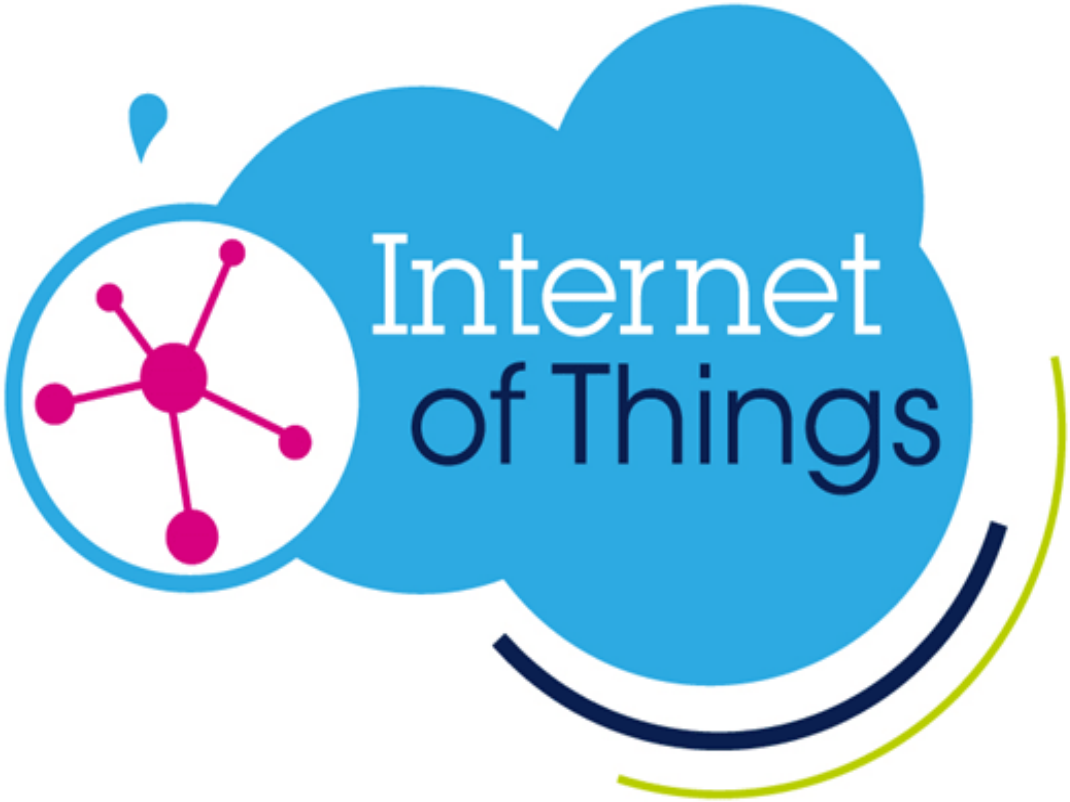
Les IOT en entreprise



Février 2019

RAPPORT FORUM TECHNIQUE

Réalisé par:

BUCQUOY Mathieu

GARCIA Alexis

ECHEVERRIA Sébastien

THEVENET Raphaël

Date soutenance :

26–02--2019

Session :

MSSI Octobre 2018

Table des matières

Chapitre I. Présentation de l'IOT

I.1 Définition

L'Internet des Objets (IoT) est la matérialisation d'Internet dans le monde réel.
Il concerne tous les objets, voitures, bâtiments et d'autres éléments reliés à un réseau d'Internet physique par une puce électronique, un capteur, une connectivité réseau leur permettant de communiquer entre eux, de collecter et d'échanger des données.

« Quand le sans-fil sera parfaitement appliqué, la Terre entière sera convertie en un gigantesque cerveau » (Tesla, 1926).

I.2 Historique de l'IOT

Dans les années 1800s, on a pu voir les premiers équipements électroniques de communication. Tel que les fax, radios ou encore les télégrammes.
En 1989, marque la naissance du World Wide Web créé par Tim Berners-Lee.
Le terme IOT est utilisé pour la première fois en 1999 par Kevin Ashton, employé de Procter & Gamble. P&G est une multinationale américaine spécialisée dans les biens de consommation courante.
En 2000 l'entreprise LG lance le projet de la conception d'un réfrigérateur connecté.
Depuis 2001, l'internet des objets a été l'occasion de permettre la création et l'évolution de jeunes startups désireuses de nous faire entrer dans le futur.
Le premier objet connecté est commercialisé en 2003 par la firme Violet. C'est la lampe DAL, équipée de 9 leds qui s'allument en fonction des évènements (météo, bourse, pollution, alertes google ou encore des envois de messages de couleurs par SMS ou email). Deux ans plus tard, en 2005, Violet lance le célèbre lapin Nabaztag. Ce lapin connecté en WI-FI peut lire des mails à haute voix, émettre des signaux visuels et diffuser de la musique. L'objet est encore commercialisé sous le nom de Karotz.
En 2007, nous avons connu l'apparition des smartphones.
IPSO alliance a fait la promotion de l'utilisation du Protocol internet (IP) dans les objets connectés en 2008. On retrouve également la création de Sigfox.
En 2010, lancement de la société Sense par Rafi Haladjian. Elle a pour but de développer des objets connectés et une plateforme afin de récolter les données de la vie quotidienne et tenter de leur donner du sens.
En 2011, création de l'IPV6 qui permet de connecter 340 undecillion.
LoRa a vu le jour en 2012.
En 2013, Intel pénètre ce marché avec l'Internet of Things solutions Group qui cible notamment l'automatisation dans l'industrie, le retail (le commerce de détail), l'aérospatiale et l'automobile.
Deux ans plus tard, en 2014. : les IOT définissent le futur d'un monde où les appareils interagissent entre eux via (différent réseaux) le cloud, le réseau internet et cellulaire pour analyser de grandes quantités de données via différentes technologies comme le big Data & bi. Management 4.0 qui reposent sur les IOT.
En 2014, avec la création de Mother, un système permettant de connecter chaque objet grâce à de petits capteurs. Une espèce d'objet connecté universel principalement tourné vers la domotique.

I.3 Marché de l'IOT

Evolution des IOT :

Le marché des IOT est sans cesse en évolution. On prévoit 50 milliards d'IOT dans le monde en 2020. Mais cette évolution ne s'arrête pas là. On prévoit également 75 milliards d'IOT dans le monde d'ici 2025.

Aujourd'hui le marché représente 7 à 8 milliards d'IOT dans le monde contre 2.5 milliards en 2009.

Chiffre d'affaire des IOT

Les IOT représentaient un chiffre d'affaire de 400 millions d'euros en 2015. En 2020, le marché des IOT représentera 7 milles milliards de dollars.

En 2025, le chiffre d'affaire des IOT tend vers plusieurs trillons de dollars.

I.4 Périmètre du forum technique

Le périmètre des IOT est vaste. Il touche tous les domaines : la domotique, l'industrie, les entreprises, les voitures, les smartphones etc.

Pour la réalisation de ce forum technique, notre expertise s'est focalisée sur les IOT en entreprise. Il est essentiel que les entreprises soient sensibilisées aux risques auxquels les IOT les exposent.

Par le biais de nos recherches, nous vous présenterons les types d'attaques auxquelles les entreprises sont exposées. Comment s'en protéger avec la transmission des bonnes pratiques. Quel coût représente la sécurisation des IOT mais également les impacts financiers en cas d'attaques.

Pour terminer, nous ferons une présentation des cibles favorites des attaquants et les pires piratages d'IOT.

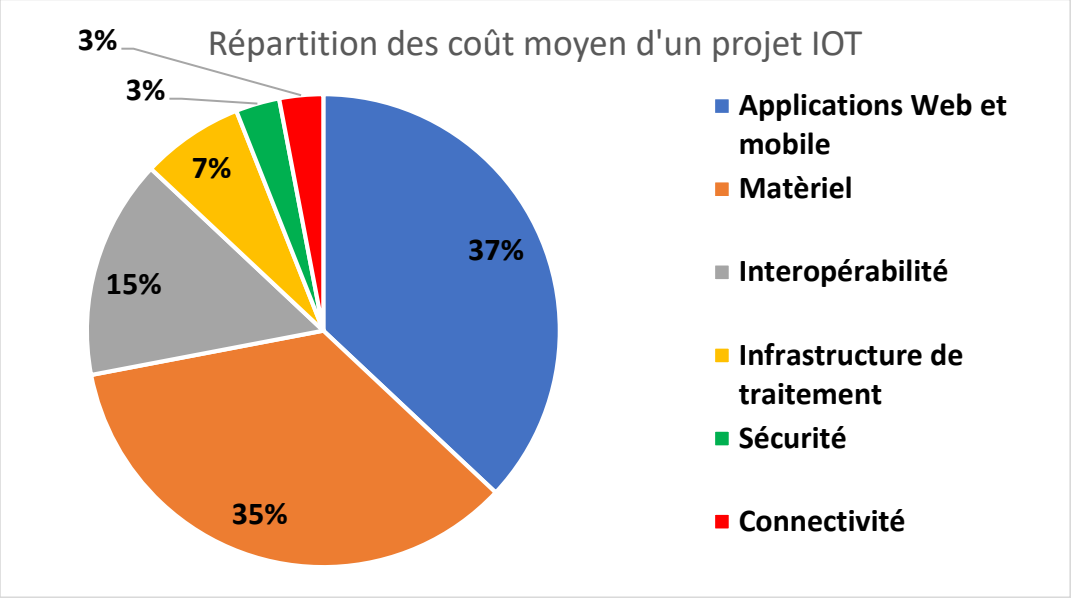
Chapitre II. Le succès des IOT

II.1 Technologie économique

Il est difficile aujourd'hui d'établir une fourchette de prix des capteurs, tant ils sont nombreux et leurs usages diversifiés. Pourtant, la diminution du prix d'achat et de fabrication est un fait avéré. La montée de la concurrence et l'accroissement de la demande de produits connectés à bas coût, font chuter les prix.

De plus, l'amélioration de la miniaturisation des microprocesseurs, de leur performance et la diminution de leur consommation énergétique expliquent l'explosion des IOT ces dix dernières années.

Le schéma, ci-après, montre la répartition des coûts moyens d'un projet de conception d'un IOT.



SOURCE : BUSINESS INSIDER

II.2 Les forces données à l'entreprise

Les IOT visent aussi à faciliter la prise de décision dans de multiples domaines (diagnostic intelligent, maintenance prédictive, optimisation d'asset.)
Lorsqu'un IOT émet une information, elle va transiter par internet jusqu'à l'entreprise. En fonction du type d'IOT et d'informations, l'entreprise pourra alors prendre une décision. Un IOT peut aussi bien fournir une simple notification et une alerte (dépassement de température, emplacement de l'IOT). L'entreprise peut alors anticiper et réagir plus rapidement face à un incident.

Une entreprise qui met en place un IOT va pouvoir répondre à plusieurs problématiques :

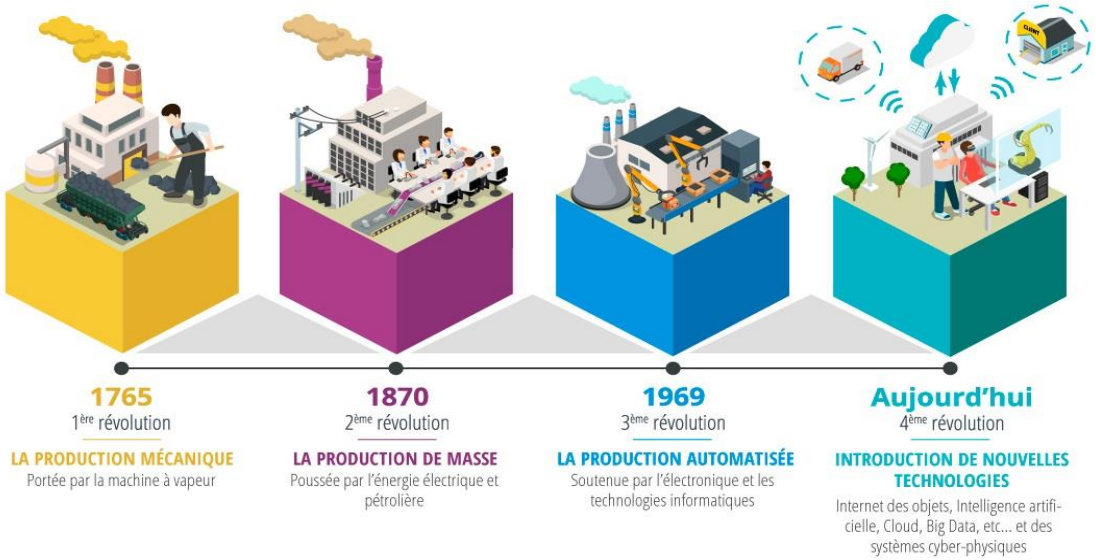
- Comment être réactif en cas de piratage de mes équipements ? Pour cela, il est possible de mettre en place IOT qui contrôlera tout comportement anormal.
- Comment améliorer mon image et satisfaire mes clients ? Pour cela, l'utilisation d'IOT va permettre d'améliorer des processus métiers à partir de données collectées par l'IOT.
- Comment garantir la sécurité de mes collaborateurs ? Pour cela, il est possible de mettre en place des IOT qui contrôlent les accès et la surveillance des locaux en temps réel. Il existe même des capteurs qui surveille la position et les mouvements des collaborateurs et ainsi éviter tout accident.

On peut facilement surveiller à distance la température d'une pièce (salle serveur).

BÉNÉFICES CLÉS DE L'IOT
efficacité opérationnelle optimisée
prise de décision optimisée (BU)
optimisation de la productivité
meilleur monitoring des actifs
expérience utilisateur améliorée (UX)
optimisation des produits
fiabilité de production
développement d'usages et de services
exploitation de la smart data
lutte contre la fraude
réduction des immobilisation via maintenance prédictive
satisfaction client
optimisation des coûts
migration du business model

II.3 Industrie 4.0

L'industrie 4.0 est née de l'émergence de nouvelles technologies. Elle désigne une nouvelle génération d'usines connectées, robotisées et intelligentes. C'est une usine où les capacités de production se déploient en fonction de ce que l'usine doit produire.



Les apports des IOT dans l'industrie 4.0

Les IOT s'impose de plus en plus dans les processus industriels. C'est l'un des piliers constituant l'industrie 4.0.
Ils vont permettre de contrôler la qualité de l'automatisation, de réaliser des maintenances préventives. Tout en offrant une aide pour la gestion et le renforcement de la sécurité des installations. S'ajoute à cela, la gestion des ressources et des stocks dans le but de maximiser la production et limiter les pertes.

II.4 Les secteurs porteurs

Parmi les secteurs touchés par les IOT. Certains secteurs sont plus porteurs que d'autres. On retrouvera le secteur de l'industrie, la logistique, l'agriculture et la santé.

- **L'industrie (industrie 4.0)** : Surveillance de la température et de la pression d'une chaudière. Capteur indice de production.
- **L'agriculture** : Capteur pour prévoir le gel et protéger les cultures.
- **La logistique :** Tracking des palettes ou encore de conteneurs, également avec la possibilité d'effectuer des inventaires en temps réel. Guidage des robots pour centre de tri en chine.
- **La santé** : Tracking du matériel médical, les robots de téléprésence.

II.5 Les applications

Les entreprises utilisent des IOT sans même réellement le savoir. Parmi ces IOT nous retrouverons :

- Imprimantes connectées
- Télévisions (salles de réunion)
- Vidéoprojecteurs
- Caméras de surveillance

- Alarmes connectées

On retrouvera d'autres IOT qui sont plus spécifiques au domaine de l'entreprise, comme :

- Les robots de téléprésence dans le domaine médical.
- Chaussures de sécurité et les casques connectés dans le domaine de l'industrie et des travaux public.
- Les automates utilisés dans le domaine de l'industrie et du bâtiment.

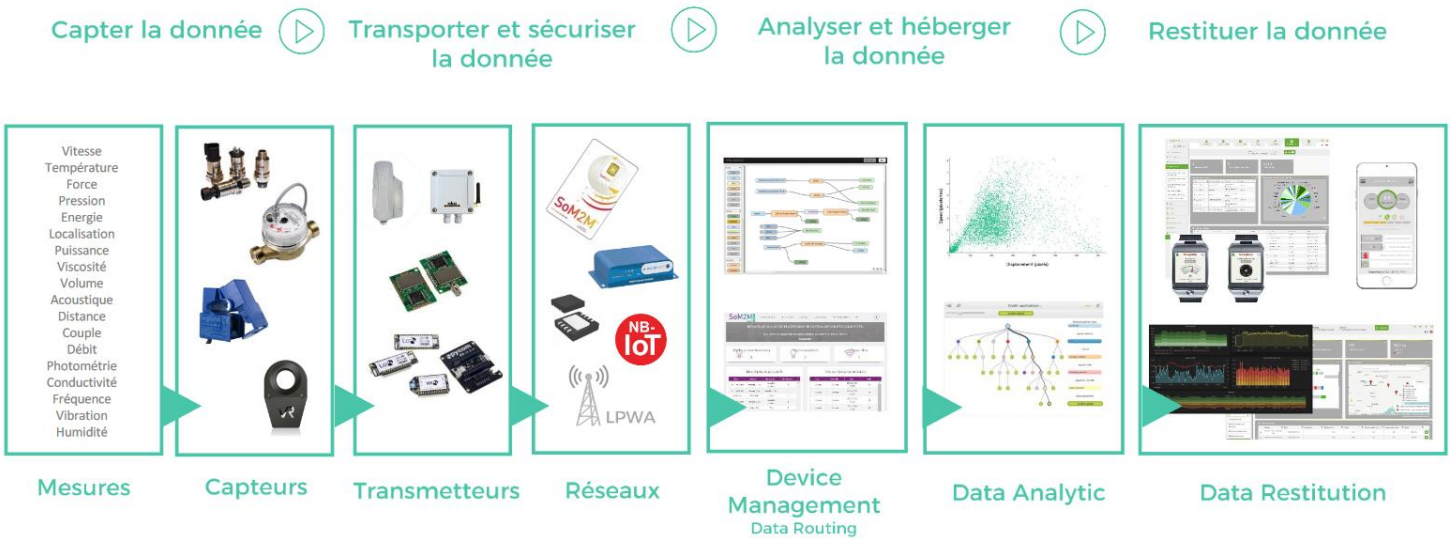
Des entreprises fabriquent ou utilisent d'autres IOT dans un but précis :

- **Bayard :** robinets intelligent pour surveiller en temps réel un parc incendie en horodatant toutes les manipulations : ouverture/fermeture. Dans le but d'également récupérer des informations tel que des rapports, les estimations du volume d'eau prélevé, détection du renversement de poteau.
- **Coval :** automates pour automatiser les réseaux de vide industriel (pompes à vide, ventouse)
- **Crouzet automation :** utilisation d'automates pour la gestion de l'eau et des accès.
- **Hager :** fabrication d'alarmes connectées.
- **Vape rail :** automates pour la surveillance des chemins de fer.

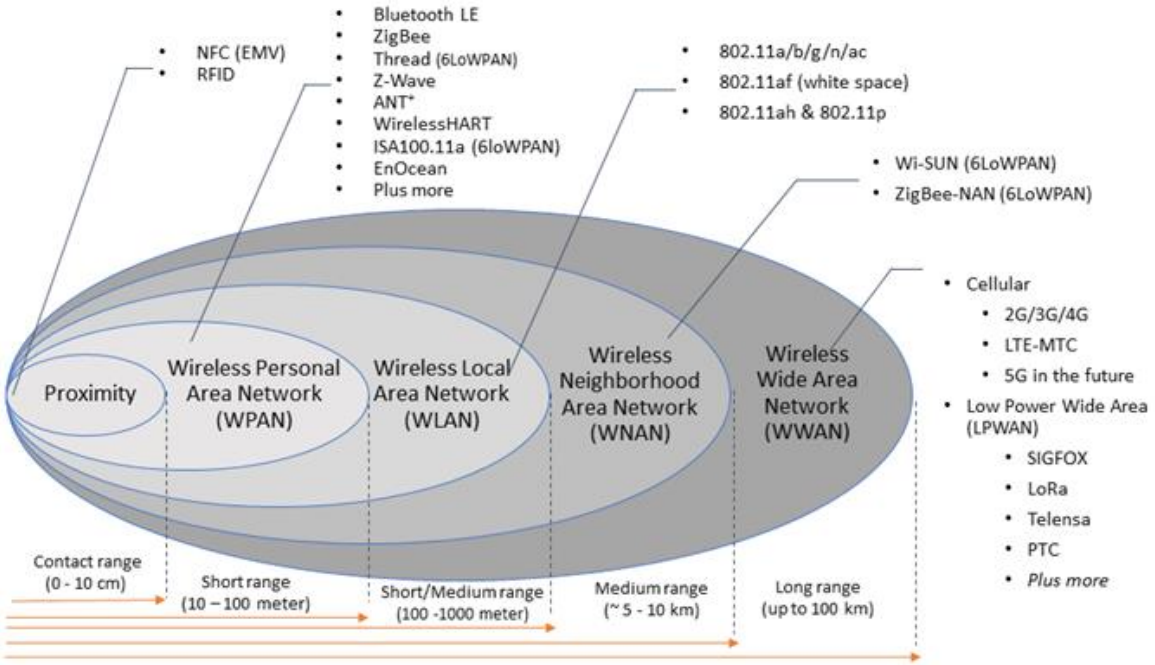
II.6 Nouvelles technologies

L'internet des objets et le Big Data sont deux technologies interconnectées et indissociables. Les objets connectés génèrent des données grâces à des puces et des capteurs embarqués, qui peuvent être analysées pour dégager des tendances et informations à des fins diverses. A mesure que le nombre d'objets connectés augmente, le volume de données générées explose. Ainsi pour pouvoir les prendre en charge et les analyser en temps réel pour en extraire des informations exploitables, il est nécessaire de s'en remettre aux outils analytiques des Big Data. C'est la raison pour laquelle le Big Data et les IoT sont liés.
Les données à retrouver vont par exemple être un rythme cardiaque, un nombre de pas, une localisation. Certains capteurs vont même mesurer les performances des machines et prévoir d'éventuelles défaillances.
Le Machine Learning va ensuite permettre de repérer des modèles de données et les entreprises pourront notamment, avec ces patterns, mettre en place une maintenance prédictive sur des machines industrielles.
Toutes les notions de prédictions vont être améliorées et poussées à un niveau de précision plus élevé grâce à l'intelligence artificielle. La grande évolution de ce secteur permettra dans le futur de faire des prédictions plus précises et d'anticiper au mieux les besoins des utilisateurs et surtout les menaces liées à la sécurité.
La combinaison de toutes ces technologies va pouvoir également contribuer à la Business Intelligence (BI) qui va proposer des analyses plus visuelles pour permettre une prise de décision plus facile dans les différents niveaux hiérarchiques des entreprises.

Chapitre III. Le fonctionnement de l'IOT

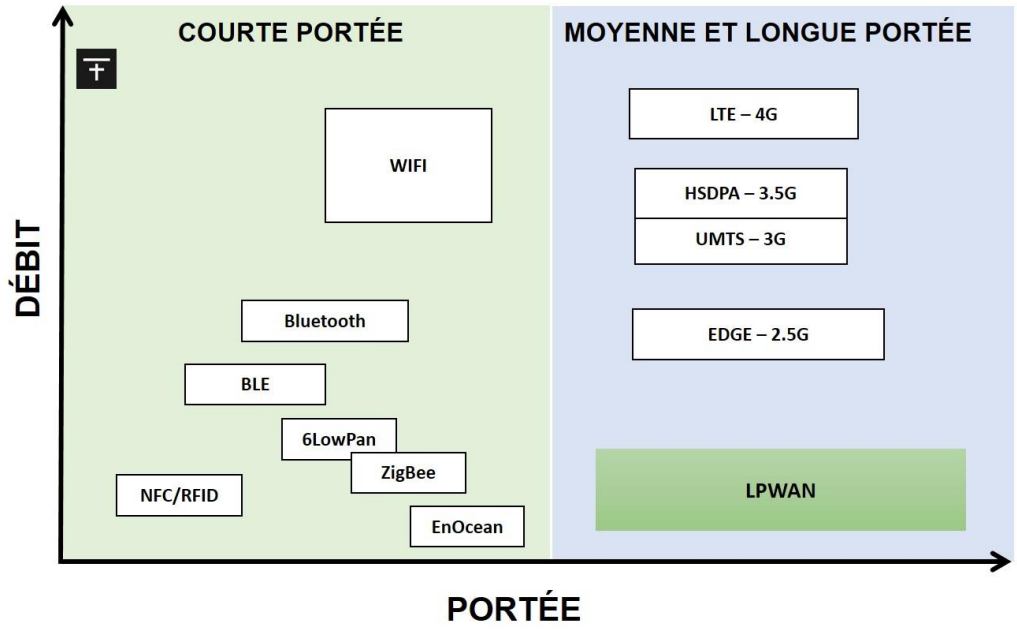


III.1 Présentation des différentes liaisons



III.2 LPWAN

Les réseaux LPWAN (low-power wide-area network) sont des réseaux sans fils bas débit à longue portée, optimisés pour des dispositifs dont les ressources sont limitées. Leur essor répond à un besoin grandissant de connectivité, d'information et d'efficience énergétique.



Parmi les plus notables, on peut citer SigFox et LoRaWan. Ces deux réseaux LPWAN font l'objet d'une très grande attention. De nombreuses entreprises et grands groupes investissent sur ces technologies prometteuses.

III.2.1 Sigfox

III.2.1.1 Présentation

Sigfox est un réseau longue portée et à bas débit qui permet l'émission et la réception de données de taille réduite (quelques octets de charge utile).
C'est un système de connexion utilisant des signaux de fréquence radio ultra rapide et de longues portées. Elle est appelée bande ultra étroite (UNB = Ultra Narrow Band).

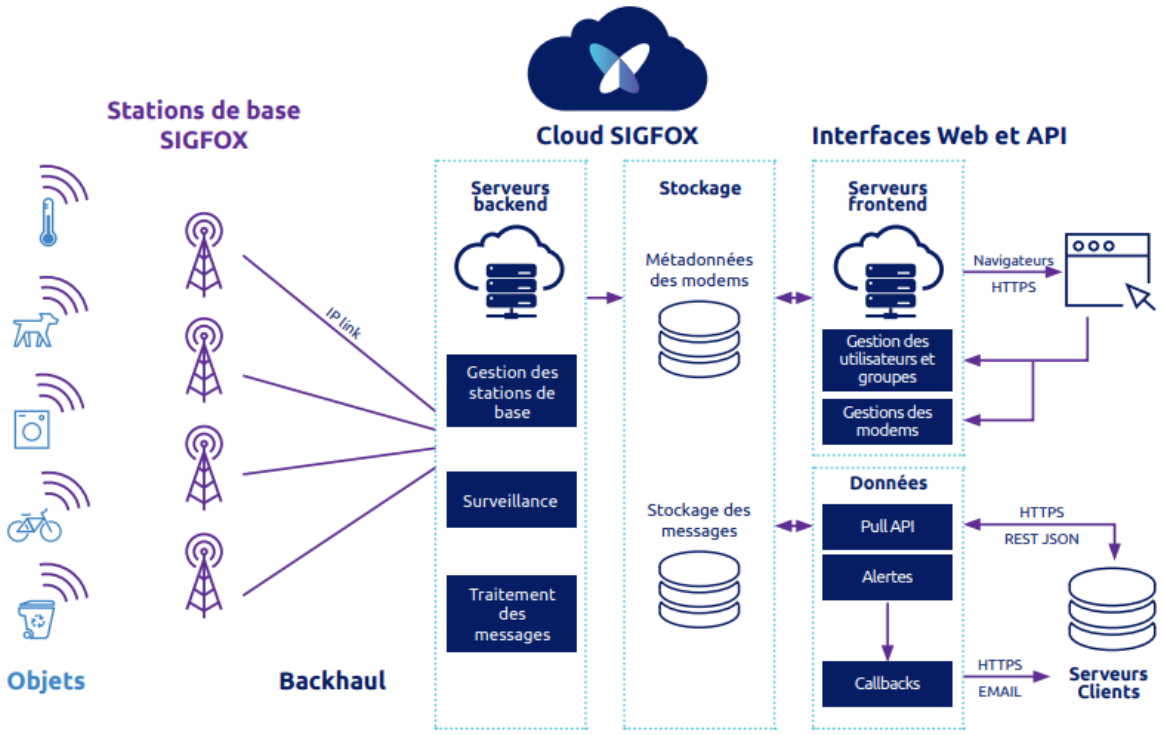
III.2.1.2 Technologie SigFox

La technique d'émission innovante introduite par SigFox repose sur ce que l'on appelle la bande ultra étroite (UNB – Ultra Narrow Band). Ce type de signal, en plus de couvrir une longue portée, fait quelques dizaines de hertz de large contre une centaine de kHz voire MHz dans le monde GSM, ainsi ce signal concentré est beaucoup plus performant et résiste plus efficacement aux brouillages.
Il est à noter que le protocole de communication SigFox est propriétaire.
La portée théorique est exprimée en dB et est désignée sous le terme « bilan de liaison ». Le bilan de liaison est la somme de la sensibilité de la station de base, du gain des antennes et de la puissance de sortie du côté de l'objet.
Sur le forum de l'opérateur, un des employés de SigFox, Aurelien Lequertier, fait une démonstration théorique avec un modèle d'antenne particulier et en environnement dégagé. Dans ces conditions, le signal émis a une atténuation de l'ordre de 160 dB, ce qu'il résume à une portée de l'ordre de 2500 Km environs.
Dans un cas réel, dans un environnement dégagé, une portée de 1151Km a été enregistrée sur les côtés Portugaises.
En Zone urbaine cela dépend de beaucoup de facteurs (atténuation, obstacles, matériaux, espacement des relais…).

Quoi qu'il en soit, la stratégie de la société SigFox n'est pas temps de proposer de telles portées à ses clients, mais un maillage efficace d'antenne relais sur des distances permettant une réception fiable.

III.2.1.3 Architecture technique

L'architecture de l'infrastructure du réseau SigFox peut être décomposée en 3 grandes parties :



La particularité de SigFox tient entre autres à son modèle commerciale et son infrastructure. La partie gérée par SigFox est très orientée service clé en main, assurant un confort certain pour les entreprises.

Les détails techniques du protocole sont gardés secret.
Il en est de même pour l'infrastructure « cloud ». Toutefois la société communique sur la fiabilité et la sécurité de cette « boite noire », tout cela pour faire naitre un sentiment de confiance.
Il est à noter que la société autorise toute entreprise cliente à obtenir des informations plus détaillées sous condition d'une signature d'un contrat de non divulgation.

III.2.1.4 Modèle économique

SigFox se positionne comme opérateur de réseau. Il assure également une certification du matériel auprès de ses constructeurs partenaires.
SigFox délègue la construction du matériel à des entreprises associées tout en assurant une certification de ces dernières. Cet encadrement de la chaine de production permet de garder une maitrise sur la qualité des dispositifs se connectant au réseau et répondant à un cahier des charges stricte.
Le modèle commercial s'oriente également vers le service via la solution SigFox Cloud. Un système d'abonnement est proposé mais les tarifs sont peu communiqués et dépendent

grandement du type d'objet et de leur nombre. Il s'agirait d'offres entre 3€ et 9€ par an et par objet. Ces informations sont toutefois à prendre au conditionnel.

III.2.1.5 Détail des communications

La réglementation européenne autorise l'utilisation de la bande de fréquence publique pendant 1 pour cent du temps, ce qui correspond à six messages de 12 octets par heure ou 140 messages par jour.
La communication entre le dispositif IoT et l'infrastructure peut avoir lieu de manière bidirectionnelle. Toutefois, la majorité de la communication se fait du dispositif vers l'infrastructure.
Chaque message est transmis 3 fois, sur 3 fréquences aléatoires sur un court laps de temps (~45ms entre chaque message). Ce mécanisme permet d'augmenter les chances de bonne réception du message par le relai ou par le périphérique.

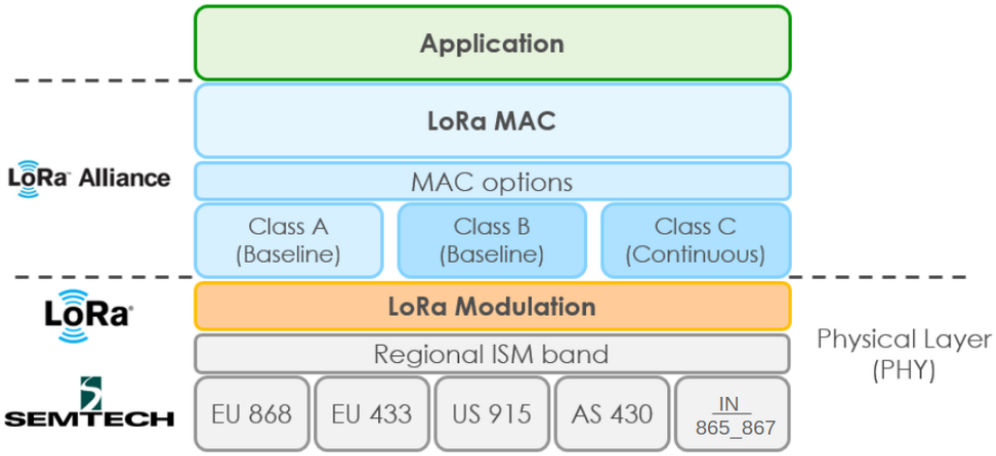
III.2.1.6 Sécurité

Bien que le protocole et l'infrastructure ne soit pas divulgué, des travaux de reverse engineering ont été conduits, les plus notables sont ceux de Paul Pinault et Florian Euchner.
De leurs travaux nous apprenons que l'intégrité et l'authenticité des messages se fait via un algorithme CBC-MAC (cipher block chaining Message Authentication), et qu'à leur connaissance, pas de vulnérabilité d'implémentation n'a encore été identifié (février 2019).
Tous les messages inclus un compteur pour se prémunir des attaques par replay (anti-réexécution)
De base, il n'existe pas de mécanisme pour assurer la confidentialité des données (des offres existent cependant). La documentation technique indique un « Chiffrement de la charge utile en option pour garantir la confidentialité des données. ».
Toutefois, sans cette option, les données sont brouillées via un algorithme identifié par Florian Euchner, il est donc possible, avec un nombre de trame intercepté et les bons outils disponibles sur internet, de les déchiffrées relativement facilement.
Il s'agit d'un choix de design assumé par SigFox, cela permet entre autres de voir à la baisse la consommation d'énergie (les mécanismes de chiffrement sont par essence gros consommateur de ressources systèmes)
Ce point peut être important selon le projet conduit. Le chiffrement proposé en option par SigFox n'est pas un chiffrement de bout en bout. Avec cette offre, la charge utile (les données) est déchiffrée dans la partie « cloud » sans que des détails ne soient communiqués par la société sur ce point. Bien entendu, il est nécessaire d'acquérir du matériel stipulant cette possibilité.

III.2.2 LORAWAN

III.2.2.1 Présentation

Le réseau LoRaWan (Long Range ou longue portée) est un protocole de communication radio qui permet aux objets connectés d'échanger des données de faible taille en bas débit.
Une des couches du protocole LoRaWan est propriétaire (LoRa PHY), les autres sont open sources. Cela permet à tout organisme, de mettre en place son propre réseau.
De plus, un groupement d'industriel, la LoRa Alliance tend vers une standardisation.

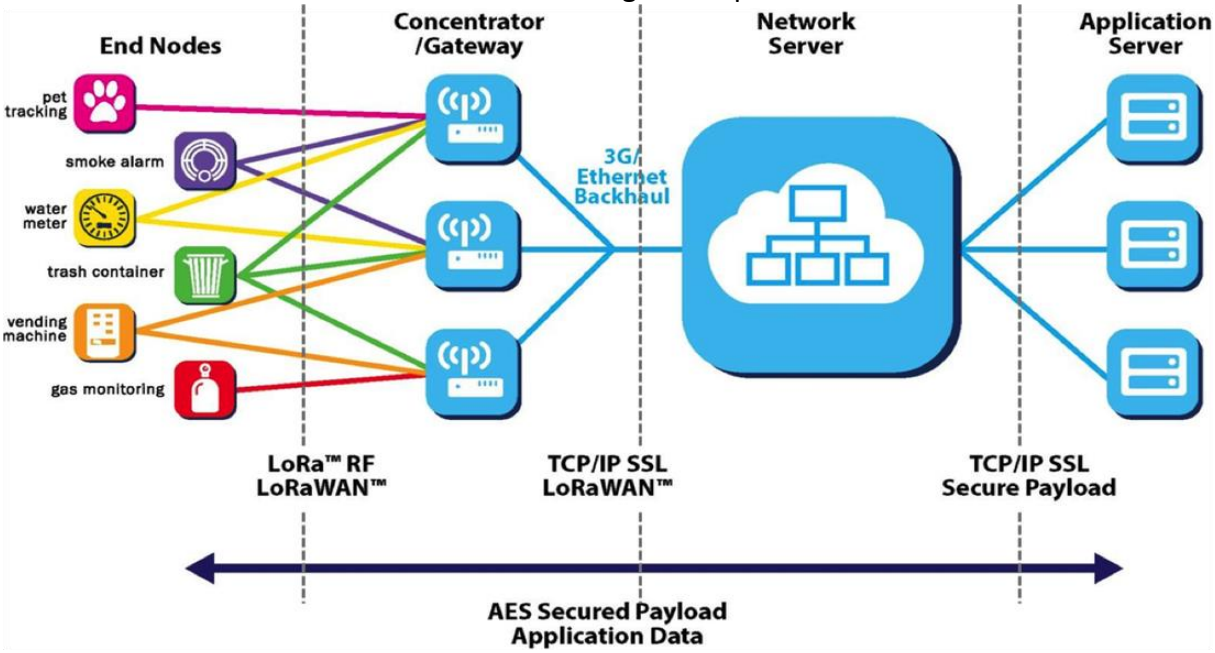


III.2.2.2 Technologie LoraWan

La modulation LoRa utilise une variante de l'étalement de spectre appelée Chirp Spread Spectrum pour coder l'information.
Il s'agit d'un signal sinusoïdal dont la fréquence augmente ou diminue au cours du temps. Initialement destinée à des applications militaires, cette modulation est également utilisée par les radars et les sonars. Elle est robuste contre les perturbations et les brouillages.

III.2.2.3 Architecture technique

La LoRa Alliance standardise l'architecture en 4 grandes parties :



III.2.2.4 Modèle économique

La grande force de LoRa est de permettre aux entreprises comme aux particuliers de créer eux-mêmes leur propre réseau ou bien de d'utiliser les réseaux des grands opérateurs. Cette souplesse permet, dans le cadre d'une entreprise souhaitant implémenter le sien, de s'assurer la maitrise complète de tout son réseau.

L'utilisation d'un réseau existant est soumise à un abonnement qui varie selon les opérateurs (en moyenne entre 3€ et 10€ par dispositif et par mois).
La mise en place de son propre réseau dépend de son envergure. A titre informatif, les coûts d'un seul relais peuvent varier de 200€ à plus de 2000€ selon les modèles.

III.2.2.5 Détail des communications

Selon la classe du dispositif, des particularités techniques s'appliquent.
Concernant les classes A, les messages ascendants (à savoir du dispositif vers le relai), une transmission est émise suivi par un passage très bref en mode écoute. Ce mode d'écoute autorise les transmissions descendantes (de l'infrastructure vers le dispositif) et peut être utilisée pour modifier la configuration du dispositif.
Cette classe de dispositif est la plus économique en termes d'énergie.

III.2.2.6 Modèle d'enrôlement des dispositifs

Pour qu'un dispositif puisse intégrer un réseau LoRaWan, deux méthodes d'enrôlement sont proposées.
Over The Air Activation (OTAA) : Cet enrôlement permet de générer des sessions à chaque communication, un peu à la manière d'une connexion TLS. Dans ce mode, le dispositif intègre un jeu de clée privées : une identifiant le dispositif, une identifiant la couche applicative, une pour chiffrer les communications.
Activation By Personalization (ABP) : Cet enrôlement intègre des identifiants de sessions pré-générés. Il est idéal pour les phases de recette.

III.2.2.7 Sécurité

L'intégrité et l'authenticité est assurée par un algorithme de chiffrement éprouvé. Cependant, l'implémentation a souffert de quelques failles par le passé et permettait d'usurper l'identité du dispositif émetteur du message. Depuis, l'implémentation a été revue et corrige ce problème.
Le chiffrement de bout en bout est la norme pour LoRaWan. Cependant, le même problème d'implémentation a été détecté en 2016 et a depuis été rectifié.
La stratégie open source de LoRa est une de ses forces et permet d'identifier et de corriger ce genre d'erreur de conception.

Chapitre IV. La sécurité de l'IOT

IV.1 Attaques des IOT

Comme dans tous les secteurs de l'informatique, il existe des grandes attaques sur des objets connectés ou grâce à des objets connectés. Les conséquences sont parfois graves car elles peuvent mettre aussi bien les utilisateurs en danger mais aussi compromettre toute l'activité d'une entreprise. Ici nous présentons les plus connus et celles dont nous avons le plus entendu parler.

Le botnet Mirai : En octobre 2016, la plus grande attaque de déni de service a été lancée sur le fournisseur de services Dyn. Les attaquants recherchaient des IOT vulnérables sur internet et les utilisaient pour envoyer un grand nombre de requêtes vers les serveurs de Dyn. L'accumulation de ces requêtes venant de plusieurs centaines de milliers d'IoT compromis a entrainé la surcharge des serveurs et a eu un impact sur plusieurs multinationales notamment Twitter, The Guardian, Netflix, Reddit ou CNN.

Les dispositifs cardiaques piratables de St Jude : Début 2016, la FDA a confirmé que les dispositifs cardiaques implantables de St. Jude Medical présentaient des vulnérabilités qui pourraient permettre à un pirate informatique d'y accéder. Une fois dedans, ils pourraient épuiser la batterie ou administrer une stimulation ou des chocs incorrects.

Le Jeep Hack : En exploitant une vulnérabilité de mise à jour du micrologiciel, des pirates informatiques ont pris le contrôle du véhicule par-dessus le réseau cellulaire Sprint et ont découvert qu'ils pouvaient le faire accélérer, le ralentir et même le faire s'écarter de la route.

IV.2 Mauvaises pratiques des constructeurs

Les constructeurs d'IOT sont dans une démarche de rentabilité et d'innovation constante. La sécurité des IOT lors de la conception ne fait pas partie des priorités des constructeurs. Ils jugent le coût pour la sécurité de l'IOT trop important pour la prendre en compte lors de la conception du produit.

Les nouveaux IOT commercialisés ne bénéficient pas d'un suivi rigoureux de la part des constructeurs. Les firmwares ne sont pas mis à jour régulièrement dans le but de contrer des cyberattaques.

Un nouveau produit est à peine commercialisé qu'un nouveau produit le remplace. Forçant les constructeurs à abandonner le suivi du produit pour en créer un nouveau pour contrer la concurrence.

IV.3 Maquettes

IV.3.1 Shodan

Shodan est un moteur de recherche d'appareils connectée à internet. Il a été créé en 2009 par John Matherly. Son objectif est de rechercher à travers le web toutes les adresses IP des objets connectés et de les répertorier en fonction de leurs caractéristiques. Il va être possible de faire des recherches en fonction du type d'objet (webcam, imprimante, routeur, porte de garage, ampoule, etc…), de la position géographique, du système d'exploitation, du constructeur et même d'une plage d'adresses IP.

Pour avoir accès à l'entièreté de la base de données d'objets connectés, Shodan oblige à payer mais les recherches sont également possibles gratuitement avec comme restriction des résultats de recherche limités.

Le moteur de recherche est particulièrement prisé par les spécialistes et passionnés de la sécurité informatique mais aussi par des personnes malveillantes car il permet de révéler un bon nombre de failles présents sur internet.

Shodan n'est évidemment pas le seul moteur de recherche présent, il en existe quelques autres moins connus mais pouvant être tout aussi efficace comme:

- FOFA
- CENSYS
- ONYPHE

L'objectif lors de la présentation est de montrer que certaines caméras sont facilement accessibles et peuvent montrer des images mettant en danger les acteurs et les activités d'une entreprise.

Shodan nous permet ainsi de se rendre compte qu'aujourd'hui le manque de sécurité sur les IoT est très présent et peut être facilement exploitable à travers ces outils. Que ce soit des caméras montrant des intérieurs d'entrepôts ou également des interfaces de systèmes SCADA, l'enjeu de la cybersécurité est important et la sensibilisation des entreprises et même des particuliers doit se faire au plus vite.

IV.3.2 Exploitation d'un Firmware

Le firmware représente le logiciel interne qui est embarqué dans l'objet connecté et qui permet de le faire fonctionner.
Notre deuxième démonstration avait une vision davantage technique et le choix a été de montrer une fois de plus que la partie sécurité lors du développement d'un firmware d'un IoT est absente.
Le fait de voir dans le binaire du firmware le nom d'utilisateur et le mot de passe le démontre facilement et même si l'utilisateur final n'est pas directement touché par cette faille de sécurité, on peut questionner les méthodes de développement utilisées et le chiffrement choisi par les entreprises. Des méthodes qui sont inquiétantes et qui donnent une idée de l'intérêt que portent les entreprises pour la sécurité de leurs objets.

IV.4 Les bonnes pratiques à mettre en place

IV.4.1 Les bons constructeurs

Les fuites de données sont de plus en plus fréquentes aujourd'hui et les entreprises doivent comprendre qu'elles sont en grande partie responsables et c'est pour cela qu'elles doivent prendre les risques au sérieux. La sensibilisation fait partie des points importants comme dans tout le secteur de la sécurité informatique et contribue à faire prendre conscience aux entreprises les responsabilités qu'elles ont envers les utilisateurs. Les entreprises peuvent aussi se prémunir des répercussions en prenant des assurances pour être protégé financièrement en cas d'attaque.
Les menaces peuvent également venir des différentes parties prenantes du projet et les entreprises doivent donc, pour garantir la sécurité de leurs objets, s'assurer que les fournisseurs soient conscients des risques et qu'ils aient une vision de la sécurité en accord avec tous les acteurs.
L'obtention de certification est un bon moyen pour l'entreprise de faire le point sur l'existant et de définir les bons outils qui aideront à améliorer les éléments manquants pour être certifié. Les certifications sont aussi un bon argument face aux clients qui aura davantage confiance vis-à-vis du respect de la sécurité.

IV.4.2 Sigfox

Risque : Les clés privées assurant l'authenticité et l'intégrité des données sont identiques sur tous les dispositifs. En cas de compromission d'un des dispositifs, l'intégralité de la flotte d'IOT est compromise.
Solution : S'assurer que les clés privées utilisées pour assurer l'authenticité et l'intégrité des données est bien unique. Pour cela SigFox assure la chaine de production de tous les dispositifs éligibles à son réseau. Notre préconisation est donc de se rapprocher des constructeurs partenaires et certifiés par SigFox.

A noter que cela ne sera bientôt plus systématique. En effet, SigFox depuis février 2019 a ouvert une partie de son code propriétaire et encourage les constructeurs à produire des dispositifs compatibles avec son réseau, il s'agit donc d'un point critique à prendre en compte.

Risque : Opacité quant à la sécurité annoncée dans la partie « infrastructure » de SigFox.
Solution : SigFox autorise toute entreprise à obtenir des informations sur son infrastructure sous condition de signature d'une clause de non divulgation. Nous préconisons donc de se rapprocher de SigFox et, selon la nature de votre projet, d'envisager avec eux un audit de cette dernière.

Risque : La charge utile contenant les données transite sur le réseau SigFox (des dispositifs aux relais) n'est pas chiffrées mais passée dans un algorithme de brouillage (scrambling algorithm) permettant à un individu ayant les bons outils (disponibles librement sur internet pour la partie applicative) de décrypter les données.
Solution : SigFox offre une solution de chiffrement basée sur de l'AES 128 et une puce dédiée. Cette offre, annoncée gratuite, n'est pas un chiffrement de bout en bout mais permet de chiffrer la charge utile du dispositif vers l'infrastructure SigFox. Puis, les données transitent sur internet via un chiffrement TLS vers le backend du client. Ce point est à prendre en compte et rejoint la partie confiance en l'infrastructure SigFox.
Si les données sensibles ne doivent pas être déchiffrées par une autre entité que votre entreprise, SigFox recommande d'avoir recours au développement d'une solution de chiffrement de bout en bout. Pour cela, il convient de se rapprocher de SigFox pour obtenir les librairies et informations nécessaires.

Risque : Une vulnérabilité a été trouvée dans le protocole, dans un firmware… et pourrait être exploitée.
Solution : Dans le cadre de nos recherches, nous n'avons pas trouvé de mention claire quant au patch management des dispositifs (end-devices). Nous préconisons de se rapprocher de la société SigFox pour obtenir des solutions concrètes.

IV.4.3 LoraWan :

Risque : Les clés privées assurant l'authenticité et l'intégrité des données sont identiques sur tous les dispositifs. En cas de compromission d'un des dispositifs, l'intégralité de la flotte d'IOT est compromise.
Solution : S'assurer que les clés privées embarquées (DevEUI, AppEUI, AppKey permettant une activation OTAA – ou NwkSKey et AppSKey permettant une activation APB) sont bien unique sur chacun des dispositifs. Pour cela, il convient de se rapprocher du constructeur de dispositif.

Risque : Compromission des clés (NwkSKey and AppSKey) lors d'une activation APB (Activation By Personalization) permettant une attaque de type homme du milieu (man in the middle).
Solution : Privilégiez dans la mesure du possible une activation Over The Air Activation (OTAA). Cela permet une génération de nouvelles clées (NwkSKey et AppSKey) à chaque session de communication entre un dispositif et un relai.

Risque : Compromission physique d'un dispositif, permettant à un attaquant de récupérer les clés privées embarquées utilisées pour le chiffrement des données et communications.

Solution : Il convient de s'assurer que le dispositif stock les secrets à l'aide d'un microcontrôleur sécurisé. Ces dispositifs permettent de garantir l'authenticité des secrets stockées et empêches l'extraction et le clonage. Nous préconisons de se rapprocher du constructeur du dispositif pour évaluer l'intégration d'un tel dispositif.

Risque : L'implémentation de LoRa n'est pas conforme aux spécifications préconisées par LoRa Alliance.
Solution : En effet, tout opérateur est en charge de son réseau et de la gestion de son infrastructure. Les entreprises utilisant un réseau existant géré par un de ces opérateurs doit s'assurer que l'implémentation est conforme ou adaptée. Pour cela nous préconisons de se rapprocher de l'opérateur pour lancer des actions d'audit.

Risque : Les dispositifs ne sont pas conformes aux spécifications préconisées par LoRa Alliance.
Solution : Il convient de s'assurer auprès du constructeur/fournisseur du respect des spécifications préconisées par la LoRa Alliance. Nous insistons en particulier sur la génération des clés privées (voir risque plus haut)

Risque : Une vulnérabilité a été trouvée dans le protocole, dans un firmware… et pourrait être exploitée.
Solution : Selon la LoRa Alliance, il est possible de déployer un nouveau firmware sans intervention physique sur les dispositifs, appelé Firmware Over-The-Air (FOTA). Nous préconisons de se rapprocher du constructeur du dispositif ainsi que du gérant du réseau pour s'assurer que cette méthode peut être mise en œuvre.

IV.4.4 Minimiser les vulnérabilités des IOT

Pour minimiser les vulnérabilités liées aux IOT, il est important de respecter les points suivants :

- Changer le mot de passe par défaut du périphérique. Si le mot de passe ne peut pas être changeable, il est préférable de ne pas s'en servir.
- Réaliser un ensemble de test avant de mettre en production le périphérique.
- Segmenter son réseau enfin d'isoler les périphériques potentiellement vulnérables. Dans le but de les éloignés des ressources et des réseaux centraux.
- N'utiliser que les fonctionnalités dont vous avez besoin. (Exemple : une télévision connectée qui est simplement utilisée pour de l'affichage. Nous pouvons désactiver l'utilisation de la connectivité à internet)
- Mettre en place d'un cycle d'amélioration continu avec des mises à l'épreuve de l'IOT : audit, des pentestes.
- Mettre en place le chiffrement à l'envoi et la réception de données.
- Mettre à jour régulièrement les périphériques.
- Utiliser les produits qui ne sont plus maintenu par les fabricants.

IV.5 RGPD et l'IOT

Avec l'évolution de l'informatique par le biais des télécommunications, des objets connectés et du Big Data, il est apparu que les réglementations mises en place n'étaient plus adaptées, qu'il fallait aller plus loin et surtout simplifier.
Le règlement général sur la protection des données personnelles (RGPD) est un règlement européen entré en vigueur le 25 mai 2018 sur tout le territoire de l'Union européenne. Il

concerne toutes les entreprises qui traitent ou hébergent les données à caractère personnel des résidents européens.

Le RGPD impose aux entreprises et organismes traitant des données sensibles (données à caractère personnel) de nombreuses obligations.
Les entreprises et organismes doivent :

- Garantir la sécurité maximale des données personnelles
- Demander en aval le consentement des personnes concernées
- Etre transparente dans le traitement des données – c.à.d. une obligation d'information et de conseil des personnes concernées
- Respecter les droits de la personne concernée lors du traitement des données
- Tenir un registre des traitements de données – ce registre est obligatoire quand le volume d'une entreprise dépasse les 250 personnes
- Nommer un délégué à la protection des données (DPO)
- Effectuer des Analyses d'impact préalables aux traitements des données personnelles permettant de gérer les risques éventuels lors du traitement (une fuite des données par exemple)

Les entreprises vont devoir instaurer des mécanismes et des procédures internes qui devront leur permettre de démontrer le respect aux règles relatives à la protection des données.
La protection et la sécurisation des données à caractère personnel doivent être intégrées dès l'origine d'un projet IOT avec le concept de Privacy By design.

Les fabricants et les concepteurs d'objets connectés vont devoir penser à l'impact que le traitement peut avoir sur la vie privée des utilisateurs. Ils devront y penser, mais devront pouvoir le démontrer et pour se faire disposer en interne de « cahiers de développement ». Ils pointeront et identifieront toutes les mesures qui permettent d'assurer la protection des données de l'utilisateur dès la création de l'objet et tout au long de son cycle de vie.

De plus, chaque responsable de traitement devra mettre en place les mesures techniques et organisationnelles appropriées permettant d'assurer la traçabilité des données. Chaque fois qu'un fabricant sera informé d'une faille de sécurité concernant son produit, d'un piratage ou de quelque violation que ce soit, il devra en informer l'autorité de contrôle (en France : la CNIL) dans les 72h ainsi que les personnes concernées.

Dans le cas d'un piratage ou d'un vol de données, le renvoi de l'objet connecté est inutile. Le méfait a eu lieu et les données sont « dans la nature ». La mise en conformité est réalisée après coup par le biais d'une mise à jour afin que le problème soit corrigé.
Le RGPD donne aux autorités de contrôle le pouvoir d'imposer des amendes allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire annuel mondial en cas de non-respect des règles relatives à la protection des données

Chapitre V. Recommandations

Les recommandations représentent les conseils que l'utilisateur final peut appliquer pour garantir un peu plus sa sécurité et celle de son entourage.

Dans un premier temps, il est important de se tenir informer régulièrement des nouvelles bonnes pratiques et de l'actualité autour des IoT. Cela contribuera à une partie du travail de

sensibilisation qu'il est nécessaire d'avoir car l'utilisateur sera au courant des conséquences d'une mauvaise gestion de la sécurité et pourra prévoir des mesures pour diminuer les impacts.

Le deuxième point est la mise à jour régulière des équipements, cela concerne tout l'informatique y compris les objets connectés et représente la meilleure défense face aux nouvelles vulnérabilités. Normalement très simple à appliquer pour l'utilisateur final, les mises à jour dans le secteur des IoT sont encore une pratique peu efficace car les constructeurs préfèrent développer de nouveaux objets plutôt que de garantir la pérennité de leur IoT en proposant des mises à jour régulières et faciles à installer.

Le troisième point est également important pour tout type de projet informatique car l'objectif est de s'assurer que tous les acteurs ayant participés au développement de l'IoT sont dignes de confiance et sont en accord avec les normes de sécurité existantes. Des tests d'intrusion devraient être réalisés en amont du projet et tout au long du développement pour finalement proposer un objet qui répond au concept "Security-by-design" signifiant que la sécurité de l'objet a été prévue dès la conception.

Chapitre VI. Annexes

Table des matières

VI.1 Glossaire

- - A - -

Alimentation par Ethernet (PoE) : L'alimentation par Ethernet (ou PoE) se compose de plusieurs systèmes normalisés qui permettent de transférer les données et l'alimentation électrique par l'intermédiaire d'un seul et même système Câble Ethernet, d'une source d'alimentation (PSE) à plusieurs appareils à basse tension (PD), tels que caméras, téléphones VoIP, routeurs Wi-Fi et autres.
Remarque : Povers over HDBaseT (PoH) est une version de PoE spécialement conçue pour les applications multimédia, permettant jusqu'à 10,2 Gbps de vidéo et audio non compressées, 100BaseT Ethernet, signaux de commande et alimentation pour partager le même câble, sur des distances pouvant atteindre 100 m, avec des connecteurs RJ45.
Analytics : Systèmes logiciels qui analysent les données générées par les dispositifs IoT. L'analyse peut être utilisée pour une variété de scénarios, tels que la maintenance prédictive.
API (Application Programming Interface) ou Interface de Programmation : Moyen pour un logiciel de communiquer avec un autre logiciel
Appliance : Le terme « Appliance » est un anglicisme, qui correspond en réalité à "appareil", "équipement", associé la plupart du temps à un logiciel intégré ou fourni dans la même offre.

Attaque (ou menace informatique) : C'est l'exploitation d'un faille d'un système informatique à des fins non connues par l'exploitant du système et généralement préjudiciable.

- - B - -

Baie informatique : C'est une armoire technique qui centralise des équipements informatiques et téléphoniques.

Baie de stockage : Une baie de stockage peut être considérée comme un serveur spécialisé et totalement intégré, dont l'objectif principal est de servir des espaces sécurisés de stockage vers des serveurs d'applications.

Bande passante : Désigne le débit binaire maximal d'une voie de transmission.

Big data : Des actifs d'information à haut volume, à grande vitesse et/ou à grande variété qui exigent des formes rentables et novatrices de traitement de l'information qui permettent d'améliorer la compréhension, la prise de décision et l'automatisation des processus.

Bilan de liaison : Le bilan de liaison est un calcul par étapes permettant de déterminer la qualité d'une liaison.

- - C - -

CBC-MAC : Il s'agit de l'un des algorithmes pour les codes d'authentification de message (MAC). Il est basé sur un chiffrement par bloc

Charge utile : Désigne la partie d'une trame qui contient les données à transporter

Chirp Spread Spectrum : Type de modulation de fréquence utilisé dans certains protocoles de radiofréquence

Cloud computing : L'informatique en nuage consiste à exploiter la puissance de calcul ou et de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet.

Continuité de service : Le concept de continuité de service tend à se généraliser à l'ère du numérique pour la simple raison que les points de vulnérabilité sont aujourd'hui bien plus nombreux. Catastrophes naturelles, maladies, problèmes de transport et pannes de courant existent depuis toujours, mais le vaste réseau des technologies utilisées au 21e siècle et l'avènement des données numériques sont venus enrichir la liste des aléas commerciaux parfois appelés « points de vulnérabilité ».

Il est indispensable de pallier les défaillances des applications métier, les indisponibilités des sites Web (notamment si la plupart des activités s'effectuent sur Internet) ou les délais de récupération des données.

La planification de la continuité de service consiste avant tout à prévenir et envisager comment la société peut continuer à honorer ses obligations envers ses clients et ses actionnaires en toute situation. Vous devez assurer vos engagements de qualité de service en temps de crise, et être en mesure de restaurer tous ses systèmes et toutes ses données pour un retour à la normale dans les plus brefs délais.

Convergence IP : La convergence IP fait référence à la capacité de l'Internet d'agir comme une base unique pour diverses fonctions qui avaient traditionnellement leurs propres plates-formes.

- - D - -

Datacenter : Un centre de données, en français, est un endroit physique où sont rassemblées de nombreuses machines (bien souvent des serveurs) contenant des données informatiques.

DMZ : Une zone démilitarisée (en anglais : demilitarized zone) est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

Downlink : Réception de données

- - E - -

Edge (Une philosophie de l'IoT) : La migration des applications, des données et des services informatiques des nœuds centralisés vers les extrêmes logiques d'un réseau, ce qui permet d'effectuer des analyses et de générer des connaissances à la source des données.

- - F - -

Fail Over : Le basculement (en anglais, *fail-over* se traduit par « passer outre à la panne ») est la capacité d'un équipement à basculer automatiquement vers un réseau ou un système alternatif ou en veille.

Federated Identity (Login) : Les moyens de relier l'identité et les attributs d'une personne, stockés dans de multiples systèmes distincts de gestion de l'identité. (Comme le Single Sign-on (SSO), dans lequel le ticket d'authentification unique d'un utilisateur, ou token, est

approuvé par plusieurs systèmes informatiques ou même par plusieurs organisations. Le SSO est un sous-ensemble de la gestion fédérée des identités, car il ne concerne que l'authentification et s'entend au niveau de l'interopérabilité technique.

Firewall : Un pare-feu (en anglais : *firewall*) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant les types de communications autorisées sur ce réseau informatique.

Fog (Une architecture IoT) : Une approche d'architecture qui utilise une multitude de clients utilisateurs finaux ou d'appareils de périphérie proches de l'utilisateur pour effectuer une quantité importante de stockage temporaire, de communication, de contrôle, de configuration, de mesure et de gestion.

- - G - -

Gateway (Moteur IoT) : Une passerelle IoT est un dispositif qui permet la communication de machine à machine en connectant les appareils à un autre réseau comme internet.

GSM : Global System for Mobile Communications est une norme numérique de seconde génération pour la téléphonie mobile

- - H - -

Healthcare : Appareils ou applications mobiles liés au secteur du conditionnement physique et du bien-être qui s'intègrent les uns aux autres de façon transparente pour créer une expérience client forte.
Hosting : Le fait d'héberger des ressources cloud du client.

Housing : Le fait d'héberger des équipements appartenant au client, non à l'hébergeur.

- - I - -

IA (Intelligence Artificielle) : Simulation de processus d'intelligence humaine par des machines, en particulier des systèmes informatiques. Ces processus comprennent l'apprentissage (l'acquisition de l'information et les règles d'utilisation de l'information), le raisonnement (l'utilisation de règles pour tirer des conclusions approximatives ou définitives) et l'autocorrection. Les applications particulières de l'IA comprennent les systèmes experts, la reconnaissance vocale et la vision industrielle.
IaaS : L'infrastructure en tant que service ou, en anglais, *infrastructure as a service* est un modèle où l'entreprise dispose sur abonnement payant d'une infrastructure informatique (serveurs, stockage, sauvegarde, réseau) qui se trouve physiquement chez le fournisseur.

Infraction : L'infraction est une violation d'une loi ou d'une réglementation.

Infrastructure informatique : L'infrastructure désigne les équipements informatiques matériels : matériel informatique ; réseau informatique. L'infrastructure est un élément-clé pour réaliser une bonne interopérabilité entre les éléments des systèmes d'information, comme les logiciels.

Interopérabilité : Capacité que possède un produit ou un système à pouvoir communiquer avec d'autres produits ou systèmes.

IoT ou IdO (Internet des Objets) : L'Internet des objets est un réseau de points finaux (ou « objets ») identifiables de façon unique qui contiennent une technologie intégrée pour détecter, collecter, communiquer et échanger des données localement ou avec des environnements externes, sans interaction humaine.

- - L - -

LAN : Un réseau local, *Local Area Network*, est un réseau informatique à une échelle géographique relativement restreinte, par exemple une salle informatique, une habitation particulière, un bâtiment ou un site d'entreprise.

Loadbalancing : La répartition de charge (en anglais : *load balancing*) est un ensemble de techniques permettant de distribuer une charge de travail entre différentes machines d'un groupe.

- - M - -

Moteur IoT : Combinaison de l'infrastructure réseau et des dispositifs actifs pour prendre en charge l'environnement IoT : par exemple PoE, WAP, passerelles, périphériques, etc.
MPLS : MPLS est un réseau privé virtuel, qui ne sort pas sur Internet pour une meilleure sécurité. Il est maitrisé par l'opérateur, qui administre lui-même le routage au sein de son réseau, car le client n'a pas la main sur celui-ci.

- - N - -

NAT : Mécanisme de translation d'adresses (en anglais : *Network Address Translator*) permettant de faire correspondre plusieurs adresses IP du réseau local à une seule adresse IP publique.

- - P - -

PaaS : Plate-forme en tant que service, de l'anglais *platform as a service*, permet de mettre à disposition des entreprises un environnement d'exécution rapidement disponible, en leur laissant la maîtrise des applications qu'elles peuvent installer, configurer et utiliser elles-mêmes.

Perte exploitation : La perte d'exploitation est une notion juridique qui définit des pertes ou un manque à gagner pour une entreprise. Dans le langage financier, elle correspond à un résultat d'exploitation négatif. Un résultat d'exploitation positif correspond à un bénéfice d'exploitation.

Politique de sécurité : C'est un plan d'action définie pour maintenir un certain niveau de sécurité.
Problématique : elle est la présentation d'un problème sous différents aspects. La problématique représente un cheminement regroupant un thème, des interrogations évoquées par ce thème, une question précise et l'hypothèse que l'on en fait.

- - Q - -

QoS : La qualité de service (en anglais : *Quality of Service*) est un concept de gestion qui a pour but d'optimiser les ressources d'un réseau ou d'un processus et de garantir de bonnes performances aux applications critiques pour l'organisation.

- - R - -

Réseau (informatique) : Ensemble de moyens matériels et logiciels mis en œuvre pour assurer les communications entre les différents périphériques informatiques.
Réseau filaire : C'est un réseau que l'on utilise grâce à une connexion avec des câbles.
Réseau sans fil : Réseau qui connecte différents postes ou systèmes entre eux par des ondes radio.
Routeur : Equipement réseau, qui permet d'interconnecter deux réseaux au niveau 3 du modèle OSI.
Routage : C'est un processus, qui permet de sélectionner des chemins dans un réseau pour transmettre des données depuis un expéditeur jusqu'à un ou plusieurs destinataires.

- - S - -

SaaS : Le logiciel en tant que service ou software as a service (SaaS) est un modèle de distribution de logiciel à travers le Cloud. Les applications sont hébergées par le fournisseur de service.

Scalabilité : Elle désigne la capacité d'un produit à s'adapter à un changement d'ordre de grandeur de la demande (montée en charge), en particulier sa capacité à maintenir ses fonctionnalités et ses performances en cas de forte demande.

Service Informatique : Service interne de l'entreprise qui gère le parc informatique.

Système d'information : noté SI, il représente l'ensemble des éléments participant à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'entreprise.

SLA : Le service-level agreement est un document qui définit la qualité de service requise entre un prestataire et un client.

- - T - -

Tableau de bord : Affiche des informations sur l'écosystème IoT aux utilisateurs et leur permet de contrôler leur écosystème IoT.
Transformation numérique : désigne le processus qui consiste, pour une organisation, à intégrer pleinement les technologies digitales dans l'ensemble de ses activités.

TLS : Transport Layer Security (TLS) ou Sécurité de la couche de transport, et son prédécesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet

- - U - -

Ultra Narrow Band : (UNB) bande ultra étroite de fréquence

Uplink : Envoi ascendant de données

UTM : Unified threat management (en français : gestion unifiée des menaces) décrit des pare-feu réseaux qui possèdent de nombreuses fonctionnalités supplémentaires qui ne sont pas disponibles dans les pare-feu traditionnels.

- - V - -

VLAN : Un réseau local virtuel, communément appelé VLAN (Virtual LAN), est un réseau informatique logique indépendant permettant d'isoler logiquement un ensemble de machines sur le réseau.

VPN : Un réseau privé virtuel, communément appelé VPN (Virtual Private Network), est un système permettant de créer un lien direct entre des ordinateurs distants. La connexion entre les machines est gérée de façon transparente par le logiciel de VPN, créant un tunnel entre eux.

- - W - -

WAN : Un réseau étendu, (Wide Area Network), est un réseau informatique ou un réseau de télécommunications couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, ou de la planète entière. Le plus grand WAN est le réseau Internet.

VI.2 Webographie

Liens génériques :

https://r-stylelab.com/company/blog/iot/internet-of-things-how-much-does-it-cost-to-build-iot-solution)
https://www.cnil.fr/
https://fr.wikipedia.org
https://www.ssi.gouv.fr
https://www.gartner.com/en
https://www.objetconnecte.net/histoire-definitions-objet-connecte/
https://www.minalogic.com/fr/actualite/des-siecles-de-reve-et-dinnovation-jusqua-liot
https://www.objetconnecte.com/infographies-mot-histoire-amour-1908/
https://www.sfrbusiness.fr/room/internet-des-objets/comment-iot-change-les-habitudes-des-entreprises.html
https://www.docdoku.com/blog/2017/10/23/iot-historique-applications-et-defis-de-lacquisition-des-donnees/
https://www.objetconnecte.com/infographies-mot-histoire-amour-1908/
https://www.welcometothejungle.co/articles/focus-sur-l-internet-of-things-iot-l-essentiel-a-savoir
https://www.minalogic.com/fr/actualite/des-siecles-de-reve-et-dinnovation-jusqua-liot
https://www.objetconnecte.net/histoire-definitions-objet-connecte/
https://www.connect-object.com/histoire-des-objets-connectes/
https://www.meilleure-innovation.com/2014/08/infographie-internet-objets/
http://www.digitaldimension.solutions/blog/avis-d-experts/2016/02/lpwan-le-reseau-emergent-de-liot/
https://www.visiativ-industry.fr/industrie-4-0/
https://www.adentis.fr/comment-l-iot-faconne-lindustrie-4-0/
https://www.synox.io/internet-des-objets-iot-qu-est-ce-que-cest/
https://www.journaldunet.com/ebusiness/internet-mobile/1197635-lora-reseau-differences-sigfox/

LoRa & SigFox :

https://www.capital.fr/entreprises-marches/le-cofondateur-de-sigfox-explique-pourquoi-ce-sont-davantage-les-rhinoceros-dafrique-que-les-boitiers-free-qui-pourraient-assurer-lavenir-de-son-reseau-1321237
https://www.boursorama.com/bourse/forum/1rPEKI/detail/451247758/
https://fr.wikipedia.org/wiki/Freebox#Freebox_Delta
https://www.capital.fr/entreprises-marches/xavier-niel-donne-un-coup-de-pouce-a-2-entreprises-de-la-tech-francaise-avec-la-nouvelle-freebox-voici-pourquoi-ce-partenariat-est-essentiel-pour-elles-1318470
https://www.businessinsider.fr/ludovic-le-moan-dit-pourquoi-perennite-sigfox-depend-rhinoceros
https://www.ismac-nc.net/wp/wp-content/uploads/2017/08/presentationtechniquedesigfoxjuillet2017-170802084415.pdf
https://fr.wikipedia.org/wiki/Bilan_de_liaison
https://fr.wikipedia.org/wiki/CBC-MAC
https://www.disk91.com/2018/technology/sigfox/stop-telling-me-sigfox-is-clear-payload-for-real-youre-just-lazy/

https://www.usriot.com/news/wireless-networking-technology-uses-frequency.html
https://www.sigidwiki.com/wiki/SIGFOX
https://www.ebds.eu/applications-docs/documentation/fréquences-libres-en-france/
https://fr.wikipedia.org/wiki/Bande_industrielle,_scientifique_et_médicale
https://www.etsi.org/deliver/etsi_en/300200_300299/30022002/03.01.01_30/en_300220 2v030101v.pdf
https://fr.wikipedia.org/wiki/European_Telecommunications_Standards_Institute
http://sss-mag.com/pdf/part15-91905.pdf
https://www.survivingwithandroid.com/2018/07/sigfox-protocol-network-architecture-iot-protocol-stack.html
https://www.domotique-info.fr/2014/02/sigfox-technologie-de-rupture-pour-le-marche-du-m2m/
https://www.objetconnecte.com/sigfox-protocole-radio/
https://www.journaldunet.com/ebusiness/internet-mobile/1195953-sigfox-rend-publique-la-specification-de-son-protocole-radio/
https://www.sigfox.com/sites/default/files/1701-SIGFOX-White_Paper_Security.pdf
https://jeija.net/renard-slides/#/23
https://blog.st.com/stsafe-a1sx-sigfox-secure-element/
https://www.st.com/en/secure-mcus/stsafe-a1sx.html
http://www.ioi-labs.com/technologies/comprendre-reseau-lorawan
https://enterpriseiotinsights.com/20180516/channels/fundamentals/the-difference-between-lora-and-lorawan-tag40-tag99
http://www.linuxembedded.fr/2017/12/introduction-a-lora/
http://jensd.be/755/network/lorawan-simply-explained
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5038744/
https://www.frugalprototype.com/technologie-lora-reseau-lorawan/
https://openiot.in/blog/Get-Started-with-LoRaWAN-in-India/
https://smartmakers.io/en/lorawan-range-part-2-range-and-coverage-of-lorawan-in-practice/
http://lorawan.blogspot.com
https://www.thethingsnetwork.org/docs/lorawan/
https://www.thethingsnetwork.org/docs/lorawan/security.html
https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf
https://lora-alliance.org/sites/default/files/2018-04/lorawantm_regional_parameters_v1.1rb_-_final.pdf
https://www.youtube.com/watch?v=dxYY097QNs0&feature=youtu.be
http://www.frugalprototype.com/wp-content/uploads/2016/08/an1200.22.pdf
https://lora-alliance.org/sites/default/files/2018-07/lorawan1.0.3.pdf
http://www.techplayon.com/lora-long-range-network-architecture-protocol-architecture-and-frame-formats/
https://www.thethingsnetwork.org/docs/lorawan/
https://www.link-labs.com/blog/sigfox-vs-lora
https://fr.flossmanuals.net/camposv/point-industrie-40/static/LoRa.pdf
https://lora-alliance.org/about-lorawan
https://www.newieventures.com.au/blogtext/2018/2/26/lorawan-otaa-or-abp
http://www.industrie-mag.com/article9917.html

https://www.digikey.fr/fr/articles/techzone/2018/jun/use-a-crypto-chip-to-add-secure-boot-to-iot-device-designs
https://www.researchgate.net/publication/318575428_Exploring_the_Security_Vulnerabilities_of_LoRa
https://fernandokuipers.nl/papers/IoTDI2018.pdf
https://www.objetconnecte.com/tout-savoir-sur-sigfox/
https://www.objetconnecte.com/tout-savoir-reseau-lora-bouygues/
https://fr.wikipedia.org/wiki/Sigfox

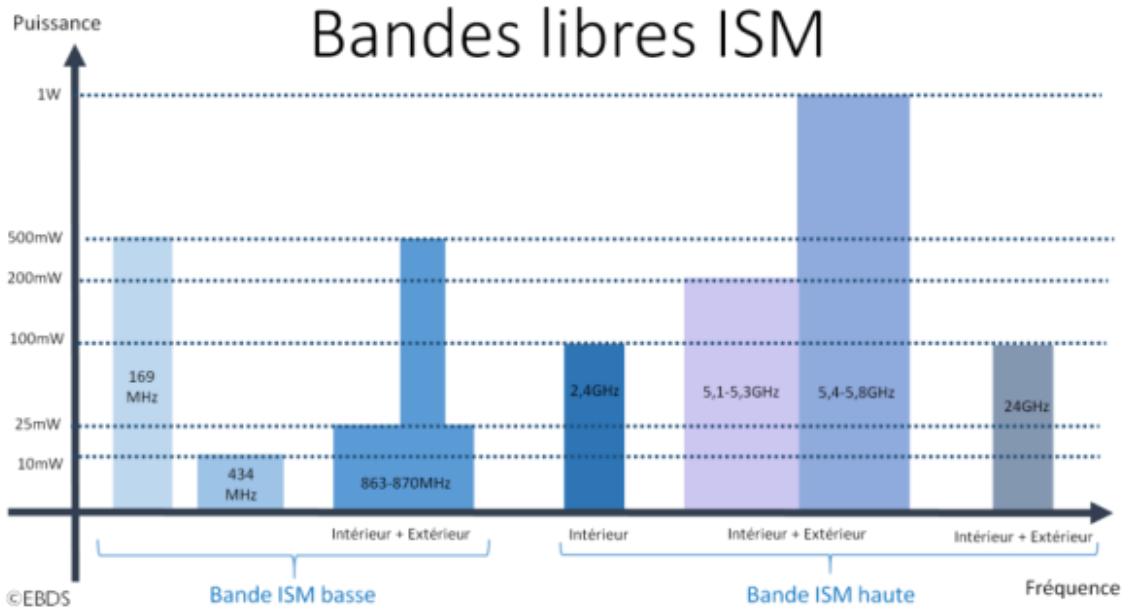
Sécurité :
https://www.iotworldtoday.com/2016/07/27/10-most-vulnerable-iot-security-targets/
https://www.techrepublic.com/article/4-best-practices-to-combat-new-iot-security-threats-at-the-firmware-level/
https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/
https://www.silicon.fr/
http://webdesobjets.fr/
https://www.iotsworldcongress.com/
https://www.thingful.net/
https://www.shodan.io/
https://www.01net.com/actualites/objets-connectes-les-reseaux-lorawan-vulnerables-aux-attaques-de-hackers-1042538.html
https://www.01net.com/actualites/objets-connectes-le-reseau-francais-sigfox-une-passoire-en-matiere-de-securite-957875.html

VI.3 Utilisation de la bande ISM SigFox

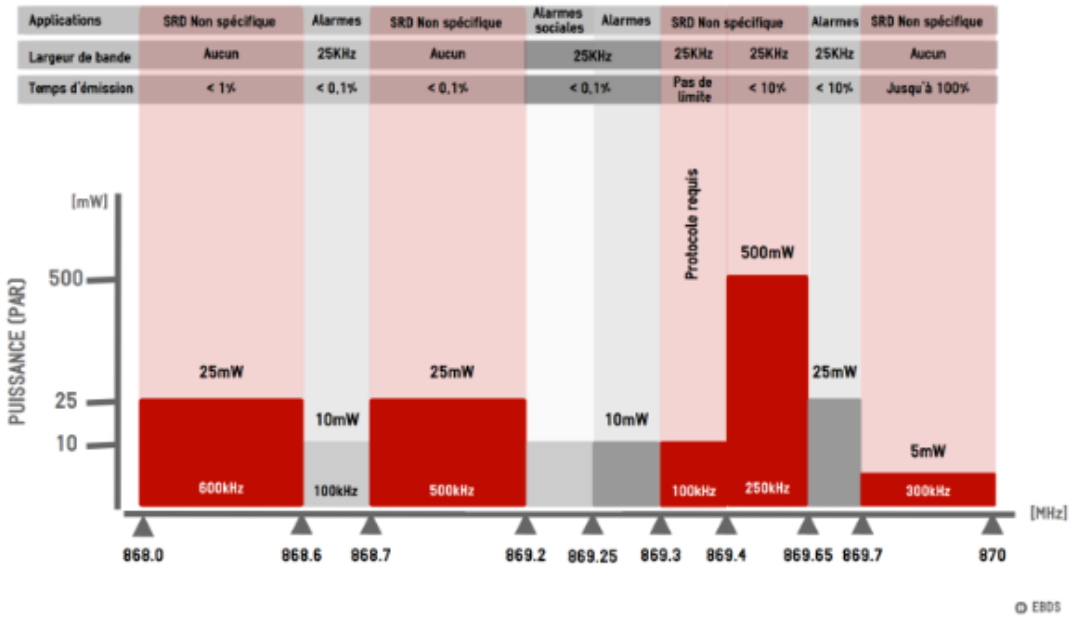
Spectre de fréquence et règlementation :

Utilise 192 KHz de la bande de fréquence libre ISM (industriel, scientifique et médical)

- 868 MHz à 868,2 MHz en Europe (régulation ETSI 300-220 – ETSI : European Telecommunications Standards Institute)
- 902 MHz à 928 MHz dans le reste du monde (restrictions applicables selon la règlementation locale, par exemple aux USA 902 MHz (FCC part 15) et 920 MHZ pour l'Amérique du nord, l'Australie, la Nouvelle Zélande… (ANATEL 506, AS/NZS 4268))



La bande 868MHz dans le détail



VI.4 Détail des communications SigFox

La communication entre le end device et le relai peut se faire selon deux modes :

- Uplink : Le message est envoyé du périphérique IOT vers le relai. Ce type de message est initié par le périphérique, soit dans un intervalle de temps déterminé, soit par un évènement détecté par le périphérique (par exemple un déplacement si le message contient des coordonnées GPS).

- Downlink : Ce type de message permet d'envoyer des informations vers le périphérique.

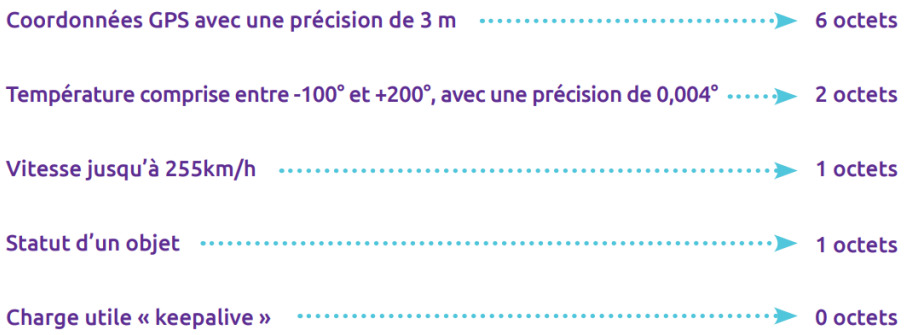
Des contraintes pour ce type de message existent : Le device doit d'abord émettre un message uplink avec un flag particulier (indique l'attente d'un ACK sur un temps donné).
Puis, avec un laps de temps d'inactivité de l'ordre de plusieurs secondes (20s), le périphérique se met en écoute sur un temps donné (25s). Alors, le message en downlink peut être émit par le relai.

- Le périphérique ne transmet pas d'ack de prise en compte du message de downlink. A noter également que la quantité de données transmise (charge utile) est moindre par rapport à un message en uplink.

Chaque message est transmis 3 fois, sur 3 fréquences aléatoires sur un court laps de temps (~45ms entre chaque message). Ce mécanisme permet d'augmenter les chances de bonne réception du message par le relai ou par le périphérique.

	Uplink	Downlink
Payload Limit (bytes)	12	8
Throughput (bps)	100	600
Maximum Messages per Day	140	4
Modulation Scheme	DBPSK	GFSK
Sensitivity (dBm)	<14	<27

A noter que les messages en uplink peuvent avoir une charge utile de 0 octet, c'est utile pour donner un signal de vie du périphérique.



Exemple de charge utile et leur taille

VI.5 Termes LoRa

LoRa : LoRa, pour Long Range, est le nom donné à la couche physique, voir le schéma (a noter que la couche modulation est propriétaire)
LoRaWan : LoRa Wide Area Network, désigne LoRa plus la partie MAC et applicative
LoRa PHY : Voir LoRa
LoRa Alliance : Créée en 2015, la LoRa Alliance est un consortium d'industriels et d'opérateurs, regroupés autour de LoRa dont l'objectif est la standardisation des réseaux à longue distance LPWAN et notamment de permettre l'interopérabilité de ces réseaux de télécommunication.
LoRa MAC : Fait référence à l'implémentation de LoRa utilisée pour n'effectuer que des communications pair à pair

Classe A, B, C : Désigne des spécificités de communication intégrée aux end-devices (voir détails dans la suite du document partie Classe)

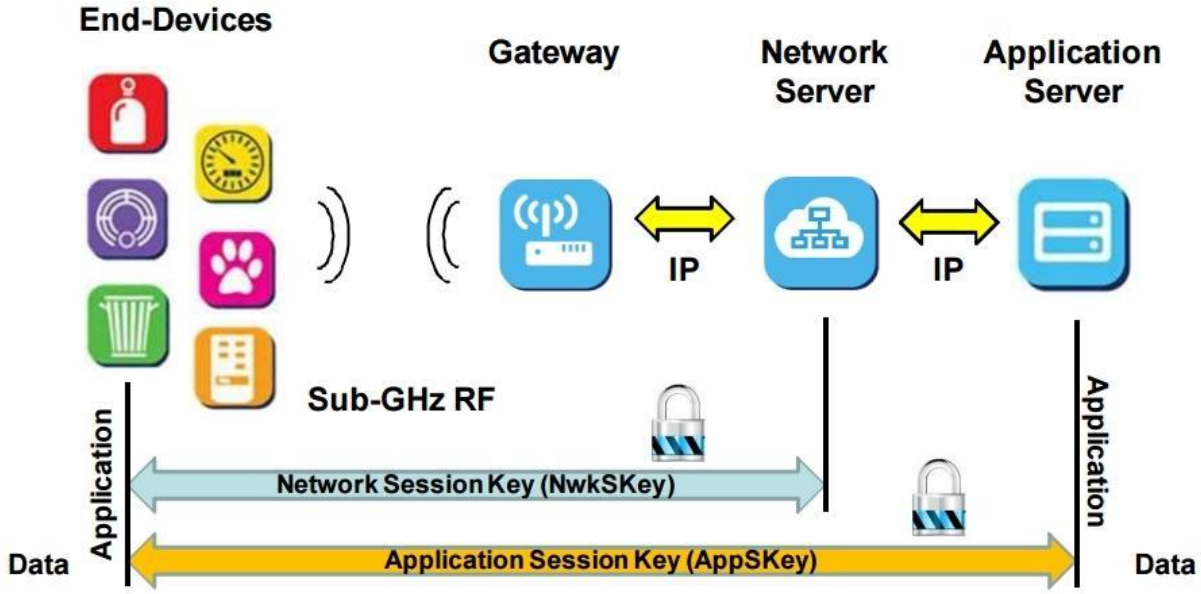
VI.6 Utilisation de la bande ISM LoRa

Tout comme SigFox, LoRa fonctionne sur la bande de fréquence libre ISM (industriel, scientifique et médical). Selon le pays d'implémentation, des règlementations s'appliquent.
En France, LoRa peut être utilisé sur les fréquences allant de 433.05 MHz à 434.79 MHz (EU433) et de 863 MHz à 870 MHz (EU863-870)

France	433.05 - 434.79 MHz	EU433
	863 - 870 MHz	EU863-870

VI.7 Chiffrements LoRaWan

Deux couches de chiffrements sont annoncées dans les spécifications techniques. Il est à noter que cela dépendant de l'implémentation qui en est faite, aussi bien sur le enddevice que sur les relais.



Représentation des deux couches de chiffrement

Pour assurer la sécurité du réseau et des données, le réseau LoRaWAN a recours à deux chiffrements AES-128. Le premier via la clé de session réseau – Network Session Key (NwkSKey) – assure l'authenticité des équipements sur le réseau ; quant au deuxième chiffrement, il assure via la clé de session applicative – Application Session Key (AppSKey) – la sécurité et la confidentialité des données transmises à travers le réseau.
En d'autres termes, la clé réseau permet à l'opérateur de sécuriser son réseau alors que la clé applicative permet au fournisseur de l'application de sécuriser les données qui transitent à travers le réseau.
Les données utiles que souhaite transmettre l'équipement sont tout d'abord chiffrées via la clé de session applicative. Une en-tête, contenant entre autres l'adresse de l'équipement, est ensuite ajouté aux données chiffrées. À partir de cette concaténation, le MIC – Message Integrity Code – est calculé via la clé de session réseau. Le MIC permet au réseau de vérifier

l'intégrité des données et de l'équipement sur le réseau. Enfin, le MIC est ajouté au message contenant l'en-tête et les données chiffrées avant transmission.
À réception du message par le serveur de gestion du réseau, ce dernier pourra vérifier l'intégrité des données grâce au MIC tout en préservant la confidentialité des données (chiffrées par la clé de session applicative).

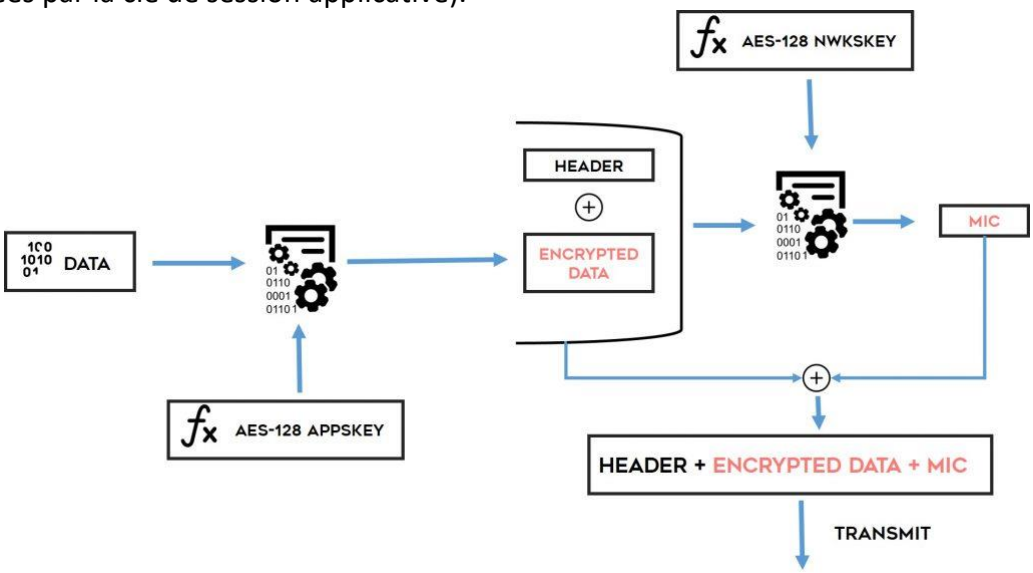


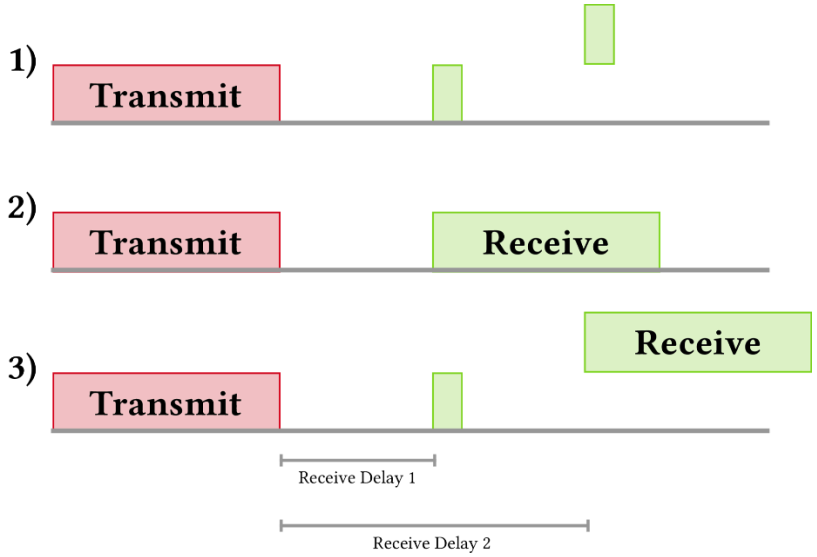
Schéma du processus de chiffrement

Pour les classes A (voir plus bas), en uplink à savoir du device vers la gateway, une transmission est émise suivi par un passage très bref en mode écoute (ce mode d'écoute intervient à 1s puis 2s après l'envoi). Si aucun signal n'advient en retour vers le device, il faut attendre le prochain uplink.

VI.8 Classes d'équipements LoRa

Classe A, B, C

A : Communication bi-directionnelle (upling et downlink). Le device peut initer une communication selon ses propres informations (changement d'état, détection d'un évènement…). Le downlink peut être effectuée après une séquence de 2 brefs uplink dans une fenêtre de temps bien définie. La classe A est la moins consommatrice d'énergie mais offre moins de flexibilité quant aux possibilités de downlink
B : Communication bi-directionnelle. Le device peut initier une communication selon ses propres informations. Le downlink fonctionne de la même mani_re que la classe A, à ceci près que peuvent être ajouté des fenêtres prédéfinies de downlink.
C : Communication bi-directionnelle. Même chose que la classe A mais offre des possibilités supérieures en downlink en étant pratiquement en permanence en écoute. Tout ceci a une forte répercussion sur la consommation d'énergie et ce type de classe est plus adapté lorsque le device peut être en permanence raccordé à une source d'alimentation



Représentation de l'alternance transmission (rouge) et écoute (vert) pour les Classe A & B

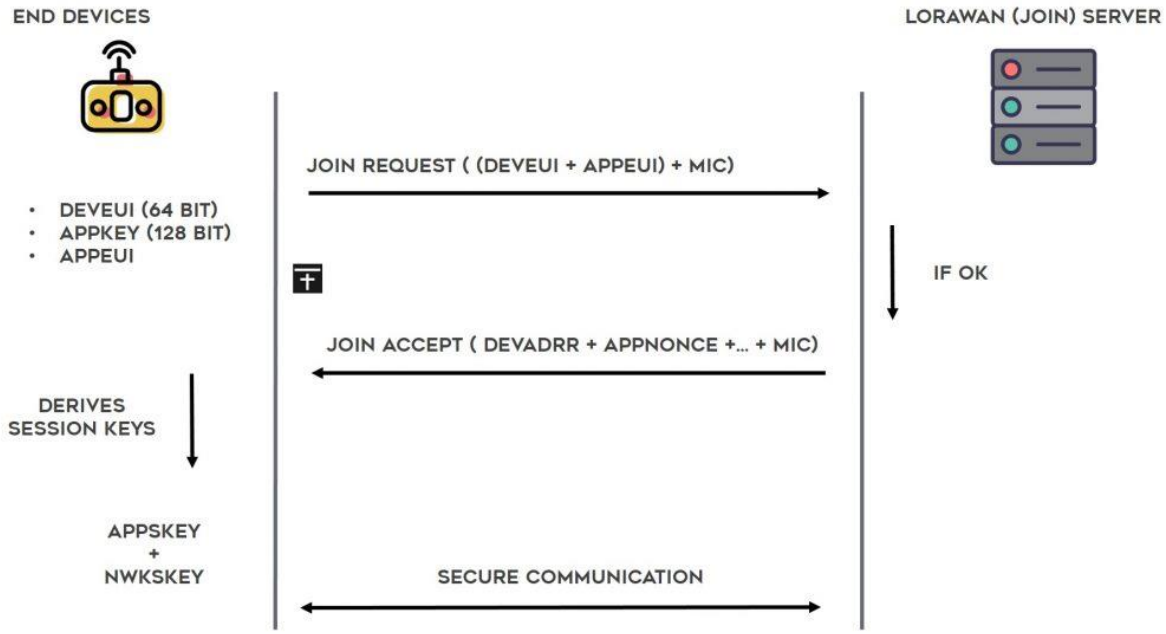
Représentation du fonctionnement des classes C

VI.9 Modes d'activation sur le réseau LoRa

Over The Air Activation (OTAA)

Pour activer un équipement sur le réseau par la méthode OTAA, l'équipement doit transmettre au réseau une demande d'accès : join request. Pour ce faire, celui-ci doit être en possession de trois paramètres :

- Le DevEUI, identifiant unique (de type EUI 64) de l'équipement (fourni par l'équipementier).
- AppEUI, identifiant du fournisseur de l'application (EUI 64).
- AppKey, clé AES 128 déterminée par le fournisseur de l'application.



L'équipement envoie, à travers le réseau, la requête join request, contenant DevEUI, AppEUI ainsi qu'un MIC calculé via la clé AppKey. Cette requête est transmise au serveur d'enregistrement qui vérifie le MIC via la clé AppKey (qui lui a été communiquée au préalable). Si l'équipement est autorisé par le serveur d'enregistrement, la requête join accept est transmise en réponse à l'équipement.
Cette réponse contient des données à partir desquelles l'équipement va pouvoir calculer les clés de session (réseau et applicative). Parmi les données contenues dans cette réponse, se trouve également l'adresse – Device Adress (DevAddr) sur 32 bits – qu'utilisera l'équipement pour communiquer sur le réseau.
A chaque nouvelle session, les clés de session sont renouvelées.

Activation By Personalization (ABP)

Pour la seconde méthode, APB, les clés de session NwkSKey et AppSKey ainsi que l'adresse de l'équipement (DevAddr) sont directement inscrits dans l'équipement LoRaWAN. Ainsi, l'équipement n'a plus besoin d'envoyer de requête avant de communiquer sur le réseau. L'utilisation de cette méthode implique que les équipements communiquent avec un réseau spécifique car les clés de session sont connues par avance. Et contrairement à la méthode OTAA, les clés de session sont statiques.
En résumé, la méthode OTAA est plus complexe à implémenter que la méthode APB mais offre un niveau de sécurité supérieur. Dans le cas d'un prototypage ou pour une utilisation sur un réseau connu, la méthode APB suffit largement. Cependant, lorsqu'un déploiement à plus grande échelle est envisagé, il est conseillé d'utiliser la méthode OTAA, plus sécurisée et plus agile.