Internet des objets : zoom sur la technologie réseau sans fil longue portée et basse consommation LoRaWAN

L'Internet des objets exige une architecture réseau conçue pour gérer des milliers de capteurs qui peuvent éventuellement être placés loin de toute zone habitée et dans des lieux difficiles d'accès, le tout avec un niveau élevé de sécurité. Ces mêmes capteurs doivent pouvoir être alimentés sur pile ou batterie durant de longues périodes. La technologie LoRa et le protocole LoRaWAN répondent à ces exigences.

L'Internet des objets (IoT) implique un certain nombre de prérequis, quelle que soit la technologie de connectivité réseau utilisée. L'IoT exige en effet une architecture réseau conçue pour gérer des milliers de capteurs qui peuvent éventuellement être placés loin de toute zone habitée et dans des lieux difficiles d'accès, depuis les capteurs qui surveillent le débit de l'eau et la pollution des rivières et canaux, jusqu'aux compteurs d'énergie installés dans les caves des habitations. Une architecture IoT nécessite également la prise en charge de capteurs alimentés par pile ou batterie de façon sécurisée tout en facilitant l'installation et la maintenance. Ce qui désigne clairement les communications sans fil comme un moyen d'éviter le surcoût que représentent les câbles. La technologie réseau doit aussi prendre en compte les contraintes énergétiques parfois strictes des nœuds d'extrémité, dont beaucoup doivent pouvoir fonctionner pendant 10 ans sur batterie sans recharge possible. Elle doit en plus offrir un bon niveau de sécurité permettant de prévenir les tentatives d'espionnage et déjouer les piratages de données.

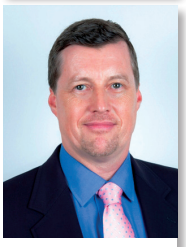
Eclairage sur la technologie radio LoRa

La conception de ce type de technologie réseau commence dès la couche physique. Tout comme de nombreux autres protocoles sans fil utilisés pour les applications IoT, la technologie LoRa utilise une technique de modulation à étalement de spectre. L'une des principales différences entre LoRa et les autres protocoles existants réside dans l'utilisation d'une technologie adaptative reposant sur des signaux « chirp » plutôt que sur l'étalement de spectre à séquence directe (DSSS, Direct-Sequence Spread Spectrum) habituellement utilisé. Cette approche offre un compromis entre la sensibilité en réception et le débit de données maximal, ce qui, grâce à la conception de la modulation, permet cette adaptation nœud par nœud.

Avec la technologie DSSS, la phase de la porteuse est décalée de façon dynamique selon une séquence de code pré-calculée. Un certain nombre de codes successifs sont appliqués à chaque bit devant être transmis. Cette séquence de décalages de phase pour chaque bit crée un signal qui varie beaucoup plus rapidement que la porteuse et « étale » donc les données sur une large plage de fréquence. Plus il y a de « morceaux » de code, plus le facteur d'étalement est élevé. Cet étalement fait que le signal est moins sensible aux interférences mais il réduit par ailleurs le débit de données effectif et augmente l'énergie par bit émis. Cependant, parce qu'il est plus résistant aux interférences, l'émetteur peut réduire au global les niveaux de puissance. En général, pour un même taux d'erreur binaire, la technologie DSSS offre une plus faible consommation d'énergie.

Il existe toutefois un coût énergétique et financier avec la technologie DSSS, qui diminue les possibilités d'utilisation avec des nœuds de capteurs IoT. Afin de s'assurer que le récepteur puisse traiter les « morceaux » de bit entrants et convertir le flux en données, la technologie DSSS s'appuie sur une horloge de référence fiable intégrée à la carte électronique. Ce type d'horloge est en général assez onéreux et une précision plus grande va de pair avec une consommation énergétique plus élevée. De son côté, la technique de l'étalement de spectre chirp (CSS, Chirp Spread-Spectrum) utilisée par LoRa peut être mise en œuvre à un

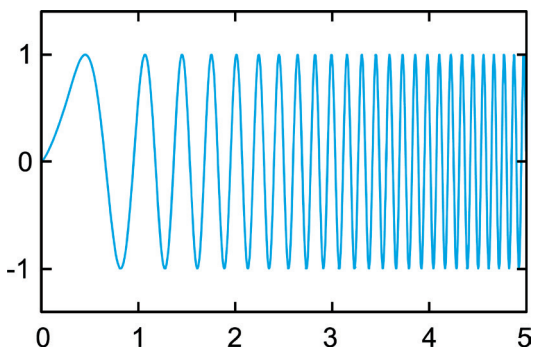
AUTEUR



Patrick van Eijk, directeur en charge des solutions IoT, Semtech.

1 EXEMPLE DE SIGNAL « CHIRP » UTILISÉ POUR L'ÉTALEMENT DE SPECTRE EN TECHNOLOGIE LORA

L'une des principales différences entre LoRa et les autres protocoles existants réside dans l'utilisation d'une technologie adaptative reposant sur des signaux « chirp » plutôt que sur l'étalement de spectre à séquence directe (DSSS, Direct-Sequence Spread Spectrum) habituellement utilisé.



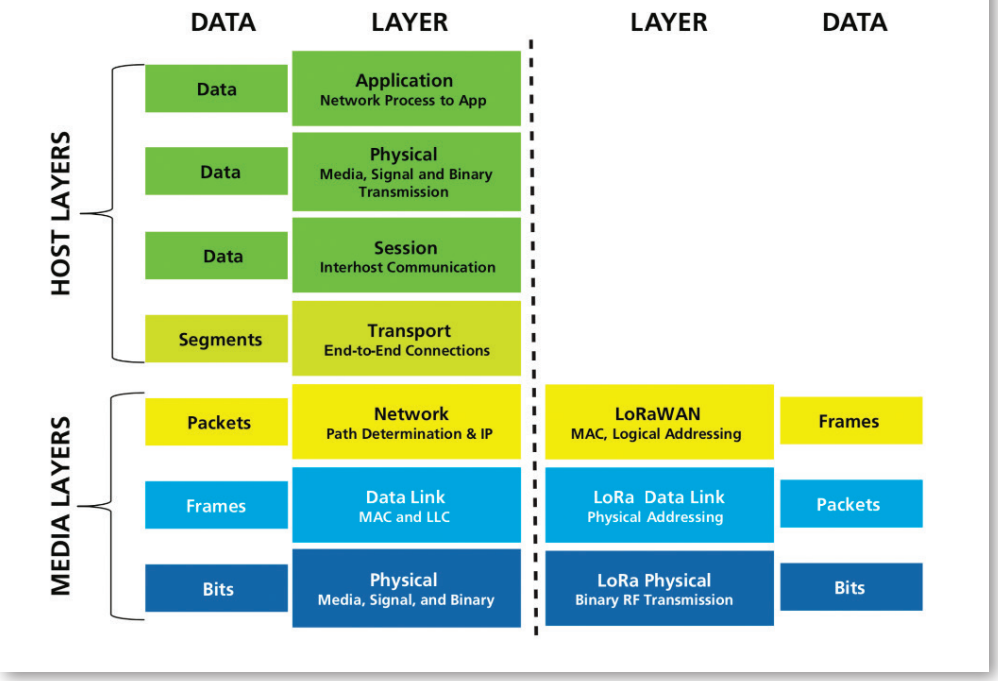
moindre coût car elle ne s'appuie pas sur une horloge précise.
Un signal chirp est un signal qui varie en fréquence au cours du temps. Dans le cas de LoRa, le signal augmente en fréquence sur la longueur de chaque groupe de « morceaux » de bit de données (figure 1). Pour une meilleure résilience, LoRa ajoute une information de correction d'erreur aux flux de données.
En plus de la résistance aux interférences inhérente aux systèmes à étalement de spectre, la technologie CSS offre une immunité élevée à la distorsion et à l'évanouissement multitrajets, phénomènes qui posent souvent problème en milieu urbain, ainsi qu'aux décalages Doppler. Ce type de décalage entraîne un changement de la fréquence apparente, ce qui implique le recours à des horloges très précises. Cependant, la technologie CSS est plus résiliente car les décalages Doppler n'entraînent qu'une petite modification du signal en bande de base sur l'axe du temps. Tout comme la technologie DSSS, LoRa peut faire varier le nombre de morceaux de code par bit. Le standard définit ainsi 6 facteurs d'étalement (SF, Spreading Factor) différents. Avec un facteur d'étalement plus élevé, il est possible d'étendre la portée du réseau, au prix de davantage de puissance par bit et d'un débit de données global plus faible. Avec un facteur d'étalement SF7, le débit de données maximal est d'environ 5,4 kbit/s avec un signal assez fort pour voyager sur 2 km (la distance réelle dépendra du terrain). A un facteur d'étalement SF10, la portée estimée passe à 8 km, avec un débit de données d'un peu moins d'1 kbit/s. Il s'agit du facteur d'étalement le plus élevé sur une liaison ascendante, c'est-à-dire une transmission entre un nœud et la station de base. Les liaisons descendantes peuvent utiliser deux facteurs SF encore plus élevés.
Les codes d'étalement SF sont par ailleurs orthogonaux, ce qui permet à différents nœuds d'utiliser différentes configurations de canaux sans s'affecter entre eux.

LoRaWAN : deux couches logiques de niveau 2 et 3

Au-dessus de la couche physique qui prépare les données pour la modulation CSS et la transmission, le protocole LoRaWAN définit deux couches logiques qui correspondent aux couches 2 et 3 du modèle de réseau OSI (Open Systems Interconnection) (figure 2).
La couche 2 est la couche de liaison de données LoRa, qui comprend une protection basique de l'intégrité des messages, reposant sur des contrôles de redondance cycliques (CRC). Comme dans tout autre protocole de couche 2 dans le modèle OSI, la mise en œuvre de la technologie LoRaWAN offre une communication point-à-point classique.
La couche 3 ajoute la fonctionnalité de protocole réseau qui fait que LoRaWAN est particulièrement bien adapté aux besoins des applications IoT. Le protocole réseau offre la capacité pour les nœuds de se signaler les uns les autres ou d'envoyer des données dans le nuage par l'intermédiaire d'Internet grâce à un concentrateur ou à une passerelle. LoRaWAN utilise une topologie en étoile : tous les nœuds terminaux communiquent via la passerelle la plus appropriée. Les passerelles s'occupent de l'ensemble du routage et peuvent, si plusieurs passerelles se trouvent à portée d'un nœud terminal et que le réseau local est encombré, renvoyer la communication vers un chemin alternatif.

2 MODÈLE DE RÉFÉRENCE OSI EN SEPT COUCHES POUR LES RÉSEAUX

Au-dessus de la couche physique LoRa qui prépare les données pour la modulation CSS (Chirp Spread Spectrum) et la transmission, le protocole LoRaWAN définit deux couches logiques qui correspondent aux couches 2 et 3 du modèle de réseau OSI (Open Systems Interconnection).



Certains protocoles IoT utilisent des interconnexions maillées pour augmenter la distance maximale entre un nœud terminal et une passerelle. Néanmoins, cette fonctionnalité entraîne un surcoût énergétique sur les nœuds utilisés pour envoyer les messages vers et depuis les passerelles ainsi que des effets secondaires inévitables et imprévisibles sur l'autonomie des batteries. L'architecture LoRaWAN, quant à elle, garantit que chaque nœud du réseau IoT peut disposer d'une batterie idéalement calibrée pour l'application.
La passerelle fait en outre office de pont entre, d'une part, des protocoles plus simples qui conviennent mieux aux nœuds terminaux contraints en termes de ressources et, d'autre part, les protocoles Internet (IP) utilisés pour fournir les services de niveau IoT (figure 3). Le protocole LoRaWAN prend également en compte les différences de capacité et de profils énergétiques des produits finis par le biais de trois classes d'accès différentes.

Trois classes d'accès différentes

Tous les dispositifs et appareils LoRaWAN doivent pouvoir prendre en charge la classe A. Il s'agit du mode le plus simple, utilisé pour

contribuer à optimiser l'autonomie de la batterie. Cette classe utilise le protocole Aloha largement répandu. Un appareil peut envoyer un message en liaison ascendante vers la passerelle à tout moment ; le protocole intègre des mécanismes anticollision au cas où deux appareils ou plus tenteraient d'envoyer des données en même temps. Une fois la transmission terminée, le nœud d'extrémité attend un message descendant en réponse, qui doit arriver dans l'un des deux intervalles de temps (time slot) disponibles à cet effet. Dès que la réponse arrive, le nœud d'extrémité peut se mettre en veille, ce qui contribue à maximiser son autonomie.

Une passerelle LoRaWAN ne peut pas réveiller un nœud d'extrémité de classe A s'il est en veille : l'appareil doit se réveiller seul. En général, on y parvient en utilisant des temporisateurs locaux ou une activation pilotée par un événement, en général un changement au niveau d'une entrée d'un capteur local.

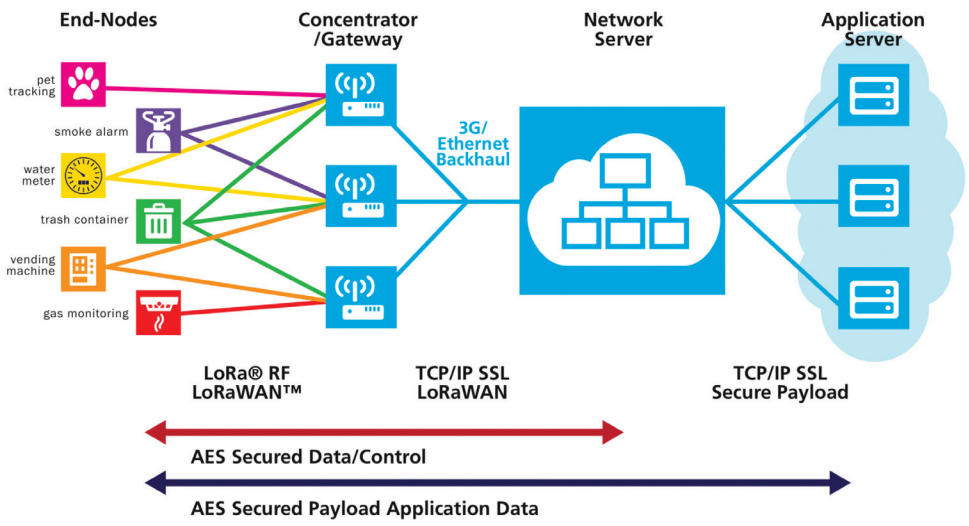
Les actionneurs tels que des vannes dans les systèmes de contrôle de fluides doivent pouvoir recevoir des commandes envoyées par une application réseau, y compris en l'absence de données locales à traiter ou à envoyer. Ces appareils utilisent les modes de classe B ou C. Avec la classe B, chaque appareil se voit affecté un « time slot » au cours duquel il doit actionner son récepteur pour vérifier l'arrivée de messages descendants. Le nœud peut être en veille entre ces intervalles de temps. Les messages en liaison ascendante, quant à eux, peuvent être envoyés à tout moment quand l'appareil n'est pas programmé pour écouter un message descendant. La classe B est en général utilisée quand une latence maximale de plusieurs minutes est tolérée.

La classe C permet des temps de latence bien plus faibles pour les réponses aux messages descendants, du fait que les étages d'entrée du récepteur restent actifs quasiment en permanence. Le seul moment où un appareil de classe C n'est pas en train d'écouter est quand il émet ses propres messages ascendants. Cette classe est en général utilisée par les nœuds d'extrémité raccordés au secteur électrique.

Contrairement à un certain nombre de protocoles utilisables avec les objets connectés, LoRaWAN met en œuvre le chiffrement de bout en bout pour les données de l'application, et ce jusqu'aux serveurs dans le nuage mis en œuvre pour la gestion et la fourniture du service.

4 PRINCIPE ARCHITECTURAL D'UN RÉSEAU LORAWAN EN ÉTOILE

La passerelle fait office de pont entre, d'une part, le protocole LoRaWAN qui convient bien aux nœuds terminaux contraints en termes de ressources et, d'autre part, les protocoles Internet (IP) utilisés pour fournir les services de niveau IoT.



Authentification et identification

Parallèlement au chiffrement de bout en bout, LoRaWAN garantit que tout appareil qui rejoint le réseau possède les autorisations nécessaires et permet aux nœuds du réseau IoT de vérifier qu'ils ne se connectent pas à une passerelle dotée d'une fausse identité. Pour fournir le niveau d'authentification requis, chaque appareil raccordé au réseau LoRaWAN est programmé en usine à l'aide d'une clé unique, qui porte le nom de clé AppKey dans le protocole. L'appareil est également fourni avec un numéro d'identification unique au niveau mondial. Pour que les appareils identifient facilement leurs connexions aux passerelles, chaque réseau possède son propre identifiant, enregistré et géré par la LoRa Alliance.

Des ordinateurs, désignés sous le nom de Join Servers, sont utilisés pour authentifier la clé AppKey de chaque appareil qui veut rejoindre le réseau. Une fois que le Join Server a identifié la clé AppKey, il crée deux clés de session qui sont utilisées pour les transactions qui suivront. La clé NwkSKey est utilisée pour chiffrer les messages servant à contrôler les changements de niveau réseau, tels que ceux utilisés pour paramétrer un appareil sur une passerelle spécifique. La seconde clé, dénommée AppSkey, chiffre toutes les données au niveau application. C'est grâce à cette séparation que les messages de l'utilisateur sont sûrs de ne pas être interceptés ni déchiffrés par un opérateur réseau tierce partie.

Un autre niveau de sécurité est assuré grâce à l'utilisation de compteurs de sécurité intégrés au protocole du message. Les attaques par rejeu, qui consistent pour un hacker à intercepter des paquets de données et à les manipuler avant de les réintroduire dans le flux de données, peuvent ainsi être évitées. Tous les mécanismes de sécurité sont mis en œuvre à l'aide de mécanismes de chiffrement AES, une méthode de chiffrement qui a fait ses preuves avec un haut niveau de sécurité.

En résumé, en prenant en compte des paramètres tels que le besoin d'une large couverture, la consommation énergétique et la sécurité, les développeurs du protocole LoRaWAN se sont assurés que ce protocole constitue le meilleur choix pour créer des réseaux d'objets connectés. ■

(*) Les illustrations sont extraites du livre blanc « Migrating an IoT Sensor to LoRaWAN ».