Machine-to-Machine Communications

Design of PHY and MAC layers for a WSN regarding the application

5ISS

T.U. Communication technologies for IoT - Wireless Sensors Network

Gaël LOUBET, Lamoussa SANOGO, Daniela DRAGOMIRESCU, Eric ALATA

first_name.name@{laas; insa − toulouse}.fr

2023-2024

Table of contents

1. Learning objectives
2. Conduct of the laboratory project
3. Ressources
4. Evaluation
5. General introduction
6. Machine-to-Machine Communications
7. Software Designed Radio
8. Digital modulations
9. Proposed applications

Table of contents

1. Learning objectives
2. Conduct of the laboratory project
3. Ressources
4. Evaluation
5. General introduction
6. Machine-to-Machine Communications
7. Software Designed Radio
8. Digital modulations
9. Proposed applications

Learning objectives

- Make the connection between courses, theory and applications.

- Understand how SDR (Software Defined Radio) works and its advantages, but also use tools like GnuRadio and USRP (Universal Software Radio Peripherals) to imagine and implement applications.

- Study, then design and implement a Machine-to-Machine (M2M) communication using Wireless Sensors Network (WSN) for different applications.

- Explicit and consider the specifications of each application, but also the constraints specific to WSN (e.g. energy efficiency).

➜ Design of an energy efficient M2M communication at PHY (Physical) and MAC (Medium Access Control) layers.

Table of contents

1. Learning objectives
2. Conduct of the laboratory project
3. Ressources
4. Evaluation
5. General introduction
6. Machine-to-Machine Communications
7. Software Designed Radio
8. Digital modulations
9. Proposed applications

Conduct of the laboratory project

- 5 laboratory sessions in GEI 105 (for 13 hours and 45 minutes)
  - 3 supervised (Gaël LOUBET and Lamoussa SANOGO)
    Introductory presentation during the first session
  - 2 in autonomy
- Work group
  - 6/7 students per group from different specialities
  - An application per group
  - 2 students working on each layer

Table of contents

1. Learning objectives
2. Conduct of the laboratory project
3. Ressources
4. Evaluation
5. General introduction
6. Machine-to-Machine Communications
7. Software Designed Radio
8. Digital modulations
9. Proposed applications

Ressources

- Dilhac, Jean-Marie. *Une introduction aux télécommunications.* Presses Universitaires du Mirail, 2009.
- Proakis, John G., and Masoud Salehi. *Digital communications.* Vol. 4. New York: McGraw-hill, 2001.
- Johnson Jr, C. Richard, and William A. Sethares. *"Telecommunication Breakdown." Concepts of Communication Transmitted via Software-Defined Radio.* Pearson: Prentice Hall, 2004.

- Projet RALF : https://sourceforge.isae.fr/projects/ralf/wiki

- Cours INSA et Moodle...
  - ➔ Boyer, Alexandre. *Canaux de transmissions bruités.*
  - ➔ Dragomirescu, Daniela. *Réseaux mobiles.*

Table of contents

1. Learning objectives
2. Conduct of the laboratory project
3. Ressources
4. Evaluation
5. General introduction
6. Machine-to-Machine Communications
7. Software Designed Radio
8. Digital modulations
9. Proposed applications

Evaluation

Report and attendance

A self-sufficient report per group to be included in the portfolio.

The report should include:

- an introduction with the context.
- a summary of all the work carried out during the laboratory project (explanations of the concepts covered, justification of the choices made, problems encountered and solutions implemented, etc.).
- a conclusion with an analysis of your work and of the knowledge and skills developed during this course.

Table of contents

1. Learning objectives
2. Conduct of the laboratory project
3. Ressources
4. Evaluation
5. **General introduction**
6. Machine-to-Machine Communications
7. Software Designed Radio
8. Digital modulations
9. Proposed applications

Telecommunications

Transmission or communication

Emission from one point and reception from one or several points of something (material, data, energy)

Examples

Mail, pneumatic tubes, etc. — Sound, ultrasound, etc. — Heat, electrons, etc.

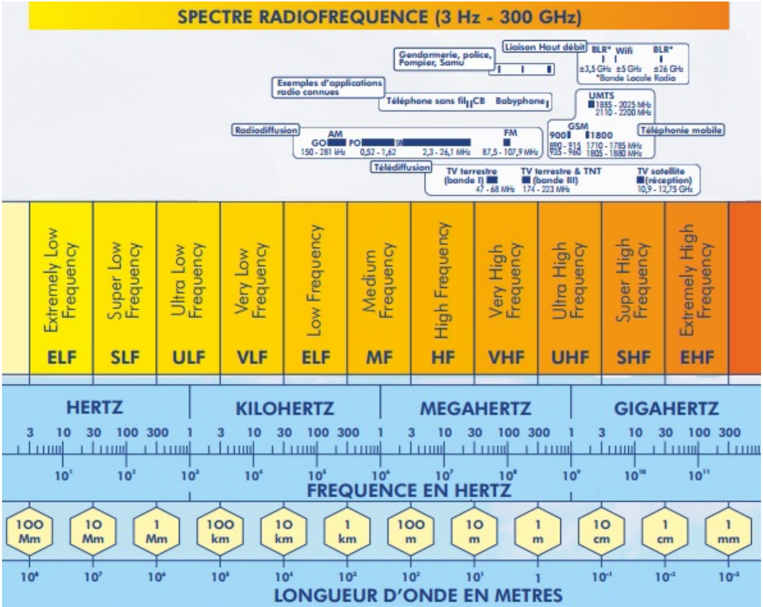
Telecommunication

The transmission -emission and reception- of information from one point to one or more points by means of electromagnetic signals.

Examples

Electricity (electric wires, coaxial cables, twisted cables, etc.) — Electromagnetic waves (magnetic waves, radio frequency waves, light waves (fibres), etc.) — Conducted or radiated.

Radio frequency spectrum



Radio frequency spectrum regulation

Standardisation agencies

ITU	International Telecommunication Union
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
AFNOR	Association Française de NORmalisation
IEEE	Institute of Electrical and Electronics Engineers

Regulation agencies

ARCEP	Autorité de Régulation des Communications Electroniques, des Postes et de la distribution de la Presse
➔ ART	Autorité de Régulation des Télécommunications
ANFR	Agence Nationale des FRéquences

Radio frequency spectrum regulation

ISM – Industrial, Scientific and Medical frequency bands for radiocommunicationq

ETSI	EN 55011
European Radiocommunications Committee (ERC)	Recommendation 70-03

The frequency bands and associated transmission powers depend on a number of factors (international and national standards, types of application, etc.).

Not everything is allowed, neither in transmission nor in reception!

Main ISM bands

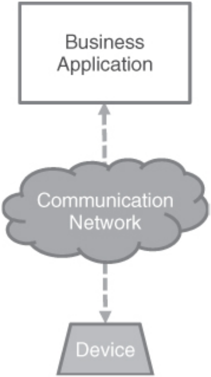
6.765 - 6.795 MHz	
13.553 - 13.567 MHz	
26.957 - 27.283 MHz	
40.660 - 40.700 MHz	
433.05 - 434.79 MHz	10 mW or 10 dBm
863 - 870 MHz	500 mW or 27 dBm
2.4 - 2.5 GHz	100 mW or 20 dBm
5.725 - 5.875 GHz	200/1000 mW or 23/30 dBm
24.0 - 24.25 GHz	
61.0 - 61.5 GHz	
122.0 - 123.0 GHz	
244.0 - 246.0 GHz	

Table of contents

1. Learning objectives
2. Conduct of the laboratory project
3. Ressources
4. Evaluation
5. General introduction
6. Machine-to-Machine Communications
7. Software Designed Radio
8. Digital modulations
9. Proposed applications

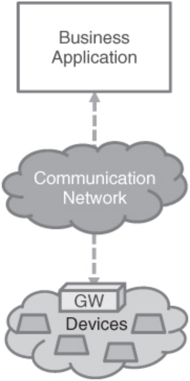
What is M2M?

M2M is to establish the conditions that allow a device to exchange information with a business application *via* communication network.
So, we often call it M2M which is shortened called for M2(CN2)M:
Machine-to-(communication-network-to-) Machine.



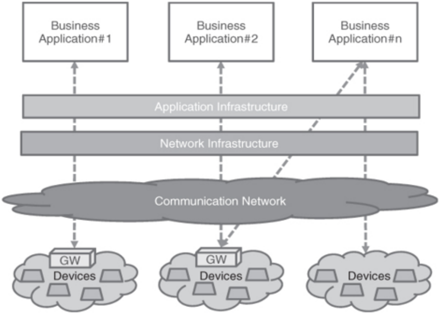
Mediated M2M relationship

M2M involves a group of devices communicate with a single application. Because of the limited capacities, the relationship is mediated by gateway. This M2M area network provides physical and MAC layer connectivity between different M2M devices in the same M2M area network, then allowing M2M devices to gain access to a public network *via* a router or a gateway.



M2M service layer

A set of architectures and processes will be functional separated. This kind of separated infrastructure will improve the cooperation between each network and protocol. Besides, the deployment of M2M applications could benefit from these building blocks which can accelerate the development, test and deployment life cycles.

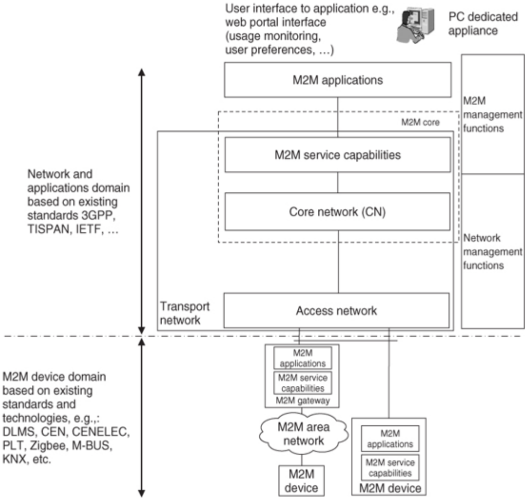


M2M system architecture

The common M2M system architecture includes:

- M2M device: Device that runs M2M application, using M2M service capabilities and network domain functions with direct connectivity or using a gateway as a network proxy.
- M2M area network: providing PHY and MAC layers connectivity between different M2M devices connected to the same M2M area network or allowing M2M device to gain access to a public network via a router or gateway, such as IEEE802.15.X, Zigbee, Bluetooth, PLC or WIFI.
- M2M gateway: It is an equipment that has at least a WAN communication module (e.g. GPRS/UMTS) in addition to one or several communication modules that allow access to the M2M area network (e.g. Zigbee, PLC, etc.). The M2M gateway will provide access network, transport network and sometimes M2M applications

M2M system architecture


User interface to application e.g., web portal interface (usage monitoring, user preferences, ...)
PC dedicated appliance
M2M applications
M2M core
M2M service capabilities
Core network (CN)
Transport network
Access network
M2M management functions
Network management functions
Network and applications domain based on existing standards 3GPP, TISPAN, IETF, ...
M2M applications
M2M service capabilities
M2M gateway
M2M area network
M2M device
M2M applications
M2M service capabilities
M2M device
M2M device domain based on existing standards and technologies, e.g.,: DLMS, CEN, CENELEC, PLT, Zigbee, M-BUS, KNX, etc.

Future of M2M systems

In the future, for a real deployment of M2M systems, applications will increasingly focus on logic functions such as data mediation, security and device management. It will be based on a set of open, standardized and IT-friendly APIs. Horizontal platform has to provide access to more core network interfaces with services like location or QoS, without the burden of implementing protocols, because the complexity has to be hidden through the use of single open API. Devices have to implement an open interface toward the horizontal platform and service capabilities are exposed to device applications similar to the network side.

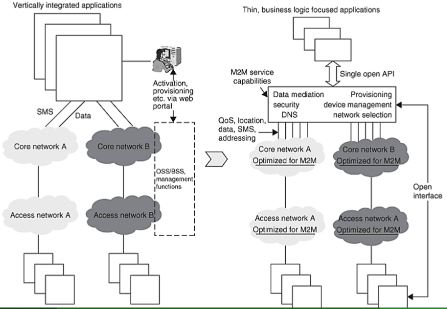

Vertically integrated applications
Activation, provisioning etc. via web portal
SMS
Data
Core network A
Core network B
OSS/BSS, management functions
Access network A
Access network B
Thin, business logic focused applications
M2M service capabilities
Single open API
Data mediation
security
DNS
Provisioning
device management
network selection
QoS, location, data, SMS, addressing
Core network A Optimized for M2M
Core network B Optimized for M2M
Open interface
Access network A Optimized for M2M
Access network A Optimized for M2M

Table of contents

1. Learning objectives
2. Conduct of the laboratory project
3. Ressources
4. Evaluation
5. General introduction
6. Machine-to-Machine Communications
7. Software Designed Radio
8. Digital modulations
9. Proposed applications

Software Designed Radio

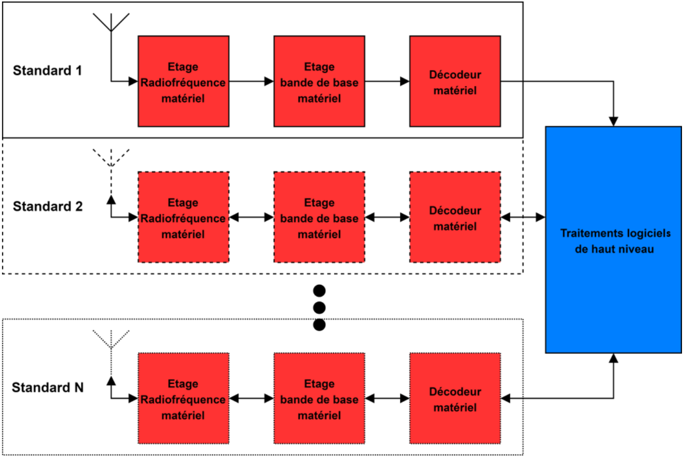
Context

- Always more users
  - Both human and objects: Internet of Things
- More and more radio communication systems: (smartphone example)
  - NFC
  - GSM (2G), GPRS (2.5G), EDGE (2.75)
  - UMTS (3G), HSDPA/HSUPA (3.5G), HSPA+ (3.75G)
  - LTE (4G), LTE-A (4G+)
  - Bluetooth/BLE
  - AM and FM radio
  - 5G
  - Wi-Fi
- More and more standardised or proprietary solutions: Bluetooth/BLE (IEEE 802.15.1), Cellulaire, LoRaWAN, LTE-M, NB-IoT, NFC (ISO/IEC 14443), RFID (ISO/IEC 18000), RuBee (IEEE 1902.1), SigFox, UWB (IEEE 802.15.3), Wi-Fi (IEEE 8902.11), WiMAX (IEEE 802.16), ZigBee (IEEE 802.15.4), Z-Wave, etc.
- Increasingly complex systems
  - Need of documentation
  - Increasing cost of equipment

Software Designed Radio

Current solution: hardware-based

➔ A hardware architecture for each standard. . .


Standard 1
Etage Radiofréquence matériel
Etage bande de base matériel
Décodeur matériel
Standard 2
Etage Radiofréquence matériel
Etage bande de base matériel
Décodeur matériel
Traitements logiciels de haut niveau
Standard N
Etage Radiofréquence matériel
Etage bande de base matériel
Décodeur matériel

Software Designed Radio

Current solution: hardware-based

- ... with pros...

  Optimized: compact (small and light) and very fast

  Low power consumption

  Low unit cost for large quantities (production)

- ... and cons

  Specific: non-evolving, non-updatable and non-reusable

  Long and expensive development

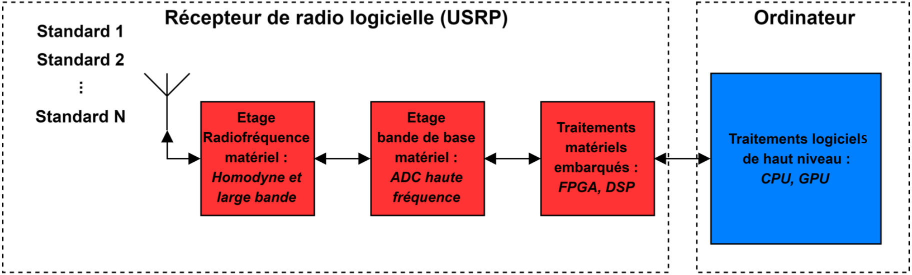
  Hard integration (EMC, placement)

  Always more interfaces in the same object

Software Designed Radio

New paradigm: software-based

➔ A generic hardware architecture and a specific software for each standard. . .


Récepteur de radio logicielle (USRP)
Standard 1
Standard 2
⋮
Standard N
Etage Radiofréquence matériel : *Homodyne et large bande*
Etage bande de base matériel : *ADC haute fréquence*
Traitements matériels embarqués : *FPGA, DSP*
Ordinateur
Traitements logiciels de haut niveau : *CPU, GPU*

Software Designed Radio

NNew paradigm: software-based

- … with pros…

  Generic harware

  Flexible and modular: scalable, updatable and reusable

  Fast development and production

- … and cons

  Expensive equipment

  Expensive production (currently)

  Hard integration (size, weight, energy consumption)

  No very efficient generic treatment

Software Designed Radio

This shift from an essentially hardware-based approach to an essentially software-based approach requires generic development hardware:

Universal Software Radio Peripheral (USRP)

Software Designed Radio

Universal Software Radio Peripheral (USRP)

National Instruments B210

Frequency band	*70 MHz – 6 GHz*
Sample frequency	*15 MS/s (up to 61)*
ADC accuracy	*12 bits/S*
Integrated or available processing devices	*FPGA, CPU*
Parallel implementation of applications	*Simultaneous Rx and Tx*
Ability to update on the fly without stopping or rebooting	
Price	*>1000 €*

https://www.ni.com/pdf/manuals/374924c.pdf

Software Designed Radio

Universal Software Radio Peripheral (USRP)

Analog Devices Adalm-Pluto

Frequency band	*325 MHz – 3.8 GHz*
Sample frequency	*65.2 kS/s to 61.44 MS/s*
ADC accuracy	*12 bits/S*
Integrated or available processing devices	*CPU*
Parallel implementation of applications	*Simultaneous Rx and Tx*
Ability to update on the fly without stopping or rebooting	
Price	*>200 €*

Other solutions:

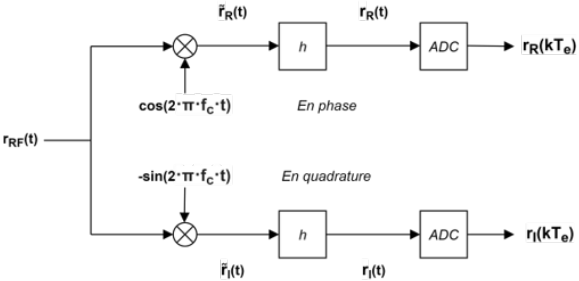
RTL-SDR, HackRF, etc.

Other USRP are available at INSA, some of which are specifically designed for stand-alone deployment.

Reception

Two layers:

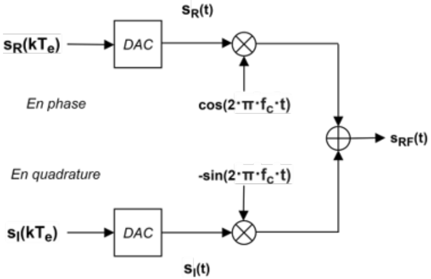
- An in-phase and quadrature demodulator (I/Q): to transpose the radio frequency signal into baseband and decompose it into electrical signals in phase and quadrature
- An analogue to digital converter (ADC): to sample signals in phase and quadrature



Emission

Two layers:

- A digital to analogue converter (DAC): to unsample signals in phase and quadrature
- An in-phase and quadrature modulator (I/Q): to compose a 'high frequency' radio frequency signal from electrical signals in phase and quadrature.



Software Designed Radio

GNURadio

- GNURadio

  Free and open-source software dedicated to the Software Defined Radio on Linux

- GNURadio Companion

  Graphical interface for graphical programming

Other development solutions:

Matlab/Simulink, Python, C, etc.

Examples of applications:

Spectrum analyser — FM broadcasting with RDS — Planes locations from ADS-B — TV broadcasting with dvbt — etc.

Table of contents

1. Learning objectives
2. Conduct of the laboratory project
3. Ressources
4. Evaluation
5. General introduction
6. Machine-to-Machine Communications
7. Software Designed Radio
8. Digital modulations
9. Proposed applications

Coding binary information

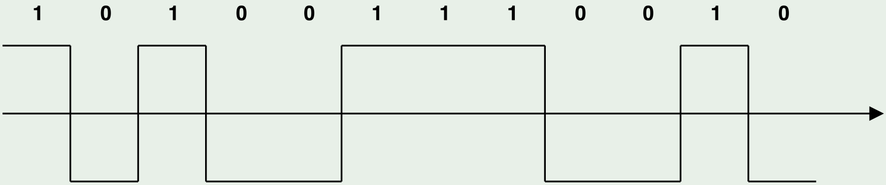
Reference binary sequence

1 0 1 0 0 1 1 1 0 0 1 0

Digital modulations

Coding binary information

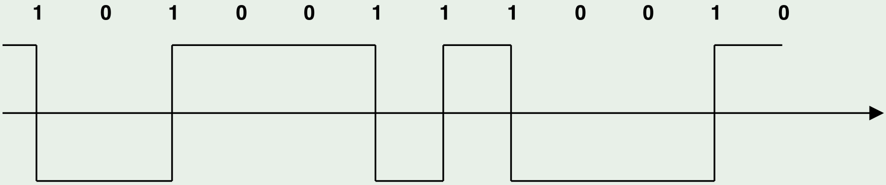
- Two-level or unipolar coding
  - Non Return to Zero (NRZ)
    '0' Low level
    '1' High level



Benefit(s) :	Simple
Drawback(s) :	Inversion / Few transitions / Difficult to synchronise
Example(s) :	RS-232 (+/-12 V)

Coding binary information

- Two-level or unipolar coding
  - Non Return to Zero Inverted (NRZI)
    '0' Maintained level
    '1' Inverted level

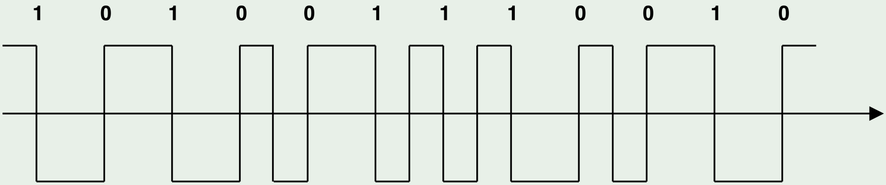


Benefit(s) :	Simple / good bandwidth
Drawback(s) :	Few transitions / Difficult to synchronise
Example(s) :	USB (with inverse logic and stuffing)

Digital modulations

Coding binary information

- Two-level or unipolar coding
  - Manchester
    ‘0’ Rising edge
    ‘1’ Falling edge

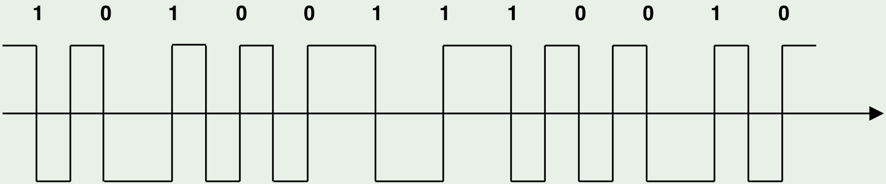


Benefit(s) :	Simple / Synchronisation / No DC component
Drawback(s) :	Doubled bandwidth
Example(s) :	Ethernet

Digital modulations

Coding binary information

- Two-level or unipolar coding
  - Differential Manchester
    ‘0’ Edge identical to the previous one
    ‘1’ Edge opposite to the previous one



Benefit(s) :	Simple / Synchronisation / No DC component
Drawback(s) :	Large bandwidth
Example(s) :	Token Ring

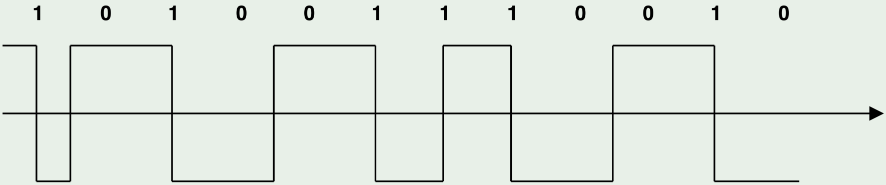
Digital modulations

Coding binary information

- Two-level or unipolar coding
  - Miller

    ’0’ Level maintained and edge between two ’0’s

    ’1’ Reverse edge to previous one

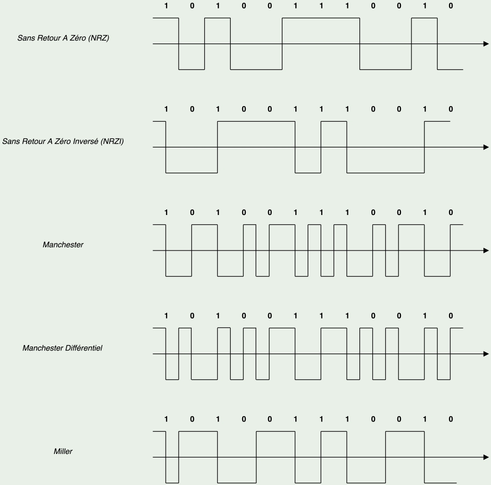


Benefit(s) :	Simple / Good bandwidth / Synchronisation
Drawback(s) :	DC component
Example(s) :	

Digital modulations

Coding binary information

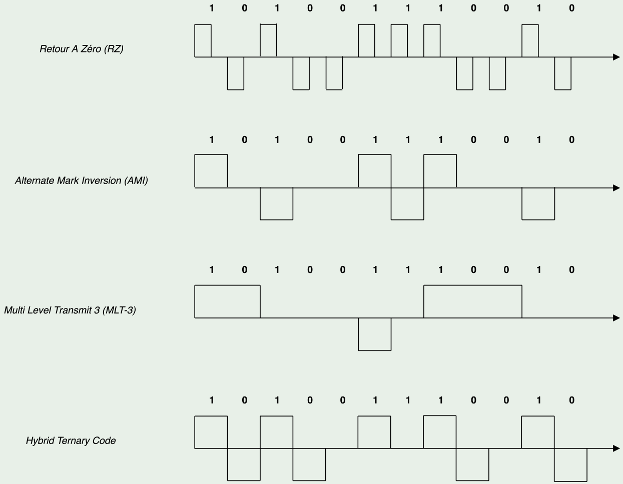
- Two-level or unipolar coding



Digital modulations

Coding binary information

- Three-level or bipolar coding



Retour A Zéro (RZ)

1 0 1 0 0 1 1 1 0 0 1 0

Alternate Mark Inversion (AMI)

1 0 1 0 0 1 1 1 0 0 1 0

Multi Level Transmit 3 (MLT-3)

1 0 1 0 0 1 1 1 0 0 1 0

Hybrid Ternary Code

1 0 1 0 0 1 1 1 0 0 1 0

Digital modulations

Gray code

Decimal	Natural binary	Reflected binary code or Gray code
0	000	000
1	001	001
2	010	011
3	011	010
4	100	110
5	101	111
6	110	101
7	111	100

One bit differs at each increment.

➔ No transient at logic circuit level.

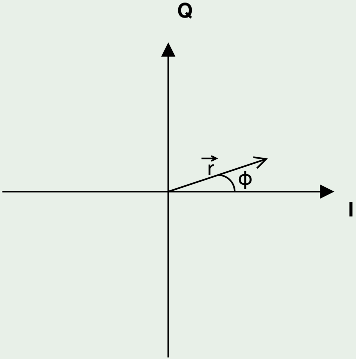
➔ circularity.

Digital modulations

Constellation diagram

Polar representation

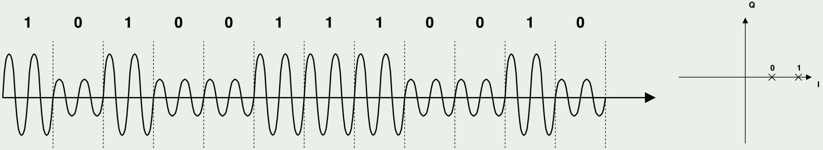
- ➔ Angle ϕ *Phase*
- ➔ Norm $|\vec{(r)}|$ *Amplitude*



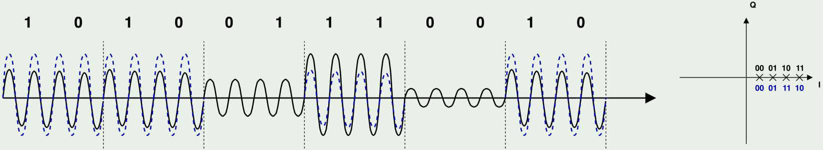
Digital modulations

Amplitude Shift Keying (ASK)

- 2-ASK



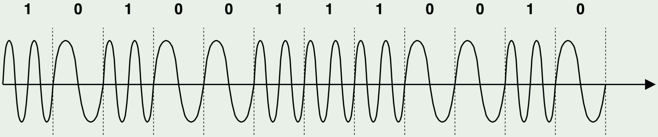
- 4-ASK



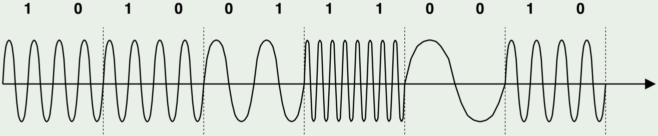
- 2^n-ASK If $n = +\infty$, it tends toward AM.

Frequency Shift Keying (FSK)

- 2-FSK



- 4-FSK

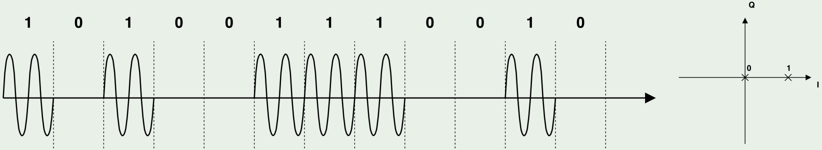


- 2^n-FSK If $n = +\infty$, it tends toward FM.

Digital modulations

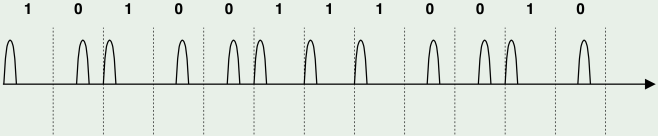
On-Off Keying (OOK)

- ASK: $A(t) = 0$ or $A(t) = A$
- FSK: $f(t) = 0$ or $f(t) = F$ (hypothesis: no DC component)

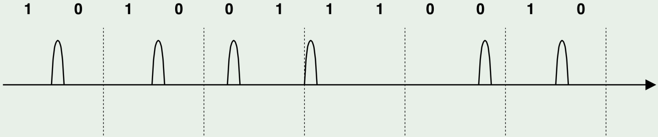


Pulse Position Modulation (PPM)

- 2-PPM



- 4-PPM

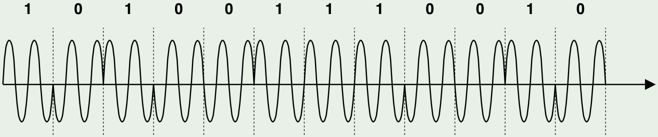


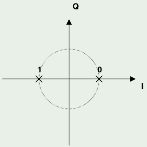
- 2^n-PPM

Digital modulations

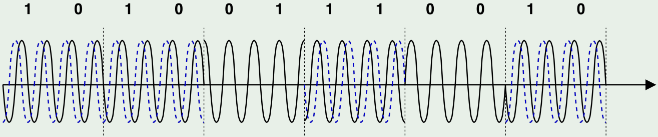
Phase Shift Keying (PSK)

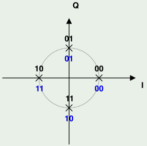
- 2-PSK or BPSK





- 4-PSK or QPSK





- 2^n-PSK

Digital modulations

Differential Phase Shift Keying (DPSK)

- It is no longer the phase but its change that encodes the information.
- No phase reference is required.
- The phase shift induced by the propagation medium (assumed to be homogeneous) is no longer a problem.

Digital modulations

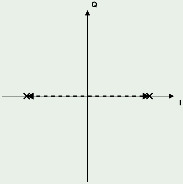
Offset Phase Shift Keying (OPSK)

- The constellation diagram is rotated with each new symbol.
- If this shift corresponds to half the phase shift between two contiguous phases (i.e. there are two constellation diagrams superimposed), then this forces a phase change with each new symbol and means that the carrier is not extinguished by passing through the origin.

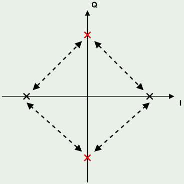
Digital modulations

Offset Phase Shift Keying (OPSK)

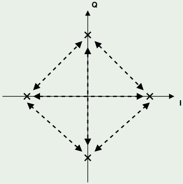
BPSK



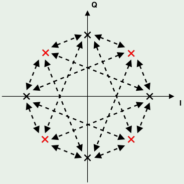
$\frac{\pi}{2}$-BPSK



QPSK



$\frac{\pi}{2}$-QPSK



Digital modulations

Other phase shift keyings

- Minimum Shift Keying (MSK)
- Gaussian Minimum Shift Keying (GMSK)
- etc.

Digital modulations

Complex modulations

- Amplitude and Phase Shift Keying (APSK)
  2^n-APSK
- Quadrature Amplitude Modulation (QAM)
  2^n-QAM

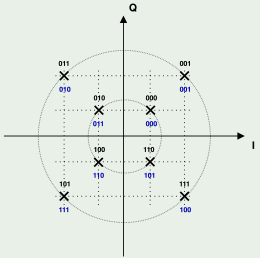
BPSK ⇔ 2-PSK ⇔ 2-APSK ⇔ 2-QAM

QPSK ⇔ 4-PSK ⇔ 4-APSK ⇔ 4-QAM

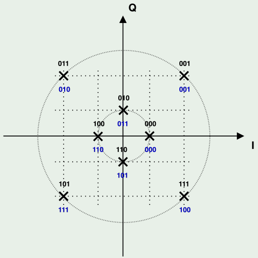
Digital modulations

Complex modulations

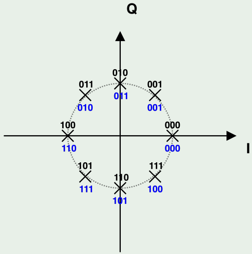
8-QAM



8-APSK



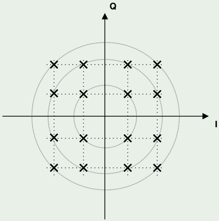
8-PSK



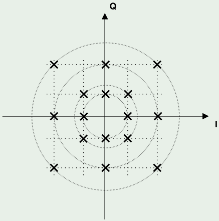
Digital modulations

Complex modulations

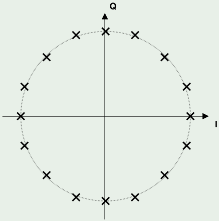
16-QAM

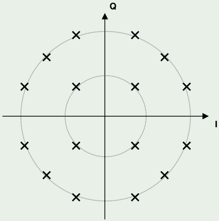


16-APSK



16-PSK

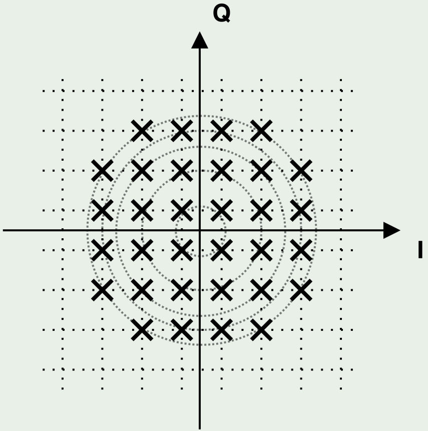




Digital modulations

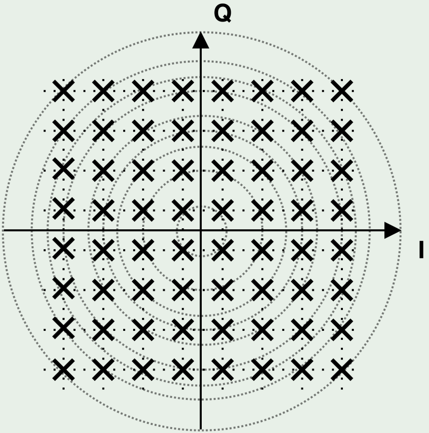
Complex modulations

32-QAM



Complex modulations

64-QAM



Digital modulations

Signal to Noise Ratio (SNR)

- Ratio of signal power to background noise power.
- Expressed in decibels (dB).

Bandwidth

- Frequency interval in which the signal has a power above a defined threshold.
- Expressed in Hertz (Hz).

Bit rate

- Measures the amount of data transmitted per unit of time.
- Expressed in bit/s.

Bit Error Rate (BER)

- Number of bit errors out of the number of bits transmitted.
- Expressed in 10^{-n}.

Digital modulations

Encoding binary information

Block code / Encoding table

4B5B	4 bits coded on 5 bits
4B3T	4 bits on 3 symbols at three levels
6B8B	6 bits coded on 8 bits
8B10B	8 bits coded on 10 bits
64B66B	64 bits coded on 66 bits
etc.	

Redundancy and reliability by avoiding problematic sequences.

Protocol formatting

Transmission of protocol information

Example of Ethernet frame:

Synchronisation preamble (7 bytes)
Start of frame delimiter (1 byte)
Destination address (6 bytes)
Source address (6 bytes)
Data quantity and type (2 bytes)
Data and padding ($>$46 bytes)
Frame check sequence (4 bytes)

Multiplexing

Techniques for shared use of a transmission channel.

- Time division multiplexing
  Each communication is allocated a channel access time.
- Frequency division multiplexing
  Each communication is allocated a frequency sub-band.
  e.g.: Orthogonal Frequency Division Multiplexing (OFDM)

Digital modulations

Spread spectrum

Techniques for the frequency distribution of a signal to enable it to pass below the noise level.

- Direct Sequence Spread Spectrum (DSSS)
  A combination of communication with a higher frequency pseudo-random sequence.
- Frequency Hopping Spread Spectrum (FHSS)
  Use of several sub-channels in a pseudo-random sequence for a communication.
- Time Hopping Spread Spectrum (THSS)
  Similar to pulse position modulation (PPM).
- Chirp Spread Spectrum (CSS)
  Use of chirps (continuous evolution of the carrier frequency) to transmit information.

Table of contents

1. Learning objectives
2. Conduct of the laboratory project
3. Ressources
4. Evaluation
5. General introduction
6. Machine-to-Machine Communications
7. Software Designed Radio
8. Digital modulations
9. Proposed applications

Proposed applications

Proposed applications

- Wireless Sensors Network for Structural Health Monitoring in aerospace
- Wireless Sensors Network for smart (medical) home
- You are free to propose your own application!
- The specifications of each application will be established during the supervised sessions!