État de l'art

LoRa & LoRaWAN

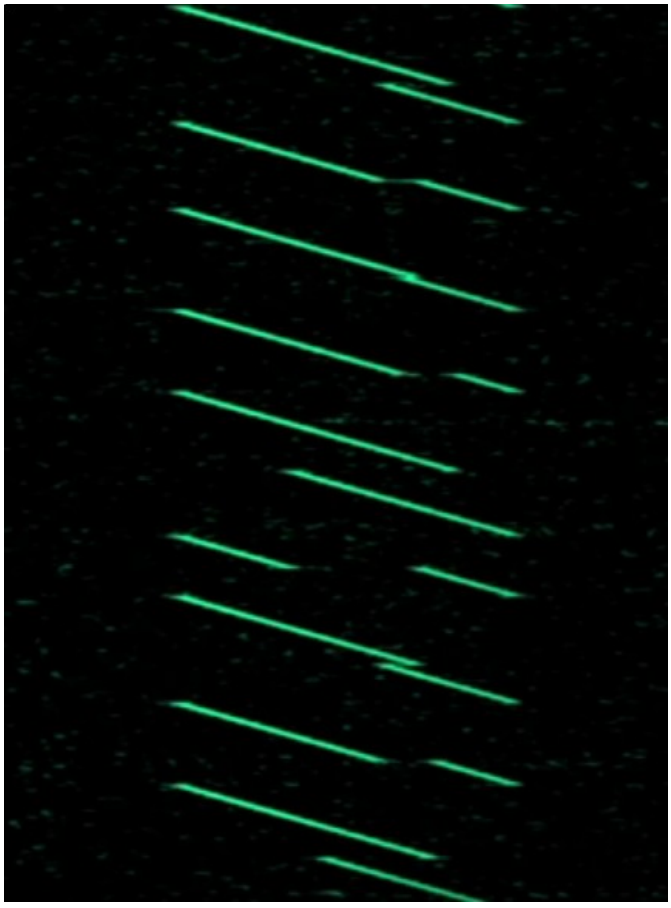


Table des matières

Introduction

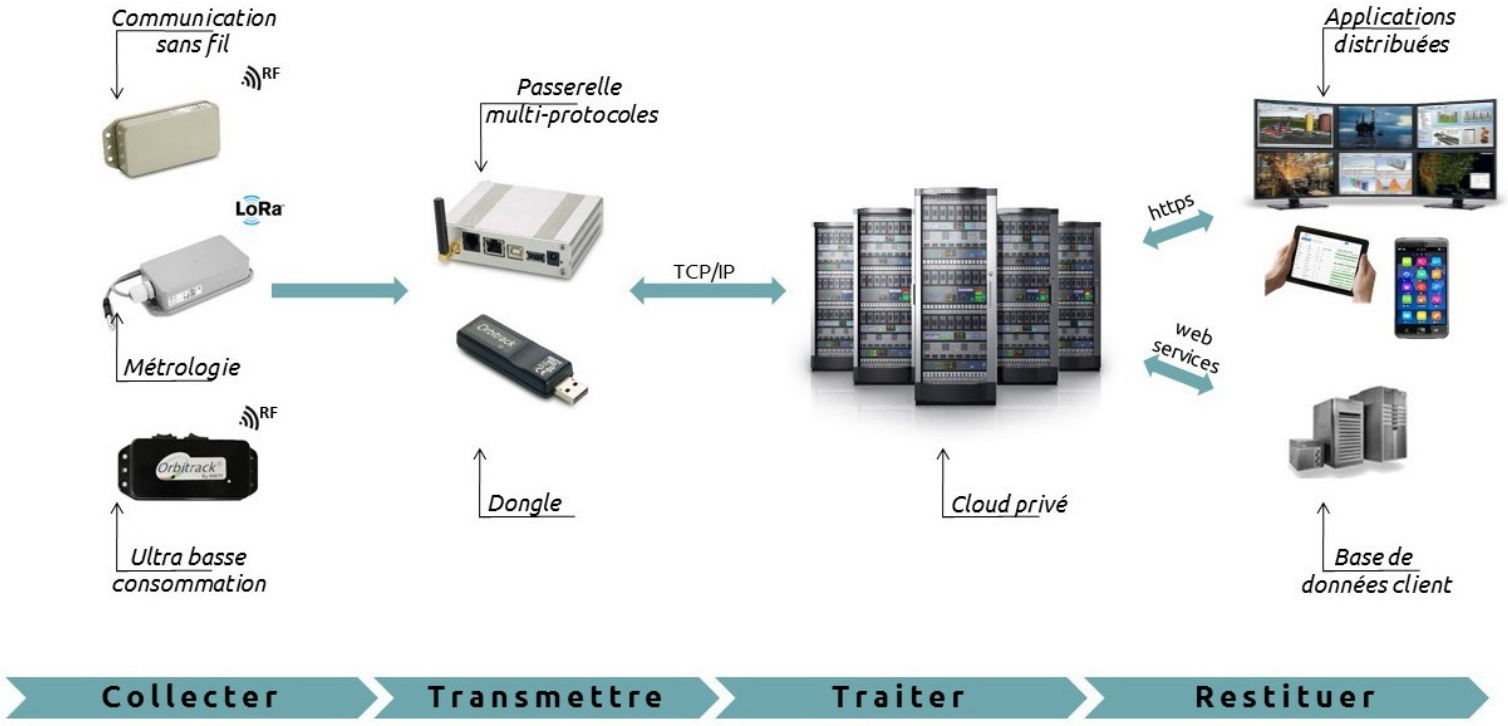
LoRa (Long Range – réseau étendu à longue portée) est le nom donné à une technologie de modulation à étalement de spectre inventée en 2010 et brevetée en 2012 par la startup française Cycleo. Cette entreprise grenobloise a été rachetée par le fabricant américain de semi-conducteur Semtech pour 5 millions de dollars. C'est la partie propriétaire de la technologie.

LoRaWAN décrit le protocole de transport qui utilise la modulation LoRa. Cette couche est open-source et relativement bien documentée. Cette récente technologie est au centre de l'actualité et de toutes les attentions puisque Semtech a trouvé des investissement à hauteur de 50 millions de dollars et la technologie a été bien accueillie au CES 2017. La technologie concurrente Sigfox a levé quant à elle 150 millions de fonds.

Nous allons dans un premier temps faire un rapide rappel sur les réseaux d'Internet Of Things (IOT), puis décrire le fonctionnement de LoRa et enfin sa surcouche LoRaWAN.

Les réseaux IOT

Voici un schéma qui résume les quatre grandes étapes de la communication d'un réseau IOT.

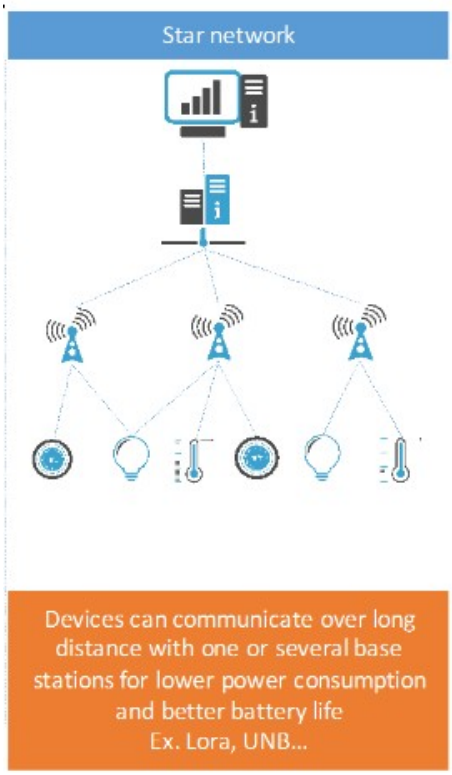


Dans l'IOT, on considère souvent des objets (capteurs) qui ont des contraintes matérielles et logicielles qui ne leur permettent pas de se connecter directement au réseau Internet. Ils s'y connectent à travers une passerelle (gateway). En effet, d'un côté internet n'est pas dimensionné pour gérer l'adressage d'autant d'objets connectés. D'un autre côté l'ipv6 est un protocole souvent trop lourd pour être exploité directement par les capteurs. Aujourd'hui l'ipv6 est utilisé via le protocole 6LowPAN (I*Pv6 Low power Wireless Personal Area Networks*) qui est exploité au-dessus des protocoles réseaux régis par l'**IEEE 802.15.4**.

Les gateways traduisent aussi les protocoles propriétaires (exemple zigbee, BLE) vers un protocole compréhensible sur internet et certaines peuvent jouer le rôle d'agrégateurs de réseaux.

Les réseaux qui les connectent doivent aussi répondre à ces besoins et ne pas coûter cher. Ainsi, les opérateurs télécom doivent s'adapter car utiliser les réseaux cellulaires pour transmettre quelques kilo d'octets par capteur coûte très cher. De plus, le réseau 2G est en cours d'extinction. Ceci offre une opportunité pour développer des réseaux sans fils Machine↔Machine à longue portée, basse énergie et très bas débit qui coûtent beaucoup moins cher que les réseaux cellulaire. La France est une pionnière dans ce domaine.

Le réseau LoRa présenté ensuite a principalement été conçu pour l'utilisation d'un schéma en étoile. Ceci a l'avantage d'avoir une grande simplicité et une faible consommation énergétique de la part des équipements émetteurs. Les particularités des technologies sans fil longue distance permettent ce type d'architecture.



Voici quelques technologies et protocoles actuels autour du monde de l'IOT :

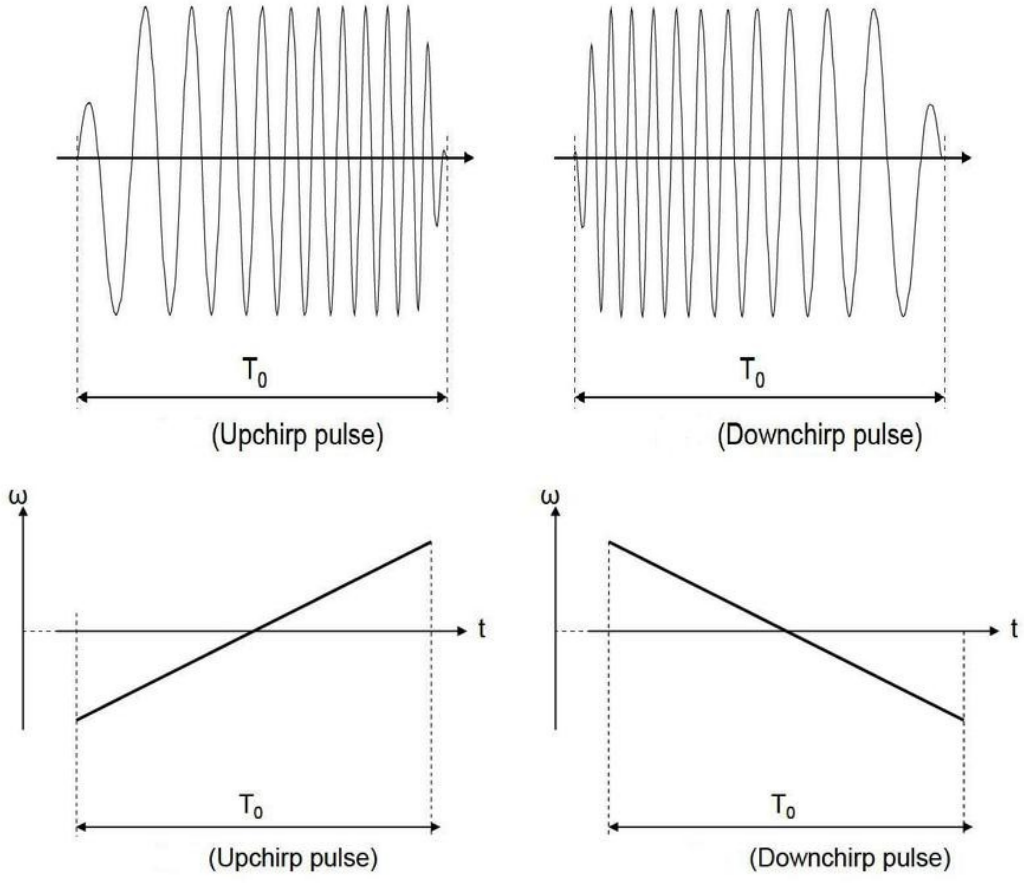
- LoRaWAN
- Sigfox
- ZigBee
- 6LoWPAN
- OCARI
- DASH-7
- Bluetooth Low-Energy (BLE)
- NFC

Couche physique – LoRa

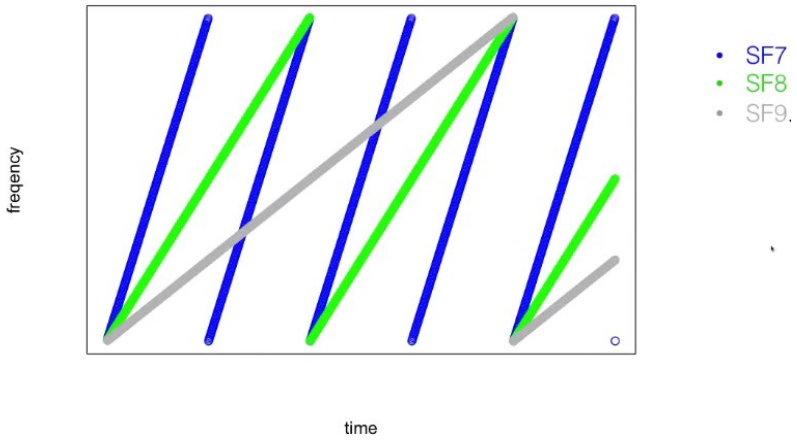
Théorie

Seuls deux documents officiels publiés par Semtech nous aident à étudier LoRa: la spécification du brevet déposé et l'*Application Note 1200.22*. Cependant il faut prendre ces informations avec prudence car il n'y a aucune garantie que le protocole réel corresponde parfaitement à ce qui est décrit. En effet la documentation fournie par Semtech cherche aussi à **offusquer le fonctionnement réel** pour protéger leur technologie.

LoRa utilise le **Chirp Spread Spectrum** (CSS). L'évolution de la fréquence d'un tel signal est toujours strictement croissante ou décroissante et linéaire au cours du temps. Cela rend la transmission très résistante aux interférences tout en restant peu gourmande en énergie. Cette modulation de fréquence est également utilisée par les Radars. La fréquence est généralement étendue sur une bande passante de 125kHz. La robustesse du signal est vital pour les technologies émettant dans les bandes ISM déjà très « bruyantes ». En effet la bande de fonctionnement typique de LoRa en Europe est 868MHz. On peut également communiquer sur les bandes 915MHz et 433MHz.



Grâce à ce signal on peut transmettre entre 7 et 12 bits par symbole. On peut choisir le nombre de symbole pour s'adapter à l'utilisation. On peut également influer sur le ratio d'encodage (CR – valeur comprise entre 1 et 4) et la bande passante. Si la communication nécessite un fort débit, on privilégiera un **spreading factor (SF)** faible. On aura donc un chirp moins étalé et moins résistant aux perturbations (faible distance) mais le nombre de bits transmis par symboles sera plus grand (débit plus grand). Ci-dessous on voit l'influence du SF sur l'allure du chirp.



BitRate = SF . *Bandwidth / 2*^SF *bits/sec* **BitPerSymbol** = SF . 4 / (4 + CR) *bit/symbol*

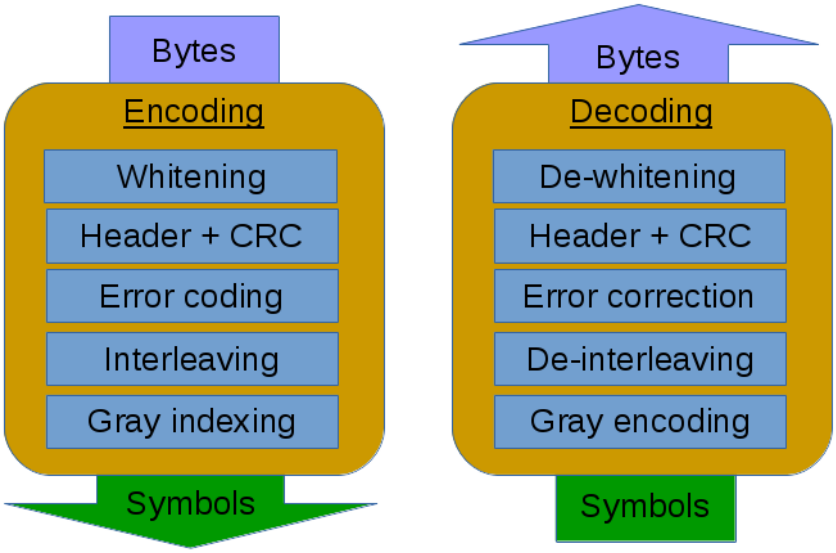
Exemple pour une bande passante de 125kHz, SF = 8 et CR = 4 (cas le plus courant) :

BitRate = **3904 bits/sec** = 488 octets/sec	BitPerSymbol = **4 bit/symbol** 2^4 → 16 fréquences de shift

Pour un spreading factor maximum (12), le payload est limité à 51 octets. Cependant pour être dans des conditions optimales de réception il est conseillé de ne pas dépasser 20 octets par message. Ceci permet un débit de l'ordre du kilooctet par seconde.

Avant de transmettre les symboles, LoRa décrit 2 étapes principales :

- Le signal est conjugué avec une séquence de bruit blanc connue pour ajouter de l'entropie (whitening)
- Entrelacement entre les bits de la trame et les bits de correction/ détection d'erreur (interleaving & error coding)

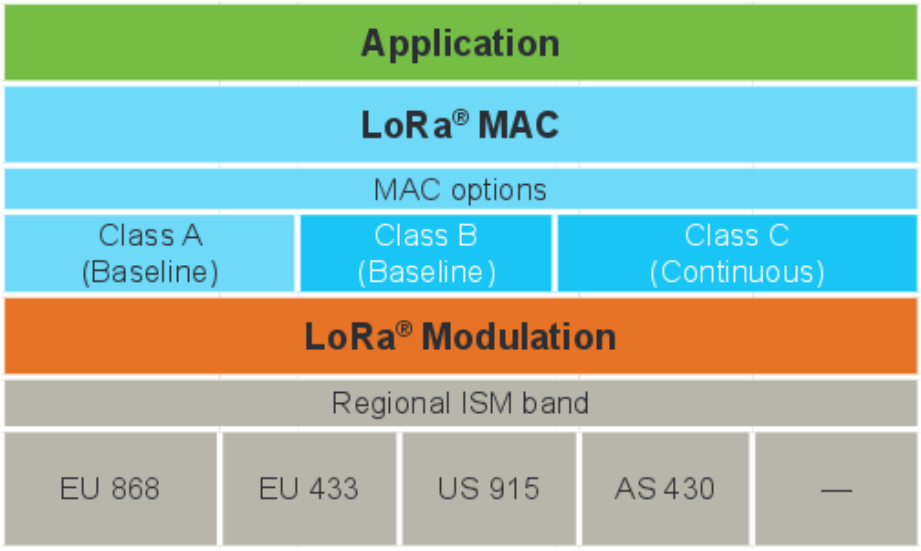


La modulation LoRa permet de capter des signaux émis même quand le rapport signal à bruit est inférieur à un. On peut par exemple avoir un rapport signal à bruit de -20dB avec un SF de 12.

Les équipements émettant selon cette technologies sont classés en fonction de leur comportement. Nous allons principalement étudier le protocole avec des émetteurs de classe A.

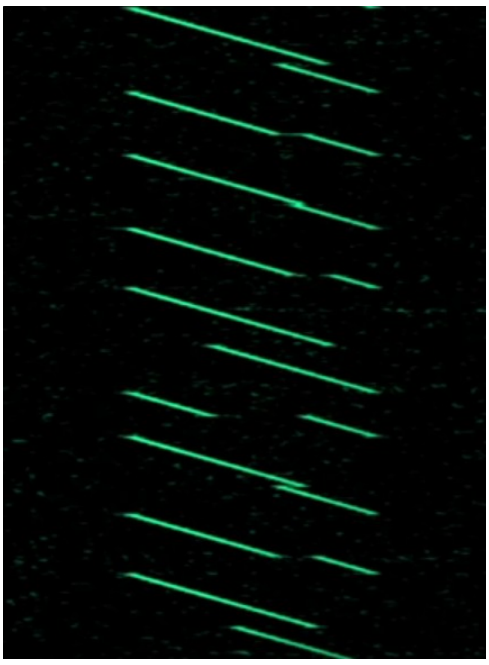
Class name	Intended usage
A (« all »)	**Battery powered sensors**, or actuators with no latency constraint Most energy efficient communication class. Must be supported by all devices
B (« beacon »)	**Battery powered actuators** Energy efficient communication class for latency controlled downlink. Based on slotted communication synchronized with a network beacon.
C (« continuous »)	**Mains powered actuators** Devices which can afford to listen continuously. No latency for downlink communication.

Pratique



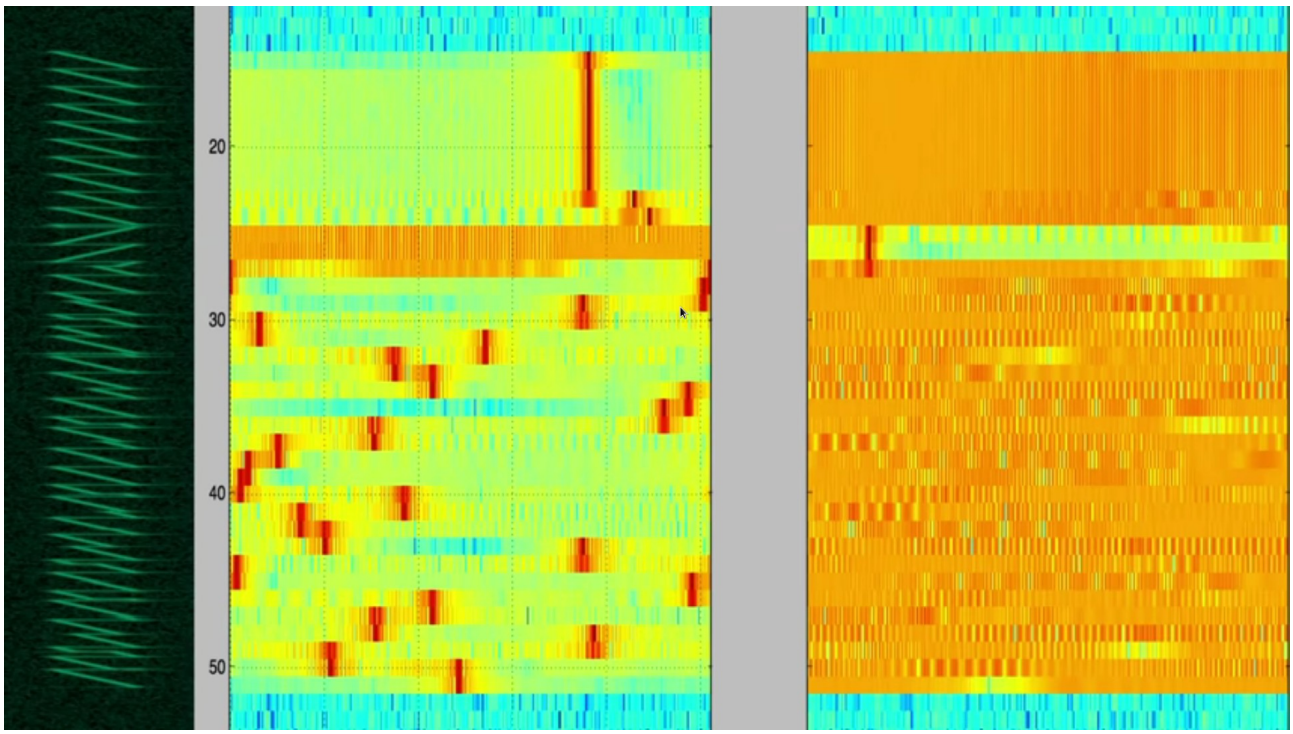
Matt Knight a réalisé une excellente analyse du protocole physique LoRa par *reverse engineering*. En partant du signal brut transmis, il explique chaque étape de la modulation, tout en la comparant à la documentation fournie par Semtech.

La première étape consiste à capter un message transmis et à analyser grossièrement l'allure du signal (modulation, chirp, préambule du message).



Ensuite il « de-chirp » le signal en combinant le message transmis avec des up et down-chirps générés localement. Ceci permet de ramener le problème à l'étude d'une MFSK (multiple-frequency shift key).

La figure ci-contre montre l'évolution de la fréquence (abscisse) et de l'amplitude (cote) en fonction du temps (ordonnée) d'un signal LoRa. On y voit clairement les discontinuités provoquées par les changements de fréquence.



On peut voir sur le graphe ci-dessus le signal original à gauche, le signal conjugué avec des up-chirps ensuite, et à droite le signal conjugué avec des down-chirps. Les pentes des chirps se compensent et laissent apparaître des constantes. Ces constantes indiquent les sauts de fréquences et contiennent l'information (symboles). Le préambule est une série de down-chirps suivit de 2 up-chirps qui servent à la synchronisation. On est en présence d'un SF valant 8, et d'un CR valant 4 d'où les symboles codés sur 16 fréquences.

Ensuite se pose la question de ce que représente ces symboles. En effet ici le payload transmis à subit les étapes de whitening et d'interleaving. En transmettant un message uniquement rempli de 0, on arrive à récupérer la matrice de whitening. Lors de cette étape, le message subit un XOR avec la matrice aléatoire connue. En passant un message rempli de 0 on retrouve donc exactement la matrice de whitening. Cependant, une deuxième matrice est utilisée pour les entêtes, ce qui rend la tache difficile.

Couche transport – LoRaWAN

LoRaWAN (Long Range Wide Area Network) est la couche de contrôle d'accès au média pour le protocole LoRa. La spécification de la première version a été publiée en janvier 2015 et une version 1.1 est en cours d'élaboration.

On distingue dans cette partie les « end-device » (émetteur) de la « gateway » (récepteur). LoRaWAN est compatible avec plusieurs options mais très peu sont obligatoire. Le chiffrement de bout en bout par exemple est supportée mais aucunement obligatoire. On peut également citer l'adaptation automatique du taux d'échange de données (ADR – adaptive data-rate), adaptation dynamique du SF etc. Grâce à l'ADR, une seule gateway peu communiquer avec plusieurs end-devices différents avec des data-rates différents.

De manière native, les end-device changent automatiquement de canal dans la bande ISM données pour être plus robuste aux interférences. Dans la bande des 868MHz par exemple, LoRaWAN décrit **3 canaux sont disponibles**. En Europe, il faut faire attention au « maximum transmit duty cycle » qui est réglementé et qui ne doit pas dépassé 1 % pour les end-devices.

Structure des paquets

Voici la structure générale d'un paquet LoRaWAN :

Radio PHY layer:

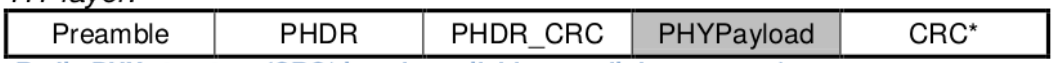


Figure 5: Radio PHY structure (CRC* is only available on uplink messages)

PHYPayload:

Figure 6: PHY payload structure

MACPayload:

Figure 7: MAC payload structure

FHDR:

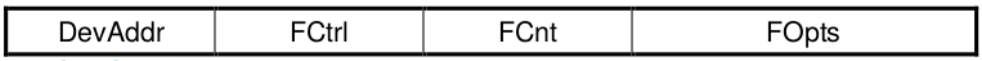


Figure 8: Frame header structure

Processus d'authentification et d'activation

Avant de communiquer, tous les end-devices doivent être personnalisés et activés. Il existe deux méthodes pour cela, la plus pratique est dite « à-la-volée » (On-The-Air Activation). Un serveur centralise les informations essentielles. Sur un réseau de taille réduite, le serveur peut être associé à la gateway (RaspberryPi + module LoRa par exemple).

Au préalable il est nécessaire de préparer le device en lui renseignant :

- Un identifiant global unique (DevEUI)
- Un identifiant global d'application (AppEUI - identifie le propriétaire)
- Une clé AES-128 unique pour chaque device (AppKey)

Le serveur du réseau auquel le device se connecte possède les informations suivantes :

- L' AppKey du device
- Une black-list des nonce déjà utilisés pour ce device (initialement vide)
- Un identifiant global unique de réseau (NwkID)
- Une adresse réseau libre à fournir au device (NwkAddr)

Seulement alors peut commencer le processus d'authentification et d'activation à la volée. Un premier paquet est émis en clair sur le canal par défaut par le device :

Size (bytes)	8	8	2
Join Request	AppEUI	DevEUI	DevNonce

Le message est envoyé en clair mais le code d'intégrité du message (Message integrity code - MIC) est calculé. Grâce à ces informations, le serveur vérifie que le device est bien associé à son réseau. Uniquement si les informations sont correctes, le serveur lui répond par un message « join_accept ». Le DevNonce est black-listé par le serveur pour éviter le rejeu.

Size (bytes)	3	3	4	1	1	(16) Optional
Join Accept	AppNonce	NetID	DevAddr	DLSettings	RxDelay	CFList

Ce message est chiffré par AES-128 avec l'AppKey en mode *Electronic CodeBook* (ECB).Grâce aux champs NetID et DevAddr, le device récupère les informations nécessaires pour communiquer et être identifié au sein du réseau. L'AppNonce permet de dériver une paire de clés à partir de l'AppKey :

> ***NwkSKey*** *= aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce | pad16)*
> ***AppSKey*** *= aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce | pad16)*

L'AppSKey encrypte le payload pour les messages applicatifs alors que la NwkSKey encrypte les messages MAC. L'opérateur n'a pas connaissance de l'AppSKey.

Risques et limites

Les adresses du réseau sont codées sur 25 bits, il y a donc plus de 33 millions de devices par réseau. Le nombre de réseau potentiel cependant est codé sur 7 bits, il ne peut donc y avoir « que » 128 réseaux superposés. Ces valeurs indiquent que la limite réside plutôt dans l'allocation de la bande passante.

L'algorithme de chiffrement AES-128 est très robuste. Par exemple, les documents classifiés et secrets américains peuvent être chiffrés par cette méthode. La meilleure attaque actuelle contre cet algorithme utilise 9 petaoctet de stockage et quelques milliards d'années. L'échange de clé cependant est par contre beaucoup moins sécurisé. L'utilisation de l'AES-128-ECB semble non justifiée par rapport à un chiffrement par cipher-block chain (CBC).

La clé d'application doit être générée de telle sorte qu'elle soit unique pour chaque end-device. Compromettre la sécurité de cette clé ne remet donc pas en question la totalité du réseau.

Sources

Référence 802.15.4:
http://www.ieee802.org/15/pub/TG4.html

Guide du développeur d'Orange
https://partner.orange.com/wp-content/uploads/2016/04/LoRa-Device-Developer-Guide-Orange.pdf

LoRa Application Note
http://www.semtech.com/images/datasheet/an1200.22.pdf

LoRaWAN Specifications
https://www.lora-alliance.org/portals/0/specs/LoRaWAN%20Specification%201R0.pdf

LoRa Design Guide
https://www.semtech.com/images/datasheet/LoraDesignGuide_STD.pdf

Etudes déjà réalisées sur LoRa par reverse-engineering
https://revspace.nl/DecodingLora

Matt Knight full reverse-engineering
https://github.com/matt-knight/research/tree/master/2016_12_29_ccc-33c3