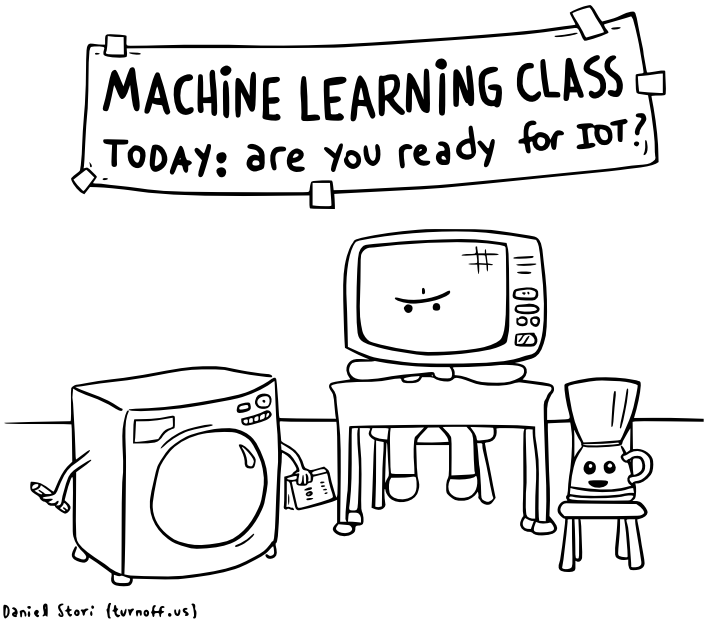
IAE LIMOGES
École Universitaire
de Management

Licence 3ème année



Internet des Objets — P-F. Bonnefoi

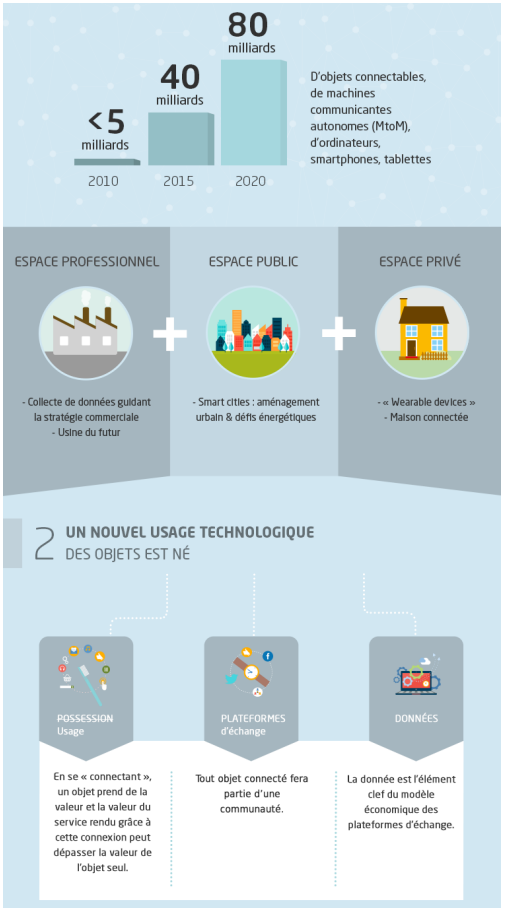
Version du 3 décembre 2025

Évolution naturelle d'Internet

Années 1960 Internet est né	**1989-2000** Une première révolution	**Début des années 2000** Internet devient universel	**Aujourd'hui** L'Internet des objets : la nouvelle étape
			
L'Internet connecte les ordinateurs entre eux et transmet des messages simples avec une capacité d'échange de données limitée.	Les technologies Web permettent de lier des documents. Le WWW est né (Web 1.0).	L'Internet est désormais une plateforme de communication universelle. Il transporte tout le contenu vocal, vidéo ou informationnel, les médias sociaux permettant le contenu généré par l'utilisateur (Web 2.0).	L'IoT est la prochaine étape vers la numérisation où tous les objets peuvent être interconnectés entre eux ou avec des personnes via des réseaux de communication, dans et entre les espaces privés, publics et industriels, et rendre compte de leur état et/ou de l'état de leur environnement.

L'IoT est un élément clé du développement de l'Internet, car il se caractérise par la collecte massifiée des données connectées et analysées.

Évolution naturelle d'Internet



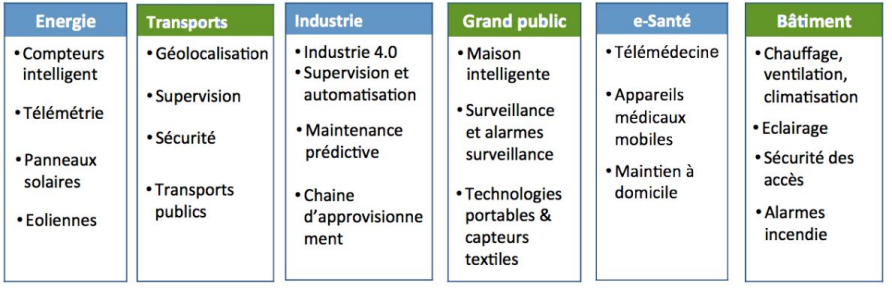
Défintions

- L'Internet des objets, également appelé en anglais «*Web of Things*», IoT «*Internet of Things*», M2M «*Machine-to-machine*» ;
  - **Objets** : une définition en B2C, «*Business-to-Client*», plutôt que B2B, «*Business-to-Business*» ;
  - **Internet** : les «*objets*» ne sont pas nécessairement connectés au réseau Internet et peuvent rester sur des réseaux privés (LAN) ; $\Longrightarrow$ «*objets connectés*»

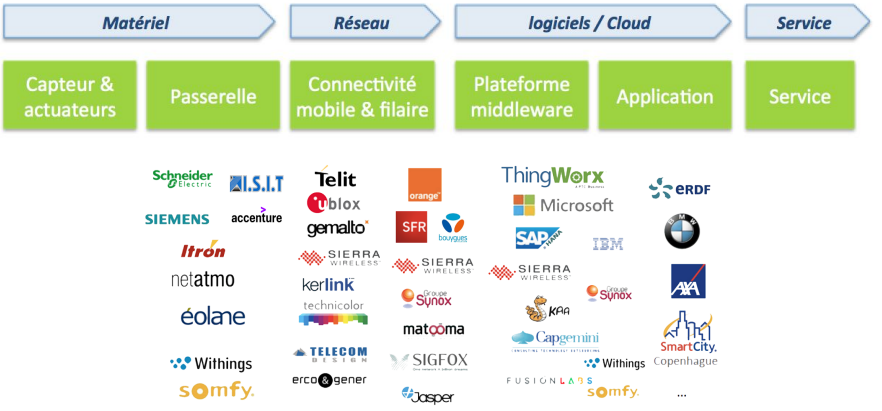
- opposition en IoT et M2M :
  - IoT : objets de technologies très variées connectés à du Cloud par Internet ;
  - M2M : machines connectées entre elles ou par un réseau WiFi ou cellulaire à un système centralisé propriétaire et privé.

Les domaines

- Énergie,
- Transports,
- Industrie (machines industrielles, logistique...) industrie 4.0,
- Maison connectée (domotique...),
- Loisirs,
- Bâtiment connecté (tertiaire),
- Santé et bien-être,
- Commerce et distribution,
- Ville intelligente (Smart City).



Les principaux acteurs



Et chez soi ?

La Domotique !

La domotique ? Kézako ?

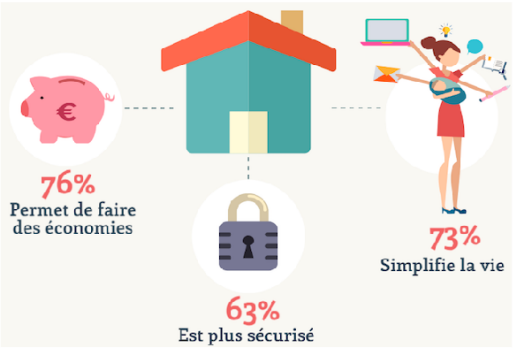
Définition

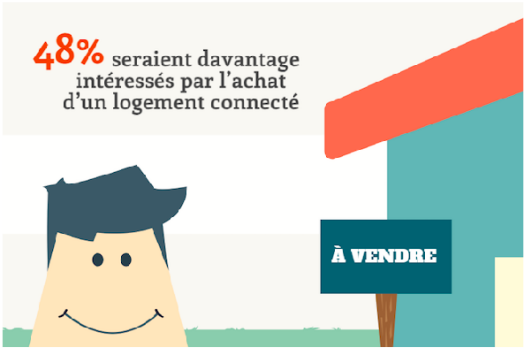
Ensemble des techniques et technologies visant à intégrer à l'habitat tous les automatismes en matière de sécurité, gestion de l'énergie, communication, etc.

- Domaines d'activités principaux
  - La sécurité des biens et personnes
  - La gestion des consommations
  - La gestion des communications
  - Le confort et la qualité de vie

La domotique ? Kézako ? (suite)

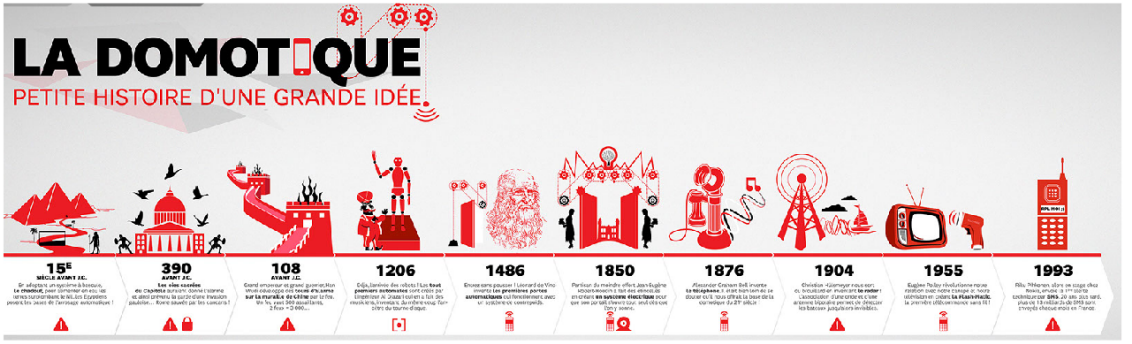
- Quelques chiffres
  - 36% des Français ont des objets connectés à leur domicile
  - 63% des Français souhaitent s'équiper d'objets connectés [2]
  - Environ 30 objets connectés par foyer d'ici 2020 [3]





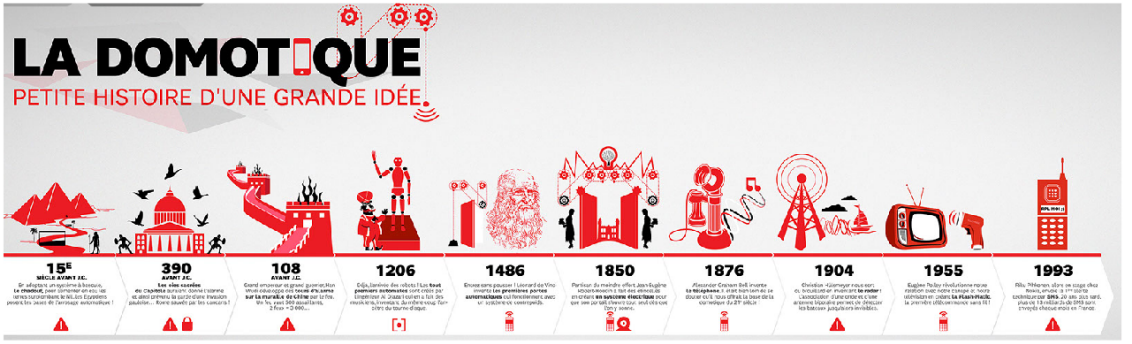
2. https://www.maison-et-domotique.com/67986-infographie-logements-connectes-francais-rapport-tendu
3. Prévisions Institut GFK : https://www.gfk.com/fr/press/gfk-sonde-les-attentes-des-francais-envers-la-maison-connectee

Quel historique ?



- **1898** : Les télécommandes sans fil (Nicolas Tesla)
- **20e siècle** : Les appareils ménagers (aspirateur à moteur (1901), aspirateur électrique (1907), réfrigérateurs, sèche-linge, machines à laver, fers à repasser, etc.)
- **1966** : 1er système d'automatisation baptisé "Echo IV" (Jim Sutherland). Permet de faire une liste d'achats, contrôler la température, allumer et éteindre les appareils
- **1969** : Ordinateur de cuisine Honeywell créant des recettes

Quel historique ?



- **1898** : Les télécommandes sans fil (Nicolas Tesla)
- **20e siècle** : Les appareils ménagers (aspirateur à moteur (1901), aspirateur électrique (1907), réfrigérateurs, sèche-linge, machines à laver, fers à repasser, etc.)
- **1966** : 1er système d'automatisation baptisé "Echo IV" (Jim Sutherland). Permet de faire une liste d'achats, contrôler la température, allumer et éteindre les appareils
- **1969** : Ordinateur de cuisine Honeywell créant des recettes

Quel historique ? (suite)

- **1971** : Le microprocesseur
- **1984** : Invention du terme "smart home" par l'*American Association of House Builder*
- **1990** : Géron-technologie = gérontologie + technologie dans le but d'améliorer la vie des personnes âgées
- **1993** : Utilisation du terme "domotique" afin de décrire la combinaison des appareils ménagers avec des ordinateurs
- **1998** : Maison millénaire Integer à Watford démontrant l'intégration de la domotique à une maison avec des systèmes de chauffage, de sécurité, lumières, portes, etc.
- **2000** : Début de la révolution technologique (technologies plus efficaces et moins coûteuses)

Et maintenant ?

- De nos jours, la domotique est partout !
  - Pas toujours conscience de cela
  - Contrôle des téléviseurs, du chauffage, des lumières, des alarmes via nos smartphones et contrôleurs

Et maintenant ? (suite)

- L'avenir
  - Notre imagination comme seule limite !
  - Avancées technologiques = pouvoir de tout faire (ou presque)
    - Miroirs connectés
    - Réfrigérateurs connectés
    - Armoires intelligentes

---

https://technplay.com/miliboo-miroir-connecte-ekko-1611

Quels avantages ?

- Protection des biens et personnes
  - Alarmes anti-intrusion
  - Détection d'incendie
  - Vidéosurveillance
  - Suivi médical

Quels avantages ? (suite)

- Économies d'énergie
  - Gestion automatique du chauffage
    - Baisser la température de 1°C = 7% d'économie sur le chauffage
  - Détection des défaillances
    - Fuite sur un robinet = 44m^3 d'eau gâchée, +18% sur la facture
  - Programmation des appareils électroménagers en heures creuses

Quels avantages ? (suite)

- Gain en confort et qualité de vie
  - Arrosage automatique
  - Ouverture/fermeture automatisée des volets/portes de garage
  - Programmation des éclairages (intérieur/extérieur)

Les applications et objets connectés

- Recherche simplicité + fonctions basiques ?
  - Utiliser des objets connectés reliés à des applications de smartphone !
    - Alternative intéressante aux installations compliquées des box domotiques
- Exemples
  - Thermostat intelligent
    - Réduction 40% consommation énergétique résidentielle via meilleure gestion du chauffage
  - Interrupteur connecté
    - Contrôle des différents éclairages de la maison via smartphone

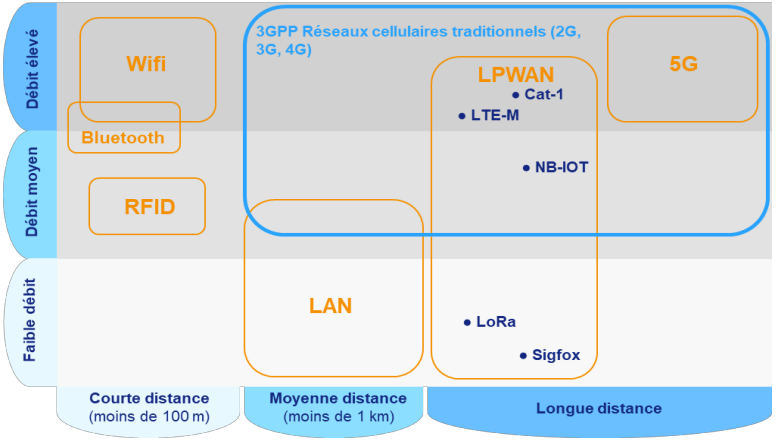
Les applications et objets connectés (suite)

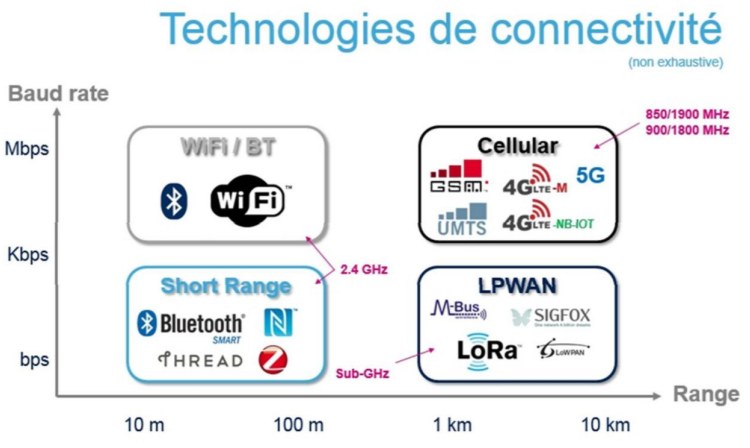
- Concept lié : l'Internet des Objets (IoT)
  - Réseau de terminaux physiques (les "objets") intégrant des capteurs, des logiciels et d'autres technologies en vue de se connecter à d'autres terminaux et systèmes sur Internet afin d'échanger des données avec eux
  - Kevin Ashton (pionnier RFID) invente l'expression "IoT" en 1999
- Enjeux des objets connectés
  - Analyse des données exportées
    - Amélioration des services et produits
    - Suivi de la consommation des usagers
- Exemples
  - Wearables : montres, bracelets, Google Class
  - Domotique : caméra, alarme, four
  - Logistique : suivi des livraisons, géolocalisation

Les applications et objets connectés (suite)

- Avantages
  - Accès aisé aux informations
  - Solutions pilotables à distance
- Inconvénients
  - Compatibilité entre chaque objet...
  - ...et **sécurité du protocole** !

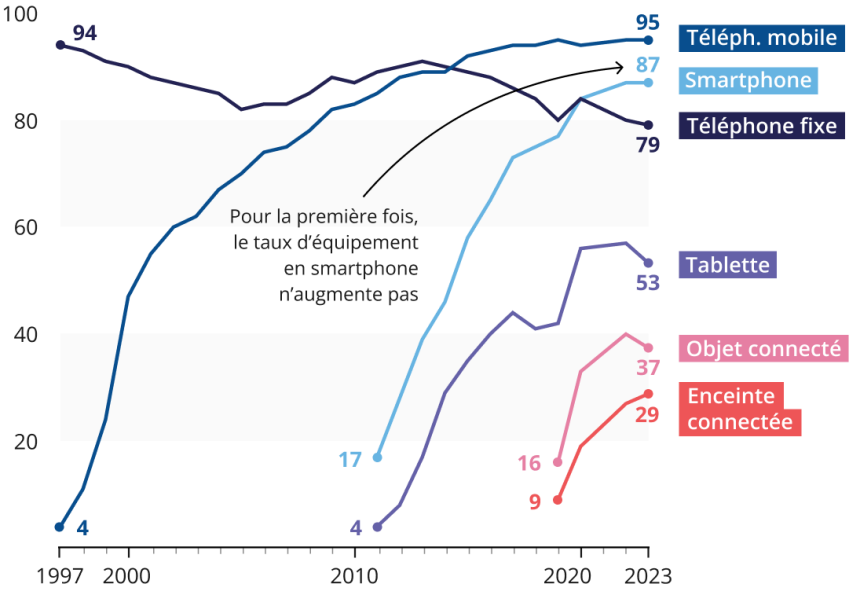
Mais un object connecté, ça communique...
sans fil !


Débit élevé
Débit moyen
Faible débit
Wifi
Bluetooth
RFID
3GPP Réseaux cellulaires traditionnels (2G, 3G, 4G)
LPWAN
• Cat-1
• LTE-M
• NB-IOT
5G
LAN
• LoRa
• Sigfox
Courte distance (moins de 100 m)
Moyenne distance (moins de 1 km)
Longue distance


Technologies de connectivité
(non exhaustive)
Baud rate
Mbps
Kbps
bps
WiFi / BT
Cellular
850/1900 MHz
900/1800 MHz
5G
Short Range
2.4 GHz
LPWAN
Sub-GHz
Range
10 m
100 m
1 km
10 km

Les taux d'adoption des équipements courants se stabilisent, les équipements les plus récents continuent de se diffuser

Evolution du taux d'équipement des répondants (%)



Transmission de l’Information

1 Transmission de l'information : Aspects numériques

Transmission de données numériques

La transmission numérique consiste à faire transiter les informations sur le support physique de communication **sous forme de signaux numériques**.

Les informations numériques :

- ne peuvent pas circuler sous forme de 0 et de 1 directement ;
- doivent être **codées** sous forme d'un **signal** possédant deux états.

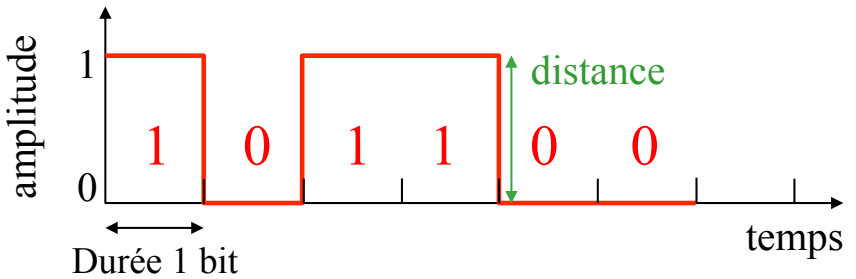
Un signal est une quantité mesurable variant au cours du temps ou dans l'espace.

Exemple :

- deux niveaux de tension par rapport à la masse ;
- la différence de tension entre deux fils ;
- la présence/absence de courant dans un fil ;
- la présence/absence de lumière ;
- *etc.*

La **transformation de l'information binaire sous forme d'un signal** à deux états est réalisée par l'interface.

Exemple : bits codés suivant une différence de tension



L'interface réalise le «*codage en bande de base*».

On parlera de «transmission numérique» ou «transmission en bande de base», *baseband*.

Codage par modulation : les détails

La **modulation** consiste à faire varier une des caractéristiques d'un signal purement sinusoïdal.

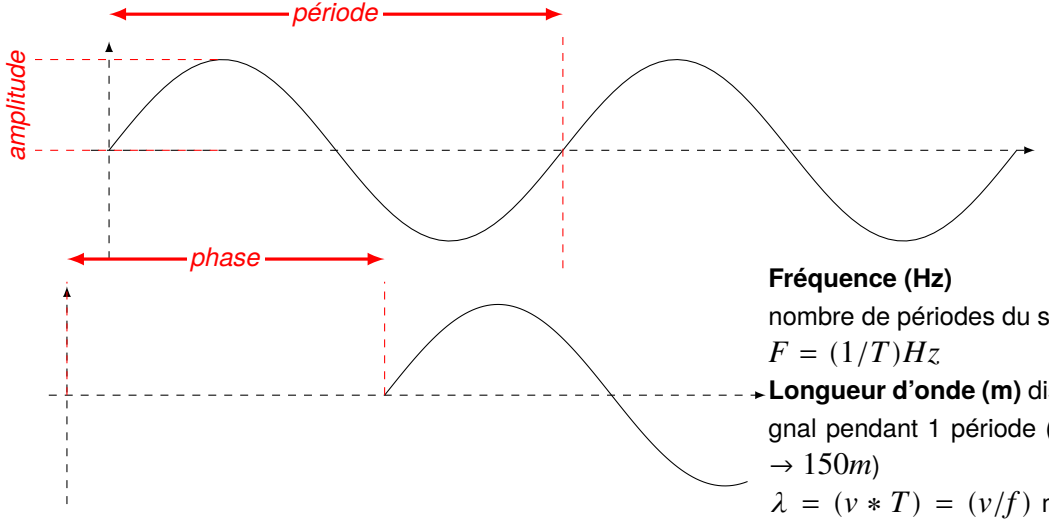
Gain espéré par rapport au codage en bande de base

La fréquence fondamentale de ce signal est beaucoup plus élevée que la fréquence maximale du signal en bande de base (débit des informations binaires à transmettre en fonction de l'horloge).

Conserver et changer

Changer le codage la variation d'un des paramètres se fait en fonction du signal en bande de base (données+horloge), donc seul le codage diffère.
Codage représentation «carrée» → Codage représentation «analogique»

Un signal sinusoïdal est défini par trois paramètres :



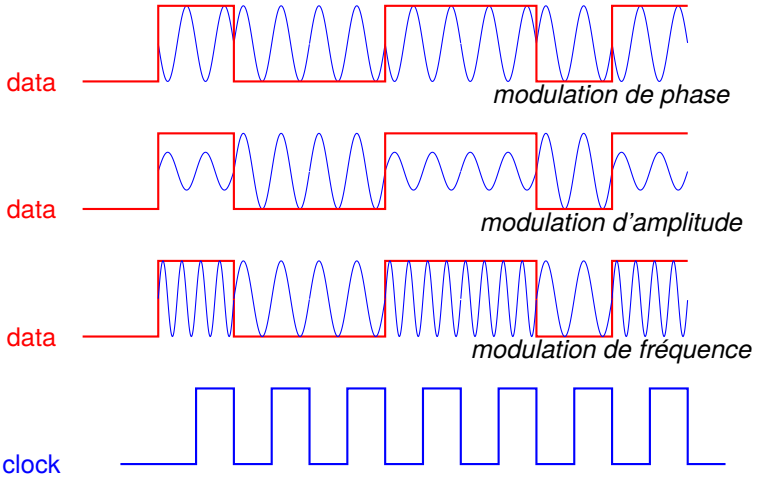
Fréquence (Hz)
nombre de périodes du signal pendant 1 seconde
$F = (1/T)Hz$

Longueur d'onde (m) distance parcourue par le signal pendant 1 période ($1MHz \rightarrow 300m$, $2MHz \rightarrow 150m$)
$\lambda = (v * T) = (v/f)$ mètre avec v, la vitesse de déplacement du signal.

Modulations

- Modulation de **phase** : amplitude et fréquence fixes, phase variable : 0 et $phase$ par exemple ;
- Modulation **d'amplitude** : phase et fréquence fixes, amplitude variable : A_0 et A_1 par exemple ;
- Modulation de **fréquence** : phase et amplitude fixes, fréquence variable : f et $2f$ par exemple ;

Les données à transmettre sont : `1,0,0,1,1,0,1`

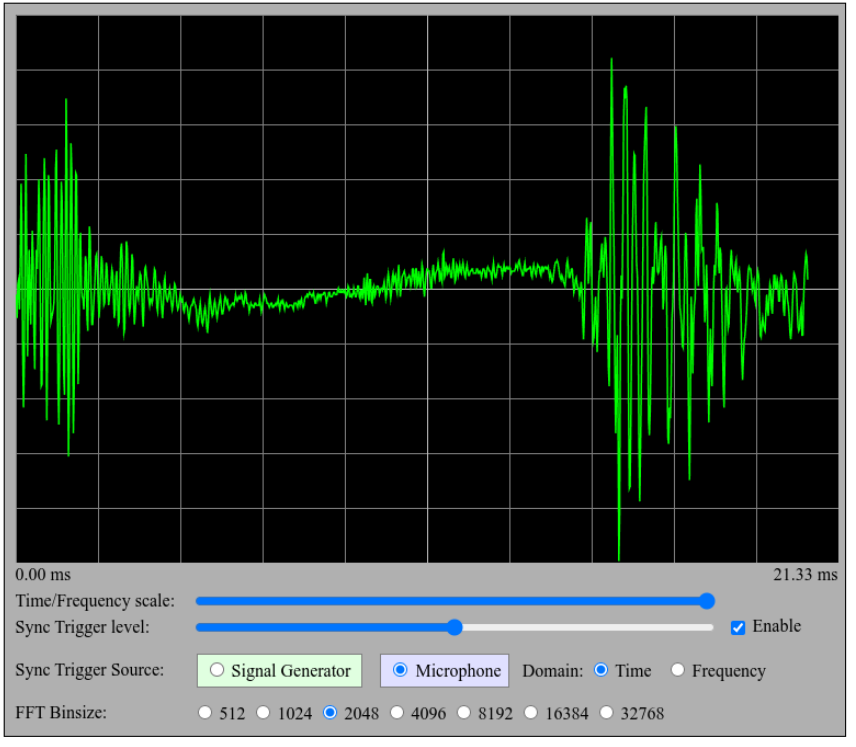


Modulation

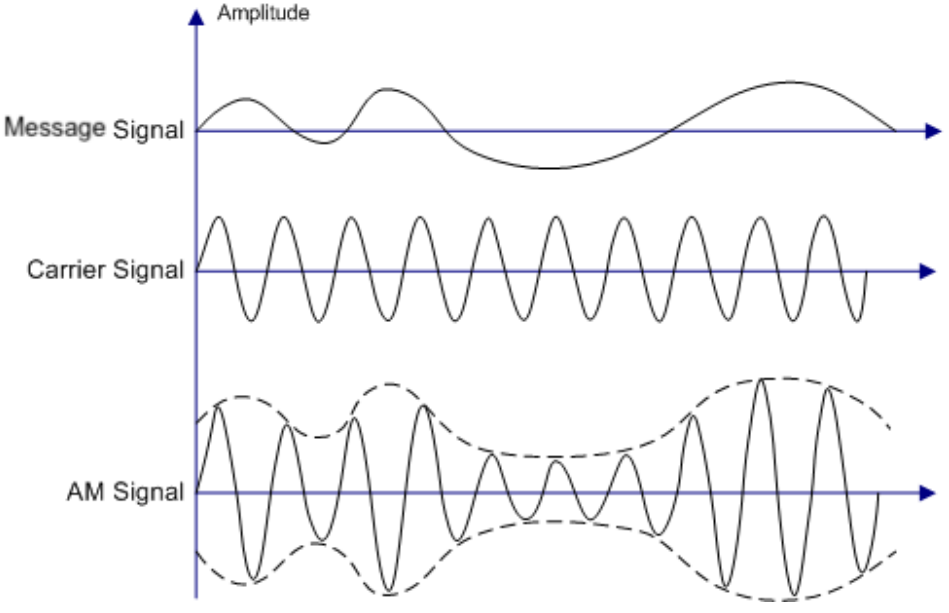
La **variation du paramètre** amplitude, phase ou fréquence peut être faite de manière :

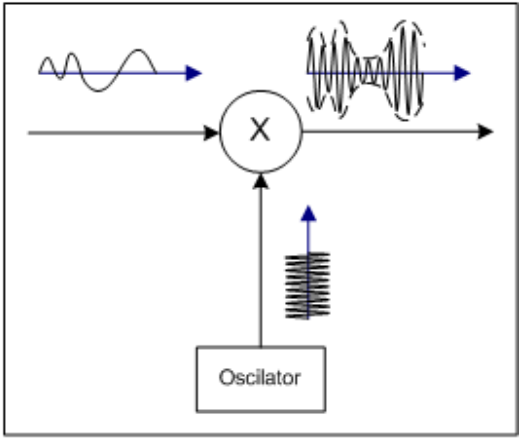
- ▷ **continue** ou *analogique* : on parlera de FM, AM, PM pour «*Frequency Modulation*», *etc*
- ▷ **discrète** ou *numérique* : on parlera de FSK, ASK, PSK, pour «*Frequency Shift Keying*», *etc*

Onde sonore : une capture de la voix



Modulation d'amplitude





En résumé

Transmission

- l'information est **binaire** ;
- elle est envoyée au rythme d'une **horloge** $\Longrightarrow$ lien avec le **débit** ;
- à chaque bit 0 ou 1, on associe un **codage** :
  - fait de transitions «*brutales*» $\Longrightarrow$ codage numérique ;
  - fait de transitions «*douces*» $\Longrightarrow$ codage analogique ;
- en **analogique**, on parle de **modulation**.

Le débit est-il limité ?

Oui...

La «bande passante» : éviter les mauvaises fréquences

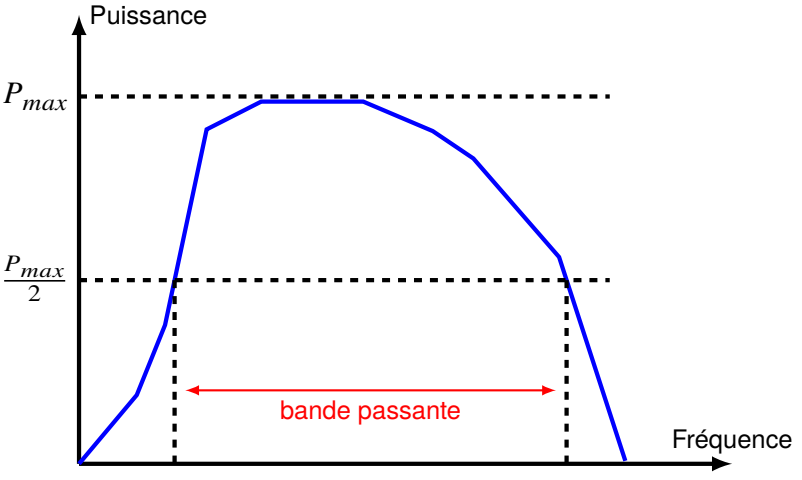
Notion de bande passante

Elle désigne la **différence**, en Hz, entre la plus haute et la plus basse des **fréquences utilisables** sur un support de transmission.

Dans la pratique, ce terme désigne le débit d'une ligne de transmission, calculé en quantité de données susceptibles de transiter dans un laps de temps donné (exprimé en bits par seconde).

Plus la **bande passante est large**, **plus** le volume d'informations qui peut transiter est **important**.

Bande passante :
Largeur de la bande de fréquence pour laquelle la puissance reçue est **supérieure à la puissance émise maximale divisée par deux** $(-3dB)$



Exemples :

- Une ligne de téléphone a une bande passante comprise entre 300 et 3400 Hertz environ pour un taux d'affaiblissement égal à 3db ;
- Paire métallique : $10MHz$, Câble coaxial : GHz, Fibre optique : $100GHz$.

La capacité d'une ligne de transmission

Remarques

D'après la **bande passante**, certaines fréquences ne peuvent être utilisées.
En particulier, les fréquences **les plus hautes**.

Intuitivement, plus la fréquence augmente plus on peut coder d'information.
$\Longrightarrow$ il existe une **borne maximale** pour la quantité d'information que l'on peut encoder !

Cette **borne maximale** :

- dépend du **bruit**, qui dépend de la nature de la ligne de transmission ;
- définit une notion de **capacité** de la ligne de transmission.

La **capacité** d'une ligne de transmission est la **quantité d'informations** (en bits) pouvant être transmis sur la voie en **1 seconde**.

Théorème de Shannon

La capacité se caractérise de la façon suivante :

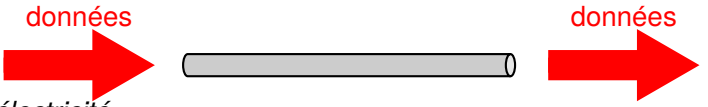
$$C = W \log_2(1 + \frac{S}{N})$$

- C capacité (en bits/s) ;
- W largeur de bande (en Hz) ;
- S/N rapport signal sur bruit, «*noise*», de la ligne de transmission.

Et pour les transmissions sans fil ?

Transmission de l'information

- Dans un fil de cuivre, le **signal** en entrée est **récupéré** en sortie :



Le fil de cuivre conduit l'électricité.

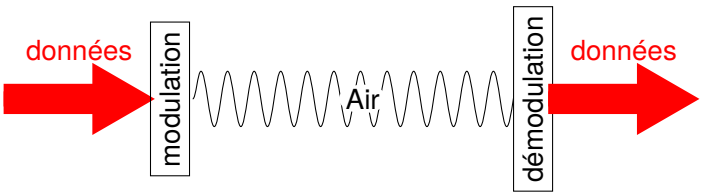
- L'air est un **isolant** pour l'électricité :

L'air ne conduit pas l'électricité...

- les **ondes électromagnétiques** peuvent être transportées dans l'air sur de longues distances :

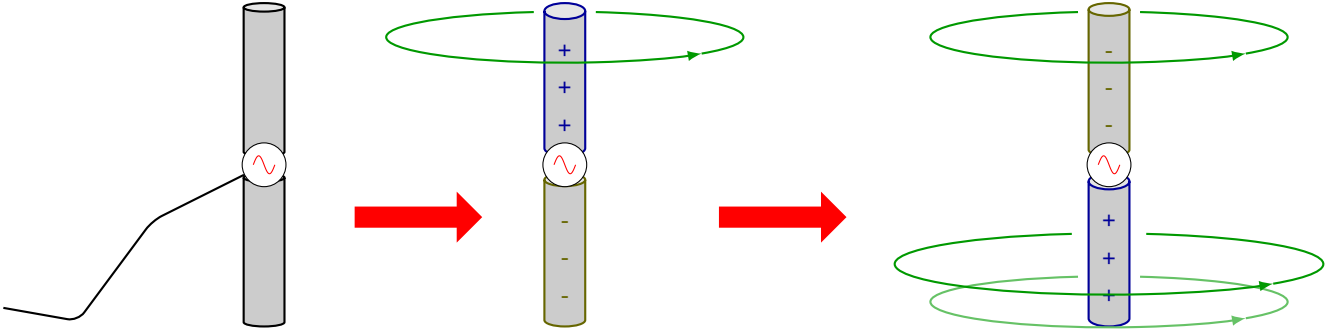
Les données doivent être :

- ▷ «portées» *par l'onde électromagnétique* ⟹ «modulation»
- ▷ *récupérées lors de leur réception* ⟹ «démodulation»

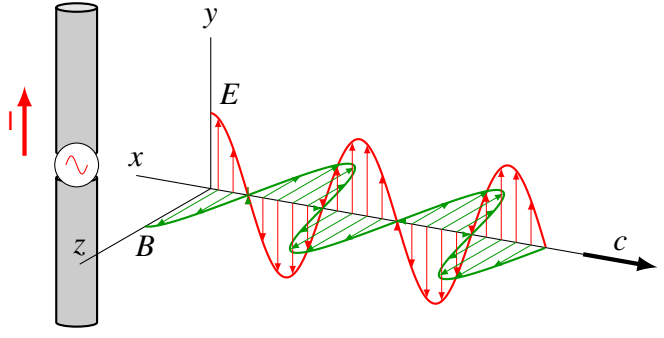


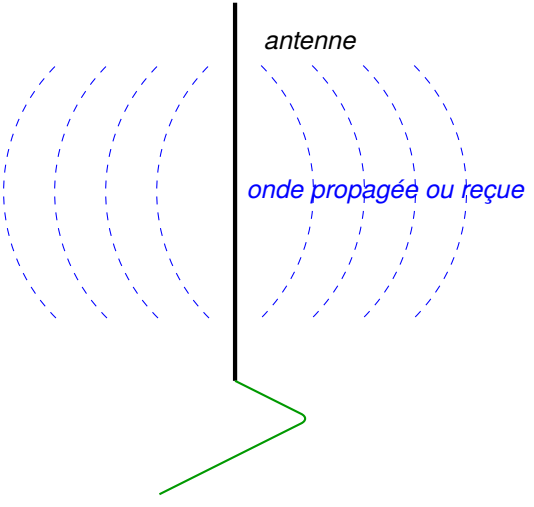
Champs électrique *vs* Champs magnétique

La **variation** d'un courant alternatif dans un **dipole** crée une onde électromagnétique :



Cette variation de champs électrique induit la variation d'un champs électromagnétique et **réciproquement** :





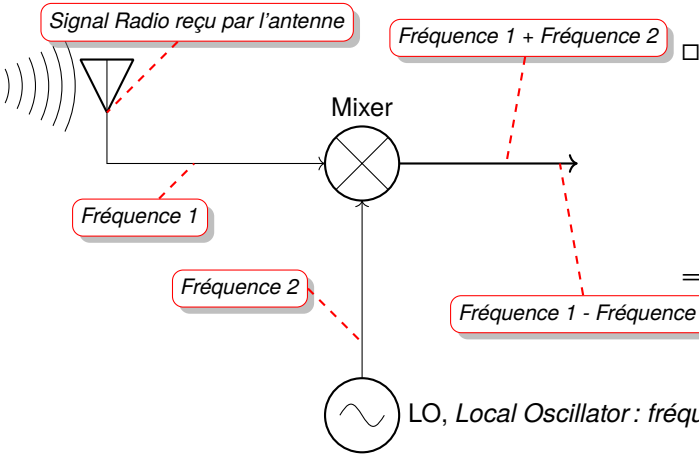
Où :

E	champs électrique
B	champs magnétique (valeurs instantanées)
c	vitesse de la lumière

2 Réception radio et traitement du signal

Traitement du signal **hétérodyne**

Combiner un signal de **haute** fréquence avec un autre pour produire un signal de **basse** fréquence.



- Création de **nouvelles fréquences** par la combinaison ou le mixage de **deux fréquences** :
  - une fréquence **plus basse** : la *différence* des fréquences ;
  - une fréquence **plus haute** : la *somme* des fréquences ;

  } *Appelées hétérodynes*

$\Longrightarrow$ **décalage de la fréquence du signal original !**

- Exemple : **décalage** du signal de 110MHz à 10MHz par mixage avec une fréquence de 100MHz
  $\Longrightarrow$ on travaille sur 10MHz, ce qui est plus facile.

Transmission/Réception

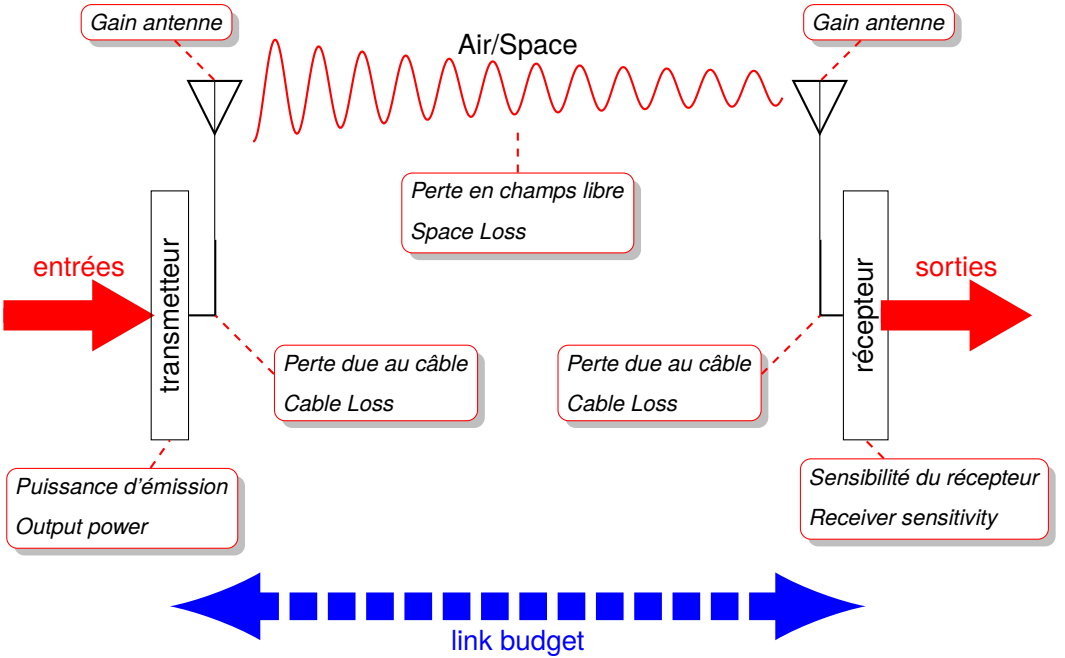
- on choisit une fréquence de transmission adaptée : réglementation, propriétés physiques (FSL, coût de l'électronique, *etc*) $\Longrightarrow$ ce sera la **fréquence support** ou «*porteuse*» ou «*carrier*»
- on choisit une **modulation** adaptée à ce que l'on veut transmettre ;
- on **décale** cette modulation vers la porteuse grâce à l'opération **hétérodyne**.

En résumé

Transmission

- la transmission radio est possible grâce aux ondes électromagnétiques ;
- elles sont créées par une variation du courant électrique ;
- grâce au **principe hétérodyne**, on peut «*placer*» une **modulation** à une fréquence voulue qui peut être **bien plus élevée** que celle de l'horloge ;
- **Mais comment s'y retrouver ?** $\Longrightarrow$ **le «*bilan de liaison*»** qui prend en compte :
  - la **puissance** de transmission ;
  - les p**ertes subies** par l'onde électromagnétique ;
  - les caractéristiques de l'émetteur et du récepteur :
    - qualité des **composants** ;
    - **antenne** ;
    - **sensibilité** ;
    - **bruit** présent sur le récepteur.

Le bilan de liaison ou «*link budget*»



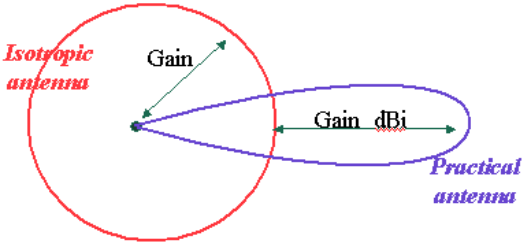
Le «*Link budget*» permet de :

- **mesurer** les différents **paramètres** et **composants** intervenant sur la liaison entre émetteur et récepteur ;
- **déterminer** si une communication est **possible** suivant ces paramètres et composants.

Antenne et transmission effective

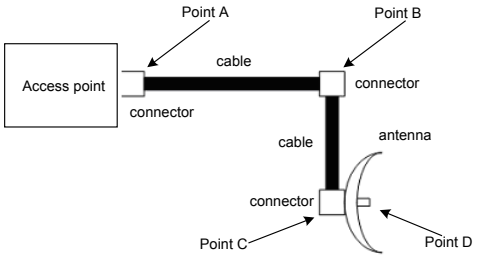
Une antenne **isotrope** est une *antenne théorique* qui rayonne de **manière uniforme** dans **toutes les directions**, c-à-d suivant une sphère et son gain est égal à l'unité.

Une antenne **quelconque** émet *plus dans une direction*, c-à-d qu'elle a un **gain** par rapport à l'antenne isotrope dans cette direction.
Le gain est exprimé en dBi.



La puissance émise au niveau du transmetteur

L'«EIRP», «*effective isotropically radiated power*», ou PIRE, «puissance isotrope rayonnée équivalente» :



	Access Point	Point A	Point B	Point C	Point D
	100 mW	-3 dB	-3 dB	-3 dB	+12 dBi
=	100 mW	÷2	÷2	÷2	(x2 x2 x2 x2)
=	100 mW	÷2	÷2	÷2	x16
=	50 mW		÷2	÷2	x16
=	25 mW			÷2	x16
=	12.5 mW				x16
=	200 mW				

$$EIRP_{[\text{dBm}]} = P_{T_{[\text{dBm}]}} - L_{c_{[\text{dB}]}} + G_{a_{[\text{dBi}]}}$$

où :

- ▷ P_T est la puissance de transmission ;
- ▷ L_c est la perte, «*loss*», dans les câbles et connecteurs ;
- ▷ G_a est le gain de l'antenne.

Affaiblissement en espace libre, «*Free Space Loss*»

D'après Wikipedia

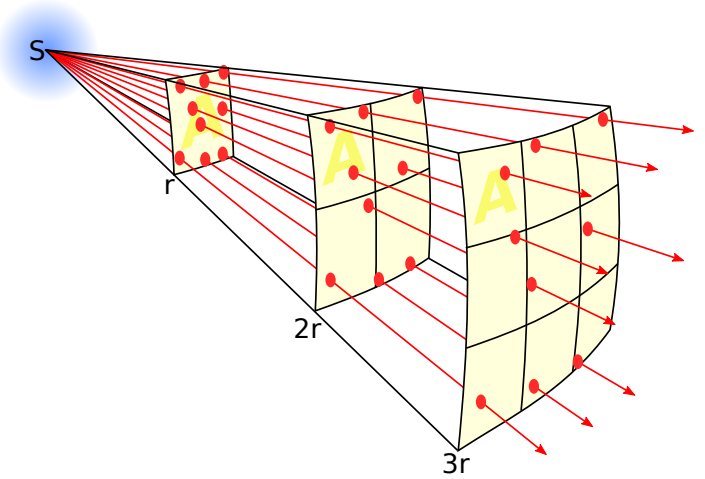
En physique, une loi en **carré inverse** est une loi physique postulant qu'une quantité physique (énergie, force, ou autre) est inversement proportionnelle au carré de la distance de l'origine de cette quantité physique.

L'intensité est **inversement proportionnelle** au **carré de la distance** :

$$\text{Intensité} \propto \frac{1}{\text{distance}^2}$$

Affaiblissement en espace libre : la puissance du signal est diminuée par la répartition géométrique du «front d'onde».

On parle de FSL, «*Free Space Loss*» ou de FSPL «*Free Space Path Loss*».



*La **puissance du signal** se répartit sur le front d'onde, dont la surface augmente en même temps que la distance depuis la source augmente. C'est pourquoi l**a densité de cette puissance diminue** (les lignes de flux issues de la source, en rouge sur le schéma, ont une densité moindre si la distance augmente).*

Affaiblissement en espace libre, «*Free Space Path Loss*»

$\text{FSPL}_{\text{dB}} = 10\log_{10}\left(\frac{4\pi df}{c}\right)^2$ où d est la distance en mètre,
f est la fréquence en Hertz et c, la vitesse de la lumière.

$\text{FSPL}_{\text{dB}} = 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right)$

Ce qui donne : $\text{FSPL}_{\text{dB}} = 20\log_{10}(d) + 20\log_{10}(f) - 147,55$

Et si on exprime
▷ f en MHz
▷ d en km,
cela donne la formule suivante :

$\text{FSPL}_{\text{dB}} = 20\log_{10}(d) + 20\log_{10}(f) + 32,45$

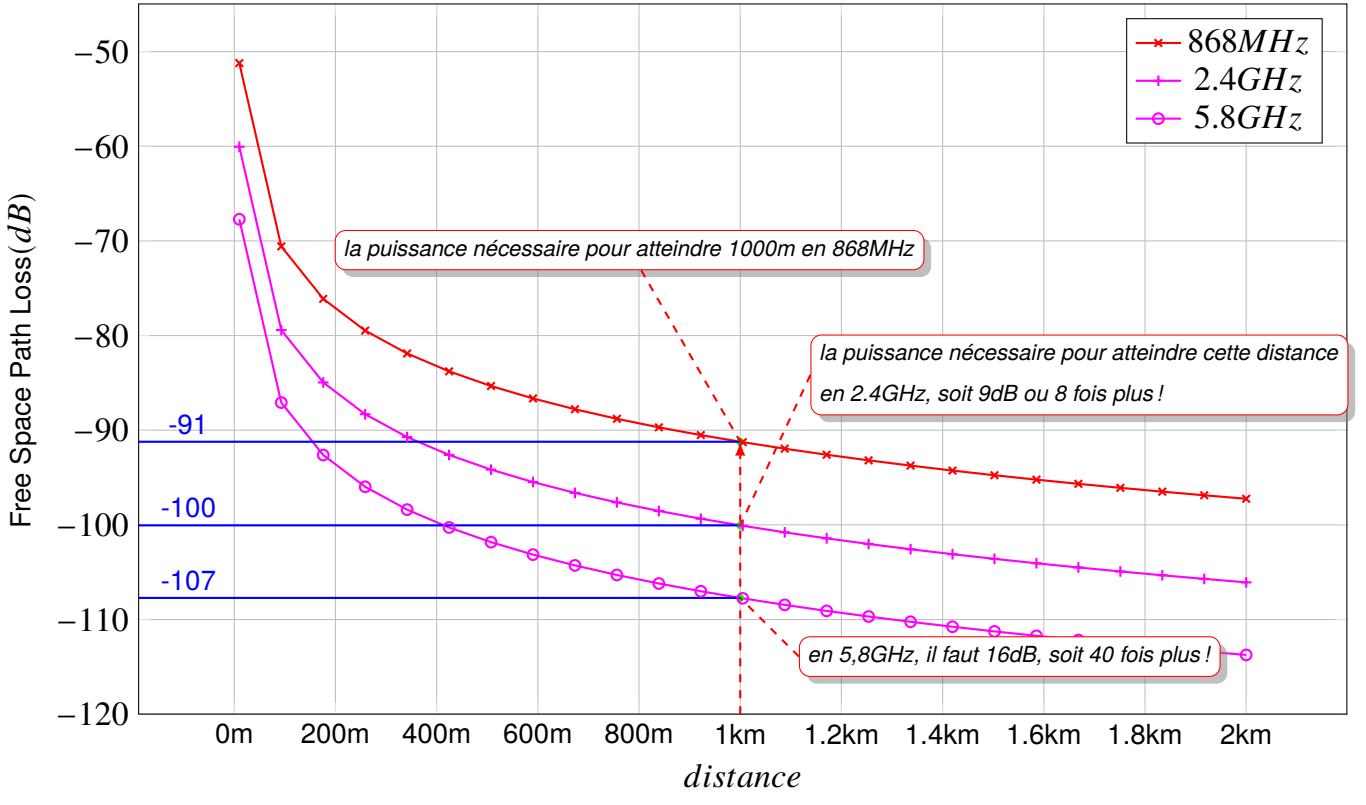
D'où la table suivante :

On remarquera que pour la fréquence du WiFi de $2485Mhz$, on obtient la formule simplifiée :
$\text{FSPL}_{\text{dB}} = 100 + 20\log_{10}(d)$, avec une distance exprimée en km.

	Fréquence		
Distance	868MHz	2.4GHz	5.8GHz
1km	91.22	100.05	107.72
2km	97.24	106.07	113.74
3km	100.76	109.60	117.26
4km	103.26	112.10	119.76
5km	105.20	114.03	121.70
10km	111.22	120.05	127.72
20km	117.24	126.07	133.74
30km	120.76	129.60	137.26
40km	123.26	132.10	139.76
50km	125.20	134.03	141.70

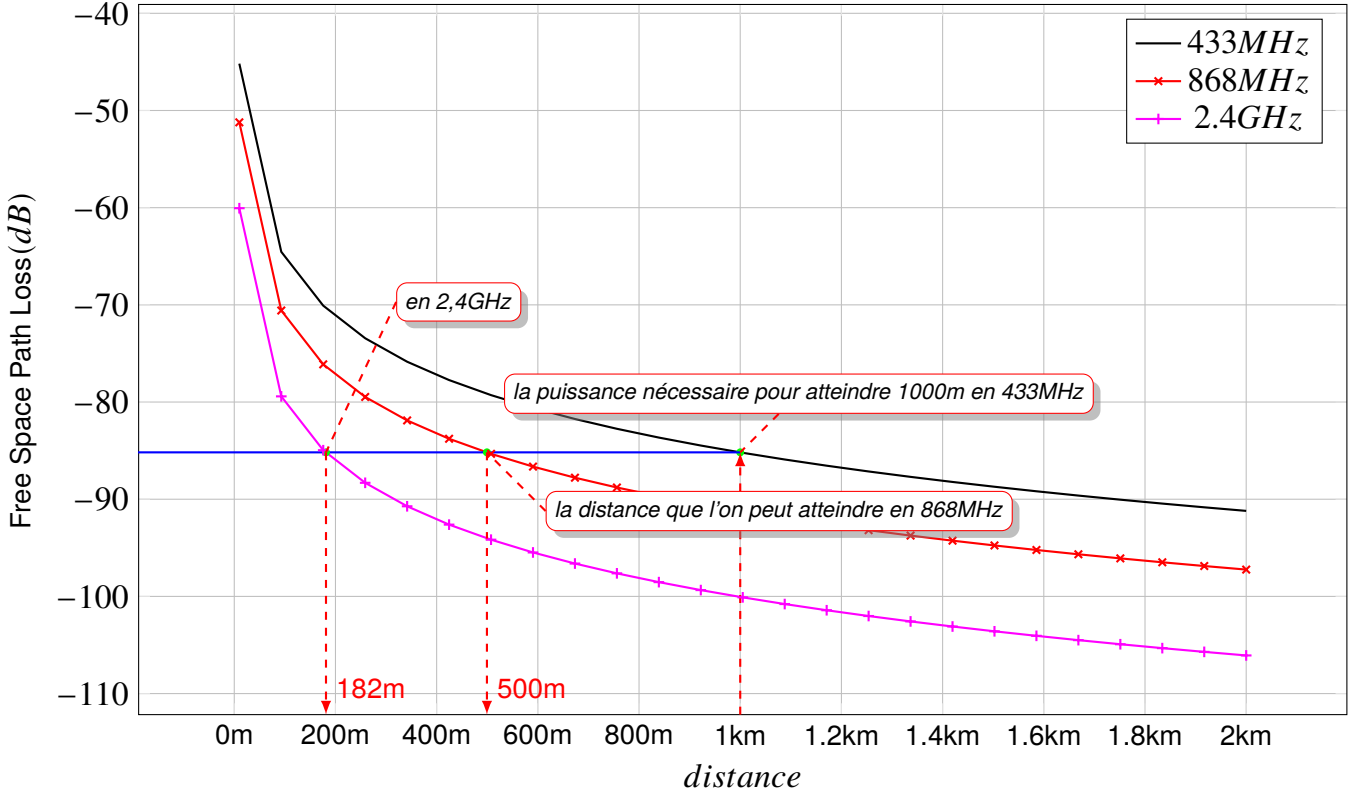
Affaiblissement en espace libre, «*Free Space Path Loss*»

Plus la **fréquence** est **élevée**, plus la **perte** est **importante** :



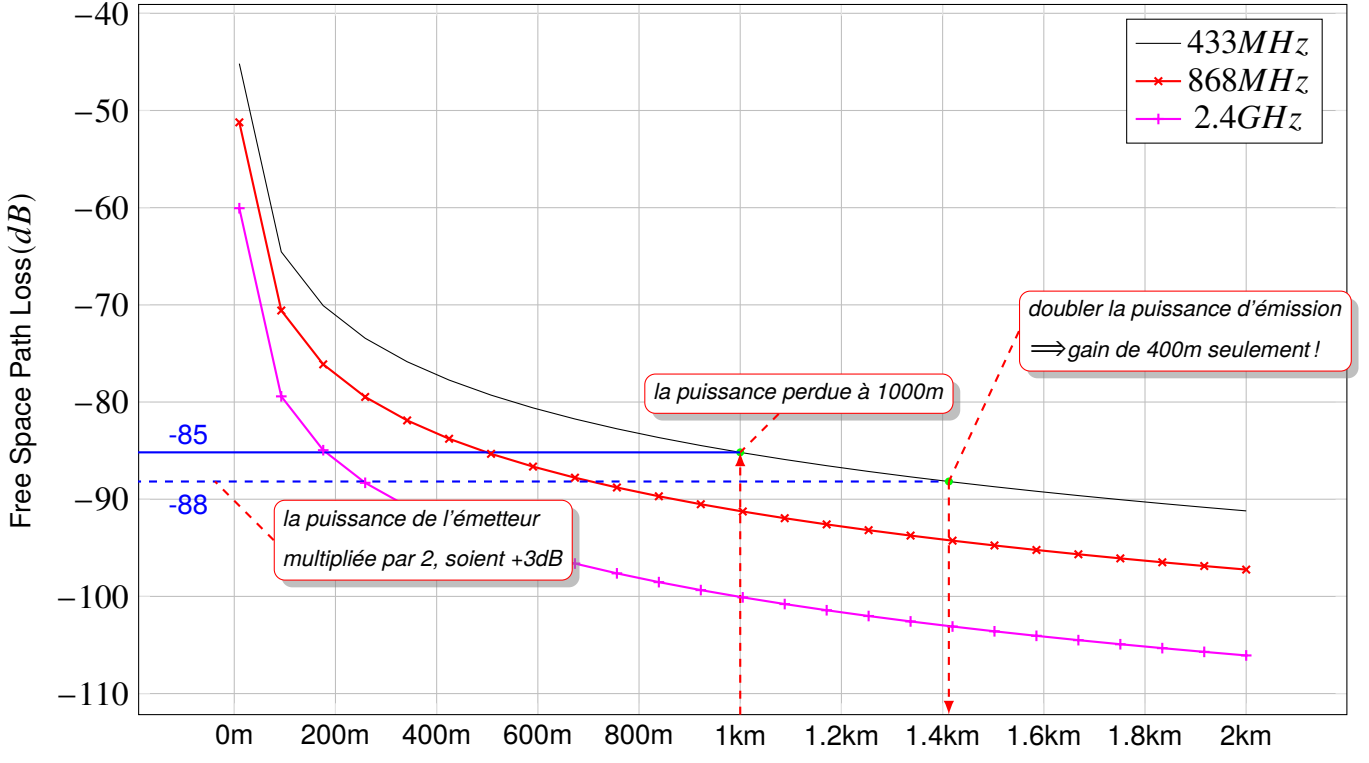
Affaiblissement en espace libre, «*Free Space Path Loss*»

Pour des fréquences standards de $433MHz$, $868MHz$ et $2,4GHz$:



Affaiblissement en espace libre, «*Free Space Path Loss*»

En considérant la fréquence de $433MHz$, on constate que **doubler la puissance** permet un gain de **distance** :



$\Longrightarrow$Un gain de $+3dB$, peut être **facilement** obtenu avec une **meilleur antenne** !

Obstacles et pertes

La réception est affectée par la **traversée des matériaux** occultant la ligne de vue, «*line of sight*» :

Materiaux	**Atténuation à 900MHz**
Verre 6mm	0,8 dB
Verre 13mm	2 dB
Bois 76mm	2,8 dB
Brique 89mm	3,5 dB
Brique 178mm	5 dB
Brique 267mm	7 dB
Béton 102mm	12 dB
Parpaing 203mm	12 dB
Parpaing 406mm	17 dB
Béton 203mm	23 dB
Béton renforcé 203mm	27 dB
Parpaing 610mm	28 dB
Béton 305mm	35 dB

Le béton est un très bon atténuateur...

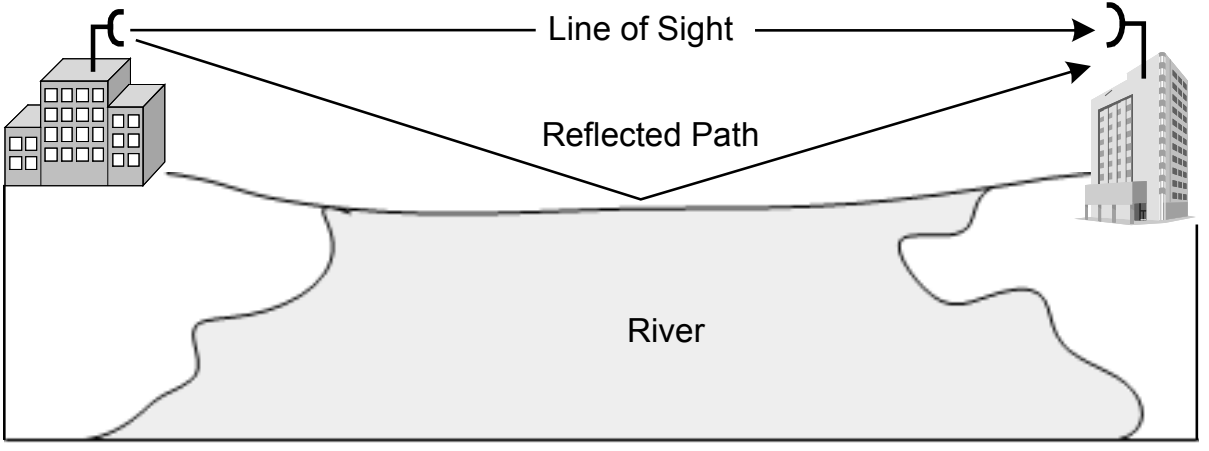
Autres atténuations et améliorations

Suivant la nature des obstacles à traverser, la perte est plus ou moins importante :

- ▷ arbres : 10 à 20dB ;
- ▷ murs : de 10 à 15dB ;
- ▷ sols : de 12 à 27dB (du sol en bois à celui en béton armé) ;

Mais...

Les obstacles peuvent **améliorer** le signal reçu :



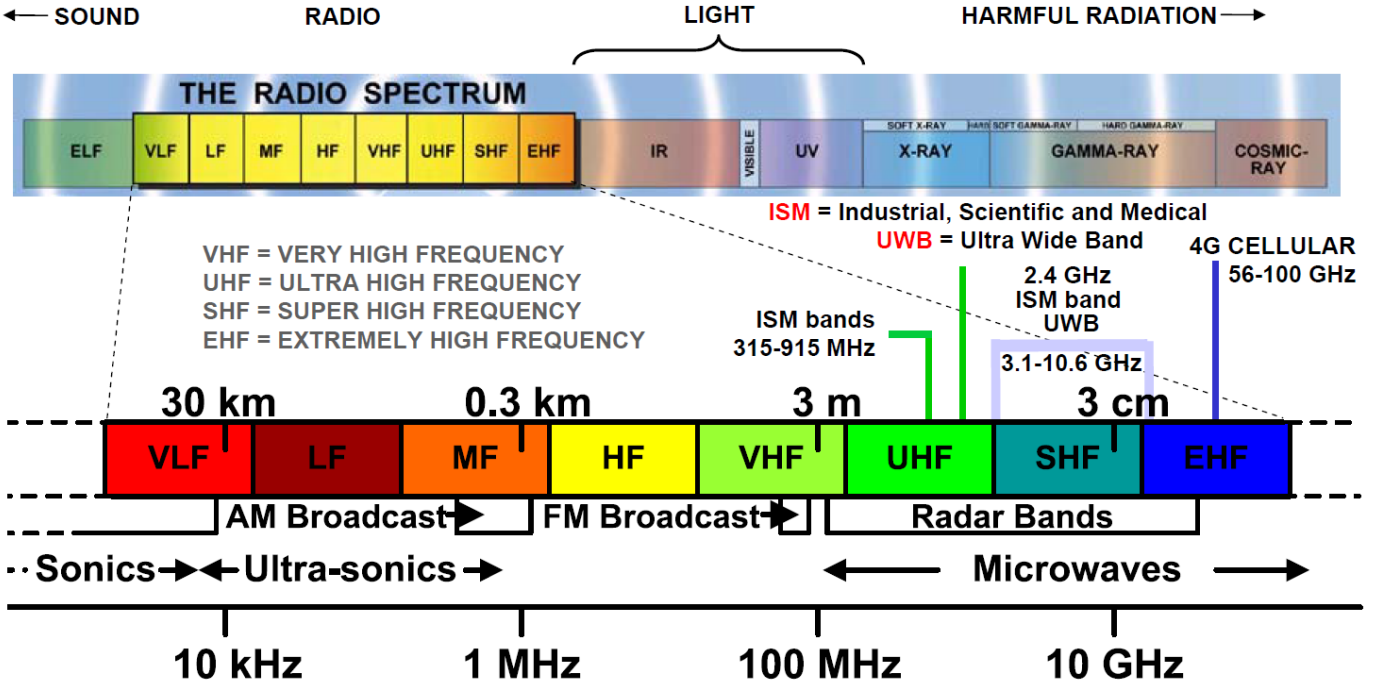
On se sert des multiples chemins, «multipath» *pour améliorer la réception du signal à l'aide de plusieurs antennes,* «diversity».

Peut-on utiliser toutes les fréquences ?

La répartition des fréquences

L'allocation des fréquences est :

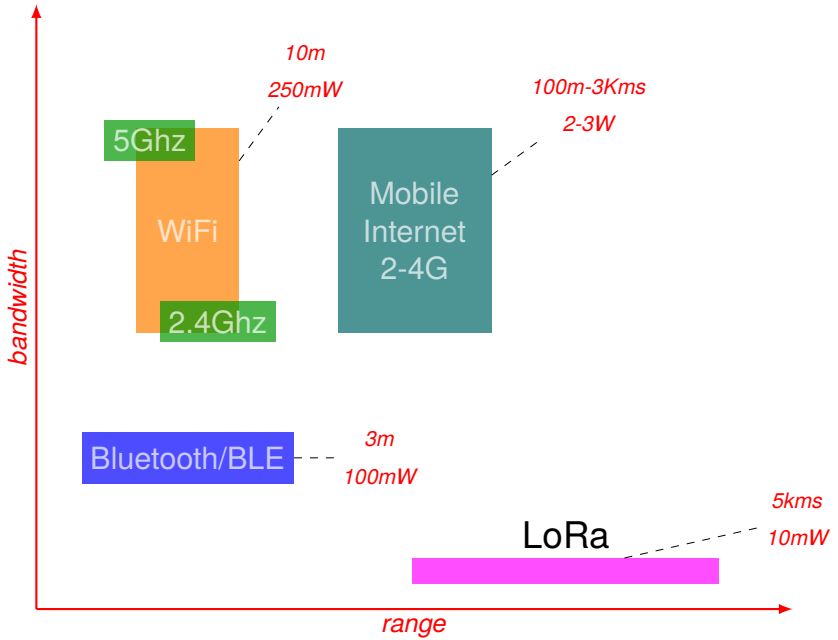
- ▷ relatives aux aspects physiques et propriétés de ces fréquences : son, lumière, radiation ;
- ▷ soumises à régulation des états : allouées aux radios diffusant de la musique, bande ISM, *etc*.



Application au LoRa

Low Power Wide Area Network : LPWAN

- «*Low Power*» *vs Wide Area* : pour transmettre sur de longues distances avec un **minimum d'énergie** on doit utiliser une faible bande passante ou «*bandwidth*» ;
- **faible bande passante** $\Longrightarrow$ faible capacité de communication du canal (théorême de Shannon) ;



LoRa, fréquences autorisées :

- 868 MHz ;
- 915 MHz ;
- 433 MHz ;

OVERVIEW – Usages

Long rage communications even in dense urban areas

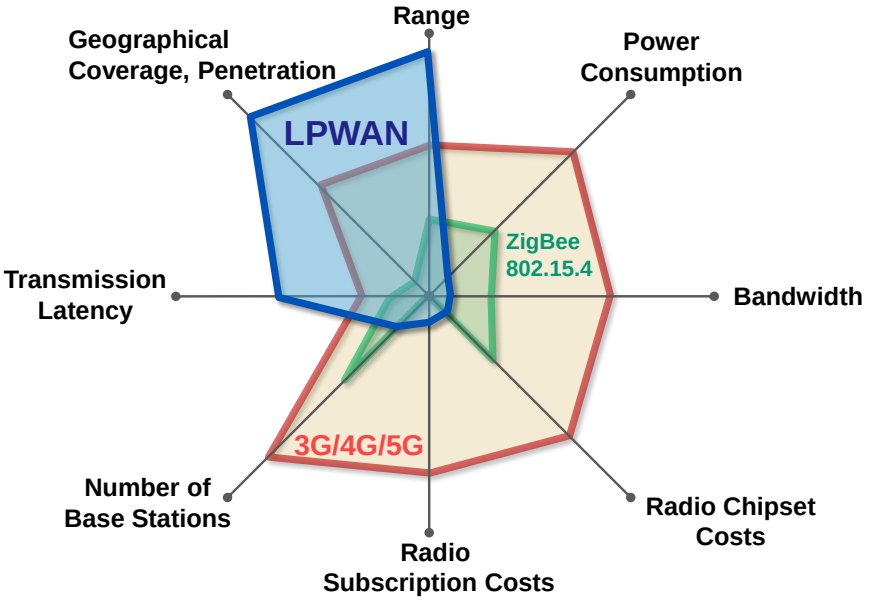
Smart City: smart grid, metering, lighting, structural health monitoring…
Smart Industry: predictive maintenance…

Isolated assets for applications requiring long life battery

Smart Agriculture: irrigation systems, …
Smart Grid / Water: metering

2. LPWAN requirements and characteristics (1/2)

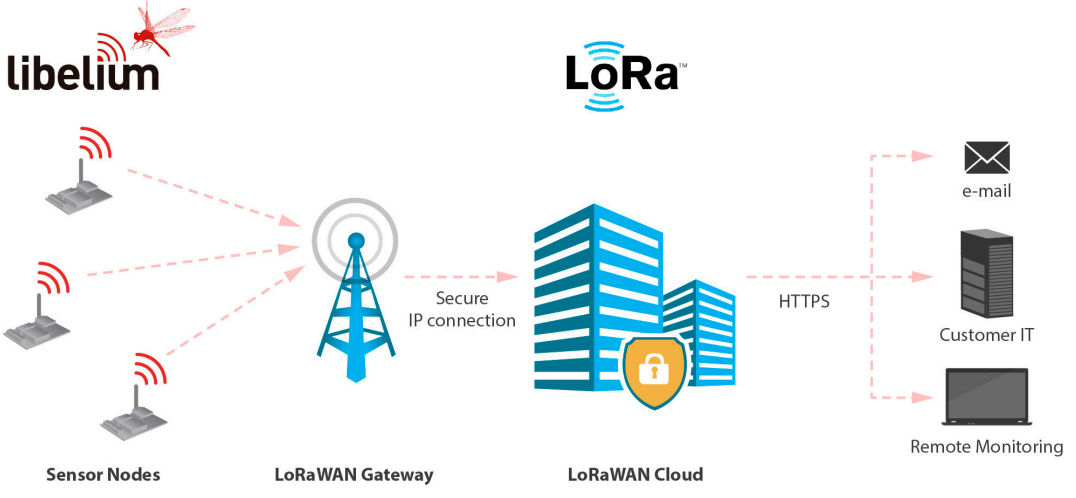
The needs of IoT and M2M applications pose some unique requirements on LPWAN technologies as shown in the comparison with other wireless technologies:



LoRaWan

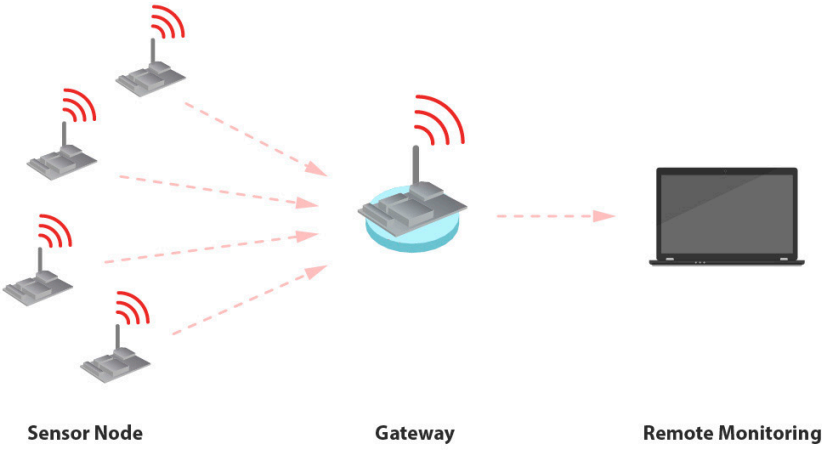
LoRa vs LoRaWan

- **LoRa** correspond au «*link layer protocol*» : peut être utiliser pour des communications P2P entre les nœuds ;
- **LoRaWan** inclus la «couche réseau» en plus : possible d'envoyer des informations à n'importe quelle «base station» déjà connectée au Cloud $\Longrightarrow$ c'est ce modèle qui correspond à l'internet des objets, «*IoT*».
  Les modules LoRaWan fonctionnent sur plusieurs canaux et mêmes plusiseurs fréquences simultanéments (plusieurs antennes) :
  - communications entre les nœuds et les «*gateways*» : différents canaux et différents débits, «data rate» :
    - différents débits : compromis entre portée radio et durée du message ;
    - différents canaux (étalement de spectre + choix d'un canal) : pas d'interférences entre les communications et création de canaux «virtuels» : augmente la capacité de la passerelle ;
    - ADR, «*Adaptive Data Rate*» : permet d'adapter le débit, la puissance de transmission pour augmenter la capacité de gestion de la passerelle et optimiser la batterie des nœuds ;
  - «*gateways*» : connectées par IP et capable de s'intégrer au Cloud ;



LoRa *vs* LoraWan

Lora : communications en P2P



- ▷ pas de «*base station*», ni de Cloud (pas d'abonnement à une plateforme de médiation) ;
- ▷ The Internet of Things Network, TTN, `https://www.thethingsnetwork.org`

LoRaWan, est-ce nécessaire ?

- ▷ sensibilité de -136dBm combinée avec une puissance d'émission de +14dBm : 140dB de «*link budget*» ;
- ▷ portée en LOS, «*Line of Sight*» de 22km ou 2km en NLOS ;
- ▷ fréquence de 868MHz contre 2,4GHz pour le WiFi :
  - ◇ meilleure pénétration des matériaux : briques, ciment, arbres ;
  - ◇ moins d'atténuation en FSPL, «*free-space path loss*» ;

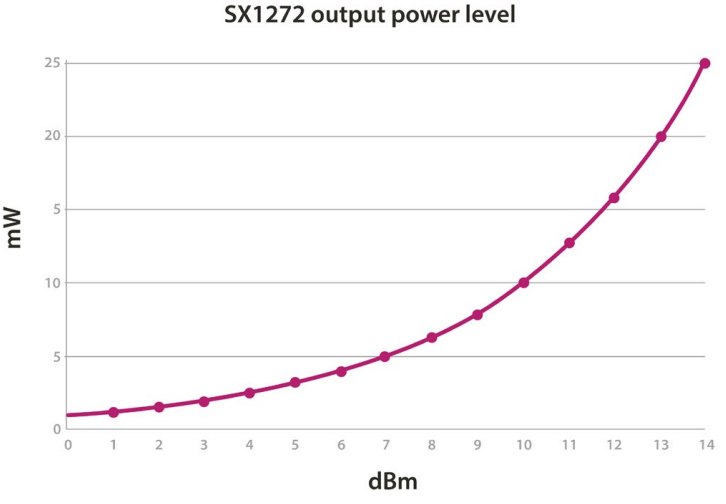
Et en vrai, ça donne quoi ?

LoRa : le composant SX1272

Choix du canal et de la puissance de transmission

Channel Number	Central frequency
CH_10_868	865.20 MHz
CH_11_868	865.50 MHz
CH_12_868	865.80 MHz
CH_13_868	866.10 MHz
CH_14_868	866.40 MHz
CH_15_868	866.70 MHz
CH_16_868	867 MHz
CH_17_868	868 MHz

Parameter	SX1272 power level
'L'	0 dBm
'H'	7 dBm
'M'	14 dBm

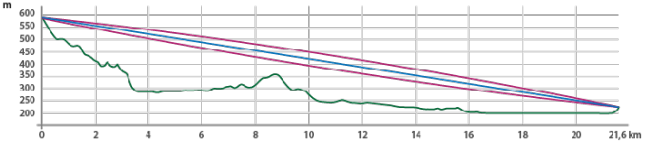


LoRa : test

Coupe du terrain :

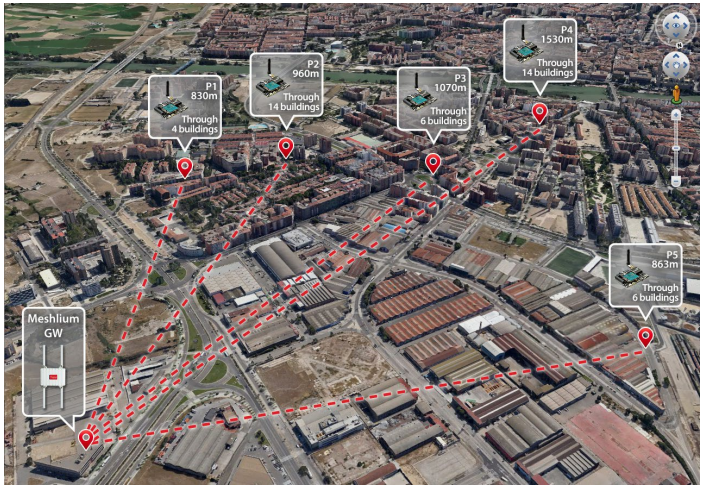
- ▷ la ligne bleue représente la ligne de vue ;
- ▷ l'ellipse mauve représente la zone de Fresnel ;

On notera qu'il n'y a pas d'obstacles dans la zone, ce qui minimise la FSPL, «Free-Space Path Loss».



LoRa Mode	Range	Power	Channel	Success (%)	Mean SNR (dB)	Mean RSSI (dBm)	Mean RSSI packet(dBm)	Sensitivity (dB)	Margin (dB)
Mode 1	21.6 km (13.4 miles)	High	CH_12_868	100	-9.79	-113.72	-126.79	-134	7.21
		Max		100	-4.33	-113.76	-121.76	-134	12.24
		High	CH_16_868	100	-10.06	-114.28	-127.06	-134	6.94
		Max		100	-3.20	-113.97	-120.21	-134	13.79
Mode 3	21.6 km (13.4 miles)	High	CH_12_868	95	-10.29	-114.16	-127.29	-129	1.71
		Max		95	-3.73	-114.08	-120.73	-129	8.27
Mode 6	21.6 km (13.4 miles)	High	CH_12_868	99	-14.77	-107.22	-125.77	-125.5	-0.27
		Max		100	-8.42	-106.60	-119.43	-125.5	6.07
Mode 9	21.6 km (13.4 miles)	High	CH_12_868	0	-	-	-	-117	-
		Max		49	-9.95	-107.68	-120.95	-117	-3.95

LoRa : test

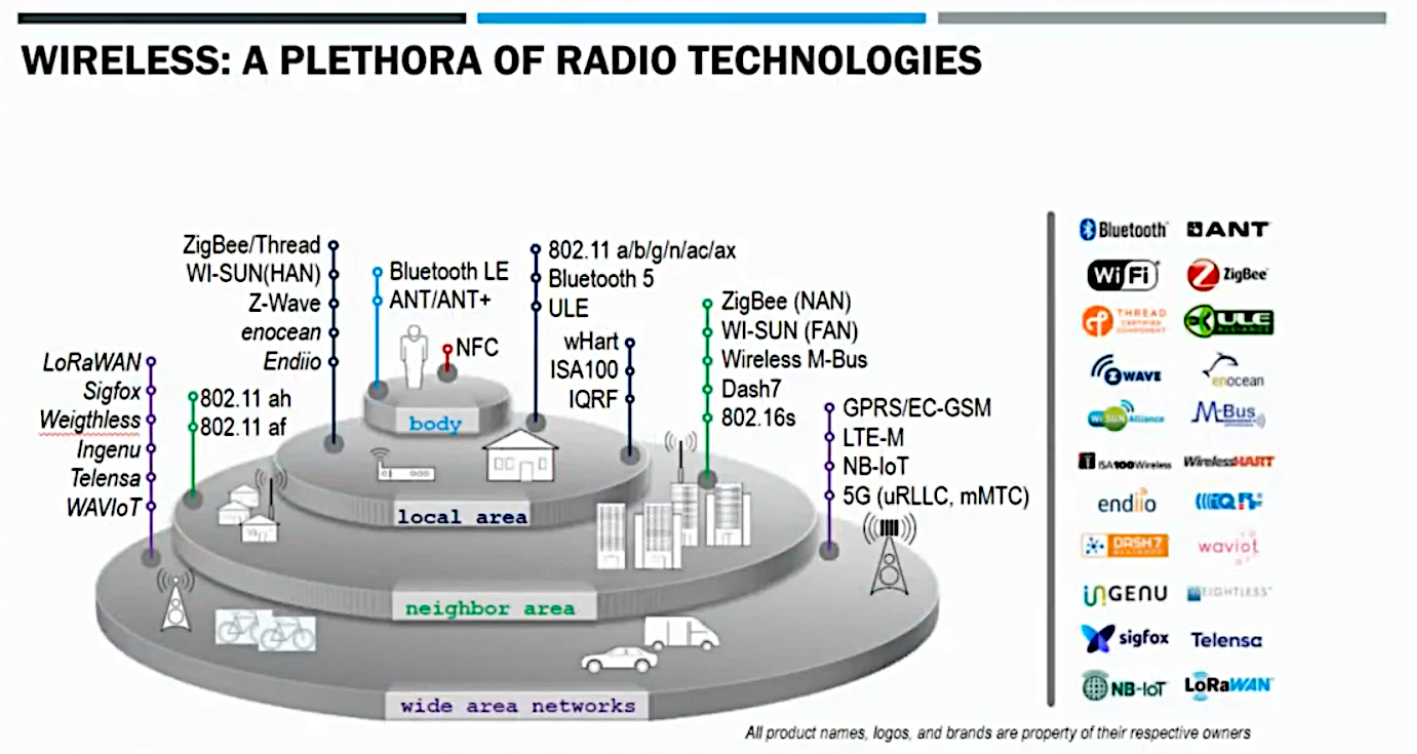


Les différents points :

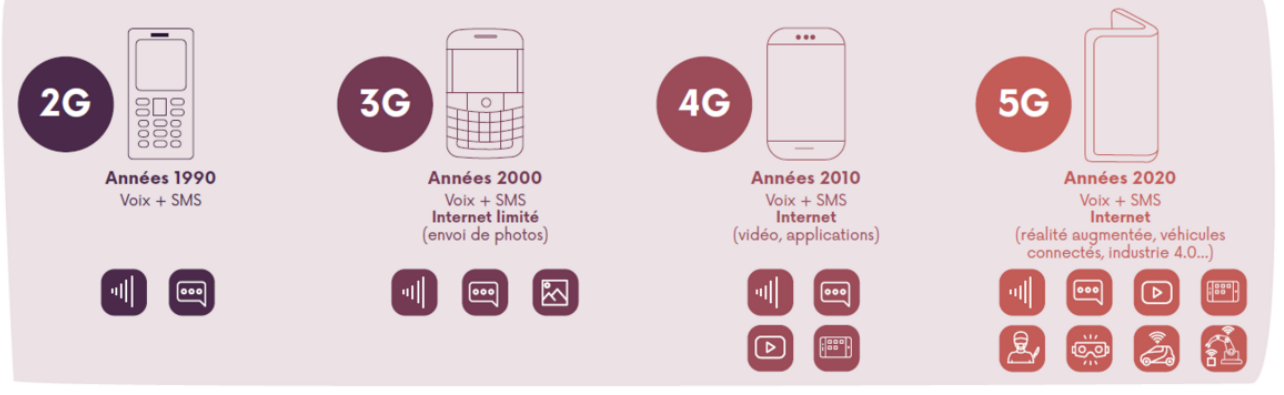
1. le signal passe par 4 bâtiments : 3 élevés et un bas, avec un espace ouvert mais pas de LOS ;
2. 14 bâtiments dont un groupe résidentiel ;
3. 6 bâtiments dont des bâtiments industriels ;
4. 14 bâtiments pour le plus long chemin avec des bâtiments résidentiels et industriels et un espace ouvert ;
5. 6 bâtiments industriels et pas d'espace ouvert.

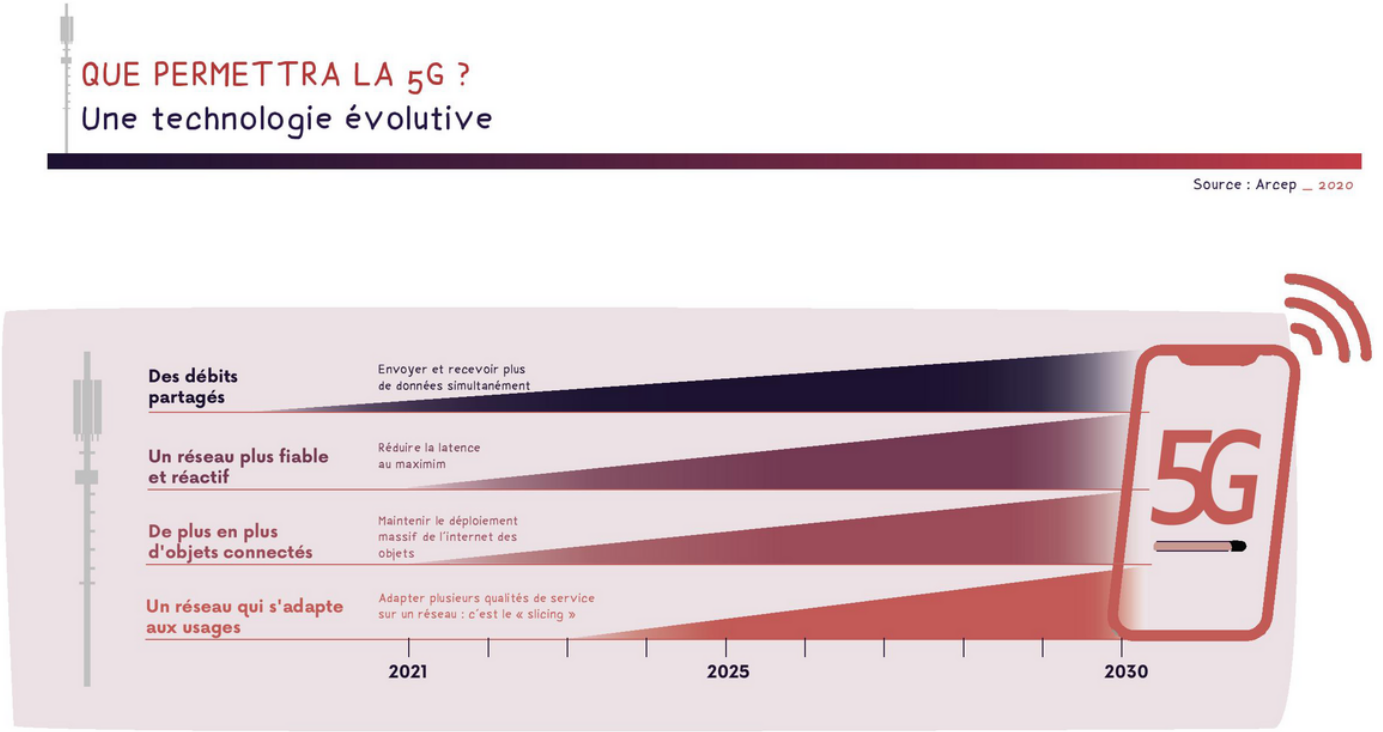
Point	Range (m)	Number of Buildings (signal going through)	Success (%)	Mean SNR (dB)	Mean RSSI (dBm)	Mean RSSI packet (dBm)	Margin (dB)
Point 1	830	4	96	-7.89	-112.95	-124.89	9,11
Point 2	960	14	92	-14.26	-111.26	-131.26	2,74
Point 3	1070	6	98	-3.22	-114.14	-120.24	13,76
Point 4	1530	14	98	-13.16	-112.24	-130.16	3,84
Point 5	863	6	100	-3.42	-113.48	-120.42	13,58

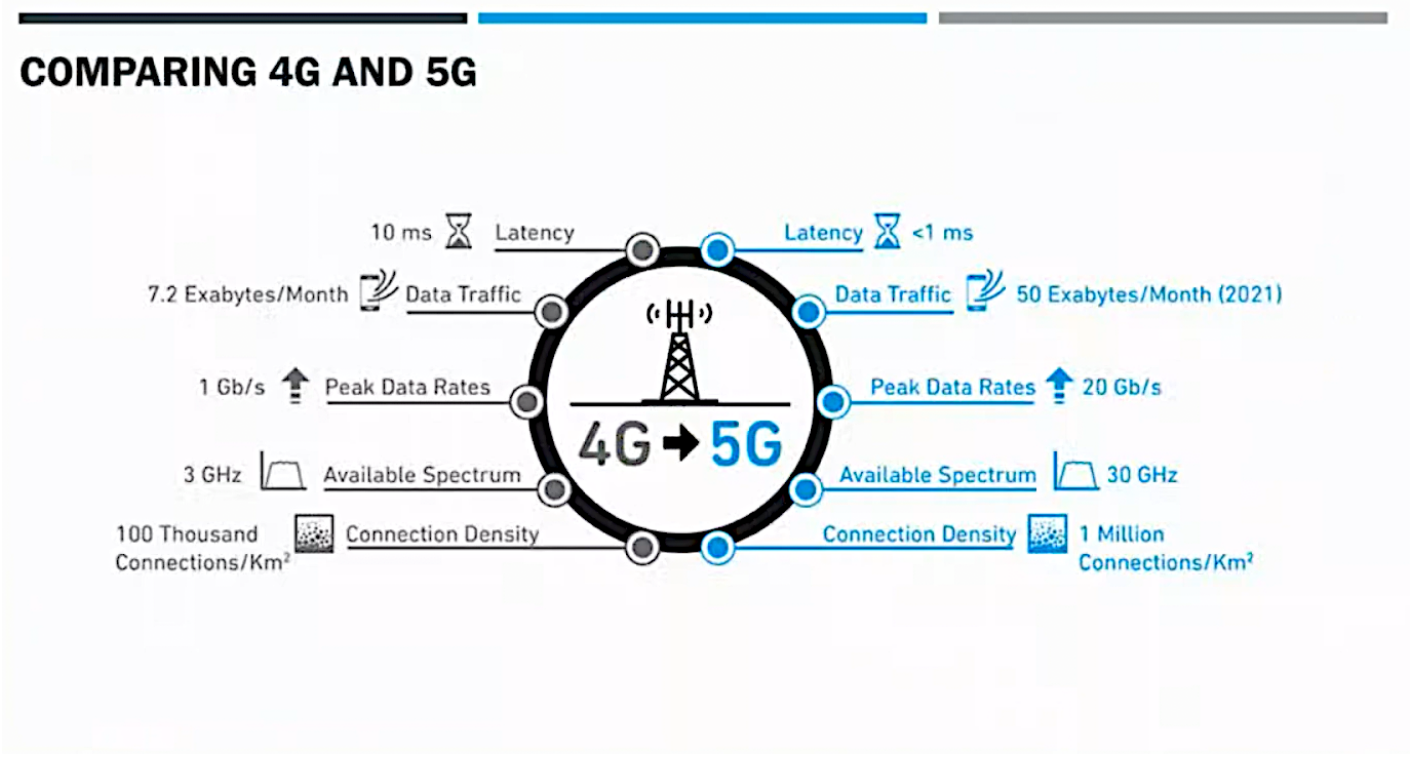
La 5G
Ou la technologie support de l'IoT

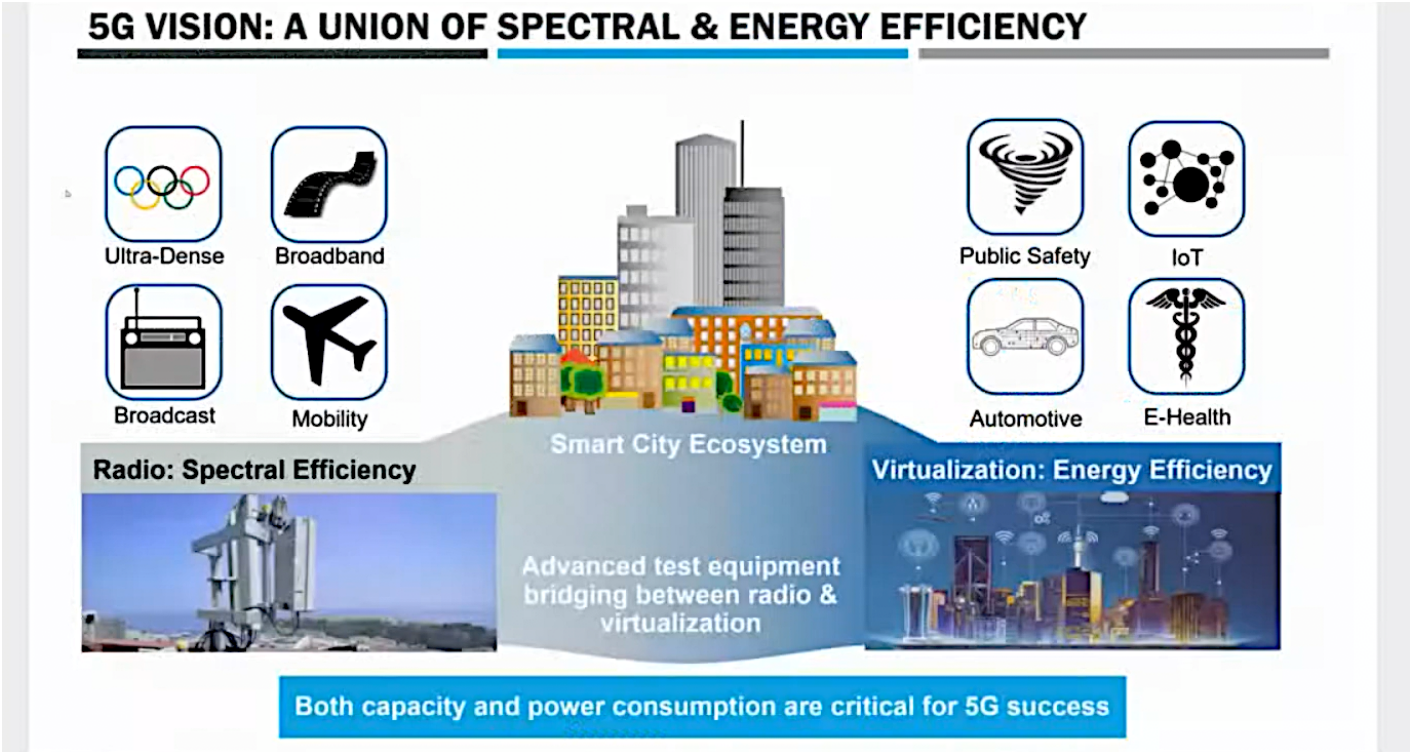

WIRELESS: A PLETHORA OF RADIO TECHNOLOGIES
LoRaWAN
Sigfox
Weigthless
Ingenu
Telensa
WAVIoT
ZigBee/Thread
WI-SUN(HAN)
Z-Wave
enocean
Endiio
802.11 ah
802.11 af
Bluetooth LE
ANT/ANT+
NFC
802.11 a/b/g/n/ac/ax
Bluetooth 5
ULE
wHart
ISA100
IQRF
ZigBee (NAN)
WI-SUN (FAN)
Wireless M-Bus
Dash7
802.16s
GPRS/EC-GSM
LTE-M
NB-IoT
5G (uRLLC, mMTC)
body
local area
neighbor area
wide area networks
Bluetooth
ANT
WiFi
ZigBee
THREAD
ULE
Z-WAVE
enocean
Wi-SUN Alliance
M-Bus
ISA100 Wireless
WirelessHART
endiio
IQRF
DASH7
wavIoT
INGENU
SIGHTLESS
sigfox
Telensa
NB-IoT
LoRaWAN
All product names, logos, and brands are property of their respective owners

Source : Arcep _ 2020



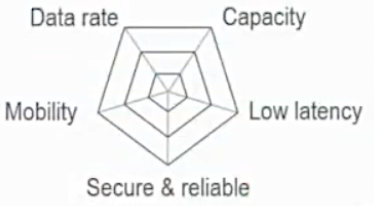

QUE PERMETTRA LA 5G ?
Une technologie évolutive
Source : Arcep _ 2020
Des débits partagés
Envoyer et recevoir plus de données simultanément
Un réseau plus fiable et réactif
Réduire la latence au maximim
De plus en plus d'objets connectés
Maintenir le déploiement massif de l'internet des objets
Un réseau qui s'adapte aux usages
Adapter plusieurs qualités de service sur un réseau : c'est le « slicing »
2021
2025
2030
5G

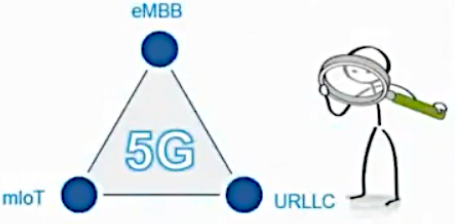

COMPARING 4G AND 5G
10 ms
Latency
7.2 Exabytes/Month
Data Traffic
1 Gb/s
Peak Data Rates
3 GHz
Available Spectrum
100 Thousand Connections/Km²
Connection Density
4G → 5G
Latency
<1 ms
Data Traffic
50 Exabytes/Month (2021)
Peak Data Rates
20 Gb/s
Available Spectrum
30 GHz
Connection Density
1 Million Connections/Km²

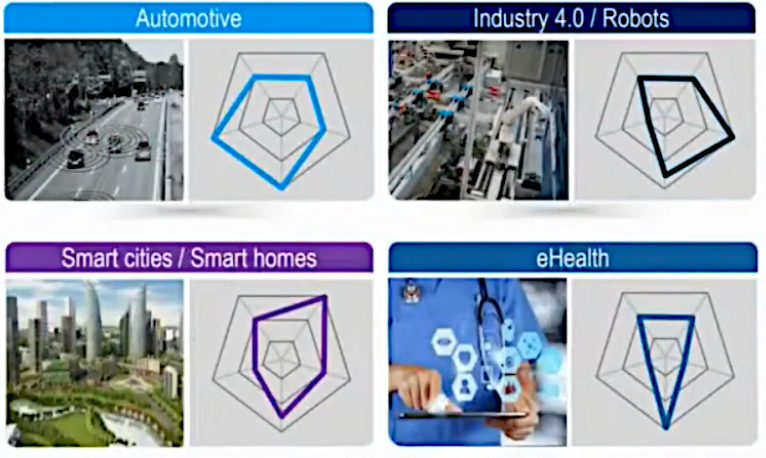

5G VISION: A UNION OF SPECTRAL & ENERGY EFFICIENCY
Ultra-Dense
Broadband
Broadcast
Mobility
Public Safety
IoT
Automotive
E-Health
Smart City Ecosystem
Radio: Spectral Efficiency
Virtualization: Energy Efficiency
Advanced test equipment bridging between radio & virtualization
Both capacity and power consumption are critical for 5G success

THE TRIANGLE OF 5G USE CASES

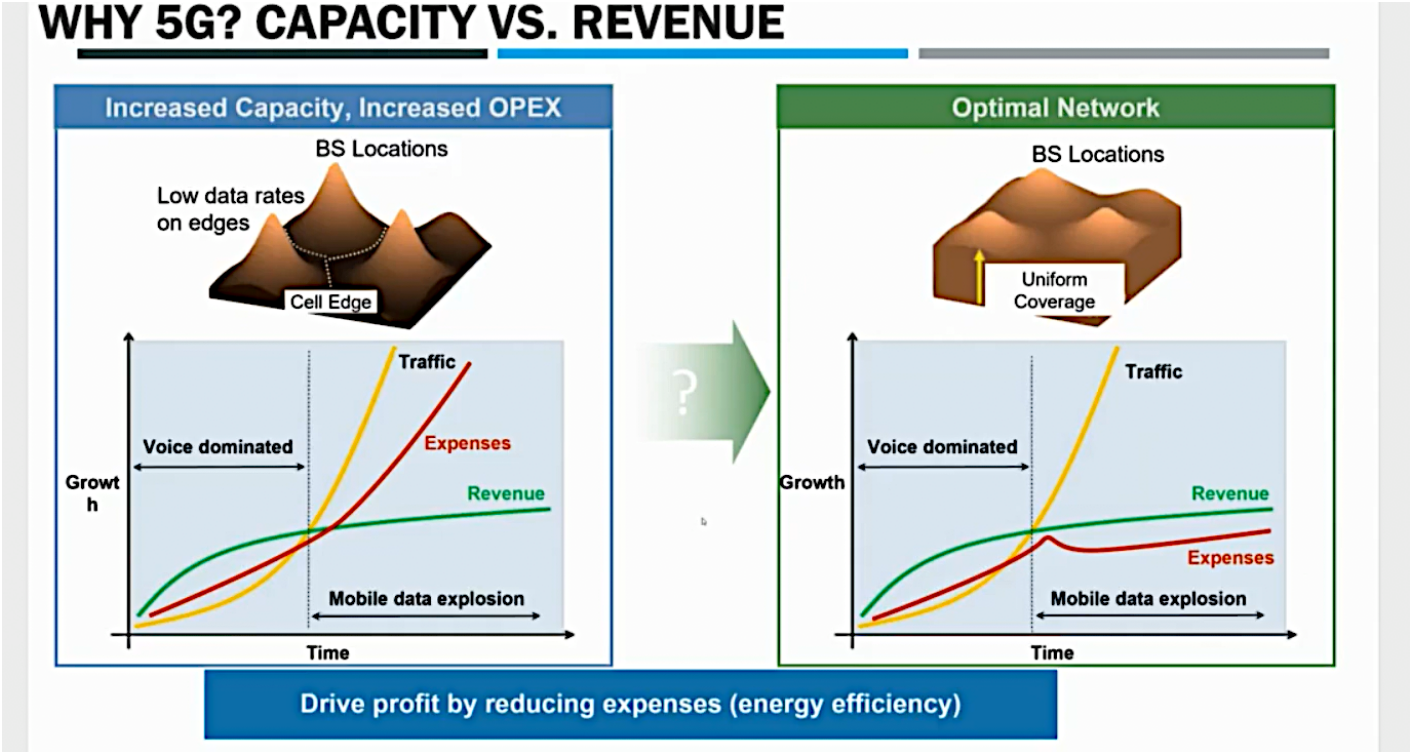
EMBB REMAINS PRIORITY 1, BUT URLLC OPENS NEW MARKETS!



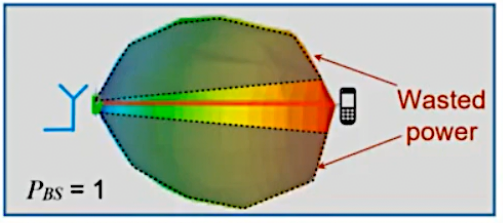


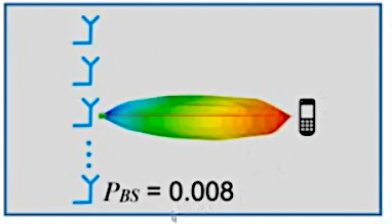


December 13, 2022


WHY 5G? CAPACITY VS. REVENUE
Increased Capacity, Increased OPEX
BS Locations
Low data rates on edges
Cell Edge
Growth
Traffic
Voice dominated
Expenses
Revenue
Mobile data explosion
Time
?
Optimal Network
BS Locations
Uniform Coverage
Growth
Traffic
Voice dominated
Revenue
Expenses
Mobile data explosion
Time
Drive profit by reducing expenses (energy efficiency)

ENERGY EFFICIENCY: WHY MASSIVE?



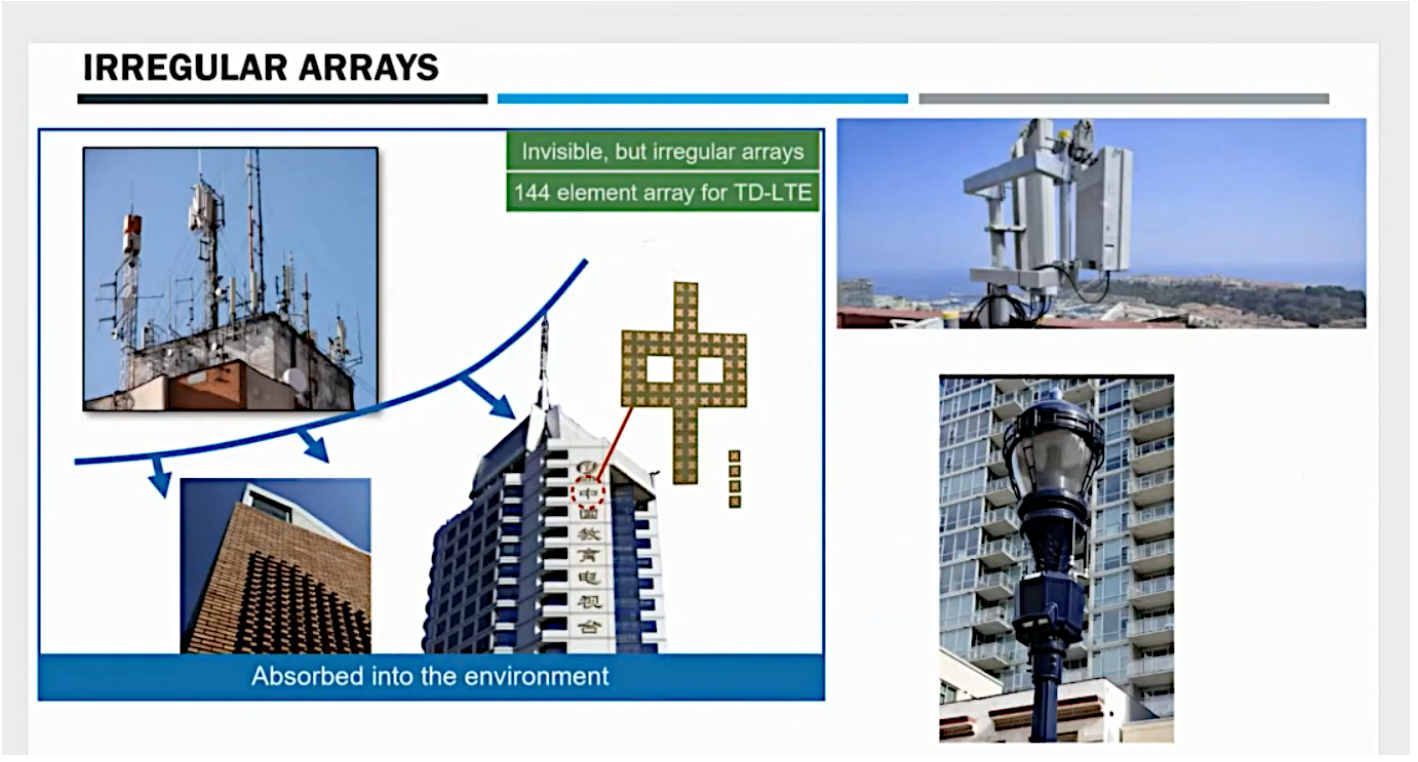


Number of Antennas = 1	
Number of BS transmit antennas (M_t)	1
Normalized output power of antennas	$P_{ant} = \frac{1}{M_t} = 1$
Normalized output power of base station	$P_{total} = \sum_{i=1}^{M_t} P_{ant}{}^{i} = 1$

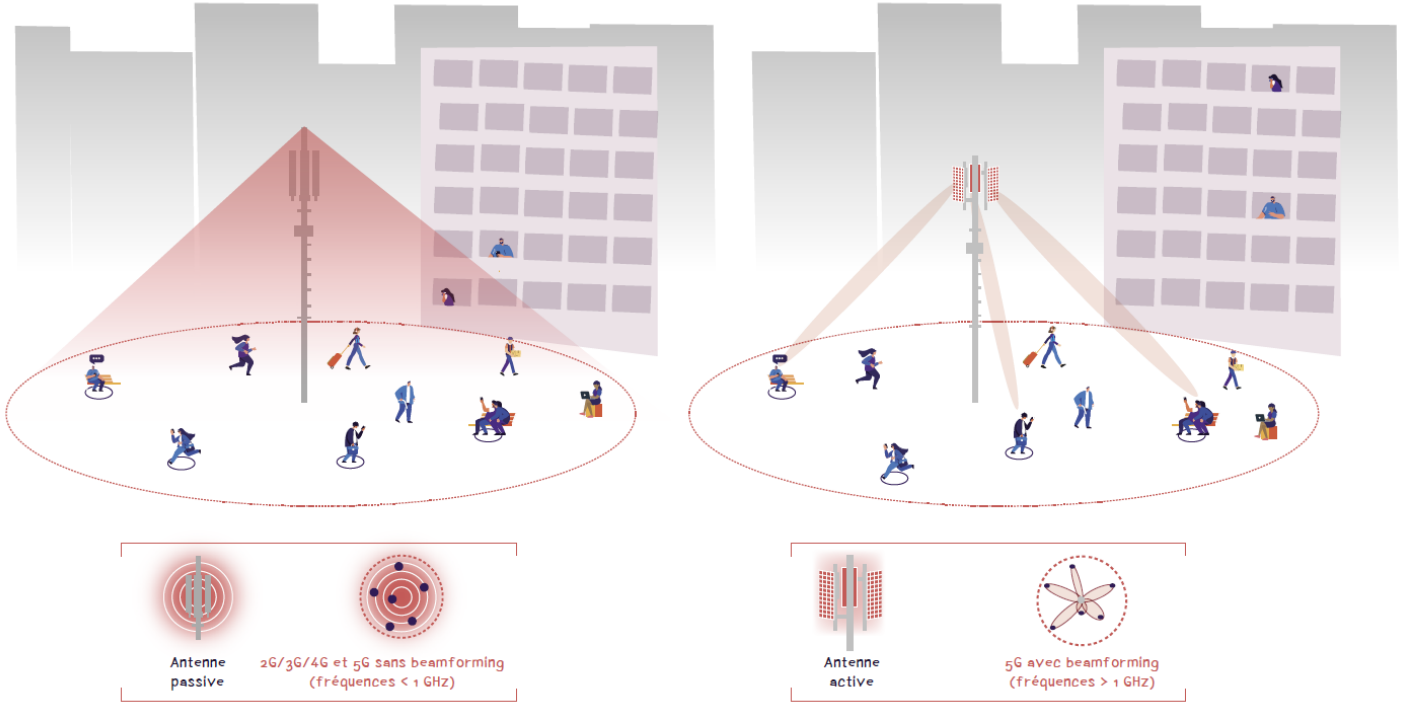
Number of UEs: 1 120 antennas per UE	
	120
	$P_{ant} = \frac{1}{M_t{}^2}$
	$P_{total} = \sum_{i=1}^{M_t} P_{ant}{}^{i} = 0.008$

Source: IEEE Signal Processing Magazine, Jan 2013

Improve energy efficiency: more antennas


IRREGULAR ARRAYS
Invisible, but irregular arrays
144 element array for TD-LTE
Absorbed into the environment

Antennes passive «*vs*» actives : le beamforming



Le «*beamforming*» permet de «*cibler*» un utilisateur :

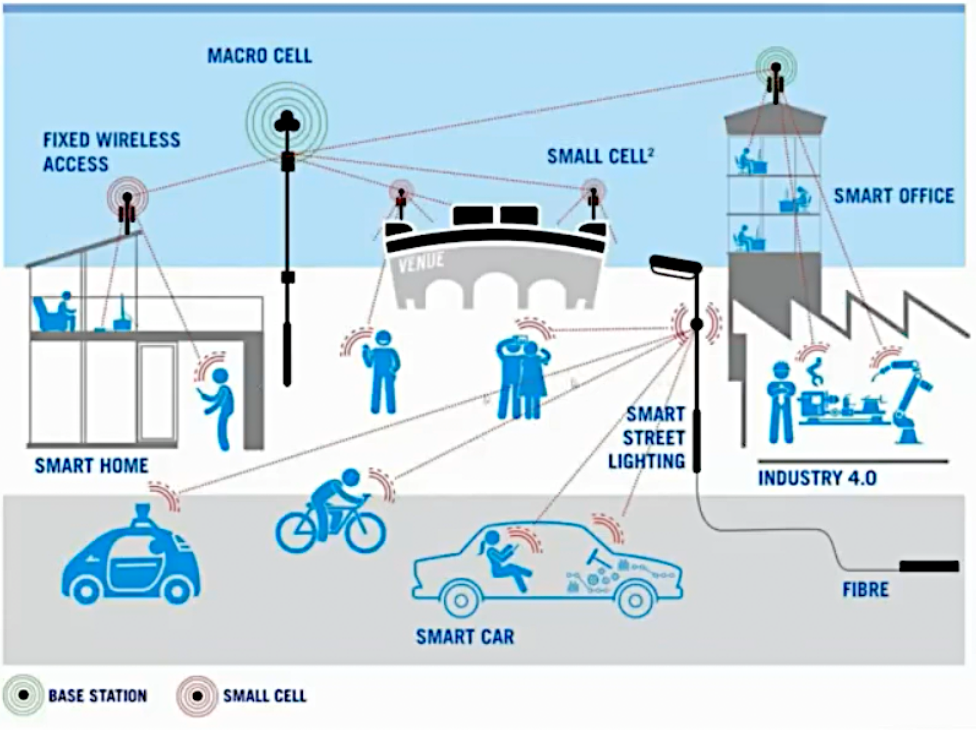
⟹ Plus de multiplexage spatial ;

⟹ Diminue le «*gâchis*» d'énergie diffusée.

STREET LANDSCAPE

Shorter range = more physical infrastructure.

FIGURE 1 (NOT TO SCALE)



5G ELECTROMAGNETIC FIELD MEASUREMENTS

Switzerland halts rollout of 5G over health concerns

The country's environment agency has called time on the use of all new towers

Sam Jones in Zurich FEBRUARY 12 2020

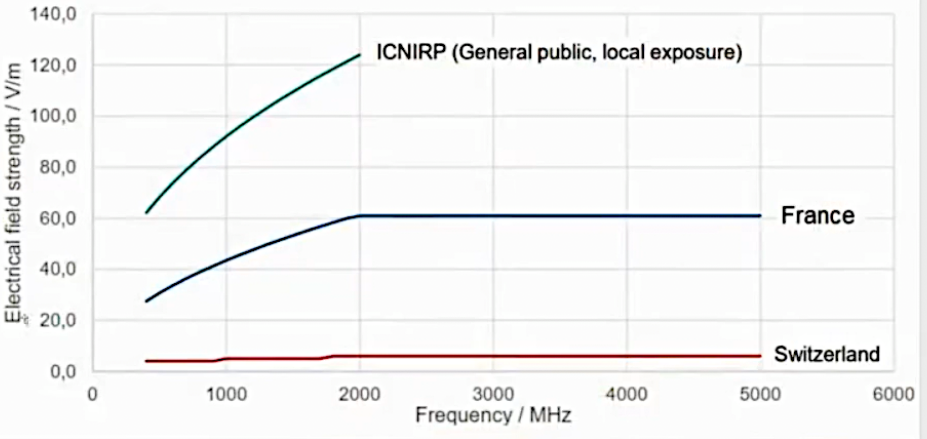
Reference:

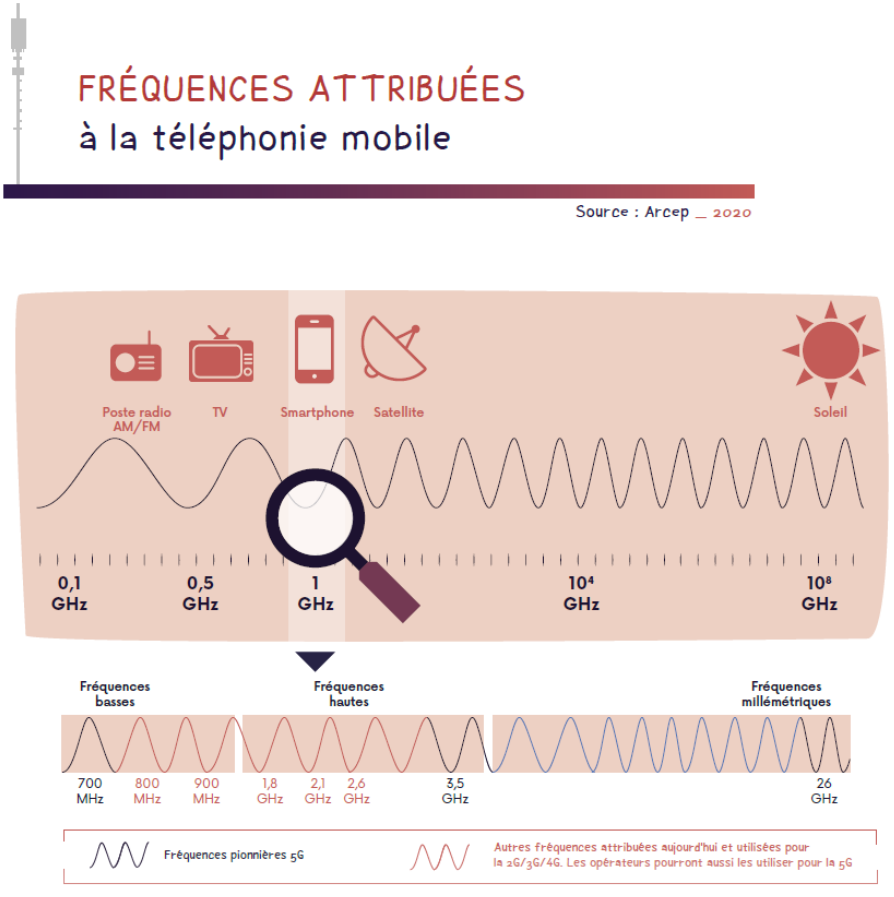
Guidelines for Limiting Exposure to Electromagnetic Fields (100 kHz to 300 GHz)

International Commission on Non-Ionizing Radiation Protection (ICNIRP)[1] **Author Information**

Health Physics: May 2020 - Volume 118 - Issue 5 - p 483-524
doi: 10.1097/HP.0000000000001210

► French regulation stricter than ICNIRP
► Swiss regulation much stricter than ICNIRP




FRÉQUENCES ATTRIBUÉES
à la téléphonie mobile
Source : Arcep _ 2020
Poste radio AM/FM
TV
Smartphone
Satellite
Soleil
0,1 GHz
0,5 GHz
1 GHz
10⁴ GHz
10⁸ GHz
Fréquences basses
Fréquences hautes
Fréquences millimétriques
700 MHz
800 MHz
900 MHz
1,8 GHz
2,1 GHz
2,6 GHz
3,5 GHz
26 GHz
Fréquences pionnières 5G
Autres fréquences attribuées aujourd'hui et utilisées pour la 2G/3G/4G. Les opérateurs pourront aussi les utiliser pour la 5G

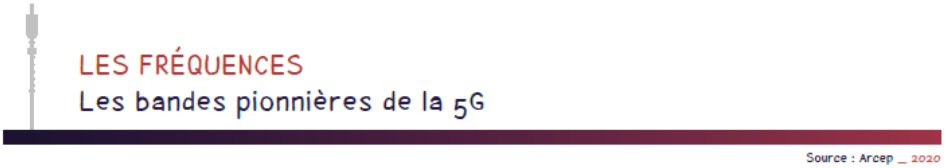
LES FRÉQUENCES

Les autres bandes attribuées aux opérateurs

Source : Arcep _ 2020

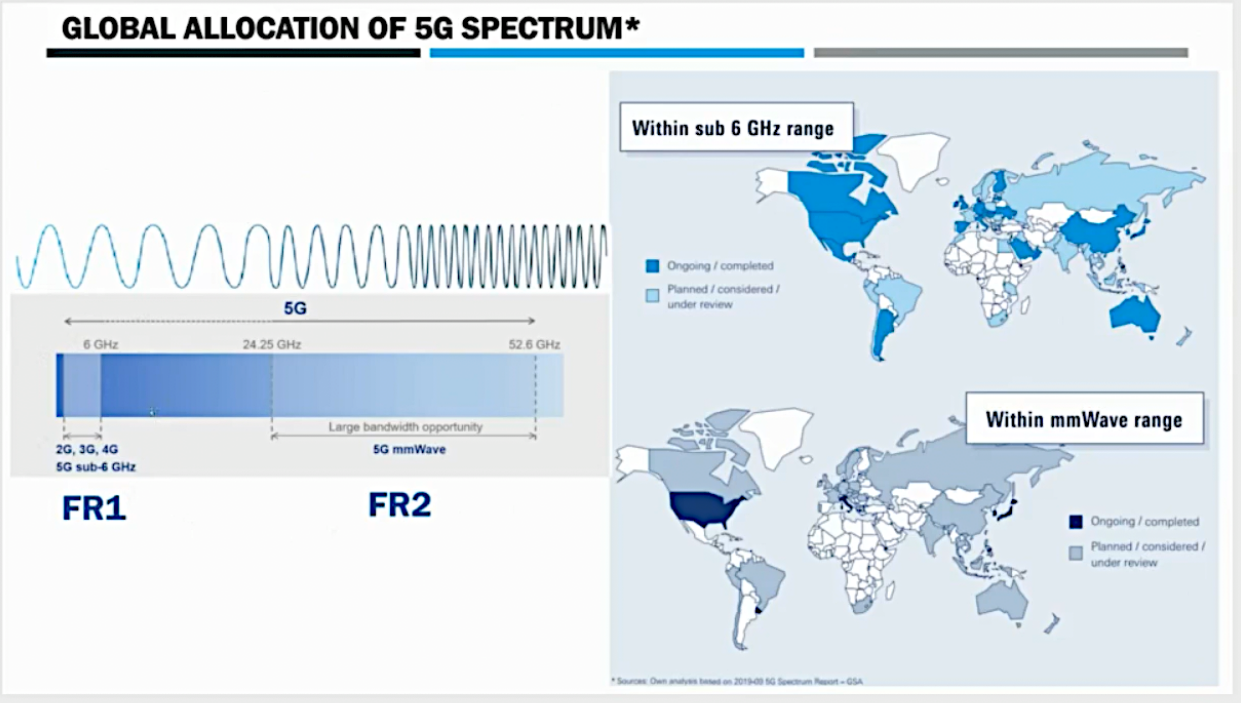
Fréquences	Date	Pénétration à l'intérieur	Portée	Débit maximum
800 MHz	Attribuée dès 2012	★★★★	★★★★	★
900 MHz	Attribuée dès 1986	★★★★	★★★★	★
1,8 GHz	Attribuée dès 1994	★★★	★★★	★★
2,1 GHz	Attribuée dès 2001	★★★	★★★	★★
2,6 GHz	Attribuée en 2012	★★	★★	★★

La 5G : les fréquences pionnières

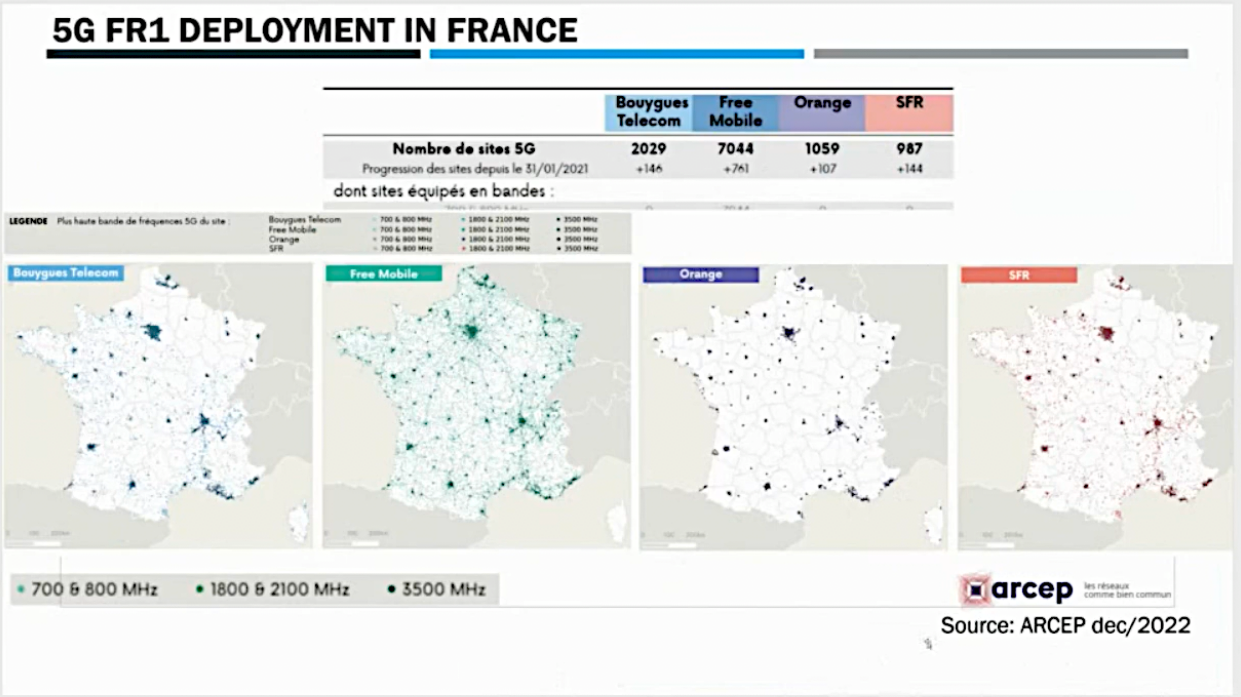


	Fréquences	Pénétration à l'intérieur	Portée	Débit
5G	700 MHz — Déjà attribuée aux opérateurs depuis 2015, elle est pleinement disponible depuis mi-2019	★★★★	★★★★	★
5G	3,5 GHz — En cours de réorganisation, elle offre un bon ratio couverture/débit et est souvent identifiée comme la bande "cœur 5G"	★★	★★★	★★★
5G	26 GHz — Jusqu'à présent utilisée pour les liaisons satellitaires ou d'infrastructures, elle permettra des débits très importants dans les cellules de petite taille	★	★	★★★★

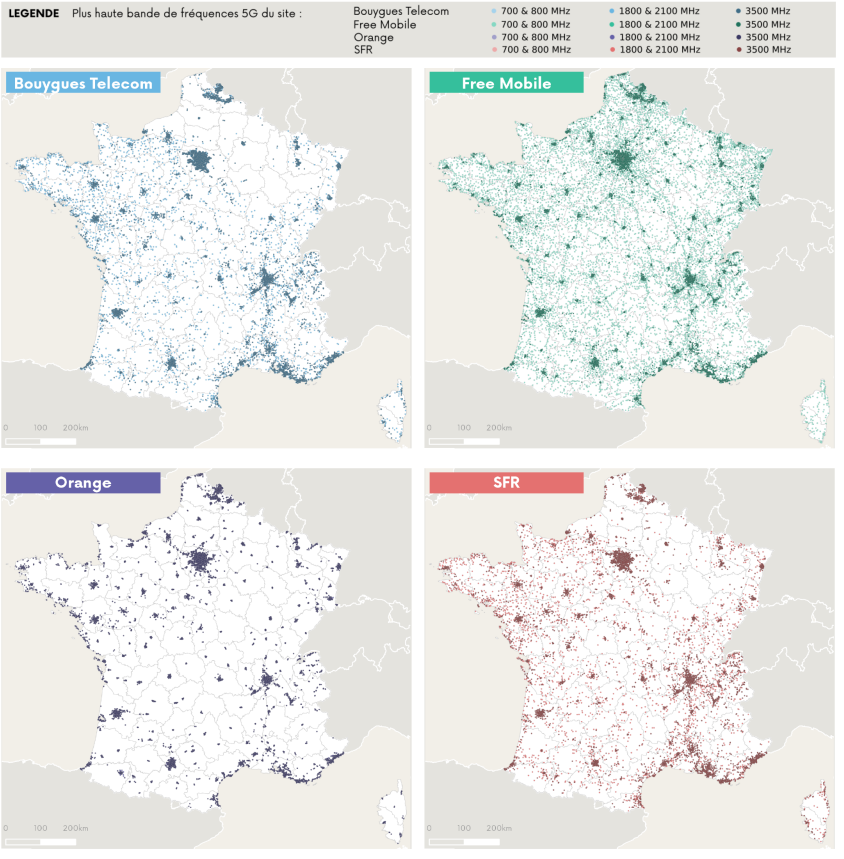
La 5G : allocation de nouvelles fréquences et récupération des anciennes



La 5G : les différents opérateurs français



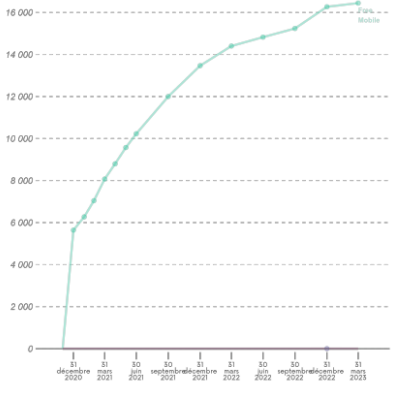
La 5G : les différents opérateurs



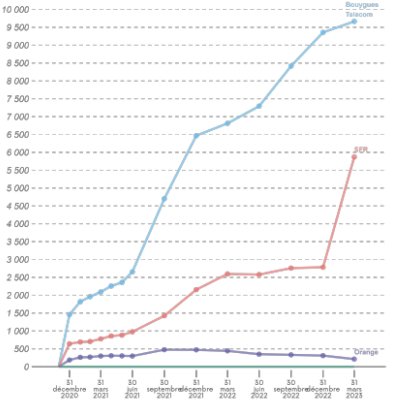
La 5G : les différents opérateurs

	Bouygues Telecom	Free Mobile	Orange	SFR
Nombre de sites 5G	**9 942**	**16 644**	**6 267**	**8 936**
Progression des sites depuis le **31/12/2022**	**+297**	**+288**	**+670**	**+532**
dont sites équipés en bandes :				
700 & 800 MHz	0	16 447	0	0
1800 & 2100 MHz	9 666	0	212	5 870
3500 MHz	**5 645**	**4 501**	**6 160**	**6 008**

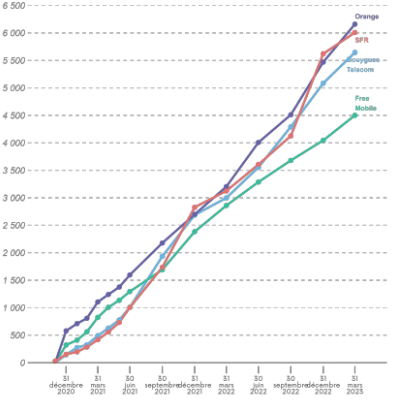
Bandes de tréquences basses :
700 & 800 MHz



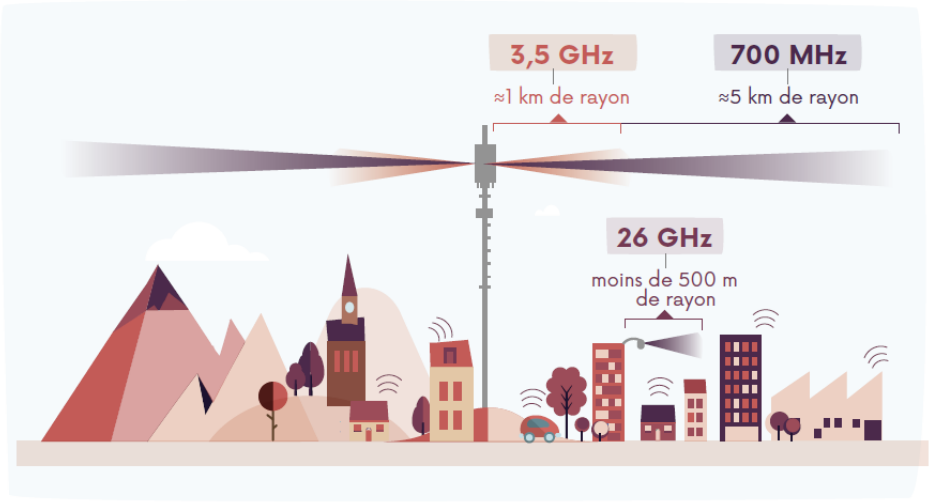
Bandes de tréquences moyennes :
1800 & 2100 Mhz

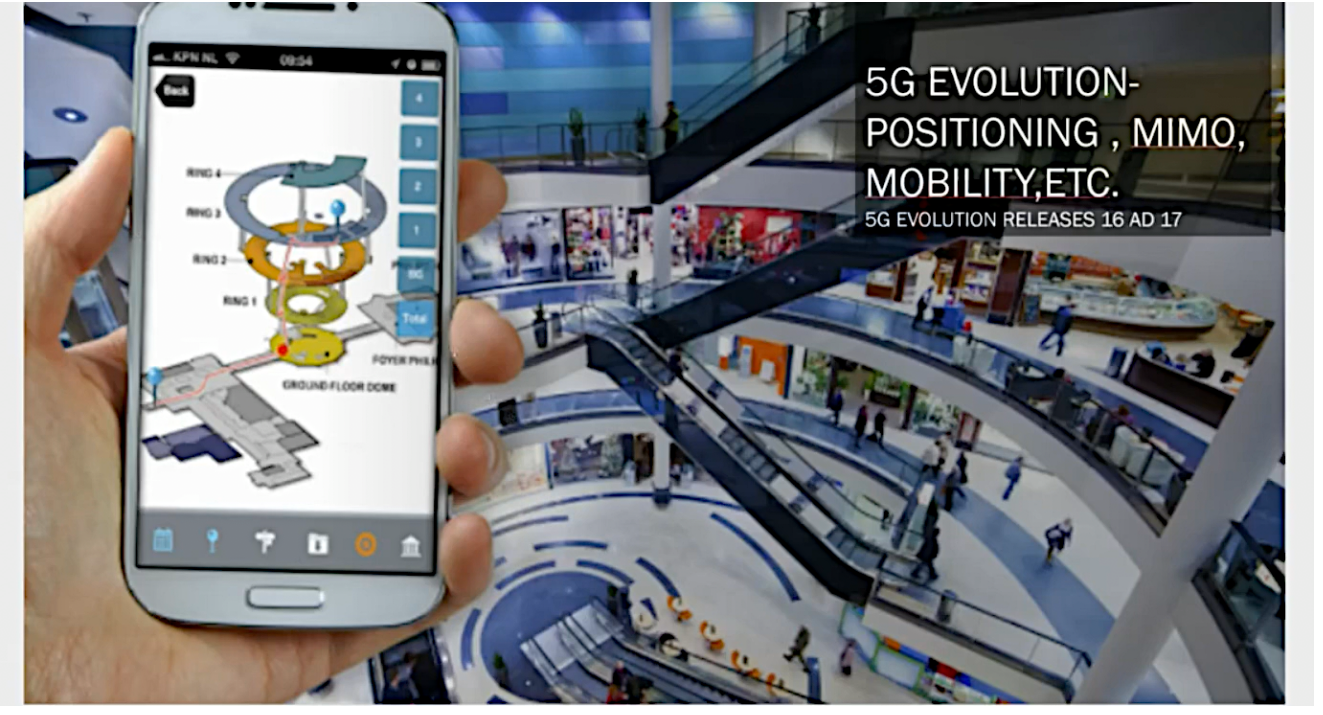


Bande de tréquences hautes :
3500 Mhz



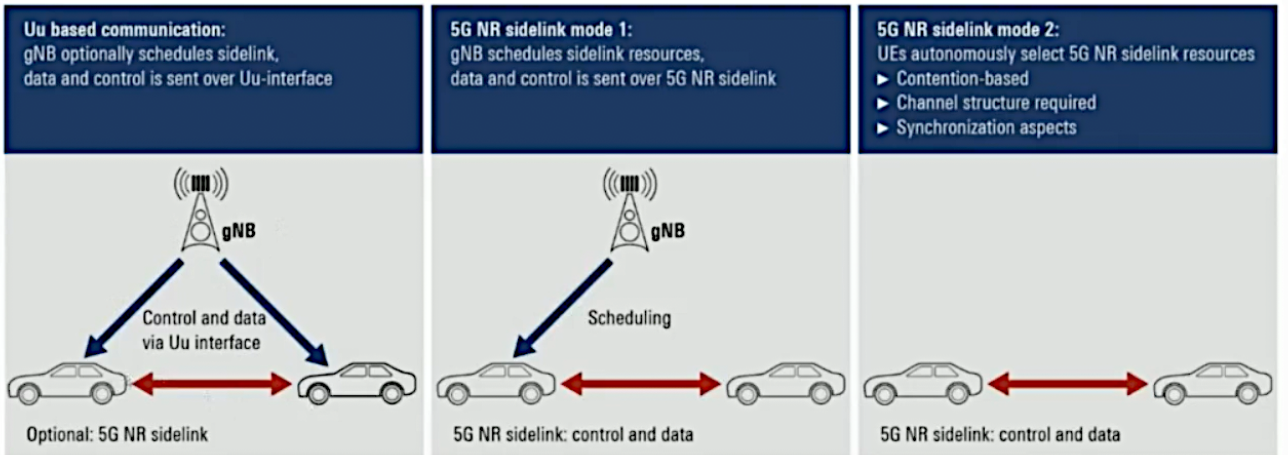

5G
la portée des 3 bandes
Source : Arcep _ 2020


3,5 GHz
≈1 km de rayon
700 MHz
≈5 km de rayon
26 GHz
moins de 500 m
de rayon


5G EVOLUTION-
POSITIONING , MIMO,
MOBILITY,ETC.
5G EVOLUTION RELEASES 16 AD 17


CONNECTING THE MOBILITY
WORLD WITH 5G-V2X
5GAA
Automotive Association
Ext. audio player
Do Not Turn
600ft
5G NR C-V2X
5G EVOLUTION RELEASES 16 AD 17
Fleet control tower
Fully autonomous,
electric truck
Remote
controllable
via 5G network
2.500 km apart

5G NR C-V2X COMMUNICATION MODES AT PHY LAYER

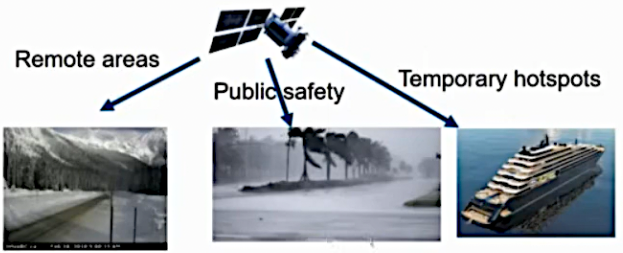


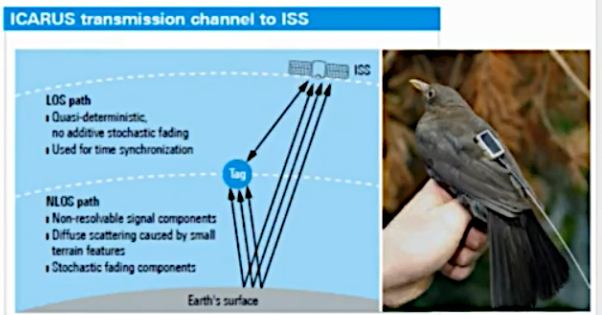

NON-TERRESTRIAL
NETWORKS
5G EVOLUTION, RELEASES 16 AND 17

NON TERRESTRIAL NETWORK APPLICATIONS

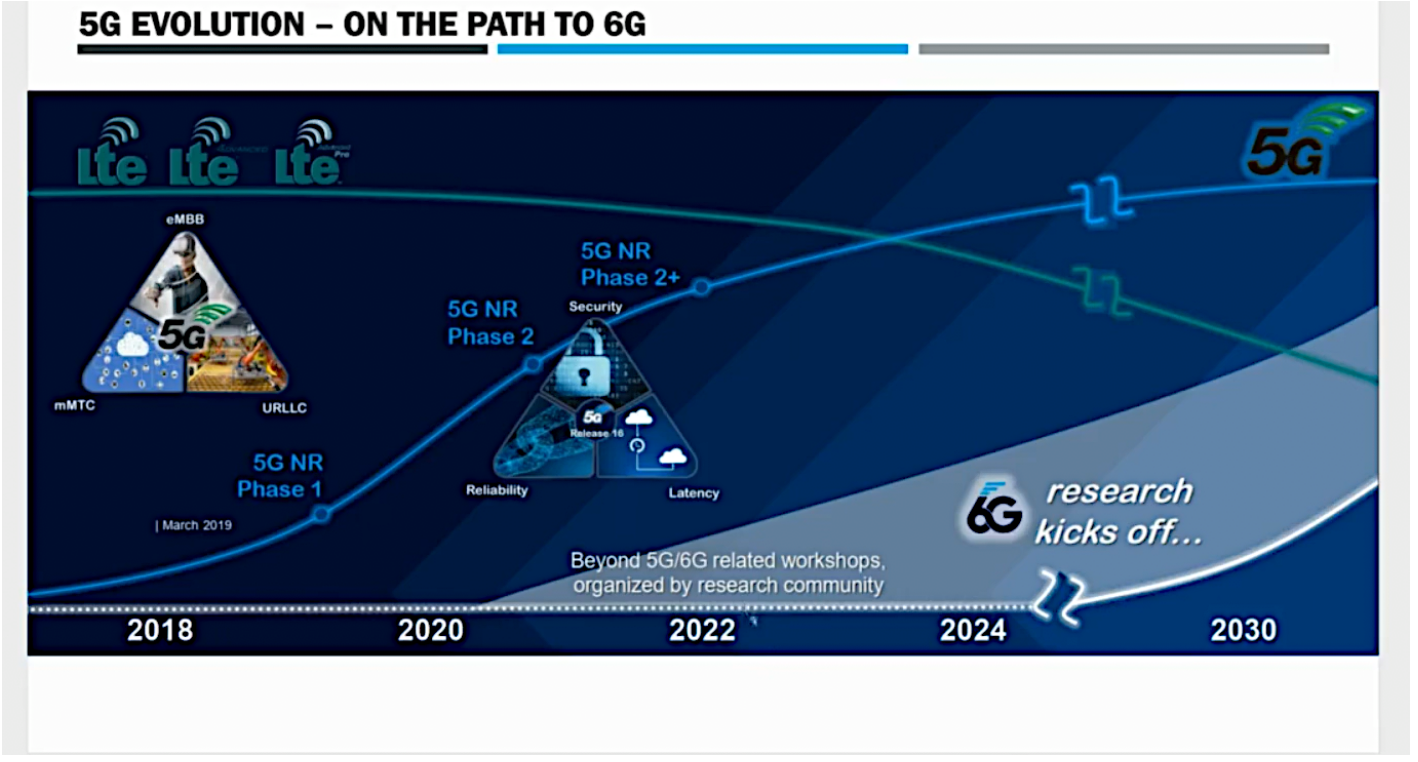
3GPP: NR over NTN
5G NR air interface adopted to NTN
GEO, LEO, HAPS -> air to ground
Fixed or moving terrestrial cells
UE support GNSS + NTN
Business case: human: eMBB

3GPP: IoT over NTN
NB-IoT & LTE-M adopted to NTN
GEO, LEO, HAPS -> air to ground
Business case: IoT
ICARUS: Internet of animals @400MHz






BEYOND 5G
5G EVOLUTION RELEASES 16 AD 17
6G


5G EVOLUTION – ON THE PATH TO 6G
Lte
Lte
Lte
5G
eMBB
5G
mMTC
URLLC
5G NR
Phase 1
| March 2019
5G NR
Phase 2
5G NR
Phase 2+
Security
5G
Release 16
Reliability
Latency
6G
research
kicks off…
Beyond 5G/6G related workshops,
organized by research community
2018
2020
2022
2024
2030

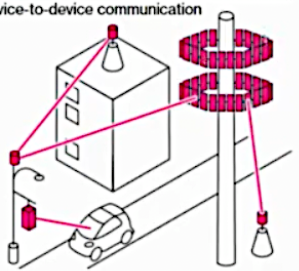
5G EVOLUTION – ON THE PATH TO 6G

5G

Signals, that were broadcast in all directions in 4G, are focused

Small base stations extend reach and handle some exchanges directly

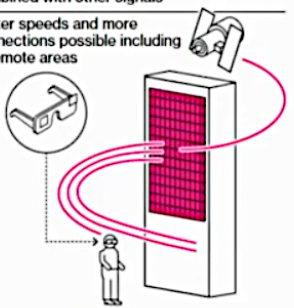
Device-to-device communication



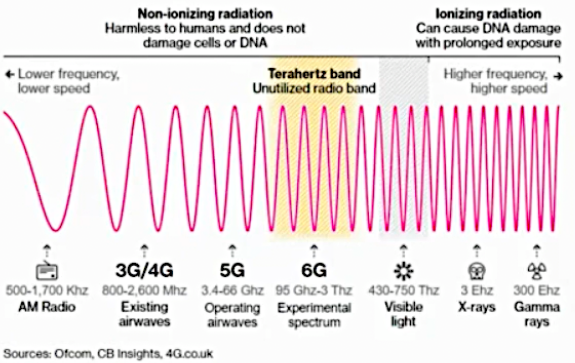
6G

Smaller signals could be reflected off intelligent surfaces, sharpened and combined with other signals

Faster speeds and more connections possible including in remote areas



Sources: Samsung, Institute of Electrical and Electronics Engineers



Sources: Ofcom, CB Insights, 4G.co.uk

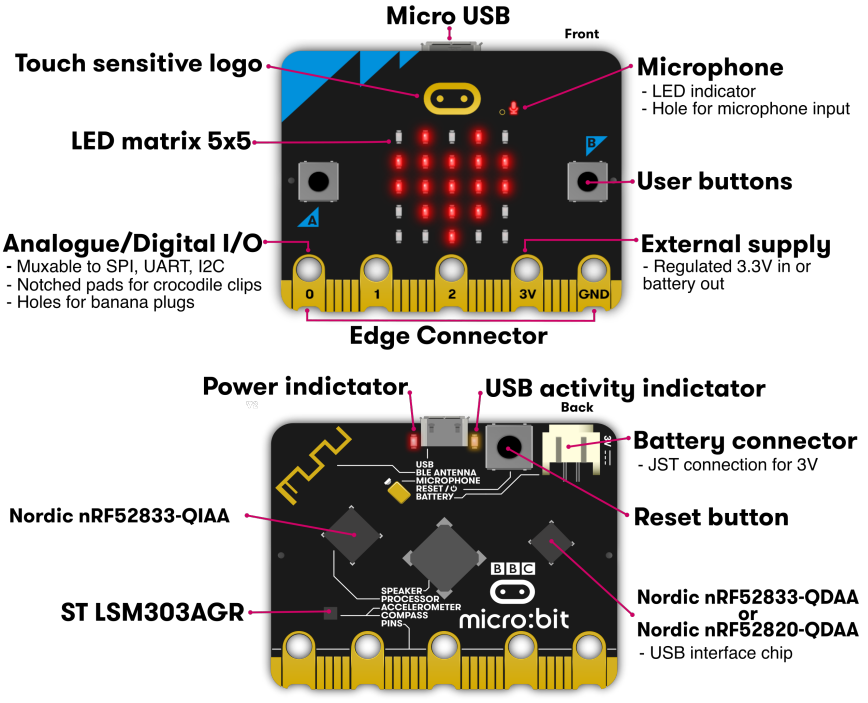
Network Innovation

Reflective surfaces may help transmit terahertz signals that don't travel very far

Experimental Band

Terahertz waves could meet 6G's speed, latency requirements

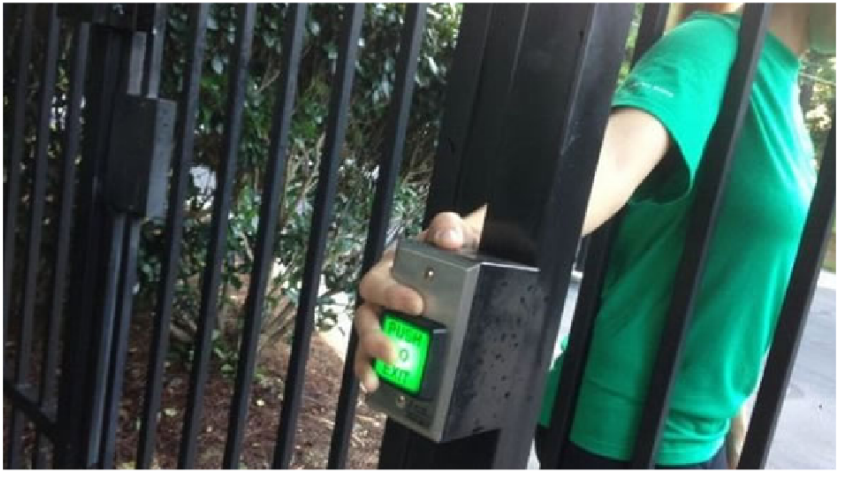
Micro:bit v2


Micro USB
Front
Touch sensitive logo
Microphone
- LED indicator
- Hole for microphone input
LED matrix 5x5
User buttons
Analogue/Digital I/O
- Muxable to SPI, UART, I2C
- Notched pads for crocodile clips
- Holes for banana plugs
External supply
- Regulated 3.3V in or battery out
0
1
2
3V
GND
Edge Connector
Power indictator
USB activity indictator
Back
Battery connector
- JST connection for 3V
USB
BLE ANTENNA
MICROPHONE
RESET / O
BATTERY
Nordic nRF52833-QIAA
Reset button
SPEAKER
PROCESSOR
ACCELEROMETER
COMPASS
PINS
ST LSM303AGR
Nordic nRF52833-QDAA
or
Nordic nRF52820-QDAA
- USB interface chip

Et la sécurité ?

La sécurité, parlons-en !

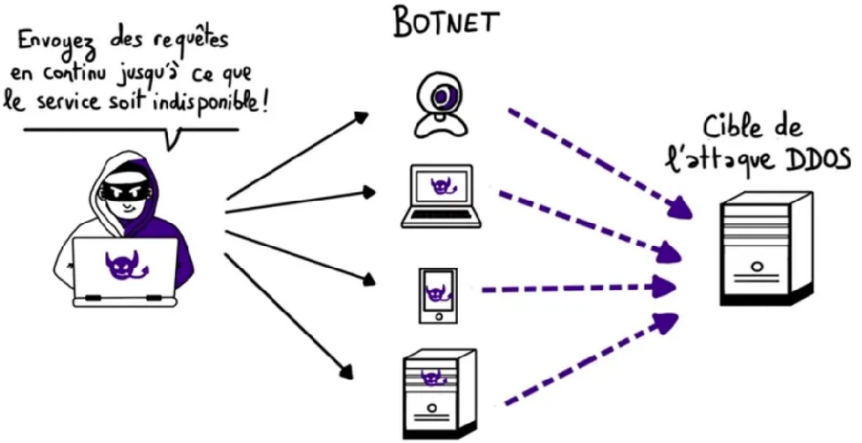
- *The "S" in "IoT" stands for "security"*



- **DISCLAIMER** : les vulnérabilités et menaces suivantes peuvent heurter la sensibilité des fabricants non avertis

Les vulnérabilités

- Systèmes informatiques (logiciel)
  - Attaques classiques sur un système/réseau
    - Déni de service
    - Écoute du réseau (sniffing)
    - Prise de contrôle à distance



Les vulnérabilités (suite)

- Systèmes électroniques ou mixtes
  - Mécanismes d'appairage trop "simples"
    - Bip pour portail, porte de garage
  - Mauvaise implémentation d'une solution
    - Contrôle d'accès et badgeuse MiFare
  - Mauvaise conception
    - Caméras IP low-cost [4]
  - Systèmes trop bavard
    - SSID Wi-Fi, mDNS
  - Absence et/ou déficience du chiffrement
    - Interception de données, injection de commandes

4. https://hitek.fr/actualite/un-moteur-de-recherche-pour-espionner-les-webcams-de-vos-voisines_8319

Les menaces et scénarii

- Surface d'attaque
  - Plusieurs protocoles de communication
    - Bluetooth, Wi-Fi, Z-wave
  - Nombre de composants
    - Isolé, réseau local, Cloud
  - Variété des composants
    - Microcontrôleurs, OS, capteurs, services web
  - Exemple
    - Détourner microphone intégré à un objet connecté afin d'écouter des conversations

Les menaces et scénarii (suite)

- Risques liés à un individu ou objet isolé
  - Exemple : serrures connectées Okidokeys
- Risques liés à une infrastructure
  - Compteurs Veolia, EDF Linky
    - Exemple : DDoS infrastructure de contrôle du trafic routier
- Risques business
  - Vol de données, usurpation, réputation
    - Exemple : simulation d'un clique Amazon Dash Button [6] (plusieurs commandes/individu : impact fort sur l'entreprise)

6. https://github.com/Nekmo/amazon-dash

La sécurité des objets domotiques courants

1. Déni de service "simple" : brouillage
2. Protection des communications
3. Prise de contrôle des objets domotiques
4. Les protocoles propriétaires
5. Les protocoles spécialisés
6. Les mauvaises configurations

Déni de service "simple" : brouillage

- Dispositif de brouillage tri-bande
  - Coût : ∼60€
  - Fréquences supportées : 433/868MHz, 2.4GHz
- Attaques possibles
  1. Empêcher envoi de données (flux caméra de surveillance)
  2. Bloquer réception d'ordres (fermeture porte, armement alarme)

Protection des communications

- Majorité d'objets communicant en clair
  - Système de PIN pour éviter les interférences
    - Et/ou gérer plusieurs objets
  - Pas de confidentialité/intégrité/authentification des données
  - Concerne majorité des objets low-cost
    - Interrupteurs, prises, thermostats
- Attaques possibles
  1. Récupération des données (présence ?)
  2. Rejeu/modification/injection de données
     - Arrêt interrupteur, ouverture porte
  3. Prise de contrôle des objets

Les protocoles propriétaire

- Utilisés par certains objets domotiques
  - Station météo, sonnette sans fil, thermostat connecté
- Sécurité... par l'obscurité !
  - Utilisation de plage de fréquences non classique
  - Encodage des trames non documenté
  - Exemple : projet `cc1101-X2D6-Heaters`[8] permettant de contrôler les thermostats X2D

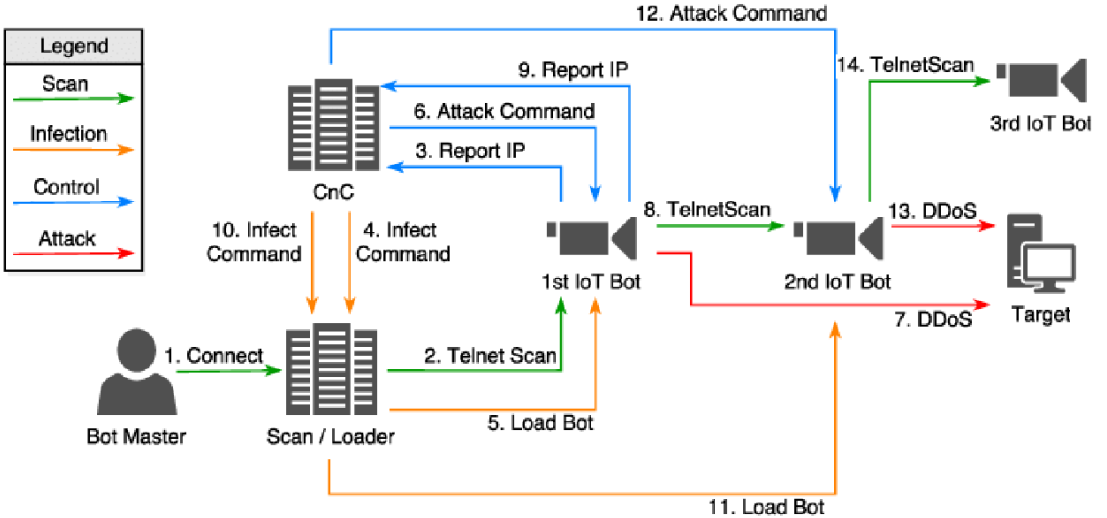
8. `https://github.com/SixK/CC1101-X2D-Heaters`

Les mauvaises configurations

- Configuration par défaut
  - Possibilité d'accès à distance via identifiants connus...
    - ...et parfois non modifiables
  - Exposition d'objets sur Internet (caméra)
  - Exposition de services non documentés (Telnet)
  - Fonctionnalités de sécurité désactivées

Les mauvaises configurations (suite)

- Le meilleur exemple : le botnet *Mirai*
  - 30 000 passerelles AirLink compromises
    - Login/mot de passe par défaut
  - Infection des objets connectés puis intégration au botnet
  - Potentiellement +1 million d'objets infectés
  - DDoS réalisé avec 100 000 bots



1 Mars 2021, faille de sécurité Verkada : $2,95 millions d'amende

Un collectif de hackers a obtenu un accès administrateur complet au système de vidéosurveillance Verkada en utilisant des identifiants « super-user » publiés publiquement sur Internet.

Conséquences principales

- Accès instantané à **150 000 caméras** en direct et archivées
- Visualisation de flux sensibles dans :
  - ◇ hôpitaux
  - ◇ prisons
  - ◇ écoles
  - ◇ entreprises (dont Tesla)

Cause

- ▷ **Identifiants administrateurs** exposés publiquement
- ▷ **Absence de protection renforcée** (ex. : 2FA, liste blanche IP, rotation des mots de passe) sur ces comptes privilégiés

Points clés

- □ Utilisation d'un compte « super admin » trouvé en clair sur le web
- □ Aucun mécanisme de sécurité supplémentaire pour les accès les plus critiques
- □ **Exposition massive de données sensibles** sans authentification forte requise

Recommandations relatives à la sécurité des objets connectés

---

https://www.ssi.gouv.fr/guide/recommandations-relatives-a-la-securite-des-systemes-dobjets-connectes

Recommandations relatives à la sécurité des objets connectés (suite)

1. Se renseigner avant achat sur l'objet connecté
   - Interactions avec les autres appareils électroniques
   - Données collectées lors de l'utilisation
   - Présence de failles de sécurité connues
2. Modifier les mots de passes par défaut
   - Généralement trop faibles
     - Peu de caractères, faciles à deviner, publiquement connus
   - Utiliser un mot de passe long et complexe
3. Mettre à jour ses objets connectés et applications associées
   - Patcher les failles de sécurité
   - Configurer l'installation automatique des mises à jour (si possible)

Recommandations relatives à la sécurité des objets connectés (suite)

4. Protéger ses informations personnelles
   - Communiquer le minimum d'informations nécessaires
     - Date de naissance aléatoire, âge approximatif
   - Utiliser des pseudonymes au lieu des noms et prénoms
   - Se créer une adresse de messagerie spécifique (si possible)
   - 52% des objets connectés présentent un risque pour vos données personnelles [11]
5. Vérifier paramètres de sécurité de ses objets connectés et de leurs applications
   - Exemple : désactiver le partage des données sur les réseaux sociaux

---

11. https://www.maison-et-domotique.com/67986-infographie-logements-connectes-francais-rapport-tendu

Recommandations relatives à la sécurité des objets connectés (suite)

6. Éteindre ses objets connectés hors des plages d'utilisation
   - Réduction des risques de piratage, de vol de données ou d'intrusion malveillante
7. Mettre à jour les appareils raccordés à vos objets connectés
   - Se prémunir des mouvements latéraux (pivoting réseau)
   - Mettre à jour box Internet également
8. Sécuriser sa connexion Wi-Fi
   - Utiliser un mot de passe robuste [12]
   - Vérifier que connexion Wi-Fi utilise la méthode de chiffrement la plus sûre

12. `https://www.security.org/how-secure-is-my-password`

Recommandations relatives à la sécurité des objets connectés (suite)

9. Limiter l'accès de ses objets connectés aux autres appareils électroniques ou informatiques
   - N'autorisez l'appairage de ses objets connectés qu'aux seuls appareils nécessaires aux fonctionnalités souhaitées
   - Utiliser ses objets connectés sur un réseau distinct (si possible)
     - VPN, VLAN
10. Supprimer ses données + réinitialiser l'objet lorsque vous ne vous en servez plus
    - Effacer vos données sur l'objet connecté
    - Supprimer le compte en ligne auquel l'objet peut être associé
    - Réinitialiser l'objet dans ses paramètres par défaut (si possible)
      - Configuration usine