



IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille



Approche légère et sécurisée de mise à jour de firmware dans les WSN

Edmond-P. Souapiebe

Université de Lille / IMT Nord Europe
Université de Mons / Polytech Mons

2 juillet 2026

Une question...

Imaginez que vous soyez l'auteur d'un livre de 200 pages. Après l'impression et la publication de ce dernier, vous découvrez quelques erreurs à la page 173 ?



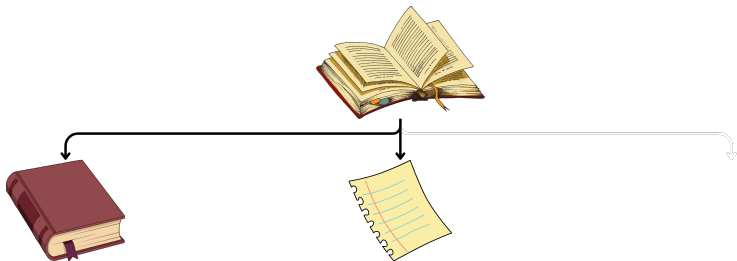
Quelle approche d'impression vous convient ?



Réimprimer tout le livre

- Simple à réaliser
- Nécessite plus de ressources

Quelle approche d'impression vous convient ?



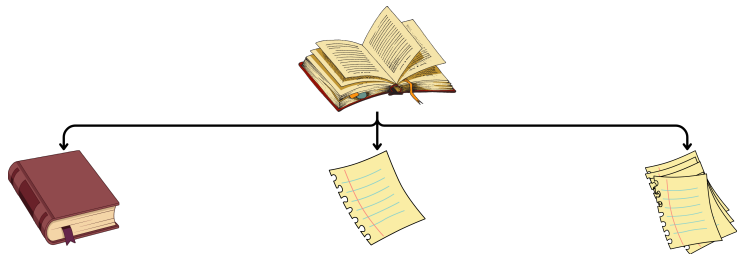
Réimprimer tout le livre

- Simple à réaliser
- Nécessite plus de ressources

Imprimer la page 173

- Très rapide
- Économise en ressources
- Dépend de la version

Quelle approche d'impression vous convient ?



Réimprimer tout le livre

- Simple à réaliser
- Nécessite plus de ressources

Imprimer la page 173

- Très rapide
- Très économique en ressources
- Dépend de la version

Imprimer le chapitre

- Moyennement rapide
- Ne dépend pas de la version
- Possible de réimprimer tout le livre

Ces approches correspondent à trois grandes familles de mises à jour utilisées dans les réseaux IoT.

Contexte

❶ Pourquoi faire la mise à jour ?

- Ajouter de nouvelles fonctionnalités ;
- Corriger les bugs ;
- Corriger les failles de sécurité ;
- Améliorer les performances du système.



❷ Plusieurs contraintes peuvent se poser

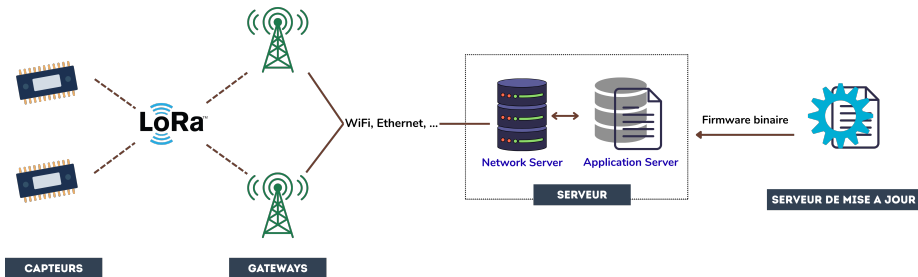
- Accès difficile
- Noeuds sur batteries
- Très faible espace de stockage
- Instabilité de la connection avec le noeud
- Inefficacité/Coût très élevé des technologies non LPWANs

Importance des méthodes légères et sécurisées pour une mise à jour efficace des noeuds contraints

Processus de mise à jour FUOTA

(Firmware Update Over The-Air)

Processus de mise à jour FUOTA

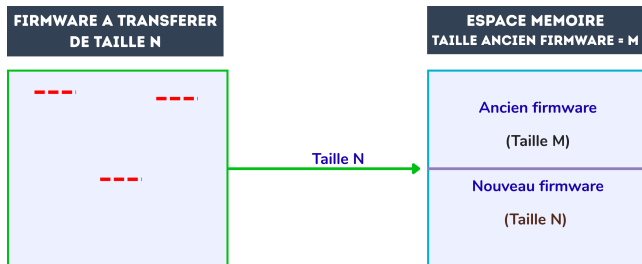


Étapes d'une mise à jour FUOTA

- Création du nouveau firmware.
- Préparation de la mise à jour.
- Transmission du firmware via **LoRaWAN**.
- Réception et reconstruction du firmware par le capteur.
- Installation de la nouvelle version.

Quelques approches de mise à jour FUOTA

Principales approches de mise à jour FUOTA

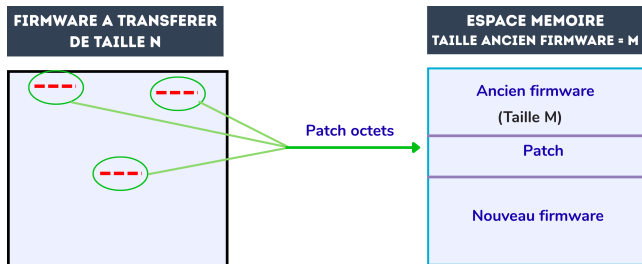


Mise à jour complète

- Solution simple à implémenter
- Temps de mise à jour très long
- Forte consommation d'énergie
- Nécessite un plus grand espace de stockage

Simple... mais très coûteuse

Principales approches de mise à jour FUOTA

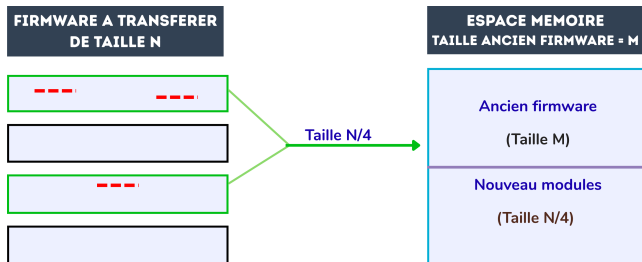


Mise à jour différentielle

- Seules les différences entre l'ancien et le nouveau firmware sont transmises
- Nombre de paquets très réduit
- Dépend de la version du firmware et de l'architecture du microcontrôleur
- Nécessite une mémoire pouvant contenir l'ancien firmware, le nouveau et le patch

Très efficace... mais fortement dépendante des versions

Principales approches de mise à jour FUOTA



Mise à jour modulaire

- Indépendant de l'architecture du microcontrôleur
- Indépendant des versions déployées
- Maintient la continuité du service
- Faible optimisation de la taille des données transférées si tous les modules sont concernés par la mise à jour

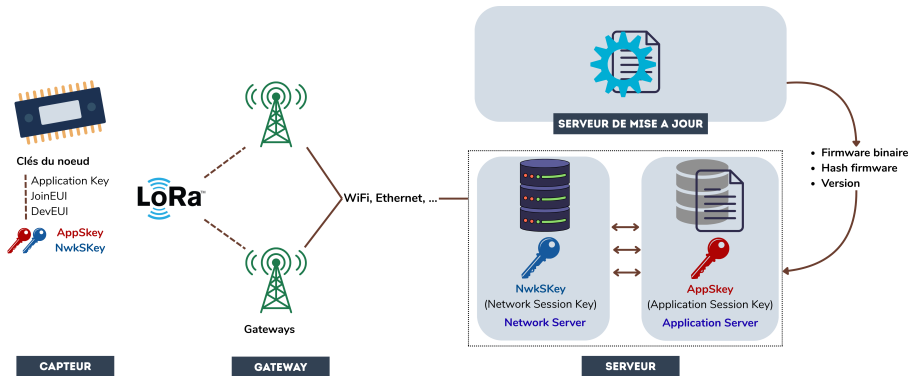
Flexible... mais peu optimale lorsque beaucoup de modules changent.

Synthèse des principales approches de FUOTA

Auteur(s)	Année	Approche	Objectif principal
FUOTA (LoRa Alliance)	2018	FUOTA standard	Standardiser les mises à jour OTA des dispositifs LoRaWAN.
Ruckebusch et al.	2018	État de l'art des méthodes de mise à jour	Classier les différentes approches de mise à jour de firmware.
De Simone et al.	2025	Bpatch	Réduire la taille des mises à jour grâce aux patches différentiels.
Sun et al.	2023	FLoRa	Améliorer l'efficacité énergétique et la fiabilité des mises à jour.
Nguyen et al.	2024	FUOTA modulaire	Permettre des mises à jour modulaires sans redémarrage.
Nguyen et al.	2025	FUOTA modulaire avec multicast	Réduire la consommation d'énergie grâce au multicast tolérant aux interruptions.
Heeger et al.	2021	FUOTA sécurisé avec ADR	Optimiser les mises à jour sécurisées par adaptation dynamique du débit.
Victor et al.	2024	Combinaison Unicast/Broadcast	Accélérer les mises à jour OTA par diffusion hybride.
Clément et al.	2026	FUOTA ciblé et automatisé	Optimiser le temps de mise à jour et la consommation d'énergie.

Table – Synthèse des principales approches de FUOTA.

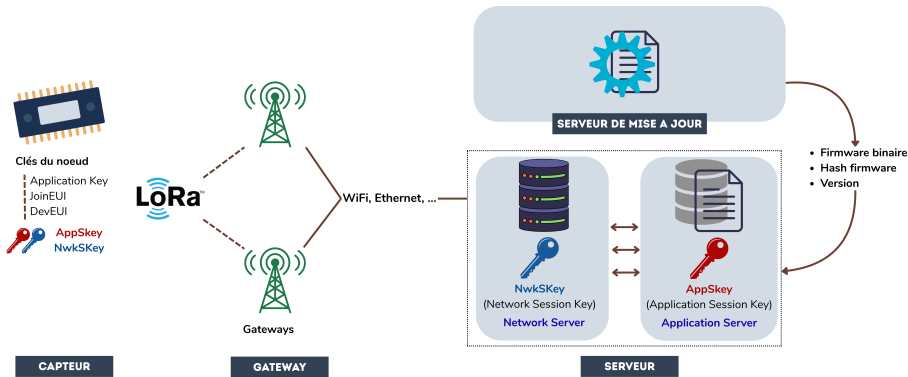
Niveaux de sécurité dans le processus de mise à jour FUOTA



Mécanismes de sécurité utilisés

- **NwkSKey** → Authentification et intégrité côté **Network Server**
- **AppSKey** → Chiffrement côté **Application Server**
- **Hash du firmware** → Intégrité côté **FUS**

Niveaux de sécurité dans le processus de mise à jour FUOTA



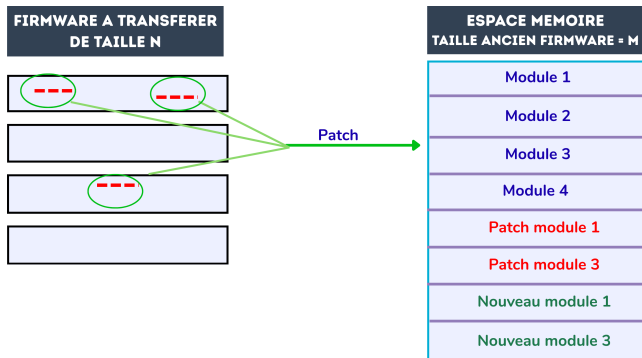
Mécanismes de sécurité utilisés

- **NwkSKey** → Authentification et intégrité côté **Network Server**
- **AppSKey** → Chiffrement côté **Application Server**
- **Hash du firmware** → Intégrité côté **FUS**

Ces mécanismes protègent la transmission, mais le capteur ne peut pas vérifier directement que le firmware provient bien de son constructeur.

Pistes de recherches

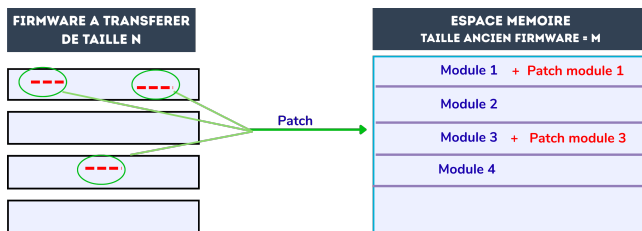
Pistes de recherches : modulaire + différentielle



Combiner modulaire et différentielle

- Uniquement le patch est transmis
- Patch calculé pour chaque module
- Indépendant des versions déployées
- Indépendant de l'architecture
- Assure la continuité du service

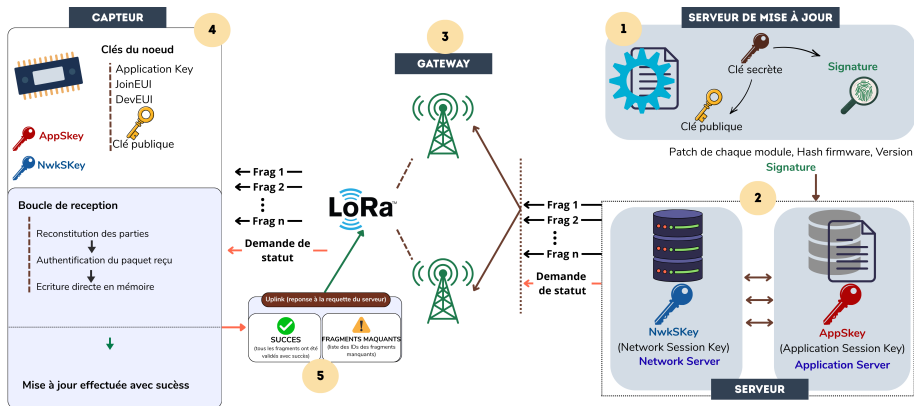
Pistes de recherches : Mise à jour à la volée



Technique d'écriture en mémoire

- Proposer une mise à jour à la volée
- Authentification de chaque paquet
- Écriture directe en mémoire
- Pas de mémoire supplémentaire nécessaire

Pistes de recherches : Authentification de bout en bout



Intégrer une authentification du constructeur du firmware au capteur

Notre objectif est donc de lever les principales limitations identifiées dans les approches actuelles.

- **Piste 1 :** **Modulaire + Différentiel** → Permet de :
 - Taille très faible des paquets
 - Mise à jour indépendante de la version
 - Mise à jour des noeuds hétérogènes
- **Piste 2 :** **Mise à jour à la volée**
- **Piste 3 :** **Authentification du constructeur** → Ajouter une couche de sécurité permettant au capteur d'authentifier son constructeur