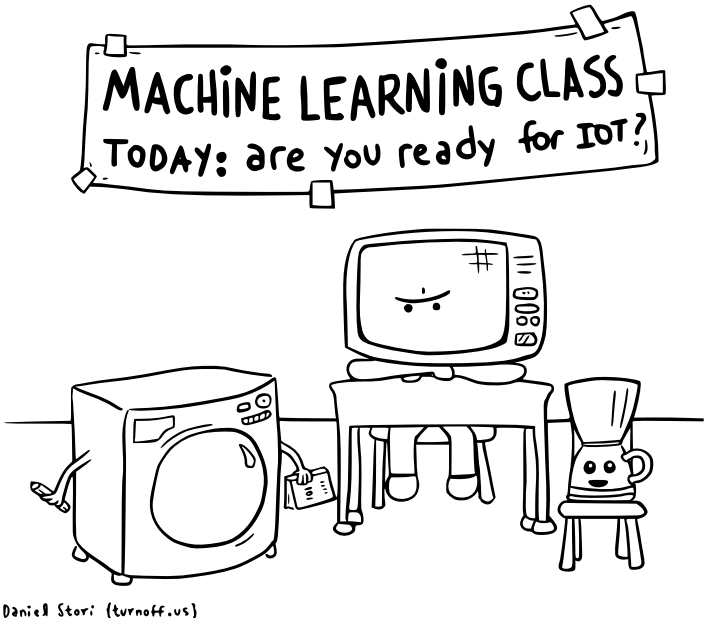
IAE LIMOGES
École Universitaire
de Management

Licence 3ème année



Internet des Objets — P-F. Bonnefoi

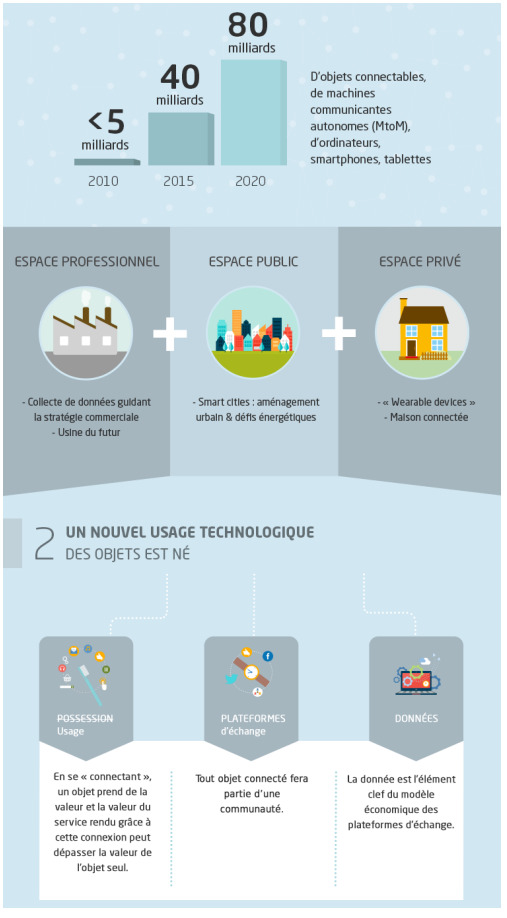
Version du 25 novembre 2024

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



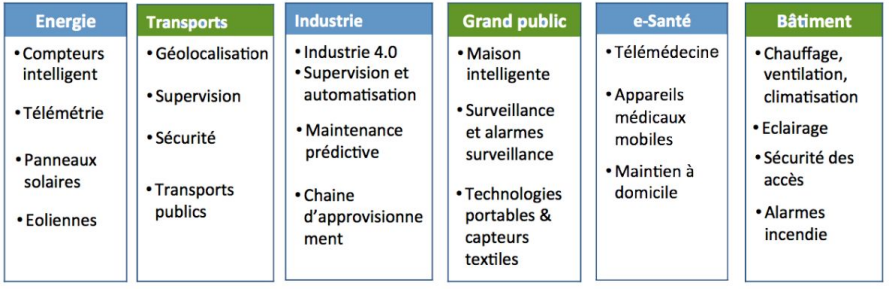
Défintions

- 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*»

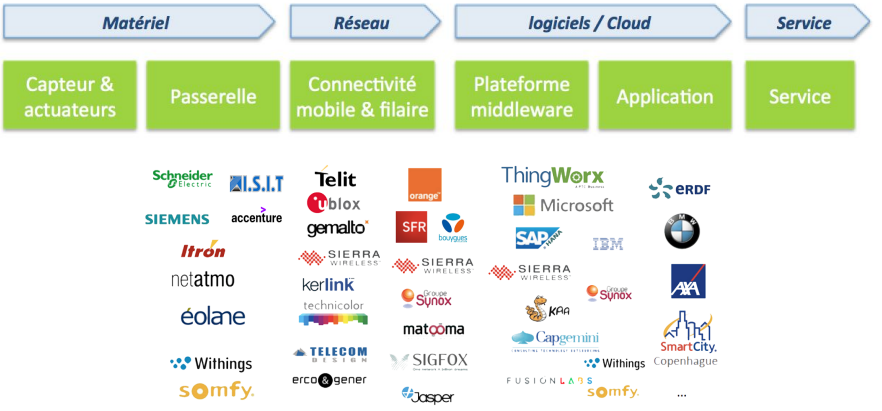
- opposition en IoT et M2M :
  - IoT : objets de technologies très variées connectés à du Cloud par Internet ;
  - M2M : machines connectées entre elles ou par un réseau WiFi ou cellulaire à un système centralisé propriétaire et privé.

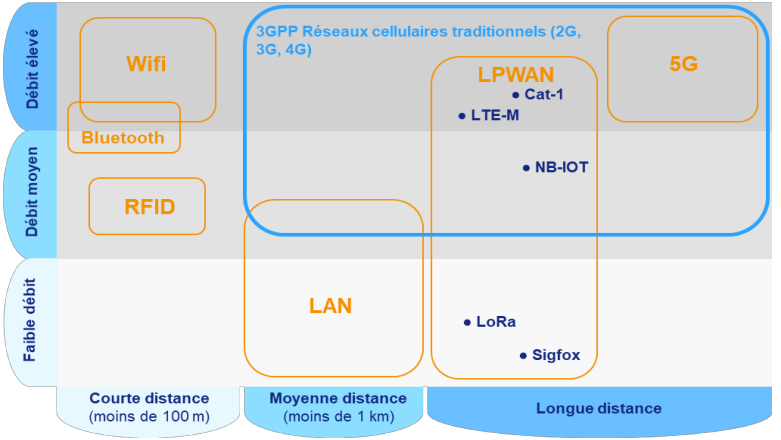
Les domaines

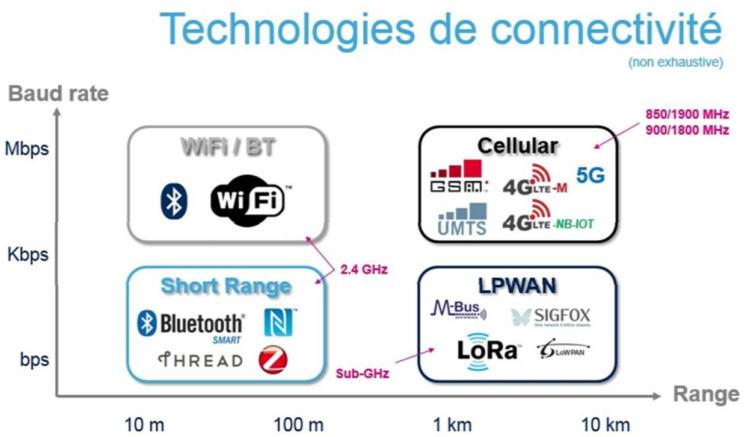
- Énergie,
- Transports,
- Industrie (machines industrielles, logistique...) industrie 4.0,
- Maison connectée (domotique...),
- Loisirs,
- Bâtiment connecté (tertiaire),
- Santé et bien-être,
- Commerce et distribution,
- Ville intelligente (Smart City).



Les principaux acteurs

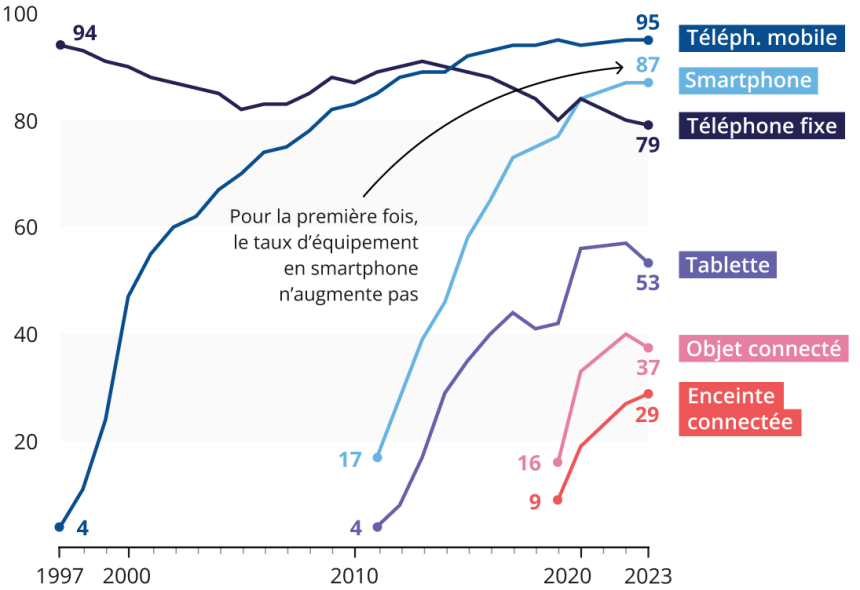



Débit élevé
Débit moyen
Faible débit
Wifi
Bluetooth
RFID
3GPP Réseaux cellulaires traditionnels (2G, 3G, 4G)
LPWAN
• Cat-1
• LTE-M
• NB-IOT
5G
LAN
• LoRa
• Sigfox
Courte distance (moins de 100 m)
Moyenne distance (moins de 1 km)
Longue distance


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 (%)



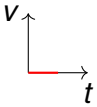
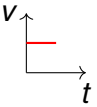
Plan de l'intervention

- Transmission de l'information :
  - comprendre la transmission radio : portée radio, débit et multiplexage ;
  - calcul du «*bilan de liaison*» ;
  - application à une communication à longue distance et faible consommation : le LoRa ;
- La 5G : technologie clé pour l'essort de l'IoT :
  - le «*beamforming*» pour augmenter la densité des réseaux ;
  - utilisation de nouvelles bandes de fréquences ;
  - des nouveaux usages : positionnement et couverture étendue ;
- les risques sur l'IoT :
  - récupération des données sur un IoT : recherche d'accès bas niveau, accès direct au contenu de la mémoire ;
  - exploitation du Bluetooth Low Energie ;
  - la sécurité et préconisations ;

Transmission de l’Information

Qu'est-ce qu'un bit, «*binary digit*» ?

Un **bit** représente un système à **deux états** possibles :

- «*allumé*»,  ou «*éteint*»,  ;
- «*allumé*», (I) ou «*éteint*», (O), d'où le symbole présent sur les interrupteurs poussoir :  ou 
- «*Vrai*» ou «*Faux*» ;
- un **voltage** «*bas*»  ou un voltage «*haut*»  (où «*v*» est le voltage et «*t*» le temps) ;
- une **magnétisation** de sens nord-sud N|S ou de sens sud-nord S|N sur un support magnétique ;
- la **valeur** «*1*» ou la valeur «*0*».

Qu'est-ce qu'un bit de mémoire dans un ordinateur ?

«*Un bit est juste un emplacement de stockage d'électricité :*

- ▷ *s'il n'y a pas de charge électrique alors le bit est 0 ;*
- ▷ *s'il y a une charge électrique alors le bit est 1*

La seule chose que l'ordinateur peut mémoriser est si le bit est à 1 ou 0.»

Chaque bit de mémoire correspond à une case dans laquelle on peut stocker un bit de données, soit la valeur 1, soit la valeur 0.

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.

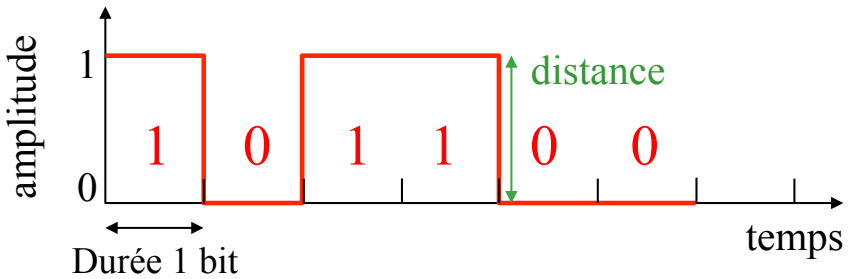
Un signal est une quantité mesurable variant au cours du temps ou dans l'espace.

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*.

Transmission Synchrone *vs* Asynchrone : le synchrone

Transmission série sur un seul fil pour une liaison synchrone

- *émetteur*, E, et *récepteur*, R, utilisent une **même base de temps** pour émettre les bits (horloge) ;
- il sont **cadencés** suivant la même horloge ;
- à chaque «top d'horloge», un bit est envoyé et R sait donc «quand» récupérer ce bit.

Le récepteur reçoit de façon continue les informations au rythme auquel l'émetteur les envoie.

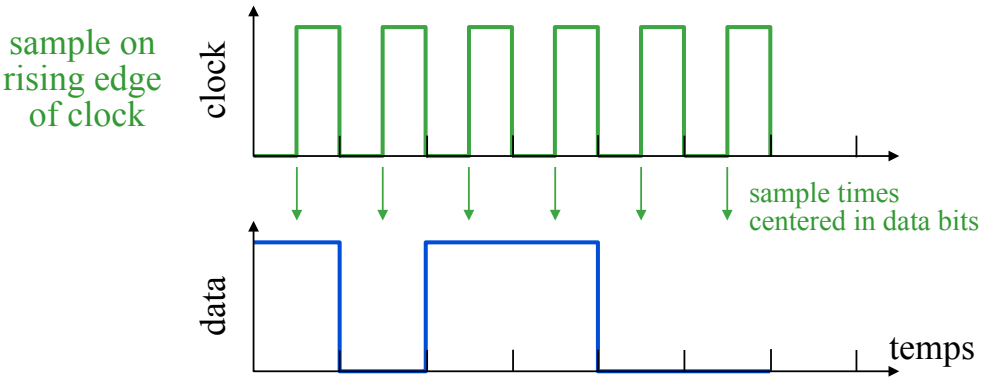
Inconvénient :

▷ la reconnaissance des informations au niveau du récepteur : il peut exister des différences entre les horloges de l'émetteur et du récepteur.

C'est pourquoi chaque envoi de bit doit se faire **sur une durée assez longue** pour que le récepteur la distingue.

Ainsi, la vitesse de transmission **ne peut pas être très élevée** *dans une liaison synchrone sans recourir à du matériel coûteux.*

Transmission série sur deux fils pour une liaison synchrone



Codage en «bande de base» et codage numérique

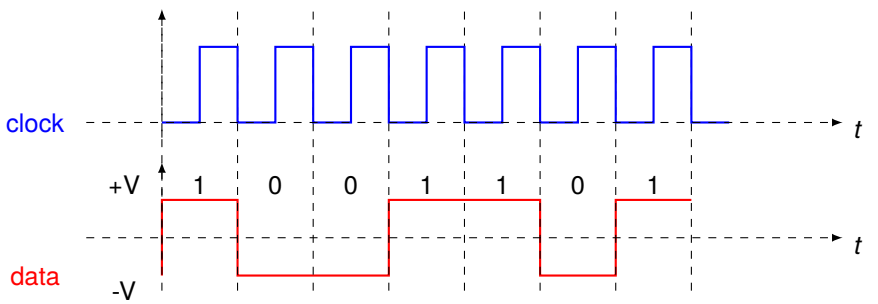
Généralisation des codages

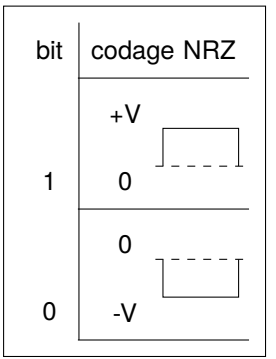
- Chaque variation des **informations transmises** est faite suivant un rythme prédéfinie : les «tics» d'horloge.
- Il est possible de considérer l'horloge comme un *signal* qui varie régulièrement.
- Un codage consiste alors à modifier les **caractéristiques** du signal d'horloge en fonction :
  - des bits à transmettre ;
  - d'une façon de réaliser ces modifications : un codage.

Cette transformation du signal d'horloge : «**codage en bande de base**».

Exemple : pour le code NRZ binaire (non retour à zéro) et un signal d'horloge sur front descendant

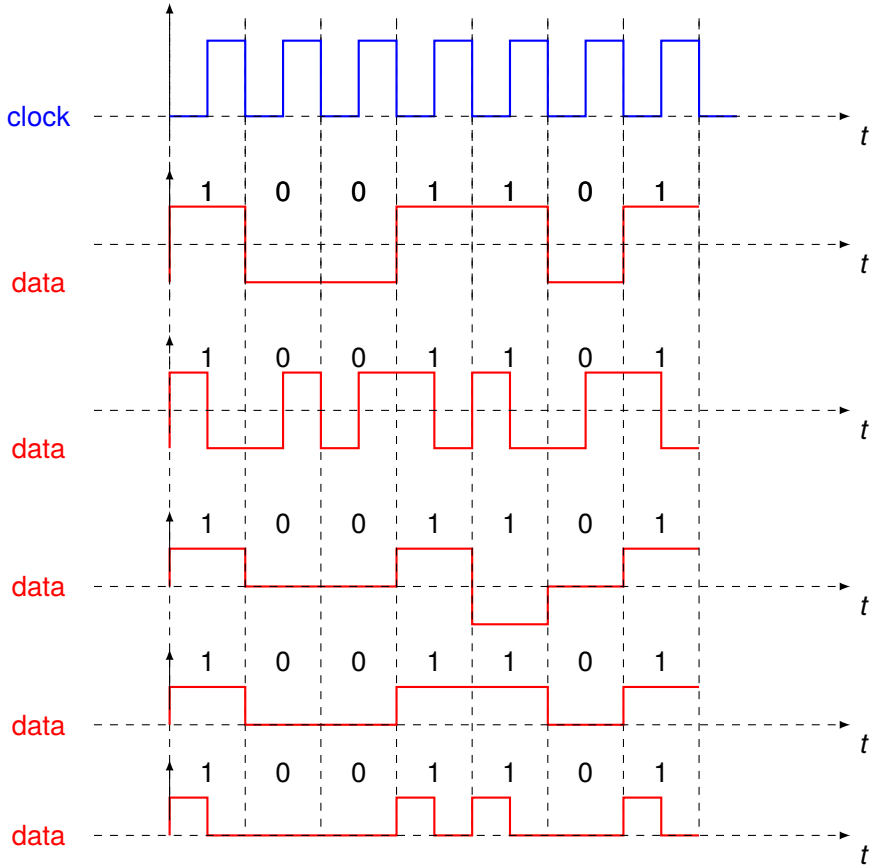
Les données sont : `1,0,0,1,1,0,1`





Récapitulatif de différents codages numériques

Représentation des 0 et de 1 par variation du voltage du courant



code **NRZ**

code **Manchester**

code **bipolaire**
pas de courant continu

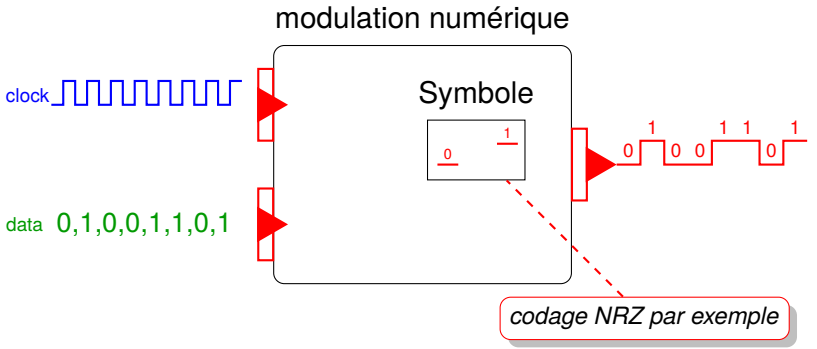
code **tout ou rien**
présence d'un courant continu

code **Return to Zero**

Le codage numérique ou en «bande de base», «*baseband*»

Généralisation du codage

- ▷ des **données binaire** à transmettre ;
- ▷ un **signal d'horloge** qui rythme l'utilisation de chaque bit de données ;
- ▷ un codage où **chaque bit** va être associé à un **symbole** suivant le codage choisi ;



Le débit de sortie du codage dépend du rythme de l'horloge, c-à-d de sa **fréquence**.

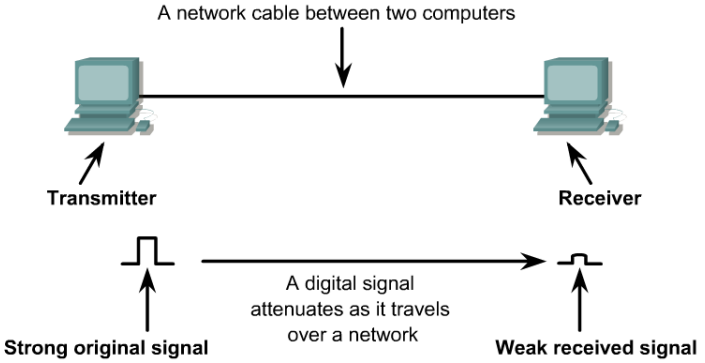
Une horloge à $1MHz \Longrightarrow 1Mbps$ pour un «*méga bit par seconde*».

Dépasser les limitations du codage numérique

Le codage en bande de base :

- vise à transmettre un signal dans sa «forme» initiale (signal carré) ;
- utilise du courant continu.

Les contraintes physiques des supports de transmission utilisés entraînent une dégradation très rapide du signal transmis :



Lorsque le signal est reçu, il est devenu **très difficile** de reconnaître les éléments de codage et ainsi de retrouver l'information binaire transmise (distortion, affaiblissement, *etc.*).

Pour dépasser les limitations d'un codage en bande de base : utilisation de la «modulation»

On utilise :

▷ un signal analogique avec des transitions douces et continues qui seront moins dégradées ;

▷ d'**autres types de codage** basés sur des modifications des **caractéristiques** de ce signal analogique

Ces codages sont appelés «modulation».

Codage par modulation : les détails

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

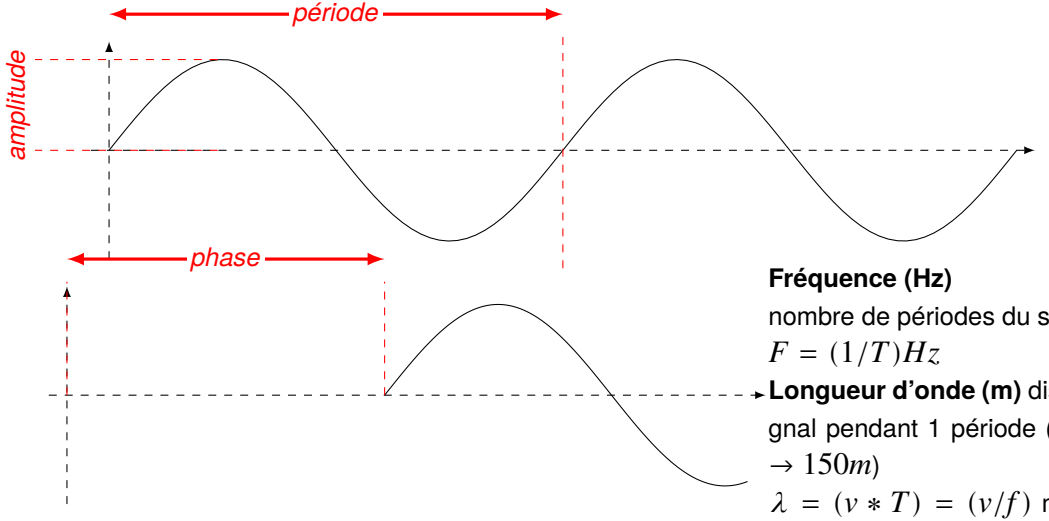
Gain espéré par rapport au codage en bande de base

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 :



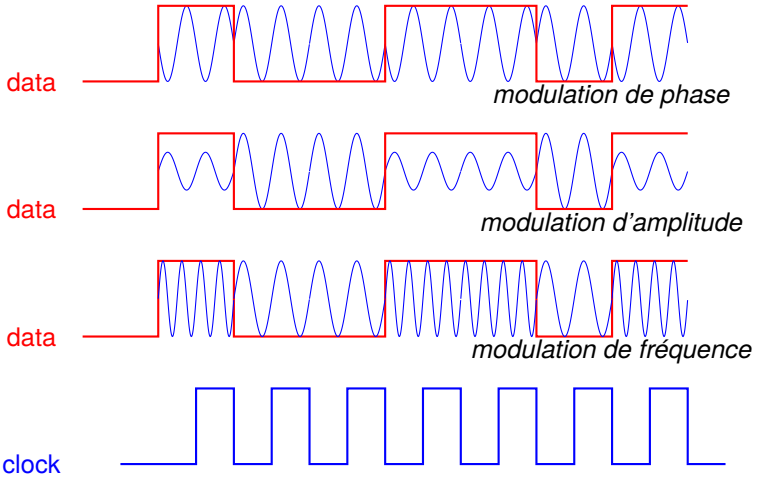
Fréquence (Hz)
nombre de périodes du signal pendant 1 seconde
$F = (1/T)Hz$

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`



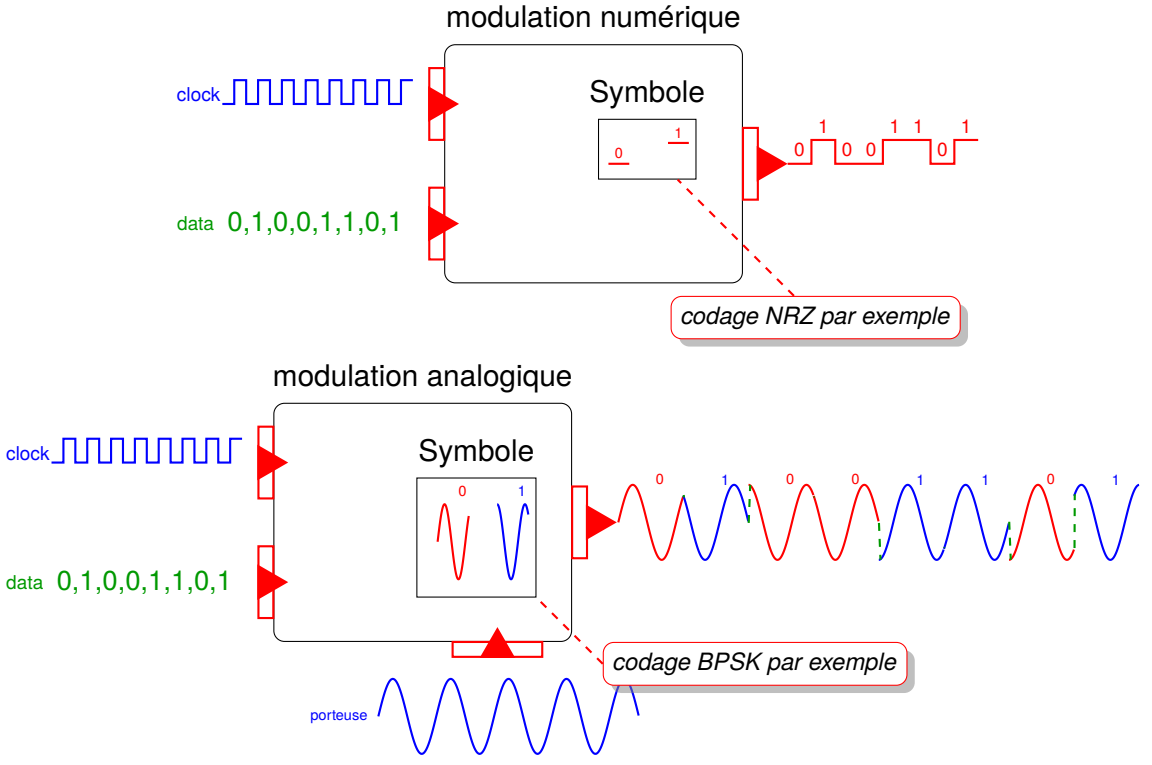
Modulation

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*

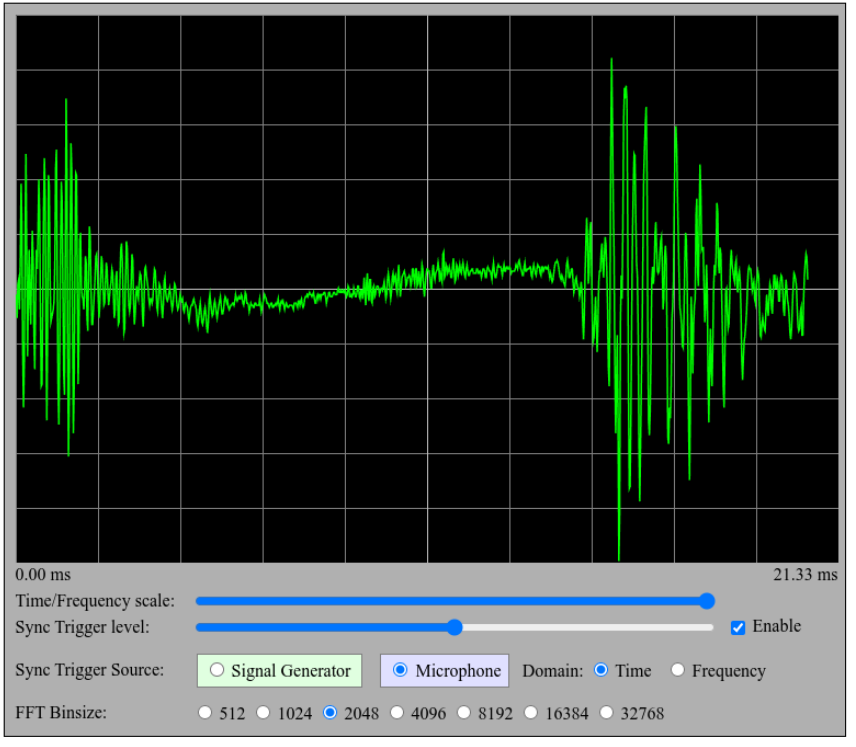
La modulation : codage en «*broadband*»

Généralisation du codage

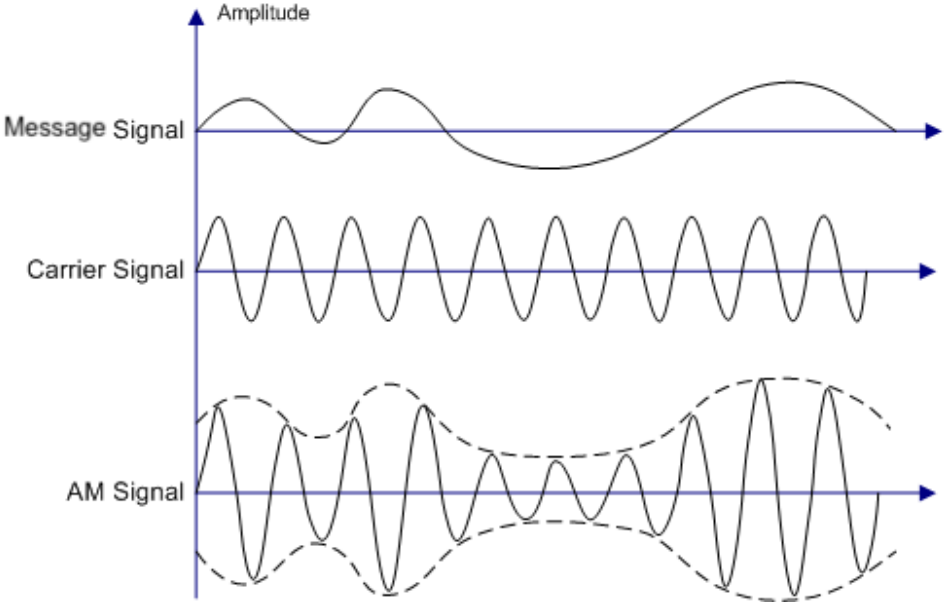


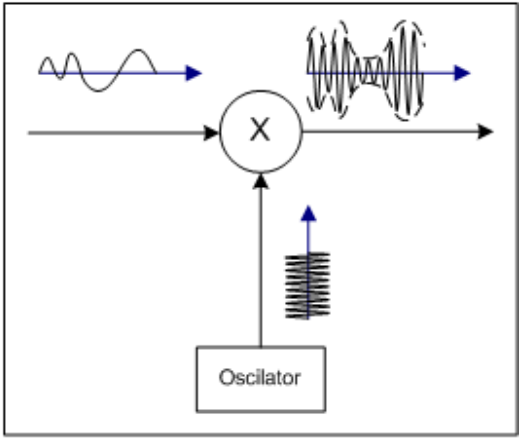
Le **débit** dépend de la **vitesse de modulation**, c-à-d du rythme des transformations réalisées sur la **porteuse**.

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

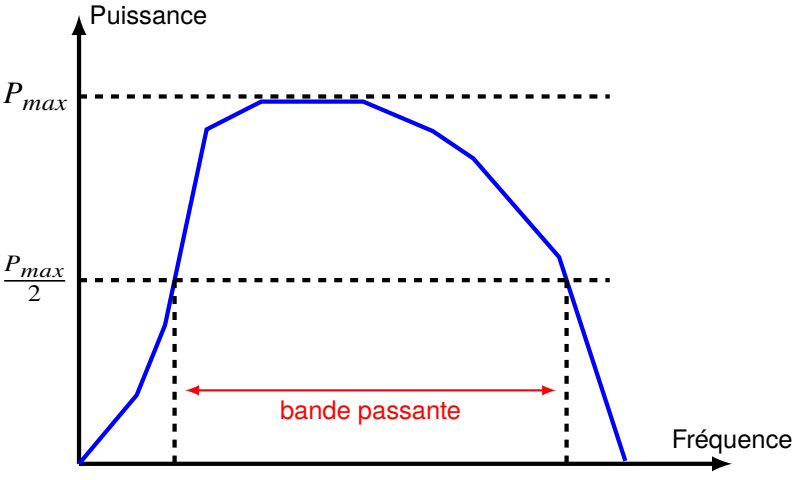
Notion de bande passante

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.

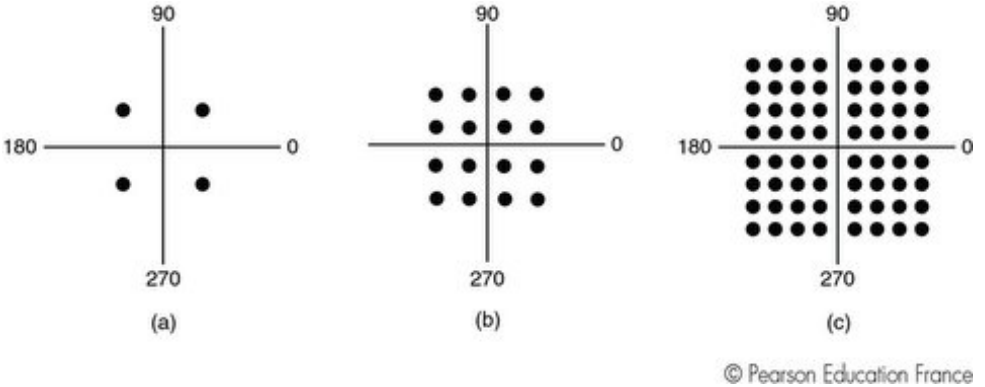
Amélioration des modulations

Il est possible :

- ▷ d'utiliser plusieurs paramètres pour une même modulation ;
- ▷ de combiner plusieurs types de modélisation simultanément ;
- ▷ de faire les deux !

Exemple :

- QPSK, *Quadrature Phase Shift Keying* (a) : 4 états de modulation de phase ou 4 symboles ;
- QAM, *Quadrature Amplitude Modulation* (b) : 4 états de modulation d'amplitudes et 4 de phases ou 16 symboles ;
- QAM-64 (c) : 8 états et 8 états ou 64 symboles.



Définition du bauds

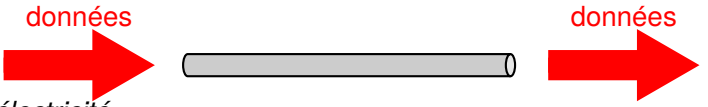
C'est le nombre de modulation transmise par seconde, ou de symboles transmis.

Pour passer au nombre de bits que l'on peut transmettre, on calcule 2^n = nombres de symboles (où n est le nombre de bits).

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.

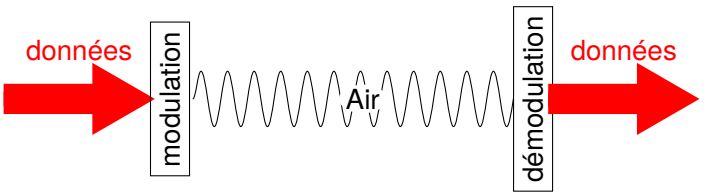
- L'air est un **isolant** pour l'électricité :

L'air ne conduit pas l'électricité...

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

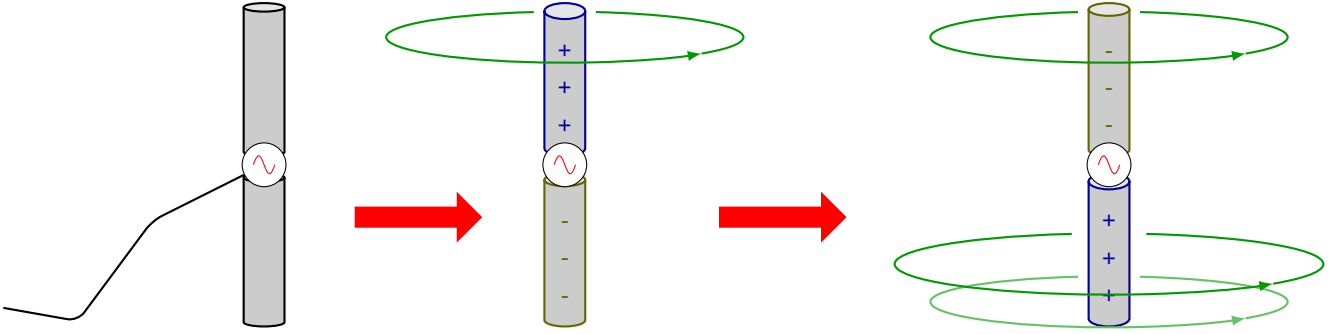
Les données doivent être :

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

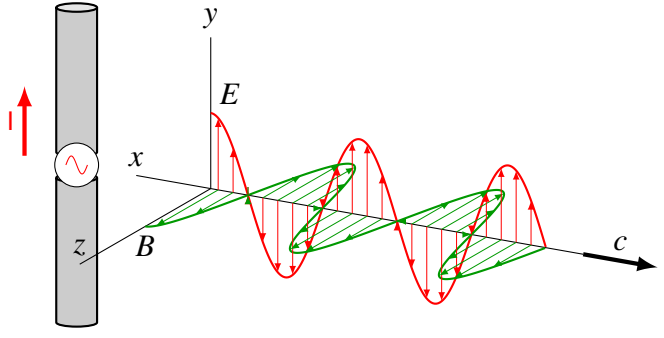


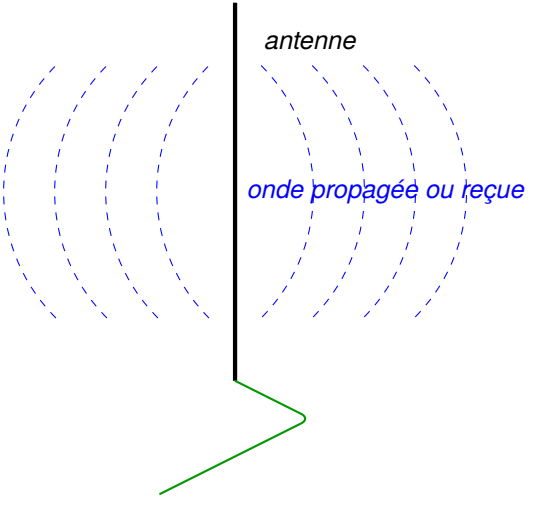
Champs électrique *vs* Champs magnétique

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** :





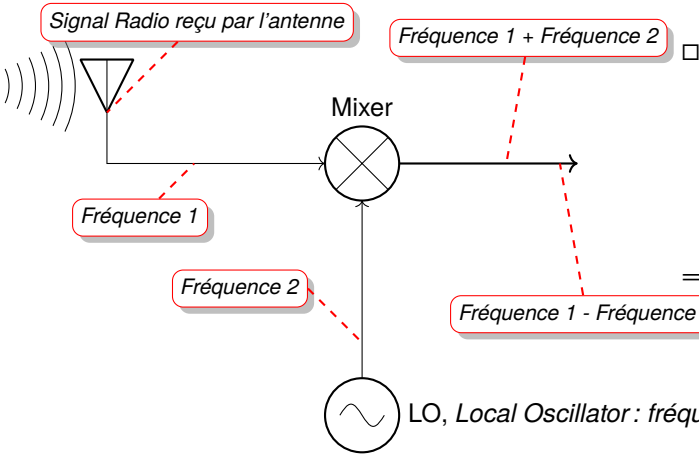
Où :

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

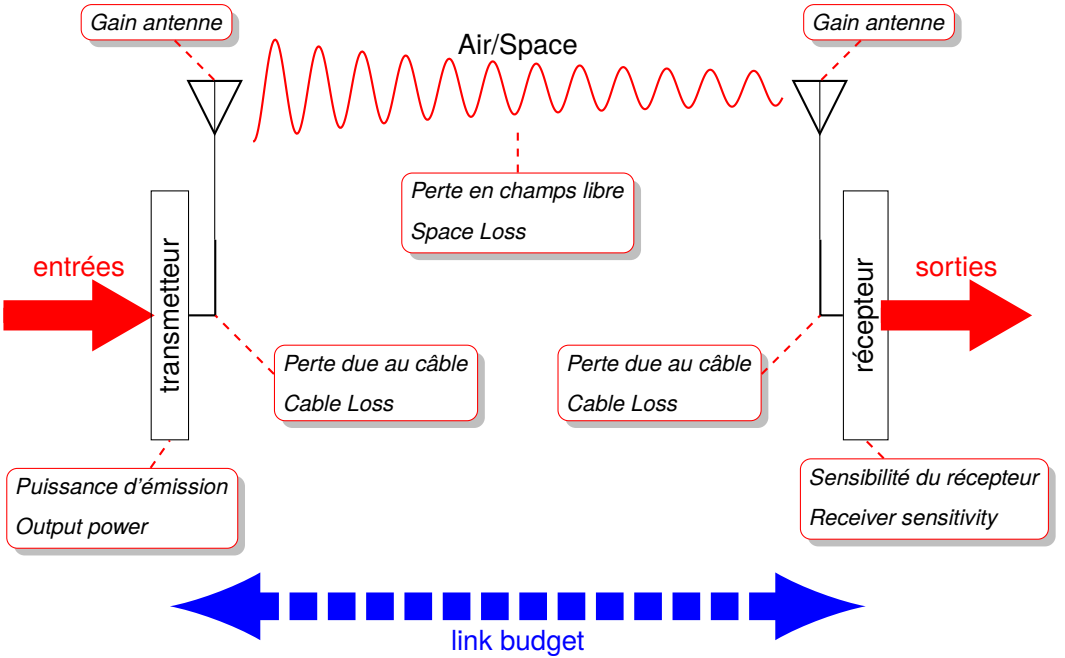
- on choisit une fréquence de transmission adaptée : réglementation, propriétés physiques (FSL, coût de l'électronique, *etc*) $\Longrightarrow$ ce sera la **fréquence support** ou «*porteuse*» ou «*carrier*»
- on choisit une **modulation** adaptée à ce que l'on veut transmettre ;
- on **décale** cette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



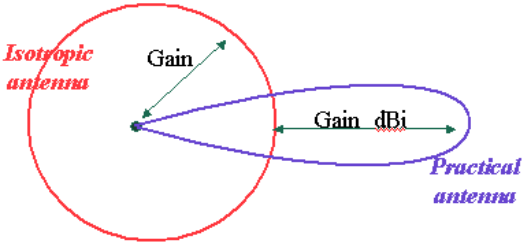
Le «*Link budget*» permet de :

- **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

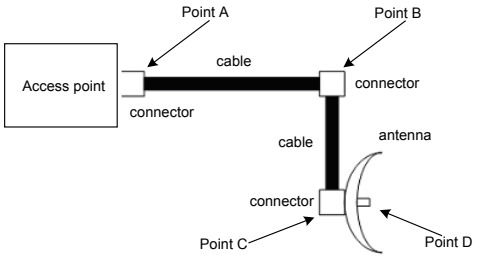
Une antenne **isotrope** est une *antenne théorique* qui rayonne de **manière uniforme** dans **toutes les directions**, c-à-d suivant une sphère et son gain est égal à l'unité.

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

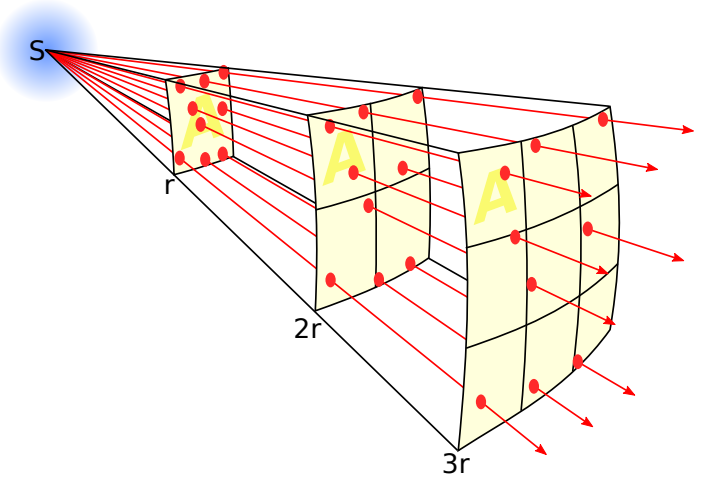
En physique, une loi en **carré inverse** est une loi physique postulant qu'une quantité physique (énergie, force, ou autre) est inversement proportionnelle au carré de la distance de l'origine de cette quantité physique.

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 :

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

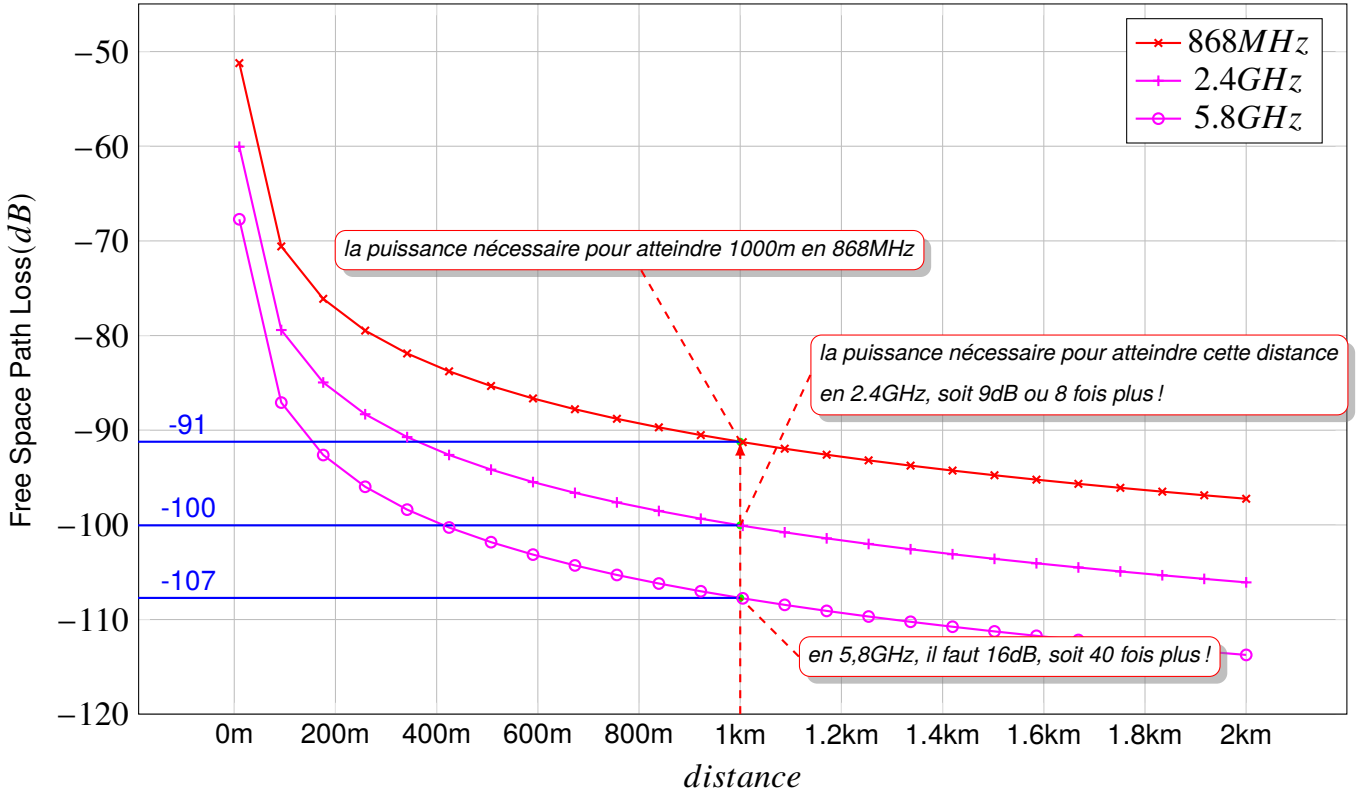
D'où la table suivante :

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

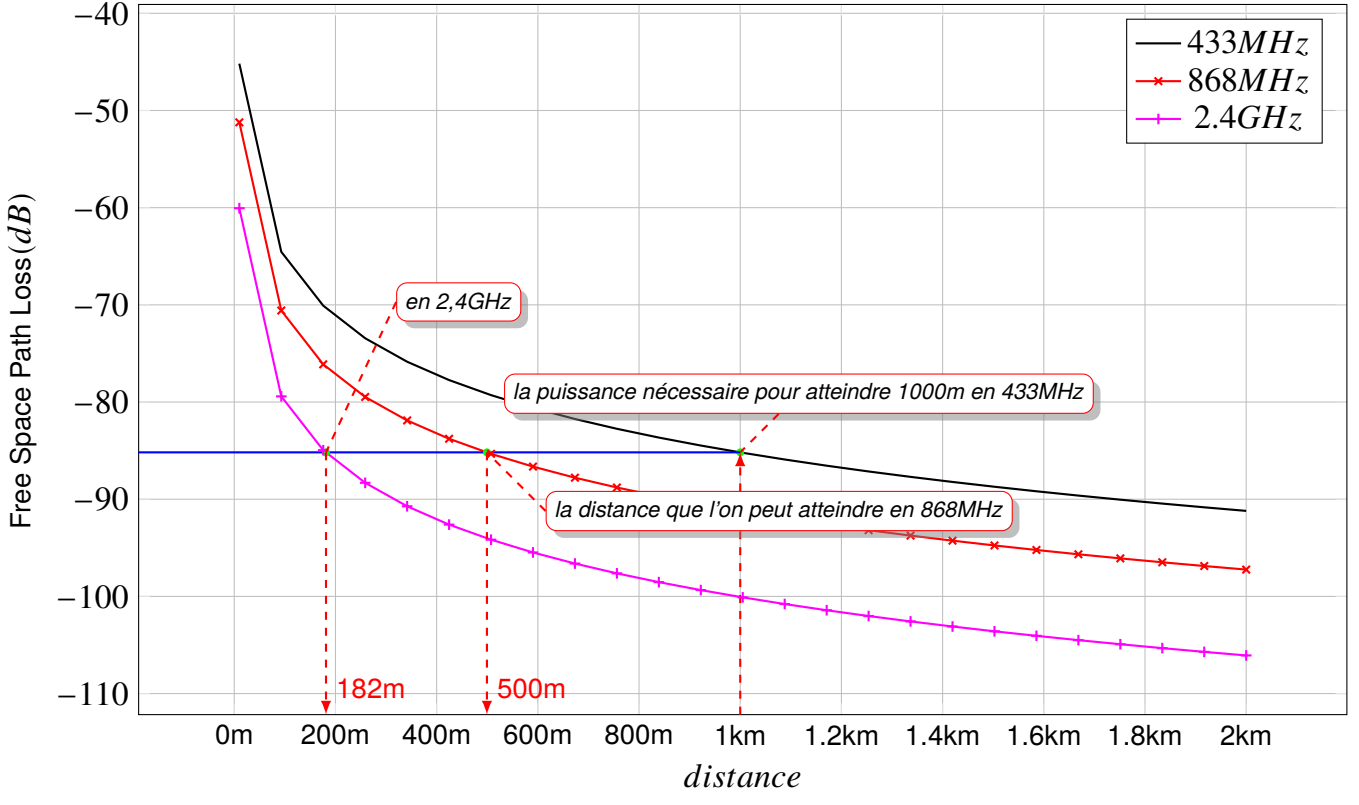
Affaiblissement en espace libre, «*Free Space Path Loss*»

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



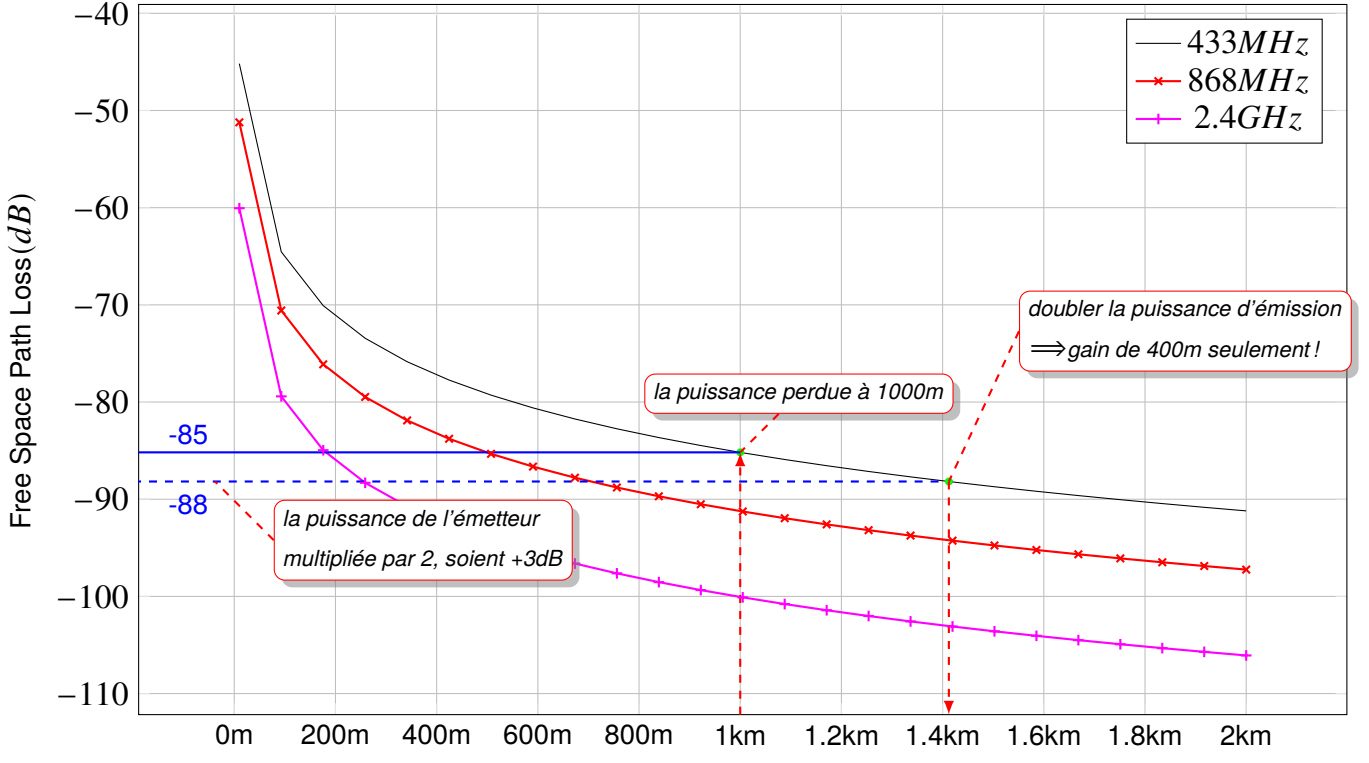
Affaiblissement en espace libre, «*Free Space Path Loss*»

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** !

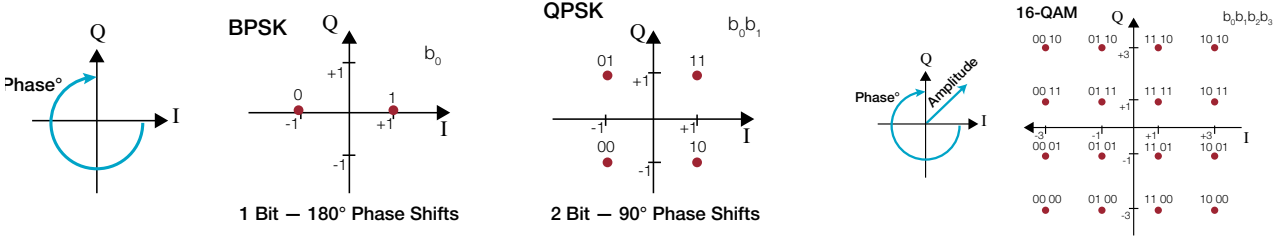
«*Link budget*»

- Le «*Link Budget*» permet de quantifier les **performances** d'un lien.
- La puissance reçue dépend de plusieurs paramètres :
  - la puissance transmise ;
  - le gain de l'antenne d'émission ;
  - le gain de l'antenne de réception ;
  - la perte en espace libre ;
  - la fréquence utilisée ;
  - la modulation utilisée.
- La performance d'un lien de communication dépend de la **qualité du matériel utilisé**.
- Si la **puissance** moins **l'atténuation** en espace libre du chemin est **supérieure** au niveau **minimal** de réception du signal de la radio du récepteur alors une liaison est **possible** ;

  La sensibilité, «*Sensitivity*» du récepteur

  C'est la **valeur minimale** de la puissance du signal que le récepteur est **capable de discerner**.
- La différence entre le minimum de niveau du signal reçu, la **sensibilité** du récepteur, et la puissance reçue est appelée le «***link margin***», «**marge de liaison**».
- La **sensibilité** de la radio du récepteur dépend de la **modulation** utilisée $\Longrightarrow$ plus elle est complexe, plus elle est dure à discerner.
- Le «*link margin*» doit être **positif** et doit être **maximisé**, c-à-d supérieur à au moins $10dB$ pour une communication fiable.

Modulation et bruit ambiant sur le récepteur



Le rapport Signal/Bruit, «SNR»

La technique de modulation détermine :

- ▷ le débit et la capacité du canal de communication ;
- ▷ la fiabilité du système :
  - ◇ compromis entre le débit et la distance ;
  - ◇ plus la technique de modulation est efficace plus le SNR doit être élevé ;
  - ◇ 64-QAM demande un **SNR plus élevé** alors que BPSK se suffit d'un **SNR moins élevé** car il est plus résistant au bruit présent sur le canal de communication.

Le codage ou «*coding*»

Correction d'erreurs : x bits sont convertis en y bits :

Data Bits	Coded Bits	Coding Rate	Efficiency	Reliability
1	2	1/2	Less	More
2	3	2/3		
3	4	3/4		
5	6	5/6	More	Less

On définie alors le **SNR** nécessaire au récepteur pour atteindre un niveau de fiabilité en terme de «BER», «*Bit Error Rate*» acceptable :

SNR = Puissance reçue − Bruit du canal de communication

Modulation & Codage	Débit (Mbps)	SNR (dB)
BPSK 1/2	6	8
BPSK 3/4	9	9
QPSK 1/2	12	11
QPSK 3/4	18	13
16-QAM 1/2	24	16
16-QAM 3/4	36	20
64-QAM 2/3	48	24
64-QAM 3/4	54	25

Plus de bruit sur le récepteur $\Longrightarrow$ moins de débit possible !

«*Link budget*» : un exemple

- ▷ fréquence de travail : 2,4GHz ;
- ▷ distance entre le point d'accès et la radio du client : 5km ;
- ▷ le point d'accès est connecté à une antenne :
  - ◇ gain : 10dBi ;
  - ◇ puissance d'émission : 20dBm ;
  - ◇ sensibilité de réception : -89dBm ;
- ▷ le client est connecté à une antenne :
  - ◇ gain : 14dBi ;
  - ◇ puissance d'émission : 15dBm ;
  - ◇ sensibilité de réception : -82dBm ;
- ▷ les câbles de connexion à l'antenne sont courts des deux côtés avec une perte de 2dB.

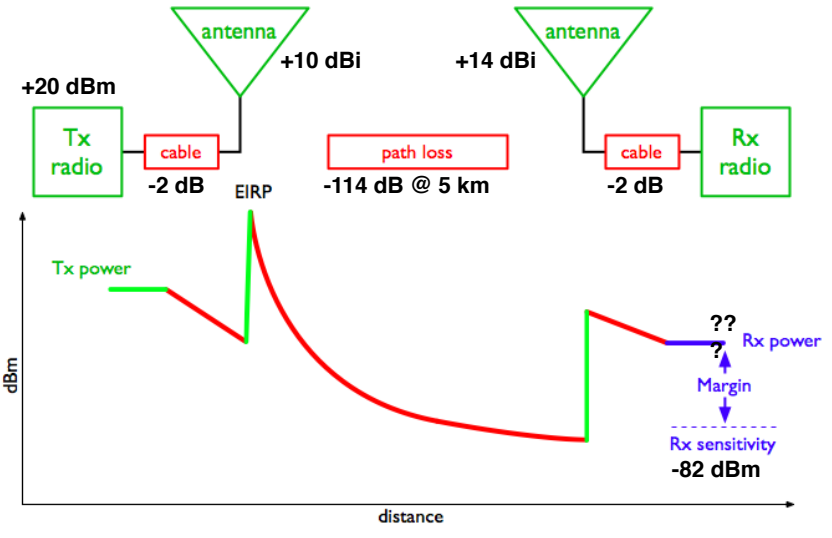
AP vers le client

Link Budget	Description
20dBm	TX Power AP
+10dBi	Antenna Gain AP
-2dB	Cable Losses AP
+14dBi	Antenna Gain Client
-2dB	Cable Losses Client

40dB	gain total
-114dB	FSPL pour 5km

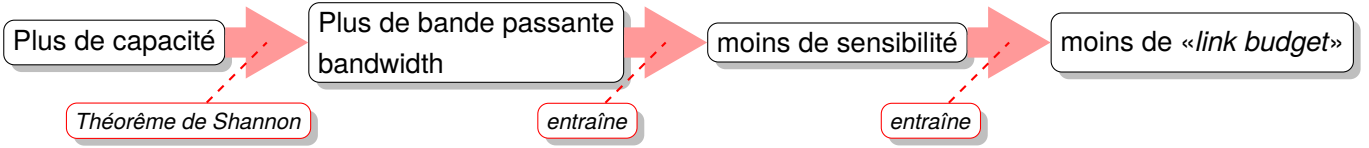
-74dBm	niveau de signal reçu
-82dBm	sensibilité du client

8dB	link margin



Du côté du recepteur

Si on veut augmenter la capacité de communication⟹on réduit le «*link margin*»



Pour augmenter le «*link margin*»⟹améliorer l'antenne

Quelle sorte d'antenne utiliser pour augmenter le «*link budget*» ?

- le récepteur n'est **pas régulé** contrairement à l'émetteur
  ⟹on peut utiliser une antenne avec un bon gain ;
  ⟹un bon gain permet d'augmenter le «*link margin*» ;

- directionnelle ? cela dépend :
  - si les nœuds sont fixes et l'on sait où est la «*gateway*»⟹ **bonne** idée !
  - si les nœuds sont répartis n'importe où ⟹ **pas une bonne** idée !
  - si les nœuds bougent ⟹ **pas une bonne** idée !

Pour augmenter le «*link margin*»⟹changer la modulation utilisée avec l'émetteur

Une modulation offrant **plus de débit** exige une **meilleure sensibilité**.
Un **débit plus bas**⟹ un «*link margin*» plus **important**.

Pour augmenter le «*link margin*»⟹utiliser un «*LNA*», «*Low Noise Amplifier*»

L'utilisation d'un **amplificateur** améliore la sensibilité mais demande des composants de **meilleure qualité**.

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...

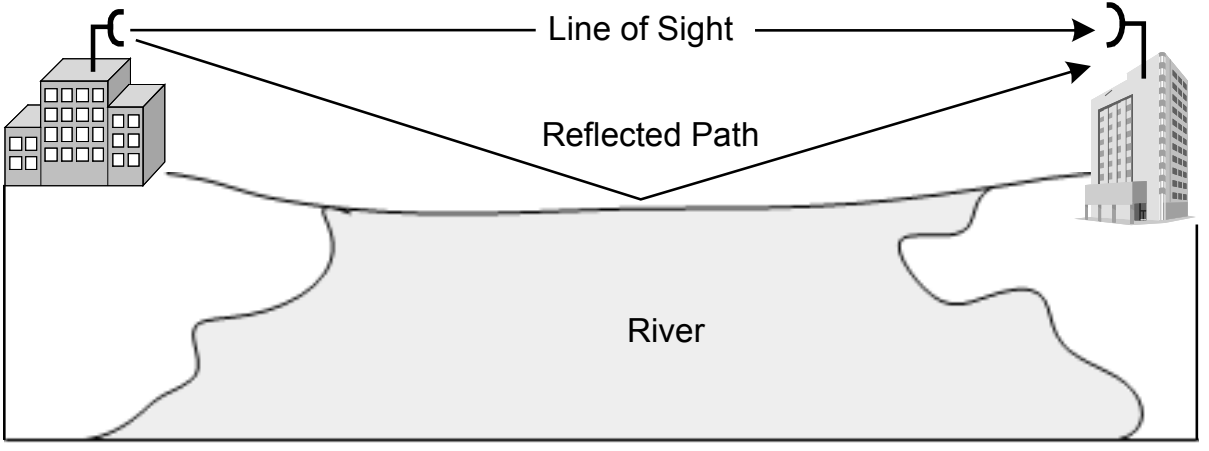
Autres atténuations et améliorations

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 :



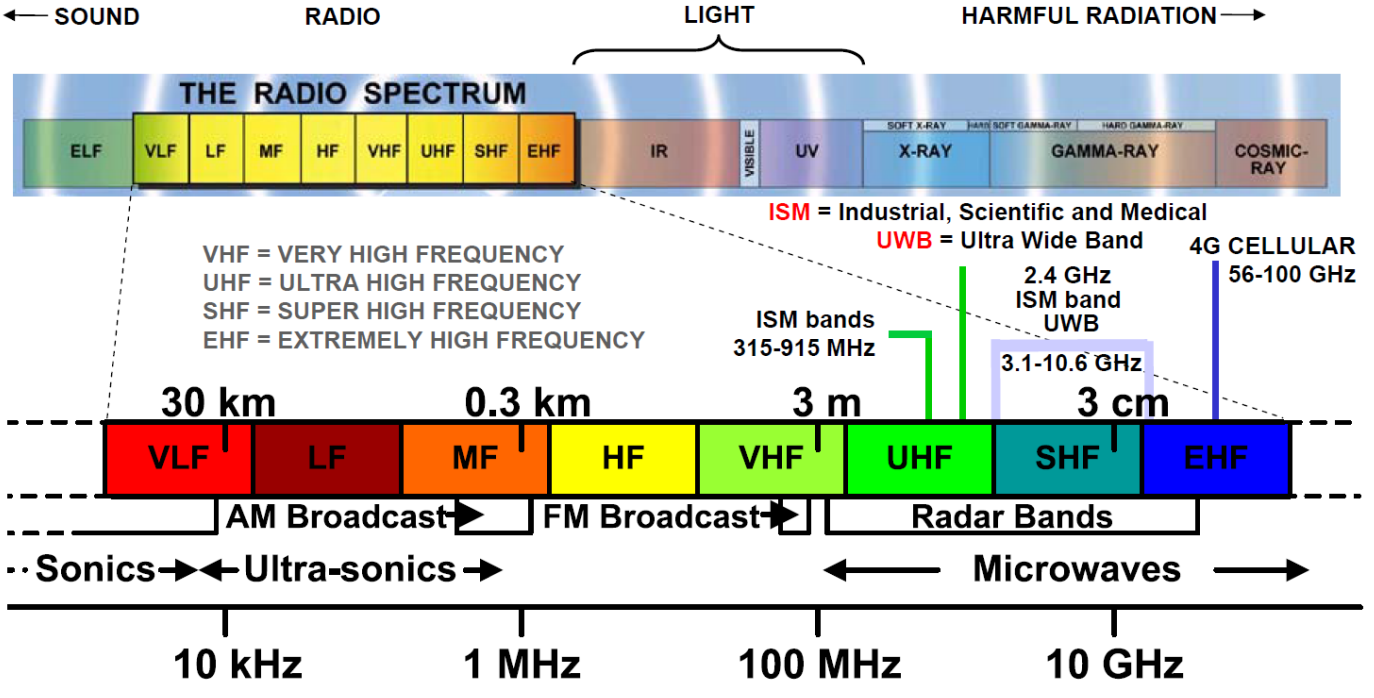
On se sert des multiples chemins, «multipath» *pour améliorer la réception du signal à l'aide de plusieurs antennes,* «diversity».

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

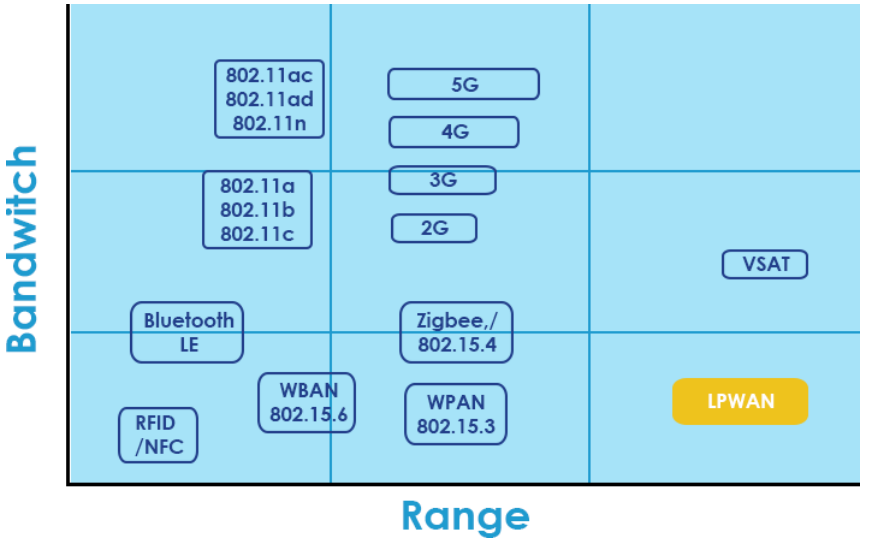
3 LoRa, «*Long Range*»

Plan

- LPWAN : «*Low Power Wide Area Network*» ;
- Technologies radio, fréquence et capacité ;
- Usages et caractéristiques ;
- Pourquoi des communications longue portée quand on en a de courte portée ?
- Différentes technologies radios : limitations techniques et administratives ;
- Les communications longue portée : aspects transmission.

OVERVIEW - Positioning

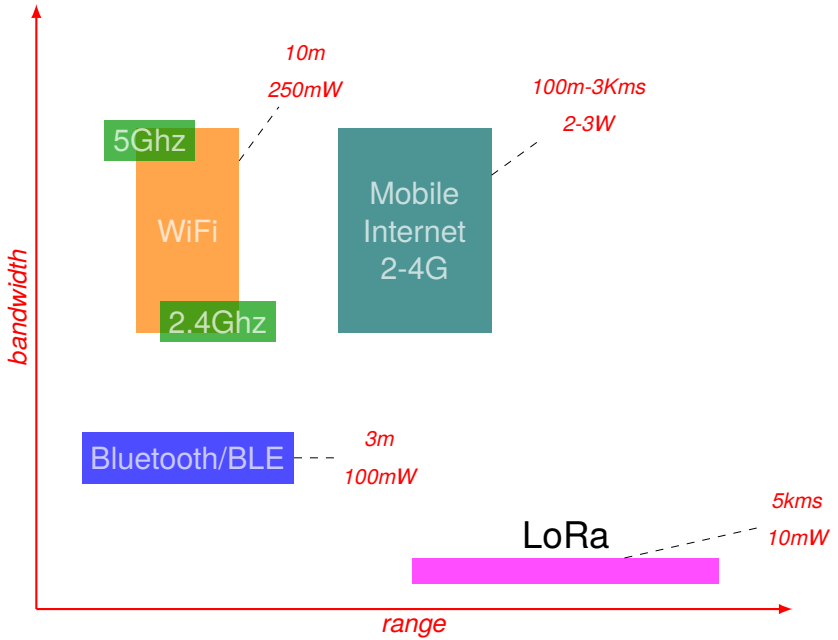
A sweet spot for LPWAN that suits the Internet of Things usages.
Besides LPWAN, no other technologies fulfills the needs of IoT applications.



Source : Perter R. Egli (http://fr.slideshare.net/PeterREgli/lpwan)

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

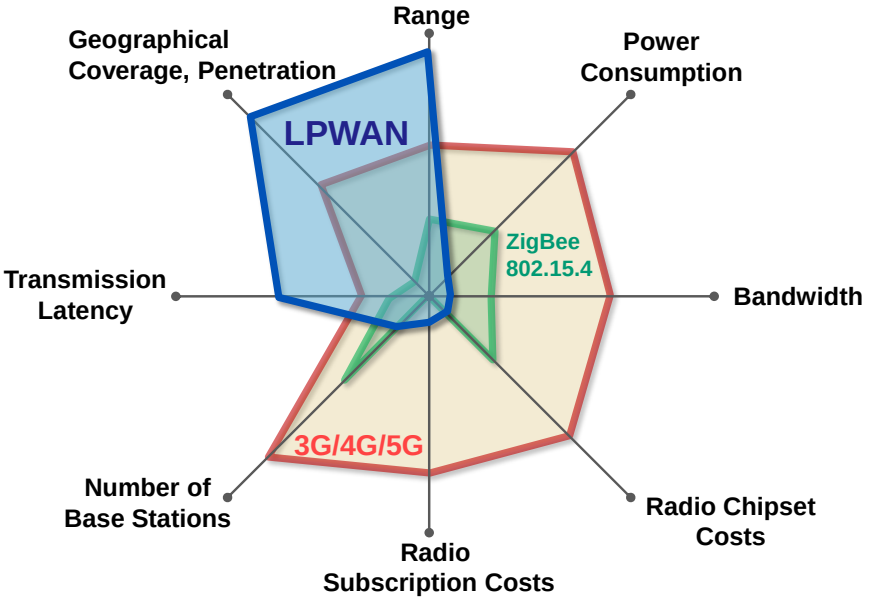
Smart City: smart grid, metering, lighting, structural health monitoring…
Smart Industry: predictive maintenance…

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:



Différentes propositions de communication longue portée

	LoRaWAN	Narrow-Band	LTE Cat-1	LTE Cat-M	NB-LTE
Modulation	SS Chirp	UNB/GSK/BPSK	OFDMA	OFDMA	OFMA
Rx Bandwidth	500-125KHz	100Hz	20MHz	20-1.4MHz	200KHz
Data rate	290bps-50Kbps	100bps 12/8 bytes max	10Mbps	200kbps-1Mbps	20Kbps
Max output power	20dBm	20dBm	23-46dBm	23/30dBm	20dBm
Battery lifetime 2000mAh	105 months (9 years)	90 months (7.5 years)		18 months (1.5 years)	
Link budget	154dB	151dB	130dB	146dB	150dB
Security	Yes	No	Yes	Yes	Yes

5G

On remarque que le «link budget» de LoRa est de 154dB qui est supérieur à celui du LTE Cat-1 qui utilise une énergie supérieure de 23 à 46 dBm.

Link budget :

- ▷ «rempli» par la **puissance de transmission** de l'émetteur et la **sensibilité** du récepteur ;
- ▷ dépend de la **fréquence** de transmission ;
- ▷ «diminué» par les **obstacles** (câbles, murs, arbres, *etc*), et la **distance** ;
- ▷ dépend de la **qualité** et de la **directivité** de **l'antenne**.

Allocation des fréquences et réglementation

Quelles sont le fréquences utilisables librement ?

Frequency	Band	Notes
13.553-13.567 MHz	ISM	RFID
26.957-27.283 MHz	ISM	Citizens' Band
433.050-434.790 MHz	ISM	LPD433 (70-centimeter band)
863–870 MHz		SRD860
2400.0–2483.5 MHz	ISM	13-centimeter band Heavily used by WiFi; BLE
5725–5875 MHz	ISM	5-centimeter band used by WiFi ac

Yeaahhh

Et pour le LoRa ?

SRD860

In Europe, 863 to 870 MHz band has been allocated for license-free operation using FHSS, DSSS, or analog modulation with either a transmission **duty cycle** of 0.1%, 1% or 10% depending on the band, or Listen Before Talk (LBT) with Adaptive Frequency Agility (AFA). Although this band falls under the Short Range Device umbrella, it is being used in Low-Power Wide-Area Network (LPWAN) wireless telecommunication networks, designed to allow long range communications at a low bit rate among things (connected objects).

Frequency	Duty cycle	Channel spacing	ERP
863.0 – 865.0 MHz	100% (wireless audio)		10 mW
863.0 – 865.6 MHz	0.1% or LBT+AFA		25 mW
863.0 – 868.0 MHz *			25 mW wideband up to 1 MHz (data only)
865.0 – 868.0 MHz	1% or LBT+AFA		25 mW
865.0 – 868.0 MHz *			2 W (RFID only)
865.0 – 868.0 MHz *	10% (access points), 2.5% (other devices)	4 frequencies	500 mW (data only, power control required)
868.0 – 868.6 MHz	1% or LBT+AFA		25 mW
868.6 – 868.7 MHz	1% (alarms)	25 kHz	10 mW
868.7 – 869.2 MHz	0.1% or LBT+AFA		25 mW

Radio et Infrastructure

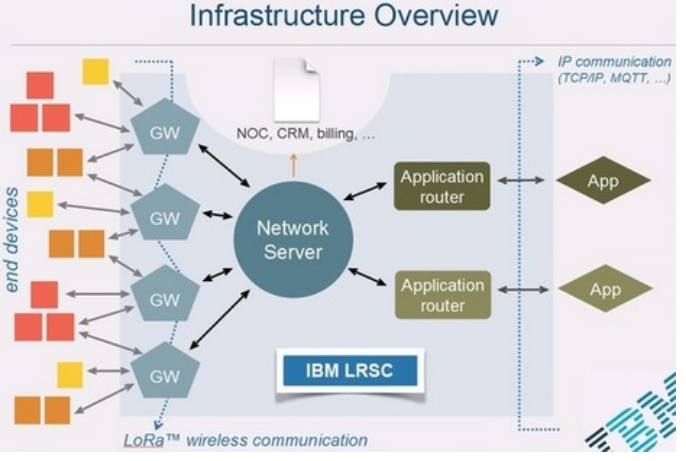
	Europe	North America	China	Korea	Japan	India
Frequency band	867-869MHz	902-928MHz	470-510MHz	920-925MHz	920-925MHz	865-867MHz
Channels	10	64 + 8 +8	In definition by Technical Committee	In definition by Technical Committee	In definition by Technical Committee	In definition by Technical Committee
Channel BW Up	125/250kHz	125/500kHz				
Channel BW Dn	125kHz	500kHz				
TX Power Up	+14dBm	+20dBm typ (+30dBm allowed)				
TX Power Dn	+14dBm	+27dBm				
SF Up	7-12	7-10				
Data rate	250bps- 50kbps	980bps-21.9kpbs				
Link Budget Up	155dB	154dB				
Link Budget Dn	155dB	157dB				

Le «*duty cycle*» assure le multiplexage

- 8 canaux $\Longrightarrow$ 8 appareils ;
- 50% «duty cycle» $\Longrightarrow$ 16 appareils ;
- 1% «duty cycle» $\Longrightarrow$ 800 appareils ;

  $\Longrightarrow$ *bandwidth encore plus réduite* !
- 250 bps/100 = 2.5bps ;

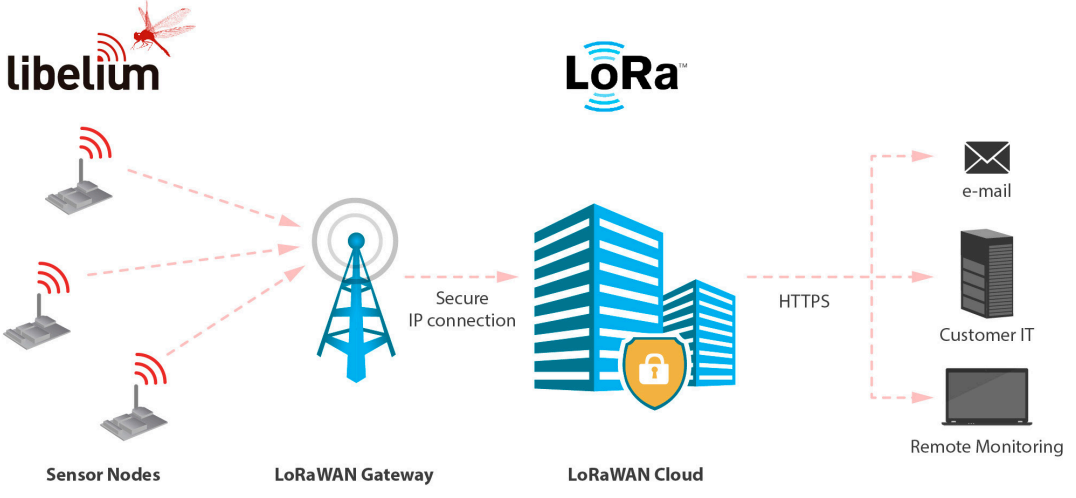
Un modèle basé sur des passerelles, «*GateWays*», des capteurs «*end devices*» et du Cloud.



LoRaWan

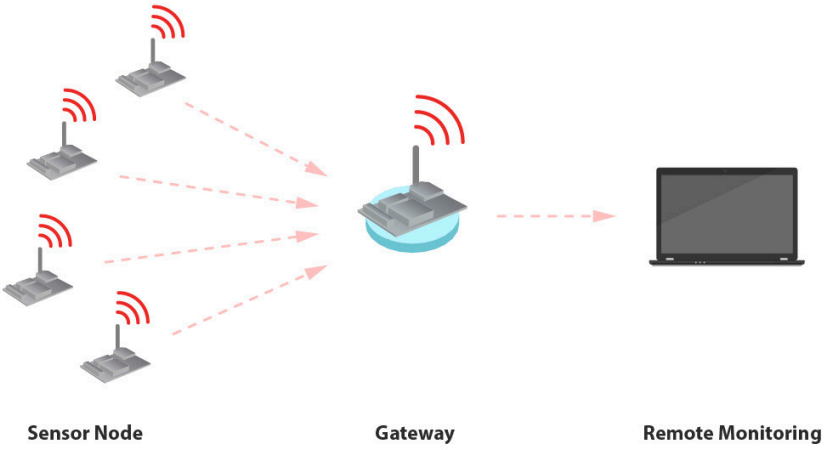
LoRa vs LoRaWan

- **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



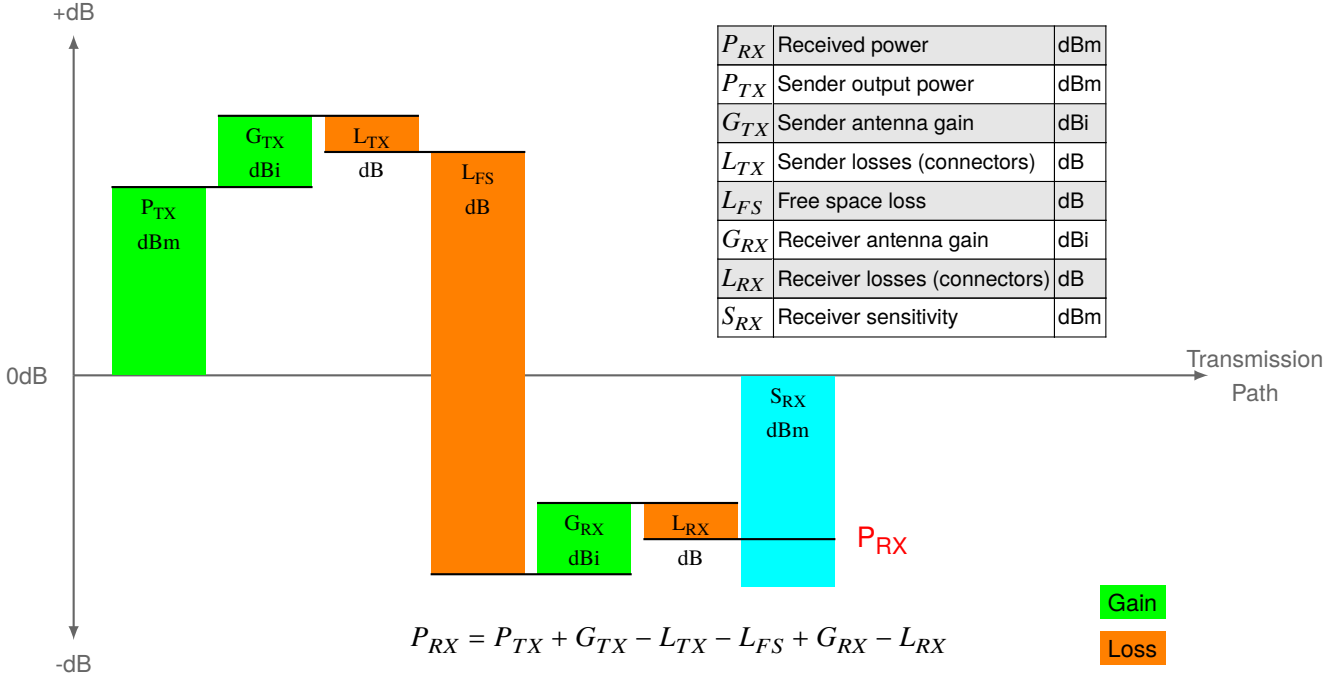
- ▷ pas de «*base station*», ni de Cloud (pas d'abonnement à une plateforme de médiation) ;
- ▷ The Internet of Things Network, TTN, `https://www.thethingsnetwork.org`

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 le bilan de liaison pour le LoRa ?

LoRa : «*Link Budget*»



P_{RX}	Received power	dBm
P_{TX}	Sender output power	dBm
G_{TX}	Sender antenna gain	dBi
L_{TX}	Sender losses (connectors)	dB
L_{FS}	Free space loss	dB
G_{RX}	Receiver antenna gain	dBi
L_{RX}	Receiver losses (connectors)	dB
S_{RX}	Receiver sensitivity	dBm

$$P_{RX} = P_{TX} + G_{TX} - L_{TX} - L_{FS} + G_{RX} - L_{RX}$$

Le «*Free Space Loss*» est le paramètre qui **réduit le plus** la puissance reçue par le récepteur.

La **sensibilité du récepteur**, «*receiver sensitivity*», doit être choisie de manière à être **égale ou inférieure** à P_{RX}.

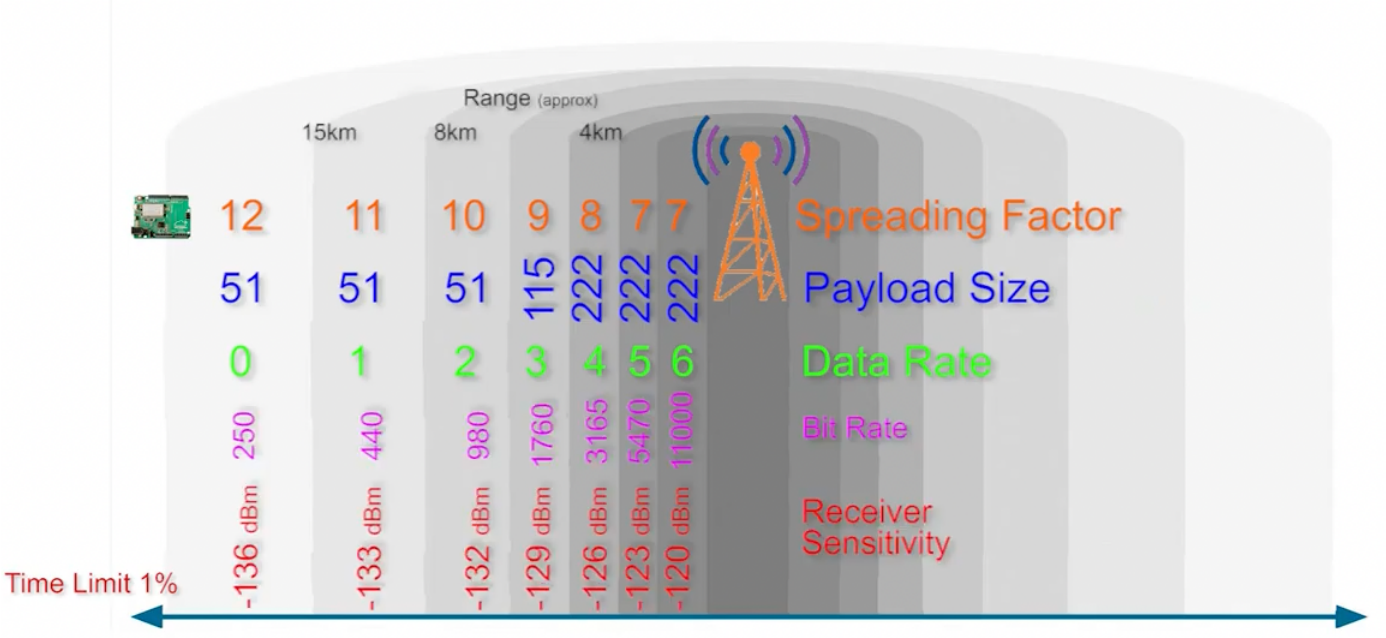
La sensibilité de LoRa est très bonne : jusqu'à $140dBm$ *!*

Le «*Link Margin*» est égale à $P_{RX} - S_{RX}$, avec S_{RX} qui est une valeur négative : il indique si **la communication est possible**.

Le **niveau maximal de bruit** supportable se calcule à l'aide du SNR,«*Signal to Noise Ratio*», minimum nécessaire pour la modulation choisie : $Max\ Channel\ Noise = P_{RX} - SNR_{MIN}$.

La **valeur courante du bruit** est mesurée sur le récepteur au travers du RSSI : elle ne doit pas dépasser celle calculée.

Paramètre d'une communication LoRa



Une affaire de compromis...

- ▷ distance ;
- ▷ durée de communication/consommation d'énergie ;
- ▷ taille des paquets ;
- ▷ débit.

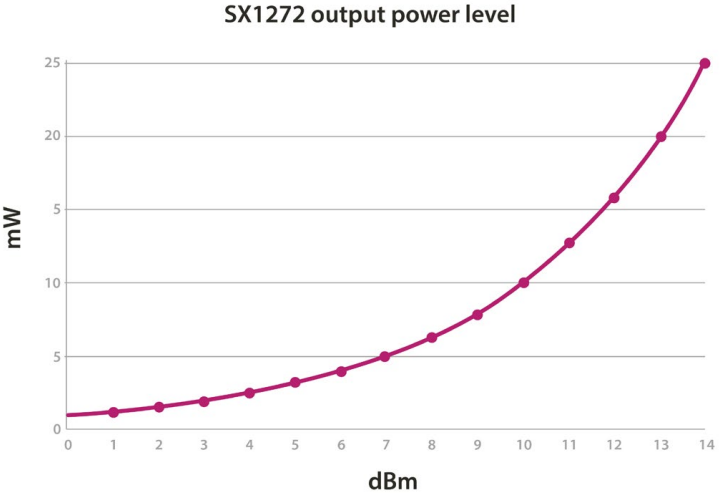
Et en vrai, ça donne quoi ?

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

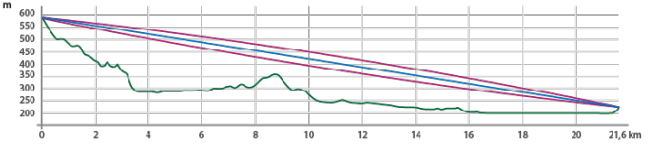


LoRa : test

Coupe du terrain :

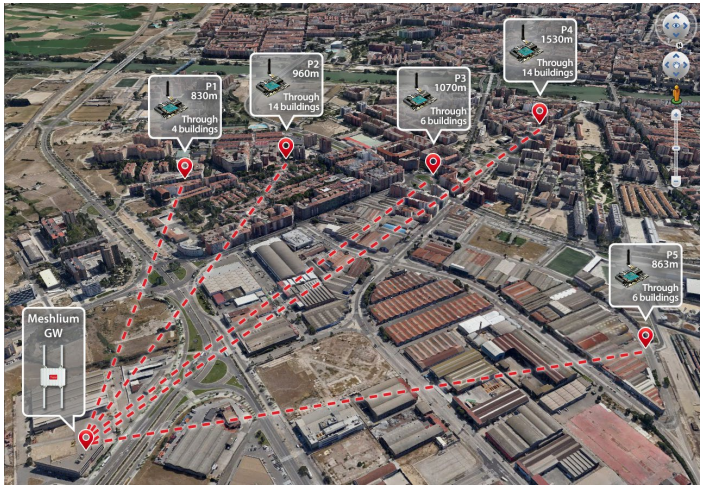
- ▷ la ligne bleue représente la ligne de vue ;
- ▷ l'ellipse mauve représente la zone de Fresnel ;

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

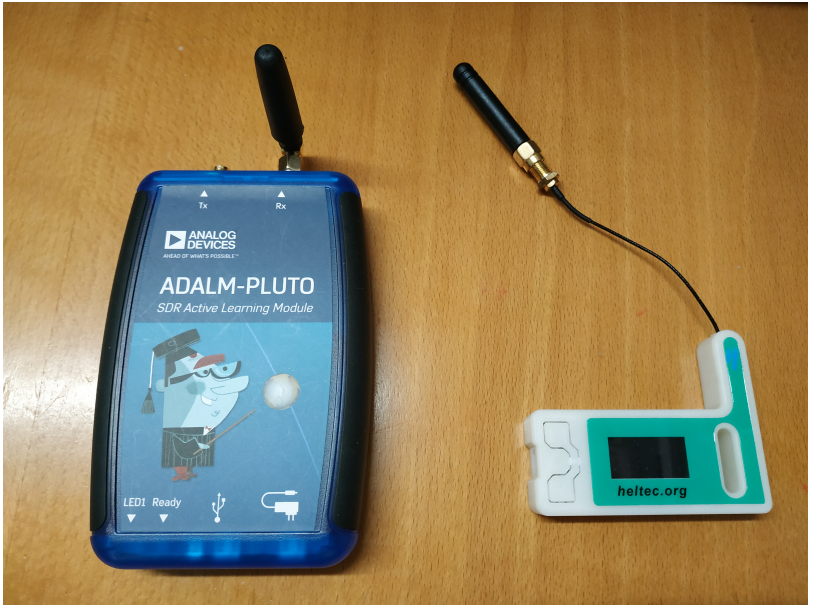


Les différents points :

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

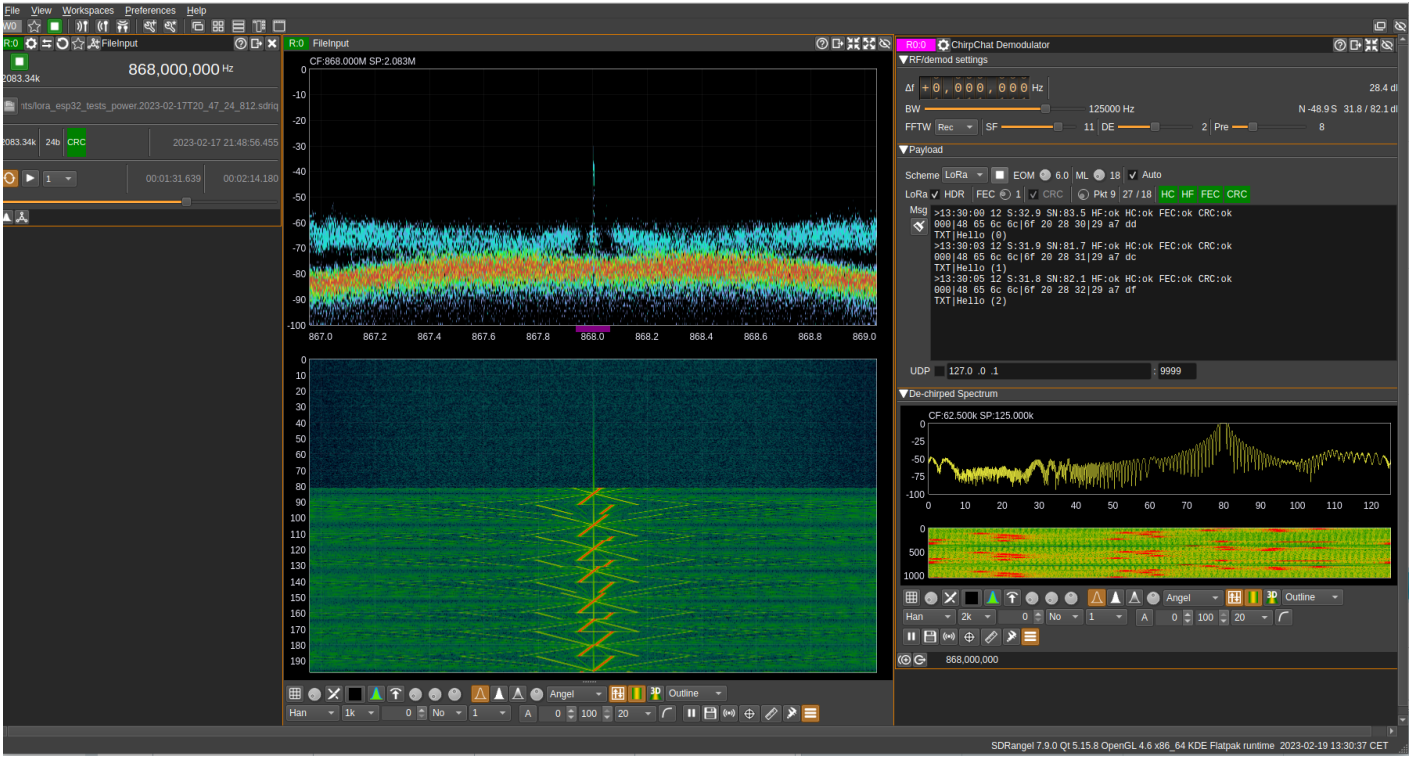
Démodulation LoRa : utilisation de la SDR «*ADALM-PLUTO*»



Features

- Based on Analog Devices AD9363–Highly Integrated RF Agile Transceiver and Xilinx® Zynq Z-7010 FPGA
- RF coverage from 325 MHz to 3.8 GHz
- Up to 20 MHz of instantaneous bandwidth
- Flexible rate, 12-bit ADC and DAC
- One transmitter and one receiver, half or full duplex
- libiio, a C, C++ and Python API
- USB 2.0 Powered Interface with Micro-USB 2.0 connector

Démodulation LoRa : le logiciel SDRangel



Le logiciel SDRangel permet de démoduler le LoRa pour un SF de 11.

Sur cette capture on voit :

- ▷ *la* «waterfall» *avec les chirps de la modulation LoRa ;*
- ▷ *la démodulation avec les messages* «`Hello (i)`».

Démodulation LoRa

Ici, la bande passante de modulation est de 125kHz :

- ▷ *l'énergie transmise est répartie entre les différentes fréquences de 0 à 125kHz ;*
- ▷ *on observe une mini «*waterfall*».*

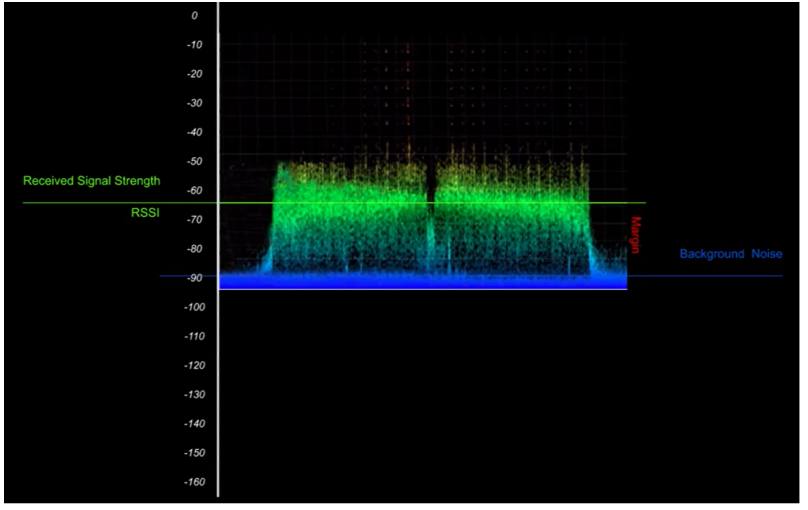
RSSI et SNR ?

RSSI, «*Received Signal Strength Indicator*»

- **mesure relative** qui permet de savoir si le signal reçu est suffisamment fort pour avoir une bonne réception depuis l'émetteur ;
- mesuré en dBm et sa valeur est négative ;
- plus le RSSI est proche de zéro plus le signal reçu est fort ↗
- influencé par : la perte en champs libre (FSPL), gain de l'antenne, pertes dues aux câbles/connecteurs, pertes dues aux obstacles.

SNR, «*Signal-to-Noise Ratio*»

Il est calculé par : SNR (dB) = Preceived_signal (dBm) - Pnoise (dBm)
On est en dB, c-à-d que $\frac{S}{N}$ *se traduit par* $S - N$ *en logarithme*.



Ici, le RSSI est de $-65dBm$ *et le niveau de bruit est de* $-90dBm$*, ce qui donne :*

SNR (dB) = -65 dBm -(-90 dBm) = 25 dB

$\Longrightarrow$ *la valeur positive de 25dBm, le récepteur sera en mesure de démoduler le signal reçu.*

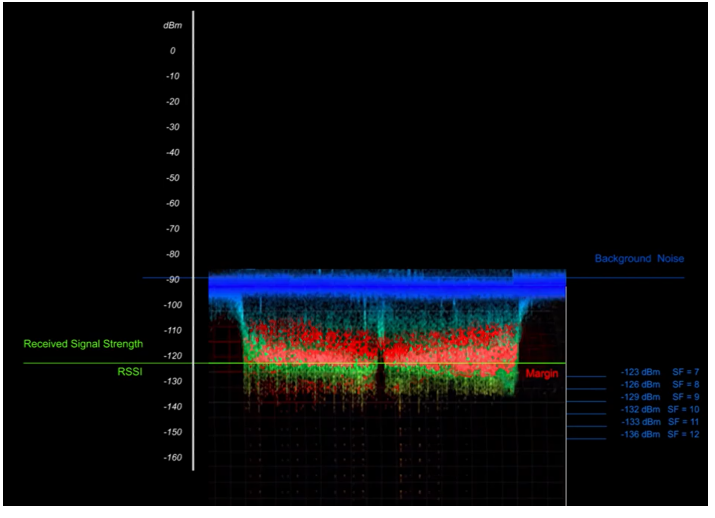
RSSI et SNR ? en LoRa

Si le RSSI est **en-dessous** du niveau de bruit, il est **impossible** de démoduler le signal.

Mais en LoRa, avec l'aide du SF on peut démoduler **en dessous** du niveau de bruit :

SpreadingFactor (RegModulationCfg)	Spreading Factor (Chips / symbol)	LoRa Demodulator SNR
6	64	-5 dB
7	128	-7.5 dB
8	256	-10 dB
9	512	-12.5 dB
10	1024	-15 dB
11	2048	-17.5 dB
12	4096	-20 dB

Exemple



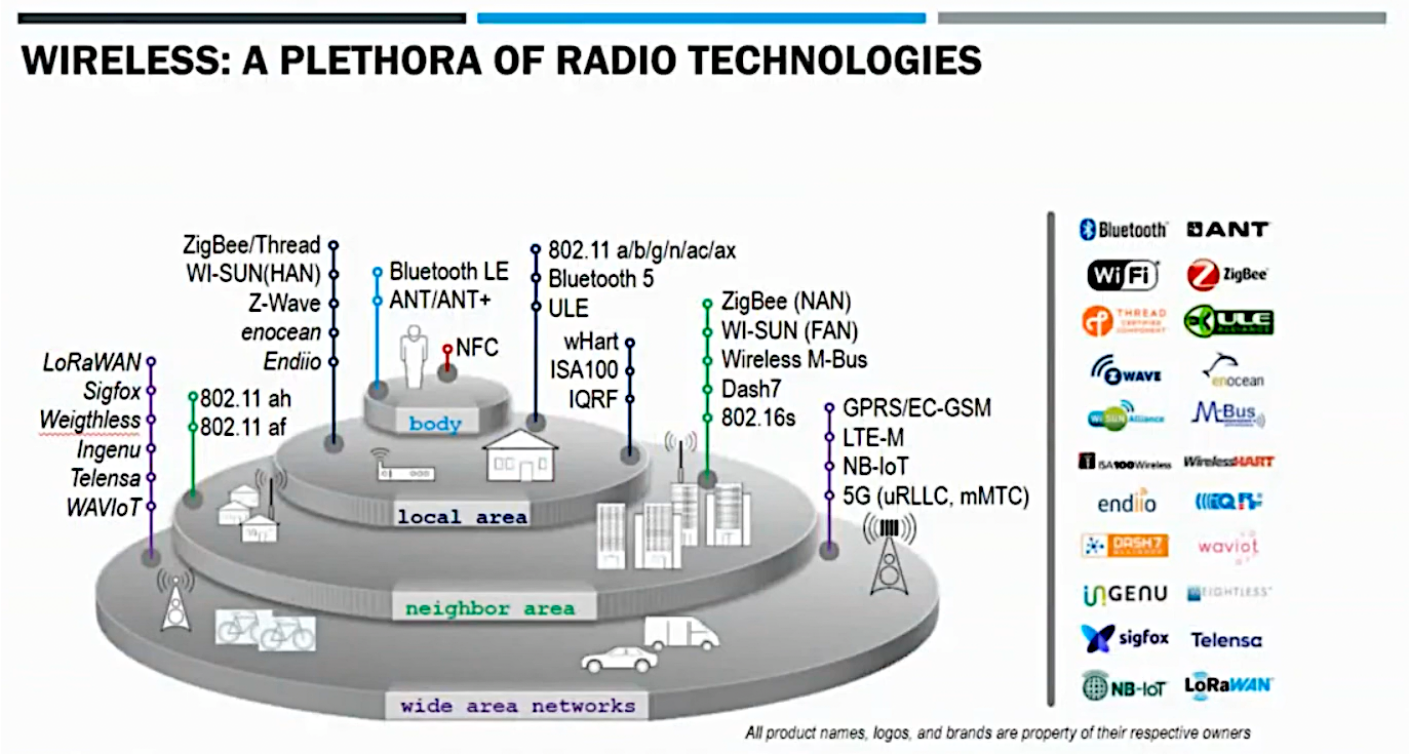
Ici, le RSSI est de -120dBm pour un niveau de bruit de -90dBm

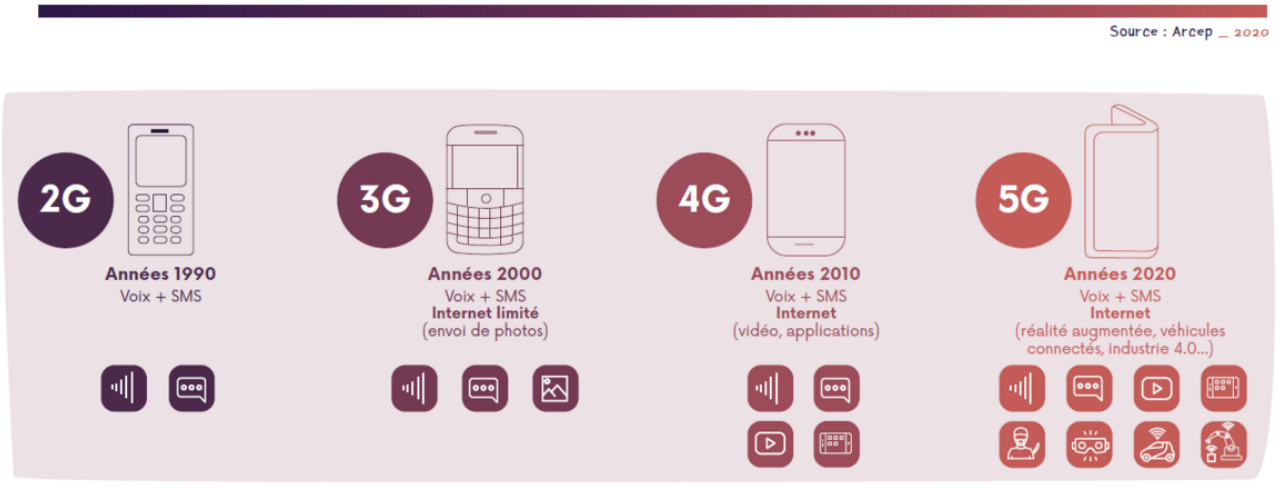
SNR (dB) = Preceived_signal (dBm) - Pnoise (dBm)

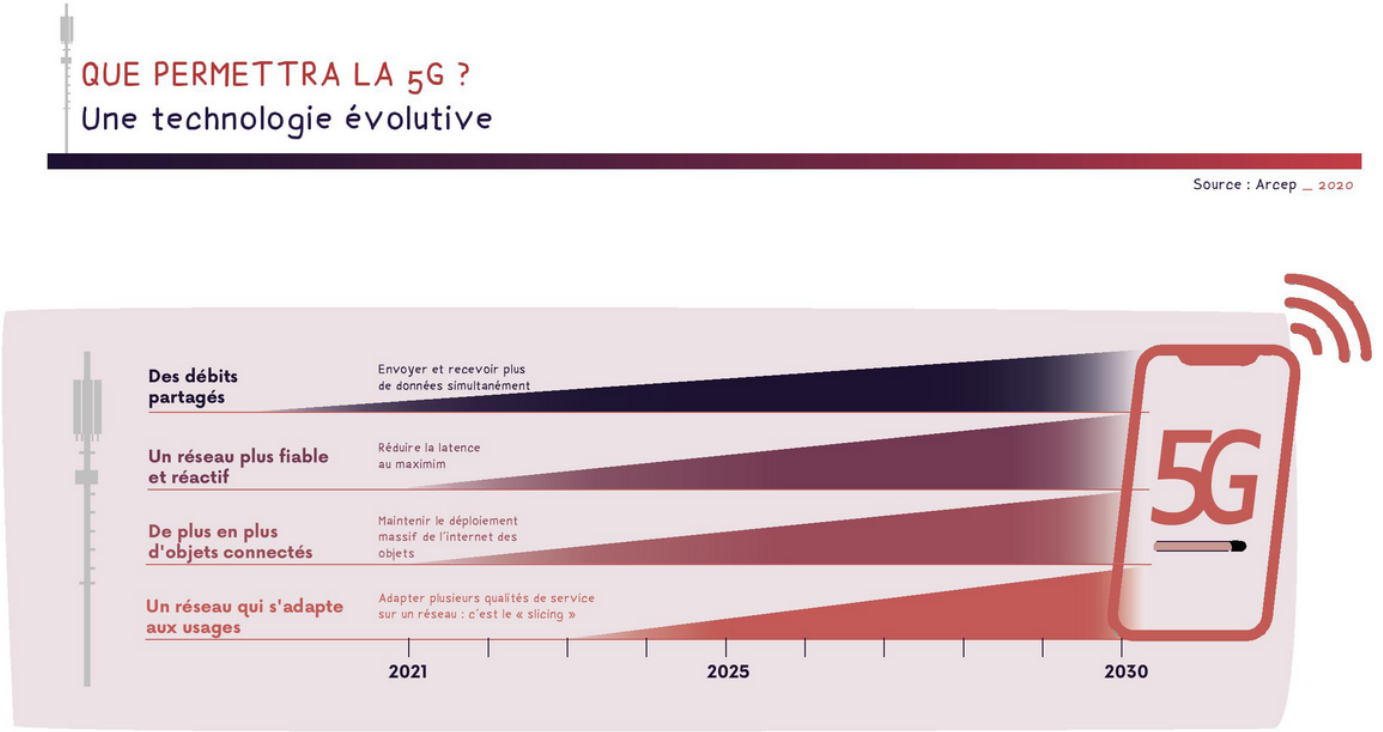
SNR (dB) = -120 dBm -(-90 dBm) = -30 dB

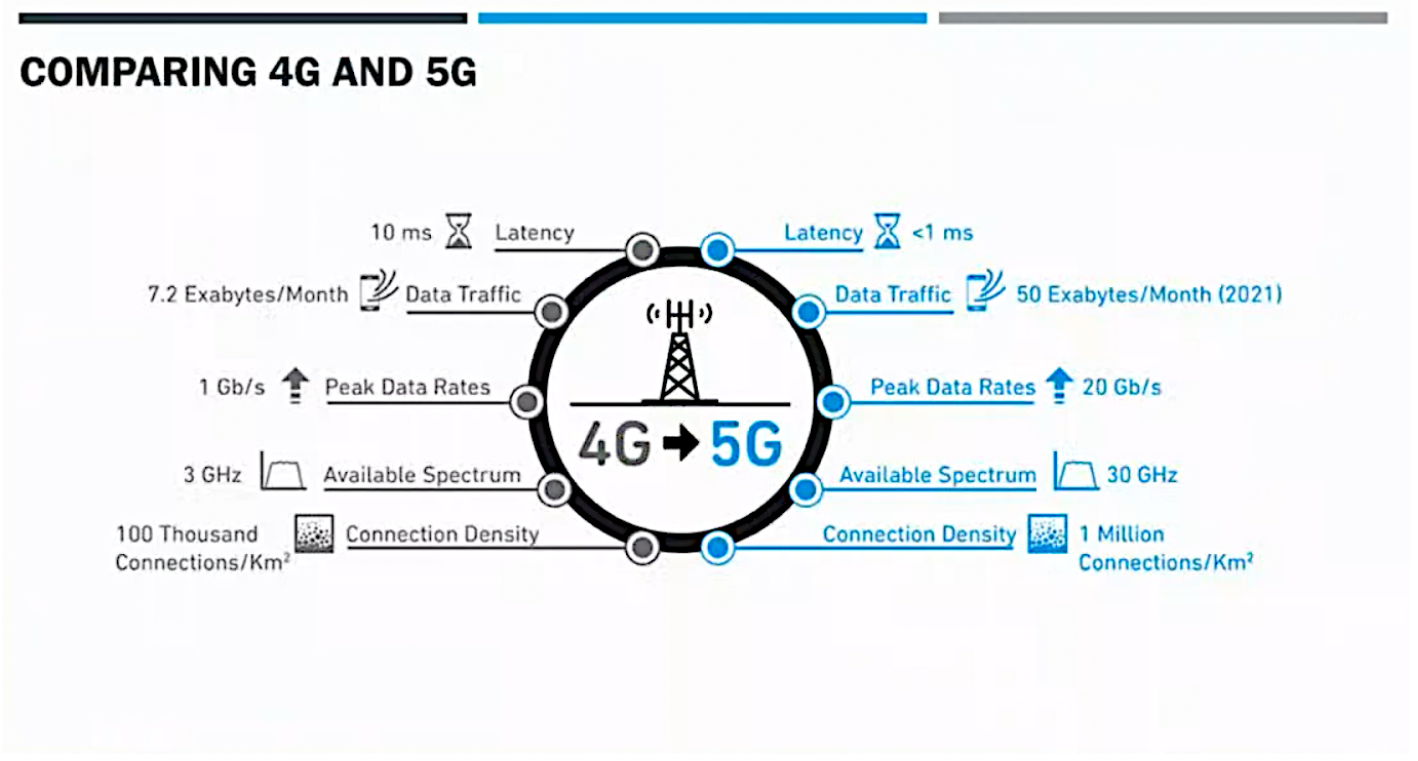
La valeur obtenur du SNR de -30dBm est en-dessous du niveau de SNR minimum du LoRa de -20dBm pour un SF=12
⟹le récepteur ne pourra pas démoduler quand même le signal reçu.

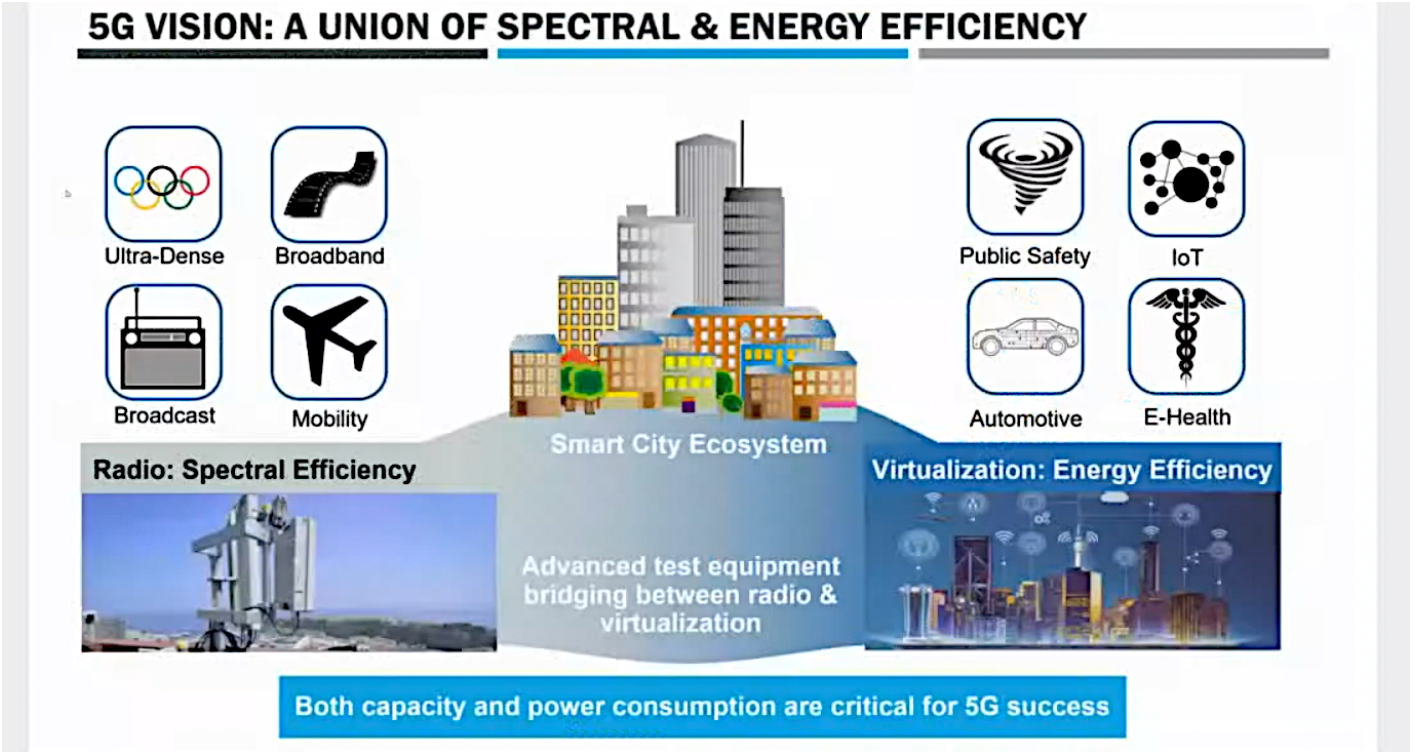
La 5G
Ou la technologie support de l'IoT


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
2G
Années 1990
Voix + SMS
3G
Années 2000
Voix + SMS
Internet limité
(envoi de photos)
4G
Années 2010
Voix + SMS
Internet
(vidéo, applications)
5G
Années 2020
Voix + SMS
Internet
(réalité augmentée, véhicules connectés, industrie 4.0...)

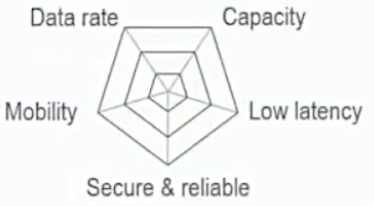

QUE PERMETTRA LA 5G ?
Une technologie évolutive
Source : Arcep _ 2020
Des débits partagés
Envoyer et recevoir plus de données simultanément
Un réseau plus fiable et réactif
Réduire la latence au maximim
De plus en plus d'objets connectés
Maintenir le déploiement massif de l'internet des objets
Un réseau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

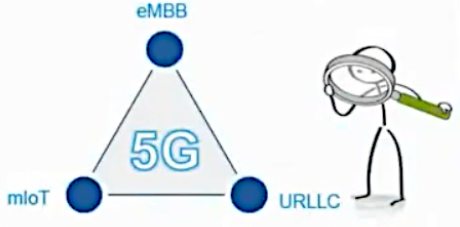

COMPARING 4G AND 5G
10 ms
Latency
7.2 Exabytes/Month
Data Traffic
1 Gb/s
Peak Data Rates
3 GHz
Available Spectrum
100 Thousand Connections/Km²
Connection Density
4G → 5G
Latency
<1 ms
Data Traffic
50 Exabytes/Month (2021)
Peak Data Rates
20 Gb/s
Available Spectrum
30 GHz
Connection Density
1 Million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

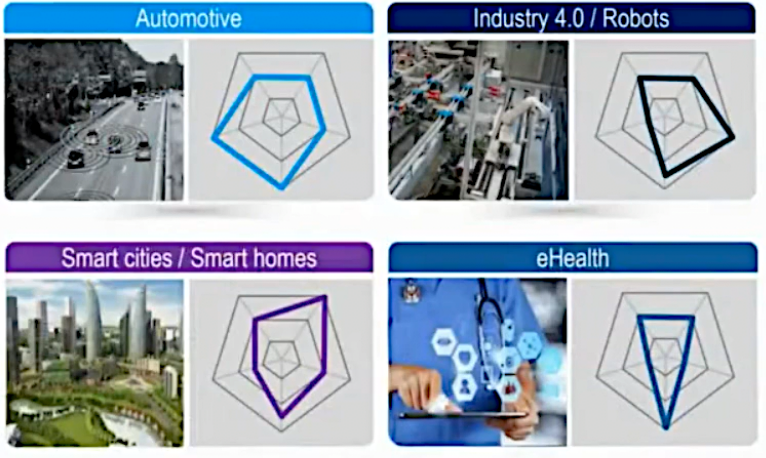

5G VISION: A UNION OF SPECTRAL & ENERGY EFFICIENCY
Ultra-Dense
Broadband
Broadcast
Mobility
Public Safety
IoT
Automotive
E-Health
Smart City Ecosystem
Radio: Spectral Efficiency
Virtualization: Energy Efficiency
Advanced test equipment bridging between radio & virtualization
Both capacity and power consumption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

THE TRIANGLE OF 5G USE CASES

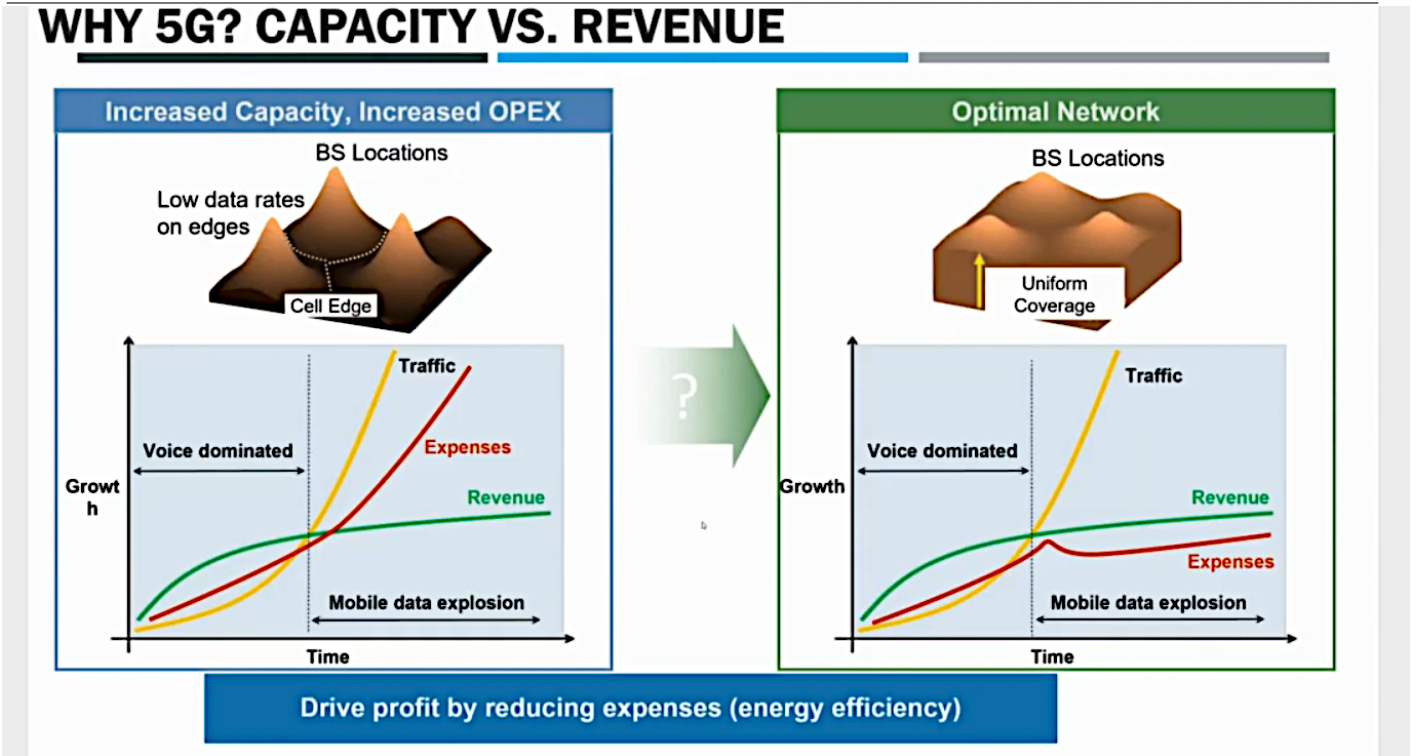
EMBB REMAINS PRIORITY 1, BUT URLLC OPENS NEW MARKETS!







December 13, 2022

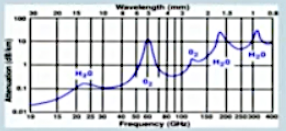

WHY 5G? CAPACITY VS. REVENUE
Increased Capacity, Increased OPEX
BS Locations
Low data rates on edges
Cell Edge
Growth
Traffic
Voice dominated
Expenses
Revenue
Mobile data explosion
Time
?
Optimal Network
BS Locations
Uniform Coverage
Growth
Traffic
Voice dominated
Revenue
Expenses
Mobile data explosion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

5G KEY TECHNOLOGY COMPONENTS

NR BUILDS ON FOUR MAIN PILLARS

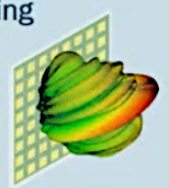
New Spectrum

- < 1GHz
- ~ 3.5 GHz
- ~ 26/28/39 GHz



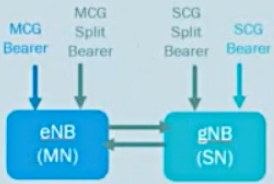
Massive MIMO / Beamforming

- Hybrid beamforming
- > 6GHz also UE is expected to apply beam steering



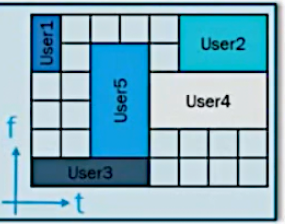
Multi-Connectivity

- Initially based on Dual Connectivity with E-UTRA as master

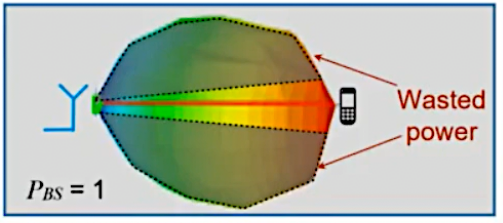


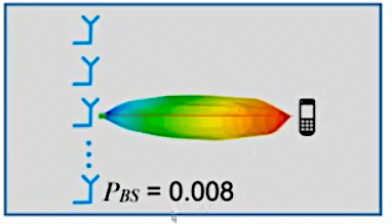
Network Flexibility

- Flexible physical layer numerology
- Network Slicing
- NFV/SDN



ENERGY EFFICIENCY: WHY MASSIVE?





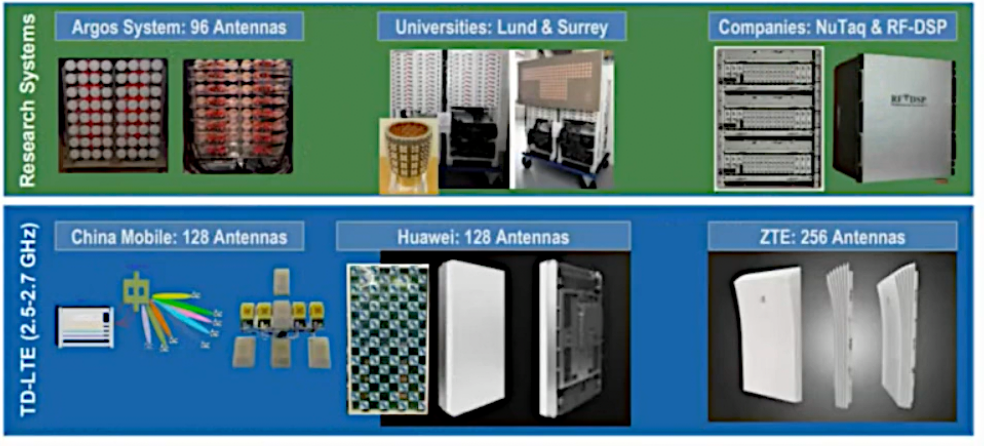
Number of Antennas = 1	
Number of BS transmit antennas (M_t)	1
Normalized output power of antennas	$P_{ant} = \frac{1}{M_t} = 1$
Normalized output power of base station	$P_{total} = \sum_{i=1}^{M_t} P_{ant}{}^{i} = 1$

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

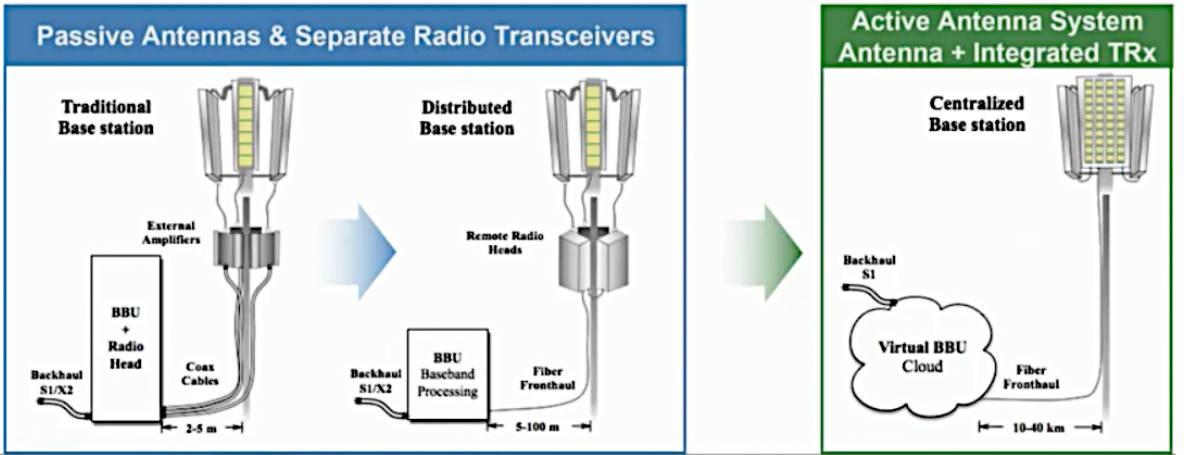
Source: IEEE Signal Processing Magazine, Jan 2013

Improve energy efficiency: more antennas

HARDWARE PERSPECTIVE: MASSIVE MIMO = BEAMFORMING + MIMO

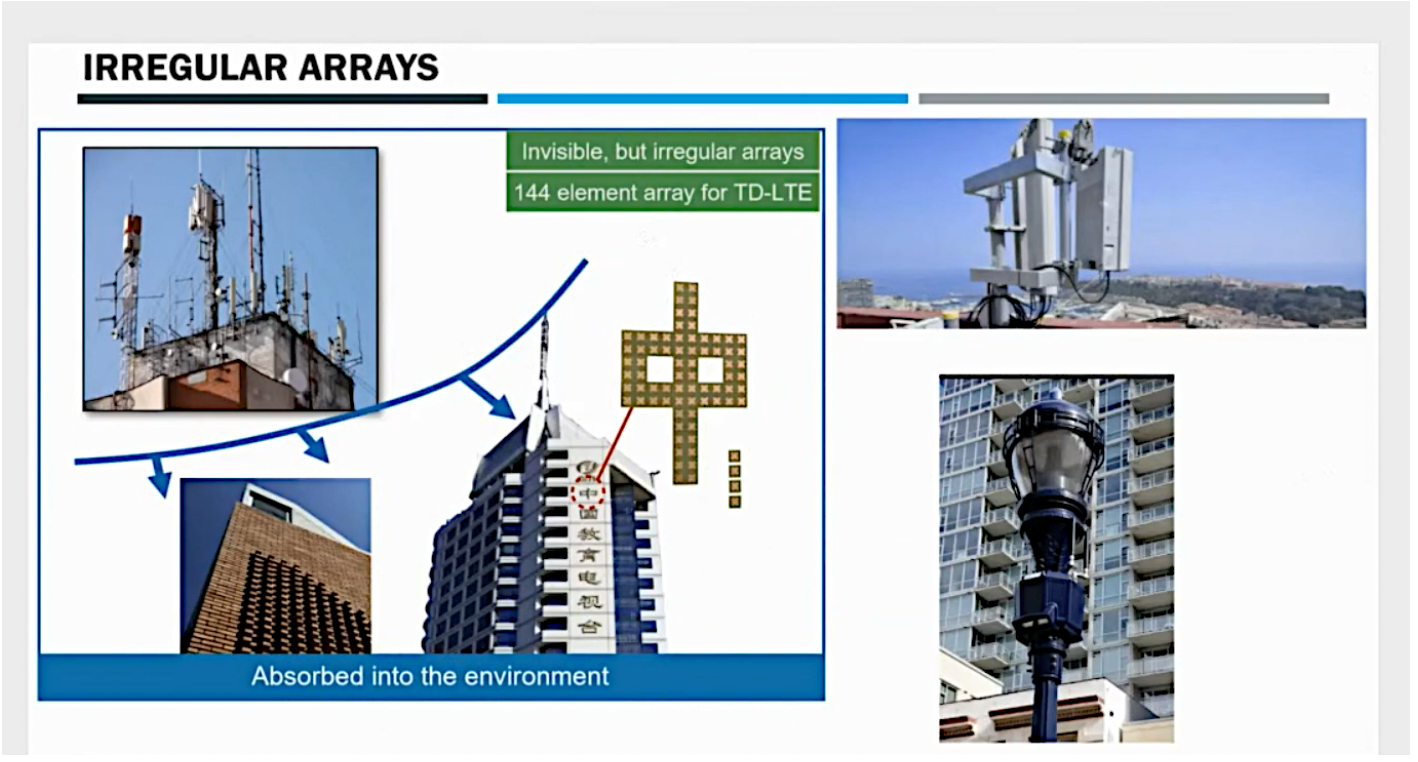


CELLULAR INFRASTRUCTURE EVOLUTION TO 5G

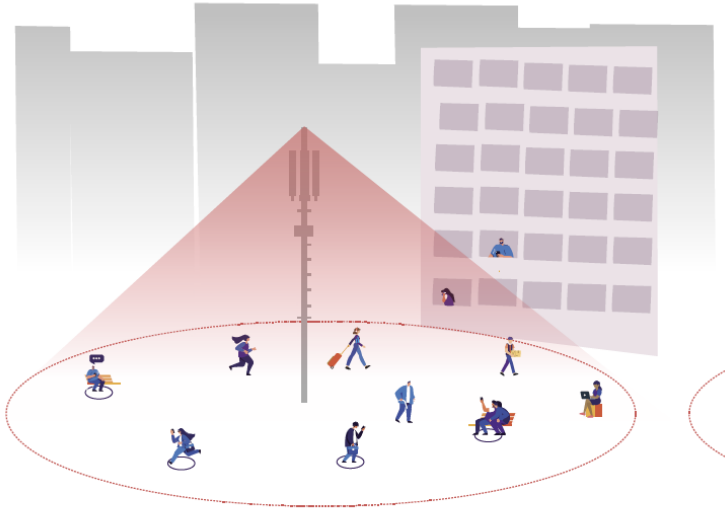


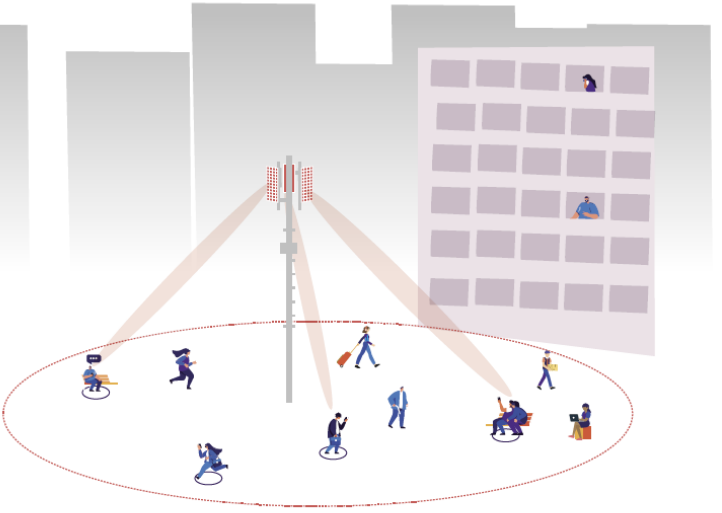
Traditional: 1G & 2G	Distributed: 3G & 4G	Centralized: 4.5G & 5G
0.45 to 1.9 GHz	0.7 to 3.6 GHz	3.4 to 6 GHz & 20 to 60 GHz
8 dual-polarized antennas	8+ dual-polarized passive antennas	128 to 512 active antennas
Peak data rate: 114 kbps	Peak data rate: 150 Mbps	Peak data rate: 10 Gbps

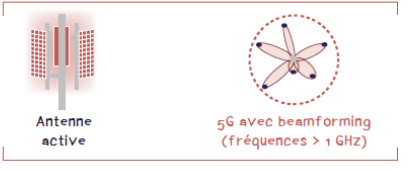
Massive MIMO: Requires new T&M paradigms


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 :

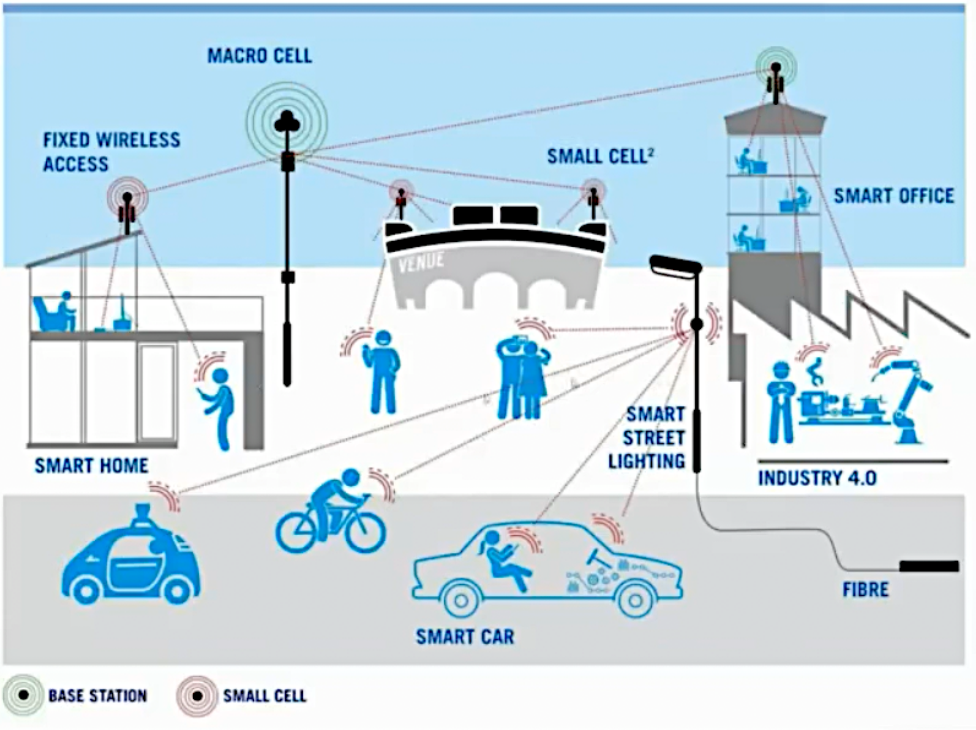
$\Longrightarrow$ Plus de multiplexage spatial ;

$\Longrightarrow$ 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

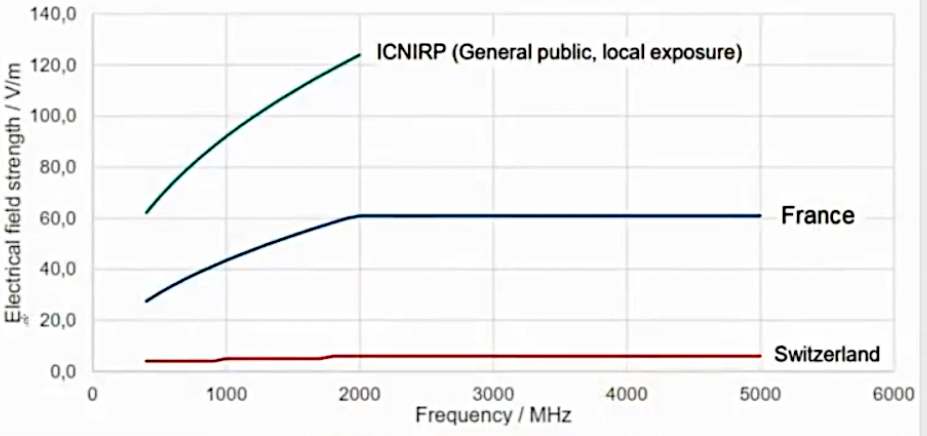
Reference:

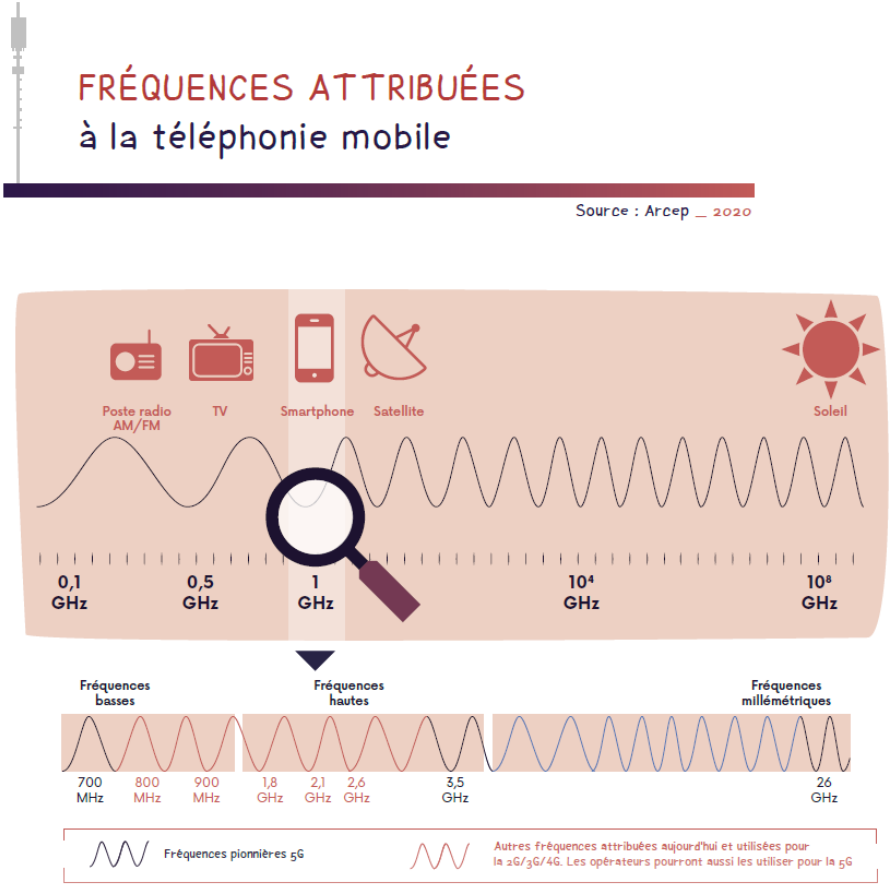
Guidelines for Limiting Exposure to Electromagnetic Fields (100 kHz to 300 GHz)

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	★★	★★	★★

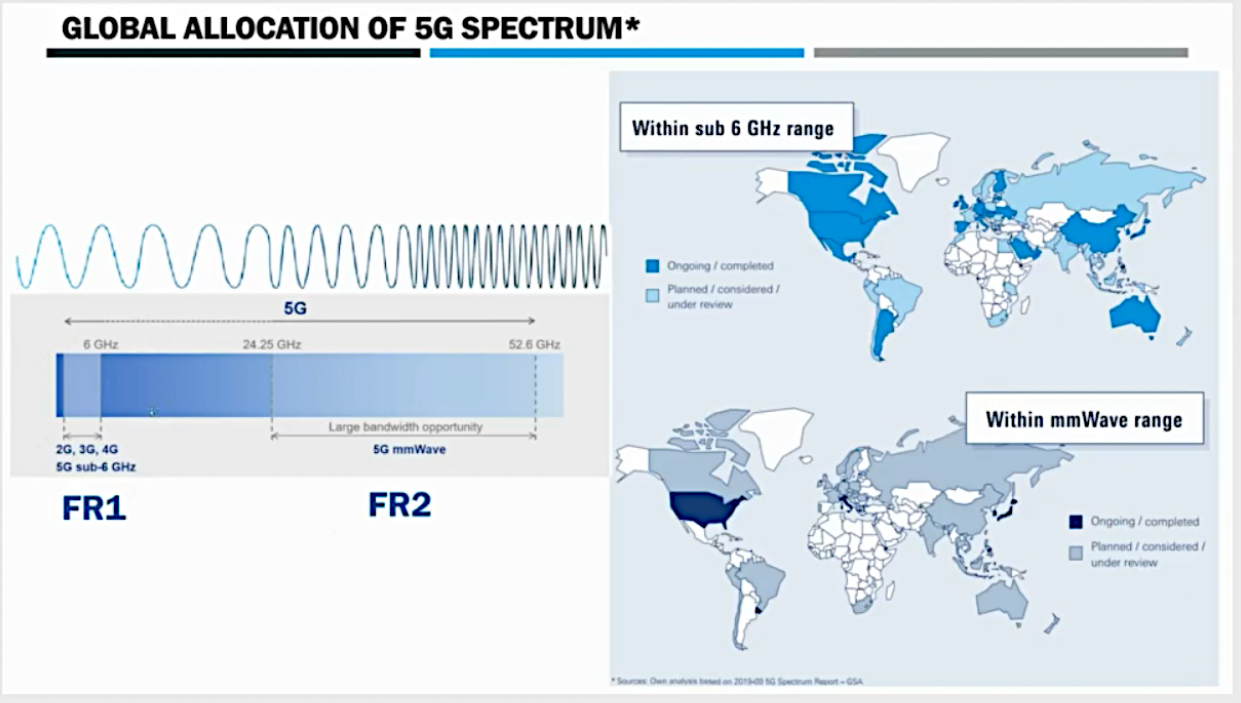
La 5G : les fréquences pionnières

LES FRÉQUENCES
Les bandes pionnières de la 5G

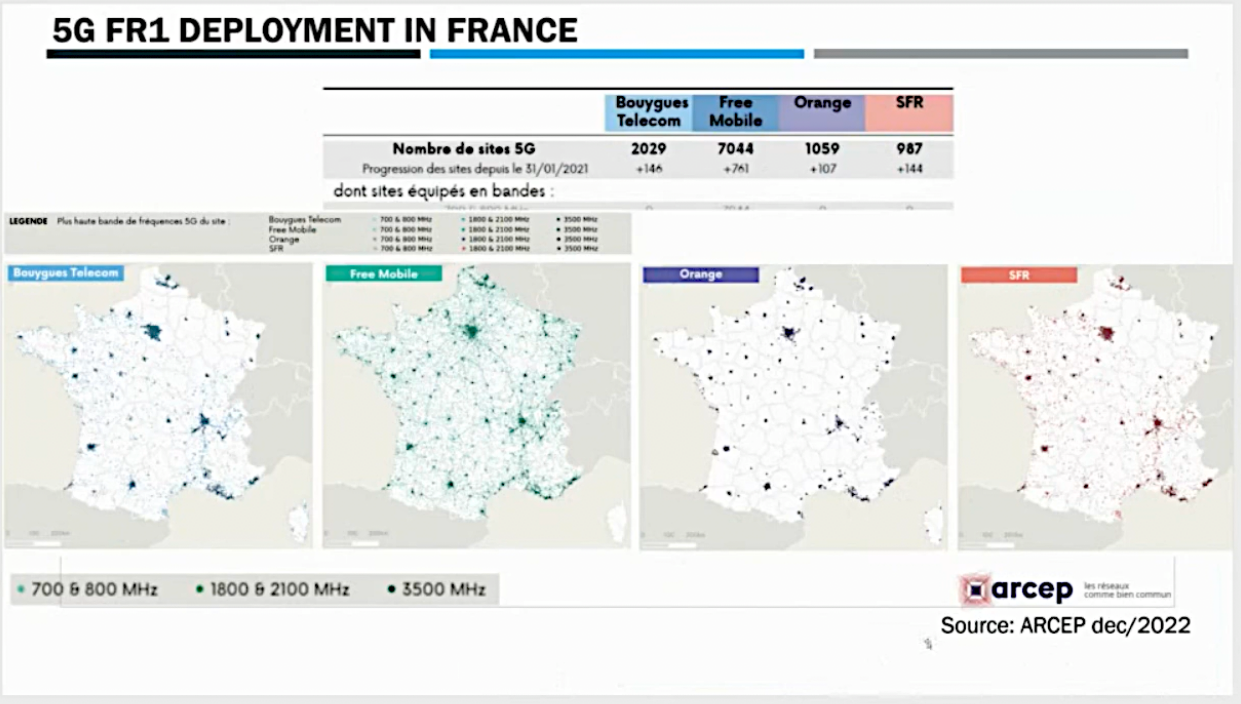
Source : Arcep _ 2020

	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	★	★	★★★★

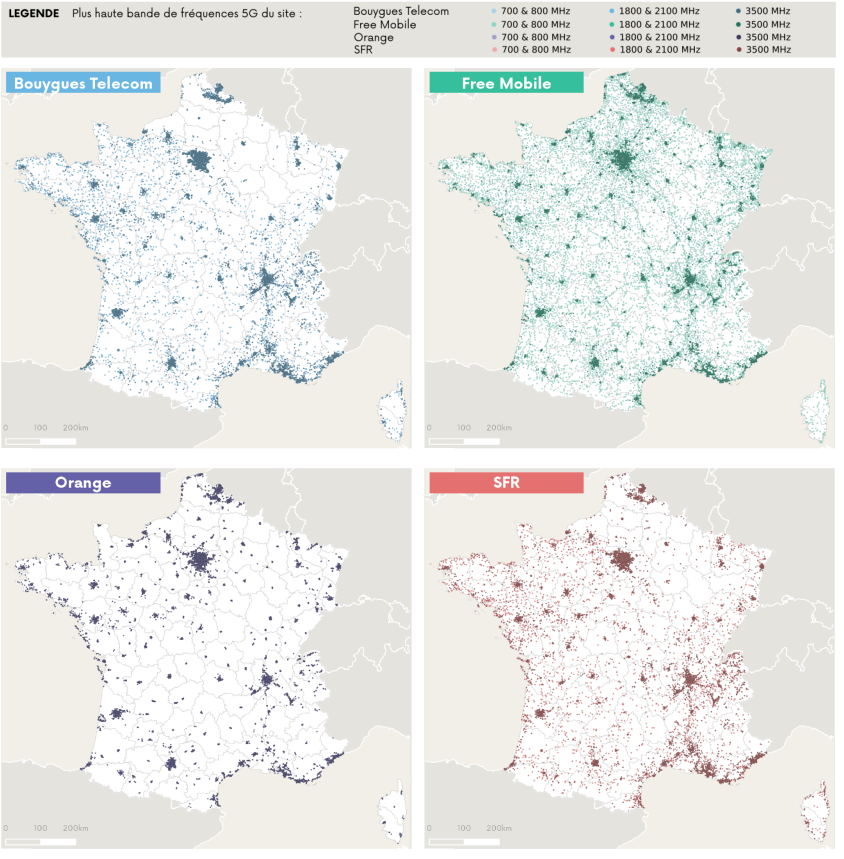
La 5G : allocation de nouvelles fréquences et récupération des anciennes



La 5G : les différents opérateurs français



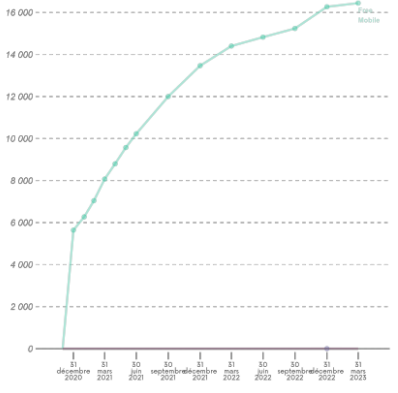
La 5G : les différents opérateurs



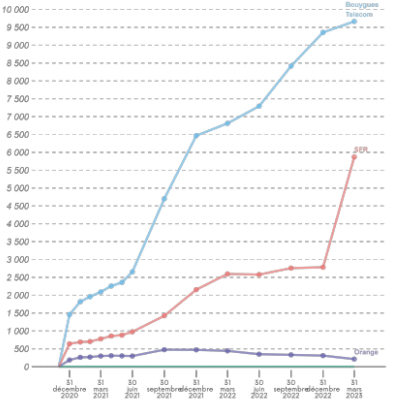
La 5G : les différents opérateurs

	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**

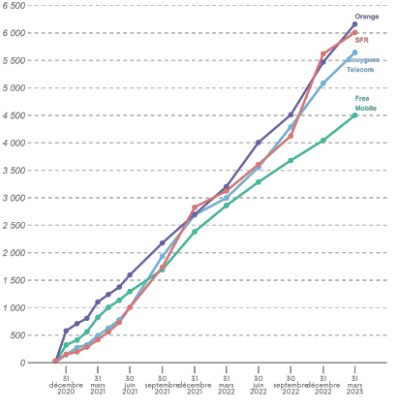
Bandes de tréquences basses :
700 & 800 MHz



Bandes de tréquences moyennes :
1800 & 2100 Mhz



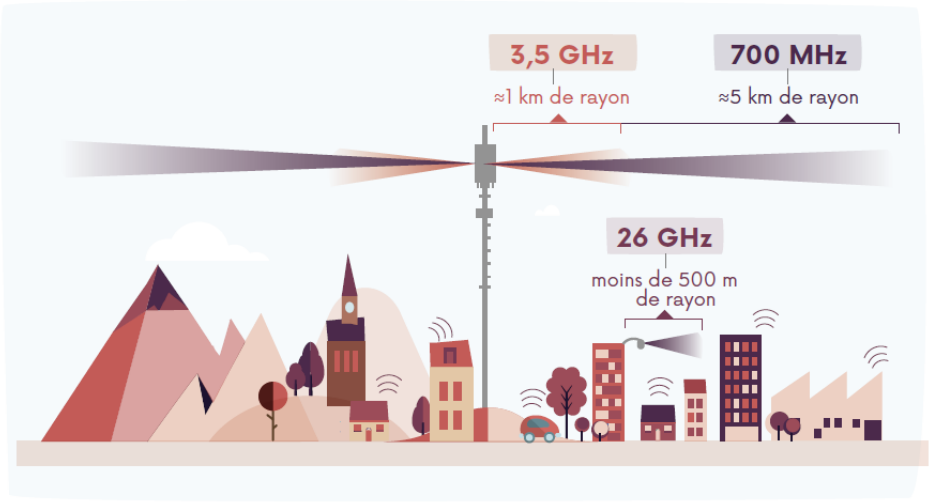
Bande de tréquences hautes :
3500 Mhz



Portée radio des différentes fréquences

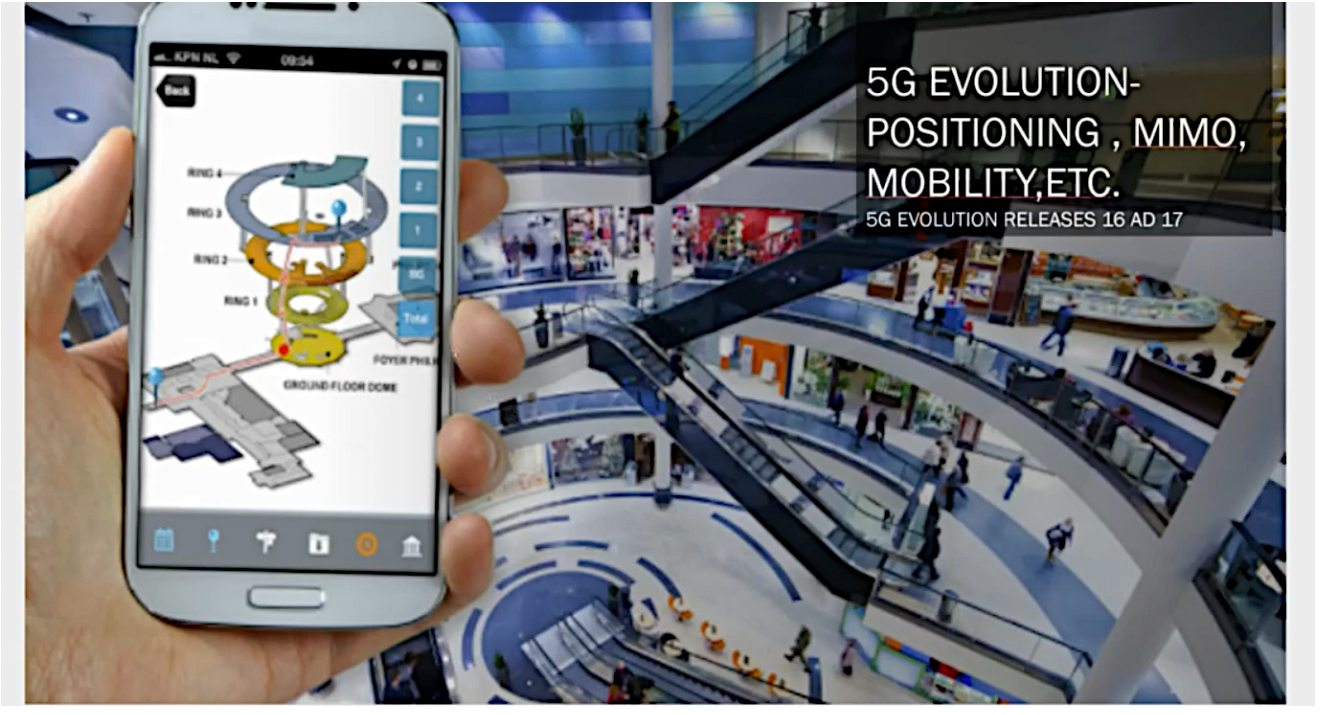
5G
la portée des 3 bandes

Source : Arcep _ 2020



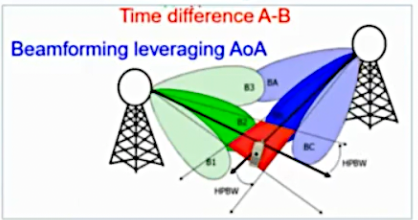
Les différentes fréquences pionnières et le «*beamforming*»

Fréquences		Pénétration à l'intérieur	Portée	Débit	Attribution aux opérateurs	Beamforming
700 MHz	Déjà attribuée aux opérateurs depuis 2015, elle est pleinement disponible depuis mi-2019	★★★★	★★★★	★	✓	✗
3,5 GHz	Elle offre un bon ratio couverture/débit et est souvent identifiée comme la bande "cœur 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	★	★	★★★★	✗	✓

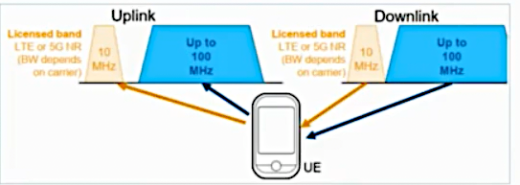

5G EVOLUTION-
POSITIONING , MIMO,
MOBILITY,ETC.
5G EVOLUTION RELEASES 16 AD 17

5G EVOLUTION – POSITIONING, MIMO, MOBILITY, ETC.

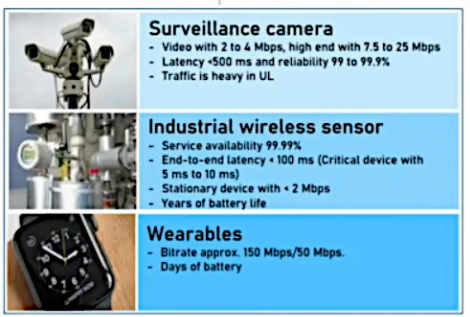
Positioning



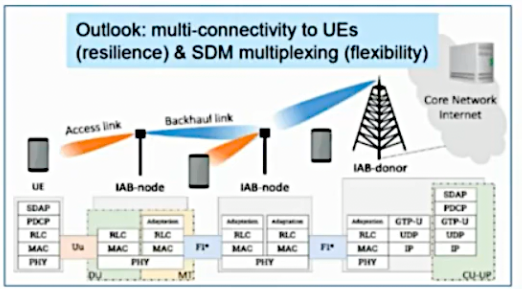
5G NR IN UNLICENSED SPECTRUM (NR-U)



5G NR light



NR INTEGRATED ACCESS AND BACKHAUL (IAB)




INDUSTRIAL IOT
5G EVOLUTION RELEASES 16 AD 17

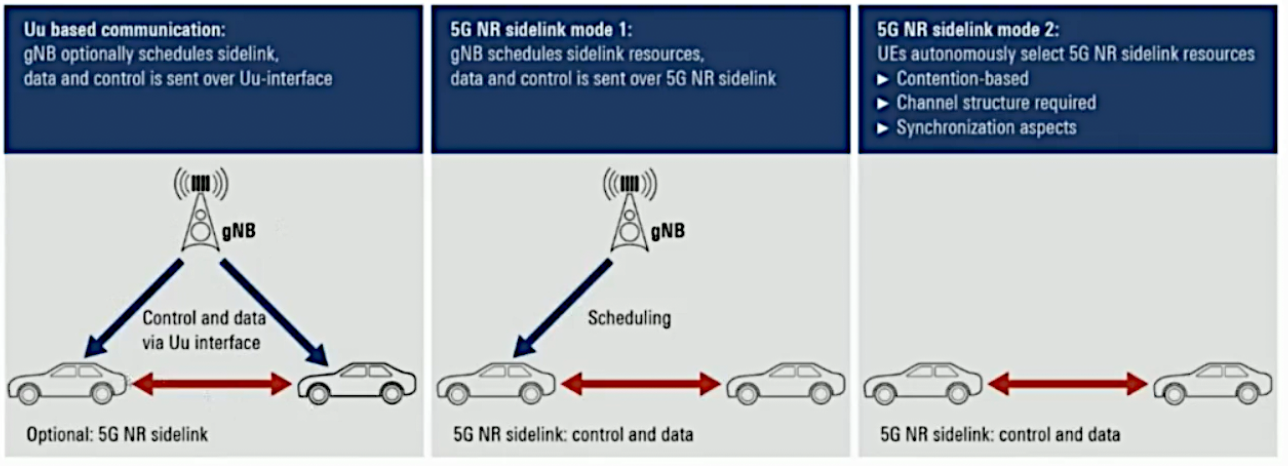
INDUSTRIAL IOT

How can we reduce network delays?
5G URLLC approach

Traffic prioritization by QoS and network virtualization	Short symbol times, min-slots, semi-persistent scheduling	High speed data connection leveraging more bandwidth	Local processing, by edge/fog computing, non-public networks


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

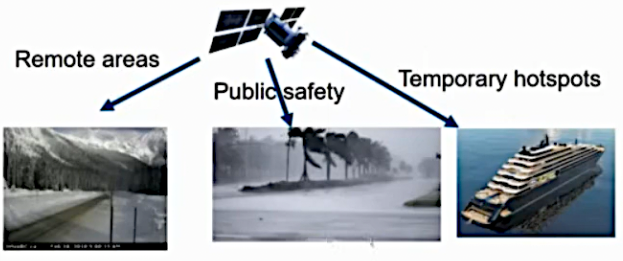


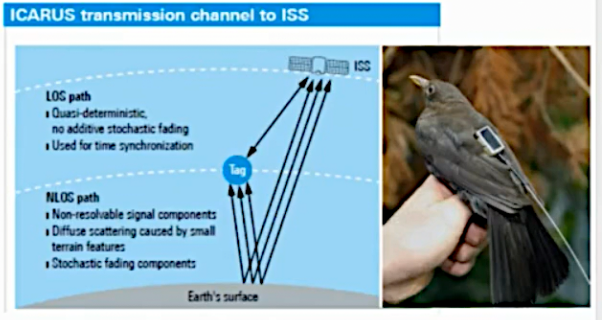

NON-TERRESTRIAL
NETWORKS
5G EVOLUTION, RELEASES 16 AND 17

NON TERRESTRIAL NETWORK APPLICATIONS

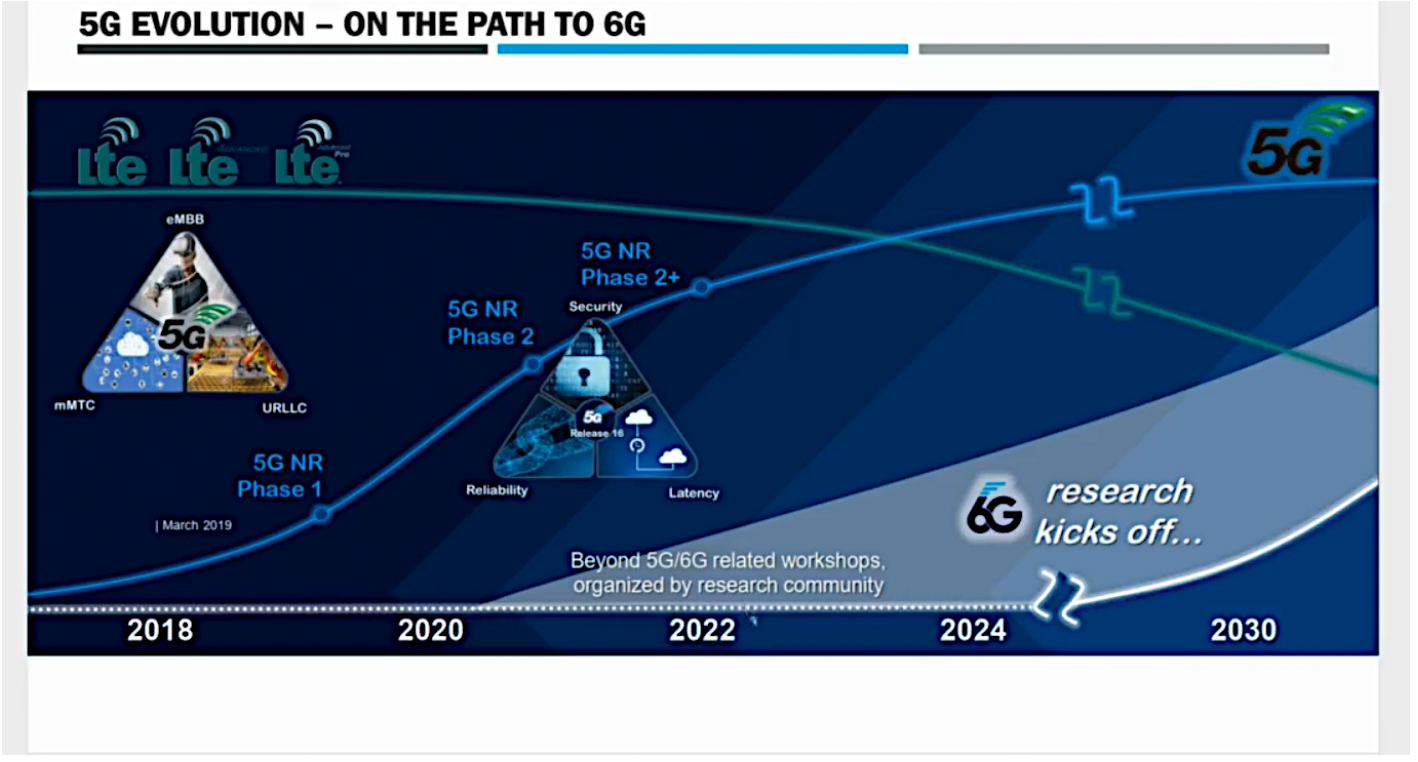
3GPP: NR over NTN
5G NR air interface adopted to NTN
GEO, LEO, HAPS -> air to ground
Fixed or moving terrestrial cells
UE support GNSS + NTN
Business case: human: eMBB

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

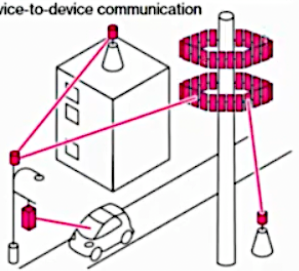
5G EVOLUTION – ON THE PATH TO 6G

5G

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

Small base stations extend reach and handle some exchanges directly

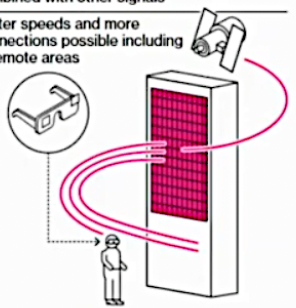
Device-to-device communication



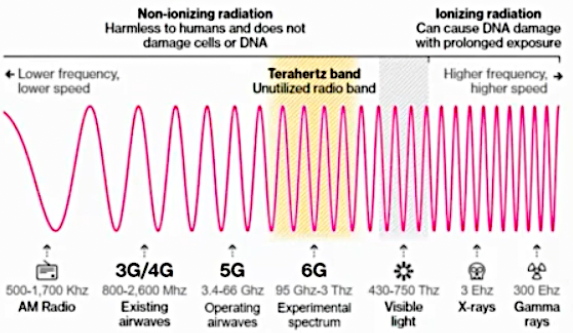
6G

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

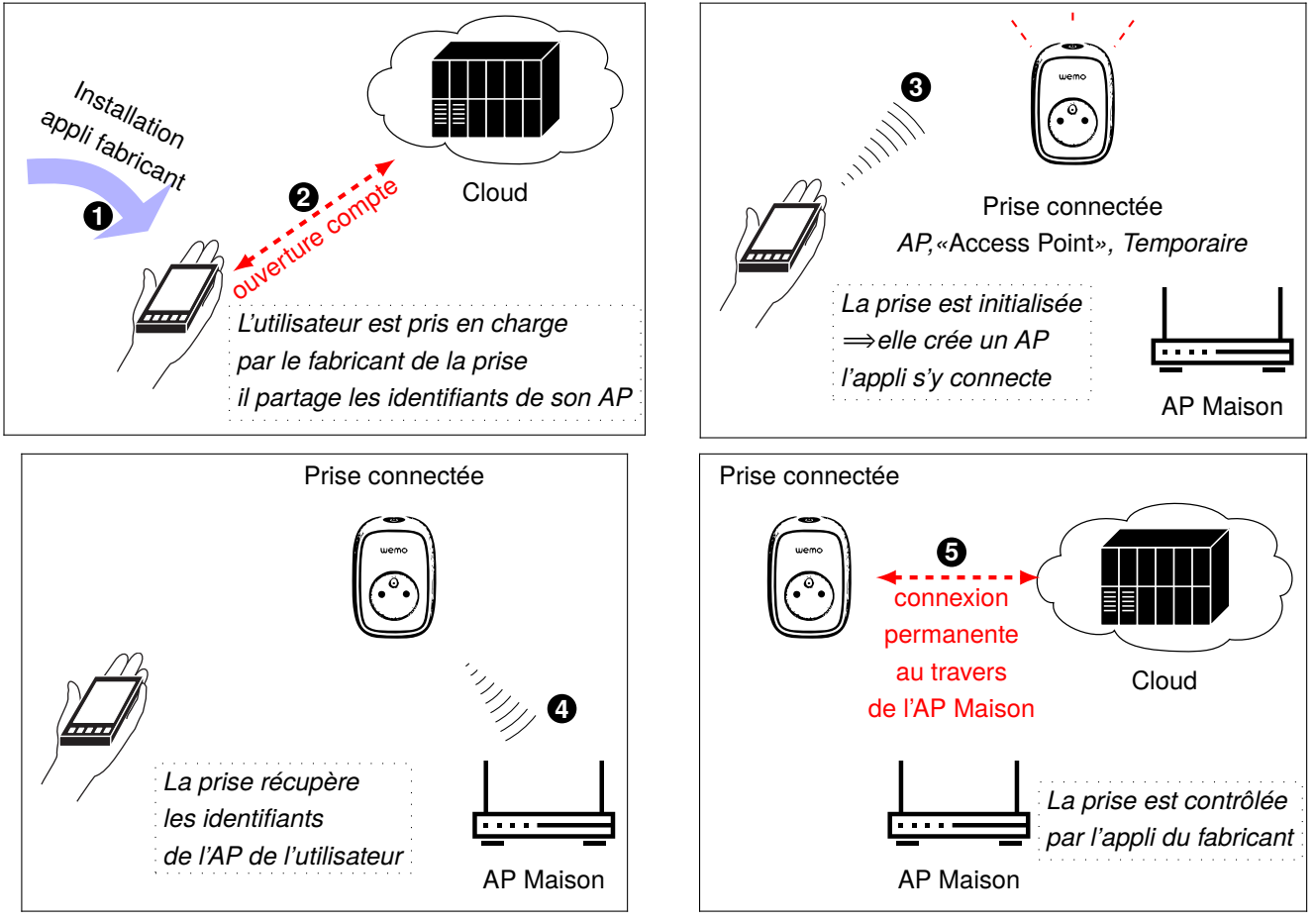
Reflective surfaces may help transmit terahertz signals that don't travel very far

Experimental Band

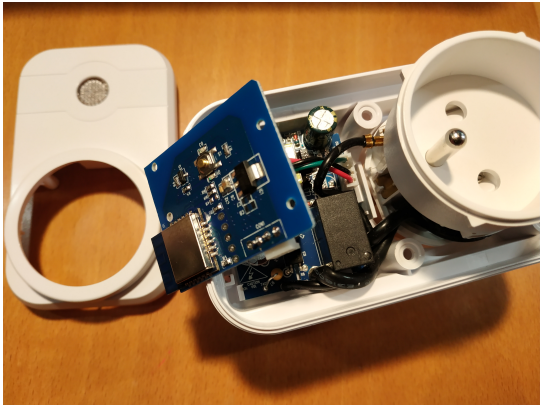
Terahertz waves could meet 6G's speed, latency requirements

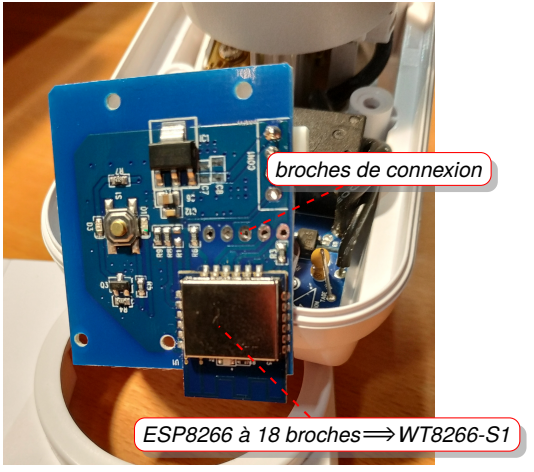
Accès physique à un IoT
Récupération des secrets de sécurité

Scénario de l'intégration d'une prise connectée à la maison



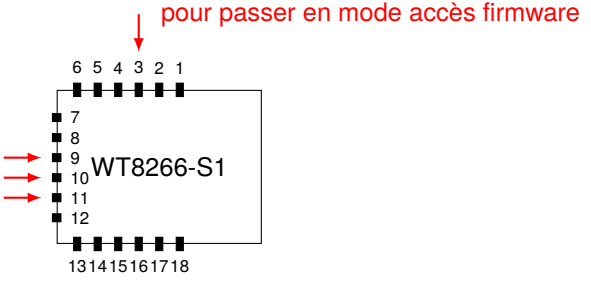
Récupération du firmware : recherche d'un port série, «*UART*»





Identifier les broches du WT8266-S1 à l'aide d'un multimètre et de la doc constructeur

Pin	Info
3	IO0
9	URXD
10	GND
11	UTXD



Pour récupérer le firmware présent dans la mémoire flash de 16Mb ou 2MB avec un adaptateur USB/série :

xterm

```
$ esptool.py --port /dev/ttyUSB0 read_flash 0x00000 0x200000 tuya.bin
```

Récupération du firmware : communication par le port série, «*UART*»

Une fois le firmware récupéré, on peut regarder ce qu'il contient :

xterm

```
$ strings tuya.bin | less
http://a.gw.tuyaeu.com/gw.json
http://a.gw.tuyaus.com/gw.json
...
mq.gw.airtakeapp.com
mq.gw1.airtakeapp.com
...
mqtt_client.c
...
ESP.ty_ws_mod.dev_ap_ssid_key={"ap_ssid":"SmartLife","ap_pwd":null}
ESP.ty_ws_mod.gw_active_key={"token":null,"key":null,"lo
cal_key":null,"http_url":null,"mq_url":null,"mq_url_bak":null,"timeZone":null,"re
gion":null,"reg_key":null,"wxappid":null,"uid_acl":null}
ESP.ty_ws_mod.dev_if_rec_key={"id":"04200063b4e62d00468a","sw_ver":"1.0.0","sche
ma_id":null,"etag":null,"product_key":"n8iVBAPLFKAAAszH","ability":0,"bind":false,"sync":false}
ESP.ty_ws_mod.wf_nw_rec_key={"ssid":null,"passwd":null,"wk_mode":0,"mode":0,"type":0,"source":0,
"path":0,"time":0,"random":0}
ESP.ty_ws_mod.gw_sw_ver_key={"sw_ver":"1.0.0","bs_ver":"5.06","pt_ver":"2.1"}
:ESP.device_mod.dp_data_key={"relay_switch":false,"switch":true,"work_mode":1,"bright":180,"tem
per":255,"colour_data":"1900000000ff19","scene_data":"00ff0000000000","rouguang_scene_da
ta":"ffff500100ff00","binfeng_scene_data":"ffff8003ff000000ff000000ff00000000000000000","xuan
cai_scene_data":"ffff5001ff0000","banlan_scene_da
ta":"ffff0505ff000000ff00ffff00ff00ff0000ff000000"}
ESP.device_mod.fsw_cnt_key={"fsw_cnt_key":0}
ESP.device_mod.appt_posix_key={"appt_posix":0}
ESP.device_mod.power_stat_key={"power":0}
{"mac":"68a","prod_idx":"04200063","auz_key":"TJJ7AGs644QGICVFovUcpeVeGz0JTbR1","prod_test":false}
```

l'URL de la requête

un FQDN

une bibliothèque utilisée

le SSID et le mot de passe non encore renseigné

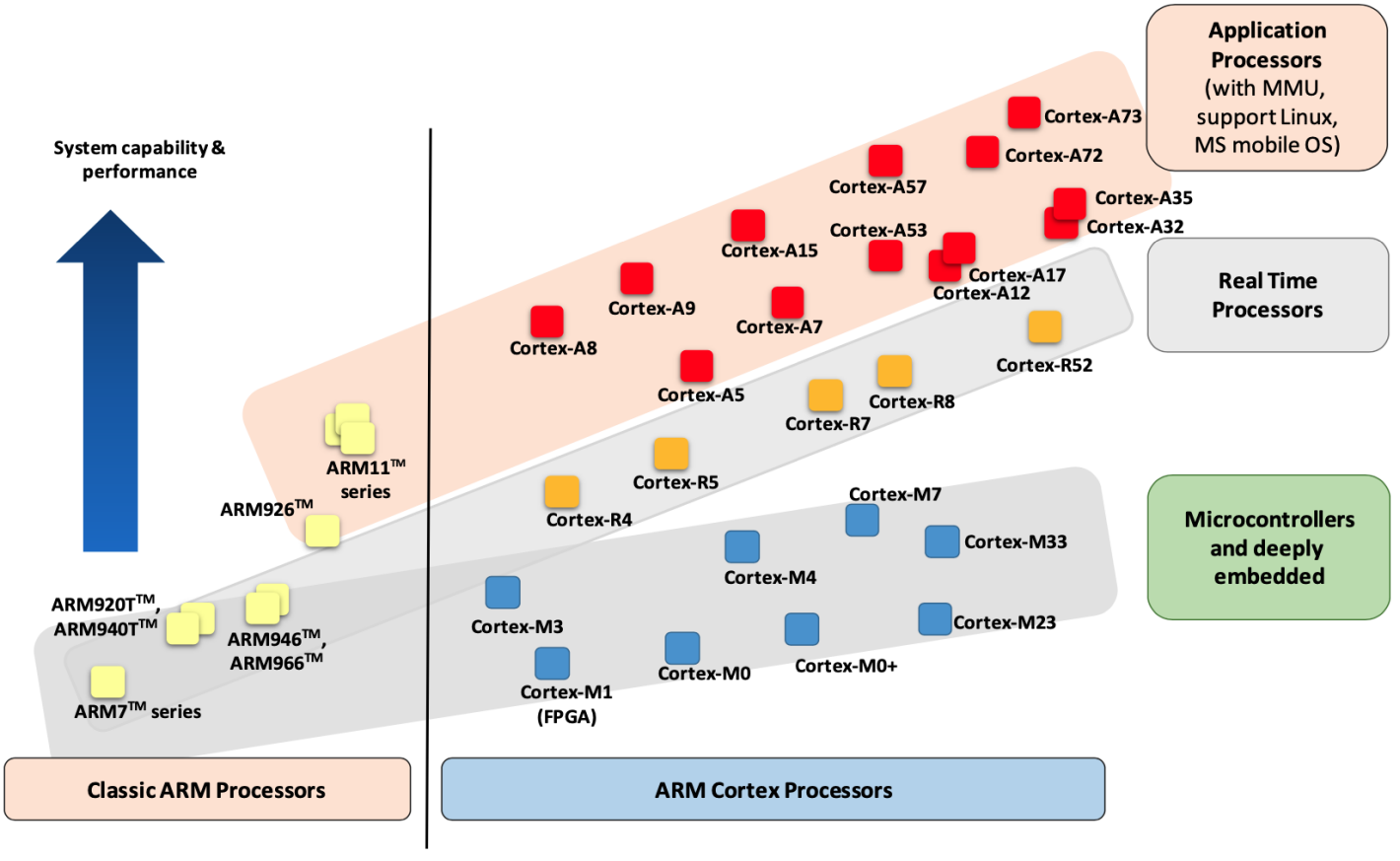
une clé produit

une clé d'API

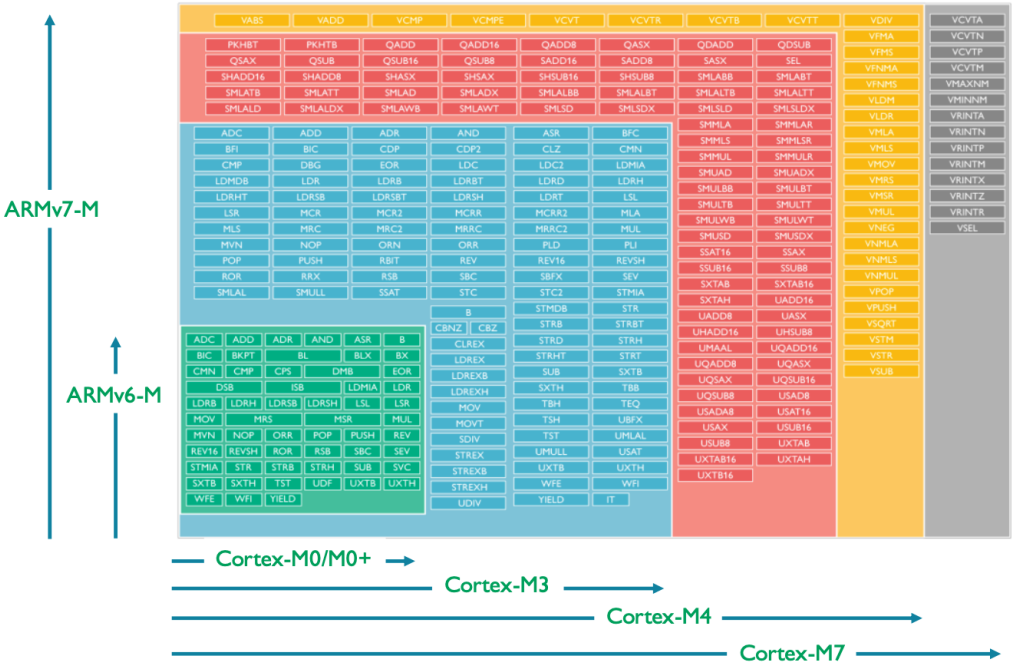
xterm

```
$ dig +short mq.gw.airtakeapp.com
120.55.106.107
$ curl http://a.gw.tuyaus.com/gw.json
{"t":1537555117,"e":false,"success":false,"errorCode":"API_EMPTY","errorMsg":"API"}
```

ARM Cortex et ISA



ARM Cortex et ISA



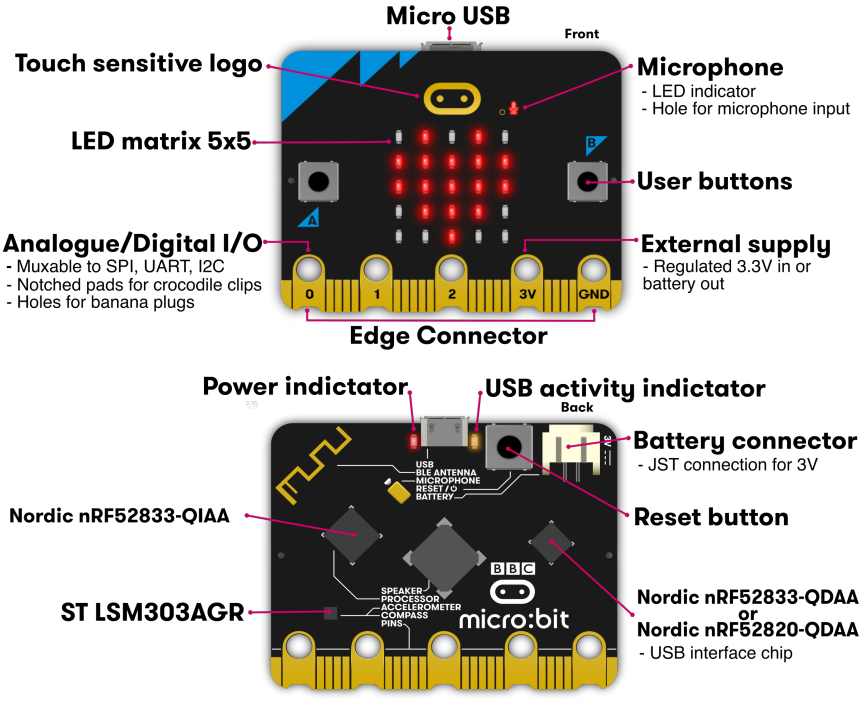
Floating Point

DSP (SIMD, fast MAC)

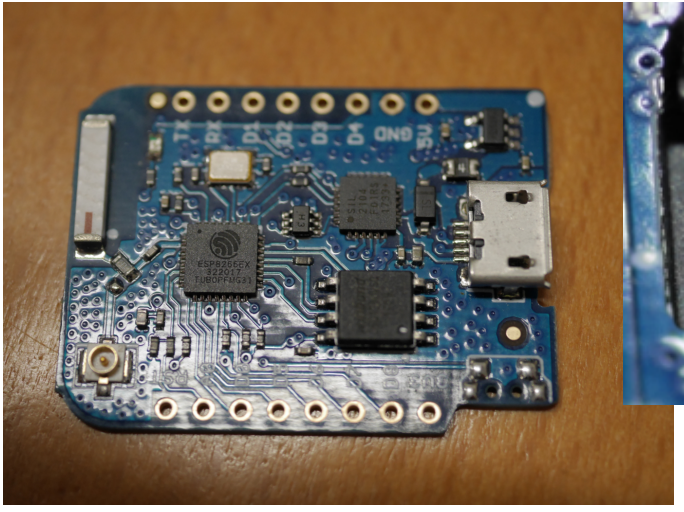
Advanced data processing
bit field manipulations

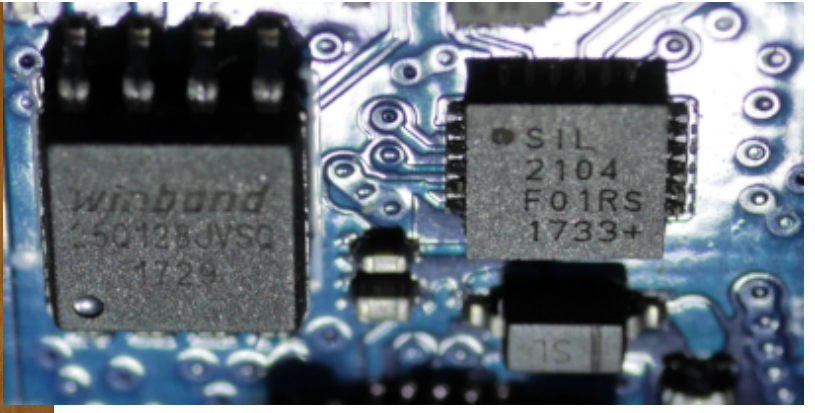
General data processing
I/O control tasks

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

Récupération directe du Firmware par lecture de la mémoire flash



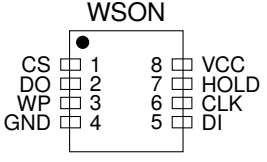


On peut lire la référence du composant mémoire :
Winbond 25Q128JVSQ

On peut récupérer la documentation à :

`https://www.winbond.com/resource-files/W25Q128JV%20RevI%2008232021%20Plus.pdf`

On obtient la description des broches du composant :



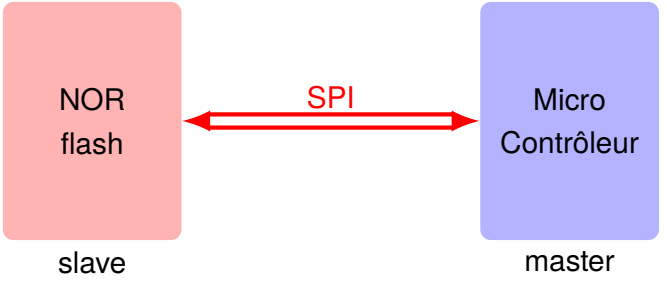
Ce qui permet de le connecter au **Bus Pirate**.

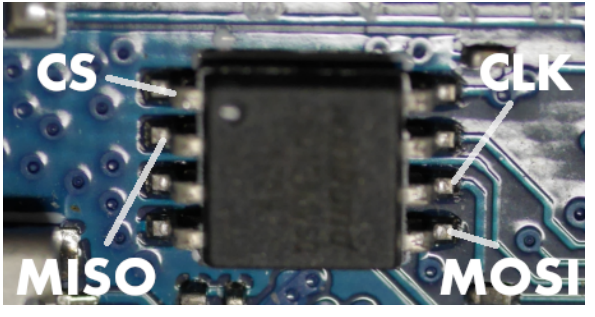
WSON	Bus Pirate
VCC	3.3v
GND	GND
CS	CS
CLK	CLK
DO	MISO
DI	MOSI

Récupération directe du Firmware par lecture de la mémoire flash

NOR Flash : mémoire accessible par SPI

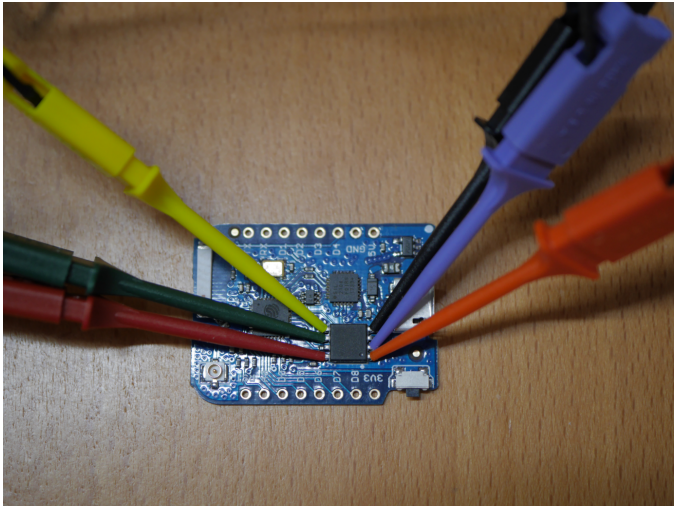
- Support de stockage pour données **non volatiles** : les données restent dans le composant jusqu'à ce qu'elles soient réécrites et elles sont conservées même si le circuit embarqué est éteint ;
- Les données peuvent être lues **octet par octet** : avec de la mémoire NAND, on ne peut lire qu'un, dix ou 100 octets à la fois : par page de 4096 ;
- Mémoire **sans défaut** : pas de système de correction d'erreur nécessaire contrairement à la mémoire de type NAND ;
- **faible latence** d'accès : utilisable pour l'exécution directe de code ;
- utilisée en général pour stocker des données en faible quantités ;
- communication par le bus SPI : communication **synchrone**, **full duplex** avec 4 signaux : CS, CLK, MISO et MOSI.

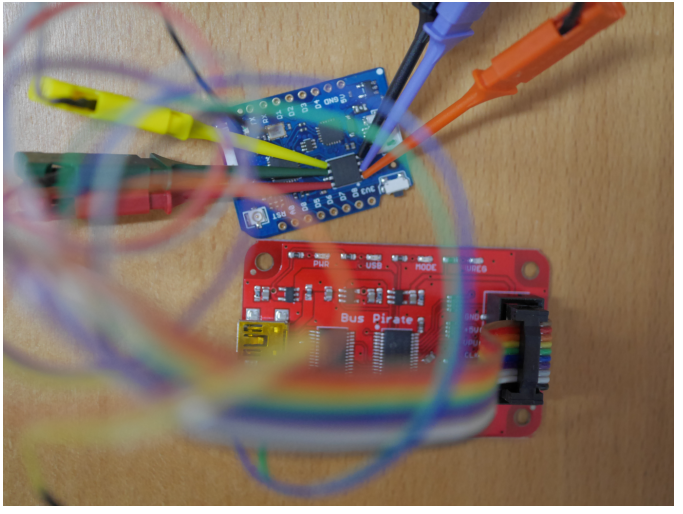




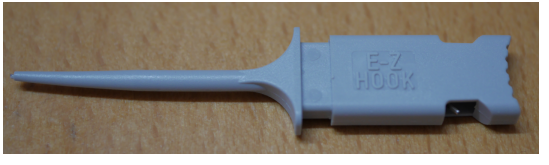
Récupération directe du Firmware par lecture de la mémoire flash

On utilise des sondes, «*probes*» pour se connecter à chaque broche du composant mémoire :





Chacune de ces sondes est reliées au **Bus Pirate**.



Le **Bus Pirate** est un circuit opensource qui permet :

- ▷ d'alimenter le composant à tester en 3,3v ou 5v ;
- ▷ de disposer d'une interface USB/série ;
- ▷ de disposer d'un **micro-contrôleur** dédié à :
  - ◇ lire des **ordres** en provenance de la machine de l'utilisateur par l'intermédiaire du port série simulé par USB ;
  - ◇ **interpréter** ces ordres avec un firmware spécialisé opensource ;
  - ◇ de gérer **différents protocoles de communication** inter-composants : I2C, SPI, 1-Wire, ... ;
  - ◇ **d'envoyer et recevoir des données** du protocole choisi sur des broches connectées au composant à tester ;
- ▷ *Ici, on va utiliser le bus SPI pour communiquer avec le composant mémoire.*

Récupération directe du Firmware par lecture de la mémoire flash

Utilisation de l'outil `flashrom`

xterm

```
$ flashrom -p buspirate_spi:dev=/dev/ttyUSB0,spispeed=1M
flashrom v1.2 on Linux 5.15.0-47-generic (x86_64)
flashrom is free software, get the source code at https://flashrom.org

Using clock_gettime for delay loops (clk_id: 1, resolution: 1ns).
No EEPROM/flash device found.
Note: flashrom can never write if the flash chip isn't found automatically.
```

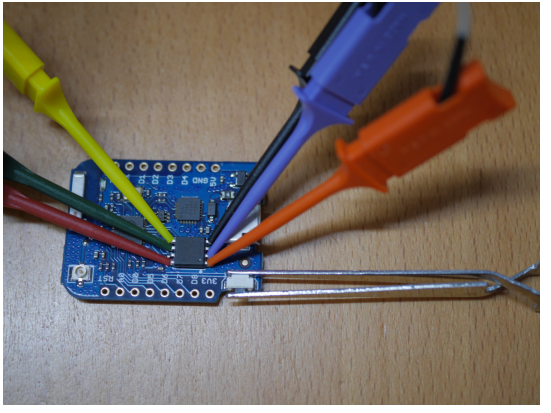
Il y a un **conflit d'accès** au composant mémoire :

- le processeur accède à la mémoire pour **exécuter le firmware** ;
- le Bus Pirate accède à la mémoire pour **l'identifier**.

$\Longrightarrow$ il faut **bloquer le processeur** en le maintenant dans l'état RESET !

*Heureusement, sur la carte de développement un **bouton RESET** permet de le faire.*

$\Longrightarrow$On va utiliser une **pince** pour le bloquer.



xterm

```
$ flashrom -p buspirate_spi:dev=/dev/ttyUSB0
flashrom v1.2 on Linux 5.15.0-47-generic (x86_64)
flashrom is free software, get the source code at https://flashrom.org

Using clock_gettime for delay loops (clk_id: 1, resolution: 1ns).
Found Winbond flash chip "W25Q128.V" (16384 kB, SPI) on buspirate_spi.
No operations were specified.
```

Le composant est correctement identifié !

Récupération directe du Firmware par lecture de la mémoire flash

Récupération finale du firmware

xterm

```
$ flashrom -p buspirate_spi:dev=/dev/ttyUSB0 -r dump_esp8266.bin
flashrom v1.2 on Linux 5.15.0-47-generic (x86_64)
flashrom is free software, get the source code at https://flashrom.org

Using clock_gettime for delay loops (clk_id: 1, resolution: 1ns).
Found Winbond flash chip "W25Q128.V" (16384 kB, SPI) on buspirate_spi.
Reading flash... done.
```

Contenu du firmware

xterm

```
$ strings dump_esp8266.bin
...
Access denied
WebREPL connected
>>>
Password:
wH&@wH&@SH&@#H&@#H&@;H&@wH&@
9(@_
...
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept:
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
Sec-WebSocket-Key:
Not a websocket request
Sec-WebSocket-Key
...
Welcome to MicroPython!
For online docs please visit http://docs.micropython.org/en/latest/esp8266/ .
For diagnostic information to include in bug reports execute 'import port_diag'.
Basic WiFi configuration:
```

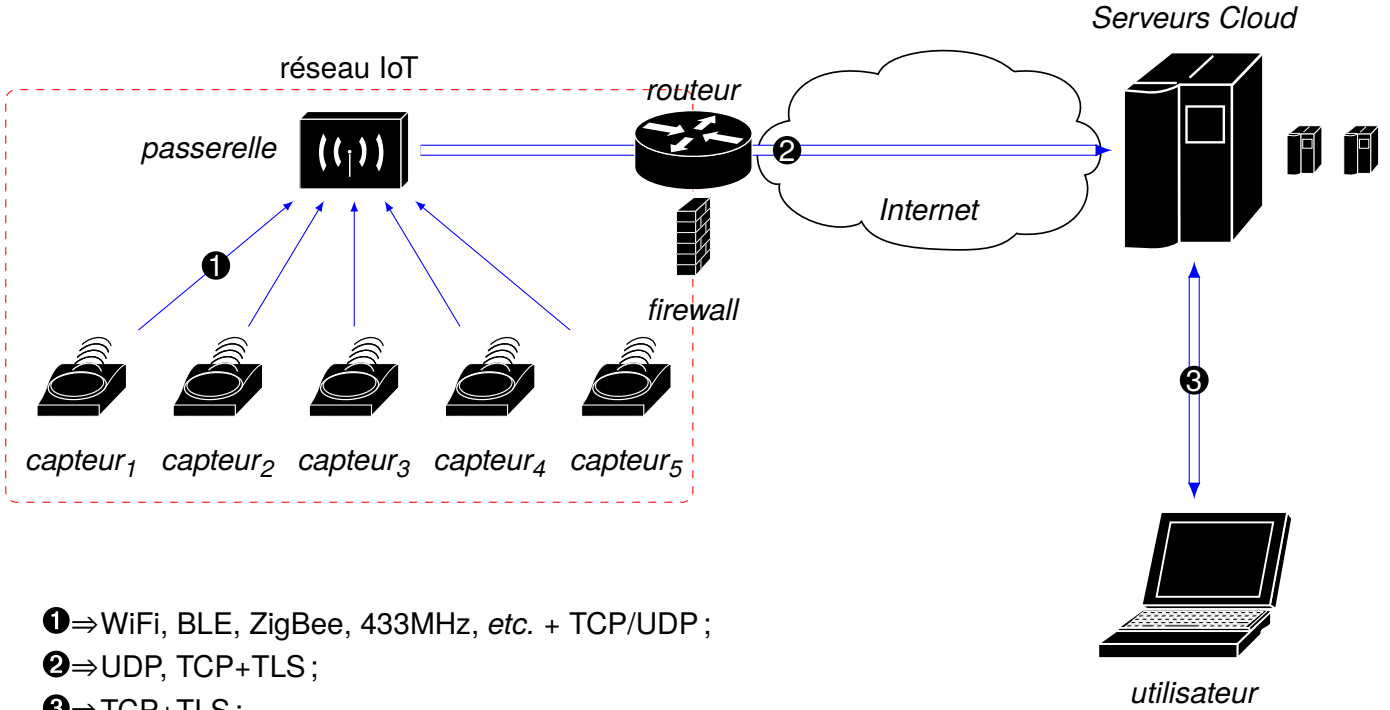
la commande `strings` permet d'extraire les chaînes de caractères

Peut-être un token secret...

Le firmware est basé sur microPython !

Panorama des architectures IoT
et
de la Sécurité associée

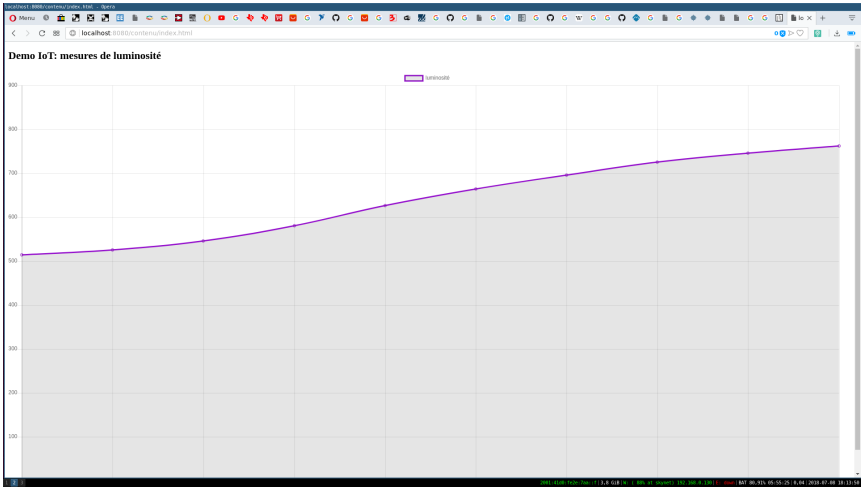
Composition d'une infrastructure IoT



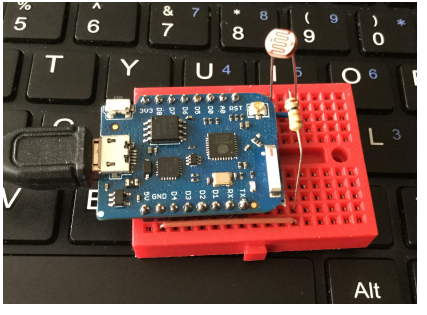
❶⇒WiFi, BLE, ZigBee, 433MHz, *etc.* + TCP/UDP ;
❷⇒UDP, TCP+TLS ;
❸⇒TCP+TLS ;
L'«*application IoT*» est composée :
- de capteurs ;
- d'une composante logicielle hébergée dans le Cloud ;
- d'une passerelle assurant l'aggrégation et la liaison.

Utilisation de la sécurité fournie par la passerelle et d'une liaison basée WiFi

Un serveur exploitant les WebSockets

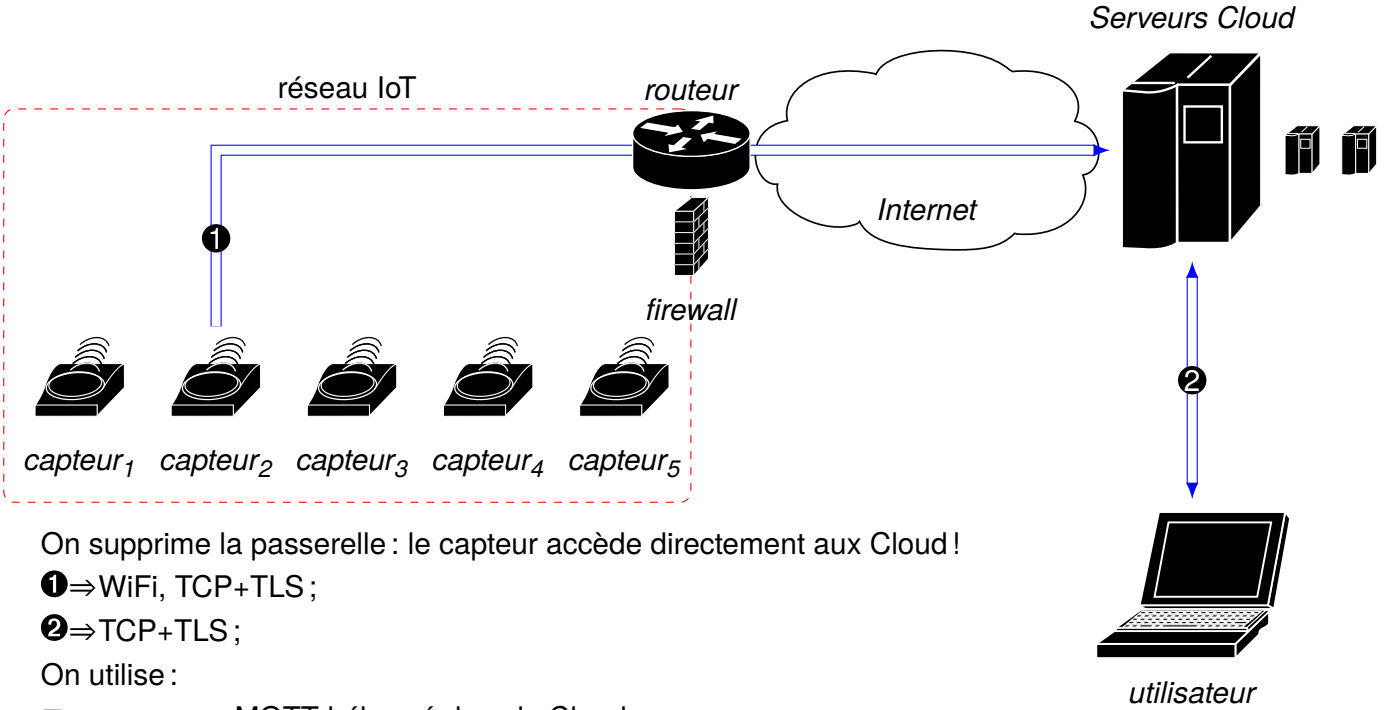


- un navigateur se connecte sur le serveur logiciel tournant sur la passerelle :
  - une liaison permanente est établie basée sur un stream SSE, «*Server Sent Events*» ;
  - il obtient en temps réel les nouvelles valeurs transmises par le capteur ;
  - affiche un graphe des dix dernières valeurs reçus ;
- le capteur réalise périodiquement des requêtes REST vers le serveur logiciel de la passerelle : il envoie la valeur courante de son ADC ;



Code source du serveur disponible sur `https://git.p-fb.net/pef/iot_bottle_sse`

Composition d'une infrastructure IoT avec accès direct capteur/Cloud



On supprime la passerelle : le capteur accède directement aux Cloud !

❶⇒WiFi, TCP+TLS ;

❷⇒TCP+TLS ;

On utilise :

- ☐ un serveur MQTT hébergé dans le Cloud
- ☐ une connexion sécurisée capteur/serveur MQTT avec du TLS ;
- ☐ des **certificats** client et serveur.

Utilisation d'un composant de sécurité dédié pour l'embarqué

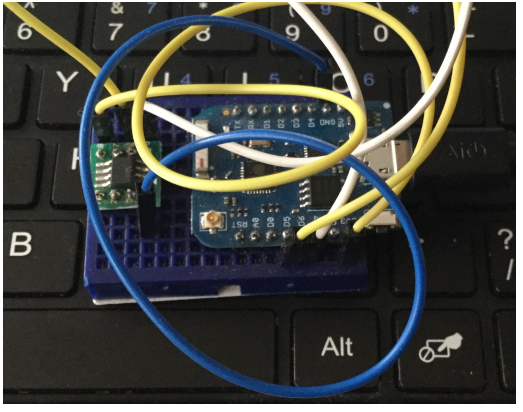
ATECC508A ☆

Status: In Production

View Datasheet

Features:

- Easy way to run ECDSA and ECDH Key Agreement
- ECDH key agreement makes encryption/decryption easy
- Ideal for IoT node security
- Authentication without the need for secure storage in the host
- No requirement for high-speed computing in client devices
- Cryptographic accelerator with Secure Hardware-based Key Storage



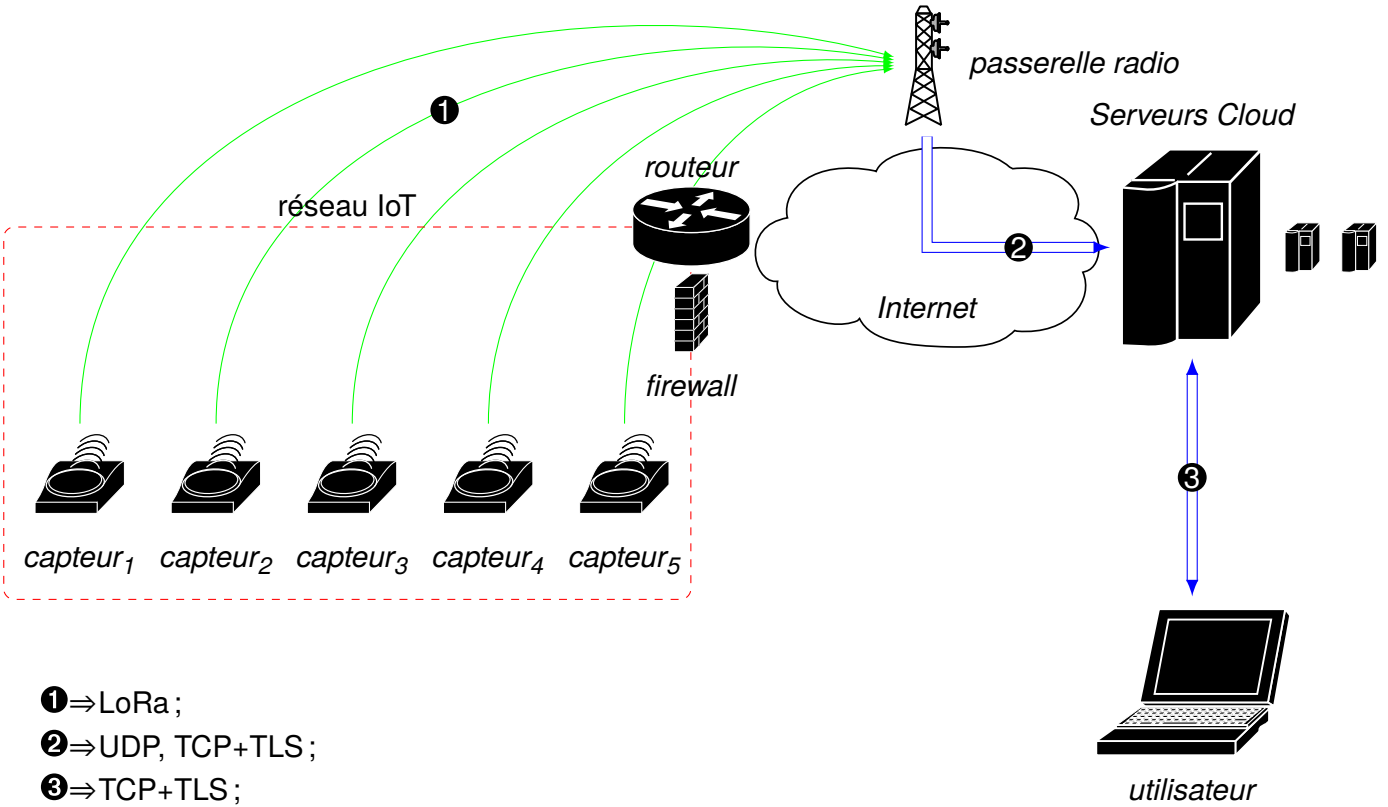
*DH : Diffie-Hellman permet d'assurer la PFS, «*Perfect Forward Secrecy*» : la récupération de la clé privée du capteur ne permet pas de déchiffrer les messages échangés précedemments, elle ne sert qu'à l'authentification, pas pour génerer une clé de session*

Comparaison des différentes technologies de communication radio

Technology	802.11ah	WLAN	ZigBee	LTE-M	Sigfox	LoRa
Sensitivity	-106 dBm	-92 dBm	-100 dBm	-117 dBm	-126 dBm	-134 dBm
Link Budget	126 dB	112 dB	108 dB	147 dB	146 dB	154 dB
Range (O=Outdoor, I=Indoor)	O: 700m I: 100m	O: 200m I: 30m	O: 150m I: 30m	1.7km urban 20km rural	2km urban 20km rural	3km urban 30km rural
Data rate	100kbps	6 Mbps	250 kbps	1 Mbps	600 bps	12.5 – 0.970 kbps
Tx current consumption	300 mA 20 dBm	350 mA 20 dBm	35 mA 8 dBm	800 mA 30 dBm	120 mA 20 dBm	120 mA 20 dBm
Standby current	NC	NC	0.003mA	3.5mA	0.001mA	0.001mA
RX current	50 mA	70 mA	26 mA	50 mA	10 mA	10 mA
Battery life 2000 mAh				18 months	90 months	105 months
Localization	no	1- 5m	no	200m	no	10-20m
Interference Immunity	moderate	moderate	bad	moderate	bad	good
Network Type	Star	Star	Mesh	Star	Star	Star
End Node Capacity	Large	Medium	Small		>1.3Mu*	>1.3Mu*

(*) One message per day

Composition d'une infrastructure IoT avec LoRa



❶⇒LoRa ;
❷⇒UDP, TCP+TLS ;
❸⇒TCP+TLS ;

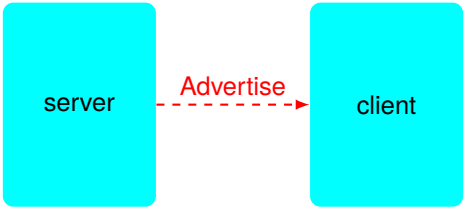
Contournement du firewall de l'utilisateur...plus de passerelle...un lien (presque) direct vers le Cloud !

BLE, ou «*Bluetooth Low Energy*»

BLE, «*Bluetooth Low Energy*»

Deux types de modules :

- ▷ serveur : fournisseur de données, il diffuse son service, «*advertisement*» ;
- ▷ client : scanne le canal de communication ;



Chaque service est identifié par un UUID, «*Universally Unique ID*».

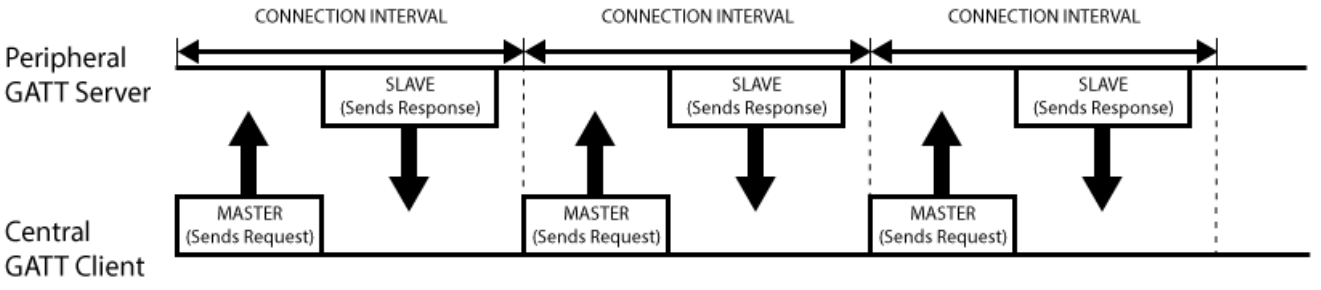
UUID :

- ☐ identifie les «*services*», «*characteristics*» et les «*descriptors*» ;
- ☐ diffusé par radio :
  - ◇ en version courte sur 16bits pour économiser du temps et de l'énergie ;
    Il existe une base d'enregistrement à `https://www.bluetooth.com/specifications/gatt/services`

Heart Rate	org.bluetooth.service.heart_rate	0x180D	GCD

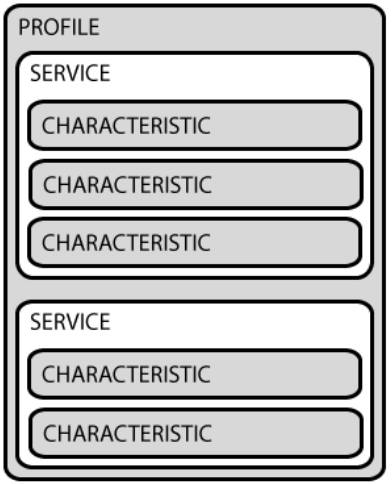
  - ◇ en version complète sur 128bits qui identifie de manière unique l'appareil (pas de registre commun d'enregistrement) ;

Modèle «client/esclave»



BLE, «*Bluetooth Low Energy*»

GATT, *Generic Attribute Profile*



- Chaque «*device*» dispose d'un profile qui définie et organise ses **services**.
- Chaque service dispose de «*characteristics*» dont la présence, «*requirement*», peut être `optional`, `mandatory`, obligatoire, ou `excluded`.
- Les «*characteristics*» ont des **propriétés** dont la présence peut être `optional`, `mandatory`, ou `excluded`;

Exemple pour le «*Heart Rate*» service, il dispose de :

– la «*characteristic*» «*Heart Rate Measurement*» :
  - `mandatory` : obligatoire$\Longrightarrow$ cette characteristic est obligatoire dans le cas d'un capteur cardiaque ;
  - propriétés :
    - `Read`, `Write`, `WriteWithoutResponse`, `SignedWrite`, `Broadcast`, *etc.* : `Excluded` $\Longrightarrow$ interdite ;
    - `Notify` : `Mandatory` $\Longrightarrow$ le serveur informe à intervalles réguliers ;

Polar H7
Service
Heart Rate `0x180D`
Characteristic
Heart Rate Measurement `0x2A37`
Characteristic
Body Sensor Location `0x2A38`
Characteristic
Heart Rate Control Point `0x2A39`

`Notify`

Vous trouverez le code pour l'ESP32 d'émulation du capteur cardiaque Polar H7 à l'adresse suivante :
`https://github.com/SensorsIot/Bluetooth-BLE-on-Arduino-IDE`

BLE : Découvrir le service

xterm

```
pef@cube:~$ sudo bleah

          .                                                   .
        .n                    .                 .                      n.
  .   .dP                   dP                   9b                    9b.    .
 4    qXb         .       dX    BLEAH v1.0.0     Xb       .           dXp     t
dX.    9Xb      .dXb    __                         __    dXb.     dXP     .Xb
9XXb._       _.dXXXXb dXXXXbo.                 .odXXXXb dXXXXb._       _.dXXP
 9XXXXXXXXXXXXXXXXXXXVXXXXXXXXOo.           .oOXXXXXXXXVXXXXXXXXXXXXXXXXXXXP
  `9XXXXXXXXXXXXXXXXXXXX'~   ~`OOO8b   d8OOO'~   ~`XXXXXXXXXXXXXXXXXXXXP'
    `9XXXXXXXXXXP' `9XX'    *     `98v8P'     *    `XXP' `9XXXXXXXXXP'
        ~~~~~~~       9X.          .db|db.          .XP       ~~~~~~~
                        )b.  .dbo.dP'`v'`9b.odb.  .dX(
                      ,dXXXXXXXXXXb     dXXXXXXXXXXb.
                     dXXXXXXXXXXP'   .   `9XXXXXXXXXXb
                    dXXXXXXXXXXXb   d|b   dXXXXXXXXXXXb
                    9XXb'   `XXXXXb.dX|Xb.dXXXXX'   `dXXP
                     `'      9XXXXXX(   )XXXXXXP      `'
                              XXXX X.`v'.X XXXX
                              XP^X''b   d'`X^XX
                              X. 9  `   '  P )X
                              `b  `       '  d'
                               `          '

               Made with  by Simone 'evilsocket' Margaritelli

@ Scanning for 5s [-128 dBm of sensitivity] ...

 24:0a:c4:81:69:e2 (-63 dBm)
 Vendor                 Espressif
 Allows Connections
 Flags                  LE General Discoverable, BR/EDR
 Tx Power               u'eb'
 Complete 16b Services  u'0d18'
 0x12                   u'20004000'
 Complete Local Name    FT7
```

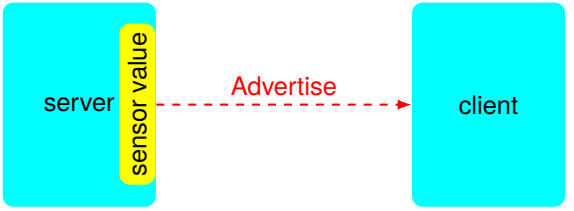
BLE, «*Bluetooth Low Energy*»

xterm

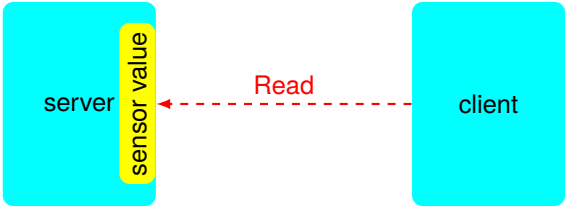
```
pef@cube:~$ sudo bleah -b "24:0a:c4:81:69:e2" -e

          .                                                   .
        .n                   .                 .                  n.
  .   .dP                  dP                   9b                 9b.    .
 4    qXb         .       dX    BLEAH v1.0.0     Xb       .        dXp     t
dX.     9Xb      .dXb    __                         __     dXb.     dXP     .Xb
9XXb._       _.dXXXXb dXXXXbo.                  .odXXXXb dXXXXb._       _.dXXP
 9XXXXXXXXXXXXXXXXXXXVXXXXXXXXOo.           .oOXXXXXXXXVXXXXXXXXXXXXXXXXXXXP
  `9XXXXXXXXXXXXXXXXXXXXX'~   ~`OOO8b   d8OOO'~   ~`XXXXXXXXXXXXXXXXXXXXXP'
    `9XXXXXXXXXXP' `9XX'    *     `98v8P'     *    `XXP' `9XXXXXXXXXXP'
        ~~~~~~~       9X.          .db|db.          .XP       ~~~~~~~
                        )b.  .dbo.dP'`v'`9b.odb.  .dX(
                      ,dXXXXXXXXXXb     dXXXXXXXXXXb.
                     dXXXXXXXXXXP'   .   `9XXXXXXXXXXb
                    dXXXXXXXXXXXb   d|b   dXXXXXXXXXXXb
                    9XXb'   `XXXXXb.dX|Xb.dXXXXX'   `dXXP
                     `'      9XXXXXX(   )XXXXXXP      `'
                              XXXX X.`v'.X XXXX
                              XP^X'`b   d'`X^XX
                              X. 9  `   '  P )X
                              `b  `       '  d'
                               `              '
                  Made with  by Simone 'evilsocket' Margaritelli

@ Connecting to 24:0a:c4:81:69:e2 ... connected.
@ Enumerating all the things ...

 Handles       Service > Characteristics                                                  Properties  Data

 0001 -> 0005  Generic Attribute ( 00001801-0000-1000-8000-00805f9b34fb )
 0003            Service Changed ( 00002a05-0000-1000-8000-00805f9b34fb )                  INDICATE

 0014 -> 001c  Generic Access ( 00001800-0000-1000-8000-00805f9b34fb )
 0016            Device Name ( 00002a00-0000-1000-8000-00805f9b34fb )                     READ        u'FT7'
 0018            Appearance ( 00002a01-0000-1000-8000-00805f9b34fb )                      READ        Unknown
 001a            Central Address Resolution ( 00002aa6-0000-1000-8000-00805f9b34fb )      READ        '\x00'

 0028 -> ffff  Heart Rate ( 0000180d-0000-1000-8000-00805f9b34fb )
 002a            Body Sensor Location ( 00002a38-0000-1000-8000-00805f9b34fb )            READ        '\x02'
 002d            Heart Rate Measurement ( 00002a37-0000-1000-8000-00805f9b34fb )          NOTIFY
```

BLE, «*Bluetooth Low Energy*»

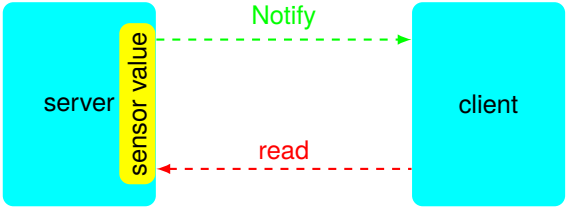
❶⇒ le capteur cardiaque «Polar 7» offre son service, :
Le client le découvre.



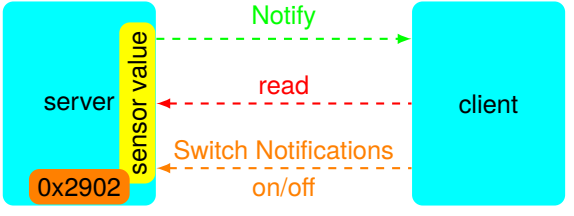
❷⇒ le téléphone et son application mobile lit les données :
Pour la lecture des valeurs du capteur, le client risque de ***gâcher de l'énergie*** *: il ne sait pas quand le capteur dispose d'une nouvelle valeur*.



❸⇒ Il faut que le client soit «**notifié**» de la modification de la valeur :



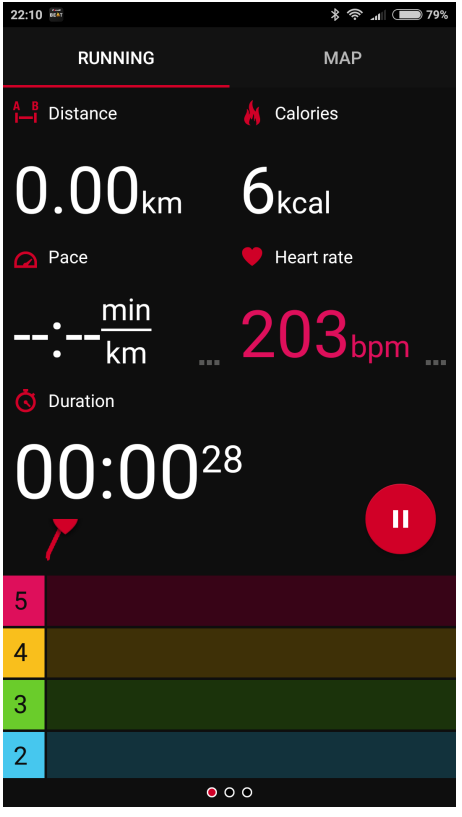
❹⇒ Pour **éviter** que le capteur diffuse ses notifications sans qu'il n'y est de client, il est nécessaire au travers du service d'UUID `2902`, d'activer ou de désactiver ces notifications :



BLE, «*Bluetooth Low Energy*»

201...202...203

Ca fait combien un octet ?



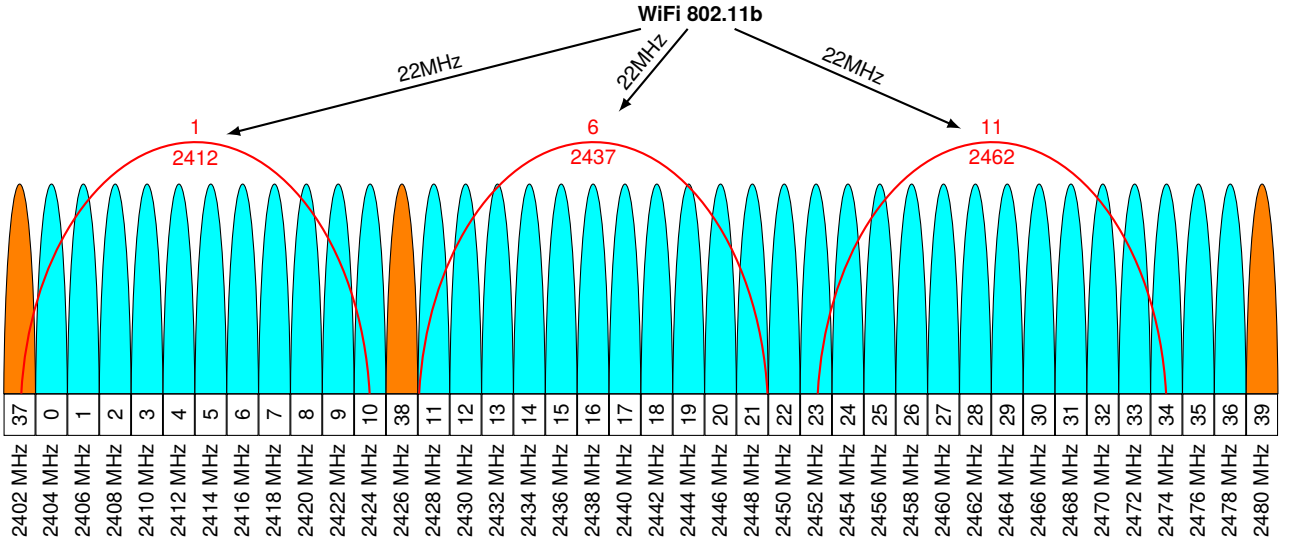
Ici, un ESP32, modèle supérieur à l'ESP8266 disposant d'un module BLE en plus du WiFi, simule une bande de capture du ryhteme cardiaque.
Les valeurs transmises à l'application Android proviennent d'un simple compteur...transmettant un rythme cardiaque de 0 à 255 !

BLE : Radio

BLE utilise 40 canaux de 2400MHz à 2480MHz regroupé en deux types :

– données : ◇ de 0 à 36 ;
◇ communication bidirectionnelle entre éléments connectés ;
◇ saut de fréquence adaptatif : $f_{n+1} = (f_n + \text{hop}) mod 37$ avec hop allant de 5 à 16 ;

– «*advertising*» : 37, 38 et 39 ;



Wifi 802.11b en mode DSSS, des blocs de 22MHz, soient 3 blocs indépendants (sans chevauchement) :

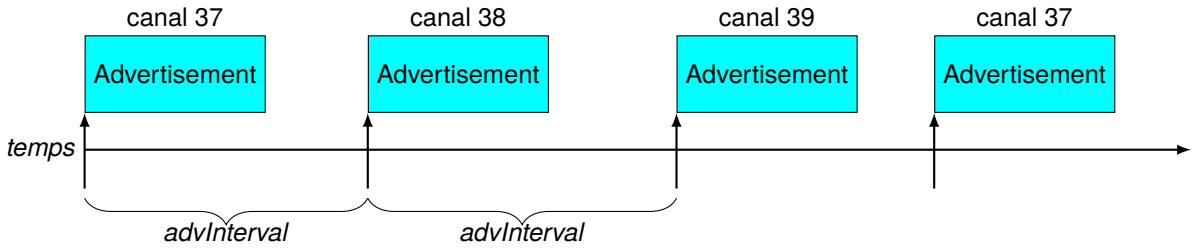
▷ Channel 1 : centré sur 2412, de 2401 (2412-11) à 2423 (2412+11) ;

▷ Channel 6 : centré sur 2437, de 2426 (2437-11) à 2448 (2437+11) ;

▷ Channel 11 : centré sur 2462, de 2451 (2462-11) à 2473 (2462+11) ;

BLE, 3 canaux d'«*advertisement*» : 37, 38 et 39 ;

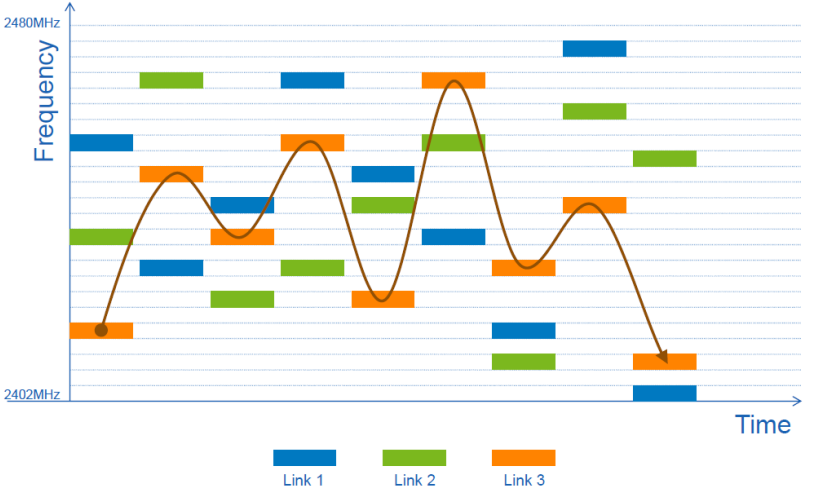
BLE : Radio



$advInterval = advDelay + advRandom$ avec :

- $advDelay$ de 20ms à 10.24s ;
- $advRandom$ de 0ms à 10ms.

Les sauts de fréquences en BLE



IoT et sécurité

❶⇒Qu'est-ce que «l'IoT» ;

❷⇒Les menaces sur l'IoT ;

❸⇒Des vulnérabilités spécifiques ;

❹⇒Les mécanismes de sécurité ;

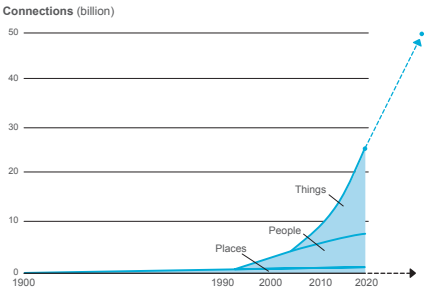
❺⇒Analyse de risques : approche réseau ;

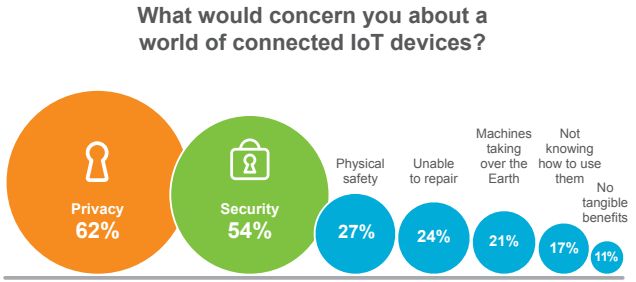
❻⇒Approche matérielle : le «root of trust» ;

❼⇒Chiffrement et IoT.

1 «*The Internet of Things*»

Jusqu'à 26 milliards d'objets connectés en 2020





Des éco-systèmes très différents

- un **large spectre** de «*devices*» :
  - capteurs fortements contraints construit avec de l'électronique imprimable ;
  - véhicules autonomes comme des camions, voitures et avions ;
- des **scénarios d'usage** étendus :
  - surveillance de la température ;
  - surveillance de processus industriels critiques ;
- des **attentes de sécurité** différentes :
  - public : sécurité des données personnelles et «*privacy*» ;
  - entreprise : sécurité des secrets industriels et des infrastructures critiques ;
- **mais des bénéfices considérables** :
  - **analyse de données**, «*big data*» ;
  - **automatisation** ;
  - **optimisation** des ressources et des traitements ;

«*The Internet of Things*»

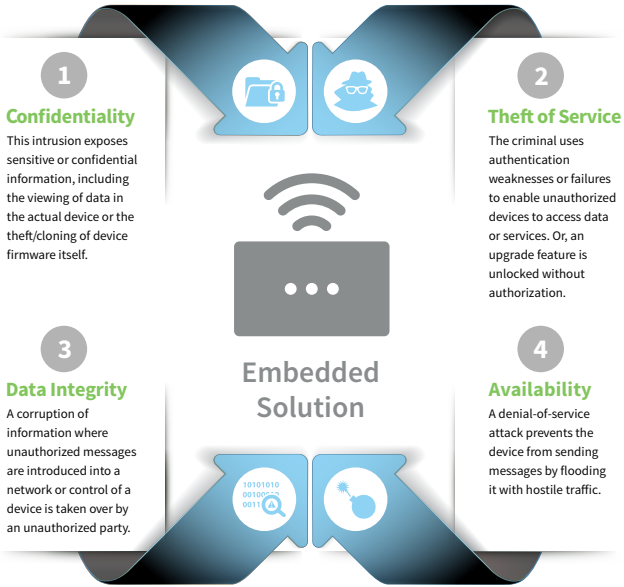
Une définition et une infrastructure

Un réseau d'objets connectés à Internet capables de collecter et d'échanger des données.

- des **objets** qui nous entourent au quotidien embarquent :
  - des capteurs plus ou moins sophistiqués ;
  - des SoC, «*System-On-Chip*» ;
- les **données capturées** d'un objet sont :
  - envoyées à une passerelle qui les envoie ensuite sur Internet ;
  - stockées dans le «*cloud*» pour y être analysées ;
- après **analyse**, les données traitées sont transmises à une application IoT qui :
  - exploite ces données suivant différents besoins ;
  - est bâtie sur une plateforme offrant un langage commun capable de faire communiquer capteurs et actionneurs embarqués dans les objets
- il existe **différentes plateformes** :
  - certaines basées sur le «*cloud*» pour intégrer les données de nombreux objets ;
  - d'autres supportant le développement d'applications IoT ;

2 Les menaces sur l'IoT

- **ressources disponibles limitées** : faible capacité en batterie, mémoire et vitesse de traitement
  $\Longrightarrow$ ne peut pas supporter les mesures de sécurité habituelles ;
- **manque d'intérêt pour les données** : les données de l'IoT ne sont pas forcément vues comme importante, ce n'est pas la motivation première des attaques : c'est le défi qu'ils représentent ;
- **disponibilité des outils** : tous les outils pour modifier/analyser/étudier les IoTs sont disponibles pour tous ;
- **pas besoin d'un accès physique** : utilisation de communication sans fil ;
- **interface différente et limitée** : les rapports d'erreurs et de sécurité peuvent être facilement ignorés ;
- des **ports d'accès physiques** : utilisés pour la programmation ou le déboguage.



Des attaques médiatisées : «Mirai Botnet» constitué de caméras IP et de router personnels ;

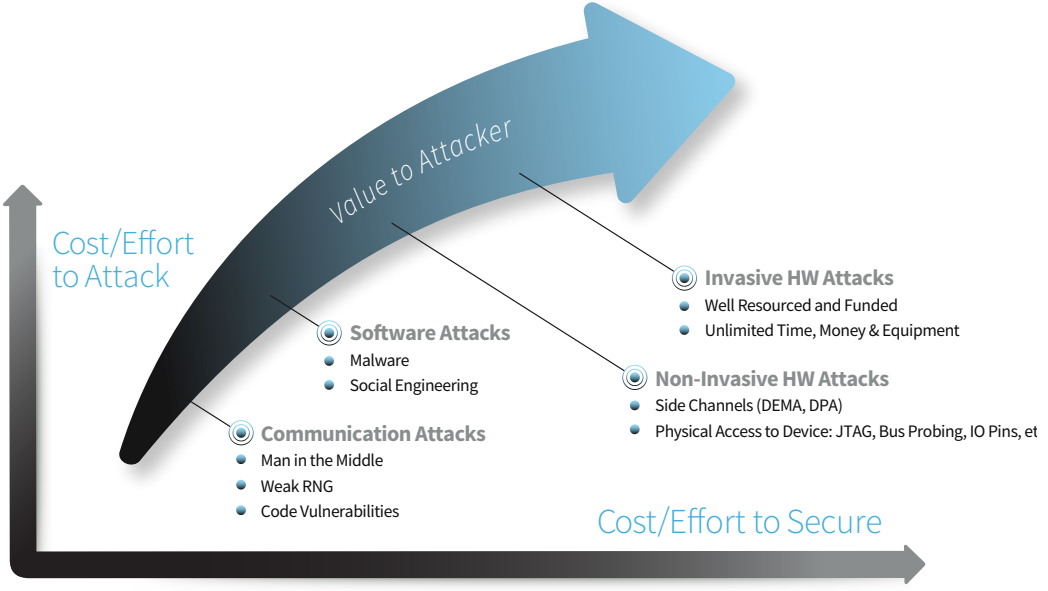
«DDoS» : détournement d'IoT pour

- ▷ créer un botnet pour attaquer une cible à l'intérieur ou à l'extérieur du réseau IoT ;
- ▷ épuiser la batterie de l'IoT victime.

Les menaces sur l'IoT

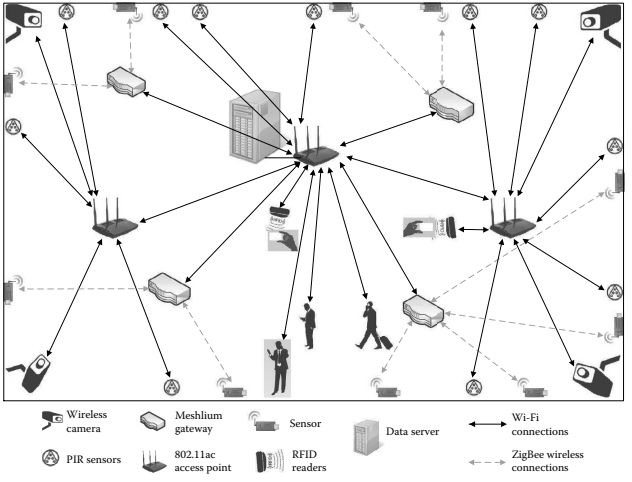
La sécurité est un équilibre entre le coût et le bénéfice

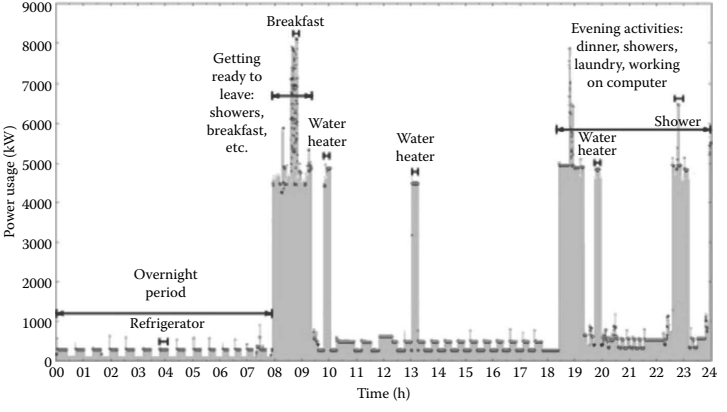
- un attaquant disposant de **suffisamment** de **temps**, **d'argent** et **d'expertise** peut hacker n'importe quel système ;
- le but de la sécurité est de rendre le **coût** de l'attaque **trop important** par rapport au gain espéré ;



- **attaques matérielles invasives** : «*reverse engineering*», utilisation de micro-sonde sur le processeur ;
- **attaques logicielles passives** : exploiter une vulnérabilité dans le code du firmware de l'objet ;
- **attaques sur les communications** : exploiter des vulnérabilités dans les protocoles réseaux, dans la cryptographie utilisée ou dans les clés de chiffrement utilisées ;

IoT : attaque sur la vie privée

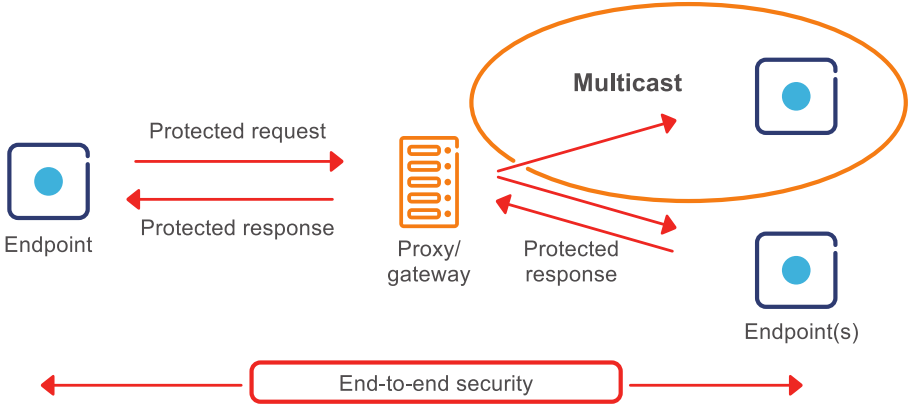




5 «*The Internet of Things*» : analyse des risques, approche réseau

- Pour être utile : communication **temps réel** et **bi-directionnelle** vers Internet ;
  ⟹ type de communication notoirement difficile à sécuriser

- besoin d'un **nouveau modèle** de sécurité
  ⟹ protocoles et «best practices» pour les serveurs, les ordinateurs personnels et les smartphones sont bien connus mais inapplicables directement
  ⟹ besoin de solution «*plug and play*» : pas de mise en service, de logiciel et de firmware à mettre à jour à effectuer par l'utilisateur
  ⟹ décaler le problème de la sécurisation du constructeur matériel vers la couche réseau : plus de flexibilité et de robustesse ;
  ⟹ assurer une sécurité bout en bout, «*end-to-end*».

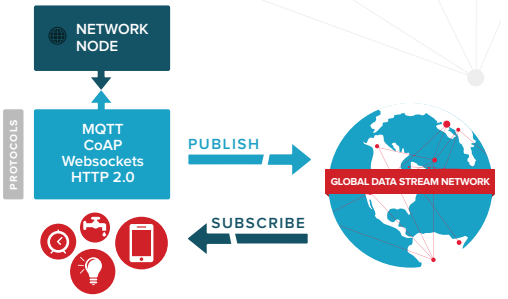


«*The Internet of Things*» : préconisations

- les objets **ne doivent pas disposer** de port ouvert en **entrée** :
  - pour qu'un serveur puisse envoyer des données, «*push*», à un objet, celui-ci doit être en attente : disposer d'un port de connexion sur lequel le serveur peut se connecter.

    $\Longrightarrow$ risque massif de sécurité :
    - installation de malware ;
    - modification et/ou vol de données ;
    - attaque par «DoS» ;
    - exécution de code ;

  $\Longrightarrow$ l'objet connecté doit effectuer **uniquement des connexions sortantes** :
  - utiliser le modèle publier/s'abonner, «*publish/subscribe*», pour disposer de lien de communication bi-directionnel ;
  - supporter le «*scaling*» du modèle : jusqu'à 50 milliards d'objets connectés
    - serveurs hautes performances ;
    - nombreux points de présence répartis sur la planète ;



Les protocoles adaptés : MQTT, CoAP, Websockets et HTTP 2.0.

«*The Internet of Things*» : préconisations

- **Chiffrement de «bout en bout»**, «*end to end*» :
  - utilisation de **TLS**, «*Transport Layer Security*» :
    - chiffrement des communications de l'objet au serveur ;
    - authentification du serveur et aussi de l'objet ;
  - utilisation **d'AES** pour le chiffrement des données produites par l'objet connectés ;

- utilisation du **modèle d'enveloppe** :
  - les données de l'objet sont chiffrées par AES pour le destinataire final avec une clè secrète partagée ;
  - ces données chiffrées sont intégrées dans une enveloppe contenant des **données en clair** pouvant être utilisées par les intermédiaires :
    - filtrage/routage ;
    - analyse

L'intégralité de l'enveloppe est échangée de manière chiffrée au travers de TLS.

«*The Internet of Things*» : préconisations

- □ **Surveillance du status d'un objet** :
  - ◇ surveiller constamment le status «online/offline», la présence, d'un appareil :
    ⟹ **Alerter l'utilisateur** ou le système de surveillance si un appareil **arrête d'émettre ou de recevoir** des données
    Que ce soit dans l'IoT des particuliers ou bien industriel : capteur sur une plateforme pétrolière, système de surveillance de domicile, appareil électroménager etc.
    ⟹ un appareil offline peut signifier :
    - ▷ une tentative locale de manipulation, «*tampering*» ;
    - ▷ une situation de perte de connexion Internet ou une panne de courant ;
  - ◇ disposer d'un **canal indépendant et sécurisé** pour échanger des données de présence pour chaque appareil qui peut être personnalisé :
    - ⋆ statut online/offline ;
    - ⋆ température ;
    - ⋆ accélération ;
    - ⋆ géolocalisation ;

    Par exemple :
    - ⋆ *la serrure d'une porte connectée peut alerter son propriétaire du changement de statut de la serrure si son téléphone n'est pas à 10m de là ;*
    - ⋆ *si un ensemble de capteurs d'une usine de génération d'énergie solaire passent offline, le réseau peut dépêcher un technicien pour identifier le problème ;*

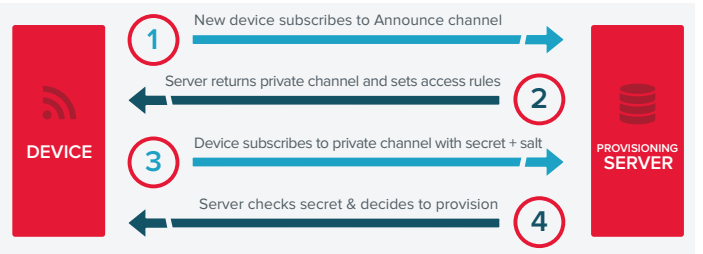
«*The Internet of Things*» : préconisations

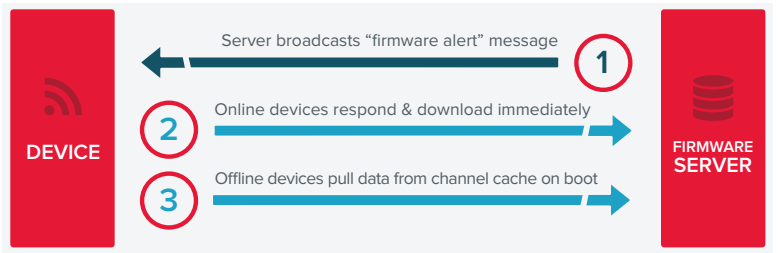
- «User friendly» configuration et mise à jour :
  - différentes étapes dans la vie d'un objet connecté :
    - l'objet est opérationnel et se connecte à Internet ;
    - l'objet doit être configuré et son logiciel doit être maintenu à jour ;

    Exemple : un utilisateur vient d'acheter un système de 6 caméras connectées avec détection de mouvement pour la sécurité de sa maison : il espère que tout va fonctionner...

    mais il doit :
    - *configurer son firewall qui bloque leur connexion ;*
    - *mettre à jour leur firmware : mise à jour des fonctionnalités et correction des failles de sécurité ;*

    et souvent, si cela marche il ne fera plus de mise à jour...
- Utilisation du modèle publier/souscrire avec les ports HTTP en sortie (port 80 et 443) :
  - 1. souscription à un canal d'annonce et s'annonce su le réseau ;
    2. le serveur renvoie un canal privé partagé :
       - ▷ définir les règles d'accès ;
       - ▷ intégrer l'objet ;



  - 

    La mise à jour du firmware peut être faire automatiquement :
    1. le serveur informe les objets au travers d'un canal en diffusion ;
    2. chaque objet effectue sa mise à jour ;
    3. en cas d'un objet offline, il fera la mise à jour au moment où il redeviendra online ;

6 Protection matérielle : «*roots of trust*»

- **protection automatique** de leur fonctionnement et des données contenus ;

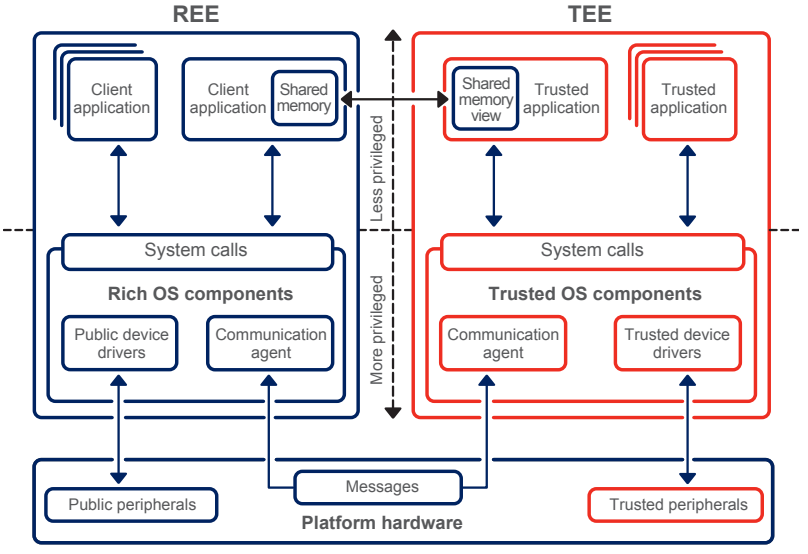
⟹ *les données* sensibles *conservées dans un stockage non-sécurisé doivent être chiffrées et leur intégrité protégée pour fournir une fonction de* ***stockage sécurisé*** *;*

- **vérification basée sur la cryptographie** du logiciel embarqué et des mises à jour ;
- possibilité de **mise à jour à distance**, «OTA», «*Over-The-Air*», du firmware même en cas de malware ;
- **espace mémoire suffisant** pour permettre d'aller vers une version antérieure de firmware en cas de faille critique mais de manière sécurisée : empêcher une attaque par «*rollback*».

⟹ *ces propriétés de sécurité doivent être* ***isolées*** *des applications présentes sur l'objet.*

- **chemin sécurisé** : les données à protéger ne doivent pas circuler par des canaux non sécurisés

⟹ *adaptation du DMA pour gérer des canaux sécurisés, plusieurs bus de données, MMU avec tables distinctes, etc.*



Isolation basée hardware

▷ **Trusteed Execution Environment** :

- ◇ **réalise** toutes les opérations de sécurité évoquées plus haut ;
- ◇ **protège** les applications contre :
  - ⋆ les **autres applications** ;
  - ⋆ un **système d'exploitation compromis** ;

⟹ Pour un «bootstrapping» automatique et sécurisé : **installation des «*credentials*»** lors de leur fabrication **en usine**.

▷ **Rich Execution Environment** : l'environnement normal d'exécution.

7 Chiffrement et IoT

- Cryptographie **asymétrique** :
  - utilisable sur la plupart des processeurs embarqués ;
  - difficulté sur des processeurs «*ultra low-cost*» ;

  $\Longrightarrow$ remplacement par de la cryptographie «post-quantum» : taille beaucoup plus grande des clés et signatures ;

- Cryptographie **symétrique** :
  - le coût énergétique est négligeable par rapport à celui des communications sans fil ;

- Cryptographie «***Lightweight***» :
  - réservée aux environnements fortement contraints : étiquette RFID, capteurs, carte sans-contact, *etc.*
  - combinaison de «*Block Ciphers*», «*Stream Ciphers*» et «*Hash Functions*»/MAC demandant de faible ressources en lors de l'exécution (taille RAM et puissance CPU) et en espace mémoire (taille faible des clés et des données) ;

Symétrique	**ECC**	**DH/DSA/RSA**	**recommandé**
80	163	1024	
112	233	2048	RFC 7525
128	283	3072	ENISA 2013
192	409	7680	
256	571	15360	

  - Chiffrement **asymétrique** :
    - implémentation efficace de courbes elliptiques (Curve25519), mais prends du temps si non accéléré matériellement ;
    - obligatoire pour l'utilisation de TLS.