

Wireless Sensors Network

Sigfox

Tom Lassalle
Anya Meetoo
Florent Miranville
Julie Revelli

2025 - 5 ISS INSA Toulouse
Prof. Daniela Dragomirescu

Sommaire

Introduction-----	3
1. Histoire-----	4
2. Couche physique-----	5
2.1. Introduction à la couche physique-----	5
2.2. Modulation-----	5
2.3. Fréquence radio-----	8
3. Couche MAC-----	10
3.1. Rappels-----	10
3.2. La couche MAC chez Sigfox-----	11
3.2.1. Accès au medium-----	11
3.2.2. Gestion des collisions et fiabilité-----	12
3.3. Limites-----	12
4. Consommation énergétique dans le temps-----	14
4.1. Introduction-----	14
4.2. Définitions, paramètres et procédures-----	14
4.3. Résultats et interprétations-----	16
4.3.1. Conclusion des deux expériences-----	20
4.3.2. Comparaison avec les autres technologies-----	20
5. Security-----	22
5.1. Mécanisme de contrôle d'intégrité des données-----	23
5.1.1. Vérification à la réception-----	23
5.2. Numéro de séquence associé aux trams-----	24
5.2.1. Protection mise en place par Sigfox-----	24
5.3. Principe d'authentification MAC (Message Authentication Code)-----	25
5.3.1. Génération du MAC sur un objet utilisant Sigfox-----	25
5.3.2. Vérification du MAC côté backend-----	26
5.4. Génération et l'approvisionnement des éléments d'authentification-----	26
5.5. Limitation-----	27
Conclusion-----	28
Sources-----	29

Introduction

En 2025 le secteur de l'Internet des Objets (IoT) enregistre une augmentation de 14% des dispositifs connectés, atteignant ainsi 21,1 milliards à l'échelle mondiale.

L'IoT s'impose aujourd'hui comme un pilier de la transformation numérique, permettant à une multitude d'objets capteurs, compteurs, véhicules, appareils domestiques de collecter, échanger et exploiter des données en temps réel.

Cette révolution ouvre la voie à des applications innovantes dans des domaines variés tels que la ville intelligente, la gestion énergétique, la logistique ou encore la surveillance environnementale.

Dans le cadre du cours Wireless Sensor Networks dispensé en cinquième année à l'INSA, nous nous intéressons à une technologie emblématique de cette évolution : Sigfox. Cette solution de communication repose sur un réseau à très basse consommation énergétique, conçu pour transmettre de petites quantités de données sur de longues distances.

Grâce à cette approche minimalistre et efficace, Sigfox se positionne comme une alternative économique et durable pour connecter des objets de faible puissance tout en garantissant une couverture étendue.

Dans ce rapport, nous présenterons tout d'abord le principe de fonctionnement des couches physique et MAC de Sigfox. Nous analyserons ensuite la consommation énergétique de la technologie ainsi que ses mécanismes de sécurité.

1. Histoire

Sigfox est une entreprise française fondée en 2009 à Labège, près de Toulouse, par Ludovic Le Moan et Christophe Fourtet. Conçue dès l'origine pour l'Internet des Objets (IoT), la société s'est donné pour mission de créer un réseau mondial à très faible consommation énergétique et à bas coût, indépendant des réseaux mobiles traditionnels. Ce réseau est spécialement adapté aux objets connectés qui transmettent de petites quantités de données.

Sigfox se positionne comme un opérateur de réseau « 0G », une appellation désignant une génération de réseau dédiée aux objets connectés à bas débit, par opposition aux réseaux cellulaires classiques (2G, 3G, 4G, 5G) conçus pour la communication entre humains.

Afin de soutenir son développement international, Sigfox a réalisé plusieurs levées de fonds majeures :

- Mars 2014 : environ 15 millions d'euros auprès de fonds tels qu'Idinvest Partners, Elaia Partners, Intel Capital, Ixo et Partech.
- Février 2015 : une levée record de 100 millions d'euros, alors la plus importante pour une start-up française, destinée à accélérer le déploiement à l'étranger.
- Novembre 2016 : une nouvelle levée de 150 millions d'euros, confirmant les ambitions mondiales de l'entreprise.

L'objectif de Sigfox était de construire un réseau global couvrant de nombreux pays grâce à une technologie radio optimisée pour les faibles débits et la sobriété énergétique.

Malgré son expansion rapide, Sigfox a rencontré d'importantes difficultés financières. En janvier 2022, la société a demandé l'ouverture d'une procédure de redressement judiciaire auprès du tribunal de commerce de Toulouse, invoquant un « cycle d'adoption plus lent que prévu de sa technologie malgré le soutien efficace des actionnaires ».

Le 21 avril 2022, la société singapourienne UnaBiz, cofondée par un ancien salarié de Sigfox, a été désignée repreneuse de Sigfox SA et de sa filiale française. Cette acquisition marquait alors un nouveau chapitre pour l'entreprise.

Cependant, malgré cette reprise, le 11 septembre 2025, UnaBiz SAS et UnaBiz Network SAS ont annoncé que le tribunal de commerce de Toulouse avait accordé leur demande de placement en redressement judiciaire, afin de « créer les conditions nécessaires à la restructuration de l'entreprise ».

2. Couche physique

2.1. Introduction à la couche physique

Sigfox est l'une des principales technologies LPWAN (Low Power Wide Area Network), conçue pour connecter des objets IoT sur de longues distances avec une consommation d'énergie extrêmement faible.

Sa couche physique repose sur une transmission en bande ultra-étroite (Ultra-Narrow Band, UNB), utilisant une largeur de bande très réduite et des débits de données très faibles.

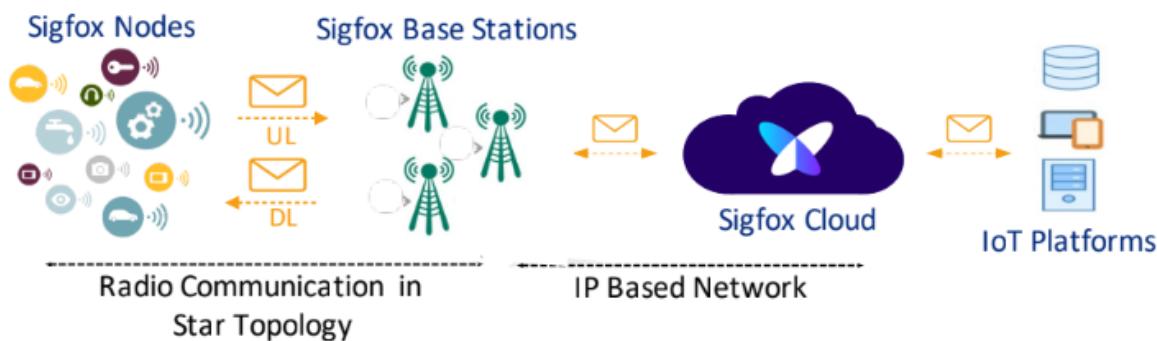


Figure 1 : Architecture de base du réseau Sigfox

2.2. Modulation

Sigfox utilise la modulation DBPSK (Differential Binary Phase Shift Keying) pour la liaison montante (uplink) et la modulation GFSK (Gaussian Frequency Shift Keying) pour la liaison descendante (downlink).

Dans la modulation DBPSK, on encode le changement de phase entre deux symboles successifs, pas la phase absolue.

- Si la phase ne change pas → bit = 0
- Si la phase change de 180° → bit = 1

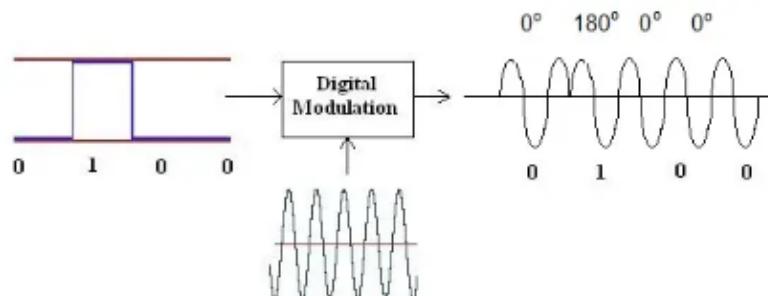


Figure 2 : DBPSK modulation

Le récepteur n'a donc pas besoin de connaître la phase absolue de l'émetteur, il se base sur la différence entre symboles successifs pour décoder les bits.

Cela rend le système plus robuste face aux erreurs de synchronisation et aux variations de phase (et donc plus simple à implémenter dans des dispositifs peu coûteux et peu puissants, comme les objets Sigfox).

Pour la liaison descendante (downlink), Sigfox emploie la modulation GFSK (Gaussian Frequency Shift Keying).

Dans ce cas, l'information est codée dans de légères variations de fréquence autour de la porteuse centrale, le signal étant filtré par une fonction gaussienne afin de réduire le spectre émis et de limiter les interférences.

Cette modulation est plus simple à détecter côté terminal et plus tolérante aux erreurs de synchronisation, ce qui la rend idéale pour les messages courts envoyés du réseau vers les objets.

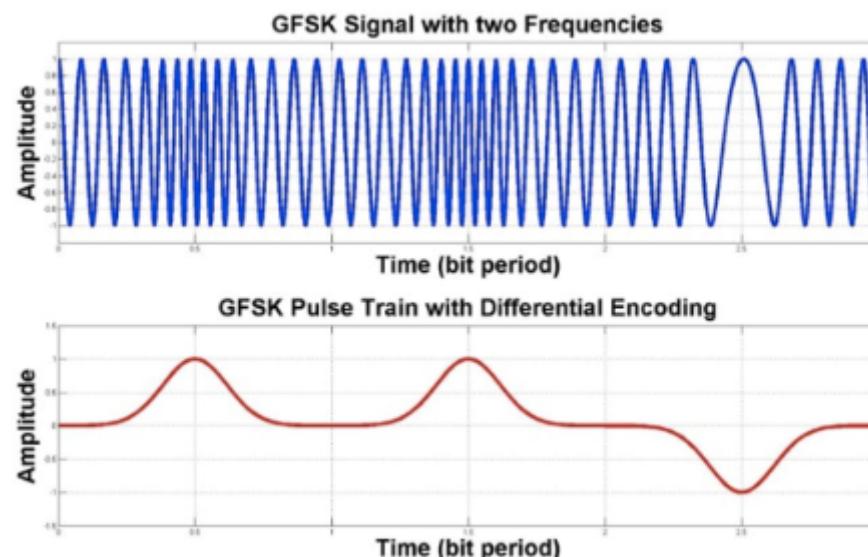


Figure 3 : GFSK modulation

La bande de base fonctionne à 100 bit/s en Europe (et jusqu'à 600 bit/s dans d'autres régions).

Chaque message contient :

- Un preamble et une séquence de synchronisation
- L'identifiant du dispositif ou un code correcteur d'erreur
- Le payload (les données utiles)
- Un code d'authentification du message (MAC)
- Une séquence de contrôle de trame (FCS)

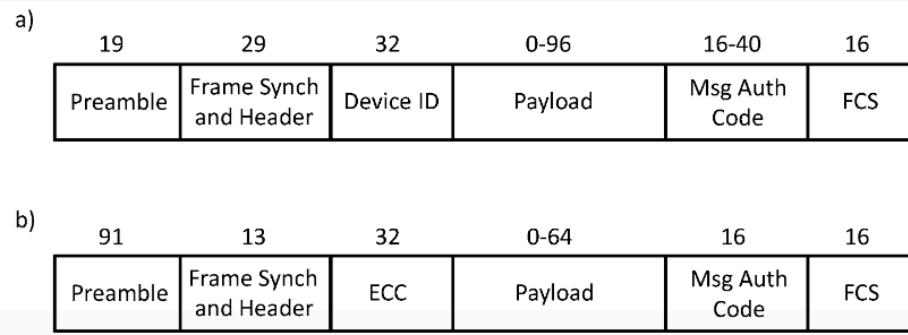


Figure 4 : Formats de trames Sigfox : (a) liaison montante et (b) liaison descendante.

Pour améliorer la fiabilité, chaque message est transmis trois fois sur des fréquences aléatoires à l'intérieur de la bande disponible.

À l'origine, Sigfox ne permettait qu'une communication unidirectionnelle, c'est-à-dire uniquement du nœud vers la passerelle (uplink). Le mécanisme de communication passerelle vers nœud (downlink), permettant un échange bidirectionnel, a été ajouté par la suite.

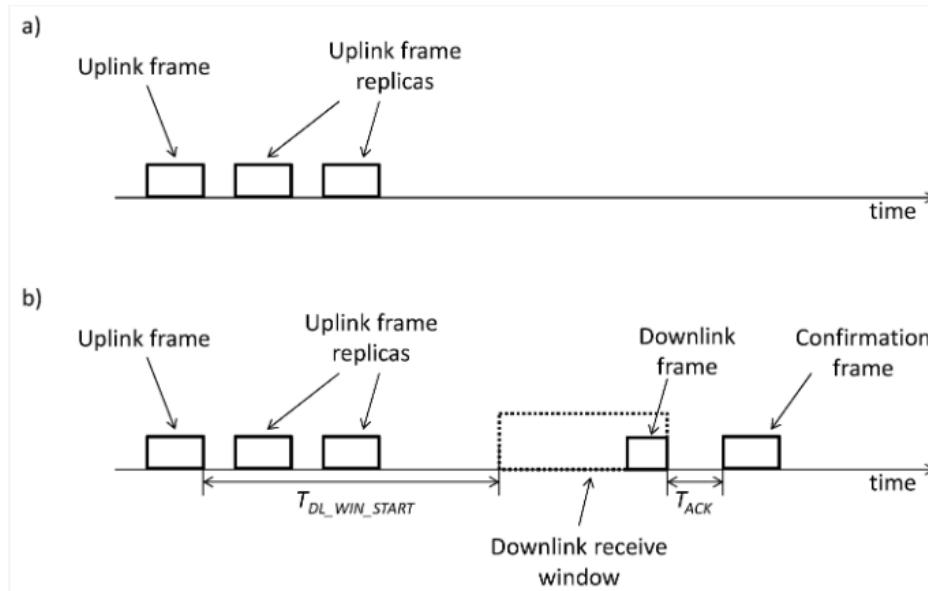


Figure 5 : (a) Unidirectional and (b) bidirectional transactions in Sigfox.

Sigfox définit deux types d'échanges de messages : les transactions unidirectionnelles et les transactions bidirectionnelles (voir Figure 3).

Dans le premier cas, le dispositif transmet une trame montante (uplink) sur un canal de fréquence choisi aléatoirement, puis envoie deux répliques identiques de cette trame sur d'autres canaux de fréquences aléatoires, à des intervalles de temps différents. Cette méthode apporte une diversité en fréquence et en temps, ce qui améliore la robustesse de la communication face à des phénomènes comme l'évanouissement multi-trajets (multipath fading) ou les interférences.

Dans les transactions bidirectionnelles, un message uplink est d'abord transmis par le dispositif selon la même procédure que pour les transactions unidirectionnelles.

Après un délai appelé TDL_WIN_START (à partir de la fin de la première trame montante), le dispositif ouvre une fenêtre de réception afin de permettre la réception d'une trame descendante (downlink) envoyée par une station de base. Cette trame descendante peut contenir des données applicatives destinées au dispositif et, en même temps, servir d'accusé de réception pour la trame montante. Après la réception du message downlink, le dispositif envoie une confirmation uplink après un temps appelé TACK.

2.3. Fréquence radio

Le front-end radiofréquence (RF) convertit le signal de bande de base en une onde radio centrée à 868 MHz (en Europe) ou 915 MHz (en Amérique).

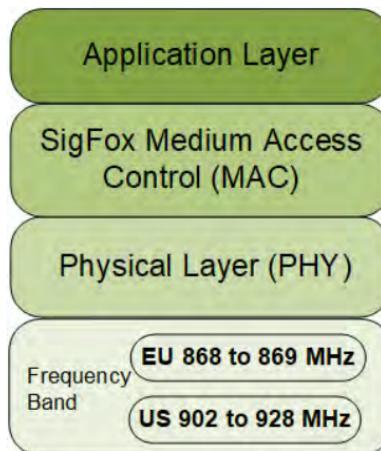


Figure 6 : Pile de communication Sigfox

Une chaîne typique d'un dispositif Sigfox se compose comme suit :

Émetteur :

Microcontrôleur → DAC / modulateur → Amplificateur de puissance (PA) → Filtre passe-bande → Antenne

Récepteur (station de base) :

Antenne → Amplificateur à faible bruit (LNA) → Filtre → Mélangeur / Convertisseur analogique-numérique (ADC) → Démodulateur

Ces fréquences offrent un excellent compromis entre :

- une portée étendue (perte de trajet plus faible qu'à 2,4 GHz),
- une taille d'antenne modérée (environ 8 cm pour un quart d'onde),
- une bonne pénétration à travers les murs.

	Sigfox	
	UL	DL
Spectrum [MHz]	868.1-868.3	869.425-869.625
Tx power [dBm]	14	27
Modulation	DBPSK	GFSK
Bandwidth [kHz]	0.1	0.6
Max payload [bytes]	12	8
Scheduling	Uplink initiated	
MCL [dB]	158	161

Figure 7 : Vue d'ensemble de la technologie

Chaque trame montante (uplink) occupe environ 100 Hz de spectre. L'ensemble de la bande Sigfox en Europe s'étend sur environ 192 kHz (de 868,130 MHz à 868,320 MHz). À l'intérieur de cette plage, le système définit environ 1 920 sous-canaux virtuels de 100 Hz chacun. Les dispositifs choisissent aléatoirement une fréquence pour chaque transmission, ce qui assure une diversité fréquentielle, augmentant la robustesse face aux interférences.

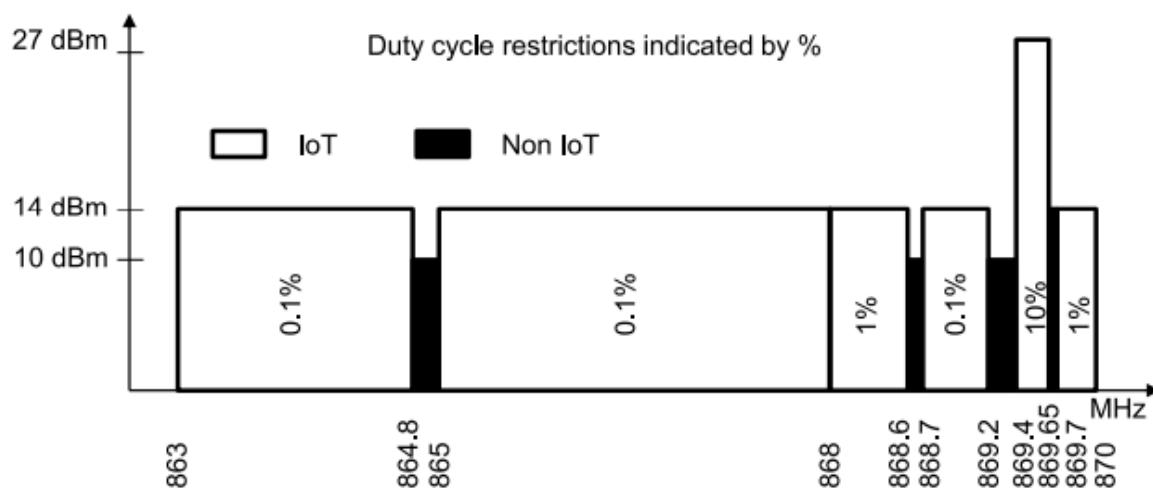
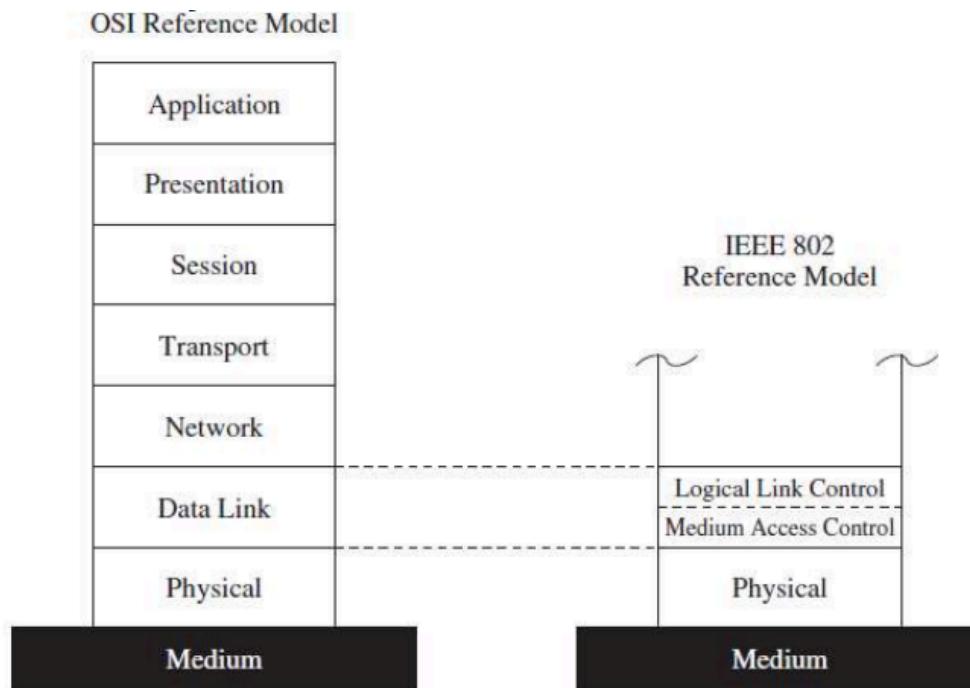


Figure 8 : Bande ISM européenne à 868 MHz — puissance et limitations du cycle d'émission

La technologie Sigfox est soumise à un duty cycle (cycle d'émission) dont les restrictions varient entre 0,1 % et 10 % selon la bande de fréquence et les réglementations régionales. En Europe, la puissance d'émission est limitée à 14 dBm, et la limitation du duty cycle pour la sous-bande utilisée dans la bande ISM 868 MHz est de 1 %. Cela signifie qu'un dispositif final ne peut émettre que 36 secondes par heure et par canal. Sigfox respecte strictement cette contrainte, ce qui explique la brièveté et la faible fréquence de ses messages.

3. Couche MAC

Dans un réseau sans-fil, les nœuds échangent leurs données en empruntant un même support de transmission, plus communément appelé médium de communication. Afin d'éviter le plus possible les interférences, il est essentiel de définir plusieurs règles pour organiser l'accès au canal de transmission. La couche MAC intervient donc à cette éffigie, il s'agit d'une sous-couche de la couche liaison de données dans le modèle OSI.



The MAC layer in the IEEE 802 reference model.

Figure 1. La couche MAC dans deux modèles de protocoles

3.1. Rappels

Tout d'abord, rappelons quelques fonctions principales de la couche MAC. Elle agit comme une interface entre la couche physique et permet aux couches supérieures d'avoir un moyen simple d'envoyer et de recevoir des trames de données, en cachant la complexité matérielle (signaux électriques ou radios) de la couche physique. La couche MAC gère également l'accès multiple au médium de communication, lorsque plusieurs appareils veulent transmettre au même moment, et décide donc quand un nœud a le droit de transmettre, et par quelle méthode d'accès (ex. CSMA, TDMA, ALOHA). Elle gère ainsi les collisions et permet la retransmission des données s'il y en a.

Toujours dans l'optique de la gestion des collisions, les protocoles MAC peuvent appartenir à deux catégories de protocoles, à savoir "contention-free" ou "contention-based".

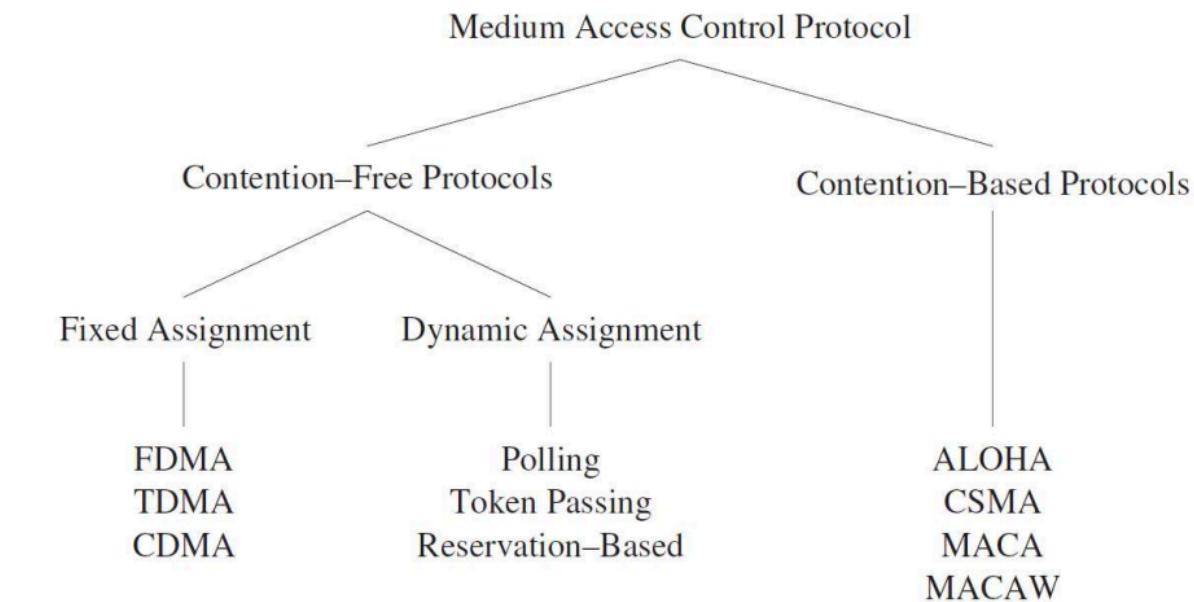


Figure 2. Les modes de contention de la couche MAC

Les protocoles MAC de la catégorie contention-free vont gérer l'accès au médium de communication de sorte à ce qu'un seul appareil y accède à un instant donné t , pouvant être fixe ou dynamiquement assigné.

La catégorie contention-based au contraire va permettre à tous les appareils d'accéder au médium simultanément, en offrant des mécanismes pour réduire les collisions, comme par exemple l'attente d'une durée aléatoire avant le renvoi des données après une collision.

3.2. La couche MAC chez Sigfox

Comme ses sœurs LoRa et NB-IoT, Sigfox est une technologie sans-fil dite LPWAN (Low Power Wide Area Network) développée pour répondre à l'essor imminent des objets connectés. Comme son nom l'indique, ce type de technologie doit répondre aux contraintes de portée et de consommation réduite pour assurer une bonne autonomie. Sigfox se situe dans la bande ISM à 868 MHz en Europe, et sa couche MAC a été modifiée pour atteindre ces objectifs d'efficacité énergétique et de longue portée.

3.2.1. Accès au medium

La couche MAC de Sigfox s'appuie sur le protocole RFTDMA (Random Frequency and Time Division Multiple Access), basé sur le modèle du protocole ALOHA pur. Cela signifie que n'importe quel appareil peut accéder au médium de communication à tout moment. L'accès au médium a donc été simplifié, car les appareils n'ont pas besoin de vérifier si le canal est libre avant d'émettre. La consommation énergétique est donc réduite malgré le risque plus élevé de collisions.

3.2.2. Gestion des collisions et fiabilité

Sigfox s'appuie sur une diversité fréquentielle, temporelle et spatiale. Chaque message émis par un appareil Sigfox est envoyé trois fois, et est soumis au "frequency hopping" dans une bande passante opérationnelle B définie dans un intervalle continu (de 868,130 MHz à 868,320 MHz). En effet, lors de la transmission, les données sont envoyées dans des canaux aléatoires avec des fréquences porteuses comprises dans B sur une portée pouvant aller jusqu'à 1 920 sous-canaux virtuels de bande de fréquence $W = 100$ Hz. En rappelant que Sigfox utilise la modulation DBPSK pour une liaison uplink avec un débit $R = 100$ bit/s, l'expression du signal transmis r_s est :

$$r_s^{ns}(t) = \sum_{k \in \mathcal{S}_s} A_k g(t - kT_s) e^{j2\pi f_p t}$$

Avec :

- $T_s = \frac{1}{R}$ la période d'un symbole
- A_k qui est le symbole DBPSK transmis à un instant kT_s
- $f_p \in \left\{ \frac{B}{2} \right\}$ la fréquence porteuse utilisée pour la transmission de la donnée
- \mathcal{S}_s est l'ensemble des symboles de la trame transmise et dépend donc de la structure de la trame
- $g(t)$ est le filtre de mise en forme d'impulsion du signal à bande passante W

Chaque trame peut être reçue par 3 stations de base différentes donc si une copie est perdue, elle a de grande chance d'être récupérée par une autre station de base. Sigfox s'appuie donc sur la redondance des envois de données et le frequency hopping afin d'augmenter la probabilité de réception correcte des données. Avec ce modèle d'envoi, le récepteur doit décoder la totalité des signaux reçus sur la bande passante B pour identifier le message émis, surtout si le démodulateur écoute la totalité de la bande passante B sans connaître la fréquence porteuse utilisée par l'émetteur.

3.3. Limites

Bien que le protocole RFTDMA cherche à favoriser une fiabilité de la réception correcte des données et une réduction de la consommation d'énergie, le fait que l'accès au médium de communication soit sans vérification et le nombre important de transmissions crée des collisions sur les nœuds actifs.

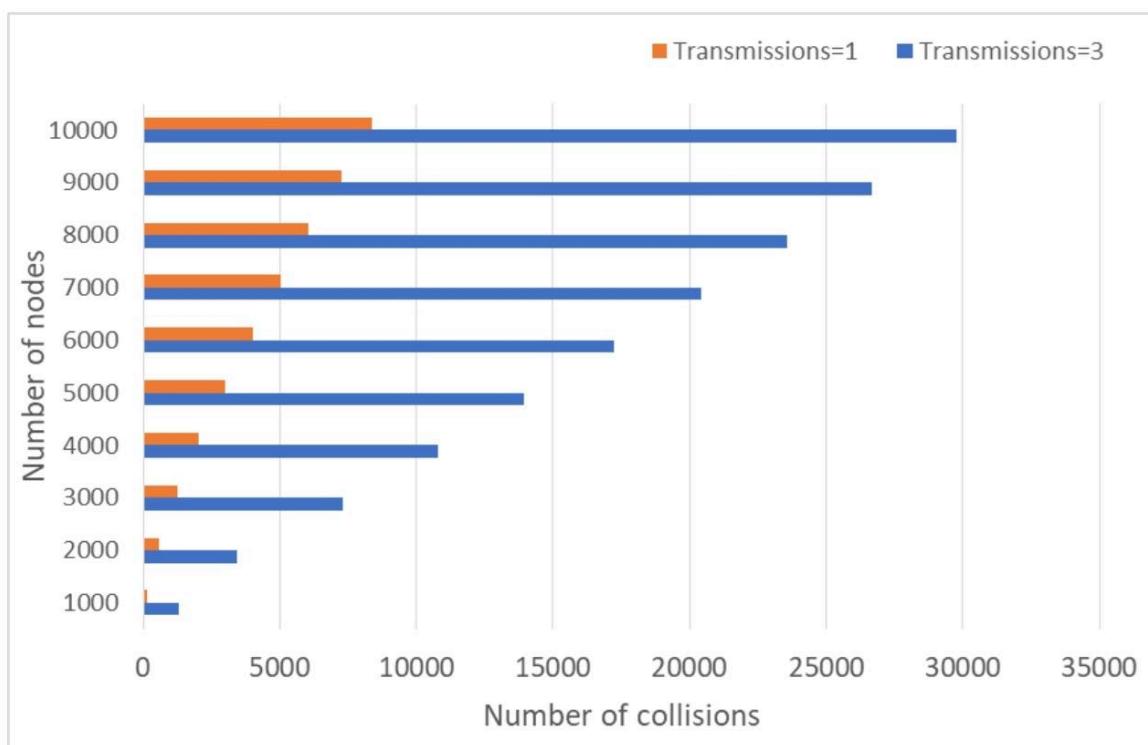


Figure 3. Nombres de collisions quand le nombre de noeuds augmente de 1000 à 10000 en fonction du nombre de transmission

Le nombre de collision augmente drastiquement lorsque la redondance est activée avec un grand nombre de noeuds actifs, on atteint les 29000 collisions avec 10000 noeuds alors qu'on en a que 8500 environ avec une seule transmission. Une solution pourrait être d'ajuster le nombre de transmissions en fonction du nombre de noeuds concernés. Avec ces paramètres, Sigfox permet une portée d'envoi de données allant de 50 à 100 km, pour une gestion d'environ 1 million d'appareils par station de base. Ces informations restent valides tant que Sigfox ne partage pas sa bande passante B avec une autre technologie LPWAN, et la coexistence avec le réseau LoRa sur la bande ISM à 868MHz contrecarre cette gestion d'un important nombre d'appareils.

4. Consommation énergétique dans le temps

4.1. Introduction

Dans le domaine de l'Internet des Objets (IoT) ou des petits objets connectés, la question de la consommation énergétique dans le temps revient constamment, car ces dispositifs sont souvent limités en termes de source d'énergie. Cela renforce l'importance d'étudier cette consommation et de chercher à l'optimiser.

De nos jours, Sigfox est devenu l'une des principales technologies Low-Power Wide Area Network (LPWAN), adaptée aux besoins des IoT en matière de faible consommation d'énergie.

Dans cette partie, nous aborderons la définition de la consommation énergétique dans le temps, les paramètres à considérer, les méthodes de mesure, ainsi que les différents scénarios pouvant influencer les résultats. Nous terminerons par une comparaison avec les autres technologies.

4.2. Définitions, paramètres et procédures

Cette section sert à expliquer les diverses mesures de calculs qui suivront dans l'analyse de la consommation énergétique dans le temps.

Qu'est-ce que c'est la consommation énergétique dans le temps ?

La consommation énergétique dans le temps correspond simplement à la quantité d'énergie utilisée par un objet pendant un lapse de temps donné. Elle permet de comprendre comment et quand l'énergie est dépensée, et d'identifier les phases où elle peut être optimisée.

Rappel, la consommation énergétique est le calcul de la puissance dans le temps qui se définit généralement par des kWh.

Ce calcul dépend de plusieurs mesures physiques. Dans ce contexte, la consommation énergétique repose sur les notions :

- d'une période de temps T_{Period}
- une tension constante V
- du courant moyen sur un temps donné

[Article [1] - Eq 1 : Courant moyen consommé par l'objet en communication unidirectionnel en considérant les différents scénarios]

$$I_{avg_uni} = \frac{1}{T_{Period}} \sum_{i=1}^{N_{states_uni}} n_i \cdot T_i \cdot I_i$$

Nous pouvons donc identifier une formule qui regroupe le tout, pour exprimer la consommation énergétique dans le temps

$$E_{period} = V \times I_{avg, uni} \times T_{period}$$

Qu'est-ce que c'est l'énergie par bit ?

L'énergie par bit est l'indicateur de combien coûte la transmission d'une donnée d'un bit ou plus précisément, l'énergie en Joules consommée pour transmettre un bit de donnée depuis l'objet au cloud de service.

Dans l'article *A Sigfox Energy Consumption Model*, cela est formalisé par deux équations:

[Article [1] - Eq 6 : Energie consommée par l'objet par bit de donnée transmis dans un système de communication unidirectionnel]

$$EC_{delivery_uni} = \frac{I_{avg_uni} \cdot V \cdot T_{Period}}{E[l_{delivery}]}$$

[Article [1] - Eq 6 : Energie consommée par l'objet par bit de donnée transmis dans un système de communication bidirectionnel]

$$EC_{delivery_bi} = \frac{I_{avg_bi} \cdot V \cdot T_{Period}}{E[l_{delivery}]}$$

Ici, l'énergie par bit est calculé grâce à la mesure d'un courant moyen I_{avg} , avec une tension fixe V , pour une période donnée T_{period} en fonction d'une quantité de données attendue $E[l_{delivery}]$ qui peut être calculée grâce à la Frame Loss Rate et la fram payload size. Pour bien différencier nos calculs à ce dernier, la formule de la quantité de données attendue est définie et bien expliquée dans l'article 1 à la page 20.

Procédure de mesure

Après avoir compris les différents calculs à faire pour trouver la consommation énergétique totale et l'énergie par bit de Sigfox, il est possible de suivre la procédure logique suivante :

1. Il faut configurer le module Sigfox - configuration de l'alimentation en à 3,3V à 5V et choisir une donnée de taille fixe pour l'instant. L'alimentation peut se faire soit en continue soit par batterie.
2. Mesurer la tension et le courant pendant que le système est en veille (avant transmission / mode READY) pendant un lapse de temps
3. Transmission d'une donnée
4. Faire les mesures en même temps - il faut prendre en considération le temps de transmission, le courant instantané, et voltage
5. Faire le calcul de l'énergie consommée en utilisant les valeurs relevées, note que pour le voltage, il est possible de supposer que cela reste constant mais si nous voulons de la précision, il faut mesurer le voltage instantané.
6. Noter le nombre de bits transmis = taille du message + l' overhead du protocol
7. Faire le calcul de l'énergie par bit
8. Répéter les étapes 4 à 7 en configurant les différents paramètres (tension en entrée, taille de donnée, environnement de test, modules Sigfox, antennes)
9. (complémentaire) mesurer la température ambiante
10. Faire des graphiques qui résume bien les mesures pour les différents paramètres

4.3. Résultats et interprétations

Pour bien comprendre l'impact de la consommation de courant sur la consommation d'énergie dans le temps, nous nous appuyons sur deux articles [1] [2], qui effectuent deux expériences dans des environnements contrôlés.

Première expérience : un système alimenté par un power analyser à 3V

Le premier [1] consiste d'un système Arduino MKRFOX1200. Un extrait de l'article précise ci-dessous les paramètres mis en place avant l'expérience.

"The voltage supplied by the power analyzer is 3 V. The transmit power of the device is 14.5 dBm. The uplink bit rate supported by the device is 100 bit/s. The device is located in an indoor scenario, and makes use of the network coverage provided by Sigfox in the Barcelona area. A 16-bit Msg Auth Code field is used in uplink frames. "

[Article [1] - Fig 4 Schéma du branchement et disposition des équipements]

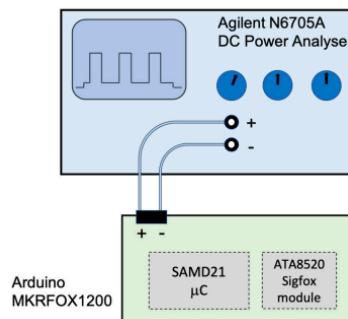


Figure 4. Experimental setup for the current consumption characterization of the MKRFOX1200 Sigfox module (on the left) using an Agilent N6705A power analyzer.

[Article [1] - Table 2 Résultats expériences en unidirectionnel]

Table 2. States, variables and measurement results for Sigfox unidirectional transactions. For a bit rate of 100 bit/s, T_{tx} can take values between 1200 ms (1-byte payload) and 2080 ms (12-byte payload). T_{sleep_uni} ranges in this study from 0 up to $\sim T_{Period}$ (T_{sleep_uni} tends to T_{Period} for very high T_{Period} values).

State Number	Description	Duration		Current Consumption	
		Variable	Value (ms)	Variable	Value (mA)
1	Wake up	T_{wu}	287	I_{wu}	10.4
2	Transmission	T_{tx}	[1200,2080] (4)	I_{tx}	27.2
3	Wait next transmission	T_{wntx}	486	I_{wntx}	1.2
4	Cool down	T_{cd}	510	I_{cd}	1.2
5	Sleep	T_{sleep_uni}	[0, T_{Period}] (2)	I_{sleep}	16×10^{-3}

[Article [1] - Table 3 Résultats expériences en bidirectionnel]

Table 3. States, variables and their values for Sigfox bidirectional transaction. For a bit rate of 100 bit/s, T_{tx} can take values between 1200 ms (1-byte payload) and 2080 ms (12-byte payload). The reception duration ranges from 387 ms up to $T_{DL_WIN_MAX} = 25$ s (in US and EU regions), with an average of $T_{rx} = 12.69$ s. T_{sleep_bi} ranges in this study from 0 up to $\sim T_{Period}$ (T_{sleep_bi} tends to T_{Period} for very high T_{Period} values).

State Number	Description	Duration		Current Consumption	
		Variable	Value (ms)	Variable	Value (mA)
1	Wake up	T_{wu}	305	I_{wu}	10.7
2	Transmission	T_{tx}	[1200,2080] (4)	I_{tx}	27.6
3	Wait next transmission	T_{wntx}	493	I_{wntx}	1.2
4	Wait next reception	T_{wnrx}	16493	I_{wnrx}	1.3
5	Reception	T_{rx}	12690 (11)	I_{rx}	18.5
6	Wait confirm. transmission	T_{wctrl}	1430	I_{wctrl}	1.2
7	Confirmation transmission	T_{ctrl_tx}	1850	I_{ctrl_tx}	27.0
8	Cool down	T_{cd}	495	I_{cd}	1.2
9	Sleep	T_{sleep_bi}	[0, T_{Period}] (9)	I_{sleep}	16×10^{-3}

Pour la première expérience, nous pouvons reconnaître 5 scénarios communs (wake up, transmission, wait next transmission, cool down et sleep) et 4 autres supplémentaires pour le bidirectionnel. Si nous faisons une comparaison en termes de valeurs, à des durées mesurées très proches, nous avons presque les mêmes valeurs en mesure de courant consommé pour les 5 scénarios communs. Logiquement, le bidirectionnel consomme beaucoup plus que l'unidirectionnel car il passe par plusieurs autres scénarios pour une transmission.

Après plusieurs expériences, nous pouvons faire une moyenne des scénarios et obtenir ces différentes courbes ci-dessous,

[Article [1] - Figure 7 Résultats moyens des expériences en bidirectionnel et unidirectionnel en fonction de la période de transaction]

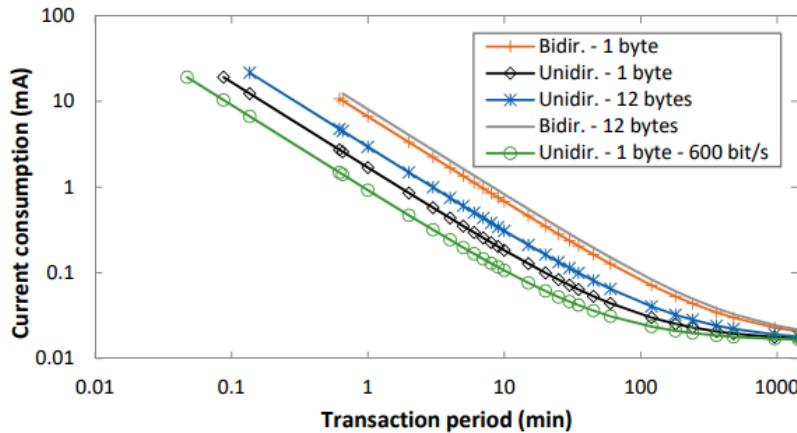


Figure 7. Average current consumption of the device, for unidirectional and bidirectional transactions, as a function of T_{Period} , for FLR = 0, and for uplink payload sizes of 1 byte and 12 bytes.

Les résultats montrent que la consommation diminue quand la période de transmission entre deux messages augmente, car l'objet passe plus de temps en veille.

La communication unidirectionnelle consomme beaucoup moins de courant que la communication bidirectionnelle pour les périodes courtes. Par exemple, pour une période de 10 minutes et un message de 1 byte, le courant moyen est de 0,18 mA pour l'unidirectionnel et 0,68 mA pour le bidirectionnel.

La taille du message a un impact plus critique sur la communication unidirectionnelle, tandis que l'augmentation du débit de transmission à 600 bit/s réduit la consommation pour les périodes courtes en unidirectionnel, car le temps de transmission est plus court. Pour la communication bidirectionnelle, cela ne change pas grand chose. Pour toutes les communications, l'impact diminue quand la période augmente.

Deuxième expérience : un système alimenté par une batterie de 4,5V

La deuxième [2] consiste d'un système Raspberry Pi 5, Otti Ace Pro et HT32SX. Ici, les chercheurs ont décidé d'utiliser une **batterie de 4,5V à capacité 3Ah**. Ce système est très intéressant car ils peuvent simuler une utilisation des modules LPWAN dans des cas plus typiques qui utilisent des piles pour fonctionner.

[Article [2] - Fig 1 Schéma du branchement et disposition des équipements]

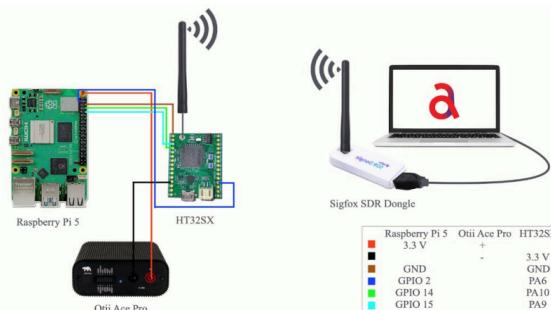


Fig. 1. Experimental setup of the devices while measuring the uplink, downlink, delay, RTT, sleep time periods and the transmission power.

Les Figures 7 et 8 montrent la consommation énergétique du module Sigfox en fonction de deux paramètres critiques : la puissance de transmission (Fig. 7) et la taille des messages (Fig. 8).

[Article [2] - Fig 7 Consommation du courant en fonction de la puissance de transmission]

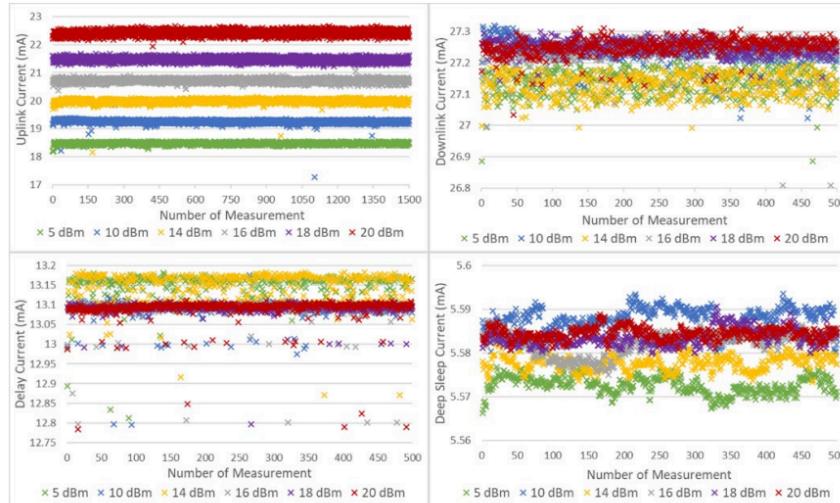


Fig. 7. The relationship between uplink/downlink, delay, RTT, sleep and deep sleep current and the transmission power in Sigfox.

La Figure 7 démontre une relation entre la puissance de transmission (de 5 à 20 dBm) et la consommation en uplink, downlink, delay et deep sleep. Pour le uplink, cette relation est linéaire et chaque augmentation de puissance fait monter le courant, ce qui est prévisible. Cela montre que des puissances élevées réduisent l'autonomie. Cependant, la consommation en downlink reste stable (26,79–27,32 mA) et reste supérieure à celle de l'uplink même à puissance maximale. Les phases de délai et de deep sleep présentent une consommation constante et minimale. Pour le deep sleep, nous sommes à < 5,58 mA, ce qui est nécessaire pour prolonger la durée de vie de la batterie.

[Article [2] - Fig 8 Consommation du courant en fonction de la taille des messages]

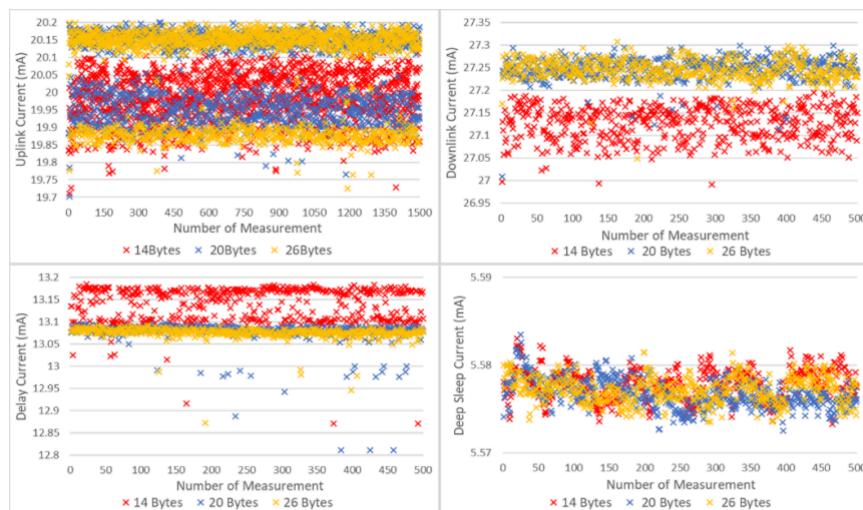


Fig. 8. The relationship between uplink/downlink, delay, RTT, sleep and deep sleep current and the message size in Sigfox.

La Figure 8 montre que la taille des messages (14, 20, 26 octets) influence un peu la consommation. Ce qui veut dire que les messages plus longs allongent légèrement le temps de transmission en uplink, mais le courant reste presque pareil. Comme pour la Figure 7, le downlink reste la phase la plus consommatrice en énergie, tandis que le deep sleep conserve une consommation stable et très faible peu importe la taille des messages.

4.3.1. Conclusion des deux expériences

Nous pouvons en déduire que la technologie Sigfox dépend autant bien de son mode de communication (uni ou bi-directionnel), de la puissance de transmission et de la taille des messages.

La consommation du module Sigfox baisse quand le délai entre deux transmissions augmente, car il passe plus de temps en deep sleep. La communication unidirectionnelle est aussi beaucoup moins gourmande que la bidirectionnelle, surtout pour des délais courts. Les messages plus gros consomment plus d'énergie, mais augmenter le débit à 600 bit/s réduit cette consommation en raccourcissant le temps de transmission, selon le type de communication.

La plus grande différence entre les deux expériences est l'alimentation. Dans la première expérience, une tension constante de 3V est délivrée au système. Dans cet environnement contrôlé, le but est d'effectuer les calculs autour de ce système pour se rapprocher des modèles théoriques et ne pas tenir en compte des conditions réelles d'utilisation. D'après ce système, un module Sigfox peut avoir une durée de vie allant jusqu'à 14,6 ans pour des périodes de transaction très espacées.

En comparaison, la deuxième expérience consiste de l'utilisation d'une batterie à 4,5V. Ce système dépend donc d'un environnement peu contrôlé qui diffère à cause des pertes supplémentaires (auto-décharge, résistance interne, effets de température). Bien que Sigfox consomme peu d'énergie pendant les phases actives, sa consommation en veille profonde reste élevée, limitant la durée de vie de la batterie à environ 2 à 4 ans pour une batterie de 3 Ah, selon le débit (100 ou 600 bit/s). La différence entre les deux expériences est flagrante et importante. Il faut bien choisir les conditions d'expérience pour avoir des résultats réels et pertinents.

Cependant, globalement parlant, il est donc recommandé de réduire la puissance de transmission, avoir des messages plus courts, espacer les transmissions et avoir une communication unidirectionnel pour réduire la consommation énergétique dans le temps avec Sigfox.

Il manque beaucoup de recherches sur la consommation énergétique des composants Sigfox, souvent avec une batterie différente et des expériences dans des environnements non-contrôlés.

4.3.2. Comparaison avec les autres technologies

[Article [2] - Fig 20 Graphiques comparatifs de la consommation de courant de Sigfox et autres technologies en transmission de données]

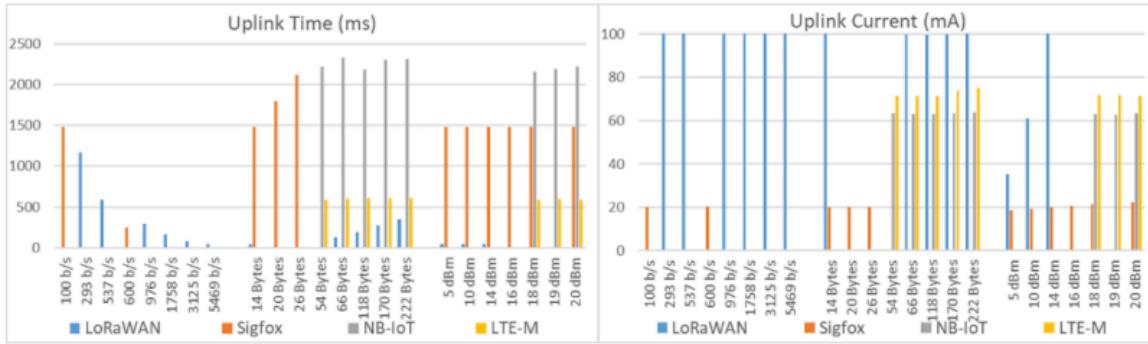


Fig. 20 Comparison between LoRaWAN, Sigfox, NB-IoT and LTE-M in the Uplink period in terms of duration and current consumption.

D'après ce graphique ci-dessus qui compare Sigfox, NB-IoT, LTE-M et LoRaWAN en uplink. LoRaWAN consomme beaucoup de courant (~100 mA) mais reste le plus économique grâce à sa transmission rapide jusqu'à 5469 bit/s. A l'opposé, Sigfox a un faible courant (~20 mA) mais son efficacité est limitée par ses transmissions répétées et son faible débit (100–600 bit/s). NB-IoT et LTE-M consomment plus. Sigfox n'est toujours pas à la hauteur de LoRaWAN en termes de balance de maximisation d'autonomie des dispositifs IoT.

5. Security

Dans le contexte de l'Internet des Objets (IoT), la fiabilité et la sécurité des échanges de données sont des enjeux majeurs. Par conséquent le protocole Sigfox impose la mise en œuvre de mécanismes spécifiques afin d'assurer l'intégrité, l'authenticité et la protection des messages échangés. Ainsi, plusieurs dispositifs sont intégrés au protocole pour garantir la sécurité des communications.

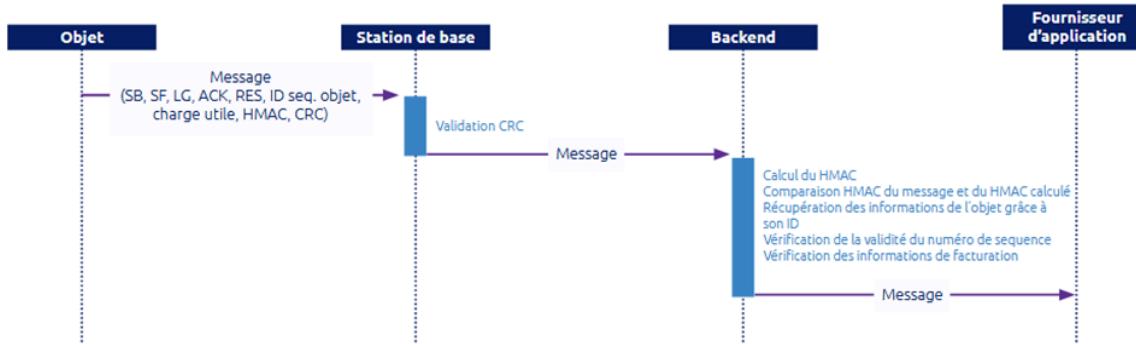


Figure 1 : Architecture Sigfox (4)

Ces mécanismes, bien que complémentaires, présentent certaines limites. L'étude de ces dispositifs permet de mieux comprendre les choix techniques opérés par Sigfox en matière de sécurité, ainsi que les vulnérabilités potentielles inhérentes à ce type de réseau IoT. En effet, Sigfox étant un système low power conçu pour minimiser la consommation énergétique des objets connectés, l'intégration de mécanismes de chiffrement et de sécurité avancés implique un coût supplémentaire, tant en calcul qu'en énergie. Ces contraintes expliquent en partie les compromis réalisés entre niveau de sécurité, simplicité de traitement et autonomie énergétique des dispositifs Sigfox.

Dans la suite de cette sous-partie, nous nous baserons sur les trames utilisées par Sigfox. Vous trouverez ci-dessous un récapitulatif de la composition des différents éléments de la trame, qui seront détaillés au cours de cette partie.

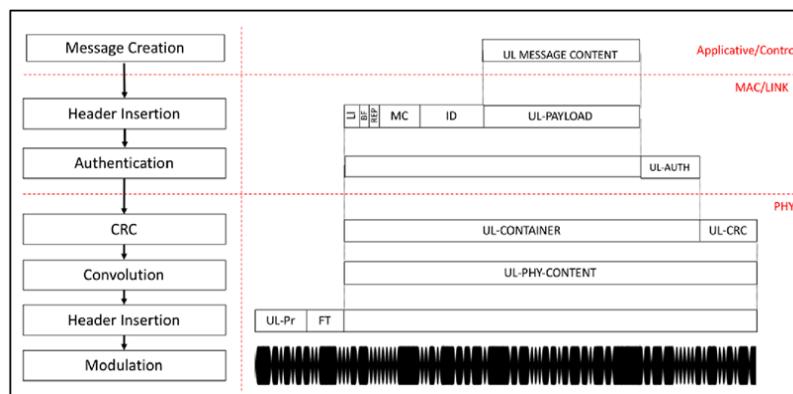


Figure 2 : Trame Sigfox (2)

5.1. Mécanisme de contrôle d'intégrité des données

Sigfox utilise un mécanisme permettant de vérifier que le message reçu n'a pas été altéré pendant sa transmission radio. Ce mécanisme s'appelle CRC (Cyclic Redundancy Check, ou contrôle de redondance cyclique).

Dans le cas de Sigfox, il s'agit d'un CRC 16 bits, inséré dans le champ UL-CRC de la trame. Le CRC est calculé à partir de l'UL-CONTAINER, c'est-à-dire l'entête et la charge utile du message.

Pour effectuer ce calcul, toutes les données sont traitées en binaire, puis divisées par le polynôme générateur suivant :

$$X^{16} + X^{12} + X^5 + 1$$

Ce polynôme correspond au binaire :

1 0001 0000 0010 0001

Le reste de cette division constitue le CRC. Ensuite, un XOR avec 0xFFFF est appliqué pour inverser les bits, donnant ainsi le UL-CRC final, qui est ajouté à la fin de la trame avant son envoi vers une station de base Sigfox.

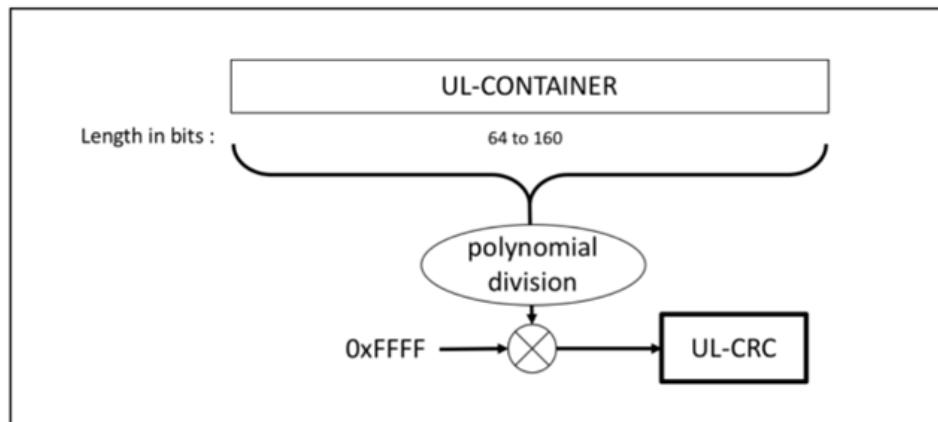


Figure 3 : Calcul CRC (2)

5.1.1. Vérification à la réception

Lorsque la trame est reçue par la station de base Sigfox, celle-ci recalcule le CRC sur les données reçues avant de les transmettre au backend.

- Si le CRC recalculé correspond au CRC reçu : aucune erreur n'a été détectée.
- Si le CRC recalculé ne correspond pas : une erreur d'intégrité est détectée.

Le CRC ne protège pas contre les attaques malveillantes ; il sert uniquement à détecter les erreurs accidentelles survenues pendant la transmission (par exemple, des bits modifiés à cause du bruit ou d'interférences). Il est efficace pour détecter des erreurs aléatoires, mais il ne protège pas contre un attaquant capable de calculer correctement le CRC.

5.2. Numéro de séquence associé aux trams

Le numéro de séquence est un mécanisme utilisé par Sigfox afin d'éviter les potentielles attaques par rejet (replay attacks).

Une attaque par rejet (1) est un type d'attaque dite « *Man in the Middle* » consistant à intercepter un message valide envoyé par un objet connecté, puis à le renvoyer ultérieurement (ou plusieurs fois) sans y apporter de modification.

Étant donné que le message est authentique, il peut aisément passer les systèmes de vérification et ainsi tromper le serveur.

Exemple concret : Imaginons un capteur IoT Sigfox utilisé pour détecter si la porte d'un garage est ouverte ou fermée. Un pirate peut, à l'aide d'un récepteur radio, écouter et enregistrer le message envoyé par le capteur. Il pourra ensuite le rejouer. Si le système n'est pas protégé, le pirate peut induire le système en erreur concernant l'état réel de la porte du garage.

5.2.1. Protection mise en place par Sigfox

Pour se prémunir contre ce type d'attaque, Sigfox a mis en place un compteur de messages inclus dans chaque trame Sigfox, appelé Message Counter (MC), codé sur 12 bits (2).

Le numéro de séquence reçu doit se situer dans une plage de valeurs calculée entre :

$$[\text{dernier numéro enregistré} + \text{Min}] \quad [\text{dernier numéro enregistré} + \text{Max}]$$

La plage est calculée comme suit (3) :

$$\text{Max} = \text{jours} * 300$$

$$\text{Min} = \text{contrat} * (\text{jours} + 2)$$

Où :

Jour : le nombre de jours écoulés entre deux messages ; le même jour (période glissante de 24 heures) comptera pour 1.

Contrat : nombre maximal de messages montants quotidiens autorisés par le contrat utilisé.

Le numéro de séquence est vérifié par le Sigfox Support System, au niveau du backend Sigfox, afin de détecter les tentatives de reproductions ou de rejet d'un message.

5.3. Principe d'authentification MAC (Message Authentication Code)

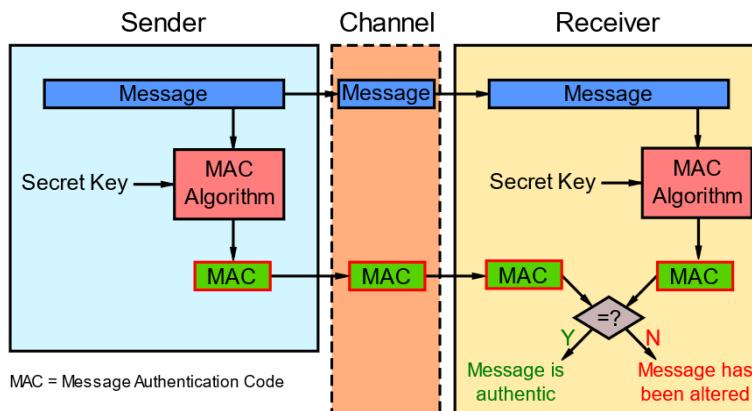


Figure 4 : Schéma de principe d'un code d'authentification de message (MAC)

L'authentification d'un message par MAC (Message Authentication Code) permet de vérifier l'origine et l'intégrité du message. Ce mécanisme repose sur des techniques cryptographiques qui garantissent la légitimité des données reçues. Le MAC assure ainsi que le message provient bien de l'émetteur légitime et qu'il n'a pas été altéré, falsifié ou généré par un utilisateur malveillant.

Chaque objet utilisant Sigfox possède :

- Un identifiant (ID) unique codé sur 4 octets ;
- Une clé NAK (Network Authentication Key) ou Secret Key utilisant AES-128 ;

5.3.1. Génération du MAC sur un objet utilisant Sigfox

Pour générer le MAC, l'objet utilise la charge utile (payload) à laquelle est ajouté un en-tête composé des champs suivants :

- Length Indicator (LI) : 2 bits, défini en fonction de la longueur de la charge utile ;
- Bidirectional Flag (BF) : 1 bit, indiquant le type de procédure (uplink/downlink) ;
- Repeated Flag (REP) : 1 bit, indiquant si le message est une répétition ;
- Message Counter (MC) : 12 bits, compteur de messages ;
- Identifier (ID) : 32 bits, identifiant unique de l'objet.

Le MAC est ensuite calculé à partir de la concaténation de la charge utile et de l'en-tête, en utilisant la clé NAK avec un chiffrement AES-128 qui est un algorithme de chiffrement symétrique qui transforme des données claires en données chiffrées à partir d'une clé 128 bits :

$$MAC = AES_128(NAK, LI \& BF \& REP \& REP \& MC \& ID \& Payload)$$

où ‘&’ représente la concaténation des champs.

5.3.2. Vérification du MAC côté backend

À la réception d'une trame, le backend Sigfox :

1. Récupère le Device ID et recherche la clé NAK (Secret Key) correspondante dans sa base
2. Recalcule le MAC à partir de l'en-tête et de la charge utile, en utilisant la NAK récupérée
3. Compare le MAC recalculé avec celui transmis par l'objet : Compare le MAC recalculé avec celui transmis par l'objet :
 - Si les deux correspondent le message est authentique et intact ;
 - Sinon le message est rejeté ;

Ainsi, la vérification par MAC permet :

- L'intégrité : le message n'a pas été modifié pendant la transmission ;
- L'authentification de l'expéditeur : le message provient bien de l'objet légitime.

5.4. Génération et l'approvisionnement des éléments d'authentification

La génération des clés et des identifiants (ID et NAK) pour un objet ne peut être effectuée que par un fabricant disposant de la certification requise par Sigfox (4).

La procédure est la suivante (4) :

1. Demande d'ID et de NAK auprès de Sigfox

Le fabricant envoie une requête à Sigfox pour obtenir un lot d'ID et de NAK, en fournissant son certificat de conformité.

2. Attribution d'une plage d'ID d'objets

Une fois la demande validée, Sigfox assigne une plage d'ID correspondant au nombre d'objets que le fabricant prévoit de produire. Lancement de la génération par le CRA

3. Génération des clés par le CRA

Le Central Registration Authority (CRA) est l'entité centrale qui gère l'authentification des objets sur le réseau Sigfox. Produit la clé d'authentification réseau (NAK) pour chaque objet associé à l'ID de chaque objets. Ainsi que le Porting Authorization Code (PAC). Ce code sera utilisé lors de l'activation de l'objet. Il permet de lier ce dernier à un compte.

4. Récupération des fichiers par le fabricant

Le fabricant récupère les fichiers de sortie auprès du CRA contenant les clés et identifiants générés.

5. Chargement des clés et ID dans les objets

Le fabricant programme chaque objet avec son ID et sa clé d'authentification.

6. Enregistrement par l'utilisateur final

L'utilisateur final peut alors enregistrer son objet sur le réseau en fournissant l'ID et le PAC à un opérateur Sigfox.

5.5. Limitation

Le fait que la clé NAK de Sigfox, utilisée pour calculer le MAC, ne change pas pendant toute la durée de vie du dispositif rend les attaques par rejet possible pour le réseau Sigfox. Avec l'abonnement Sigfox le plus coûteux (Platinum), le nombre maximal de messages par jour est de 140, et le compteur de message (MC) peut se réinitialiser tous les 30 jours. Après cette réinitialisation, un attaquant peut théoriquement rejouer indéfiniment n'importe lequel des 4096 paquets précédents, car la clé de sécurité NAK utilisée pour calculer les MAC reste constante (5).

Cependant, une limitation existe : comme mentionné précédemment, une plage de valeurs minimale et maximale est autorisée pour le compteur de séquence ; tout paquet en dehors de cette plage est rejeté (3). Cette restriction peut néanmoins avoir des conséquences non négligeables. Elle crée un risque de DoS (Denial of Service) si des paquets sont rejoués au-delà de l'écart maximal autorisé.

De plus, cette limitation du compteur de séquence peut provoquer un DoS « naturel » pour les nœuds finaux : si un dispositif reste hors couverture pendant une période prolongée, il peut dépasser l'écart maximal autorisé et voir ses paquets rejetés, sans qu'aucun attaquant n'intervienne. Un attaquant peut également exploiter cette vulnérabilité en brouillant un nombre de paquets équivalent à l'écart maximal, provoquant ainsi un DoS sur le dispositif ciblé (5).

Une expérience menée par (5) a confirmé cette vulnérabilité aux attaques par rejet, démontrant la menace réelle que représente la réutilisation des paquets dans le contexte de Sigfox.

Conclusion

En conclusion, Sigfox a été l'un des pionniers de la connectivité bas débit pour l'Internet des objets (IoT), en proposant un réseau simple, peu énergivore et adapté aux objets nécessitant une faible transmission de données. Cependant, malgré cette avance technologique, Sigfox a dû faire face à une forte concurrence, notamment celle de l'alliance LoRaWAN, qui repose sur un modèle plus ouvert et flexible, permettant à de nombreux opérateurs et entreprises de déployer leurs propres réseaux.

Contrairement à Sigfox, qui s'appuyait sur une infrastructure centralisée et propriétaire, LoRaWAN a séduit de grands opérateurs télécoms (comme Orange, Bouygues Telecom ou Swisscom) grâce à son interopérabilité et à sa capacité à s'intégrer facilement dans leurs offres IoT. Cette diversité d'acteurs a renforcé l'écosystème LoRaWAN, tandis que Sigfox a dû revoir son modèle pour rester compétitif.

Aujourd'hui, même si Sigfox conserve une valeur technologique solide et une présence mondiale, son avenir dépendra de sa faculté à collaborer avec les opérateurs et à s'ouvrir à des partenariats stratégiques, afin de trouver sa place aux côtés d'autres standards comme LoRaWAN, NB-IoT ou LTE-M.

Sources

Introduction / Histoire :

La start-up iot sigfox dépose le bilan - LEBIGDATA.FR. *LEBIGDATA.FR* [en ligne]. [sans date] [consulté le 5 novembre 2025]. Disponible sur :
<https://www.lebigdata.fr/sigfox-depose-bilan>

L'état de l'IoT en 2025 : une augmentation de 14% des dispositifs connectés, atteignant 21,1 milliards à l'échelle mondiale. *OBJETCONNECTE.COM* [en ligne]. [sans date] [consulté le 5 novembre 2025]. Disponible sur :

<https://www.objetconnecte.com/letat-de-liot-en-2025-une-augmentation-de-14-des-dispositifs-connectes-atteignant-211-milliards-a-lechelle-mondiale/>

Plan de continuation d'UnaBiz SAS & ; UnaBiz Network SAS sous la protection du tribunal de commerce - UnaBiz France. *UnaBiz France* [en ligne]. [sans date] [consulté le 5 novembre 2025]. Disponible sur :

<https://www.unabiz.fr/2025/09/11/unabiz-sas-redressement-judiciaire/>

Radware Page [en ligne]. [sans date] [consulté le 5 novembre 2025]. Disponible sur :
<https://www.usine-digitale.fr/article/sigfox-repris-par-le-singapourien-unabiz.N1996042v>

Source Couche Physical :

A Sigfox Energy Consumption Model: <https://www.mdpi.com/1424-8220/19/3/681>
 Wayback Machine [en ligne]. Disponible sur : <https://web.archive.org/web/20180719140108id>

What is GFSK Modulation ? Disponible sur :

<https://www.everythingrf.com/community/what-is-gfsk-modulation>

DPSK vs. BPSK : Understanding Modulation Techniques. [en ligne]. Disponible sur :
<https://www.rfwireless-world.com/terminology/dpsk-vs-bpsk>

Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT :
[lien](#)

A Sigfox Module for the Network Simulator 3.pdf. Google Docs [en ligne]. Disponible sur :
<https://drive.google.com/file/d/1-KCnPiCAay5hhhjy0sZaPmyBbTdYuwj/view>

IEEE Xplore Full-Text PDF: IEEE Xplore [en ligne]. Disponible sur :
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8660398>

Digital Modulation Schemes Employed in Wireless Communication : A Literature review - [lien](#)

Source Couche MAC :

Dr. Mukesh Bathre (2023). "Wireless Sensor Networks – MAC Layer" Department of Computer Science and Engineering

[\(PDF\) MAC layer-based evaluation of IoT technologies: LoRa, SigFox and NB-IoT](#)

https://hal.science/hal-01768341v1/file/Phy_Mac_layer_LoRa_Sigfox.pdf

<https://athene-forschung.unibw.de/doc/151319/151319.pdf>

<https://www.rfwireless-world.com/tutorials/sigfox-mac-frame-structure>

https://www.researchgate.net/publication/331539234_Long_Range_SigFox_Communication_Protocol_Scalability_Analysis_Under_Large-Scale_High-Density_Conditions

M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, “Long-range communications in unlicensed bands: the rising stars in the iot and smart city scenarios,” IEEE Wireless Communications, vol. 23, October 2016.

Source consommation d'énergie :

- [1] Gomez, C., Veras, J. C., Vidal, R., Casals, L., & Paradells, J. (2019). A Sigfox Energy Consumption Model. Sensors, 19(3), 681. <https://doi.org/10.3390/s19030681>
- [2] Trendov, S., Sariiev, E., Mukhtar, K. B. S., Kachan, D., & Siemens, E. (2025). Comparison of performance and power consumption in SigFox, NB-IoT, and LTE-M. In Lecture notes in networks and systems (pp. 127–158).
https://doi.org/10.1007/978-3-031-89296-7_8

Source Sécurité :

- [1] Qu'est-ce qu'une attaque par rejeu et comment s'en prémunir ? (s. d.). /.
<https://www.kaspersky.fr/resource-center/definitions/replay-attack>
- [2] *Sigfox connected objects : Radio specifications.* (2023).
<https://storage.googleapis.com/public-assets-xd-sigfox-production-338901379285/ce13c427-f2ed-4b94-b9f9-2bff0a96c8c9.pdf>
- [3] Sequence number : general knowledge | Sigfox Resources. *Sigfox Support* [en ligne]. [sans date]. Disponible sur :
<https://support.sigfox.com/docs/sequence-number:-general-knowledge>
- [4] Présentation technique de Sigfox [en ligne]. Juillet 2017. Disponible sur :
https://lms.fun-mooc.fr/asset-v1:univ-toulouse+101001+session02+type@asset+bloc_k/Presentation_technique_de_Sigfox_Juillet_2017.pdf
- [5] COMAN, Florian Laurentiu et Krzysztof Mateusz MALARSKI. Security issues in internet of things : vulnerability analysis of lorawan, sigfox and nb-iot [en ligne]. [sans date]. Disponible sur : doi:10.1109/GIOTS.2019.8766430