

COURS : L'INTERNET DES OBJETS

SOMMAIRE

<i>Internet des objets</i>	2
Introduction	2
Définition et grands principes	2
<i>Les types d'objets connectés</i>	4
<i>Les infrastructures réseaux</i>	4
Les réseaux très courte distance	4
Les réseaux moyenne distance	5
Les réseaux longue distance	5
<i>Les systèmes embarqués</i>	7
<i>Architecture matérielle</i>	8
<i>Les antennes</i>	9
<i>Le spectre RF</i>	10
<i>Bilan de puissance</i>	12
<i>Protocoles de communication</i>	13
Implémentation d'un protocole	13
Protocole BC	13
<i>Classes et modes de communication</i>	15
<i>Sources</i>	16

L'Internet des objets (IdO ou IoT pour Internet of Things en anglais) représente l'extension d'Internet à des choses et à des lieux du monde physique alors que le Web des objets désigne l'intégration de tout appareil interrogeable ou contrôlable à distance, dans le monde du World Wide Web.



Internet des objets

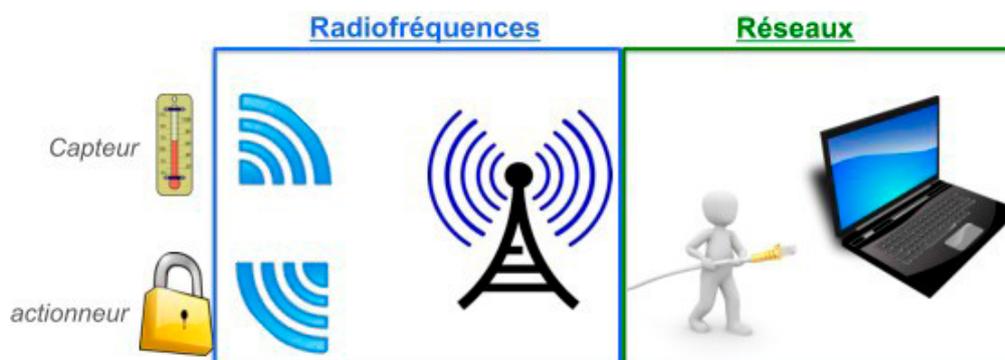
Introduction

Dans «un objet connecté» il y a tout d'abord «objet». Bien entendu il faut que l'objet en question ait quelque chose à émettre ou alors qu'on puisse exercer une action sur lui. Il est donc muni de capteurs et/ou d'actionneurs. Ces capteurs ou actionneurs communiquent avec le monde extérieur par ondes radio.

Généralement ces capteurs actionneurs communiquent via Internet. C'est pour cela que l'on parle d'Internet des objets. Cette connexion à Internet va permettre d'accéder à distance à des données d'un capteur ou à la commande d'un actionneur. Le verrou d'une porte par exemple. Attention, il existe des cas où la connexion radio est remplacée par la connexion filaire ou par fibre optique. Il peut arriver aussi que l'on ne transite pas par Internet. Par exemple une montre connectée qui envoie des données directement un téléphone portable qui affiche ces données et les stocke avec le jour et l'heure.

Définition et grands principes

L'architecture d'une solution connectée est constituée par des objets connectés (capteurs et actionneurs) et par un réseau avec une partie radiofréquence pour les communications sans fil et une autre partie qui utilise Internet (qui constituent le réseau à proprement parler).



Retrouvez éducol sur



Quand on parle de liaison par radiofréquence, la première caractéristique à identifier est la fréquence de ses ondes RF. Les fréquences RF ne sont pas toutes librement utilisables ou sans contrainte. Ainsi les opérateurs doivent acheter des bandes de fréquences à l'État. Par contre, les licences ISM (industrial scientific and medical) sont libres de droits. Toutefois «libres» ne veut pas dire sans contrainte et les puissances d'émission sont limitées.

L'émission peut être unidirectionnelle comme dans le cas d'un capteur de température qui envoie seulement une donnée, ou bidirectionnelle dans le cas d'un téléphone portable.

Une autre caractéristique des objets connectés est sa portée. La portée est la distance à laquelle les ondes ne sont plus captées par les objets. Cette portée définit alors un disque de couverture dans lequel les objets peuvent être adressés. Le disque de couverture radio s'appelle une cellule. Pour former un réseau cellulaire, il faut considérer que la cellule est octogonale. Ainsi, six cellules contiguës vont être pilotées par une station de base et former un réseau.

Pour que ce système cellulaire fonctionne, il faut que chaque cellule opère à des fréquences RF différentes pour éviter les brouillages en bord de cellule. Évidemment, il faut également une coordination des stations de base.

Une autre caractéristique majeure d'une communication est son débit. Le débit se mesure en bits par seconde. Pour transmettre une température le débit nécessaire sera de quelques dizaines de bits/s alors que pour télécharger un film HD en 10 secondes il faudra un débit de 10 Gb/s.

L'autonomie d'un objet connecté est également une performance capitale qui mesure le temps maximal entre deux charges d'un accumulateur. L'autonomie est fortement dépendante des capacités de l'objet et notamment du débit des communications. Elle peut varier d'une journée dans le cas des téléphones portables à une dizaine d'années dans le cas d'un détecteur de fumée connecté.

L'intégration de l'électronique d'un objet connecté dépendra fortement de sa technologie. Elle détermine l'autonomie et les capacités de transmission d'un objet. Un téléphone qui opère en 4G, Wifi et Bluetooth aura évidemment une technologie différente d'une montre connectée qui n'opère qu'en Bluetooth. L'intégration et le coût sont primordiaux pour aboutir à la miniaturisation d'une électronique communicante.

Les types d'objets connectés

Aujourd'hui, grâce à l'explosion de ces réseaux informatiques, les objets sont pleinement connectés c'est à dire qu'ils peuvent transmettre des données après avoir été sollicités, ou bien suite à leur propre initiative de manière périodique (par exemple, un indicateur de présence) ou bien sporadiques (une alarme par exemple).

La principale problématique rencontrée aujourd'hui dans les réseaux d'objets connectés est essentiellement focalisée sur l'utilisation et la gestion de l'énergie embarquée sur l'objet lui-même c'est pour cela que l'on distingue deux principaux types d'objets connectés :



certains objets sont dits passifs c'est à dire qu'ils puisent leur énergie sur un autre élément du réseau. C'est principalement le cas des objets sans contact de type RFID et NFC.



Les objets actifs qui disposent d'une pile ou d'une batterie rechargeable pour pouvoir communiquer.

Toute la problématique relève de la gestion de cette énergie stockée sur une pile pour ne pas avoir à la recharger trop régulièrement. On considère acceptable qu'un objet soit autonome énergiquement au moins pendant deux ans.

Les objets actifs radiofréquences sont très nombreux et leur nombre ne cesse de croître. Ils sont équipés de différents systèmes de communication au travers des technologies wifi, bluetooth mais aussi sigfox et lora. Le smartphone devient naturellement le pivot ou la passerelle des communications des objets connectés car ils ont des capacités de modularité, c'est à dire la possibilité de combiner plusieurs technologies pour étendre les portées de communication, avec des coûts raisonnablement maîtrisés.

Les infrastructures réseaux

Les infrastructures de réseaux sont classifiées en trois principales catégories.

Les réseaux très courte distance

Les réseaux personnels ou wpan (wireless personal area network) sont des réseaux qui utilisent principalement la technologie bluetooth permettant l'interconnexion des objets de proximité comme les oreillettes, les enceintes sans fil mais également le transfert de données peu volumineuses.

Les réseaux de capteurs ou wsn (wireless sensor network) sont des réseaux dédiés à la collecte d'informations issues de capteurs de température, d'humidité, de présence, de fumée, ... et qui sont installés principalement dans les environnements industriels et domestiques.

Les réseaux corporels ou wban (wireless body area network) sont des réseaux portés sur le corps humain ou animal. Ils sont interconnectés avec l'infrastructure de wpan ou de réseau local.

Les réseaux moyenne distance

Les réseaux moyenne distance ou réseaux locaux wlan (wireless local area network) sont exclusivement centrés autour de la technologie wifi qui ne cesse d'évoluer depuis 1996.

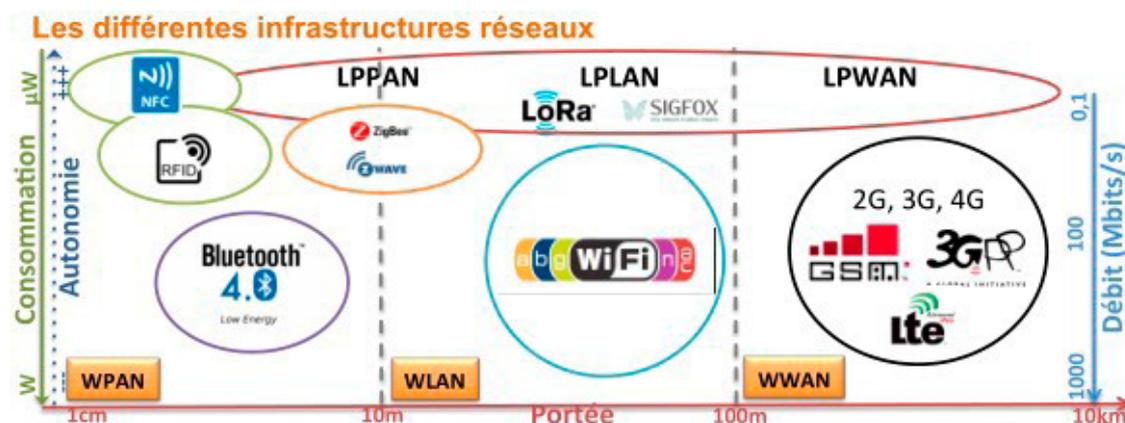
Les réseaux longue distance

Les réseaux longue distance ou wwan (wireless wide area network) sont principalement les réseaux de téléphonie mobile 2g, 3g, 4g mais également les réseaux métropolitains de type wimax.

Le réseau iot quant à lui est en phase de déploiement de réseaux de type LPWAN (low power wan), c'est à dire longue distance et faible consommation d'énergie.

Cette classification s'appuie sur des critères spécifiques ; les principaux critères de classification sont le débit (du kilo bits au méga bits par seconde), la portée (du cm au km), la consommation d'énergie (du microWatt au Watt), l'autonomie (d'une heure à dix ans) et le coût (de 10 centimes à une centaine d'euros).

La figure représentée ici a pour but de synthétiser les différentes infrastructures de réseaux en intégrant les quatre premiers critères que nous venons d'énoncer.



Les distances indiquées ici correspondent à une valeur optimale généralement données dans un contexte de transmission en champ libre c'est à dire en visée directe sans obstacle. Les distances réelles constatées sont souvent inférieures à cause des perturbations de l'environnement (bâtiments, végétation, le relief à l'extérieur, la nature des murs) et la présence humaine à l'intérieur.

	 WiFi	 ZigBee (802.15.4)	 Bluetooth	 NFC
Network topology	 Star	 Mesh	 Point-to-point	 Point-to-point
Range	 30-100 m	 10-20 m	 10 m	 < 0.1 m
Discovery	 Broadcast	 Broadcast	 Broadcast	 Response to field
Power	 High	 Low	 Classic: Mid  LE/Smart: Low	 Tag: Zero  Reader: Very low
Privacy				

Aujourd'hui quasiment tous les téléphones portables sont dotés d'un composant bluetooth et nfc permettant ainsi de communiquer avec des objets connectés utilisant l'une ou l'autre voire les deux technologies.

Certains objets connectés sont également dotés d'une interface wifi dans la mesure où le volume d'informations échangées est important et surtout que l'objet puisse disposer d'une source d'énergie suffisante pour son alimentation statique.

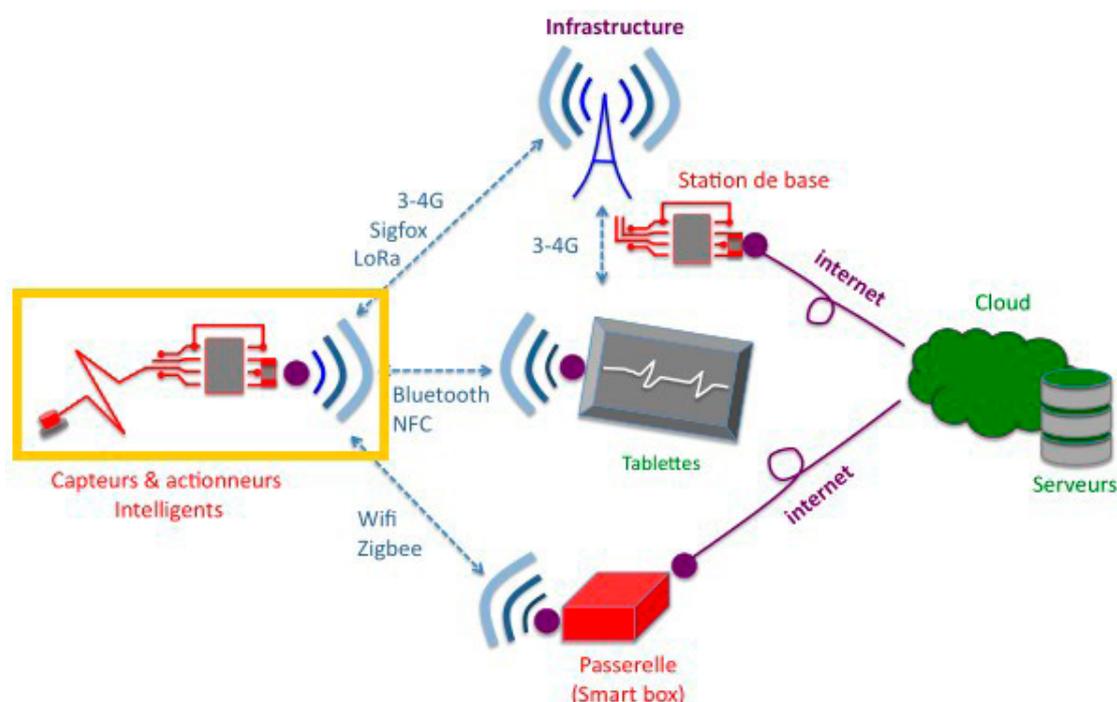
Pour agréger ces différents modes de communication, des passerelles appelées aussi gateway en langage réseaux sont indispensables pour effectuer le lien d'une technologie à une autre. Par exemple, une donnée issue d'un réseau personnel, transmise par un objet connecté en bluetooth, sera nécessairement retransmise ou relayée en wifi ou lora par exemple pour être enfin transmise à un serveur de collecte sur le cloud.

Retrouvez éducol sur



Les systèmes embarqués

Voilà schématisé ci-dessous une architecture générique d'un système d'objets.



Tout commence par des capteurs ou actionneurs ou les deux. Par exemple, un capteur en charge de mesurer une grandeur physique ou un actionneur commandant un verrou de porte. Ces éléments feront l'interface entre le monde physique et le monde numérique avec lesquels ils interagissent. Ces capteurs et actionneurs sont environnés par des systèmes électroniques embarqués qui leur confèrent des fonctionnalités.

On parle de «systèmes embarqués» quand il s'agit de l'association de matériel électronique, le hardware, piloté par un programme informatique, le software, le tout constituant un ensemble autonome.

Prenons l'exemple d'un capteur en charge de mesurer les battements cardiaques. Le système embarque non seulement la mesure de l'électrocardiogramme mais aussi le traitement de ces signaux (filtrage des parasites, amplification, numérisation) et l'analyse des signaux qui va permettre de déduire un rythme cardiaque en battements par minute : c'est cette information que le système va communiquer.

Ces communications se font la plupart du temps par ondes radio fréquence et sont donc sans fil. C'est une partie importante des systèmes embarqués : leurs aptitudes de radiocommunications.

Il est indispensable que les radiocommunications, et plus largement toute communication, soit intelligente. Cela veut dire que tout message doit être clairement identifié et identifiable : on doit connaître son origine et sa destination. Son chemin de transmission au sein d'un réseau de tel point à tel point est pris en charge par les protocoles réseaux.

Retrouvez éducol sur



Architecture matérielle

Sur le plan matériel, les objets connectés sont généralement architecturés autour d'un système à microprocesseur, d'une interface réseau le plus souvent sans fil et de dispositifs d'entrées sorties.

Bien que les progrès de l'électronique soient constants, les objets connectés ne sont pas toujours équipés du dernier processeur pour des questions d'autonomie énergétique. Des processeurs plus lents que les processeurs d'ordinateurs sont ainsi fréquemment utilisés sur les objets connectés.

On retrouve généralement deux architectures matérielles pour les objets connectés :

- une première architecture basée sur un microcontrôleur
- une seconde architecture basée sur un système sur puce ou soc (system on chip)



L'architecture basée sur un microcontrôleur est la plus économe en énergie mais elle est également moins puissante que l'architecture basée sur un soc. En général, le processeur inclus dans un microcontrôleur a des capacités très limitées en terme de calcul (comme la taille du bus de données 8, 16 ou 32 bits et la fréquence de travail quelques mégahertz) et de capacité mémoire qui est l'une des sources de consommation d'énergie très importante sur un objet électronique.



Beaucoup d'objets connectés simples sont pilotés par un microcontrôleur : des plateformes matériellement ouvertes comme arduino reposent sur un microcontrôleur. En termes de réseau, l'architecture basée sur un microcontrôleur pourra intégrer des technologies basse consommation énergétique comme le bluetooth ou zigbee. Les protocoles du monde internet comme ip ne sont pas toujours présents, dans ce cas une passerelle pourrait être chargée de publier les informations sur internet.

L'architecture basée sur un soc est la plus riche. Un soc contient généralement un processeur assez puissant tournant à plusieurs centaines de mégahertz et reposant sur plusieurs dizaines voire centaines de mégaoctets de mémoire vive. On retrouve les architectures soc sur les objets électroniques comme des tablettes ou des montres connectées.

Des plateformes matériellement ouvertes comme le raspberry pi ou beagle bone sont basées sur une architecture soc. D'un point de vue réseau un système basé sur un soc peut être très riche : wifi, bluetooth, 4G, NFC. IP et les technologies internet sont généralement présents de manière native. Elles sont plus consommatrices d'énergie, cela impliquera que l'objet connecté devra être rechargé plus souvent.

Les antennes

Pour réduire la taille des antennes des objets connectés, il faut travailler à hautes fréquences. En effet, plus la taille des antennes est proche de la longueur d'onde et plus la fréquence de la porteuse sera élevée.

$$v_p = \lambda \cdot f$$

- v_p : vitesse de propagation (m/s)
- λ : longueur d'onde (m)
- f : fréquence (Hz)

Pour s'en convaincre voici quelques exemples d'antenne utilisée en radiocommunications :

- la première antenne est celle de l'émetteur de France Inter située à Allouis dans le cher. Celui-ci fonctionne à la fréquence de 162 kHz soit une longueur d'onde de 1852 m. L'antenne est disposée sur deux pylônes de 350 mètres de haut et la puissance de l'émetteur est de 2000 kW.
- la seconde antenne est celle de la station radio KBRC. Elle est située dans l'état de Washington aux Etats Unis. L'émetteur fonctionne à la fréquence de 1,43 MHz soit une longueur d'onde de 210 m. Le pylône d'une hauteur de 61 mètres sert également d'antenne et la puissance de l'émetteur est de 1 kW.

Pour ces deux antennes les dimensions des infrastructures sont comprises entre 0,2 et 0,3 longueur d'onde.

- continuons notre montée en fréquence avec une antenne fonctionne en 433 MHz et qui sert à commander l'ouverture à distance d'un portail. A cette fréquence, la longueur d'onde est de 69 cm et la longueur de l'élément rayonnant est de 16 cm soit une valeur assez proche du quart de la longueur d'onde.
- le dernier exemple est une borne wifi. La fréquence de fonctionnement se situe autour de 2,4 GHz soit une longueur d'onde de 12,5 cm. La borne comprend quatre antennes, l'élément rayonnant a une longueur d'environ 6 cm.

L'utilisation de fréquences porteuses pour des fréquences supérieures à une centaine de MHz permet de réduire les dimensions des antennes. L'encombrement et le poids des équipements sont ainsi considérablement réduits. Toutefois, en utilisant des fréquences porteuses élevées, supérieures à 1 GHz, d'autres problèmes apparaissent qui sont liés à la propagation des ondes dans l'air. Les pertes en espace libre augmentent avec le carré de la fréquence et les obstacles ont un impact non négligeable. La connexion à internet sera moins bonne si les obstacles comme des murs, des cloisons ou des planchers se trouvent entre la borne wifi et l'appareil mobile.

Le signal qui contient une information que l'on souhaite transmettre et qui se propage dans l'atmosphère n'est pas tout seul. Il existe aussi un très grand nombre de sources radioélectriques qui peuvent être liées à l'activité humaine ou qui ont une origine naturelle. Ces sources peuvent avoir un effet néfaste à la réception des signaux et engendrent ce que l'on appelle un bruit de fond. Le niveau de celui-ci est très élevé en basses fréquences.

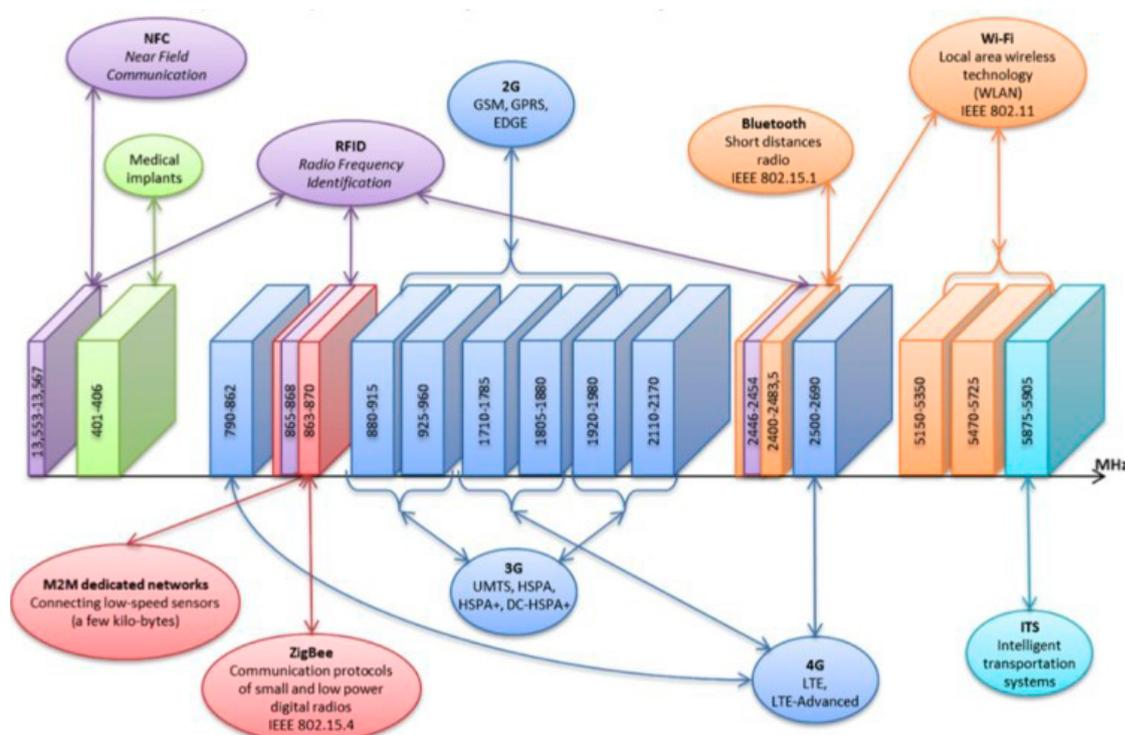
Prenons le cas de France Inter à 162 kHz. Si on veut que l'émission radio soit audible, il faut que la puissance de l'émetteur soit importante pour que le signal reçu à quelques centaines de kilomètres soit supérieur au bruit de fond ; ce qui explique la valeur de 2 MW de l'émetteur. Pour des valeurs de fréquences inférieures à quelques GHz, le niveau de bruit de fond diminue quand la fréquence augmente. Voilà donc un nouvel argument pour utiliser des porteuses de très hautes fréquences car ceci permet de réduire la puissance des émetteurs. Au-delà de quelques GHz, le niveau de bruit augmente avec la fréquence sans toutefois dépasser les niveaux atteints pour les fréquences inférieures à 100 MHz.

Le spectre RF

« Les fréquences radioélectriques appartiennent au domaine de l'état et celui-ci a confié à l'agence nationale des fréquences d'émission de planification, de gestion de l'implémentation des émetteurs, de contrôle et enfin de délivrance de certaines autorisations et certificats radio. »

Agence Nationale des Fréquences Radio (ANFR) – <http://www.anfr.fr>

Chaque gamme de fréquences présente des propriétés de propagation propre. Par exemple quand on opère dans la gamme des ondes longues de 150 kHz à 280 kHz, les ondes suivent la courbure de la terre et par conséquent la portée peut atteindre 1000 km si l'on utilise des émetteurs de plusieurs MW.



En ondes courtes de 2,3 à 26 MHz, les ondes se réfléchissent sur la ionosphère et par rebond leur portée et va ainsi au-delà de l'horizon.

Enfin, en intermédiaire, les ondes dites moyennes de 520 kHz en 1620 kHz opèrent entre ondes de sol et réflexions ionosphériques. La portée est plus limitée, à l'échelle d'un pays par exemple.

Quand la fréquence dépasse les 30 MHz, la propagation se fait en ligne droite.

Pour les objets connectés, le spectre est découpé en tranches. A chaque bande de fréquences correspond une gamme d'applications bien définies par l'arcep et l'anfr. La téléphonie mobile opère sur des bandes licenciées, on y voit la bande de la 4g dite alors de 790 à 862 MHz. Puis de haut en bas et de gauche à droite, on a des bandes de libre pour les communications courte distance nfc et rfid. On a aussi le bluetooth, le wifi et le zigbee (qui est aussi un wifi plus frugal en énergie mais au prix d'un débit plus faible).

Pour les communications longue distance de machine à machine, c'est à dire pour les objets connectés, on trouve deux bandes d'utilisation mais avec des contraintes suivantes : une puissance rayonnée inférieure à 25 ou 500 mW et un taux d'occupation par dispositif inférieur à 1 % ou 10 % du temps. Ces deux points : puissance et temps d'émission limité sont parmi les conditions à respecter pour utiliser ces bandes libres. Ce sont sur ces bandes que les réseaux d'objets connectés dit longue portée opèrent, comme par exemple le réseau sigfox.

Ces bandes sont en effet libres de toute licence, ce qui permet un modèle économique low cost pour un déploiement de masse et les contraintes d'utilisation de ces bandes ne posent pas de problème pour adresser le domaine des objets connectés faibles. Puissance rayonnée et temps d'utilisation riment tous deux avec frugalité de consommation des objets et donc une autonomie dépassant 10 ans.



La première génération de rfid s'appuie exclusivement sur l'utilisation radio en basses fréquences appelées aussi LF pour Low Frequency à 125 et 134 kHz.

Les évolutions de rfid ont amené l'utilisation des ultra hautes fréquences appelées aussi UHF pour ultra high frequency à 433, 850 et 950 mégahertz généralement utilisées pour des applications de logistique. Par exemple la lecture massive d'objets à longue distance, c'est-à-dire sur quelques dizaines de mètres.

La technologie nfc quant à elle se caractérise par l'utilisation de la haute fréquence ou HF pour high frequency à 13,56 mégahertz. C'est une technologie d'identification radio qui se caractérise par une commune communication en champ proche. Cette technologie a connu un essor dès lors qu'elle a été intégrée sur les terminaux portables tels que les smartphones.

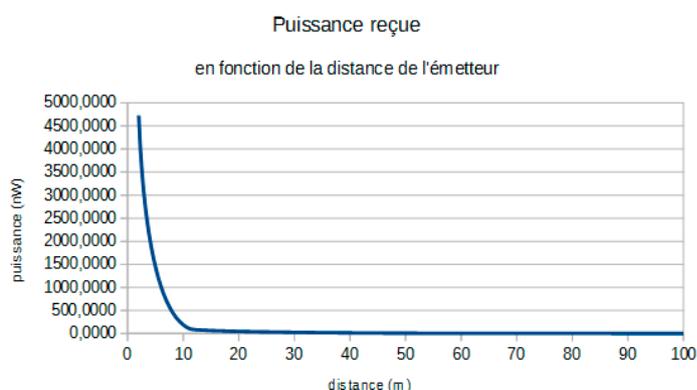
Bilan de puissance

La puissance reçue est proportionnelle à la puissance émise et inversement proportionnelle au carré de la distance séparant émetteur et récepteur et du carré de la fréquence. Le coefficient de proportionnalité k dépend des antennes d'émission et de réception, de l'absorption atmosphérique et des réflexions multiples.

$$P_r = k \frac{P_e}{f^2 \cdot d^2}$$

Exemple : à 868 MHz. A cette fréquence $k = 5,7 \cdot 10^{14} \text{ Hz}^2 \cdot \text{m}^2$. On considère que la contribution des antennes est de 1, que l'absorption atmosphérique est négligeable et qu'il n'y a pas de réflexions multiples. Pour une puissance émise de 25 mW, on obtient la courbe ci-dessous :

k	5,7E+14 Hz ² .m ²	d (m)	Pr (nW)
f	868 MHz	2	4728,413
Pe	25 mW	10	189,137
		20	47,284
		50	7,565
		100	1,891
		150	0,841
		200	0,473
		500	0,076
		1000	0,019
		1500	0,008
		2000	0,005



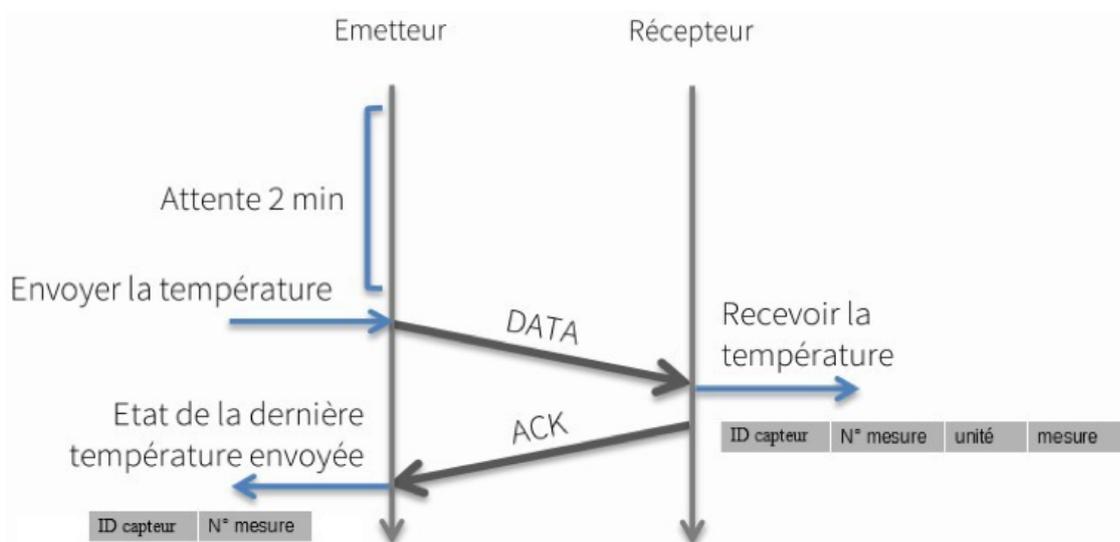
Si l'on considère que le récepteur est capable de traiter des signaux jusqu'à des puissances de 4,8 pW, la distance maximale entre émetteurs récepteurs atteint alors 2 km. En réalité les imperfections des antennes, de l'absorption atmosphérique et les réflexions multiples dégradent la puissance rayonnée de typiquement un facteur 1000, ce qui fait chuter la puissance reçue de ce même facteur. Pour une même puissance minimale acceptable en réception, la portée s'en trouve réduite à 63 m...

Protocoles de communication

Implémentation d'un protocole

Le protocole à mettre en place doit s'assurer de la bonne transmission d'un message de données, désigné par data, qui sera émis par le nœud émetteurs. Le récepteur devra confirmer la bonne réception de data par un message d'acquiescement désigné par ACK.

Si l'émetteur ne reçoit pas l'acquiescement alors il doit remettre data jusqu'à trois répétitions. Au bout de quatre envois non acquiescés la couche supérieure sera prévenue qu'il est impossible de contacter le récepteur.



Il faut spécifier le format des messages échangés : cela consiste à reprendre la question «quel doit être le contenu des messages transmis et reçus pour arriver à l'objectif fixé ?». Par exemple, si l'identifiant d'un émetteur doit être connu du récepteur alors le message doit contenir l'identifiant du nœud émetteur. Dans ce cas, un premier message data devra comporter la température à transmettre ainsi qu'un identifiant indiquant que la donnée est une température exprimée en degrés Celsius et une troisième information qui identifiera le numéro de la mesure. A chaque nouvelle température ce numéro sera augmenté. Enfin une dernière information identifiera le thermomètre de façon unique pour le cas où il y aurait plusieurs thermomètres sur un même nœud du réseau.

Parce que le protocole demande une confirmation du récepteur, un second message d'acquiescement doit être spécifié. On désignera ce message par à ACK. Il reprendra l'identifiant du thermomètre et le numéro de la mesure.

Protocole BC

L'une des contraintes majeures dans le domaine des objets connectés est la consommation énergétique de l'objet. Même s'il dispose de moyens technologiques pour se recharger tout seul, comme par exemple par la lumière du soleil ou par l'énergie produite par ses propres mouvements, il sera presque toujours considéré comme contraint en énergie et donc devra déployer des ruses pour limiter sa propre dépendance énergétique.

La communication réseau est un poste potentiellement très consommateur d'énergie sur un objet connecté. Les techniques de modulation et de démodulation du signal sont de plus en plus évoluées et de ce fait le processeur utilisé pour le traitement du signal est généralement gourmand, notamment quand il est en mode de réception.

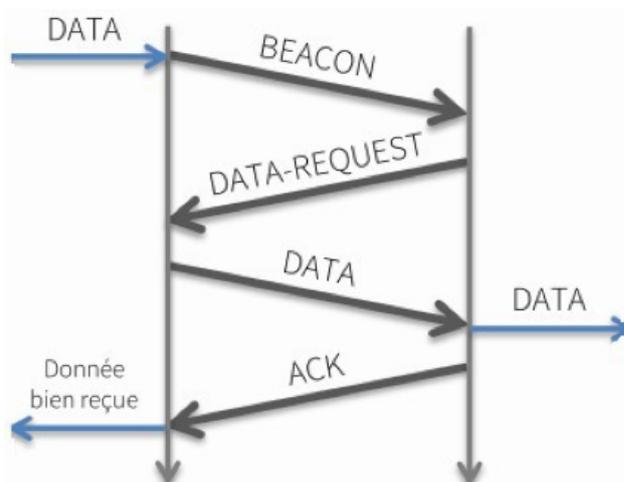
Le mode émission est lui aussi gourmand mais quand un message doit être transmis sa longueur est connue et on peut facilement prédire l'énergie nécessaire pour l'envoyer.

En réception cette tâche est plus complexe car il faut commencer par se mettre à la disposition du nœud émetteur ce qui n'est pas forcément simple à prédire. Les nœuds doivent être synchronisés car si un nœud émetteur envoie un message à un récepteur alors que celui-ci est désactivé pour économiser de l'énergie, le message sera tout simplement perdu et l'émetteur aura dépensé de l'énergie pour rien.

Il existe cependant des techniques pour qu'un émetteur puisse réveiller un récepteur à distance par l'envoi de messages comme c'est le cas avec nfc ou rfid.

L'une des techniques les plus courantes est la technique du rendez-vous ou deux nœuds auront un rendez-vous l'un avec l'autre dans un futur plus ou moins proche pour s'échanger des données. D'ici le rendez-vous, les deux nœuds peuvent choisir d'économiser de l'énergie en se mettant en veille, communiquer avec d'autres nœuds ou faire autre chose.

La technique de rendez-vous est très utilisée dans les technologies bluetooth et zigbee.

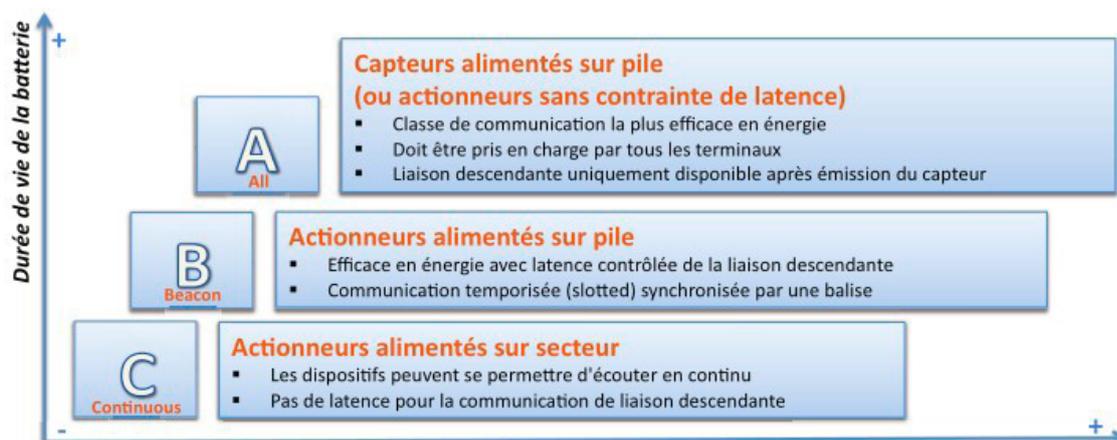


Bien entendu, la fréquence de ces rendez-vous a un impact direct sur la consommation d'énergie. Plus les rendez-vous sont rares, plus l'économie d'énergie est forte. Cependant, si les rendez-vous sont trop rares, les possibilités de communication seront également rares. Ceci aura pour conséquence d'augmenter la latence du réseau forçant l'utilisateur à patienter pour obtenir une réponse ce qui n'est pas toujours acceptable : dans une application domotique, il sera très inconfortable d'attendre cinq ou dix secondes qu'une lumière s'allume après avoir appuyé sur un interrupteur.

Pour que la technique des rendez-vous soit la plus performante possible, il faut que les rendez-vous soient gérés de manière dynamique en fonction des contraintes de l'application.

Classes et modes de communication

Le réseau lora a défini trois classes de communication possibles des objets vers le réseau. Ces classes sont identifiées sur la figure ci-dessous :



On lit en abscisse la latence du réseau en réception, c'est à dire le temps que peut mettre une donnée à parvenir aux serveurs applicatifs depuis le capteur et vice versa.

On lit en ordonnée la durée de vie de la batterie sans compter que de nombreux objets de la classe C sont dépourvus de batteries puisqu'ils sont alimentés sur secteur.

- La classe A est dédiée aux capteurs alimentés sur piles ou actionneurs sans contrainte de latence. Cette classe correspond à une communication la plus économe en énergie. Tous les objets du réseau doivent commencer à communiquer dans cette classe puis éventuellement faire évoluer leurs classes de communication vers B ou C. La liaison descendante ou downlink est uniquement disponible après l'émission de l'objet vers le réseau.
- La classe B est destinée aux actionneurs alimentés sur piles mais efficaces en énergie avec une latence contrôlée de la liaison descendante. Cette communication dite temporisée est synchronisée par mécanisme de balises, d'où le terme de beacon transmises périodiquement par les passerelles. Les objets utilisant cette classe B devront se synchroniser grâce aux balises sur les fenêtres de réception.
- La classe C est destinée aux actionneurs alimentés sur secteur. Les dispositifs peuvent se permettre d'écouter en continu le canal radio et il n'y a pas de latence pour la communication de la liaison descendante. Les objets qui utilisent cette classe sont destinés à être connectés en permanence sur le réseau lora.

La latence de la classe A est plus importante que celle de la classe C car en classe A les communications des objets ne sont pas contraints temporellement. Par contre les objets appartenant à la classe A sont plus autonomes et doivent avoir une durée de vie de batterie d'au moins 10 ans comme le préconise la norme.

Une des caractéristiques d'un réseau d'iot est sa capacité à pouvoir communiquer vers les objets. On parle alors de communications bidirectionnelles. Cela est fondamental dès lors que l'on souhaite commander, paramétrer, mettre à jour un objet à distance au travers le réseau.

Sources

<https://www.anfr.fr/>

<https://fr.wikipedia.org>

<https://www.univ-toulouse.fr/>

<https://www.automation-sense.com>

<https://blog.econocom.com/blog/tag/objet-connecte/>

<https://www.iim.fr/les-objets-connectes-un-nouveau-secteur-sous-haute-menace/>

<https://atelier.bnpparibas/smart-city/article/guerre-ondes-objets-connectes-intensifie>

<https://www.raspberrypi.org/>

<https://www.arduino.cc/>

Retrouvez éduscol sur

