WIRELESS NETWORKS & EMBEDDED SYSTEMS — INDEX (INITIAL PARTS)

LECTURE 1 / INTRO TO THE COURSE

- INTERNET (What? Based on which technologies? files?)
- IoT (Model 4 pillars, components? internet)
- Embedded systems (What? Importance?)
- TLC NETWORK VS TLC SERVICE (What? Differences? Usage?)
  - Classification of TLC networks (Types of NETworks)
- MAIN STANDARDIZATION BODIES (Responsibilities, main Technologies & Contributions of them) = DEU main lessons
- TRANSMISSION MEDIA (Different types of them? Differences? Types of invisible media)
- MAC TECHNIQUES (What for? Usage?)
  - DUPLEXING (What is it? Technique? Types of DUPLEXING? Good?)
  - MULTIPLEXING (What? What for?)
    - MULTIPLE ACCESS
    - "DOMAINS" for MULTIPLEXING?
      - EQUALIZE
      - CDMA
    - DFT, CFT, INVERSE F.T.
- PHY VS MAC LAYER (Responsibilities, functionings)

LECTURE 2 – PHYSICAL LAYER

- ANALOG DATA (What? What for? Examples?)
- DIGITAL DATA (What? Purpose? Examples? Advantages? Disadvantages?)
- ANALOG | DIGITAL (A/D) CONVERSION STEPS
  - SAMPLING PROCESS (What? What for? Functioning?)
    - MINIMUM SAMPLING RATE | NYQUIST THEOREM
  - QUANTIZATION (What? Functioning?)
    - # QUANTIZATION LEVELS? (Consequences? Impact on signal quality?)
  - ENCODING (What? Encoding types? NRZ?)
    - PCM
    - PAM
- ELECTROMAGNETIC SIGNAL (What?)
  - Mono signal?
  - DOMAINS
    - TIME ↔ FREQUENCY
    - TRANSMISSION / MODULATION
  - TIME-DOMAIN CONCEPTS (What? Draw on paper!)
    - PERIODIC SIGNAL
      - (PEAK) AMPLITUDE (A)
      - FREQUENCY (f)
      - PERIOD (T)
      - PHASE (φ)
      - WAVELENGTH (λ)
  - FOURIER TRANSFORM
  - FOURIER SERIES
  - FREQUENCY-DOMAIN CONCEPTS
    - Fundamental frequency
    - SPECTRUM
    - BANDWIDTH
- POWER
- ENERGY

- DATA RATE VS BANDWIDTH
  - [RELATION (NYQUIST)]
- ANALOG VS DIGITAL TRANSMISSION
  - (Differences, devices used, benefits)
  - WHAT IS MODULATION / DEMODULATION?
- **ANALOG TRANSMISSION & MODULATION**
  - ANALOG MODULATION (What? Functioning? Steps?)
    - VS ANALOG TRANSMISSION
  - ENCODING TECHNIQUES for ANALOG TRANSMISSION
    - AMPLITUDE MODULATION + DSB-TC
      - (Functioning? What is modulated? Applications? Range?)
      - Transmitted power
    - PHASE MODULATION
      - ~~Angle Modulation (What gets modulated?)~~
      - Phase Modulation
        - ~~Instantaneous~~ frequency
    - FREQUENCY MODULATION
      - (What? What gets modulated?)
      - INSTANTANEOUS FREQUENCY
  - ANALOG MODULATIONS' COMPARISON (Advantages & different techniques)
- **DIGITAL TRANSMISSION & MODULATION**
  - DEMODULATION / DETECTION
  - DIGITAL MODULATION (What?

ANGLE MODULATION

DIGITAL

↳ ENCODING TECHNIQUES
(What does it consist of?)

↳ PULSE AMPLITUDE MODULATION (PAM)
AMPLITUDE-SHIFT KEYING (What gets modulated? Limitations?)
↳ (MPAM) M-ary Pulse Amplitude Modulations
BAUD = SYMBOL RATE = BIT RATE

↳ PHASE-SHIFT KEYING (PSK)
(Ex: BPSK) (What gets modulated?)
BPSK
↳ MPSK, M-ARY PHASE-SHIFT KEYING (Energy efficiency? What varies?)
DPSK

↳ QUADRATURE-AMPLITUDE MODULATION (QAM)
(What gets modulated? Functionality?)
↳ spectral efficiency

↳ MULTIPLE FREQUENCY-SHIFT KEYING (MFSK)
(# frequencies used | duration & output signal's element)
Functionality?
↳ BFSK
↳ MSK
↳ DFSK
↳ Bandwidth required?
↳ Minimum frequency separation?

↳ COMPARISON OF DIGITAL MODULATION TECHNIQUES
(Criteria. Which are ignored?)

ANALOG Can't Draw DIGITAL!

LECTURE 3 - PHYSICAL LAYER (II)

PROPAGATION MODES

- GROUND-WAVE PROPAGATION
  (How are waves propagated? Generated when? How?)
- SKY-WAVE PROPAGATION
  (How does propagation occur?)
  - over the seas
  - REFLECTION (What?) (CAN & REFLECTION)
  - REFRACTION (What?)
    - SNELL'S LAW
  - DIFFUSION (Occurring when? What is it?)
    - SCATTERING
  - ABSORPTION (What?)
- LOS PROPAGATION:
  (How does LOS work. occur?)

WIRELESS TRANSMISSION IMPAIRMENTS

- LARGE-SCALE PROPAGATION IMPAIRMENTS
  (What are? Occurring when?)
  - ATMOSPHERIC ABSORPTION
    (Importing wireless frequencies TLC Services? (in dB))
  - THERMAL NOISE (in 1 Hz vs B Hz)
    (Caused by what? Relevant for what? Dependent on frequency?)
  - SNR (Signal/Noise Ratio)
    (definition)

- AWGN NOISE (What?)
- ATTENUATION ISSUES (Attenuation dependent on what? What does it affect? (definition?))
- ANTENNAS (What for?)
  - (ISOTROPIC)
  - OMNIDIRECTIONAL ANTENNA
    - Model for FREE-SPACE PATH LOSS
    - ANTENNA GAIN
  - (NON-ISOTROPIC ANTENNA)
    - Model for free-space
  - PARABOLA PATH LOSS (FRIIS Law)
    - ANTENNA GAIN
  - [Usage? Application?] HALF-WAVE DIPOLE
  - QUARTER-WAVE DIPOLE
- PROPAGATION EFFECTS (What does it do?)
  - REFLECTION (What?)
  - DIFFRACTION (What?)
  - SCATTERING (Caused by what?)
- TWO-RAY TRANSMISSION (What does it consist of?)
  - RAY TRACING (What? For [multipath signal] what?)
    - 4TEN-RAY TRACING
      - GENERAL RAY TRACING (What do we model?)

PATH LOSS MODEL → BER per Bit
↳ BER per Symbol
↳ INDOOR ATTENUATION FACTORS
↳ PATH LOSS MODEL ✗✗✗ Formula? Explanation?
↳ SHADOWING / FADING ✗ (model?) ✗
↳ Time-variant vs space-variant
↳ DIGITAL MODULATION DETECTION & CHANNEL CAPACITY:
↳ DEFINITIONS & NOISE
↳ DATA BIT RATE
↳ BANDWIDTH
↳ RECEIVED SNR
↳ BIT-ERROR RATE (SNR per bit ✗✗ SNR per symbol ✗)
↳ NYQUIST BANDWIDTH (& NYQUIST THEOREM) (What does it say?)
↳ BINARY SIGNAL
↳ MULTI-LEVEL SIGNAL (M-ARY)
↳ SHANNON'S CAPACITY (& SHANNON'S THEOREM) (What? How much?) ✗✗✗
Example & NYQUIST / SHANNON'S THEOREM APPLICATION ✓ ✗

LECTURE 4 - CELLULAR NETWORKS

CELLULAR NETWORK ORGANIZATION

- WIRELESS CELLULAR NETWORK (What? What for?)
- COMPONENTS & a CELLULAR NETWORK (Device entities make up into) architecture?
  - FUNCTIONS of a CELL & MTSO & Handle
  - CELL COVERAGE'S SHAPE (What? How much? Motivation?) OMNIDIRECTIONAL VS SECTORIZED
  - CHANNEL REUSE (Strategies? How to allow multiple channels?)
    - ERLANG-B FORMULA (meaning?)
    - LITTLE'S FORMULA
    - CLUSTER & CAPACITY ISSUE
      - (# Channels in/for cells)
      - APPLICATION & USAGE (frequency reuse)
    - INTERFERENCE EFFECTS (What? How to address?)
      - INTRA-CELL INTERFERENCE (What? Reasons?)
      - INTER-CELL INTERFERENCE (SINR? What?)
  - CELL SIZE (How large? Types of cells?)
    - CELL SECTORING (What? Functioning? How?)
    - CELL SPLITTING (What & how?)
    - CELL FREQUENCY RE-USE (How?)

CENTER-EXCITED CELL

EDGE-EXCITED CELL

SIR

REUSE DISTANCE

- CALL ESTABLISHMENT PROCESS
  (Achieved how? 6 STEPS to make call)

EVOLUTION of CELLULAR NETWORKS

- 1G - First Generation (characteristics)
  - Battery duration estimation
    - calculation
  - MAN STANDARDS
    - NMT (frequency bands, years, range, security)
    - AMPS (frequency bands, security)
    - TACS (usage where)
- 2G - Second Generation
  - Main 2G Standards (EU, Japan, USA) → Multiple times
    - Features & 2G → Advantages
      - GSM → NOKIA → MOTOROLA
      - (Standardized by whom)
    - IS-136 D-AMPS (characteristics)
    - PDC
    - Uplink band
    - Downlink band (Signaling band)
- 2.5G (Upgrade rates followed)
  - EU, Japan, US
  - HSCSD (Functioning, Data rate)
  - GPRS (" , architecture, modulation) → Data rate
- 2.75G : EDGE

- IS-95B / CDMA one / data rates / Functionality
- 3G – (Standardization by whom?)
  - EU vs US
    - (WCDMA) ✓
    - (CDMA 2000) ✓
      - 1×EV
      - 3×
      - 2FA
      - version
  - Characteristics
  - Frequencies
  - Channel width
  - Data rates
    - required data rate (up to)
    - new SW / HW needed
  - 3G TD-SCDMA [China]
    - (Where? Functionality)
  - LIMITATIONS ✓
- 4G – (Standardization where? When?)
  - OBJECTIVES (QoS) ✓
    - Data rate ✓
  - PURPOSE (Introduced why?) ✓
    - CONVERGENCE & NETWORK STRUCTURE
  - NETWORKS ✓ NETWORKS via 4G ✓
  - APPLICATIONS

LECTURE 5 | 6 – 4G | 5G ✓

- 4G – LTE:
  - Bandwidth ✓
  - Latency ✓
  - Coding ✓ + Modulation ✓ & ×
  - TECHNICAL ENHANCEMENTS over 3G
  - MOTIVATION for 4G → TRAFFIC (LTE supports)
  - LTE KEY FEATURES & REQUIREMENTS ✓
    - UPLINK
    - DOWNLINK
    - (Data rate, Capacity, transmitter)
    - channel use
    - modulation
    - DUPLEXING
    - MAC used

OFDM vs OFDMA
(Each one used when? Where?)
- Modulation
- Coding
- Frequency Domain Equalization
- Multi-path channel
- SC-FDMA (What? Why vs OFDMA?)
- Downlink vs Uplink (Make use of which mechanism?)
- 3G vs Network Architecture
- Network Architecture in 4G (Which elements? What for?)
  - Heterogeneous network
- Protocol stack in LTE?

SELF-ORGANIZING NETWORK
(Where? Layer? Functioning?)
- Goal?
- Standardization (different releases)
- Architecture?
  - distributed
  - centralized
  - hybrid

5G – 5th Generation Network
- Performance goals (What targets to achieve?)
- Frequencies?
- Technological aspects (Main features?)
- 4G -> 5G migration strategies
  - ~~Protocol stack~~
- Main application fields
  - & network slicing
- Standardization level? By whom?
- Health concerns & 5G?

LECTURE 7 – C-ITS

ITS – Intelligent Transport Systems
(What is it? What for?)

↳ KETs (Key Enabling Technologies)
(Which technologies are required for C-ITS?)

↳ EC INITIATIVES for C-ITS

↳ STANDARDS / Normation?
(Open VS vertical implementation)

↳ (EU) NORM (What is it?)
(What? Different norms at different levels)

Harmonized standards

NORM VS STANDARD
(Differences? What for)

↳ STANDARD
(International → EU → National)
↳ STANDARDIZATION PROCESS

↳ ITS STANDARDS
(Walls? EU?)

↳ Spectrum allocation for ITS?

↳ ETSI (Tenors for?)
(Responsibilities & role?)

ARCHITECTURE for INTEROPERABILITY

MINIMUM STANDARDS for INTEROPERABILITY?

↳ APPLICATIONS of C-ITS?

↳ DAY 1 SERVICES?

↳ DAY 1.5 SERVICES?

↳ GEONETWORKING?
(What is it?)

LECTURE 8 – Wi Fi

- Wi Fi (What is it? What for?)
  - (Widespreadness)
  - Wireless Technologies
    - (Main IEEE 802.11 types & Data Rate)
  - WLAN Requirements & effective Modes
  - WLAN Applications
    - Nomadic access
    - Ad-hoc networking
  - ARCHITECTURE TERMINOLOGY
    - MPDU
    - MSDU
    - BSS
    - ESS
  - IEEE 802 PROTOCOL LAYERS
    - (Which layers does it make up?)
    - Interaction with Ethernet (IEEE 802.3)
      - Modulation?
      - PHY Layer in IEEE 802.11 – original standard
        - DSSS [Direct Sequence Spread Spectrum]
          - (What is it? Purpose?)
        - FHSS [Frequency Hopping Spread Spectrum]
          - (What for? Functioning?)
        - OFDM
          - (Wide-band VS Narrow-band)
          - ISI, Orthogonality
    - MAC Layer in IEEE 802.11
      - Collision resolution in Wi-F.
        - IFS for PRIORITY
          - (Which ones?)
        - DCF / PCF

- DCF - Distributed Coordination Function
- PCF - Point Coordination Function
- FURTHER MAC FEATURES & FUNCTIONALITIES
- MOBILITY in Wi-Fi (IEEE 802.11p)
  - Data rate, CHANNEL WIDTH supported, PHY, frequency used ranges
  - MAC layer → WBSS (What?)
  - VRR
  - IEEE 802.11bd → frequency?
    - DSRC (What in NR? Deployment?)
    - C-V2X (What in NR?)
    - REQUIREMENTS (What can have deployment by IEEE 802.11bd)
    - FEATURES supported

LECTURE 9 - SECURITY in IoT

- CONCEPT & SECURITY (currently in IoT)
  - ATTACKER'S perspective
  - DEFENDER'S perspective
    - FAVOURITE ATTACK TARGETS?
- SECURITY REQUIREMENTS in IoT ENVIRONMENTS
  (What do we need in IoT to have a secure deployment?)

- MAIN ATTACKS OF (What gets exploited? How? Where?)
  - INFORMATION LAYER ✓
  - CONNECTIVITY LAYER ✗
  - APPLICATION LAYER ✓
- MAIN REASONS for the OCCURRENCE of SECURITY BREACHES (At different levels, many risks?)
  - Ex: Man-in-the-middle ✓
  - SYBIL ATTACK ✓
- SECURITY LEVEL of an APPLICATION (Determined how?)
  - SECURITY MECHANISMS
    - AUTHENTICATION (Main ones?)
- IDS - Intrusion Detection System (Based on what? What for?)
- IPS - Intrusion Prevention System (Based on what? What for?)
- FUTURE IoT SECURITY
  - (Challenges inter IoT devices)
    - Remote authentication?
    - Remote attestation?
- ATTACKS considered in TESTS

LECTURE NO - VLC (Visible Light Communication)

↳ VLC - IEEE 802.15.7
(What? Reasons for introduction?)

↳ CHARACTERISTICS
(Frequency, power, λ, security)

↳ VLC APPLICATIONS
(Benefits, drawbacks VS RF)

↳ PRINCIPLES & VLC

↳ TX / RX COMPONENTS
(Where are TX/RX? Physics' principles?)

↳ MOTIVATION(S) for VLC?

↳ INITIATIVES over the globe?
(Ex: Li-Fi, IrDa systems)
(Data rate? Functioning?)

↳ MODULATION in VLC
Issues, functioning

↳ Modulation schemes for DIMMING?

~~PWM~~ ~~PPM~~

↳ OOK

↳ VPPM (PWM, PPM)

↳ CSK (Color-Shift Keying)

IEEE 802.15.7 STANDARD (Data rate, PDU)

↳ MAC

↳ PHY (Need for? Functioning?)

& FEC

↳ REED-SOLOMON CODING
(How it operate it?)

& FEC

IDEA:
Reed
BINARIZATION

↳ REED-SOLOMON CODING [SYNDROME PROPERTY]

↳ REED-SOLOMON DECODING

↳ VLC in ITS

(Usage how? Where? What for?)

↳ PHY as prototypes?

↳ EXISTING ISSUES?

↳ OPEN ISSUES & RESEARCH DIRECTIONS in the field

WIRELESS NETWORKS & EMBEDDED SYSTEMS

LECTURE 1-2

PLATFORMS for SENSORS' NETWORKS.

Environment existing & its own SW stack for solution.

Dr. Paolo Pagano's research: Acquire, analyze data from vehicular network in the area & Livorno to bring benefits to commuters and the local population.

Ex. RSUs, Road-Side Units.

31.8 GHz - 33.4 GHz spectrum. Used for extremely short-range communications.

ITU-T: Sets standards.
ITU-R: Allocates the actual spectrum.

4G vs 5G

NSA: Non-Stand Alone architecture. Leverage existing architecture

(NO BW. COMPATIBILITY)

SA: Standalone architecture (backwards compatibility with 4G equipment is maintained)

FREQUENCY RANGES

0 - 1 GHz: Omnidirectional (3G, 4G)

1 - 40 GHz: Directional with BEAM-FORMING

> 40 GHz: Infrared (LEDs) to light create signals in light.

NB: The higher the frequency, the more directional is the signal & the faster the signal fades

IMSN:

MAXWELL'S EQUATIONS:

Set of PARTIAL DIFFERENTIAL EQUATIONS that, together with LORENTZ FORCE LAW, form the FOUNDATION of CLASSICAL ELECTRODYNAMICS

LORENTZ FORCE LAW explains the force experienced by a particle with a charge q moving with a velocity v in an electric field E and a magnetic field B as:

$$F = q \cdot E + q \cdot v \cdot B$$

⟹ MATHEMATICAL MODEL for electric, optical, and radio technologies (e.g.: wireless telecommunications, lenses, radars, ...)

(MAXWELL'S EQUATIONS)

- they describe how ELECTRIC and MAGNETIC fields are generated by CHARGES, CURRENTS, and changes of the fields. [light is an ELECTROMAGNETIC PHENOMENON!]

∇ = 3-D GRADIENT OPERATOR

(GAUSS'S FLUX THEOREM)

- GAUSS' S LAW:

Relates the distribution of electric charge to the resulting electric field

$$\nabla \cdot E = \frac{\rho}{\varepsilon_0}$$

E: ELECTRIC FIELD; ρ: ELECTRIC CHARGE DENSITY; ε₀: DIELECTRIC CONSTANT (of free space)

- GAUSS'S LAW for MAGNETISM:

"The magnetic field has DIVERGENCE equal to 0"

$$\nabla \cdot B = 0$$

B: MAGNETIC FIELD

(i.e.: it is a SOLENOIDAL VECTOR FIELD) ⇒ Magnetic monopoles do not exist, only magnetic dipoles

- MAXWELL - FARADAY EQUATION

(Faraday's law of induction)

$$\nabla \times E = -\frac{\partial B}{\partial t}$$

(MAGNETIC FIELD; ELECTRIC FIELD)

Predicts how a magnetic field will interact with an electric circuit to produce an ELECTROMOTIVE FORCE (EMF), which is also known as ELECTROMAGNETIC INDUCTION.

⇒ "A spatially-varying/time-varying electric field always accompanies a time-varying magnetic field."

- AMPERE'S CIRCUITAL LAW

$$\nabla B = \mu_0 \left(\quad + \varepsilon_0 \cdot \frac{\partial E}{\partial t} \right)$$

Relates the integrated magnetic field around a CLOSED LOOP to the electric current passing through the loop.

NFC: Near-Field Communication
(Low-frequency 13.56 MHz, Max. transm. rate 424 kbit/s)
Used for contactless cards/RFIDs.
(4 cms range or less)

HERTZ: Experimentally proved Maxwell's equations

MARCONI: Tested the early (WIRELESS) radio apparatus in 1895 (antenna)

2012: 95% of world's population covered by 2G+ networks.

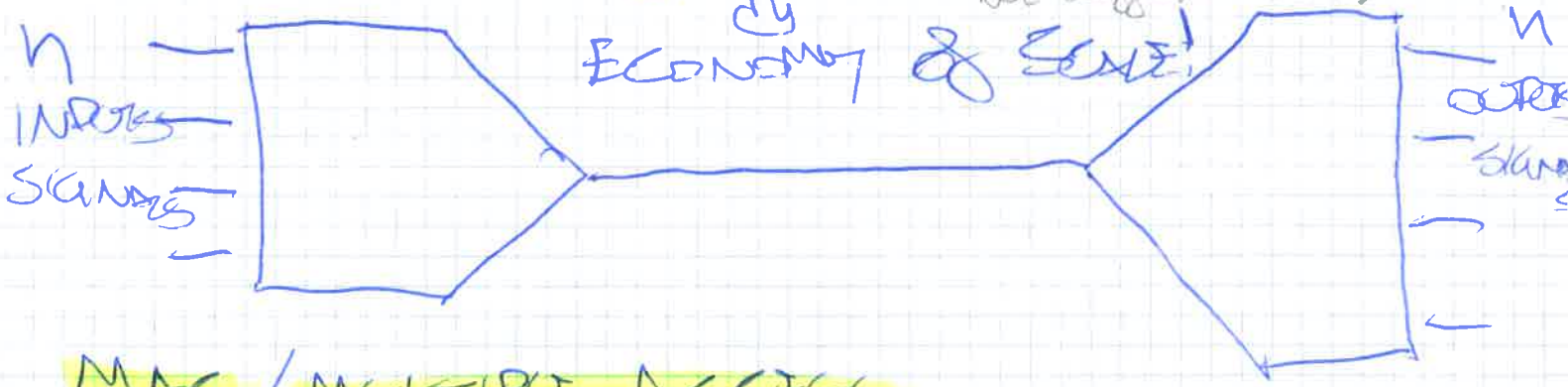
2020: Begin of 5G's technology commercialization.

DUPLEXING: Capacity of a device to receive & transmit simultaneously [Ex: Part of spectrum used]

↳ FULL DUPLEX: Both RX & TX at the same time.

↳ SINGLE DUPLEX: Can either RX or TX at a certain point in time.

MULTIPLEXING: Capacity of a device to ~~~~ accomodate multiple SIGNALS/and users on a single medium at the same time | at different times



MAC / MULTIPLE ACCESS TECHNIQUES

Methods that determine how a medium is accessed such that the channel is shared among multiple users' data traffic.

TECHNIQUES & MULTIPLEXING.

- TDM. (Ex: Tennis court booking).
Divide the time into slots and assign each slot to a user in a ROUND-ROBIN fashion.

Every user in their slot can transmit

- FDM: Frequency Division Multiplexing
Divide SPECTRUM into smaller frequency channels, then assign user channel to a USER.

↳ LEVERAGES

FOURIER TRANSFORM

- PERIODIC SIGNAL. The spectrum consists of discrete frequency components repeated in time, centered at the fundamental frequency and its HARMONICS.

- APERIODIC SIGNAL. The spectrum consists of a continuum of frequencies.

↳ Spectrum can be defined by the FOURIER TRANSFORM (i.e. transform to the FREQUENCY DOMAIN)

For a signal $x(t)$ with a spectrum $X(f)$, the following relationships hold:

CONTINUOUS FOURIER TRANSFORM

$$x(t) = \int_{-\infty}^{+\infty} X(f)\, e^{j2\pi f t}\, df$$

COMPLEX PART

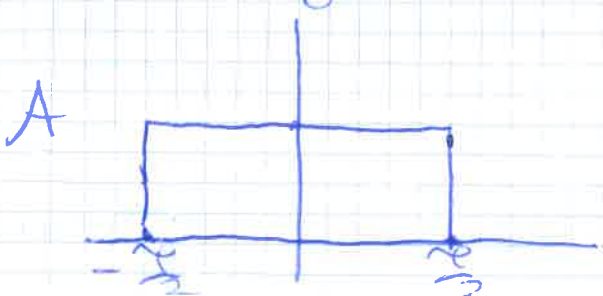
INVERSE FOURIER TRANSFORM

$$X(f) = \int_{-\infty}^{+\infty} x(t)\, e^{-j2\pi f t}\, dt$$

DISCRETE FOURIER TRANSFORM

$$X_k = \sum_{n=0}^{N-1} x_n \cdot e^{-\frac{i 2\pi}{N} kn}$$

EXAMPLE: $x(t)$ RECT function $\xrightarrow{FT}$ $X(f)$



$$A\tau \cdot \frac{\sin(\pi f \tau)}{\pi f \tau}$$

- SDM: Space Division Multiplexing. Use directional antennas to leverage different directions in SPACE for transmission.

- TDMA: Time Division Multiple Access. Requires ADAPTIVE EQUALIZATION due to high transmission rates.
  - EQUALIZER: Filter used for SPECTRAL SHAPING of a SIGNAL's Response.
    - adaptive filter
  - ADAPTIVE EQUALIZER: Equalizer endowed with some "intelligence", which can establish their own RESPONSE CURVE based on on-going real-time measurements.
    - Adaptively compensate for the dispersion of signals on a COMMUNICATION CHANNEL
    - [Ex: Use coherent modulations, such as PSK, and mitigate the effects of multipath propagation and Doppler spreading]
- CDMA: Code Division Multiple Access. Downlinks may be based on ORTHOGONAL SPREADING CODES, such as Walsh-Hadamard.
  - Error correcting code & ERROR DETECTION & CORRECTION used when transmitting over noisy & unreliable V.

SIGNALS & ATTENUATION, ANTENNA, TRASMISSION

ANALOG SIGNAL: Signal where the signal intensity varies in a broader (continuous) fashion.

DIGITAL SIGNAL: Signal where the signal intensity maintains a constant level for some time, then changes to another constant level.

SIGNAL: Electric & electromagnetic representation of data.

MODEM: Converts binary voltage pulses into an analog signal by modulating a carrier frequency (Ex: Data over PSTN)

CODEC: Represent analog data over digital signals (Ex: Video CODING/DECODING)

ATTENUATION: It represents the main source of signal loss & quality degradation

$$L = 10 \cdot \log_{10} \left(\frac{4\pi d}{\lambda} \right)^2 \; dB$$

~~$\frac{4\pi d}{\lambda}$~~

→ SIGNAL Loss varies as the square of DISTANCE.

NB: Attenuation is increased with RAINFALL (especially above 10 GHz)

FOR GUIDED MEDIA loss varies exponentially with DISTANCE (linearly with dB).

Longer λ => Less attenuation
(least impact by OBSTACLES)

GAIN: It is expressed as a RATIO in decibels between Pout & Pin.

$$G_{dB} = 10 \cdot \log_{10} \frac{P_{out}}{P_{in}}$$

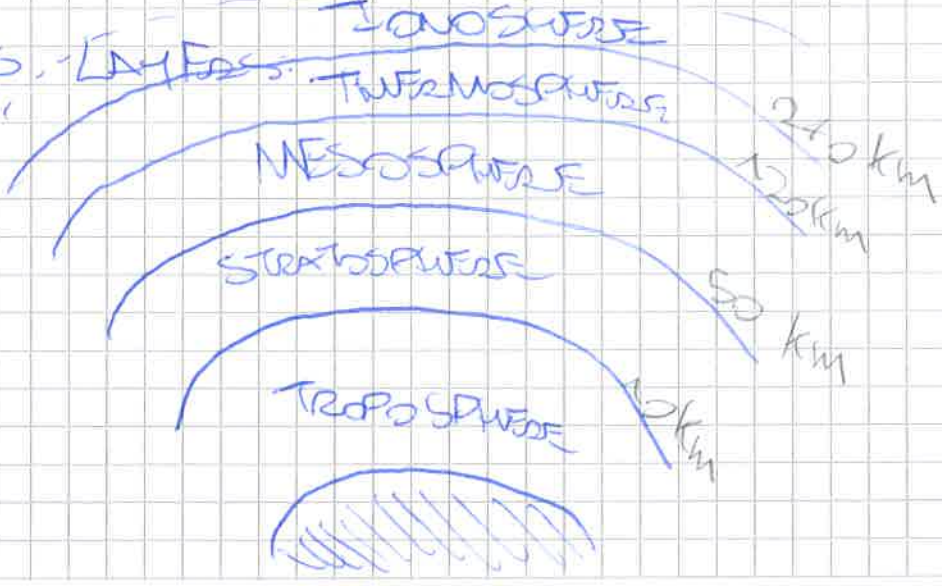
ANTENNA: Electrical conductor system, or system of CONDUCTORS. It is used either for radiating electromagnetic energy (TX) or for collecting electromagnetic energy (RX).

↳ TRANSMISSION: RF-electrical energy from the transmitter converted into electromagnetic energy by the antenna.

↳ RECEPTION: Electromagnetic energy incoming to the antenna converted into RF electrical energy and fed into receiver

TX: RF -> EM

Rx: EM -> RF



LECTURE 3 – PROPAGATION EFF

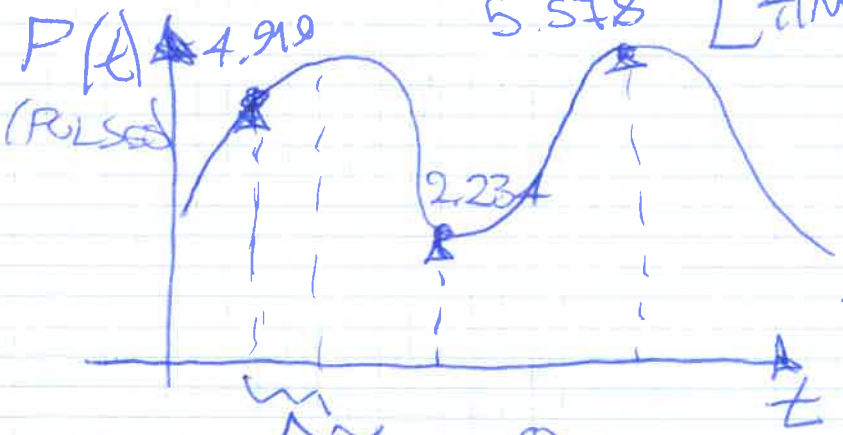
PROPAGATION EFFECTS

All the real-world PHENOMENA (OBSERVABLE) are ANALOG, but they can possibly converted to DIGITAL format.

ANALOG SIGNAL → DIGITAL SIGNAL

It involves three steps:

1. SAMPLING: Convert continuous-time signals into discrete-time signals.



[TIME → horizontal axis]

PARAMETER: Sampling rate. The higher the more accurate the representation.

PAM: Pulse Amplitude Modulation.
Sample pulses from the signal over the amplitude component.

NYQUIST THEOREM: Describes the minimum sampling rate that should be used to avoid LOSS as: (Because of a given bandwidth (B) the highest signal rate that can be carried is 2B)

$$S = 2 \cdot f_{MAX}$$

SAMPLING RATE (Hz) — Max. frequency component of the SIGNAL

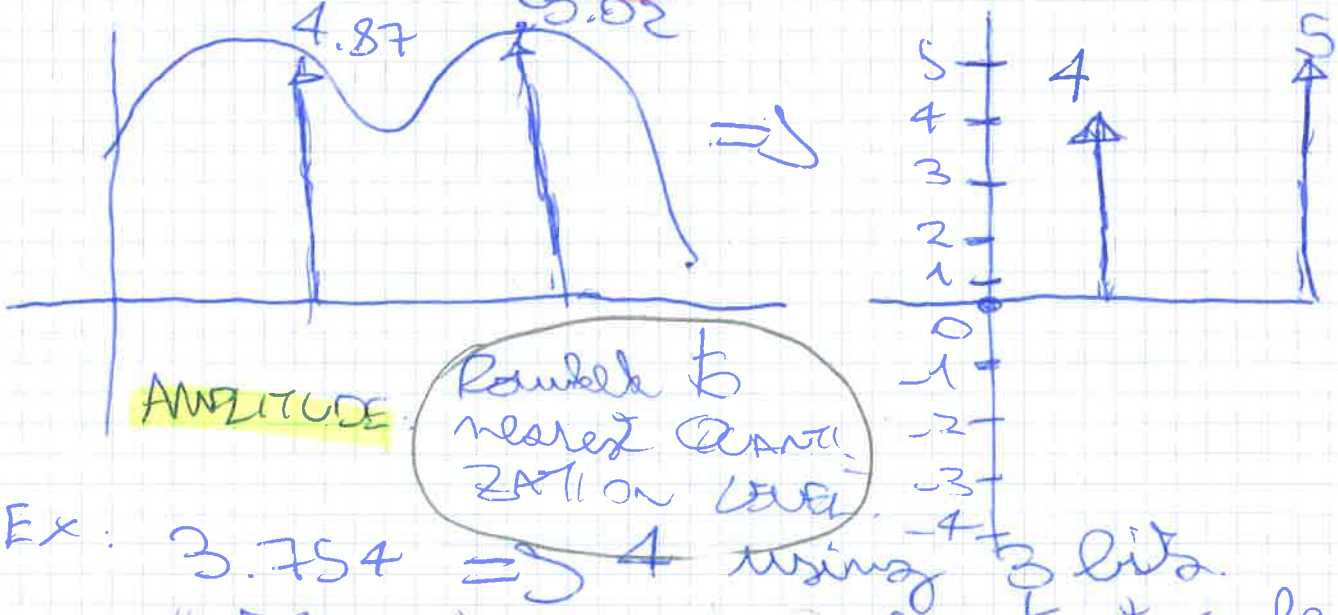
B/T (Baud) — MULTI-LEVEL SIGNAL

EPOCH

$$C = 2 \cdot B \cdot \log_2 M$$

INTERSIMBOL INTERFERENCE

2. QUANTIZATION: It consists of the conversion of Real sampled values into discrete values using n bits.



Ex: 3.754 ⇒ 4 using 3 bits.

L = # Different possible values that can be quantized.
L = # QUANTIZATION LEVELS. (Ex: 10 LEVELS)

$L \leq 2^n$, where $n = \lceil \log_2 L \rceil$

Using L QUANTIZATION LEVELS, we are able to represent values in range:

$l \in \left[-\frac{L}{2}; +\frac{L}{2}\right]$ or $[0; L-1]$, where Δ is the QUANT. STEP.

NB: Quantization noise bounds by $\pm \frac{\Delta}{2}$

QUANTIZATION levels determines the FIDELITY of the QUANTIZED SIGNAL

(PERFECT FIDELITY achieved only with $L = \infty$ # QUANT. LEVELS)

NB: A CODE can be potentially assigned to each QUANTIZATION LEVEL!

3. ENCODING: Process of representing quantized values in DIGITAL FORMAT. (i.e. binary format)

Many different ENCODING STRATEGIES exist, either DIGITAL ENCODING or ANALOG ENCODING.

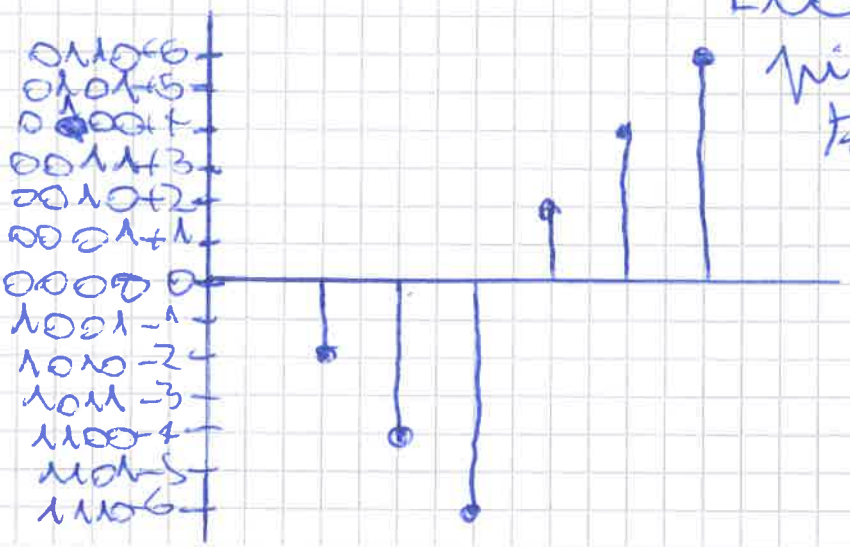
DIGITAL ENCODING (MODULATION): Consists of encoding digital data onto analog signals. It encompasses techniques to carry digital data on analog signals (i.e.: the sender must before transmit turns the data onto the ANALOG MEDIUM)

ANALOG ENCODING (MODULATION): Process of encoding an analog signal over an analog medium. Encompasses techniques for such purpose (i.e.: they just before the actual analog transmission takes place)

TWO-COMPLEMENT ENCODING:

LEADING 0 = Positive number
LEADING 1 = Negative number

EXAMPLE:



ENCODING = A mapping from data bits to signal elements

SIGNALS:

SIGNAL: It is a time-varying oscillating ELECTRIC FIELD, onto which information is conveyed by "changing" some of its components (Ex: Amplitude/Phase/Frequency).

POWER IN A SIGNAL:

For a PERIODIC signal with period T, the average Power in their period is given by its Avg. energy over T.

$$P(T) = \frac{1}{T}\int_0^T |x(t)|^2 \, dt \quad [W]$$

Where $x(t)$ is specified in Voltage/Intensity.

ENERGY IN A SIGNAL:

OHM'S LAW: $E = V \cdot A$ → Voltage, → Intensity

$$E(T) = \int_0^T |x(t)|^2 \, dt \quad [W \cdot s] \text{ or } [J]$$

It is defined as...

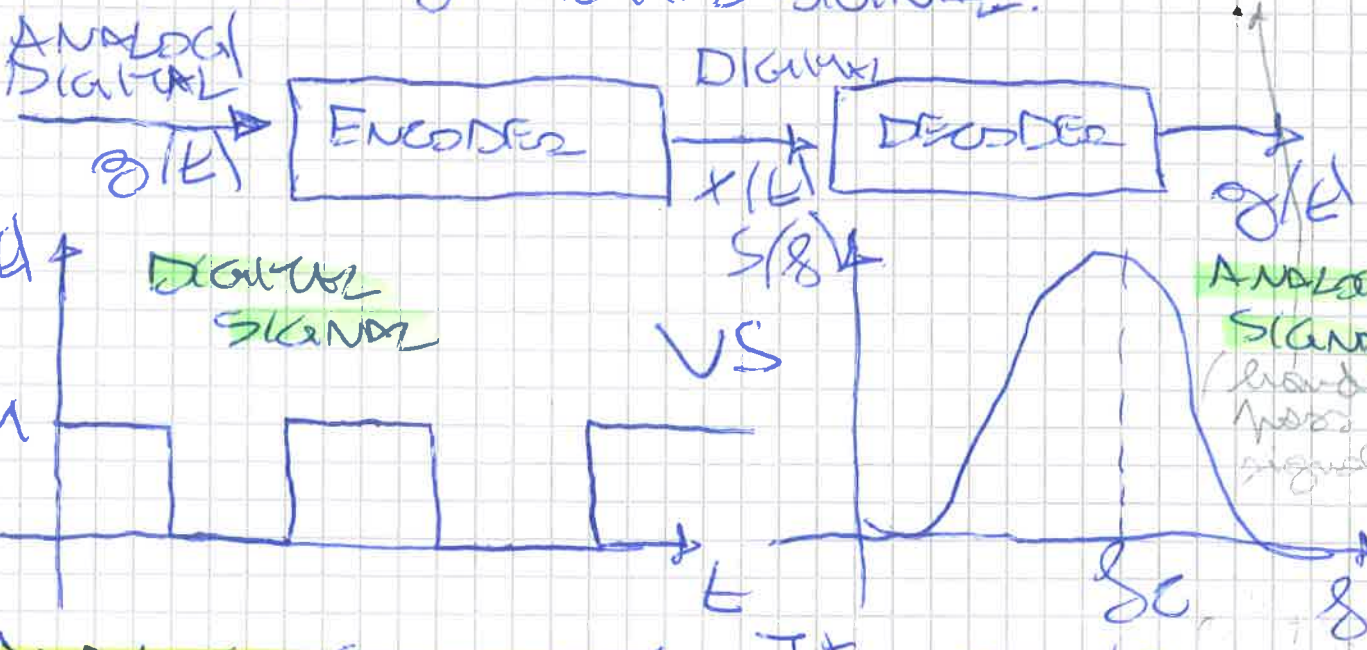
(NB. An oscilloscope can be used to measure the VOLTAGE of a SIGNAL)

GENERAL SIGNAL'S SINEWAVE:

$$S(t) = A \cdot \sin(2\pi f t + \phi)$$

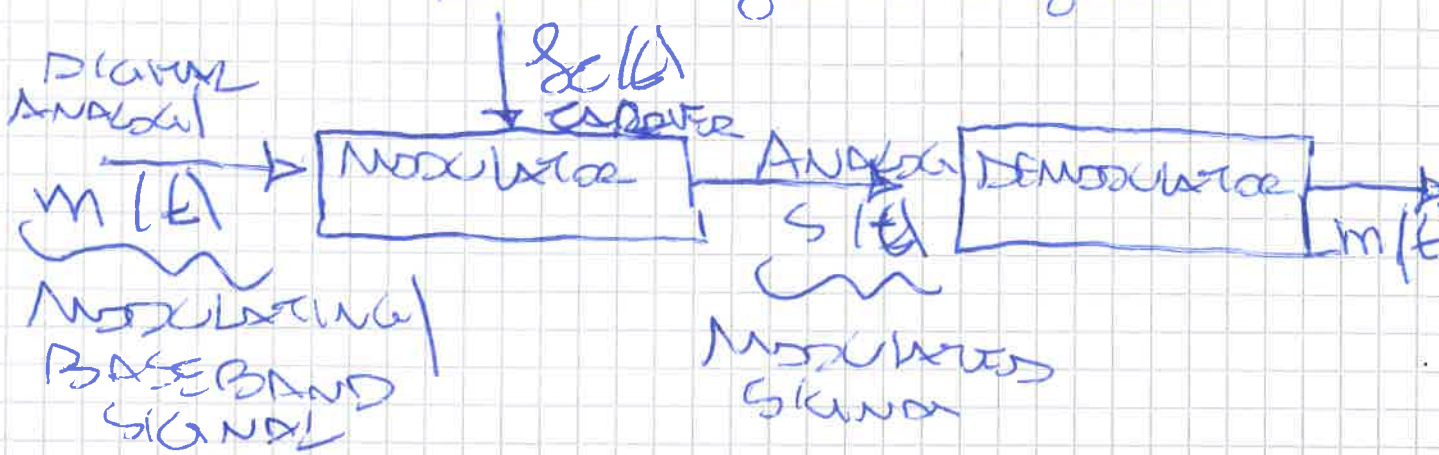
DIGITAL SIGNALING: It consist of ENCODING an ANALOG/DIGITAL signal $g(t)$ into a DIGITAL SIGNAL $x(t)$. BAND-LIMITED SIGNAL

NB: No CARRIER is required! Only a DIGITAL SIGNAL.



ANALOG SIGNALING: It requires a CARRIER SIGNAL (ANALOG): Continuous constant-frequency signal used to carry another signal by means of MODULATION.

MODULATION = Process of encoding source data (analog/digital) onto a CARRIER SIGNAL with frequency f_c by varying a certain component of this signal.



MODULATION:

$$s(t) = m(t) \oplus g_c(t)$$

DEMODULATION:

$$m(t) = s(t) \ominus g_c(t)$$

Process of decoding the source data from a carrier.

DIGITAL → ANALOG: For wireless transmission

ANALOG → ANALOG: Voice/video signal modulated for transmission over a medium.

ANALOG → DIGITAL: Digitize voice/signal to export better data quality.

$$\text{DATA RATE} = \frac{\#\text{bits}}{\text{second}}$$

$$\text{MODULATION RATE} = \frac{\#\text{SYMBOLS}}{\text{second}} = \frac{\#\text{SIGNAL LEVELS}}{\text{second}}$$

(Channel rate) / Bandwidth.

$$SNR = \frac{E_b}{N_0} =$$

SNR dB → SNR CONVERSION:

$$SNR_{dB} = 10 \cdot \log_{10} SNR$$

EX: $SNR_{dB} = 24$ dB

$$\Rightarrow 24 = 10 \cdot \log_{10} SNR \quad \uparrow \quad 24 = \log_{10} SNR$$

$$10^{2.4} = 10^{\log_{10} SNR}$$

$$SNR = 10^{2.4} = 251$$

ANALOG MODULATION

It consists of ENCODING analog data onto an analog signal prior to transmission.

over

ANALOG DATA → ANALOG MEDIUM

Modulation is still required for 2 reasons.

- Higher frequency may be required for transmission (PASSBAND operation)
- Modulation allows for FDM.

Three main ANALOG MODULATION TECHNIQUES exist:

- AM - Amplitude Modulation.
- ANGLE MOD. { - FM - Frequency Modulation
  - PHASE MODULATION

AM - Amplitude Modulation

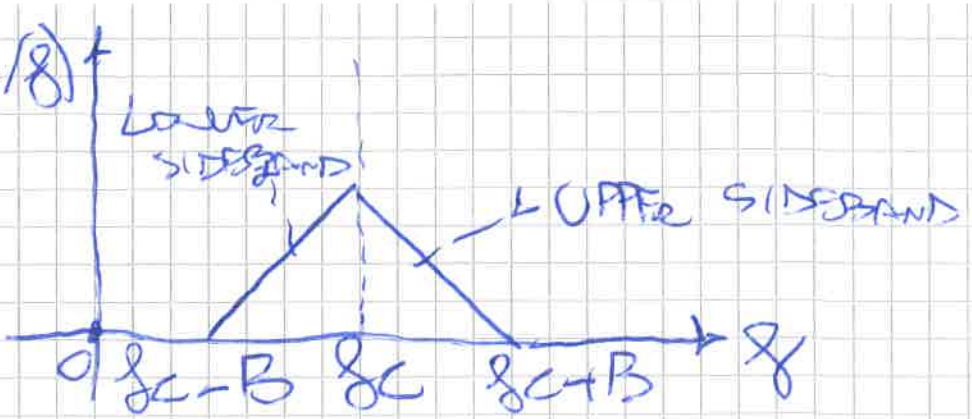
It consists of modulating the AMPLITUDE level of the input signal, jointly with the carrier.

$$s(t) = [1 + n_a \cdot x(t)] \cos(2\pi f_c t)$$

- $x(t)$: INPUT ANALOG SIGNAL
- $\cos(2\pi f_c t)$: CARRIER
- 1: DC component, to prevent loss of INFORMATION.
- n_a: Modulation index (ratio of amplitude of input signal to the carrier)

NB: The INPUT SIGNAL is multiplied by the CARRIER.

SPECTRUM of an AM SIGNAL:



$0 \leq n_a \leq 1$

↑ usually desired to have max. it to have most of signal power

$$P_L = P_C \cdot \left(1 + \frac{n_a^2}{2}\right)$$

P_L = total transmitted power in S(t)

P_C = transmitted power in the carrier

n_a = power required to carry INFO

SSB = Single-SideBand. Only send one of the sidebands (and no carrier)

DSBTC = Double-SideBand Transmitted Carrier (current version) carrier included

DSBSC = Double-Sidebands Suppressed Carrier

NB: The carrier can be used for synchronization purposes

ANGLE MODULATION:

Both Frequency Modulation & Phase Modulation are two sub-classes of Angle Modulation

The modulated signal is expressed as:

$$S(t) = A_C \cdot \cos(2\pi f_c t + \phi(t))$$

PM - PHASE MODULATION:

The phase is proportional to the modulating SIGNAL.

$$s(t) = A_c \cdot \cos\left(2\pi f_c t + \phi(t)\right)$$

$$\boxed{\phi(t) = n_p \cdot x(t)}$$

(n_p: PHASE modulation index)

INSTANTANEOUS SIGNAL FREQUENCY (At a certain point in time):

$$f_i(t) = f_c + \frac{1}{2\pi}\frac{d}{dt}\phi(t)$$

(f_c: carrier frequency)

$$= f_c + \frac{1}{2\pi}\frac{d}{dt}\left(n_p \cdot x(t)\right)$$

FM - FREQUENCY MODULATION:

(rate of change of PHASE)

The derivative of the phase (frequency) is proportional to the modulating signal

$$s(t) = A_c \cdot \cos\left(2\pi f_c t + \phi(t)\right)$$

$$\boxed{\frac{d}{dt}\phi(t) = n_f \cdot x(t)}$$

(n_f: frequency modulation index)

INSTANTANEOUS FREQUENCY:

$$f_i(t) = f_c + \frac{1}{2\pi}\frac{d}{dt}\phi(t)$$

$$= f_c + \frac{1}{2\pi}\left(n_f \cdot x(t)\right)$$

ANGLE MODULATION ⇒ Require constant power & different magnitude.

FM ⇒ AM → Also includes carrier cos(2πft)

(not modulated immunity over Amplitude)

Noise

⇓

Produces a wide range of frequencies

FM & PM require greater bandwidth than AM!

AM ⇒ Low cost receivers

Ex: FM RADIO WAVE

$\lambda = \frac{c}{f}$. $f = 105.5$ MHz

$c = 3 \cdot 10^8 \frac{m}{s}$

$\lambda [m] = \frac{c \left[\frac{m}{s}\right]}{f \left[\frac{1}{s}\right]}$

$\Rightarrow \lambda = \frac{3 \cdot 10^8 \frac{m}{s}}{105{,}5 \cdot 10^6 \frac{1}{s}} = \frac{300}{105{,}5} m = 2.84 m$

Pretty large RADIO wavelength, not so susceptible to noise & interference as AM. Radio wavelengths ($\lambda \gtrsim d_{object}$) $\Rightarrow$ SCATTERING

EXCURSUS about UNITS of MEASURE

10^9 = Giga(G) 10^6 = Mega(M) 10^3 = kilo(K) 10^0 10^{-3} = milli(m) 10^{-6} = micro(μ) 10^{-9} = nano(n)

10^{12} = Tera(T) ; 10^{-12} =

DIGITAL ENCODING

DIGITAL ENCODING = How digital data (0/1) is transmitted over an analog signal.

(Ex: transmit digital data over the PSTN by means of a MODEM (ADSL Technology))

Ex: NRZ [Non-Return-To-Zero]

We assign Positive / Negative amplitude

based on the ~~value~~ value of the Binary Signal.

$$s(t) = \begin{cases} +1\,V & \text{if } 1 \\ -1\,V & \text{if } 0 \end{cases}$$

It's called NRZ, because we literally never go back (return) to Zero.

MODULATION: Involves "changing" one/more components of the CARRIER SIGNAL. Three main techniques are:

- ~~PAM: Pulse Amplitude Modulation~~
- PSK: Phase Shift Keying
- FSK: Frequency Shift Keying
- ASK: Amplitude Shift Keying

ASK | PAM [Pulse Amplitude Modulation]

NB: Two Binary values are represented by two different amplitudes of the CARRIER FREQUENCY (Generally, one of the amplitudes is Zero).

$$s(t) = \begin{cases} A \cdot \cos(2\pi f_c t) & \text{if Binary 1} \\ 0 & \text{if Binary 0} \end{cases}$$

→ Binary 1 ⇒ Presence of the carrier at constant amplitude

Ex: Used in OPTICAL FIBERS, where LEDs can:

1 ⇒ Presence of light

0 ⇒ Absence of light.

DRAWBACKS: • Susceptible to sudden gain changes (Bit error may be present)
• High power required to support MPAM.
• Rather inefficient modulation technique
• Need for carrier phase recovery & synching (tough)!

MPAM | MASK (Multiple levels for ASK: M-ary)

Each amplitude level assigned $K = \log_2 M$ bits each.

Based on GRAY ENCODING. Two successive values differ by one BIT.
(Distance between 2 levels affects the BER)

$$s(t) = \begin{cases} \frac{A}{4}\cdot\cos(2\pi f_c t) & \text{if } 00 \\ \frac{A}{2}\cdot\cos(2\pi f_c t) & \text{if } 01 \\ \frac{3A}{4}\cdot\cos(2\pi f_c t) & \text{if } 10 \\ A\cdot\cos(2\pi f_c t) & \text{if } 11 \end{cases}$$

for $M = 4$

$$R = \frac{K}{T_s}$$ where $K = \log_2 M$

T_s = time to transmit one BIT.

4 BIT RATE

PSK - PHASE SHIFT KEYING

The phase of the carrier signal is shifted to represent data.

BPSK: Use TWO LEVELS to represent the two BINARY DIGITS.

$$s(t) = \begin{cases} A\cdot\cos(2\pi f_c t) & \text{if BIN. 1} \\ A\cdot\cos(2\pi f_c t + \pi) & \text{if BIN. 0} \end{cases}$$

{ANALOGOUS FSK} $= \begin{cases} A\cdot\cos(2\pi f_c t) & \text{if BIN. 1} \\ -A\cdot\cos(2\pi f_c t) & \text{if BIN. 0} \end{cases}$

⇒ Because a phase shift of π implies a FLIP in the SINE WAVE.

DPSK :- Differential Phase Shift Keying

Instead of sensing the ABSOLUTE PHASE, we sense VARIATIONS of the phase w.r.t. the previous phase.

$$\Delta\phi_n = \phi_n - \phi_{n-1}$$

⇒ No need for COHERENT PHASE DETECTION & storage of preceding phase.

$$s_d(t) = A\cdot d(t)\cdot\cos(2\pi f_c t)$$

Where $d(t) = \frac{d}{dt}\phi(t)$

Ex. BPSK $\pi, -\pi, \pi, \pi, -\pi, -\pi, \pi$

DPSK $\times, \Delta, \Delta, 0, \Delta, 0, \Delta$

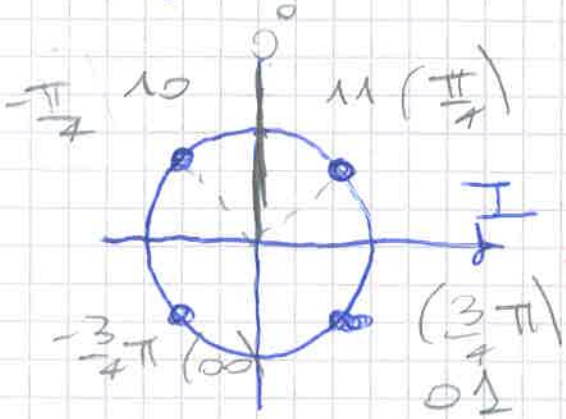
⇒ INFORMATION TRANSMITTED is represented in terms of changes between successive data symbols phase

M PSK - M-Ary Phase Shift Keying

In MPSK, each one of the M phases are

der $\log_2 M$ bits. => More efficient use of BANDWIDTH is made.

(Ex: QPSK = Quadrature Phase Shift Keying, using 4 levels - each one shifted by $\frac{\pi}{2}$)



$$s(t) = \begin{cases} A\cdot\cos(2\pi f_c t + \frac{\pi}{4}) & 11 \\ A\cdot\cos(2\pi f_c t + \frac{3}{4}\pi) & 01 \\ A\cdot\cos(2\pi f_c t - \frac{3}{4}\pi) & 00 \\ A\cdot\cos(2\pi f_c t - \frac{\pi}{4}) & 10 \end{cases}$$

BIT RATE =

$$D = \frac{R}{L} = \frac{R}{\log_2 M}$$

Modulation rate [Baud]

L = # bits per signal element

Higher Bit rates can be achieved using more complex modulation schemes, which allow to increase R.

FSK - Frequency Shift Keying

Frequency-Shift Keying encodes digital data into the frequency component of the waveform.

BFSK - Binary Frequency Shift Keying

It makes use of two different

frequencies to encode BINARY DATA.

$$s(t) = \begin{cases} A \cdot \cos(2\pi f_1 t) & \text{if BIN. 1} \\ A \cdot \cos(2\pi f_2 t) & \text{if BIN. 0} \end{cases}$$

EXAMPLE: Used for high frequency RADIO TRANSMISSION on LANs over COAXIAL CABLES [3–300 MHz] RADIO.

+ Less susceptible to error than ASK (especially if multiple levels employed)

M-FSK – Multiple Frequency Shift Keying

Multiple different FREQUENCY LEVELS are used to modulate the signal.

$$s_i(t) = A \cdot \cos(2\pi f_i t)$$

$$f_i = f_c + (2i - 1 - M) \cdot f_d$$

f_c = CARRIER frequency

f_d = difference frequency

M = # different signal levels / elements

⇒ Each signalling element represents more than ONE BIT.

NB: To maintain the data rate of the input BIT STREAM, each output signal is held for:

$$T_s = L \cdot T_b$$

L = # BITS per signal element

T_b = time to transmit one BIT.

T_s = time to transmit a SIGNAL

$$R = \frac{1}{T}$$

One SIGNAL element encodes L bits.

$$L = \log_2 M$$

, where

M = # MODULATION LEVELS.

TOTAL BANDWIDTH REQUIRED.

$$B = 2 \cdot M \cdot \delta_d$$

(difference in frequency from "for" frequencies etc)

Where the minimum frequency separation is given by $[$ the adjacent frequency

$$2\delta_d = \frac{1}{T_s} \Rightarrow \delta_d = \frac{1}{2 \cdot T_s}$$

$\Rightarrow$ The MODEM requires a transmission δ:

$$W_d = 2 \cdot M \cdot \delta_d = 2M \cdot \frac{1}{2T_s} = \frac{M}{T_s}$$

MSK = MFSK with minimum frequency separation.

QAM - Quadrature Amplitude Modulation

QAM is a combination of ASK and PSK, in which two NON-OVERLAPPING SIGNALS are sent simultaneously over the same carrier frequency.

CARRIER 2 $\Rightarrow$ Modulate the AMPLITUDE.

SIGNAL $\Rightarrow$ Modulate the PHASE.

$$s(t) = d_1(t)\sqrt{\frac{2}{E_s}}\cos(2\pi f_c t) + d_2(t)\sqrt{\frac{2}{E_s}}\sin(2\pi f_c t)$$

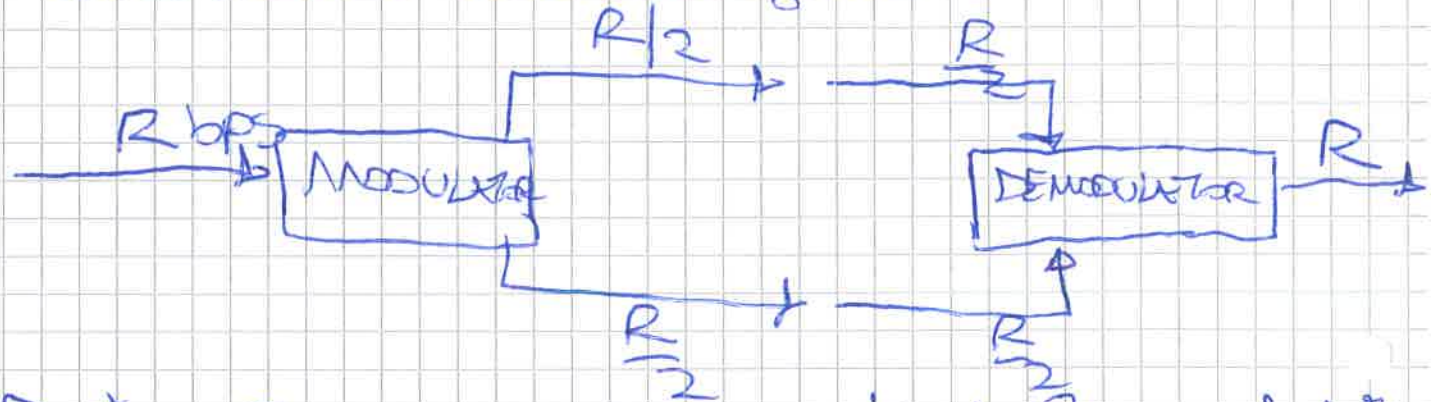
TRANSMITTED SIGNAL. CARRIER SIGNAL (1) CARRIER SIGNAL (2)

$\Rightarrow$ The two signal copies are ORTHOGONAL to each other.

APPLICATION: Used in some Wireless standards (Ex: Wi-Fi).

TX: Send the two signals simultaneously, modulating the carrier like ASK.

RX: The two signals are demodulated and the result combined again.



Both QUAD = AMPLITUDE used for modulation

(2-QAM)

2-LEVEL ASK used ⇒ Each Bit Stream can be in one of 2 STATES.

⇒ COMBINED: 4 = 2x2 STATES.

~~4-level ASK = QAM~~ Quadrature Amplitude

(4-QAM)

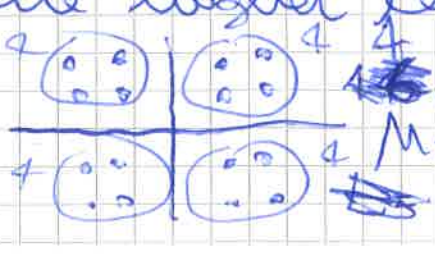
4-LEVEL ASK used

⇒ Each Bit Stream can be in one of 4 STATES

⇒ COMBINED: 16 STATES: 4x4.

16-QAM | 64-QAM | 256-QAM have all been successfully implemented (at video BER through)

The higher the #STATES, the higher the DATA RATE achievable.



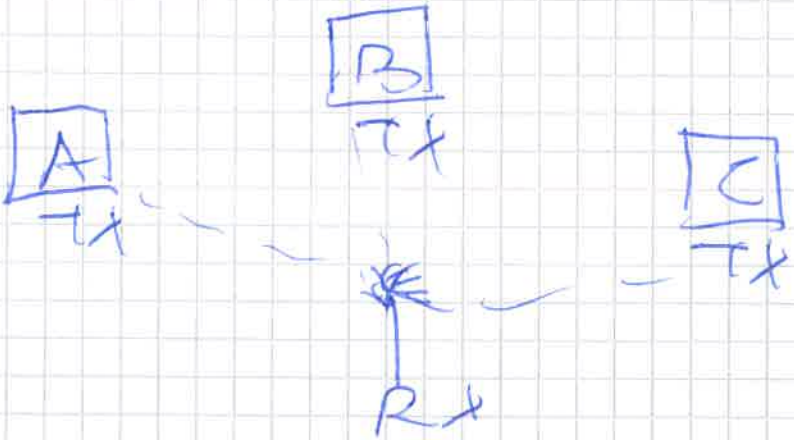
$$D = \frac{R}{K} = \frac{R}{\log_2 M}$$

M = # QUANTIZATION LEVELS

K = # BITS per signal element

NB: CARRIER is ASK - modulated
SIGNAL is PSK - modulated

EXCURSUS about CDMA:
CDMA allows multiple users to TX at the same time, while making use of different ORTHOGONAL CODES for every single user.



$R = \bar{B} + C$ [$\bar{B}$ and C are orthogonal to each other]

$R \cdot C = \cancel{B} + C \cdot C$

REQUIREMENTS for CDMA:
- All stations are SYNCHRONOUS
- All codes used at the TX are orthogonal to one another
- The RX knows the codes used by other TX stations

PROPAGATION.

Wireless COMMUNICATION is heavily affected by PROPAGATION EFFECTS in different manners.

[The higher the frequency, the smaller the λ ⇒ The more strongly the signal is affected by ATTENUATION; IMPAIRMENTS; ATMOSPHERIC CONDITIONS; INTERFERENCE]

The SIGNAL can be propagated in 3 main modes:

- GROUND-WAVE PROPAGATION
- SKY-WAVE PROPAGATION
- LINE- & -SIGHT

• GROUND-WAVE: Generated when the height of the TX antenna is small compared to the λ of the transmitted signal.

⇒ GROUND-WAVE PROPAGATION leads to the ground being used as a conductor & electric DIPOLES.

$$h << \lambda$$

1st PRINCIPLE & THERMODYNAMICS:

$$dU = \underbrace{Tds}_{\text{THERMAL}} - \underbrace{PdV}_{\text{MECHANICAL}} + \underbrace{EdP}_{\text{ENERGY}} + \underbrace{HdM}_{\text{MAGNETISM}}$$

An exchange of energy occurs when DIPOLES are ~~[illegible]~~ created & transmitted (i.e.: dipoles flipping).

A "Signal induces a GROUND WAVE when being transmitted"

DIPOLO ELETTRICO: CARICA POSITIVA, CARICA NEGATIVA

Due cariche puntiformi $+q$ e $-q$ distanti ② costituiscono un DIPOLO ELETTRICO

MOMENTO DEL DIPOLO: $\vec{p} = q \cdot \vec{a}$ VETTORE

CHARGE

$\vec{a}$ orientato dalla carica negativa alla carica positiva.

~~[illegible]~~

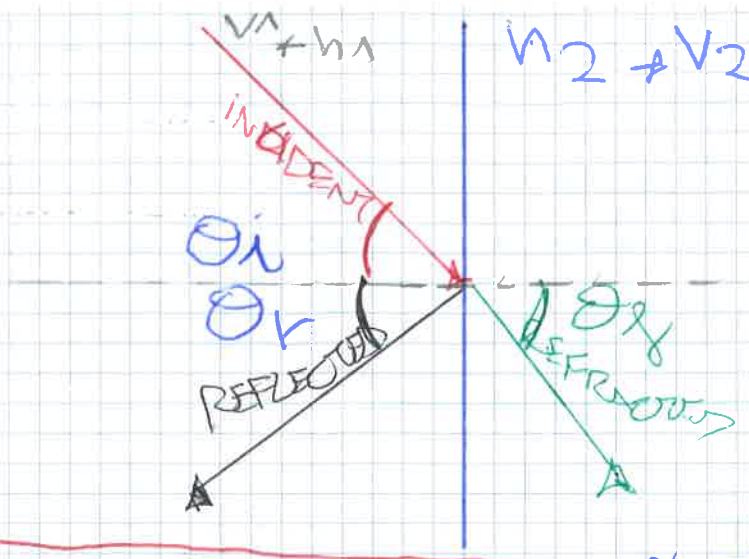
• SKY-WAVE: When being transmitted waves "bounce" against the IONOSPHERE by REFRACTION. Bending of MICRO WAVES by the atmosphere (CHANGE in DIRECTION)

Allowed MARCONI'S experiment to succeed

When a wave passes from two mediums of different DENSITY (respective index = n_1, n_2 respectively)

LAW of REFLECTION:

"The angle of incidence equals the



LAW OF REFLECTION: "The angle of REFLECTION equals the angle of INCIDENCE".

θ_r θ_i

$$\theta_r = \theta_i$$

SNELL'S LAW: The angle of INCIDENCE θ_i is related to the angle of REFRACTION θ_g as:

$$\frac{\sin(\theta_i)}{\sin(\theta_g)} = \frac{n_2}{n_1} = \frac{V_1}{V_2}$$

V_1, V_2 is the velocity of light in each medium, respectively

NB: V_1 / V_2, the velocity of light in a medium, depends on the density of the medium / i.e. the more DIELECTRIC CONSTANT)

$$n = \frac{c}{V}$$

Refractive index of a medium

$$V = \frac{c}{\varepsilon_0 \mu}$$

speed of light in VACUUM is MEDIUM-SPECIFIC

μ = magnetic permeability

ε = DIELECTRIC CONSTANT

NOISE TYPES; FADING

- **THERMAL NOISE**: Inherently present in a medium; due to agitation of electrons

$$N_0 = K \cdot T \quad \left[\frac{\text{Watts}}{\text{Hz}}\right]$$ [For 1 Hz Bandwidth]

$K = 1.3803 \cdot 10^{-23}$ J/K (Boltzmann's constant) T = Temperature (in Kelvins)

⇒ For B Hz of Bandwidth:

$$N = K \cdot T \cdot B$$

- **INTERMODULATION NOISE**: Caused by multiple signals (at different frequencies) sharing the same medium.
  ⇒ Resulting frequency is the SUM/DIFFERENCE of the original frequencies or a multiple thereof.

- **CROSSTALK**: Unwanted COUPLING between signal paths
  - WIRELESS: When multiple signals are picked up by antennas. (Ex: Hear another radio station)
  - WIRED: When signal cables carry multiple signals. (Ex: Hear another phone conversation)

[Typically less than thermal noise]

- IMPULSE NOISE: Irregular pulses or noise spikes of short duration and high amplitude present in a medium. Generated by EM perturbances in the medium, such as LIGHTNING, FAULTS, FLAWS in the communication system.

[Primary source of errors in digital data transmission]

FADING: Time variation of received signal power caused by changes in the transmission medium or paths.

~~(Ex: interference) body on the way / impairments / weather / distance~~

→ FIXED ENVIRONMENT: Affected by atmospheric conditions.

→ MOBILE ENVIRONMENT: Location of antennas relative to each other is the main issue causing FADING.

PROPAGATION MECHANISMS:

REFLECTION: [Done already]

DIFFRACTION: Occurs at the EDGE of an impenetrable body that is large compared to the wavelength of the radio wave.

SCATTERING: Occurs when the size of an obstacle is on the same order of the wavelength
=> Signal scattered into several rubber signals

DENSITY OF CHARGE: $\frac{dE}{dx} = \frac{\rho}{\varepsilon_0}$ = Amount of electric charge per unit length / surface area / volume.

LECTURE 5

RADIO CHANNEL IMPAIRMENTS

IMPAIRMENTS: Phenomena disturbing communication at certain frequencies or in certain conditions.

LARGE-SCALE PROPAGATION: Impact over long-range communication.
(Ex: Refraction / noise / path loss)

SMALL-SCALE PROPAGATION: Small time-varying effects over propagation distances & low wavelengths or short time duration.
(E: fading / doppler effect)

THz waves 'frequency ⇒ VISIBLE LIGHT COMMUNICATION (experiment at CNR)

DIFFUSION: Allows for the propagation & waves beyond the horizon

THERMAL NOISE:
Caused by AGITATION of electrons that / while moving / create RANDOM NOISE.

$E = T + V$

POTENTIAL ENERGY: Energy held by an object because of its position relative to other objects

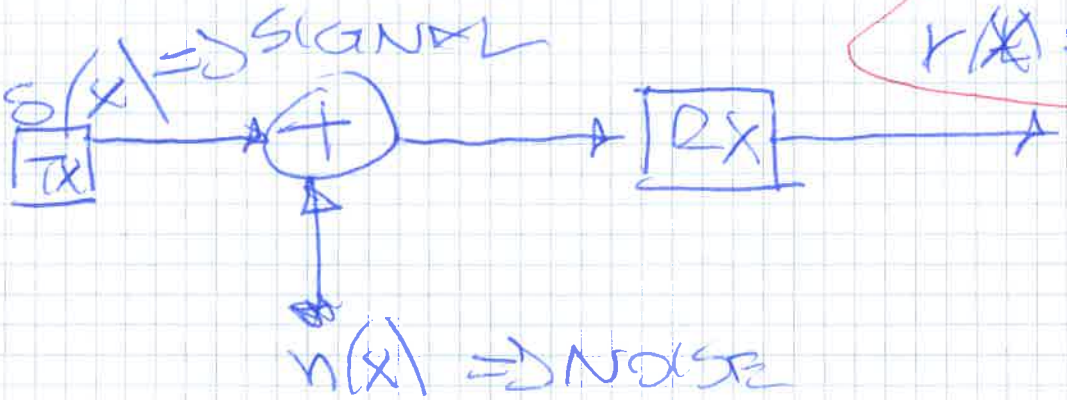
THERMAL ENERGY = THERMAL NOISE: Energy contained in a system responsible for its temperature

$\langle T \rangle \simeq \frac{3}{2} K \cdot T$

HEAT = Flow of thermal energy

Additive White Gaussian Noise

AWGN: Medium's Noise adds up to the signal when being transmitted.



$$r(x) = s(x) + n(x)$$

SNR - Signal-to-Noise Ratio

$$SNR = \frac{\text{Average Signal power}}{\text{Average Noise power}} \quad (dB)$$

⚠ It limits the BIT RATE achievable over a MEDIUM (UPPER BOUND)

$$dB = 10 \cdot \log_{10} \frac{A_2}{A_1}$$

A_2 → Signal level

A_1 → Noise level

LOGARITHMIC SCALE → Needs an exponential increase to have a linear increase in the # dBs measured

It can also be expressed in mW lost per meter/kilometer

FREE SPACE PATH LOSS

When using an **ISOTROPIC ANTENNA**, the transmitted in ALL directions according to a SPHERICAL MODEL.

(SURFACE) Area of sphere $= 4\pi r^2$ → Power irradiated in all directions = Omnidirectional antenna

r = Radius

$$\frac{P_r}{P_L} = \frac{\lambda^2}{(4\pi d)^2} = \frac{c^2}{(4\pi f d)^2}$$

P_r = Signal power at RX antenna

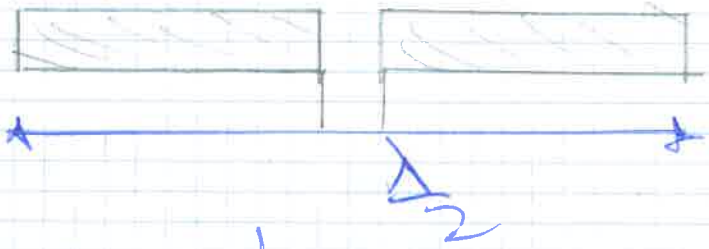
P_L = Signal power at TX antenna

d = Prop. distance between antennas

ANTENNA TYPES.

- **ISOTROPIC ANTENNA**: Irradiates power in all directions, analogously to a sphere with the antenna in its center.
  - BEAMWIDTH: Measure of the DIRECTIVITY of the antenna in a certain direction ⇒ How much beamforming it can perform.
- **DIPOLES ANTENNAS**:
  - HALF-WAVE (HERTZ): Made up of two straight collinear conductors of equal length, separated by a small gap.

antenna $\ell = \frac{\lambda}{2}$ the signal that can be transmitted most efficiently



(uniform) omnidirectional radiation pattern (More complex antenna configs. can be used to produce a directional beam)

- QUARTER-WAVE (MARCONI): Vertical commonly used for automobile radios and portable radios

PARABOLIC REFLECTIVE ANTENNA

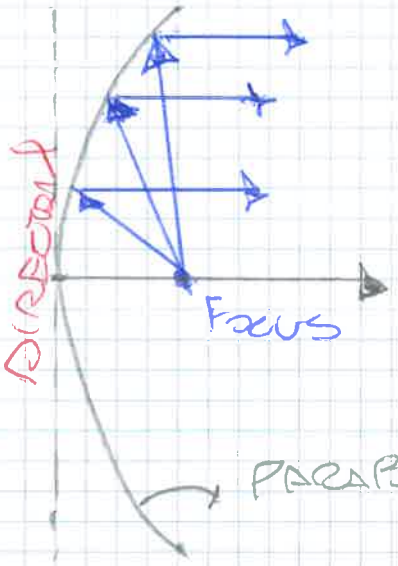
Used in TERRESTRIAL MICROWAVE and SATELLITE APPLICATIONS.

PARABOLA: Locus of all points equidistant from a fixed line and a fixed point not on the line (i.e.: FOCUS is the point, DIRECTRIX is the line)

↳ APPLICATION: Optical & Radio telescopes, automobile headlights because of its FOCAL PROPERTY:

"If a source of electromagnetic energy (or sound) is placed at the focus of the paraboloid, and if the paraboloid is a reflecting surface, then the wave will bounce back in lines parallel to the axis of the paraboloid".

VISUALLY:



(The converse is also true: if incoming waves are parallel to the axis of the reflecting paraboloid, then the resulting signal will be concentrated at the focus)

ANTENNA GAIN: Measure of the DIRECTIVITY/DIRECTIVITY of an antenna. It is defined as the power output in a particular direction, compared to that produced by an omnidirectional antenna (with the same input power).

$$G_t = \frac{4\pi f^2 A_e}{c^2}$$

G_t: ANTENNA GAIN

A_e: effective area & (physical size antenna) (the larger the A_e, the greater the gain)

[Generally, we consider the maximum gain obtainable in a direction as GAIN]

- NON-ISOTROPIC ANTENNAS: - FRIIS LAW

Receiving

Measures the free-space loss of an antenna located at distance d from a non-isotropic transmitting antenna.

$$\frac{P_r}{P_t} = \frac{G_t \cdot G_r \cdot \lambda^2}{(4\pi d)^2} = \frac{G_t \cdot G_r \cdot c^2}{(4\pi f d)^2}$$

$$\lambda = \frac{c}{f}$$

$G_t = 1$ for isotropic antenna.

MULTIPATH EFFECT: Multiple rays are generated due to REFLECTION and REFRACTION. (original ray & other travelling rays need to be summed up at the receiver) ⇒ FINAL RECEIVED SIGNALS are summed

IN-DOOR ATTENUATION: Strongly affected by walls' depth and obstructing objects on the way ⇒ lose capability of reaching a DESTINATION.

NB: At high frequencies, material's & building's penetration loss particularly impacting factor.

PATH LOSS MODEL:

$$P_r = P_t \cdot K \cdot \left(\frac{d_0}{d}\right)^{\gamma}$$

- P_r: Received power
- P_t: Transmitted power
- K: Antenna - dependent CONSTANT
- d_0: reference distance
- d: TRANSMITTER - RECEIVER DISTANCE
- γ: PATH LOSS EXPONENT

$\gamma \approx 2$ for free-space PROPAGATION

VALID

$\gamma \approx 4$ for two-ray PROPAGATION

SHADOWING:

FADING: Propagation effect affecting the SIGNAL TRANSMISSION / SNR

Issue occurring when mobiles experience random variations in their intensity because of the presence of disorders on the way from the objects present in the SIGNAL PATH, which reflect the signal and cause scattering of the signal.

$\Rightarrow$ Power FLUCTUATES based on a log-NORMAL DISTRIBUTION.

$\Rightarrow$ PROBABILITY DISTRIBUTION of the dB of the STATISTICAL VARIABLE (ψ_{dB}) is GAUSSIAN

$$\mu = \mu_{\psi_{dB}} \qquad \sigma = \sigma_{\psi_{dB}}$$

$$\psi_{dB} = \frac{\text{Transmitted power}}{\text{Received power}} \quad \text{RATIO}$$

$$P\{\psi_{dB}\} = \frac{1}{\sqrt{2\pi}\cdot\sigma_{\psi_{dB}}} \cdot \exp\left[-\frac{(\psi_{dB} - \mu_{\psi_{dB}})^2}{2\sigma_{\psi_{dB}}}\right]$$

$\mu_{\psi_{dB}}$ = Sum of PATH LOSS (AVG. attenuation from Eldrose)

FADING

⇒ PATH LOSS MODEL + SHADOWING MODEL

They can be SUPERIMPOSED!

$$\frac{P_r}{P_t} = 10\log_{10} K - 10 \cdot \gamma \log_{10}\left(\frac{d}{d_0}\right) - \psi_{dB}$$

ψ_{dB} → GAUSSIAN R.V. $\mu = 0$, VAR: $\sigma_{\psi_{dB}}$

POWER RECEIVED:

$$P_{RX} = P_{TX}^{DB} + G_{TX}^{DB} + G_{RX}^{DB} - P_L$$

G = Gain, P = Power

LECTURE 6 -

PHYSICAL CHANNELS (SHANNON, NYQUIST) & CHANNEL CAPACITY

A variety of impairments can corrupt a signal, both in AETHEREUM (wireless media) or in wired media (i.e.: optical fibers, copper cables) & unwanted signal

NOISE ⇒ Common impairment that combines onto the SIGNAL & degrades the QUALITY.

"To what extent does noise limit fundamental the data rate that is achievable?"

concepts:

- DATA RATE: bits per second (bps) at which data is transmitted.
- BANDWIDTH: Spectrum available to the transmitted signal, limited by the medium transmitting it.
- NOISE: AVG. noise level in the communication path.
- ERROR RATE: Rate at which errors occur

* CHANNEL CAPACITY: Maximum rate at which data can be transmitted over a given data under given conditions.

Generally: • Capacity ↑ ⇒ $$$ ↑

• Limited bandwidth available (in spectrum | political/economical reasons)

↓

Need to make efficient use of the available BANDWIDTH.

[i.e.: as high data rate as possible for a particular limit of error rate] for a certain BANDWIDTH!

• NYQUIST BANDWIDTH: (noise-free channel)

⇒ Directly follows from the NYQUIST SAMPLING THEOREM:

$$S_{rate} = 2 \cdot B_{MAX} \quad (\leq B)$$

"Need to sample at 2. TRANSMISSION RATE"

"In a noise-free channel, the data rate is uniquely limited by the signal's bandwidth, i.e., and more precisely:

⇒ If the rate of signal transmission is 2B, then a signal with frequencies no greater than B (BANDWIDTH) is enough to carry the signal.

[Conversely, given a bandwidth B, the highest signal rate that can be carried is 2B]

BINARY TRANSMISSION: $C = R_b \leq 2B$ ($M = 2$ modulation levels)

TRANSM. rate

$R_b = \frac{1}{T_b}$

EXAMPLE: BINARY transmission (2 levels)

B Hz $\Rightarrow$ $2B$ bps $= C$

Bandwidth & Channel — transmission rate (CAPACITY C)

VOICE COMMUNICATION / TELEPHONE:

$B = 3100$ Hz

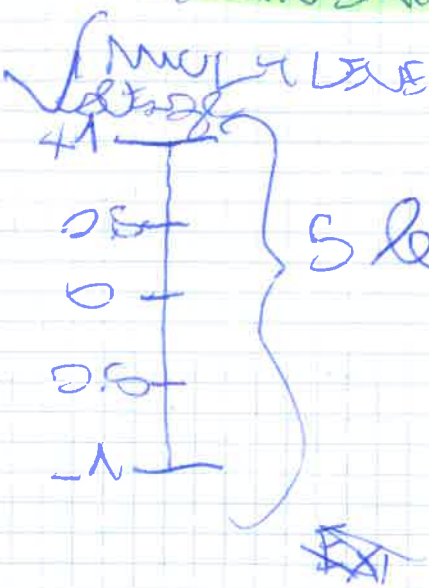
$C = 2B = 6200$ bps

M-ARY SIGNAL TRANSMISSION

$\Rightarrow$ Every signal element can represent more than one bit

(Ex: Multiple voltage levels Multilevel signals)

MODULATION LEVELS



$$C = R \leq 2B \log_2 M$$

If $M = 2 \Rightarrow \log_2 2 = 1$

$\Rightarrow$ For a certain BANDWIDTH, we can increase the TRANSM. RATE logarithmically by increasing the # LEVELS in the transmitted signal and linearly by increasing the BANDWIDTH.

NB. The transmission Rate of a DEVICE is always upper bounded by the capacity of the CHANNEL onto which it transmits.

- SHANNON'S THEOREM: Shannon took into consideration also the NOISE, the ERROR RATE, other than the DATA RATE.

NOISE => May corrupt one or more bits. (higher data rate => smaller bits transmitted in time)

(BACKGROUND NOISE + occasional large spikes)

At a given noise level, the higher the data rate, the higher the error rate.

NB: A noise may change a 1 into a 0 and the channel, hence "confusing" the receiver.

[Increasing the SIGNAL STRENGTH would improve the ability to receive data correctly in the presence of noise]

$$SNR_{dB} = 10 \cdot \log_{10} \frac{\text{SIGNAL POWER}}{\text{NOISE POWER}}$$

At a certain point in time = RATIO of power in signal / power in noise

(10 Bis always in a base-10 logarithm) mic drop

Higher SNR => high-quality signal.

NB: The SNR represents the upper bound on the achievable data rate over a channel.

$$R \leq C = B \cdot \log_2(1 + SNR)$$

R: TRANSM. RATE; B: BANDWIDTH; NOT in bits

THEOREM: MAXIMUM that can be achieved in practice, as it does not consider a multitude of factors.

- DELAY DISTORTIONS
- IMPULSE NOISE
- Only assumes thermal (AWGN)

$$R = \frac{1}{T_b} \leq 2B$$

For a BINARY SIGNAL, transmission rate is limited by this RELATION

"Using a suitable SIGNAL CODE, it is theoretically possible to obtain a transmission rate R up to C ERROR-FREE"

NB As the signal strength increases, so do the effects of NON-LINEARITIES in the system, leading to an increase in intermodulation noise.

WHITE NOISE ⇒ The wider the Bandwidth the more noise influences the system

CELLULAR NETWORKS

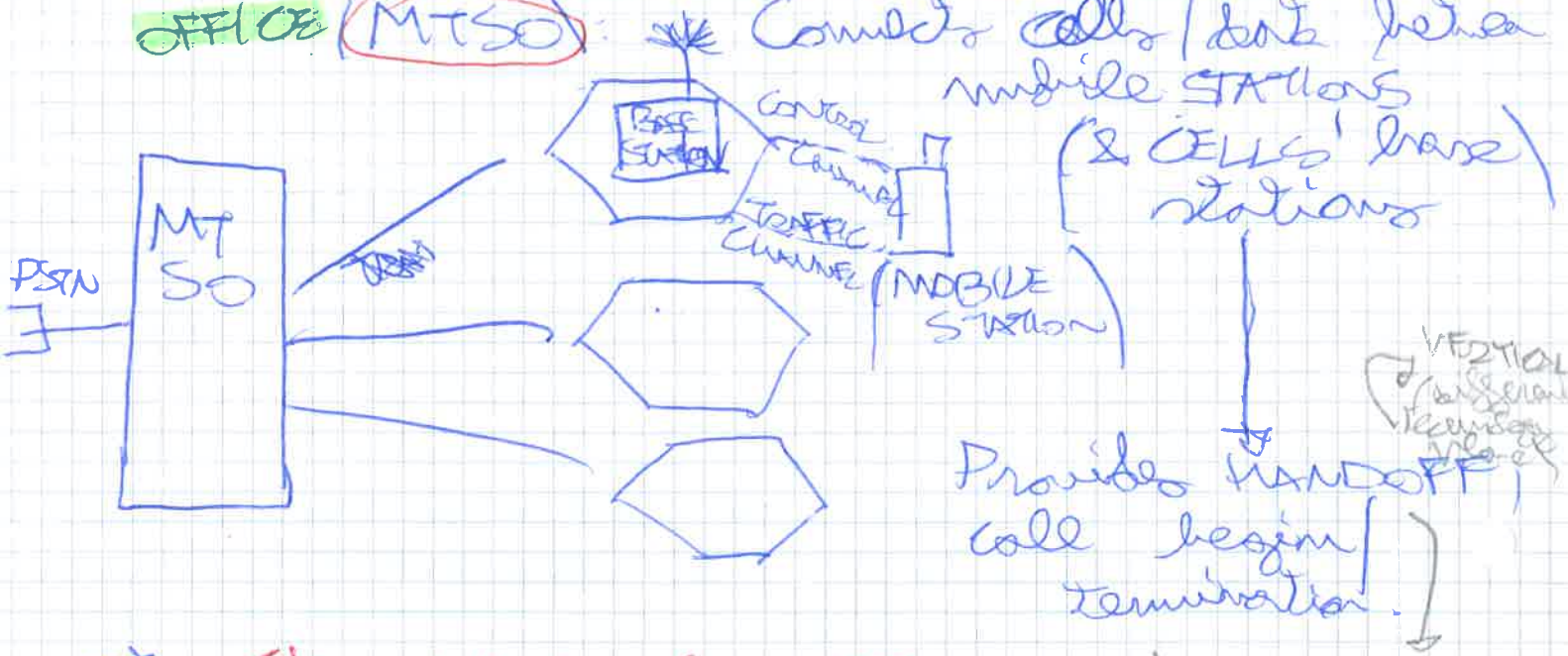
Cellular networks connect a moving mobile User Entity (UE) to a network (e.g. for VOICE / DATA transmission purposes)

CELL = Coverage area of a base station, providing connectivity to the devices in its RANGE.

BASE TX/RX STATION

Multiple Entities are involved in a cellular network:

- BASE STATION (BS): Antenna, controller, and a set of RECEIVERS.
- MOBILE TELECOMMUNICATIONS SWITCHING OFFICE (MTSO): Connects calls / data between mobile STATIONS (& CELLS' base stations)



Provides HANDOFF (call begin / termination)

CHANNELS for CELLS

Channels can exist in different dimensions & are created based on:

- FDMA, TDMA, CDMA

⇒ Each channel has its own channel set (C_n) and every cell is assigned a channel set

Equidistant antennas wherever at least C_n assigned to it

Cells are located & organised strategically to avoid INTERFERENCE (CROSSTALK) between one another, with the goal of reusing CHANNELS in nearby cells.

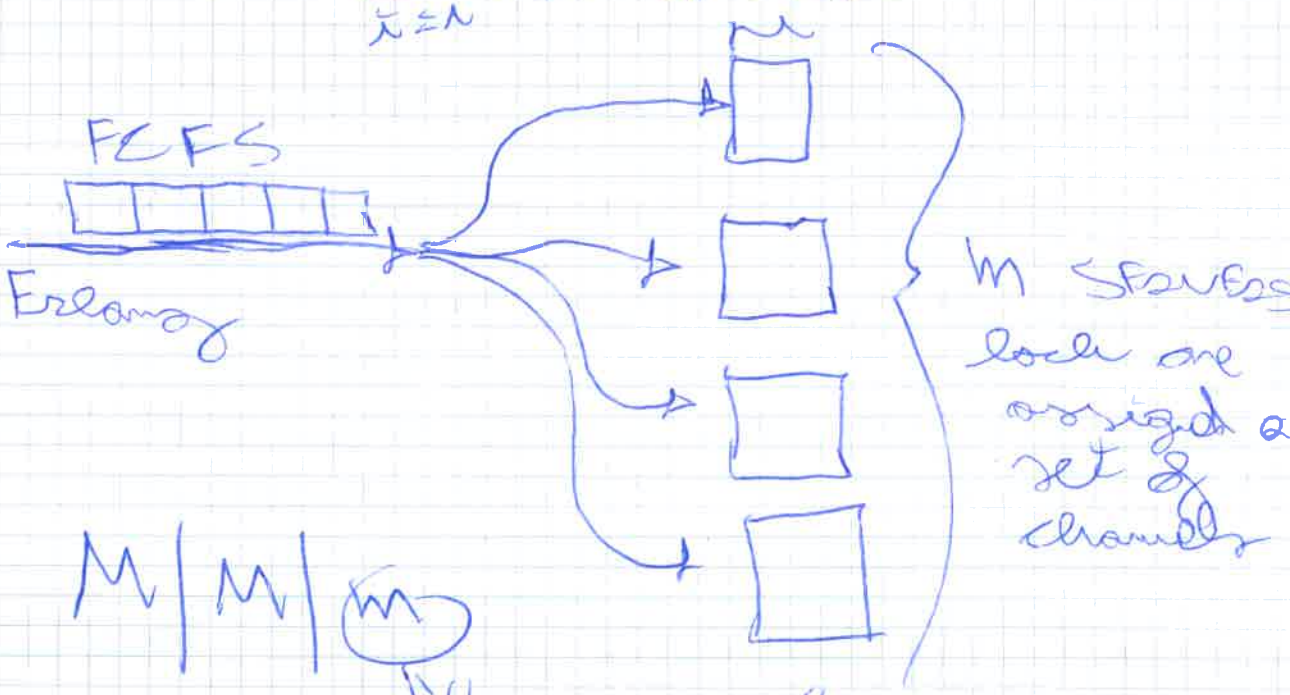
(Ex: FDMA ⇒ n frequencies assigned to each cell)

CHANNELS in each CHANNEL SET

QUEUING THEORY can be employed to properly dimension the # CHANNELS to be assigned to a cell.

ERLANG $A = \Lambda \cdot \underbrace{E\{T_S\}}_{\text{Expected service time}} = \frac{\Lambda}{\mu}$

$\Lambda = \sum_{i=1}^{n} \lambda_i$ μ SERVER



CHANNELS should ensure that $P_B = P\{\text{BLOCKING}\}$ is below a certain threshold.

ERLANG-B FORMULA

$$P_B = \frac{\frac{(\Lambda/\mu)^m}{m!}}{\sum_{i=0}^{m} \frac{(\Lambda/\mu)^i}{i!}} \leq \text{THRESHOLD} \quad [0-1]$$

Write $A = \frac{\lambda}{\mu}$, where $\lambda = \sum_{i=1}^{n} \lambda_i$

A = Mean # calls in progress at a given time

λ = AVG

μ = SERVICE RATE

$A = \rho \cdot m$ | M/M/m

$\rho = \frac{\lambda}{\mu}$

Avg. # trunks

$$P_B = \frac{\frac{A^m}{m!}}{\sum_{i=1}^{m} \frac{A^i}{i!}} \leq \text{THRESHOLD}$$

MTSO is tasked with placing calls over a channel & manages calls' quality.

(free) CELLS

AVOID INTERFERENCE by reducing the cell size & increasing the bandwidth.

=> Re-use existing (acquired) CHANNELS by increasing the #CELLS to accomodate more BANDWIDTH.

S = # CHANNELS (available for reuse)

k = # CHANNELS allocated to a cell, in a disjoint manner

N = # CELLS

$$\boxed{S = k \cdot N}$$

$$k = \frac{S}{N}$$

CLUSTER: Set of N cells, which collectively use the whole complete set of available frequencies.

If a cluster is replicated M times, the # DUPLEX CHANNELS as a measure of capacity is:

$$C = M \cdot k \cdot N$$

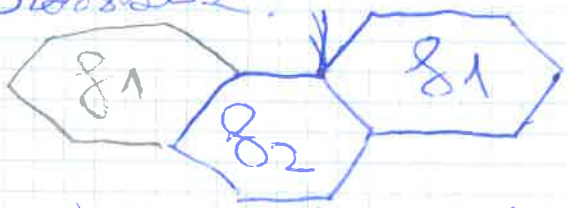
OVERALL CAPACITY of whole SYSTEM | # CLUSTERS

Capacity is directly proportional to replication factor

SMALL CLUSTER ⇒ Cells closer to one another

INTERFERENCE

Adjacent cells in an area are assigned different frequencies (i.e.: channels) to avoid interference and/or crosstalk.



After a certain distance (i.e.: non-neighboring cells), channels can be re-used once again (RE-USE FACTOR)

SMALLER CELLS: reduction in power irradiated from the base station (low-power devices can be used) ⇒ less inter-cell interference & inter-cell interference.

INTER-CELL INTERFERENCE:

Avoid MATRIX structure of cells for this very reason & OMNIDIRECTIONAL ANTENNAS

⇒ HONEYCOMB (HEXAGONAL) such that cells are equidistant one from another when the user is moving from one cell to another.

↳ SIGNAL degradation occurs because of interference as well.

CELL ASSIGNMENT: When the mobile unit first connects to the network, the BASE STATION with MAX. POWER SIGNAL is assigned to it (i.e.: it will handle its data and calls)

↳ SINR: Signal-to-Interference-plus-Noise Power Ratio

We would like to minimize it to increase the call's signal strength.

$$SINR = \frac{P_K}{N_0 \cdot B + P_I}$$

THERMAL ENERGY NOISE

ENERGY: ADDITIVE PHENOMENON (Also energy from different appliances)

$$E = \sum_{i=N}^{N} E_i$$

[See: INTENSIVE & EXTENSIVE PHYSICAL PROPERTIES]

TEMPERATURE: MEDIATING PHENOMENON

$$T = \frac{\sum_{i=1}^{N} T_i}{N}$$

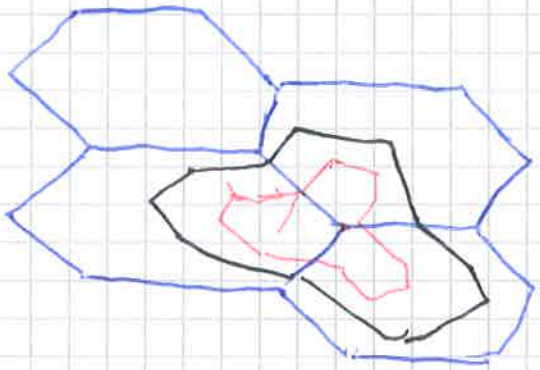
CELL SIZE & CAPACITY

Because TRAFFIC within a CELL is VERY VARIABLE (i.e.: high variance in its INTENSITY), we may want to apply some MECHANISMS to accomodate sharp bursts in intensity. For this purpose, there exist several approaches:

- ADDING NEW CHANNELS. Use unused channels in a region.
- FREQUENCY BORROWING: "Take" frequencies from adjacent cells to serve traffic in CONGESTED CELLS.
- CELL SPLITTING: Split highly used cells into smaller cells (Ex: Microcells)

  ORIGINAL CELLS = 6.5 Km - 13 Km → Increase BANDWIDTH

  SMALLER CELLS = 1.5 Kms. (reduced power level)



- CELL SECTORING: A CELL is divided into a set of WEDGE-SHAPED SECTORS, each one with its own set of channels.

→ Uses DIRECTIONAL ANTENNA & MICROCELL

- MICRO CELLS / PICO CELLS / NANO CELLS to accomodate peaks in TRAFFIC demand.
- SOFT FREQUENCY REUSE: The cell is split into a CELL-CENTER-AREA & a CELL-EDGE AREA.

↳ EDGE: Only a part of the spectrum is available.

↳ CENTER: Whole spectrum is available

CONTROL CHANNELS:
Used to carry control information requi= red to setup / tear down CALLS or setup a DATA PACKETS' channel.

TRAFFIC CHANNELS:
Used to carry the actual data exchanged among users.

IONISING RADIATION: (0.01-10nm waves)
Radiation carrying sufficient energy to detach ELECTRONS from ATOMS or molecules.
↳ X-RAYS: Photons carrying enough energy to ionize atoms and disrupt molecu= lar bonds (harmful for living beings)
↳ γ-RAYS: Penetrating electromagnetic ra= diations arising from the RADIOACTIVE DECAY of atomic nuclei

EVOLUTION OF CELLULAR TECHNOLOGIES:

1G-1 GENERATION CELLULAR NETWORKS

1G systems quickly became popular in the 1980s / beginning of 1990s.

TRANSMISSION: Fully - analog, with no well-defined world-wide STANDARDISATION
[Transmit over the air with NO ENCRYPTION]

NMT - Nordic Mobile Telephone
1970 / 1981 early deployments [Netherlands, Scandinavia, Russia, Poland]

RANGE: 2 up to 30 kms.

FREQUENCIES: NMT-450 (MHz)
NMT-900 (MHz)

OTHER FEATURES: Basic support for SMS in NMT handsets

AMPS - Advanced Mobile Phone System
USA! U-SA - standard

FDD + FDMA based on 2 25-MHz bands.

832 Channels { TX: 824-849 MHz
RX: 869-894 MHz

30 kHz per channel.
Each operator allocated 12.5 MHz for competition in market.

ISSUE: ESN/Electronic Serial Number cloned
Need large B for large population

TACS - Total Access Communication System

AMPS - variant developed by Motorola & deployed in the UK/UK, Ireland.

↳ ETACS extended TACS with more channels.

2G - 2. GENERATION CELLULAR NETWORKS

2G - DIGITAL COMMUNICATION introduced.
(Digital modulation for better DIGITAL DATA transmission introduced) ⇒ SMS/emails

⇒ + ENCRYPTION of USER TRAFFIC.
+ ERROR DETECTION.
+ Less power emitted from phones (longer lasting)

MAC & MUX: TDMA/FDD or CDMA/FDD } DYNAMIC CHANNEL SHARING

More user population supported, with better TRANSMISSION QUALITY.

⇒ Phones & TX/RX base stations getting cheaper (better spectral/power efficiency)

GSM - Global ~~Subscribers~~ System for Mobile Communications

Developed by ETSI to unify mobile 2G transmission in Europe into one system.
(Very successful technology - 2.27 B subs/212 countries)

FREQUENCIES
FDD-based { 800 MHz / 1900 MHz bands generally usable

BANDWIDTH: -25 MHz for uplink
-25 MHz for downlink

~~192 channels~~

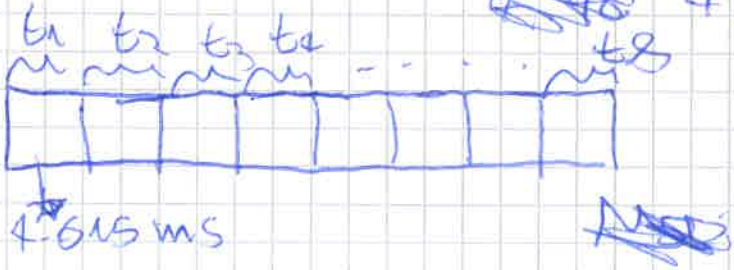
MODULATION:
GMSK

CARRIER: 200 KHz.

125 full duplex channels

CHANNEL DATA RATE = 270.833 Kb/s

~~MAC~~ MAC TECHNIQUE: 8-SLOT TDMA, with frame duration of ~~4.76~~ 4.615 ms.



8 SLOTS!

IN-BAND SIGNALING

IS-136 | D-AMPS - Digital AMPS (USA-NA)

MAC: 3-SLOT TDMA, still FDD-based { 800 MHz bands

CHANNEL BANDWIDTH: 30 KHz.

PDC - Pacific Digital Cellular (Japan)
Channel Bandwidth: 25 KHz. similar to IS-136
11.2 Kbps - 3-SLOT | 5.6 Kbps - 6 SLOT
800 MHz | 1.5 GHz bands

IS-95 | CDMA or (USA | NA)

Based on CDMA, with 64 users. Strong, really good & cool. Still Digital!

Channel bandwidth: 1.25 MHz.

Channel data rate: 1.2288 Mchips/s

2.5G → 3G

2.5G upgrades compatible with 2G technology & HW (cost reduction)

HSCSD: High-Speed Circuit Switched Data

Use consecutive time slots in GSM. (also data on top of GSM)

4 SLOTS

9.6 Kbps (GSM) → 14.4 Kbps (next version) ⇒ 57.6 Kbps

GPRS - General Packet Radio Service

Allows MULTI-USE of channel sharing & radio channels.

8 SLOTS ⇒ 171.2 Kbps (8 × 21.4)

EDGE - Enhanced Data Rate for GSM Evolution

MODULATION: 8-PSK for high rate

⇒ Adaptive modulation, using MCS (multiple Modulation and Coding Scheme)

DATA RATE: 1 Mb/s possible. (384.4 Kb/s)

IS-95B | CDMA ONE (CDMA)

Multiple allocated user channels

IS-95A → 64 users, 14.4 Kbps.

Data rate: 8 × 14.4 Kbps = 115.2 Kbps

3G - 3. GENERATION

REQUIREMENTS: Some of 4G's.

Full STANDARDISATION by ITU for interoperability among countries.

ARCHITECTURE: Fully PACKET-SWITCHED

2 UPGRADE PATHS

2G: IS-95b / CDMA One → 3G: CDMA 2000 NA [3GPP2]

GSM → W-CDMA / UMTS EU [3GPP]

DATA RATE: 5-10 Mbps.

W-CDMA / UMTS → Wideband Code Division Multiple Access

- Expensive equipment ($$$, need to replace old infrastructure.
- + Backward compatible with GSM.

Data Rate: 8 Kbps (up to 2 Mbps over single channel)
FUTURE: 8 Mbps

Bandwidth: 5, 10, 20, MHz

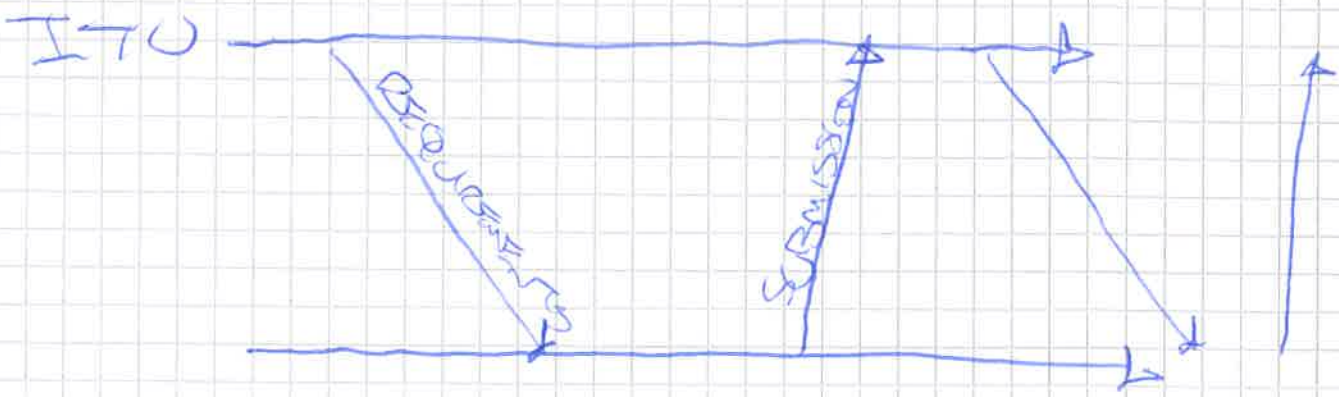
users/calls: 100 / 350 at the same time (based on prop. conditions)

CDMA 2000
+Reuse CDMA one's equipment ($)
Bandwidth: 1.25 MHz
Data rate: 307 Kbps

CDMA 2000 - 1xEV: higher data rate
CDMA 1xEx-DO: 2.4 Mbps per channel
CDMA 3xRTT:
"Group" 3 1.25 MHz channels
⇒ Channel bandwidth = 3.75 MHz
(≈ 2 Mbps data rate)

TD-SCDMA: 中国 3G
China CATT + Siemens joint venture
Bandwidth: 1.6 MHz channel & smart antennas
5 MS frames / 2 ms.

3GPP = 3rd Generation Partnership Project
World-wide organization for the creation of TELECOMM. STANDARDS.



4G - 4. GENERATION -

MOTIVATION: Better QoS, higher data rates; lower latency
"Anytime, anywhere"

+ Better spectral efficiency w.r.t. 3G (bit/s/Hz)

DATA RATE: high data rates → INDOOR: 1 Gb/s
↘ OUTDOOR: 100 Mb/s

+ Smooth VERTICAL / HORIZONTAL HANDOFF
(interoperability with 2G/3G)

FULL PACKET-SWITCHED ARCHITECTURE

DUPLEXING: TDD/FDD

+ Cost Reduction

MAC: TDMA/FDMA

LTE KEY CHARACTERISTICS:

Data rates:
- UPLINK: 50 Mb/s
- DOWNLINK: 100 Mb/s

Bandwidth: 20 MHz [Flexible] (1.5 | 2.5 | 5 | 10 | 20)

Latency: 10 ms to eNode B

Mobility: 0–15 km/h [OFDM 250] Up to 350 km/h

Modulation: AMC (Adaptive Modulation based on channel conditions)
(QPSK, QAM-16, QAM-64)
⇒ Convolutional / Turbo Coding

MAC: OFDMA downlink
SC-FDMA uplink

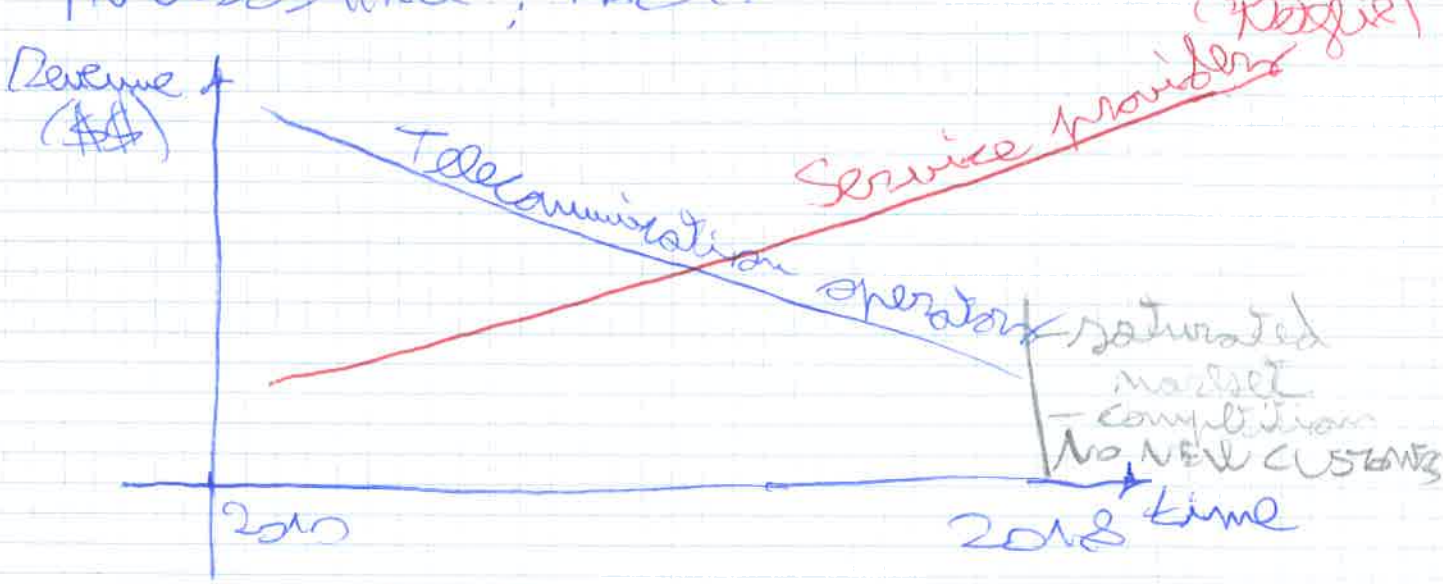
Capacity: 200 users in 5 MHz cell.

BILLING in 4G: Flatrate

↓

BILLING in 5G: More personalized offers based on QoS desired

INTERESTING FACT:

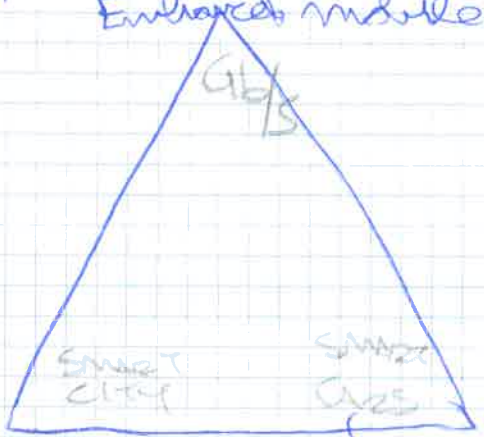


5G

4G → 5G TRANSITION

~~Cost: Reuse existing equipment~~

MMC: Massive - Machine Communication



5G-ready devices. They will have to support the 3.7 GHz frequency.

Standalone (LTE-5G) VS Non-Standalone (initially based on 4G)

CHARACTERISTICS of 5G:

- BEAMFORMING: capacity to "TRACK" a user
- MASSIVE MIMO
- CLOUD-Based RAN: Gro towards a "SOFTWARIZATION" of the network.

5G => Everything running on top of the IP layer (also control layer)

Inner: Lower power
Outer: Higher power

OBJ of 5G: Allow for the interconnection and intercomunication among machines in a NETWORK.

(EX: CARS, FACTORIES' machinery)

MAIN FIELDS: Vehicles (automotive), mining, manufacturing, transports.

↳ INDUSTRY 4.0: 4th INDUSTRIAL REVOLUTION

NO ACTUAL HEALTH RISKS INVOLVED with 5G, as the emitting radio waves are strictly NON-IONIZING and their EIRP is strongly regulated by national authorities.

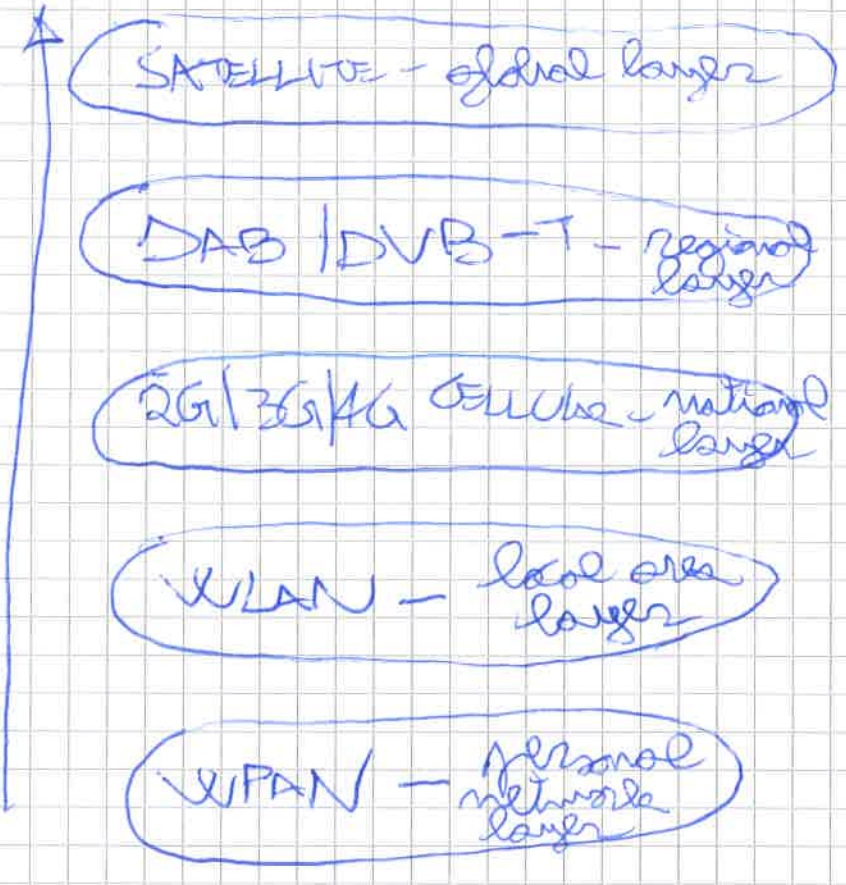
↳ 1-5 GHz: Skin heating at most

LECTURE 7

4G → 5G
(ARCHITECTURE)

4G has a particular focus on MULTIMEDIA (DATA STREAMING at high rates) = includes new potential fields called "on demand"
Ex: Video streaming, HD calls, video calls, high speed internet surfing, ...
[MULTIMEDIA]
→ 3GPP, release N°7.
100 Mb/s – 1000 Mb/s speed.

INTERWORKING LAYERS:

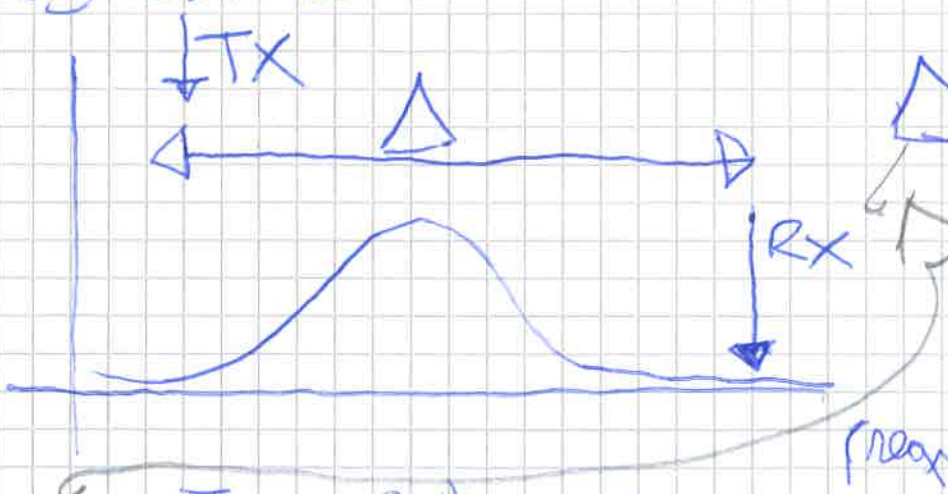


VERTICAL HANDOVER
(different technology)

BILLING:
In the future based on the QoS & the network.

HORIZONTAL HANDOVER
(same technology, just change the area "handoff" to different cell base station)

QoS Classes (FX & for error management)
↳ RELIABLE CONNECTION via TCP/IP.



DELAY: Time between sending and receiving.

STREAM & DATA: No delay in transmission is actually noticed by the final user.

REAL BRAKE: Delay-sensitive action, need for hard QoS.

JITTER: Δ of the PACKETS' arrival distribution.

~~4G~~ 4G - Release 7:
Specification & UE's technical requirements (4G-ready devices)

↓
4G - Release 10
Long-Term Evolution (Advanced)
LTE-A

Single-carrier
Orthogonal (non-overlapping)

≈ Up to 200 users.

AMC = Modulation & coding (Turbo Codes) selected based on channel quality (SNR)
QPSK, QAM-16, QAM-64.

MIMO = 2x2 | 4x4 antennas.

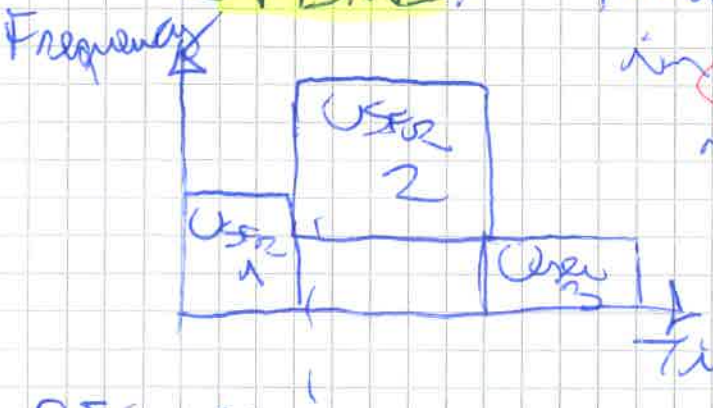
Low energy consumption!

Working 0-15 km/h optimized for.

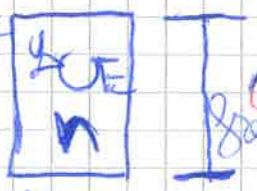
Up to 350 km/h, still working! (Kind of)

Ex: Play arena on a Chinese roller train.

OFDMA: Multiplex OFDM symbols in time and frequency with each user transmitting one or multiple OFDM symbols.



Resource Block:



over 12 subcarriers

0.5ms ≈ 7 OFDM symbols

MULTIPATH CHANNEL: (MULTI-PATH EFFECT)

Multiple copies of same signal arriving to UE | BASE STATION.

⇒ MULTIPATH causes ISI (Inter-Symbol Interference) and FADING in the time domain.

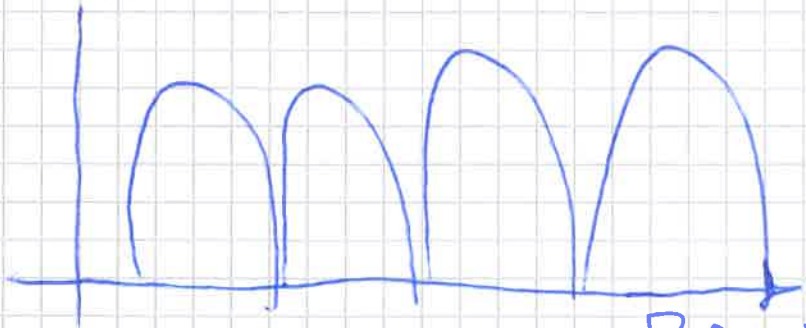
FREQUENCY SELECTIVITY: different frequency being "turned on" in the frequency domain.
↳ [High variance of the frequency over time]

FREQUENCY DOMAIN EQUALIZER:

EQUALIZATION = Process of adjusting the BALANCE ~~between~~ among the frequency components of a signal.

↳ DFT allows to equalize over frequency instead of time (similar to OFDMA)

SC-FDMA: Single-Carrier FDMA. Single-carrier modulation | DFT-spread orthogonal frequency MUXING and frequency domain equalization.



Multiple smaller SUBCARRIERS over the bandwidth

FREQUENCY DOMAIN: Perform channel inversion equalization

↳ "SINGLE CARRIER": Because sequential transmission of SYMBOLS over a single frequency carrier.

OFDMA vs SC-FDMA:

In SC-FDMA, symbols of different users are MUXed together over the frequency domain => Works because UPLINK ≠ DLINK

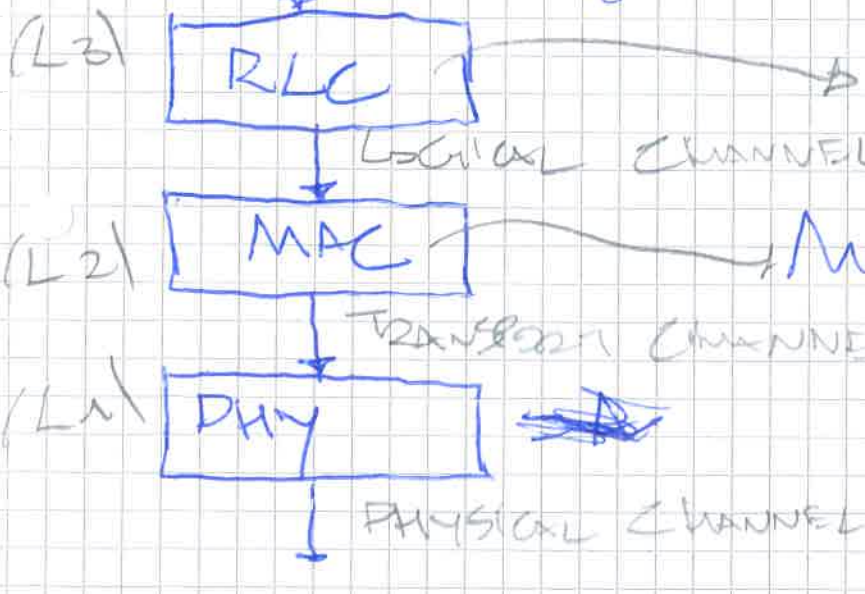
PROTOCOL STACK

USER-PLANE (U-Plane)

(Architecture: see slides)

Responsible for handling user data

Payload signalling

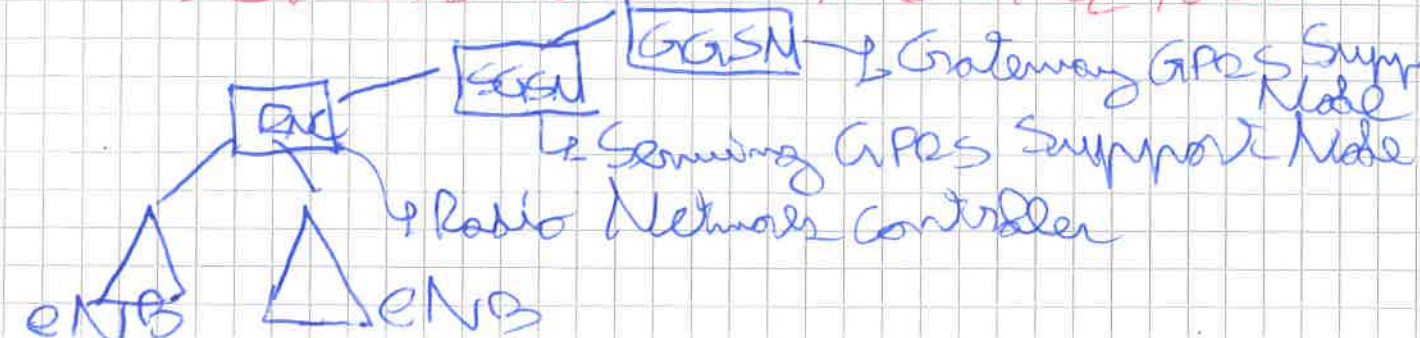


CONTROL PLANE (C-Plane)

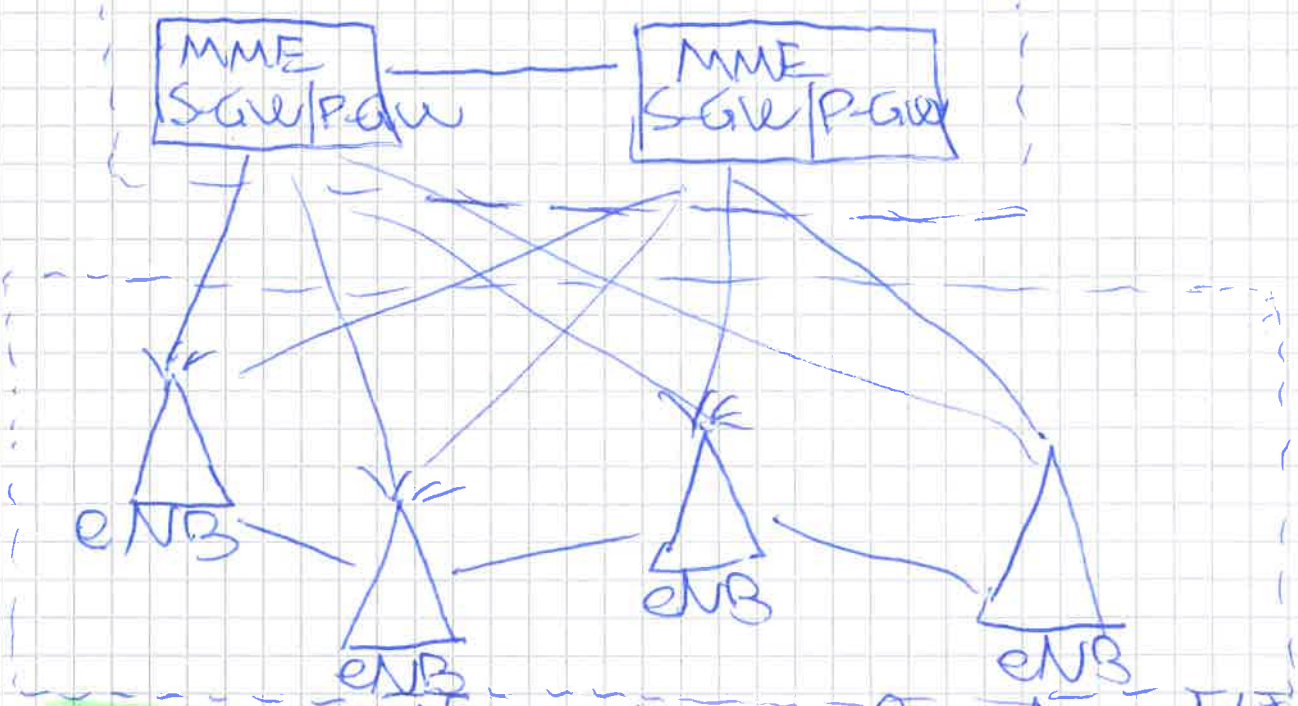
(See slides)

Responsible for handling control messages

3G-NETWORK ARCHITECTURE



4G NETWORK ARCHITECTURE:



E-UTRAN [Evolved UMTS Radio Access Network]

S-GW [Serving Gateway]: Responsible for routing and forwarding user data packets from the E-UTRAN to the EPC (using Mobility Management Entity "tracks" the user as it moves & coordinates handoffs through paging).

P-GW: [PDN (Packet Data Network) gateway] Connects UEs to the external packet data networks (Provides IP address & actual "network connectivity" (registers)

E-UTRAN: When the UE first connects to the network one MME is selected by it to which the UE is attached.

↳ eNodeB performs scheduling & paging of user data | QoS | encryption | routing | mobility | management.

HETEROGENEOUS NETWORK in LTE:

Network made up of different (heterogeneous) components [CELLS at eNodeB]:
Ex: Macrocells, picocells, femtocells, nanocells.

Each one of them with different ranges & bit rate provided
[Map of eNodeB in Trento]

milli = 10^{-3}
micro = 10^{-6}
nano = 10^{-9}
pico = 10^{-12}

kilo = 10^{3}
mega = 10^{6}
giga = 10^{9}
tera = 10^{12}

INTERFERENCE AVOIDANCE in HETEROGENEOUS NETWORKS:

Need to make use of TDD | FDD to reduce (& avoid) interference among different carriers.

=> Use: 1) CARRIER AGGREGATION over frequency | time
2) SILENT PERIODS (Almost Blank Frames)
Add carrier quando hanno over time.

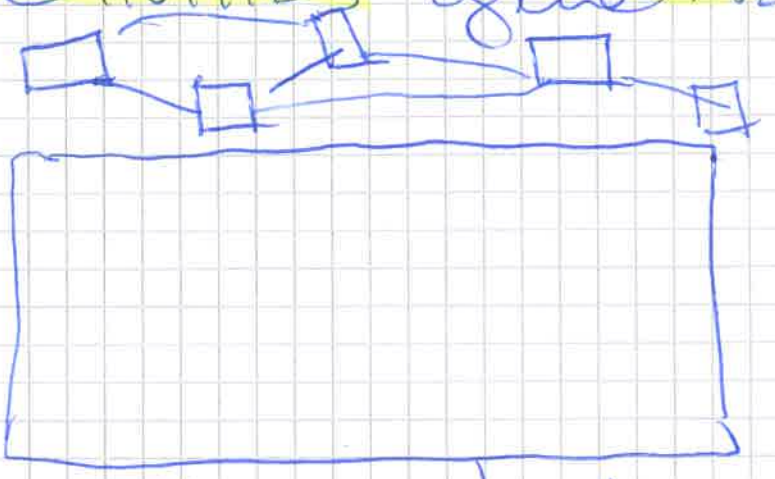
SPATIAL | TEMPORAL | FREQUENCY DIVERSITY to avoid interference!

SON - Self-Organizing Networks

↳ operated by 3rd-parties [running overlay nodes]

LS - Application Layer network built on top of traditional IP-layer networks.

for AUTOMATION & MANAGEMENT ACTIVITIES of the NETWORK



Overlay nodes are tasked with SERVICE-SPECIFIC data forwarding & control functions enabled by VIRTUAL OVERLAY LINKS.

GOAL:
- Cost reduction in the network's OPEX costs.
- Reduce human error & human intervention

R8: → Self-configuration functionalities

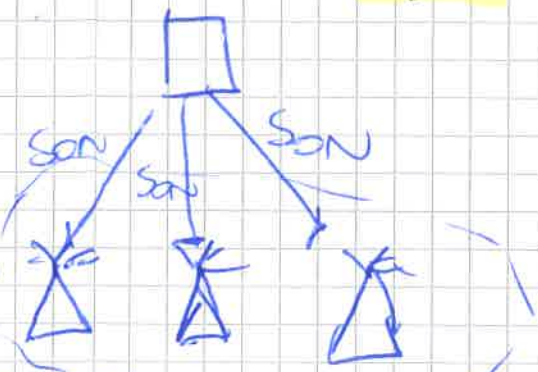
R9 [NETWORK OPTIMIZATION] Mobility Robustness | Hand over optimization E.g.: Load balancing | inter-cell interference reduction

→ R10 [ENHANCEMENTS] Coverage & capacity optimization

→ R11 [More ENHANCEMENTS] Automatic Neighbor Relation Discovery Energy saving

SDN ARCHITECTURE can be:

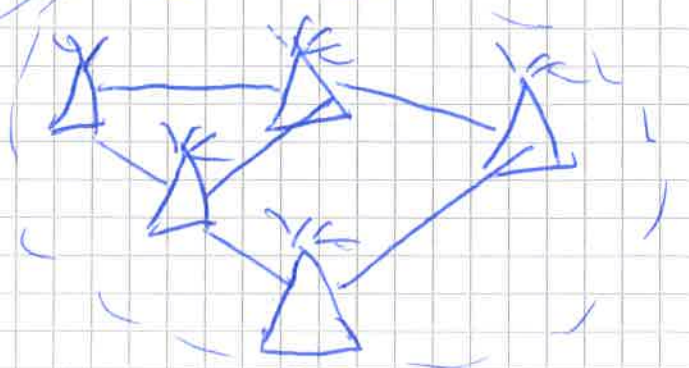
CENTRALIZED:



+ OPTIMAL DECISIONS, with No convergence issues

- Higher latency
- Single PoF

DISTRIBUTED



+ No single PoF
- Slower OPTIMAL convergence
+ Distributed intelligence

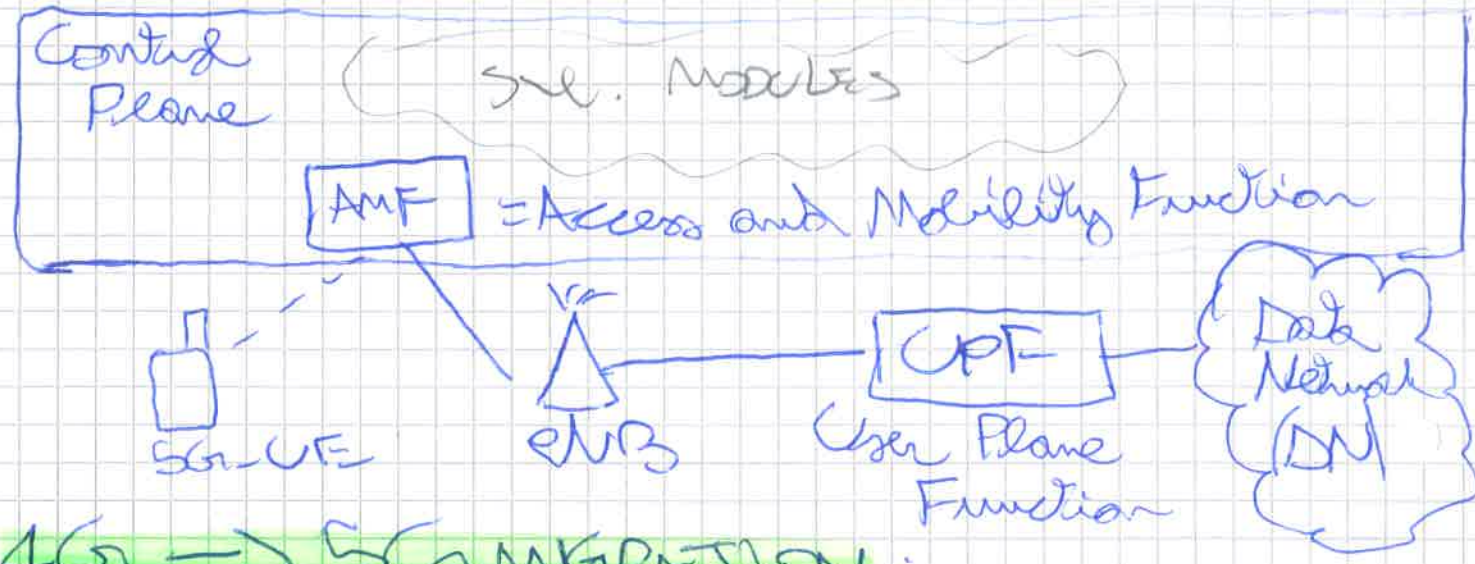
HYBRID.

Both of the two approaches "put together"

SDN PROVIDER ≠ NETWORK PROVIDER

5G NETWORK ARCHITECTURE

5G-ready devices: 3.7 GHz, following 3GPP Release 15.



4G → 5G MIGRATION:

Control layer running on top of IP layer.

1. OPTION:

5A:

(Standalone)

eNB

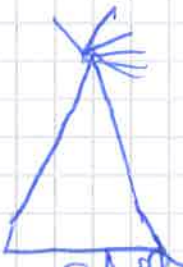
(Evolved Packet Core | 5G Core)

Brand new equipment deployed on the field.

2. OPTION:

NSA

(Non-Standalone)



ng-eNB

eNB has NO support for legacy E-UTRAN interfaces

ng-NB = Next-Generation Base Station

Still maintain some legacy equipment at the base stations.

gNB

LECTURE 9

C-ITS = Cooperative Intelligent Transport Systems

ITS = Intelligent Transport System

⇒ Effort to add "ICT" to transport infrastructure and vehicles to
- Reduce cost
- Reduce environmental impact (pollution)
+ Increase safety (fewer accidents)
+ Increase efficiency (cost & travel)
- Reduce congestion & fuel consumption

⇒ New "actor" in the market, going in the direction of autonomous & connected cars: Apple, Google, Samsung, ...

KETs: Key Enabling Technologies

ISSUE: Very heterogeneous car market, with evolving regulations

ADAS = Advanced Driving Adaptive System

FUTURE TRANSPORT SYSTEM = Internet of vehicles, with vehicles connected to one another and infrastructure "communicating" with vehicles

RSU ⇝ OBU

Road-Side Unit & On-Board Unit

COOPERATIVE SYSTEM: Network of systems collaborating for a common goal, interconnected with one another.

INFRASTRUCTURE (ROAD): Needs to support ALL the vehicles running on it.

⇓

STANDARDIZATION ⇒ EU required!

CAES 20/CAS 21 within the Digital Agenda for Europe (DAE)

⇒ Deliver sustainable economic & social benefits from a digital single market based on:

EU NORM: Non-mandatory technical specifications to be followed (adopted) by the different EU member states.

HARMONIZED STANDARDS: Based on request of a Commission for harmonization

- INTERNATIONAL STANDARD (ISO) International Standard
- EUROPEAN STANDARD (ETSI) (European Norm)
- NATIONAL STANDARD (Norma Tecnica Nazionale)

STANDARD'S APPROVAL: Requires a consensus among a set of experts of that field.

2014 → C-ITS PLATFORM for a "SHARED" VISION of C-ITS

2019 → Large-scale implementation C-ITS

ALL ABOUT STANDARDS:

STANDARD ≠ PROPRIETARY VERTICAL IMPLEMENTATIONS (complex & costly to develop & maintain)

Allows for COMPETITION / INNOVATION / INTEROPERABILITY / INTERCHANGEABILITY (e.g. for the consumer)

STANDARD = Technical document that uses as a RULE [agreed way to do something]

ETSI = European Telecommunications Standards Institute

Produces standards applicable not just to Europe, but also worldwide.
Big companies also have some power to affect standards!

V2X = Vehicle-To-X

X = { Infrastructure / Vehicle }

IEC (Electrotechnical) | ISO | ITU (Telecommunications)
CENELEC | CEN | ETSI

Made up of one representative per member state [CABINET GOVERNMENT-like]

EUROPEAN COMMISSION: Executive body of EU; responsible for proposing legislation, implementing decisions, upholding EU treaties and 'running' the EU.

SPECTRUM ALLOCATION: — ITS

5,875 – 5.85 MHz for safety-related ITS applications
"free" spectrum

ETSI : Sophia-Antipolis (France).
GSM (3GPP), Smart Cards, Electronic Signatures, IoT M2M
64 countries, 5 continents (not yet)

"PLUGTESTS" = interoperability events organized.

STANDARDIZATION follows a (long) process from the standardization request of the EC (European Commission).

ITS' #1 GOAL: ROAD SAFETY for RELEASE 1.

DAY-1 SERVICES of ITS: high-priority services for increasing safety level on motorways / urban scenarios.
(Ex: Hazardous pedestrians / crashed cars / visibility, traffic jam warning, Emergency vehicle signaling)

DAY 1.5: SERVICES & ITS

Increasing traffic's efficiency with intersection safety / vulnerable road users protection.

APPLICATIONS:
- Cooperative Road Safety
- Cooperative traffic efficiency

GEONETWORKING: (L-3)

Address internet peer via their geographical location (≠ IP-based addressing)

=> Send data to a specific geographical location [GPS-based].

GEOMULTICAST / GEOBROADCAST: Send data to all systems in a certain area

=> Need a way to address IPS based on their geographical location

SERVICE CHANNEL VS CONTROL CHANNEL
(Not real-time - critical) (real-time critical)

ISSUE: "Packets' storm".
A crash occurs & its signal log many different cars.
=> A STORM of PACKETS is sent & interference is created (CONGESTION)

⇒ We need a CONGESTION-CONTROL MECHANISM, that allows to:

- Prioritize CONTROL MSGS
- Slow down the rate of messages being transmitted (PAYLOAD, actual data transmitted)

Cars equipped with IEEE 802.11p are already on the road! ⇒ We still need ways for them to interoperate with one another.

GEONETWORKING means a SPACE + TIME way to address cars (at a certain location, in a certain time interval)

+ MOBILITY over IPV6 (NEMO ⇒ Standards for Network Mobility.

LECTURE 8 - WiFi

WiFi = Wireless Fidelity (IEEE 802.11)

Most widespread WIRELESS communication medium (& continuing)

WPAN -> WMAN -> WLAN
(Bluetooth) (LTE) (WiFi)

WiFi dominates when it comes to WLAN connections!

Remember: Signal's data rate decreases as strength (SNR) decreases.

SNR ↓ Data rate ↓

WiFi's FREQUENCIES: 2.4 GHz | 5 GHz | 60 GHz
Depending on the version adopted.

WiMax: Up to 50 kms range.

IEEE 802.11 a/b/g: 54 Mb/s

IEEE 802.11 n: + MIMO
Up to 600 Mb/s

IEEE 802.11 ac: Up to 1 Gb/s, in multi-station mode.

WLAN REQUIREMENTS

- SCALABILITY in the # NODES
- SECURITY against eavesdroppers
- ROBUSTNESS

- ISM band for frequencies / FREE, unregulated spectrum
- RANGE: 100-300 m
- SPECTRUM = allocation into a set of channels, to be used by different base stations for reduced interference.
  (EU: lower power & range ; US: higher power allowed)
- ROAMING among different base stations, switch over spots.

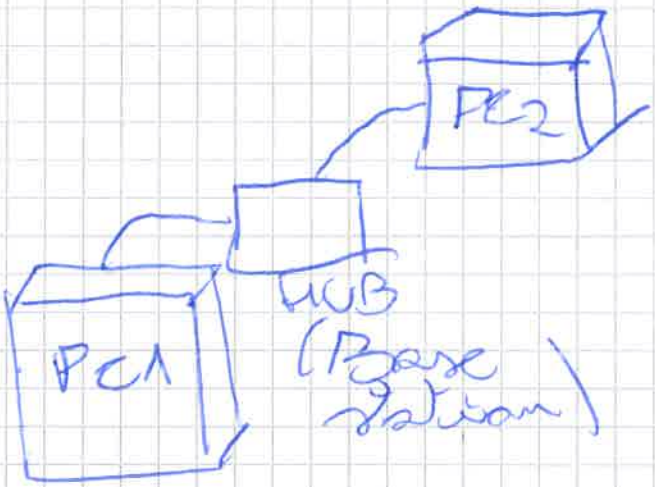
(PDU) = Packet Data Unit, made up of protocol-specific information.

↳ UDP ⇒ Datagram

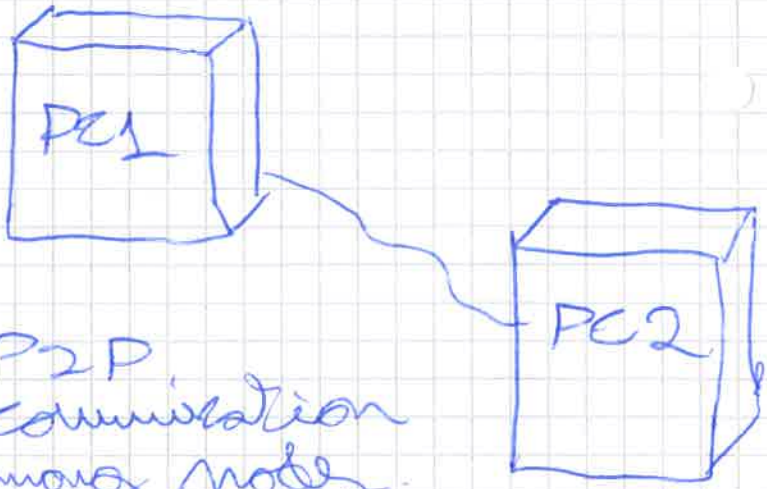
↳ TCP ⇒ Segment

WIFI - MODES:

NOMADIC ACCESS



AD-HOC ACCESS



IEEE 802.11

ARCHITECTURE

Many different versions (STANDARDS) of IEEE 802.11

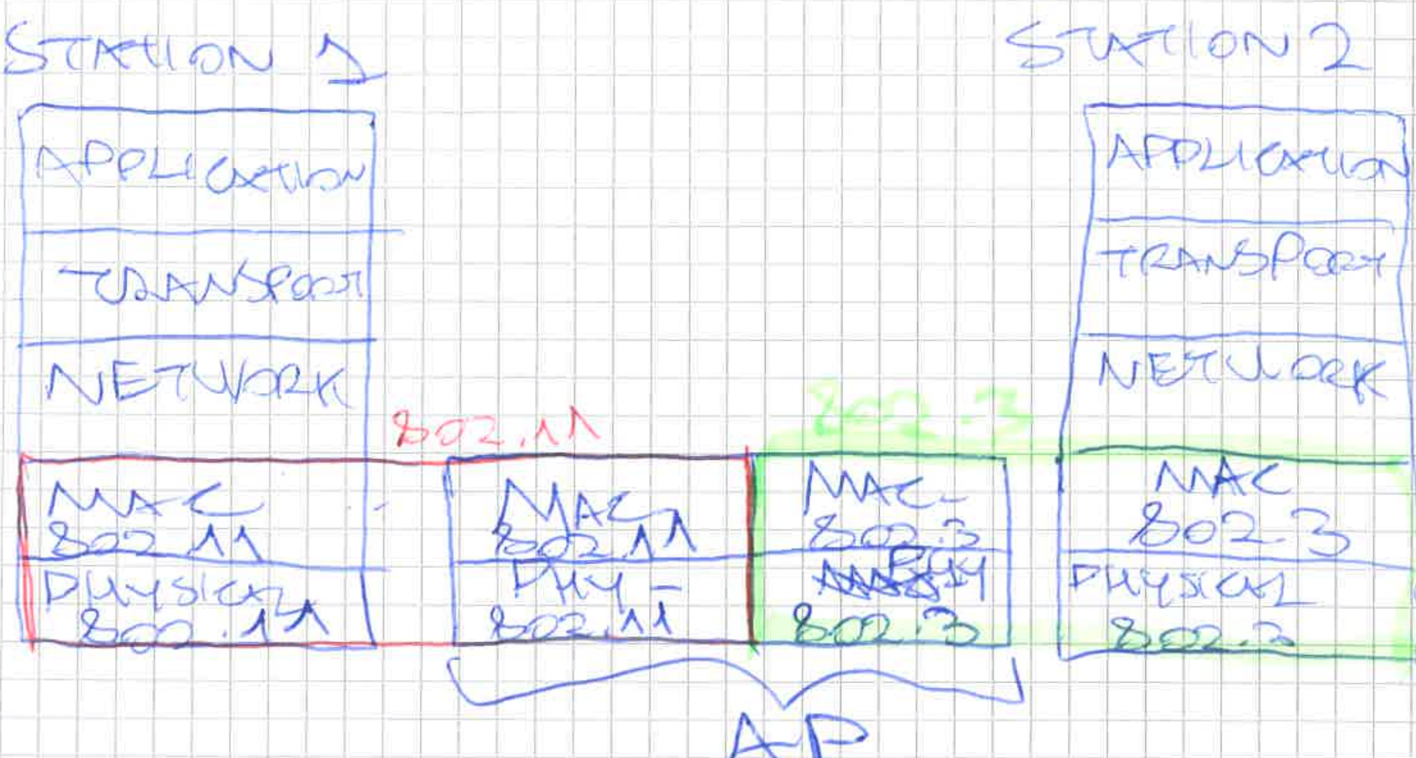
sist, but they all share some common CHARACTERISTICS.

[Different standards => Different frequencies]

Different BANDWIDTH & DATA RATE <=> different modulation techniques.

NB: The higher the frequency, the higher the data rate, the more expensive the equipment & the higher the SENSIBILITY to INTERFERENCE & to IMPAIRMENTS [& the smaller the range]
(because of smaller λ)

ETHERNET [802.3 => Acts as a backbone LAN for 802.11]



IEEE 802.11 defines the PHY & MAC standards only.

	LLC - Logical Link Control	MAC
	MAC	
(Mapping of MAC units to MPDUs) PLCP	PHY-LAYER CONVERGENCE PROCEDURES	PHY
(Characteristics of wireless medium) PMD	PHYSICAL-MEDIUM DEPENDENT	

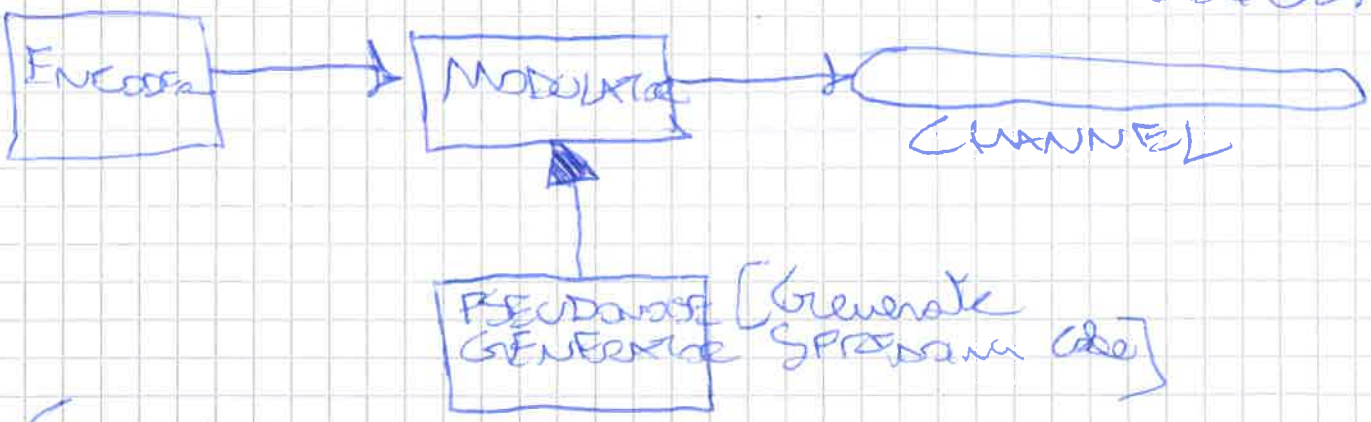
SPREAD - SPECTRUM TECHNIQUES.

SPREAD SPECTRUM is a technique Used to transmit either ANALOG or DIGITAL data using an ANALOG SIGNAL.

ORIGIN:
⇒ Developed initially for MILITARY & INTELLIGENCE requirements.

IDEA: Spread the INFORMATION SIGNAL over a wide transmitted to make JAMMING & INTERCEPTION more difficult

⇒ Signal is MODULATED using a sequence of DIGITS [SPREADING CODE / SPREADING SEQUENCE]



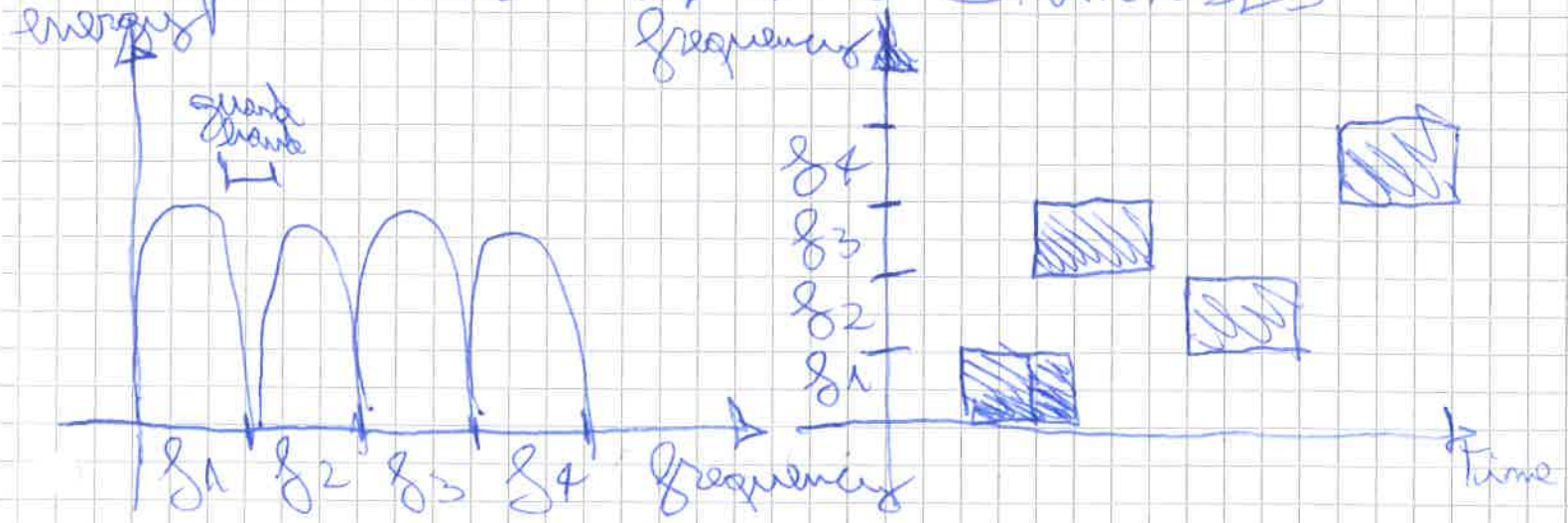
GOAL:
⇒ By modulating the signal with a SPREADING CODE, we aim to

- Increase significantly the BANDWIDTH (side effect)
- Gain IMMUNITY from NOISE & MULTIPATH DISTORTION. (Ex: Jamming)
- Hide & encrypt SIGNALS. (need to know SPREADING CODE for decoding data)
- Share BANDWIDTH with minimal INTERFERENCE through CDMA.

Reduced impact & INTERFERENCE & JAMMING

FHSS - FREQUENCY HOPPING SPREAD SPECTRUM

In FHSS, the available bandwidth is split into MULTIPLE CHANNELS



=> To TX, the SIGNAL is broadcast over an apparently RANDOM SERIES of RADIO FREQUENCIES, hopping from frequency to frequency at regular time intervals

=> To RX, the receiver hops among frequencies in the same manner as the transmitter (They need to be SYNCHRONIZED)

2 APPROACHES:

- SLOW HOPPING: One frequency for many BITS' transmission
- FAST HOPPING: One frequency for few bits' transmission

=> HOPPING SEQUENCE: Pattern according to which the channels are "hopped" by the transmitter & receiver

Cons: (Different TRANSMITTERS cannot use different HOPPING SEQUENCES at the same time!)

DSSS – DIRECT SEQUENCE SPREAD SPECTRUM

In DSSS, each BIT of the original BIT STREAM is represented by multiple BITS in the transmitted SIGNAL, using a SPREADING CODE. The SPREADING CODE spreads the signal across a wider frequency band in direct proportion to the # BITS used for spreading.

(EX: 10-BIT spreading code spreads the signal across a frequency band 10 times greater than a 1-BIT spreading code)

ONE TECHNIQUE USED – XOR rule:

$0 \oplus 0 = 0 \quad 0 \oplus 1 = 1 \quad 1 \oplus 1 = 0$

The SEQUENCE with which the original signal is XORed is called CHIPPING SEQUENCE

⇒ Need to know the CHIPPING SEQUENCE to decode the SIGNAL

PSEUDO-RANDOM NOISE

⇒ t_b = BIT DURATION

t_c = CHIP DURATION

⇒ Bandwidth increases by

⇒ Data rate goes down by $\frac{t_b}{t_c}$ → BIT duration / CHIP duration (& CHIP SEQUENCE)

$\frac{t_b}{t_c} = \#$ BITS used for spreading

⇒ REDUNDANT BITS introduced

$t_c << t_b$

Also, DSSS performs a XOR of the signal with a CHIPPING code (need for the CHIPPING code to recover the signal)

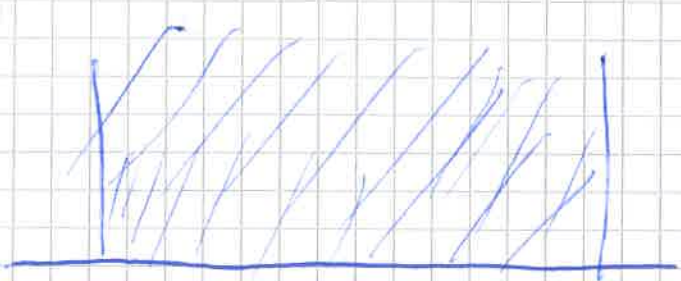
FHSS: The pattern followed by transmitters to hop over channels is called "HOPPING SEQUENCE".

=> Different transmitters may use different HOPPING SEQUENCES, so that they do NOT interfere with each other & transmissions are MUXed effectively

OFDM: Orthogonal Frequency Division Multiplexing

Solves the problem of MULTI-PATH interference with one single CARRIER.

WIDE-BAND



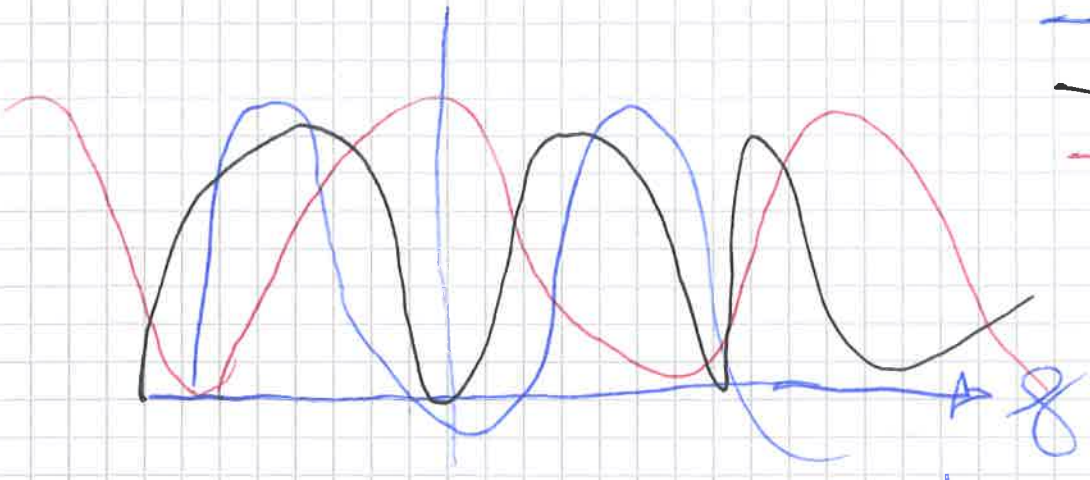
Transmit over a large BAND

↳ Lots of INTERFERENCE

NARROW-BAND CHANNELS

Transmit concurrently over multiple ORTHOGONAL sub-channels, hence reducing interference among different sub-channels

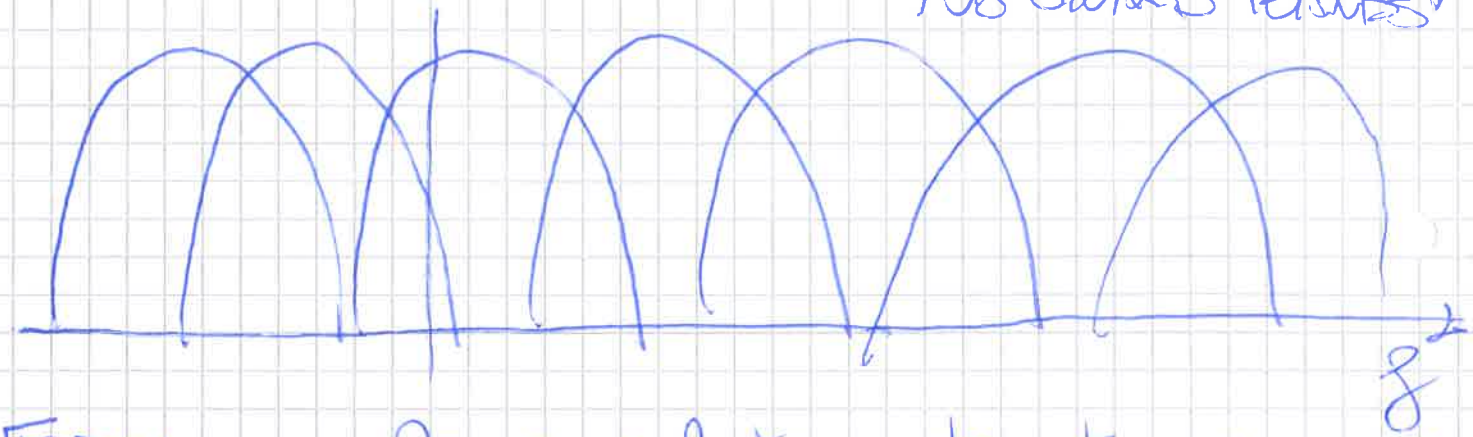
NO GUARD BANDS are needed & multi-carrier interference is REDUCED.



DIVISION SUB-CARRIERS

OFDM

In OFDM NO GUARD BANDS

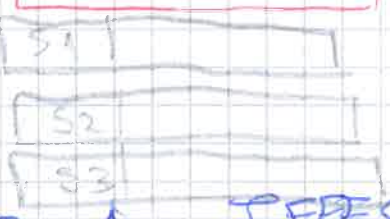


FDM is also a solution to the issue of INTER-SYMBOL INTERFERENCE: in fact leveraging MULTIPLE CARRIERS, the interference is reduced and high data rates can still be attained! (fewer symbols rate for same DATA THROUGHPUT)

Data rate 54 Mb/s => 64-QAM MODULATION

IEEE

MAC IN 802.11



ASYNCHRONOUS data servicing in IEEE 802.11

=> TIME-BOUNDED service, with different users competing for the same resources in INFRASTRUCTURE-BASED mode.

↳ CSMA/CA used for resolving collisions in DCF (DISTRIBUTED COORDINATION F...

DCF - DISTRIBUTED COORDINATION FUNCTION.

Mandates the use of CSMA/CA:

[Carrier Sense Multiple Access / Collision Avoidance]

"~~Random~~ Binary Exponential backoff": whenever a collision occurs, must wait 2x as much time before transmitting again.

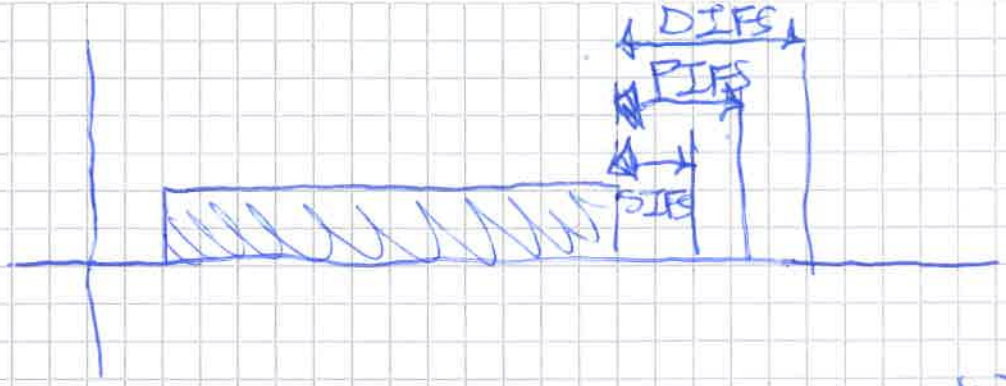
→ 2, 4, 8, 16, 32, ...

Idea: Before transmitting, sense the channel & transmit only if no one is transmitting [CHANNEL detected to be idle]

→ PRIORITY of DATA: managed via IFS, Inter-Frame Spacing.

Separates the frames being transmitted / the shorter, the higher the priority!

- 1 DIFS (Distributed InterFrame Spacing) [longest, ASYNC. frames]
- 2 PIFS: Used by central coordinator to handle polling (Point InterFrame Spacing)
- 3 SIFS: (Short InterFrame Spacing) Used for REAL-TIME / immediate response actions, Ex: ACKs.

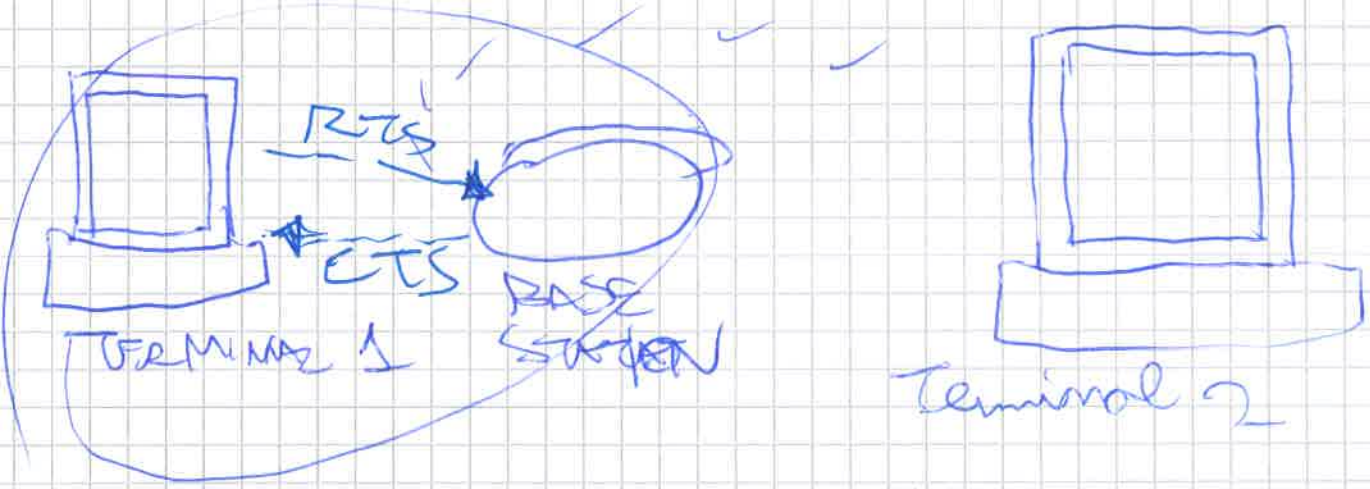


RANDOM BACKOFF: $[0, 2^n]$, where n = # OF TRANSMISSION ATTEMPTS.

X = Waiting time, $X \in$ in the range given.

If a collision occurs, $n = n+1$.

HIDDEN TERMINAL PROBLEM:



Terminal 1 don't see terminal 2, yet collisions still occur at the base station.

Over the NAV Net Allocation Vector

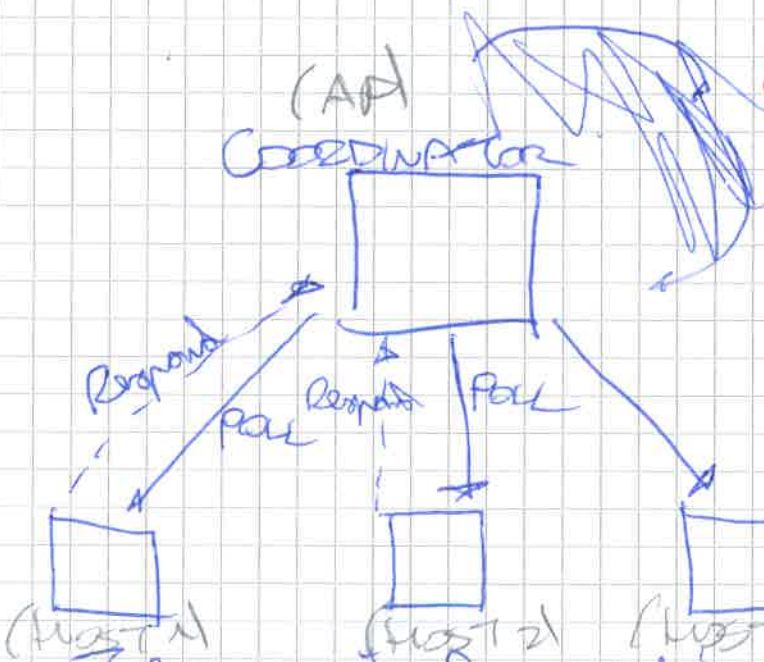
=> Use an RTS (Request To Send) to reserve transmitter to transmit.

=> Use a CTS (Clear To Send) to "confirm that transmission can indeed happen (no AP → host)

PCF - Point Coordination Function

Transmit in a ROUND-ROBIN fashion over time periods reserved for different stations

wanting to transmit.



(AP)
COORDINATOR "polls" each station, asking if it wants to transmit [BEACONS]
by
Each station can respond or stay silent.

Centralized: AP receives requests and PIFS.

The central coordinator can then schedule the requests it has received over the NAV.

~~MOBILITY in IEEE~~

FURTHER MAC FEATURES:

POWER SAVING: via sleep functionalities

ROAMING: for joining a network / changing AP

ASSOCIATION: Establish initial connection between device and AP.

AUTHENTICATION: Establish stations' identity to each other.

MOBILITY in IEEE 802.11p

IEEE 802.11p, amendment for VEHICULAR NETWORKS

(RSU ↔ OBU communication) VANETS

PHY + MAC changed

20 MHz → 10 MHz channel

DATA RATE: 6 - 27 Mbps

higher power level, to fit an outdoor high-speed scenario. [Up to 1 Km range]

V2X → X = Vehicle
→ X = Infrastructure

VRR = Vehicular Reactive Routine protocol.

Take advantage of multi-channel scheme to support:

- Up to ≈ 200 Km/h
- Response times Up to 100 ms
- Range ≈ 1 Km

Radio Access Technologies

Current RATs are:

C-V2X = Cellular V2X

DSRC = Dedicated Short-Range Communication

5.9 GHz band

Issues in the deployment

~~4G~~ 5G GHz +

IEEE 802.11bd

IEEE task group aimed at evolving IEEE 802.11p [BACKWARD COMPATIBILITY ensured & INTEROPERABILITY

INTEROPERABILITY, FAIRNESS and CO-EXISTENCE

IEEE 802.11p.

OFDM-based transmission

+ DUAL-CARRIER modulation (over frequency) to achieve diversity

2x RETRANSMISSION to increase reliability

LECTURE 9 - SECURITY IN IoT CONTEXT

SECURITY CONTEXT:

A large Technology EXPLOSION has enabled the GROWTH IN # CONNECTED DEVICES (IoT Devices & CLOUD) connected to the internet

↳ ATTACK surface has GROWN & has raised attention of MALICIOUS USERS

ATTACKED: Ever-more complex Attacks, exploiting one vuln in the system.
[Continuously changing techniques, mainly straightforward, yet effective]

DEFENDED: Needs to DEFEND the system against all possible THREATS ⇒ Needs to "cover" all the rules of the system
[In-advance training]

CISCO IoT REPORT - 2018:

- MALWARE: Ever more sophisticated & complex
- CLOUD SERVICES: Used also for malicious intents
- IoT / CLOUD SERVICES: Adversaries use SECURITY GAPS in such systems
  ↳ IoT BOTNETS (Ex: Mirai) are increasing!

⇒ IoT DEVICES keep being added to organizations, yet few of them even know how many IoT devices there are

SYMANTEC – 2019 INTERNET SECURITY THREATS REPORT:

MAIN ~~ATTACK TARGETS~~ SOURCES & IOT ATTACKS: Router | Camera. Instrumented for an ATTACK.

MAIN TARGETED PROTOCOLS: Telnet | HTTP | SSH.

MAIN PORTS: 23 (Telnet), 80 (HTTP)

SECURITY REQUIREMENTS in IoT:

- Authentication: Accessibility to resources is granted only to authenticated users.
- Availability: Data can be retrieved when needed by authorized users.
- Authorization: Only authorized users can access Data/Resources.
- Privacy: Data protected from intrusions & non readable from unauthorized entities.
- Confidentiality: Network knows where to and from where data is sent.
- Integrity: Data is complete, accurate.

[Analogous to requirements in a DB]

⇒ Attacks are carried out at 3 main layers, them being:

- INFORMATION LAYER: DATA COLLECTION, EXTRACTION/PERCEPTION means

[Ex: Sensors gathering data] WSNs, wireless sensors getting data from the field.

⇒ ATTACKS: Sensing, probing, eavesdropping, mining.

SEC. GOALS:

[Need to respect user/DATA privacy & AUTHORIZATION to ensure SECURITY]

- CONNECTIVITY LAYER: Transmit the DATA received by the INF. LAYER from one terminal to another one.

[Ex: Router | Switch for WiFi | Bluetooth | Zigbee]

↳ ATTACKS: Manipulation of computation on the users' data | man-in-the-middle.

↳ SYBIL ATTACKS: DoS & more listening & requesting resources are simulated.

↳ SINKHOLE ATTACKS: Gather | divert resources of a device, such that actual users cannot use them.

(Analogous to DDOS)

SEC. GOALS: Data INTEGRITY & AUTHENTICATION

- APPLICATION LAYER | MIDDLEWARE LAYER: Provides final access to FEATURES to the user [what a programmer actually codes ⇒ heterogeneous implementation]

↳ ATTACKS: spoofing, sniffing, DoS attacks.

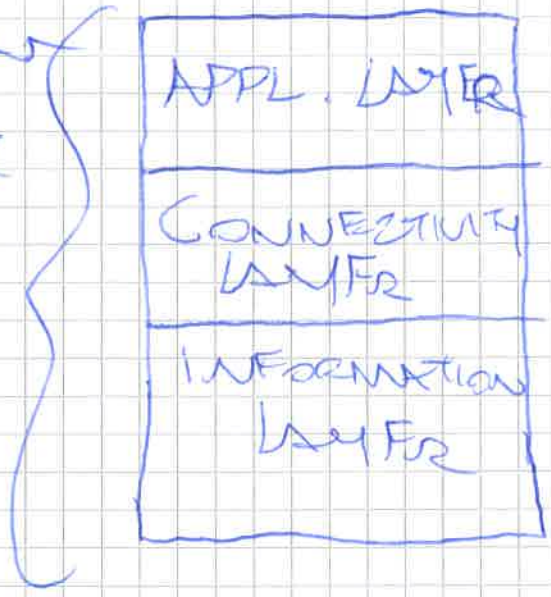
SEC. GOALS:

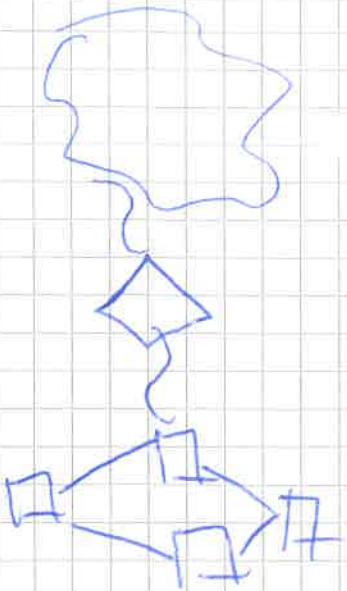
[Authorization, DoS are respected]

⇒ Based on the SECURITY REQUIREMENTS of an application, fitting corresponding SECURITY MECHANISMS & TECHNOLOGIES need to be picked.

MAIN SECURITY THREATS:

LAYERS' STACK in IoT WORLD





APPL. LAYER THREATS

- Programmers not concerned about SECURITY ASPECTS.
- 3rd-PARTY SW used "blindly" ⇒ not be managed

SOLUTIONS:

To "protect" your system
- Hire a Team of SECURITY EXPERTS
- OAUTH for "delegating" authentication in REST.

CONNECTIVITY LAYER THREATS

- Use BLOCKCHAIN and a distributed AUTHENTICATION mechanism.
-

INFORMATION LAYER THREATS:

- Loopholes in IoT devices are always present!
- Increase the # DEVICES ⇒ lower QoS & higher latency

STANDARDS (EX: ONEM2M) are NOT sufficient to ensure SECURITY.

=> Need to be aware of:
1) #DEVICES in network
2) SECURITY REQUIREMENTS of each services

SECURITY LEVEL of an APPLICATION:

$$\text{SECURITY LEVEL} = \min_{i=1}^{n} \{SC_1, \ldots, SC_n\}$$

The SECURITY LEVEL is given by the least secure component in the network.

=> We need to ensure all links are SECURE to have a fully-secure application

~~CRITICAL FLOWS~~ FUTURE of IoT SECURITY:

IoT, CLOUD, FOG COMPUTING: More and more attack targets => Need for SECURITY SOLUTIONS over all parties involved (Distributed securing)

BLOCKCHAIN: One of the candidate approaches for SECURITY PROBLEMS in IoT Environment.

EXAMPLES → TRACK SYSTEM information To detect ~~malfunctions~~ anomalies
→ LOGGING DEVICE BEHAVIOUR over time, ensuring FAIR system Resources' distribution
=> DISTRIBUTED TRANSACTIONS' PROCESSING

DATA INTEGRITY & TRUSTWORTHINESS:
Needs to be well-preserved to prevent/detect cyber attacks.

→ 3 MAIN APPROACHES →
- CRYPTOGRAPHY (public-private key encryption)
- BYZANTINE AGREEMENT (distributed systems)
- DATA PROVENANCE (logs to track data movements)

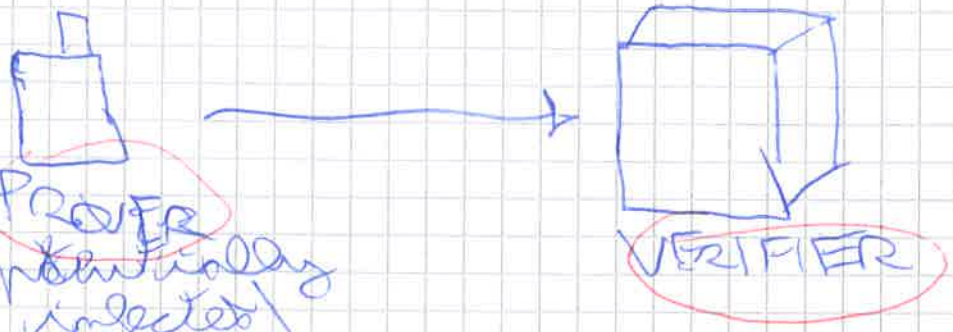
CRITICAL FLOW (financial transactions) needs to be encrypted & protected from cyber attacks

SDNs more and more widely deployed to improve resilience of CRITICAL FLOWS via ISOLATION & GLOBAL VISIBILITY.

Software-Defined Networking
L SDN CONTROLLER (has global knowledge)

OPEN CHALLENGES in IoT

- AUTHENTICATION (before "you-know", "you-have", "you-are" paradigm)
  - PUBLIC VS PRIVATE CERTIFICATES? → no longer applies in embedded IoT devices
- DYNAMIC NETWORK & IoT DEVICES: # DEVICES constantly changing in a network
  - = SCALABLE to large # DEVICES - RISK-AWARE
  - = DECENTRALIZED, ~~no single PoF~~ RISK-TOLERANT



REMOTE ATTESTATION carried out to ensure that a device is who he claims to be.

PAST REMOTE ATTESTATION: Static, based on security protocols or HASH (Ex: Hash of a signature or a SW BINARY)

Simple Mover retrieval

CURRENT REMOTE ATTESTION: ~~Control-Flow~~

Needs to ADAPT to a DISTRIBUTED Mover retrieval with millions of devices.
[& Real-time attestation constraints]
⇒ SWARM ATTESTATION required

DEFENSE SYSTEMS

DEFENDER: Want to PREVENT & DETECT possible attacks occurring to the system.
⇒ MONITOR SYSTEMS for ANOMALIES (Ex: Intrusion Attacks)

ATTACKER: Would like to stay anonymous & "stealthy", in order to avoid to hack the system.
[New techniques recorded]

IPS - Intrusion Prevention System

TASK: Apply an ACTIVE RESPONSE MECHANISM to block detected attacks
(Ex: Blacklist IPs temporarily)
⇒ Implies that an ATTACK has been DETECTED.

IDS - Intrusion Detection System:

TASK: Detects an ATTACK being conducted against the system as a PASSIVE RESPONSE MECHANISM
(Ex: Alert System Administrator)

Tesi's MASTER THESIS:
NIDS: Pro software system used to create a tunable & configurable detection system to AUTOMATICALLY PROTECT system by applying rules to protect the network.
4 ATTACK SCENARIOS:
1. SSH - BRUTE FORCE
2. SQL INJECTION
3. IP FRAGMENT OVERLAP
4. TCP SEGMENT OVERLAP;
GOAL: Reduce response time to detect an attack being conducted

HONEYPOT: Vulnerable host left unguarded for the purpose of logging & identifying attacks

ATTACK TYPES CONSIDERED

- **SQL INSECTION**: Caused by LACK of sanitization in handling USER INPUT when passing it to SQL QUERIES
  ISSUE: [Contruction of SQL queries when user input is passed to them]
  DEFENSE: Temporary service Block for a certain IP (PROXY - Chain Drill) Possible

- **SEGMENT OVERLAP ATTACK**: Attacks caused by the MANIPULATION of the sequence number field in the TCP HEADER.
  ISSUE: [RFC does not mandate reassembling policies to be used for TCP/IP => OS-dependent implementation]
  => Use same SEQUENCE NUMBER, but different PAYLOAD.
  DEFENSE: Packet inspection checks for VULNERABLE PACKETS => Blocks IP sending such packets.

=> IOT: Specialize tools to adapt to the specification of the system under test (IoT scenario).

=> MONITOR SYSTEM'S CONDITIONS & report behaviours detected to an OPERATOR.

LECTURE 10 - VISIBLE LIGHT COMMUNICATION

VLC = (V)isible (L)ight (C)omunication

IEEE 802.15.7

Prof. Ciaramella Sant'Anna

RF = Radio Frequency "Standard" radio wave used (invisible)

Line-of-Sight

LOS "You see what you need".

Visible-spectrum communication

⇒ HARMLESS TRANSMISSION in eye-safe frequency bands.

430 THz ; 428 THz [Visible band of light]

RF'S DRAWBACK:

In some application scenarios [HOSPITALS, PLANES], RFs may be harmful for existing infrastructures & may be overcrowded.

⇒ VLC may mitigate RF's drawbacks, covering & may be deployed where RFs cannot be deployed.

⇒ However, principles & lessons learned from RF can also be applied to the VLC world.

PRINCIPLES & VLC:

- Photoelectric effect (Einstein, 1905)

- LED (1927) (Light Emitting Diode) Used for TX

- DIODE Used for RX

WIRELESS VLC: Receive/transmit via a DIODE. No radio waves involved

TX:

DEVICE:

LED → Can to 100 Mb/s. transmits by repeatedly being switched ON/OFF

RX DEVICE

CMOS ⇒ Each pixel is a small photodiode [Image acquisition & data reception]

PHOTODIODE ⇒ Can to 1 Gb/s

NOTIFICATIONS:

- Functions VLC cluster using overcrowded (RF) bands (congested)
- $$$ SAVING, since we can use the energy for LIGHTNING also for DATA TRANSMISSION.
- CHEAP COMPONENTS in VLC devices

LI-FI: Wolfgang Bulb experimental

VLC → downlink 10 Mb/s

RF → uplink 10 Mb/s

NO COMMERCIAL devices are available yet, but MANY companies highly interested & involved.

POWER: Needs to be controlled to ensure eye-safe transmission.

EXISTING VLC DEVICES & DEPLOYMENTS:

- **PURE LiFi**: Inspired by LiFi (IEEE 802.11)
  DOWNLINK: 10 Mbps VLC
  ↑LINK: 10 Mbps RF-based
  RANGE: 3m, standard light fixtures
  FULL MOBILITY enabled by Fine installation & several Access Points (APs)
  [multiple users, multiple lights]
  BANDWIDTH bottleneck

- **FRAUNHOFER VLC**:
  DATA RATE: Up to 500 Mb/s.
  RANGE: 100 m – 120 Mb/s rate.
  3 m – 100 Mb/s
  [Non-LOS]
  Ethernet RJ45 input network.

- **RONJA SYSTEM**: (Building-to-Building)
  DATA RATE: 10 Mb/s FULL DUPLEX ETHERNET (P2P)
  RANGE: 1.4 Km
  Meant for outdoor usage & based on red INFRARED LIGHT.

- **IrDA** for EMBEDDED SYSTEMS
  DATA RATE: 2.4 Kb/s – 4 Mb/s
  RANGE: 1 m
  MODULATION: • RZI if bit rate ≤ 4 Mb/s
  • 4 PPM, at 4 Mb/s
  HALF-DUPLEX LINK.
  Cheap (100 $)

⇒ Industry group - owned.

EYE-SAFETY ⇒ Serious concern @ high DATA RATES.

MODULATION ISSUES in VLC:

RF RESEARCH ⇒ New / upgraded methods for DIGITAL MODULATION.

(EX: TechIP: pureLiFi)

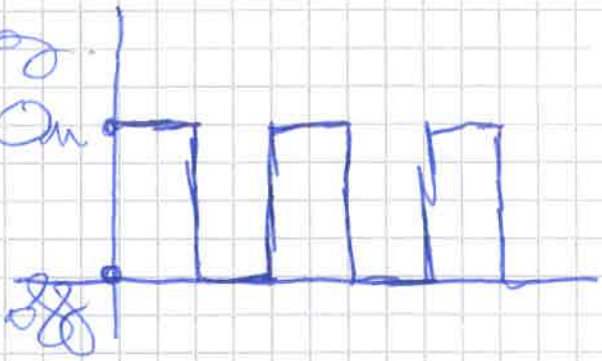
↓ DMT ↓ OFDM

LIGHT DIMMING: [Decrease in LUX & light in an environment]

⇒ We would like to preserve DIMMING functionalities, while still maintaining a reliable broadband channel.

MODULATION SCHEMES for DIMMING.

- OOK: On-Off Keying
  Repeatedly turn ON & OFF the signal, using CONDENSATED SYMBOLS to avoid LIGHT FLICKERING.



- PWM: Pulse Width Modulation
  The pulse WIDTH controls the power load.
- PPM: Pulse Position Modulation
  The pulse POSITION encodes message bits.

PPM & PWM can be combined into VPPM = Variable Pulse Position Modulation

↳ Pulse-width control for light dimming support, mitigating intra-frame FLICKER

IEEE 802.15.7 / 2011 STANDARD

"First safe & capable LIGHTNING fast data communication"

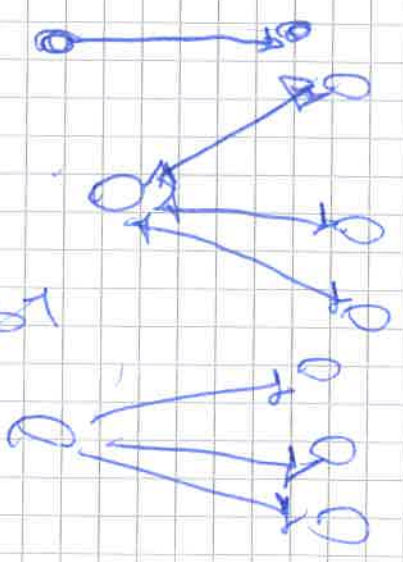
EYE SAFETY is #1 PRIORITY!

IEEE 802.15.7 is a STANDARD for LOCAL & METROPOLITAN Wireless Optical Communication based on Visible Light.

PHY: { PHY I (OUTDOOR) - 11.67 - 266 Kb/s
PHY II 1.25-96 Kb/s

SUPPORTS for DIMMING / FLICKER MITIGATION, VISIBILITY & COLOR FUNCTION.

NETWORK TOPOLOGIES → P2P, STAR, BROADCAST



The PHY LAYER is responsible for:
- Activation & DE TX/RX
- Channel selection

- Data transmission & reception
- Error correction

The MAC LAYER is responsible for handling access to the PHY layer and supports the following tasks:

- Supporting VISIBILITY
- Supporting DIMMING
- FLICKER MITIGATION

PHY TYPES

- PHY I: OUTDOOR USAGE, low data rates [OOK (VPPM)] 100 kHz
- PHY II: INDOOR USAGE, moderate data rates [OOK (VPPM)] 10x Mb/s
- PHY III: CSK (Color Shift Keying) Multiple light sources & detectors 96 x Mb/s

MODULATION TECHNIQUES:

- OOK [ON-OFF KEYING]: Digital data is represented as PRESENCE (ON) OR ABSENCE (OFF) of a signal. No complete switch OFF required
- VPPM [Variable Pulse-Position Modulation] Uses the characteristics of 2-PPM [Pulse-Position Modulation] for NON-FLICKER and PWM for dimming control & brightness.
- CSK [Color Shift Keying] Multiple light sources, RGB

=> Average emitted color & power control

FLICKER MITIGATION

FLICKER = Fluctuation of brightness level in light.

→ INTER-FRAME FLICKER MITIGATION

Use RLL (Run Length Limiting) coding / modulation schemes.

→ INTER-FRAME FLICKER MITIGATION

Accomplished by transmission of an IDLE PATTERN between data frames (where Avg. brightness = that of the data frame)

~~RLL Encoder~~

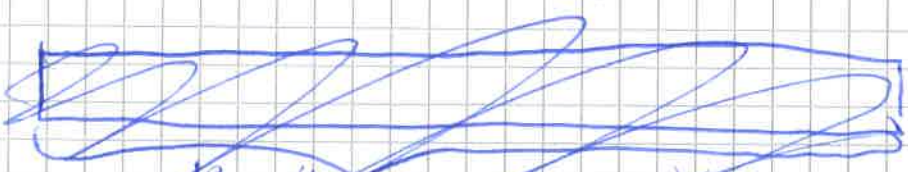
RLL CODE: Bit mapping providing DC balance, clock recovery, flicker mitigation.

FEC: Forward Error Correction: Accomplished by adding REDUNDANCY to the transmitted information using an ALGORITHM

→ REED-SOLOMON CODING

Performs a mapping:

MESSAGE → CODEWORD



K = # SYMBOLS in the message

n = #SYMBOLS IN CODEWORD

$2t = n - K$, where t = MAX. #ERRORS that can always be corrected.

RS(n, K): n = #SYMBOLS IN MSG, K = #SYMBOLS IN CODEWORD, t = MAX. #ERRORS CORRECTABLE

multi-bit SYMBOLS

(S = #BITS in each symbol) ($2t = n - K$)

EXAMPLE:

$n = 15$, $K = 11$ } $2t = n - K$ => $t = \frac{n-K}{2}$

$t = \frac{15-11}{2} = 2$

S = SYMBOL SIZE (#BITS PER SYMBOL)

$n = 2^S - 1 \Rightarrow S = \log_2(1+n) = \log_2(16) = 4$ BITS

NB: THE MATHS FOR ENCODING/DECODING WITH REED-SOLOMON IS ACTUALLY VERY HW-FRIENDLY (JUST XORS / BIT-SHIFTS).

VLC for ITS:

- TRAFFIC SIGNALS & VEHICLES are shifting from "traditional light bulbs to LEDs.

  → V2V, V2I, I2I } Made possible by LED light

⇒ VLC may be a VALUABLE option wrt. RF in case of:
- PACKETS' BROADCAST STORM
- PLATOONING

ISSUES:

- MOBILITY: Not good for LINE-OF-SIGHT communication ⇒ Optimize positioning
- SUNLIGHT / ARTIFICIAL LIGHTS: Noise may affect VLC ⇒ Use optical FILTERS & optimize electronics
- VLC OUTDOOR: FEC mandatory because very frequent errors
  (However, DIFFERENT FECs are suitable for DIFFERENT SCENARIOS)

CURRENT VLC PROTOTYPES:
- Cheap ($)
- Off-the-shelf components
- Standards-compliant

⇒ GOING TOWARDS:

SCALABLE & PERVASIVE VLC integrated into complex VLC systems

RESEARCH in Sant'Anna:

Creation of VLC PROTOTYPES:

- "SIMPLEX" VLC DEVICE, based on 802-like components and standard-compliant (MAC, PHY)

[EX. Seed Eye Board. Wireless Sensor Nodes for C-ITS.

↳ IEEE 802.15.4 interface
↳ IEEE 802.3

S.W DEVELOPMENT ENVIRONMENT

FREERTOS OS: Free Real-Time OS (standard for automotive embedded systems)
1-4 KBs FOOTPRINT.

PROTOTYPE'S ARCHITECTURE:

- PHY LAYER: Activate/deactivate VLC transceiver.
  Data transmission/reception.
  ↳ PHY I: Target low data rates.
  11.67 Kb/s at 200 KHz.

TRANSMITTER

MAC LAYER → RS → Convolutional Encoder → Manchester Encoding

MANCHESTER ENCODING: At the TX.
VITERBI DECODER: At the RX.

RESULTS:

Error-free comunication achieved up to 5.1 meters.

$BER < 10^{-3}$ at 10.2 m.

⇒ FASTER ELECTRONIC DEVICES needed to handle error-correction process & IEEE 802.15.7a achieve higher bit rates.

WORK IN PROGRESS [WIP]:

- "Port" optical RX/TX functions to an FPGA (Parallel processing HARDWARE) Field Programmable Gate Array
- Implement IPv6 - IEEE 802.15.7 for IoT infrastructures.
- Low-cost interface for RX and TX, suitable for peer-to-peer VLC.
- Standardize IEEE 802.15.7 at the ETSI & ISO level.

Ex: - Smart HEADLAMPS for cars.

- Full-DUPLEX IEEE 802.15.7

OPEN ISSUES:

- High speed DATA TRANSMISSION (bandwidth)
- LOS & mobility (handover) undergoing
- How to use VLC in current telecom networks?

APPLICATION AREAS of VLC:

- High-speed indoor wireless communication
- Hybrid solutions VLC/WiFi
- Vehicular Ad-hoc Networks (VANET)
- Underwater communication

CLOUD COMPUTING

IoT

C-ITS

Personalized HEALTH CARE

FPGA: Portable Integrated Circuits