Présentation technique de Sigfox

Novembre 2018

Table des matières

1 Introduction

Ce document présente la synthèse générale de la technologie et du réseau mondial Sigfox.
Il présente d'abord les principes de la technologie Sigfox permettant la communicaton entre les objets et le réseau. Il détaille les avantages concurrentiels de cette technologie sur le marché de l'Internet des objets (IoT).
La deuxième partie décrit l'architecture du réseau Sigfox avec ses différents composants, leurs rôles et responsabilités.
Dans la troisième partie sont décrits les mécanismes et les processus en place au sein de Sigfox pour sécuriser les données des clients, ainsi que l'infrastructure du réseau, des stations de base aux composants du réseau central.
La dernière partie présente les différentes fonctionnalités de Sigfox permettant l'évaluation de la qualité du service et la prédiction de la couverture.

Comment créer des solutions basées sur Sigfox ?

Rendez-vous sur le site Internet dédié aux fabricants d'objets : build.sigfox.com
Vous découvrirez comment procéder simplment à l'intégration de la technologie Sigfox dans un objet et avec une plateforme informatique.
Visitez aussi notre chaine Youtube où des vidéos explicatives sont disponbiles.

Sigles et abréviations

Termes techniques dans leur dénomination d'origine en langue anglaise

ABREVATION	DEFINITION
AES	Advanced encryption standard
API	Application programming interface
BSS	Business support system
CRA	Central registration authority
ETSI	European telecommunications standards institute
IoT	Internet of things
ISM	Industrial, scientific and medical
IT	Information technology
LPWAN	Low power wide area network
MAC	Message authentication code
NAK	Network authentication key
NOC	Network operation centre
OSS	Operation support system
OTA	Over the air
PAC	Porting authorisation code
RF	Radio frequency
TPM	Trusted platform module
UNB	Ultra-narrow band
VPN	Virtual private network

2 Positionnement de Sigfox

Connecter le monde

Il est déjà possible aujourd'hui de mettre en place les grandes idées de demain, qui ne sont freinées que par des questions financières et énergétiques. Le fait est que les petits objets peu coûteux ne sont tout simplement pas assez puissants pour communiquer avec les grands réseaux mobiles. Sigfox a donc innové dans le domaine de la connectivité bas débit pour compléter les solutions à large bande passante.

Les solutions de connectivité bas débit Sigfox améliorent non seulement les activités existantes, mais offrent également de nouvelles perspectives pour les entreprises dans tous les secteurs. Les possibilités sont illimitées.

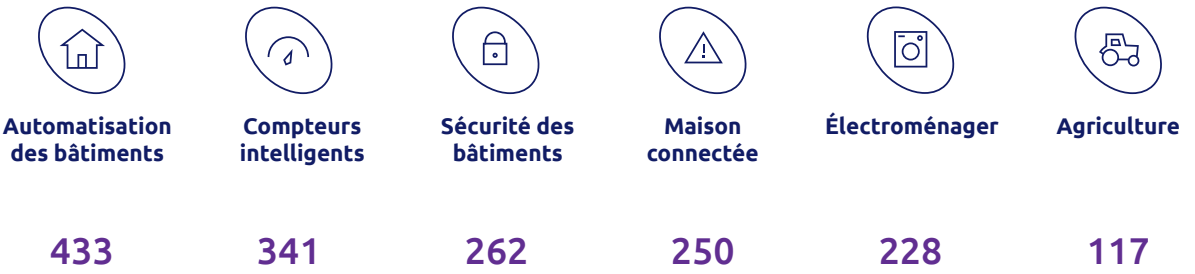


Figure 1 : Sigfox est présent dans tous les secteurs

Sigfox fait avancer le monde

Grâce à son réseau LPWA mondial et à son riche écosystème de partenaires experts, Sigfox fournit des services de communication clé en main, bidirectionnels et sécurisés pour révéler le véritable potentiel de l'Internet des objets (IoT).

Sigfox définit une façon standardisée de collecte des données à partir de capteurs et d'objets avec un ensemble unique et normalisé d'interfaces de programmation d'applications (API). En outre, la technologie innovante de Sigfox complète le « machine-to-machine » cellulaire traditionnel grâce à la mise en place de solutions globales et offrant une longue autonomie énergétique au coût le plus bas.

Sigfox est, en tant que connectivité secondaire, une solution très prometteuse pour atteindre une consommation énergétique très réduite et améliorer l'expérience des utilisateurs.

Sigfox fournit le réseau, la technologie et crée l'écosystème indispensables pour aider les entreprises et les organisations à atteindre leurs objectifs en matière d'IoT.

3 Principes de la technologie

Présentation des fondamentaux de la technologie Sigfox pour comprendre son positionnement et ses avantages compétitifs.

3.1 Bande ultra-étroite (UNB)

Sigfox utilise 192 KHz de la bande non licenciée ISM pour échanger des messages par liaison radio. La technique d'émission est ce que l'on appelle la bande ultra-étroite (UNB – Ultra Narrow Band). Chaque message occupe 100 Hz (zones ETSI) ou 600 Hz (zones FCC) et est transféré à un débit de 100 ou 600 bits par seconde selon la région.

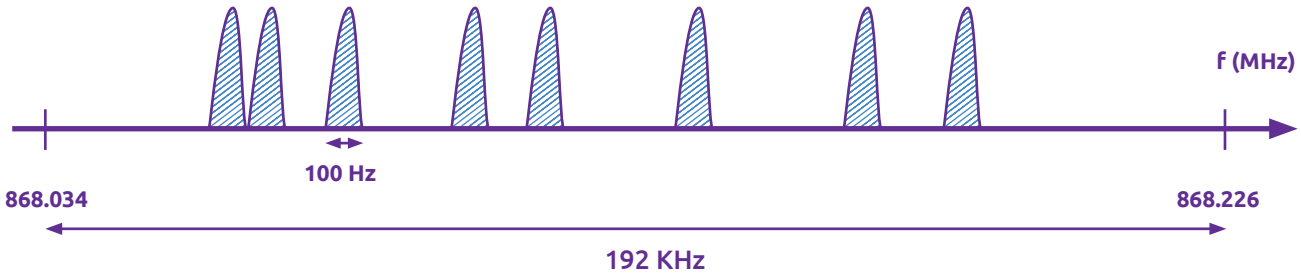


Figure 2 : Technologie Sigfox UNB

Cette technologie permet aux stations de base Sigfox des communications sur de longues distances sans être affectées par le bruit.

La bande utilisée varie en fonction des zones geographiques :

- **dans les pays suivant les normes ETSI,** la bande utilisée est comprise entre 868 et 868,2 MHz ;
- **dans le reste du monde,** la bande utilisée est comprise entre 902 et 928 MHz, et des restrictions sont applicables selon la réglementation locale.

L'envoi par liaison radio d'un message avec une charge utile de 12 octets nécessite 2,08 secondes à une vitesse de 100 bps.

Les stations de base Sigfox surveillent le spectre complet de 192 kHz et recherchent des signaux UNB à démoduler.

3.2 Accès aléatoire

L'accès aléatoire est une fonctionnalité essentielle pour obtenir un service de haute qualité. La transmission n'est pas synchronisée entre l'objet et le réseau. L'objet émet un message sur une fréquence aléatoire, puis envoie succesivement deux répliques sur des fréquences différentes, ce que l'on appelle « la diversité temporelle et fréquentielle ».

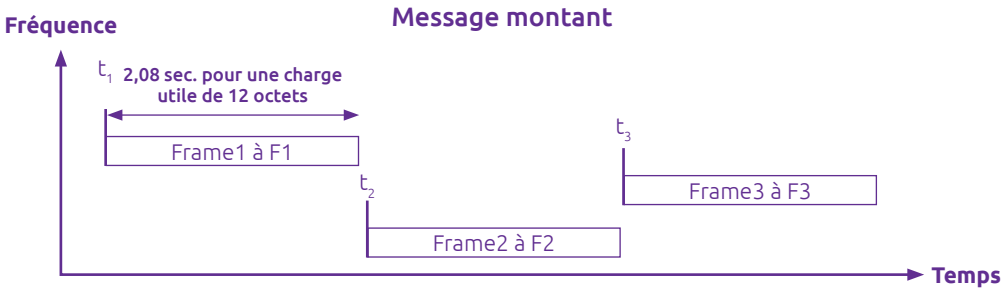


Illustration 3 : Saut de fréquence sur les répliques

3.3 Réception coopérative

Le principe de la réception coopérative est que, contrairement aux protocoles cellulaires, les objets ne sont pas attachés à une station de base spécifique. Le message envoyé est reçu par n'importe quelle station de base à proximité. Le nombre de stations de base recevant chaque message est de trois en moyenne. Il s'agit de la notion de « diversité spatiale ».

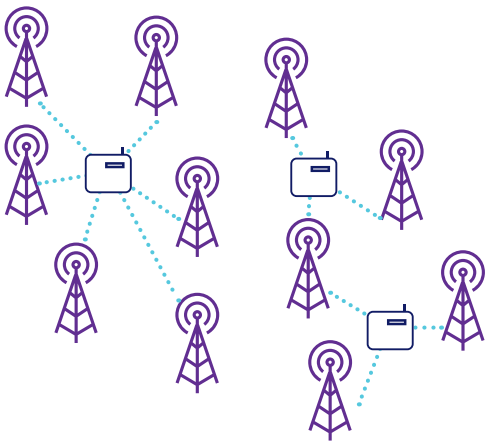


Illustration 4 : Réception des messages par plusieurs stations de base Sigfox

La diversité spatiale, associée à la diversité temporelle et fréquentielle des répétitions, sont des facteurs déterminants de la grande qualité de service du réseau Sigfox.

3.4 Messages courts

Pour répondre aux contraintes de coûts et d'autonomie des objets isolés fonctionnant sur batteries, Sigfox a conçu un protocole de communication pour les petits messages dont la taille est comprise entre 0 et 12 octets. Une charge utile de 12 octets suffit à transférer les données produites par un capteur, le statut d'un événement tel qu'une alerte, des coordonnées GPS voire des données d'application.

Nous avons répertorié quelques exemples de tailles de charge utile :

Coordonnées GPS avec une précision de 3 m ····► **6 octets**

Température comprise entre -100° et +200°, avec une précision de 0,004° ····► **2 octets**

Vitesse jusqu'à 255km/h ····► **1 octets**

Statut d'un objet ····► **1 octets**

Charge utile « keepalive » ····► **0 octets**

La réglementation européenne stipule que nous pouvons occuper 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. Si la réglementation diffère dans d'autres régions, l'offre commerciale Sigfox reste la même pour le moment.

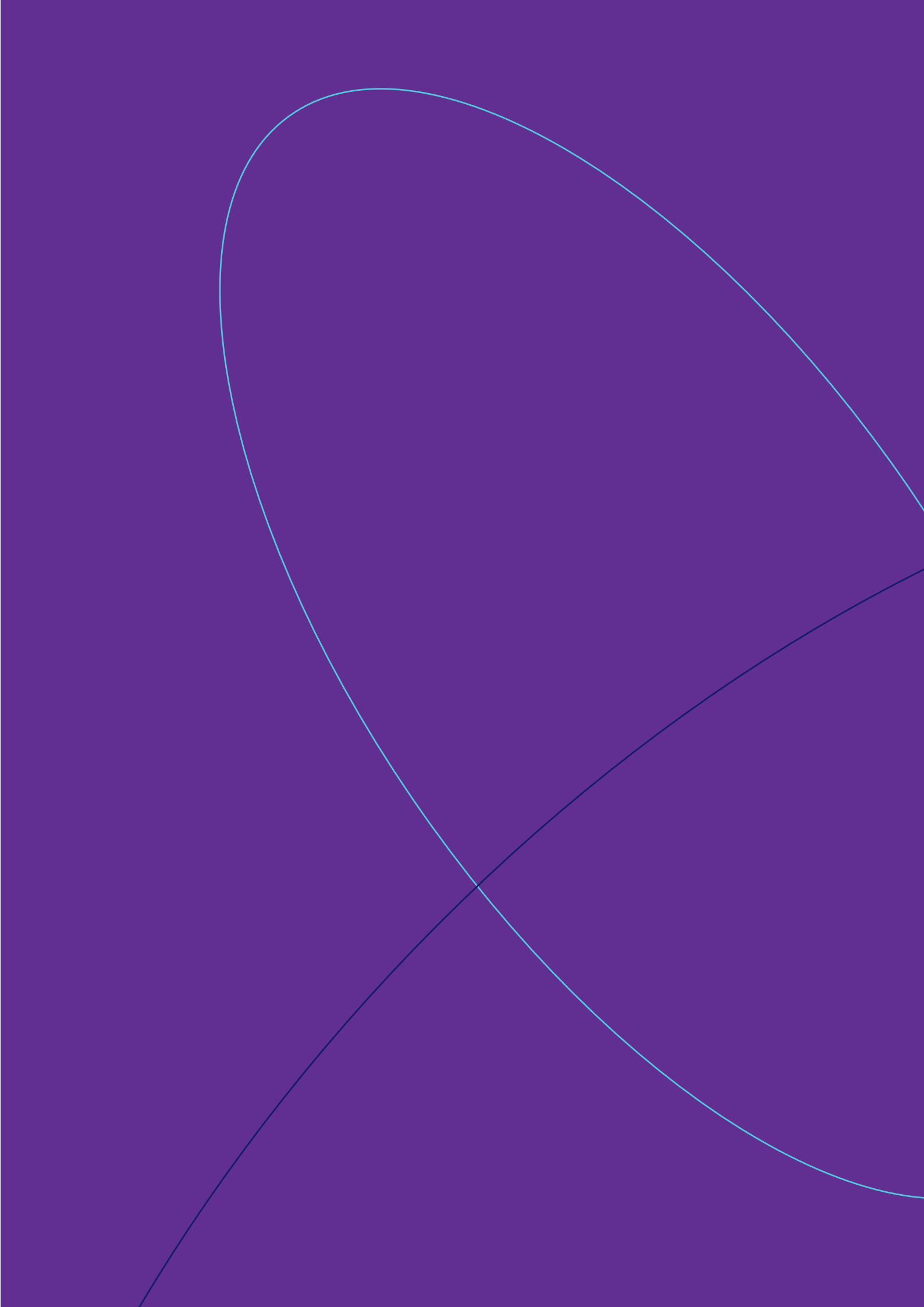
La taille de la charge utile des messages descendants est fixe : 8 octets. Une fois encore, une taille de 8 octets permet de transférer une quantité importante d'informations. Cela suffit pour recaler un capteur, ajuster la fréquence d'un objet, envoyer une requête pour obtenir des données additionelles, changer le mode de fonctionnement de l'objet

Le cycle de service de la station de base en émission est de 10 pour cent, ce qui garantit quatre messages descendants par objet et par jour. L'objet peut recevoir davantage de messages s'il reste des ressources disponibles au niveau des stations de base.

3.5 Communication bidirectionnelle

Le message descendant est déclenché par l'objet. Une fois qu'il a émis son message, l'objet retourne en veille pendant 20 s puis se réactive pendant 25 s pour recevoir le message descendant emis par la station de base.

La fréquence descendante est la fréquence du premier message montant plus un delta défini.



4 Principales fonctionnalités du réseau

Ce chapitre traite des principales caractéristiques du réseau Sigfox en matière d'architecture et de performances.

4.1 Vue d'ensemble de l'architecture du réseau

Ce chapitre présente le réseau Sigfox et fournit une description détaillée de ses différents composants.

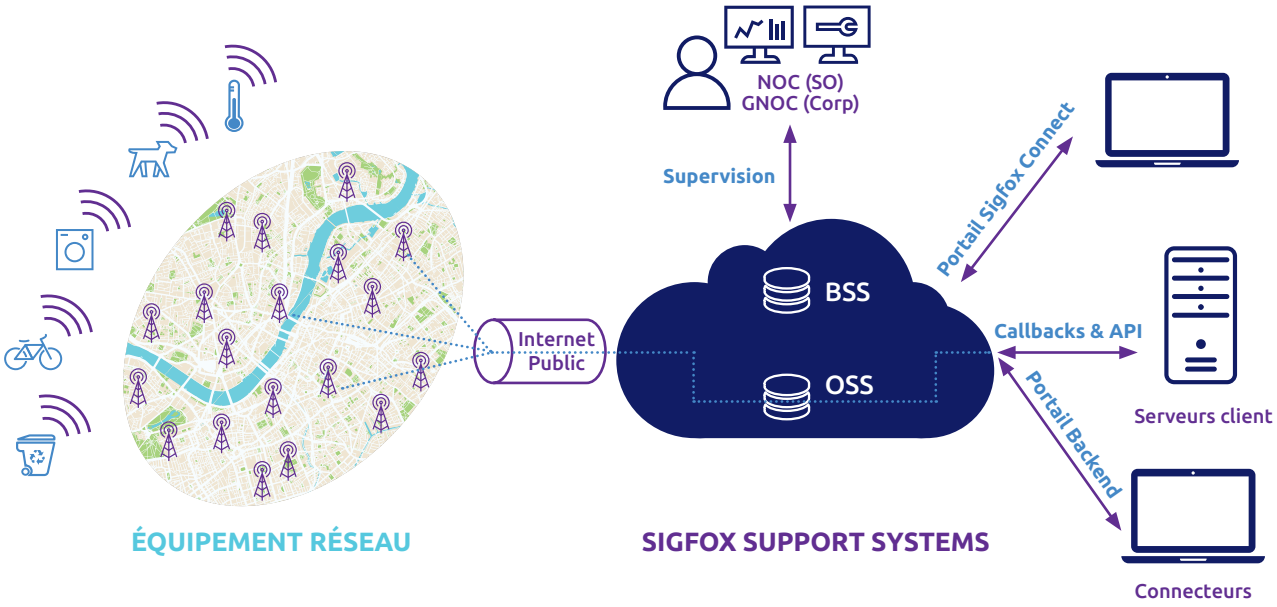


Illustration 5 : Architecture de haut niveau du réseau Sigfox

L'architecture du réseau Sigfox est horizontale, légère et composée de deux parties principales.

- La partie de l'équipement réseau est essentiellement composée des stations de base (et d'autres éléments, notamment les antennes) chargées de la réception des messages provenant des objets et de leur transfert aux systèmes d'assistance Sigfox.

- Le système de soutien operationel (OSS) est la deuxième partie de ce qui constitue le cœur du réseau, chargé du traitement des messages et de leur envoi au système du client par le biais de callbacks. Cette partie forme également le point d'entrée pour les différents acteurs de l'écosystème (Sigfox, Opérateurs Sigfox, partenaires commerciaux et clients finaux) pour interagir avec le système par l'intermédiaire d'interfaces Web ou d'API. Elle comprend aussi des modules et des fonctionnalités qui sont essentiels au déploiement, au fonctionnement et à la supervision du réseau, tels que le « Business Support System » (BSS) pour les commandes et la facturation, le « Radio Planning » pour le déploiement du réseau. Elle inclut également les espaces de stockage et les outils pour analyser les données collectées ou générées par le réseau.

Comme indiqué sur l'illustration ci-dessus, la liaison entre les deux couches est assurée par l'Internet public, mais sécurisée via une connexion VPN.

Les chapitres suivants décrivent les différents composants de ces deux parties du réseau Sigfox.

4.2 Architecture réseau plate

L'architecture plate de Sigfox permet de réduire à la fois les dépenses d'investissement et les dépenses d'exploitation. La radio logicielle Sigfox nous permet de réduire les coûts matériels des stations de base. Nous avons décidé de ne pas utiliser de matériel spécifique, mais plutôt un algorithme logiciel pour traiter efficacement la démodulation, ce qui réduit considérablement le coût total d'exploitation.

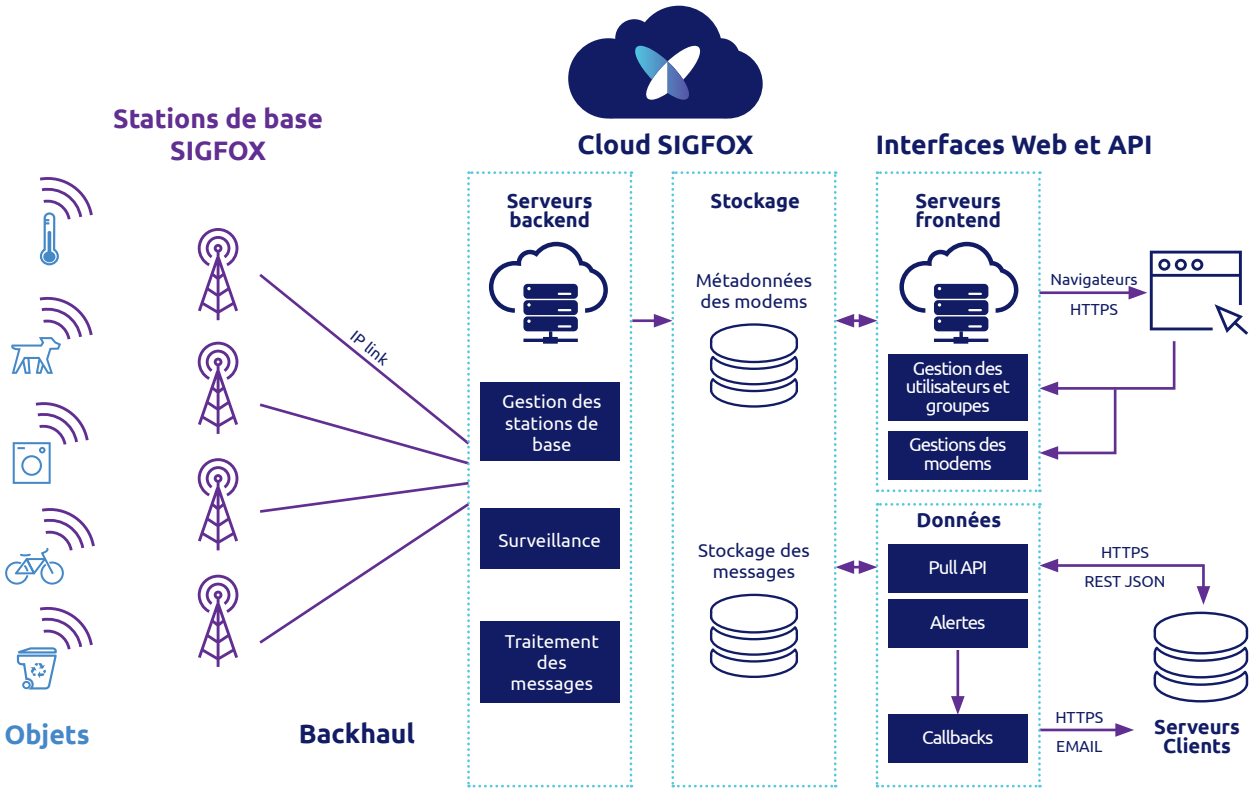


Figure 6 : Architecture plate

Les données sont envoyées aux stations de base par liaison radio, puis passent par réseau backhaul, qui utilise essentiellement une connexion DSL ou LAN comme connexion primaire et la 3G ou 4G comme connexion secondaire. En cas d'indisponibilité, une connexion par satellite peut être utilisée comme technologie de secours.

Le Cloud Sigfox assure le traitement des messages. Il peut y avoir un nombre important de répliques du même message qui parviennent au cœur du réseau, mais un seul doit cependant être stocké. Les serveurs au cœur du réseau surveillent également le statut du réseau et gèrent l'ensemble des stations de base.

L'infrastructure du réseau conserve les messages à deux emplacements : les métadonnées à utiliser pour les services de développement d'un côté, et les messages des clients de l'autre, de sorte que les clients puissent les récupérer ultérieurement.

Pour terminer, l'interface Web et API permettent aux clients d'accéder à leurs messages. Ils peuvent accéder à notre plateforme via leur navigateur Web ou utiliser une API REST ou callabacks pour les synchroniser dans leur système informatique et transmettre les messages descendants vers les objets.

4.3 Réseau haute capacité

La capacité du réseau est très élevée, ce qui permet à Sigfox de faire face aux milliards d'objets que nous ciblons. La capacité massive de l'infrastructure du réseau Sigfox est le résultat des facteurs décrits précédemment :

- la modulation UNB, qui utilise le spectre de manière efficace et résiste aux brouilleurs, toute l'énergie étant concentrée dans une bande passante très étroite;
- la diversité fréquentielle et temporelle découlant de l'accès aléatoire;
- la diversité spatiale, qui est due au chevauchement des cellules réseau.

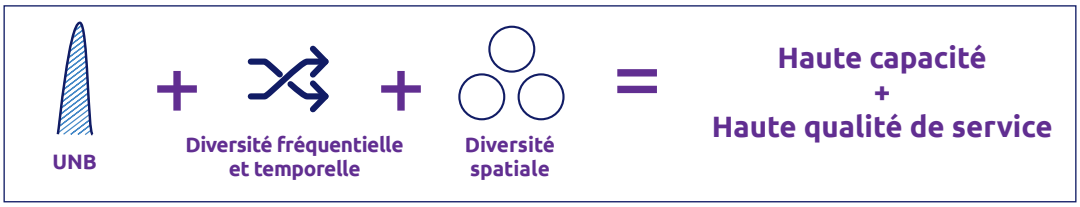


Illustration 7 : Combinaison des spécificités de la technologie Sigfox

Notre capacité est la même quelle que soit la liaison radio, tandis que la capacité d'autres réseaux diminue lorsque la qualité de la liaison radio décline.

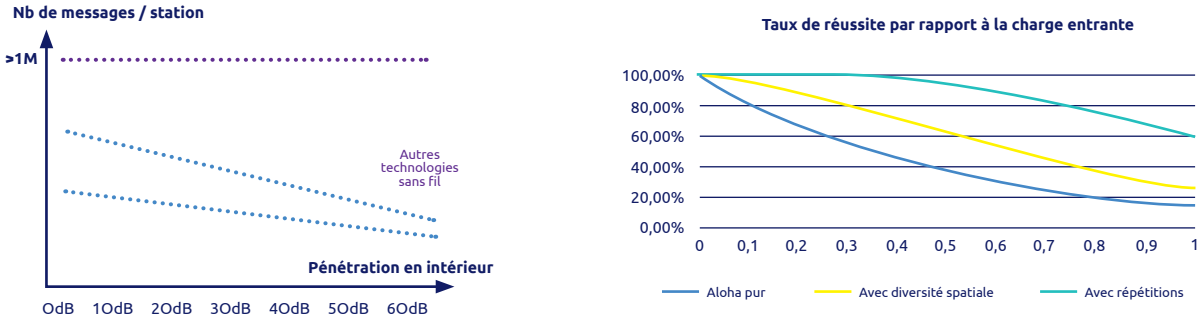


Illustration 8 : Maintien de la capacité quelle que soit la qualité de la liaison radio

Si la qualité de service que nous visons est de 99,99 %, la charge du réseau ne doit pas être supérieure à 14 %. En d'autres termes, la probabilité de perte de messages due aux potentielles collisions reste inférieure à 0,01 % jusqu'a 270 objets communiquant en parallèle avec la même station de base.

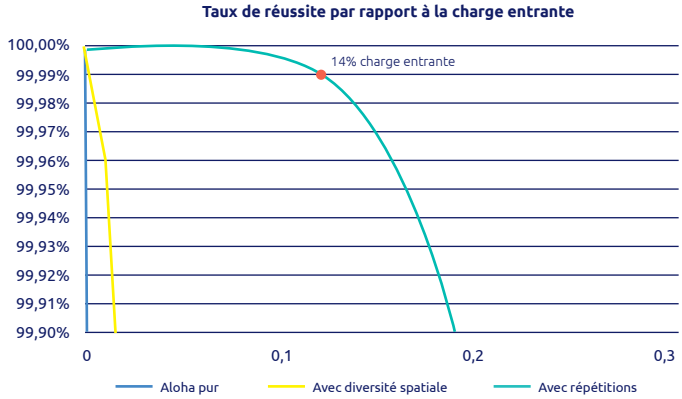


Illustration 9 : Impact limité de la charge sur la qualité du service grâce aux répétitions

4.4 Efficacité énergétique élevée

L'efficacité énergétique élevée fournie par la technologie Sigfox repose également sur les partenaires Sigfox spécialisés en semiconducteurs, puisque leurs puces électroniques consomment de 10 à 50 mA en transmission, selon le partenaire et la puce utilisée.

Ces valeurs sont valables en Europe où la puissance de sortie est de 14 dBm. La puissance est plus élevée aux États-Unis, où une valeur de 22 dBm est requise. La durée d'émission est six fois inférieure, la durée de vie de la batterie est donc approximativement la même.

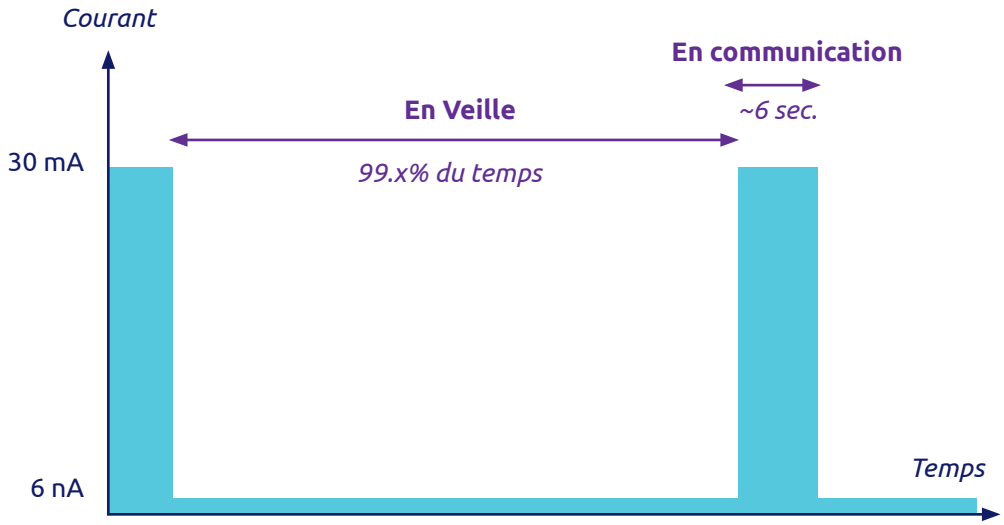


Illustration 10 : La faible consommation en mode veille augmente économise la batterie

Il y a deux autres facteurs permettant d'expliquer la longévité de la batterie avec la technologie Sigfox.

- Aucun apairage n'est nécessaire, ce qui signifie qu'il n'y a pas de message de synchronisation échangé entre l'objet et la station de base avant la transmission des données. Il s'agit d'un avantage considérable par rapport aux autres technologies qui incluent toutes cette étape supplémentaire.

- Un objet passe plus de 99% du temps en veille, la consommation en veille étant également très faible (souvent quelques nano-ampères), donc quasiment négligeable.

4.5 Longue portée

Le principal avantage de la technologie Sigfox par rapport à la concurrence réside dans le déploiement d'une grande couverture avec un nombre limité de stations de base :

- Pour une puissance de sortie donnée, la portée de la liaison radio est déterminée par le débit, c'est-à-dire qu'un débit moindre permet de disposer d'une plus longue portée.

- Le deuxième facteur est le bilan liaison, il est déterminé par la somme de la sensibilité de la station de base et la puissance de sortie de l'objet.

- La portée dépend beaucoup de la topographie.

- La couverture intérieure obtenure est bonne grâce à l'utilisation de la bande sub-GHz

La longue portée des stations de base permet à Sigfox de déployer à moindres coûts un réseau à l'échelle nationale.

Pour illustrer cette portée, Sigfox utilise un élément de mesure appelé bilan de la 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.
- Le bilan est légèrement plus élevé dans la zone ETSI (Institut européen des normes de télécommunications), d'où des cellules plus grandes.
- La bonne couverture de Sigfox en intérieur s'explique par l'utilisation de la bande sub-GHz. D'autres technologies mettant pourtant en avant un bilan de liaison supérieur et utilisant la bande de 2,4 GHz offrent une moins bonne couverture en intérieur.

4.6 Résistance aux brouilleurs

La technologie Sigfox dispose de capacités anti-brouillage uniques grâce à la résistance intrinsèque de l'UNB associée à la diversité spatiale des stations de base.

La modulation UNB est extrêmement résistante dans un environnement encombré d'autres signaux, y compris à spectre étalé. Les réseaux à spectre étalé sont cependant affectés par les signaux UNB. La modulation UNB est donc le meilleur choix pour l'utilisation dans la bande publique réservée aux applications industrielles, scientifiques et médicales (ISM).

La grande résistance aux brouilleurs est essentielle pour fonctionner efficacement dans la bande ISM publique.

La preuve incontestable de la grande résistance aux brouilleurs réside dans la capacité à transmettre en dépit de la présence de signaux de brouillage. La modulation UNB présente une résistance intrinsèque, car le chevauchement avec le bruit est très faible. Pour qu'un message puisse être reçu, le signal doit être au moins 8 dB supérieur au bruit de fond.

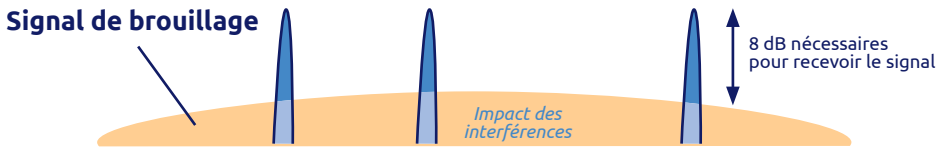


Figure 11 : Résistance aux brouilleurs grâce à la modulation UNB

Les technologies concurrentes basées sur la modulation à spectre étalé sont particulièrement impactées par le bruit, la surface qu'elles ont en commun étant bien plus grande. La modulation UNB est le meilleur choix de signalisation possible pour l'utilisation de la bande ISM publique.

4.7 Sécurité par défaut

L'écosystème Sigfox intègre un dispositif de sécurité par défaut :

- Authentification + intégrité + anti-réexécution sur les messages diffusés sur le réseau.
- Cryptographie basée sur le protocole AES, sans transmission des clés de sécurité dans le lien radio (OTA).
- Chiffrement de la charge utile en option pour garantir la confidentialité des données.
- Isolation de chaque partie du réseau et évaluation des risques de manière à ce que seul un segment mineur du réseau soit concerné en cas de piratage.

Concernant les objets, Sigfox a défini trois niveaux de sécurité. En fonction du cas d'usage et de la sensibilité, le fabricant ou le fournisseur d'application décidera du niveau à appliquer.

- Niveau intermédiaire – les données d'identification de sécurité sont stockées dans l'objet.
- Niveau élevé – les données d'identification de sécurité sont stockées dans une zone logicielle protégée.
- Niveau très élevé – les données d'identification de sécurité sont stockées dans un élément sécurisé.

L'élément sécurisé permet également de chiffrer les données transférées via le réseau. Le code secret est uniquement connu de l'objet et du client final. L'algorithme n'a pas d'impact sur la taille de la charge utile. Lorsque le message est chiffré, la charge utile est toujours de 12 octets.

Le réseau Sigfox vérifie que l'identifiant de l'objet n'a pas été dupliqué tout au long du cheminement du message. En cas d'objet corrompu, celui-ci est placé sur liste noire.

Dès le départ, Sigfox a conçu le réseau sans jamais perdre de vue la sécurité, et a donc réparti les fonctions sur différents serveurs. Par exemple, le serveur générant les identifiants dispose d'une sécurité renforcée.

5 Vue d'ensemble de la sécurité

Fort de son expertise et de ses divers partenariats, Sigfox a appliqué le principe de sécurité par conception (Security by Design) à toutes les étapes de définition de son protocole ainsi que dans le développement de son infrastructure.

De plus, Sigfox applique les principes de sécurité par défaut (Security by Default) à tous les composants proposés aux utilisateurs et opérateurs de Sigfox, aux fabricants d'objets ainsi qu'aux clients finaux.

Ceci englobe la chaîne de l'IoT composée des maillons suivants : les objets, l'infrastructure réseau ainsi que les services cloud (voir ci-dessous).

OBJET

- Capacités de cryptage
- Gestion des abonnements
- Gestion de l'objet

DONNÉES

- Intégrité des données
- Cryptage des données : confidentialité
- Protection des données

RADIO

Protéger les DONNÉES EN TRANSIT

- Robustesse de la modulation radio UNB
- Authentification et intégrité

CLOUD

Protéger les DONNÉES STOCKÉES

- Hébergement sécurisé
- Sécurité du backhaul
- Détection des messages corrompus

Illustration 12 : Sécurité dans la conception et par défaut

Un pare-feu intégré

Bien que les objets intégrant la technologie Sigfox entrent dans la catégorie de l'Internet des Objets (IoT), ils ne sont pas directement connectés à Internet et n'utilisent pas le protocole Internet pour communiquer. En fait, ces objets ne sont connectés à aucun réseau ni à aucune station de base.

Lorsque des données doivent être transmises ou reçues par l'intermédiaire d'Internet, l'objet émet un message radio. Ce message est ensuite recueilli par diverses stations de base et transmis au Sigfox Support System qui le transfère à son tour à une destination prédéfinie, en général une application IoT.

Si l'objet exige une réponse, l'application IoT a la possibilité, dans un délai limité, de délivrer une réponse à l'objet par l'intermédiaire du Sigfox Support System et des stations de base.

Cette conception implique que les objets n'ont jamais la capacité d'envoyer des données à des entités inconnues par Internet. Ils sont par conséquent protégés d'Internet par un parefeu très strict.

Sécurité des données en transit

L'authentification des messages et les mesures anti-réexécution constituent le fondement de la sécurité des données en transit et sont critiques pour gagner la confiance de l'ensemble de l'écosystème. Le protocole Sigfox fournit ce genre de fonctionnalités par défaut. Une mesure optionnelle anti-écoute complète le tout.

Sécurité des données stockées

Les données sensibles sont réparties dans chacun des maillons de la chaîne IoT, allant des objets stockant leurs clés d'authentification aux actifs de sécurité du Sigfox Support System concernant le réseau et les données clients. Cela implique divers mécanismes de sécurité au sein de l'écosystème Sigfox ainsi que des bonnes pratiques et processus veillant à l'intégrité, à la disponibilité et à la confidentialité de ces données dans le respect de la législation locale.

La clé de chiffrement de message étant unique pour chaque objet, la compromission de l'un des objets aura un impact très limité. Néanmoins, des pratiques de sécurité efficaces et un stockage sécurisé doivent être mis en place par le concepteur de l'objet.

Sigfox a travaillé avec son écosystème pour améliorer le niveau de sécurité des objets par l'adoption de pratiques exemplaires en matière de sécurité. De plus, les éléments sécurisés dédiés aux objets Sigfox sont désormais disponibles et garantissent une résistance aux intrusions.

Pour finir, Sigfox s'est associé à des entreprises spécialisées en évaluation de la sécurité afin d'aider les clients disposant d'applications critiques à atteindre des niveaux de sécurité corrects.

Les stations de base stockent les informations utilisateurs permettant de communiquer avec le cœur du réseau Sigfox. Elles sont sécurisée grâce à des méthodes pointues en la matière notamment une puce TPM (Trusted Platform Module). Le cœur du réseau Sigfox stocke les clés d'authentification des objets Sigfox Ready™, ainsi que les métadonnées relatives au trafic. Des solutions de pointe ont été déployées pour garantir l'intégrité, la disponibilité et la confidentialité de ces données. Un processus d'amélioration continue a été défini pour garantir la conformité du réseau Sigfox à la législation locale.

5.1 Sécurité relative au traitement des messages

Comme présenté dans la partie précédente, le réseau mondial Sigfox réalise plusieurs étapes de vérification lors du traitement des messages (voir ci-dessous).

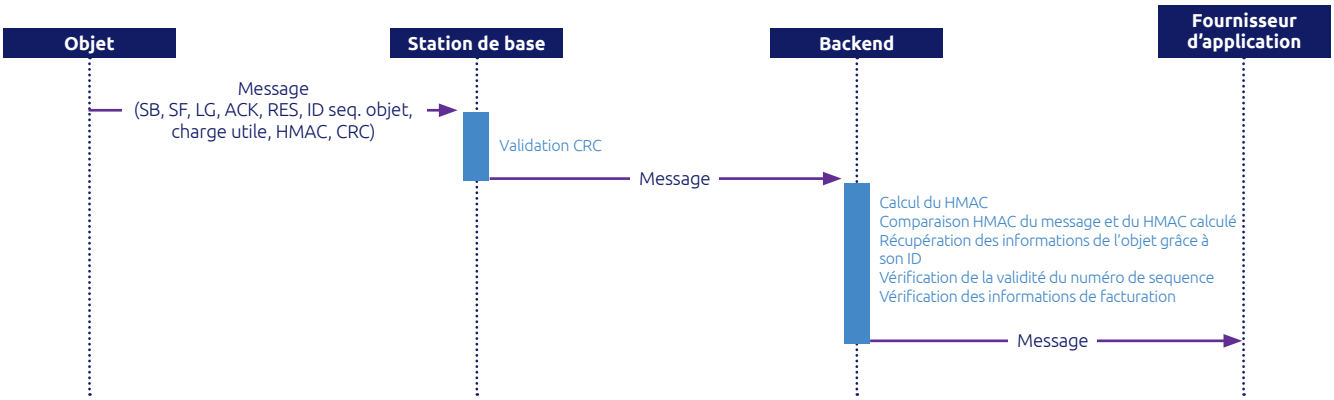


Figure 13: Différentes vérifications réalisées lors du traitement d'un message montant

Les paragraphes suivants présentent en détails les divers mécanismes mis en œuvre.

5.1.1 Numéro de séquence

Le numéro de séquence est un mécanisme anti-réexécution (associé au MAC). Il s'agit d'un simple compteur de messages à nombre entiers partant de zéro à un octet (rotation d'un mois avec 140 messages/jour).

Le numéro de séquence est vérifié par le Sigfox Support System afin de détecter et d'éliminer les tentatives de reproduction. L'intégrité du compteur est garantie par un jeton d'authentification du message.

Ce numéro de séquence est en mesure de recevoir des messages pour une fenêtre de validité donnée. Cette plage est comprise entre deux valeurs : le [dernier numéro de séquence validé +1] et le [dernier numéro de séquence validé +1 + 3 x le type d'abonnement – correspondant au nombre maximal de messages générés par l'objet chaque jour, avec une valeur minimale de 20].

Par exemple, si le dernier numéro de séquence validé est 5, la fenêtre de validité pour le numéro de séquence suivant sera déterminée comme suit, en fonction du type d'abonnement :

- pour un abonnement platine avec 140 messages par jour, le numéro de séquence sera compris entre 6 et 426 (6 + 3 x 140) ;
- pour un abonnement avec un message par jour, le numéro de séquence sera compris entre 6 et 26 (6 + 20) car 3 x 1 messages < 20.

5.1.2 Vérification MAC

Un chiffrement symétrique unique des clés d'authentification est attribué pour chaque objet au cours du processus de fabrication. Chaque message envoyé ou reçu par l'objet contient un jeton cryptographique calculé d'après cette clé d'authentification. La vérification du jeton garantit : l'authentification de l'expéditeur (l'objet pour un message montant ou le réseau Sigfox pour un message descendant) ainsi que l'intégrité du message. Dans le segment IT, l'authentification des communications entre le cœur du réseau Sigfox et les serveurs d'applications se base sur des approches classiques d'Internet telles le VPN ou HTTPS.

La vérification MAC garantit :

- l'intégrité – le message n'est pas altéré ;
- l'authentification de l'expéditeur.

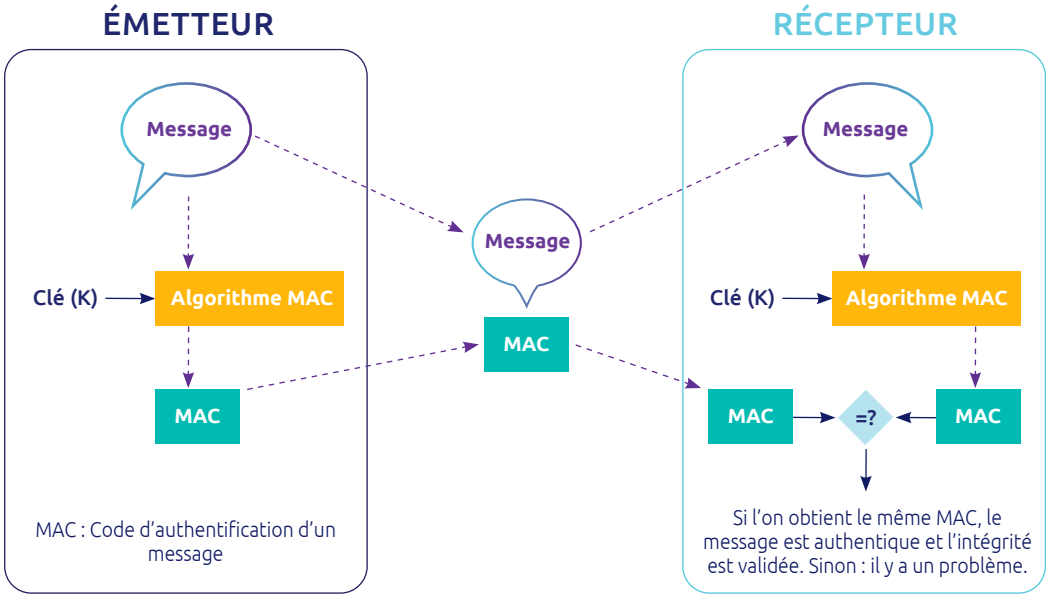


Figure 14: Vérification MAC de l'intégrité du message et de l'authentification de l'objet (source Wikipédia)

Si le message contient le numéro de séquence (voir la partie précédente), il ne peut être relu, même si le numéro de séquence est augmenté. En effet, la vérification MAC ne correspondra pas.

5.1.3 Chiffrement des messages

By default, data is conveyed over the air without any encryption. However, Par défaut, les données sont transmises par liaison radio sans cryptage. Toutefois, en fonction de l'application, ces données peuvent être de nature sensible et leur confidentialité doit être garantie.

Sigfox permet aux clients de choisir entre la mise en œuvre de leur propre solution de cryptage complète ou d'une solution de cryptage fournie par le protocole Sigfox. Cette solution de cryptage a été spécialement conçue pour des messages Sigfox très courts en collaboration avec le CEA-LETI. La clé de cryptage est dérivée de la clé de l'objet. Le cryptage utilisera le NAK (clé de l'appareil), le compteur de séquences ainsi que le compteur de roulement.

5.2 Sécurité des stations de base et communication

AUne station de base peut être déployée dans un environnement hostile, même si elle contient une Propriété Intellectuelle qui doit être protégée. Sigfox a intégré la fonctionnalité TPM dans les stations de base afin de sécuriser toutes les clés impliquées dans les divers mécanismes de sécurisation des stations de base.

- Il est impossible de dérober un logiciel sensible Sigfox.

- Il est impossible d'altérer le système d'exploitation d'une station de base :
  - un démarrage sécurisé vérifie son intégrité ;
  - l'IMA (Integrity Measurement Architecture) garantit l'intégrité de l'exécution.

- Il existe un lien entre le système d'exploitation (OS) et le matériel :
  - la station de base peut uniquement démarrer un OS créé par Sigfox ;
  - l'OS peut uniquement s'exécuter sur un matériel d'une station de base.

La communication entre la station de base et le Sigfox Support System est sécurisée par un VPN empêchant toute intrusion dans l'infrastructure centrale à partir de la station de base. Les identifiants VPN sont également protégés par le TPM.

5.3 Sécurité relative à la génération et l'approvisionnement de clés

La génération et l'approvisionnement de clés correspondent aux procédures de commande et d'approvisionnement des identifiants de l'objet (ID et NAK) dans l'objet (dans un élément sécurisé, un module de communication, un système sur puce - SoC - ou l'objet directement).

Ce processus ne peut être réalisé que si le fabricant correspondant réussit à obtenir la certification exigée par Sigfox pour communiquer sur le réseau. Il existe divers niveaux de certification, en fonction du composant (module ou objet).

Ce processus est décrit ci-après.

- Le fabricant envoie un email à Sigfox avec une requête pour un lot de N ID d'objet accompagné du certificat associé.

- Une fois la commande validée en interne, Sigfox assigne une plage d'ID d'objets au fabricant pour le certificat donné et procède au lancement de la génération. Le CRA (Central Registration Authority) génère la clé d'authentification réseau des objets (NAK) ainsi qu'un code d'autorisation (Porting Authorization Code – PAC). Le PAC est utilisé ultérieurement lors du processus d'activation de l'objet. La base de données est provisionnée avec les résultats de la génération.

- Le fabricant récupère les fichiers de sortie auprès du CRA :
  - un fichier binaire contenant des paires (ID d'objet, clé) chiffrées en AES-ECB ;
  - un fichier texte contenant des paires (ID d'objet, PAC).

- Le fabricant utilise une application Sigfox ainsi qu'une clé dédiée délivrée par Sigfox pour décrypter et charger la clé ainsi que l'ID d'objet dans chaque module, voire le code PAC initial.

- Le fournisseur/client final de l'application reçoit des objets/modules du fabricant avec leurs ID d'objet et leurs PAC.

- Le fournisseur/client final de l'application peut accéder au portail Internet « Operations Support System » (OSS) afin d'enregistrer l'objet en fournissant son ID et son PAC à un Opérateur Sigfox.

- L'OSS vérifie dans le CRA, l'ID d'objet et le PAC avant de générer un nouveau PAC qui sera renvoyé vers le fournisseur/client final de l'application. Ce renouvellement du PAC empêche qu'il soit réutilisé par un autre Opérateur Sigfox.

Grâce à cette approche, les NAK ne sont jamais rendus visibles en dehors de l'environnement sécurisé d'exécution dédié aux calculs cryptographiques.

5.4 Sécurité des centres de données

Le Sigfox Support System est essentiellement un réseau déployé dans le cloud. Ainsi, il bénéficie du savoir-faire de fournisseurs Internet et de technologies reconnues dans ce domaine.

- Plus précisément, le Sigfox Support System est hébergé dans des centres de données certifiées sécurisés. L'accès physique à chaque ensemble bénéficie d'une protection biométrique.

- Chaque centre de données est raccordé à Internet par deux fournisseurs d'accès indépendant.

- L'architecture Sigfox est par définition entièrement redondée et distribuée depuis les routeurs réseau jusqu'aux applications situées sur des machines virtuelles elles-mêmes localisées sur des serveurs physiques différents.

- Au niveau de la couche d'application, chaque composant est entièrement redondant, étroitement surveillé et entièrement modulable pour supporter une augmentation du trafic.

Le modèle Sigfox basé sur le cloud garantit un accès quasiment immédiat aux composants de services de l'OSS et du BSS Sigfox, permettant ainsi de minimiser le temps d'indisponibilité et de réduire les autres risques opérationnels contrôlés par le plan de continuité des services Sigfox.

large éventail de cyber-attaques comme les attaques par déni de service (DoS), les attaques par déni de service distribuées (DDoS), les attaques réfléchies (RDoS) ainsi que les attaques réfléchies distribuées (DRDoS).

service de protection cloud avec un certain nombre de centres de filtrage afin de détecter et de prévenir les cyber-attaques contre les réseaux ou les sites Internet. Cette solution utilise des algorithmes propriétaires de mitigation et de détection correspondant aux modèles spécifiques de transmission des données pour éviter les faux positifs.

6 Outils de couverture de service

Sigfox fournit au public ainsi qu'à ses partenaires differentes fonctionnalitées pour évaluer la couverture des services.

6.1 Accès public à la couverture de service

Un lien sur le site Web Sigfox permet d'accéder à une carte des zones de couverture : **www.sigfox.com/coverage**

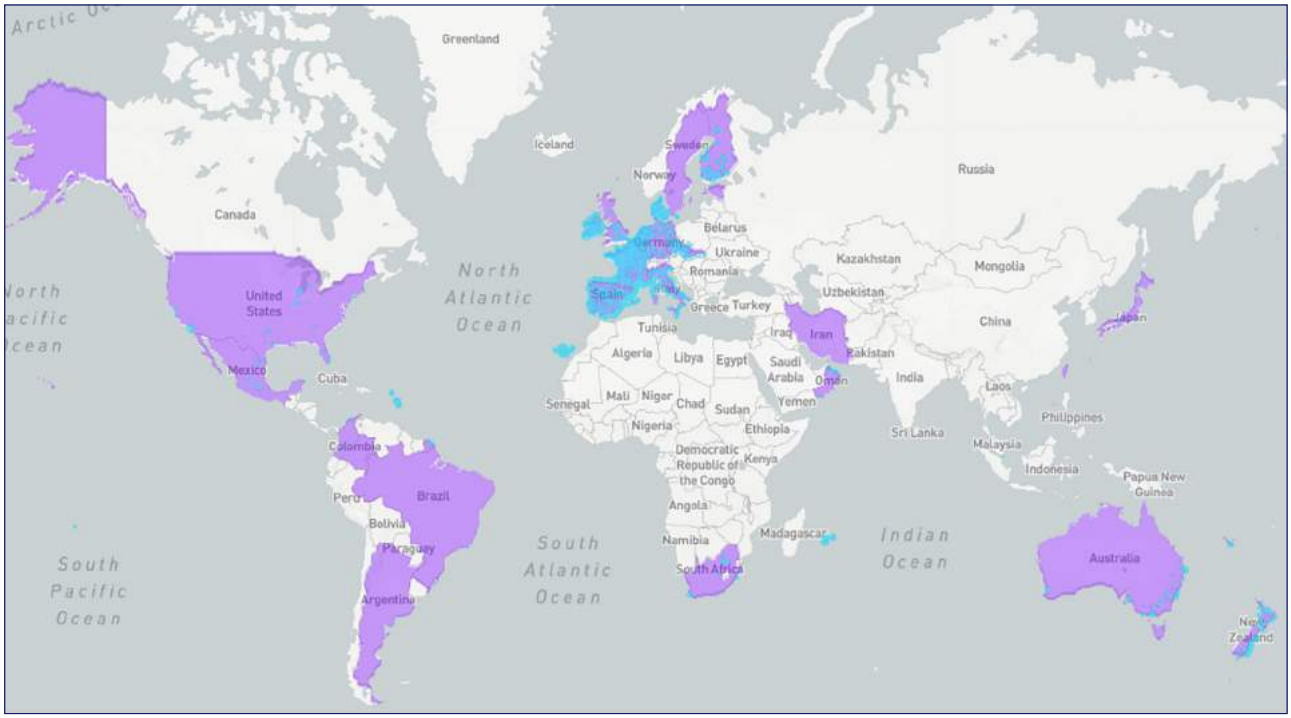


Figure 15: Carte mondiale des zones de couverture (cette carte est régulièrement mise à jour, veuillez consulter notre site www.sigfox.com/coverage)

Cette carte est fournie à titre indicatif et ne constitue aucune garantie du niveau de service. L'estimation de la couverture s'appuie sur des prédictions informatiques en extérieur pour la classe d'objets U0 (niveau de sortie maximal d'après les critères de certification de SIGFOX Ready™). SIGFOX tente de fournir des informations précises et complètes grâce à cet outil d'estimation de la couverture en ligne. Cependant, SIGFOX et ses distributeurs opérant dans les régions couvertes ne peuvent en aucun cas garantir la qualité, l'exactitude ou l'intégralité des informations. L'outil d'estimation de la couverture est fourni à titre indicatif, « en l'état » et sans garantie de quelque nature que ce soit, expresse ou implicite. SIGFOX et les distributeurs concernés dans les régions couvertes figurant sur cette carte ne sauraient être tenus responsables d'un quelconque dommage résultant de l'utilisation ou de l'utilisation abusive de l'outil d'estimation de la couverture.

Cette carte est accessible au public et affiche la couverture réseau en direct, ainsi que les pays en cours de déploiement.

6.2 Carte de couverture de services

Une carte de couverture de service est disponible dans le portail de l'OSS pour les Opérateurs Sigfox et les partenaires.

Elle fonctionne comme une carte thermique et fournit des informations en temps réel concernant la couverture. Il est possible d'affiner le resultat en ajustant la catégorie de l'objet en liaison montante et la marge de liaison radio souhaitée pour obtenir la carte de services Sigfox correspondant à l'application.

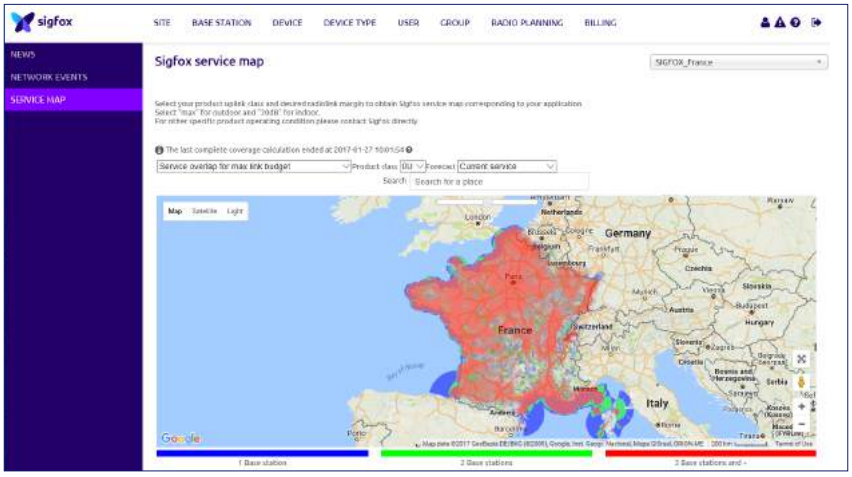


Figure 16 : Carte de prédiction de services intégrée dans le portail OSS

6.3 Interface de programmation d'applications (API) de couverture globale

Une nouvelle API est en cours de développement et sera accessible à tous les utilisateurs du portail OSS (opérateurs et clients).

L'objectif est d'indiquer la qualité de couverture de tous les opérateurs publics Sigfox du monde entier tout en étant adapté à tous les types d'application (pénétration, objets, etc.).

La requête de type GET devra fournir la latitude et la longitude {lat, long} ou une adresse postale spécifique. Le résultat sera la marge de signal des meilleures cellules.

GLOBALE

- Qualité de la couverture pour tous les opérateurs publics Sigfox dans le monde
- Accessible à tous les utilisateurs ayant accès au backend (opérateurs et clients)

FLEXIBLE

- Convient à tout type d'application (pénétration, objets)

SIMPLE

- Entrée simple : {lat, long}, inutile de saisir le pays recherché
- Résultats clairs : {marge de signal des meilleures cellules}
- Requêtes par lot : POST API

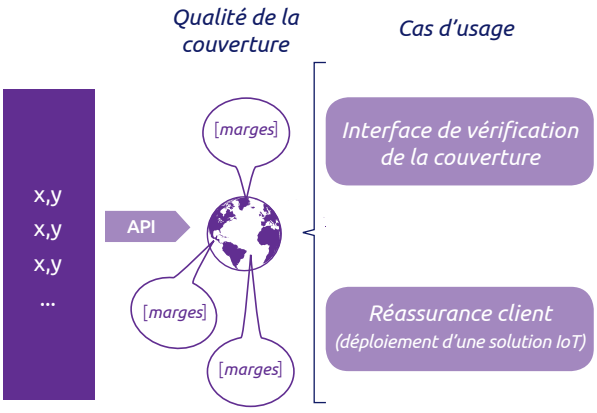


Figure 17 : API de couverture pour évaluer la couverture du réseau à différents endroits

+33 (0)5 82 08 07 10
Bâtiment E-volution
425, rue Jean Rostand
31670 Labrège – France
sigfox.com

sigfox