Université de Mons
Faculté des Sciences
Département d'Informatique
Réseaux et Télécommunications

Conception et évaluation d'une architecture hybride de réseaux de capteurs reposant sur les technologies radio LoRa et IEEE 802.15.4

Directeur : Mr Bruno QUOITIN

Rapporteurs : Mr Prénom NOM
Mr Prénom NOM

Mémoire réalisé par
Arnaud PALGEN

en vue de l'obtention du grade de
Master en Sciences Informatiques

UMONS
Université de Mons

Faculté
des Sciences

Année académique 2020-2021

Remerciements

Nous remercions ...

Table des matières

Table des figures

Chapitre 1

Etat de l'art

1.1 Projets similaires

1.2 LoRa

LoRa (Long Range) [6][7] est une technologie radio fonctionnant sur une modulation propriétaire détenue par Semtech et basée sur *chirp spread spectrum (CSS)*. Cette modulation consiste en un signal d'une amplitude constante pour lequel la fréquence diminue ou augmente au cours du temps. Ces variations qui sont pour LoRa linéaires, sont respectivement appelées *downchirp* et *upchirp*. Cette modulation permet d'obtenir des communications longues portées et basses énergie.

Une communication LoRa dépend des paramètres suivants :

- **Spreading Factor (SF)** est une variable qui définit la vitesse de balayage du signal radio (Fig 1.1). Le spreading factor est compris entre 7 et 12. Plus sa valeur est grande, plus la vitesse de balayage est petite. Ceci implique un signal plus facile à décoder, mais avec un débit de données plus faible. Donc, inversement à une petite valeur de SF, une grande valeur de SF a un débit plus faible et une QoS (Quality of Service) plus élevée.
- **Bandwidth (BW)** détermine la largeur de la bande passante. Une bande passante plus large augmente la qualité du signal. Pour LoRa, en Europe, les valeurs de BW sont limitées à 125 KHz et 250KHz [8].
- **Coding rate (CR)** détermine la quantité de bits redondants ajoutés par le codage d'erreur cylique utilisé par LoRa pour la détection et la correction d'erreurs. Cette méthode de correction d'erreur permet au signal de supporter de courtes interférences. Ainsi il possible de coder des données de 4 bits avec des redondances de 5, 6, 7 ou 8

bits. La valeur du CR se note donc 4/5, 4/6, 4/5 ou 4/8.

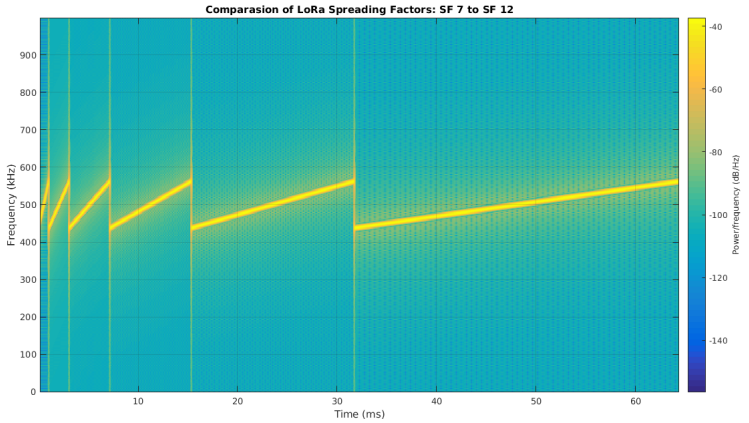


FIGURE 1.1 – Spectogramme des différents Spreading Factors [1].

Le format des paquets LoRa (Fig. 1.2) peut être explicite ou implicite. Dans le mode implicite, le header n'est pas inclus dans le paquet. Pour cela, la taille de la payload, le coding rate et la présence de la Payload CRC doivent être configurés. Ce mode permet de réduire la taille du paquet et donc du temps de transmission.

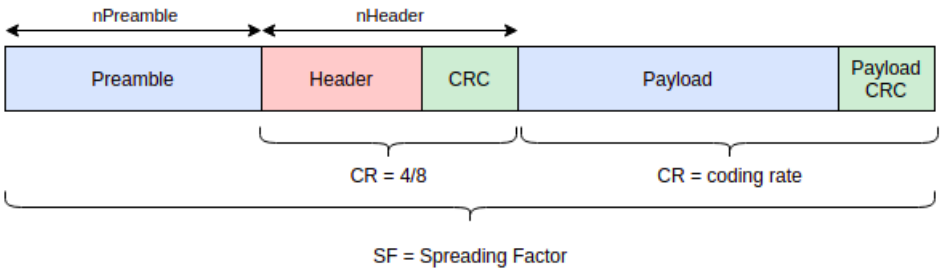


FIGURE 1.2 – Format d'un paquet LoRa.

La datasheet du SX1276 intégré dans le RN2383, utilisé comme transceiver LoRa pour ce projet (c.f. 2.5), définit le temps d'émission d'un paquet LoRa reprit par l'équation 1.1.

$$T_{frame} = T_{preamble} + T_{payload} \tag{1.1}$$

Où $T_{preamble}$ et $T_{payload}$ sont respectivement le temps d'émission du preamble et du payload définis aux équations 1.2 et 1.3.

$$T_{preamble} = (n_{preamble} + 4,25)T_{sym} \tag{1.2}$$

$$T_{payload} = n_{payload} * T_{sym} \tag{1.3}$$

Où $T_{sym} = \frac{1}{R_s}$, $n_{preamble}$ et $n_{payload}$ sont le nombre de symboles du preamble et du payload. $n_{preamble}$ est une valeur paramétrable du module radio et $n_{payload}$ est défini par l'équation 1.4.

$$n_{payload} = 8 + max\left(ceil\left[\frac{8PL - 4SF + 28 + 16CRC - 20IH}{4(SF - 2DE)}\right](CR + 4), 0\right) \tag{1.4}$$

où :

- PL est le nombre d'octets de la payload (1 à 255)
- $IH = 0$ si le header est présent, $IH = 1$ sinon
- $DE = 1$ si $LowDataRateOptimize = 1$, $DE = 0$ sinon. $LowDataRateOptimize$ permet d'optimiser la robustesse d'une transmission quand celle-ci est longue.
- CR prend la valeur 1 pour 4/5, 2 pour 4/6, etc

1.3 IEEE 802.15.4e

802.15.4 est un protocole défini par IEEE en 2003. Il est destiné aux communications à faible débit réalsisées par des dispositifs ayant une alimentation en énergie limitée. Ce protocole qui est un standard pour les réseaux PANs (Personal Area Networks) couvre la couche physique et MAC du modèle OSI. En 2012, IEEE 802.15.4e a été défini pour palier certains problèmes de IEEE 802.15.4.

Types de noeuds et topologie

Cette norme définit deux types de noeuds : les Full Function Devices (FFD) qui peuvent être des coordinateurs de PAN, de simple coordinateurs ou de simple noeuds et les Reduced Function Devices (RFD) qui utilisent une implémentation réduite du protocole et ne peuvent être que de simples noeuds.

Ces noeuds peuvent former des réseaux suivantes plusieurs topologies comme la topologie en étoile pour laquelle plusieurs RFD sont connectés à un FFD qui joue le rôle de coordinateur ou encore la topologie peer-to-peer pour laquelle les FFD sont connectés les uns aux autres.

Modes d'accès

La norme 802.15.4 définit en 2003 fournit deux modes d'accès : Beacon Enabled mode et Non-Beacon Enabled mode. Dans le premier, le réseau est synchronisé par des messages de contrôles (beacons) et une structure appelée Superframe.

Comme l'illustre la figure 1.3, Cette Superframe est divisée en deux périodes : la période active et la période inactive. La période active est elle-même divisée en deux périodes : contention acces period (CAP) et contention free period (CFP). Dans la première, l'accès au canal se fait par l'algorithme slotted CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance).

Dans la deuxième, l'accès au canal se fait par TDMA (Time Division Multiple Access). C'est à dire que les 7 slots de cette période sont attribués par le coordinateur aux noeuds ayant émis une requête durant la CAP pour l'utilisation d'un slot.

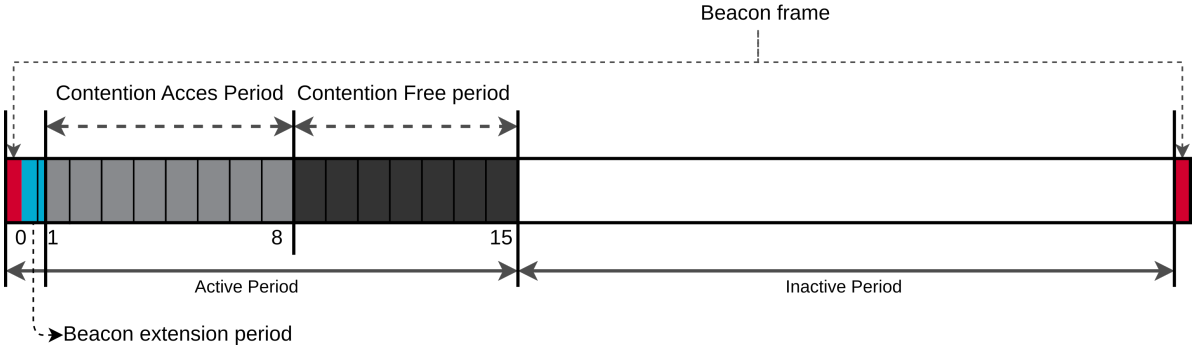


FIGURE 1.3 – 802.15.4 structure de la Superframe.

Dans le mode Non-Beacon Enabled, il n'y a pas de synchronisation. l'accès au canal se fait par l'algorithme Unslotted CSMA-CA.

Ces modes d'accès ont un certains nombres de limitations discutées dans l'article de Domenico De Guglielmo et ses co-auteurs [9] :

- Aucune garantie sur le délai maximal pour qu'un paquet puisse atteindre sa destination ne peut être fourni avec l'algorithme CSMA-CA.
- La fiabilité des communications est limitée par l'utilisation de l'algorithme slotted CSMA-CA qui offre un taux de transmission faible.
- Aucune protection contre les interférences en raison de l'utilisation d'un seul canal et en l'absence de mécanismes de sauts de fréquence (frequency hopping)

Ces limitations ont menés à la création de 802.15.4.e en 2012 qui redifinit les protocoles MAC du standard. Ainsi, 5 modes de fonctionnement de la couche

MAC sont introduits :

1. Time Slotted Channel Hopping (TSCH)
2. Deterministic and Synchronous Multi-channel Extension (DSME)
3. Low Latency Deterministic Network (LLDN)
4. Asynchronous multi-channel adaptation (AMCA)
5. Radio Frequency Identification Blink (BLINK)

D'après l'article de Domenico De Guglielmo et ses co-auteurs [9], le standard ne définit que brièvement AMCA et BLINK. LLDN est destiné aux réseaux à un seul saut et utilisant un seul canal. Il n'est donc pas pertinent pour ce projet. DSME utilise le concept de multi-superframe semblable aux superframes de IEEE 802.15.4 mis à part la CFP qui divise chacun des 7 slots en plusieurs fréquences.

TSCH (Time Slotted Channel Hopping)

Ce mode de fonctionnement de la couche MAC, comme son nom l'indique, supporte à la fois les sauts en fréquence et des communications divisées en temps. Ces mécanismes réduisent efficacement les effets des interférences et les collisions ce qui améliore la fiabilité du réseau.

Slotframe

Dans ce mode, le concept de superframe de 802.15.4 est remplacé par le concept de slotframe. Une slotframe est un intervalle de temps qui est divisé en timeslots et se répète infiniment. Chaque timeslot permet à un noeud d'envoyer une trame et d'éventuellement recevoir son acquitement (ACK). Chaque timeslot possède un identifiant appellé *Absolute Slot Number* (ASN) et un identifiant au sein de la slotframe appelé *Time Slot Number* (TSN).

TSCH permet l'utilisation de timeslots partagés et dédiés. Dans les timeslots partagés plusieurs noeuds peuvent communiquer. Dans ce cas, CSMA/CA est utilisé. Pour les timeslots dédiés, seuls deux noeuds peuvent communiquer. La figure 1.4 illustre une slotframe composée de trois timeslots. Dans cet exemple, on considère 3 noeuds : N, T et U. Chaque timeslot permet une communication entre deux noeuds. Par exemple le timeslot ayant comme TSN 0, permet à N de transmettre vers T.

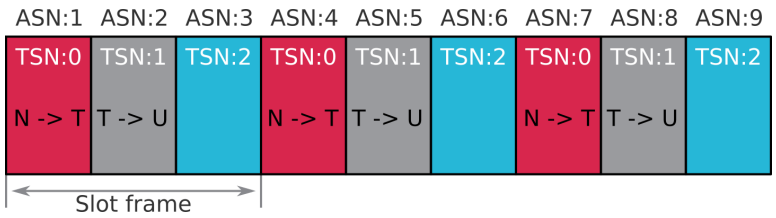


FIGURE 1.4 – Exemple de Slotframe.

Channel Hopping

TSCH peut utiliser 16 canaux différents. Un lien entre deux noeuds dans TSCH est alors défini par la paire (timeslot, canal). Ainsi, chaque slotframe est divisée par le nombre de canaux utilisés dans le réseau (Fig. 1.5). La fréquence f utilisée pour la communication entre deux noeuds est calculée comme suit :

$$f = F[(ASN + channelOffset)\%N_{channels}]$$

où $N_{channels}$ est le nombre de canaux utilisés pour le réseau et F peut être vue comme une table qui contient une permutation pseudo-aléatoire de canaux.

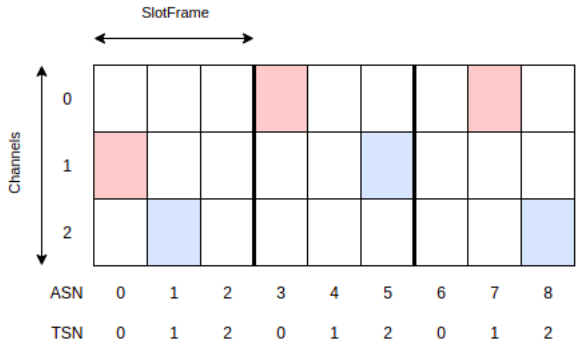


FIGURE 1.5 – Time Slotted Channel Hopping.

1.4 RPL

Routing Protocol for Low-Power and Lossy Networks [10] est un protocole de routage IPv6 destiné aux réseaux dont les noeuds sont contraints en énergie et dont les liens sont soumis à des pertes importantes de paquets (Low-power and Lossy Networks, LLNs).

D'après l'article de Tripathi, Oliveira et Vasseur [11], après avoir été étudiés par le groupe de travail IETF roll (Routing Over Low power and Lossy networks), il s'est avéré que les protocoles tel que OSPF, AODV ou OLSR ne satisfont pas toutes les exigences des LLNs. C'est pour cette raison que ce groupe de travail a introduit RPL. Ce protocole à vecteur de distance est un protocole proactif, c'est à dire que les routes sont établies avant qu'elles ne soient nécessaires.

RPL sépare le traitement et la transmission des paquets de contrôle de l'optimisation de l'objectif de routage. Cela permet de l'adapter à un large éventail d'applications des LLNs comme la domotique, l'automatisation industriel ou encore la récolte de données dans divers environnements.

Cette section décrit le fonctionnement de RPL. Cette description est basée sur le RFC 6550 [10].

Topologie

RPL construit un DODAG (Destination Oriented Directed Acyclic Graph) qui est un graphe dirigé acyclique (DAG) ayant une seule racine (Fig. 1.6). De par cette architecture RPL est adapté aux applications de collecte de données ce qui est le principale objectif de ce projet. En effet, la route d'un noeud à la racine est facilement établie car tous les noeuds du chemins envoient les données à leur parent.

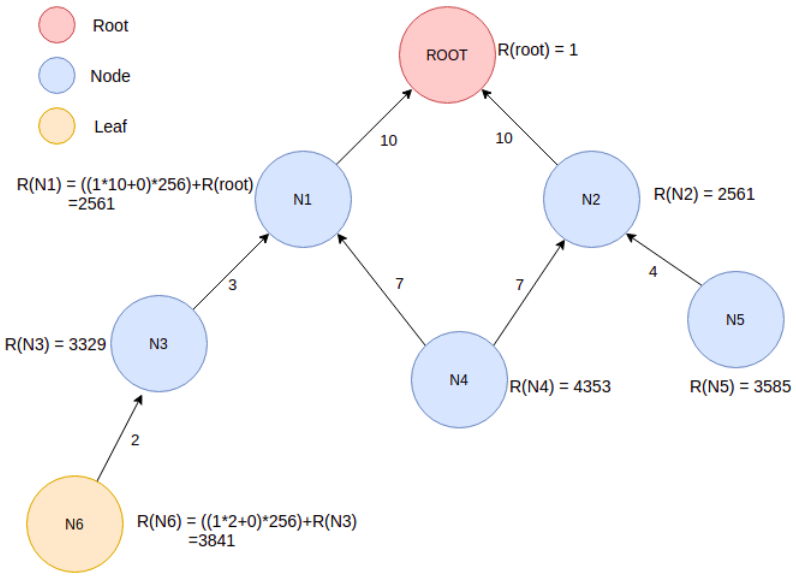


FIGURE 1.6 – DODAG.

Fonctions objectif

Une fonction objectif (OF) définit comment plusieurs métriques sont utilisées pour calculer le rang d'un noeud. Celui-ci détermine la position du noeud dans le DODAG par rapport aux autres noeuds. Le rang augmente strictement dans le sens descendant et diminue strictement dans le sens montant. Ainsi, pour un noeud n, la propriété $rang(n) > rang(parent(n))$ est toujours vérifiée. La figure 1.6 illustre un DODAG avec des valeurs de rang calculées avec la fonction objectif OF0, ses paramètres par défaut et des coûts de liens attribués administrativement. Sur cet exemple, la racine du DODAG a comme rang, la valeur par défaut ROOT_RANK = 1 définie dans le RFC 6550.

Les fonctions objectif OF0 et MRHOF, implémentées dans Contiki, sont décrites sur base du RFC 6552 [12] et du RFC 6719 [13].

OF0

Objective Function Zero est une fonction dont l'objectif est de choisir un parent qui permettra à un noeud d'être le plus proche possible la racine du DODAG. Le calcul du rang d'un noeud N, $R(N)$, est décrit par l'équation 1.5. Il est calculé pour chaque parent potentiel. Le parent préféré choisi sera alors le parent potentiel qui implique le plus petit $R(N)$.

Le calcul du rang commence par le calcul de la variable *step_of_rank*

(Sp) qui est basée sur les propriétés et métriques du lien avec le parent potentiel. Le RFC recommande de baser ce calcul sur des propriétés dynamiques comme la métrique *expected transmission count (ETX)* décrit dans l'article de Couto, Aguayo, Bicket et Morris [14], qui est une métrique qui permet de minimiser le nombre de transmissions requises pour transmettre un paquet. L'utilisation de propriétés dynamiques est recommandée car utiliser des propriétés statiques, comme un coût administratif, revient à avoir un rang analogue au nombre de sauts.

Sp est ensuite mutlipliée par la variable *rank_factor* (Rf) qui est utilisée pour multiplier son effet dans le calcul de *rank_increase*. Rf doit être un entier strictement positif et sa valeur par défaut est 1.

Sr est un terme plus petit ou égal à la variable *stretch_of_rank* qui est l'augmentation maximum de *step_of_rank* avec le parent.

La variable *rank_increase* est finalement multipliée par le facteur *MinHopRankIncrease* qui est défini par le RFC 6550 [10] comme l'augmentation minimum du rang entre un noeud et n'importe lequel de ses parents. Sa valeur par défaut est DEFAULT_MIN_HOP_RANK_INCREASE qui a une valeur de 256.

Le calcul du rang est la somme du rang du parent potentiel P, $R(P)$, et de *rank_increase*.

$$\begin{aligned} rank\_increase &= (Rf * Sp + Sr) * MinHopRankIncrease \\ R(N) &= R(P) + rank\_increase \end{aligned} \tag{1.5}$$

MRHOF

Minimum Rank with Hysteresis Objective Function est une fonction dont l'objectif est de sélectionner les routes qui minimisent une métrique additive en utilisant l'hystérésis pour réduire les changements de parents en réponse a de petites variations de la métrique.

Pour cela, un noeud va calculer le coût des chemins avec chaque candidat parent. Ce coût sera la somme de deux éléments :

- La valeur de la métrique utilisée contenue dans les DIOs d'un candidat parent
- La valeur de la métrique pour le lien entre ce noeud et le candidat parent

Si le coût d'un chemin est plus grand qu'une constante MAX_LINK_METRIC dont la valeur recommandée par le RFC 6719 [13] est 512, le noeud va exclure le candidat parent utilisant ce lien. Un noeud va choisir comme parent le candidat parent pour lequel le coût du chemin est le plus petit. Le changement

de parent ne s'effectue que si la condition suivante est satisfaite :

$$|cost - old\_cost| > \text{PARENT\_SWITCH\_TRESHOLD}$$

Le RFC 6719 recommande 192 comme valeur pour *PARENT_SWITCH_TRESHOLD* si la métrique utilisée est ETX.

Messages RPL

RPL défini quatre types de mesages de contrôles : DIO, DIS, DAO et DAO-ACK. Ces messages de contôles sont des messages ICMPv6. Le RFC 6550 [10] indique que ces messages ont la portée d'un lien, à l'exception des DAO/DAO-ACK qui dans le mode de fonctionnement *non-storing* sont envoyés en unicast et donc utilisent des adresse unique-local ou global. Pour tous les autres messages, les adresses sources sont des adresses link-local et les adresses de destination sont soit link-local, soit l'adresse multicast pour tous les noeuds RPL qui est `ff02::1a`.

DIO

Les DIOs (DODAG Information Object) annoncent des informations sur le DODAG qui permettent aux noeuds de découvrir une instance RPL, de sélectionner un parent ou encore de maintenir le DODAG. Un DIO, illustré à la figure 1.7, inclu notamment les champs suivants :

- InstanceID : Identifie l'instance RPL du DODAG
- Rank : Le rang du noeud qui émet le DIO
- MOP (Mode of Operation) : Le mode d'opération de l'instance RPL (c.f. section 1.4 Modes de fonctionnements).
  0. Pas de routes descendantes
  1. Non-storing mode
  2. Storing mode sans multicast
  3. Storing mode avec multicast
- DODAGID : Adresse IPv6 définie par la racine qui identifie le DODAG

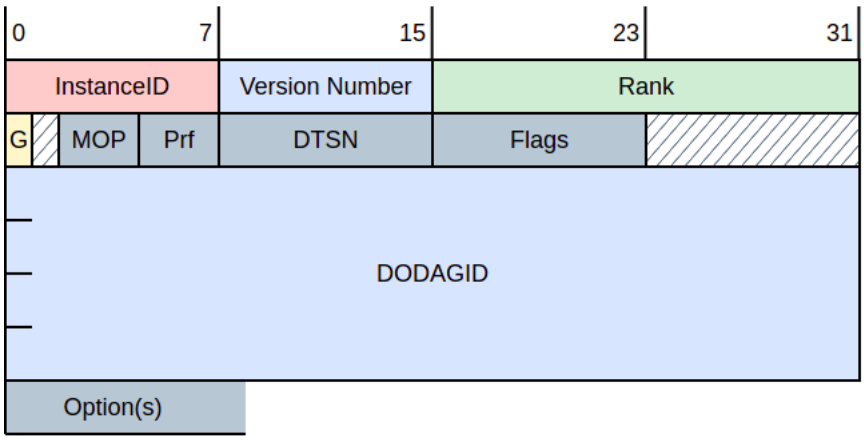


FIGURE 1.7 – DODAG Information Object.

Les DIOs sont transmis en utilisant l'algorithme Trickle [15]. Cet algorithme permet de réduire la quantité de messages envoyés en réduisant les transmissions quand les conditions sont stables et en les augmentant lorsque qu'un changement est observé dans le réseau.

DIS

Les DODAG Information Solicitation (DIS) sont utilisés pour soliciter un DIO d'un noeud RPL.

DAO

Les DAOs (Destination Advertisement Object) sont utilisés pour établir les routes descendantes. Ils sont donc envoyés vers le haut du DODAG. Le format du DAO est illustré à la figure 1.8. Un DAO est composé des champs suivants :

- InstanceID : identifie l'instance du DODAG
- K : indique que le destinataire doit répondre avec un DAO-ACK
- D : indique que le DODAGID est présent
- DAOSequence : Incrémenté à chaque DAO d'un noeud et répété dans le DAO-ACK
- DODAGID (optionnel)

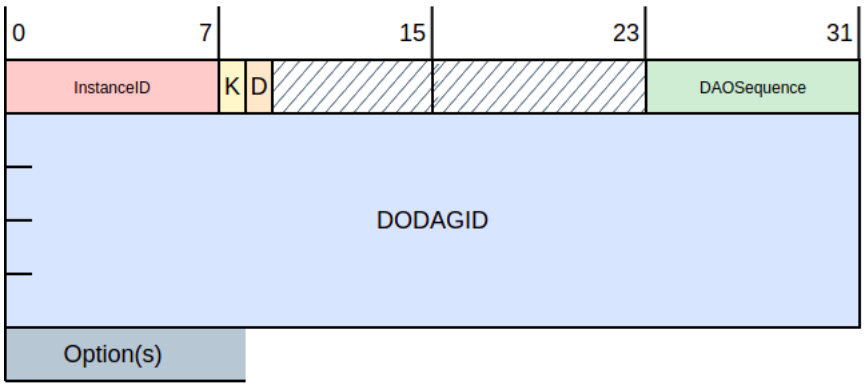


FIGURE 1.8 – DODAG Information Object.

DAO-ACK

Le format d'un DAO-ACK est similaire à celui d'un DAO. Il n'est donc pas utile de le décrire.

Construction du réseau

La construction d'un DODAG est réalisée via l'échange de messages DIOs pour les routes montantes et de DAOs pour les routes descendantes. La figure 1.9 illustre l'échange de ces messages.

Routes Montantes

Les routes montantes sont construites et maintenues avec les DIOs. L'algorithme de construction du DODAG est le suivant :

1. Les noeuds étant configurés comme racine d'un DODAG diffusent des DIOs en multicast à tous les noeuds RPL
2. Les noeuds voulant rejoindre un DODAG écoutent ces DIOs et utilisent leurs informations pour rejoindre le DODAG (i.e. sélectionner un parent) ou maintenir le DODAG existant en accord avec la fonction objectif
3. Les noeuds rajoutent des entrées dans leur table de routage pour les destinations spécifiées dans le DIO via leurs parents
4. Une fois qu'un noeud a rejoint le DODAG, il diffuse à son tour des DIOs pour que d'autres noeuds puissent rejoindre le DODAG.

Les noeuds qui opèrent comme feuille peuvent émettre des DIOs mais le rang contenu dans le DIO doit être l'infini. De cette manière une feuille ne sera pas choisie comme parent.

Si une adresse de destination n'appartient pas au DODAG, la racine du DODAG peut transférer les paquets à l'exterieur de ce réseau, ou, si elle n'en est pas capable, les ignorer.

Routes Descendantes

Les routes descendantes sont construites et maintenues avec les DAOS. L'échange des DAOs différe selon le mode de fonctionnement (MOP) du réseau. Ces différences sont détaillées en section 1.4 Modes de fonctionnements.

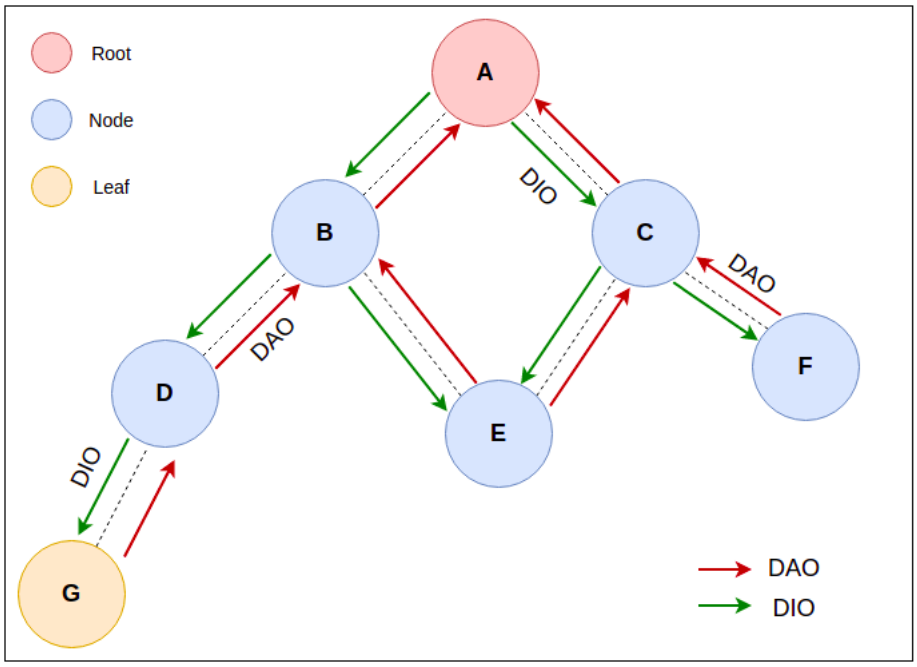


FIGURE 1.9 – Propagation des DIOs et DAOs.

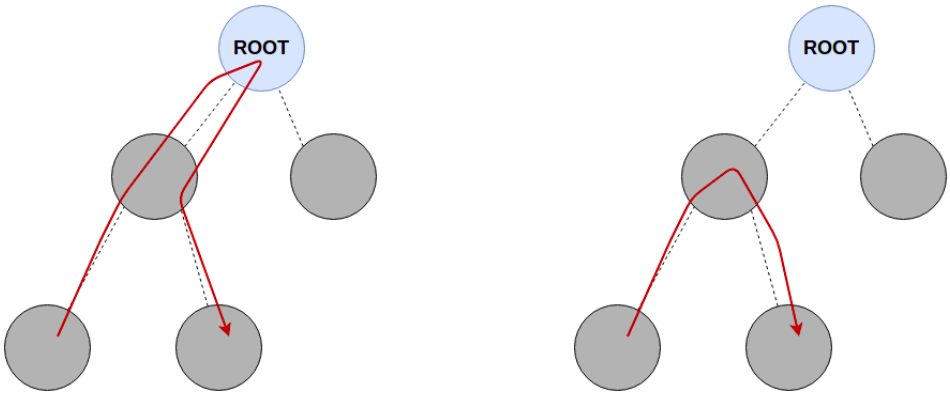
Modes de fonctionnements

Le mode de fonctionnement d'une instance RPL, est défini administrativement et est annoncé par la racine. Les modes suivants sont disponibles :

- **Pas de routes descendantes**
  RPL ne maintient pas de routes descendantes. Dans ce MOP, les DAOs ne sont pas émis par les noeuds d'un DODAG, et les noeuds ignorent les DAOs.
- **Non-storing mode**
  Dans ce mode, les DAOs sont envoyés en unicast à la racine du DODAG. Les noeuds ne stockent pas de routes descendantes.

L'envoi des paquets le long de ces routes se fait donc par source-routing. Cela signifie qu'une en-tête de routage est ajoutée aux datagrammes par la racine. Le RFC 6554 [16] défini les mécanismes liés à ce type d'en-tête ainsi que son format qui est similaire à celui de l'en-tête de routage IPv6 [17] (de Type 0). Toutefois, il introduit en plus un mécanisme qui permet de compresser les adresses quand elles ont toutes le même préfixe.
Dans ce mode, les paquets remontent donc jusqu'à la racine, qui rajoute l'en-tête de routage pour ensuite redescendre jusqu'au noeud de destination (Fig. 1.10a).

- **Storing mode**
  Le storing mode peut être utilisé avec ou sans multicast. Dans ce mode, les DAOs sont envoyées en unicast par les noeuds à leur parent. Les paquets remontent jusqu'à un ancêtre commun avec la destination avant de redescendre vers celle-ci (Fig. 1.10b). Les noeuds stockent les routes de leur sous DODAG. Ainsi, chaque saut dans un chemin examine sa table de routage pour choisir le saut suivant.



(a) Non-Storing. (b) Storing.

FIGURE 1.10 – Chemin d'un paquet en fonction du MOP.

Un noeud voulant rejoindre un DODAG doit être compatible avec le MOP du DODAG. Si ce n'est pas le cas, il doit rejoindre le DODAG comme feuille.

1.5 RTOS

Un RTOS (Real Time Operating System) est un sytème d'exploitation temps réel principalement destiné aux systèmes embarqués. Il permet d'abstraire le matériel en fournissant une couche logicielle facilitant le développement d'une application. Un RTOS permet également de découper une application en tâches qui sont gérées par l'ordonnanceur.

Le RTOS choisi doit supporter la plateforme de utilisée. Sa pile réseau du RTOS doit comprendre les protocoles suivants : 802.15.4 pour la couche physique, TSCH avec un ou plusieurs algorithme d'ordonnancement pour la couche MAC, le support d'IPv6 et d'un algorithme de routage comme RPL pour la couche réseau et enfin, pour le transport, TCP et/ou UDP.

Une implémentation de LoRa n'est pas nécessaire car les communications Lora sont réalisées via le RN2483 qui est controlé par UART.

Pour effectuer ce choix, les RTOS suivants ont été comparés : Contiki OS, FreeRTOS et RIOT OS.

Contiki OS

Le développement publique de Contiki [18] a débuté en octobre 2012 [1]. Dans un premier repository : **contiki** [19]. Un fork de contiki a démarré en mai 2017 sous le nom de **contiki-ng** [20]. Comme le premier développement n'est plus maintenu, c'est ce dernier qui est utilisé pour la comparaison et qui est dénommé par la suite "Contiki".

L'implémentation des processus est basée sur la librairie Protothreads [21] qui abstrait la gestion de la programmation événementielle par des protothreads dont l'utilsations est similaire aux threads. L'ordonnanceur de cette libraire est cooperatif, c'est à dire qu'il ne va jamais forcer un changement de contexte (ensemble des ressources nécessaires à l'éxécution d'un processus) d'un processus à un autre (contrairement à un ordonnanceur préemptif). Le changement de contexte ne s'effectue que quand un processus rend volontairement le contrôle à l'ordonnanceur.

Ce RTOS open-source et multi-plateforme implémente toute une série de protocoles de communications basse énergie tels que IEEE 802.15.4, 6TiSCH, IPv6/6LoWPAN et RPL. En plus de 6TiSCH, un ordonnanceur TSCH, Orchestra, est implémenté.

Contiki supporte plusieurs plateformes en fournissant pour chacune un BSP (Board Support Package). Pour le Zolertia RE-Mote, le BSP supporte notemment la gestion de l'alimentation, des leds, des deux antennes ainsi que

1. Date de création du repository Github.

des interfaces UART, SPI et I2C.

Ce RTOS également est accompagné de Cooja, un simulateur réseau qui permet de simuler les communications entre plusieurs noeuds l'utilisant.

FreeRTOS

D'après le site officiel de FreeRTOS [22], ce RTOS est développé depuis 15 ans. Le repository initial [23] a été créé en 2004.

L'ordonnanceur de tâches de FreeRTOS peut être configuré comme coopératif ou préemptif via le flag *configUSE_PREEMPTION* du fichier de configuration.

Ce RTOS également open-source et multi-plateforme offre des librairies divisées en trois catégories :

- **FreeRTOS+** qui contient notemment la librairie TCP/IP et les protocoles applicatifs MQTT et HTTP,
- **AWS IoT Libraries** qui fourni des librairies permettant la connectivité avec Amazon Web Services (AWS)
- **FreeRTOS Labs** qui contient des librairies complètement fonctionelles mais qui sont encore en cours d'amélioration comme le support d'IPv6, LoRaWan ou le support de plusieurs interfaces réseau

FreeRTOS n'a pour le moment pas été porté pour le Zolertia RE-Mote ou le CC2538. Fournir un tel support est un investissement conséquent et n'est pas l'objectif de ce mémoire.

RIOT OS

Le développement publique de RIOT [24] a débuté en décembre 2012[1].

RIOT est un RTOS qui utilise des standards comme la programmation en C++ ou une compatibilité POSIX pour faciliter le développement d'applications IoT.

L'ordonnanceur de RIOT est tickless, c'est à dire qu'il n'utilise pas un timer déclenché périodiquement pour effectuer les changements de contexte. L'ordonnanceur est préemptif et basé sur des priorités. Les changements de contexte sont initiés lors d'interruptions, volontairement ou quand une opération bloquante a lieue.

La pile réseau de RIOT comporte notemment les protocoles 6LoWPAN, IPv6, RPL, LoRaWan, 802.15.4. RIOT OS intègre la pile réseau OpenWSN [25] mais cette intégration est pour le moment expérimentale.

OpenWSN est une implémentation open-source d'une pile réseau destinée à l'IoT. Cette pile réseau comprend les protocoles IEEE802.15.4e, 6LoW-

PAN, RPL, UDP et CoAP. L'objectif de cette implémentation est qu'elle puisse être utilisée sur une variété de RTOS et de plateformes.

D'après le site officiel, ce RTOS supporte 229 carte de développement et 64 CPU dont le Zolertia RE-Mote.

Conclusion

Le table 1.1 résume la comparaison de ces RTOS avec les critères les plus importants pour ce mémoire. Dans cette comparaison, l'utilisation d'OpenWSN n'a pas été prise en compte pour RIOT OS car son intégration reste expérimentale.

RTOS	802.15.4	TSCH	ord. TSCH	IPV6	Routage IP	comp. RE-Mote
Contiki OS	√	√	6Tisch, Orchestra	√√	RPL	√
FreeRTOS	×	×	×	√	×	×
RIOT OS	√	×	×	√√	RPL	√

TABLE 1.1 – Comparatif de différents RTOS.

Le RTOS choisi est Contiki OS. Il est choisi pour sa maturité, la prise en charge du Zolertia RE-Mote et sa pile réseau complète et stable.

Chapitre 2

Architecture

2.1 Topologie

Cette section décrit et motive la topologie et les types de noeuds du réseau de capteurs hybride IEEE 802.15.4-LoRa. Cette topologie a été choisie pour correspondre au mieux au cas d'utilisation décrit dans l'introduction.**TODO: REF INTRO + à savoir ...**

Types de noeuds

Le protocole élaboré pour ce réseau hybride définit 3 types de noeuds :
- La **racine LoRa** est la passerelle entre le réseau et un réseau IP externe. Elle possède donc une interface LoRa et par exemple une interface Wi-Fi, Ethernet ou 3G/4G. La radio LoRa est toujours allumée car ce noeud n'est pas contraint en énergie.
- Les **racines RPL** sont les racines des réseaux RPL. Elles possèdent une interface LoRa pour communiquer avec la racine LoRa et une interface 802.15.4 pour communiquer avec les noeuds du réseau RPL.
- Les **noeuds RPL** sont des noeuds des réseaux RPL.

Topologie

Comme l'illustre la figure 2.1 la topologie choisie est une topologie mixte.

On a d'abord un ensemble de réseaux RPL possèdant chacun un préfixe de sous-réseau IP attribué par la racine LoRa (par exemple $0x02$ ou $0x04$ sur la figure 2.1), dans lesquels les communications se font par IEEE 802.15.4. Comme RPL est utilisé, chaque réseau forme un DODAG.

Ensuite, chaque réseau RPL est connecté à la racine LoRa via sa racine RPL. Les liens entre les racines RPL et la racine LoRa forment une topologie en étoile.

Ce choix de topologie a comme avantage de simplifier l'administration du réseau. En effet, un réseau RPL pourrait, par exemple, correspondre à une parcelle de terrain. Comme cette topologie est composée d'un ensemble de réseau RPL, la défaillance d'une racine RPL pourrait impliquer la déconnexion d'un réseau RPL, contrairement à une topologie qui utilise un seul réseau RPL où la défaillance de la racine pourrait impliquer la déconnexion de l'ensemble des noeuds.

L'inconvéninent de cette topologie est que la racine LoRa constitue un seul point de défaillance. Une solution plus robuste qui a été envisagée, est un réseau maillé pour les communications LoRa. Cependant, une telle architecture est difficile à mettre en oeuvre car le protocole MAC a établir pour les liens LoRa est plus complexe et nécessite un protocole de routage.

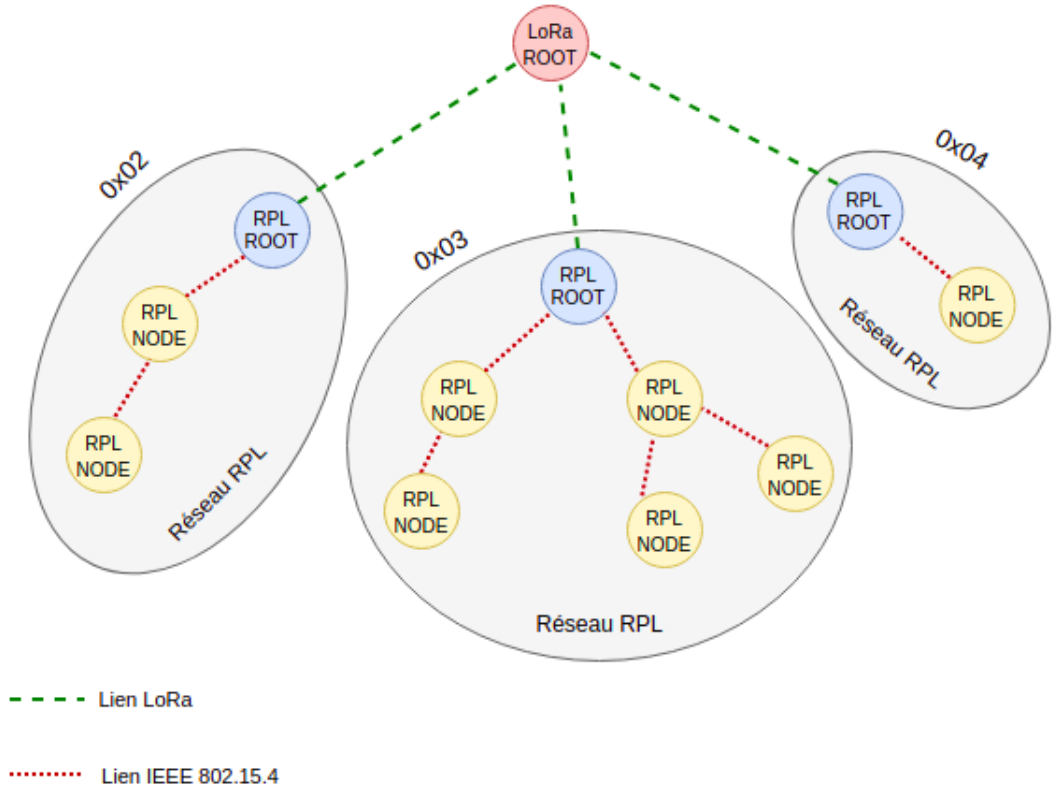


FIGURE 2.1 – Topologie du réseau hybride.

L'essentiel du travail consite donc à définir et mettre en place un protocole MAC utilisant LoRa pour les communications entre les racines RPL

et la racine LoRa ainsi que les mécanismes permettant de passer d'un réseau à un autre. Le routage est le transfert des paquets dans les réseaux RPL est quand à lui assuré par RPL et IPv6. Les sections suivantes décrivent le protocole MAC mis en place pour les communications LoRa.

2.2 Format d'adresse

Cette section décrit les possibilités envisagées pour le choix du format des adresses utilisées pour les communications LoRa et motive le choix d'un format. Dans chaque hypothèse, un réseau RPL possède un préfixe de sous-réseau qui lui est propre.

Adresse IPv6

La première solution envisagée est d'utiliser les adresses IPv6 des noeuds. Une racine RPL peut ainsi vérifier si un paquet est destiné à son réseau et la racine LoRa à elle même, via le préfixe de sous réseau de l'adresse de destintation. Cette solution est la plus simple à mettre en oeuvre car elle ne nécéssite pas de table de routage ou de processus de conversion d'adresse. Cette approche a néanmoins le désavantage que les adresses IP de 128 bits sont transportées sur un lien LoRa ce qui représente un temps de transmission important.

Néanmoins la taille des adresses IP est de 128 bits.

Préfixe et *node-id*

Une seconde approche est d'utiliser un préfixe et le *node-id*. Ce dernier est un identifiant de noeud sur 16 bits utilisé dans Contiki. Son calcul, basé sur les deux derniers octets de l'adresse MAC du noeud (*link-layer address*) est le suivant :

$$node\_id = link\_addr[s-1] + (link\_addr[size-2] << 8)$$

où s est la taille de la *link-layer address*.

Le format d'adresse utilisé serait alors un préfixe sur 8 bits et le *node-id* sur 16 bits ce qui fait un total de 24 bits.

L'avantage de cette solution est que la taille des adresses est réduite d'un facteur de 18,75%. Néanmoins, un processus de conversion est nécessaire ainsi qu'une table de conversion d'un *node-id* vers une adresse MAC pour chaque noeud RPL. En effet, le calcul du *node-id* ne permet pas de

reconstituer l'adresse MAC de 64 bits à partir de celui-ci. Un autre inconvénient est que l'utilisation du préfixe de 8 bits limite le nombre de réseaux RPL à 256, ce qui reste néanmoins acceptable.

Préfixe et adresse MAC

La troisième approche envisagée a pour objectif de résoudre le problème de la conversion *node-id*↔ adresse MAC, en remplaçant le *node-id* par l'adresse MAC d'un noeud.

Cette solution permet une conversion d'adresse simple et la taille des adresses est de 72 bits (64 bits de l'adresse MAC et 8 bits du préfixe).

Solution retenue

La solution retenue est l'utilisation du préfixe de 8 bits et du *node-id* car c'est la solution qui offre les adresses les plus courtes. Pour éviter l'utilisation d'une table de conversion *node-id*↔ adresse MAC, une meilleure solution que d'utiliser les adresses MAC des noeuds et de modifier les 6 premiers octets de cette dernière. Cela permet de reconstituer une adresse IPv6 simplement, mais cela réduit le nombre d'adresses possibles qui reste cependant largement suffisant pour ce projet.

L'adresse de l'interface LoRa de la racine LoRa est quand à elle configurée administrativement.

2.3 Trames LoRaMAC

Le protocole MAC mis en place pour les communications LoRa utilise un seul format de trames illustré à la figure 2.2.

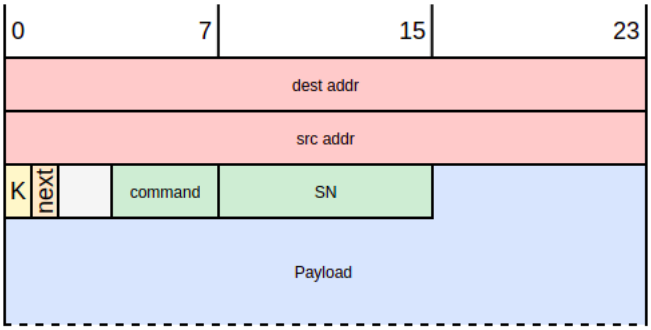


FIGURE 2.2 – Format de trame LoRaMAC.

Les trames LoRaMAC sont composées des champs suivants :

- **dest_addr** : l'adresse de destination (24 bits)
- **src_addr** : l'adresse source (24 bits)
- **K** : un flag qui indique si la trame nécessite un acquittement (1 bit)
- **next** : un flag qui indique si une autre trame suit (1 bit)
- **reserved** : 2 bits réservés pour évolution future
- **command** : la commande MAC (4 bits).
  Les 5 commandes disponibles ainsi que leurs valeurs sont reprises dans la table 2.1. Il est possible d'ajouter 10 commandes supplémentaires pour des usages futurs.
- **SN** : le numéro de séquence de la trame (8 bits)
- **Payload** : la payload ayant une taille maximale de 247 octets. Cette limitation provient de la radio LoRa utilisée (le RN2483 c.f. **TODO: ref**) qui limite les transmissions à 255 octets, valeur de laquelle est soustrait les 8 octets des champs précédents.

Valeur	Commande	description	payload
0	JOIN	requête pour rejoindre le réseau	×
1	JOIN_RESPONSE	réponse à la commande JOIN	préfixe du sous réseau
2	DATA	transport de données	données
3	ACK	acquittement	×
4	QUERY	demande de trafic descendant	×

TABLE 2.1 – Description des commandes LoRaMAC.

2.4 LoRaMAC

Cette section décris le protocole MAC mis en place pour les communications LoRa. Ce protocole est donc utilisé pour les communications entre la racine LoRa et les racines RPL. Ces dernières étant contraintes en énergie, leur radio LoRa n'est pas tout le temps allumée. Le protocole prend donc en compte cette contrainte.

Etats d'une Racine RPL

Les racines RPL utilisent 4 états illustrés dans le diagramme d'état de la figure 2.3. A l'initiation du réseau, une racine RPL se trouve dans l'état *alone*. Elle demande ensuite son préfixe à la racine LoRa. Si la transmission échoue trop de fois, elle entre dans l'état *sleep* jusqu'à ce que l'évènement *wake up* soit déclenché pour retourner dans l'état *alone*. Si la transmission est réussie,

et donc que le préfixe est reçu, la racine RPL se trouve dans l'état *ready*. Quand une racine RPL envoie une trame qui nécessite un acquittement, tant que celui-ci n'est pas reçu elle se trouvera dans l'état *wait_response*. Une fois l'acquittement reçu, elle retournera dans l'état *ready*.

Les trames qui doivent être envoyées le seront en fonction de l'état dans lequel se trouve une racine RPL. Dans l'état *ready*, les trames de données peuvent être envoyées, mais ce n'est pas le cas dans les états *alone* et *wait_response*. En effet dans le premier la racine RPL ne peut pas envoyer de données car elle n'a pas encore rejoint le réseau et dans le second, elle attend une réponse.

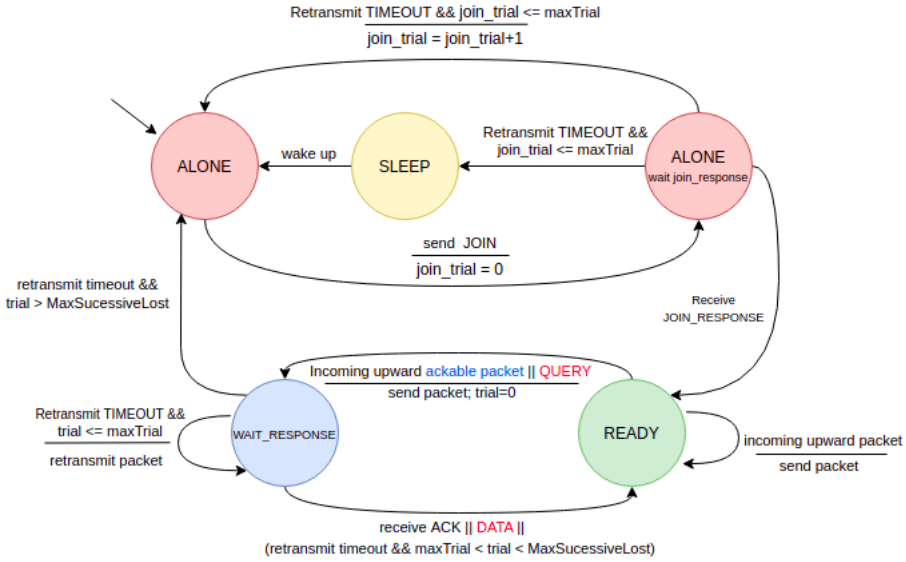


FIGURE 2.3 – Diagramme d'état des racines RPL.

Construction du réseau

A l'initialisation du réseau, une racine RPL doit envoyer une trame avec la commande JOIN. Une fois reçue par la racine LoRa, celle-ci va répondre avec une trame JOIN_RESPONSE qui fait office d'acquittement de la trame JOIN et dont la payload est le préfixe IP que la racine RPL doit diffuser dans son réseau.

Si la trame JOIN ou la trame JOIN_RESPONSE ne sont pas reçues, la racine RPL retransmettra la trame JOIN à l'expiration d'un timer *retransmit_timer* déclenché à l'envoi de la trame JOIN. Cette retransmission se répète au maximum MAX_ATTEMPT fois. Ensuite la racine RPL attend SLEEP_TIME secondes avant de répéter le processus.

Une fois le préfixe reçu, la racine RPL peut initialiser le réseau RPL et y diffuser le préfixe.

Communications montantes

Lorsq'un paquet est destiné à la racine LoRa, il va remonter jusqu'à la racine RPL. Ensuite celle-ci va l'envoyer à la racine LoRa.

Si la trame LoRaMAC envoyée à la racine LoRa nécessite un acquittement, la racine RPL n'enverra pas d'autres trames tant que l'acquittement n'a pas été reçu (état *wait_response*). A l'envoi de cette trame, le timer *retransmit_timer* est déclenché. S'il expire avant que l'acquittement ne soit reçu, la trame sera retransmise pour un maximum de 3 fois. Si la transmission échoue après ces trois tentatives, la racine RPL va faire une pause de SLEEP_TIME secondes avant de réessayer. Si la communications échoue toujours, la racine RPL retourne dans l'état initiale et va recommencer la procédure pour rejoindre le réseau.

Si la trame LoRaMAC envoyée à la racine LoRa ne nécessite pas d'acquittement, la récéption ne cette trame n'est pas garantie et la racine RPL peut directement envoyer d'autres trames.

Communications Descendantes

La racine LoRa possède un buffer pour chaque réseau RPL dans lequel elle accumule les paquets destinés à ce réseau. Pour chaque racine RPL, lors de l'expiration, à intervalle régulier, du timer *query_timer*, une trame avec la commande QUERY est transmise à la racine LoRa.

La réponse à cette trame doit être un acquittement, si la racine LoRa n'a pas de paquets pour cette racine RPL, ou une trame avec la commande DATA.

Si la racine LoRa possède plusieurs paquets à destination du même réseau RPL, la valeur du flag *next* doit être à 1 pour toutes les trames envoyées expecté la dernière.

Comme pour les communications montantes, les retransmissions sont initiées par les racines RPL. Le timer *retransmit_timer* est activé lorsque la QUERY est envoyée et lorsqu'une trame DATA a le flag *next* à 1.

Si une trame nécessite un acquittement et que l'acquittement n'est pas reçu, la racine LoRa n'envoie pas le paquet suivant. Dans ce cas deux situations sont possibles :

- La trame avait le flag *next* à 1 :
  La racine RPL s'attend à une autre trame. L'acquittement va donc

être retransmis à l'expiration du *retransmit_timer*. Il y a maximum 3 retransmissions.

- La trame avait le flag *next* à 0 ou l'acquittement a déja été retransmis trois fois :
  La racine LoRa retransmettra le paquet concerné lors de la réception d'une QUERY.

Gestion des numéros de séquence

Les racines RPL et la racine LoRa possèdent deux compteurs : *expected_sn* et *next_sn*.

La valeur du compteur *expected_sn* est le numéro de séquence attendu de la prochaine trame reçue. Ce compteur permet de savoir si une trame a été perdue. Sa valeur est le numéro de séquence de la dernière trame reçue incrémenté de 1.

La valeur du compteur *next_sn* est le numéro de séquence de la prochaine trame. Il est incrémenté de 1 lorsqu'une trame a été envoyée.

Exemple de communications

Les figures 2.4 et 2.5 ci-dessous, illustrent le protocole LoRaMAC qui vient d'être décrit dans cette section. La première illustre les échanges de messages sans retransmissions et la deuxième avec retransmissions. Les détails des timers ne sont pas présents sur ces figures pour plus de clarté.

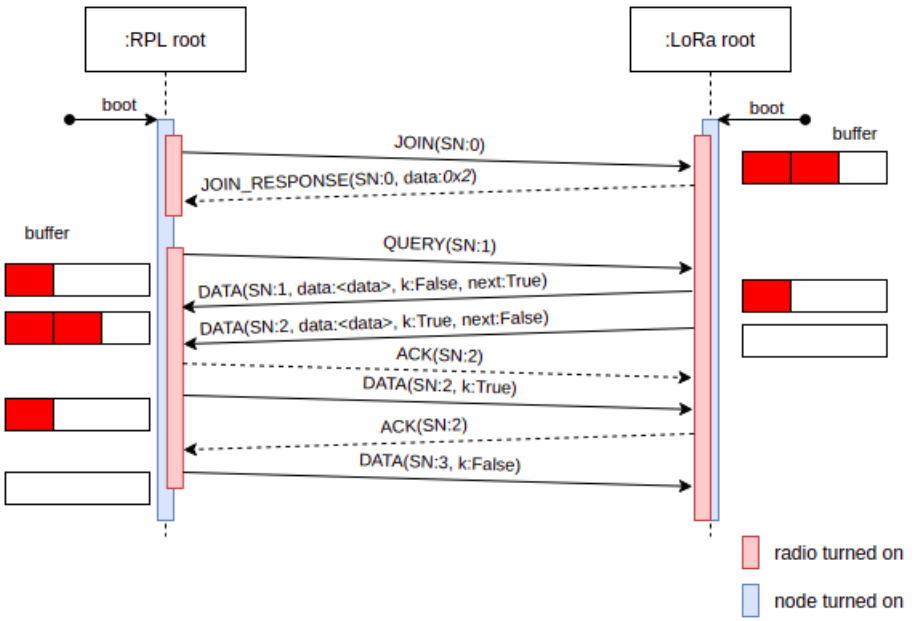


FIGURE 2.4 – Diagramme de séquence LoRaMAC.

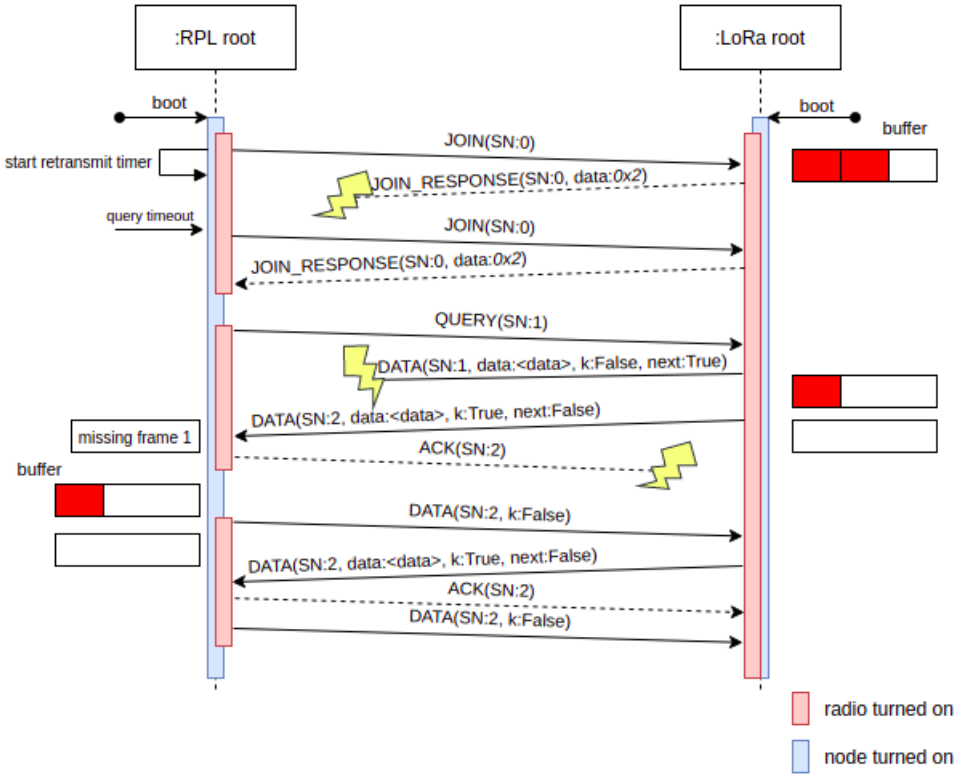


FIGURE 2.5 – Diagramme de séquence LoRaMAC avec retransmissions.

2.5 Plateformes de développement

Cette section décrit le matériel utilisée pour mettre en oeuvre la topologie décrite en **TODO: ref**. Pour les racines RPL, la plateforme de développement Zolertia RE-Mote revision B est utilisée, et, pour la racine LoRa, un Raspberry pi 3B+ est utilisé. Leur interface LoRa est un RN2483. Les noeuds des réseau RPL sont également la plateforme de développement Zolertia RE-Mote revision B.

RN2483

Le RN2483 (Fig. 2.6) est un modem LoRa compatible LoRaWAN^{TM} basse énergie. D'après Nestor Ayuso [26], il intègre un transceiver Semtech SX1276 [6] et un microcontrôleur Microchip PIC18LF46K22. La communication avec ce modem est effetuée par des commandes ASCII envoyées via une interface UART. Il prend en charge les modulations FSK, GFSK et LoRa. Il possède également 14 GPIOs (General Purpose Input/Output). Ses fréquences opérationnelles sont situées dans les bandes 433 MHz et 868 MHz. D'après la datasheet [3], sa portée maximale est de 15km en agglomération et 5km en zone urbaine. Comme l'illustre la figure. 2.6, pour ce mémoire, le RN2483 a été monté sur un carte d'interface réalisée par B.Quoitin qui comporte deux LEDs, une petite hélicoïdale ainsi que les connecteurs permettant d'utiliser des câbles de prototypages.

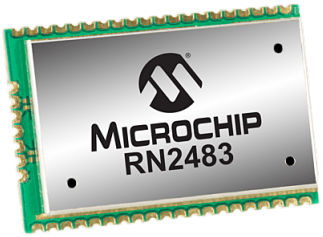


FIGURE 2.6 – RN2483 [2].

La figure 2.7 reprend le schéma-bloc du RN2483. Il contient notemment l'interface UART, les antennes 433 MHz et 868Mhz ainsi que les GPIOs et la stack LoRaWan.

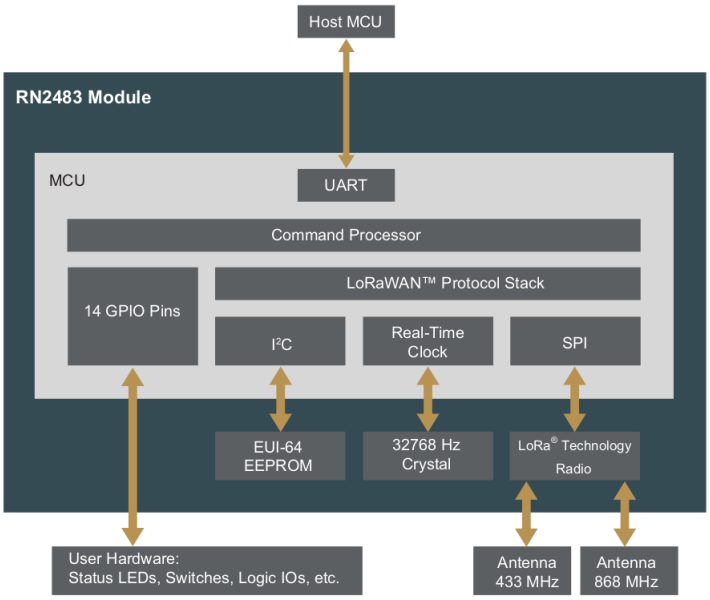


FIGURE 2.7 – Schéma-bloc du RN2483 [3].

La table 2.2 reprend la consommation électrique du RN2483 en fonction de son mode de fonctionnement pour alimentation de 3.3V qui est celle fournie par le RE-Mote et le Raspberry Pi.

Mode	Courant(mA) VDD=3.3V
Idle	2.8
Transmit	38.9
Sleep	0.0016
Receive	14.22

TABLE 2.2 – Consommation de courant (à 25 °C) [3].

Raspberry Pi

Le Raspberri Pi est un ordinateur monocarte. Il possède notemment 40 pins GPIO, une interface Wi-Fi, Bluetooth, 4 ports USB 2.0 et un connecteur pour une caméra. Toutes ces caractéristiques en font une passerelle idéale pour ce projet. En effet, ils permettent d'utiliser plusieurs interfaces réseaux et d'y connecter des capteurs et actuateurs.

Le modèle utilisé pour ce projet est un Raspberry Pi 3 modèle B+ (Fig. 2.8). Ce modèle est équipé d'un processeur quadri-coeur Broadcom

BCM2837B0, Cortex-A53 64-bit SoC cadencé à 1.4GHz et embarque 1GB de mémoire RAM.

La table 2.3 reprend les principales caractéristiques de ce modèle.

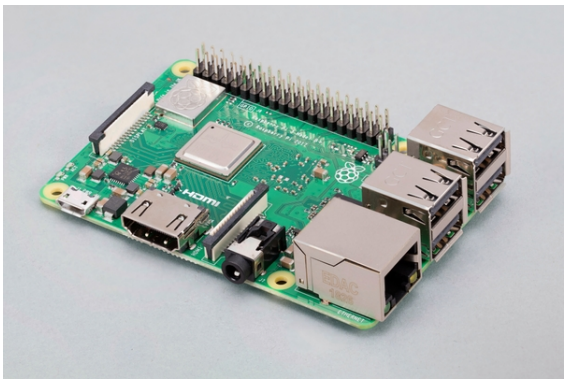


FIGURE 2.8 – Raspberry Pi 3B+ [4].

Element	Spécification
CPU	Broadcom BCM2837B0, Cortex-A53 64-bit SoC à 1.4GHz
Mémoire	1GB LPDDR2 SDRAM
Connectivité	• IEEE 802.11.b/g/n/ac, Bluetooth 4.2, BLE • Gigabit Ethernet over USB 2.0 • 4 × USB 2.0 ports
Alimentation	5V/2.5A DC

TABLE 2.3 – Spécifications du Raspberry Pi 3B+ [4].

Zolertia RE-Mote

Pour ce mémoire, la plateforme Zolertia RE-Mote revision B (Fig. 2.9) est utilisée. Cette plateforme, basée sur un system on chip (SoC) CC2538 ARM Cortex-M3, a été conçue par des universités et des industriels dans le but de permettre aux chercheurs et makers de développer des applications IoT et des objets connectés.

Le Zolertia RE-Mote a été choisie car elle est équipée de deux radios compatibles IEEE 802.15.4, permet une consommation électrique faible et possède de nombreux pins de connexion qui peuvent être utilisés pour y connecter des capteurs, actuateurs, radios, etc.

Le prix du constructeur pour cette plateforme est de 93,95€ [5].

FIGURE 2.9 – Zolertia RE-Mote révision B [5].

La table 2.4 reprend les principales spécifications du Zolertia RE-Mote rev.b.

Element	Spécification
Radio	- IEEE 802.15.4 2.4 GHz - IEEE 802.15.4 863-950 MHz
CPU	ARM® Cortex® -M3 jusqu'à 32 MHz
RAM	32 KB (16 KB pour tous les Power Modes)
Flash programmable	512KB
I/O	- RGB led, boutton user et reset - Slot Micro-SD - USB 2.0 à 12Mbps - Real-Time Clock

TABLE 2.4 – Spécifications du Zolertia RE-Mote rev.b [27].

Bibliographie

[1] Sakshama Ghoslya. Lora : Symbol generation. [Accès en ligne le 11 juillet 2021].

[2] RN2483. `https://www.microchip.com/wwwproducts/en/RN2483`. [Accès en ligne le 14 juin 2021].

[3] Microchip. *Low-Power Long Range LoRa® Technology Transceiver Module*, 6 2020. Rev. E.

[4] Raspberry Pi 3 Model B+. `https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/`. [Accès en ligne le 15 juin 2021].

[5] Zolertia RE-Mote. `https://zolertia.io/product/re-mote/`. [Accès en ligne le 14 juin 2021].

[6] Semtech Corporation. *SX1276/77/78/79 - 137 MHz to 1020 MHz Low Power Long Range Transceiver*, 5 2020.

[7] Tapparel Joachim. Complete reverse engineering of lora phy.

[8] LoRa Alliance Technical Committee Regional Parameters Workgroup. *RP002-1.0.2 LoRaWAN® Regional 40 Parameters*, 10 2020.

[9] Domenico De Guglielmo, Simone Brienza, and Giuseppe Anastasi. Ieee 802.15.4e : A survey. *Computer Communications*, 88 :1–24, 2016.

[10] Roger Alexander, Anders Brandt, JP Vasseur, Jonathan Huii, Kris Pister, Pascal Thubert, P Levis, Rene Struik, Richard Kelsey, and Tim Winter. RPL : IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550, March 2012.

[11] Joydeep Tripathi, Jose Oliveira, and J.-P Vasseur. A performance evaluation study of rpl : Routing protocol for low power and lossy networks. pages 1–6, 03 2010.

[12] Pascal Thubert. Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL). RFC 6552, March 2012.

[13] Omprakash Gnawali and P Levis. The Minimum Rank with Hysteresis Objective Function. RFC 6719, September 2012.

[14] Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris. A high-throughput path metric for multi-hop wireless routing. 2003.

[15] P Levis, Thomas H. Clausen, Omprakash Gnawali, Jonathan Huii, and JeongGil Ko. The Trickle Algorithm. RFC 6206, March 2011.

[16] David Culler, Jonathan Huii, JP Vasseur, and Vishwas Manral. An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL). RFC 6554, March 2012.

[17] Dr. Steve E. Deering and Bob Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 8200, July 2017.

[18] Adam Dunkels, Björn Grönvall, and Thiemo Voigt. Contiki - a lightweight and flexible operating system for tiny networked sensors. In *Proceedings of the First IEEE Workshop on Embedded Networked Sensors (Emnets-I)*, Tampa, Florida, USA, November 2004.

[19] The Contiki Operating System. `https://github.com/contiki-os/contiki`. [Accès en ligne le 15 juin 2021].

[20] Contiki-NG : The OS for Next Generation IoT Devices. `https://github.com/contiki-ng/contiki-ng`. [Accès en ligne le 15 juin 2021].

[21] Adam Dunkels, Oliver Schmidt, Thiemo Voigt, and Muneeb Ali. Protothreads : Simplifying event-driven programming of memory-constrained embedded systems. In *Proceedings of the Fourth ACM Conference on Embedded Networked Sensor Systems (SenSys 2006)*, Boulder, Colorado, USA, November 2006.

[22] FreeRTOS Real-time operating system for microcontrollers. `https://freertos.org/index.html`. [Accès en ligne le 15 juin 2021].

[23] Initial repository of FreeRTOS. `https://freertos.org/index.html`. [Accès en ligne le 15 juin 2021].

[24] Emmanuel Baccelli, Cenk Gündoğan, Oliver Hahm, Peter Kietzmann, Martine S. Lenders, Hauke Petersen, Kaspar Schleiser, Thomas C. Schmidt, and Matthias Wählisch. Riot : An open source operating system for low-end embedded devices in the iot. *IEEE Internet of Things Journal*, 5(6) :4428–4440, 2018.

[25] OpenWSN. `https://openwsn.atlassian.net/wiki/spaces/OW/overview?mode=global`. [Accès en ligne le 22 juin 2021].

[26] Nestor Ayuso. Microchip rn2483 teardown : The french (wireless) connection, Jul 2015. [Accès en ligne le 11 juillet 2021].

[27] Zolertia. *Zolertia RE-Mote Revision B Internet of Things hardware development platform, for 2.4-GHz and 863-950MHz IEEE 802.15.4, 6LoWPAN and ZigBee® Applications*, 9 2016. v.1.0.0.