INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

# RAPPORT
# WSN SIGFOX

5A ISS - 2024/2025

Par Brian Biendou
Clément Marcé
Marie Brunetto
Timothé Bigot

**SOMMAIRE**

**Introduction.....2**
**I - Description Technique de Sigfox.....2**
1. Couche Physique – Interface Radio.....2
2. Couche MAC.....3
3. Le réseau Sigfox.....4
4. La sécurisation logiciel et matériel du réseau Sigfox.....5
**II - Analyse de la Consommation Énergétique.....7**
1. Les avantages du protocole en matière d'énergie.....7
2. Les chiffres clés de la consommation des appareils Sigfox.....8
**III- Avantages et Limites du WSN Sigfox.....10**
1. Avantages et Applications Idéales pour Sigfox.....10
A. Faible consommation énergétique.....10
B. Portée longue distance.....11
C. Simplicité d'installation et de gestion.....11
2. Limites.....12
A. Débit de données limité.....12
B. Protocole ALOHA et gestion des collisions.....12
C. Couverture dépendante des opérateurs et limites géographiques.....13
D. Comparaison avec les technologies concurrentes.....13
**Conclusion.....13**
**Références.....14**

# Introduction

Sigfox est une technologie de communication sans fil dédiée aux objets connectés (IoT), offrant une connectivité longue portée et basse consommation. Ce réseau de type Wide Area Network (WAN) cible les applications nécessitant une faible quantité de données et une transmission peu fréquente, comme la surveillance environnementale, la gestion de la chaîne d'approvisionnement, et les capteurs de bâtiments intelligents. À travers ce rapport, nous allons voir les caractéristiques de la technologie sous trois aspects : la description technique, l'analyse de la consommation énergétique et enfin les avantages et limitations que Sigfox présente

# I - Description Technique de Sigfox

## 1. Couche Physique – Interface Radio

Sigfox repose sur des stations de base pour recevoir des messages envoyés par des appareils IoT sans infrastructure réseau complexe. Pour se faire, il opère principalement dans la bande de fréquence non licenciée ISM. Ces bandes dépendant des zones géographique, on retrouve alors des caractéristiques différentes selon la zone de déploiement de la technologie :

- En zone suivant les normes ETSI (Principalement pays européen), une bande de 192 kHz est utilisée entre 868 MHz et 868,2 MHz, avec des messages de 100Hz.
- Dans le reste du monde, la bande utilisée est comprise entre 902 MHz et 928 MHz, avec des messages atteignant eux les 600Hz. Des restrictions supplémentaires sont appliquées selon les réglementations locales sur les télécommunications.[1] Actuellement, sept zones géographiques constituent le réseau Sigfox, reposant sur des zones géographiques larges ou des pays précis (Japon, Corée, Russie, Inde)[4]

**En termes de modulation**, Sigfox utilise des bandes ultra étroites, aussi appelées Ultra Narrow Band ou UNB, expliquant la taille modeste de la bande utilisée, notamment en zone ETSI. Cela permet aux signaux transmis avec des stations de parcourir de grandes distances en ayant une meilleure résistance aux bruits.[1] En plus de l'UNB, Sigfox utilise une modulation D-BPSK, ou Differential Binary Phase Shift Keying. Cette technologie offre l'avantage d'être peu coûteux en plus d'une facilité d'emploi et de sensibilité accrue par les récepteurs.[2]

**La portée des signaux** Sigfox est une caractéristique souvent mise en avant par sa distance avantageuse. Dépendant d'abord de la topologie, elle dépend également du débit : augmenter le débit induira une réduction de la portée possible.[1] Cette portée est estimée pouvant atteindre les 10 km en zone urbaine et 40 km en zones rurales. L'utilisation de répéteurs permet d'augmenter cette distance si une application le nécessite.[3]

**Concernant la taille des messages échangés**, Sigfox est une technologie conçue pour l'échange de messages courts: entre 0 et 12 octets de charge utile (ou 8 dans le cas de paquets descendants). En plus des caractéristiques vues précédemment tels que la haute portée et le faible coût, cela justifie son utilisation importante dans des cas de réseaux d'objets connectés utilisant capteurs, statuts d'événements ou transferts de données GPS. À titre indicatif, des coordonnées GPS s'écrivent sur 6 octets, une température peut s'écrire sur 2 octets, tandis qu'une vitesse ou un statut peut s'écrire sur un unique octet. Les 12 octets proposés par Sigfox permettent ainsi de couvrir de nombreux cas d'utilisation de cas d'échanges de messages simples.[1]

## 2. Couche MAC

Au-delà de la couche physique, Sigfox propose également une gestion du réseau sur la couche réseau. Pour cela, un protocole est proposé, dont les spécifications sont publiques depuis 2019.

Chaque objet communicant avec le protocole sigfox possèdent deux numéros permettant de les identifier, le couple ID et PAC (Porting Authorization Code), sans quoi la communication sur le réseau Sigfox ne peut s'effectuer.[2]

Les trames Sigfox dépendent de la nature de l'émetteur et du récepteur. Il existe ainsi :

- **Les trames montantes**, dites Uplinks. Il s'agit des trames envoyées par le module au réseau Sigfox. Celles-ci possèdent une charge utile de 0 à 12 octets qui, ajoutée aux données protocolaires, nous donne une trame totale de 24 octets. Il comprend notamment le couple ID/PAC permettant la communication Sigfox.[2]
- **Les trames descendantes**, dites Downlinks. Il s'agit des trames reçues du cœur réseau par le module. Celles-ci sont en revanche limitées à 8 octets de charge utile. La taille totale de la trame descendante est elle plus volumineuse, possédant davantage de données liées au protocole.[2]

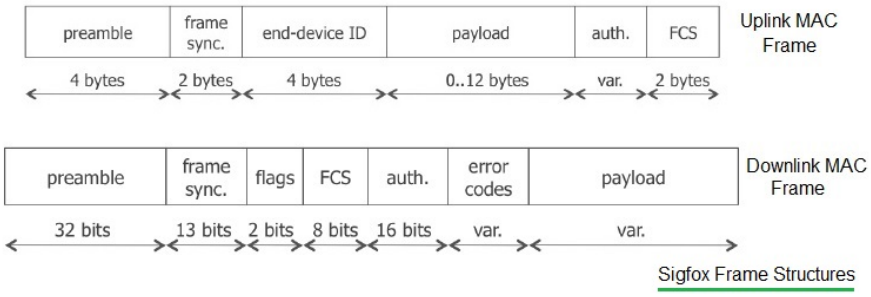



*Figure 1 - Structure des trames Sigfox, selon la nature montante ou descendante du message [2]*

Afin de gérer les différents types de pertes, de multiples sécurités sont mises en place dans ce protocole :

- **Redondance des paquets :** Afin de compenser des potentielles pertes dûes à un canal bruité ou des collisions, les paquets sont toujours émis par salves de trois.

- **Des numéros de séquences :** Permet de pallier des pertes de paquets intermédiaires ou de contrer des attaques de ré-émissions.
- **Des Frame Check Sequence (FCS) :** Données en queue de trame permettant de vérifier l'intégrité du message et détecter les erreurs, que ce soit dû à un brouillage intentionnel (par attaquant) ou non (canaux bruités, erreur bit). Cette vérification se fait avec l'algorithme dit de Cyclic Redundancy Check (CRC), plus précisément CRC-16.
- **Encryption :** Enfin, une encryption AES 128 est mise en place pour l'authentification, certifiant la confidentialité des données.[2]

## 3. Le réseau Sigfox

Les communications faites par un capteur sont transmises et reçues par une ou plusieurs stations de base. Ces stations de bases sont réparties dans les villes et constituent la première partie du réseau Sigfox. Ces stations relaient alors les informations au cœur du réseau, qualifié de Sigfox Cloud, la seconde partie du réseau Sigfox. La liaison entre ces deux parties se fait sur l'internet à travers un connexion sécurisée.[1]

Le cloud communique avec les utilisateurs et les APIs logiciels et de serveurs afin de pouvoir stocker, relayer et traiter les données récupérées du réseau de capteurs.

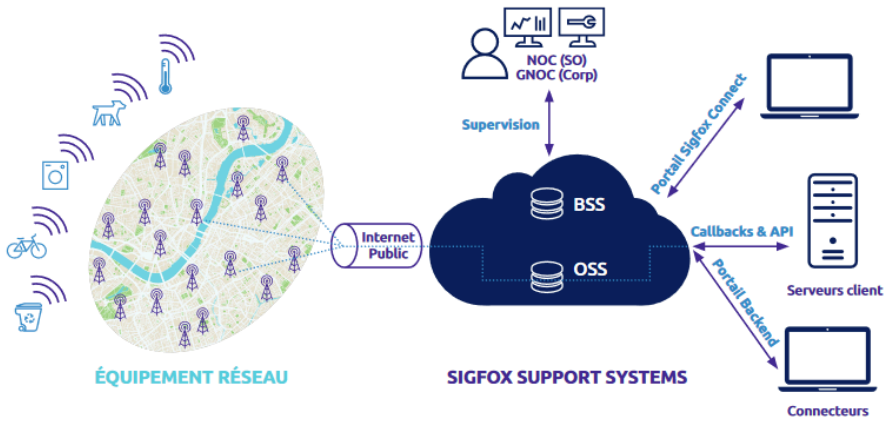



*Figure 2 - Vue simplifiée de l'architecture du réseau Sigfox*

Comme mentionné en Section I-1, le réseau est divisé en 7 zones de configuration radio. Ceci est dû aux réglementations locales et autres lois qui peuvent varier selon les pays/continents. Ces zones sont susceptibles d'évoluer en raison des changements législatifs et de l'arrivée de Sigfox dans de nouveaux pays. Ces zones sont appelées réseaux d'appartenances, ou RC.[4]

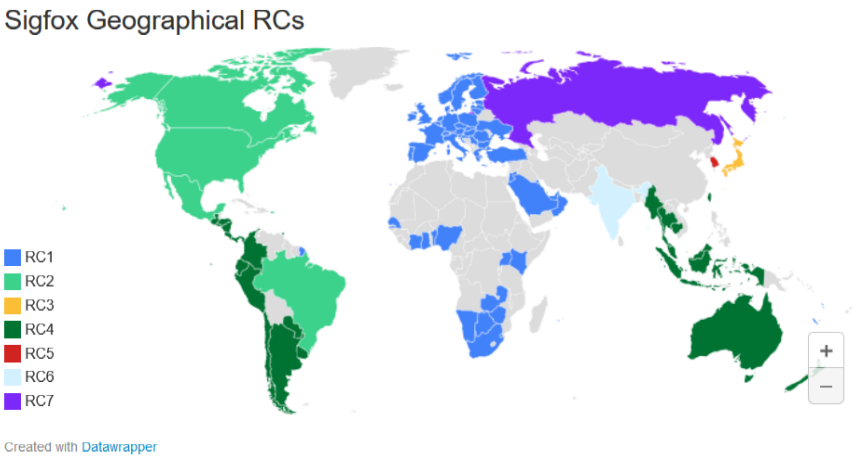



*Figure 3 - Carte représentant les 7 différentes zones de configurations radio du réseau Sigfox [4]*

Ces zones répondant à des normes différentes, un appareil supportant Sigfox devra être configuré afin de répondre à l'une de ces zones. Il est donc conseillé de créer des variations des appareils selon la configuration réseau d'appartenance. Il est néanmoins possible de réaliser du multi-RC, notamment à travers Sigfox Monarch, qui est une fonctionnalité permettant la reconnaissance et l'adaptation selon la configuration réseau.

# 4. La sécurisation logiciel et matériel du réseau Sigfox

Plus tôt dans cette partie, nous avons vu quelques procédés mis en place pour assurer une bonne qualité de service, via la redondance, le FCS et le chiffrement, notamment. Nous allons maintenant aller plus en détails dans cette section sur cet aspect de sécurisation de ce réseau d'un point de vue logiciel et matériel.

Tout d'abord, deux propriétés relevant de la sécurité sont proposées lors de l'utilisation de Sigfox : l'**authenticité des messages**, et leur **confidentialité** [5] :

- L'authentification, elle, est native au système même lors de son installation et utilisation, et permet d'être certain et de vérifier qu'un capteur appartient bien au réseau défini et d'éviter l'interception de message et l'usurpation d'identité. Cela est mis en place via AES, utilisé en mode CBC-MAC (Cipher Block Chaining - Message Authentication Code) et repose sur un tag d'authentification qui couvre l'en tête du message (qui contient l'identifiant du terminal et le compteur de message) ainsi que les données applicatives. Cette identifiant unique codé sur 4 à 5 octets est donc associé à une clé AES 128 et un jeu d'algorithme permettant un changement direct du champs d'authentification, qui à l'avantage de n'être manipulé que par l'objet connecté, et le système centrale de Sigfox.[6]

- Le caractère confidentiel des messages est une option que l'utilisateur est libre de choisir ou non, et consiste à chiffrer les données à envoyer dans le cas où elles pourraient être sensibles et consultées par un tiers malveillant. AES est utilisé dans ce cadre également, soit en mode CTR soit en mode compteur. En cas de chiffrement, le payload ou sont les données en clair est utilisé pour stocker à la place les données chiffrées, comme indiqué sur la figure ci-bas.[5]

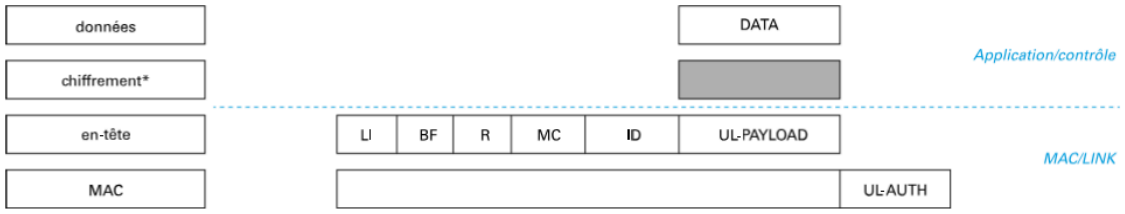



*Figure 4 - Construction d'un message montant Sigfox, les opérations optionnelles sont indiquées avec * et les champs optionnels apparaissent en gris* [5]

À ces deux éléments s'ajoutent des processus liés à la caractéristiques intrinsèque de ce réseau, en particulier sa capacité cognitive et intelligente. Cette autonomie qui a été pensée lors de sa conception lui permet de **détecter automatiquement des comportement anormaux**, parmis les suivant [6] :

- Des mouvements d'objets normalement fixes  mais se déplacent peut être détecté et lever un signalement

- La corrélation activité/distance, d'un objet mobile ne pouvant dépasser une certaine vitesse mais, dont on remarque qu'une grande distance a été parcouru en un faible temps permet déduire une compromission éventuel

- Des dispositifs radioélectriques de saturation de stations, en imitant des objets du réseau peuvent rapidement détecté et localisé

De plus, Sigfox, en plus d'avoir cette capacité d'autonomie sur de potentielles intrusions, a été pensé au **niveau structurel pour réduire les risques**. Les stations radios ne disposent d'aucun algorithme de sécurité, lié à l'authentification, mais redirigent seulement les trames à travers le réseau et vers les serveurs. Pour ces stations en particulier néanmoins, l'utilisation de structures logiciels sécurisées ont été mises en place, par VPN (Virtual Private Network) et TMP (Trusted Platform Module). Il est aussi important de noter que le processus d'authentification à lui seul est suffisant dans le cas d'une compromission au niveau physique du capteur, de sorte à ne pas compromettre les autres capteurs et le réseau Sigfox.[6]

Cependant, des **vulnérabilités matérielles** peuvent être présentes, et doivent être considérées en complément des failles possible logiciels. Particulièrement sur les capteurs, dont la fabrication n'est pas nécessairement du ressort de Sigfox, mais dont des standards de fabrication existent pour fiabiliser au mieux ces dispositifs [6]. Des mesures au sein de la chaîne d'approvisionnement sont possible et encouragé pour paliers à de possibles risques [5], notamment effectuer des audits au niveau fournisseur, imposer un cahier des charges strict, privilégier des composants certifiés ANSSI (Agence nationale de la sécurité des systèmes d'information), impliquer le service achat dans la sécurité. Toutes ces dispositions ont un coût et doivent donc être évaluées au mieux.

Des **vulnérabilités au niveau logiciel** sont aussi possibles. Le **nombre restreint et la faible taille des messages** permet d'injecter sur le réseau des messages supplémentaires, souvent des copies. Le but est d'exploiter le fait que le compteur de message va boucler à un moment donné pour faire acquitter des trames montantes qui ne devraient pas l'être. Pour un message, on compte 12 bits maximum, sans chiffrement, donc au bout de 2^12 = 4096 messages, le compteur est remis à zéro  et des messages montants précédemment envoyés redeviennent cryptographiquement valides. Dans le cas d'un abonnement platinium, le compteur reboucle au bout de compteur 4096/140=29 jours. Cette taille relativement réduite du compteur permet donc d'enfreindre la propriété d'authenticité des messages que le système Sigfox promet de garantir. Cette faille a cependant été corrigé, une solution est d'inclure dans le calcul du tag d'identification, les 8 bits de compteur additionnel, même sans chiffrement pour obtenir une taille de 20 bits, soit un compteur remis à zéro tout les 2^20/140 = 20 ans, suffisant pour résoudre ce problème [5]. Une autre vulnérabilité, corrigée depuis, consiste à **exploiter un défaut du mode CBC-MAC** et de créer un message valide d'un point de vue cryptographique mais ce, sans la clé NAK sur serveur Sigfox, pourtant indispensable. La solution a été d'utiliser le mode HMAC ou CMAC qui assure le processus d'authentification pour des messages de taille variable, qui était à l'origine du problème.

# II - Analyse de la Consommation Énergétique

## 1. Les avantages du protocole en matière d'énergie

Sigfox est considéré comme un protocole optimisé pour la faible consommation d'énergie pour différentes raisons.

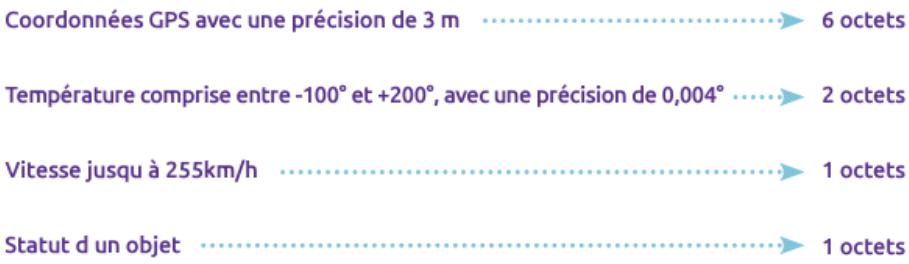
**Une communication réduite au strict nécessaire :** Le protocole Sigfox met en avant une communication limitée en temps et en quantité d'information pour ne solliciter les appareils que lorsque cela est nécessaire.

Comme vu précédemment, le protocole repose sur l'utilisation d'une bande de fréquence publique dont l'accès est limité dans le temps par des normes ; 1% du temps max par jour en Europe par exemple. De plus, nous avons vu que les trames Sigfox sont limitées à 12 ou 8

octets. Avec un débit allant de 100 à 600 bits par seconde selon les régions, le nombre total de trames émises se limite à 140 par jour en Europe soit 6 par heure.

Le nombre d'émissions d'informations des appareils Sigfox est donc réduit au maximum, incitant les capteurs à ne communiquer que lorsque cela est strictement nécessaire.

Contrairement à ce que l'on pourrait penser, ce fonctionnement n'est pas contraignant puisque la construction des trames a été pensée pour permettre de contenir suffisamment d'informations dans la plupart des applications IoT. En voici quelques exemples :




**Le mode veille des appareils :** Dans une communication Sigfox type, les trames Uplink (les données du capteur remontent vers le serveur) sont privilégiées et constituent la majorité des trames transmises. Le mode Downlink est uniquement utilisé pour mettre à jour la configuration intrinsèque des appareils depuis le serveur. Ce trafic principalement unidirectionnel permet aux capteurs de ne pas avoir à être constamment "sur écoute" mais plutôt de rester en mode veille jusqu'à ce qu'ils aient une donnée à transmettre. Ainsi, les batteries sont moins sollicitées et leur durée de vie est prolongée, pouvant atteindre entre 5 et 15 ans selon les types d'applications. Dans le futur, des moyens d'auto-alimentation des capteurs pourraient même permettre de ne plus avoir à changer les batteries des appareils, du moins jusqu'à ce qu'elles ne fonctionnent plus.

**Un type de modulation faible consommation :** Comme vu précédemment, la modulation UNB est également un gros avantage en termes de consommation. Elle permet, en plus de réduire le bruit, de consommer moins d'énergie pour émettre de l'information. Ceci vient du fait que l'UNB fait abstraction de beaucoup plus de fréquences que l'UWB par exemple.

## 2. Les chiffres clés de la consommation des appareils Sigfox

Maintenant que nous avons étudié les principaux aspects du protocole qui visent à optimiser l'énergie utilisée, analysons plus concrètement la consommation des appareils sur le réseau Sigfox :

**Le mode veille** dans lequel se trouve les capteurs la majorité du temps est ce qui nous intéresse en premier. Dans ce mode, les appareils consomment généralement moins de **10 uA**,

ce qui s'apparente à la consommation de veille d'un microcontrôleur type sur le marché. Certains appareils Sigfox optimisés low énergie peuvent descendre jusqu'à quelques dixièmes de micro ampères.

Cette consommation est relativement faible en comparaison au mode actif des capteurs où l'on se situe généralement plus autour de quelques dizaines de mA. L'image suivante illustre un exemple de consommation de modules Sigfox, l'un optimisé low énergie et l'autre non:

| Module Sigfox | Consommation en veille | Consommation pendant transmission |
|---|---|---|
| Wisol SFM10R1 | 0,5 - 2 µA | 50 - 60 mA |
| TD1208 (Telecom Design) | 1 - 2 µA | 35 - 60 mA |

**En émission**, nous allons considérer l'envoi d'un message de taille maximale : 12 octets. Un message de 12 octets contient 12*8=96 bits. En considérant que le débit de communication Sigfox se situe autour de 100 bps en Europe, l'émission d'une trame prend environ 1 seconde.

La consommation d'une émission sigfox étant d'environ 60 mA, l'énergie d'une émission Sigfox est de 60*1/3600 = **0.016 mAh.** Cela fait également **160 nAh/bit.**

Un appareil Sigfox émet au maximum 6 messages par heure, ce qui fait une consommation totale de 0.1 mAh (à laquelle s'ajoute la consommation de veille qui est négligeable).

**En réception**, la consommation est moindre. Tout d'abord un appareil Sigfox ne se met en écoute que lorsqu' une réponse est attendue à la suite d'une émission. Nous avons vu précédemment que ce cas de figure intervient très rarement car l'émission est privilégiée par le protocole. Lorsqu'un capteur attend une réponse, la fenêtre d'écoute qu'il ouvre est plus longue qu'une émission ; environ 20 secondes. Pendant celle-ci, la consommation est cependant estimée à la moitié de celle d'une émission, c'est à dire 30 mA.
La consommation d'une réception est donc de 30*20/3600 = **0.16 mAh.**

Bien que la consommation en réception soit supérieure à celle d'une émission, il est difficile d'estimer la consommation des réceptions lors d'un usage tant celles-ci interviennent rarement. Il est également difficile de comparer la consommation de réception de ce protocole à d'autres, on peut cependant penser que celle-ci sera plus faible car elle intervient moins fréquemment.

**Dans un cas d'usage type**, nous pouvons considérer un capteur de température ambiante dont les caractéristiques sont les suivantes :

| | |
|---|---|
| Plage de températures | [-50 ; +50] ° |
| Précision | 0.01 ° |
| Nombre de bits nécessaires | 2^n > 100 * 0.01 soit n = 14 bits |
| Nombre d'octets nécessaires | 2 (sur les 12 disponibles) |
| Nombre d'émission par jour | 24 (1/heure) |
| Nombre de réception par jour | 1 (1 acknowledge en fin de journée) |
| Consommation de veille | 2 uA |
| Consommation d'émission | 60 mA |
| Consommation de réception | 30 mA |

Dans ce cas de figure la consommation est la suivante :

- **Émission** : Une émission de 1s toutes les heures soit 24s d'émission en tout dans une journée. Une émission consomme 60 mA donc la consommation journalière d'émission est de 60 * 24 / 3600 = **0.4 mAh par jour.**
- **Réception** : une réception complète qui annonce la bonne acquisition des 24 mesures du jour. Consommation de **0.16 mAh par jour.**
- **Veille** : Le temps total en mode veille de l'appareil est de 24*3600-24-20 = 86 356 s. La consommation dans ce mode est en moyenne de 2 uA. On a donc une consommation journalière de (86 356/3600)*(2/1000) = **0.048 mAh par jour.**
- **Total : 0.4 + 0.16 + 0.048 = 0.608 mAh/jour.**

En comparaison avec un capteur Bluetooth Low Energy dans le domaine du relevé de températures, on s'attend typiquement dans la documentation à avoir une consommation de l'ordre de deux fois la valeur de celle-ci. Évidemment, il faut garder à l'esprit que ces résultats dépendent énormément de différents facteurs et notamment du nombre de réception que l'application requiert.

# III- Avantages et Limites du WSN Sigfox

## 1. Avantages et Applications Idéales pour Sigfox

Sigfox est conçu pour répondre à des besoins spécifiques de l'Internet des Objets (IoT) en offrant une connectivité longue portée avec une très faible consommation énergétique, ce

qui en fait une option particulièrement adaptée pour des applications de capteurs à bas débit et faible fréquence de transmission. Voici les avantages principaux :

## A. Faible consommation énergétique

- Consommation ultra-faible : Sigfox est optimisé pour les dispositifs alimentés par batterie, souvent dans des lieux où le remplacement fréquent des batteries n'est pas possible. Grâce à la modulation BPSK (Binary Phase Shift Keying) en bande ultra-étroite (UNB), Sigfox consomme peu d'énergie par transmission, avec des valeurs typiques de l'ordre de quelques nanojoules par bit (nJ/bit).
- Adapté aux dispositifs longue durée de vie : Cette faible consommation permet aux appareils Sigfox de fonctionner sur des périodes très longues (plusieurs années) avec une seule batterie, réduisant ainsi les coûts de maintenance. Cela est particulièrement avantageux dans les applications de capteurs en zones reculées ou dans des environnements difficilement accessibles.

**Exemple d'applications :**

**Suivi de la faune sauvage :** Des capteurs de position et de température pour le suivi des animaux sauvages peuvent envoyer des données de manière sporadique, sans nécessiter de remplacement fréquent de batteries.

**Capteurs environnementaux en zone rurale** : Mesure de la qualité de l'air, de la température ou de l'humidité avec des intervalles de plusieurs heures, évitant les infrastructures coûteuses.

## B. Portée longue distance

**Capacité de couverture étendue** : Sigfox peut couvrir jusqu'à 50 km en zones rurales dégagées et environ 10 km en zones urbaines denses, ce qui réduit le nombre de stations de base nécessaires pour des déploiements sur de larges zones géographiques. En utilisant une bande passante étroite (100 Hz par canal), il minimise les interférences et permet une meilleure sensibilité du signal, ce qui est idéal pour des déploiements dans des zones isolées ou faiblement peuplées.

**Exemple d'applications** :

- **Gestion des ressources naturelles** : La gestion des niveaux d'eau dans des barrages ou des réservoirs dans des régions éloignées où l'installation de stations de base serait coûteuse est facilitée par la portée étendue de Sigfox.
- **Suivi d'infrastructures** : Surveillance des pipelines de pétrole ou de gaz, et des lignes de distribution d'eau ou d'électricité en zones rurales.

### C. Simplicité d'installation et de gestion

- **Absence de synchronisation d'horloge** : Le protocole ALOHA pour de Sigfox et son absence de synchronisation d'horloge permettent des transmissions sans gestion stricte de l'accès au réseau, simplifiant ainsi l'installation et la maintenance du réseau. Cette approche « fire-and-forget » (envoi sans confirmation) est pratique pour les capteurs IoT qui envoient de petites quantités de données peu fréquemment.
- **Faible coût d'infrastructure** : La simplicité du réseau Sigfox réduit les coûts opérationnels et de déploiement, ce qui est un avantage pour les entreprises cherchant des solutions IoT à moindre coût pour des applications massives ou de grande portée.

**Exemple d'applications** :

- **Suivi de la chaîne d'approvisionnement** : Capteurs de suivi pour conteneurs ou palettes, qui envoient des mises à jour sporadiques sur leur emplacement.
- **Bâtiments intelligents** : Surveillance des installations comme les compteurs d'eau ou de gaz, les détecteurs de fumée, ou les capteurs d'inondation, où des mises à jour fréquentes ne sont pas nécessaires.

## 2. Limites

Malgré ses avantages, Sigfox présente certaines limites qui restreignent son adoption à des applications spécifiques, notamment en raison de ses caractéristiques techniques qui réduisent sa polyvalence par rapport à d'autres technologies IoT. Voici une analyse des principales limitations :

### A. Débit de données limité

- **Faible taux de transmission** : Avec un débit maximal d'environ 100 bps, Sigfox ne permet pas le transfert de grandes quantités de données, ce qui restreint son utilisation à des applications à très faible débit. Cette limite le rend peu adapté pour des applications nécessitant des mises à jour fréquentes ou la transmission de données complexes, comme l'audio, la vidéo, ou des capteurs nécessitant des échantillons fréquents.
- **Impact sur les applications** : Les capteurs à haut débit ou nécessitant des réponses en temps réel, comme ceux utilisés dans les soins de santé (surveillance médicale), sont mal desservis par Sigfox. Cette limitation de débit empêche aussi les utilisateurs de regrouper de grandes quantités de données avant de les transmettre, imposant des transmissions très limitées en volume.

## B. Protocole ALOHA et gestion des collisions

- **Pas de gestion stricte des collisions** : En utilisant un modèle ALOHA pur, Sigfox tolère les collisions entre messages. Cela peut entraîner des pertes de données, surtout dans les environnements densément peuplés d'appareils. Cette limite en fait un choix moins fiable pour les applications critiques, où des données perdues pourraient avoir un impact sérieux.
- **Concurrence avec d'autres appareils** : La bande ISM, étant partagée, est également utilisée par d'autres technologies, telles que WiFi, Bluetooth et d'autres solutions IoT, ce qui augmente les risques d'interférences et peut dégrader les performances de Sigfox dans les zones densément peuplées.
- **Impact sur le marché** : Dans les environnements urbains où le nombre de dispositifs IoT augmente, les utilisateurs peuvent se tourner vers des solutions avec un meilleur contrôle des collisions et de la qualité de service (QoS), comme LoRa ou NB-IoT.

## C. Couverture dépendante des opérateurs et limites géographiques

- **Couverture restreinte par l'infrastructure de Sigfox** : Sigfox est dépendant de son propre réseau d'infrastructure. Bien que présent dans plusieurs pays, sa couverture n'est pas aussi omniprésente que celle des réseaux cellulaires (comme NB-IoT). Pour les entreprises ayant besoin de connectivité IoT mondiale, cette restriction de couverture peut poser des limites.
- **Dépendance vis-à-vis de l'opérateur** : Les utilisateurs ne peuvent pas installer leurs propres stations de base Sigfox comme c'est possible avec LoRa, limitant les possibilités de déploiement en fonction de la couverture réseau Sigfox existante.
- **Impact sur le marché** : Les entreprises cherchant une flexibilité de déploiement dans des zones non couvertes peuvent privilégier LoRaWAN, qui offre une solution décentralisée avec la possibilité de créer des réseaux privés.

## D. Comparaison avec les technologies concurrentes

**Position sur le marché IoT** : Sigfox occupe une niche dans le marché IoT avec des applications simples et peu énergivores. Cependant, des technologies comme LoRa, NB-IoT, et même LTE-M, gagnent en popularité car elles offrent plus de flexibilité (débits de données variés, meilleures options de QoS, gestion de la densité des appareils). NB-IoT, par exemple, bénéficie de l'infrastructure cellulaire existante, offrant une meilleure couverture et une plus grande capacité pour des applications industrielles.

# Conclusion

En somme, Sigfox s’impose comme une solution IoT spécialisée, parfaitement adaptée aux applications à faible débit et faible consommation énergétique, grâce à sa modulation en bande ultra-étroite et son protocole simplifié. Bien qu'il offre une couverture longue portée et permette une autonomie prolongée des capteurs, sa faible bande passante et sa gestion des collisions via ALOHA limitent son usage aux environnements moins denses et aux applications nécessitant peu de données. Face à des concurrents comme LoRa et NB-IoT, qui offrent davantage de flexibilité, Sigfox se distingue avant tout pour les applications de surveillance à distance où la simplicité et la durée de vie des capteurs priment sur la quantité de données échangées.

# Références


[1] SIGFOX (2017, Jul). *Présentation technique de Sigfox* [Online].
Available:
https://lms.fun-mooc.fr/asset-v1:univ-toulouse+101001+session02+type@asset+block/Presentation_technique_de_Sigfox_Juillet_2017.pdf

[2] G. Paquet. (2020, Mar, 27). *Introduction à SIGFOX* [Online].
Available: https://www.linuxembedded.fr/2020/03/introduction-a-sigfox

[3] *Sigfox Build - Qualification* [Online].
Available: https://build.sigfox.com/study

[4] *Sigfox - Radio Configurations* [Online].
Available: https://build.sigfox.com/sigfox-radio-configurations-rc

[5] D. Armand, A. De Bock, L. Ferreira (2021, May, 10) *Risques en cybersécurité de l'IoT - Panorama des principales menaces* [Online].
Available:https://www-techniques-ingenieur-fr.gorgone.univ-toulouse.fr/base-documentaire/technologies-de-l-information-th9/cybersecurite-attaques-et-mesures-de-protection-des-si-42313210/risques-en-cybersecurite-de-l-iot-h5846/les-protocoles-radio-longue-distance-de-l-iot-sont-ils-securises-h5846niv10003.html#niv-nv192261976939

[6] C. Goursaud, C. Fourtet (2023, Feb, 10) *Technique de transmission UNB de SigFox - Principes et performances* [online]
Available:
https://www-techniques-ingenieur-fr.gorgone.univ-toulouse.fr/base-documentaire/technologies-de-l-information-th9/internet-des-objets-42612210/technique-de-transmission-unb-de-sigfox-te8016/securite-te8016niv10004.html

[7] J. Browne. (2018, Feb, 7) *Comparing Narrowband and Wideband Channels* [Online].
Available: https://www.mwrf.com/technologies/embedded/systems/article/21848973/comparing-narrowband-and-wideband-channels

[8] *rms.lu- Sigfox* [Online].
Available: https://www.rms.lu/sigfox/

[9] B. Duval. (2021, Jun, 14). *Tout savoir sur Sigfox* [Online].
Available: https://airicom.com/blog/tout-savoir-sur-sigfox/