

Internet des Objets

Buzzword ou Révolution ?



A terme, le développement urbain entrainera un besoin accru de rationalisation dans la gestion des ressources, des transports, des parkings, de l'éclairage.



En zone rurale, la captation des besoins réels des plantes, la régulation des processus d'irrigation ou la gestion des stocks deviendront des questions stratégiques.



Partout, les médecins pourront gérer une masse importante d'informations en temps réel sur notre diabète, notre pression artérielle, notre activité cérébrale ou encore notre consommation de médicament.



Dans l'industrie, la production sera de plus en plus intégrée aux services de vente pour être au plus proche de la demande, la maintenance pourra être mieux anticipée et optimisée.



Dans la distribution, la gestion des produits se fera petit à petit en temps réel..

Pour tous ces besoins, l'internet des objets ou IoT, c'est l'idée qu'une connexion entre machines peut permettre une action intelligente et la création de nouveaux services. **Schématiquement, un système IoT fonctionne autour de capteurs, qui transfèrent de la donnée sur des plateformes cloud par des protocoles radios innovants.**

Les promesses de l'internet des objets sont innombrables. Au point où l'on peut se demander s'il s'agit d'évolutions sérieuses, ou d'un nouveau buzzword créé par les professionnels de l'industrie des télécom pour maintenir sous perfusion leur haut niveau d'activité.

Mais de quelles technologies parle-t-on exactement ? Quels acteurs sont à la manœuvre ? Avec quelles solutions ?

LA REVOLUTION DES CAPTEURS

Basiquement, un capteur, c'est un instrument qui assure la conversion entre un signal physique et un signal électrique. Le signal d'origine peut être :



mécanique

pour capter le déplacement, la vitesse, l'accélération, la force, la pression, l'acoustique



chimique

pour capter l'humidité, le niveau de PH, la concentration d'odeurs)



biologique

pour capter le niveau de sucre, de protéines



thermique

pour capter la température, les flux thermiques, l'entropie



magnétique

pour capter les champs magnétiques, les flux)



de rayonnement

comme les rayons gamma, les rayons X, les ondes radios, les micro-ondes

Les capteurs les plus courants sont les capteurs de pression, de température, d'inclinaison et d'accélération. On les trouve partout, du bouton on-off de l'ascenseur à la centrale inertielle 9 axes d'un drone, en passant par des capteurs complexes comme les caméras ou les lasers de proximité.

Ce qu'il faut retenir c'est que ces capteurs deviennent de plus en plus petits, de moins en moins cher, de plus en plus intelligents tout en consommant de moins en moins d'énergie.

Ce phénomène est une transformation rapide. Pour donner un ordre de grandeur, le coût de production d'un capteur qui coûtait une vingtaine d'euros il y a quelques années ne va coûter que quelques centimes aujourd'hui. En terme de rendement d'énergie, certains capteurs peuvent désormais tenir plusieurs années sans avoir à changer une pile ou une batterie.

Concrètement, ces évolutions ouvrent un champ de plus en plus ouvert de possibilités. N'importe quel objet peut désormais être connecté pour presque rien. Laissant la place à de nouvelles perspectives de services.

LA REVOLUTION DES PROTOCOLES TELECOM

En parallèle aux évolutions présentes au niveau des capteurs, il y a également un mouvement qui se met en place dans le monde des télécom autour de l'IoT. Là où on pouvait schématiquement séparer les types de réseaux entre les réseaux domestiques (HAN) et les réseaux cellulaires, l'IoT amène une troisième échelle avec les LPWAN, des réseaux à faibles puissance couvrant une zone relativement étendue. Cette nouvelle catégorie ouvre un nouveau champ des possibles en permettant à des réseaux de simples capteurs et d'actuateurs de réaliser des tâches immensément complexes, à faible coût.

Réseaux domestiques : ne jetons pas trop vite le WiFi !

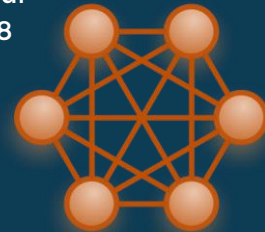
En ce qui concerne les réseaux domestiques, les protocoles les plus courants, aussi bien en termes d'utilisation que d'acteurs industriels travaillant sur la question sont évidemment le Wi-Fi et le Bluetooth qui utilisent respectivement des fréquences en 2,4 GHz and 5 GHz.



Mais ces technologies ont plusieurs défauts en ce qui concerne leur utilisation dans un système IoT.

Pour le Wi-Fi, le vrai problème c'est les interférences, le nombre de machines qui peuvent être connectés en simultané et le niveau de consommation d'énergie nécessaire. Pour le Bluetooth, le problème est qu'il est difficile de maintenir l'intégrité du signal face à des obstacles comme les murs ou les portes.

Ainsi Z-Wave et Zigbee ont développés des technologies, qui fonctionnent respectivement sur des bandes de 908.42MHz et 868.8 MHz. Ces technologies fonctionnent sur un réseau "mesh", ce qui veut dire, qu'au lieu d'être connectées à une station centrale comme le Wi-Fi et le bluetooth classique, les machines sont connectées les unes aux autres. Chaque point devenant un nouveau relai, elles peuvent avoir une bien plus grande portée.



Pour s'adapter à ces évolutions, la Wifi Alliance et Bluetooth SIG, les consortiums en charge de la normalisation des technologies Bluetooth ont dévoilés de nouvelles solutions en 2016, le Bluetooth 5 et le Wifi "HaLow". Ces nouveautés semblent donc être de bons compromis entre les technologies traditionnelles qui permettent de transférer beaucoup d'informations (et donc de faciliter la sécurité) et les réseaux mesh.

Le Bluetooth 5 a été conçu sur le modèle des systèmes "mesh", ce qui lui permet d'atteindre une portée quatre fois plus importante que la portée habituelle et une consommation d'énergie proche de celles de Zigbee et Z-Wave.

De même le WiFi dit "HaLow" permet d'atteindre une longue portée et son mode "veille" intelligent lui permet d'être largement moins énergivore que le Wi-fi traditionnel. Sur de nombreux points, et notamment sur son utilisation de la bande des 900 MHz, le WiFi "HaLow" ressemble aux LPWAN de types Sigfox ou LORA.

LPWAN : Quelques clés de compréhension

De fait, lorsqu'on parle des réseaux IoT à bas débit, longue portée et faible consommation de batterie, ce sont bien les entreprises françaises Sigfox et Cycleo, qui viennent le plus rapidement à l'esprit. La première a réalisé d'impressionnantes levées de fonds et d'important partenariats auprès des banques et des industriels comme Goldman Sachs, Lazard, Air Liquide, Total ou encore Engie. La deuxième est surtout soutenue par les acteurs traditionnels des télécom comme Bouygues et Orange pour le système LORA.



Mais il existe d'autres acteurs sur ce nouveau segment d'activité. On peut citer **Ingenu** (qu'on appelait jusqu'à récemment On-ramp Wireless) qui a été développé avec le soutien d'At&T, **Weightless-N** qui a été développé par Nwave avec le soutien de Cisco et Huawei, **Telensa** qui a été soutenu par Philips, **Platanus**, développé par M2COMM, **NB-FI** qui a été développé par Waviot ou encore **DASH7**, qui a été développé par Lockheed Martin.

Ces systèmes sont simples à déployer. Ils nécessitent peu d'antennes et ne nécessitent pas de racheter des fréquences au prix fort comme pour la 4G.

Du coup on assiste à une véritable course de fonds entre les différents acteurs. A ce jeu là, Sigfox a encore un temps d'avance. La technologie est bien déployée dans les principaux pays occidentaux et le déploiement est en cours dans les BRICS et les MINT. Mais le déploiement de LORA est également très volontariste et il bénéficie de bons partenariats en Russie et aux Etats-Unis (respectivement avec Lace et Senet). Les autres systèmes ont des dimensions qui restent plutôt régionales, Ingenu est bien implanté aux Etats-Unis, Telensa est plutôt installé au Royaume-Unis, Platanus en Asie. Mais ils ont également des éléments sérieux à faire valoir.

Si on le prend plus concrètement, d'un point de vue **technique**. Ces nouveaux réseaux peuvent être séparés en deux catégories, les réseaux **UNB** (Ultra Narrow Band) comme Sigfox, Waviot ou Telensa et les **systèmes à étalement de spectre** comme LORA et Ingenu. Ces deux techniques étaient déjà connues et utilisées dans le secteur spatial, l'UNB permettait de communiquer avec la navette spatiale, l'étalement de spectre est largement utilisée dans les systèmes de navigation. Schématiquement, l'UNB est plus performant en terme de portée (un réseau Sigfox peut théoriquement aller jusqu'à 50 km) et de consommation d'énergie. L'étalement de spectre permet de meilleures performance en terme de transmission de données (LORA permet d'envoyer 500x plus de bit par secondes). Encore une fois, il n'y a pas de réseau parfait, le tout réside dans l'usage, le niveau d'utilisation et le type de données à transférer.

Dans le fond, la vraie question derrière la guerre commerciale qu'on peut voir à l'œuvre pour ce type de réseaux IOT, c'est l'arrivée de la 5G pour laquelle toutes les entreprises se positionnent bien en amont pour devenir le standard de référence. A ce titre, les technologies cellulaires gagnent un intérêt croissant de la part des différents acteurs du domaine.

Les réseaux cellulaires : la fin du jeux ?

Long Term Evolution Machine (appelé **LTE-M** ou encore LTE MTC Cat M1), *Narrow Band Internet of Things* (appelé **NB-IoT** ou Clean Slate IoT) et l'*Extended Coverage Global System for Mobile Telecommunication in the Internet of Things* (**EC-GSM-IOT**) sont des protocoles cellulaires qui ont été présentés à la fin de l'année dernière par le consortium 3GPP, la structure de coopération internationale sur les standards relatifs aux technologies du mobile.

Globalement les performances de ces standards sont supérieures aux LPWAN que nous avons évoqués avec une quinzaine de kilomètres de portée, une capacité à transférer plus de données, plus rapidement et de manière plus sécurisée (NB-IoT permet un transfert 15 fois supérieur à LORA). En outre LTE-M et l'EC-GSM-IOT sont basés sur les infrastructures existantes, et qui vont donc pouvoir se développer rapidement. Le NB-IoT permet lui de s'émanciper des gateways. Ces protocoles ont néanmoins le désavantage d'utiliser des bandes spectrales qui sont règlementées, ce qui signifie que leur utilisation engendre un coût. Un paramètre important à prendre en compte dans la balance.

L'industrie des semi-conducteurs et les principaux opérateurs télécom sont d'ores et déjà en ordre de bataille sur le sujet. AT&T, Verizon, Orange ou encore Telefonica ont fait le choix de LTE-M. Les Etats-Unis, le Mexique et quelques pays européens (notamment l'Espagne et la Belgique) devraient être équipés d'ici la fin de l'année. NB-IoT est lui soutenu par Huawei, Vodafone et Deutsche Telekom. Son déploiement devrait être rapidement effectif en Chine. En ce qui concerne l'EC-GSM-IoT, ce sont Ericsson, Intel et Orange qui se sont positionnés.

LA REVOLUTION DES PROTOCOLES APPLICATIFS

Les protocoles applicatifs permettent de transformer la donnée brute issue des protocoles que nous avons évoqués (Sigfox et autres) pour les transformer en données qui peuvent facilement être traitées et analysées. Ils ne sont pas spécifiques à l'IoT (tout le monde connaît le protocole http). Mais les machines et les réseaux télécoms utilisés pour l'IoT ont un fonctionnement contraint, du fait notamment de leur faible consommation d'énergie.

Et c'est pour cette raison qu'un certain nombre de protocoles sont assez spécifiques à l'IoT, http étant trop lourd. Parmi ces protocoles, on peut citer **REST, MQTT, XMPP ou encore AMQP**.

De manière un peu caricaturale, on peut considérer qu'il y a deux catégories de protocoles applicatifs, les protocoles avec une architecture dite « Publish Scribe » comme MQTT, XMPP ou AMQP et les protocoles avec une architecture « request/response » (comme CoAP). Mais bien sûr, les choses ne sont jamais simples et certains protocoles sont des constructions hybrides.

Pour rentrer un peu plus dans le détail, le protocole **MQTT** est le premier protocole de l'IoT. Il a été développé par IBM et l'Arcom et standardisé par la Fondation Eclipse. Son intérêt c'est qu'il permet de transférer des données simples avec un bon niveau de sécurité (il est basé sur TCP/IP) et sans altération (même dans des conditions de communication instable).

En deux mots, il fonctionne comme un réseau avec plusieurs nœuds et un « broker ». Contrairement à d'autres protocoles, et contrairement notamment à CoAP. Le broker est le centre du réseau et il n'y a pas de connections entre les nœuds. Le système fonctionne même quand un nœud est défaillant.

CoAP ressemble plus au protocole *http*. Il utilise d'ailleurs les mêmes concepts et terminologies (comme GET, PUT, POST et DELETE). La différence c'est qu'il utilise des plus petits paquets et qu'il utilise le protocole UDP (User Datagram Protocol) plutôt que le classique TCP. CoAP a l'avantage d'être rapide et de permettre de développer facilement des passerelles avec le protocole *http*.

Mais contrairement à MQTT, l'information va directement du client au serveur c'est donc le nœud qui est au centre du réseau, pas le broker. En outre le fait que CoAP soit basé sur UDP pose de réels problèmes de sécurité dans la mesure où le nombre de hacking déclarés sur ce protocole augmente de 15% par ans.

Comme pour les protocoles radio, le tout dépend donc de l'usage. MQTT est utile pour des applications simples comme un réseau de capteurs pour la température ou l'humidité et CoAP est plus utile dans le cadre d'applications complexes (comme des diagnostics) qui ne nécessitent pas d'être sûr à 100% que l'intégralité de l'information arrive à la plateforme. Au-delà de l'opposition classique entre MQTT et CoAP, d'autres systèmes comme XMPP ou AMQP semblent être de bons compromis pour la mise en place de systèmes IoT.

Comme pour les protocoles télécom, le besoin de standardisation se fait donc de plus en plus sentir et des initiatives se mettent en place pour éviter une dispersion des protocoles qui nuirait à l'ensemble du secteur. On peut citer notamment l'Open Cloud Computing Interface (OCCI) ou l'Industrial Internet Consortium (IIC) initié par AT&T, Cisco, GE, IBM and Intel.

Mais comme pour les protocoles télécom, les entreprises ont du mal à coopérer car chacun essaie d'imposer sa technologie, son point de vue à tous les autres. Par exemple IBM cherche à défendre MQTT, Cisco étant à l'inverse plutôt derrière XMPP...



LA REVOLUTION CLOUD

Si la guerre des protocoles telecom est de loin le sujet le plus abordé lorsqu'on parle d'IoT, c'est au niveau du cloud que se situe la majorité des perspectives concrètes pour les entreprises et les start-ups. C'est dans leur traitement que l'énorme quantité d'informations en provenance des capteurs prend de la valeur et qu'elle peut se transformer en services. C'est pour ça que les **principaux acteurs du numérique** essayent de se positionner sur cette niche pour tenter de devenir incontournable. Pour l'instant, c'est surtout Amazon qui semble tirer son épingle du jeu avec sa plateforme Amazon Web Services, mais l'entreprise de Jeff Bezos devra faire face à des concurrents comme Microsoft, IBM et Google.

Même si ils n'ont pas les mêmes objectifs, les **opérateurs télécom** comme Bouygues, Altice, AT&T ou Telit et les **groupes industriels** comme Dassault, Bosch, GE et Siemens ont développés leurs propres plateformes. Sur cette question d'importance, le monde de **l'open source** est également largement concerné et des projets tel que KAA ont également des arguments à faire valoir.

Pour être un peu schématique, on considère souvent l'IoT en faisant la distinction entre des solutions en mode Infrastructure as a service (IaaS), Platform as a service (PaaS) ou Software as a service (SaaS).

Dans le premier cas il s'agit comme son nom l'indique des infrastructures, c'est-à-dire des services physiques de location de serveurs et de virtualisation. Les plateformes sont quant à elles, des environnements sur lesquels les applications et services peuvent être mis en place. Le SaaS étant la couche applicative elle-même.

IaaS : Du datacenter à l'edge-computing ?

La mise en place de l'IoT devrait considérablement augmenter la masse globale d'informations à traiter dans les années à venir. Le besoin de scalabilité, c'est-à-dire le besoin de pouvoir faire face à d'importants pics d'activités en maintenant le même niveau de performance, se fait de plus en plus prégnant.



Ainsi, les datacenters évoluent vers des systèmes de plus en plus optimisés, de plus en plus distribués, de plus en plus sécurisés et dont les capacités de stockage ne cessent d'augmenter. Les interconnexions et la gestion des datacenters prennent donc une ampleur stratégique.

Cette évolution se retrouve dans le concept d'« edge computing ». C'est-à-dire l'idée de traiter l'information en amont dans des nœuds et des passerelles pour ne pas saturer les datacenters et assurer sereinement la montée en charge. De tels systèmes distribués n'en sont qu'à leurs balbutiements mais les principales plateformes proposent leurs services. On peut citer notamment Amazon AWS Greengrass, Microsoft Azure IoT Edge, Siemens MindConnect Edge Analytics, ou les projets d'Orange.

Néanmoins, si ces solutions de traitement hétérogène laissent entrevoir d'impressionnantes perspectives, les processeurs à multicœur actuels, ne sont pas non plus sur le point de disparaître du jour au lendemain. La construction des data-centers est une question véritablement politique qui pèse d'ores et déjà 15 milliards par ans à l'échelle mondiale. Cet investissement devrait être multiplié par cinq dans les prochaines années, avec un volontarisme particulièrement marqué en Chine.

PaaS : Les plateformes cloud au cœur de l'IoT

Les plateformes cloud permettent de faire le lien entre les données de bases issues des capteurs et les applications qui permettent d'en extraire des informations et services à haute valeur ajoutée. C'est pour ça que les principaux acteurs du numérique essaient de se positionner sur la question. Leur but, c'est de devenir l'OS central de ce nouveau marché, comme Android l'est devenu pour le mobile et Windows pour les ordinateurs personnels.

Mais elles ne sont pas seules sur ce terrain. Pour les entreprises du secteur des télécoms, les plateformes permettent d'apporter des solutions qui valorisent les protocoles télécom sur lesquelles elles ont parié. Par exemple, le système Objenious est compatible avec LORA et NB-IOT, Altice avec LTE-M et Sigfox, Orange avec LORA etc...

De même, pour les groupes industriels comme Siemens ou GE, l'objectif est d'être le point central des entreprises en créant des liens forts entre différentes étapes de production. Le déploiement d'une solution de cloud est en effet stratégique pour une entreprise, une fois le processus engagé, il est compliqué et coûteux de se retirer dans la mesure où il engage tous les outils informatiques déployés (CRM, CAO, ERP etc...) et une bonne partie des sous-contractants. En cela la concurrence est actuellement féroce entre les différents acteurs du secteur.

Les plateformes permettent d'apporter à l'utilisateur final une station de travail pour gérer et analyser des systèmes complexes. Pour certains créateurs des plateformes IoT, le but n'est pas tant de créer eux même les applications, mais de fournir le cadre adéquat pour que les clients construisent eux même des solutions adaptées à leurs besoins. Pour cela ils mettent en place des kits de développement de software (SDK) et laissent de nombreux outils à disposition des développeurs pour faciliter les tests, analyser les codes source etc..

Un des aspects les plus intéressants du développement est la mise en place d'API (Application programming interface), qui permettent aux développeurs de se connecter à d'autres applications pour échanger des données et des services avec celles-ci sans entrer dans la complexité de leur mode opératoire. Le système des API existe déjà dans de nombreux cas que nous utilisons tous les jours (par exemple quand on utilise Facebook pour s'identifier sur Deezer ou Blablacar..) mais la croissance du secteur de l'IoT ouvre très grand le champ des possibles. Le système BigQuery de Google par exemple va pouvoir permettre de faire rentrer la puissance de la base de données Google dans des applications liées aux objets connectés.

La manière dont vont être mis en place ces outils vont créer une véritable différence de stratégie entre les entreprises. Sur AWS, vu que le paiement fonctionne à la donnée utilisée, l'entreprise Amazon a plutôt tendance à développer des solutions elle-même (Amazon Dynamo DB, Amazon Athena, Amazon Kinesis...), Azure est plutôt utilisé par Microsoft comme un moyen de « repackager » des solutions préalablement existantes. Google essaie surtout de tisser d'intégrer des entreprises émergentes comme Helium, Losant ou Tellmeplus. Pour les autres, le développement d'applications sur leurs plateformes IoT est l'occasion de nouer des partenariats stratégiques. On peut citer les alliances de Siemens avec ATOS, GE avec Accenture, PTC avec Dassault Systems etc...

Enfin l'usage des API ne se fait pas aussi librement sur des plateformes à vocations généralistes et sur des plateformes industrielles, qui intègrent beaucoup plus le facteur de sécurisation des données.

SaaS : Du concept à l'application

Nous avons évoqué les nombreux usages qui peuvent être réalisés grâce à l'internet des objets. Le mode SaaS est le niveau qui rend concret ces usages. De nombreux outils sont disponibles pour créer et construire ces applications.

Couplé à de l'analytics ou de la blockchain, l'IoT permet de faire émerger un certain nombre d'activités et de nouvelles perspectives. Des solutions existent par exemple pour centraliser et analyser l'information en provenance de plusieurs caméras et en extraire des informations importantes en temps réel.

Le marché de l'IoT commence tout juste à se structurer. De nombreuses fusions et acquisition se mettent en place, particulièrement sur ce segment de l'application.

L'IoT est donc une affaire à suivre de près, quel que soit son secteur d'activité. En 2020, 20 milliards d'objets devraient être connectés et les revenus issus du secteur devraient se chiffrer en centaines de milliards d'euros. Petit bémol néanmoins sur le manque de standardisation à toutes les échelles. A terme il pourrait ralentir la tendance.