Remerciements

Nous remercions ...

Table des matières

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 technoligies utilisées pour l'IoT étaient les technologies sans fil déja 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 cout d'infractrucutre trop important.

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

L'expansion de L'Iot soulève une nouvelle problèmatique de sécurité. Entre autres, l'indentification des noeuds au sein des réseaux est essentielle. Il a été découvert que des noeuds 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 noeuds 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 concept de télécommunication de base. Ce chaptire 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 expérimental du sujet. Les aspect pratique y seront appliqués, notamment l'utilisation de radio logicielle afin de capturer des signaux radio. Ces signaux seront ensuite analysé grace à diverse méthodes détaillé dans ce chapitre.

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

Chapitre 1

Rappels et nomination des technologies

1.1 Traitement du signal et 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 dépent 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 incompatible car il est souvent nécessaire en télécommication de pouvoir passer de l'un à l'autre.

L'utilisation de signaux radio en télécomunication confère de nombreux avanages, comme la portée, la vitesse de transmisison , la résistance aux interférence ou encore le coût de propagation. Tout ces avantages sont possible car un signal peut être modulé. La modulation est un 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 principals attributs d'un signal radio :

- la frécquence, mesurée en Hertz. Elle détermine le combre de cycle qu'accomplie le signal par seconde.
- La largeur de spectre, elle dépent de la fréquence car c'est l'écart entre la plus haute fréquence et la plus basse du signal. Une plus grande parleur permets 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 caractéristique principale d'identification du signal mesurant l'ampleur du

signal. dans un signal numérique l'amplitude set plutot 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 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 excatement 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.

Parmis ces différents attributs, certains sont utilisés pour effectuer une modulation. Les deux modulations les plus utilisés sont basées sur les attributs de la frécquence et de l'amplitude. La modulation en fréquence (ou FM pour $frequency\ modulation$) consiste à encoder l'information en faisant varier la frécquence en maitenant l'amplitude constance. La modulation en amplitude (AM) est le procédé inverse, c'est à dire encoder l'informatino en faisant varier l'amplitude tout en gardant la frécquence 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 ?

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

plus loin dans l'impact du bruit ?

1.2 LoRa

$LoRa$ (Long Range) est une technologie de communication sans fil basée sur la modulation en fréquence chirp spread spectrum (CSS), 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 utilisée dans de nombreux domaines, tels que l'Internet des objets (IoT), la télématique, la météorologie, la surveillance environnementale, la gestion de l'énergie, la sécurité et la santé. 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.

LoRa utilise une bande de fréquences dédiée, qui varie selon les régions du monde. En Europe, par exemple, la bande de fréquences autorisée est comprise entre 863 et 870 MHz, tandis qu'aux États-Unis, elle se situe entre 902 et 928 MHz. 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.

LoRa est conçue pour être utilisée dans des réseaux de communication à mailles (mesh networks), où chaque appareil peut agir en tant que nœud de transmission et de réception, ce qui permet de créer des réseaux étendus et robustes. 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.

1.2.1 couche physique LoRa

Dans le premier chapitre de ce travail se trouve une analyse de l'impementation de LoRa dans un SDR. Cette analyse a été faite en $reverseengeneering$. 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. 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 dernirèe des méthode d'amélioration de la robustesse de la tranmission 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'im-

pact 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 aux 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 noeud éméteur.
— demodulation CSS
— dewhitening
— deineterleaving
— decoding

1.2.2 modulation CSS

1.2.3 LoRaWAN

Chapitre 2

Travaux similaires et autres contributions

Chapitre 3

Expérimentations

3.1 Ressources

3.1.1 Matériel

La radio logicielle (SDR, pour $Software\text{-}DefinedRadio$) 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 permet une plus grande souplesse et adaptabilité. Les systèmes SDR peuvent être facilement reconfigurés pour prendre en charge différents types de systèmes de radio et de protocoles en modifiant le logiciel qui les contrôle. Cela rend les systèmes SDR particulièrement utiles pour les applications qui nécessitent la possibilité de prendre en charge plusieurs systèmes de radio ou qui doivent être reconfigurées pour prendre en charge de nouveaux types.

Les systèmes SDR sont utilisés dans une variété de domaines comme la télécommunication, la radiodiffusion ou encore la défense.

3.1.2 logiciel

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.

3.2 mise en place d'un scénario

3.3 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