An insight into Internet based technologies and protocols for Wirelessly connected things

Agenda

- Course Objectives & Logic
- A brief introduction and overview of wireless network technologies for the IoT
- A brief overview of Low-Power Wireless PANs (LP-WPAN), i.e. IEEE 802.15.4
- A brief overview of an IP based Network Architecture for IoT networks (historically designed for LP-WPAN)

UF & Course Objectives

- **What are the design objectives of communication protocols for wirelessly connected things**
  - Refer to Daniela's lectures
- **Analyze and devise low-layer protocols (MAC** & PHY**) suited to an IoT use case/application**
  - Refer to Daniela's lectures
- **A brief introduction to cellular IoT, mainly 5G/6G, and 5G/6G usages in IoT**
  - Refer to Etienne's lectures

- **A brief overview of Low-Power Wireless PANs (LP-WPAN) a.k.a IEEE 802.15.4**

UF & Course Objectives

- **What are the challenges facing the development of communication protocols in a wireless multi-hop context**
  - To be addressed from a network perspective

- **A brief overview of an Internet-technology based Network architecture for Low-power multi-hop wireless IoT network**

Course organisation

- **3 class lectures**
- **2 practice labs**
- **Learning skills :**
  1. assess the general benefits and main limitations of adopting an Internet (i.e. IPv6) based protocol stack for an IoT network (typically, wireless)
  2. set-up and operate a basic IPv6 based IoT Network
- **Course grading :**
  - **Mandatory** : Provide course takeaways
    - *Link :*
  - Optional / Bonus : Quiz to validate the different learning skills

Link to the course : https://moodle.insa-toulouse.fr/course/view.php?id=979

A brief overview of wireless network technologies for the IoT

- *An attempt to characterize IoT Networks*
- *Main IoT network technologies*
- *Course Bias & motivation*
- *Some background on wireless communications*

An attempt to characterize IoT Networks

- **IoT : abundance, omnipresence of things => scalability**
  - scaling up Internet technologies to a tremendous number of inexpensive smart objects or things that interact with the physical world **=>**
  - to make this scaling up economically and physically viable, scaling down the characteristics of each of these objects and of the networks being built out of them **== leads ==>**
    - *constrained nodes*
    - *constrained networks*

- **IoT Network**
  - constrained nodes and/or
  - constrained network

An attempt to characterize IoT Networks

- **Constrained node, aka smart object / Thing / Device**
  - The different facets to the constraints on nodes, w.r.t familiar Internet nodes
    - *maximum code complexity (ROM/Flash) + size of state and buffers (RAM),*
    - *processing power : the amount of computation feasible in a period of time*
    - *available power and energy. Energy limitations may be*
      - **Event energy-limited**: limited amount of energy available for a specific event, e.g., for a button press in an energy-harvesting light switch
      - **Period energy-limited**: Battery that is periodically recharged or replaced or olar powered
      - **Lifetime energy-limited**: Non-replaceable primary battery
      - **No limitations** : Mains-powered
    - *user interface and accessibility in deployment (ability to set keys, update software, etc.)*
    - *Physical constraints (size, etc.) & costs*

An attempt to characterize IoT Networks

- Constraints are mainly due to
  - *production and operational* ***costs reduction***
  - *physical constraints* related to node characteristics such as size, weight, and available power and energy.
  - *the environment where nodes/network are deployed (harsh environment, etc.)* + *regulation*

Constrained networks

- Constraints are mainly due to
  - ***Constrained nodes that compose the network***
  - ***Production & operation cost reduction***
  - *Wireless nature of the media (which is the default media)*
    - physical constraints (e.g., environmental constraints, media constraints such as underwater operation, limited spectrum for very high density, electromagnetic compatibility),
    - regulatory constraints, such as very limited spectrum availability (including limits on effective radiated power and duty cycle) or explosion safety, and
  - *technology constraints, such as older and lower-speed technologies that are still operational and may need to stay in use for some more time*

An attempt to characterize IoT Networks

- **Constrained networks (continued)**
  - They exhibit the following constraints w.r.t network technologies (link-layer) in common use in the Internet
    - *Very often, low achievable bitrate (including limits on duty cycle)*
    - *high packet loss with high variability (=> delivery rate)*
    - *highly asymmetric link characteristics*
    - *severe penalties for using larger packets*
    - *limits on reachability over time*
    - *lack of (or severe constraints on) advanced services such as multicast/broadcast*

An attempt to characterize IoT Networks

- **Can conventional computer networks be used as IoT networks ?**
  - What are the implicit assumptions of conventional nets : TCP/IP + conventional physical nets
    - *Hosts*
      - always on
      - Decent amount of resources
      - one interface
      - No mobility
    - *Physical network*
      - Typically deployed in a soft (not harsh) environment
      - decent frame size
      - decent performance
        - high throughput
        - very low packet loss
        - symmetric communications
        - decent RTT
      - decent costs
- **Do all these assumptions hold in the context of IoT ?**

An attempt to characterize IoT Networks

- **IoT network = Low-Power and Lossy Network (LLN)**
  - mostly composed of nodes with tight limits on power, energy, memory, and processing resources
  - interconnected via links (typically wireless) that exhibit considerable loss at the physical layer, with significant variability of the delivery rate, and some short-term unreliability

  which intrinsically

  - pays a careful attention to the
    - ***energy usage and***
    - *network bandwidth usage*
  - Built under the assumptions of
    - **Nodes with very limited resources**
    - Varying and short-term poor packet transmission performance in terms of reliability
    - lack of full connectivity guarantee (unreachability of nodes) and effective broadcat/multicast capabilities

An attempt to characterize IoT Networks

- **An insight on node constraints implication on the design of IoT networks**
  - From an Energy perspective
    - *Communications consume a big portion of the total energy of a device, notably for radio communications*
    - *The energy consumed is influenced*
      - Basically by, the duration of transmissions, receptions, and the time waiting for an eventual reception
      - But also by, the used spectrum, the desired range, and the bitrate aimed for

        == influence => the energy consumed during transmissions and receptions
    - *Energy constraints Implications are :*
      - mostly, on low-layer protocols,
      - but higher layer protocols should also be energy friendly

An attempt to characterize IoT Networks

- From an Energy perspective (continued)
  - *Depending on the type of the energy source (battery or mains powered, etc.) and the communication needs, a device can be*
    - ➢ Always on (connected to the network all the time)
      - » no reason for extreme measures for power saving, but
      - » May be useful to employ power friendly hardware or limit the number of wireless transmissions, CPU speeds, and other aspects for general power-saving and cooling needs
    - ➢ Normally-off (devices sleep for very long period)
      - » Sleeping period is so long that it loses, in some way, its attachment to the network (no data is saved)

        ==> reattachment process should require little communication effort
    - ➢ Low-power (devices need to operate on a very small amount of power + able to communicate on a relatively frequent basis)
      - » extremely low-power hardware & link-layer transmissions
      - » despite their sleep, devices retain attachment to the network, i.e. data packet are saved on behalf of the sleeping node
      - » the effort of reestablishing communications after wake-up should be very limited
      - » tuning the frequency of communications should be allowed

An attempt to characterize IoT Networks

Node constraints implication

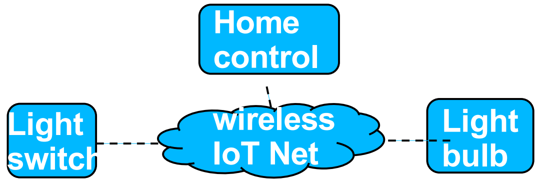
- From a resource perspective => Mostly on high-layer protocols
  - *Three different classes of nodes can be distinguished:*
    - severely constrained nodes in memory and processing capabilities (data <<10kiB / code << 100kiB) =>
      - Not able to implement conventionnel protocol and connect the device securely to the internet => These functions are outsourced and implemented at a **network gateway**
    - Constrained node (data ~10kiB / code ~ 100kiB)
      - Still not sufficient to employ a full conventional protocol stack to connect to the Internet
      - can make it with a protocol stack specifically designed for constrained nodes (such as the Constrained Application Protocol (CoAP) over UDP without the help of a gateway
    - Less constrained nodes (data size > 50 KiB / code size > 250 KiB)
      - fundamentally capable of supporting a full conventional protocol stack to connect to the Internet
      - can benefit from lightweight and energy-efficient protocols and from consuming less bandwidth

An attempt to characterize IoT Networks

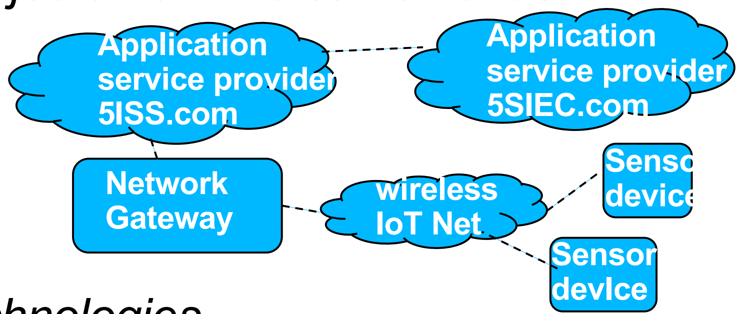
where does the IoT network sit?

▪ Communication patterns in IoT applications

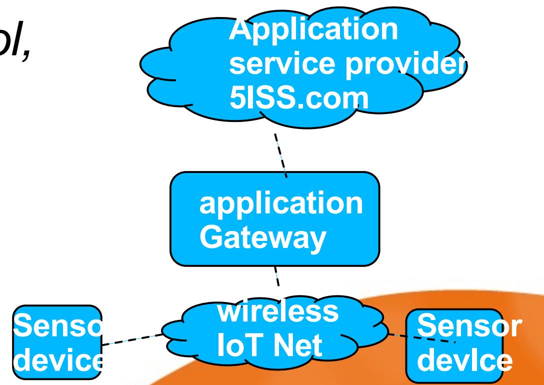
- Device to device communication
  - *Usually devices from the same vendors*



- Device to cloud communication with optionally back-end data sharing
  - *Usually, application service provider and smart objects from the same vendor*



- Device to gateway communication
  - *Gateway used to allow less-widely-used radio technologies or some application level functionality (local access control, data level filtering, etc.)*
  - *Usually the gateway and IoT devices are provided by the same vendor*



INSA de Toulouse • 135, Avenue de Rangueil • 31077 Toulouse
Tél. : +33(0)5.61.55.95.13 • Fax : +33(0)5.61.55.95.00 • www.insa-toulouse.fr

An attempt to characterize IoT Networks

IoT trends ?

- **IoT object**
  - Size is decreasing
  - Power need is decreasing
  - Processing and computing resources are increasing
    - *objects are no longer assumed to exclusively distribute sensed data, but are able to carry out processing and eventually transferring (off-loading) part of the processing to devices with more resources or with mains supply (Edge,fog, cloud etc.)*
  - Communication capabilities are increasing
  - Internet connectivity is being considered in increasingly different industry verticals
- **Communication technologies are increasingly being standardized with a move toward infrastructure based wireless technologies**

Main IoT network technologies

to answer the IoT applications' communication requirements

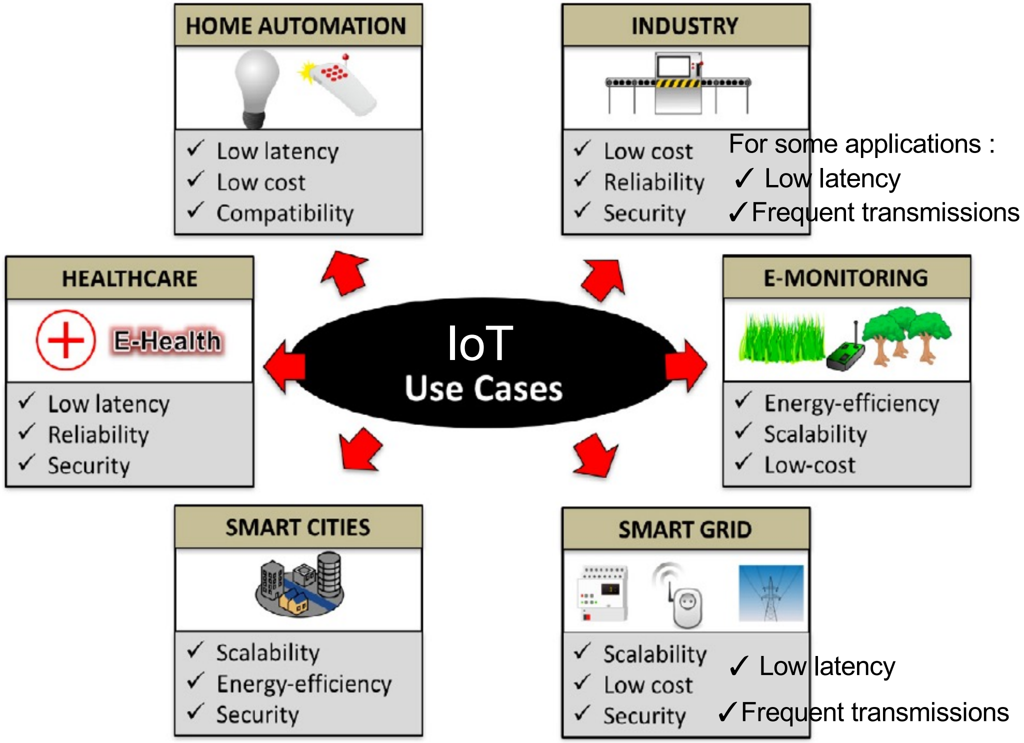
- **Multiple technologies to answer the variety of IoT applications**
- **IoT applications' communication requirements**
  - Various and fully dependent on the considered IoT use case/application, can be expressed in terms of :
    - *Expected Traffic profile*
      - A few messages a day, or more frequent and sustained message transmissions
      - Message size, etc.
    - *Expected QoS on message delivery*
      - Latency
      - Reliability
        - with and without explicit acknowledgment
        - Better than best effort with some form of transmission redundancy in the time or frquency space
      - Bandwidth (information rate)
    - *Energy consumption efficiency and constraints (for battery powered devices)*
      - IoT device network life time for non-mains powered devices: usually expressed from a few months to 10 years
      - Recharging interval for those that can be plugged to a power bank

- **IoT applications' communication requirements (continued)**
    - a private access network that connects IoT devices (opposed to a service subscription from an IoT network operator)
    - Network connectivity coverage/point of presence
        - Out-door, in-door with loose or deep penetration expectation, underground, etc.
    - Cost investment & operation
        - Device
            - Network mechanisms/techniques shouldn't be very complex and hence induce high production costs
        - Network connectivity/services
    - Scalability
        - Number of networked IoT devices with their traffic profile and QoS
  - *Mobility/Nomadicity support*
  - *Network based Localization*
  - *Firmware update over the air*
  - *Security*

Main IoT network technologies

to answer the IoT applications' communication requirements

- **IoT use cases main requirements**



Source: elsevier

Average importance of main IoT communications requirments

Use Case	Scalability	Data rate	Reliability	Low Latency	Low Consumption	Cost	Security	Compatibility
Home Automation	Low	Medium	Medium	High	Medium	Medium	Medium	High
Industry	Medium	Medium	High	High	Medium	High	High	Medium
Environmental Monitoring	High	Low	Low	Low	High	High	Medium	Low
Smart City & Building	High	Medium	High	Medium	High	High	High	High
Healthcare	*Variable*	*Variable*	High	High	Low	Low	High	Low
Smart Grid	High	High	High	High	Low	High	High	High

Main IoT network technologies

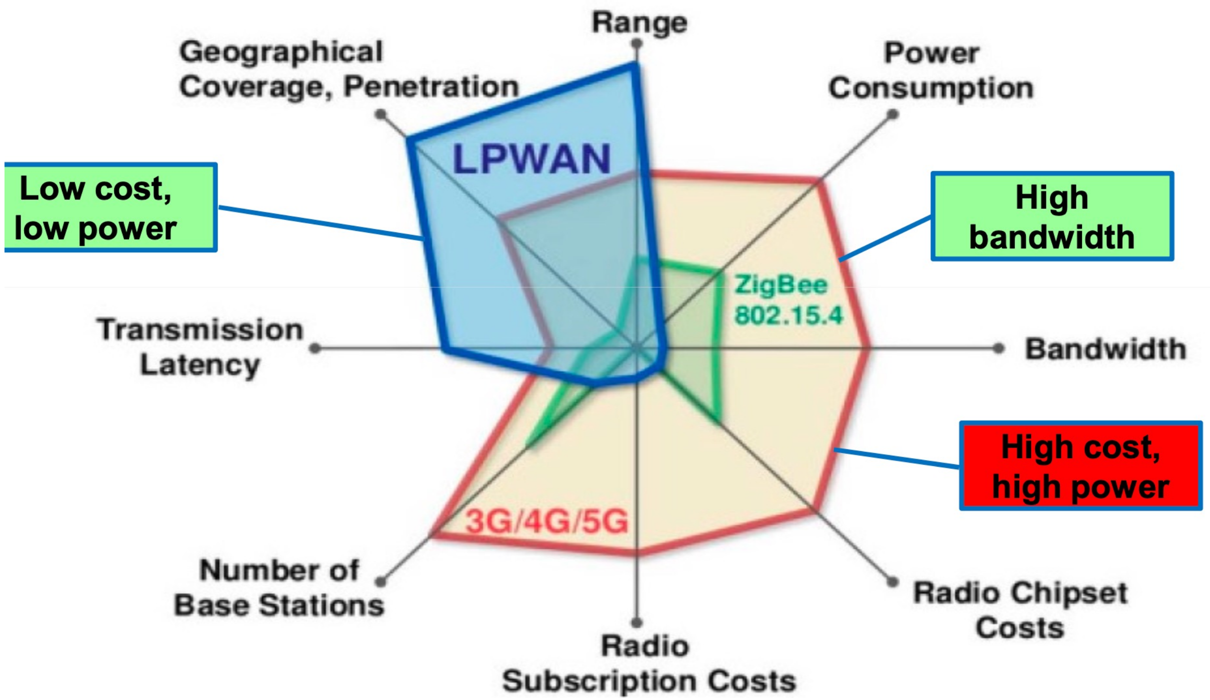
A brief review of IoT network technologies

- **Various Wireless network technologies to answer the various traffic characteristics and needs of the broad range of IoT applications**
- **Main choice criteria**
  - Traffic profile (few bytes a day or bursty and heavier traffic) & QoS requirements
    - *How much data is being sent, at which range and at which speed and intervals?*
    - *Delivery delay, reliability ?*
  - Power consumption requirements
    - *How important is the autonomy (and battery life) of your devices?*
  - Coverage and penetration capabilities in urban environments
    - *RF band ? Data range? Outdoor? Indoor?*
  - Equipment cost
  - Connectivity cost
  - Mobility/Nomadicity support
  - Network based Localization, Firmware update over the air support

Main IoT network technologies

A brief review of IoT network technologies

- **Various Wireless network technologies to answer the various traffic characteristics and needs of the broad range of IoT applications**
- **Main choice criteria**



Source ITU-T

- **Short range communication technologies**

Name	Spectrum	Bandwidth	Peak DR	Range	Topology	PHY Modulation	MAC Access
BLE	2.4 GHz	2 MHz	1 Mbps	100 m	Star	GFSK (FHSS)	TDMA
Thread 6LowPAN	2.4 GHz	5 MHz	250 kbps	10–75 m	Mesh	OQPSK (DSSS)	CSMA/CA
ZigBee	2.4 GHz	2 MHz	250 kbps	10–75 m	All	OQPSK (DSSS)	S-CSMA/CA
ZigBee	915 MHz	1.2 MHz	40 kbps	10–75 m	All	BPSK (DSSS)	S-CSMA/CA
ZigBee	868 MHz	600 kHz	20 kbps	10–75 m	All	BPSK (DSSS)	S-CSMA/CA
WirelessHART	2.4 GHz	3 MHz	250 kbps	30–90 m	Mesh	OQPSK (DSSS)	TDMA
ISA 100.11a	2.4 GHz	5 MHz	250 kbps	30–90 m	Mesh	OQPSK (DSSS)	TDMA
Z-Wave	868/908 MHz	200 kHz	9.6–40 kbps	30–100 m	Mesh	FSK	TDMA
Z-Wave 400	2.4 GHz	–	200 kbps	30–100 m	Mesh	FSK	TDMA
INSTEON	908 MHz	–	38.4 kbps	45 m	Mesh	FSK	TDMA
EnOcean	868/315 MHz	62.5 kHz	125 kbps	30 m	Mesh	ASK, FSK	TDMA
D7AP Hi-Rate	433/868/915 MHz	200 KHz	166.67 kbps	10 m	Tree	GFSK	CSMA/CA
D7AP	433/868/915 MHz	200 KHz	55.55 kbps	100 m	Tree	GFSK	CSMA/CA
DECT ULE	1.8/1.9 GHz	1.728 MHz	1152 kbps	70–300 m	Star	GFSK	TDMA

Long range communication technologies

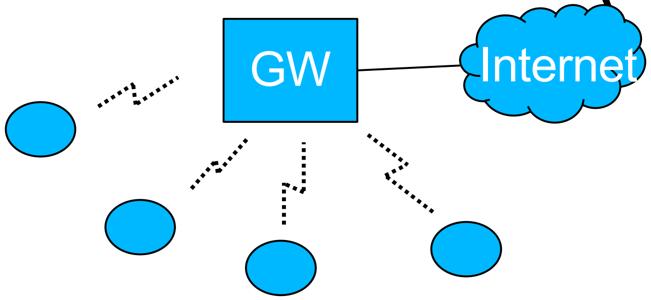
- LPWAN : Low Power Wide Area Network (refer to Daniela D. & Etienne's lectures)

Name	Spectrum	Bandwidth	Peak DR UL	Peak DR DL	Range	PHY Modulation	MAC Access
D7AP Lo-Rate	433/868/915 MHz	25 kHz	9.6 kbps	9.6 kbps	∼5 km	GFSK	CSMA/CA
SigFox	868–915 MHz	192 kHz	∼100 bps	∼100 bps	>20 km	GFSK/DBPSK (UNB)	ALOHA
Ingenu MN	2.4 GHz	1 MHz	∼30 kbps	∼30 kbps	∼15 km	FSK, PSK (DSSS)	RPMA
LoRa	868–915 MHz	125 kHz	∼50 kbps	∼50 kbps	∼11 km	CSS	ALOHA
Weightless-N	868 MHz	200 Hz (?)	∼100 kbps	–	∼5 km	DBPSK (UNB)	S-ALOHA
Weightless-P	868 MHz	12.5 kHz	∼100 kbps	100 kbps	∼2 km	GMSK, OQPSK (UNB)	FDMA,TDMA
Weightless-W	470–790 MHz	6-8 MHz	∼10 Mbps	∼10 Mbps	∼10 km	DBPSK/QPSK /16-QAM (DSSS)	FDMA,TDMA

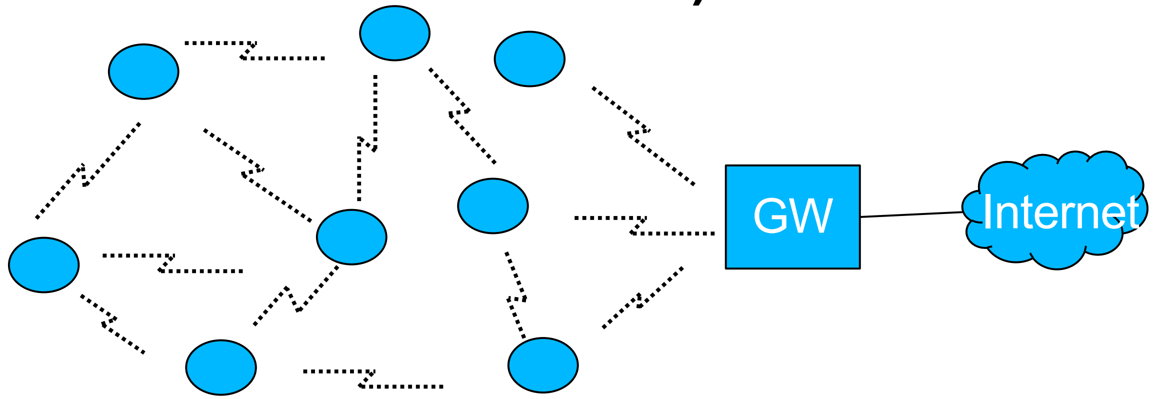
- Cellular IoT (refer to Etienne S.'s lectures)

Name	Spectrum	Bandwidth	Peak DR UL	Peak DR DL	Range	Modulation	Access
EC-GSM	700–900 MHz	200 kHz	∼10 kbps	∼10 kbps	∼15 km	GMSK	TDMA
LTE-M	700–900 MHz	1.4 MHz	∼1 Mbps	∼1 Mbps	∼11 km	QPSK, 16-QAM, 64-QAM	OFDMA
NB-LTE-M	700–900 MHz	200 kHz	∼144 kbps	∼200 kbps	∼15 km	QPSK, 16-QAM, 64-QAM	OFDMA
NB-CIoT	800–900 MHz	180 kHz	∼36 kbps	∼45 kbps	∼15 km	BPSK, QPSK, 16-QAM	OFDMA

- **Device-to-Device wireless networks vs Infrastructure based wireless networks (one hop wireless transmission)**



one-hop / star topology

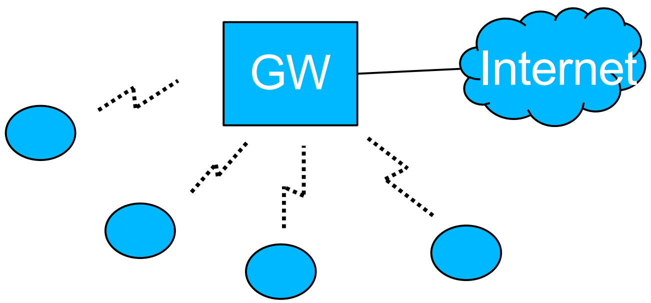


Device to device network

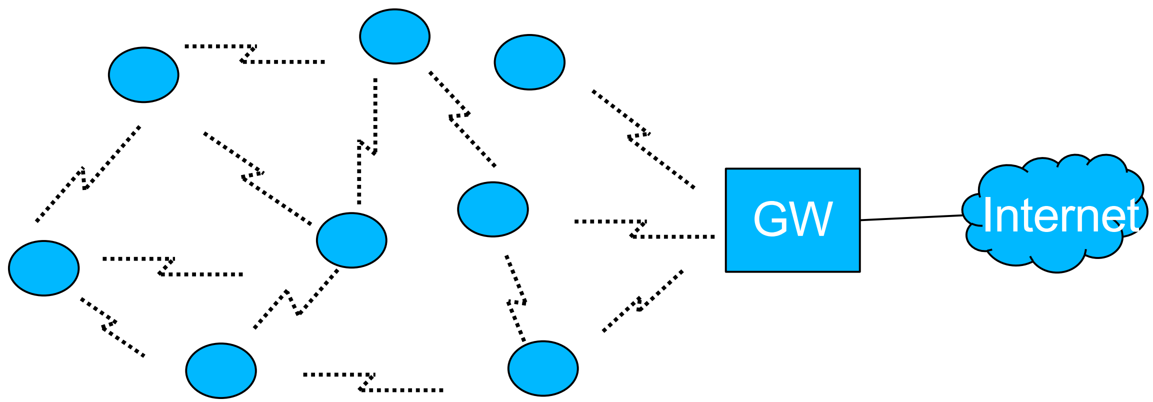
- A network of smart objects communicating through wireless technologies
- Most nodes are constrained nodes
- Some nodes act as relays =>
  - Wireless multi-hop network
  - energy constraints =>
    - Low-Power transmissions =>
      - Limited transmission range
      - Lossy transmissions & changing topology
      - Limited transmission speeds
  - mesh topology: each node has at least two neighbours to transmit data to

INSA de Toulouse • 135, Avenue de Rangueil • 31077 Toulouse
Tél. : +33(0)5.61.55.95.13 • Fax : +33(0)5.61.55.95.00 • www.insa-toulouse.fr

- **Device to Device Networks, historically known as Wireless Sensor Networks** (also called: *Low-power Wireless Personal Area Nets (LP-WPAN)*)



one-hop / star topology



Cons

- Limited security
- Limited transmission speeds
- The environment has a greater impact
- Efficient design harder, i.e. tradeoff among : *the overall network capacity, end-to-end delays, network reliability, energy consumption*

Pros

- Greater deployment flexibility
- Scaling to more devices is simple
- Low implementation costs
- Easy to introduce new devices
- Self-maintained and cope well with the dynamicity

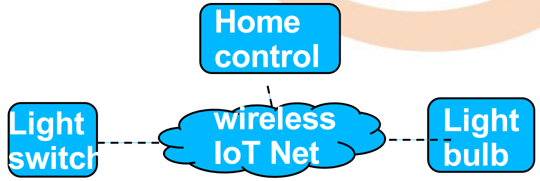
Main applications : Home automation, Home security and health applications, Industrial applications (control automation) and "smart utility networks"

• Course Bias & motivation

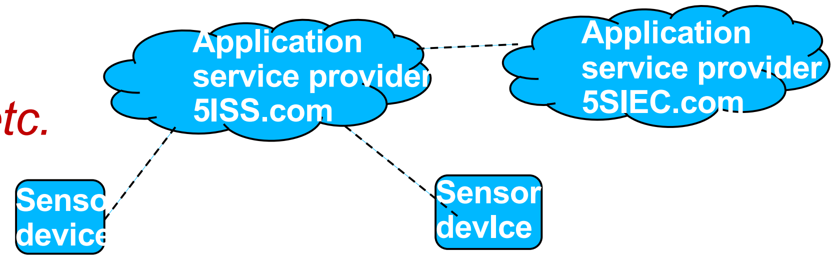
- **Even if for very specific cases, designing IoT networks tailored to a particular application (from scratch or by extending/modifying existing protocols) is necessary, the bias of this course is to rely on/adopt Internet-technology-based IoT networks**
  - a large number of already-standardized Internet protocols are relevant for smart object deployments.
  - developing new protocols and mechanisms is generally more risky and expensive (design, implementation, testing, and deployment, training)
  - for long lived smart objects, in comparison to ad-hoc proprietary solutions, Internet technology based protocols are likely to remain relevant over a longer period of time. In addition, Internet technology continuously evolves over the years
  - Enable end-to-end security
  - IP is scalable, resilient & ubiquitous

• Course Bias & motivation

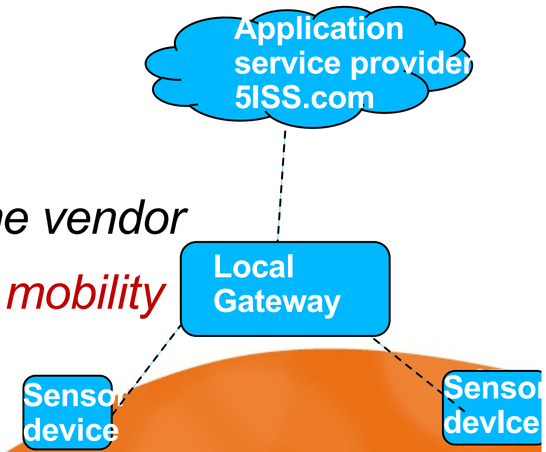
▪ Enhanced interoperability



- Device to device communication
  - *Usually devices from the same vendors*
  - *IP lets devices from different manufacturers inter-operate and communicate directly*
- Device to cloud communication with optionally back-end data sharing
  - *Usually, application service provider and smart objects from the same vendor*
  - *IP allows multiple device vendors +*
    Third-party application service providers, etc.



- Device to gateway communication
  - *Gateway used to allow less-widely-used radio technologies*
    or some application level functionality (local access control,
    data level filtering, etc.)
  - *Usually the gateway and IoT devices are provided by the same vendor*
  - *IP helps adopting more generic gateways (GW), enables GW mobility*



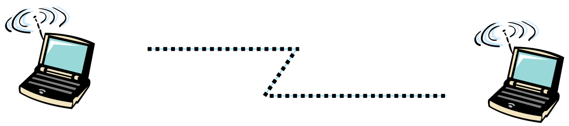
Some background on wireless communications

- **For many IoT use cases, mostly wireless**
  - Wired are also being used : PLC (power Line communication), legacy fieldbus and wired LAN
- **Some background on wireless communication & networking**
  - Wired Link Abstraction

Characteristics and performance

- *Steadiness&predictability ?*
- *Quality (QoS) ?*
- *states ?*
- *Symétry ?*

  - What about the Wireless Link Abstraction ? Does the wired abstraction hold for wireless ?

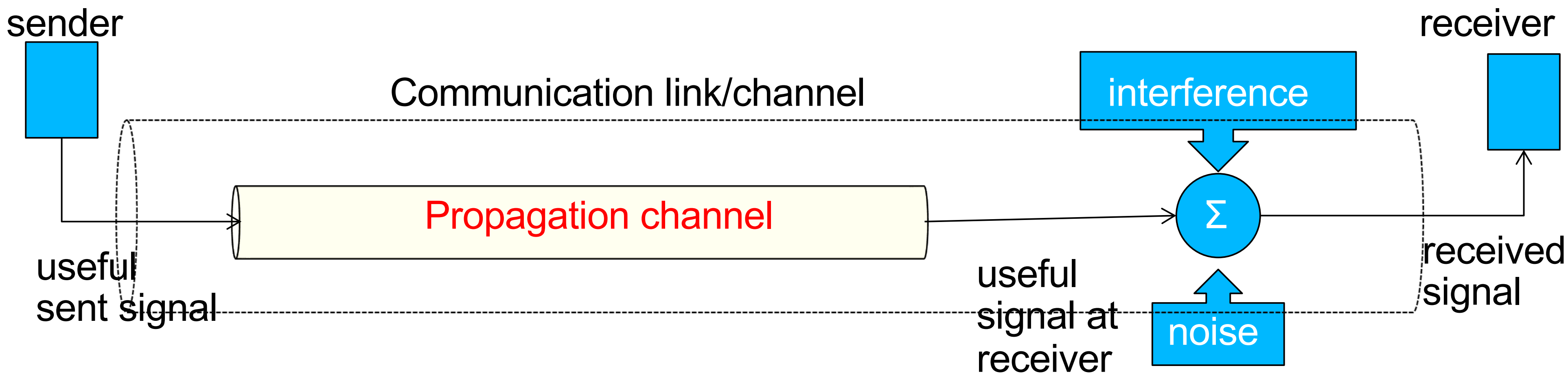


Characteristics and performance

- *Varying & unpredictable*
- *Average, sometime poor*
- *Non binary*
- *asymetric*

Some background on wireless communications

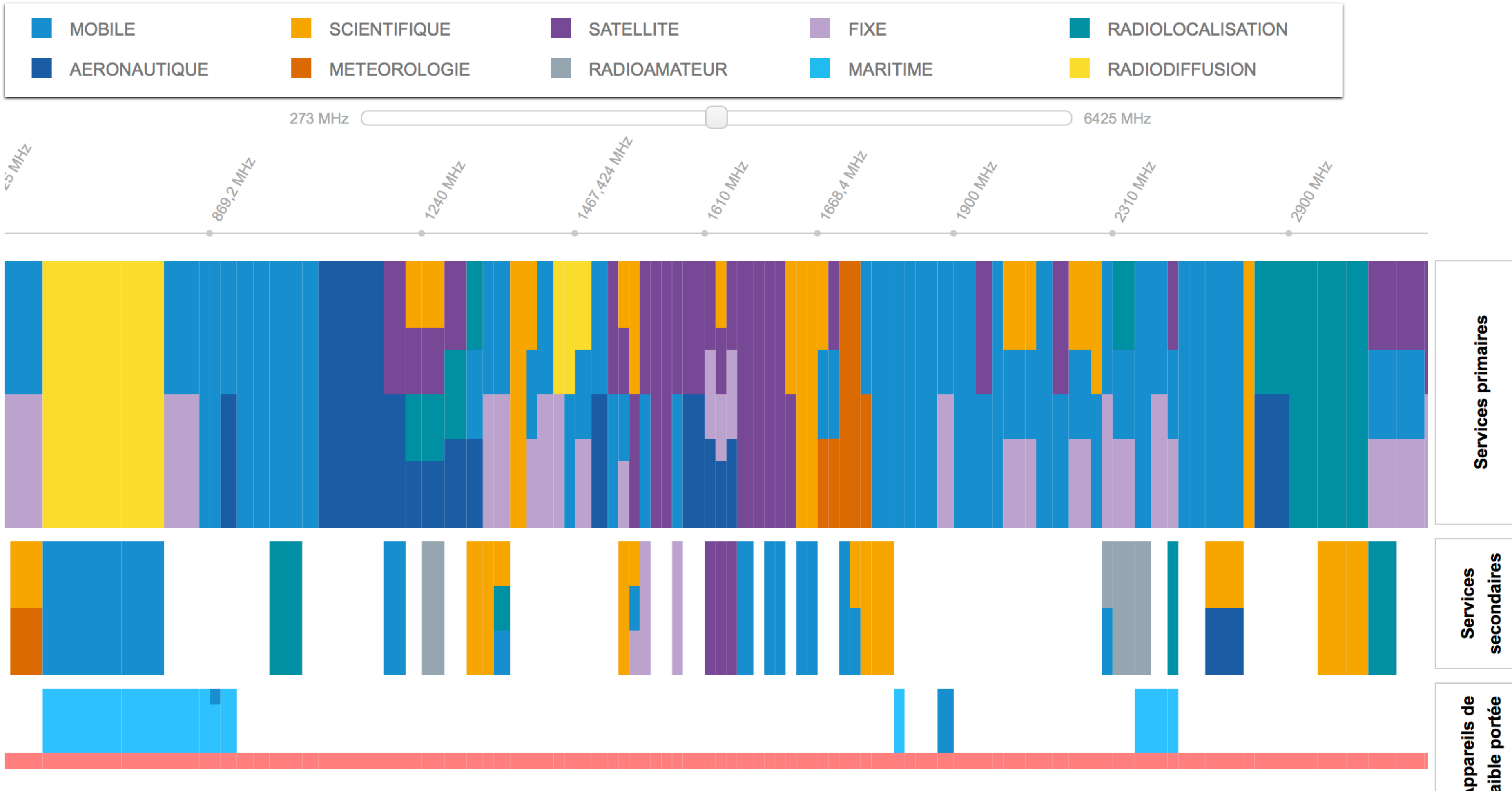
- **Why such an abstraction ?**
  - Based on a **non-guided** and **shared** communication channel
    - *Mostly a **radio wave** channel, but could be infra-red, visible light or sound*



- ***Non-guided propagation channel*** + ***shared*** => ***interference***

Some background on wireless communications

- **Non-guided propagation channel and shared => Interference**
  - Wireless communication is subject to spectrum regulation
    - *ANFR & ARCEP*



Frise ANFR : https://www.anfr.fr/gestion-des-frequences-sites/tnrbf/frise-interactive/

Some background on wireless communications

- **Non-guided propagation channel and shared => Interference**
  - *for Licence-free bands, to limit interference,*
    - ➢ Licence-free bands are dedicated to specific usage (device categories)

Fréquences	Utilisations notables
13 553 – 13 576 kHz	RFID, NFC
169,4 – 169,8125 MHz	Wize
433,05 – 434,79 MHz	Talkies-walkies, télécommandes, LoRa
863 – 868,6 MHz	z-Wave, Sigfox, LoRa, RFID UHF, Zigbee
868,7 – 869,2 MHz	
869,3 – 869,65 MHz	
869,7 – 870 MHz	
2400 – 2483,5 MHz	Wi-Fi, Bluetooth, Zigbee, Thread
5150 – 5350 MHz	Wi-Fi
5470 – 5725 MHz	

https://www.arcep.fr/la-regulation/grands-dossiers-reseaux-mobiles/le-guichet-start-up-et-innovation/le-portail-bandes-libres.html

Some background on wireless communications

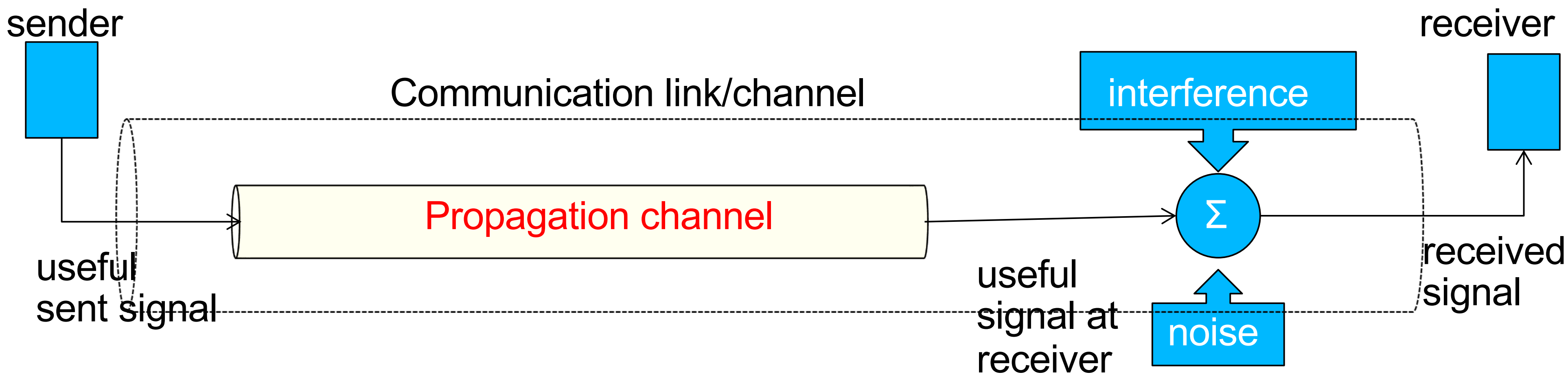
- **Non-guided propagation channel and shared => Interference**
  - *for Licence-free bands, to limit interference, devices must respect*
    - A maximum transmit power, and eventually
    - A maximum usage rate

Bande de fréquences	Catégorie de dispositifs à courte portée	Limite de puissance /d'intensité de champ / de densité de puissance	Paramètres supplémentaires (règles d'accès aux voies et d'occupation des voies)	Autres restrictions d'utilisation
863-865 MHz	Dispositifs de transmission en mode continu/à coefficient d'utilisation élevé	10 mW PAR		Cet ensemble de conditions d'utilisation ne concerne que les dispositifs audio sans fil et les dispositifs multimédia de lecture en continu.
865-865,6 MHz	Dispositifs d'identification par radiofréquences (RFID)	100 mW PAR	Espacement des canaux: 200 kHz.	
865,6-867,6 MHz	Dispositifs d'identification par radiofréquences (RFID)	2 W PAR	Espacement des canaux: 200 kHz	
867,6-868 MHz	Dispositifs d'identification par radiofréquences (RFID)	500 mW PAR	Espacement des canaux: 200 kHz	
865-868 MHz	Dispositifs à courte portée non spécifiques	25 mW PAR	Doivent être utilisées des techniques d'accès au spectre et d'atténuation des interférences au moins aussi performantes que celles décrites dans les normes harmonisées adoptées en vertu de la directive 1999/5/CE. Alternativement, un coefficient d'utilisation limite de 1 % peut également être utilisé.	Les applications audio analogiques autres que vocales sont exclues. Les applications vidéo analogiques sont exclues.
863-865 MHz	Dispositifs à courte portée non spécifiques	25 mW PAR	Doivent être utilisées des techniques d'accès au spectre et d'atténuation des interférences au moins aussi performantes que celles décrites dans les normes harmonisées adoptées en vertu de la directive 1999/5/CE. Alternativement, un coefficient d'utilisation limite de 0,1 % peut également être utilisé.	Les applications audio analogiques autres que vocales sont exclues. Les applications vidéo analogiques sont exclues.

https://www.arcep.fr/uploads/tx_gsavis/14-1263.pdf

Some background on wireless communications

- **Why such an abstraction ?**
  - Based on a **non-guided** and **shared** communication channel



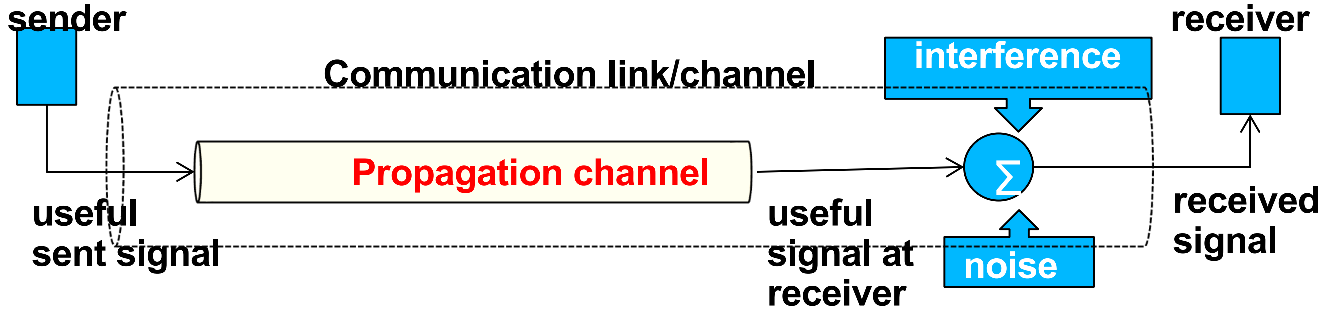
– ***Non-guided propagation channel** + **shared** => **interference***

➢ Caused by transmissions on **the same network**, on **co-located networks**, potentially based **on a different technology**, eventuellay **non-communicating appliances** (home,medical,motor etc.)

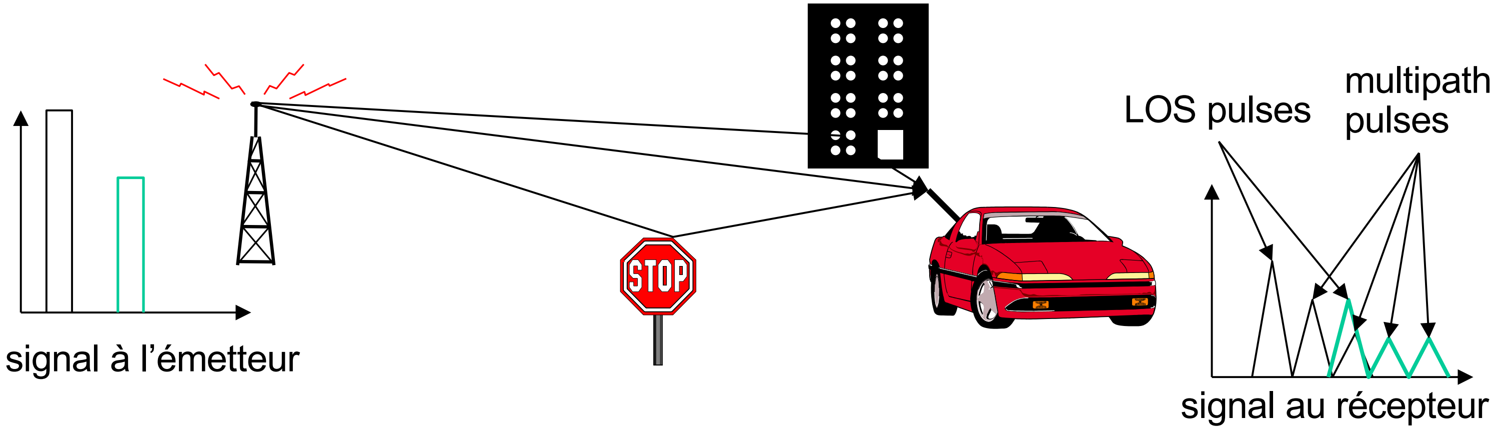
- Successful Transmission : received useful signal's strentgh (power) is not <<< received signal's strentgh

Some background on wireless communications

- **Why such an abstraction ?**
  - propagation channel induces high attenuations
    - *In a nominal wlan communication : Tx pw: tens of mw -> Rw power: tens of pw, a power loss of 10^{-9} (noise around : 0.1 pw)*

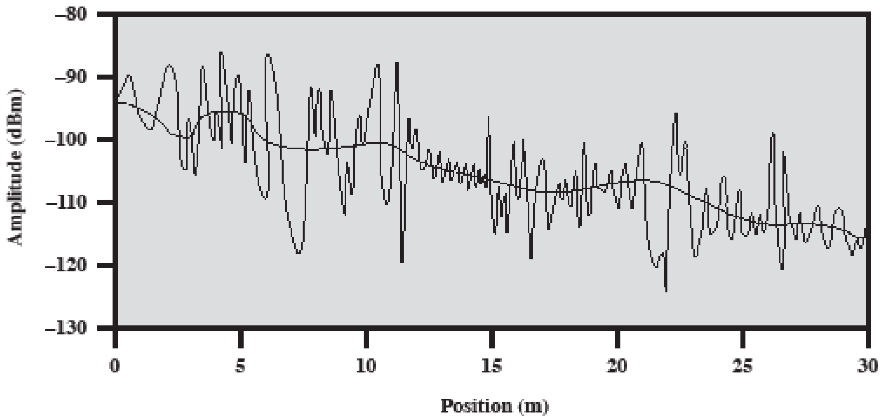


    - *Path loss*
    - *Shadowing*
    - *Multi-path*



Some background on wireless communications

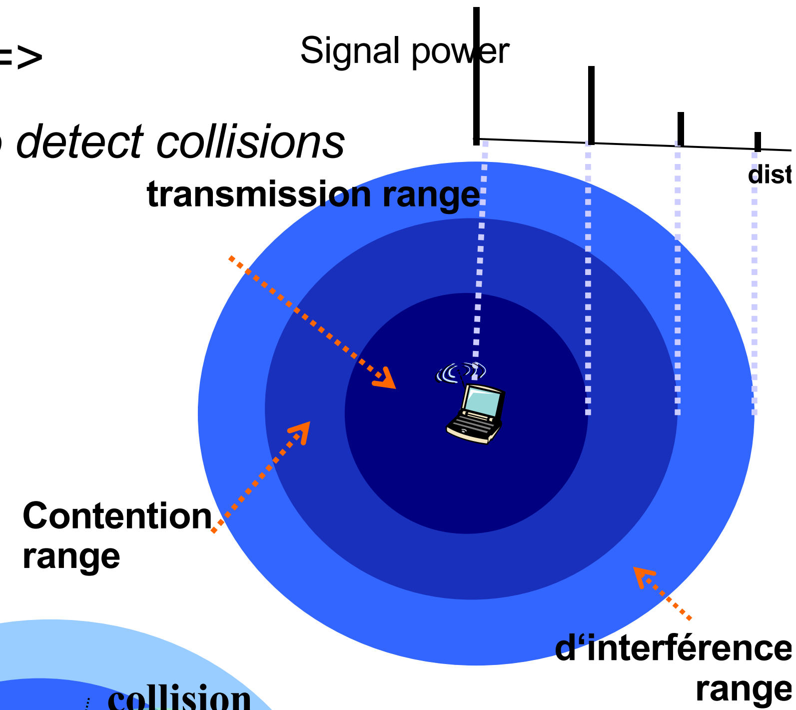
- **Why such an abstraction ?**
  - propagation channel induces high attenuations **with fast and significant fluctuations**
    - *Path loss*
    - *Shadowing*
    - *Multi-path*

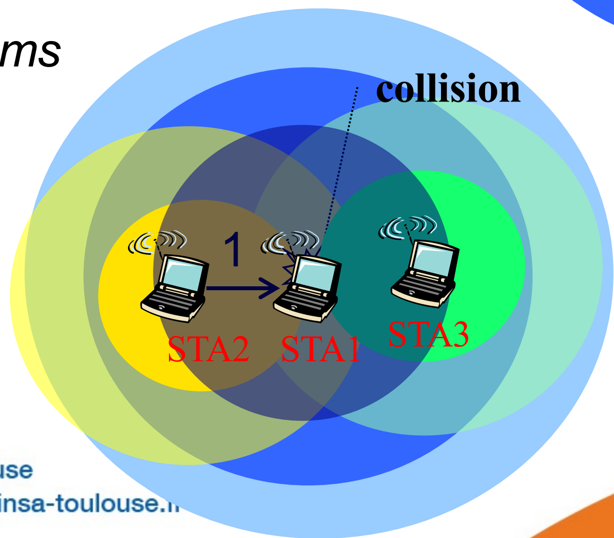


Source : Wiley Typical Slow and Fast Fading in an Urban Mobile Environment

Some background on wireless communications

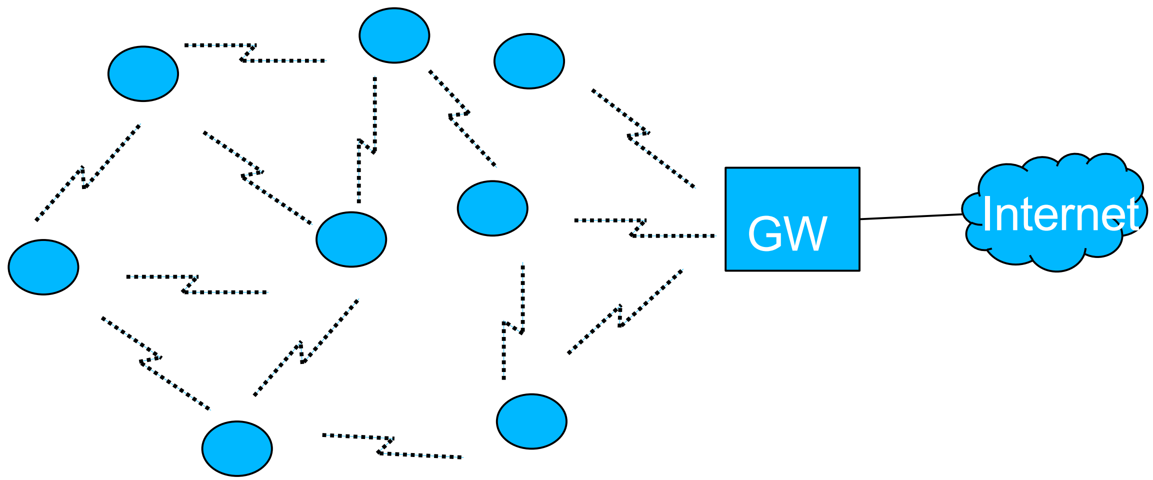
- **Why such an abstraction ?**
  - propagation channel induces high attenuations =>
    - *A node is blinded when transmitting => unable to detect collisions*
    - *Each node has its own :*
      - ➢ Transmission range
      - ➢ Contention range
      - ➢ Interference range
    - *Hidden and exposed terminal problems*





Some background on wireless communications

- **Why such an abstraction matters, especially in wireless multi-hop networks ?**



Some background on wireless communications

- **How are the challenges of wireless communication addressed in practice ?**
  - Mitigating Interference?
    - *Spread spectrum techniques*
    - *Channel selection*
    - *Transmit power control*
  - Improving performance ?
    - *MIMO*
    - *adaptive physical modes*
    - *Multi-path mitigation with OFDM based techniques*
    - *Acknowledgment, fragmentation, etc.*
    - *Transmission redundancy in time and frequency domain*
  - Sharing the medium
    - *That copes with the specificities of wireless communications : « blinded phenomenon », hidden node, etc.*

Some background on wireless communications

- **How are the challenges of wireless communications addressed in practice ?**
  - Energy consumption ?
    - *Duty cycles,*
    - *Access techniques,*
    - *..*
  - Mobility management
    - *Implicit : as in LoraWan*
    - *Requires explicit procedures*
    - *Routing for wireless multi-hop networks*
  - Security
    - *Low level security mechanisms for improved confidentiality, integrity and authentication and access control*

Some background on wireless communications

- **Wireless Network Topology ?**
  - single-hop networks (often Infrastructure based)

    - *Based on cellular networks*
      - 2G : well used in many IoT applications:
        fleet management, ..
      - 3G & 4G : not commonly used because of power consumption and costs
      - LTE-MTC (Machine Type Communications) : better power consumption
      - NB-IOT (Narrow Band -IoT) : LPWAN techniques built on top of a cellular infrastructure
    - *Based on LPWAN (Low Power Wide Area Networks) : SigFox, LoRaWAN, Weightless, etc.*
      - Very low power consumption
      - Reduced equipment & connectivity costs
      - Wide coverage with good penetration in urban environments
      - Suited for uplink traffic
      - Targeted applications : very limited daily traffic with loose perf. requirements

Some background on wireless communications

- single-hop networks (continued)
  - *Wlan (infrastructure based or ad-hoc)*
    - Low Power Wi-fi (HaLow)
      - Improved coverage and penetration capabilities (sub 1GHZ technology)
      - Improved power consumption
    - Bluetooth Low Energy (BLE)
      - Bluetooth v5 enables mesh networking
- Wireless Multi-hop networks (mesh, tree, etc.)
  - *Ad-hoc deployments*
  - *Under an effective network management : better capacity, better performance (reiability, loss and delay) and clearly the most suited for the industrial IoT !*
    - Number & relay placement,
    - Interference mitigation
    - ..