Sécurité du protocole LoRaWAN

La Revue 3E.I
Culture Sciences de l'Ingénieur

Édité le 11/06/2024

école normale supérieure paris-saclay

Maxime SECHEHAYE[1]

[1] *ENS Paris-Saclay – DER Nikola Tesla*

Cette ressource fait partie du N°112 de La Revue 3EI du 2ème trimestre 2024.

Cette ressource présente les mécanismes de sécurité existants dans le protocole de communication sans fil LoRaWAN. Il ne s'agit pas d'un rapport complet sur le protocole LoRaWAN et de la technologie de modulation LoRa (déjà présentés dans le numéro 96 [5]) qu'il utilise mais plutôt d'un exposé sur les outils mis à disposition par ce protocole pour sécuriser les échanges de données. On insistera ainsi sur les choix importants qu'un développeur d'application IoT souhaitant utiliser LoRaWAN devra effectuer afin d'assurer la sécurité de son application.

Après avoir introduit le protocole LoRaWAN et rappelé son architecture, nous listerons les éléments de sécurité proposés par ce protocole puis nous étudierons dans le détail le mécanisme de connexion d'un nouveau terminal dans un réseau LoRaWAN déjà existant.

1 - Introduction

LoRaWAN est un protocole de communication radio qui permet à différents terminaux d'établir une communication sans fil et de constituer un LPWAN (*Low Power Wide Area Network*, réseau étendu à basse consommation). Ce protocole utilise la technologie de modulation LoRa pour la communication entre les terminaux et les passerelles, d'où son nom.

Sans rentrer dans les détails de fonctionnement de LoRaWAN et de la technologie LoRa, car ce n'est pas l'objectif de cette ressource, nous allons ici brièvement rappeler les éléments d'un tel réseau LoRaWAN.

L'architecture d'un réseau LoRaWAN suit une topologie de réseau en étoile. Les différents éléments de ce réseau sont :

- Les terminaux (*End Devices*) : objets connectés (capteurs, actionneurs…) qui communiquent avec les passerelles en utilisant la technologie de modulation LoRa ;
- Les passerelles (*Gateways*) : appareils faisant le lien entre les terminaux et les serveurs. Les passerelles ne réalisent aucun traitement sur l'information reçue, elles ne servent que de relais ;
- Le ou les serveurs réseau (*Network Server NS*) : pièce centrale du réseau LoRaWAN qui en assure la gestion et qui vérifie l'intégrité des échanges s'y déroulant ;
- Les serveurs d'application (*Application Servers*) : serveurs qui se chargent de traiter l'information envoyée par les terminaux et si nécessaire d'envoyer une réponse.

Sur un **réseau propriétaire**, tous les équipements appartiennent à la même entreprise, dans une zone limitée (une gare par exemple).

Sur un **réseau opéré**, les terminaux appartiennent à une entreprise A et les passerelles et serveurs réseau à un opérateur B. Le serveur d'application peut appartenir à l'entreprise A ou être hébergé dans un datacenter « cloud » C (OVH, AWS, Azure…). Notons que l'entreprise A peut-être un *fournisseur de service, les données appartenant alors à une entreprise D.*

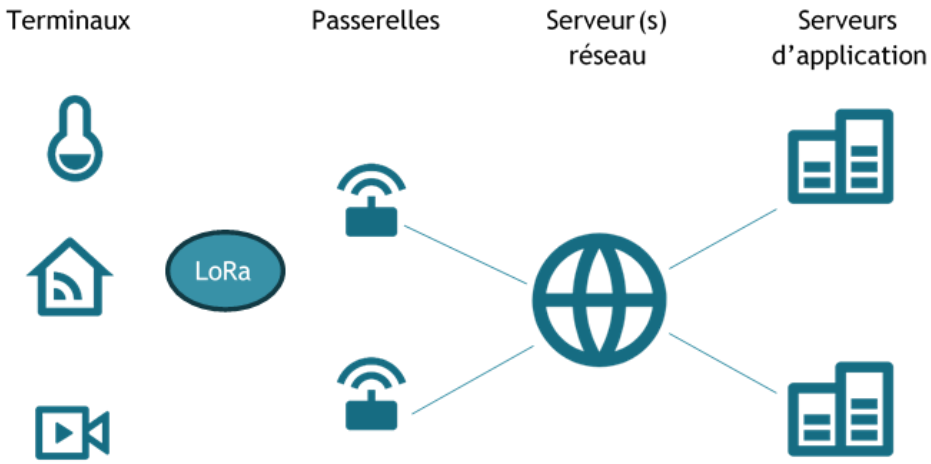

Figure 1 : Schéma de l'architecture d'un réseau LoRaWAN

Il est à noter qu'un terminal n'est pas associé à une unique passerelle. Lorsqu'un terminal souhaite envoyer une information à son serveur d'application, il transmet son message via LoRa et toutes les passerelles à proximité suffisante pour capter ce message le relaieront au serveur réseau. Si le serveur réseau s'aperçoit alors que plusieurs messages identiques arrivent, il n'en gardera qu'un. On a donc une multiplication du message qui permet de réduire la probabilité de devoir l'émettre à nouveau en cas de perte.

LoRaWan ayant une grande portée, « toutes les passerelles à proximité » reçoivent le message signifie que même les messages émis par les terminaux d'un réseau propriétaire sont reçus par les passerelles des opérateurs environnant.

2 - Éléments de sécurité d'un réseau LoRaWAN

Lorsqu'un terminal souhaite envoyer une donnée, son message transitera par au moins trois appareils différents : au moins une passerelle, un serveur réseau et un serveur d'application. Sur un réseau opéré, les 2 premiers appartiennent à l'opérateur, dont on ne maitrise pas la politique de sécurité. Il faut donc que la connexion entre chacun de ces appareils soit sécurisée pour assurer la sécurité de l'ensemble de la chaîne de transmission d'information, tout en restant compatible avec la faible consommation souhaitée et la faible puissance des processeurs.

Voici les éléments de sécurité présents dans le réseau LoRaWAN qui permettent d'augmenter la sécurité des communications établies :

- Des clés de sécurité sont générées et utilisées pour chiffrer les communications depuis les terminaux jusqu'aux serveurs d'application grâce à l'algorithme *AES-128* mais aussi pour vérifier qu'une trame n'a pas été altérée entre son émission et sa réception. Ces clés de sécurité servent donc à assurer l'intégrité et la confidentialité des échanges. Nous reviendrons en détail sur l'établissement et l'utilisation de ces clés de sécurité.
- Deux compteurs de trames (*Frame Counter*) sont utilisés lors de chaque nouvelle connexion entre le terminal et le réseau LoRaWAN et s'incrémentent chaque fois qu'un message ascendant est envoyé (depuis le terminal) ou bien chaque fois qu'un message descendant est envoyé (vers le terminal). On ne peut donc pas retransmettre une trame déjà envoyée.

3 - Établissement d'une connexion sécurisée sur LoRaWAN

Nous allons ici décrire le processus d'établissement d'une connexion sécurisée sur LoRaWAN. Comme expliqué précédemment, ce sont les clés de sécurité qui permettent d'assurer la confidentialité et l'intégrité des messages échangés. Il faut donc s'assurer que l'établissement et le partage de ces clés soient sécurisés.

Il existe deux types d'ajout d'un nouveau terminal sur un réseau LoRaWAN :

- L'activation sans fil (*Over The Air activation*, *OTAA*) où toutes les données liées à la sécurité des communications futures sont établies de manière sans fil entre le serveur du réseau (NS) et le terminal lors de l'établissement de la connexion.
- L'activation par personnalisation (*Activation By Personalization*, *ABP*) où toutes les données liées à la sécurité sont déjà stockées sur le terminal et le réseau LoRaWAN avant les premiers échanges.

Avec la méthode ABP, les mêmes clés de sécurité sont donc utilisées à chaque session et il faut les changer manuellement si besoin. C'est donc la méthode la moins sécurisée des deux.

On va donc s'intéresser ici à l'activation sans fil qui est la méthode d'activation la plus sécurisée.

4 - Activation sans fil d'un nouveau terminal sur LoRaWAN

Avant l'activation, le terminal doit posséder les informations suivantes :

- DevEUI : identifiant unique sur 64 bits attribué dès la fabrication, similaire à une adresse MAC
- AppEUI : identifiant unique d'une application sur le réseau LoRaWAN considéré, sur 64 bits et modifiable
- AppKey : clé sur 128 bits partagée par le terminal et le serveur réseau

La clé AppKey est spécifique à chaque nouveau terminal sur le point de rejoindre un réseau LoRaWAN. Elle n'est *jamais transmise sur le* réseau LoRaWAN pour des raisons évidentes de sécurité et doit donc être transmise entre le terminal et le serveur réseau par un moyen extérieur (provisionnement physique, connexion sécurisée HTTPS…)

4.1 - Demande de connexion (*Join Request*)

Comme son nom l'indique, la première étape consiste à une demande de connexion du terminal au serveur. Cette demande contient :

Le *DevNonce* est un nombre aléatoire et unique. En effet, le serveur réseau conserve les *DevNonce* précédemment utilisés par chaque terminal et rejette toutes les demandes de connexion avec un *DevNonce* déjà utilisé. Cela empêche les attaques par rejeu.

Il y a aussi un *Message Integrity Code (MIC)* qui est calculé à partir des trois champs et de l'AppKey. Il permet de s'assurer, comme son nom l'indique, de l'intégrité du message reçu et de s'assurer de l'expéditeur du message.

Le MIC est systématiquement le résultat d'un chiffrement CMAC-AES sur 128 bits sur les données du message et avec AppKey

La demande de connexion n'est pas chiffrée car elle ne contient pas d'information sensible

4.2 - Acceptation de connexion (Join Accept)

Ce message est envoyé par le serveur réseau au terminal. Il contient les champs suivants :

On va rapidement expliquer ces différents champs :

- AppNonce : Nombre aléatoire fournie par le serveur réseau
- NetID : Ses 7 bits de poids les plus forts représentent l'identifiant du réseau (NwkID) qui est unique dans une zone géographique donnée. Les autres bits donnent l'adresse du terminal dans le réseau.
- DevAddr : Adresse attribuée par le serveur réseau au terminal (similaire à une adresse IP sur un réseau local qui serait fournie par un serveur DHCP)
- DLSettings : Paramètres à utiliser par le terminal pour le *downlink* (lorsque le terminal va recevoir des messages du serveur réseau)
- RXDelay : Délai entre l'émission d'un message par le serveur réseau et le début de sa réception par le terminal
- CFList (optionnel) : Fréquences de canaux autorisées pour les communications entre le terminal et les passerelles

On calcule de nouveau un MIC et cette fois les données sont chiffrées à l'aide d'AppKey pour les protéger

4.3 - Calcul des clés de session

Le serveur réseau et le terminal peuvent alors tous les deux calculer les clés spécifiques à cette nouvelle session : NwkSKey (*Network Session Key*) et AppSKey (*Application Session Key*).

NwkSKey est utilisée pour calculer le MIC des messages mais aussi pour chiffrer les commandes MAC (*Medium Access Control*). Ces commandes sont uniquement entre le serveur réseau et le terminal et permettent de configurer et de contrôler le comportement de ce terminal LoRaWAN. La demande de connexion est un exemple de commande MAC.

AppSKey permet quant à elle de déchiffrer les données (*payload*) des messages entre le terminal et le serveur d'application.

Le serveur réseau conserve donc la clé NwkSKeyet transfère la clé AppSkey au serveur d'application. Comme le lien entre le serveur réseau et le serveur d'application peut être réalisé via n'importe quel protocole de communication, il faut s'assurer que la connexion entre ces deux serveurs soit sécurisée.

Les formules pour obtenir ces deux clés sont les suivantes :

NwkSkey = aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce | pad16)

AppSkey = aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce | pad16)

Où *pad16* signifie qu'on ajoute le nombre de zéros suffisant pour que le message chiffré avec la clé AppKey ait une taille de 16 octets.

On retrouve dans ces formules, entre autres, des données envoyées par le serveur réseau dans le message d'acceptation de connexion, ce qui justifie le chiffrement de ce dernier.

4.4 - Le terminal est intégré au réseau LoRaWAN

Maintenant que le terminal est intégré au réseau LoRaWAN, il devra garder pour cette session :

- DevAddr qui lui permet de s'identifier sur ce réseau
- NwkSKey utilisée pour calculer le MIC des messages ainsi que pour chiffrer les messages MAC
- AppSKey utilisée pour chiffrer les données utiles envoyées au serveur d'application

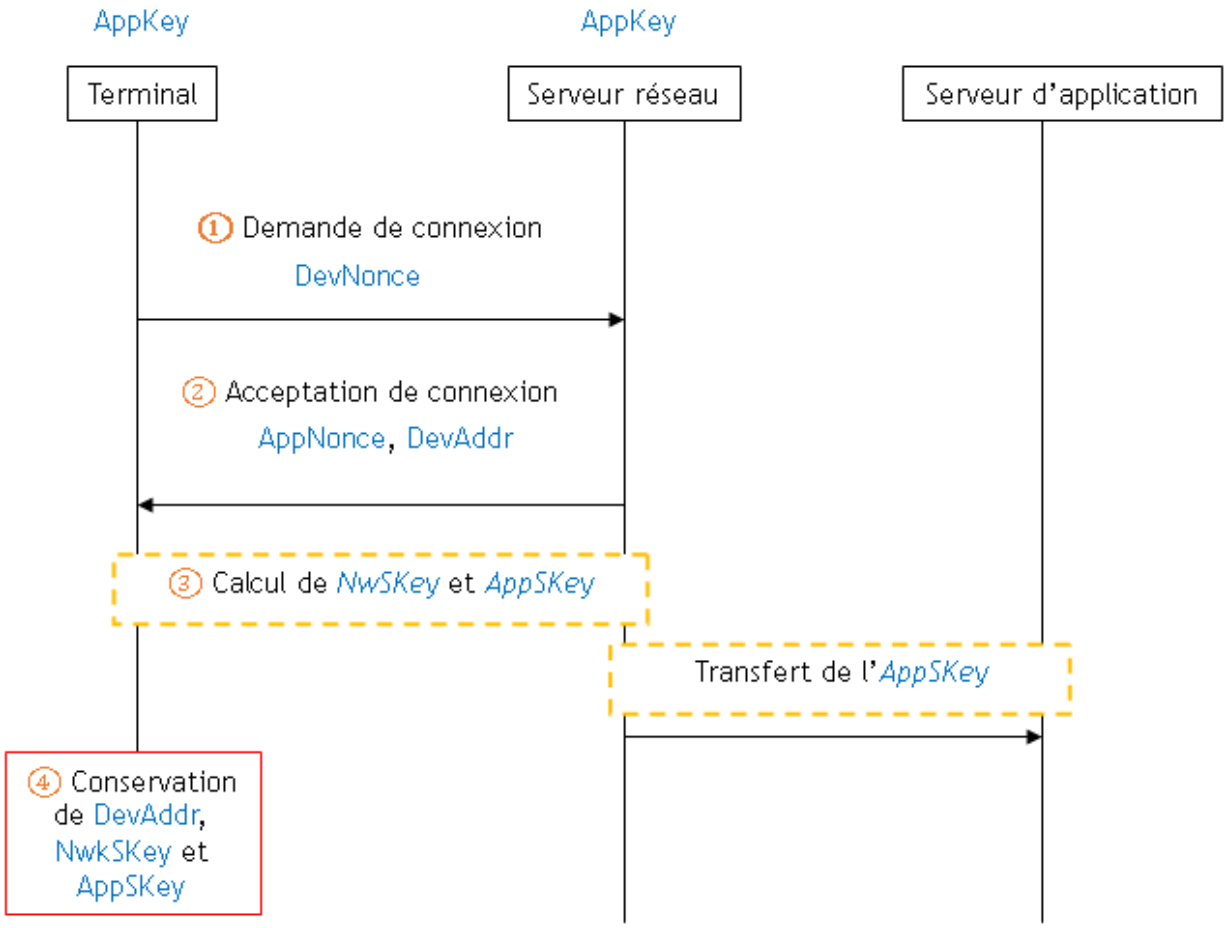

Figure 2 : Diagramme résumant les différentes étapes de l'activation sans fil d'un terminal sur un réseau LoRaWAN

5 - Différences entre LoRaWAN 1.0 et LoRaWAN 1.1

Dans LoRaWAN 1.1, tout ce qui a été exposé précédemment reste valable mais il y a quelques ajouts.

Il y a des améliorations dans la sécurité (changement du Devnonce en compteur, …).

Enfin, il y a davantage de clés de session qui permettent de déléguer au réseau visité certaines fonctions et de piloter le terminal quand le terminal est en roaming.

6 - Conclusion

Nous avons observé que le protocole LoRaWAN propose une architecture séparant les informations liées au réseau de celles liées à l'application spécifique. Pour cela, deux serveurs distincts sont utilisés dans une session : le serveur réseau et le serveur d'application. Il y aura donc une sécurité liée au serveur réseau et une autre liée au serveur d'application.

Ce protocole propose deux méthodes d'activation d'un nouveau terminal mais seule l'activation sans fil permet d'établir une session sécurisée car elle permet la création de nouvelles clés spécifiques à chaque session.

Enfin, le protocole LoRaWAN propose un mécanisme de génération et d'approvisionnement des clés de session à partir d'une clé spécifique au terminal considéré, la clé *AppKey*. Ce mécanisme est assez simple et semble sécurisé dès lors que les messages sont chiffrés, comportent un code d'intégrité ainsi qu'un compteur de trames pour éviter des attaques par rejeu.

Cependant, cette sécurité repose sur une unique clé : la clé AppKey. Ce sera toujours cette même clé qui sera utilisée lors de toute nouvelle session démarrée par le terminal considéré. Il faut donc s'assurer que cette clé est stockée de manière sécurisée et que son partage avec le serveur réseau est aussi sécurisé. Le protocole LoRaWAN n'indique rien à ce sujet, c'est à la responsabilité de l'utilisateur de ce protocole de s'assurer de la sécurité de l'approvisionnement de l'AppKey. Il en est de même pour le transfert de la clé AppSKey du serveur réseau au serveur d'application.

Voici un extrait de la spécification de LoRaWAN 1.1 [2] à ce propos :

> *Secure provisioning, storage, and usage of root keys NwkKey and AppKey on the end device and the backend are intrinsic to the overall security of the solution. These are left to implementation and out of scope of this document.*

Le protocole LoRaWAN propose donc des mécanismes de sécurité classiques et efficaces à condition d'utiliser les bonnes méthodes et d'assurer la sécurité des éléments non pris en charge par le protocole.

Références :

[1]: *LoRaWAN Specification*, LoRa Alliance Technical Committee, 2015

[2]: *LoRaWAN 1.1 Specification*, LoRa Alliance Technical Committee, 2017

[3]: *LoRaWAN Security, Full end-to-end encryption for IoT application providers*, Gemalto, Actility, Semtech, 2017

https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf

[4]: *End Device Activation*, The Things Network

https://www.thethingsnetwork.org/docs/lorawan/end-device-activation/

[5]: Réseaux très basse consommation, longue portée, bas débit, l'exemple de LoRaWAN, A. Juton, septembre 2019, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/reseau-tres-basse-consommation-longue-portee-bas-debit-exemple-lorawan