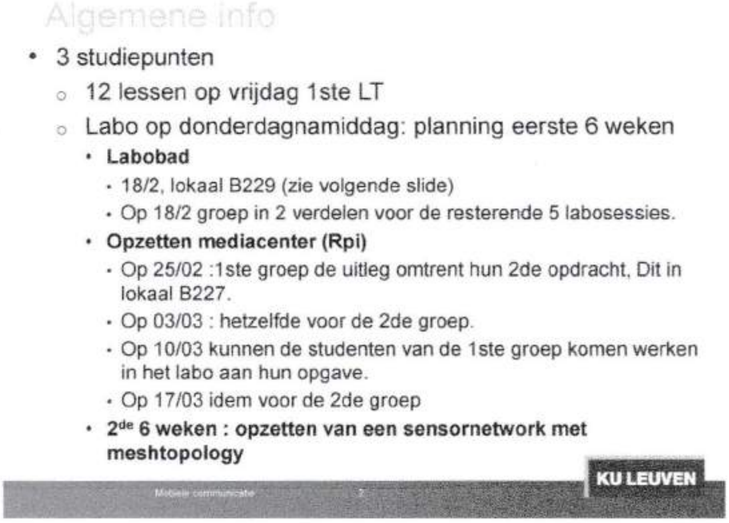
KU LEUVEN TECHNOLOGIECAMPUS GENT

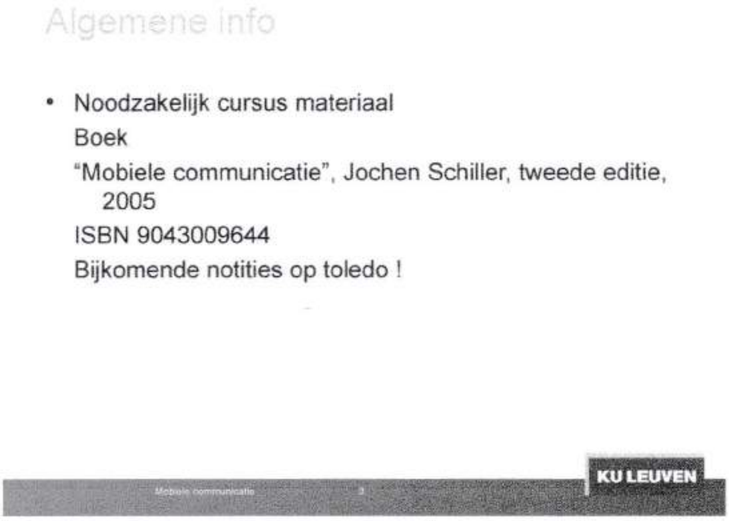
Mobiele Communicatie

Lieven De Strycker
KU Leuven Technologie Campus Gent – 2016



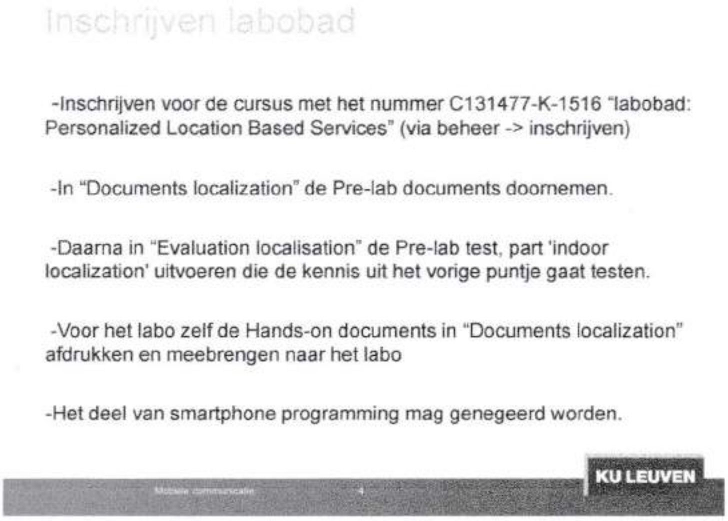
Algemene info

- 3 studiepunten
  - 12 lessen op vrijdag 1ste LT
  - Labo op donderdagnamiddag: planning eerste 6 weken
    - **Labobad**
      - 18/2, lokaal B229 (zie volgende slide)
      - Op 18/2 groep in 2 verdelen voor de resterende 5 labosessies.
    - **Opzetten mediacenter (Rpi)**
      - Op 25/02 :1ste groep de uitleg omtrent hun 2de opdracht, Dit in lokaal B227.
      - Op 03/03 : hetzelfde voor de 2de groep.
      - Op 10/03 kunnen de studenten van de 1ste groep komen werken in het labo aan hun opgave.
      - Op 17/03 idem voor de 2de groep
    - **2de 6 weken : opzetten van een sensornetwork met meshtopology**



Algemene info

- Noodzakelijk cursus materiaal
  Boek
  "Mobiele communicatie", Jochen Schiller, tweede editie, 2005
  ISBN 9043009644
  Bijkomende notities op toledo !



Inschrijven labobad

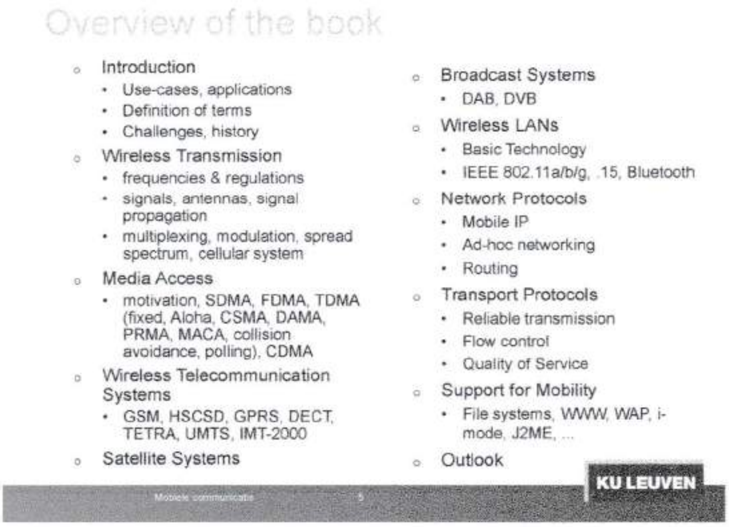
-Inschrijven voor de cursus met het nummer C131477-K-1516 "labobad: Personalized Location Based Services" (via beheer -> inschrijven)

-In "Documents localization" de Pre-lab documents doornemen.

-Daarna in "Evaluation localisation" de Pre-lab test, part 'indoor localization' uitvoeren die de kennis uit het vorige puntje gaat testen.

-Voor het labo zelf de Hands-on documents in "Documents localization" afdrukken en meebrengen naar het labo

-Het deel van smartphone programming mag genegeerd worden.



Overview of the book

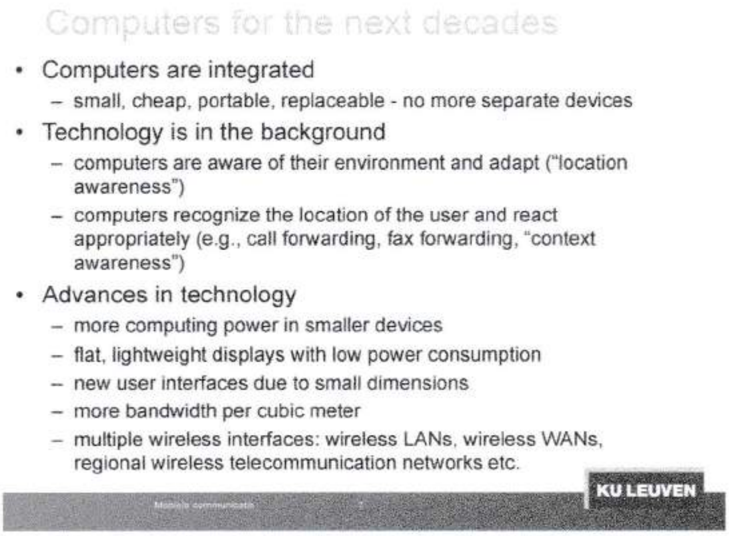
- Introduction
  - Use-cases, applications
  - Definition of terms
  - Challenges, history
- Wireless Transmission
  - frequencies & regulations
  - signals, antennas, signal propagation
  - multiplexing, modulation, spread spectrum, cellular system
- Media Access
  - motivation, SDMA, FDMA, TDMA (fixed, Aloha, CSMA, DAMA, PRMA, MACA, collision avoidance, polling), CDMA
- Wireless Telecommunication Systems
  - GSM, HSCSD, GPRS, DECT, TETRA, UMTS, IMT-2000
- Satellite Systems
- Broadcast Systems
  - DAB, DVB
- Wireless LANs
  - Basic Technology
  - IEEE 802.11a/b/g, .15, Bluetooth
- Network Protocols
  - Mobile IP
  - Ad-hoc networking
  - Routing
- Transport Protocols
  - Reliable transmission
  - Flow control
  - Quality of Service
- Support for Mobility
  - File systems, WWW, WAP, i-mode, J2ME, ...
- Outlook

KU LEUVEN

KU LEUVEN

TECHNOLOGIECAMPUS GENT

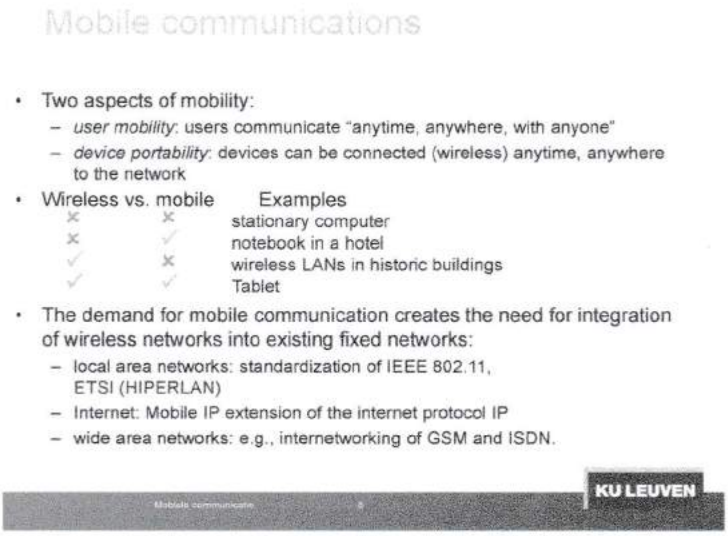
Hoofdstuk 1 - Inleiding



Computers for the next decades

- Computers are integrated
  - small, cheap, portable, replaceable - no more separate devices
- Technology is in the background
  - computers are aware of their environment and adapt ("location awareness")
  - computers recognize the location of the user and react appropriately (e.g., call forwarding, fax forwarding, "context awareness")
- Advances in technology
  - more computing power in smaller devices
  - flat, lightweight displays with low power consumption
  - new user interfaces due to small dimensions
  - more bandwidth per cubic meter
  - multiple wireless interfaces: wireless LANs, wireless WANs, regional wireless telecommunication networks etc.

KU LEUVEN



Mobile communications

- Two aspects of mobility:
  - *user mobility*: users communicate "anytime, anywhere, with anyone"
  - *device portability*: devices can be connected (wireless) anytime, anywhere to the network
- Wireless vs. mobile Examples

Wireless	vs. mobile	Examples
×	×	stationary computer
×	✓	notebook in a hotel
✓	×	wireless LANs in historic buildings
✓	✓	Tablet

- The demand for mobile communication creates the need for integration of wireless networks into existing fixed networks:
  - local area networks: standardization of IEEE 802.11, ETSI (HIPERLAN)
  - Internet: Mobile IP extension of the internet protocol IP
  - wide area networks: e.g., internetworking of GSM and ISDN.

KU LEUVEN

$CV^2 f$ CMOS

$\sim$

C_g

↑

E condensator $= \frac{1}{2} CV^2$

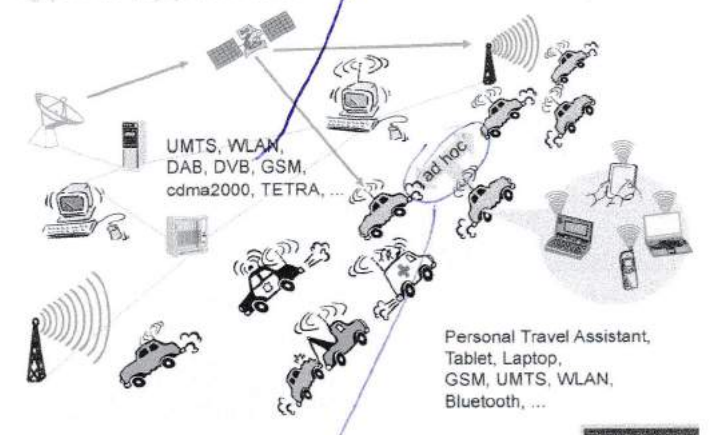
Verbeteren

- C_g ↓ door afstand ↓ ⇒ kleiner.
- V ↓ van 5V → 3.3V → 0,8V.

  limiet door bandgap (0,6V)
- dynamisch klokfreq. regelen.

DVB-T ← tussen antennes
-S ← satelieten
-H ← voor mobiele toestanden.
digital video Broadcaster

Typical application

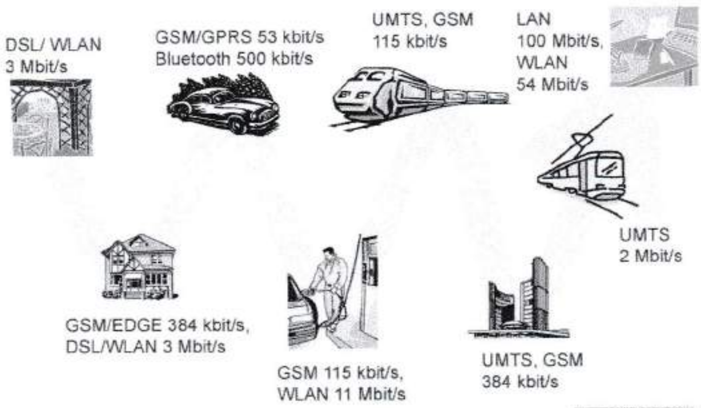


UMTS, WLAN, DAB, DVB, GSM, cdma2000, TETRA, ...

ad hoc

Personal Travel Assistant, Tablet, Laptop, GSM, UMTS, WLAN, Bluetooth, ...

Typical application



DSL/ WLAN 3 Mbit/s

GSM/GPRS 53 kbit/s Bluetooth 500 kbit/s

UMTS, GSM 115 kbit/s

LAN 100 Mbit/s, WLAN 54 Mbit/s

UMTS 2 Mbit/s

GSM/EDGE 384 kbit/s, DSL/WLAN 3 Mbit/s

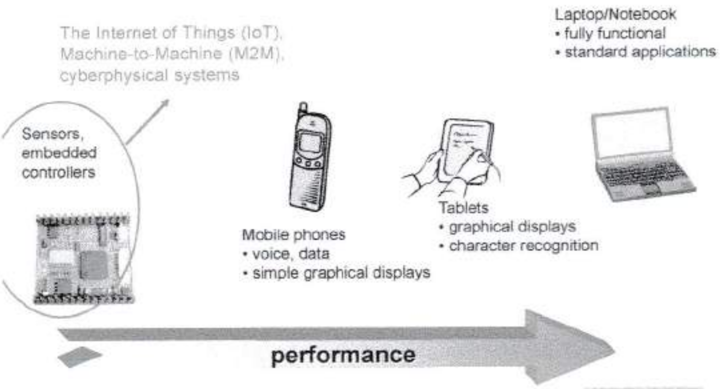
GSM 115 kbit/s, WLAN 11 Mbit/s

UMTS, GSM 384 kbit/s

geen vaste infrastructuur.
- bluethoot
- wifi tussen apparaten.

niet:
- 3G ⇒ vaste antennes
- WIFI netwerk ⇒ vaste Access Points

Mobile devices



The Internet of Things (IoT), Machine-to-Machine (M2M), cyberphysical systems

Sensors, embedded controllers

Mobile phones
- voice, data
- simple graphical displays

Tablets
- graphical displays
- character recognition

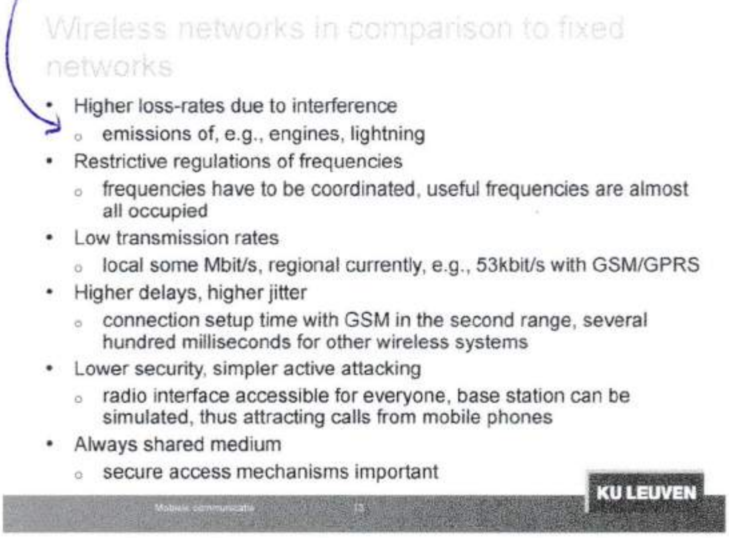
Laptop/Notebook
- fully functional
- standard applications

performance

Effects of device portability

- Power consumption
  - limited computing power, low quality displays due to limited battery capacity
  - CPU: power consumption ~ CV^2f
    - C: internal capacity, reduced by integration
    - V: supply voltage, can be reduced to a certain limit
    - f: clock frequency, can be reduced temporally
  - Battery takes up most of volume
- Loss of data
  - higher probability, has to be included in advance into the design (e.g., defects, theft)
- Limited user interfaces
  - compromise between size of fingers and portability
  - integration of character/voice recognition, abstract symbols
- Limited memory
  - limited value of mass memories with moving parts
  - flash-memory or ? as alternative

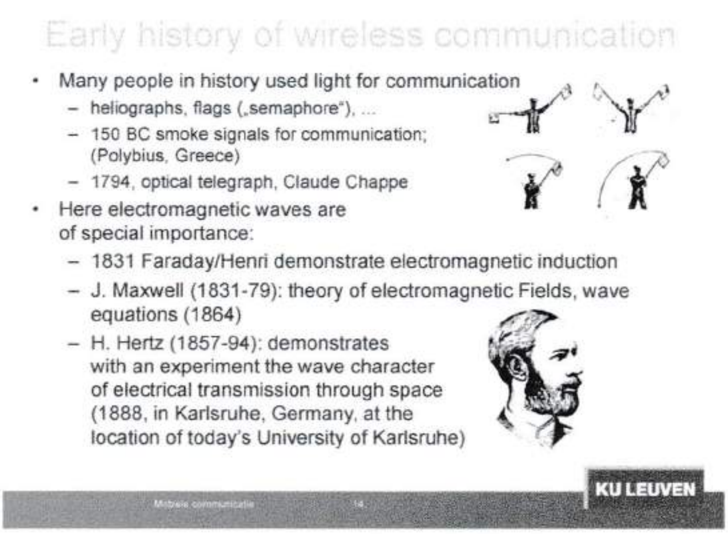
veel meer Ack, fout correctie nodig



Wireless networks in comparison to fixed networks

- Higher loss-rates due to interference
  - emissions of, e.g., engines, lightning
- Restrictive regulations of frequencies
  - frequencies have to be coordinated, useful frequencies are almost all occupied
- Low transmission rates
  - local some Mbit/s, regional currently, e.g., 53kbit/s with GSM/GPRS
- Higher delays, higher jitter
  - connection setup time with GSM in the second range, several hundred milliseconds for other wireless systems
- Lower security, simpler active attacking
  - radio interface accessible for everyone, base station can be simulated, thus attracting calls from mobile phones
- Always shared medium
  - secure access mechanisms important

KU LEUVEN

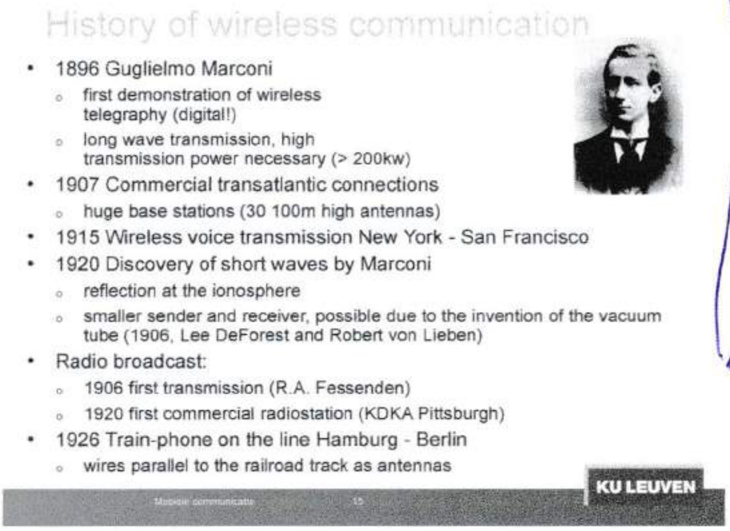


Early history of wireless communication

- Many people in history used light for communication
  - heliographs, flags („semaphore"), ...
  - 150 BC smoke signals for communication; (Polybius, Greece)
  - 1794, optical telegraph, Claude Chappe
- Here electromagnetic waves are of special importance:
  - 1831 Faraday/Henri demonstrate electromagnetic induction
  - J. Maxwell (1831-79): theory of electromagnetic Fields, wave equations (1864)
  - H. Hertz (1857-94): demonstrates with an experiment the wave character of electrical transmission through space (1888, in Karlsruhe, Germany, at the location of today's University of Karlsruhe)

KU LEUVEN

Blauw: Telefonie
Groen: mobiel
Rood: WLAN

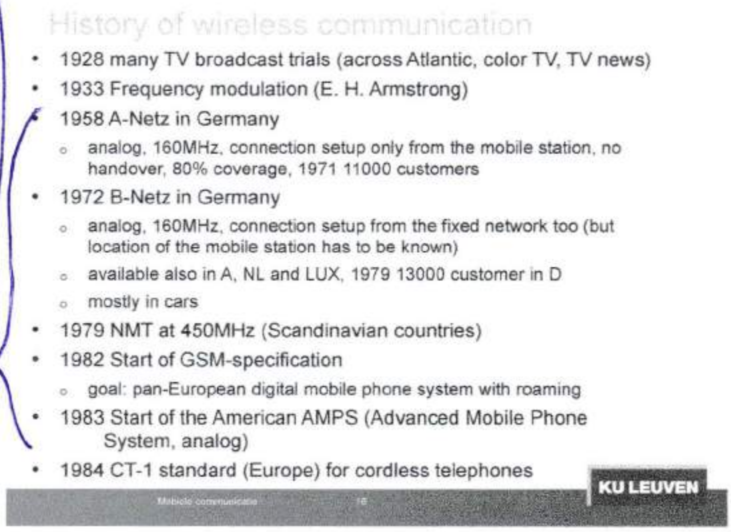


History of wireless communication

- 1896 Guglielmo Marconi
  - first demonstration of wireless telegraphy (digital!)
  - long wave transmission, high transmission power necessary (> 200kw)
- 1907 Commercial transatlantic connections
  - huge base stations (30 100m high antennas)
- 1915 Wireless voice transmission New York - San Francisco
- 1920 Discovery of short waves by Marconi
  - reflection at the ionosphere
  - smaller sender and receiver, possible due to the invention of the vacuum tube (1906, Lee DeForest and Robert von Lieben)
- Radio broadcast:
  - 1906 first transmission (R.A. Fessenden)
  - 1920 first commercial radiostation (KDKA Pittsburgh)
- 1926 Train-phone on the line Hamburg - Berlin
  - wires parallel to the railroad track as antennas

KU LEUVEN

mobiele telefonie.



History of wireless communication

- 1928 many TV broadcast trials (across Atlantic, color TV, TV news)
- 1933 Frequency modulation (E. H. Armstrong)
- 1958 A-Netz in Germany
  - analog, 160MHz, connection setup only from the mobile station, no handover, 80% coverage, 1971 11000 customers
- 1972 B-Netz in Germany
  - analog, 160MHz, connection setup from the fixed network too (but location of the mobile station has to be known)
  - available also in A, NL and LUX, 1979 13000 customer in D
  - mostly in cars
- 1979 NMT at 450MHz (Scandinavian countries)
- 1982 Start of GSM-specification
  - goal: pan-European digital mobile phone system with roaming
- 1983 Start of the American AMPS (Advanced Mobile Phone System, analog)
- 1984 CT-1 standard (Europe) for cordless telephones

KU LEUVEN

History of wireless communication

- 1986 C-Netz in Germany
  - analog voice transmission, 450MHz, hand-over possible, digital signaling, automatic location of mobile device
  - Was in use until 2000, services: FAX, modem, X.25, e-mail, 98% coverage
- 1991 Specification of DECT
  - Digital European Cordless Telephone (today: Digital Enhanced Cordless Telecommunications)
  - 1880-1900MHz, ~100-500m range, 120 duplex channels, 1.2Mbit/s data transmission, voice encryption, authentication, up to several 10000 user/km2, used in more than 50 countries
- 1992 Start of GSM
  - fully digital, 900MHz, 124 channels
  - automatic location, hand-over, cellular
  - roaming in Europe - now worldwide in more than 200 countries
  - services: data with 9.6kbit/s, FAX, voice, ...

KU LEUVEN

History of wireless communication

- 1994 E-Netz in Germany
  - GSM with 1800MHz, smaller cells
  - As Eplus in D (1997 98% coverage of the *population*)
- 1996 HiperLAN (High Performance Radio Local Area Network)
  - ETSI, standardization of type 1: 5.15 - 5.30GHz, 23.5Mbit/s
  - recommendations for type 2 and 3 (both 5GHz) and 4 (17GHz) as wireless ATM-networks (up to 155Mbit/s)
- 1997 Wireless LAN - IEEE802.11
  - IEEE standard, 2.4 - 2.5GHz and infrared, 2Mbit/s
  - already many (proprietary) products available in the beginning
- 1998 Specification of GSM successors
  - for UMTS (Universal Mobile Telecommunication System) as European proposals for IMT-2000
- Iridium
  - 66 satellites (+6 spare), 1.6GHz to the mobile phone

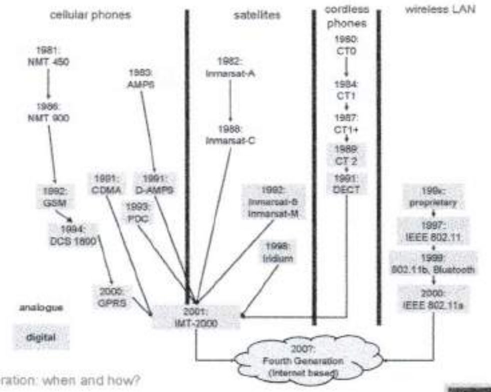
KU LEUVEN

History of wireless communication

- 1999 Standardization of additional wireless LANs
  - IEEE standard 802.11b, 2.4-2.5GHz, 11Mbit/s
  - Bluetooth for piconets, 2.4Ghz, <1Mbit/s
- Decision about IMT-2000
  - Several "members" of a "family": UMTS, cdma2000, DECT, ...
- Start of WAP (Wireless Application Protocol) and i-mode
  - First step towards a unified Internet/mobile communicaiton system
  - Access to many services via the mobile phone
- 2000 GSM with higher data rates
  - HSCSD offers up to 57,6kbit/s
  - First GPRS trials with up to 50 kbit/s (packet oriented!)
- UMTS auctions/beauty contests
  - Hype followed by disillusionment (50 B$ payed in Germany for 6 licenses!)
- 2001 Start of 3G systems
  - Cdma2000 in Korea, UMTS tests in Europe, Foma (almost UMTS) in Japan

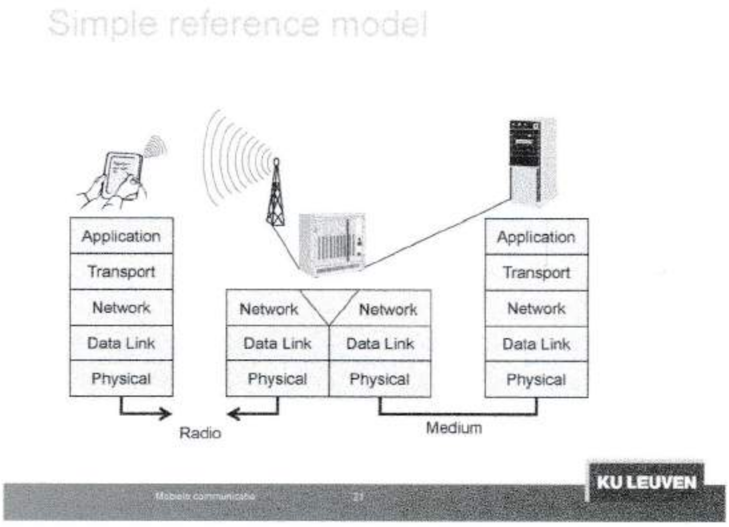
KU LEUVEN

Wireless systems: overview of the development

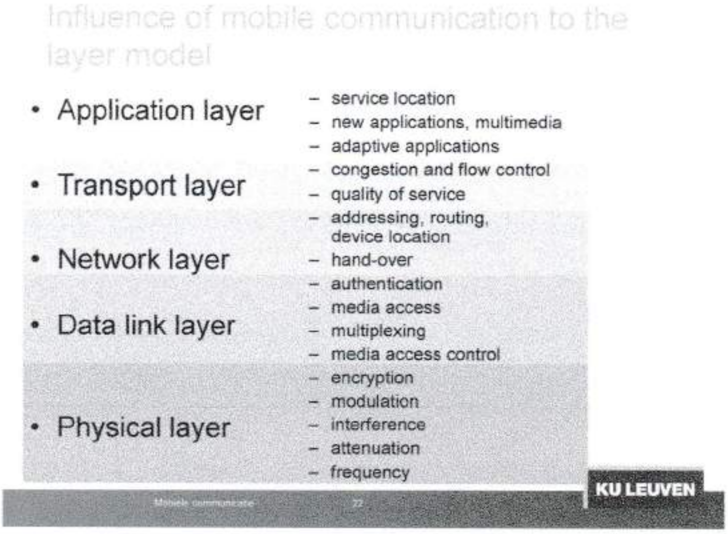


4G – fourth generation: when and how?

KU LEUVEN

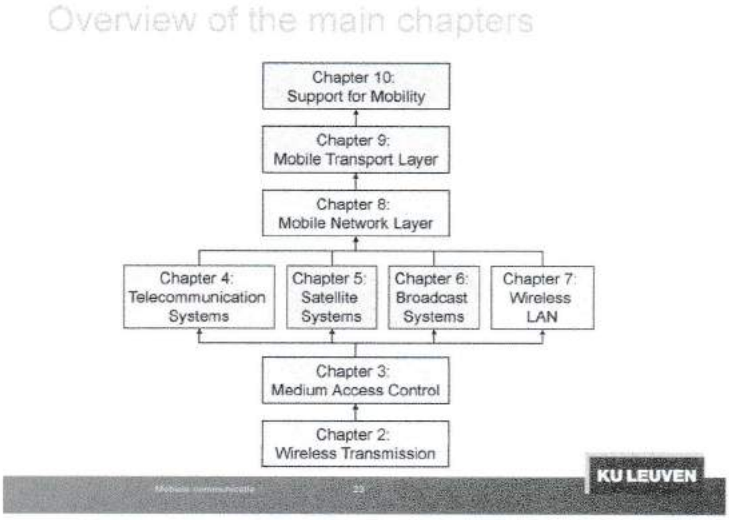


Simple reference model



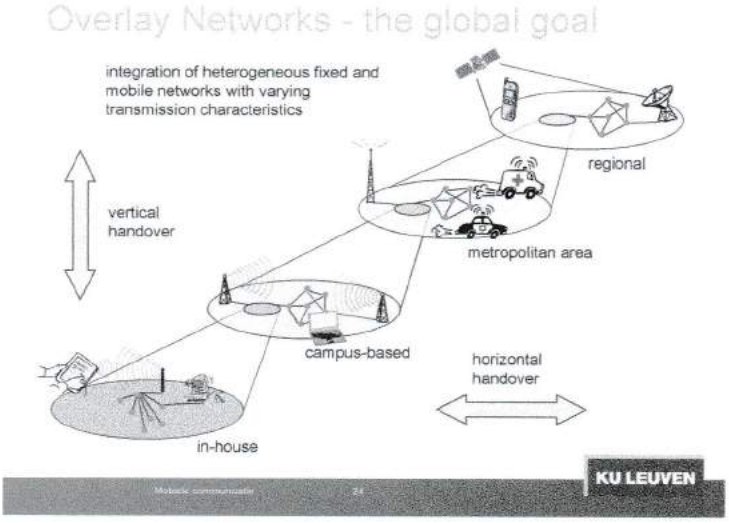
Influence of mobile communication to the layer model

- Application layer
  - service location
  - new applications, multimedia
  - adaptive applications
- Transport layer
  - congestion and flow control
  - quality of service
- Network layer
  - addressing, routing, device location
  - hand-over
- Data link layer
  - authentication
  - media access
  - multiplexing
  - media access control
- Physical layer
  - encryption
  - modulation
  - interference
  - attenuation
  - frequency



Overview of the main chapters

Chapter 10: Support for Mobility
Chapter 9: Mobile Transport Layer
Chapter 8: Mobile Network Layer
Chapter 4: Telecommunication Systems
Chapter 5: Satellite Systems
Chapter 6: Broadcast Systems
Chapter 7: Wireless LAN
Chapter 3: Medium Access Control
Chapter 2: Wireless Transmission



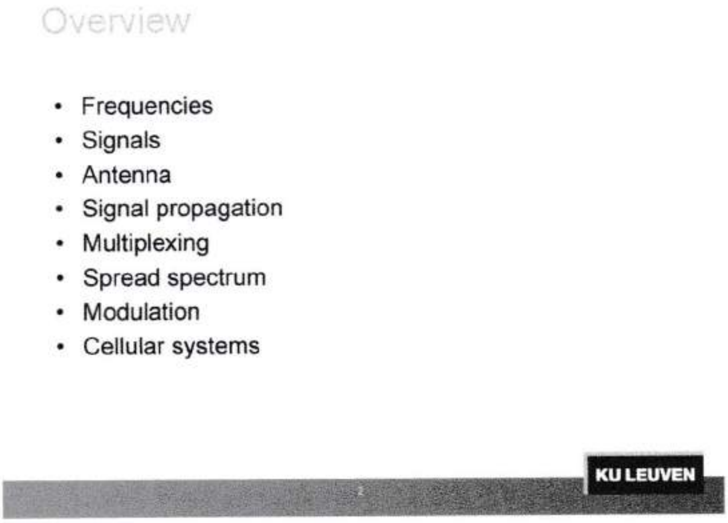
Overlay Networks - the global goal

integration of heterogeneous fixed and mobile networks with varying transmission characteristics

KU LEUVEN

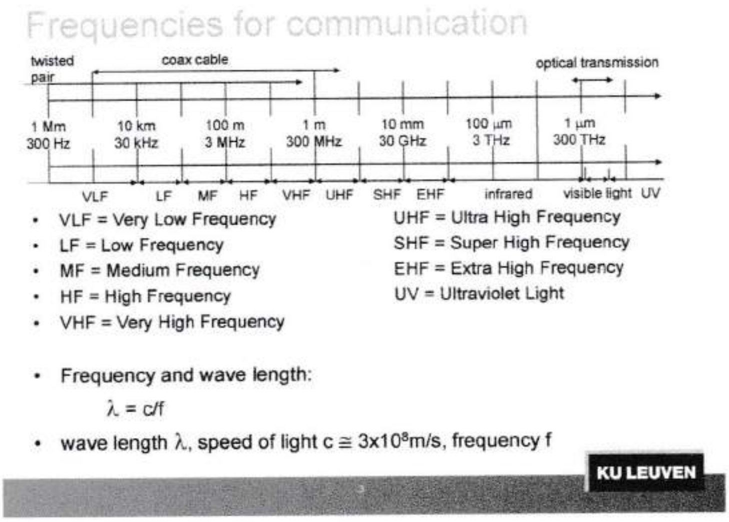
TECHNOLOGIECAMPUS GENT

Hoofdstuk 2 – Draadloze transmissie



Overview

- Frequencies
- Signals
- Antenna
- Signal propagation
- Multiplexing
- Spread spectrum
- Modulation
- Cellular systems



Frequencies for communication

- VLF = Very Low Frequency
- LF = Low Frequency
- MF = Medium Frequency
- HF = High Frequency
- VHF = Very High Frequency

UHF = Ultra High Frequency

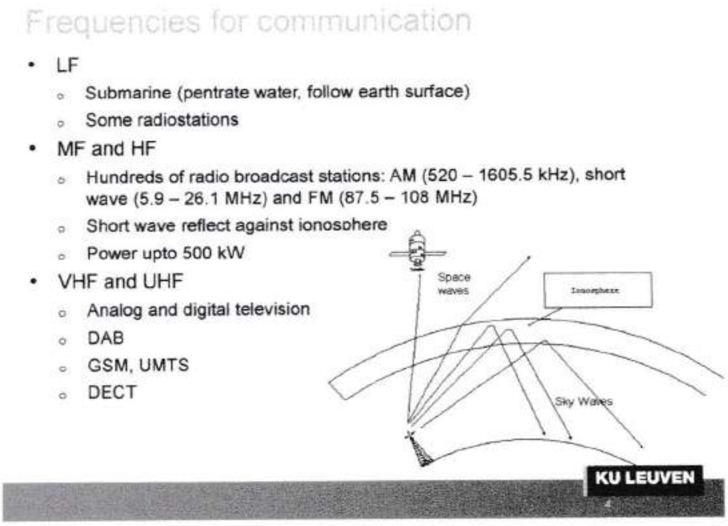
SHF = Super High Frequency

EHF = Extra High Frequency

UV = Ultraviolet Light

- Frequency and wave length:

  $\lambda = c/f$
- wave length λ, speed of light $c \cong 3x10^8$m/s, frequency f



Frequencies for communication

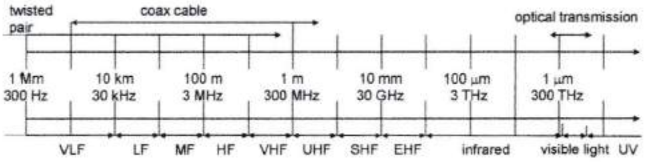
- LF
  - Submarine (pentrate water, follow earth surface)
  - Some radiostations
- MF and HF
  - Hundreds of radio broadcast stations: AM (520 – 1605.5 kHz), short wave (5.9 – 26.1 MHz) and FM (87.5 – 108 MHz)
  - Short wave reflect against ionosohere
  - Power upto 500 kW
- VHF and UHF
  - Analog and digital television
  - DAB
  - GSM, UMTS
  - DECT

Frequencies for communication

- VHF-/UHF-ranges for mobile radio
  - simple, small antenna for cars
  - deterministic propagation characteristics, reliable connections
- SHF and higher for directed radio links, satellite communication (C-band, Ku-band, Ka-band)
  - small antenna, beam forming
  - large bandwidth available
- Wireless LANs use frequencies in UHF to SHF range
  - some systems planned up to EHF (60 GHz for indoor HD TV distribution)
  - limitations due to absorption by water and oxygen molecules (resonance frequencies)
    - weather dependent fading, signal loss caused by heavy rainfall etc.
- Infra red (IR)
  - Laser between buildings
  - IrDA (850 – 900 nm) to connect laptops, PDA's,...
  - Optical fiber (1350 nm and 1500 nm)

KU LEUVEN

Frequencies



- Different frequencies for different applications: strictly regulated !
  - In Belgium controlled by BIPT
  - In U.S by FCC
  - Worldwide management ITU-T
- Example

  GSM : 890-915 MHz (up), 935-960 MHz(down) (=124 channels) and 1710-1785 MHz (up), 1805-1880 (down) (=374 channels)
- Example

  Auction 3G and '4G' bands in Belgium in 2011

BIPT

Spectrum is scarce (expensive)

KU LEUVEN

Frequencies

- License free frequency bands :

  ISM (Industrial, Science, Medical)
  - 433 MHz : e.g. wireless control (keys, doorbell)
  - 868 MHz : e.g. wireless domotics (-> 915 MHz in US)
  - 2.4 GHz : e.g. WiFi, ZigBee, Bluetooth
  - 5.7 GHz
  - 61 GHz
  - No license required BUT strict rules

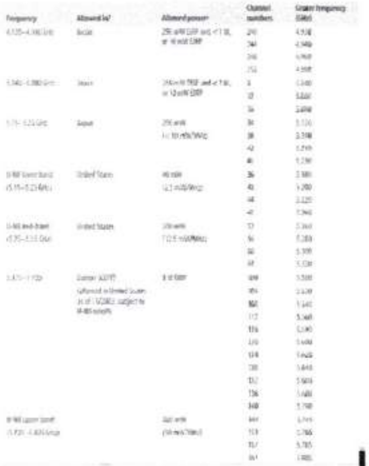
KU LEUVEN

5 GHz:

Operating channels for 802.11a/h/j

802.11h is an adapted version of 802.11a for Europe including
- Transmit Power Control
- Dynamic Frequency Selection

U-NII = Unlicensed National Information Infrastructure



Frequency	Allowed in?	Allowed power	Channel numbers	Center frequency (GHz)
4.915–4.980 GHz	Japan	250 mW EIRP and <1 W, or 10 mW EIRP	240	4.920
			244	4.940
			248	4.960
			252	4.980
5.040–5.080 GHz	Japan	250 mW EIRP and <1 W, or 12 mW EIRP	8	5.040
			12	5.060
			16	5.080
5.15–5.25 GHz	Japan	250 mW (= 10 mW/MHz)	34	5.170
			38	5.190
			42	5.210
			46	5.230
U-NII lower band (5.15–5.25 GHz)	United States	40 mW (2.5 mW/MHz)	36	5.180
			40	5.200
			44	5.220
			48	5.240
U-NII mid-band (5.25–5.35 GHz)	United States	200 mW (12.5 mW/MHz)	52	5.260
			56	5.280
			60	5.300
			64	5.320
5.470–5.725 GHz	Europe (ETSI) (allowed in United States as of 1/2003, subject to [illegible])	1 W EIRP	100	5.500
			104	5.520
			108	5.540
			112	5.560
			116	5.580
			120	5.600
			124	5.620
			128	5.640
			132	5.660
			136	5.680
			140	5.700
U-NII upper band (5.725–5.825 GHz)		800 mW (50 mW/MHz)	149	5.745
			153	5.765
			157	5.785
			161	5.805

KU LEUVEN

Frequencies and regulations

- ITU-R holds auctions for new frequencies, manages frequency bands worldwide (WRC, World Radio Conferences)

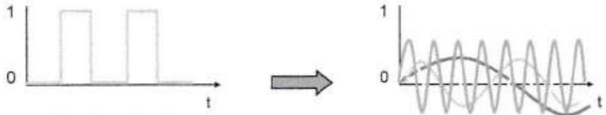
	Europe	USA	Japan
Cellular Phones	**GSM** 450-457, 479-486/460-467,489-496, 890-915/935-960, 1710-1785/1805-1880 **UMTS** (FDD) 1920-1980, 2110-2190 **UMTS** (TDD) 1900-1920, 2020-2025	**AMPS, TDMA, CDMA** 824-849, 869-894 **TDMA, CDMA, GSM** 1850-1910, 1930-1990	**PDC** 810-826, 940-956, 1429-1465, 1477-1513
Cordless Phones	**CT1+** 885-887, 930-932 **CT2** 864-868 **DECT** 1880-1900	**PACS** 1850-1910, 1930-1990 **PACS-UB** 1910-1930	**PHS** 1895-1918 **JCT** 254-380
Wireless LANs	**IEEE 802.11** 2400-2483 **HIPERLAN 2** 5150-5350, 5470-5725	902-928 **IEEE 802.11** 2400-2483 5150-5350, 5725-5825	**IEEE 802.11** 2471-2497 5150-5250
Others	**RF-Control** 27, 128, 418, 433, 868	**RF-Control** 315, 915	**RF-Control** 426, 868

Signals

- physical representation of data
- function of time and location
- signal parameters: parameters representing the value of data
- classification
  - continuous time/discrete time
  - continuous values/discrete values
  - analog signal = continuous time and continuous values
  - digital signal = discrete time and discrete values
- signal parameters of periodic signals:
  period T, frequency f=1/T, amplitude A, phase shift φ
  - sine wave as special periodic signal for a carrier:
    $s(t) = A_t \sin(2 \pi f_t t + \varphi_t)$

Fourierreeks

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft)$$

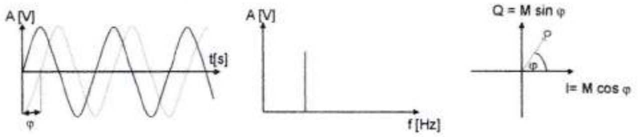


ideal periodic signal

real composition (based on harmonics)

Signals

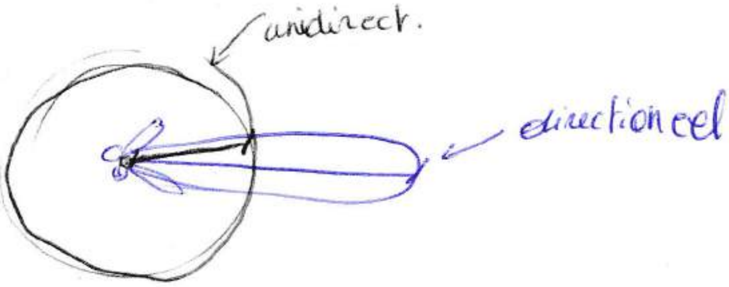
- Different representations of signals
  - amplitude (amplitude domain)
  - frequency spectrum (frequency domain)
  - phase state diagram (amplitude M and phase φ in polar coordinates)



- Composed signals transferred into frequency domain using Fourier transformation
- Digital signals need
  - infinite frequencies for perfect transmission
  - modulation with a carrier frequency for transmission (analog signal!)

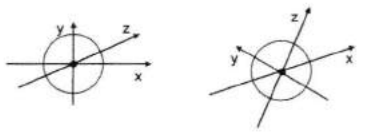
gain.

verhouding $\frac{\text{unidir.}}{\text{dir}}$



Antennas: isotropic radiator

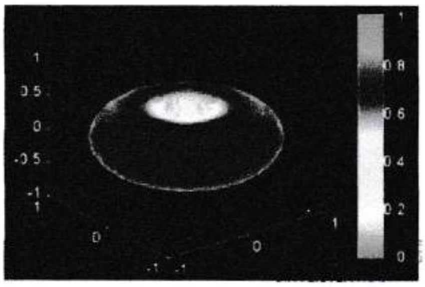
- Radiation and reception of electromagnetic waves, coupling of wires to space for radio transmission
- Isotropic radiator: equal radiation in all directions (three dimensional) - only a theoretical reference antenna
- Real antennas always have directive effects (vertically and/or horizontally)
- Radiation pattern: measurement of radiation around an antenna



ideal
isotropic
radiator

Antennas: simple dipoles

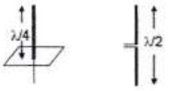
- Radiation pattern simple dipole



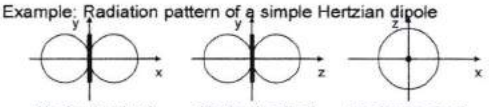
- Gain: maximum power in the direction of the main lobe compared to the power of an isotropic radiator (with the same average power)

Antennas: simple dipoles

- Real antennas are not isotropic radiators but, e.g., dipoles with lengths λ/4 on car roofs or λ/2 as Hertzian dipole
  → shape of antenna proportional to wavelength



- Example: Radiation pattern of a simple Hertzian dipole



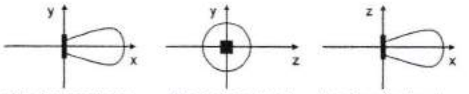
side view (xy-plane) side view (yz-plane) top view (xz-plane)

simple
dipole

- Gain: maximum power in the direction of the main lobe compared to the power of an isotropic radiator (with the same average power)

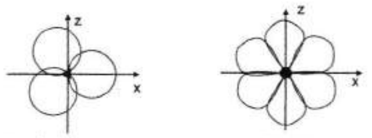
Antennas: directed and sectorized

- Often used for microwave connections or base stations for mobile phones (e.g., radio coverage of a valley)



side view (xy-plane) side view (yz-plane) top view (xz-plane)

directed
antenna



top view, 3 sector top view, 6 sector

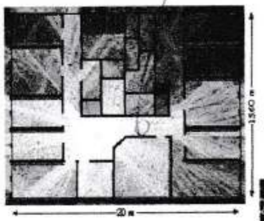
sectorized
antenna

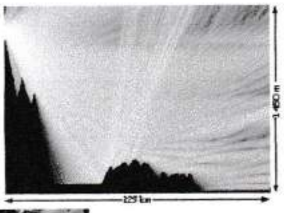
ppt circles.

slide 23

puntjes
→ zwarte puntjes

Real world example



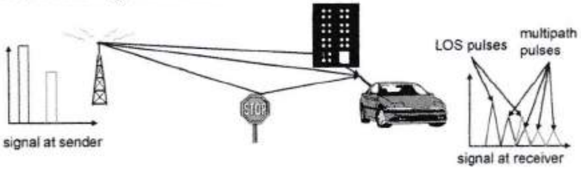


Time and frequency dependent, site survey

KU LEUVEN

Multipath propagation

- Signal can take many different paths between sender and receiver due to reflection, scattering, diffraction



- Time dispersion: signal is dispersed over time (**delay spread**)
  → interference with "neighbor" symbols, Inter Symbol Interference (ISI)
- The signal reaches a receiver directly and phase shifted
  → distorted signal depending on the phases of the different parts
  Known channel characteristics (training sequence, preamble)
  -> equalizer

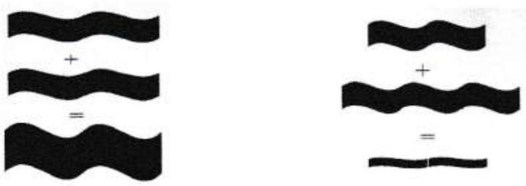
KU LEUVEN

Multipath propagation : signal strength

- **Fast fading explanation**

Two signal with difference in path distance of λ

Two signal with difference in path distance of λ/2

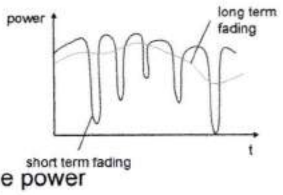


- Frequency dependent : mitigation by frequency hopping (cfr infra)
- Position dependent : mitigation by antenna diversity (switched or combined diversity)

KU LEUVEN

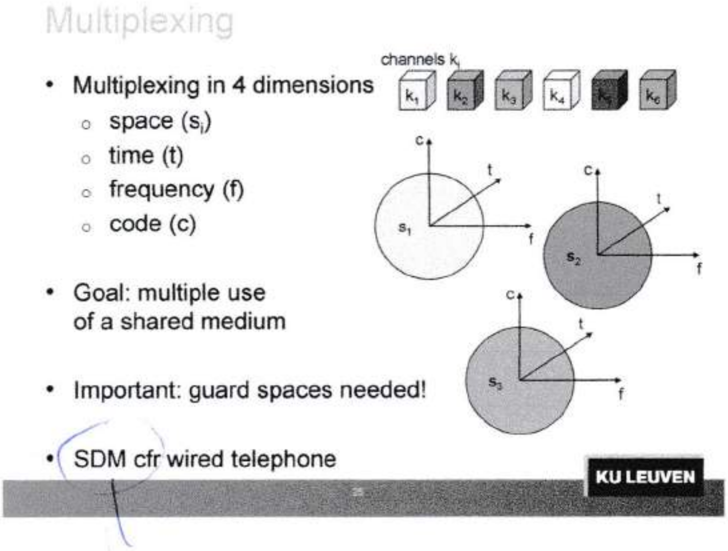
Effects of mobility

- Channel characteristics change over time and location
  - signal paths change
  - different delay variations of different signal parts
  - different phases of signal parts
- → quick changes in the power received (short term fading)



- Additional changes in
  - distance to sender
  - obstacles further away
- → slow changes in the average power received (long term fading)
- Moving sender/receiver: Doppler

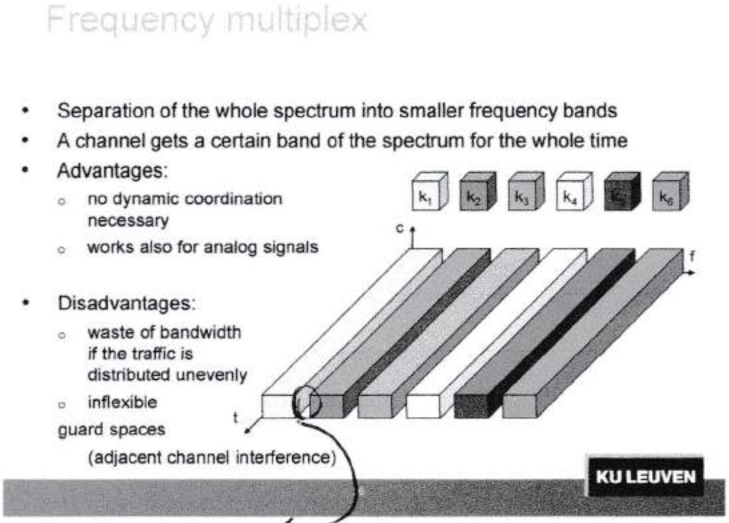
KU LEUVEN



Multiplexing

- Multiplexing in 4 dimensions
  - space (s_i)
  - time (t)
  - frequency (f)
  - code (c)
- Goal: multiple use of a shared medium
- Important: guard spaces needed!
- SDM cfr wired telephone

Space multiple
div.



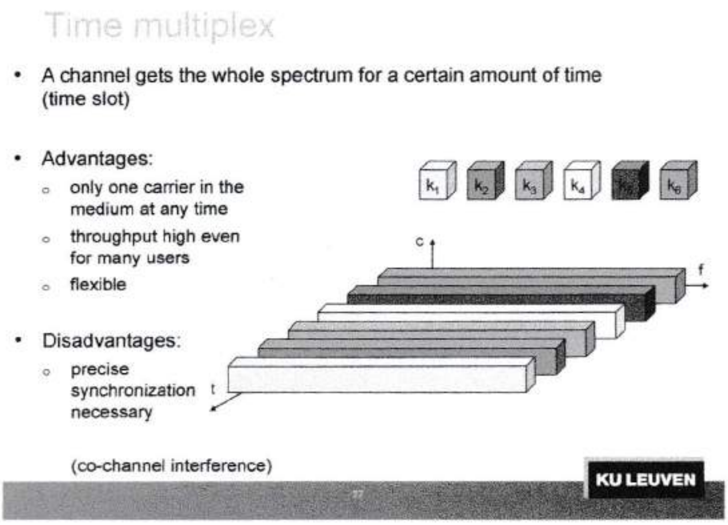
Frequency multiplex

- Separation of the whole spectrum into smaller frequency bands
- A channel gets a certain band of the spectrum for the whole time
- Advantages:
  - no dynamic coordination necessary
  - works also for analog signals
- Disadvantages:
  - waste of bandwidth if the traffic is distributed unevenly
  - inflexible

guard spaces

(adjacent channel interference)

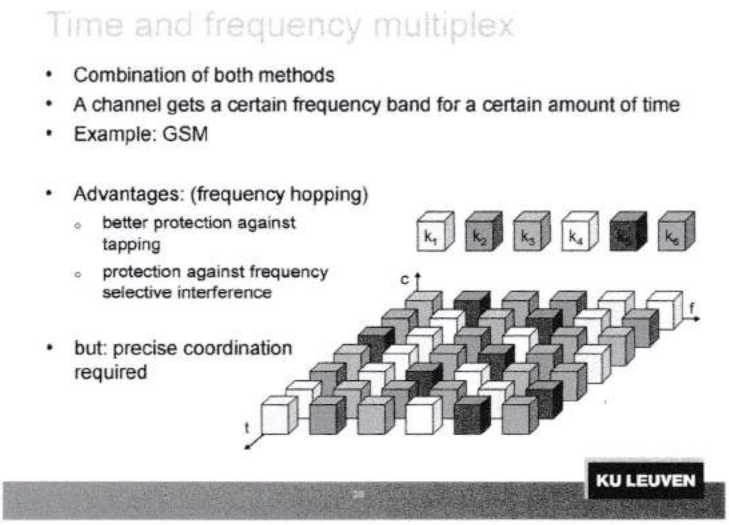
interferentie
tussen twee.



Time multiplex

- A channel gets the whole spectrum for a certain amount of time (time slot)
- Advantages:
  - only one carrier in the medium at any time
  - throughput high even for many users
  - flexible
- Disadvantages:
  - precise synchronization necessary

(co-channel interference)



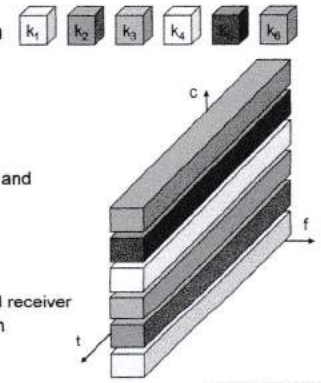
Time and frequency multiplex

- Combination of both methods
- A channel gets a certain frequency band for a certain amount of time
- Example: GSM
- Advantages: (frequency hopping)
  - better protection against tapping
  - protection against frequency selective interference
- but: precise coordination required

→ frequency hopping.

Code multiplex

- Each channel has a unique code
- All channels use the same spectrum at the same time
- Advantages:
  - bandwidth efficient
  - *no coordination and synchronization necessary*
  - good protection against interference and tapping
- Disadvantages:
  - Power control
  - more complex signal regeneration
  - synchronisation between sender and receiver
- Implemented using spread spectrum technology
- Guard spaces -> orthogonal codes

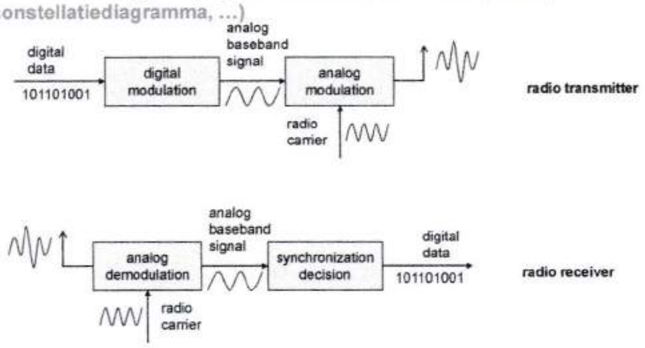


Modulation

- Digital modulation
  - digital data is translated into an analog signal (baseband)
  - ASK, FSK, PSK - main focus in this chapter
  - differences in spectral efficiency, power efficiency, robustness
- Analog modulation
  - shifts center frequency of baseband signal up to the radio carrier
- Motivation
  - smaller antennas (e.g., λ/4)
  - Frequency Division Multiplexing
  - medium characteristics
- Basic schemes
  - Amplitude Modulation (AM)
  - Frequency Modulation (FM)
  - Phase Modulation (PM)

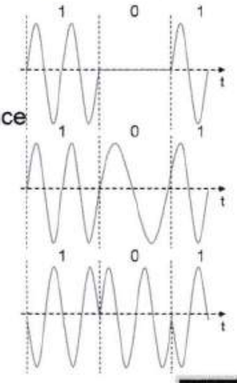
Modulation and demodulation

Zie cursus vorig jaar (digitale modulatie, I en Q componten, constellatiediagramma, ...)



Digital modulation

- Modulation of digital signals known as Shift Keying
- Amplitude Shift Keying (ASK):
  - very simple
  - low bandwidth requirements
  - very susceptible to interference
- Frequency Shift Keying (FSK):
  - needs larger bandwidth
- Phase Shift Keying (PSK):
  - more complex
  - robust against interference



Zender

$Ad = $ "1" → 1

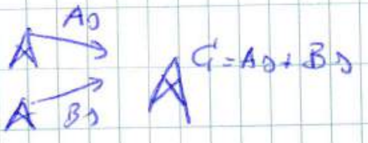
$Bd = $ "0" → -1

$\Rightarrow \quad As = Ad * Ak = -1 \ 1 \ -1 \ -1 \ \ 1 \, 1$

$Bs = Bd * Bk = -1 \ -1 \ 1 \ -1 \ 1 \ -1$

Ontvanger

$C_1 = As + Bs = -2 \ 0 \ 0 \ -2 \ 2 \ 0$



→ Ad uitfilteren:

C_1	-2	0	0	-2	2	0
Ak	-1	1	-1	-1	1	1

$\circ + \Sigma = 2 + 0 + 0 + 2 + 2 + 0 = \underbrace{6}_{\text{'1'}} > 0$

Bd

C_1	-2	0	0	-2	2	0
Bk	+1	+1	-1	+1	-1	+1

$\circ + \Sigma =$

$-2 + 0 + 0 - 2 - 2 + 0 = \underbrace{-6}_{\text{'0'}} < 0$

$C_1 = As + Bs = Ad * Ak + Bd * Bk$

$C_1 \cdot Ak = (Ad * Ak) \circ Ak + (Bd * Bk) \cdot Ak$

$= Ad * \underbrace{(Ak \cdot Ak)}_{=6} + Bd * (\underbrace{Bk \cdot Ak}_{0})$

vervalt

scalair product orthogonaal = 0 ⇒ ⚠

⚠ Synchronisatie

Robuustheid

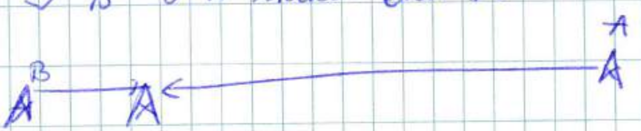
$$\begin{array}{lrrrrrr}
C_i \rightarrow & -2 & 0 & 0 & -2 & +2 & 0 \\
\text{interferentieruis} \rightarrow & 1 & 0 & 1 & 1 & -2 & 2 \\
\hline
 & -1 & 0 & 1 & -1 & 0 & 2 \\
A_k & -1 & 1 & -1 & -1 & 1 & 1 \\
\hline
\end{array}$$

$$\circ \Sigma \quad -1 + 0 + -1 + +1 + 0 + 2 = \cancel{4}\ \underbrace{3 \begin{array}{l} < 6 \\ > 0 \end{array}}_{\Rightarrow \text{'1'}}$$

grotere spreiding ⇒ betere robuustheid

Vermogen controle

Stel Bv. B is 5 x sterker dan A



"near-far"

$$\begin{array}{lrrrrrr}
A_k: & -1 & 1 & -1 & -1 & 1 & 1 \\
5B_k: & -5 & -5 & 5 & -5 & 5 & -5 \\
\hline
\end{array}$$

$C_i \cdot A_k = 6 \leftarrow C_i = -6\ -4\ 4\ -6\ 6\ -4$

$C_i \cdot B_k = -30$

$$\underbrace{+ \text{ ruis / interferentie}}_{\Rightarrow\ = \text{probleem.}}$$

Hoe vind je orthogonale codes?

vb uit UMTS (3G) : OVSF (p167)

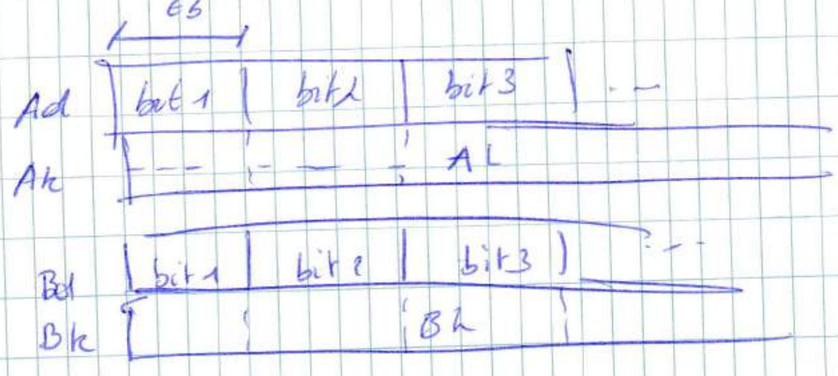
Hadamard matrices

$$1 \rightarrow \underbrace{\left(\begin{array}{c|c} 1 & 1 \\ \hline 1 & -1 \end{array}\right)}_{\text{1 keer omgekeerd teken}} \rightarrow \left(\begin{array}{cc|cc} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \hline 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}\right) \leftarrow \text{orthogonale codes} \quad \ldots$$

Tot hiertoe: lengte code = lengte bit

Praktijk: langere codes → doorlopen

fig 3.14 t.e.m 3.18

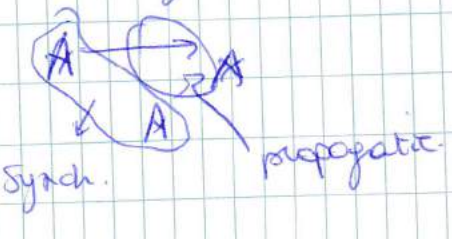


cross correlatie tussen 2 bits in Ak & Bk (over 1 bit) ≈ 0

⇒ ¬ perfect orthogonaal. ↑ lage correlatie waarde

= quasi-orthog. codes

⇒ oplossen problem v. synchronisatie op chip-niveau



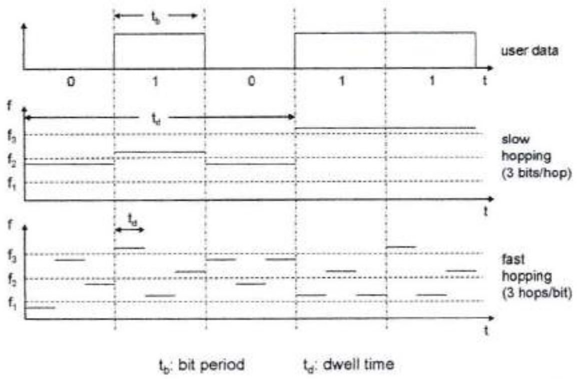
Alternatief: zender XOR / ontvanger *) → zorgt voor inversie (zo in boek)

verder slide 25 H3

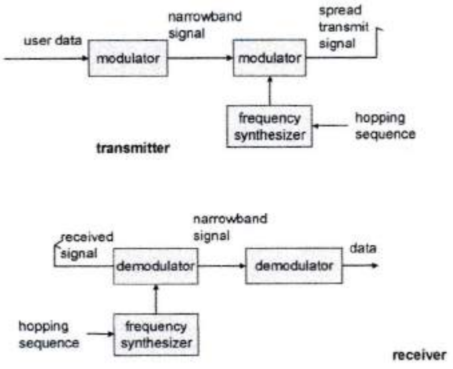
FHSS (Frequency Hopping Spread Spectrum) I

- Discrete changes of carrier frequency
  - sequence of frequency changes determined via pseudo random number sequence
- Two versions
  - Fast Hopping: several frequencies per user bit
  - Slow Hopping: several user bits per frequency
- Advantages
  - frequency selective fading and interference limited to short period
  - simple implementation
  - uses only small portion of spectrum at any time
- Disadvantages
  - not as robust as DSSS
  - simpler to detect

FHSS (Frequency Hopping Spread Spectrum) II



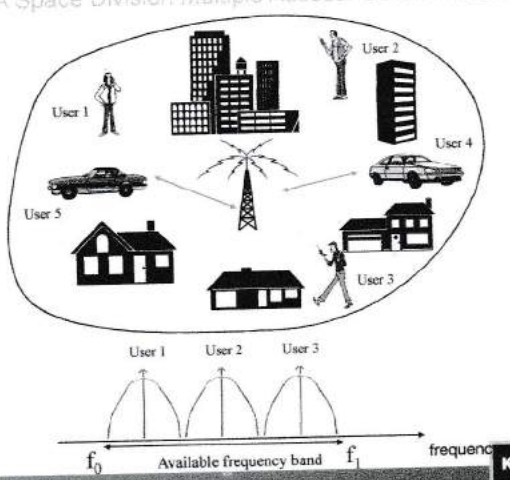
FHSS (Frequency Hopping Spread Spectrum) III



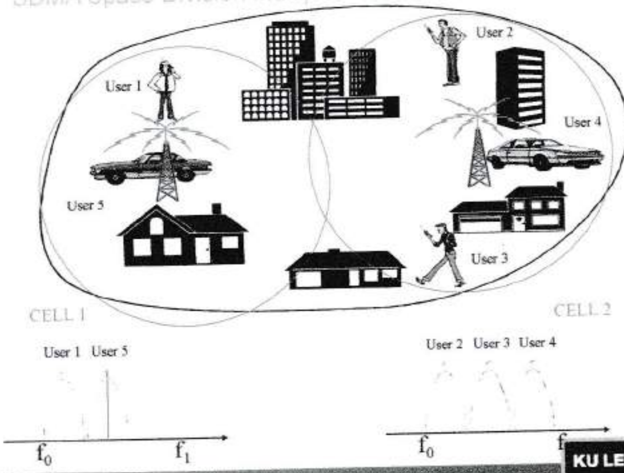
Cell structure

- Implements space division multiplex: base station covers a certain transmission area (cell)
- Mobile stations communicate only via the base station
- Advantages of cell structures:
  - higher capacity, higher number of users
  - less transmission power needed
  - more robust, decentralized
  - base station deals with interference, transmission area etc. *locally*
- Problems:
  - Complex infrastructure: fixed network needed for the base stations, location databases, ...
  - handover (changing from one cell to another) necessary
  - interference with other cells
- Cell sizes from some 100 m in cities to, e.g., 35 km on the country side (GSM) - even less for higher frequencies – not perfect circle or hexagon

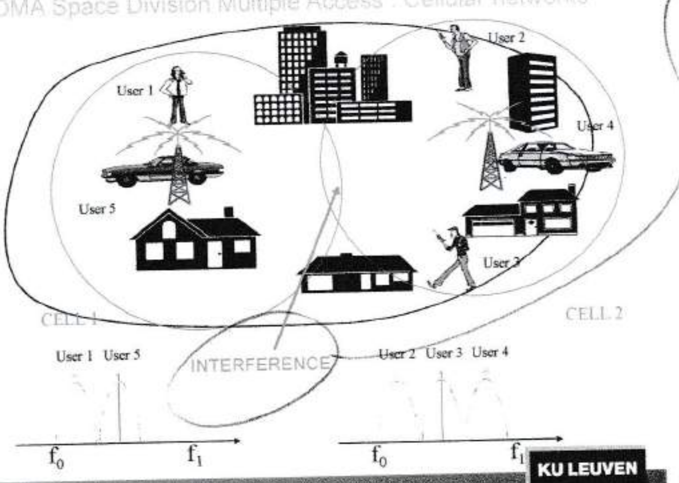
SDMA Space Division Multiple Access: Cellular networks



SDMA Space Division Multiple Access : Cellular networks



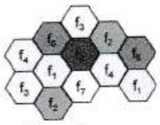
SDMA Space Division Multiple Access : Cellular networks



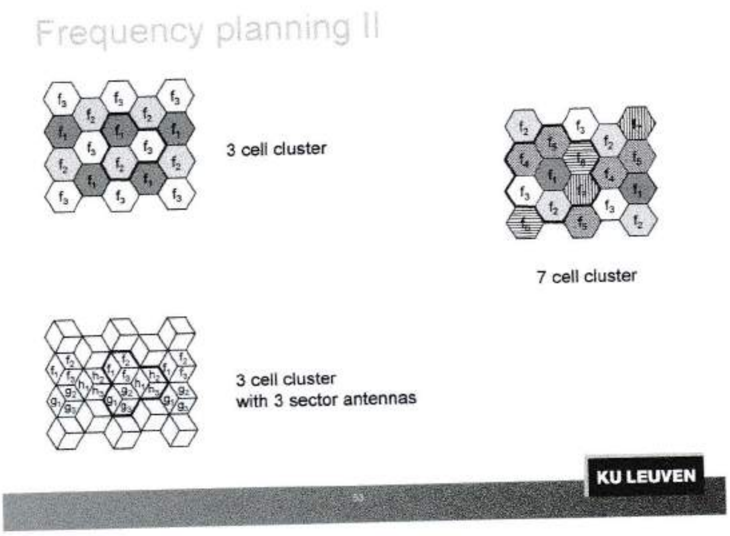
hoe oplossen

Frequency planning I

- Frequency reuse only with a certain distance between the base stations
- Standard model using 7 frequencies:



- Fixed frequency assignment:
  - certain frequencies are assigned to a certain cell
  - problem: different traffic load in different cells
  - used in GSM
- Dynamic frequency assignment:
  - base station chooses frequencies depending on the frequencies already used in neighbor cells
  - more capacity in cells with more traffic
  - assignment can also be based on interference measurements
  - used in DECT

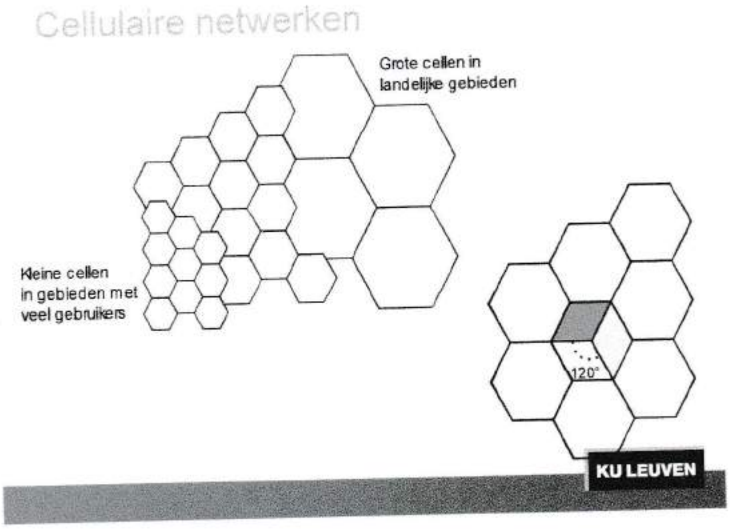


Frequency planning II

3 cell cluster

7 cell cluster

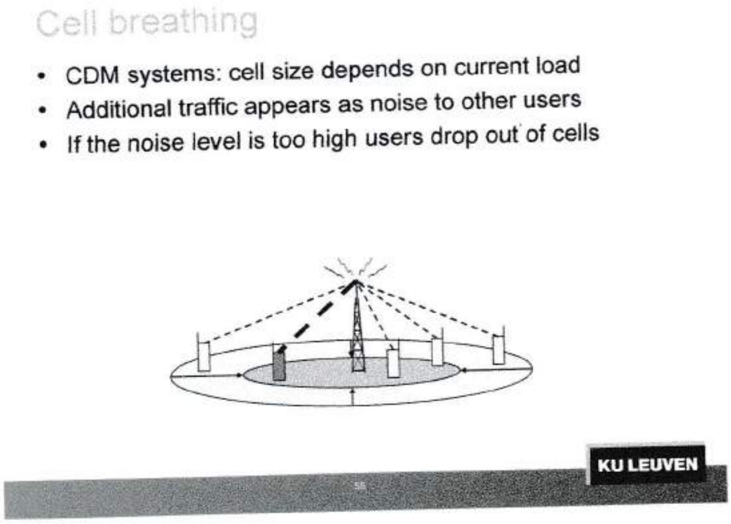
3 cell cluster
with 3 sector antennas



Cellulaire netwerken

Grote cellen in landelijke gebieden

Kleine cellen in gebieden met veel gebruikers



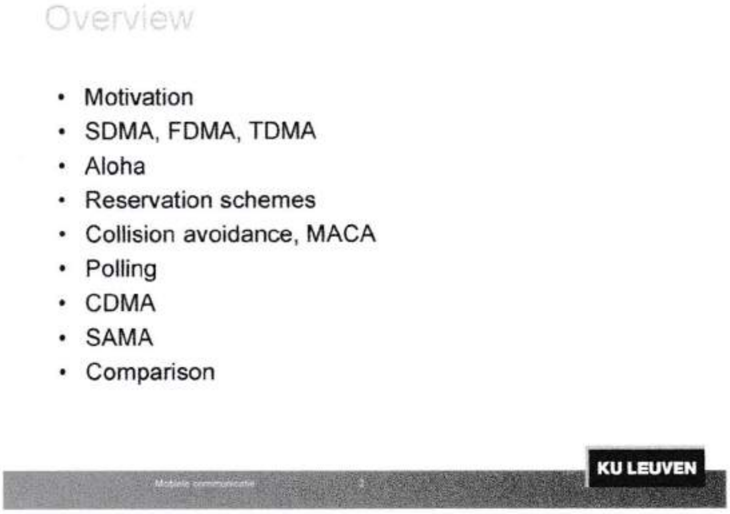
Cell breathing

- CDM systems: cell size depends on current load
- Additional traffic appears as noise to other users
- If the noise level is too high users drop out of cells

KU LEUVEN

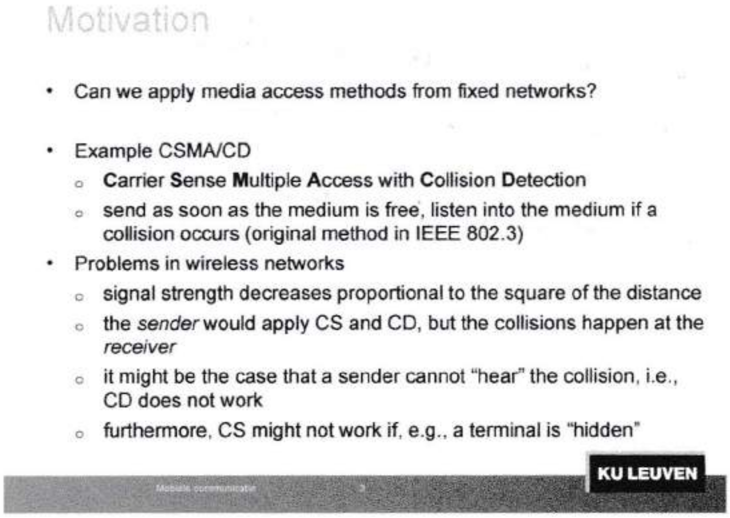
TECHNOLOGIECAMPUS GENT

Hoofdstuk 3 – Medium Access control



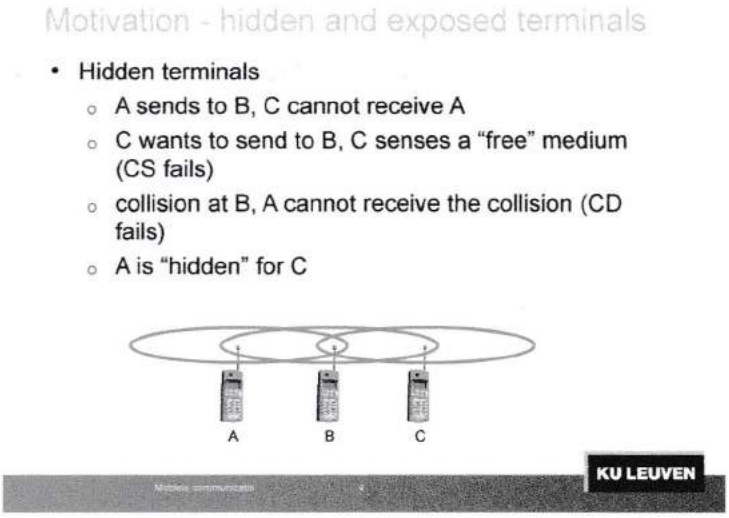
Overview

- Motivation
- SDMA, FDMA, TDMA
- Aloha
- Reservation schemes
- Collision avoidance, MACA
- Polling
- CDMA
- SAMA
- Comparison



Motivation

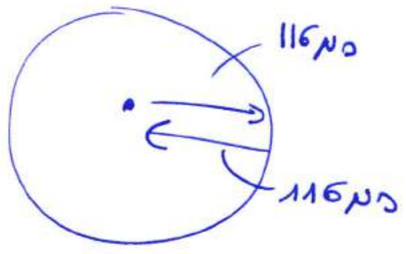
- Can we apply media access methods from fixed networks?
- Example CSMA/CD
  - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  - send as soon as the medium is free, listen into the medium if a collision occurs (original method in IEEE 802.3)
- Problems in wireless networks
  - signal strength decreases proportional to the square of the distance
  - the *sender* would apply CS and CD, but the collisions happen at the *receiver*
  - it might be the case that a sender cannot "hear" the collision, i.e., CD does not work
  - furthermore, CS might not work if, e.g., a terminal is "hidden"



Motivation - hidden and exposed terminals

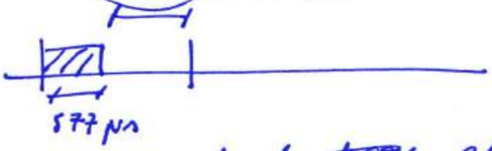
- Hidden terminals
  - A sends to B, C cannot receive A
  - C wants to send to B, C senses a "free" medium (CS fails)
  - collision at B, A cannot receive the collision (CD fails)
  - A is "hidden" for C

TDMA:



Opl: ① guard time

2x116 = 228μs



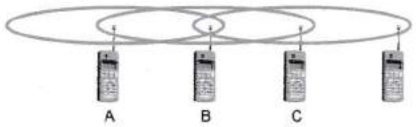
⇒ heel ~~hoge~~ lage efficientie

② vertraging meten → compenseren door gebruiker vroeger te laten zenden

↳ Timing advance

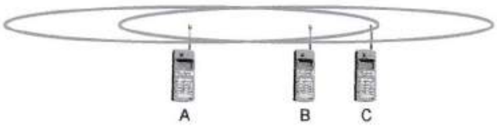
Motivation - hidden and exposed terminals

- Exposed terminals
  - B sends to A, C wants to send to another terminal (not A or B)
  - C has to wait, CS signals a medium in use
  - but A is outside the radio range of C, therefore waiting is not necessary
  - C is "exposed" to B



Motivation - near and far terminals

- Terminals A and B send (with equal strength), C receives
  - signal strength decreases proportional to the square of the distance
  - the signal of terminal B therefore drowns out A's signal
  - C cannot receive A



- If C for example was an arbiter for sending rights (i.e. C is basestation controlling medium access), terminal B would drown out terminal A already on the physical layer
- Also severe problem for CDMA-networks - precise power control needed!

Access methods SDMA/FDMA/TDMA

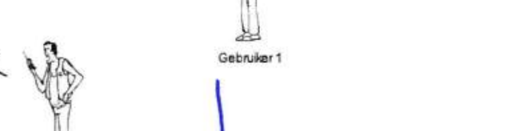
- SDMA (Space Division Multiple Access)
  - segment space into sectors, use directed antennas
  - cell structure (see also chapter 2)
- FDMA (Frequency Division Multiple Access)
  - assign a certain frequency to a transmission channel between a sender and a receiver
  - permanent (e.g., radio broadcast), slow hopping (e.g., GSM), fast hopping (FHSS, Frequency Hopping Spread Spectrum)
- TDMA (Time Division Multiple Access)
  - assign the fixed sending frequency to a transmission channel between a sender and a receiver for a certain amount of time
- The multiplexing schemes presented in chapter 2 are now used to control medium access!

≠ multiplexing 1 bron

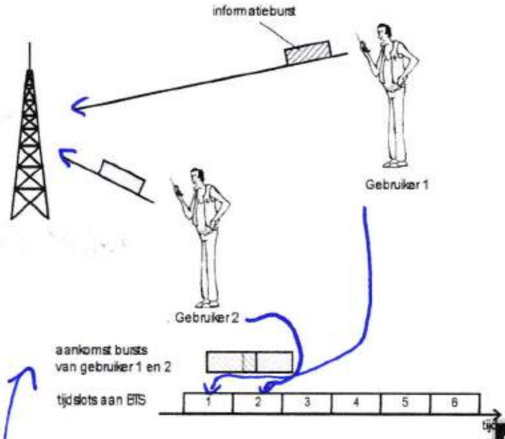
multiple Acces meerdere bronnen

max cel grootte : 35 km

$C = 3 \cdot 10^8 \frac{m}{s}$: 35 km → 116 µs



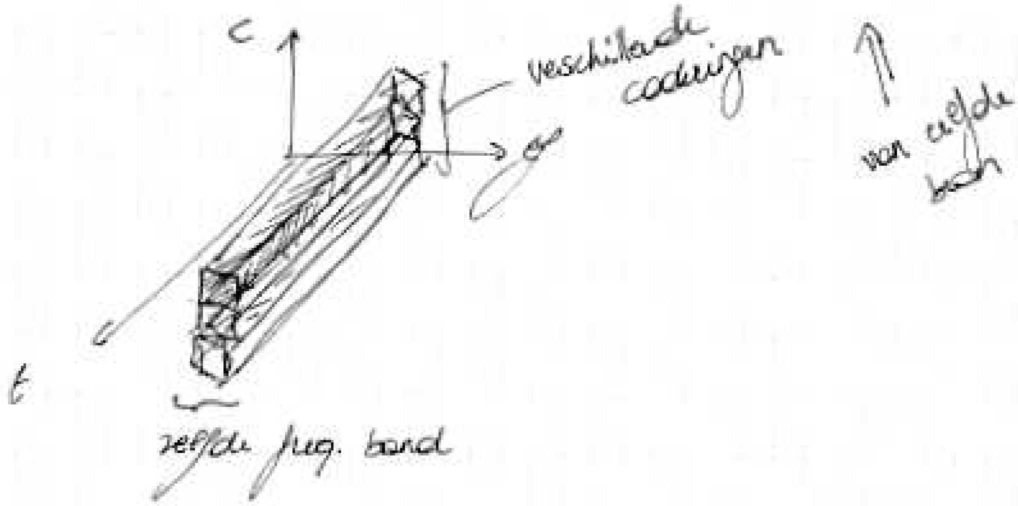
TDMA: timing advance



vertraging door ≠ afstand

CDM(A) en Spread Spectrum (SS)

H2: CDM : multiplexering met codes 2.5.4 ~~[illegible]~~



H3: CDM A : multiple access (3.5)

→ via spread spectrum (2.7) H2 slide 44

smallband signaal → breedband signaal tijdens transmissie → smallband sign. aan ontvanger.

(spreading despreading)

robuustheid

① smallband interferentie in 1 kanaal vermijden

② freq. selective fading verhelpen

fig 2.32 / 2.33 / 2.34 (slide 45) H2

SS implementatie : 1) freq. hopping (FHSS) GSM bluetooth. H2 (slide 41)

2) Direct sequence SS (DSSS) ⇒ codes

↳ in : WiFi (802.11) Barker codes enkel voor robuustheid

UMTS (3G) : multiple access + robuusth.

Access method CDMA

- CDMA (Code Division Multiple Access)
  - all terminals send on the same frequency probably at the same time and can use the whole bandwidth of the transmission channel
  - each sender has a unique random number, the sender XORs the signal with this random number
  - the receiver can "tune" into this signal if it knows the pseudo random number, tuning is done via a correlation function
- Disadvantages:
  - higher complexity of a receiver (receiver cannot just listen into the medium and start receiving if there is a signal)
  - all signals should have the same strength at a receiver
- Advantages:
  - all terminals can use the same frequency, no planning needed
  - huge code space (e.g. 2^{32}) compared to frequency space
  - interferences (e.g. white noise) is not coded
  - forward error correction and encryption can be easily integrated

KU LEUVEN

CDMA in theory

- Sender A
  - sends $A_d = 1$, key $A_k = 010011$ (assign: „0"= -1, „1"= +1)
  - sending signal $A_s = A_d * A_k = (-1, +1, -1, -1, +1, +1)$
- Sender B
  - sends $B_d = 0$, key $B_k = 110101$ (assign: „0"= -1, „1"= +1)
  - sending signal $B_s = B_d * B_k = (-1, -1, +1, -1, +1, -1)$
- Both signals superimpose in space
  - interference neglected (noise etc.)
  - $A_s + B_s = (-2, 0, 0, -2, +2, 0)$
- Receiver wants to receive signal from sender A
  - apply key A_k bitwise (inner product)
    - $A_e = (-2, 0, 0, -2, +2, 0) \bullet A_k = 2 + 0 + 0 + 2 + 2 + 0 = 6$
    - result greater than 0, therefore, original bit was „1"
  - receiving B
    - $B_e = (-2, 0, 0, -2, +2, 0) \bullet B_k = -2 + 0 + 0 - 2 - 2 + 0 = -6$, i.e. „0"

KU LEUVEN

CDMA in theory

- Codes of A en B are orthogonal

  $A_k = 010011 = (-1, +1, -1, -1, +1, +1)$

  $B_k = 110101 = (+1, +1, -1, +1, -1, +1)$

  $A_k \bullet B_k = -1 +1 +1 -1 -1 +1 = 0$

  (same as vectors in an three dimensional space)

good codes have low cross correlation -> guard space

KU LEUVEN

CDMA in theory

- The example has several simplifying assumptions
  - codes are simple and orthogonal
  - length of code is equal to the length of one databit
  - no noise involved
  - bits are precisely superimposed (synchronisation)
  - both signals have same strength:

    assume that signal from B is 5 times stronger than signal from A

    $C = A_s + 5 * B_s = (-6, -4, +4, -1, +6, +4)$

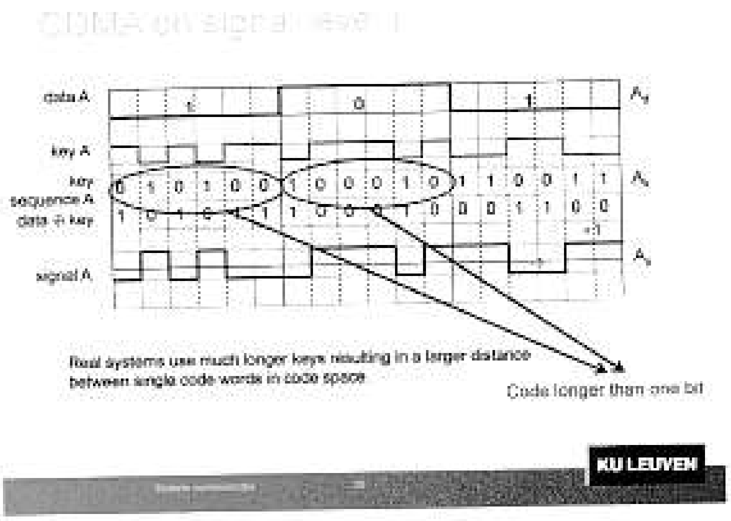
    $C \bullet B_k = -30$

    $C \bullet A_k = 6$

    with noise -> may be problem to detect A

KU LEUVEN

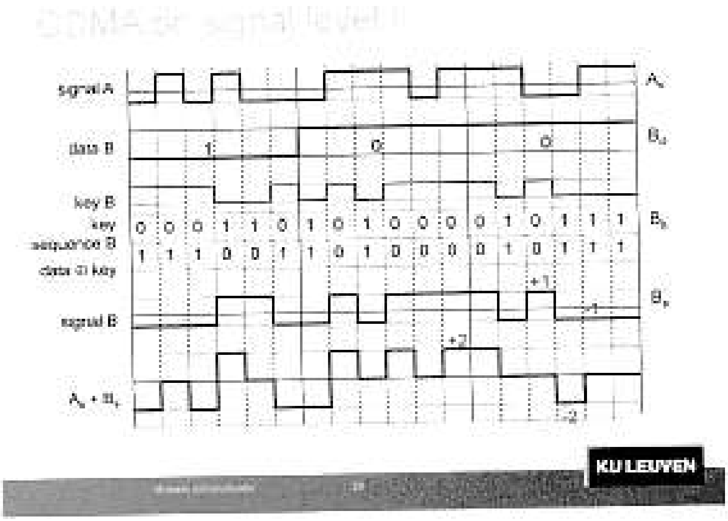
CDMA on signal level I



Real systems use much longer keys resulting in a larger distance between single code words in code space

Code longer than one bit

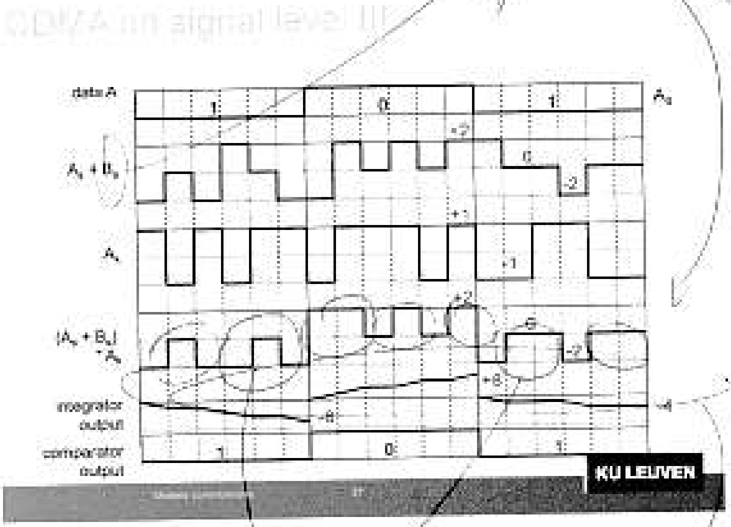
CDMA on signal level II



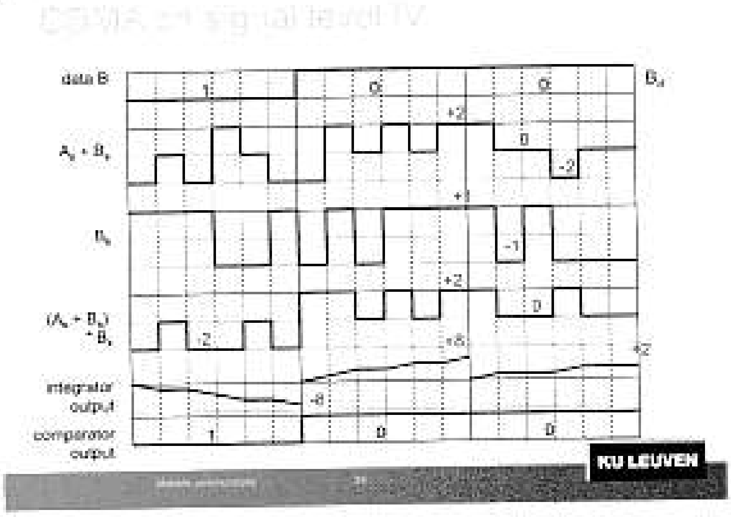
zien als 3B-punt.

weggefilterd door
↳ klein uitkomst
als #chip ↑ → uitkomst ↑

CDMA on signal level III



CDMA on signal level IV

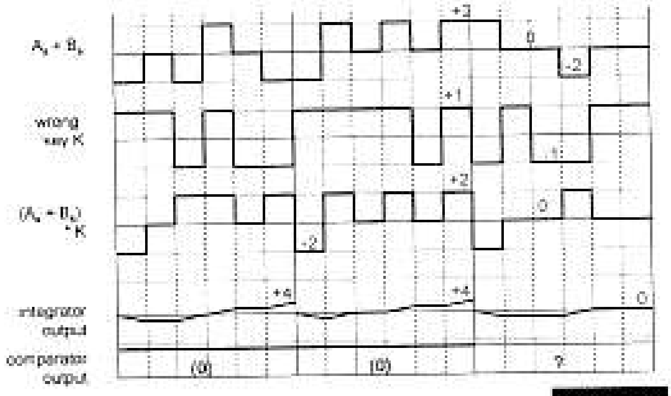


verwacht
+/-C
~~[illegible]~~

midden v
0

⇒ dus quasi-orth.
ipv. orth.

CDMA on signal level V



Synchronisation

(see book § 2.7.1)

- Good codes also have a good autocorrelation:

  example 11 bit Barker code (used in ISDN and IEEE 802.11 WLAN)

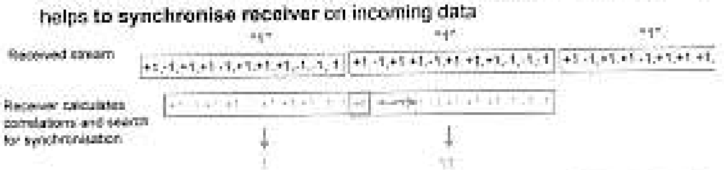
  A_k = (+1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1)

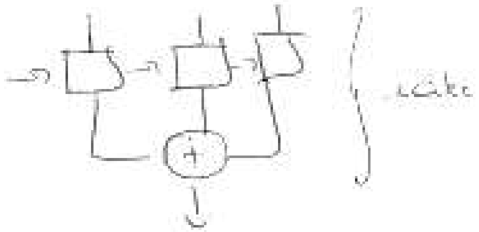
  $A_k \cdot A_k$ = 11

  if A_k is shifted one chip the correlation drops to -1

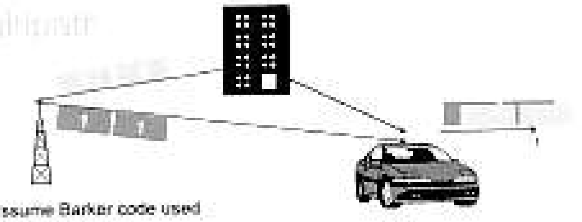
  (+1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1) • (-1, +1,-1,+1,+1,-1,+1,+1,+1,-1,-1) = -1

  helps to synchronise receiver on incoming data



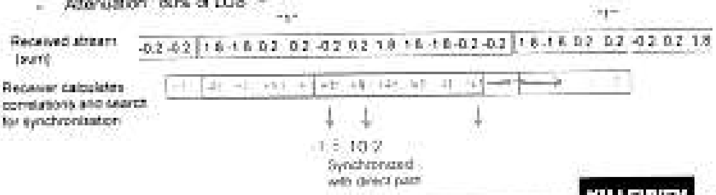


Multipath

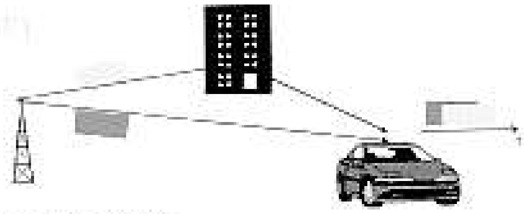


- Assume Barker code used
- Reflected signal
  - Delay equals exactly 4 chip periods
  - Attenuation : 80% of LOS

20% kwijt



Multipath



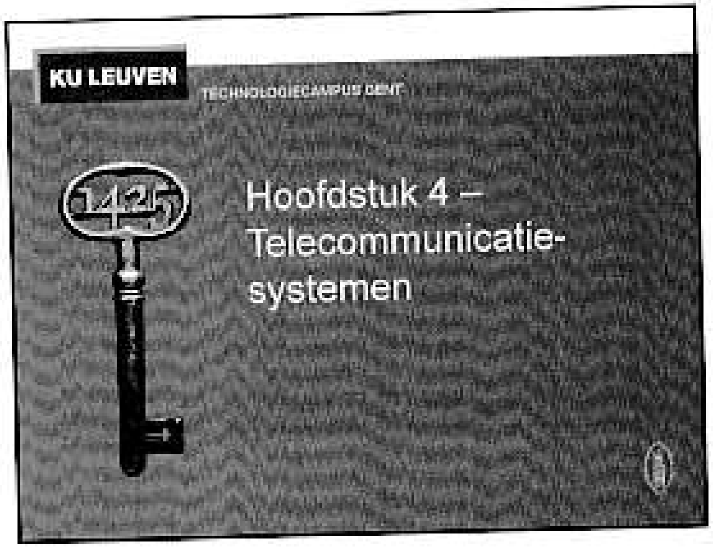
- Two synchronization timings
  - Use one correlator for each
  - Combine the results

  => Stronger signal (more robust)

This is called a **Rake receiver**, the correlators are fingers of the rake

More correlators are possible

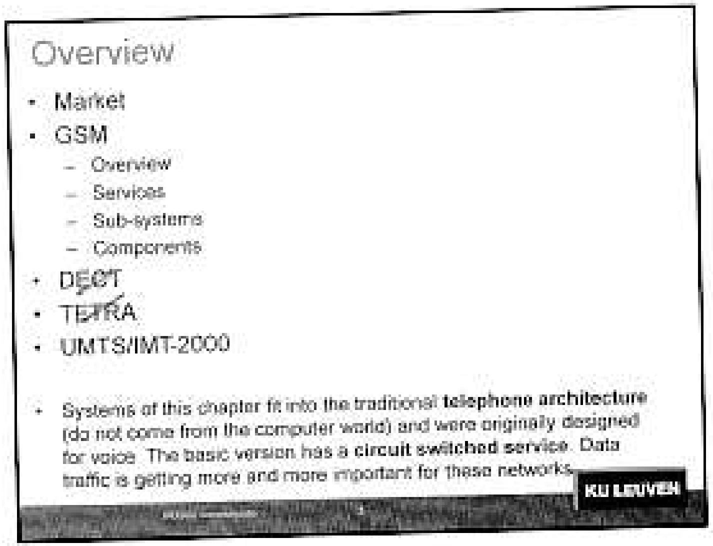
Used in UMTS (3G) to 'exploit' the multipath (with other codes than Barker codes)



KU LEUVEN

TECHNOLOGIECAMPUS GENT

Hoofdstuk 4 – Telecommunicatiesystemen

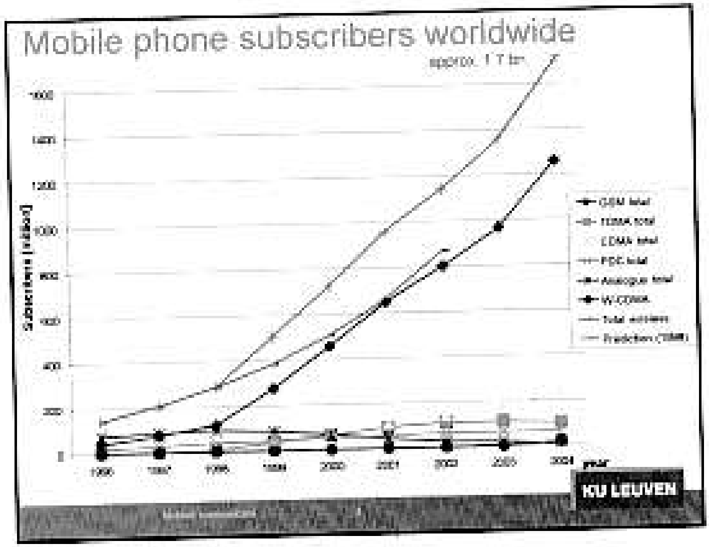


Overview

- Market
- GSM
  - Overview
  - Services
  - Sub-systems
  - Components
- DECT
- TETRA
- UMTS/IMT-2000

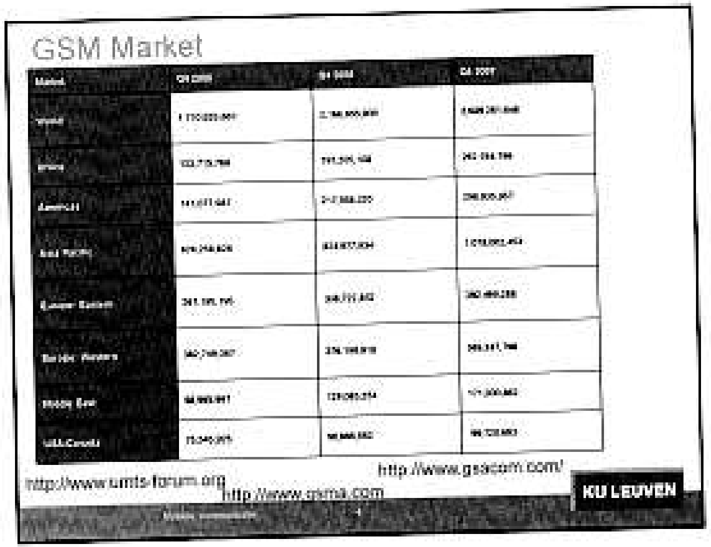
- Systems of this chapter fit into the traditional **telephone architecture** (do not come from the computer world) and were originally designed for voice. The basic version has a **circuit switched service**. Data traffic is getting more and more important for these networks.

KU LEUVEN



Mobile phone subscribers worldwide

KU LEUVEN



GSM Market

Market	[illegible]	[illegible]	[illegible]
World	[illegible]	[illegible]	[illegible]
Africa	[illegible]	[illegible]	[illegible]
Americas	[illegible]	[illegible]	[illegible]
Asia Pacific	[illegible]	[illegible]	[illegible]
Europe: Eastern	[illegible]	[illegible]	[illegible]
Europe: Western	[illegible]	[illegible]	[illegible]
Middle East	[illegible]	[illegible]	[illegible]
USA/Canada	[illegible]	[illegible]	[illegible]

http://www.gsacom.com/

http://www.umts-forum.org

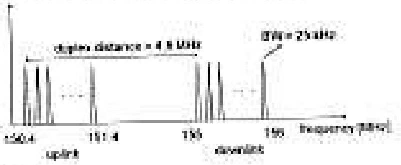
http://www.gsma.com

KU LEUVEN

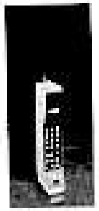
mobiel → vast

Analogue cellular systems in Belgium 1G

- MOB-1:
  - uplink : 150.4 - 151.4 MHz
  - downlink : 155 - 156 MHz
  - duplex distance : 4.6 MHz
  - number of duplex channels : 40
  - bandwidth of a channel : 25 kHz



- MOB-2: NMT-450
  - uplink : 451.3 - 455.74 MHz
  - downlink : 461.3 - 465.74 MHz
  - duplex distance : 10 MHz
  - number of duplex channels : 222
  - bandwidth of a channel : 20 kHz



KU LEUVEN

Architecture of the GSM system

- GSM is a PLMN (Public Land Mobile Network)
  - several providers setup mobile networks following the GSM standard within each country
  - subsystems
    - RSS (radio subsystem): covers all radio aspects
    - NSS (network and switching subsystem): call forwarding, handover, switching, billing, mobility management
    - OSS (operation subsystem): management of the network

KU LEUVEN

beveiliging
netwerk
parameters
(bv: problemen
controle &
management

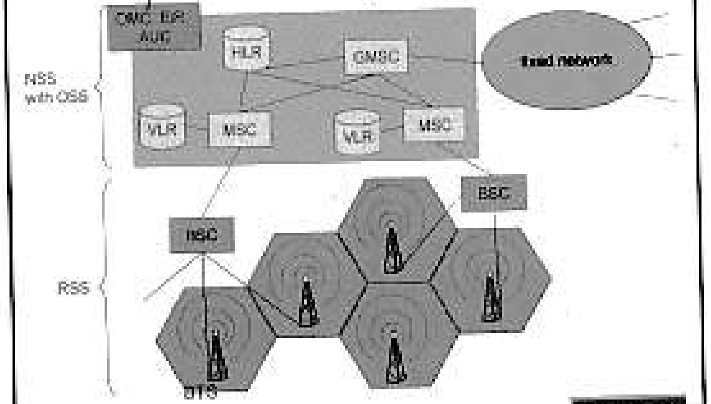
backbone

GSM: Overview

- GSM
  - formerly: Groupe Spéciale Mobile (founded 1982)
  - now: Global System for Mobile Communication
  - Pan-European standard (ETSI, European Telecommunications Standardisation Institute)
  - simultaneous introduction of essential services in three phases (1991, 1994, 1996) by the European telecommunication administrations → seamless roaming within Europe possible
  - *today many providers all over the world use GSM (more than 200 countries in Asia, Africa, Europe, Australia, America)*
  - *more than 1.2 billion subscribers in more than 630 networks*
  - *more than 75% of all digital mobile phones use GSM*
  - *over 200 million SMS per month in Germany, > 550 billion/year worldwide (> 10% of the revenues for many operators)*
    [be aware: these are only rough numbers…]
  - GSM 900, DCS 1800, PCS 1900 (GSM 400) and GSM Rail

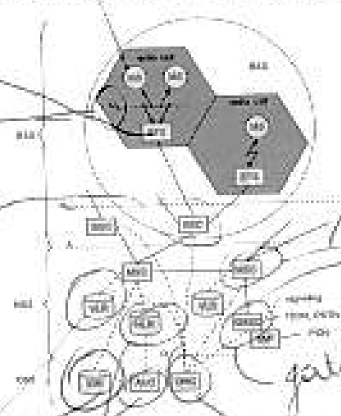
KU LEUVEN

GSM: overview



KU LEUVEN

GSM: elements and interfaces



Base transceiver station

mobile stations

binnen netwerk

Um interface

mobile switching centrale

ook extern schakelen ↓ vb. ISDN netwerk

gateway

Base station controller ↓ beheren # cellen

home location register

operation & maintenance center

visitor location register

Auth. center → [illegible] de lijn kan gemaakt

Radio subsystem

- The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers
- Components
  - Base Station Subsystem (BSS):
    - Base Transceiver Station (BTS): radio components including sender receiver, amplifiers, signal processing, antenna - if directed antennas are used one BTS can cover several cells
    - Base Station Controller (BSC): management of BTSs, handover between BTSs, controlling BTSs, managing of network resources (allocation of frequencies), paging of MSs, mapping of radio channels (U_m) onto terrestrial channels (A interface)
    - BSS = BSC + sum(BTS) + interconnection
  - Mobile Stations (MS)

mobility station → paging signaal sturen

bepaalt welke freq in welke cel

schakelen in real-time naar andere BTS

multiplexen + [illegible] - [illegible] signaal

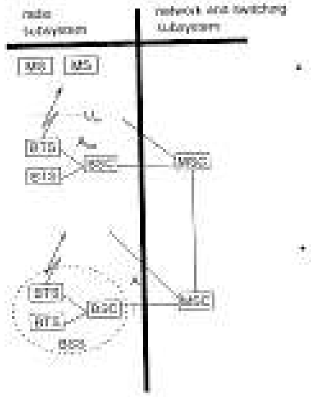
bv. allocatie v. freq

→ centrale DB

equipment identity register ↳ info over telefoon.

- blokeren controleren
- gestolen controleren ← voornamelijk registreren

System architecture: radio subsystem

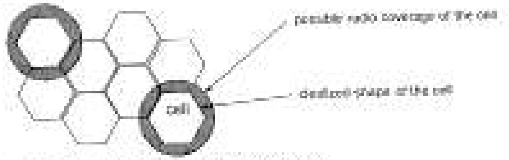


- Components
  - MS (Mobile Station)
  - BSS (Base Station Subsystem) consisting of
    - BTS (Base Transceiver Station) sender and receiver
    - BSC (Base Station Controller) controlling several transceivers
- Interfaces
  - U_m radio interface
  - A_{bis} standardized, open interface with 16 kbit/s user channels
  - A standardized, open interface with 64 kbit/s user channels

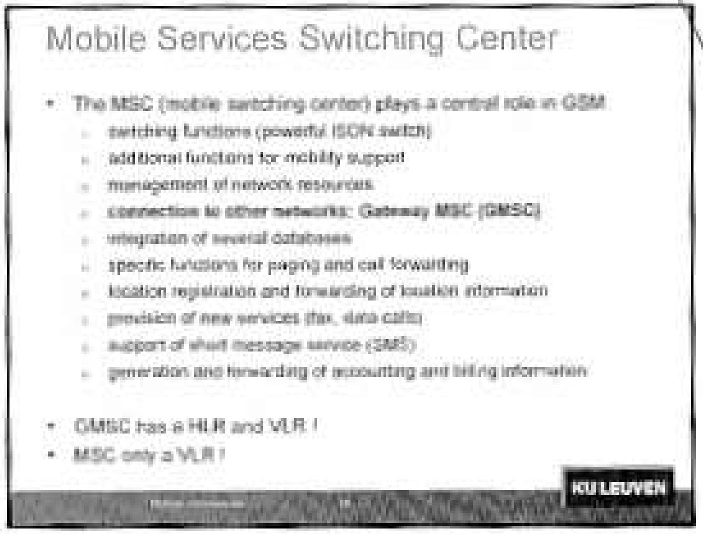
→ niet bestuderen.

GSM: cellular network

segmentation of the area into cells


possible radio coverage of the cell
idealized shape of the cell
cell

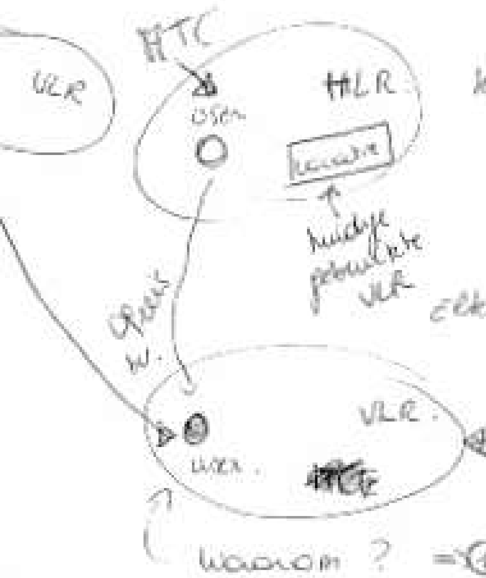
- use of several carrier frequencies
- not the same frequency in adjoining cells
- cell sizes vary from some 100 m up to 35 km depending on user density, geography, transceiver power etc.
- hexagonal shape of cells is idealized (cells overlap, shapes depend on geography)
- if a mobile user changes cells
  ➔ handover of the connection to the neighbor cell



Mobile Services Switching Center

- The MSC (mobile switching center) plays a central role in GSM
  - switching functions (powerful ISDN switch)
  - additional functions for mobility support
  - management of network resources
  - **connection to other networks: Gateway MSC (GMSC)**
  - integration of several databases
  - specific functions for paging and call forwarding
  - location registration and forwarding of location information
  - provision of new services (fax, data calls)
  - support of short message service (SMS)
  - generation and forwarding of accounting and billing information
- GMSC has a HLR and VLR !
- MSC only a VLR !

KU LEUVEN



kent informatie
- waarvoor betaald
- locatie
- ID ...

elke operator → 1 HLR ⟺

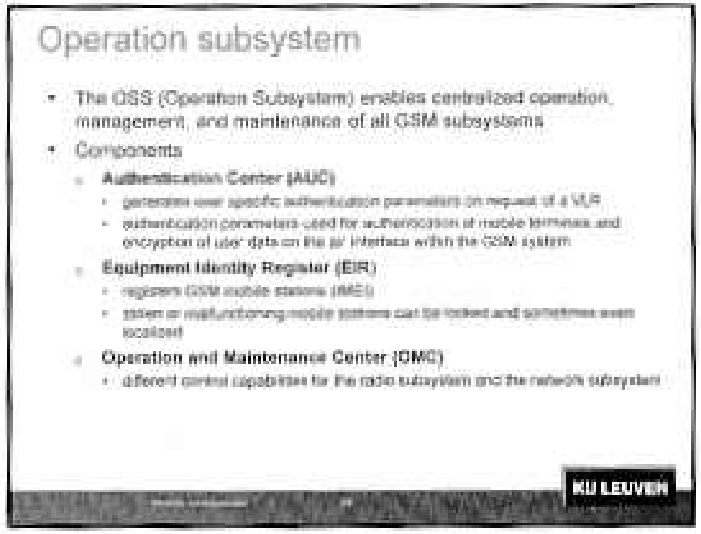
← MOC

Waarom ? = ① Data nodig by operator
- auth.
- encry.
- betaald ?

2 niet constant internationale connectie.

② MTC - mobile terminated call
↳ staan in HLR ISDN-nummer
⇒ adh prefix gsm-nummer.

MOC - mobile originating call.



Operation subsystem

- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems
- Components
  - **Authentication Center (AUC)**
    - generates user specific authentication parameters on request of a VLR
    - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
  - **Equipment Identity Register (EIR)**
    - registers GSM mobile stations (IMEI)
    - stolen or malfunctioning mobile stations can be locked and sometimes even localized
  - **Operation and Maintenance Center (OMC)**
    - different control capabilities for the radio subsystem and the network subsystem

KU LEUVEN

(27) GSM - TDMA/FDMA

(a) korte slots ⇒ beter want lange slots → grote delay.

space pauses → – nodig bij timing advance
– HW traagheid, vb. versterker

(29) Down ↔ uplink. 3 tijdsslots verschil.
reden (a) geen full-duplex nodig
(b) tijd nodig voor freq. hopping.

(30) Assoc. CC. ⇒ enkel op moment v. traffic channel.
↳ slow → altijd: kwaliteit v. link.
↳ fast → vb. handover → welk kanaal
→ welk tijdslot
→ ...

⇒ snel afhandelen
↳ stealing flags → user info
→ ipv v. user bits
← FACC

Stand. alone Ded. CC
⇒ connectie kunnen maken met netwerk, niet bellen

down link
(31) FCCH c ongemod. sinus ⇒ bijstellen klok

tijdsas → SCH Synch. van tijdsslots

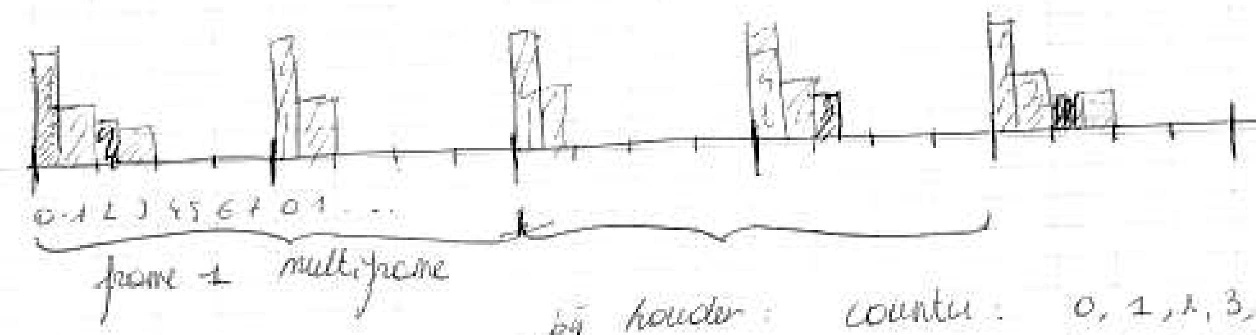
netwerk → BCCH vb. naburige cellen?

uplink RACH lege tijdsslots ⇒ random kiezen,
ik wil call opzetten, ⇒ slotted Aloha

down PAGCH – antw v. RACH access grant
– paging als u opgeroepen

SCH in BTS

management



bij houder : counter : 0, 1, 2, 3, ... ⇐ welke slots

counter : 0 ⇐ welke frame

▨ 12 kbps

▨ ▨ 6 kbps

▩ 4 kbps

□ 3 kbps

hoeveel moet versturen.

Multiplexen v. THC / SACC (53)

1 key tijdslot → data te lezen vd downlink info zeker zijn kan, alle sectoren te kunnen lezen.

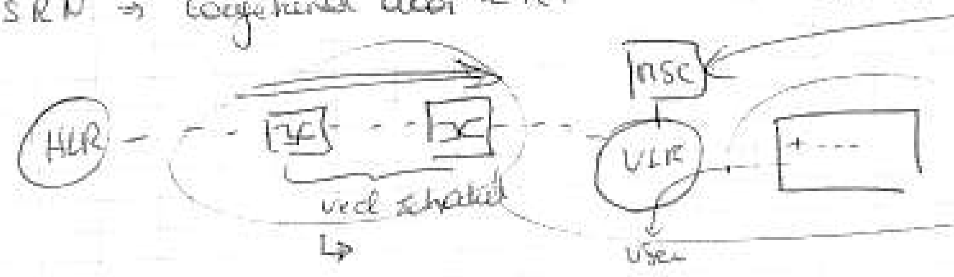
26 ⇔ 51 over elkaar schuiven.

(36) intern nummer : IMSI

MCC MNC MSIN
land Operator user

} → temp TMSI
⇔ IMSI nt laten weten a.d. lucht.
⇒ privacy
→ nt localiseren adhv. IMSI

MSRN → toegekend door VLR.

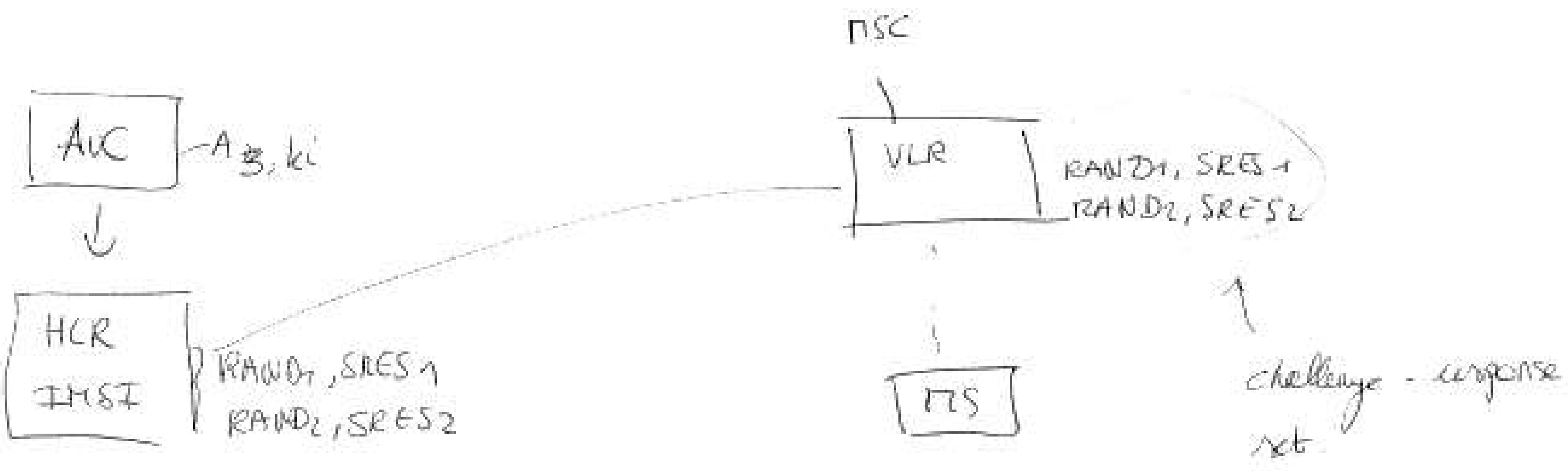


weten naar welke MSC moet.

toekenning v. ~~...~~ v. MSISDN

MSRN zorgen schakelen v. circuit
weten moet naar spanje-

Security



(A5) tijdsinfo + Kc → seq xor data

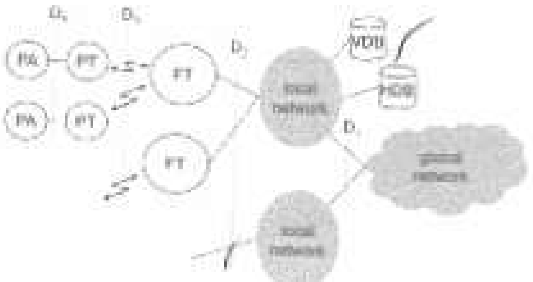
↗ mogelijk door tijdsslots.

DECT

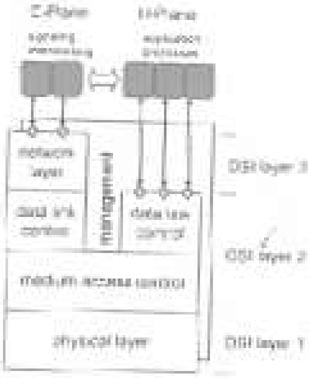
later
→ enhanced.

- DECT (Digital European Cordless Telephone) standardized by ETSI (ETS 300 175-x) for cordless telephones
- standard describes air interface between base-station and mobile phone
- DECT has been renamed for international marketing reasons into „Digital Enhanced Cordless Telecommunication"
- Characteristics
  - frequency: 1880-1900 MHz
  - channels: 120 full duplex
  - duplex mechanism: TDD (Time Division Duplex) with 10 ms frame length
  - multiplexing scheme: FDMA with 10 carrier frequencies, TDMA with 2x 12 slots
  - modulation: digital, Gaußian Minimum Shift Key (GMSK)
  - power: 10 mW average (max. 250 mW)
  - range: approx. 50 m in buildings, 300 m open space

DECT system architecture reference model



DECT reference model

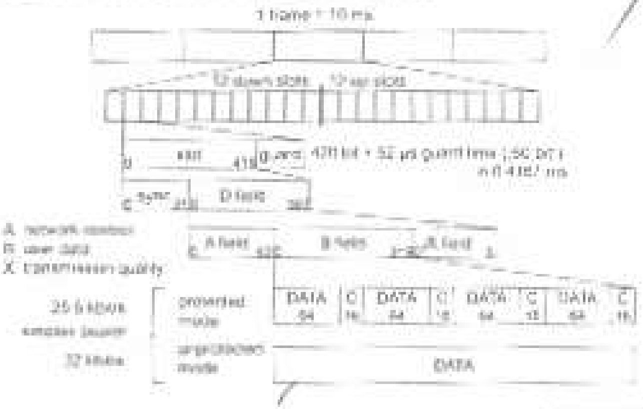


- close to the OSI reference model
- management plane over all layers
- several services in C(ontrol)- and U(ser)-plane

DECT layers I

- Physical layer
  - modulation/demodulation
  - generation of the physical channel structure with a guaranteed throughput
  - controlling of radio transmission
    - channel assignment on request of the MAC layer
    - detection of incoming signals
    - sender/receiver synchronization
    - collecting status information for the management plane
- MAC layer
  - maintaining basic services, activating/deactivating physical channels
  - multiplexing of logical channels
    - e.g., C: signaling, I: user data, P: paging, Q: broadcast
  - segmentation/reassembly
  - error control/error correction

DECT time multiplex frame



DECT layers II

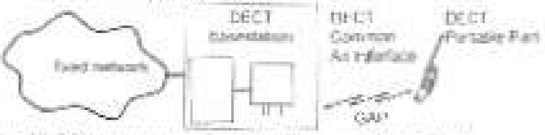
- Data link control layer
  - creation and keeping up reliable connections between the mobile terminal and basestation
  - two DLC protocols for the control plane (C-Plane)
    - connectionless broadcast service:
      paging functionality
    - Lc+LAPC protocol:
      in-call signaling (similar to LAPD within ISDN), adapted to the underlying MAC service
  - several services specified for the user plane (U-Plane)
    - null-service: offers unmodified MAC services
    - frame relay: simple packet transmission
    - frame switching: time-bounded packet transmission
    - error correcting transmission: uses FEC, for delay critical, time-bounded services
    - bandwidth adaptive transmission
    - „Escape" service: for further enhancements of the standard

DECT layers III

- Network layer
  - similar to ISDN (Q.931) and GSM (04.08)
  - offers services to request, check, reserve, control, and release resources at the basestation and mobile terminal
  - resources
    - necessary for a wireless connection
    - necessary for the connection of the DECT system to the fixed network
  - main tasks
    - call control: setup, release, negotiation, control
    - call independent services: call forwarding, accounting, call redirecting
    - mobility management: identity management, authentication, management of the location register

Enhancements of the standard

- Several „DECT Application Profiles" in addition to the DECT specification
  - GAP (Generic Access Profile) standardized by ETSI in 1997
    - assures interoperability between DECT equipment of different manufacturers (minimal requirements for voice communication)
    - enhanced management capabilities through the fixed network: Cordless Terminal Mobility (CTM)



  - DECT/GSM Interworking Profile (GIP): connection to GSM
  - ISDN Interworking Profiles (IAP, IIP): connection to ISDN
  - Radio Local Loop Access Profile (RAP): public telephone service
  - CTM Access Profile (CAP): support for user mobility

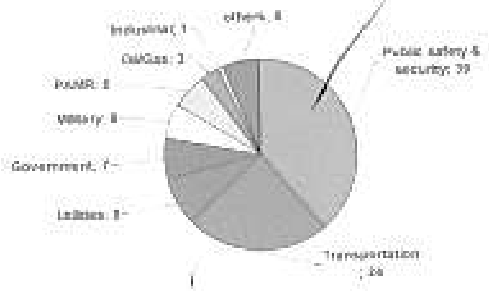
TETRA - Terrestrial Trunked Radio

- Trunked radio systems
  - many different radio carriers
  - assign single carrier for a short period to one user/group of users
  - taxi service, fleet management, rescue teams
  - interfaces to public networks, voice and data services
  - very reliable, fast call setup, local operation
- TETRA - ETSI standard
  - formerly: Trans European Trunked Radio
  - point-to-point and point-to-multipoint
  - encryption (end-to-end, air interface), authentication of devices, users and networks
  - group call, broadcast, sub-second group-call setup
  - ad-hoc ("direct mode"), relay and infrastructure networks
  - call queuing with pre-emptive priorities

KU LEUVEN

TETRA – Contracts by Sector (percentage)

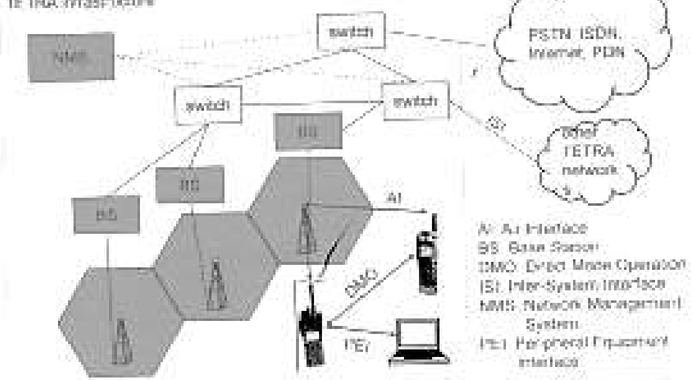
Used in over 70 countries, more than 20 device manufacturers



KU LEUVEN

TETRA – Network Architecture

TETRA infrastructure

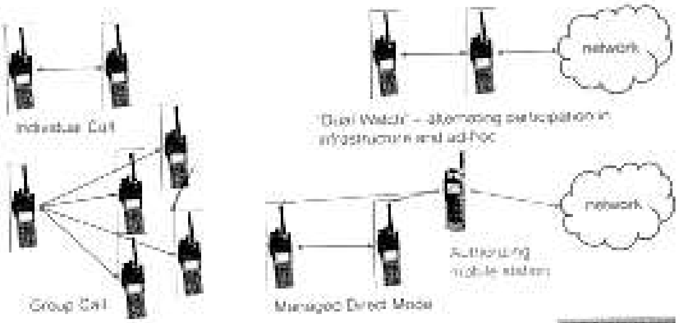


NMS
switch
switch
switch
BS
BS
BS
PSTN, ISDN, Internet, PDN
ISI
other TETRA network
AI
DMO
PEI
AI: Air Interface
BS: Base Station
DMO: Direct Mode Operation
ISI: Inter-System Interface
NMS: Network Management System
PEI: Peripheral Equipment Interface

KU LEUVEN

TETRA – Direct Mode I

- Direct Mode enables ad-hoc operation and is one of the most important differences to pure infrastructure-based networks such as GSM, cdma2000 or UMTS.

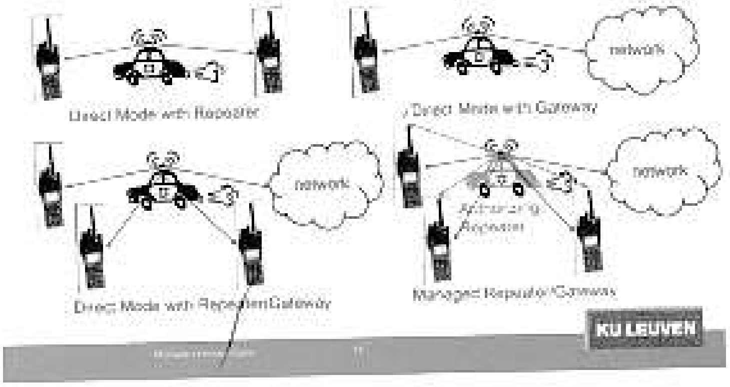


Individual Call
Group Call
network
"Dual Watch" – alternating participation in infrastructure and ad-hoc
network
Authorizing mobile station
Managed Direct Mode

KU LEUVEN

TETRA – Direct Mode II

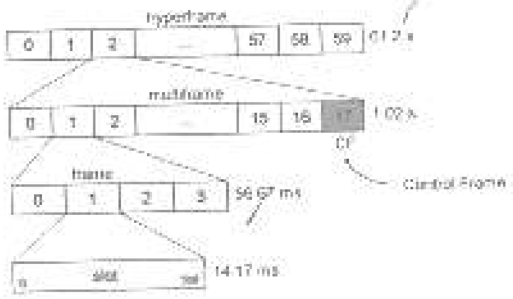
- An additional repeater may increase the transmission range (e.g. police car)



TETRA – Technology

- Services
  - Voice+Data (V+D) and Packet Data Optimized (PDO)
  - Short data service (SDS)
- Frequencies
  - Duplex: FDD, Modulation: DQPSK
  - Europe (in MHz, not all available yet)
    - 380-390 UL / 390-400 DL; 410-420 UL / 420-430 DL; 450-460 UL / 460-470 DL; 870-876 UL / 915-921 DL
  - Other countries
    - 380-390 UL / 390-400 DL; 410-420 UL / 420-430 DL; 806-821 UL / 851-866 DL

TDMA structure of the voice+data system



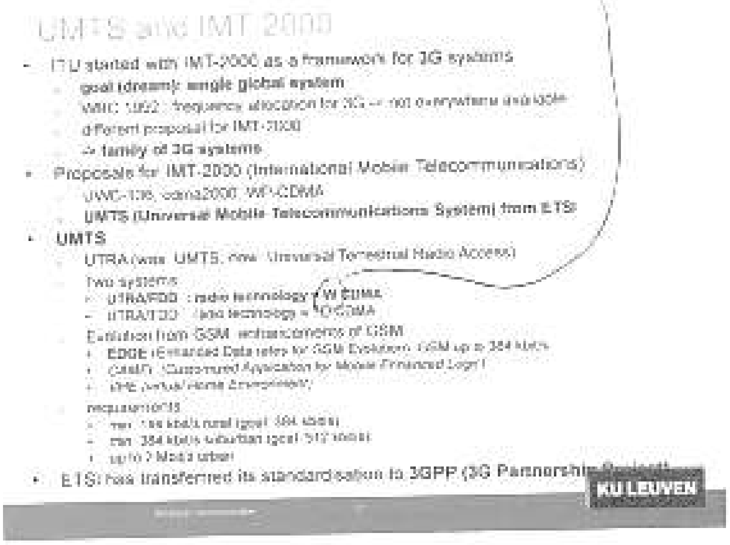
TETRA – Data Rates

- Infrastructure mode, V+D in kbit/s

No. of time slots	1	2	3	4
No protection	7.2	14.4	21.6	28.8
Low protection	4.8	9.6	14.4	19.2
High protection	2.4	4.8	7.2	9.6

- TETRA Release 2 – Supporting higher data rates
  - TEDS (TETRA Enhanced Data Service)
  - up to 100 kbit/s
  - backward compatibility

wideband

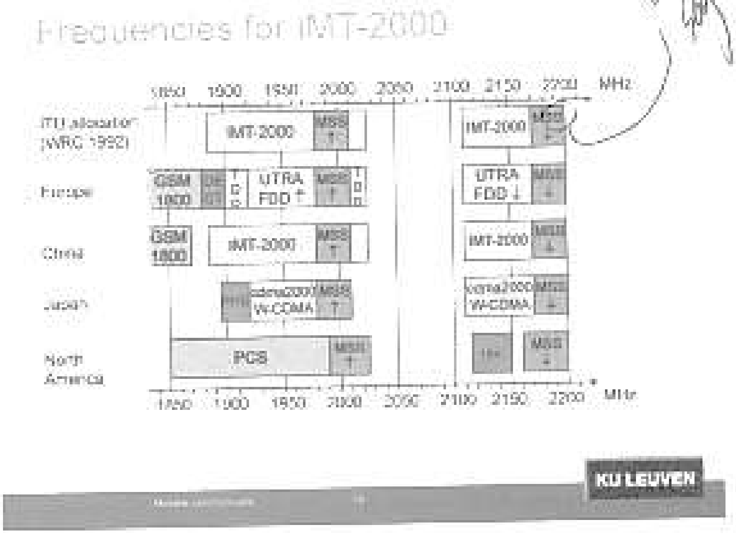


UMTS and IMT 2000

- ITU started with IMT-2000 as a framework for 3G systems
  - **goal (dream): single global system**
  - WRC 1992: frequency allocation for 3G -> not everywhere available
  - different proposal for IMT-2000
  - **-> family of 3G systems**
- Proposals for IMT-2000 (International Mobile Telecommunications)
  - UWC-136, cdma2000, WP-CDMA
  - **UMTS (Universal Mobile Telecommunications System) from ETSI**
- **UMTS**
  - UTRA (was: UMTS, now: Universal Terrestrial Radio Access)
  - Two systems
    - **UTRA/FDD** : radio technology = W-CDMA
    - UTRA/TDD : radio technology = TD-CDMA
  - Evolution from GSM, enhancements of GSM
    - **EDGE** (Enhanced Data rates for GSM Evolution: GSM up to 384 kbit/s
    - CAMEL (Customized Application for Mobile Enhanced Logic)
    - VHE (virtual Home Environment)
  - requirements
    - min. 144 kbit/s rural (goal: 384 kbit/s)
    - min. 384 kbit/s suburban (goal: 512 kbit/s)
    - up to 2 Mbit/s urban
- ETSI has transferred its standardisation to 3GPP (3G Partnership Project)

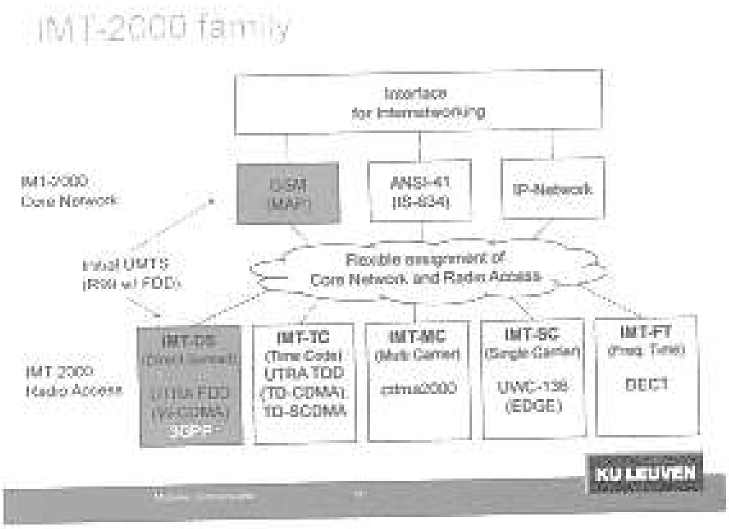
KU LEUVEN

Satellite segment



Frequencies for IMT-2000

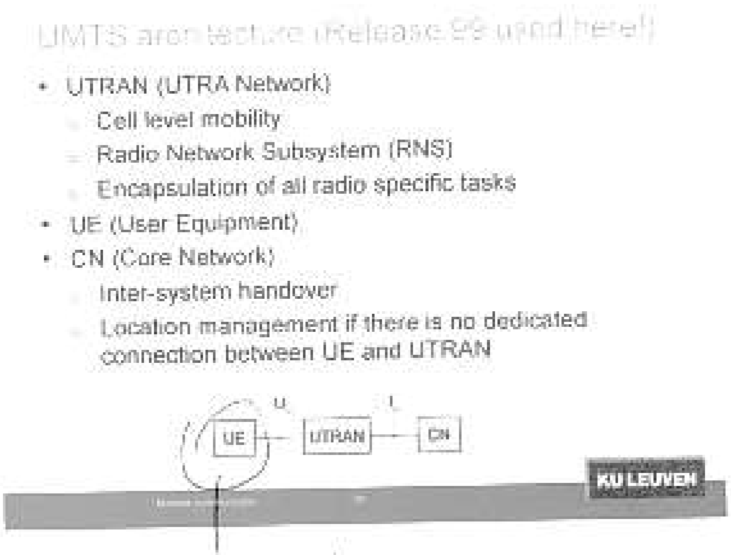
KU LEUVEN



IMT-2000 family

Interface for Internetworking
IMT-2000 Core Network
GSM (MAP)
ANSI-41 (IS-634)
IP-Network
Initial UMTS (R99 w/ FDD)
Flexible assignment of Core Network and Radio Access
IMT-2000 Radio Access
IMT-DS (Direct Spread) UTRA FDD (W-CDMA) 3GPP
IMT-TC (Time Code) UTRA TDD (TD-CDMA); TD-SCDMA
IMT-MC (Multi Carrier) cdma2000
IMT-SC (Single Carrier) UWC-136 (EDGE)
IMT-FT (Freq. Time) DECT

KU LEUVEN



UMTS architecture (Release 99 used here!)

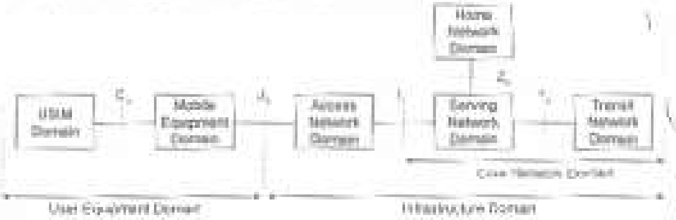
- UTRAN (UTRA Network)
  - Cell level mobility
  - Radio Network Subsystem (RNS)
  - Encapsulation of all radio specific tasks
- UE (User Equipment)
- CN (Core Network)
  - Inter-system handover
  - Location management if there is no dedicated connection between UE and UTRAN

Uu
Iu
UE
UTRAN
CN

KU LEUVEN

equivalent
aan MS.

UMTS domains and interfaces I



- User Equipment Domain
  - Assigned to a single user in order to access UMTS services
- Infrastructure Domain
  - Shared among all users
  - Offers UMTS services to all accepted users

KU LEUVEN

UMTS domains and interfaces II

- Universal Subscriber Identity Module (USIM)
  - Functions for encryption and authentication of users
  - Located on a SIM inserted into a mobile device
- Mobile Equipment Domain
  - Functions for radio transmission
  - User interface for establishing/maintaining end-to-end connections
- Access Network Domain
  - Access network dependent functions
- Core Network Domain
  - Access network independent functions
  - Serving Network Domain
    - Network currently responsible for communication
  - Home Network Domain
    - Location and access network independent functions

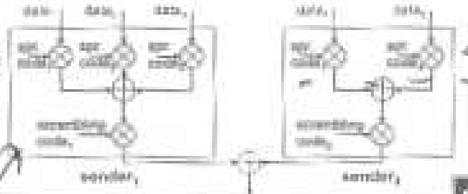
KU LEUVEN

← CDMA ipv. time slots & freq banden in 2G

na modulatie → B: 5MHz
↕
200kHz
2G

Spreading and scrambling of user data

- Constant chipping rate of 3.84 Mcps (signal bandwidth 5 MHz)
- **Two codes**: spreading codes and scrambling codes
- Spreading codes: separation of datastreams from one sender
  - different user data rates supported via different spreading factors
  - higher data rate: less chips per bit
  - spreading codes are orthogonal (OVSF) (see next slide)
- Scrambling codes: sender separation via unique, quasi orthogonal scrambling codes
  - senders are not separated via orthogonal spreading codes
  - much simpler management of codes: each station can use the same orthogonal spreading codes
  - precise synchronization not necessary as the scrambling codes stay quasi orthogonal



KU LEUVEN

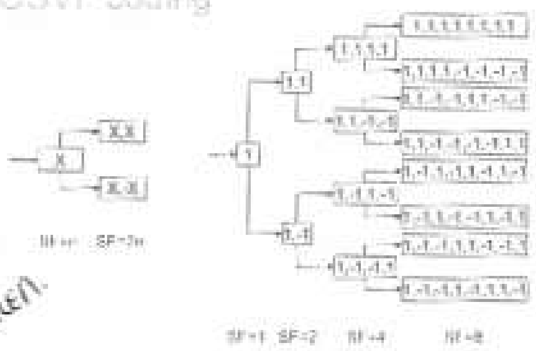
chipping code veranderen.

multiplexer v. elke bron

multiplexe- mediaa kunnen.
⇒ quasi orth.
want je kan toch niet ~~[illegible]~~ synchroniseren.

niet gelijken
○ BB
→ verschillende signalen met elkaar multiplexen

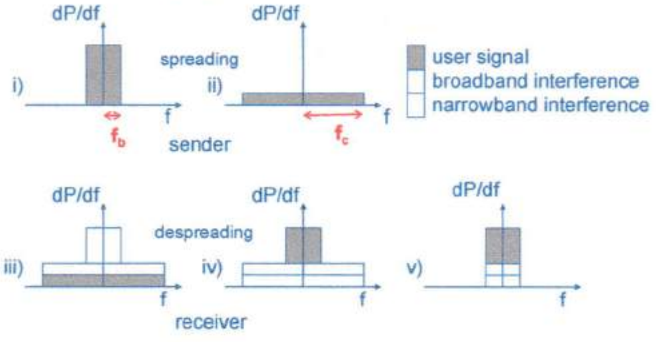
OSVF coding



Codes from different branches are orthogonal

KU LEUVEN

Processing gain



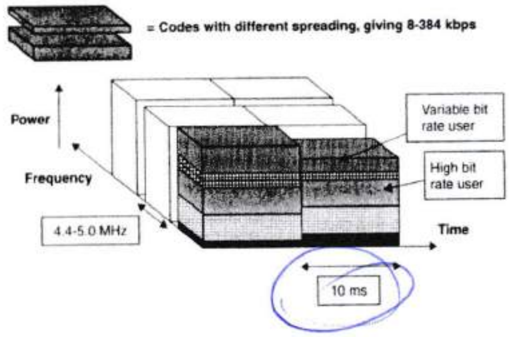
Processing gain = f_c/f_b -> improvement in SIR

hoe grote f_c -> hoe meer interferentie & ruis je kan wegwerken.

WCDMA - Spreading and despreading

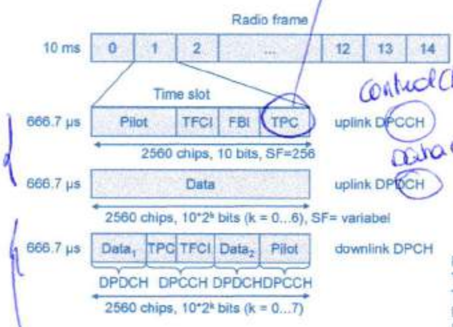
- UMTS chiprate: 3.84 Mcps (bandwidth 5 MHz)
- Example : speech
  - bitrate = 12.2 kbps
  - processing gain = 10 log (3.84 Mcps/12.2 kbps) = 25 dB
  - Required Eb/No = 5 dB
  - Signal to interference+ noise ratio SIR = 5dB - 25 dB = -20 dB => signal can be 20 dB under interference+noise
- Example : data service 2Mbit/s (max for UMTS)
  - Processing gain less than 3 dB (10 log(3.84e6/2e6) = 2.8 dB.
- **Bij UMTS worden hogere bitrates dus gerealiseerd ten koste van robuustheid tegen interferentie met andere signalen.**

WCDMA - Variabele bitrate



nodig voor periodieke [illegible]ties.
-> TT multiplexen.

UMTS FDD frame structure



W-CDMA
- 1920-1980 MHz uplink
- 2110-2170 MHz downlink
- chipping rate: 3.840 Mchip/s
- soft handover
- QPSK
- complex power control (1500 power control cycles/s)
- spreading: UL: 4-256; DL:4-512

FBI: Feedback information (e.g. for handover)
TPC: Transmit Power Control
TFCI: Transport Format Combination Indicator
DPCCH: Dedicated Physical Control Channel
DPDCH: Dedicated Physical Data Channel
DPCH: Dedicated Physical Channel

Slot structure NOT for user separation but support for periodic functions!

multiplex code

1500 cycles/s

Control Channel

Data ch.

multiplex i.d. tijd.
-> want codes al gebruikt.

SF ~ datarate

Typical UTRA-FDD uplink data rates

3F voice

foutcorrectie

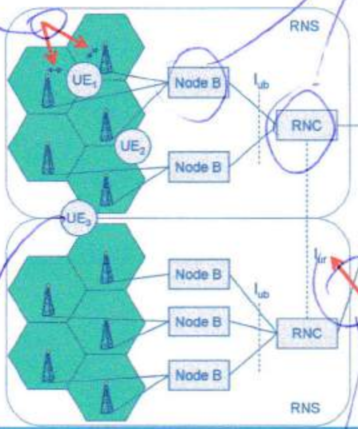
User data rate [kbit/s]	12.2 (voice)	64	144	384
DPDCH [kbit/s]	60	240	480	960
DPCCH [kbit/s]	15	15	15	15
Spreading	64	16	8	4

KU LEUVEN

2 stations tegelijk mogelijk

2gen: BSC

UTRAN architecture



RNC: Radio Network Controller

RNS: Radio Network Subsystem

Iu

CN

- UTRAN comprises several RNSs
- Node B can support FDD or TDD or both
- RNC is responsible for handover decisions requiring signaling to the UE
- Cell offers FDD or TDD

KU LEUVEN

⟺ 2gen: MS

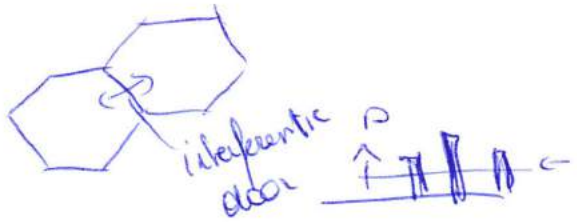
rood → verschillen.

RNC verbonden

in 2gen:

BSC
≠
BSC
MSC
handover

link niet

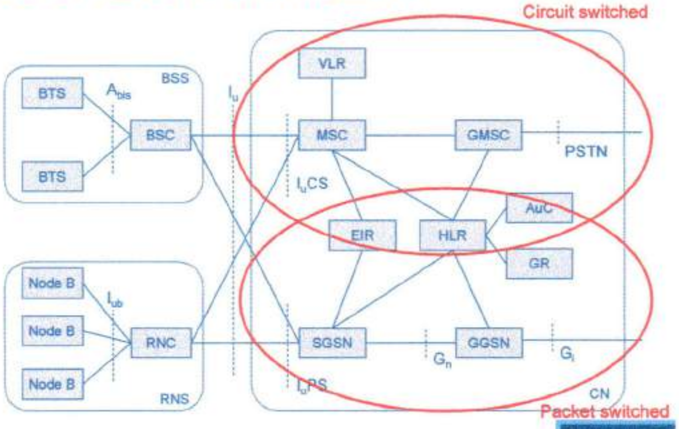


UTRAN functions

- RNC
  - Call admission control
  - Congestion control
  - Radio channel encryption
  - System information broadcasting
  - Multiplexing and protocol conversions
  - Radio resource control (incl measurement of interference and load)
  - Radio bearer set-up and release
  - Outer loop power control (slow, interference between cells)
  - Handover and RNS relocation
  - ...
- Node B
  - One or more antennas (one or more cells)
  - Inner loop power control (fast : 1500/s, near-far)
  - Softer handover

KU LEUVEN

Core network: architecture



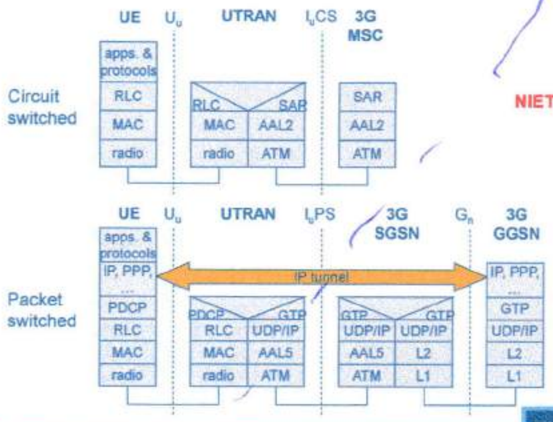
KU LEUVEN

Core network

- The Core Network (CN) and thus the Interface I_u, too, are separated into two logical domains:
- Circuit Switched Domain (CSD)
  - Circuit switched service incl. signaling
  - Resource reservation at connection setup
  - GSM components (MSC, GMSC, VLR)
  - I_uCS
- Packet Switched Domain (PSD)
  - GPRS components (SGSN, GGSN)
  - I_uPS
- Release 99 uses the GSM/GPRS network and adds a new radio access
  - Helps to save a lot of money …
  - Much faster deployment
  - Not as flexible as newer releases (5, 6) -> IP corenetwork

KU LEUVEN

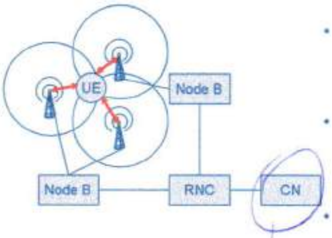
UMTS protocol stacks (user plane)



NIET

KU LEUVEN

Support of mobility: macro diversity



Macrodiversity helps against fast fading, shadowing and multipath propagation

- Beside **hard handovers** (UTRA TDD, interfrequency, intersystem handovers) **soft handovers** are possible in UTRA FDD.
- **Multicasting** of data via several physical channels (macrodiversity)
  - Enables soft handover
  - FDD mode only
- Uplink
  - simultaneous reception of UE data at several Node Bs
  - Reconstruction of data at RNC
- Downlink
  - Simultaneous transmission of data via different cells
  - Different spreading codes in different cells
- Power control in all cells
- Hidden for CN

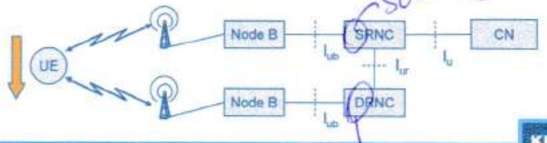
KU LEUVEN

CN weet nt v. die overgangen.

Support of mobility: handover

- **One** RNC manages the connection and sends data to CN; CN not aware of the parallel connections
- RNC controlling the connection is called SRNC (Serving RNC)
- RNC offering additional resources (e.g., for soft handover) is called Drift RNC (DRNC)
- End-to-end connections between UE and CN only via I_u at the SRNC
  - Change of SRNC requires change of I_u (hard handover)
  - Initiated by the SRNC
  - Controlled by the RNC and CN

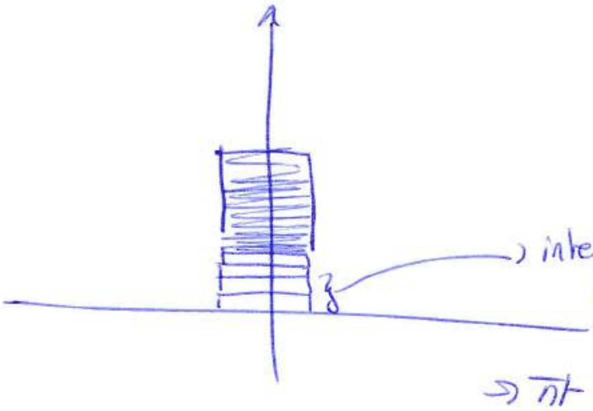
Serving



KU LEUVEN

→ drift.

teveel chaining
hard handover
CN → SRNC.



→ interferentie door andere gebruikers

⇒ $\overline{nt}$ alles kunnen wegfilteren door die quasi orth. codes

KU LEUVEN

TECHNOLOGIECAMPUS GENT

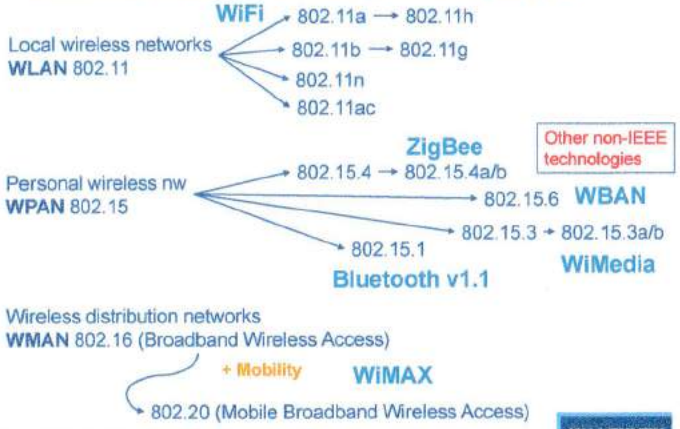
Hoofdstuk 7 – Draadloos LAN

Overview

- Characteristics
- IEEE 802.11
  - PHY
  - MAC
  - Power management
  - Roaming
  - .11a, b, g, h, i
- Bluetooth / IEEE 802.15.x

KU LEUVEN

Mobile Communication Technology according to IEEE



KU LEUVEN

Characteristics of wireless LANs

- Advantages
  - very flexible within the reception area
  - Ad-hoc networks without previous planning possible
  - (almost) no wiring difficulties (e.g. historic buildings, firewalls)
  - more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...
- Disadvantages
  - typically very low bandwidth compared to wired networks (1-10 Mbit/s) due to shared medium, interference (errors), larger delays and jitter
  - many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11)
  - products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions like, e.g., IMT-2000
  - security

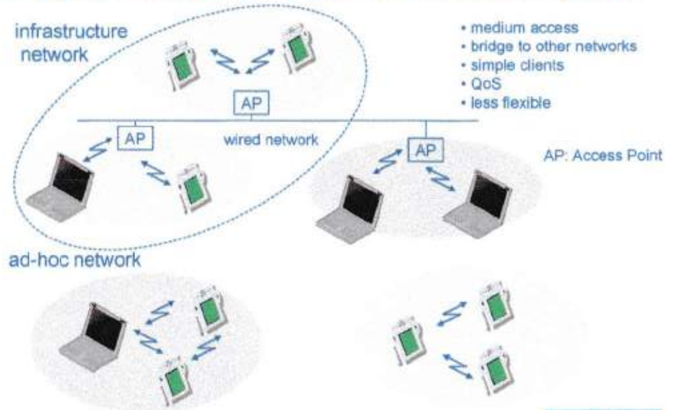
KU LEUVEN

Comparison: infrared vs. radio transmission

- Infrared
  - uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)
- Advantages
  - simple, cheap, available in many mobile devices (IrDA)
  - no licenses needed
  - simple shielding possible
- Disadvantages
  - interference by sunlight, heat sources etc.
  - many things shield or absorb IR light
  - low bandwidth
- Example
  - IrDA (Infrared Data Association) interface available everywhere some year ago

- Radio
  - typically using the license free ISM band at 2.4 GHz
- Advantages
  - experience from wireless WAN and mobile phones can be used
  - coverage of larger areas possible (radio can penetrate walls, furniture etc.)
- Disadvantages
  - very limited license free frequency bands
  - shielding more difficult, interference with other electrical devices
- Example
  - Many different products

Comparison: infrastructure vs. ad-hoc networks



- medium access
- bridge to other networks
- simple clients
- QoS
- less flexible

AP: Access Point

WLAN - WiFi

- **WiFi**: **Wi**reless **Fi**delity
  - WLAN : Wireless version of LAN
  - Based on IEEE 802.11 a, b, g, n, ac
  - WiFi guarantees that products work together
  - IEEE describes the physical layer and MAC-layer, all the rest is like wired LAN
  - Different versions of the standard: mainly different PHY (except for 802.11n and ac)

www.wi-fi.org

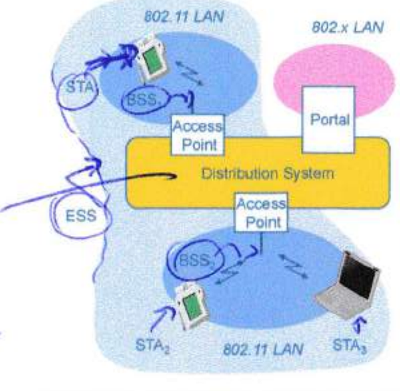
certificeren v. producten

802.11	2.4 GHz	1 or 2 Mbit/s	**DSSS**,FHSS,Ir	25 MHz	1997	
802.11a (h/j)	5.0 GHz	6 to 54 Mbit/s	OFDM	20 MHz	1999	WiFi
802.11b	2.4 GHz	5.5 or **11 Mbit/s**	DSSS	25 MHz	1999	WiFi
802.11g	2.4 GHz	**54 Mbit/s**	OFDM	25 MHz	2003	WiFi
802.11n	2.4 GHz /5 GHz	600Mbit/s (theoretical max)	OFDM - MIMO	20 and 40 MHz	2009	WiFi
802.11ac	5 GHz	Total > 1Gbit/s Single link 500Mbit/s		80 and 160MHz	Jan 2014	WiFi

kanaal breedte.

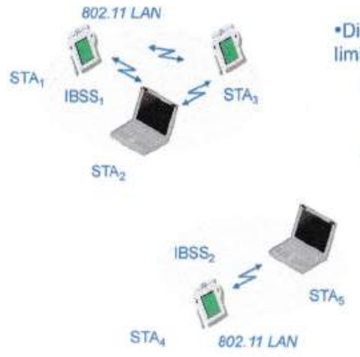
layer 2
⇒ niet gewoon een fysische link

802.11 - Architecture of an infrastructure network



- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS
  - Layer 2 connection. In practice: Ethernet LAN, AP functions as Ethernet bridge

802.11 - Architecture of an ad-hoc network

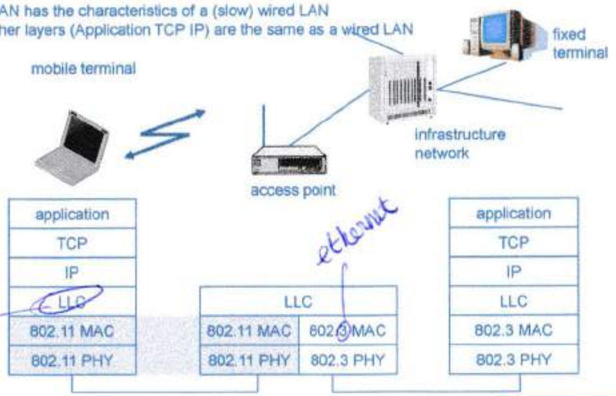


- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium
  - Independent Basic Service Set (IBSS): group of stations using the same radio frequency

KU LEUVEN

IEEE standard 802.11

WLAN has the characteristics of a (slow) wired LAN
Higher layers (Application TCP IP) are the same as a wired LAN



logic link control

802.11 describes MAC and PHY

KU LEUVEN

802.11 - Layers and functions

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - authentication, synchronization, roaming, MAC MIB (management information base), power management
- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, PHY MIB (management information base)
- Station Management
  - coordination of all management functions (e.g. interaction with distribution system)

fout authenticatie

DLC	LLC		Station Management
	MAC	MAC Management	
PHY	PLCP	PHY Management	
	PMD		

welk kanaal

KU LEUVEN

802.11 - Physical layer (classical)

- 3 versions: 2 radio (typ. 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbit/s
  - all PHY versions give a CCA to MAC
- FHSS (Frequency Hopping Spread Spectrum)
  - spreading, despreading, signal strength, typ. 1 Mbit/s
  - min. 2.5 frequency hops/s (USA), two-level GFSK modulation (1 Mbit/s)
- **DSSS (Direct Sequence Spread Spectrum)**
  - **DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)**
  - **preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s**
  - **chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)**
  - **max. radiated power 1 W (USA), 100 mW (EU), min. 1mW**
- Infrared
  - 850-950 nm, diffuse light, typ. 10 m range
  - carrier detection, energy detection, synchronization

niet voor
multiplexen
hier puur
voor robustheid

KU LEUVEN

CSMA/CA

→ ·Window variabel

collision ⇒ w↑

onbezet ⇒ w↓

DSSS PHY packet format

- Synchronization
  - synch., gain setting, energy detection (CCA), frequency offset compensation
- SFD (Start Frame Delimiter)
  - 1111001110100000
- Signal
  - data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service
  - future use, 00: 802.11 compliant
- Length
  - □ length of the payload
- HEC (Header Error Check)
  - protection of signal, service and length, $x^{16}+x^{12}+x^{5}+1$

128	16	8	8	16	16	variable	bits
synchronization	SFD	signal	service	length	HEC	payload	
PLCP preamble		PLCP header					

KU LEUVEN

802.11 - MAC layer I - DFWMAC

- 2 Traffic services
  - Asynchronous Data Service (mandatory)
    - exchange of data packets based on "best-effort"
    - support of broadcast and multicast
  - Time-Bounded Service (optional)
    - implemented using PCF (Point Coordination Function), only with AP
- 3 Access methods
  DFWMAC Distributed Foundation Wireless MAC
  - DFWMAC-DCF CSMA/CA (mandatory) (DCF=Distributed coordination function)
    - collision avoidance via randomized „back-off" mechanism
    - minimum distance between consecutive packets
    - ACK packet for acknowledgements (not for broadcasts)
  - DFWMAC-DCF w/ RTS/CTS (optional)
    - avoids hidden terminal problem
  - DFWMAC- PCF (optional)
    - access point polls terminals according to a list

KU LEUVEN

nooit echt geïmpl.

bij asynch.

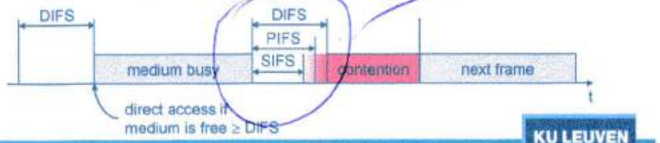
geen controle ~~[illegible]~~

controle

probleem van hidden terminal opgelossen.

802.11 - MAC layer II

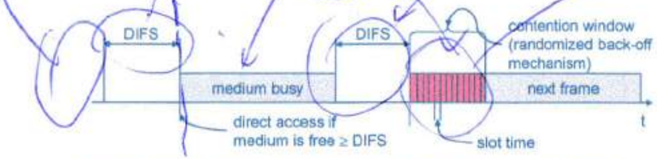
- Priorities
  - defined through different inter frame spaces
  - no guaranteed, hard priorities
  - SIFS (Short Inter Frame Spacing)
    - highest priority, for ACK, CTS, polling response
  - PIFS (PCF IFS)
    - medium priority, for time-bounded service using PCF
  - DIFS (DCF, Distributed Coordination Function IFS)
    - lowest priority, for asynchronous data service



KU LEUVEN

versies van interframe space

802.11 - CSMA/CA access method I


DIFS
medium busy
DIFS
contention window (randomized back-off mechanism)
next frame
t
direct access if medium is free ≥ DIFS
slot time

Medium is vrij

wachten

als medium bezet

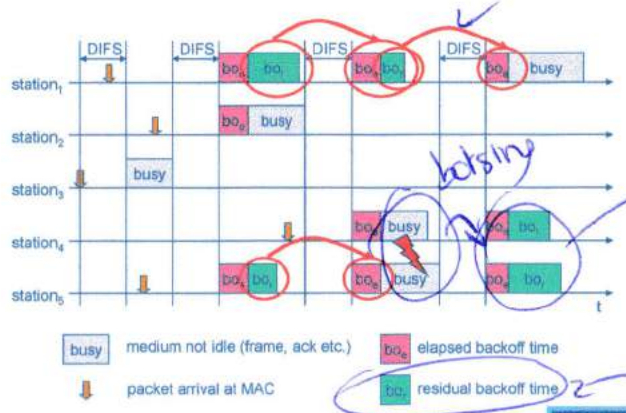
wacht

random tijd wachten voor collision Avoid. (CA)

- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

KU LEUVEN

802.11 - competing stations - simple version



voor fairness
⇒ geen nieuwe random bo
⇒ gewoon verder aftellen

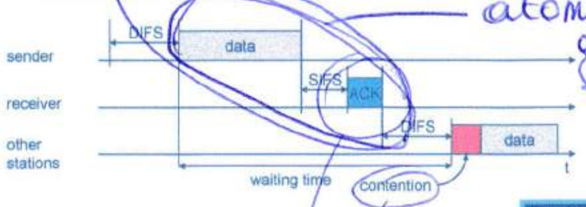
botsing

nieuwe random

2 tijd die nog moet w afgeteld.

802.11 - CSMA/CA access method II

- Sending unicast packets
  - station has to wait for DIFS before sending data
  - receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
  - automatic retransmission of data packets in case of transmission errors



atomisch geheel
= atomic operation

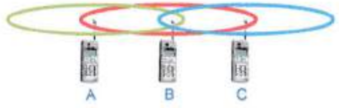
veroveringstijd (random wachten)

niet nodig in ethernet

Problem of hidden terminals (cfr supra)

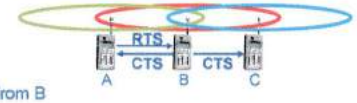
Hidden terminals

- A sends to B, C cannot receive A
- C wants to send to B, C senses a "free" medium (CS fails)
- collision at B, A cannot receive the collision (CD fails)
- A is "hidden" for C



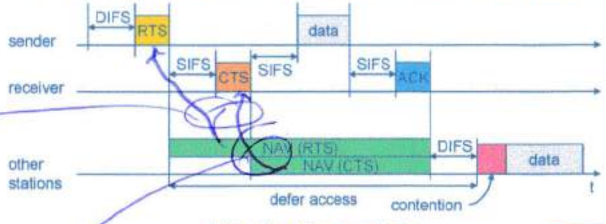
RTS/CTS solution

- A and C want to send to B
- A sends RTS first
- C waits after receiving CTS from B



802.11 – DFWMAC – DCF with RTS/CTS

- Sending unicast packets
  - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
  - acknowledgement via CTS (again with reservation parameter) after SIFS by receiver (if ready to receive)
  - sender can now send data at once, acknowledgement via ACK
  - other stations store medium reservations distributed via RTS **and** CTS



NAV = Net Allocation Vector

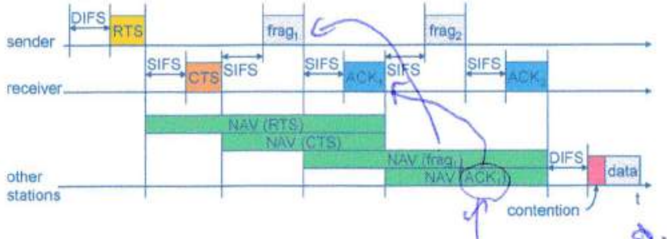
NAV gecodeerd in RTS/CTS bericht

hoe lang netwerk bezet gaat zijn

bij onbetrouwbaar netwerk => verlies pakket = opnieuw verzend

Fragmentation

Wireless communication has a higher bit error rate : use smaller frames
-> fragmentation mode

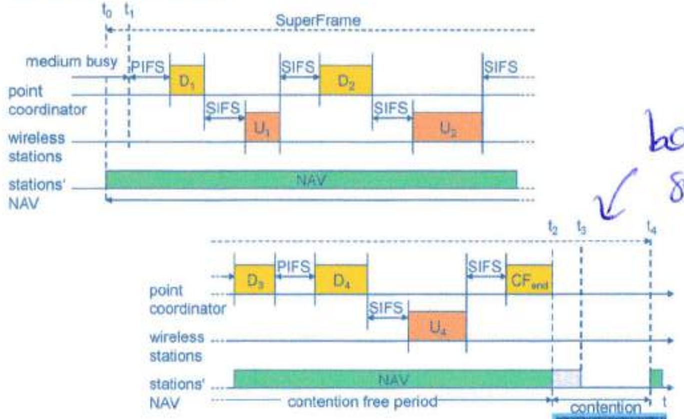


beter kleinere pakketten i.p.v. lang.

waarin gecodeerd.

AP is controle coörd.
↳ pollen.

DFWMAC-PCF



bovenop superframe vrij ook pakketten versturen.

Superframe + interactie zaken erin
=> ieder v. zijn tijd
gegarandeerde timing

802.11 - Frame format

- Duration
  - for NAV with RTS/CTS and fragmentation
- Addresses
  - 48 bit MAC addresses: receiver, transmitter (physical), BSS identifier, sender (logical), depend on DS-fields (see further)
- Sequence numbers
  - important against duplicated frames due to lost ACKs
- Types
  - control frames, management frames, data frames
- Subtype
  - e.g. subtypes of management frames: 0000 association request, 1000 beacon
  - e.g. subtypes of control frames: 1011 RTS, 1100 CTS

RTS/CTS

Beacons

voor NAV invullen

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	WEP	Order

802.11 - Frame format

- More frag
  - more fragments follow
- Retry
  - current frame is a retransmission of a earlier frame
- Power management
  - indicate status of a station after a successful frame transmission
- More data
  - sender has more packets available for receiver (e.g. AP signals to station in low power mode that more packets are available)
- WEP Wired Equivalent Privacy
- Order
  - received frames must be processed in strict order

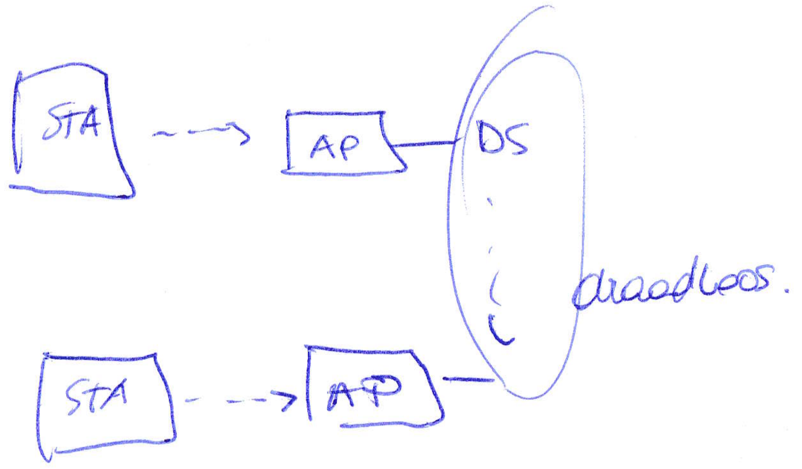
fragmentatie ↳

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	WEP	Order

↳ volgende stukje

4.



4 adressen in format

DS = distributiön Systeen

MAC address format

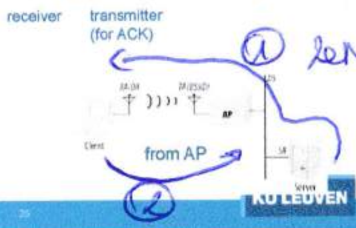
Rechtste komen v. AP →

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
④ infrastructure network, within DS	1	1	RA	TA	DA	SA

physical

logical

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address



MAC-adr. nodige

Special Frames: ACK, RTS, CTS

- Acknowledgement

ACK

bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

- Request To Send

RTS

bytes	2	2	6	6	4
	Frame Control	Duration	Receiver Address	Transmitter Address	CRC

- Clear To Send

CTS

bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

802.11 - MAC management

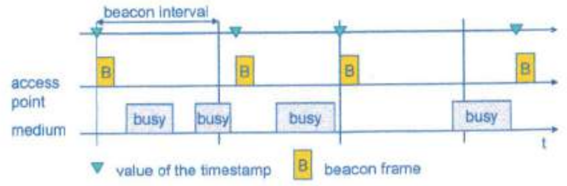
- Synchronization
  - try to find a LAN, try to stay within a LAN
  - synchronisation of internal clocks, generations of beacons
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
- MIB - Management Information Base
  - managing, read, write (accessible via SNMP)
  - contain all information on current state of AP or station

Synchronization using a Beacon (infrastructure)

← met AP

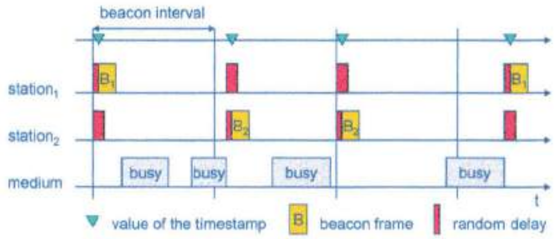
Timing Synchronisation Function (TSF) for
- power management
- PCF (superframe prediction)
- FHSS (hopping sequence)

Quasi periodic transmission of beacons (time stamp + other information)
In an infrastructure network : beacons transmitted by AP



Synchronization using a Beacon (ad-hoc)

- Each station has its own synchronisation clock.
- After beacon interval all stations start sending a beacon, random back-off applied so one beacons wins, all other stations adapt their clock and suppress the transmission of their beacon for this cycle



KU LEUVEN

Ad-hoc.

Power management

- Mobile means batteries => power saving is crucial
- Idea: switch the transceiver off if not needed
  - easy for transmitter, but for receiver ?
- States of a station: sleep and awake ← afspreken wanneer slapen wakker
- Data can be buffered at sender.
- Timing Synchronization Function (TSF)
  - stations wake up at the same time
  - sender informs the receivers if it has buffered data
  - these receivers stay awake

wacht met zenden →

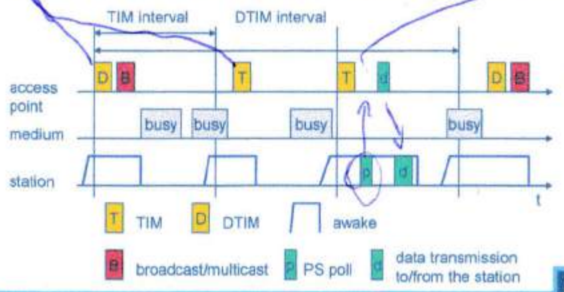
KU LEUVEN

Power saving with wake-up patterns (infrastructure)

- Infrastructure
  - AP buffers all dataframes for stations using power saving
  - Traffic Indication Map (TIM)
    - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - list of broadcast/multicast receivers transmitted by AP

voor wie AP data klaar heeft staan

na wel der



D broadcast info

T unicast

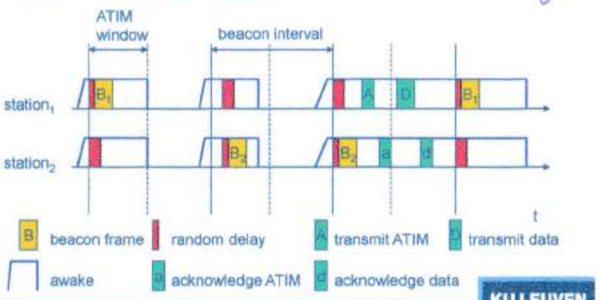
⇐ Beacons.

KU LEUVEN

Power saving with wake-up patterns (ad-hoc)

- Ad-hoc
  - Ad-hoc Traffic Indication Map (ATIM)
    - announcement of receivers by stations buffering frames
    - more complicated - no central AP
    - collision of ATIMs possible (scalability?)

slecht schaalbaar-



KU LEUVEN

802.11 - Roaming

updaten routing tabellen

- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals (passive scanning) or send probes into the medium and wait for an answer (active scanning)
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources

KU LEUVEN

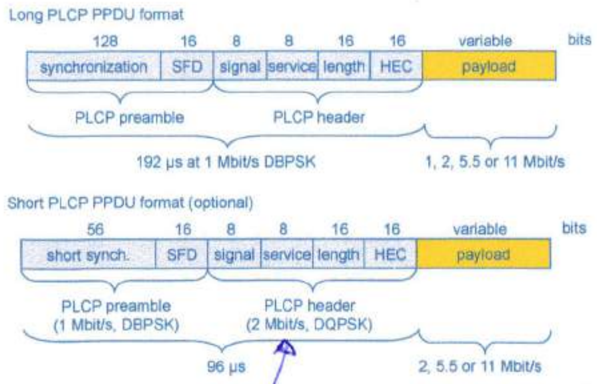
WLAN: IEEE 802.11b

- Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - User data rate max. approx. 6 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
- Frequency
  - Free 2.4 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Many products, many vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Typ. Best effort, no guarantees (unless polling is used, limited support in products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Special Advantages/Disadvantages
  - Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
  - Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

KU LEUVEN

IEEE 802.11b – PHY frame formats

headers stabiel ↑ zeker zijn dat alle stations kunnen lezen.

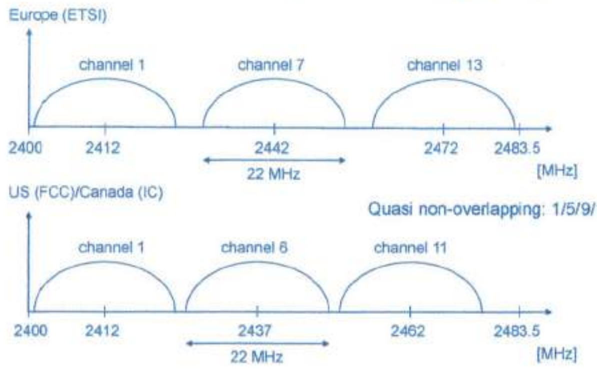


kan sneller doorsturen

verkorte headers ⇒ nog sneller

KU LEUVEN

Channel selection (non-overlapping)



Quasi non-overlapping: 1/5/9/13

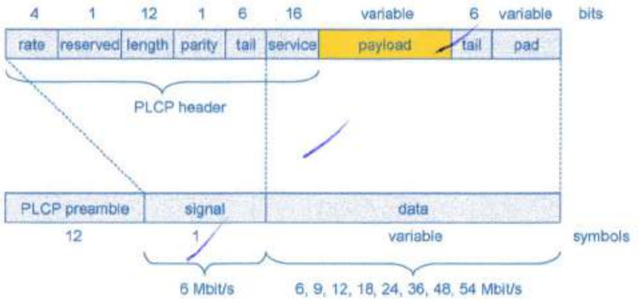
KU LEUVEN

WLAN: IEEE 802.11a

- Data rate
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
  - User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - 6, 12, 24 Mbit/s mandatory
- Transmission range
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m
- Frequency
  - Free 5.15-5.35, 5.47-5.725 GHz ISM-band (in Europe)
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Some products, some vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Typ. best effort, no guarantees (same as all 802.11 products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Special Advantages/Disadvantages
  - Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
  - Disadvantage: stronger shading due to higher frequency, no QoS

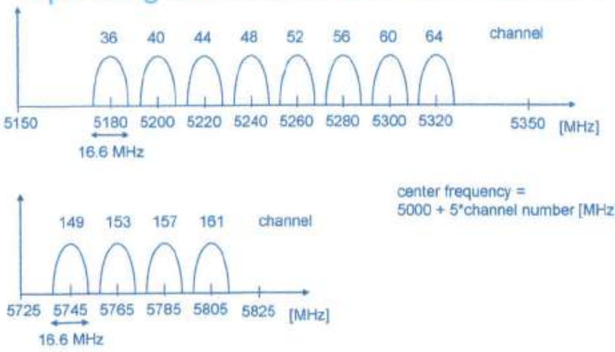
KU LEUVEN

IEEE 802.11a – PHY frame format



KU LEUVEN

Operating channels for 802.11a / US U-NII



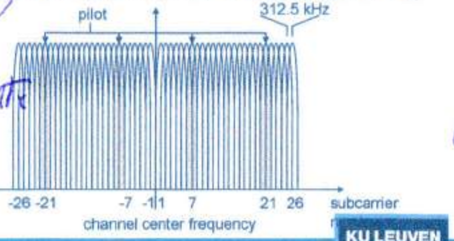
center frequency =
5000 + 5*channel number [MHz]

KU LEUVEN

ipv-DSS

OFDM in IEEE 802.11a (and HiperLAN2)

- OFDM with 52 used subcarriers : 48 data + 4 pilot
  (plus 12 virtual subcarriers gives 64 in total for FFT implementation)
- 312.5 kHz spacing
- Fixed OFDM symbol rate of 250 000 symb/s
  - 0.8 µs guardspace: to prevent ISI
  - 3.2 µs for payload
- Different bitrates:
  - Number of bits per OFDM symb (hence subcarrier modulation: BPSK, QPSK, 16 QAM, 64 QAM),
  - Codingrate (1/2, 2/3,3/4)



KU LEUVEN

verbreding door modulatie

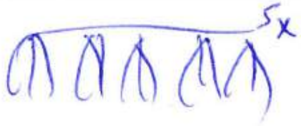
fc

pure sinus

verhogen v. data snelheid

verhoging redundante bits

OFDM

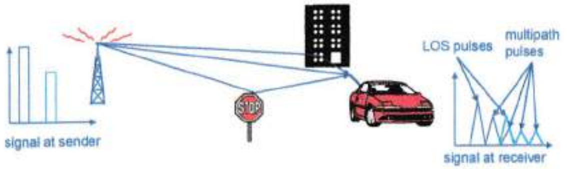


5x 200 kbit/s.

orthogonale FDM

Delay spread

- Multipath propagation: delay spread
- InterSymbol Interference (ISI)
  - => limits the datarate (e.g. **guard period** between symbols)
- Mitigate by diversity techniques
- MIMO systems exploit multipath propagation



KU LEUVEN

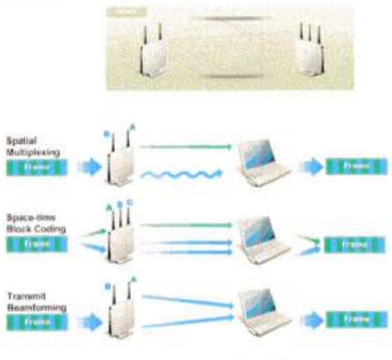
802.11n

- Published Oct 2009
- 2.4 GHz or 5 GHz band can be used
- Techniques to achieve higher bitrates
  - PHY
    - MIMO: multiple datastream using multiple send and receive antennas (spatial division multiplexing) : max 4 streams
    - 40 MHz channels (compared to 20 MHz in previous versions)
    - Shorter guard intervals (time between transmitted symbols e.g. to avoid ISI)
    - Shorter Greenfield preamble
  - MAC
    - Aggregation of frames: packing multiple MAC-frames to reduce overhead (headers, interframe spacing, ack, contention, …)
    - Block acknowledgement protocol
- Better robustness
  - Spatial diversity, Space-time block coding (STBC), Fast link adaptation
  - Transmit beamforming (TxBF), Low density parity check codes (LDPC)

KU LEUVEN

802.11n

Multiple antennas



← theoretisch
nt praktisch
in gebruik.

http://www.airmagnet.com/assets/whitepaper/WP-802.11nPrimer.pdf

KU LEUVEN

802.11n

Datarates

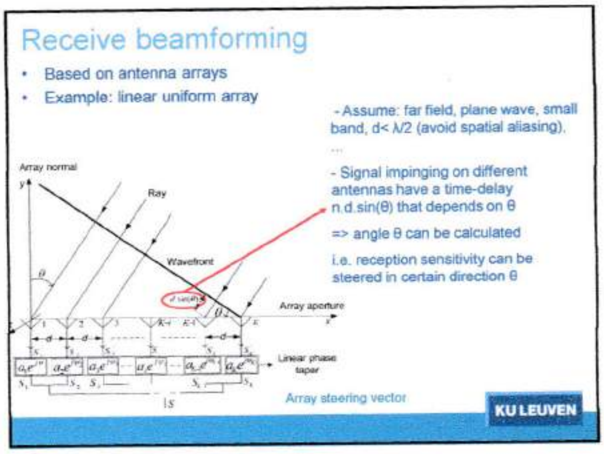
MCS Index	Spatial Streams	Modulation Type	Coding Rate	Data Rate Mb/s			
				20 MHz channel		40 MHz channel	
				800ns GI	400ns GI	800ns GI	400ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00
…	3						
23	3	64-QAM	5/6	195.00	216.00	405.00	450.00
…	4						
31	4	64-QAM	5/6	260.00	288.90	540.00	600.00

GI = Guard Interval

1. High throughput (HT) mode (Greenfield)
2. Non-HT Mode (Legacy)
3. HT Mixed Mode

http://www.airmagnet.com/assets/whitepaper/WP-802.11nPrimer.pdf

KU LEUVEN



Receive beamforming

- Based on antenna arrays
- Example: linear uniform array

- Assume: far field, plane wave, small band, d< λ/2 (avoid spatial aliasing).

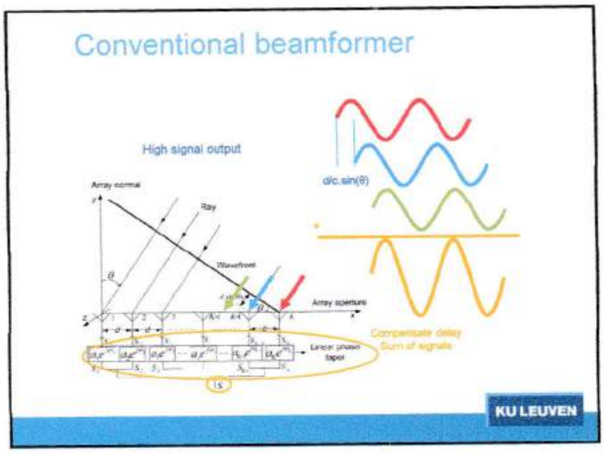
...

- Signal impinging on different antennas have a time-delay n.d.sin(θ) that depends on θ

=> angle θ can be calculated

i.e. reception sensitivity can be steered in certain direction θ

Array steering vector



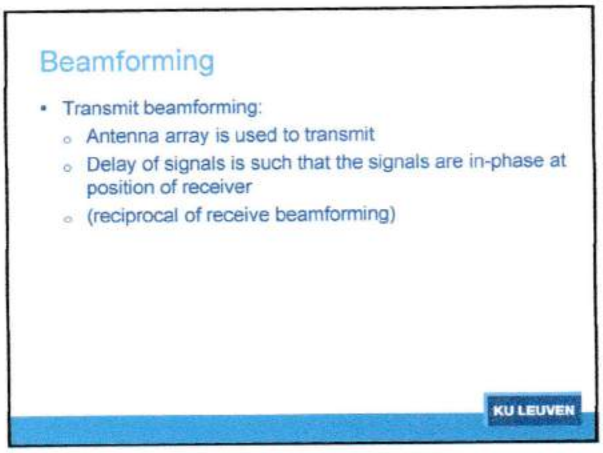
Conventional beamformer

High signal output

d/c.sin(θ)

+

Compensate delay
Sum of signals



Beamforming

- Transmit beamforming:
  - Antenna array is used to transmit
  - Delay of signals is such that the signals are in-phase at position of receiver
  - (reciprocal of receive beamforming)

WLAN: IEEE 802.11 – other developments

- 802.11c: Bridge Support
  - Definition of MAC procedures to support bridges as extension to 802.1D
- 802.11d: Regulatory Domain Update
  - Support of additional regulations related to channel selection, hopping sequences
- 802.11e: MAC Enhancements – QoS
  - Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol
  - Definition of a data flow ("connection") with parameters like rate, burst, period
  - Additional energy saving mechanisms and more efficient retransmission
- 802.11f: Inter-Access Point Protocol
  - Establish an Inter-Access Point Protocol for data exchange via the distribution system
  - Currently unclear to which extend manufacturers will follow this suggestion
- **802.11g: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM**
  - **Successful successor of 802.11b, performance loss during mixed operation with 11b**
- **802.11h: Spectrum Managed 802.11a**
  - **Extension for operation of 802.11a in Europe by mechanisms like channel measurement for dynamic channel selection (DFS, Dynamic Frequency Selection) and power control (TPC, Transmit Power Control)**

KU LEUVEN

WLAN: IEEE 802.11– other developments

- **802.11i: Enhanced Security Mechanisms**
  - **Enhance the current 802.11 MAC to provide improvements in security.**
  - **TKIP enhances the insecure WEP, but remains compatible to older WEP systems**
  - **AES provides a secure encryption method and is based on new hardware**
- 802.11j: Extensions for operations in Japan
  - Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range
- 802.11k: Methods for channel measurements
  - Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel
- 802.11m: Updates of the 802.11 standards
- **802.11n: Higher data rates above 100Mbit/s**
  - **Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP**
  - **MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible**
  - **Standardized since 2009**
- 802.11p: Inter car communications
  - Communication between cars/road side and cars/cars
  - Planned for relative speeds of min. 200km/h and ranges over 1000m
  - Usage of 5.850-5.925GHz band in North America

KU LEUVEN

WLAN: IEEE 802.11– other developments

- 802.11r: Faster Handover between BSS
  - Secure, fast handover of a station from one AP to another within an ESS
  - Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
  - Handover should be feasible within 50ms in order to support multimedia applications efficiently
- 802.11s: Mesh Networking
  - Design of a self-configuring Wireless Distribution System (WDS) based on 802.11
  - Support of point-to-point and broadcast communication across several hops
- 802.11t: Performance evaluation of 802.11 networks
  - Standardization of performance measurement schemes
- 802.11u: Interworking with additional external networks
- 802.11v: Network management
  - Extensions of current management functions, channel measurements
  - Definition of a unified interface
- 802.11w: Securing of network control
  - Classical standards like 802.11, but also 802.11i protect only data frames, not the control frames. Thus, this standard should extend 802.11i in a way that, e.g., no control frames can be forged.
-
- Note: Not all "standards" will end in products, many ideas get stuck at working group level
- Info: www.ieee802.org/11/, 802wirelessworld.com, standards.ieee.org/ge

KU LEUVEN

AD → 60 GHz.
↓
beamforming. omdat
60GHz veel ω
geabsorbeerd licht.

KU LEUVEN

TECHNOLOGIECAMPUS GENT

Hoofdstuk 7 – Draadloos LAN (part 2)

Overview

- Bluetooth
- ZigBee and IEEE802.15.4
- Near Field Communication NFC

KU LEUVEN

KU LEUVEN

TECHNOLOGIECAMPUS GENT

WPAN
Wireless Personal Area Networks

Bluetooth

- Idea
  - Universal radio interface for ad-hoc wireless connectivity
  - Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
  - Embedded in other devices, goal: 5€/device (2005: 40€/USB bluetooth)
  - Short range (10 m), low power consumption, license-free 2.45 GHz ISM
  - Voice and data transmission, approx. 1 Mbit/s gross data rate

One of the first modules (Ericsson).

KU LEUVEN

Bluetooth

- History
  - 1994: Ericsson (Mattison/Haartsen), "MC-link" project
  - Renaming of the project: Bluetooth according to Harald "Blåtand" Gormsen [son of Gorm], King of Denmark in the 10th century
  - 1998: foundation of Bluetooth SIG, www.bluetooth.org (was: Bluetooth.)
  - 1999: erection of a rune stone at Ercisson/Lund ;-)
  - 2001: first consumer products for mass market, spec. version 1.1 released
  - 2005: 5 million chips/week
- Special Interest Group
  - Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
  - Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
  - > 2500 members
  - Common specification and certification of products

Bluetooth™

History and hi-tech…

1999:
Ericsson mobile communications AB reste denna sten till minne av Harald Blåtand, som fick ge sitt namn åt en ny teknologi för trådlös, mobil kommunikation.

…and the real rune stone

Located in Jelling, Denmark, erected by King Harald "Blåtand" in memory of his parents.
The stone has three sides – one side showing a picture of Christ.

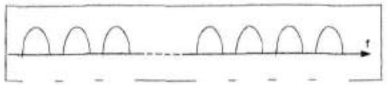
Inscription:
"Harald king executes these sepulchral monuments after Gorm, his father and Thyra, his mother. The Harald who won the whole of Denmark and Norway and turned the Danes to Christianity."

Btw: Blåtand means "of dark complexion" (not having a blue tooth…)

This could be the "original" colors of the stone.
Inscription:
"auk tani karthi kristna" (and made the Danes Christians)

Characteristics

- 2.4 GHz ISM band, 79 RF channels, 1 MHz carrier spacing
  - Channel 0: 2402 MHz … channel 78: 2480 MHz
  - G-FSK modulation, 1-100 mW transmit power, symbol rate 1Mbit/s (v1.1)

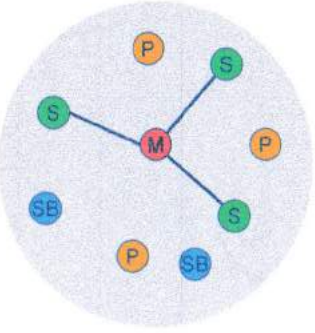


- FHSS and TDD
  - Frequency hopping with 1600 hops/s (= every 625µs)
  - Hopping sequence in a pseudo random fashion, determined by a master (Pseudo-random generator 2^27 states : 23.2 hours)
  - Time division duplex for send/receive separation
- Voice link – SCO (Synchronous Connection Oriented)
  - FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched
- Data link – ACL (Asynchronous ConnectionLess)
  - Asynchronous, fast acknowledge, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched
- Topology
  - Overlapping piconets (stars) forming a scatternet

Piconet

- Collection of devices connected in an ad hoc fashion
- One unit acts as master and the others as slaves for the lifetime of the piconet
- Master determines hopping pattern, slaves have to synchronize
- Each piconet has a unique hopping pattern
- Participation in a piconet = synchronization to hopping sequence
- Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)
- Parked devices have no active connection, but are known and can be activated within ms

synchroniseren met master



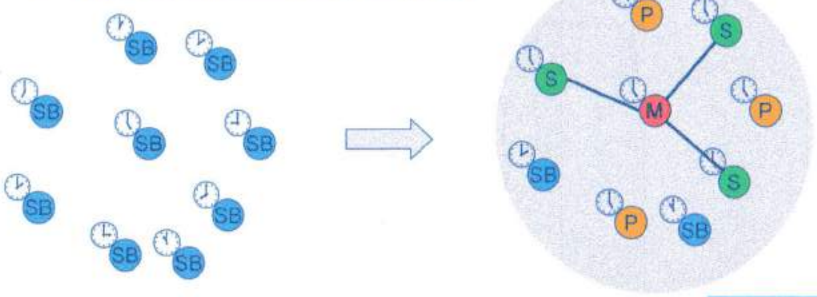
M=Master
S=Slave

P=Parked
SB=Standby

Forming a piconet

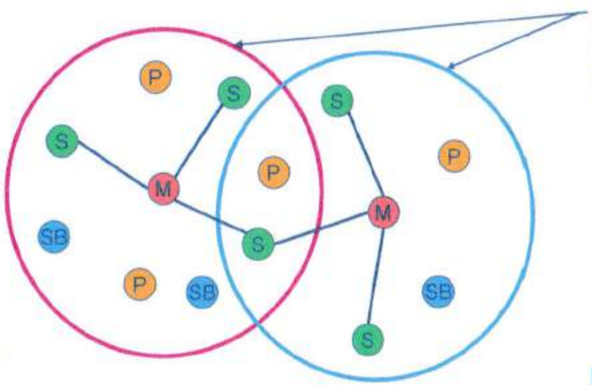
- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
    - Hopping pattern: determined by device ID (48 bit, unique worldwide)
    - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)

korte adres want adr. via id te lang



Scatternet

- Linking of multiple co-located piconets through the sharing of common master or slave devices
  - Devices can be slave in one piconet and master of another
- Communication between piconets
  - Devices jumping back and forth between the piconets



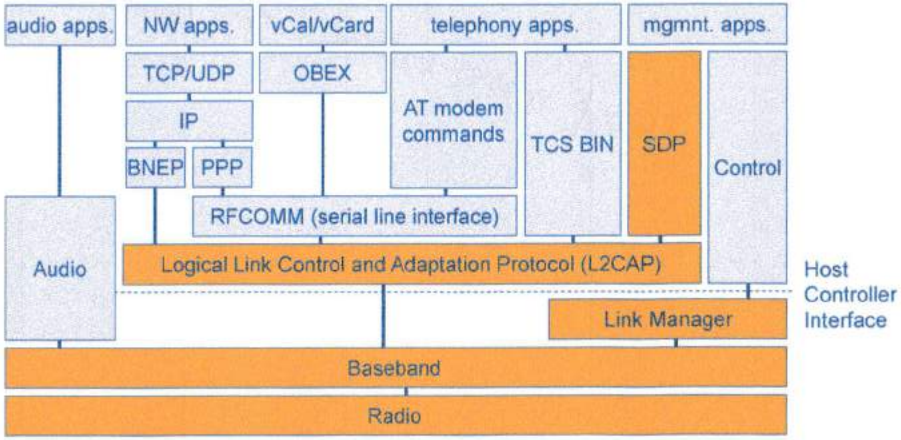
Piconets (each with a capacity of 720 kbit/s)

maar niet praktisch

M=Master
S=Slave
P=Parked
SB=Standby

Bluetooth protocol stack

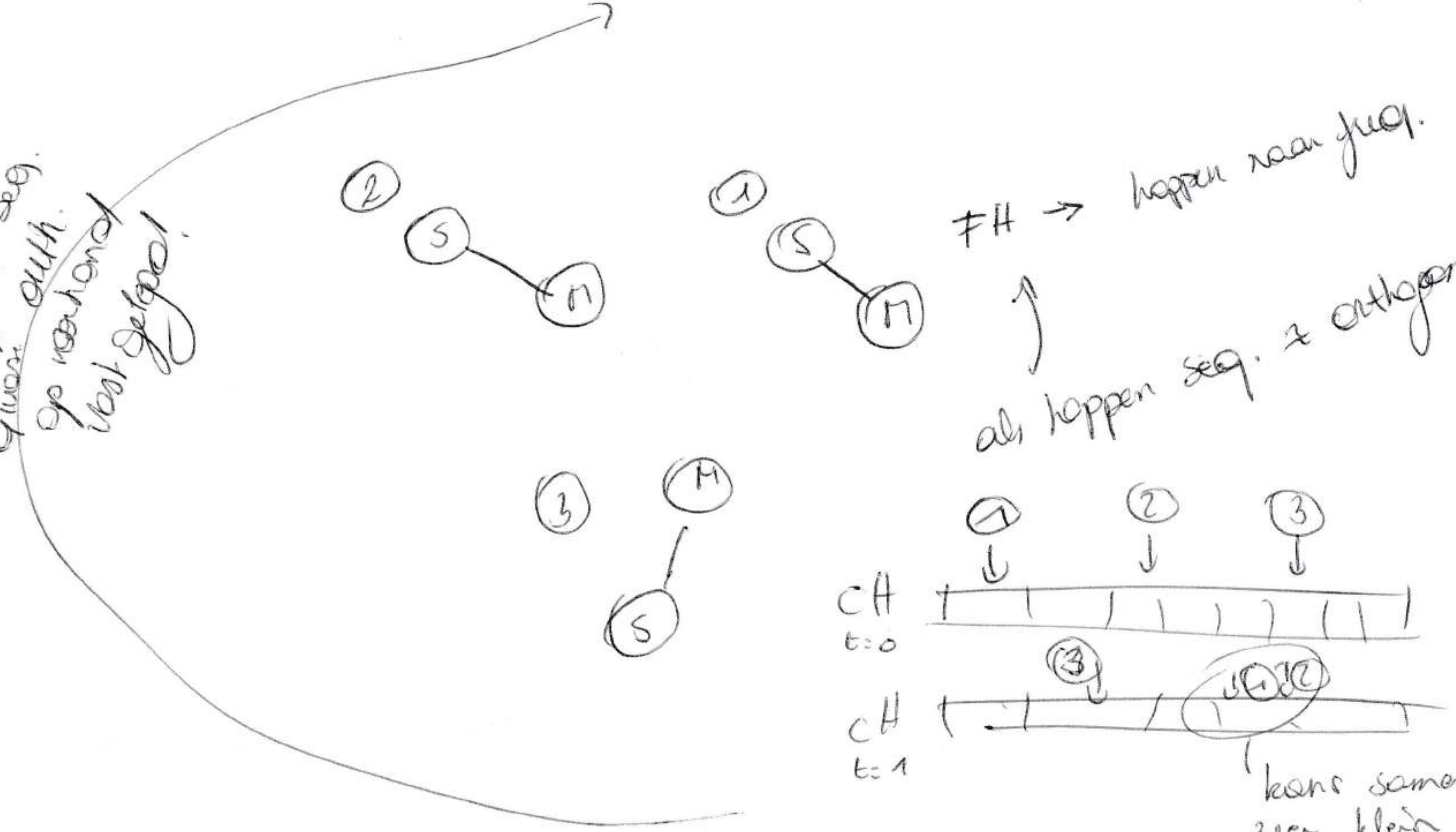
oranje : basis
blauw : optioneel



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

FH - CDMA



FH → hoppen naar freq.

als hoppen seq. ≠ orthogonaal zijn

kans samen in 1 band. zeer klein

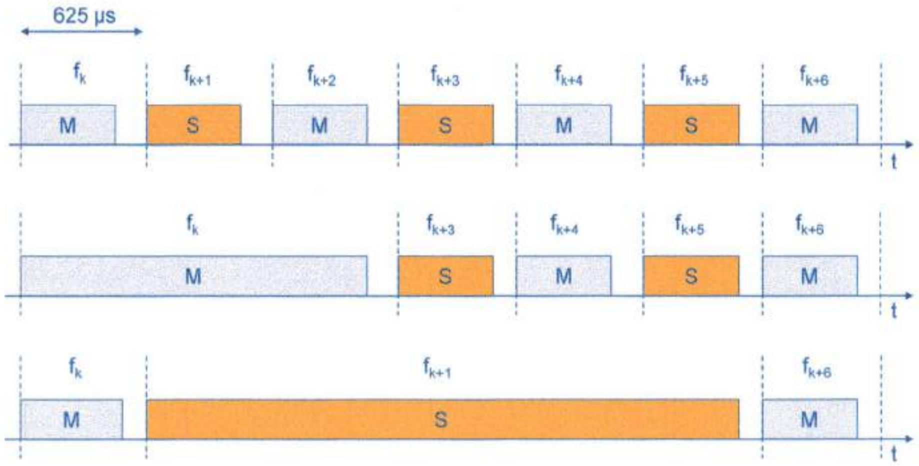
[illegible] freq. seq.
quasi auth.
op voorhand
vast gelegd!

Radio interface

- cfr supra
- Three power classes
  - Class 1: max 100 mW, 100-150 m
  - Class 2: max 2.5 mW, 10 m
  - Class 3: max 1mW

KU LEUVEN

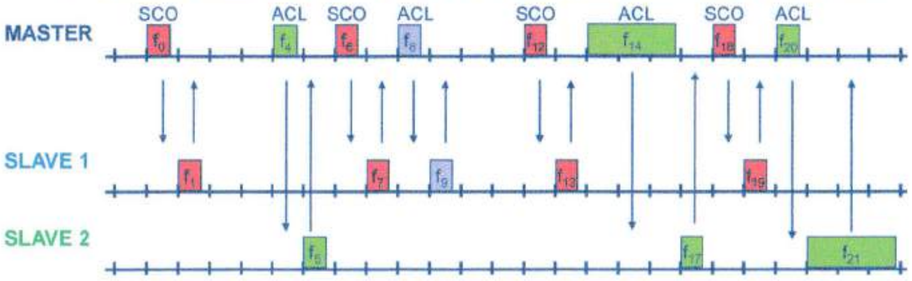
Frequency selection during data transmission



KU LEUVEN

Baseband link types

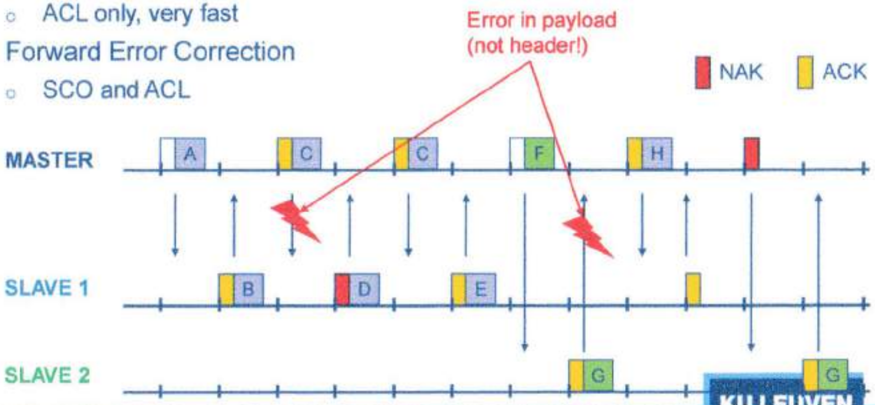
- Polling-based TDD packet transmission
  - 625µs slots, master polls slaves
- SCO (Synchronous Connection Oriented) – Voice
  - Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point
- ACL (Asynchronous ConnectionLess) – Data
  - Variable packet size (1,3,5 slots), asymmetric bandwidth, point-to-multipoint



KU LEUVEN

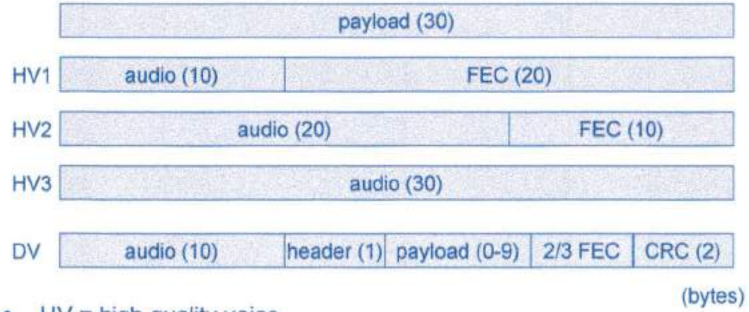
Baseband - Robustness

- Slow frequency hopping with hopping patterns determined by a master
  - Protection from interference on certain frequencies
  - Separation from other piconets (FH-CDMA)
- Retransmission
  - ACL only, very fast
- Forward Error Correction
  - SCO and ACL



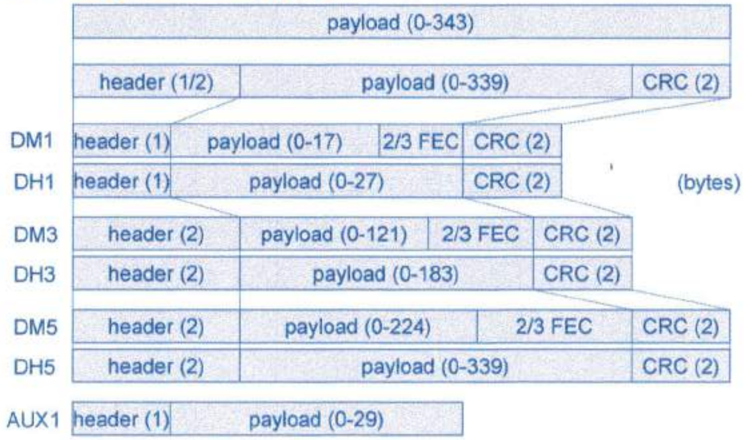
KU LEUVEN

SCO payload types



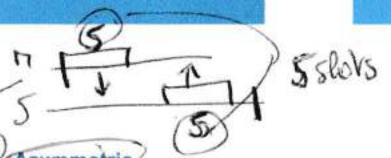
- HV = high quality voice
- DV = data voice
- symmetric, point-to-point
- uses two consecutive timeslots (up and down) with regular intervals
- 64 kbit/s with 2/3 or 1/3 FEC
- never retransmissions
- upto 3 duplex connections possible between slave and master

ACL Payload types

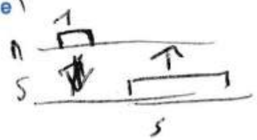


- DM = data medium rate, DH = data high rate
- symmetric or asymmetric
- polling
- 2/3 FEC possible
- ARQ
- one connection between sender and receiver

Baseband data rates

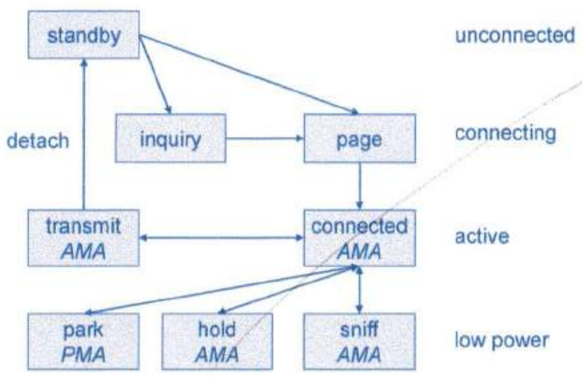


	Type	Payload Header [byte]	User Payload [byte]	FEC	CRC	Symmetric max. Rate [kbit/s]	Asymmetric max. Rate [kbit/s] Forward	Reverse
ACL 1 slot	DM1	1	0-17	2/3	yes	108.8	108.8	108.8
	DH1	1	0-27	no	yes	172.8	172.8	172.8
3 slot	DM3	2	0-121	2/3	yes	258.1	387.2	54.4
	DH3	2	0-183	no	yes	390.4	585.6	86.4
5 slot	DM5	2	0-224	2/3	yes	286.7	477.8	36.3
	DH5	2	0-339	no	yes	**433.9**	**723.2**	**57.6**
	AUX1	1	0-29	no	no	185.6	185.6	185.6
SCO	HV1	na	10	1/3	no	64.0		
	HV2	na	20	2/3	no	64.0		
	HV3	na	30	no	no	64.0		
	DV	1 D	10+(0-9) D	2/3 D	yes D	64.0+57.6 D		



Data Medium/High rate, High-quality Voice, Data and Voice

Baseband states of a Bluetooth device



Standby: do nothing
Inquire: search for other devices
Page: connect to a specific device
Connected: participate in a piconet

Park: release AMA, get PMA
Sniff: listen periodically, not each slot
Hold: stop ACL, SCO still possible, possibly participate in another piconet

Example: Power consumption/CSR BlueCore2

- **Typical Average Current Consumption (1)**
- VDD=1.8V Temperature = 20°C

Mode	
SCO connection HV3 (1s interval Sniff Mode) (Slave)	26.0 mA
SCO connection HV3 (1s interval Sniff Mode) (Master)	26.0 mA
SCO connection HV1 (Slave)	53.0 mA
SCO connection HV1 (Master)	53.0 mA
ACL data transfer 115.2kbps UART (Master)	15.5 mA
ACL data transfer 720kbps USB (Slave)	53.0 mA
ACL data transfer 720kbps USB (Master)	53.0 mA
ACL connection, Sniff Mode 40ms interval, 38.4kbps UART	4.0 mA
ACL connection, Sniff Mode 1.28s interval, 38.4kbps UART	0.5 mA
Parked Slave, 1.28s beacon interval, 38.4kbps UART	0.6 mA
Standby Mode (Connected to host, no RF activity)	47.0 µA
Deep Sleep Mode(2)	20.0 µA

- **Notes:**
- (1) Current consumption is the sum of both BC212015A and the flash.
- (2) Current consumption is for the BC212015A device only.
- (More: www.csr.com)

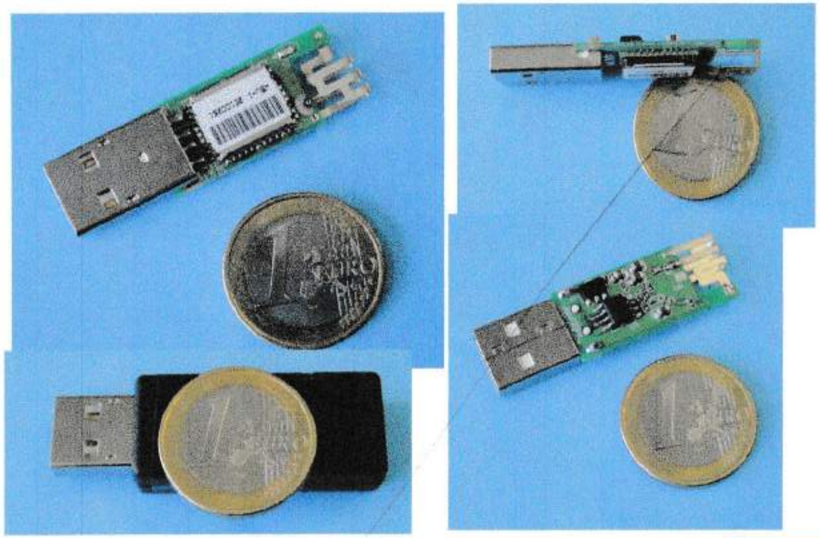
KU LEUVEN

Link manager

- Authentication, encryption, pairing (keys etc)
- Synchronization
- QoS
- Power
- Connection control
- Change state of module

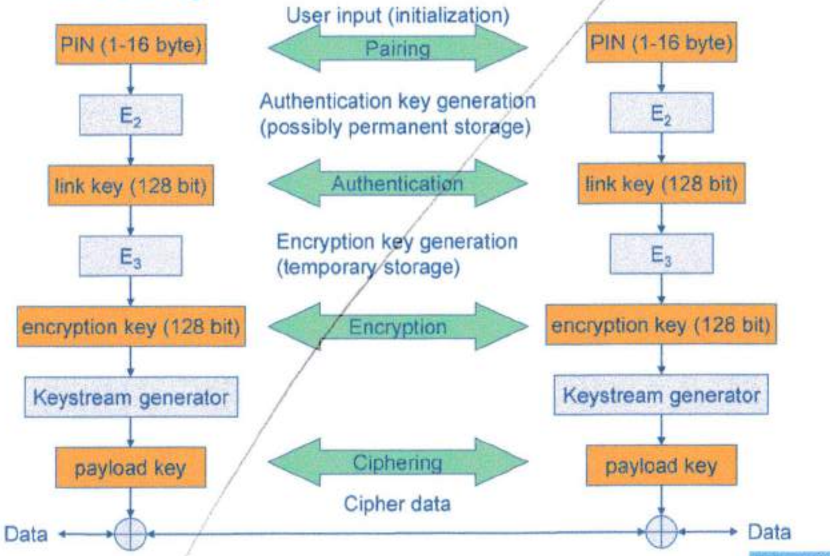
KU LEUVEN

Example: Bluetooth/USB adapter (2002: 50€)



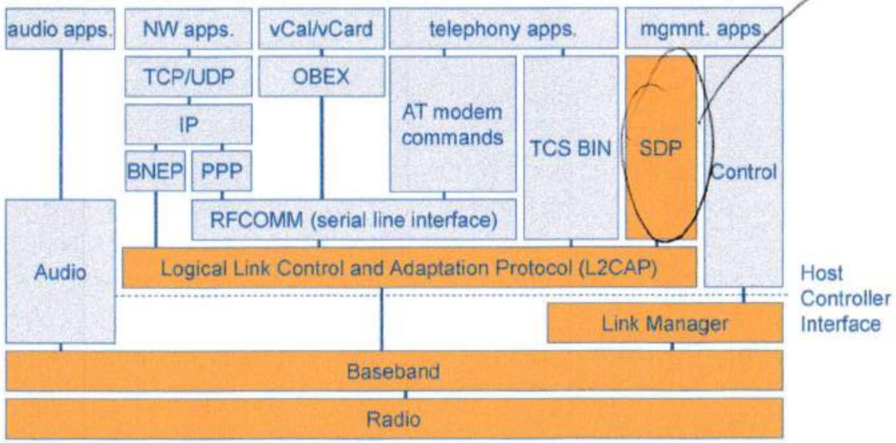
KU LEUVEN

Security



KU LEUVEN

Bluetooth protocol stack



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

KU LEUVEN

SDP – Service Discovery Protocol

- Inquiry/response protocol for discovering services
  - Searching for and browsing services in radio proximity
  - Adapted to the highly dynamic environment
  - Can be complemented by others like SLP, Jini, Salutation, …
  - Defines discovery only, not the usage of services
  - Caching of discovered services
  - Gradual discovery
- Service record format
  - Information about services provided by attributes
  - Attributes are composed of an 16 bit ID (name) and a value
  - values may be derived from 128 bit Universally Unique Identifiers (UUID)

KU LEUVEN

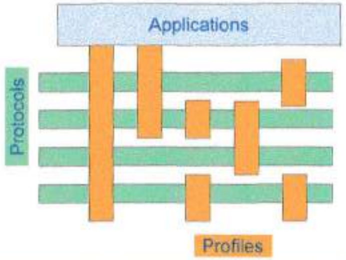
Additional protocols to support legacyprotocols/apps.

- RFCOMM
  - Emulation of a serial port (supports a large base of legacy applications)
  - Allows multiple ports over a single physical channel
- Telephony Control Protocol Specification (TCS)
  - Call control (setup, release)
  - Group management
- OBEX
  - Exchange of objects, IrDA replacement
- WAP
  - Interacting with applications on cellular phones

KU LEUVEN

Profiles

- Represent default solutions for a certain usage model
  - Vertical slice through the protocol stack
  - Basis for interoperability
- Generic Access Profile
- Service Discovery Application Profile
- Cordless Telephony Profile
- Intercom Profile
- Serial Port Profile
- Headset Profile
- Dial-up Networking Profile
- Fax Profile
- LAN Access Profile
- Generic Object Exchange Profile
- Object Push Profile
- File Transfer Profile
- Synchronization Profile



Additional Profiles
Advanced Audio Distribution
PAN
Audio Video Remote Control
Basic Printing
Basic Imaging
Extended Service Discovery
Generic Audio Video Distribution
Hands Free
Hardcopy Cable Replacement

EN

optional.

Bluetooth - Later developments

Bluetooth v2.0 + EDR (2004)

- Backward compatible with version 1.2.
- Introduction of an Enhanced Data Rate (EDR) : nominal rate of EDR is about 3 Mbit/s, the practical data transfer rate is 2.1 Mbit/s. EDR uses a combination of GFSK and PSK. EDR can provide a lower power consumption through a reduced duty cycle
- "Bluetooth v2.0 + EDR" : EDR is an optional feature

Bluetooth v2.1 + EDR (2007)

- Fully backward compatible with 1.2
- Secure simple pairing (SSP): improved pairing experience for Bluetooth devices, while increasing the use and strength of security.
- Also "Extended inquiry response" (EIR) : more information during the inquiry procedure to allow better filtering of devices before connection; sniff subrating, which reduces the power consumption in low-power mode

Bluetooth v3.0 + HS (2009)

- Theoretical data transfer speeds of up to 24 Mbit/s, though not over the Bluetooth link itself. Bluetooth link for negotiation and establishment (device discovery, initial connection and profile configuration) , the high data rate traffic over a co-located 802.11 link. **AMP (Alternate MAC/PHY)** : the addition of 802.11 as a high speed transport.
- "+HS" optional.

Bluetooth - Later developments

Bluetooth v4.0 (2010)

- Provisional names *Wibree* and *Bluetooth ULP* (Ultra Low Power) are abandoned.
- Bluetooth Core Specification version 4.0 includes *Classic Bluetooth*, *Bluetooth high speed* and Bluetooth low energy protocols. Bluetooth high speed is based on Wi-Fi, and Classic Bluetooth consists of legacy Bluetooth protocols.

Bluetooth – Low Energy

Bluetooth low energy : very low power applications running off a coin cell (10 to 20 less power compared to BT Classic)

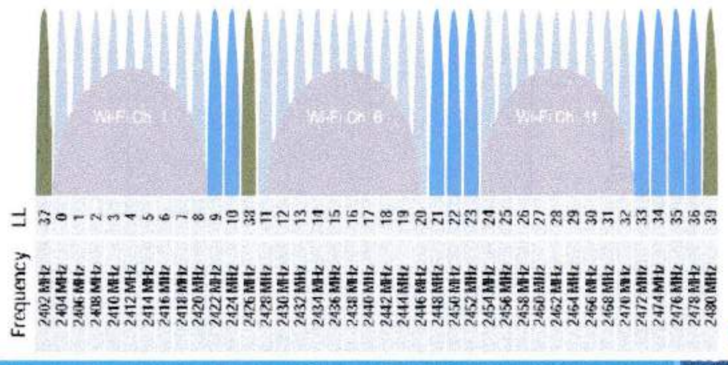
Bluetooth – Low Energy

- Two types of implementation, dual-mode and single-mode.
- In a dual-mode implementation, Bluetooth low energy functionality is integrated into an existing Classic Bluetooth controller.
- Cost-reduced single-mode chips, which will enable highly integrated and compact devices.

Bluetooth – Low Energy

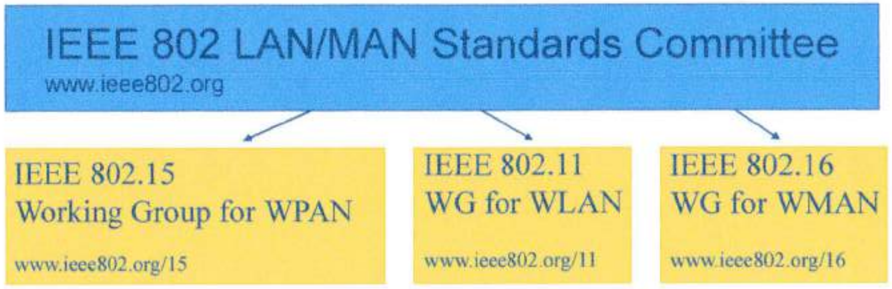
- Basic features
  - Short packages: reduced tx/rx time
  - Simple protocols
  - Less RF channels to improve discovery and connection times
  - Three advertisement channels

advertisement channel.



KU LEUVEN

Who's standardizing what ?



IEEE 802 LAN/MAN Standards Committee
www.ieee802.org

IEEE 802.15
Working Group for WPAN
www.ieee802.org/15

IEEE 802.11
WG for WLAN
www.ieee802.org/11

IEEE 802.16
WG for WMAN
www.ieee802.org/16

IEEE 802.15.1 Medium rate WPAN
Bluetooth v1.1 PHY + MAC
(not versions after v1.2)
IEEE 802.15.3 High rate WPAN
IEEE 802.15.4 Low Rate WPAN
ZigBee PHY + MAC
IEEE 802.15.6 BAN

WiFi

WiMax

KU LEUVEN

Who's standardizing what ?

Bluetooth™

Bluetooth v1.1

Bluetooth SIG
www.bluetooth.org

IEEE 802.15.1

Higher layers

PHY + MAC

ZigBee™ Alliance
Wireless Control That Simply Works

ZigBee Alliance
www.zigbee.org

IEEE 802.15.4

Higher layers

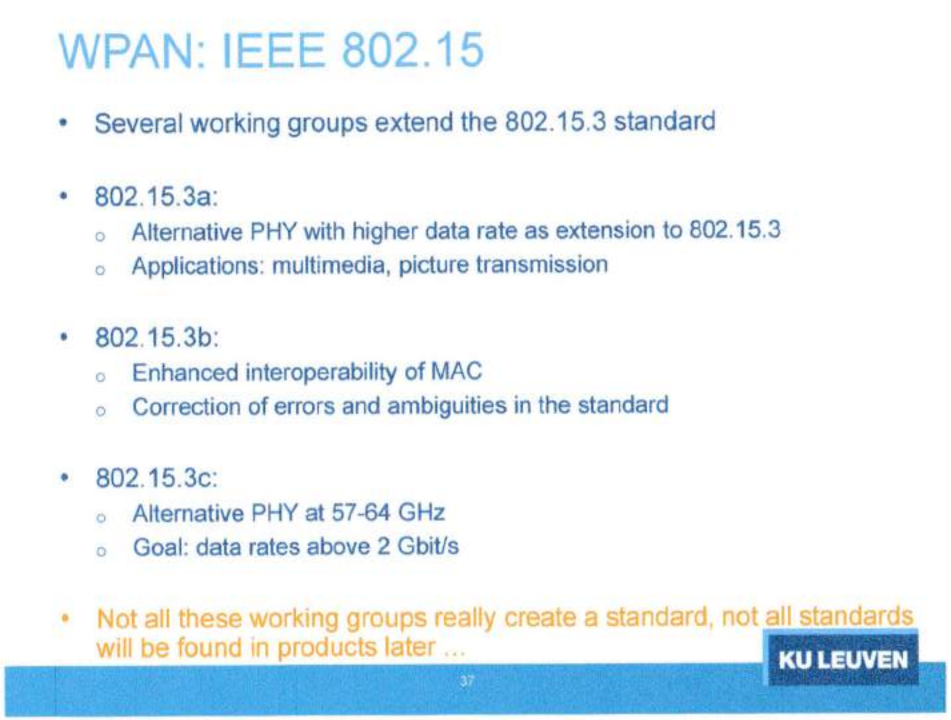
PHY + MAC

KU LEUVEN

WPAN: IEEE 802.15

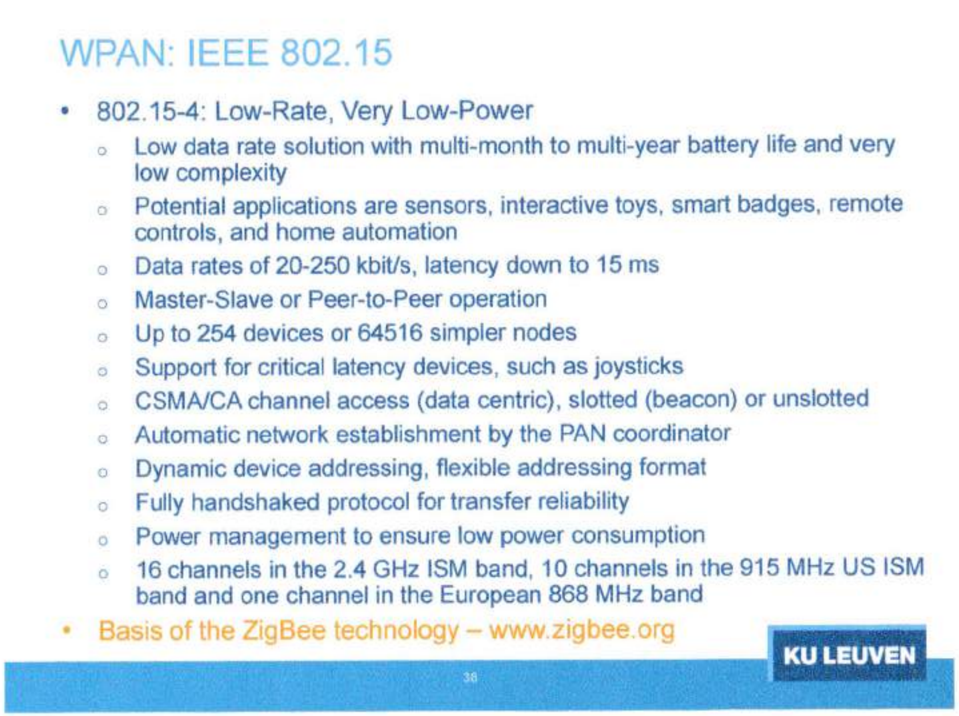
- 802.15 – 1 Bluetooth v1.1
- 802.15-2: Coexistance
  - Coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11), quantify the mutual interference
- 802.15-3: High-Rate
  - Standard for high-rate (20Mbit/s or greater) WPANs, while still low-power/low-cost
  - Data Rates: 11, 22, 33, 44, 55 Mbit/s
  - Quality of Service isochronous protocol
  - Ad hoc peer-to-peer networking
  - Security
  - Low power consumption
  - Low cost
  - Designed to meet the demanding requirements of portable consumer imaging and multimedia applications

KU LEUVEN



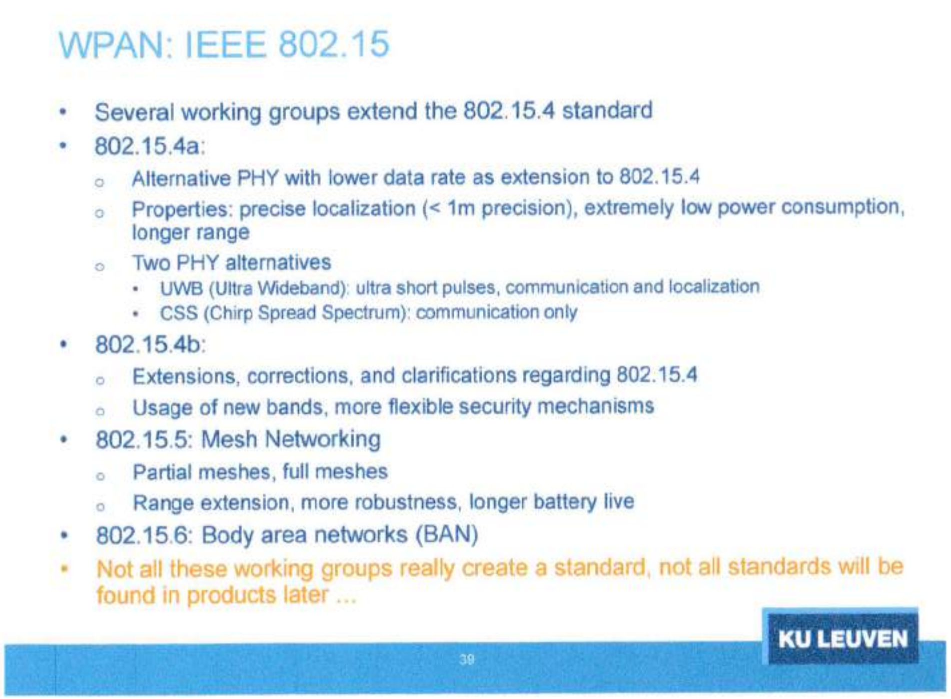
WPAN: IEEE 802.15

- Several working groups extend the 802.15.3 standard
- 802.15.3a:
  - Alternative PHY with higher data rate as extension to 802.15.3
  - Applications: multimedia, picture transmission
- 802.15.3b:
  - Enhanced interoperability of MAC
  - Correction of errors and ambiguities in the standard
- 802.15.3c:
  - Alternative PHY at 57-64 GHz
  - Goal: data rates above 2 Gbit/s
- Not all these working groups really create a standard, not all standards will be found in products later ...



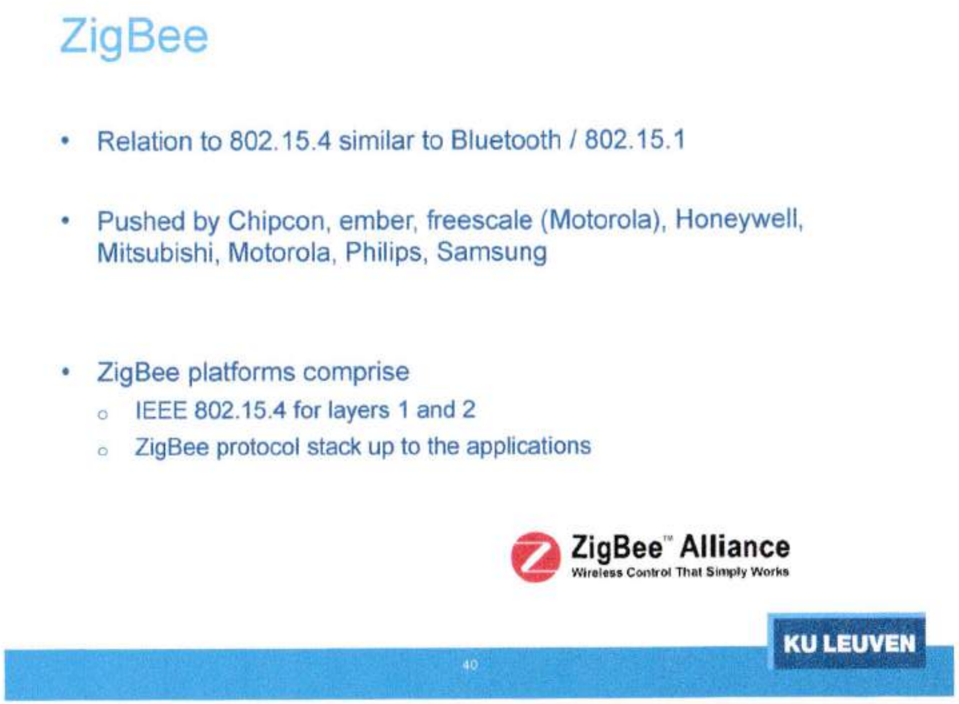
WPAN: IEEE 802.15

- 802.15-4: Low-Rate, Very Low-Power
  - Low data rate solution with multi-month to multi-year battery life and very low complexity
  - Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation
  - Data rates of 20-250 kbit/s, latency down to 15 ms
  - Master-Slave or Peer-to-Peer operation
  - Up to 254 devices or 64516 simpler nodes
  - Support for critical latency devices, such as joysticks
  - CSMA/CA channel access (data centric), slotted (beacon) or unslotted
  - Automatic network establishment by the PAN coordinator
  - Dynamic device addressing, flexible addressing format
  - Fully handshaked protocol for transfer reliability
  - Power management to ensure low power consumption
  - 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz US ISM band and one channel in the European 868 MHz band
- Basis of the ZigBee technology – www.zigbee.org



WPAN: IEEE 802.15

- Several working groups extend the 802.15.4 standard
- 802.15.4a:
  - Alternative PHY with lower data rate as extension to 802.15.4
  - Properties: precise localization (< 1m precision), extremely low power consumption, longer range
  - Two PHY alternatives
    - UWB (Ultra Wideband): ultra short pulses, communication and localization
    - CSS (Chirp Spread Spectrum): communication only
- 802.15.4b:
  - Extensions, corrections, and clarifications regarding 802.15.4
  - Usage of new bands, more flexible security mechanisms
- 802.15.5: Mesh Networking
  - Partial meshes, full meshes
  - Range extension, more robustness, longer battery live
- 802.15.6: Body area networks (BAN)
- Not all these working groups really create a standard, not all standards will be found in products later ...



ZigBee

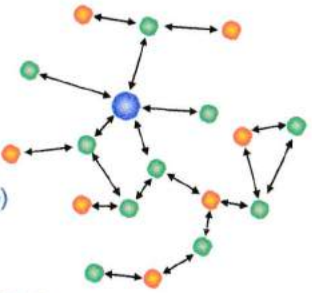
- Relation to 802.15.4 similar to Bluetooth / 802.15.1
- Pushed by Chipcon, ember, freescale (Motorola), Honeywell, Mitsubishi, Motorola, Philips, Samsung
- ZigBee platforms comprise
  - IEEE 802.15.4 for layers 1 and 2
  - ZigBee protocol stack up to the applications

Wireless sensor and control networks - WSN

- Application domains
  - Building and home automation
  - Industrial process automation
  - Energy and utility automation (smart metering)
  - RFID and logistics
  - Monitoring
- IEEE 802.15.4 PHY and MAC for low-rate WPAN
- Different technologies
  - IEEE 802.15.4 based
    - SP100.11 Wireless Systems for Automation by ISA
    - Wireless HART (Highway Addressable Remote Transducer) by HART organization
    - 6lowPAN (IPv6 over low-power personal-area network) by IETF
    - ZigBee by ZigBee Alliance
    - And others : e.g. Java programmable Sun SPOTS
  - Other
    - Z-wave
    - I/O home control

ZigBee - Applications

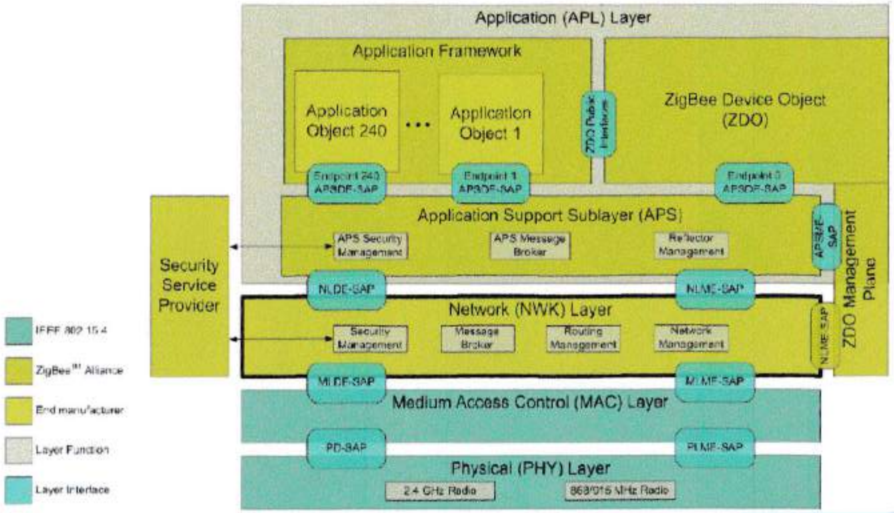
- Goal
  - Ultra low power - battery
  - Low cost/complexity
  - > Low range
  - > Low datarates (< 0.25 Mb/s)
  - > Multiple networktopologies (e.g. multihop)
  - > Flexibility
  - > ad hoc networking, self-organising



- Developed application profiles
  - Smart Energy
  - RF4CE: remote control for consumer electronics
  - Home automation
  - Commercial building automation
  - Personal, home and hospital care
  - Telecom applications

ZigBee - Applications

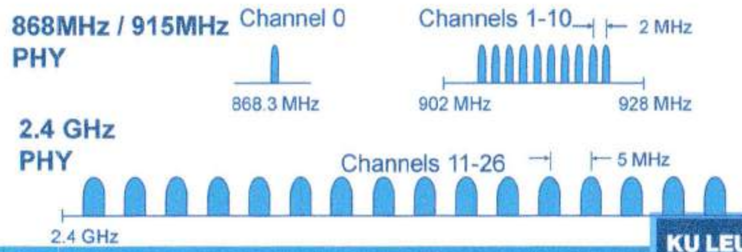
ZigBee – Protocolstack



ZigBee – Physical layer

- Physical Layer
  - ISM 2.4GHz band, 868 MHz/900 MHz
  - 27 channels
  - DSSS

Band [MHz]	Channel Number	Modulation	Bitrate [kbps]	Symbol rate [kSymb/s]	Symbool codering	Chip Rate
868	0	BPSK	20	20	Bin	300 kchip/s
915	1-10	BPSK	40	40	Bin	600 kchip/s
2400	11-26	O-QPSK	250	62.5	16-array O-QPSK	2 Mchip/s



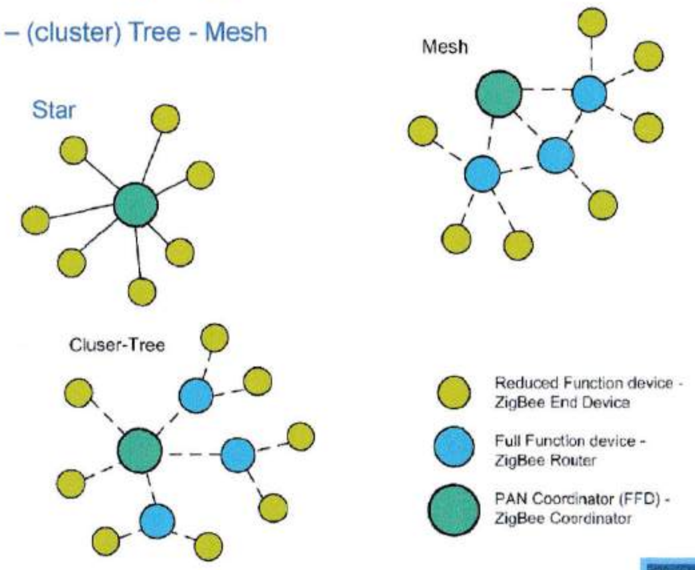
ZigBee – Devices

- IEEE802.15.4 specifies 2 types of devices
  - Full Function Device (FFD)
  - Reduced Function Device (RFD): e.g. cannot relay data
- In ZigBee
  - **Coordinator:** FFD for overall network management (network set-up, channel selection)
  - **Router** : FFD for routing in tree and mesh topologies
  - **End device**: RFD, low-power, always child of router or coordinator (parent)
  - ZigBee Trust Center
  - ZigBee Gateway
- Parents-childs
- Each node has a unique 64-bit IEEE address, ZigBee assigns a logical 16 bit address

ZigBee™ Alliance
Wireless Control That Simply Works

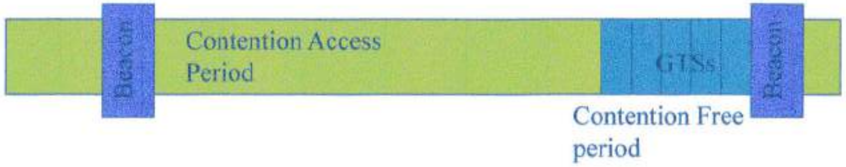
ZigBee - Topologies

- Star – (cluster) Tree - Mesh


Star
Mesh
Cluser-Tree
Reduced Function device - ZigBee End Device
Full Function device - ZigBee Router
PAN Coordinator (FFD) - ZigBee Coordinator

ZigBee - MAC

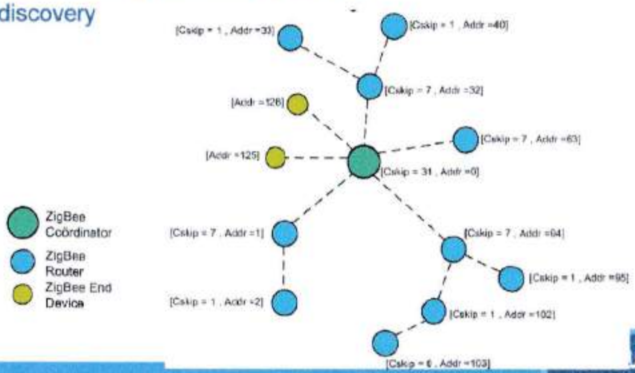
- CSMA/CA
- Beacons synchronization (beaconless mode possible)
- Structure of superframe



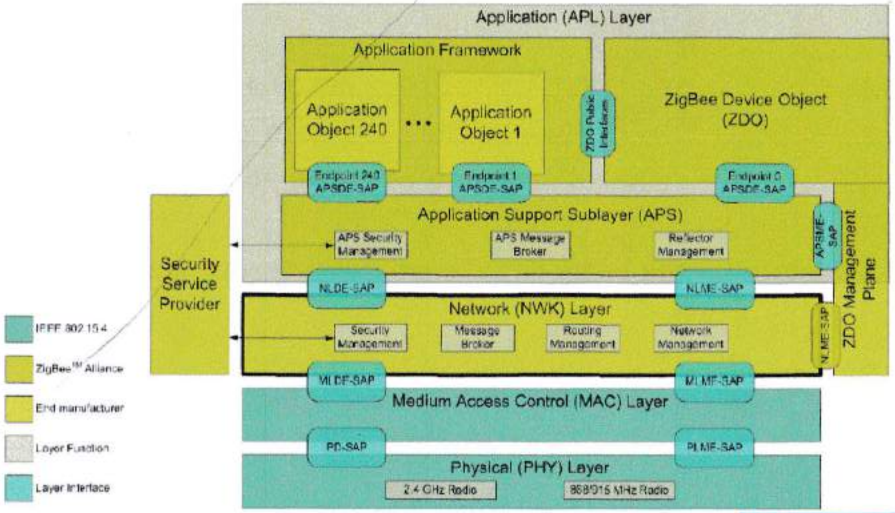
- Network devices send data frame in contention access period using CSMA-CA
- Reception confirmed with an acknowledge frame
- *Optional*: Guaranteed Timeslots (GTSs), integer multiple of timeslots (timeslot = 1/16 of time between two beacons), no CSMA-CA

ZigBee - Networklayer

- Networklayer
  - Starting a network from ZigBee coordinator
  - Managing devices joining and leaving the network
  - Assignment of addresses (Tree: distributed Cskip, ZigBee PRO: stochastic)
  - Route discovery, routing (different algorithms)
  - Neighbor discovery

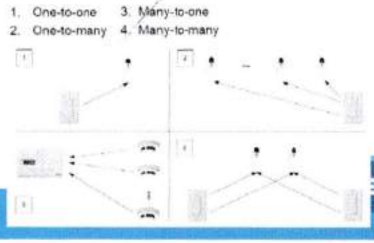


ZigBee – Protocolstack

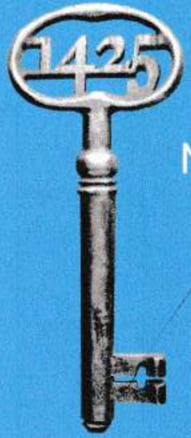


ZigBee - Application

- Application Layer
  - Application profile (public or private): collection of devices used in a certain application (e.g. Home Automation) and messages between those devices.
  - ZigBee Cluster Library : cluster is a collection of messages pertaining to a given functional domain (lighting, HVAC, ….). Clusters can be used in several application profiles.
  - Each device can have multiple Application Objects (Endpoints)
  - Applications Objects: defined by end-manufacturer, related to an application profile, defines the communication functions of a device
  - ZigBee Device Object (ZDO on endpoint 0) for management (security, network management, binding management, …)



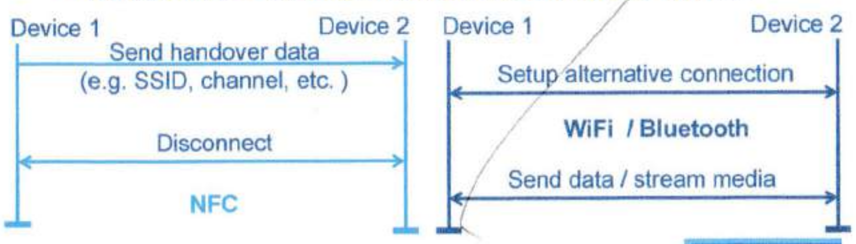
TECHNOLOGIECAMPUS GENT



Near Field Communication - NFC

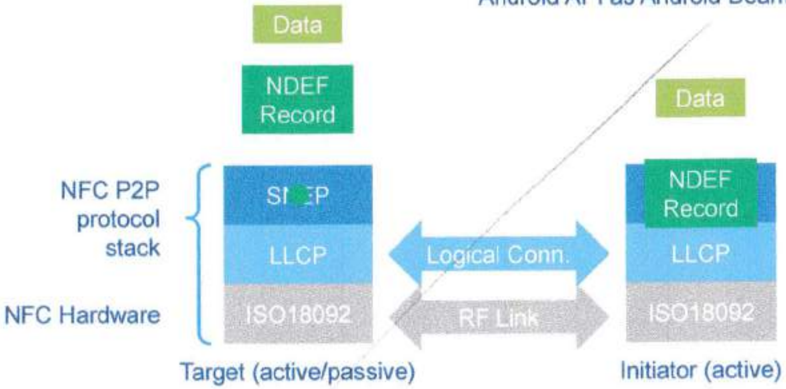
Modes of communication (2)

- Peer-to-peer mode (P2P)
  - Exchange of URL, business cards
  - Bidirectional half-duplex
  - Low data rate (424 kbits/s, raw)
    - Not suited for transferring large files or streaming media
    - Workaround = connection handover to Bluetooth, WiFi, …



NFC P2P communication mechanism

According to NFC Forum standard **BUT** Only partially implemented in current Android API as Android Beam



Expect only a few percents of the raw datarate
< 20 kbit/s @ 424 kbit/s [OvdB+14]

Future of NFC

- Currently used in public transportation
  - OV chipkaart (Netherlands)
  - Oyster card (London Metro)
  - Tickets stored on smart-phone
    - London [Cla12] and Paris [Hea11]

- 46% of all smartphones will support NFC by 2016
- 13% of the US and Western Europe citizens will use smartphone as a ticket [The12]

- What will Apple do?

Some references

- *Books :*
  - *Mobile Communications*, J. Schiller, Pearson
  - *Next Generation Wireless LANs*, E. Perahia, R. Stacey, Cambridge
  - *ZigBee Wireless Sensor and Control Network*, A. Elahi, A. Geschwender, Prentice Hall
  - *801.11 Wireless Networks, the definitive guide*, M.S. Gast, O'Reilly
  - *Fundamentals of WiMAX*,J.G. Andrews, A. Ghosh, R. Muhamed, Prentice Hall
  - Wireless Communications and networks, W. Stallings, Pearson
  - Bluetooth operation and use, R. Morrow, McGraw-Hill
  - Computer Networking, J.F. Kurose, K.W. Ross, Pearson
  - CDMA, Principles of Spread Spectrum Communication, A.J. Viterbi, Addison-Wesley
- Websites :
  - www.ieee802.org/11
  - www.ieee802.org/15
  - www.wi-fi.org
  - www.bluetooth.org
  - www.zigbee.org
  - www.wimaxforum.org

References

[OvdB+14] Geoffrey Ottoy, Sam Van Den Berge, Jean-Pierre Goemaere, Lieven De Strycker, Measuring the NFC Peer-to-Peer Data Rate, (2014). In Lecture Notes in Electrical Engineering 302, Proceedings of ECUMICT 2014, pp 109-122

[Cla12] S. Clark, Paris commuters to get travel passes that work with NFC phones, (2012). Online: http://www.nfcworld.com/2012/01/30/312832/paris-commuters-to-get-travel-passes-that-work-with-nfc-phones/

[Hea11] Heather McLean, Transport for London to accept NFC payments from 2012, (2011). Online: http://www.nfcworld.com/2011/07/12/38537/transport-for-london-to-accept-nfc-payments-from-2012/

[The13] The Point of Sale News, Where Is NFC Going? New Reports Forecast Growth, (2012). Online: http://pointofsale.com/20120319953/Mobile-POS-News/where-is-nfc-going-new-reports-forecast-growth.html (date consulted October 10, 2013)

Standards (1)

- ISO/IEC 14443-1:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics
- ISO/IEC 14443-2:2010 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface
- ISO/IEC 14443-3:2011 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision
- ISO/IEC 14443-4:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol
- ISO/IEC 18092:2013 Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)

Standards (2)

- NFC Forum. NFC Digital Protocol Technical Specification (2010)
- NFC Forum. Logical Link Control Protocol Technical Specification (2011)
- NFC Forum. Simple NDEF Exchange Protocol Technical Specification (2011)
- NFC Forum. NFC Data Exchange Format (NDEF) Technical Specification. (2006)