

Remerciements

Nous remercions ...

Table des matières

Introduction	2
1 Rappels et nomination des technologies	3
1.1 Signal radio	3
1.2 Traitement du signal	4
1.3 LoRa	8
1.3.1 couche physique LoRa	9
1.3.2 LoRaWAN	11
2 Travaux similaires et autres contributions	15
3 Expérimentations	16
3.1 Matériel	16
3.1.1 radio logicielle	16
3.1.2 logiciel	17
3.2 Génération et réception d'un signal LoRa	18
3.3 analyse du signal	18
3.4 Méthode "Constellation traces"	18
4 Résultats	19
Annexes	20
A Première annexe	20
B Deuxième annexe	21

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'émetteurs-récepteurs 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 quatre 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 rassemble les travaux qui ont déjà été effectués dans ce domaine. Le troisième 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'information. 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 *radio signal* ou signal radio. Voici les principaux attributs d'un signal radio :

- la fréquence, mesurée en Hertz (Hz). Elle détermine le nombre de cycle qu'accomplie le signal par seconde.
- La largeur de spectre, elle dépend de la fréquence car c'est l'écart entre la plus haute et la plus basse fréquence du signal. Une plus grande largeur permet de transmettre plus d'informations.
- 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 sert plutôt de marge entre les différents 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 symboles modifiés par seconde, et un symbole peut contenir plusieurs bit pour un signal numérique.

1.2 Traitement du signal

Modulation

La réception d'un signal nécessite des antennes dont les dimensions dépendent de la longueur d'onde du signal. Un signal à haute fréquence a l'avantage d'être facilement transmissible sur une grande portée. Cependant les signaux originaux (appelés *baseband signals*) sont en basse fréquence. La modulation d'un signal permet de transformer le signal en haute fréquence, devenant ainsi le signal modulé.

Parmi 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 gar-

dant la fréquence constante.

La modulation en amplitude est plus ancienne et est encore utilisée dans beaucoup de systèmes. Cette technique possède moins de contrainte et est notamment plus simple à implémenter. Elle requiert le signal modulant et un signal haute fréquence appelé *carrier signal*.

Soient un signal modulant $u(t)$ et un signal porteur (ou *carrier signal*) $v(t)$, la modulation en amplitude s'effectue en multipliant les deux signaux pour obtenir le signal modulé

$$s(t) = u(t) \cdot v(t)$$

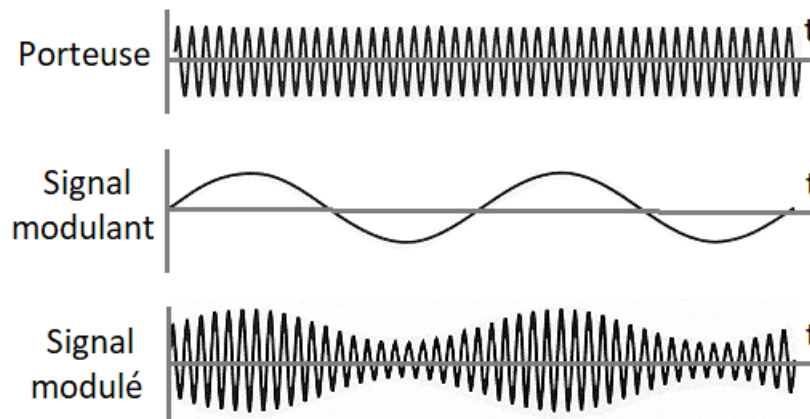


FIGURE 1.1 – Exemple de modulation en amplitude

La modulation en fréquence permet d'obtenir des transmissions de meilleures qualités plus résistantes à leur environnement tout en gardant une puissance d'émission constante.

Soient un signal modulant $u(t)$ et un signal porteur sinusoïdal

$$v_p(t) = A_p \cos(2\pi f_p t) \text{ où}$$

f_p est la fréquence de la porteuse,

A_p est l'amplitude de la porteuse,

alors le signal modulé $s(t) = A_p \cos(2\pi \int_0^t f(\tau) d\tau)$ où f est la fréquence instantanée. Elle s'exprime en fonction de la dérivation de fréquence f_Δ , c'est à dire la dérivation maximale par rapport à la fréquence de la porteuse.

$$f_p. f(t) = f_p + f_{\Delta}u(t)$$

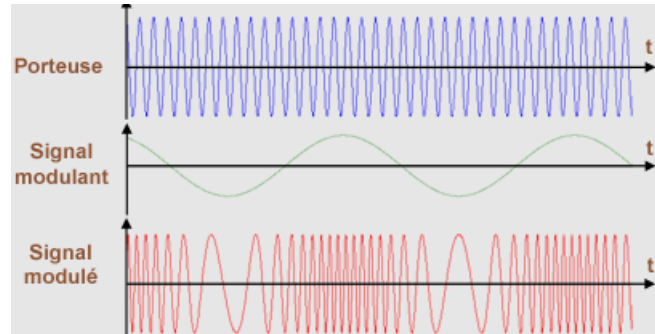


FIGURE 1.2 – Exemple de modulation en fréquence

Gestion du bruit

L'un des attributs cités concerne le bruit. Un signal est toujours affecté de petites fluctuations plus ou moins importantes, et dont les origines peuvent être diverses. Ces perturbations, appelée bruit ou *noise* en télécommunication se définissent par l'altération non souhaitée de l'intégrité d'un signal. Le bruit peut prendre différentes formes, des perturbations essentiellement impulsionnelles engendrées par des commutations de courants ou alors du bruit de fond généré dans les câbles et les composants électroniques en raison des mécanismes statistiques de la conduction électrique. Il est possible de réduire voir élimier l'influence des perturbations impulsionnelles. En revanche, le bruit de fond est lui irréductible. Tout signal sans bruit n'existe pas, même à l'émission. Il est cependant possible que le bruit devienne invisible si son niveau est très faible. L'attribut SNR est donc un critère de la qualité du signal.

transformée de Fourier

Pour effectuer une analyse de signal, sa représentation est capitale. Les Figure 1 et 2 représentent des signaux en fonction du temps écoulé. Il est possible de représenter des signaux selon une autre composante, la fréquence par exemple.

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 domaine 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 modulation*). 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 détaillée 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 dans le modèle *OSI*. la couche physique de LoRa gère la fréquence radio ainsi que la modulation. LoRaWAN gère les aspects réseaux comme la sécurité, la propagation, l'adressage et la sécurité).

1.3.1 couche physique LoRa

Découpage de la couche physique

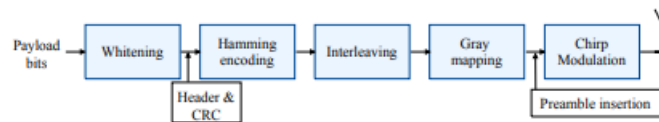


FIGURE 1.3 – Etapes de la transformation des données dans un émetteur LoRa

Les étapes de la conception de l'envoi de données dans 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 utilise la méthode *FEC* (*Forward error correction*) pour corriger les erreurs causées par du bruit. La méthode FEC ajoute de l'information redondante sur les données.
- Le mélange de canal (ou *channel interleaving*) suit la codage de canal. Cette technique consiste à réarranger les bits de data avant de les transmettre, en les intercalant entre eux de manière à les disperser sur le spectre des fréquences de la transmission. Cela permet de réduire l'impact des erreurs consécutives (*burst error*).
- Le blanchiment de canal (ou *channel whitening*) est la dernière étape avant la modulation du signal. 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 également la récupération d'horloge pour le récepteur.
- La modulation CSS est l'étape principale de LoRa. En effet, les étapes précédentes sont communes à de nombreuses technologies, mais la particularité de LoRa provient de la modulation. Cette étape est détaillée dans la section suivante du chapitre.

Chacune des étapes décrites doit être inversement réalisée pour le récepteur. Ainsi pour la récupération de donnée à l'arrivée, l'appareil récepteur gère la démodulation, le déblanchiment, le démellement et de décodage.

Cette analyse a été faite en *reverse engineering* ([citer article](#)). 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

Contrairement aux modulation classique en amplitude ou en fréquence, la modulation CSS étale le signal sur une large bande de fréquence. La modulation en fréquence est linéaire et utilise des chirps. un chirp est un signal dont la fréquence change en continue tout en conservant une amplitude constante. Il existe deux types de chirps : les *upchirp* et *downchirp*. Dans un upchirp la fréquence augmente avec le temps tandis que dans un downchirp la fréquence diminue.

le signal est donc séparé sur une large bande de fréquence, permettant par exemple plusieurs transmission sans causer d'interférence. La modulation CSS est l'une des principale contribution au fait que LoRa possède une faible consommation et une longue portée. Cette technioque est très bien intégrée aux appareils a faible puissance utilisé par les technologies LoRa.

Spreading factor

LoRa permet d'envoyer des paquets sur un longue distance à faible puissance. Selon l'environnement dans lequel les appareils LoRa sont présents, il peut être utile de pouvoir ajuster certaines capacités.

L'étalement, ou *spreading factor* permet de déterminer le taux de variation de fréquence pour un signal. Modifier le spreading factor ajuste différentes propriétés de la communications. Par exemple, si on augmente le spreading factor, les quatre conséquences principales sont :

- l'augmentation de la portée. Comme la largeur de bande est plus large, la communication peut atteindre une portée supérieure.
- Augmentation de la résistance aux interférences. Comme le signal est étalé sur une bande plus largeur, il y a moins de risque de subit des interférences.
- Plus petit débit de données. Comme la bande est large, dans un temps défini moins de données sont transmises.

- Plus faible consommation. Les données transmises à un taux plus faible consomment moins d'énergie, ce qui prolonge la durée de vie des appareils dont l'économie d'énergie est une priorité.
- Diminuer le spreading factor engendre l'effet inverse.

Structure d'un paquet LoRa

un paquet LoRa est structuré en 5 parties différentes :

- Le préambule : la première partie du paquet, composée d'un nombre variable d'upchirps. La valeur par défaut est fixée à 8 upchirps.
- L'identificateur réseau : après le préambule, le paquet contient deux symboles modulés pour l'identification réseau.
- Des symboles de synchronisation de fréquence. Après l'identificateur réseau, il y a des downchirps pour faire la distinction entre les offsets d'échantillonnage de temps ou de fréquence.
- La tête (*header*) du paquet. Elle contient les informations relatives à la taille du paquet, le code rate, la présence ou non d'un CRC (*cyclique redundancy check*) et une checksum.
- Le payload. La dernière partie du paquet contient le payload d'une taille maximale de 255 bits et l'éventuelle CRC de 16 bits.

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*.

aspects généraux de la technologie

LoRaWAN bénéficie donc d'une faible puissance de consommation et d'une portée accrue. Elle est également efficace dans différents environnements. Le signal est capable de pénétrer divers terrains et structures. Le déploiement d'une infrastructure LoRa ne nécessite pas de licence, et son réseau peut être public ou privé.

Le cœur de LoRaWAN réside sur la gestion de l'énergie, permettant aux appareils de fonctionner avec une consommation d'énergie minimale, prolongeant leur durée de vie tout en garantissant une fonctionnalité à long terme. À cette caractéristique de faible consommation d'énergie s'ajoutent ses capacités en termes de portée, capable de pénétrer divers environnements. Cela rend la technologie efficace aussi bien en milieu rural qu'urbain. LoRaWAN opère sur une bande de fréquence qui ne nécessite pas de licence d'émission, par exemple sur la bande ISM

pour *Industrial, Scientific, and Medical*. Les bandes ISM, (868 MHz en Europe ou 915 MHz aux USA) sont disponibles pour l'utilisation de différentes technologies, incluant LoRaWAN.

LoRaWAN possède des capacités de géolocalisation, permettant au réseau de détecter et de localiser précisément les appareils au sein de son domaine. LoRaWAN utilise différentes méthodes pour localiser ses appareils comme **Received signal strength indication** ou RSSI, *Time difference on Arrival* ou TDOA, une triangulation ou alors une combinaison de plusieurs des méthodes.

LoRaWAN utilise des protocoles de sécurité end-to-end, aussi bien dans un réseau public intégré que dans un réseau privé. L'architecture LoRaWAN (décrite en détails dans la section 1.3.2.2) contient plusieurs couches de sécurité. Au niveau des *end devices*, une routine d'identification est imposée avant l'accès au réseau. Seuls les appareils de confiance sont donc autorisés à communiquer. Ensuite, une fois la communication commencée, les données sont chiffrées avant d'être transmises dans le réseau. Le framework sécuritaire de LoRa ne se limite pas à l'authentification et au chiffrement. LoRaWAN gère également la mise à jour en continu par les airs, ainsi qu'une supervision continue sur d'éventuelles intrusions.

Avec toutes ces caractéristiques, LoRaWAN s'est développé dans de nombreux domaines aussi bien environnementaux qu'industriels. Les principales utilisations de LoRaWAN actuelles sont les suivantes :

- la surveillance environnementale en général. LoRaWAN peut être déployé pour surveiller des niveaux de températures, d'humidité, de bruits ou encore d'autres paramètres dans n'importe quel milieu. Une compagnie Hollandaise, Sensoterra, utilise notamment LoRaWAN pour surveiller la qualité des sols.
- Les *smart cities*. LoRaWAN est actif sur différents aspects comme la gestion intelligente de l'éclairage, la gestion des déchets, la surveillance, etc.
- l'embarqué industriel. La maintenance et la surveillance de matériel et de l'équipement peut être gérée par LoRaWAN ? TataSteel, une compagnie indienne utilise LoRaWAN pour ces équipements industriels
- la prévention de catastrophe naturelle. Que ce soit en prévision, pendant ou après d'éventuelles catastrophes naturelles, la longue portée et la surveillance en temps réel sont des atouts cruciaux pour ce genre d'évènement.

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 logis-

tique 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.

chiffrage en AES deux types de clefs

root key : clé partagé 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 les air et est stockée dans un *join server*

session keys : clé générée dynamiquement et utilisé durant l'échange de donnée pendant une session. Il y a deux session key différente, la AppSKEY pour le chiffrage des payload d'application, et la nwSKEY pour les fonctionnalité du réseau (chiffage à la couche MAC, integrity checks, etc).

un join server est un server dédié au contenu sensible à l'activation du matériel dans un réseau LoRaWAN. Il authentifie le réseau et les application du servers. 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 devices, 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 rejttant les données dépassée ou retransmise.

comment établir une session ?

de manière dynamique en rejoignant un réseau (Over the air Activation *OTAA*) ou hardcodé (activation personnalisée *ABP*) *OTAA* : procedure entre end devices 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 hardcodés

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 param (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

Annexe A

Première annexe

Annexe B

Deuxième annexe