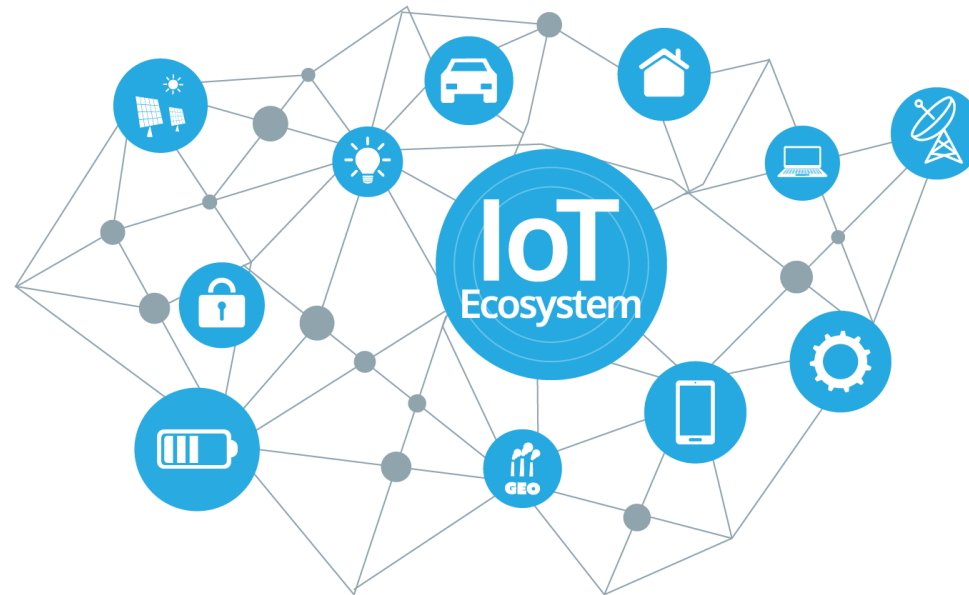


LORA / LORAWAN

Principes de base

LORA, GATEWAY, NODE, NETWORK



La technologie LORA

LoRa est l'acronyme de **Long Range**

Cette technologie sans fil permet à un émetteur (**node**) de faible consommation de transmettre des petits paquets de données (0,3 kbps à 5,5 kbps) à un récepteur sur une longue distance.

Les données passent par une passerelle (**gateway**) qui peut gérer des centaines de périphériques en même temps.



Node basé sur
une carte arduino
mkrwan 1310



Passerelle LoRaWAN
d'intérieure Dragino LPS8

NODE

Un node LoRa est constitué de 3 parties:

- Un module radio Lora avec antenne.
- Un microprocesseur.
- Une batterie.

Il est possible de créer ses propres nodes en utilisant des shields arduino ou raspberry.

On associe généralement un capteur au node. L'objectif étant de transmettre en lora les données issues de ce capteur (température/humidité/...)



DRAGINO LORA/GPS
SHIELD FOR ARDUINO
(868 MHZ)



DRAGINO LORA/GPS
HAT FOR RASPBERRY
PI (868 MHZ)

Gateway

Une gateway (passerelle) LoRa se compose de 3 parties:

- Un module radio Lora avec antenne
- Un microprocesseur pour traiter les données
- Une interface réseau (filaire ou wifi) pour se connecter à internet

Les passerelles sont alimentées par le secteur et connectées à Internet.

Suivant son type, indoor (intérieur) ou outdoor (extérieur), la passerelle a plus ou moins de couverture Lora. Pour une passerelle indoor, il faut compter un rayon de 100m. Pour une passerelle outdoor, la couverture peut atteindre un rayon de plusieurs kilomètres, mais son coût est plus élevé.

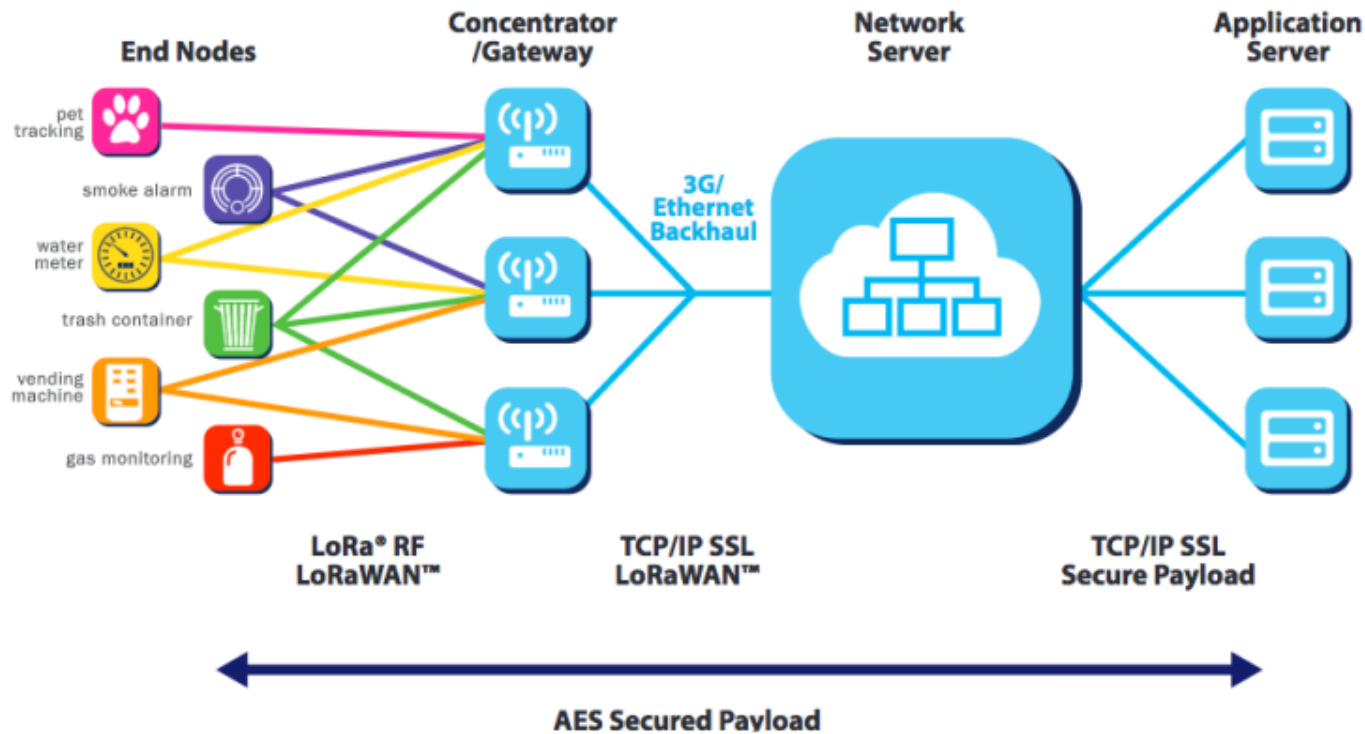


Passerelle LoRaWAN
intérieure Dragino LPS8



Passerelle LoRaWAN
extérieure Dragino DLOS8

Le réseau LORAWAN



L'architecture du réseau LoRaWAN possède une topologie en étoile.

La communication entre le node et la passerelle est bidirectionnelle et alternée (half duplex)

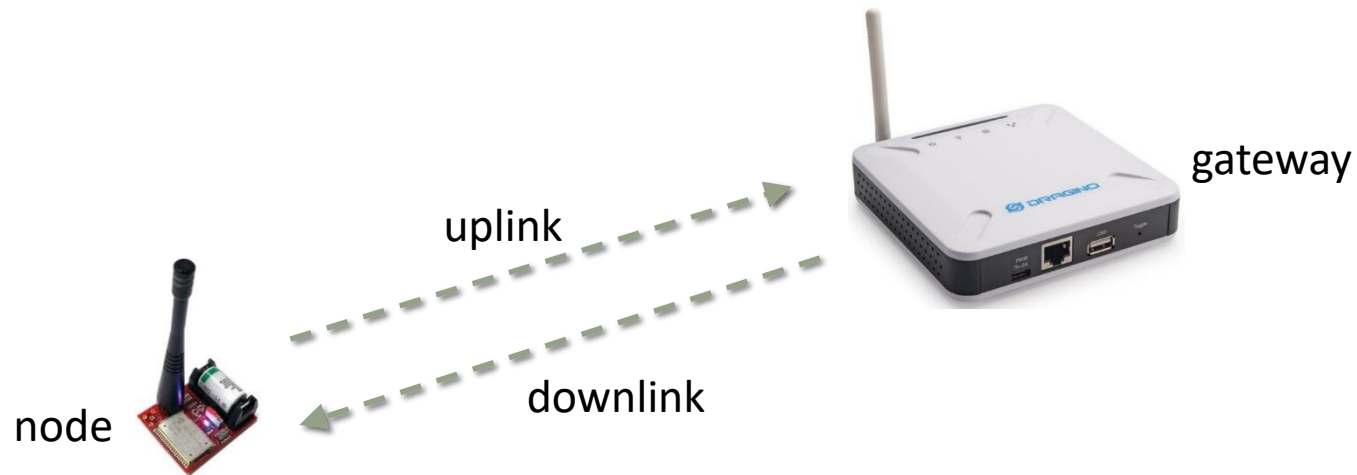
Ce qui signifie que le node peut envoyer des données à la passerelle, mais qu'il peut aussi recevoir des données de la passerelle.

Source: <https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf>

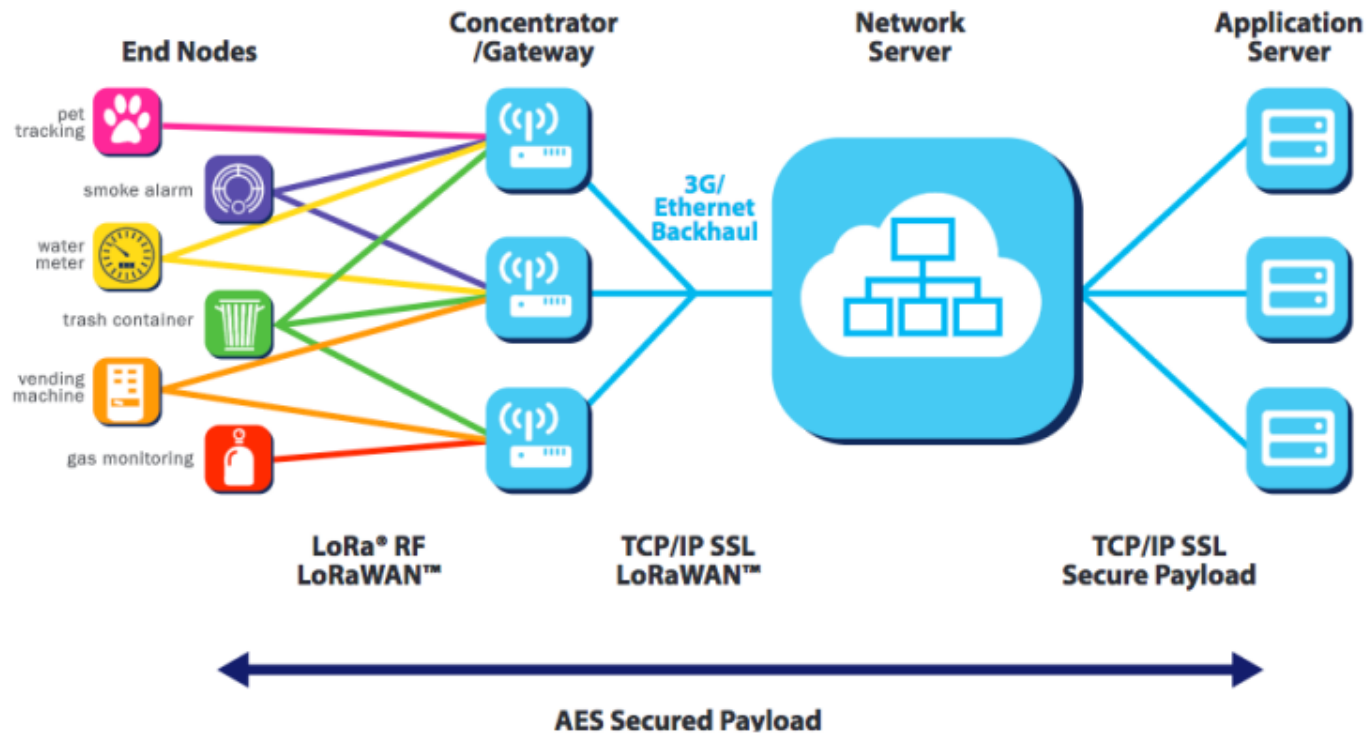
UPLINK et DOWNLINK

Lorsqu'un node transmet des données à la passerelle, cela s'appelle une liaison montante (**uplink**)

Lorsque la passerelle transmet des données au node, cela s'appelle une liaison descendante (**downlink**)



Principe de fonctionnement du LORAWAN



Un node diffuse ses données sur toutes les passerelles se trouvant à proximité.

Les passerelles transmettent ce paquet au serveur de réseau.

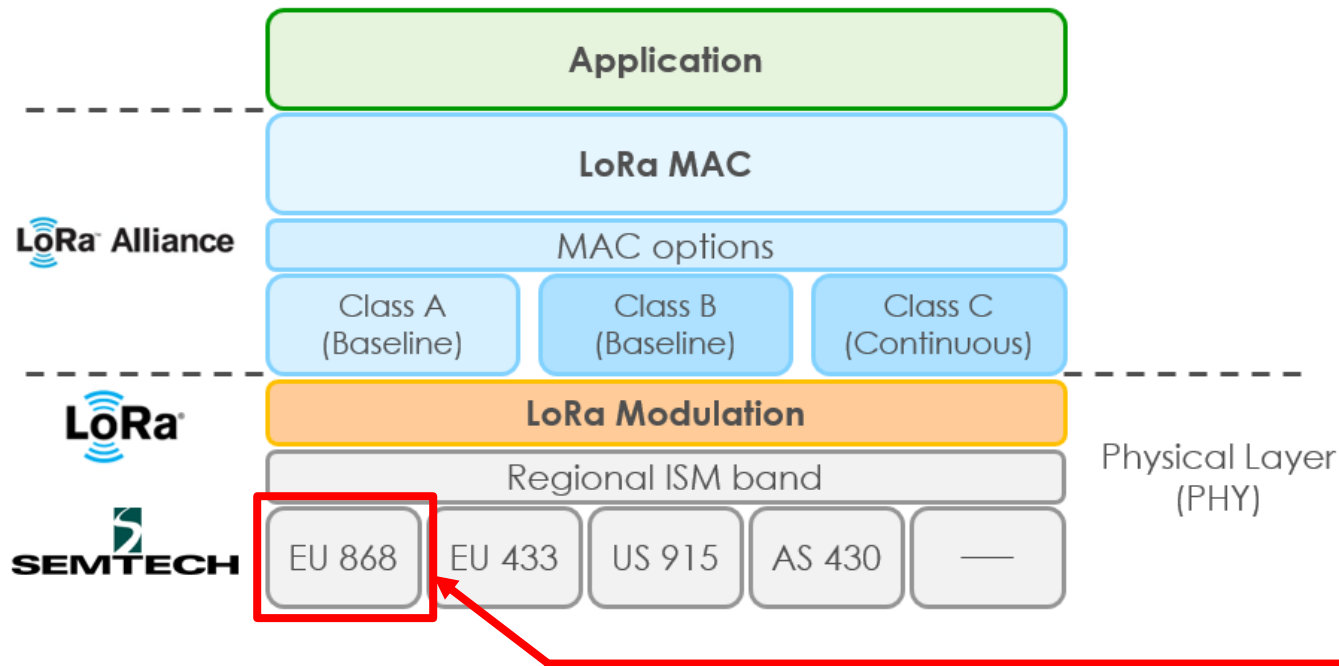
Le serveur de réseau collecte les messages de toutes les passerelles et les filtre pour ne pas dupliquer les données. Il détermine alors la passerelle qui offre la meilleure réception.

Le serveur de réseau transfère le paquet au serveur d'application approprié où l'utilisateur final peut traiter les données issues de ses nodes.

Le serveur d'applications peut éventuellement renvoyer une réponse au node.

Dans ce cas, lorsqu'une réponse est envoyée, le serveur de réseau reçoit la réponse et détermine quelle passerelle utiliser pour retransmettre la réponse au node. Il choisit la passerelle ayant mesurée, lors de la réception, le niveau de réception le plus élevé (le RSSI, voir dernière diapo)

Protocole en couche du réseau LORAWAN



Le réseau LoRaWAN (*Long Range Wide Area Network*) est défini par la LoRa Alliance.

C'est une organisation à but non lucratif de plus de 500 entreprises membres. Elle s'engage à déployer à grande échelle le LPWAN à travers le développement et la promotion du standard ouvert LoRaWAN.

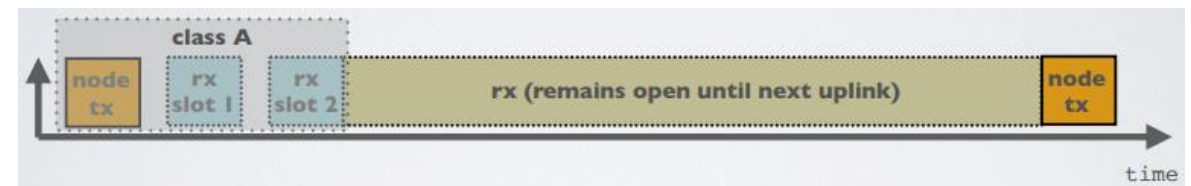
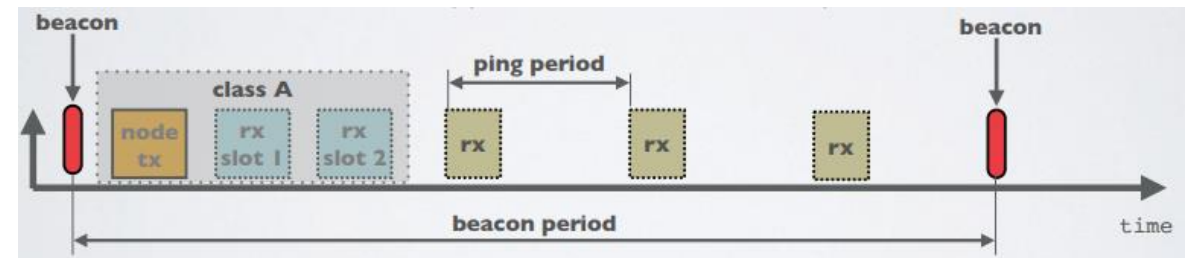
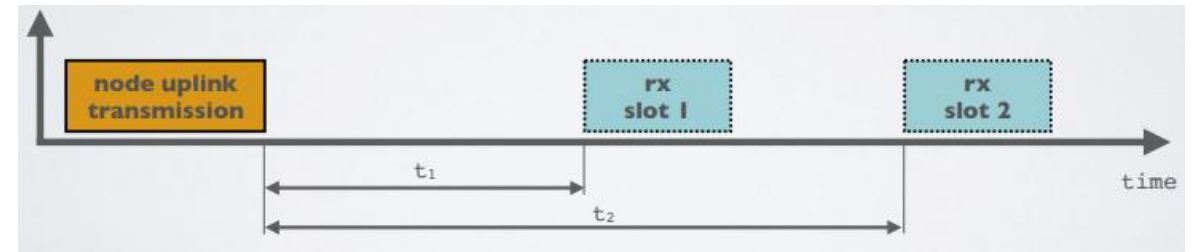
Attention lors de l'achat de votre matériel LoraWan à bien choisir des nodes et des gateways compatibles avec la fréquence européenne de **868 MHz**

- LoRa (Long Range), désigne l'interface radio (couche physique) assurant la transmission des données entre les objets connectés et la passerelle.
- LoRaWAN (Long Range Wide Area Network), désigne le réseau de communications.

LoRa est propriétaire (SEMTECH) et LoRaWAN est ouvert (LoRa Alliance)

Des nodes de classes A, B et C

| Classes | Decription |
|--------------|--|
| A(II) | Dispositifs alimentés par batterie. Lorsqu'un périphérique envoie un message à la passerelle (uplink), la transmission est suivi de deux courtes fenêtres de réception (downlink). |
| B(eacon) | Identique à la classe A, mais ces périphériques ouvrent également des fenêtres de réception supplémentaires à des instants prédéfinis. |
| C(ontinuous) | Identique à la classe A, mais ces appareils écoutent en permanence. Ils consomment alors plus d'énergie et sont souvent alimentés par secteur ou panneaux solaires. |



Les adresses

Le protocole LoRaWAN utilise plusieurs adresses pour identifier les différents périphériques sur le réseau.

- **DevEUI** – Identifie le node (end-device), format EUI-64 (unique)
- **AppEUI** – Identifie l'application, EUI-64 (unique)
- **GatewayEUI** – Identifie la passerelle, EUI-64 (unique)
- **DevAddr** – Adresse du device sur le réseau (non unique), codée sur 32 bits

Sécurité et activation

Pour être autorisé à utiliser le réseau LoRaWAN, le node doit passer par une étape d'activation afin d'obtenir deux clefs de session **NwkSKey**, **AppSKey**.

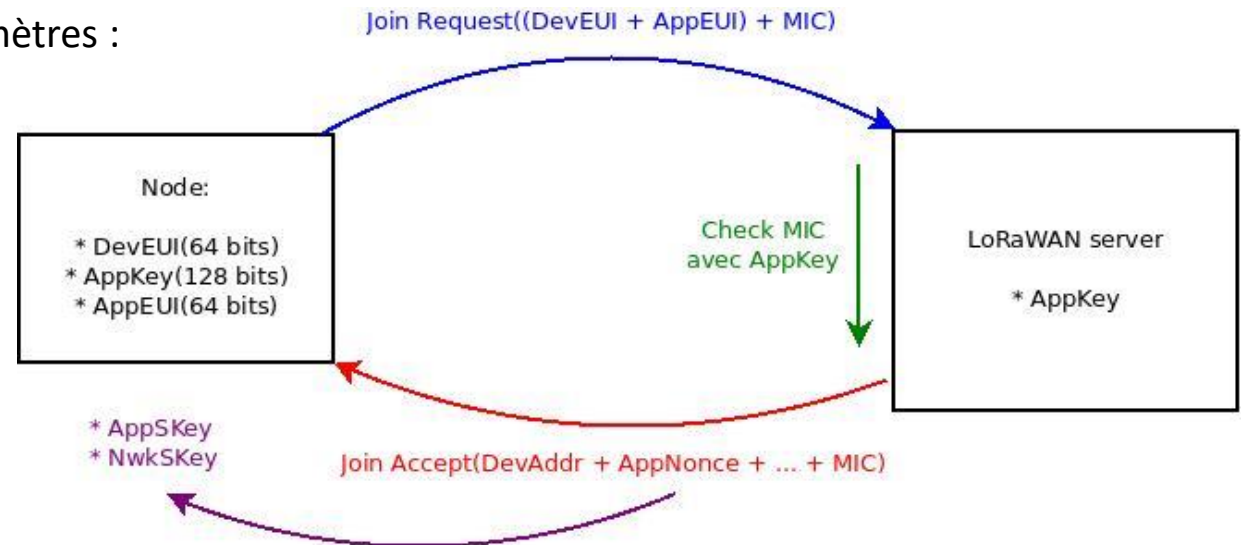
Cette étape d'activation peut s'effectuer de deux manières : Over-The-Air Activation (**OTAA**) ou Activation By Personalization (**ABP**).

En OTAA, le node doit transmettre au serveur de réseau une demande d'accès, appelée *join request*. Elle est composée de trois paramètres :

- *DevEUI*
- *AppEUI*
- Un *MIC* (Message Integrity Code) calculé avec l'*AppKey*

Le serveur d'enregistrement dispose également de l'*AppKey* utilisée pour vérifier le MIC réceptionné. Le serveur répond ensuite avec un message *join accept* qui contient l'adresse du node sur le réseau (*DevAddr* et *AppNonce*) afin de permettre au node de déterminer les clefs de session *NwkSKey*, *AppSKey*.

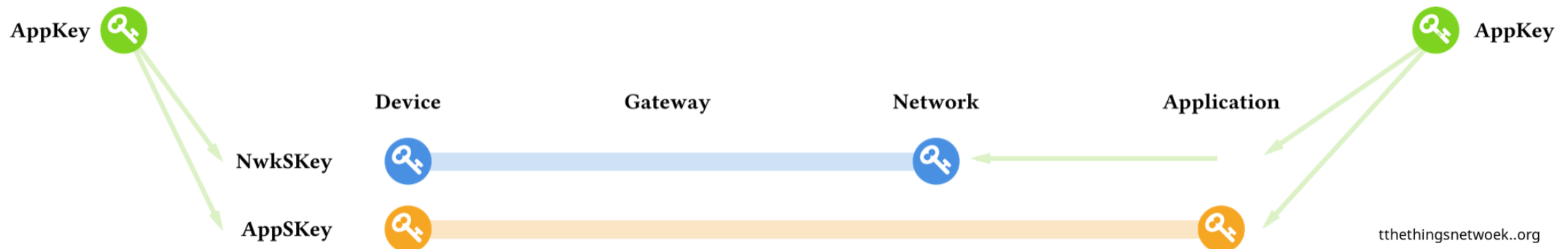
Aucune réponse n'est transmise au device si la demande est rejetée (MIC non vérifié).



Sécurité et activation

Une fois les 2 clefs de session obtenues, la communication entre le node et le serveur d'application peut commencer de manière sécurisée. En matière de sécurité, la norme LoRaWAN spécifie trois clefs AES-128 :

- **NwkSKey**, clef de session réseau, qui est utilisée lors des échanges entre le node et le serveur de réseau. Elle assure l'authenticité des nodes en calculant et vérifiant un Message Integrity Code, MIC, à partir des données transmises (Header + Payload chiffré).
- **AppSKey**, clef de session applicative, spécifique à un node, est utilisée pour chiffrer et déchiffrer le payload (qui contient le message transmis par le node).
- **AppKey**, clef applicative connue seulement par l'application (le serveur d'application) et le node. Elle permet d'obtenir les deux clefs précédentes.



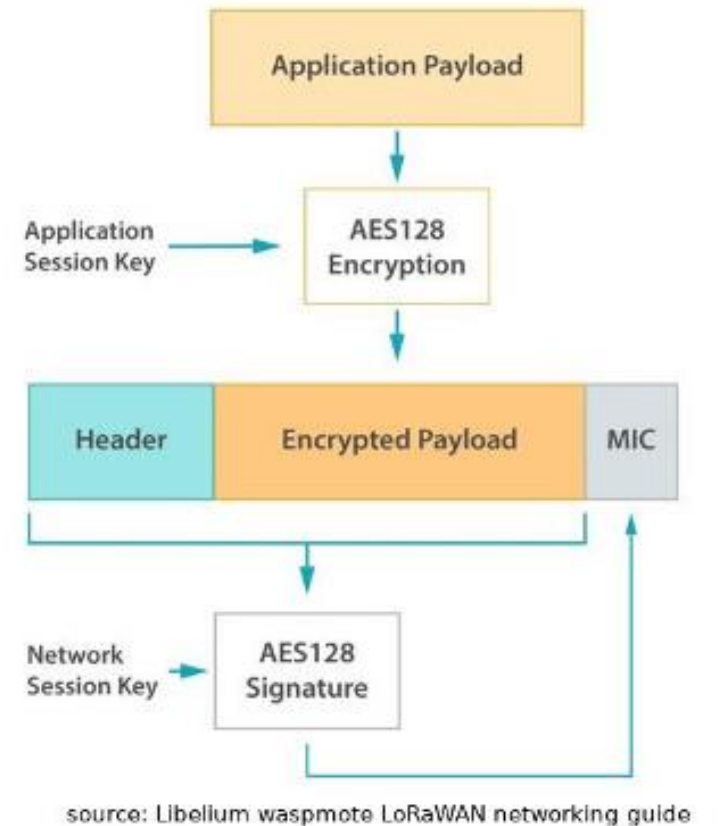
Sécurité et activation

Grâce au système de signature/chiffrement mis en œuvre lors de la communication (grâce aux 2 clefs de session), il est impossible pour un tiers de consulter les données (y compris le propriétaire de la passerelle)

Le schéma ci-contre résume le processus de signature/chiffrement :
L'information (Payload) est cryptée grâce à l'AppSkey. Le Payload ainsi crypté est alors encapsulé dans une trame encadrée par un HEADER et un MIC. Ce MIC (la signature) est calculé à partir du Payload crypté et du HEADER.

Remarque :

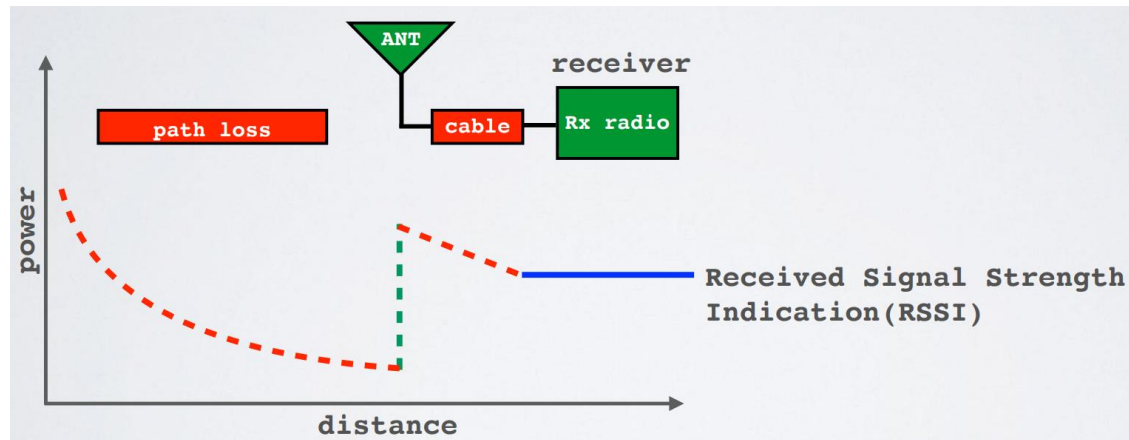
On utilise également un frame counter pour se protéger contre les attaques par replay, qui consistent à répéter une transmission interceptée. Le compteur est incrémenté à chaque transmission. La passerelle et les end-devices rejettent les transmissions dont la valeur de compteur est inférieure à celle attendue.



RSSI

Le RSSI (Received Signal Strength Indication) est la puissance du signal reçu.

Cette valeur peut être utilisée pour évaluer la qualité de réception d'une passerelle recevant un message issu d'un node.



Le RSSI est mesuré en dBm.

Sa valeur est négative.

Plus le chiffre est proche de 0, meilleur est le signal.

Si RSSI = -30dBm : le signal est fort

Si RSSI = -120dBm : le signal est faible