

Remerciements

Nous remercions ...

Table des matières

1	Rappels et nomination des technologies	2
1.1	signal radio	2
1.2	traitement du signal	3
1.3	LoRa	5
1.3.1	couche physique LoRa	6
1.3.2	LoRaWAN	7
2	Travaux similaires et autres contributions	10
3	Expérimentations	11
3.1	Matériel	11
3.1.1	radio logicielle	11
3.1.2	logiciel	12
3.2	Génération et réception d'un signal LoRa	13
3.3	analyse du signal	13
3.4	Méthode "Constellation traces"	13
4	Résultats	14
	Conclusion	15
	Annexes	16
A	Première annexe	16
B	Deuxième annexe	17

Introduction

L'avènement de L'*Internet of Things* a lancé une nouvelle ère d'appareils connectés, ouvrant de nouvelles possibilités de partage de l'information, d'automatisation et de protection. Bien que le concept lui-même soit prometteur, la technologie qui l'accompagne est essentielle.

Les premières technologies utilisées pour l'IoT étaient les technologies sans fil déjà présentes comme le Wifi ou le Bluetooth. Performantes dans certains cas, elles étaient néanmoins limitées : une consommation en énergie élevée, une portée restreinte et parfois même un coût d'infrastructure trop important.

Dans ces circonstances est apparu *LoRa*, une technologie développée en particulier pour l'IoT. Sa capacité à gérer les communications longue portée même dans des environnements peu adaptés est une révolution pour le domaine.

L'expansion de L'Iot soulève une nouvelle problématique de sécurité. Entre autres, l'identification des nœuds au sein des réseaux est essentielle. Il a été découvert que des nœuds fabriqués avec les mêmes microprocesseurs et modèles d'émetteur-récepteur radio peuvent présenter de subtiles particularités dans les caractéristiques de leurs signaux. Cette variabilité intrinsèque de la transmission des signaux radio peuvent être exploitées pour distinguer les nœuds d'un réseau. En écoutant leurs signaux radio émis et en analysant leurs signatures distinctes, il devient possible de les identifier.

Ce travail est structuré en trois parties. Le premier chapitre sert d'aperçu global du signal radio afin d'y développer et rappeler les concepts de télécommunication de base. Ce chapitre présente également les technologies LoRa et LoRaWAN à travers leurs caractéristiques et leur pertinence dans l'IoT.

Le second chapitre est dédié à l'étude expérimentale du sujet. Les aspects pratiques y seront appliqués, notamment l'utilisation de radio logicielle afin de capturer des signaux radio. Ces signaux seront ensuite analysés grâce à diverses méthodes détaillées dans ce chapitre.

La dernière partie du travail présentera une présentation des résultats obtenus en suivant l'analyse effectuée au chapitre précédent. Enfin le travail sera achevé en concluant sur de potentielles implications plus larges à ce sujet ainsi que des recherches plus approfondies.

Chapitre 1

Rappels et nomination des technologies

1.1 signal radio

Un signal est une variation dans l'espace ou dans le temps d'une quantité physique contenant de l'informations. Un signal peut être continu ou discret, on le nomme alors respectivement analogique ou numérique. Le type de signal dépend notamment de l'information qu'il contient. Un signal analogique peut contenir par exemple du son, là où un signal numérique contient généralement un nombre fini de valeur (par exemple des 0 et 1). Les deux catégories ne sont pas incompatibles car il est souvent nécessaire en télécommunication de pouvoir passer de l'un à l'autre.

L'utilisation de signaux radio en télécommunication confère de nombreux avantages, comme la portée, la vitesse de transmission, la résistance aux interférences ou encore le coût de propagation. Tous ces avantages sont possibles car un signal peut être modulé. La modulation est une technique permettant de modifier les propriétés du signal lui permettant de transporter de l'information.

En télécommunication, les signaux sont associés aux ondes radios, ainsi appelé *radiosignal* ou signal radio. Voici les principaux attributs d'un signal radio :

- la fréquence, mesurée en Hertz. Elle détermine le nombre de cycles qu'accomplit le signal par seconde.
- La largeur de spectre, elle dépend de la fréquence car c'est l'écart entre la plus haute fréquence et la plus basse du signal. Une plus grande largeur permet de transmettre plus d'information.
- L'amplitude. Selon le type de signal l'attribut possède différentes fonctions. Dans le cas d'un signal analogique l'amplitude est l'une des caractéristiques principales d'identification du signal mesurant l'ampleur du

signal. dans un signal numérique l'amplitude set plutôt demarge entre les différentes états du signal.

- la puissance, mesurée en décibel (dB). C'est la force du signal, un attribut important pour la réception du signal notamment.
- le *signal to noise ratio* ou SNR. Cet attribut mesure la qualité du signal. une valeur élevée indique que le pourcentage de bruit est faible.
- le *bit rate*, ou le taux de transmission mesure la quantité de donnée transmise en bit par seconde. cet attribut est exclusif aux signaux numériques. On parle de *Baud rate* pour les signaux analogiques. Ce n'est pas exactement l'équivalent du bit rate car c'est le nombre de symbole modifié par seconde, et un symbole peut contenir plusieurs bit pour un signal numérique.

1.2 traitement du signal

modulation

Parmis ces différents attributs, certains sont utilisés pour effectuer une modulation. Les deux modulations les plus utilisées sont basées sur les attributs de la fréquence et de l'amplitude. La modulation en fréquence (ou *FM* pour *frequency modulation*) consiste à encoder l'information en faisant varier la fréquence en maintenant l'amplitude constante. La modulation en amplitude (*AM*) est le procédé inverse, c'est à dire encoder l'information en faisant varier l'amplitude tout en gardant la fréquence constante. Les deux méthodes de modulation ont leurs points forts et sont choisies en fonction des besoins spécifiques et des considérations de chaque diffusion.

plus loin dans la technique de modulation ?

gestion du bruit

L'un des attributs cités concerne le bruit. Le bruit en télécommunication se définit par l'altération non souhaitée de l'intégrité d'un signal. Il peut prendre différentes formes, les plus courantes étant les interférences électriques ou le bruit thermique. Le bruit dégrade le signal, pouvant provoquer de l'incertitude.

plus loin dans l'impact du bruit ?

transformée de Fourier

La transformée de Fourier est un outil fondamental utilisé pour analyser et décomposer des signaux complexes en composantes fréquentielles. En transformant un signal dans le domaine temporel en sa représentation dans le do-

maine fréquentiel, la transformée de Fourier révèle les différentes composantes fréquentielles présentes dans le signal. En fonction du type de signal, la transformée de Fourier est adaptée.

Pour les signaux continus, la CFT (Transformée de Fourier continue) convertit une fonction du temps en fonction de la fréquence en intégrant le signal par rapport aux sinusoides de toutes les fréquences possibles. Cette transformation fournit les informations d'amplitude et de phase pour chaque composante de fréquence présente dans le signal.

pour les signaux discrets et échantillonnés, la DFT (Transformée de Fourier discrète) calcule un ensemble fini de composantes de fréquence. Il est calculé à l'aide d'un nombre fini d'échantillons, ce qui donne des composantes de fréquence discrètes. Il existe une méthode simplifiée pour les signaux discrets appelé FFT (Fast Fourier Transform). Il s'agit d'un moyen plus rapide de calculer la transformée de Fourier, en particulier pour les signaux numériques comportant un grand nombre de points de données. L'avantage principal de cet algorithme permet de réduire le temps de calcul en divisant la DFT en sous problèmes. La FFT est une méthode très utilisée pour l'analyse de signaux.

1.3 LoRa

LoRa (Long Range) est une technologie de communication sans fil qui permet de transmettre des données sur de longues distances avec une faible consommation d'énergie. Elle a été développée par la société française Cycleo et est maintenant gérée par la fondation LoRa Alliance, qui regroupe plusieurs entreprises et organisations du monde entier.

LoRa est principalement utilisée dans l'*IoT*. Elle se distingue par sa portée étendue, qui peut atteindre plusieurs kilomètres en milieu urbain et plusieurs dizaines de kilomètres en milieu rural, ainsi que par sa faible consommation d'énergie, qui permet de prolonger la durée de vie des appareils connectés. Une longue portée avec une puissance limitée induit une plus faible bande passante que les autres technologies sans fil (le Wifi, la 4G, Bluetooth etc).

LoRa utilise une bande de fréquences qui varie selon les régions du monde où LoRa est déployée :

- en Europe, la bande de fréquences autorisée est comprise entre 863 et 870 MHz,
- aux États-Unis, elle se situe entre 902 et 928 MHz,
- en Chine, la fréquence autorisée varie entre 779 et 787 MHz,
- les régions restantes ont elles aussi une fourchette unique.

La technologie LoRa utilise la modulation en fréquence chirp spread spectrum (CSS). la modulation CSS utilise un signal chirp, c'est à dire un signal modulé en fréquence linéaire. Ce signal a une amplitude constante mais balaie tout le spectre de la bande passante de manière linéaire dans une période de temps définie. Cette technique de modulation sera détaillé plus loin dans le chapitre.

La technologie LoRa utilise également une technique de multiplexage en temps partagé (TDMA) pour permettre à plusieurs appareils de partager la même bande de fréquences de manière à maximiser l'utilisation de la capacité de transmission. Elle utilise également une technique de diffusion de données (multicast) pour envoyer les mêmes données à plusieurs appareils simultanément, ce qui permet de réaliser des économies de bande passante et d'énergie.

En plus de sa portée étendue et de sa faible consommation d'énergie, LoRa se distingue par sa sécurité de transmission, qui est assurée grâce à l'utilisation de codes de sécurité uniques et à la possibilité de chiffrer les données transmises. Elle est également compatible avec de nombreux protocoles de communication couramment utilisés dans l'*IoT*, tels que TCP/IP, HTTP et MQTT, ce qui facilite son intégration dans les systèmes existants.

Toutes ces particularités font de LoRa une technologie complémentaire à celles déjà existante plutôt que rivale.

LoRa se compose de deux éléments principaux : la couche physique de la technologie et LoRaWAN, la couche MAC (media access control), une sous

couche de la couche liaison de données. la couche physique de LoRa gère la fréquence radio ainsi que la modulation. LoRaWAN gère les aspects réseau (sécurité, propagation, adressage et sécurité).

1.3.1 couche physique LoRa

découpage de la couche physique

Les étapes de la conception de la couche physique de LoRa sont les suivantes :

- Le codage de canal est une technique utilisée dans les systèmes de communication sans fil pour améliorer la robustesse et la fiabilité de la transmission des données. Dans le cas de LoRa, le codage de canal est une étape importante pour s'assurer que les données transmises sont correctement reçues et décodées par le récepteur en utilisant de la redondance.
- Le mélange de canal (en anglais "channel interleaving") est la dernière des méthodes d'amélioration de la robustesse de la transmission des données. Cette technique consiste à réarranger les données avant de les transmettre, en les intercalant entre elles de manière à les disperser sur le spectre des fréquences de la transmission. Cela permet de réduire l'impact des erreurs de transmission sur la qualité de la réception, en évitant que des erreurs consécutives ne se propagent et ne perturbent la décodage des données.
- Le blanchiment de canal (en anglais "channel whitening") est une méthode d'amélioration de la robustesse et de fiabilité de la transmission des données. Le blanchiment de canal est également une étape importante pour s'assurer que les données transmises sont correctement reçues et décodées par le récepteur. Cette technique consiste à utiliser une transformation aléatoire ou pseudo-aléatoire des données avant de les transmettre, de manière à répartir le spectre des fréquences de la transmission sur une large gamme de fréquences. Cela permet d'obtenir une meilleure résistance aux interférences et au bruit de fond, ainsi qu'une meilleure robustesse face aux erreurs de transmission. En effet la transformation de la séquence assure une corrélation faible entre les bits de cette dernière.
- La modulation CSS est l'étape la plus importante pour le sujet de ce travail. En effet, le signal modulé permet d'obtenir une séquence de *chirp* ou un signal *chirp*. Cette séquence est unique et permettrait l'identification du nœud émetteur.
- demodulation CSS
- dewhitening

- deinterleaving
- decoding

Cette analyse a été faite en *reverseengineering*. Le reverse engineering consiste à analyser un produit ou un système afin de comprendre comment il fonctionne ou d'identifier ses principes de conception. Dans le contexte de LoRa, le reverse engineering examine la technologie derrière LoRa afin de comprendre ses principes de base et sa conception.

modulation CSS

principe de base : le signal est modulé en sweepant sur une large bande de fréquence en utilisant des signaux "chirp". deux types de chirp "upchirp" et "downchirp".

upchirp : la fréquence augmente avec le temps downchirp : la fréquence diminue avec le temps

le signal est séparé sur une large bande de fréquence, permettant par exemple plusieurs transmissions sans causer d'interférence. la modulation CSS étale sur une bande plus large que les autres technologies de modulation.

l'une des principales contributions au fait que LoRa est low power et long range, car peu d'interférence et très bien intégré aux appareils à faible puissance utilisés par les technologies LoRa. les end devices peuvent faire la démodulation.

spreading factor

détermine le taux de variation de fréquence pour le signal modulé. spreading factor ? augmenter le spreading factor augmente le temps pour envoyer un message.

faible spreading factor permet une consommation réduite mais réduit également la portée du signal.

Ajuster le spreading factor permet également de réduire l'impact des interférences

ccl : tradeoff

1.3.2 LoRaWAN

LoRaWAN est un protocole de type *low power, wide area network* (LP-WAN) désigné pour la communication longue portée. Ce protocole opère avec la technologie LoRa et lui fournit une infrastructure capable de maintenir une communication à longue portée et à faible coût dans l'*IoT*.

avantage

pourquoi s'en servir ?, faible puissance, portée accrue, pénétration efficace de l'environnement, déploiement ne nécessite pas de license, géolocalisable (le réseau peut détecter les devices), réseau public et privé, sécurité en end to end, mise à jour des micrologicielle par les air, programme de certification, vaste écosystème,

use case

use case : aspect environnemental catastrophe naturelle prevention, agriculture intelligente et supervision animale, protection des espèces menacées

aspect industrielle controle smart cities approvisionnement chaine logistique gestion installations diverses

limitations

payload limité (entre 51 et 241 octets)

data rate faible (maximum 5.5 kbps sur une bande de 125Hz)

restrictions liées aux régions (US, EU)

communication asynchrone

topologie**image network lorawan**

lora devices et lora gateway. gateway écoute plusieurs fréquence simultanément (multichanneling) tant qu'un end devices écoute une seule fréquence à la fois. transport entre end devices et gateway : uplink. sens inverse downlink.

end nodes connecté a des gateway. pas de lien direct le gateway écoute les end devices. les gateway forward les message jusqu'à un server réseau. les serveur indentifie le end devices. il gère la partie sécurité, l'information arrive à l'application.

LoRaWAN peut adapter le data rate en fonction de la topologie. par exemple ajuster le spreading factor en fonction de la distance entre les devices et les gateway. (ex : longue distance = grand spreading factor, lower data rate)

possibilité de mesurer la qualité du canal de communication (SNR). ex ajuster le data rate si bcp de bruit

Device class : A end nodes (most common), B beacon (deep sleep), C continuous downlink.

sécurité

Authentification : qui communique avec qui

intégrité : les données ne sont pas altéré entre émetteur et récepteur

confidentialité : le réseau ne peut pas voir les données.

chiffrement en AES deux types de clés

root key : clé partagée entre un end device et le serveur réseau. Utilisée pour l'authentification initiale et l'établissement d'une communication entre les deux éléments du réseau. Cette clé n'est jamais transmise par l'air et est stockée dans un *join server*

session keys : clé générée dynamiquement et utilisée durant l'échange de données pendant une session. Il y a deux session key différentes, la AppSKEY pour le chiffrement des payloads d'application, et la nwkSKEY pour les fonctionnalités du réseau (chiffrement à la couche MAC, integrity checks, etc).

un join server est un serveur dédié au contenu sensible à l'activation du matériel dans un réseau LoRaWAN. Il authentifie le réseau et les applications du serveur. Il gère les *root keys*, il génère les *session keys* et les distribue.

Taille de clé de 128 bits, pk aes et cette taille de clés ? pas trop de ressources donc taille minimale standard en terme de sécurité

session

deux types de sessions :

1 network session :

adresse du device, la session key, MAC state et frame counters

2 application session :

la session key, frame counters

la *frame counter* est une stratégie de défense servant à éviter les *replay attacks*, en rejettant les données dépassées ou retransmises.

comment établir une session ?

de manière dynamique en rejoignant un réseau (Over the air Activation *OTAA*) ou hardcodé (activation personnalisée *ABP*) *OTAA* : procédure entre end device et serveur réseau les clés sont régénérées à chaque nouvelle session *ABP* (moins safe mais moins contraignant en terme de ressources) : pas de procédure les clés sont hardcodées

Chapitre 2

Travaux similaires et autres contributions

Chapitre 3

Expérimentations

3.1 Matériel

3.1.1 radio logicielle

La radio logicielle (*SDR*, pour *Software-DefinedRadio*) est une technologie qui permet de mettre en œuvre des systèmes de radio à l'aide de logiciels plutôt que de matériel.

Dans les systèmes de radio traditionnels, les différentes fonctions de la radio, comme l'accord sur une fréquence spécifique, la modulation et la démodulation du signal, et le filtrage du bruit, sont mises en œuvre à l'aide de composants matériels tels que des oscillateurs, des amplificateurs et des filtres. En revanche, les systèmes SDR utilisent des logiciels pour effectuer ces fonctions, ce qui les rends beaucoup plus flexible car chaque composante est reconfigurable. Les radios logicielle sont capable d'opérer sur une large portée de fréquence, aussi bien très basse fréquence comme haute fréquence. Les *SDR* peuvent jouer le rôle d'émetteur ou de récepteur voir les deux.

RTL-SDR

image rtl sdr

La première radio utilisée comme récepteur. possède différentes composantes :
 rtl2832U : digitalise les signaux RF et les envoie à l'ordinateur. Tuner chip : le tuner permet d'ajuster la fréquence. Grâce à ça la sdr peut couvrir une large portée. port usb : pour raccorder la sdr à l'ordinateur.

hackRf**module RN2483**

Le microchip RN2483 est un module de technologie spécifique à LoRa. Cet appareil permet de communiquer à longue portée et à faible consommation grâce à l'utilisation de la modulation basée sur LoRa.

quelques spécificités du module :

technologie LoRa faible puissance (idéale pour de l'IoT car faible consommation) fréquence à 433, 868 et 915MHz (regarder la région adéquate) AT command : configurable via un set de commande compatible avec le protocole LoRa-WAN pour établir ou rejoindre ce type de réseau.

pycom fipy**3.1.2 logiciel****GNU radio**

GNU Radio est un toolkit qui permet de créer des flux de traitement de signal en utilisant des blocs prédéfinis. Ces blocs peuvent être combinés pour créer des chaînes de traitement de signal pour simuler des modulations CSS, capturer des signaux et en extraire des séquences de chirp.

gqrx

logiciel open source d'analyse de fréquence radio pour les SDR.

installer gqrx via apt. (ubuntu)

sélectionner le périphérique pour analyse

image choix périphérique

visualisation du spectre

deux formes d'affichage, en spectre et en cascade.

L'affichage du spectre fournit une représentation graphique en temps réel du spectre RF sur une gamme de fréquences. Il montre la puissance du signal de différentes fréquences sur une plage de fréquences spécifiée. L'axe des x représente la fréquence, tandis que l'axe des y affiche la force du signal (mesurée en dB).

L'affichage en cascade est un spectrogramme qui visualise la force du signal au fil du temps. Il montre une série d'instantanés de spectre empilés les uns sur les autres, où l'intensité de la couleur représente la force du signal. Chaque ligne horizontale du tracé en cascade représente une vue du spectre capturée à un moment précis, créant ainsi un enregistrement historique de l'activité du signal. L'axe vertical représente la fréquence et l'axe horizontal représente le temps.

image affichage spectre

configuration de la réception :

input control (pas trop touché)

FFt settings : très important règle la ff size, le rafraichissement d'image. le laps de temps. l'averaging

Le paramètre Panadapter dB fait référence à l'échelle verticale dans la vue du spectre. Il représente la force du signal des fréquences radio reçues affichées sur l'axe vertical du graphique du spectre. Le réglage du paramètre Panadapter dB modifie l'échelle verticale de la force du signal affichée dans la vue du spectre.

Le paramètre Waterfall dB concerne l'intensité de la couleur ou l'ombrage des fréquences affichées dans le tracé en cascade. Le réglage du paramètre Waterfall dB modifie l'intensité utilisée pour afficher la force du signal dans le tracé en cascade, permettant ainsi d'ajuster le contraste ou la visibilité des signaux plus faibles ou plus forts.

Universal radio hacker, URH

logiciel open

3.2 Génération et réception d'un signal LoRa

script pour module RN2483

set up parametre signal

lancer gqrx/urh

sélectionner rtl-sdr ou hackrf comme récepteur

configurer parem (frequence, sample rate, largeur de bande)

exec script (radio tx)

signal capturer dans le software

3.3 analyse du signal

preamble identifié ? up chirp (x10) down chirp ?(x2)

3.4 Méthode "Constellation traces"

Chapitre 4

Résultats

Conclusion

Mettez votre conclusion ici. Dressez le bilan de votre travail effectué, en prenant du recul. Discuter de si vous avez bien réussi les objectifs du travail ou non. Présentez les perspectives futurs.

Annexe A

Première annexe

Annexe B

Deuxième annexe