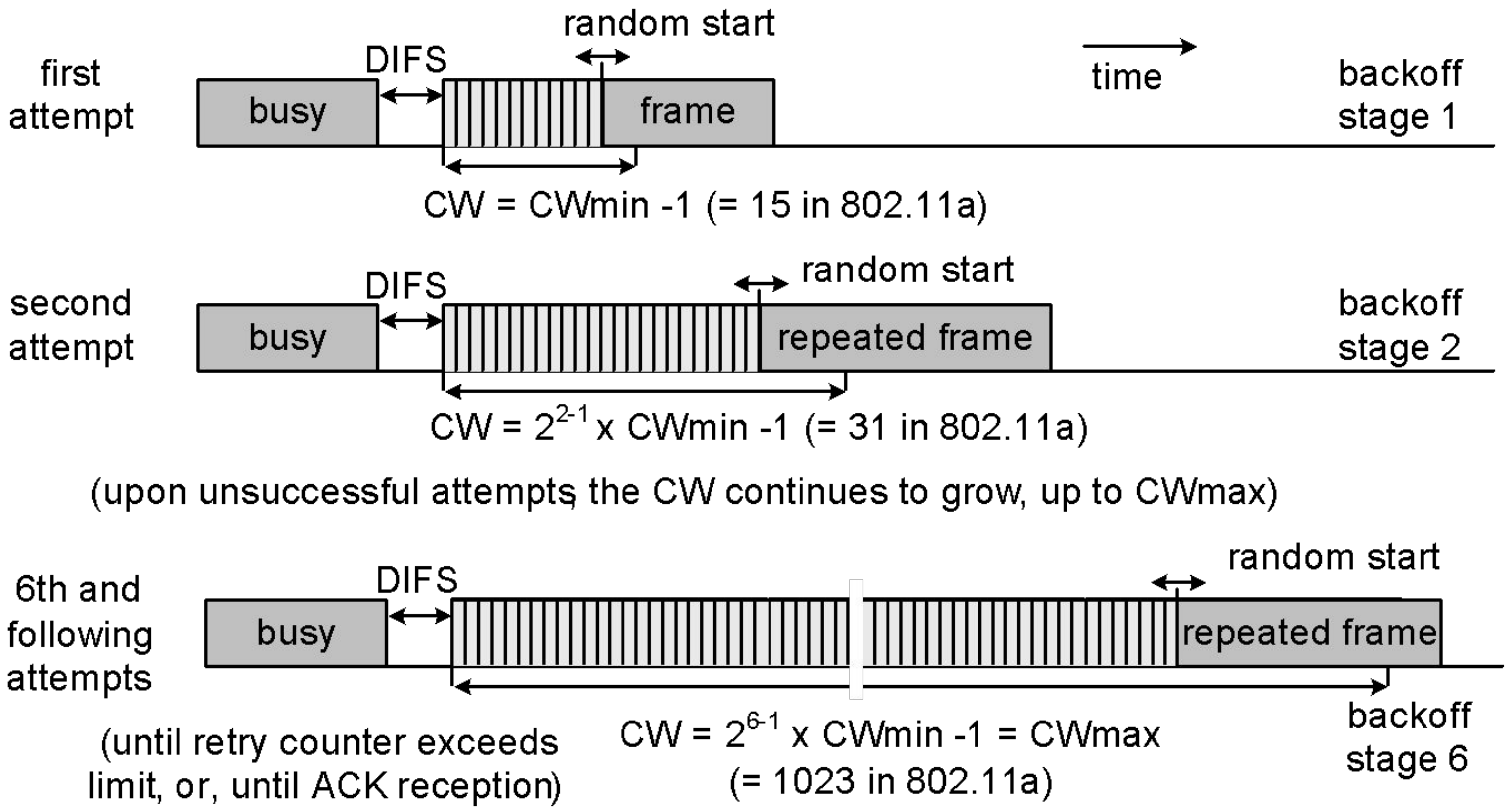
DCF Illustrated

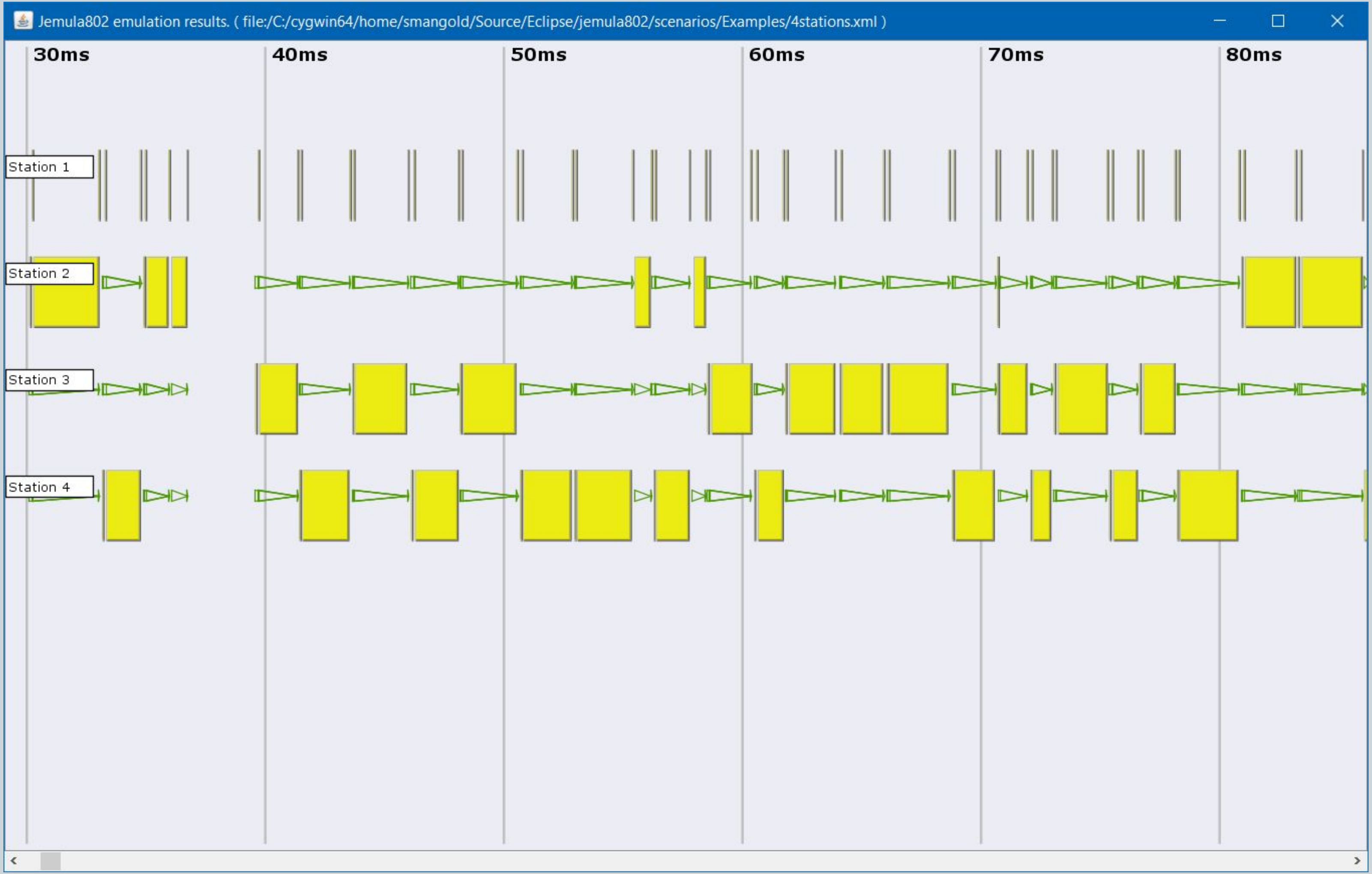


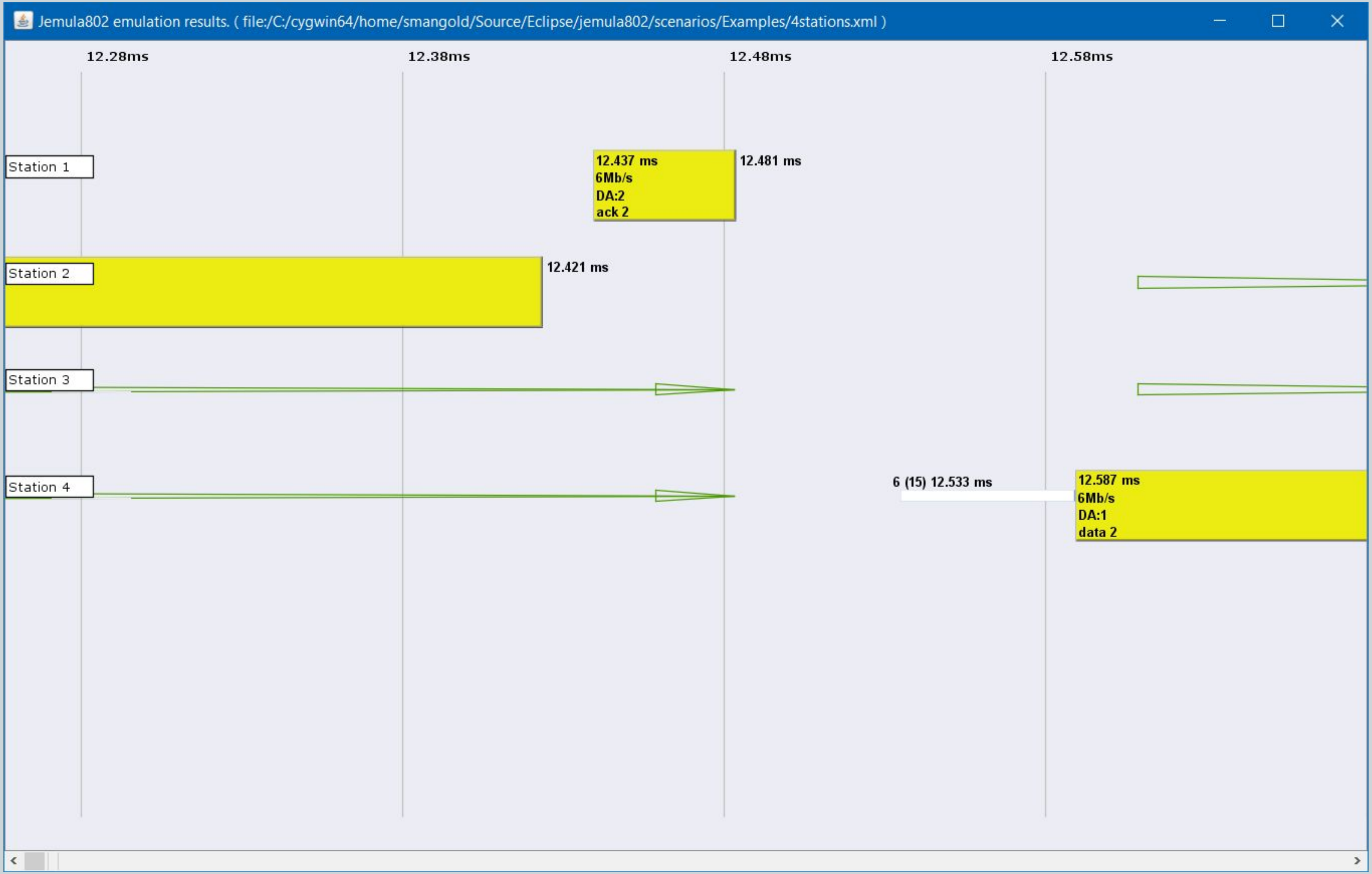
DCF Backoff Window

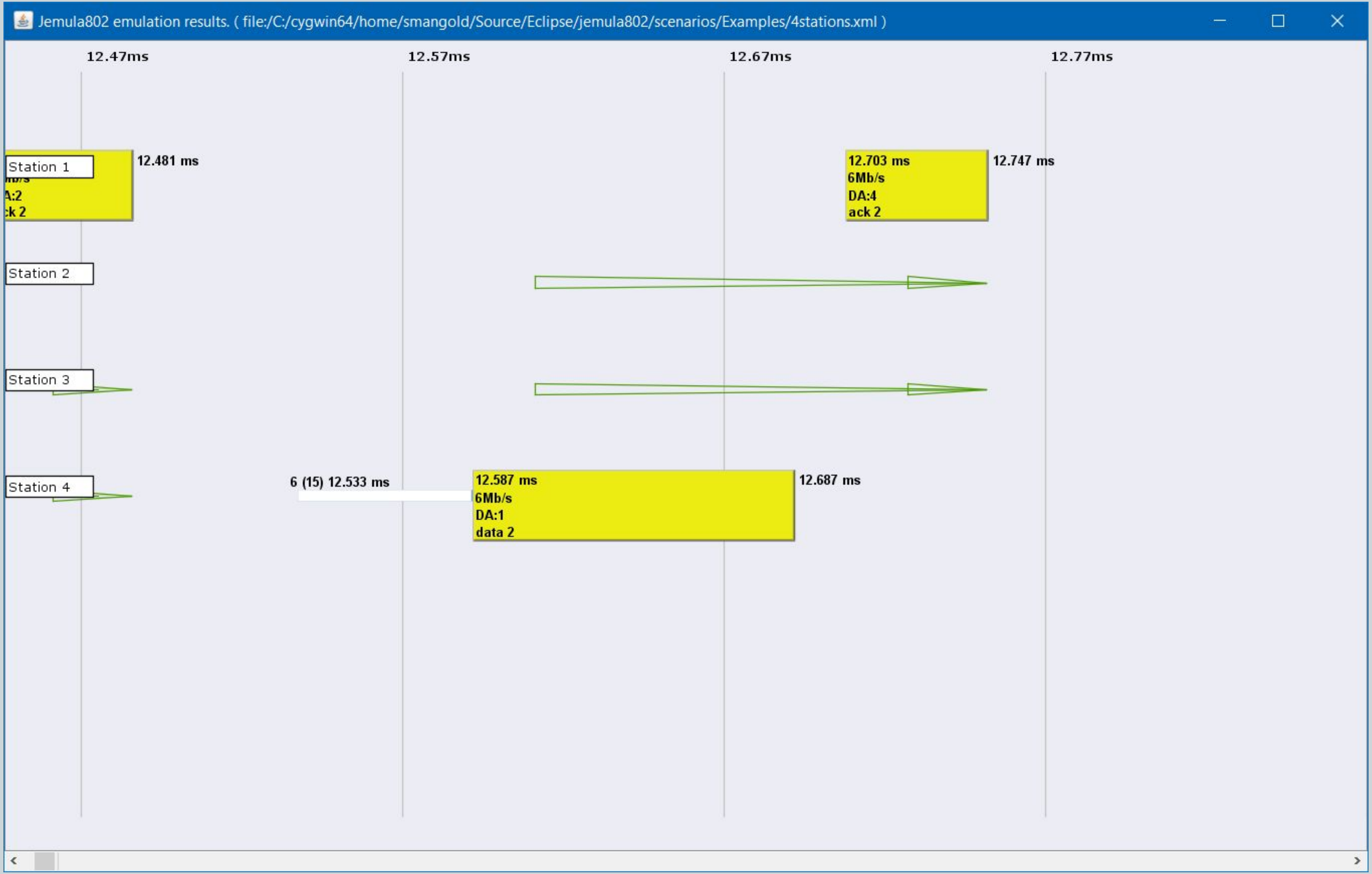
- Backoff is performed in case of collision
  - Random value is drawn out of contention window
- Backoff's contention window size (CW) is exponentially increased in case of repeated collisions
- Backoff procedure has two parameters
  - Minimum contention window size CWmin
  - Maximum contention window size CWmax
  - Example values for 802.11a: CWmin=16 and CWmax=1024

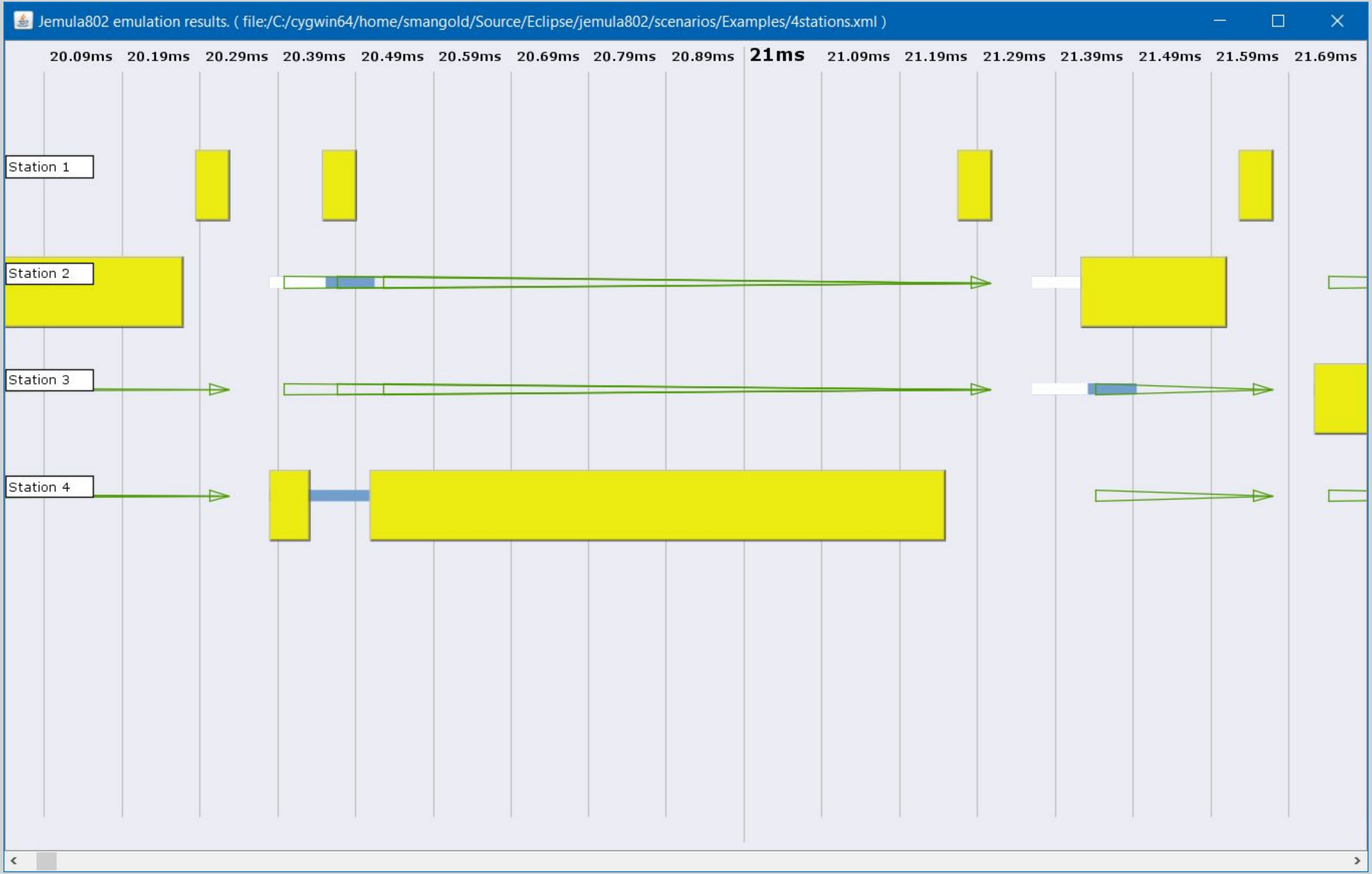
DCF Backoff Window Illustrated




Jemula802 emulation results. (file:/C:/cygwin64/home/smangold/Source/Eclipse/jemula802/scenarios/Examples/4stations.xml)
30ms
40ms
50ms
60ms
70ms
80ms
Station 1
Station 2
Station 3
Station 4


Jemula802 emulation results. (file:/C:/cygwin64/home/smangold/Source/Eclipse/jemula802/scenarios/Examples/4stations.xml)
12.28ms
12.38ms
12.48ms
12.58ms
Station 1
12.437 ms
6Mb/s
DA:2
ack 2
12.481 ms
Station 2
12.421 ms
Station 3
Station 4
6 (15) 12.533 ms
12.587 ms
6Mb/s
DA:1
data 2

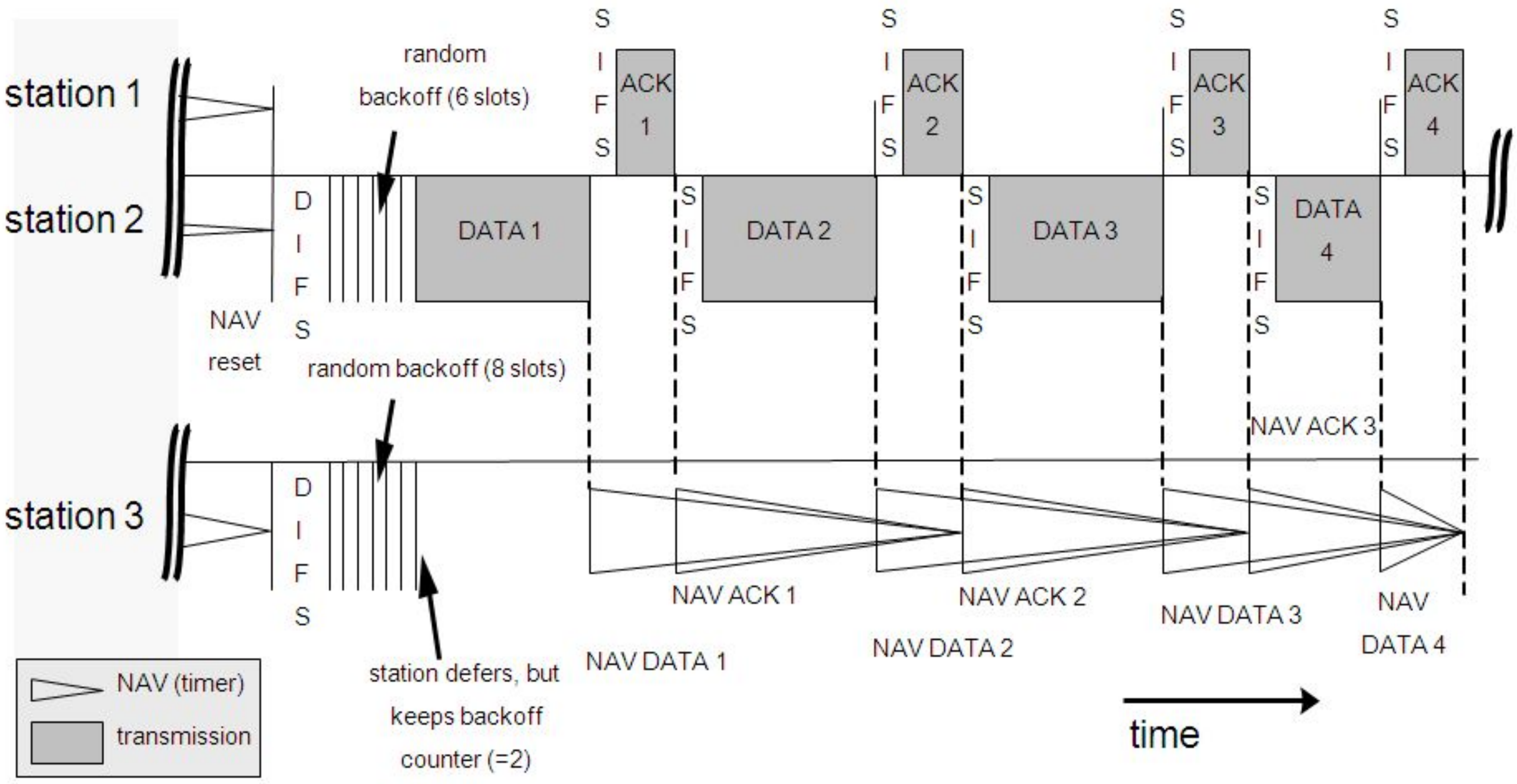

Jemula802 emulation results. (file:/C:/cygwin64/home/smangold/Source/Eclipse/jemula802/scenarios/Examples/4stations.xml)
12.47ms
12.57ms
12.67ms
12.77ms
Station 1
12.481 ms
A:2
ck 2
12.703 ms
6Mb/s
DA:4
ack 2
12.747 ms
Station 2
Station 3
Station 4
6 (15) 12.533 ms
12.587 ms
6Mb/s
DA:1
data 2
12.687 ms


Jemula802 emulation results. (file:/C:/cygwin64/home/smangold/Source/Eclipse/jemula802/scenarios/Examples/4stations.xml)
20.09ms 20.19ms 20.29ms 20.39ms 20.49ms 20.59ms 20.69ms 20.79ms 20.89ms 21ms 21.09ms 21.19ms 21.29ms 21.39ms 21.49ms 21.59ms 21.69ms
Station 1
Station 2
Station 3
Station 4

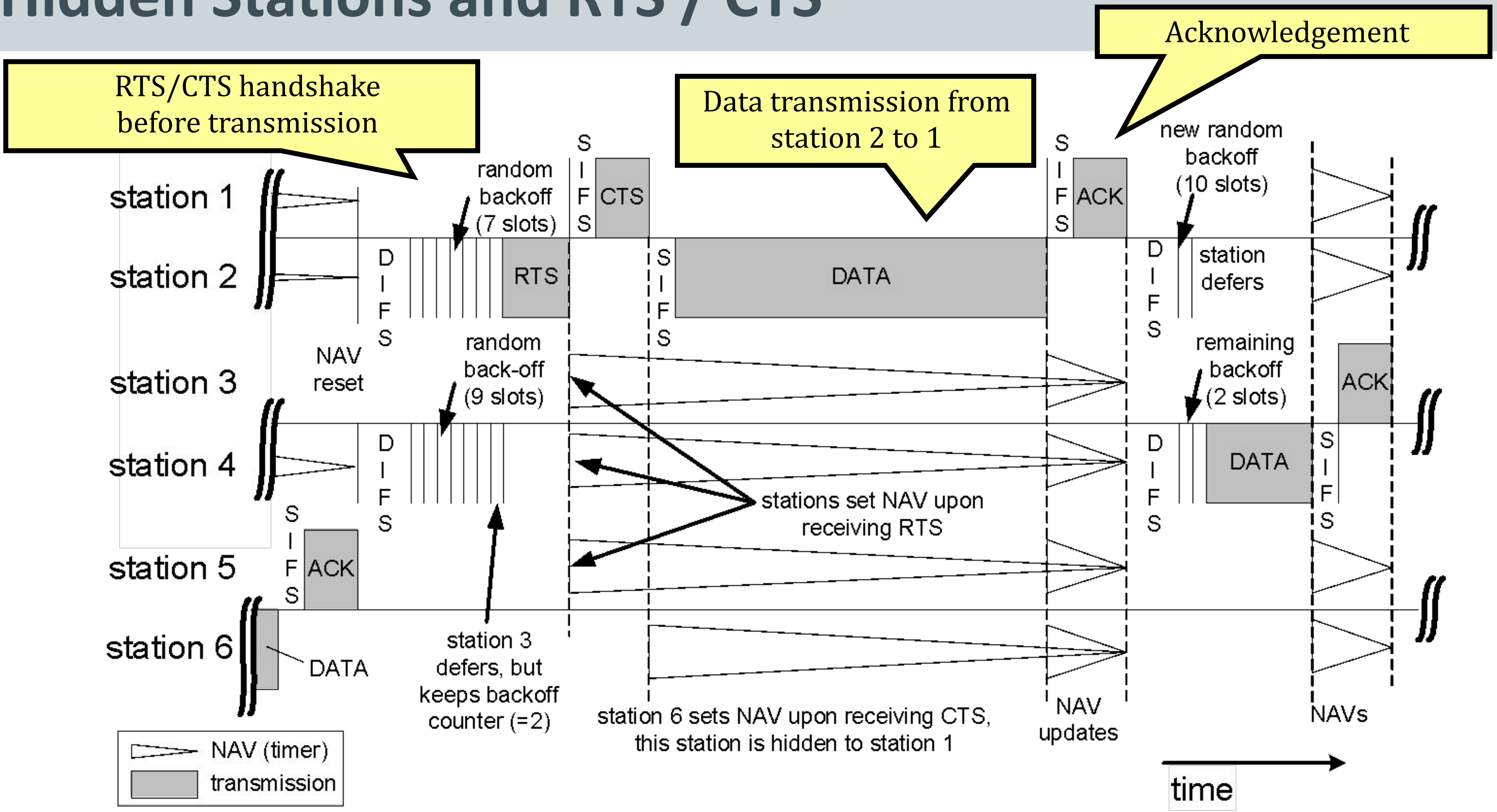
802.11 Fragmentation

- Data frames (MSDUs) can be transmitted in more than one MPDU, which is called “fragmentation”
  - If the MSDU length exceeds a certain threshold
- To reduce duration of collision times
- Each data frame is individually acknowledged
  - This results in overhead (see also block-ACK of 802.11e/n)
- Data frames protect subsequent transmissions of their ACK responses and the following data frame with NAV
- Defragmentation
  - Process of recombining MPDUs into a single MSDU at the intended receiver

802.11 Fragmentation Illustrated



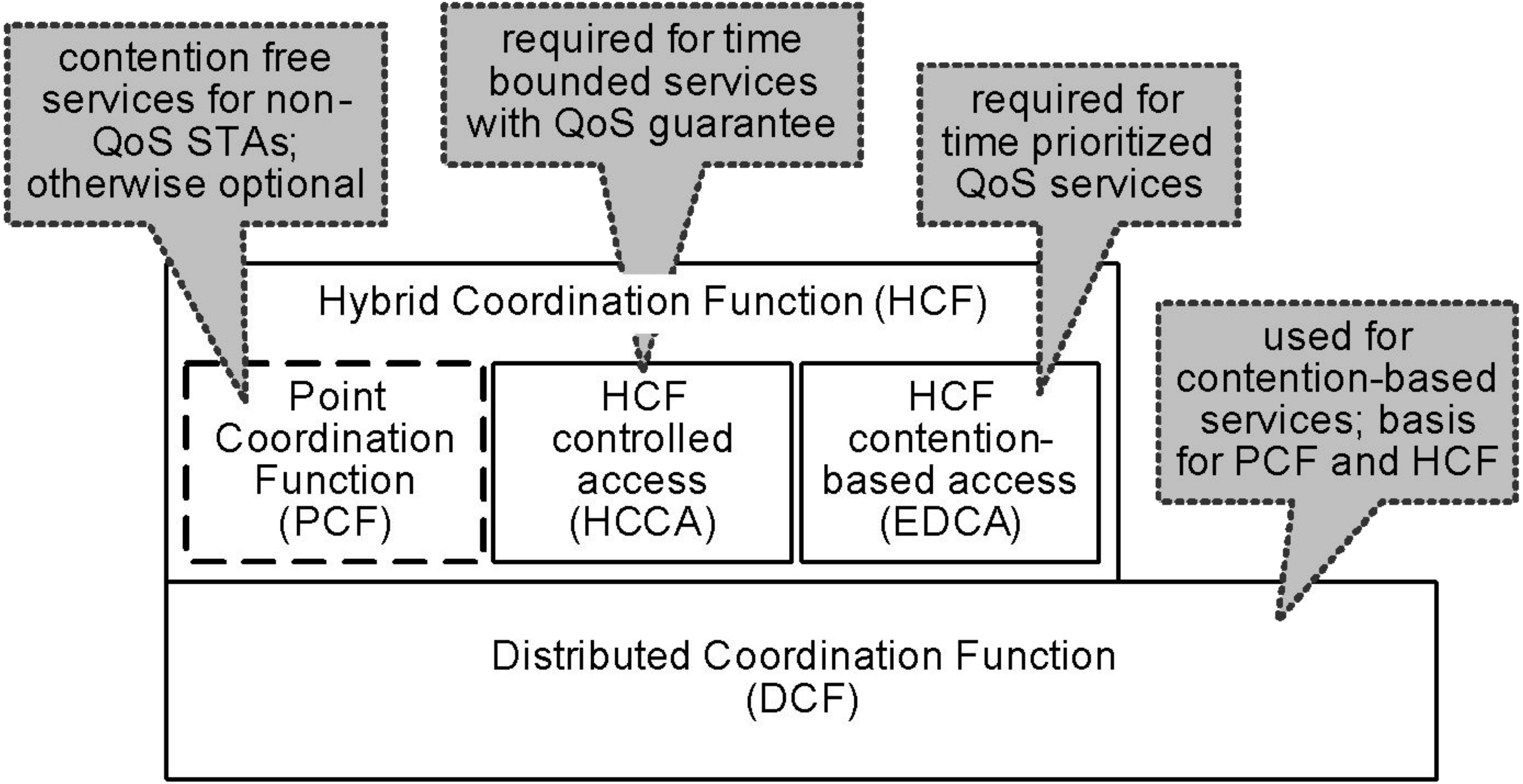
Hidden Stations and RTS / CTS



IEEE 802.11e MAC Enhancements

- Layer-2 MAC protocol with backward compatibility
- Increasing demand for Quality-of-Service (QoS) was motivation for extending this standard
  - IEEE 802.11e standard was approved in 2005
  - Intel PRO/Wireless 3945ABG chipset supports 802.11e for VoIP and video streaming
- Hybrid Coordination Function (HCF) provides QoS
- HCF defines two new coordination functions
  - Controlled channel access HCCA
  - Contention-based channel access EDCA

MAC Enhancements Illustrated



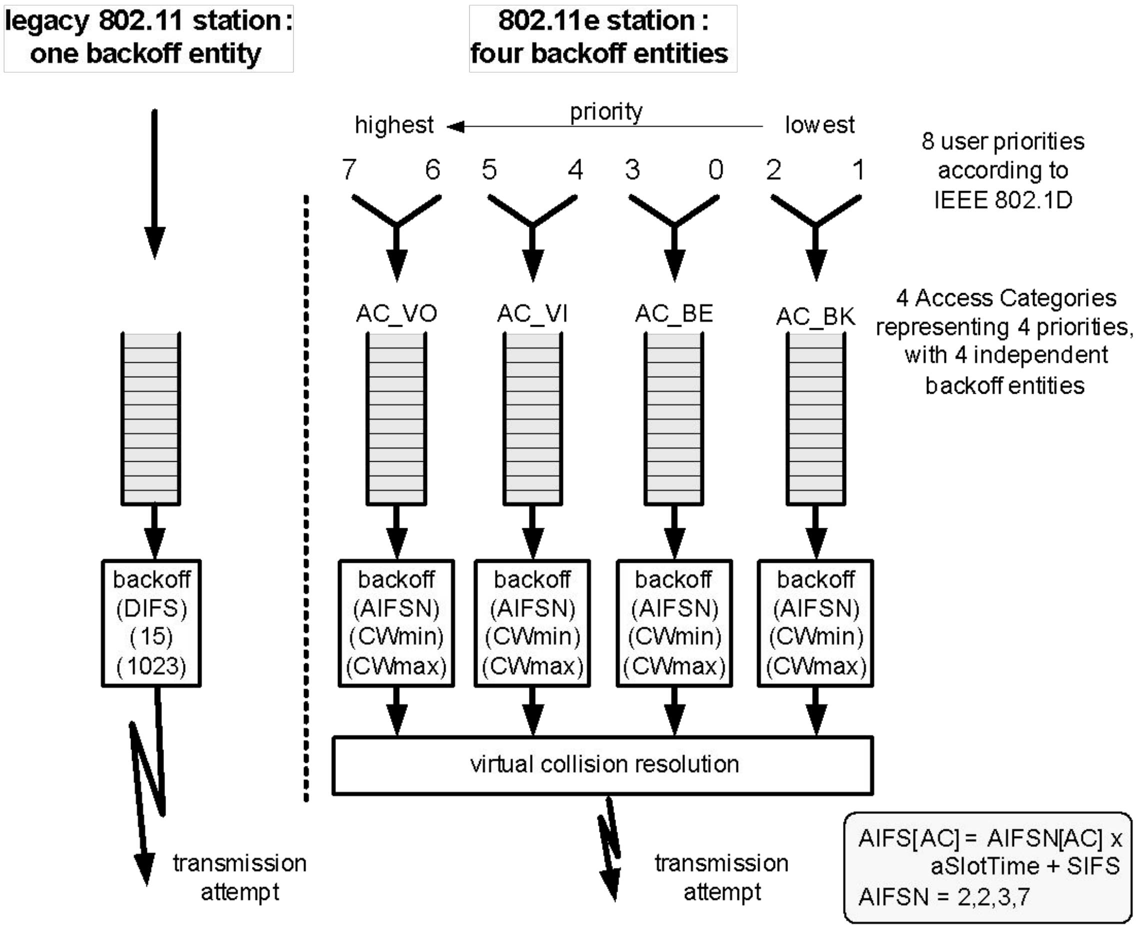
802.11e Terminology

- Quality-of-service supporting Basic Service Set (QBSS)
  - A BSS that includes an 802.11e-compliant Hybrid Coordinator (HC)
- Transmission Opportunity (TXOP)
  - Defined by its starting time and duration
  - Obtained by 802.11e station (more precisely by a backoff entity)
  - TXOP obtained via contention-based medium access, is EDCA-TXOP
  - EDCA-TXOP duration is limited by TXOPlimit
  - TXOP obtained by the HC via the controlled medium access is HCCA-TXOP
  - HCCA-TXOP is not limited by TXOPlimit
- Controlled Access Phase (CAP)
  - Time period in which the HC has control over the medium (in CFP or in CP)

802.11e EDCA Priorities

- EDCA enables a probability based support of Quality-of-Service by introducing four Access Categories (ACs)
  - each AC has different parameter sets of contention-based access
- Inside 802.11e station: ACs are realized through parallel backoff entities with virtual collision resolution
- Channel access after medium sensed as idle
  - For certain time duration (AIFS instead of DIFS)
  - And after random waiting time drawn from CW

802.11e EDCA Priorities Illustrated

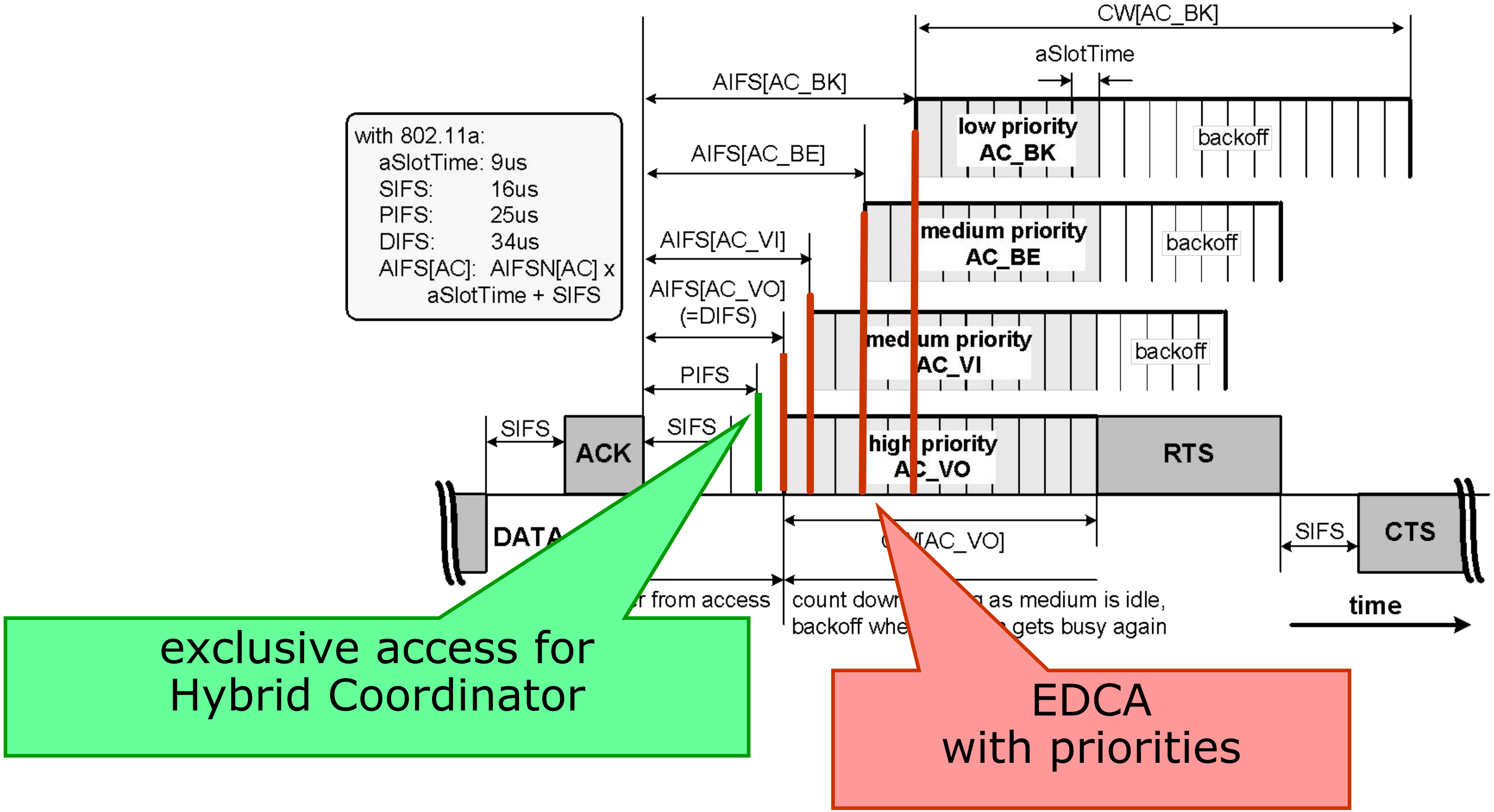


QoS Support with 802.11e EDCA

- Four Access Categories (ACs)
  - Background (AC_BK), Best Effort (AC_BE)
  - Video (AC_VI) and Voice (AC_VO)
- EDCA prioritization with parameters
  - AIFS[AC] (in microseconds)
  - Equiv. to AIFSN[AC]
  - CWmin[AC]
  - CWmax[AC]

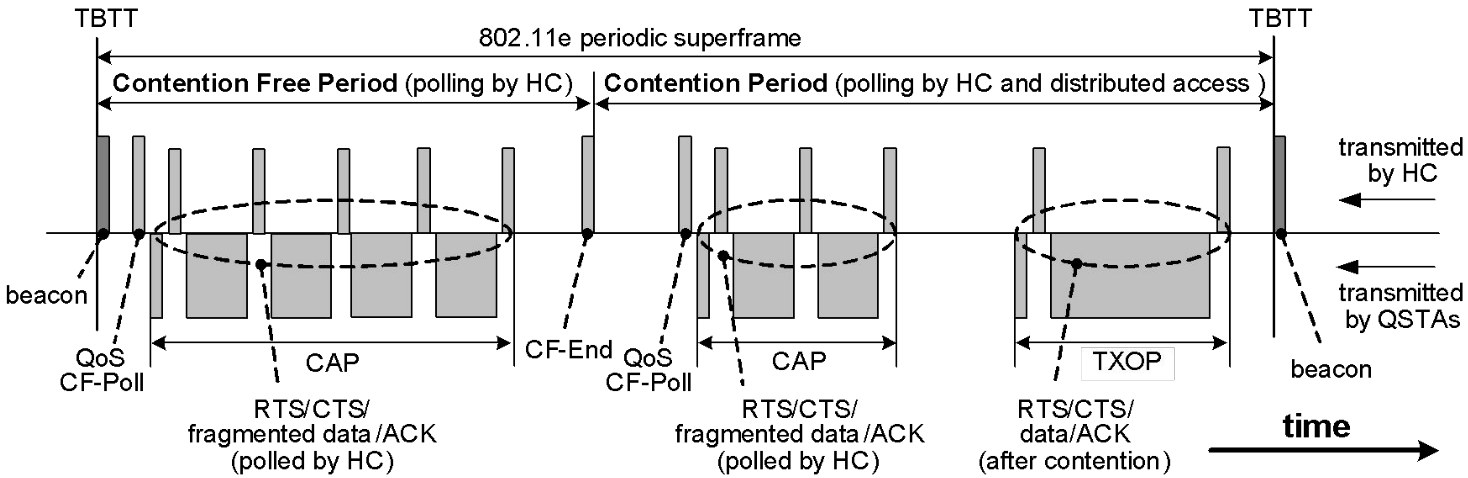
AC	CWmin	CWmax	AIFSN	AIFS
legacy	15	1023	2	34 us
AC_BK	15	1023	7	79 us
AC_BE	15	1023	3	43 us
AC_VI	7	15	2	34 us
AC_VO	3	7	2	34 us

QoS Support Illustrated

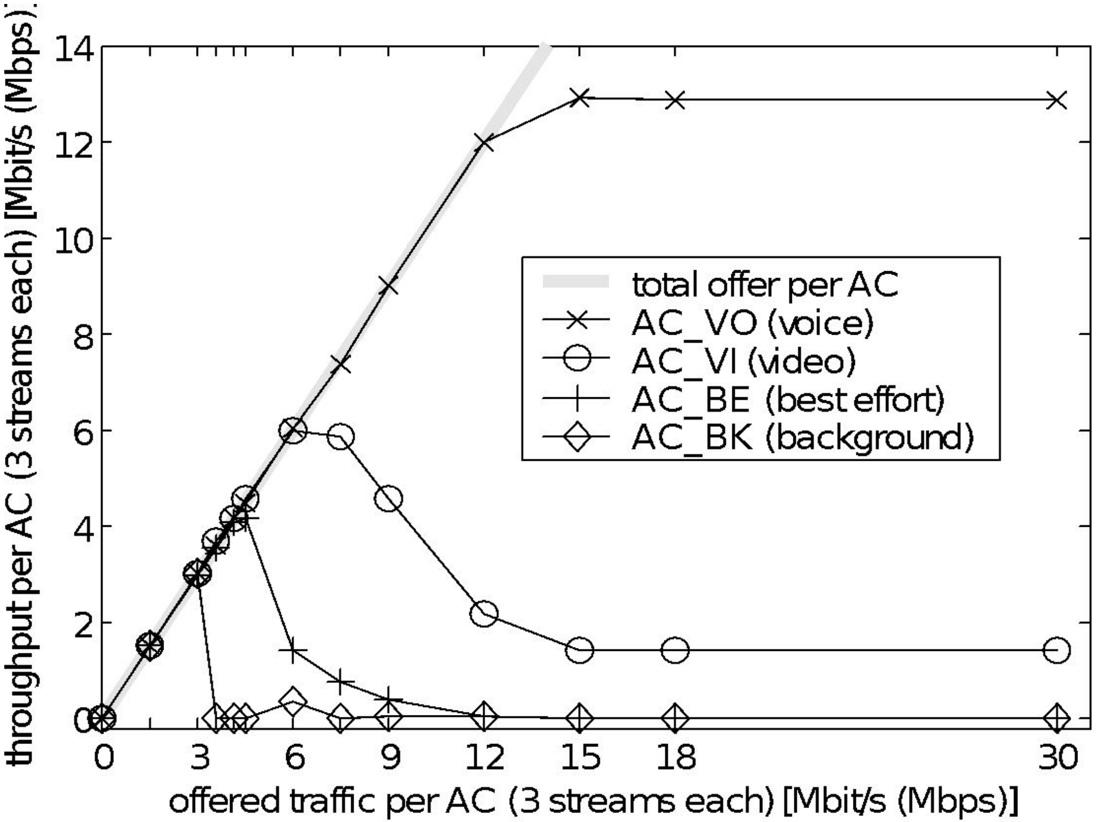


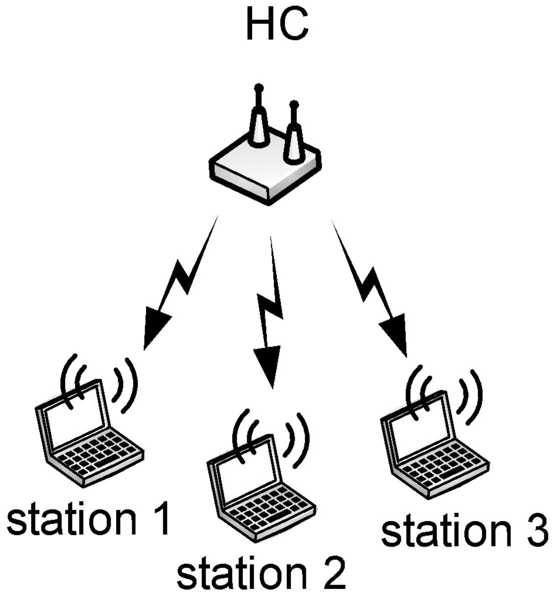
802.11e MAC Periodic Superframe Period

- Centralized operation
  - HCF Controlled Access (HCCA), exclusive channel access in Contention Free Period
- Decentralized, contention-based operation
  - Enhanced Distributed Channel Access (EDCA)
  - Listen-before-talk principle and backoff procedure in contention period

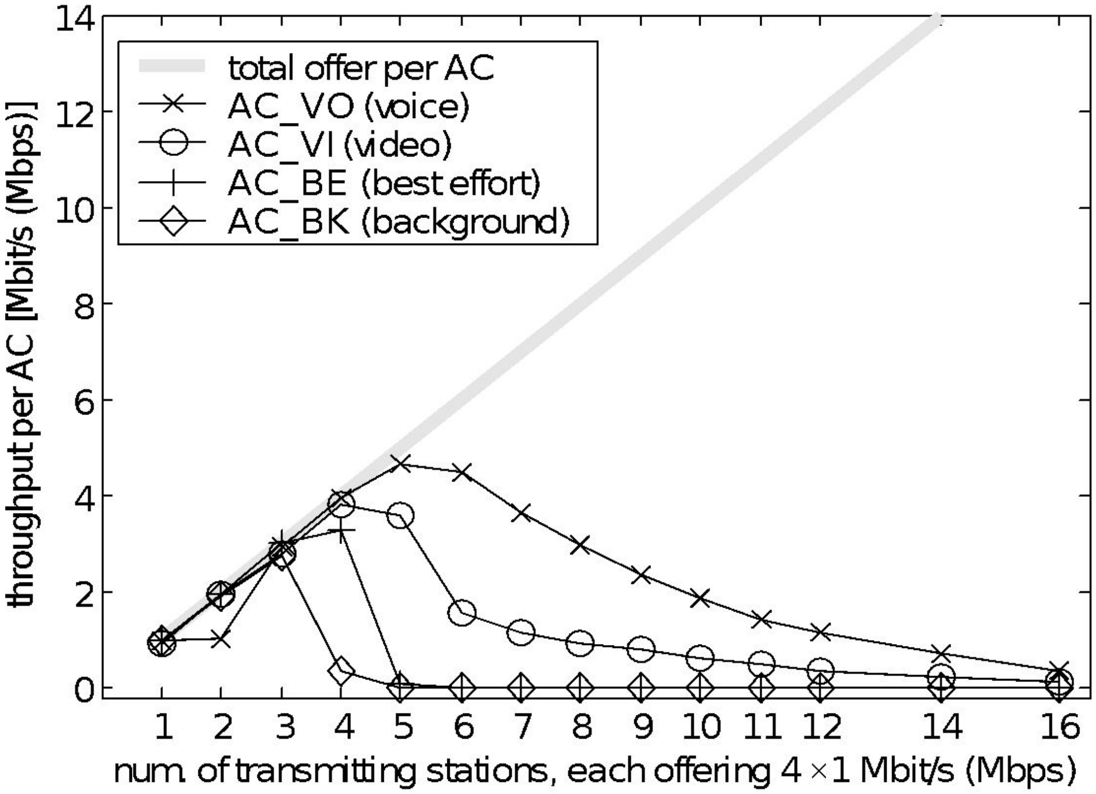


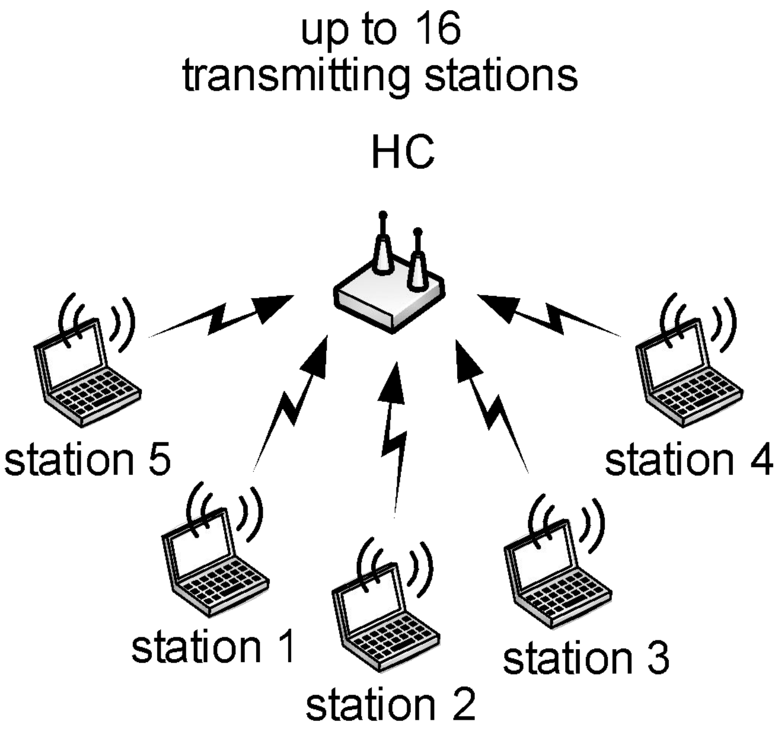
EDCA Throughput (Simulation 1/2)





EDCA Throughput (Simulation 2/2)

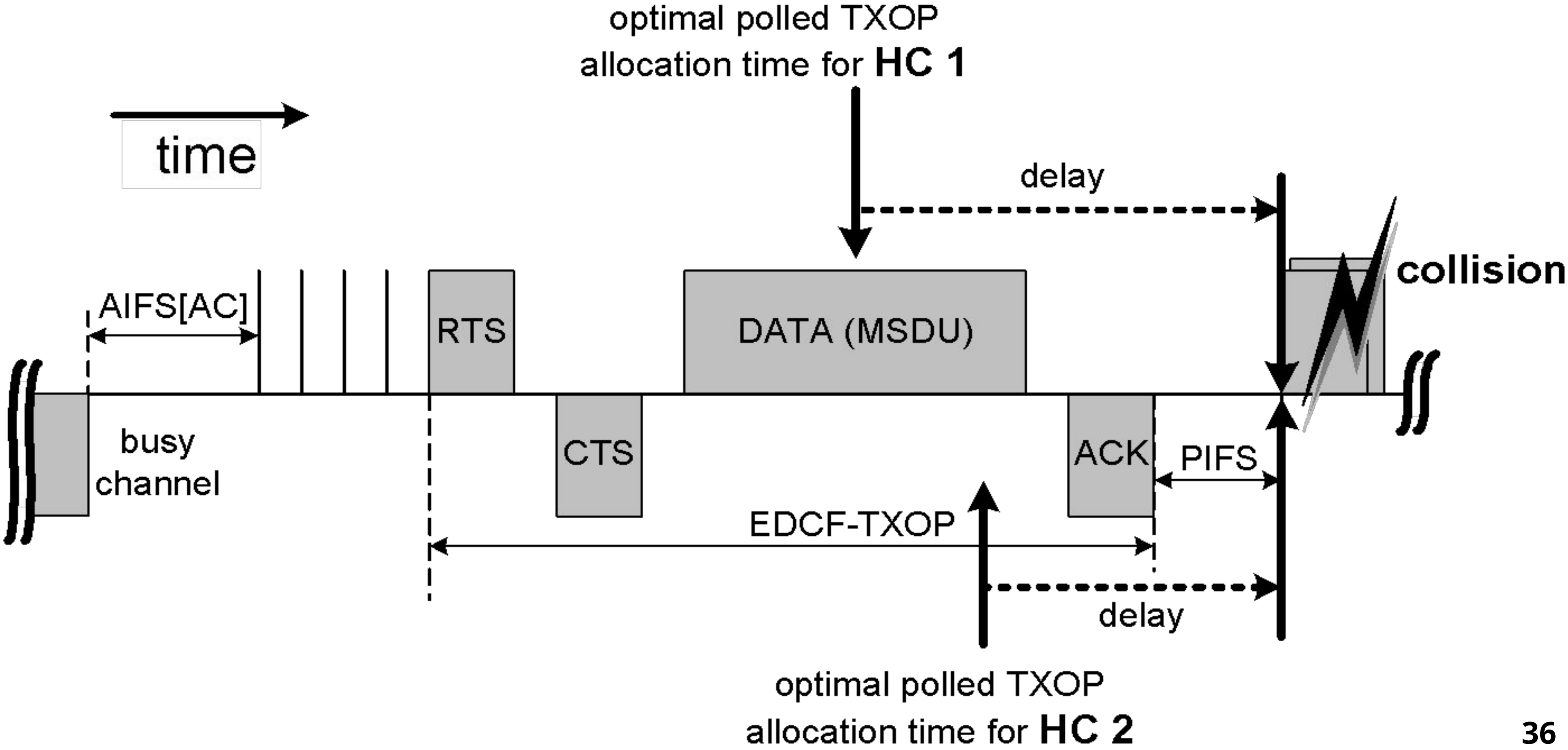




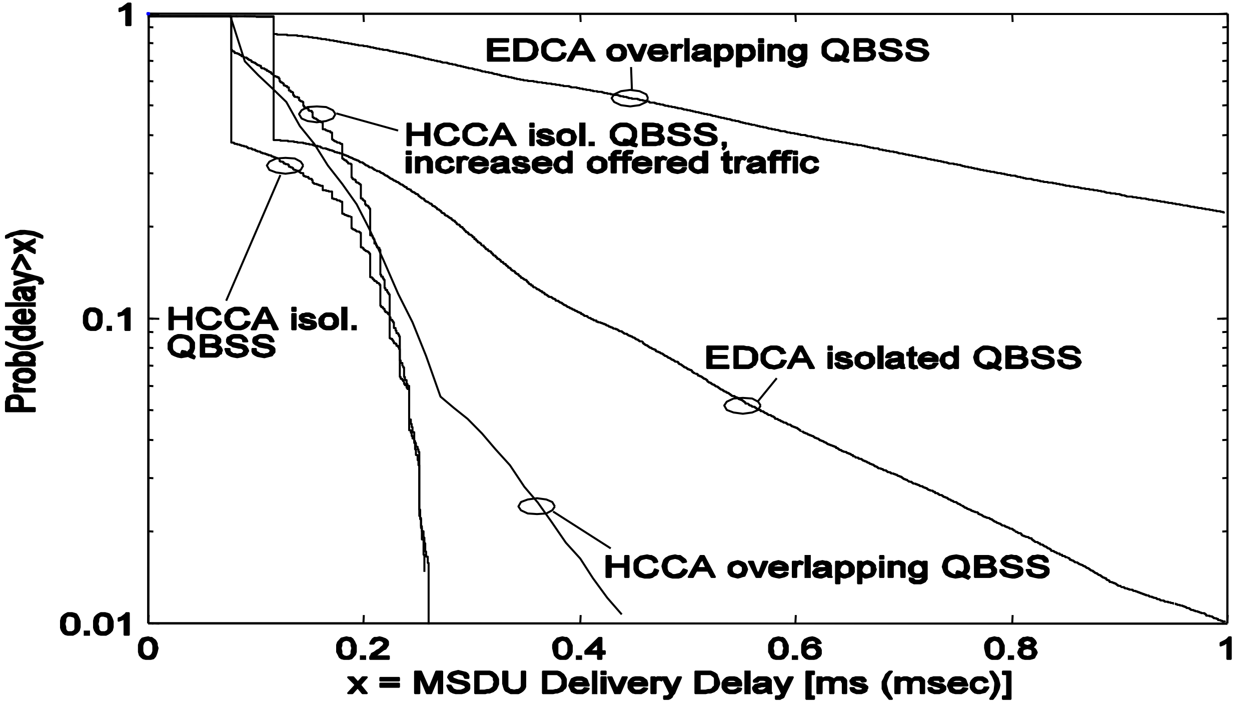
The Problem Of Overlapping BSSs

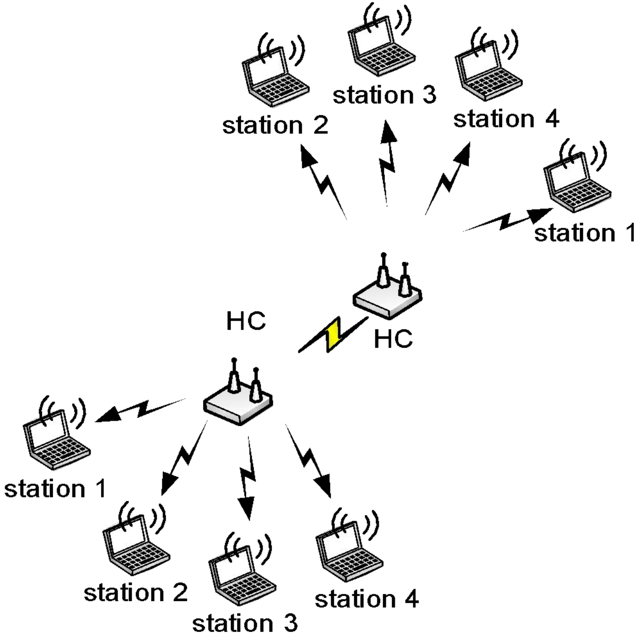
- Isolated BSS
  - Unpredictable delays may occur
  - However, maximum delay under control by HC, with the help of EDCA-TXOPlength
- Overlapping BSSs with more than one HC
  - HC has no control over opponent HC's TXOPs
  - QoS CF-Polls may collide, if both HCs access simultaneously the medium
- This is an unsolved coexistence problem!

Overlapping BSSs Illustrated



Overlapping BSS Delays (Simulation)



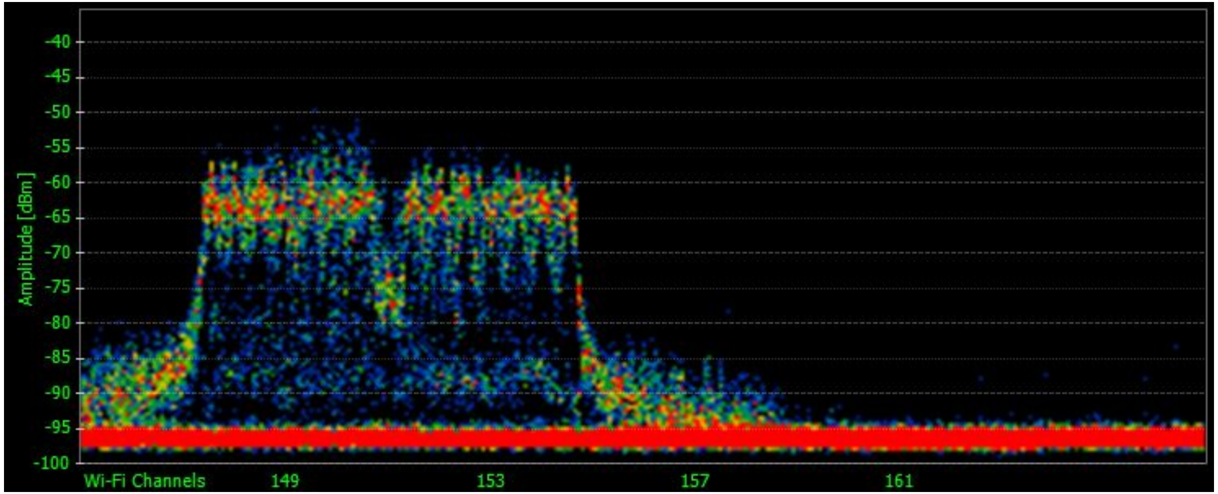


IEEE 802.11e Summary

- 802.11e HCCA introduces centralized control for QoS guarantees
- Contention-based medium access of 802.11e EDCA implies limited capability to support QoS
- Number of contending backoff entities determines (1) the level of supported QoS and (2) differentiability of QoS
- The overlapping BSS problem remains unsolved by 802.11e
    - 802.11h dynamic frequency selection (DFS) will mitigate this problem

IEEE 802.11n: High Throughput (HT)

- Multimedia applications and consumer electronics require significantly higher throughput and lower delay than today
- Economic potential, many interest groups were involved in standardization



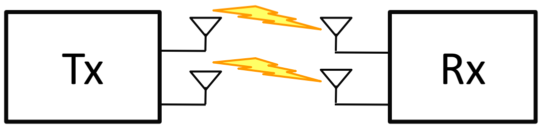
IEEE 802.11n: High Throughput (HT)

- PHY features
  - PPDU formats for 20/40 MHz operation
  - MIMO operation (spatial multiplexing), Tx beamforming, antenna selection
- MAC features
  - reduced Interframe Space (RIFS < SIFS)
  - MSDU/MPDU aggregation, block acknowledgement (see 802.11e)
- Throughput increase
  - 2x2 antenna operation at 20 MHz → 100 Mb/s
  - 4x4 antenna operation at 40 MHz → 600 Mb/s

802.11n Channel Bundling

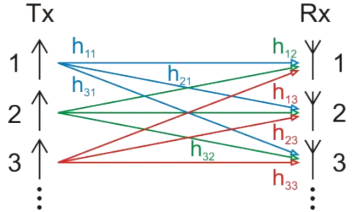
- Use adjacent pair of 20 MHz channels
  - As one 40 MHz channel, with shorter frame durations
- Implementation
  - AP indicates operation on 40 MHz
  - AP defines primary and secondary 20 MHz channel
  - Primary 20 MHz channel is used for coordination (beacon broadcast etc.)
  - Stations do not need to consider carrier sense CCA state of secondary channel
- Problem
  - Number of collisions with 20 MHz transmissions from overlapping BSS on secondary channel are increasing
  - Frame sequence of 40 MHz transmissions may be interfered on secondary channel

Multiple Input Multiple Output (MIMO) 1/2



$$\underline{H} = \begin{bmatrix} h_{11} & \cdots & h_{1n_T} \\ h_{21} & \cdots & h_{2n_T} \\ \vdots & \ddots & \vdots \\ h_{n_R1} & \cdots & h_{n_Rn_T} \end{bmatrix} \quad \text{mit } h_{ij} = \alpha + \mathrm{j}\beta$$

channel matrix



- Diversity: exploits independent fading to enhance signal diversity
  - Stream transmitted using space-time coding, no channel knowledge at transmitter
- Beamforming / precoding: increases signal gain from combining
  - Same signal is emitted from each transmit antenna with appropriate phase weighting such that signal power is maximized at receiver
  - Requires knowledge of channel state information (CSI) at transmitter
- Spatial multiplexing: create parallel channels
  - Separately encoded data signals, from each of the transmit antennas
  - Good at higher Signal to Noise Ratio (SNR), with or without channel knowledge

Background Reading: IEEE 802.11n MIMO.pdf

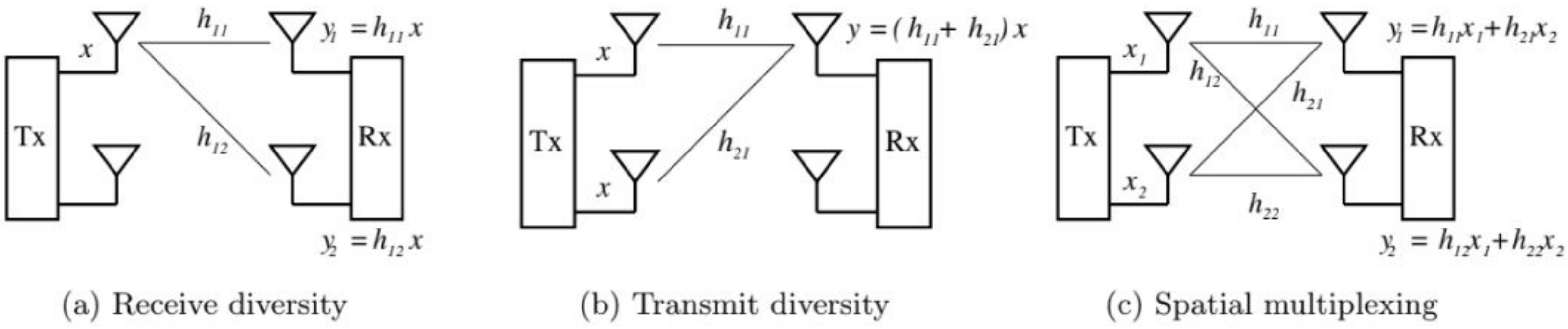
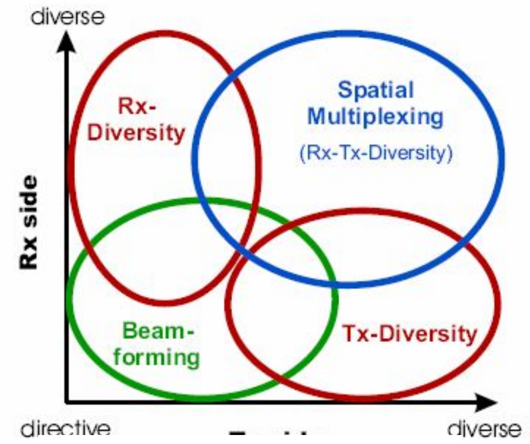


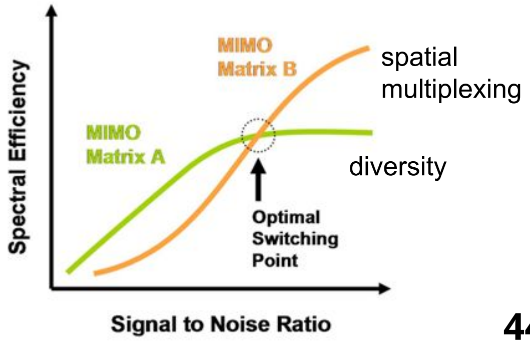
Figure 2: Using some of the transmit/receive antennas in an example 2x2 system to exploit diversity and multiplexing gain. x_i and y_i represent transmitted and received signals. The channel gain h_{ij} is a complex number indicating a signal's attenuated amplitude and phase shift over the channel between the ith transmit antenna and the jth receive antenna. The received signals y_i will additionally include thermal RF noise.

Multiple Input Multiple Output (MIMO) 2/2

- MIMO channel determines gain
  - Non-correlated channels on both Rx/Tx sides
    Lead to highest performance
- Combinations
  - Spatial multiplexing + beamforming:
    if channel is known at transmitter
  - Spatial multiplexing + diversity coding: if decoding reliability is in trade-off
- Challenge with MIMO: $\lambda/2$ antenna spacing
  - Handset implementation difficult
  - Requires large antenna arrays at base stations

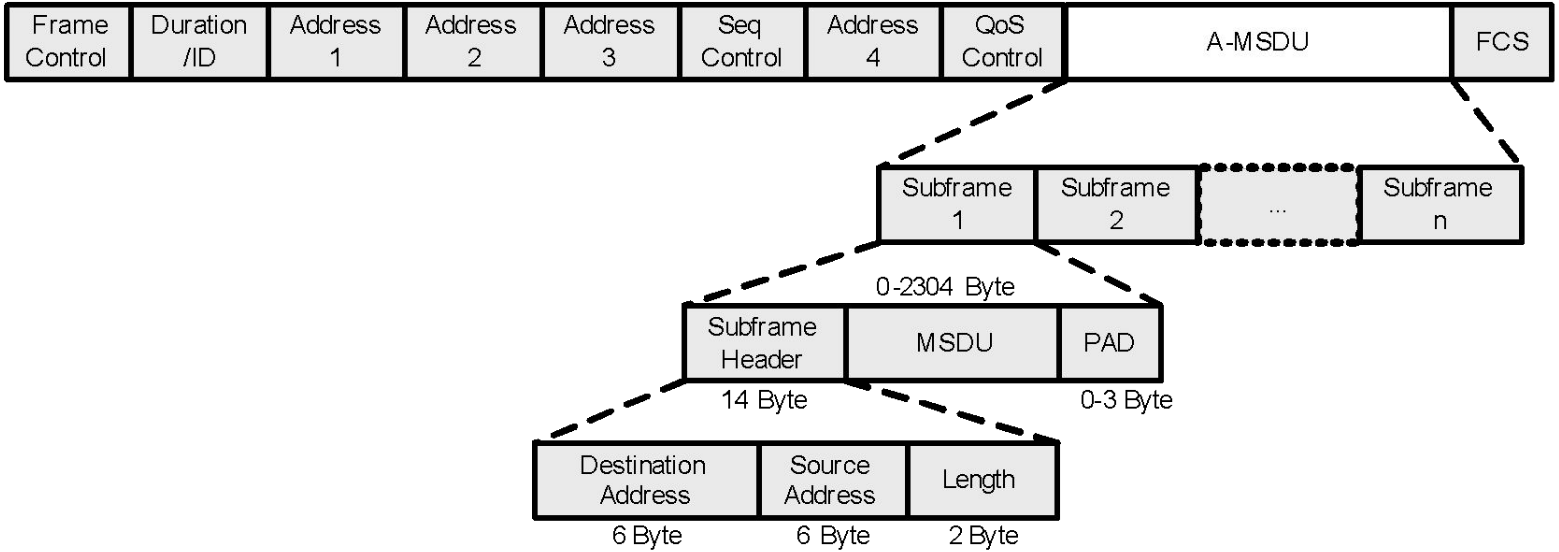


MIMO Adaptive Mode Selection



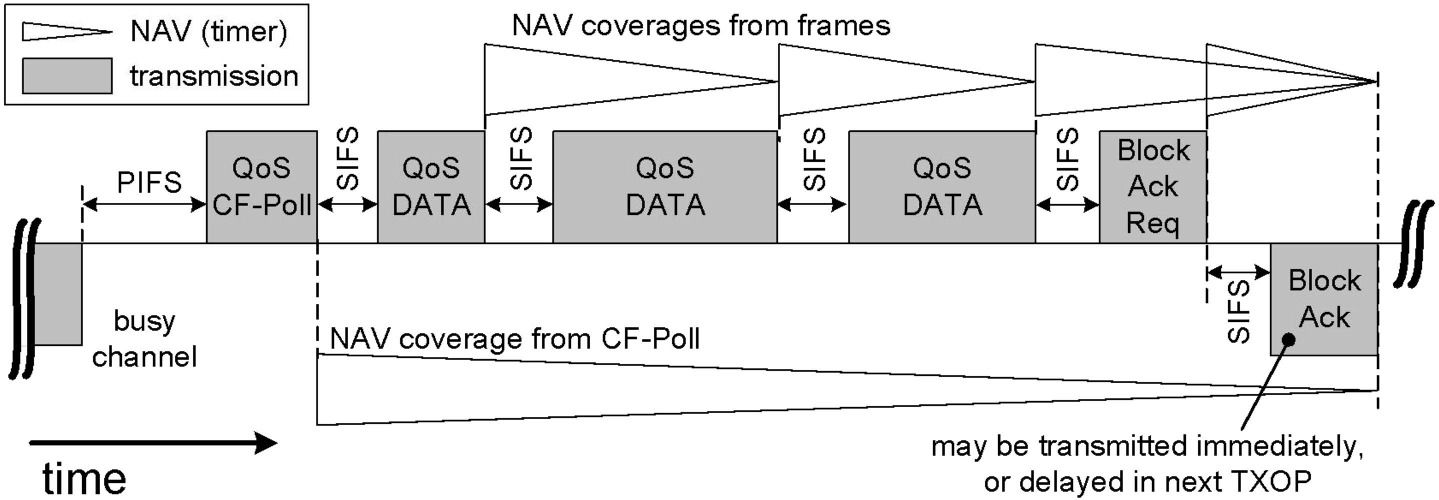
802.11n MSDU Aggregation

- Aggregation of multiple frames
  - Reduce protocol overhead
  - A-MSDU is aggregated with multiple MSDUs
  - Aggregated MSDU frames need to have same address type &priority class



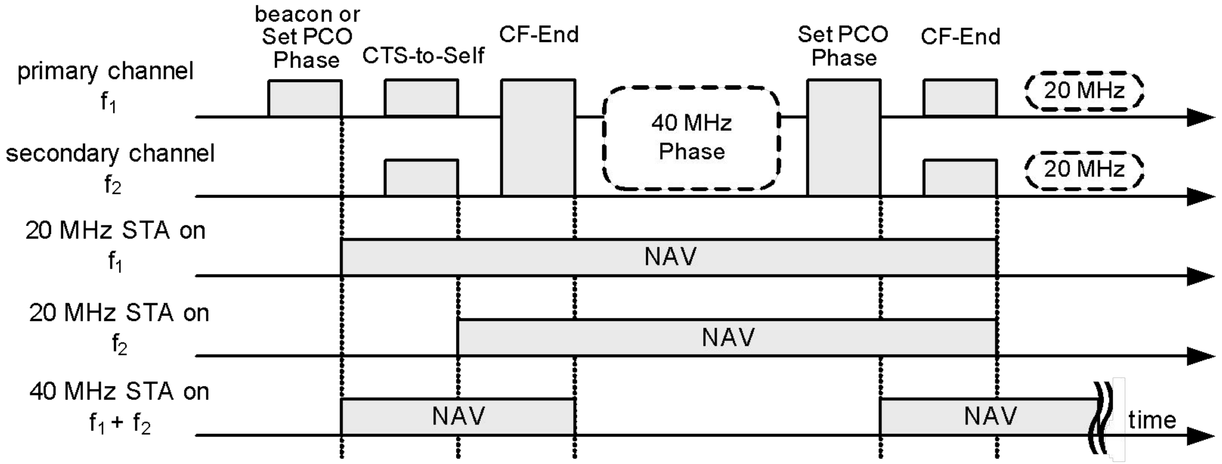
802.11e/n Block Acknowledgement

- 802.11e and 802.11n extensions
  - Implicit block acknowledgement request (BAR) → reduced overhead
  - Compressed block acknowledgement → reduced bitmap size
  - Multi-TID (Traffic Identifier) block acknowledgement → reduced overhead
  - Immediate and delayed Block ACK depending on traffic type



802.11n Phased Coex. Operation (opt.)

- AP divides channel into time intervals of alternating 20 MHz and 40 MHz phases
  - AP reserves 20 MHz primary channel and 20 MHz secondary channel in turn to start 40 MHz phase
  - AP resets NAV in 20 MHz channel in opposite order to start 20 MHz phase
  - Decision of 2x20 MHz vs. 20/40 MHz is not standardized

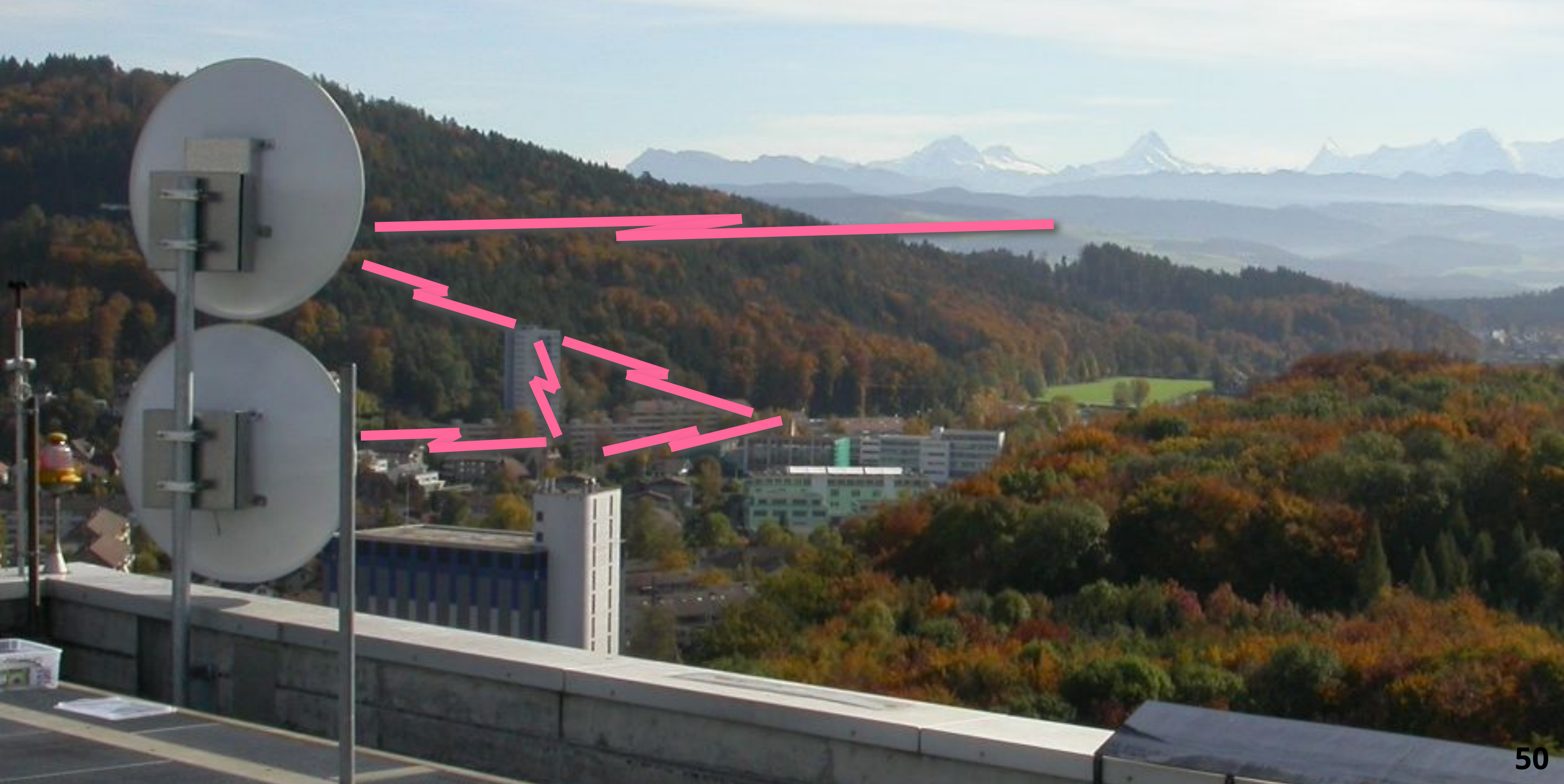


IEEE 802.11n Summary

- Maximum throughput with 802.11n is significantly increased
- High performance increase in indoor scenarios
  - Ideal environment for MIMO
- Smaller performance increase in outdoor scenarios
  - Mainly due to channel bundling
- Overloaded 2.4 GHz band, difficult to use 40 MHz option
- Good complement to 11e/11s: QoS & mesh & high rates & coverage

WLAN Long Range Links (10Mb/s over 19km)

Wi-Fi Mesh Outdoor Networks



Potential Benefits Of Mesh Networks

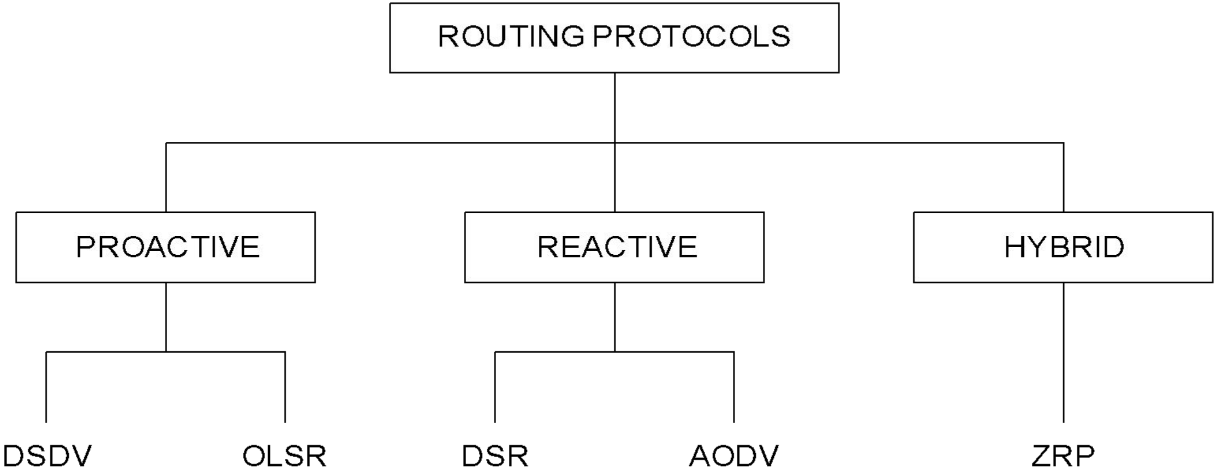
- No need for backbone infrastructure
  - Self configuration, easy deployment, cost efficiency
- Robustness against network failures or damages
  - System repairs or corrects a break-down by itself without external help, allowing higher availability
- Adaptability: system adapts to changes in the environment conditions
  - In a coordinated way
- Scalability: self-organizing networks enable scalability
  - Because of the inherent non–hierarchical concept

Problem: Hidden Stations

- Receiving station is in reception range of two other stations
- However, the two other stations out of mutual sensing, or, reception “Rx” range
- As a result, the transmissions to the receiving “Rx” station by the transmitting “Tx” station cannot be detected by a possible interferer that does not sense the transmission

Path Selection (Routing)

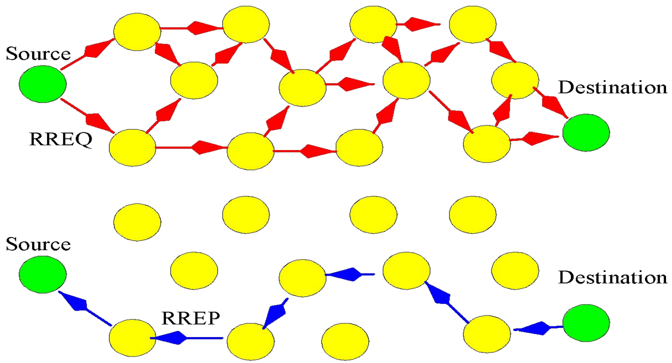
- Proactive protocols maintain & detect paths
- Reactive protocols save overhead, set-up paths only when needed
- Hybrid protocols combine both (e.g., "Zone Routing Protocol")



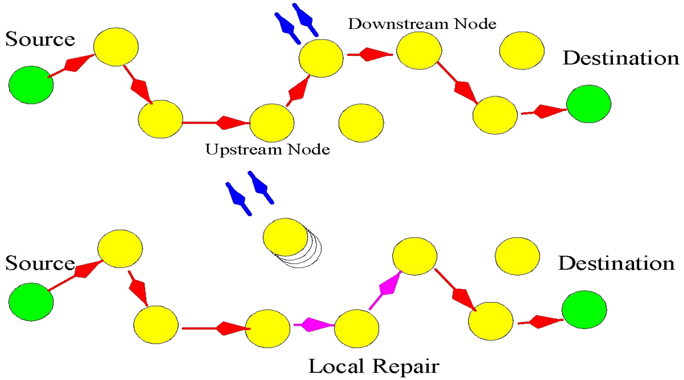
Ad-Hoc On-Demand Distance Vector Routing (AODV)

- Reactive routing protocol
  - Does not maintain routes, but builds them on demand
- A route request is flooded, and establishes the reverse path
- Destination unicasts the route replay & establishes forward path

(a) Route Discovery Process



(b) Route Repair shown for Unicasting



Optimized Link-State Routing (OLSR)

- The second most implemented, after AODV, proactive behavior
- OLSR is not “ad-hoc”, it is proactive
  - Makes use of "Hello" messages
  - To find its one hop neighbors and its two hop neighbors through their responses
  - The sender can then select its “multipoint relays”
- In capacity- and/or power-starved networks, keeping network silent when no traffic to be routed is preferred
  - One of the reasons why AODV is used more often
- Which routing protocol would be more efficient for mobile environments?

IEEE 802.11s: Overview

- Primary scope:
  - Small/medium mesh networks (~32 forwarding nodes)
  - Self-configuring, multi-hop topologies
  - Dynamic, radio-aware path selection in mesh, enabling data delivery on single-hop and multi-hop paths
  - Support uni-, multi- & broadcast traffic
- Mesh networking deployment usage scenarios:
  - Military: battlefield communication
  - Public safety: emergency & disaster area communication
  - Residential: consumer electronics
  - Public access: operated networks
  - Office: enterprise & business networks

IEEE 802.11s Medium Access Control

- Mandatory MAC functions
  - Enhanced Distributed Channel Access (EDCA) is basis of 802.11s MAC
  - Re-use of latest MAC enhancements from 802.11e
  - Compatibility with legacy devices
  - Easy to implement, with efficiency in simple Mesh deployments
- Optional MAC enhancements
  - Mesh Deterministic Access (MDA): reservation-based deterministic medium access
  - Common Channel Framework (CCF): multi-channel operation mechanism
  - Intra-mesh Congestion Control
  - Power management

Popular 11s Implementation

- One Laptop per Child (OLPC)
- All open source
  - Mesh code available
- Partially implements 802.11s-D1.0
  - HWMP without tree based routing
  - AODV mature and reliable

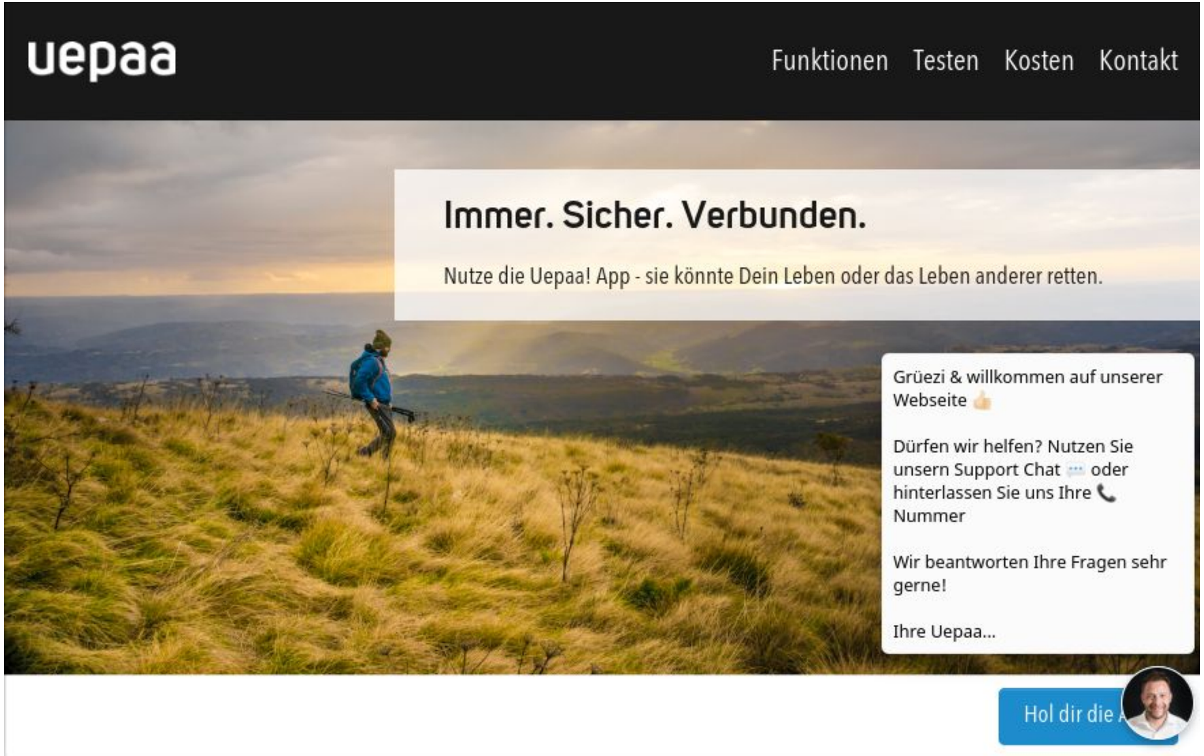
- Operates simultaneously as Station and Mesh Point
  - WLAN chipset independent of main CPU
  - WLAN Mesh operates when laptop in doze mode

IEEE 802.11s: Summary

- Amendment to IEEE 802.11 that realizes WLAN mesh networking
- Has limited performance, suffers from single-hop EDCA MAC that has never been designed to work in multi-hop topologies.
- Optional features provide MAC with functionalities to
  - Handle QoS in a multi-hop environment
  - Prioritize Mesh backhaul over local BSS frames
  - Make use of one or more frequency channels
- Cognitive radio aspects of 802.11s:
  - Awareness of local environment (neighbourhood, traffic congestion etc.)
  - Mesh used for increasing accuracy and extending this awareness
  - Distributed reservation and access to multiple channels (spectrum)

Mesh vs. Delay Tolerant Networking

DTN Use Case: https://safety.uepaa.ch/de/private



Wireless Networking and Mobile Computing

Background Information: Confidence Intervals in Stochastic Simulation

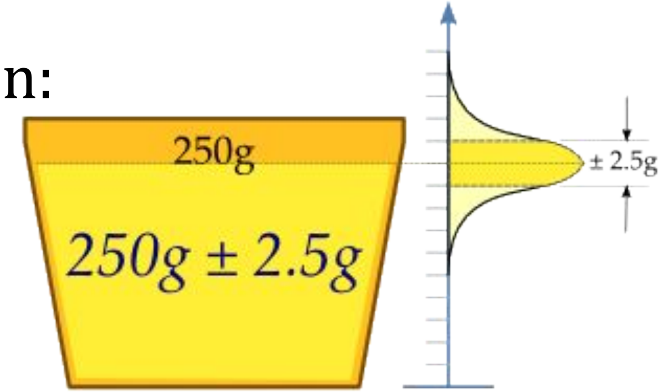
Stefan Mangold

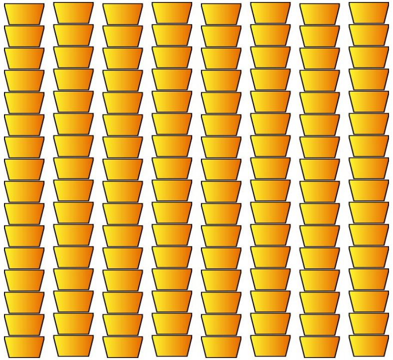
Overview of Topics

- Confidence interval
  - Filler machine example
  - Confidence level
  - Matlab code
- Statistical hypothesis testing
  - Magician example
  - Statistical significance

Filler Machine Example (1)

- Machine that fills cups with Margarine
- Content of each cup shows some variation: it is considered a random variable X
- Variation assumed to be normally distributed around the desired mean of 250g
    - With standard deviation of 2.5g





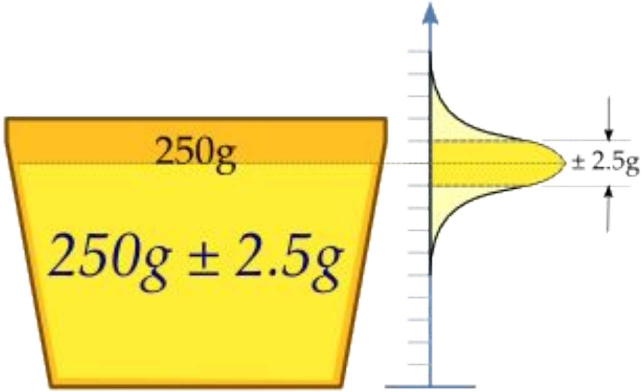
Stock Of Cups

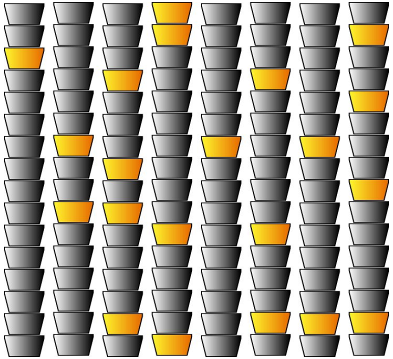
Filler Machine Example (2)

- QUESTION: How well is the machine calibrated?
- Take a sample of n = 25 cups randomly
- Compute estimated mean value $\bar{X}$:

$$\hat{\mu} = \bar{X} = \frac{1}{n}\sum_{i=1}^{n} X_i .$$

$$\bar{x} = \frac{1}{25}\sum_{i=1}^{25} x_i = 250.2\,\text{grams}.$$

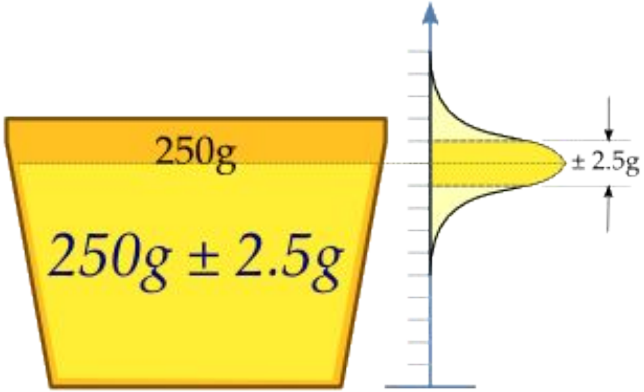


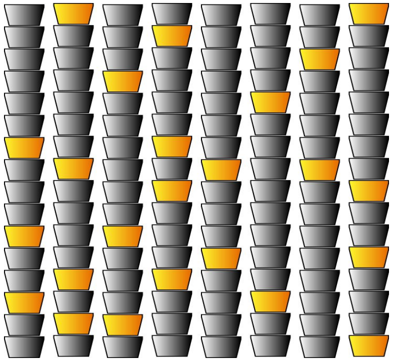


Random
Sample 1
From
Stock
Of Cups

Filler Machine Example (3)

- Take a second sample randomly
- Compute its mean value
  - This time you estimate 250.3g

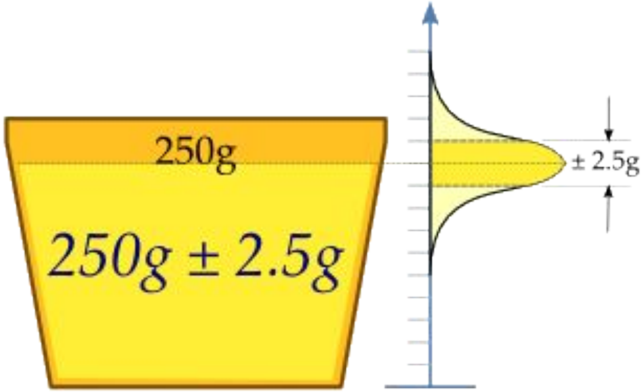


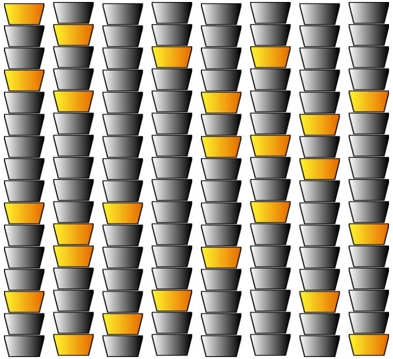


Random Sample 2 From Stock Of Cups

Filler Machine Example (4)

- Take a third sample randomly
- Compute its mean value
    - This time you estimate 249.8g

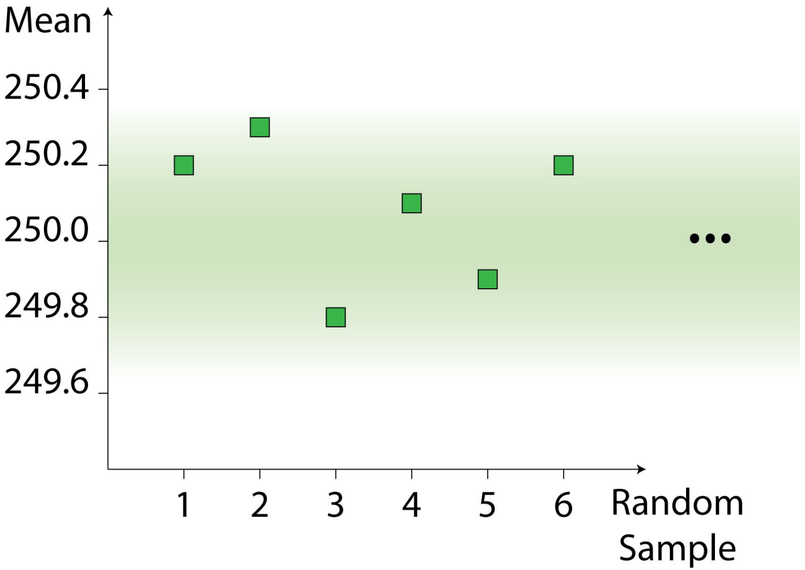




Random Sample 3 From Stock Of Cups

Filler Machine Example (5)

- By repeating the process for many samples, …



Computing the means as single values does not solve our problem, but just postpone it to the point where you have multiple mean values (one per sample). You have to figure out what to do to make sense out of them.

... the obtained means appear to be distributed around the desired value! Now what?

Confidence Interval (1)

- For each computed mean we can compute a confidence interval
  - The confidence interval is associated with a confidence level ($1-\alpha$)
  - Typical values of the confidence level are 0.95 or 0.9
- Interpretation:
  - The CI indicates how frequently, for repeated random samples, the corresponding confidence intervals cover the true parameter (real mean)
  - Although very close conceptually, it is NOT the probability that the true parameter is inside one specific confidence interval

Confidence Interval (2)

- How to compute it?
- Because the content of the cups is normally distributed, the means of the random samples are also normally distributed, with:
  - The same expected mean μ (the mean of the means should be the mean ☺️)
  - But with a different standard deviation, equal to $\sigma/\sqrt{n}$
- In our example the standard deviation is 0.5g, since σ=2.5g and n=25

Filler Machine Example (6)

- Take the first random sample ($\bar{X}$ = 250.2g)
- Standardize the random variable (enforcing the mean to zero and the variance to one) as:

$$Z = \frac{\bar{X} - \mu}{\sigma/\sqrt{n}} = \frac{\bar{X} - \mu}{0.5}$$

- Select a confidence level (1-α) = 0.95
- Denote confidence interval for Z as [-z; z]

Filler Machine Example (7)

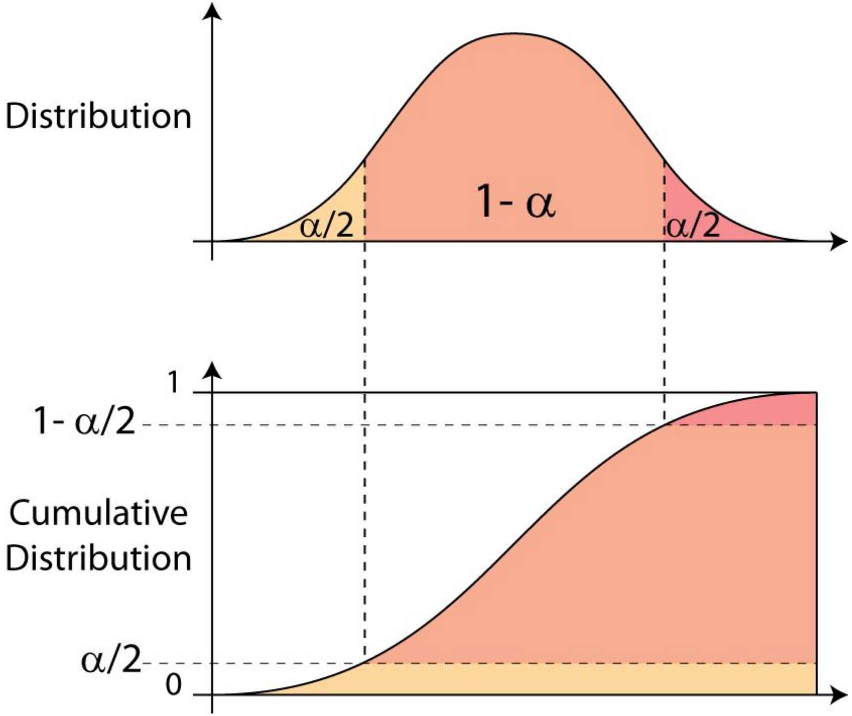
- Set the probability of Z being inside the confidence interval equal to the conf. level:

$$P(-z \leq Z \leq z) = 1 - \alpha = 0.95.$$

- To find the value z, the cumulative distribution function Φ(z) can be used:

$$\Phi(z) = P(Z \leq z) = 1 - \frac{\alpha}{2} = 0.975,$$

$$z = \Phi^{-1}(\Phi(z)) = \Phi^{-1}(0.975) = 1.96,$$



Filler Machine Example (8)

- Given the definition of Z, and the values of z, σ and n, we solve for μ:

$$0.95 = 1 - \alpha = P(-z \leq Z \leq z) = P\left(-1.96 \leq \frac{\bar{X} - \mu}{\sigma/\sqrt{n}} \leq 1.96\right)$$

$$= P\left(\bar{X} - 1.96\frac{\sigma}{\sqrt{n}} \leq \mu \leq \bar{X} + 1.96\frac{\sigma}{\sqrt{n}}\right)$$

$$= P\left(\bar{X} - 1.96 \times 0.5 \leq \mu \leq \bar{X} + 1.96 \times 0.5\right)$$

$$= P\left(\bar{X} - 0.98 \leq \mu \leq \bar{X} + 0.98\right).$$

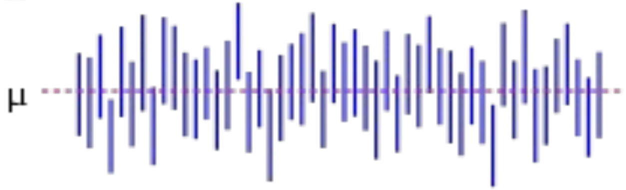
- With $\bar{X}$ = 250.2g, we obtain:

$$(\bar{x} - 0.98; \bar{x} + 0.98) = (250.2 - 0.98; 250.2 + 0.98) = (249.22; 251.18).$$

Filler Machine Example (9)

- In general, we found that for a sample $\bar{X}$, it holds:

$$0.95 = P\left(\bar{X} - 0.98 \leq \mu \leq \bar{X} + 0.98\right)$$



- Each random sample has its own confidence interval
- Each confidence interval is either hit or not by the mean
- 95% of the confidence intervals contain the true value μ = 250g
- The confidence level indicates what the probability is that the true mean μ=250g lies inside one confidence interval ONLY FOR REPEATED random samples

Filler Machine Example (10)

- To answer the original question …
- Since the desired value 250g is inside the confidence interval with confidence level of 95% generated from the first random sample, there is no reason to believe the machine is not sufficiently calibrated.

Matlab Code

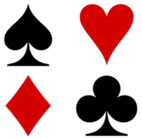
- In Matlab
    - function normfit() (Statistics Toolbox) does the work for you!
- Input:
    - Data
    - Alpha (1-a = conf level)
- Output:
    - Mean
    - Standard Deviation
    - Mean confidence interval
    - Standard deviation confidence interval

Overview of Topics

- Confidence interval
  - Filler machine example
  - Confidence level
  - Matlab code
- Statistical hypothesis testing
  - Magician example
  - Statistical significance

Magician Example (1)

- A man claims he has “clairvoyance“ (has extra-sensory perception).
  - We want to test him!
- We show him the reverse of a randomly chosen play cards 25 times and ask which suit it belongs to.
- Interpretation of the number of hits X:
  - With 5 or 6, he is clearly an impostor.
  - With 23 or 24 he truly is a magician!
  - But what about values in-between? From what value on is he gifted?



Statistical significance is a concept that allows us to treat the last question.

Statistical Significance

- A result is statistically significant if it is unlikely to have occurred by chance
  - This does not mean that the result has a real impact in the real world, but just that is statistically surprising
- Associated with a significance level α
  - Typical values: 5%, 1%, 0.1%
- Interpretation: $\alpha = 0.1\% \rightarrow$ “There is only one chance over a thousand that this could have happened by chance“

Magician Example (2)

- Denote with p the probability of a correct guess
- Two hypotheses:
  - H0: $p = 1/4$ (random guess)
  - H1: $p > 1/4$ (magic powers)
- Only one hypothesis is true
- With c, we denote how many correct guesses we require to believe that the guy is magical.
  - The higher c, the more strict and critical we are.

The first hypothesis is also called null hypothesis, as it is what we believe is the default state of things.

Magician Example (3)

- Our test will accept one of the two hypotheses
  - One way to consider our test is to look at false positive, when a random guesser is accepted as magician
- The value c influence such probability:

$$P(\text{reject } H_0 | H_0 \text{ is valid}) = P(X \geq 25 | p = \tfrac{1}{4}) = \left(\tfrac{1}{4}\right)^{25} \approx 10^{-15},$$

- With c = 25, there is a very low probability that the guy is guessing randomly
- $$P(\text{reject } H_0 | H_0 \text{ is valid}) = P(X \geq 10 | p = \tfrac{1}{4}) \approx 0.07.$$
- With c = 10, there is a higher probability to have a false positive

Magician Example (4)

- In practice, one selects a significance level α, and sets the probability of a false positive to it
  - Example: For α = 1%

$$P(\text{reject } H_0 | H_0 \text{ is valid}) = P(X \geq c | p = \tfrac{1}{4}) \leq 0.01.$$

- Then one picks the smallest c for which the inequality holds.
  - In our example c = 12.
- The general formula is:

$$P(reject\, H_0 | H_0\, is\, valid) = (\tfrac{1}{4})^c (\tfrac{3}{4})^{25-c} \frac{25!}{c!(25-c)!} \leq \alpha$$

How do I solve it? For instance using a brute force with growing ***c*** from 0 to 25.

Magician Example (5)

- Notice that a very unlikely result can be statistically significant!
  - Imagine that the guy guessed all 25 cards wrong
- The probability of guessing a card wrong is p’ = ¾
- The probability of guessing no card correctly is:

$$P(\text{reject } H_0 | H_0 \text{ is valid}) = P(X \geq 25 | p' = \tfrac{3}{4}) = \left(\tfrac{3}{4}\right)^{25} \approx 0.00075.$$

- This is very unlikely, and as well magical as high scores!

Magician Example (6)

- To answer the original question …
- 1) decide how strict you want to be!
  - for instance: very strict, with a significance level α of 1%!
- 2) compute the corresponding c
  - for $\alpha = 1\%$ we obtain $c = 12$
- 3) test the candidate and compare the number of correct guesses with c:
  - with 12 or more correct guesses the guy has magic powers
  - with less than 12 correct guesses they guy is an impostor

Further Reading

- http://en.wikipedia.org/wiki/Confidence_interval
- http://www.stat.yale.edu/Courses/1997-98/101/confint.htm
- http://en.wikipedia.org/wiki/Statistical_hypothesis_testing