I²PHEN : une nouvelle plateforme de télésurveillance médicale basée sur l'Internet des Objets

Alexis Picard

SPIM

Thèse de Doctorat

I²PHEN : une nouvelle plateforme de télésurveillance médicale basée sur l'Internet des Objets

Thèse CIFRE - laboratoire Femto-st/DISC et l'entreprise Maincare Solutions - préparée à l'Université de Franche-Comté

Alexis PICARD

SPIM

Thèse de Doctorat

THÈSE présentée par

ALEXIS PICARD

pour obtenir le

Grade de Docteur de

l'Université de Bourgogne/Franche-Comté

Spécialité : **Informatique**

I²PHEN : une nouvelle plateforme de télésurveillance médicale basée sur l'Internet des Objets

Thèse CIFRE - laboratoire Femto-st/DISC et l'entreprise Maincare Solutions - préparée à l'Université de Franche-Comté

Unité de Recherche :
Femto-st/DISC

Soutenue publiquement le 3 décembre 2020 devant le Jury composé de :

DIDIER DONSEZ	Rapporteur	Prof., Université de Grenoble Alpes
PHILIPPE ROOSE	Rapporteur	Prof., Université de Pau et des Pays de l'Adour
SAÏD TAZI	Examinateur	MdC HDR, Université de Toulouse 1 Capitole
CHRISTOPHE NICOLLE	Président	Prof., Université de Bourgogne/Franche-Comté
JEAN-CHRISTOPHE LAPAYRE	Directeur	Prof., Université de Bourgogne/Franche-Comté
RONNIE MUTHADA POTTAYYA	co-Directeur	Doc. Ingé. de Recherche - Maincare Solutions

Remerciements

Je remercie sincèrement les personnes qui m'ont épaulé durant toute l'élaboration de ma thèse. Pour son intérêt, sa disponibilité, ses nombreuses relectures et sa sympathie entre autres, je remercie tout particulièrement mon directeur de thèse Monsieur le professeur Jean-Christophe Lapayre, sans qui, la thèse n'aurait pas vu le jour, et n'aurait peut-être pas été à son terme. Je remercie chaleureusement, Ronnie Muthada Pottayya, cher collègue, pour toute son aide et son attention jusqu'à la fin, notamment dans la rédaction des articles. Pour terminer, je remercie Fouad Hanna, pour toutes ses contributions sur les articles, et ses bons conseils.

Ce travail n'aurait pas été possible sans le soutien d'Éric Garcia et de Covalia, la branche télémédecine du groupe Maincare Solutions, ainsi que le laboratoire Femto-ST de l'Université de Franche-Comté, qui m'ont permis de me consacrer sereinement à l'élaboration de ma thèse sous le dispositif CIFRE le financement de l'ANRT. Je remercie les membres du jury, Didier Donsez et Philippe Roose pour leur lecture et remarques instructives, Christophe Nicole pour sa présidence du jury, et Said Tazi.

Ce travail n'aurait pu être mené à bien sans la disponibilité et l'aide précieuse de Michael J. Kirwan, Ian Hay de la Continua Health Alliance, Gilles Lunzenfichter et Lionel Cavalliere de l'entreprise Suisse Médisanté, Laurent Bouskela de Orange, Paul Picault ambassadeur SigFox et blogueur expert en IoT ainsi que toutes les personnes qui ont pu m'aider au cours de mes recherches.

Au terme de ce parcours, je remercie enfin celles et ceux qui me sont chers, pour leurs attentions et encouragements qui m'ont accompagné tout au long de ces années :
les copains : Max, Clem, Marion, Axel, Anais, Pierre, Marie, et tous les Deluziens,
les gars du foot, Nico, Balo, Hugues et Manon (team raclette),
les BG des Essarts l'Amour, Guigui, Alizé, Mich, Wawa, Eve, Nana,
les collègues de Covalia, Thomas, Kévin, Cédric, Vince, Tommy, Mathieu, Sylvain, le reste de la team mobile, JV, toute l'équipe Covotem, le service, les Dijonnais (et j'en oublie beaucoup d'autres...),
la team du lundi midi : Lolo, JB, Roro, Fouad et JC, la team Kikoune.

Je suis reconnaissant à mes parents et à ma sœur pour leurs soutiens, et tout particulièrement à ma maman, correctrice officielle de la famille.

J'ai une pensée toute particulière pour mes grands-parents (qui se sont souciés de mon avenir avec beaucoup de prières !), ma famille, mes cousins et cousines, mes oncles et tantes, ma filleule et ma belle-famille.

Je remercie le confinement causé par la COVID 19, car sans lui, je n'aurais jamais eu assez de temps pour finir la rédaction ainsi que Google translate, sans qui, je n'aurais jamais compris certains articles.

Ces remerciements ne peuvent s'achever, sans une pensée pour ma première fan, Mégane, qui m'a soutenu tout au long et avec qui je partage ma vie depuis 8 ans. Ta présence et tes encouragements sont pour moi les piliers fondateurs de ce que je suis et de ce que je fais.

Je dédie cette thèse à notre bébé (fille ou garçon ?), peut-être qu'un jour tu liras ceci : bonne chance pour faire mieux que ton papa !

TABLE DES MATIÈRES

INTRODUCTION

INTRODUCTION GÉNÉRALE

Les objets connectés sont aujourd'hui largement utilisés dans le domaine de la santé et ils tendent à le devenir davantage. L'usage de ces dispositifs médicaux connectés pour soigner des patients en dehors de l'hôpital deviendra une pratique courante dans les années à venir : il s'agit de télémédecine, et plus précisément de la télésurveillance médicale quand il s'agit de contrôler à distance les paramètres vitaux des patients.

La télésurveillance médicale est un domaine encore en plein développement en France. C'est une branche de la télémédecine qui a pour vocation de permettre à un médecin de recueillir et d'interpréter à distance les données nécessaires au suivi médical d'un patient. Elle permet, entre autres, d'améliorer le suivi médical à distance des personnes âgées en perte d'autonomie ou atteintes de pathologies chroniques (insuffisance cardiaque, diabète et hypertension artérielle par exemple) et ainsi de favoriser leur maintien à domicile et de prévenir, au plus tôt, d'éventuelles hospitalisations. Cette médecine à distance, aidée par des dispositifs connectés, peut parfaitement tirer profit aujourd'hui de ce que l'on désigne couramment comme l'Internet des Objets (*IoT*).

L'Internet des Objets (IdO) ou *Internet of Things (IoT)* est devenu un terme couramment utilisé pour désigner l'ensemble des objets physiques connectés à Internet permettant une communication entre nos biens et leur existence numérique [Bri16]. Il a des applications dans de nombreux domaines, tels que la surveillance [Ciu19], le transport [Kir15] [Zha11], la banque [Hao18], l'environnement [Bov19], les services publics [Zha11] [Jis17], les villes intelligentes [Liu19], l'agriculture [Kha16], la santé et le bien-être [Swa19] ...

Ces applications nécessitent un nombre massif de terminaux, ce qui conduit à la nécessité de réseaux extrêmement denses. Un certain nombre d'applications est basé sur des réseaux de capteurs sans fil dans lesquels l'énergie est le problème le plus important. Ainsi, une consommation d'énergie extrêmement faible des appareils est un, si ce n'est le challenge pour les nouveaux réseaux de l'IoT.

Dans le domaine de la e-Santé, l'IoT améliore les applications de manière large : par exemple la gestion des actifs et des interventions dans les hôpitaux, la télésurveillance, l'aide à la vie autonome, le changement de comportement, l'observance du traitement, la télémédecine, la prise de médicaments plus intelligemment... Les orientations actuelles des recherches dans le domaine de l'IoT pour la santé incluent, entre autres, les architectures et plateformes de réseaux, les nouveaux services et applications, l'interopérabilité et la sécurité.

CONTEXTE DE LA THÈSE

Cette Thèse est réalisée dans le cadre d'un dispositif CIFRE (3ème Thèse de collaboration entre les deux entités). Le projet de recherche s'est déroulé entre l'Université de Bourgogne Franche-Comté (Institut CNRS Femto-st) et l'entreprise Maincare Solutions, édi-

teur majeur de solutions digitales pour le monde de la santé. Cette dernière est basée à Canéjan, près de Bordeaux, et possède une antenne de télémédecine (télédiagnostic, télésurveillance...) basée sur la Bourgogne/Franche-Comté. Cette antenne est issue de la startup Covalia/IDO-In et du Laboratoire Femto-St. Elle propose une solution logicielle de collaboration en temps réel autour de la consultation et du diagnostic à distance. La suite *Covalia*^{TM} offre des fonctionnalités de télé-consultation et de télé-expertise. Elle permet, par exemple, d'effectuer à distance avec le patient des diagnostics, dans le domaine des accidents vasculaires cérébraux, mais également la réalisation de réunions de concertations pluridisciplinaires, entre spécialistes et ce afin de coordonner les avis des différents experts.

Dans ce contexte, avec l'apparition de très nombreux *Connected Medical Devices* (plus utilisés dans le domaine domestique du sport par exemple) d'une part, et de l'avènement du monde de l'Internet des Objets (*IoT*) d'autre part, il est important de poser les bases de l'utilisation de ces nouvelles technologies dans le domaine très contraint du suivi de patients à distance : c'est le cœur même des travaux menés en collaboration entre les deux partenaires de cette thèse CIFRE.

Notons : la répartition des recherches a été de 1 jour à l'Université pour 4 jours en entreprise les deux premières années, et 2 jours à l'université pour 3 jours en entreprise la dernière année. Sur l'ensemble de la période de déroulement de la thèse, cela représente une moyenne de 1.33 jour à l'Université par semaine.

Objectifs de ces travaux

L'objectif principal de cette thèse est de présenter une nouvelle plateforme de télésurveillance médicale utilisant les technologies novatrices de l'Internet des Objets tout en s'intégrant dans les systèmes de soin existants.

Nous proposons ainsi, dans nos contributions, la nouvelle plateforme I^{2}PHEN (**I**oT **I**nteroperable **P**latform for **HE**alth mo**N**itoring low power) au sein de laquelle le suivi des paramètres de santé du patient est réalisé à l'aide d'objets connectés (tensiomètre, thermomètre, glucomètre...). Ceux-ci communiqueront avec la plateforme distante (monitoring de données distribuées) à l'aide des réseaux de l'Internet des Objets que nous étudions dans l'état de l'art.

Le premier verrou sera la consommation énergétique, en relation avec la qualité de service, de ces nouveaux réseaux dans le domaine critique de la santé.

Le second verrou, et probablement le plus difficile, est de proposer des solutions d'interopérabilité pour que les dispositifs médicaux existant sur le marché puissent s'intégrer et dialoguer facilement avec le système de télésurveillance et les autres systèmes de soin comme les plateformes de télémédecine.

Ce domaine étant nouveau, et encore peu dédié au milieu médical, il sera également nécessaire de développer de nouveaux axes de recherche comme COMMA, un nouveau mécanisme dédié à la technologie de communication LoRaWAN permettant de réduire la consommation énergétique et les interférences en mobilités quotidiennes.

Plan du mémoire

Cette thèse s'inscrit dans le domaine de la télémédecine et plus particulièrement de la télésurveillance médicale. Elle vise à élaborer une plateforme de télésurveillance médicale

novatrice en utilisant les technologies émergentes de l'Internet des Objets.

Dans la première partie de ce mémoire, nous présentons l'état de l'art dans le domaine de l'Internet des Objets et de la télésurveillance médicale.

Le premier chapitre est consacré à la présentation du contexte de notre thématique de recherche. Nous présentons l'Internet des Objets appliqué au domaine de la santé, puis de la télémédecine et particulièrement du cœur de cette thèse : la *télésurveillance médicale*. L'architecture d'une plateforme de télésurveillance médicale type est décrite puis nous comparons quelques exemples déjà existant dans la littérature.

Dans le deuxième chapitre, nous mettons en avant les dispositifs médicaux connectés et les objets connectés de santé. Nous étudions dans un premier temps l'aspect réglementaire des dispositifs médicaux. Nous listons ensuite les différents objets disponibles sur le marché et nous décrivons leurs fonctionnalités et leurs applications. Nous terminons ce chapitre avec un point sur leur intégration dans une plateforme de soin et les problématiques d'interopérabilité qui en découlent.

Le troisième et dernier chapitre de l'état de l'art est consacré aux réseaux de l'Internet des Objets. Nous évoquons dans un premier temps les communications radiofréquences, les types de réseaux par étendues spatiales, le modèle OSI ou encore les bandes de fréquences ISM. Puis, nous étudions les différent réseaux, et particulièrement les réseaux *Low-Power Wide-Area-Networks* (LoRAWAN, Sigfox, NB-IoT et LTE-M), que nous confrontons dans un tableau comparatif. Nous approfondissons plus particulièrement la technologie LoRaWAN, et son algorithme de débit adaptatif ADR ainsi que son modèle énergétique.

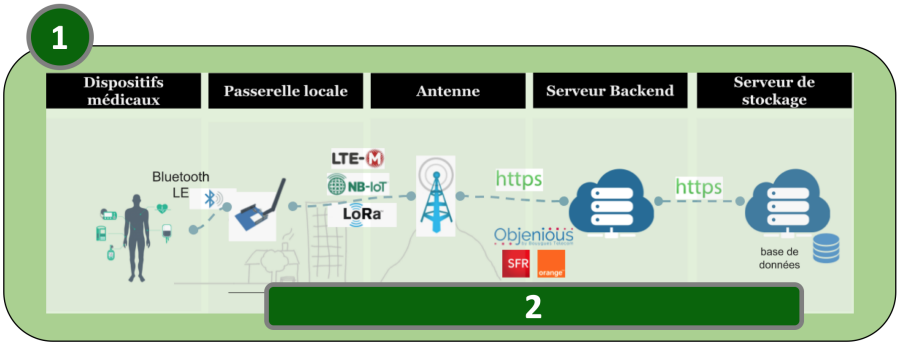


FIGURE 1 – Contribution autour de la nouvelle plateforme I²PHEN (**I***oT* **I***nteroperable* **P***latform for* **HE***alth mo***N***itoring low power*).

La deuxième partie de ce mémoire est le cœur de notre contribution (cf figure 1) :

❶ Le premier chapitre (chapitre 4), de la contribution, est consacré à la présentation de la plateforme I²PHEN (**I***oT* **I***nteroperable* **P***latform for* **HE***alth mo***N***itoring low power*), ses attentes, son architecture avec les différents acteurs, ses fonctionnalités, ses technologies de communication et sa sécurité.

❷ Le second chapitre (chapitre 5), de la contribution, est dédié à l'amélioration de l'algorithme ADR de la technologie de communication LoRaWAN, pour une utilisation en mobilité quotidienne. La description du nouvel algorithme COMMA (*Communication Optimisation Mechanism for Mobility Adaptation*) est accompagné de la phase expérimentale. À

partir des résultats obtenus et des modèles de calcul de consommation énergétique, nous comparons les performances des différents algorithmes.

En conclusion de ce mémoire, nous résumons les différents apports de nos contributions et nous exposons les perspectives et évolutions possibles de la plateforme qui pourront faire l'objet de futurs thèmes de recherche. Ainsi les perspectives des travaux communs du Laboratoire Femto-st et de l'entreprise *Maincare Solutions* sont exposées.

Quelques indications pour la lecture de ce rapport

Le plan est organisé sur quatre niveaux : Parties, Chapitres, Sections et Sous-Sections. Il est utile de savoir que la Partie II, présentant les contributions et résultats, est indépendante de la première Partie.

Les résultats de nos travaux ont pour la plupart été publiés. La liste des publications personnelles est donnée avant la bibliographie placée en fin du document.

I

ÉTAT DE L'ART

Cette partie est consacrée à l'état de l'art de la télésurveillance médicale en utilisant les nouvelles technologies de l'Internet des Objets.

Nous allons dans un premier temps définir l'Internet des Objets, ainsi que son potentiel applicatif dans le domaine de la santé. Nous parlerons de télémédecine et plus précisément de télésurveillance médicale, pratique permettant de contrôler à distance les paramètres vitaux des patients à l'aide de dispositifs médicaux connectés. Nous verrons ensemble les plateformes déjà existantes, leurs fonctionnements, et la recherche associée.

Dans un second temps, nous étudierons les objets connectés de santé et les dispositifs médicaux connectés existants. Cela nous donnera un aperçu des possibilités de suivi d'une telle plateforme. Nous définirons les contraintes réglementaires, les différentes classes de risques, et le marquage CE des dispositifs médicaux. Pour terminer, nous détaillerons leur intégration dans une plateforme de télésurveillance, dont l'interopérabilité en est la principale difficulté.

Dans le 3ème, et dernier chapitre de l'état de l'art, nous aborderons les réseaux sans fil destinés à l'Internet des Objets. Nous exposerons le fonctionnement des réseaux sans fil et les transmissions par ondes radiofréquences, les attentes de ces réseaux pour l'IoT et les différents types de réseaux par étendue spatiale. Nous nous consacrerons ensuite à la description des différents réseaux destinés à l'IoT (LoRaWAN, Sigfox, LTE-M, NB-IoT, Bluetooth Low Energie ...).

1

CONTEXTE GÉNÉRAL

Les objets connectés sont aujourd'hui largement utilisés dans le domaine de la santé et ils tendent à le devenir davantage. L'usage de ces dispositifs médicaux connectés pour soigner des patients en dehors de l'hôpital deviendra une pratique courante dans les années à venir : il s'agit de télémédecine, et plus précisément de la télésurveillance médicale quand il s'agit de contrôler à distance les paramètres vitaux des patients. Cette médecine à distance, aidée par des dispositifs connectés, s'intègre parfaitement dans ce qui est aujourd'hui couramment désigné comme l'Internet des Objets (*IoT*).

1.1/ L'INTERNET DES OBJETS POUR LA SANTÉ

L'Internet des Objets (IdO) ou *Internet of Things (IoT)* est devenu un terme couramment utilisé pour désigner l'ensemble des objets physiques connectés à Internet permettant une communication entre nos biens et leur existence numérique [Bri16].

L'IERC (*IoT European Research Cluster*) définit l'Internet des Objets comme une infrastructure mondiale de réseaux dynamiques avec des capacités d'autoconfiguration basées sur des protocoles de communication standards et interopérables dans lesquels les objets physiques et virtuels :

- possèdent des identités, des attributs physiques et des personnalités virtuelles,
- utilisent des interfaces intelligentes,
- s'intègrent de manière transparente dans le réseau d'informations.

Dit autrement, l'Internet des Objets est une infrastructure réseaux extrêmement complexe, dynamique et flexible qui peut connecter n'importe quoi, n'importe qui, n'importe quand, n'importe où, pour n'importe quel service.

L'IoT a des applications dans de nombreux domaines, tels que la surveillance [Ciu19], le transport [Kir15] [Zha11], la banque [Hao18], l'environnement [Bov19], les services publics [Zha11] [Jis17], les villes intelligentes [Liu19], l'agriculture [Kha16], la santé et le bien-être [Swa19] ... Ces applications entraînent un nombre massif de terminaux, ce qui conduit à la nécessité de réseaux extrêmement denses. Un certain nombre d'applications est basé sur des réseaux de capteurs sans fil dans lesquels l'énergie est le problème le plus important. Ainsi, une consommation d'énergie extrêmement faible des appareils est un, si ce n'est le, challenge pour les nouveaux réseaux de l'IoT.

Dans le domaine de la e-Santé, l'IoT améliore les applications de manière large : par exemple la gestion des actifs et des interventions dans les hôpitaux, la télésurveillance, l'aide à la vie autonome, le changement de comportement, l'observance du traitement, la télémédecine, la prise de médicaments plus intelligemment... Les orientations actuelles des recherches dans le domaine de l'IoT pour la santé incluent, entre autres, les architectures et plateformes de réseaux, les nouveaux services et applications, l'interopérabilité et la sécurité.

Le travail sur la diminution de la latence dans les réseaux sans fil, notamment avec l'arrivée de la 5G dès 2020, permettra également d'offrir une nouvelle vague d'innovations dans ce qui est appelé le domaine de *l'Internet tactile* par le Professeur Gerhard Fettweis [Fet14]. Ce domaine est défini comme un réseau ultra-réactif et ultra-fiable capable de fournir des expériences haptiques [1] physiques à distance [Itu14]. Cela permettrait d'offrir des services médicaux sophistiqués ubiquitaires, c'est-à-dire n'importe où, n'importe quand et à n'importe qui. L'expertise médicale à l'aide d'outils de télédiagnostic avancés en est l'exemple, permettant un examen physique à distance (même au toucher) via un robot contrôlé à distance. Les interventions téléchirurgicales sophistiquées ou bien encore les applications de télé-rééducation via un exosquelette contrôlé à distance en sont d'autres exemples.

La e-Santé est donc une application extrêmement importante à prendre en compte pour les prochaines générations de réseaux sans fil. Le marché mondial de l'IoT pour la santé devrait passer de 55,5 milliards de dollars en 2019 à 188 milliards USD d'ici 2024 avec un taux de croissance annuel composé de 27,6% selon l'étude de MarketsAndMarkets [Mam19] (cf figure 1.1).

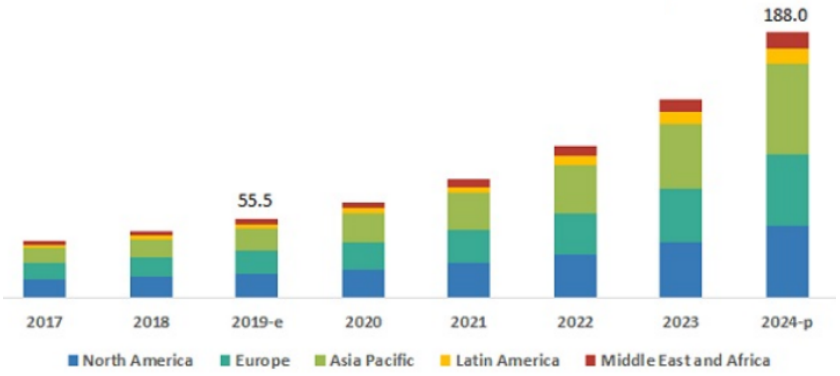


FIGURE 1.1 – L'IoT dans le marché de la santé, par région (en milliards de dollars) - [Mam19].

Le marché évolue quant à lui avec les facteurs clés suivants :

- la croissance des technologies de réseaux haute vitesse et faible latence,
- la consommation d'énergie, en lien avec la durée de vie des batteries pour l'IoT,
- la couverture des réseaux publics pour que les objets soient connectés sur l'ensemble du territoire, et indépendamment d'une passerelle tierce comme un smartphone.

1. qui concerne le sens du toucher

1.1.1/ La protection des données de santé

L'Internet des objets génère une multitude de nouveaux objets et de nouvelles applications dans la vie de tous les jours, et notamment dans la santé. La conséquence est une démultiplication de la quantité de données utilisée dans ces applications. La sécurisation et la protection des données, notamment de santé, est un enjeu crucial dans l'évolution de l'Internet des objets.

Selon le RGPD [1] [Rgp18], entré en application le 25 mai 2018, les données de santé sont *« les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne»*. Par conséquent, sont concernés par les données de santé :

- n'importe quel élément (identifiant, symbole...) pour identifier directement ou indirectement une personne physique à des fins de santé,
- toutes informations obtenues lors d'examen de santé,
- toutes informations qui concernent une maladie.

Il est intéressant de noter que les données concernant les applications de fitness ou d'alimentation ne sont pas considérées comme des donnée de santé (sans l'intervention d'un professionnel de santé).

Le règlement RGPD marque par la même occasion l'avènement d'une règlementation plus stricte, harmonisée et adaptée aux nouveaux usages de l'Internet des Objets. Les principes clés du RGPD sont notamment : une application en dehors de l'Union Européenne et harmonisée dans celle-ci, un contrôle et une visualisation des données privées par les citoyens, une transparence des entreprises sur les usages ou encore les pertes de données... Il définit enfin des sanctions conséquentes envers les entreprises qui ne suivraient pas le règlement.

Par conséquent, le RGPD définit le concept de *« privacy by design »* : sans le consentement clair et explicite de la personne concernée bien informée de la finalité, l'utilisation ou la commercialisation de données de santé relatives à une personne identifiée ou identifiable est interdite. L'utilisation des données est toutefois autorisée à des fins de médecine préventive, de diagnostics médicaux, ou d'administration de traitements si elle est mise en œuvre par un professionnel de santé ou justifiée par l'intérêt public (propagation de maladies ou dans le cadre d'une recherche publique par exemple).

Les entreprises qui récoltent, utilisent et stockent les données de santé, doivent ainsi prendre des mesures de protection conséquentes pour limiter le risque d'une fuite de données. Si le cas se produit, elle ont le devoir d'informer immédiatement l'autorité compétente en terme de protection des données à caractère personnel : la CNIL [2]. Elles peuvent être tenues pour responsable si les mesures de protection des données n'étaient pas appropriées.

Afin de renforcer la protection des données de santé à caractère personnel et la confiance dans la e-Santé, la certification HDS (*Hébergement de données de Santé*) a été mise en place. Cette certification définit les périmètres à respecter pour pouvoir héberger des données de santé (la sécurité, la disponibilité et les sauvegardes externalisées de données en sont des exemples). Par conséquence les services de e-Santé qui ont recours à un stockage de données

1. Règlement Général sur la Protection des Données
2. Commission Nationale de l'Informatique et des Libertés de France

devront obligatoirement ou bien obtenir la certification *HDS* ou bien utiliser un hébergeur externe certifié (depuis 2018).

1.1.2/ Restriction de l'utilisation des réseaux sans fil dans le milieu hospitalier

Il est très courant que les téléphones sans fil soient utilisés au sein d'un établissement de soins, y compris pour des besoins professionnels (par exemple pour la gestion des stocks, la tournée des patients, les appels d'urgence...). Ils sont également utilisés par des patients et leurs familles à l'intérieur des locaux de l'hôpital. Ces téléphones portables génèrent des ondes de radiofréquences et des champs électromagnétiques qui peuvent interférer avec les dispositifs médicaux (DMs). L'utilisation des téléphones mobiles dans les hôpitaux fait l'objet d'une circulaire DH/EM 1 numéro 40 du 9 octobre 1995. Elle invite les établissements de santé à prendre des dispositions permettant d'informer leurs personnels et les patients de la nécessité d'éteindre leurs téléphones mobiles dans les services de soins. Par exemple, le rapport [Ans15] montre que les systèmes de monitoring et d'enregistrement peuvent voir leur enregistrement modifié lors du passage d'un appel à proximité du matériel (50 cm) et provoquer des erreurs médicales.

De la même manière, de nombreux dispositifs médicaux connectés, implantables ou non, sont utilisés avec des technologies et des usages très variés : respirateurs, système de monitoring, électrocardiographes, fauteuils roulants électriques.... Ainsi qu'une grande diversité de sources de champs électromagnétiques de radiofréquence : tablettes, dispositifs bluetooth, systèmes RFID, talkies-walkies, systèmes TETRA... Cela implique donc des expositions sur de nombreuses bandes de fréquences à des signaux parfois très différents en modulations et intensités. Ces dispositifs médicaux génèrent de la même manière des champs électromagnétiques et peuvent perturber d'autres dispositifs médicaux. Par exemple, le rapport [Ans15] montre qu'un émetteur Wi-Fi à moins de 60 cm peut provoquer des perturbations sur un moniteur de rythme fœtal.

C'est l'ANSES [1] qui est chargée d'identifier toutes les sources pertinentes pouvant interférer avec les DMs utilisés au sein d'un établissement de santé ou sur des patients porteurs de dispositifs médicaux implantables actifs (DMIA) ainsi que d'évaluer :

- les risques potentiels de perturbation électromagnétique,
- et les distances minimales de sécurité à respecter en fonction des différentes sensibilités des dispositifs médicaux.

Dans ce contexte, il est important de différencier les objets connectés de santé et les dispositifs médicaux connectés. Ces derniers sont soumis à un marquage CE préalable sous la responsabilité du fabricant pour entrer sur la mise sur le marché dans l'UE. Ce marquage du DM est soumis à une procédure d'évaluation de conformité aux exigences essentielles décrites dans les directives européennes, s'appuyant notamment sur la norme 60601-1-2 (compatibilité électromagnétique des dispositifs électromédicaux - CEM ou EMC [2]). Cette norme met en avant 3 principes pour les fabricants de dispositifs médicaux :

1. Garantir un niveau d'émission et d'immunité (de non nocivité) du champ électromagnétique : de 3 V/m (volt par mètre) pour des dispositifs ne présentant pas un

1. Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail
2. ElectroMagnetic Compatibility

risque important, et de 10 V/m pour des DMs dits d'assistance vitale. Par ailleurs, les appareils de communication radiofréquence qui sont utilisés à proximité d'appareils électromédicaux sont soumis à des tests d'immunité spécifiques de niveau 30 V/m (niveau exceptionnel).

2. Émettre des recommandations d'utilisation, notamment sur les distances de séparation minimum entre les appareils électromédicaux et les émetteurs radioélectriques comme les téléphones mobiles ou tout autre type d'émetteur radio. La recommandation de distance minimale entre les téléphones mobiles et les DMs est par défaut de 3,3 m. Si l'immunité du DM est vérifiée à 30 V/m, les distances recommandées sont plus faibles comme le montre le tableau 1.1 en fonction du service (type de communication sans-fil) et de son PIRE maximum (Puissance Isotrope Rayonnée Équivalente). La distance de séparation recommandée d est calculée de la manière suivante :

$$d = [\frac{7}{V}] \sqrt{P} \text{ pour les fréquences au dessus de 800 MHz,} \quad (1)$$

$$d = [\frac{3}{V}] \sqrt{P} \text{ pour les fréquences entre 80 et 800 MHz.} \quad (2)$$

Où

- P est la caractéristique de puissance de sortie maximale de l'émetteur en Watts (selon le fabricant de l'émetteur),
- et V est le niveau d'immunité du DM (10 ou 30 V/m).

3. Faire une analyse de risques et d'impacts sur le patient en cas de défaillance de l'équipement.

Par ailleurs l'ANSES préconise la mise en place dans les centres hospitaliers de zones d'usages autorisés, limitées (distance de 1 m minimum avec les DMs) et strictement interdites aux systèmes de communication sans fil. L'objectif est une meilleure adaptation au regard de la diversité des situations d'usages des systèmes de communication sans-fil.

Service	*PIRE max (W)*	*Équation*	*Distance (m) pour 10 V/m*	*Distance (m) pour 30 V/m*
WLAN (Wi-Fi) Bluetooth	0.1	E1	NA	0.07
DECT (téléphone fixe sans fil) UMTS (3G)	0.25	E1	NA	0.12
GSM 1800 (2G et 4G)	0.6	E1	NA	0.18
802.11a (Wi-Fi)	1	E1	0.7	NA
GMS 1900 (3G)	1	E1	NA	0.23
GSM 800 / 900 (2G et 3G) TETRA 800	2	E1	NA	0.33
TETRA 400	10	E2	NA	0.32

TABLE 1.1 – Les restrictions de distances en fonction du service et du niveau d'immunité requis entre les appareils électromédicaux et les émetteurs radioélectriques - table issue ANSES.

1.2/ La télémedecine

La télémédecine est, selon le Ministère de la Santé Française, une pratique médicale à distance utilisant les Technologies de l'Information et de la Communication (TIC). Elle met en rapport, entre eux ou avec un patient, un ou plusieurs professionnels de santé, parmi lesquels figurent nécessairement un professionnel médical et, le cas échéant, d'autres professionnels apportant leurs soins au patient. L'impulsion de cette pratique a été donnée en 2009 grâce à la loi Hôpital, Patients, Santé et Territoires (HPST).

En conservant les mêmes exigences de qualité et de sécurité que des actes classiques, la télémédecine est une autre façon de soigner. Elle contribue à faire évoluer la médecine pour répondre à de nouveaux défis : le vieillissement de la population, le suivi approfondi des maladies chroniques, l'accès aux soins dans les zones fragiles et la prise en charge au plus près du lieu de vie, la coordination des professionnels de santé et les professionnels du secteur médico-social, notamment entre les établissements. Notons qu'avec la pandémie de Covid-19 la télémédecine a réellement montrer un intérêt crucial.

L'objectif de la télémédecine n'est pas de remplacer les actes médicaux au cabinet. Elle intervient en complémentarité des pratiques médicales plus habituelles afin de répondre aux défis que constitue l'offre de soin aujourd'hui.

La télémédecine doit reposer sur un projet médical répondant à des priorités et aux besoins de la population d'un territoire et des professionnels de santé. C'est en ce sens qu'elle s'intègre au sein d'un parcours de soins. Cinq chantiers prioritaires pour faciliter le déploiement de la télémédecine en France on été définis depuis 2011 : la permanence des soins en imagerie, la prise en charge de l'AVC, la santé des personnes détenues, la prise en charge des maladies chroniques, les soins en structures médico-sociales ou en hospitalisation à domicile (HAD).

FIGURE 1.2 – Le chariot de téléconsultation Maincare (Covalia) avec le logiciel de visioconférence Covalia.

Cinq types d'actes ont été définis pour la télémedecine dans le décret d'application n° 2010-1229 du 19 octobre 2010 relatif à la loi HPST de 2009 :

La téléconsultation permet à un professionnel de santé de donner une consultation à distance par l'intermédiaire des Technologies de l'Information et de la Communication. L'acte

de téléconsultation se déroule en visoconférence et il est depuis juin 2018 remboursé par la sécurité sociale. Il permet de prendre en charge et de suivre plus rapidement des patients et, parfois, permet d'éviter des déplacements inutiles (ou périeux comme en période de confinement) ou un recours aux urgences.

Tout médecin peut recourir à la téléconsultation, quels que soient : sa spécialité, son secteur d'exercice et son lieu d'exercice, en ville ou en établissement de santé. Elle est réalisable partout en France métropolitaine et dans les départements et régions d'outre-mer. En règle générale, c'est le médecin traitant (ou le médecin spécialiste vers lequel le patient a été orienté par le médecin traitant) qui propose au patient d'utiliser la téléconsultation. La consultation se fait soit à la maison (via un smartphone, une tablette ou ordinateur) soit depuis un lieu dédié (maison de santé, pharmacie ou chez un médecin traitant) où cet acte sera bien souvent accompagné par un professionnel de santé (médecin, infirmier ou autre).

La plateforme de télémédecine Covalia (logiciel phare de l'entreprise MainCare qui finance cette thèse CIFRE, cf figure 1.2) est spécialisée dans la téléconsulation. Elle permet en particulier :

- la prise en charge coordonnée entre les professionnels de santé,
- le partage des données médicales comme les comptes rendus de télémédecine entre les professionnels de l'équipe de prise en charge,
- la visioconférence HD avec pilotage des caméras à distance,
- la visualisation d'imagerie synchronisée,
- la facturation des actes,
- ...

La téléexpertise permet à un médecin de demander une expertise à distance à un autre médecin en raison de sa formation ou de sa compétence particulière. Cette pratique améliore la qualité de prise en charge des patients et réduit notamment les temps de déplacement et d'organisation des réunions pluridisciplinaire afin de libérer du temps médical. Le recours à la téléexpertise est autorisé depuis 2020 pour tous les cas dans lesquels les professionnels médicaux estiment nécessaire de recueillir l'avis d'autres professionnels de santé. Au sein de la plateforme Covalia, les demandes d'avis par un expert sont automatisées à la réception d'un examen médical, comme par exemple une radiologie (figure 1.3).

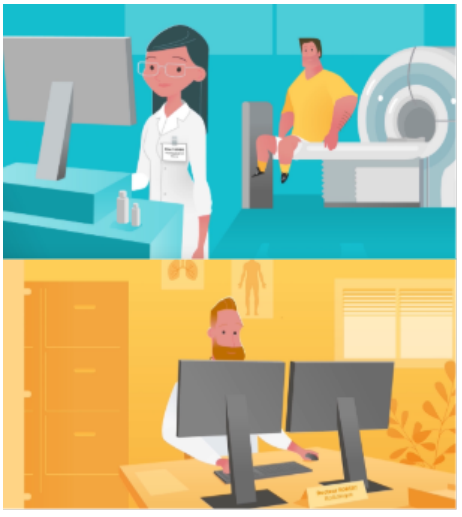


FIGURE 1.3 – Illustration d'une téléexpertise radiologique entre une manipulatrice et un expert en radiologie pour le logiciel Covotem de Maincare Solutions.

La téléassistance a pour principe d'assister un professionnel de santé à distance par un autre professionnel au cours de la réalisation d'un acte et ainsi de bénéficier des meilleurs conseils

et interventions, indépendamment du lieu dans lequel le patient se situe. Cela permet notamment de pallier certains problèmes de répartition géographique des professionnels de santé experts dans un domaine particulier.

La régulation dans le cadre des urgences est la réponse médicale en cas d'urgence ou bien en cas de conseil téléphonique (par le 15 ou numéros de régulation locaux). Les médecins régulateurs ont pour rôle de classifier les demandes d'aides médicales urgentes, d'acheminer les moyens adéquats vers les victimes et enfin de les amener directement aux services médicaux hospitaliers les plus adaptés.

La télésurveillance est l'interprétation à distance de données nécessaires au suivi médical du patient à partir d'indicateurs transmis par le patient ou par des professionnels de santé. C'est ce dernier type d'acte de télémédecine qui sera l'objet des travaux de cette thèse. En effet, l'entreprise Maincare qui développe les produits Covalia et qui finance cette thèse CIFRE souhaite développer un nouvel axe et des nouveaux produits sur cette niche.

1.3/ La télésurveillance médicale

La télésurveillance médicale est un domaine encore en plein développement en France. C'est une branche de la télémédecine qui a pour vocation de permettre à un médecin de recueillir et d'interpréter à distance les données nécessaires au suivi médical d'un patient [Fre18] [Woo01]. Elle est destinée, par exemple, aux personnes âgées et aux personnes atteintes de maladies chroniques. Les maladies chroniques sont des affections de longue durée qui, en règle générale, évoluent lentement (comme par exemple les cardiopathies, les séquelles post-AVC, les cancers, les affections respiratoires chroniques, le diabète...). Plus de 15 millions de Français sont atteints d'une pathologie nécessitant des soins au long cours et 548 000 personnes supplémentaires devraient être concernées d'ici fin 2020 (donnée avant pandémie Covid-19). Ces affections sont responsables de 63% des décès dans le monde, soit 17 millions de personnes par an.

Les centres de soins doivent assurer leur suivi et cela peut s'avérer coûteux et problématique en terme de temps dans les services hospitaliers, de temps médecins, auxquels il faut ajouter l'augmentation des coûts de santé et l'inquiétante baisse de la démographie médicale ces dernières années. Les maladies chroniques soulèvent donc d'importantes problématiques de santé publique et d'organisation des soins sur :

- la disponibilité dans les centres hospitaliers,
- la distance avec les centres hospitaliers,
- la désertification médicale,
- les coûts des soins (la moitié des dépenses de santé en France),
- ...

Le recours à la télésurveillance présente des avantages pour les patients comme pour le corps médical au cours de toutes les étapes de la maladie chronique, du stade préventif à la phase post-thérapeutique [Kla16]. Il permet entre autres :

- d'améliorer le suivi médical à distance des personnes âgées en perte d'autonomie ou atteintes de pathologies chroniques (insuffisance cardiaque, diabète et hypertension artérielle par exemple),
- de favoriser leur maintien à domicile et l'autonomie des personnes âgées,
- de prévenir au plus tôt d'éventuelles hospitalisations,
- d'anticiper au plus tôt le retour d'hospitalisation,
- de minimiser les déplacements et les hospitalisations,
- d'améliorer la coordination entre les différents corps médicaux, ce qui améliore la qualité des soins et le suivi médical du patient.

Au final, la télésurveillance permet d'améliorer la qualité de vie des patients âgés et/ou atteints de maladies chroniques ainsi que de réduire les hospitalisations et les coûts au niveau de l'établissement de santé, ainsi que le nombre et les coûts des visites à domicile (en complémentarité avec les téléconsultations).

1.3.1/ LE FONCTIONNEMENT DE LA TÉLÉSURVEILLANCE MÉDICALE

FIGURE 1.4 – Les différents acteurs d'une plateforme de télésurveillance médicale.

L'équipement médical de télésurveillance consiste à installer des dispositifs médicaux, des objets connectés ou des capteurs au domicile d'une personne âgée ou d'un patient (cf figure 1.4) comme par exemple :

- un électrocardiogramme connecté,
- un oxymètre connecté,
- un tensiomètre connecté,
- un patch mesurant la température cutanée,

- un capteur d'ouverture de porte,
- un détecteur de chute,
- un bouton d'urgence,
- ...

Ces équipements sont reliés entre eux, et permettent de collecter, d'enregistrer et de stocker des données sur la santé des patients puis de les transférer aux professionnels de santé qui pourront les analyser et prendre les décisions adéquates. On parle de biotélémétrie quand il s'agit de surveiller à distance divers signes vitaux des patients ambulatoires. Le patient peut enregistrer lui-même les données ou bien se faire accompagner par un professionnel de santé ou paramédical. Mais cela peut également se faire automatiquement lorsque le dispositif médical est porté en permanence (par exemple pendant le sommeil). Dans l'éventualité d'une urgence, les malades ou les séniors peuvent également accéder à une plateforme d'assistance médicale (par exemple en visioconférence depuis une application sur smartphone, ou simplement par téléphone).

La télésurveillance médicale est composée d'acteurs humains (le patient et le ou les professionnels médicaux), mais également d'une multitude d'acteurs matériels et/ou logiciels. C'est l'ensemble de ces acteurs qui forme la plateforme de télésurveillance médicale. La figure 1.5 montre de manière très simplifiée les acteurs d'une plateforme de télésurveillance de bout en bout, auxquels d'autres acteurs peuvent s'ajouter (comme une antenne relais, un serveur d'opérateurs téléphoniques, une base de données, un logiciel de prise en charge, une centrale téléphonique d'urgence, une application patients...).

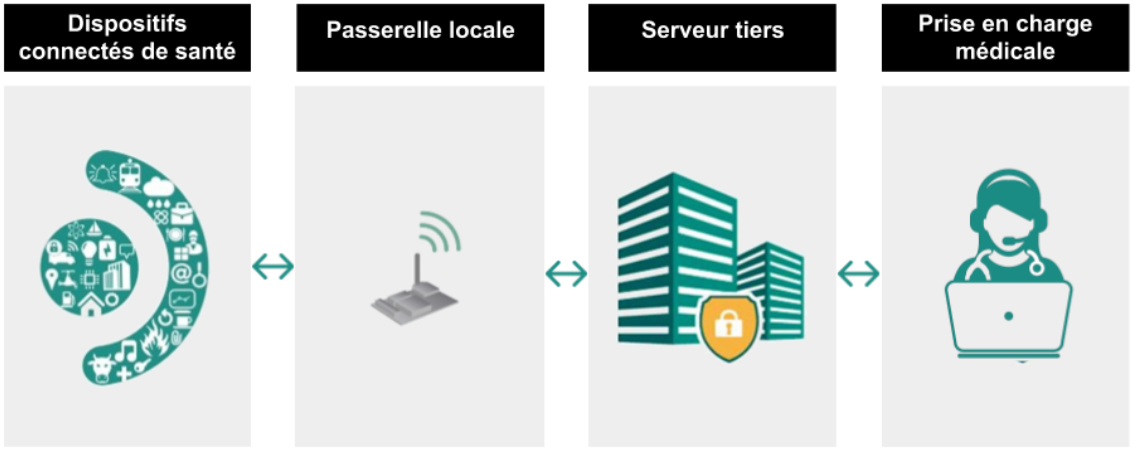


FIGURE 1.5 – Les différents acteurs d'une plateforme de télésurveillance médicale.

1.3.1.1/ LES RÉSEAUX DE CAPTEURS

Les équipements au domicile du patient forment un réseau local, également appelé LAN (*Local Area Network*), communiquant directement avec une passerelle également au domicile.

Quant il s'agit de biotélémétrie, et d'administrer les paramètres vitaux en temps réel pour l'utilisateur et pour le personnel médical superviseur, la télésurveillance peut également donner lieu à des réseaux de dispositifs sur le corps humain. Ce réseau sans fil, appelé BAN (*Body Area Network*), peut effectuer des mesures à l'aide de capteurs ou agir de façon active sur des actionneurs [Bar12] [Rag12] [Cha17]. Les BANs, également appelés BSD (*Body Sensor Network*) ou WBAN (*Wireless Body Area Network*), sont des nouveaux types de réseaux de capteurs portés directement par un humain, de petite taille, de poids légers et à ultra-faible consommation en énergie. L'IEEE 802.15.6 définit le BAN comme « une norme de communication optimisée pour les appareils à basse consommation et qui fonctionnent *sur*, *dans* ou *autour* du corps humain (mais non limitée aux humains) pour servir une diversité d'applications (y compris médicales), l'électronique grand public, le divertissement et autre » [Ban07].

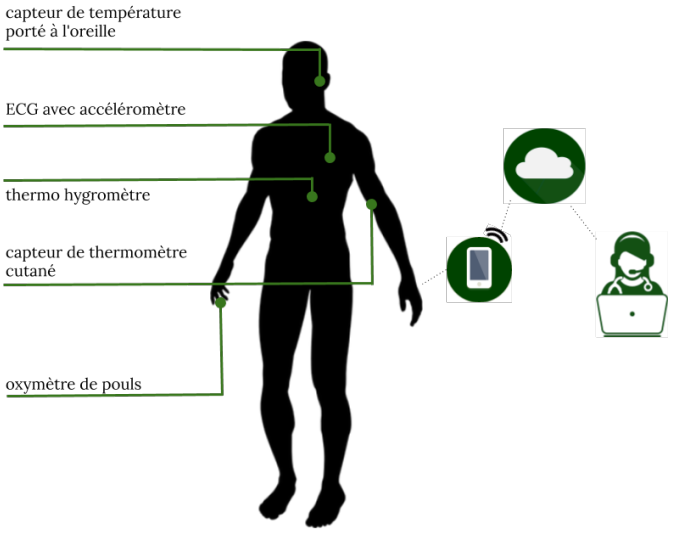


FIGURE 1.6 – Exemple de Body Area Network.

Si l'on se focalise sur le domaine médical, le terme MBAN (*Medical Body Area Network*) désigne plus précisément les BAN appliqués au domaine médical. Ils sont conçus pour la surveillance dite «intelligente» car les données peuvent être directement analysées en temps réel et automatiquement par des algorithmes intelligents, notamment des algorithmes d'intelligence artificielle (par exemple des algorithmes de détection d'arythmies cardiaques).

Un *BAN* typique, comme le montre notre figure 1.6 est composé d'un récepteur (station de base) qui communique à l'aide d'une technologie sans fil avec plusieurs nœuds qui sont placés "sur", "autour" ou "implantés dans le corps humain". C'est le récepteur qui jouera le rôle de passerelle entre le réseau de capteurs et Internet. Généralement, la collecte et la configuration des capteurs s'initie par un message de contrôle de la part du récepteur. Ce dernier ainsi que les capteurs peuvent fonctionner sur plusieurs canaux de gamme de fréquences comme spécifié dans la norme IEEE 802.15.6. Toutefois, les technologies sans fil ne sont pas seulement limitées aux ondes radiofréquence. Depuis 1996, IBM a, par exemple, développé une technologie utilisant les propriétés conductrices du corps humain pour transmettre des données [Zim96].

On distingue 3 niveaux de communication pour les *BAN* :

- *Intra-BAN* : entre les capteurs et des capteurs vers le récepteur,
- *Inter-BAN* : entre le récepteur et le point d'accès au réseau, sauf si le récepteur est lui-même un point d'accès au réseau,
- *Hors BAN* : au niveau du service qui est fourni, par exemple la télémédecine.

Les capteurs corporels (ou parfois appelés senseurs par anglicisme) collectent puis numé-

Les capteurs	*Les usages*
Accéléromètre et gyroscope	Détection des mouvements de marche, de la posture du corps, de l'estimation de la gravité des tremblements, de la détection de chute ...
Allergène	Détection d'un allergène utilisé par exemple pour l'asthme
CO_2 et oxygène	Surveillance durant la respiration humaine les variations de niveau de CO_2 et la concentration en oxygène
Électrocardiogramme	Surveillance de l'activité électrique du cœur afin de diagnostiquer une maladie cardiaque ou l'influence d'un médicament sur le cœur
Électroencéphalogramme	Mesure de l'activité électrique dans le cerveau dans un but de diagnostic en neurologie ou dans la recherche en neurosciences cognitives
Électromyogramme	Mesure des signaux électriques produits par les muscles afin de diagnostiquer des anomalies du contrôle postural et des troubles musculaires et nerveux
Glycémie	Système de surveillance de la glycémie non invasif grâce à la technologie infrarouge ou la détection optique
Oxymètre	Mesure de la saturation en oxygène (SpO2) et indirectement la fréquence cardiaque qui sont tous les deux des paramètres vitaux, pour de la surveillance post-opératoire par exemple
Pression artérielle	Mesure la pression diastolique et systolique en utilisant l'oscillométrie
Température et humidité (hygromètres)	Mesurer la température du corps et l'humidité de l'environnement d'une personne
Autres	Détection de crise d'épilepsie, capteurs sensibles à l'acide nitrique (détection de Cancer), rétine artificielle ou caméra externe ...

TABLE 1.2 – Liste des capteurs utilisés dans un BAN pour la santé.

risent des signaux analogiques correspondant aux actions physiologiques et aux activités du corps humain. Ils sont constitués de la partie capteur proprement dite, d'un convertisseur analogique-numérique, d'un processeur, d'une unité d'alimentation, d'une mémoire et d'un émetteur-récepteur. La table 1.2 présente une liste non-exhaustive des capteurs utilisables dans un réseau de type BAN [Che10].

Les actionneurs sont différents des capteurs. Ils transforment l'énergie d'entrée en énergie mécanique : ils ont donc un rôle actif pour leurs porteurs. Ils peuvent, par exemple, délivrer une substance médicamenteuse sur demande, après analyse des données mesurées par les capteurs. Un actionneur est constitué d'un émetteur-récepteur, d'une unité d'alimentation, d'une mémoire et des composants pour l'action (souvent un réservoir de substance et les composants mécaniques pour la délivrer). Voici une liste non-exhaustive des actionneurs pour la santé :

- pompe à médicament pour injecter celui-ci en cas de dépassement d'une valeur de seuil,
- actionneurs capables de stimuler les muscles pour restaurer la mobilité,
- pompe à insuline pour réduire les nuisances d'une chute de glucose,
- stimulateur agissant sur la moelle épinière et permettant de réduire les douleurs chroniques...

Les capteurs et les actionneurs communiquent directement avec le récepteur. C'est lui qui joue le rôle de passerelle entre le réseau et Internet.

1.3.1.2/ La passerelle

La passerelle est le nom donné génériquement pour désigner un dispositif permettant de relier deux réseaux informatiques de types différents. Elle permet dans le cadre de la télésurveillance de relier le réseau local au réseau Internet : et donc de mettre en contact le patient avec les professionnels de santé qui seront également connectés aussi au réseau Internet, par l'intermédiaire d'un serveur de télésurveillance. Il existe plusieurs types de passerelles couramment utilisées. Les passerelles les plus utilisées dans les articles de recherche ainsi que dans les produits commercialisés de télésurveillance sont les modems, les smartphones et les cartes programmées. Chaque type de passerelle possède des avantages et des inconvénients comme le montre la table 1.3 :

Type de passerelle	*Type de communication*	*Avantages*	*Inconvénients*
modem-routeur (ou box)	ADSL/fibre optique avec abonnement	- facilité de mise en place car souvent existant au domicile	- coût/difficulté d'installation si non existant au domicile
smartphone	GSM (2G, 3G, 4G, 5G)	- facilité/coût de mise en place si le patient en a déjà un - mobilité (non cloisonnement au domicile)	- coût d'achat si le patient n'en a pas - coût d'abonnement hors domicile - consommation d'énergie
carte programmée (ex. Raspeberry Pi ou Arduino)	GSM ou LPWAN (LoRa, Sigfox)	- mobilité (non cloisonnement au domicile) - coût d'achat faible	- praticité - coût d'abonnement hors domicile

TABLE 1.3 – Les différents types de passerelles de télésurveillance.

1.3.1.3/ Le serveur de télésurveillance

Appelé parfois VDS (*Virtual Doctor Server*) dans les application de télésurveillance [Bar12], le serveur joue un rôle déterminant dans la prise en charge du patient. Il a plusieurs rôles :

- mettre en relation le patient avec un personnel de santé sur la base des signes vitaux recueillis par les capteurs et stockés dans une base de données,
- appeler les urgences et guider un secouriste si nécessaire,
- conseiller le patient automatiquement en fonction de ses besoins, ou à l'aide de consignes administrées par l'équipe de prise en charge de ce patient,
- analyser automatiquement les données et détecter les anomalies à l'aide d'algorithmes d'apprentissage.

1.3.2/ QUELQUES EXEMPLES DE PLATEFORMES DE TÉLÉSURVEILLANCE

Cette section présente quelques exemples de plateformes issues de la littérature et se termine par une discussion sur ces travaux.

1.3.2.1/ LA PLATEFORME MULCER

Rodigues et al.[Rod13] proposent une plateforme *«mULCER»* de santé mobile pour la surveillance des escarres (ulcères de pression) chez les patients à mobilité réduite, comme les personnes âgées et les patients portant des plâtres ou des prothèses. La plateforme utilise comme intermédiaire un smartphone et la norme HL7 pour le format de données permettant une intégration facile dans un dossier de soin standardisé. Le suivi des ulcères est réalisé avec l'aide de photographie prise depuis le smartphone. Le travail d'une infirmière est nécessaire ensuite pour classifier, traiter et surveiller l'ulcère du patient. Cette plateforme entre dans le cadre de la télésurveillance, lorsque les photographies sont réalisées à la maison, ou en établissement de santé, par le patient lui-même, ou plus généralement, une infirmière et que les données sont analysées quotidiennement par un professionnel de santé.

1.3.2.2/ LA PLATEFORME BIOFEEDBACK

Costa et al. [Cos15] proposent une intégration des solutions portables dans des milieux de vie assistés ambiants (*AAL*) avec prise en charge de la mobilité. Le but est de favoriser la qualité de vie des personnes, notamment âgées, en prolongeant leur temps au domicile.

Cette plateforme comprend l'électrocardiographie (ECG), la fréquence respiratoire, les battements par minute, la température corporelle et la détection de chutes comme le montre la figure 1.7. Ces capteurs portables sont reliés en Bluetooth à un appareil mobile (smartphone) qui retransmet les données par l'intermédiaire de webservices via sa connexion internet (3G, 4G ou Wi-Fi avec routeur). La plateforme effectue donc une surveillance des patients en temps-réel et offre la possibilité aux professionnels de la santé, aux soignants ou même aux proches d'être informés de l'état de santé des patients à tous moments et n'importe où.

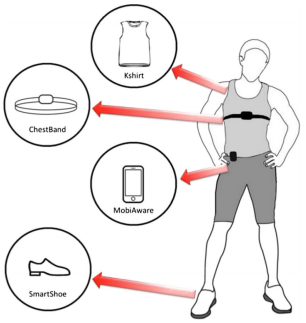


FIGURE 1.7 – Illustration d'une solution mobile de biofeedback, basée sur des capteurs portables - issue de [Cos15].

1.3.2.3/ La plateforme Telos

Jovanov et al. [Jov05] proposent une plateforme de télémédecine constituée d'un WBAN (Wireless Body Area Network) de capteurs de mouvement intelligents pour la réadaptation physique et la surveillance ambulatoire. Les capteurs physiologiques, cinétiques et environnementaux sont légers et à très faible consommation d'énergie, comme sur la figure 1.8. Ils sont intégrés directement sur le corps et forment le réseau sans fil en utilisant la technologie ZigBee. Le système effectue une analyse en temps réel des données des capteurs, fournit des conseils et des commentaires à l'utilisateur et peut générer des avertissements en fonction de l'état, du niveau d'activité et des conditions environnementales de l'utilisateur. Les auteurs décrivent l'enregistrement des données dans des dossiers médicaux électroniques sur les serveurs médicaux distants, par l'intermédiaire d'un smartphone entre les capteurs et Internet. Et ces travaux présentent également la manière de concevoir cette technologie dans nos quotidiens, en décrivant un certain nombre de difficultés telles que la configuration et la personnalisation du système, l'intégration transparente, la normalisation ou encore la sécurité et la confidentialité.

Figure 1.8 – Exemple d'un capteur de type accéléromètre sur une cheville pour la réadaptation physique - issue de [Jov05].

1.3.2.4/ La plateforme de Agarwal et al.

Agarwal et al. [Aga10] décrivent un service de télésurveillance pour les patients atteints de diabète et d'hypertension. Ils fournissent une solution de bout en bout : la collecte des relevés via un smartphone, la transmission des données aux médecins et le service permettant à ces derniers de gérer la maladie chronique de leurs patients en fournissant des conseils. Un des objets connectés utilisés est le Gluco+ de la société américaine HealthPia. C'est un glucomètre qui peut être attaché physiquement en temps que module complémentaire aux téléphones via une connectique appropriée (ou dans le GlucoPhone, un téléphone vendu avec le glucomètre intégré). Le téléphone communique avec un serveur distant via les technologies GSM (3G, 4G) et par l'intermédiaire de web-services (protocole sécurisé en https). La plateforme utilise l'architecture classique présentée juste avant, c'est-à-dire un ou des objets connectés, une passerelle qui est le smartphone, un serveur de télésurveillance, une base de données, et un service aux professionnels sous forme d'un application web (figure 1.9).

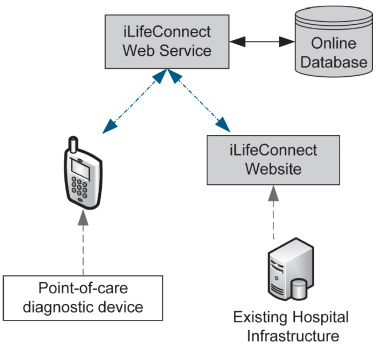


FIGURE 1.9 – Architecture de la plateforme de télésurveillance de Agarwal et al.

1.3.2.5/ La plateforme de télémédecine de Zhang et al.

Zhang et al. proposent dans [Xia11] une plateforme de télémédecine ouverte, sécurisée et flexible basée sur l'IoT et le cloud computing, pour aider à la vie ambiante (Ambient Assisted Living) ainsi que la télémédecine. Les thèmes de l'interopérabilité, la sécurité, la qualité de service (Quality of Service) pour le streaming adaptatif sont abordés. Pour l'interopérabilité, les auteurs ont choisi d'utiliser le cadre standard recommandé par la *Continua Health Alliance* (CHA), appelée maintenant *Personnal Connected Health Alliance* (PCHA). Il permet, entre autre, la communication standardisée au niveau modèles de données (HL7 ou FHIR) et protocoles de communication (Bluetooth, ZigBee ou USB), entre les capteurs et la passerelle. La passerelle utilisée sera un appareil portable ou un ordinateur fixe ou portable.

1.3.2.6/ Les travaux de Istepanian et al.

Istepanian et al. [Ist11] ont montré le potentiel de l'*«Internet of m-health Things»* (Internet des Objets de santé mobile) pour la détection non invasive du niveau de glucose. Le terme *m-health* désigne plus globalement les données de santé liées aux dispositifs médicaux portables et objets connectés. Un capteur de glycémie de type opto-physiologique est fixé sur la peau. Il analyse le taux de glucose à partir du contenu sanguin cutané. L'architecture de la plateforme est basée sur les protocoles IPV6 et 6LoWPAN (basé lui-même sur la norme IEEE 802.15.4). Le potentiel du 6LoWPAN, en plus de la connectivité IPV6, réside dans les caractéristiques de faible puissance et basse consommation énergétique. La passerelle utilisée, permettant le lien entre le capteur et le centre clinique, est un microprocesseur basse consommation MSP430 branché à un ordinateur relié à Internet.

1.3.2.7/ DISCUSSION

Plateforme	*mULCER*	*Biofeedback*	*Telos*	*Agarwal*	*Zhang*	*m-IoT*
Capteurs et OC	aucun	OC déterminés (ECG, thermomètre etc)	réseau de capteurs (BAN)	glucomètre gluco+	OC compatibles PCHA	capteurs compatibles telosB
Technologie locale	aucun	Bluetooth	IEEE 802.15.4 avec Zigbee	Bluetooth	Bluetooth, USB ou Zigbee	IEEE 802.15.4 avec IPV6 et 6LoWPAN
Type de passerelle	smartphone	smartphone	smartphone zigbee	smartphone	smartphone ou ordinateur	ordinateur
Interopérabilité	oui HL7	non	non	non	oui avec PCHA (HL7 ou FHIR)	non

TABLE 1.4 – Comparaison des plateformes de télésurveillance existantes.

Les plateformes actuelles qui sont décrites dans la littérature sont innovantes. Elles permettent la mise en place de systèmes de télésurveillance à distance pour les patients, soit avec un réseau de capteurs sur le corps, soit avec des objets connectés. Le tableau 1.4 présente une synthèse de ces différentes plateformes. L'utilisation d'un smartphone comme passerelle est présente dans la majeure partie des cas : ce qui peut être très pénalisant en terme de gestion des consommations en énergie. Les technologies de communication locales sont Bluetooth, IEEE 802.15.4 (Zigbee ou 6LowPAN) ou USB. Les passerelles ont toutes le point commun d'avoir un accès à Internet (3G, 4G ou en Wi-Fi par l'intermédiaire d'un routeur), qui permet un échange avec le serveur distant bien souvent en WebServices.

Deux des plateformes se distinguent sur leur interopérabilité : l'utilisation des standard HL7 ou FHIR sur le modèle de données (pour la santé exclusivement) permet d'interopérer plus facilement toutes les autres applications. Dans l'écosystème hospitalier, où il existe une multitude d'applications de santé, au sein d'une région ou de manière nationale, l'interopérabilité entre ces applications devient un enjeu prioritaire : notamment au niveau du dossier médical partagé. Les standards HL7 (ancienne version au format XML) et FHIR (évolution au format JSON) permettent de normaliser le modèle de données médicales : les documents de santé, l'imagerie, ou les constantes de santé remontées par les dispositifs médicaux en sont des exemples.

Les plateformes présentées ici ont chacune des fonctionnalités intéressantes pour un système de télésurveillance de patient au domicile. Cependant elle ne permettent pas :

- d'être économes en énergie à la fois au niveau des dispositifs (capteur ou dispositifs médicaux) et de la plateforme (comme par exemple avec utilisation de smartphone),
- d'avoir une interaction directe vers l'Internet, et donc un pilotage à distance,
- d'avoir un faible coût et d'être mobile (abonnement et smartphone onéreux, recharge quotidienne),

- d'une manière générale elles ne permettent pas d'être utilisées facilement et de manière transparente par des patients (comme par exemple des personnes âgées).

Ainsi nous souhaitons proposer sur la base des nouvelles technologies de l'Internet des Objets une plateforme qui soit à la fois :

- économe en énergie,
- peu coûteuse,
- mobile (utilisation dans la vie de tous les jours),
- facile et transparente d'utilisation,
- connectée de manière ubiquitaire à Internet en utilisant les technologies de l'IoT.

1.3.3/ Essais cliniques sur les plateformes de télésurveillance

Les essais cliniques sur les plateformes de télésurveillance ne permettent pas de montrer la faisabilité de celles-ci, mais plutôt leur utilité, l'acceptation des patients ou encore les contraintes de terrain. Par exemple, Milani et al. [Mil17] ont réalisé un essai clinique sur 400 patients souffrant d'hypertension et inscrits à un programme de télémédecine. Le programme consistait à des prises régulières de la pression artérielle, des questionnaires numériques et des recommandations sur la gestion des médicaments et le mode de vie par des professionnels de santé. Les résultats ont montré une baisse moyenne de la pression artérielle systolique et diastolique plus importante chez les patients inscrits au programme que chez les non inscrits.

De la même manière, Bolinder et al. [Bol16] ont montré qu'une surveillance plus stricte de la glycémie chez les patients atteints de diabète de type 1, au travers d'une plateforme de télésurveillance, permet de retarder l'apparition de complications diabétiques macrovasculaires et microvasculaires.

Synthèse du chapitre 1

SYNTHÈSE

Dans cette section nous avons défini l'Internet des Objets (*IoT*) ainsi que son potentiel applicatif dans le domaine de la santé.

Compte tenu de sa caractéristique que l'on nomme *l'ubiquité* (disponibilité n'importe où et n'importe quand), l'*IoT* convient particulièrement à la télémédecine, pour laquelle nous avons décrit les 5 types d'actes en nous basant sur notre expérience au sein de l'entreprise Maincare dans laquelle s'inscrit cette thèse CIFRE.

Nous avons retenu dans le cadre de notre travail un type d'acte : la télésurveillance médicale. Ses besoins correspondent parfaitement aux caractéristiques de l'Internet des Objets et l'apparition constante de nouveaux objets destinés au suivi médical des patients à distance.

Nous avons ainsi décrit le fonctionnement des plateformes de télésurveillance avec de nombreux exemples issus de la littérature utilisant différents capteurs et réseaux de capteurs sur le corps humain. Pour finir nous avons comparé ces plateformes afin d'en extraire les qualités et les défauts puis nous avons identifié les caractéristique attendues pour la création d'une nouvelle plateforme de télésurveillance médicale.

Le chapitre suivant est consacré aux dispositifs médicaux connectés de santé ainsi qu'à l'intéropérabilité dans le domaine de la télésurveillance médicale.

2

Les dispositifs médicaux connectés et les objets connectés de santé

Le nombre d'OCSs (*Objets Connectés de Santé*) et de DMCs (*Dispositifs Médicaux Connectés*) est en forte augmentation. Leur nombre est passé de 46 millions en 2015 à 101 millions en 2018 [Bii16]. En 2020, leur nombre est estimé à 161 millions avec un marché qui devrait atteindre les 400 millions d'euros.

Les dispositifs médicaux connectés sont utilisés pour enregistrer des données biologiques, dans le cadre bien souvent de maladies chroniques (diabète, Parkinson...) afin de prévenir d'éventuelles hospitalisations. Ces données sont agrégées et stockées dans des dossiers médicaux partagés par les membres de l'équipe médicale de prise en charge du patient (médecins, infirmiers...) : ce qui permet une meilleure coordination des soins. Ces dispositifs médicaux connectés sont différents des objets connectés de bien-être, qui proposent un suivi de l'activité physique, et du sommeil par exemple, mais qui n'ont pas d'exigence règlementaire de remontée des informations dans un dossier médical.

Les dispositifs médicaux sont développés par des sociétés privées et doivent répondre à des contraintes règlementaires comme celles de la Commission Européenne et de l'Agence Nationale pour la Sécurité du Médicament et des produits de santé (ANSM) en Europe. Ceux-ci peuvent suivre l'unique standard pour la santé connectée reconnu internationalement : Continua, développé par la *Personal Connected Health Alliance (PCHA)* [Car07] [War10]. Ce standard facilite et sécurise l'intégration de nouveaux modèles de capteurs de santé communicant avec les systèmes d'informations des hôpitaux et les plateformes de télémédecine.

2.1/ Les dispositifs et objets connectés de santé

Selon la Directive Européenne 93/42/CEE [Ans19], un dispositif médical (*DM*) correspond, comme le montre la figure 2.1, à : « Tout instrument, appareil, équipement, logiciel, matière ou autre article, utilisé seul ou en association, y compris le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostiques et/ou thérapeutiques, et nécessaire au bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins :

- de diagnostic, prévention, contrôle, traitement ou d'atténuation d'une maladie,
- de diagnostic, contrôle, traitement, d'atténuation ou de compensation d'une blessure ou d'un handicap,
- d'étude, de remplacement ou modification de l'anatomie ou d'un processus physiologique,
- de maîtrise de la conception.

et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens ».

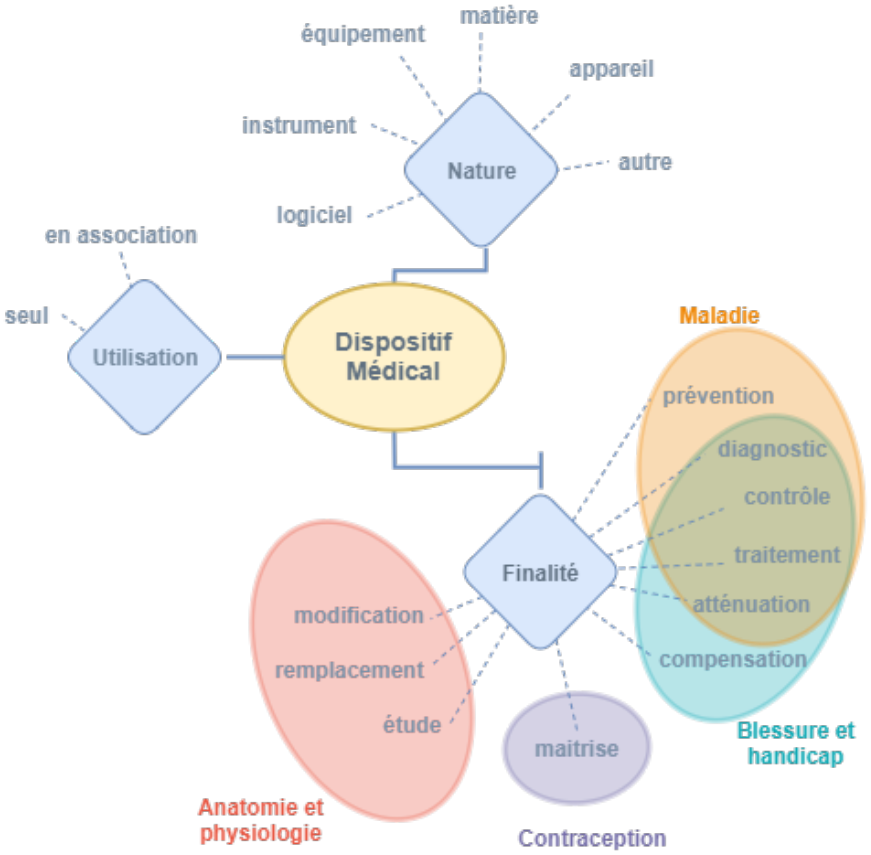


FIGURE 2.1 – Définition du Dispositif Médical - issue directive 93/42/CEE.

Le nouveau règlement européen 2017/745 [UE17], entré en vigueur le 26 mai 2017, est en application obligatoire pour les nouveaux DMs depuis le 26 mai 2020. Le niveau d'exigence a été relevé afin d'obtenir le marquage CE qui signifie une autorisation de mise sur le marché. La détermination de la classe (figure 2.2) est réalisée par le fabricant en fonction de la dangerosité du DM, son caractère invasif, la durée d'utilisation ...

Voici des exemples de dispositifs médicaux (DMs) en fonction de leur classe de risque :

- scalpels, gants d'examen (classe I),

- thermomètres, aiguilles pour seringue (classe IIa),
- respirateurs, machines de dialyse (classe IIb),
- prothèses articulaires, cathéters destinés au cœur (classe III et dispositifs médicaux implantables actifs (DMIA)).

La démarche pour placer un DM dans une classe prend en compte la durée d'utilisation, le caractère invasif ou non et le type d'invasivité, la possibilité ou non de réutilisation, la visée thérapeutique ou diagnostique et la partie du corps concernée.

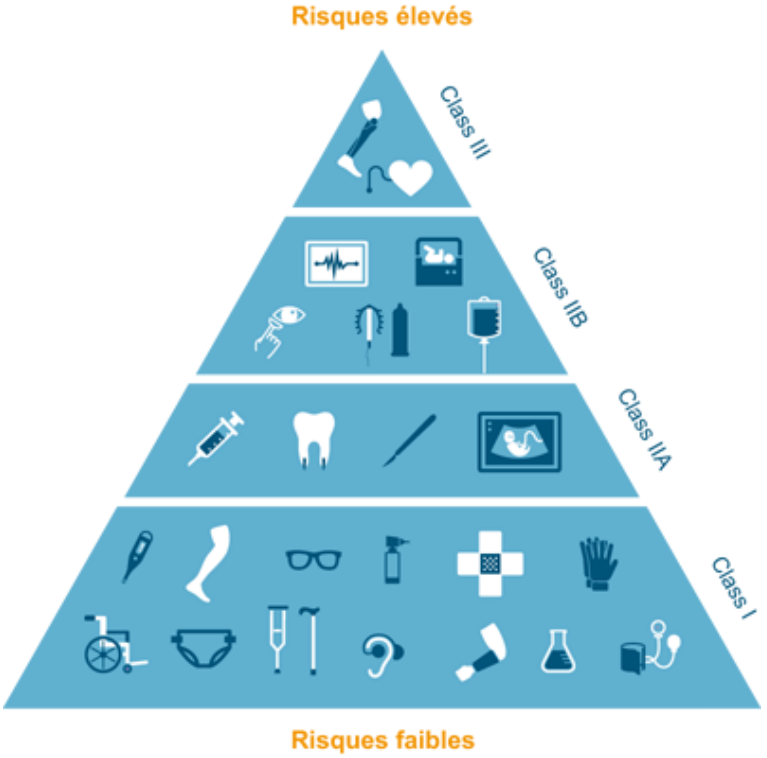


FIGURE 2.2 – Dispositifs Médicaux en fonction du risque - issue de [Szy05].

Un produit ne peut être labellisé que si son fabricant en fait la demande, même si les données concernent la santé.

La figure 2.3 représente les différentes étapes de mise sur le marché d'un nouveau dispositif médical [Sur18]. Après une définition et une détermination du niveau de risque par le fabricant, le dispositif doit également être marqué d'un numéro unique (UID) afin de pouvoir tracer celui-ci. Ensuite, il sera évalué par un organisme externe pour l'obtention du marquage CE et la mise sur le marché. L'ANSM interviendra par la suite périodiquement afin de s'assurer de la pérennité de la conformité du DM.

L'évaluation des dispositifs médicaux en vue de leur remboursement par l'assurance-maladie est à la charge de la HAS (*Haute Autorité de Santé*).

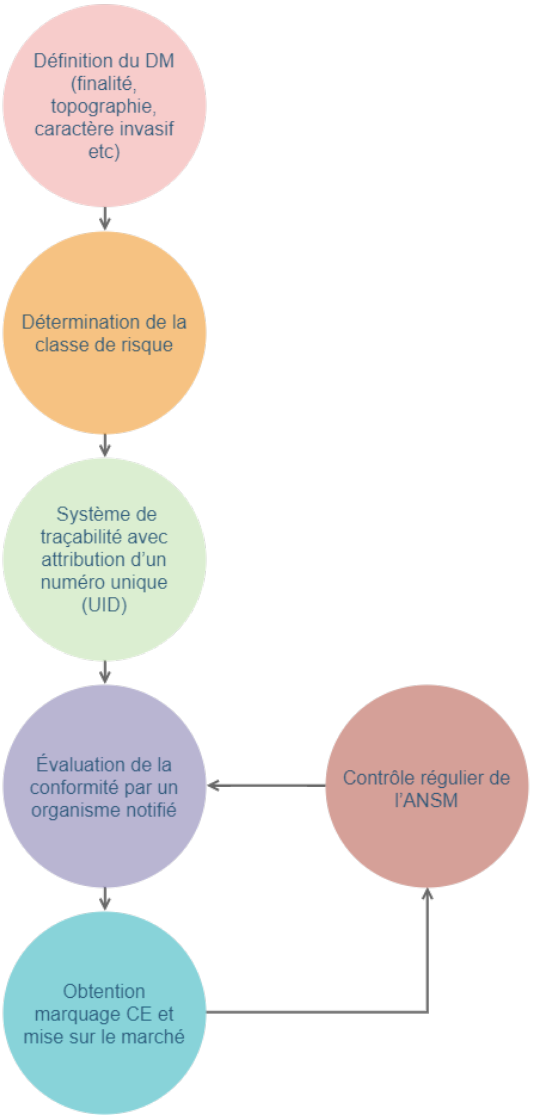


FIGURE 2.3 – Différentes étapes de mise sur le marché d'un DM - issue de [Sur18].

2.1.1/ LES DISPOSITIFS MÉDICAUX CONNECTÉS (*DMCs*)

Les dispositifs de santé connectés (***DMCs***) sont des DMs utilisés à des fins de télésurveillance médicale ou de téléconsultation ou générant une action du patient à des fins d'autotraitement ou d'autosurveillance. Pour entrer dans ces catégories, les DMCs devront être utilisés à des fins médicales, par le patient lui-même et disposer d'une fonction de télécommunication.

La suite de cette section présente les DMCs les plus couramment utilisés.

Glucomètre

Nous pouvons prendre l'exemple du diabète. Aujourd'hui, 425 millions de personnes sont atteintes du diabète selon la Fédération Internationale du Diabète. Ainsi, l'OMS [1] prévoit 50% de diabétiques supplémentaires dans le monde d'ici 2040. Le diabète se caractérise par un trouble de l'assimilation, de l'utilisation et du stockage des sucres apportés par l'alimentation. Sa cause est un manque ou un défaut d'utilisation d'une hormone : l'insuline. Cela se traduit par un taux de glucose dans le sang (aussi appelé glycémie) élevé : on parle d'hyperglycémie.

FIGURE 2.4 – Glucomètre en continu Sugarbeat (patch) et application sur montre connectée.

Le glucomètre permet au patient diabétique de connaître son taux de glycémie à tout moment de la journée. Les glucomètres connectés ne diffèrent que peu, au niveau de l'apparence, des glucomètres classiques. Ils se distinguent par leur connexion avec le smartphone du patient et la remontée et le stockage des mesures dans un logiciel dédié au suivi de la maladie. Certains modèles proposent une interconnexion possible avec d'autres applications, ce qui donne la possibilité de remonter de données vers un dossier médical partagé. Il existe deux types de glucomètres connectés suivant qu'ils sont dotés :

- ou bien d'un lecteur de bandelette et d'un auto-piqueur, couplé à une application sur smartphone ou ordinateur.
- ou bien d'un capteur indolore sur la peau (par exemple un patch), mesurant le taux de *glucose interstitiel* (liquide situé entre les cellules), dans lequel le sucre circule librement des vaisseaux capillaires vers le liquide. Les capteurs peuvent envoyer des mesures directement ou être scannés en NFC [2], et couplés à une application sur une montre ou un smartphone. Le glucomètre en continu Sugarbeat en est un exemple (figure 2.4).

Des études ont montré la fiabilité des mesures de glycémie avec l'utilisation de glucomètres connectés sous forme de patchs chez les enfants et adolescents atteints de diabète de type 1 [Mas18] et une réduction du temps passé en hypoglycémie [Bol16].

Tensiomètre

Le tensiomètre connecté est un tensiomètre classique qui utilise le principe de l'oscillométrie pour mesurer les tensions artérielles systoliques et diastoliques et la fréquence du pouls. Le tensiomètre connecté iHealth en est un exemple (figure 2.5).

1. Organisation Mondiale de la Santé
2. Near Field Communication

La spécificité est la remontée d'informations, sur des appareils mobiles ou un ordinateur, pour suivre et partager les données vitales de la pression artérielle. Suivant les modèles, il peut être utilisé par un professionnel ou en automesure par un patient. L'automesure de la tension représente un véritable intérêt, elle permet aux médecins le suivi et l'adaptation du traitement des hypertendus, pathologie qui touche 10 millions de personnes en France, et plus globalement d'anticiper les risques cardiovasculaires. Il conviendra de faire attention aux variations tensionnelles au cours d'une journée. Des études ont analysé la fiabilité et l'efficacité des tensiomètres connectés sur des patients hypertendus [Par17] [Mil17].

FIGURE 2.5 – Tensiomètre connecté iHealth.

Oxymètre

Les oxymètres de pouls permettent de mesurer la saturation en oxygène de l'hémoglobine au niveau des capillaires sanguins en utilisant le principe d'absorbance de la lumière rouge ainsi que la fréquence cardiaque. Ce dispositif est utilisé principalement dans la surveillance des pathologies cardio-respiratoires comme l'asthme ou BPCO [1], ou encore pour des patients sous anesthésie ou en salle de surveillance après intervention.

Les oxymètres connectés se posent généralement au niveau du doigt et transmettent les données en bluetooth à une application dédiée sur smartphone. Le tensiomètre connecté iHealth en est un exemple (figure 2.6). Certains modèles mettent à disposition une API [2] afin d'intégrer les capteurs dans d'autres applications non propriétaires au constructeur. Shah et al. ont montré la possibilité de prédire et d'identifier les exacerbations de BPCO à l'aide d'un oxymètre connecté [Sha17].

FIGURE 2.6 – Oxymètre connecté iHealth.

Stéthoscope

Le stéthoscope connecté peut être utilisé quotidiennement par un médecin, au même titre que le tensiomètre, la balance ou encore l'oxymètre de pouls... Il a pour objectif d'améliorer le dépistage et le diagnostic des maladies cardiovasculaires en aidant les praticiens à l'aide de données supplémentaires permettant un accompagnement au diagnostic.

1. Broncho Pneumopathie Chronique Obstructive
2. Application Programming Interface

Les stéthoscopes connectés dits « intelligents » sont équipés de fonctionnalités supplémentaires (dans une surcouche logicielle) permettant d'améliorer la qualité des données et de faciliter l'interprétation. Cela permet entre autres :

- De diminuer les bruits parasites,
- D'augmenter des sons auscultatoires et notamment les battements du cœur,
- D'enregistrer le rythme cardiaque,
- De représenter visuellement l'auscultation,
- D'analyser automatiquement les auscultations à l'aide d'algorithmes de reconnaissance audio.

FIGURE 2.7 – Stéthoscope connecté Eko Core.

L'Eko Core (figure 2.7) est le premier stéthoscope connecté a être approuvé par la FDA [1]. Il se distingue par sa capacité à analyser automatiquement les données. Les enregistrements sont comparés à l'aide d'un algorithme propriétaire de reconnaissance audio (semblable à l'application Shazam) sur une base de données d'enregistrements et de diagnostics conséquents établis par différents hôpitaux du pays. Cela aide ainsi le médecin à fournir un diagnostic et à dépister une maladie cardiovasculaire. Andrès et al. ont montré que l'utilisation d'un stéthoscope connecté intelligent (ici eStetho) permet d'obtenir un diagnostic correct dans 10% de cas supplémentaires par rapport à un stéthoscope acoustique [And16].

Thermomètre

Les thermomètres connectés se distinguent des thermomètres classiques en utilisant la technologie infrarouge et une prise de température au niveau de l'artère temporale (le thermomètre Withings en est un exemple figure 2.8). Cette prise de température est quasi instantanée et fiable à 0.2 °C près. Certains thermomètres connectés peuvent même prendre la température sans toucher la peau. Les données sont sauvegardées sur l'application dédiée et il est alors possible de consulter les courbes de températures soi-même, ou avec l'aide d'un médecin traitant. Certains modèles sont destinés au monitoring en continu. Ils permettent par exemple d'alerter les parents en cas de pic de température d'un nourrisson.

FIGURE 2.8 – Thermomètre connecté infrarouge Withings.

1. Food and Drug Administration : administration américaine en charge du matériel médical

Les thermomètres connectés peuvent également être utilisé par un médecin dans le cadre d'un examen ou par un patient dans le cadre d'une télésurveillance médicale afin de remonter directement les données dans son dossier.

Les thermomètres connectés de la marque Kinsa permettent aux utilisateurs d'associer des symptômes et des positions géographiques aux températures anormales en cas de fièvre. Les algorithmes réalisés sur le serveur permettent ensuite de prédire et de prévenir certaines pathologies contagieuses et de suivre les épidémies par région géographique [Chr15].

Pilulier

Le pilulier est un élément essentiel pour un patient atteint de pathologies chroniques. Le pilulier connecté apporte une aide supplémentaire dans la gestion de la prise médicamenteuse. Il sonne et indique avec des lumières les médicaments à prendre. Il peut également envoyer des rappels par SMS et prévenir l'entourage et les aidants en cas de problème. Le pilulier Imedipac de Médissimo est autonome et fonctionne sans smartphone (figure 2.9). Il utilise une puce 3G pour communiquer avec le serveur de l'entreprise afin de se synchroniser et d'envoyer des alertes.

FIGURE 2.9 – Pilulier connecté Imedipac de Médissimo.

L'observance est l'adéquation entre le comportement du patient et le traitement proposé. Pour les patients atteints de maladies chroniques, le score d'observance est très faible (environ 50%) . Cela signifie que 50% des médicaments prescrits ne sont pas consommés par les patients. La complexité des traitements ou encore la motivation des patients sont en cause. Le coût de la non-observance est à la fois humain et financier. En France, il est estimé à environ 8000 décès et 2 milliards d'euros par an (1 000 000 de journées d'hospitalisation et des traitements supplémentaires qui auraient pu être évités). Le pilulier connecté permet d'améliorer grandement l'observance. Vervloet et al. ont montré que l'envoi de rappel par SMS chez les patients atteints de diabéte de type 2 permettait de gagner 15% d'observance à long terme [Ver14].

Électrocardiographe

L'électrocardiographe connecté permet de réaliser des électrocardiogrammes (ECG) à la maison, à tous moments de la journée dans le but de détecter une anomalie de rythme cardiaque (arythmie). L'électrocardiographe connecté MyECG de Bewellconnect en est un exemple (figure 2.11). Les mesures peuvent être manuelles (utilisation sans fil et sans électrode), thoraciques ou avec des câbles ECG. Il est possible de visualiser les résultats sous forme de courbes soit directement sur l'appareil (pour certains), soit sur l'application mobile dédiée. L'interprétation des résultats n'est pas automatique. Il doit se faire obligatoire par un médecin (médecin généraliste ou équipe de prise en charge) à distance après retransmissions des résultats depuis l'application.

Il existe également des montres connectées capables de détecter les arythmies. Elles sont validées cliniquement, marquées CE et autorisées dans l'espace économique européen (comme la montre Move ECG (figure 2.10) ou encore l'Apple Watch Series 4). Elles analysent la régularité du rythme cardiaque mais ne peuvent pas détecter les crises cardiaques ou les AVCs. Elles sont également capables de détecter potentiellement d'autres pathologies cardiovasculaires comme l'hypertension ou l'insuffisance cardiaque : ce qui constituera une alerte pour aller consulter un médecin. L'utilisation de la montre au quotidien favorise la prévention des maladies cardiaques au plus tôt, et plus facilement. Des études ont montré que l'utilisation d'un ECG connecté au domicile permettait de diagnostiquer plus de cas de fibrillation auriculaire [1] qu'avec un parcours de soins standard [Hal17].

FIGURE 2.10 – Montre Move ECG de withings.

FIGURE 2.11 – ECG connecté MyECG de Bewellconnect.

2.1.2/ LES OBJETS CONNECTÉS DE SANTÉ (*OCSs*)

Les objets connectés de santé (OCSs) se distinguent des dispositifs médicaux connectés, car ils n'ont pas de finalité médicale déclarée et de fiabilité démontrée. Ils sont classés dans le champ du bien-être et n'ont pas d'encadrement juridique (pas de marquage CE spécifique) pour être utilisé à des fins diagnostiques ou thérapeutiques. La séparation des objets de santé et de bien-être est donc principalement règlementaire : les objets testés qui ont démontré leur fiabilité sont des objets de santé, les autres objets sont de bien-être.

Ainsi, c'est principalement la volonté du fabricant et la finalité d'usage qui feront d'un objet connecté un dispositif médical. Cependant, le marquage CE étant coûteux et contraignant, beaucoup de fabricants préfèrent rester sur des produits grand public et ne pas les classer dans les dispositifs médicaux. Il suffit alors aux fabricants d'informer les utilisateurs que leurs produits ne sont pas des DMs pour que ces derniers ne puissent pas être considérés comme tels.

Les usages ne seront donc pas centrés sur la santé ou la prise en charge médicale des personnes, mais uniquement sur le bien-être. Le bien-être est associé à l'automesure de soi (*quantified self*) et aux sports connectés. Les objets connectés de «santé» permettent donc, malgré leur nom, d'évaluer le comportement de leurs utilisateurs en les aidant à prendre soin d'eux.

Il existe de nombreux objets connectés de santé dont voici une liste non exhaustive :

1. arythmie au niveau des oreillettes et des ventricules

1 **Les balances connectées comme la Body+ de Withings (figure 2.12)** : elles permettent de suivre le poids d'un utilisateur à long terme, en relation généralement avec un smartphone pour sauvegarder et afficher les données de poids et d'IMC (Indice de Masse Corporelle) sous forme de graphique. Leurs fonctions n'étant pas critiques, elles peuvent être conseillées par un médecin pour aider les patients en surpoids.

FIGURE 2.12 – Balance connectée Body + de Withings.

2 **Les montres (smartwatch) et les bracelets connectés** : une multitude de modèles existe sur le marché, et ils sont munis de nombreux capteurs : accéléromètre, gyromètre, podomètre, altimètre, magnétomètre, cardiofréquencemètre, GPS... Ces objets sont généralement couplés en bluetooth avec une application installée sur un smartphone, mais peuvent également fonctionner seuls : pour certaines montres par exemple, les données peuvent être retransmises au serveur associé par l'intermédiaire d'une carte SIM. L'usage des montres et des bracelets connectés est généralement réservé à la pratique du sport, du fitness ou encore de l'analyse du sommeil, avec notamment l'usage du capteur cardiaque. Ces capteurs manquent souvent de fiabilité pour être de véritables dispositifs médicaux. La marque Fitbit en a notamment fait les frais avec une action en justice pour mise en danger de la vie d'autrui. Ainsi peu de constructeurs prennent le risque de passer ces objets en dispositifs médicaux.

Cependant, de nouvelles montres connectées comme l'Apple Watch Series 4 (figure 2.13) ont obtenu, depuis début 2020, le marquage CE et sont autorisées dans l'Espace Économique Européen. Ce sont donc maintenant des dispositifs médicaux connectés permettant aux utilisateurs de réaliser des électrocardiogrammes et d'être notifiés de la détection de certains types d'arythmies.

FIGURE 2.13 – Montre Apple Watch Series 4.

Dans la littérature scientifique, les montres connectées sont utilisées pour différencier des tremblements particuliers de la maladie de Parkinson à l'aide de l'accéléromètre [Wil14] ou encore pour dépister une fibrillation auriculaire chez les sportifs victimes de syncopes pendant une course [Tha17].

Nous retrouvons d'autre usages plus insolites pour les bracelets et montres connectés :

- **un bracelet anti-nausées Reliefband Neurowave de la société Reliefband Technologies (figure 2.14)** : l'objet utilise le principe de la neuromodulation en envoyant des impulsions au nerf situé sous le poignet, ce dernier agissant justement sur la nausée stomacale.

FIGURE 2.14 – Bracelet anti-nausées Reliefband Neurowave.

- **une montre pour connaître son niveau d'alcoolémie, la BACtrack Skyn (figure 2.15)** : elle fonctionne en captant les molécules d'éthanol présentes dans le corps au travers de la peau.

FIGURE 2.15 – Montre alcootest BACtrack Skyn.

- **un bracelet anti-coups de soleil *June* de la société Française Netatmo** : il capte la quantité de rayons solaires que vous recevez puis envoie les informations sur un smartphone, qui prévient alors quand renouveler l'application de la crème solaire ou quand se mettre à l'ombre.
- **un bracelet détruisant les cellules cancéreuses, le Nanoparticle Phoresis par Google** : des nanoparticules d'oxyde de fer ingérées par le patient atteint du cancer permettent aux cellules cancéreuses repérées d'émettre de la lumière. Ces cellules parviennent au poignet, attirées par des aimants puis sont détruites par un processus de phorèse de nanoparticules : des transmissions d'énergie à l'aide de champs magnétiques, de radiofréquences, de signaux lumineux, d'infrarouges ou encore de pulsations acoustiques.

3 **Les anneaux connectés comme le Motiv Ring (figure 2.16)** : tout comme les bracelets connectés, ils utilisent un capteur de fréquence cardiaque et un accéléromètre pour évaluer, via une application sur smartphone, l'activité, les calories dépensées, le nombre de pas quotidien ainsi que le suivi du sommeil.

FIGURE 2.16 – Anneau connecté Motiv Ring.

4 **Le protège-dents connectés Prevent Biometrics (figure 2.17)** : destiné aux enfants pratiquant un sport à risques, il permet aux parents de surveiller les impacts à la tête et évaluer leurs sévérités.

FIGURE 2.17 – Protège-dents connectés Prevent Biometrics.

5 **Le patch pour femme enceinte Bloomlife (figure 2.18)** : le capteur enregistre les contractions en temps réel dans une application sur le smartphone et permet une visualisation des données dans le temps.

FIGURE 2.18 – Patch pour femme enceinte Bloomlife.

6 **Les chaussures connectées comme la Sensoria Primus par Vivobarefoot (figure 2.19)** : grâce à un capteur de pression, il est possible de remonter des informations d'impact et de temps de contact avec le sol pour optimiser les courses des sportifs.

FIGURE 2.19 – Chaussures connectées Sensoria Primus de Vivobarefoot.

Une multitude d'autres objets connectés sont en étude ou déjà en vente, comme les patchs intelligents connectés, les implants contraceptifs connectés (à désactiver ou activer à distance), les électrostimulateurs, les tétines connectées, les pompes d'allaitement... Ce marché est extrêmement dynamique et avec la crise du coronavirus de nombreux autres systèmes ont été ou sont en cours de développement.

2.2/ INTÉGRATION DES DMCs ET DES OCSs

Les données collectées des *OCSs* et des *DMCs* sont souvent stockées et gérées dans des référentiels distincts qui sont déconnectés et isolés des autres systèmes contextuels. Les données sont, pour la plupart, accessibles dans des silos verticaux de systèmes propriétaires, c'est-à-dire uniquement accessibles et compréhensibles par les logiciels de l'entreprise, voir une partie des logiciels de l'entreprise. La figure 2.20 représente un exemple d'architecture en silos.

Pour traiter les données efficacement dans un système de santé, il est nécessaire que les patients et les praticiens de la santé aient une vue intégrée de l'ensemble des connaissances, tout comme les systèmes de traitement automatisés de données de santé. Ces derniers pourront tenter de résoudre des problèmes spécifiques avec l'informatique cognitive, c'est-à-dire en mimant le processus de pensée humaine dans un modèle informatisé, en faisant intervenir des systèmes d'autoapprentissage, la reconnaissance de schémas ou encore le traitement du langage naturel...

En l'absence de standard pour la santé connectée, massivement utilisée par les constructeurs, une architecture intelligente et évolutive est nécessaire pour assurer la connectivité entre ces silos. C'est les technologies du Web Sémantique [1] et les ontologies qui semblent les plus appropriées pour répondre à ce besoin.

Cependant, afin de faciliter et de sécuriser l'intégration de nouveaux modèles de capteurs de santé, en communication avec les différents systèmes d'informations des hôpitaux et avec les plateformes de télémédecine, il est nécessaire d'utiliser un standard à tous les niveaux du système. L'unique standard pour la santé connectée reconnue internationalement est le standard Continua de la PCHA (*Personal Connected Health Alliance*), basé sur les différents standards de santé existant (HL7, FHIR, IEEE 11073...).

1. extension du Web standardisée par le World Wide Web Consortium (W3C). Ces standards encouragent l'utilisation de formats de données et de protocoles d'échange normés sur le Web, en s'appuyant sur le modèle RDF (Resource Description Framework).

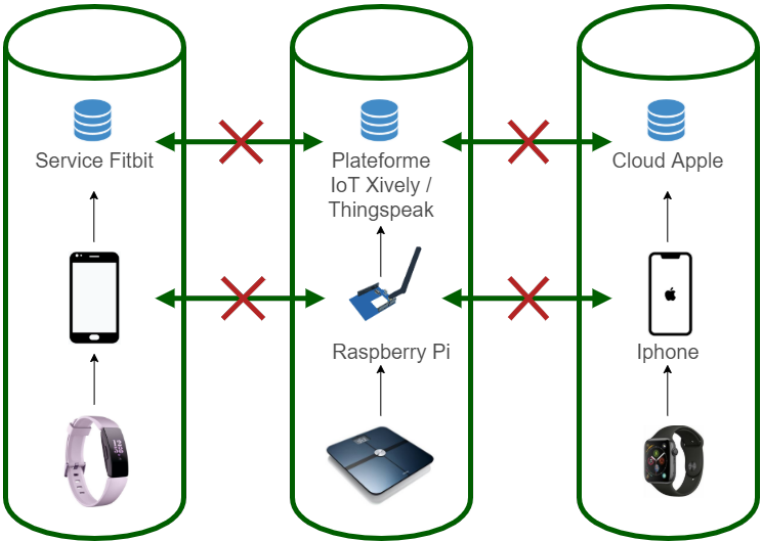


FIGURE 2.20 – Exemple d'architecture en silos.

2.2.1/ INTEROPÉRABILITÉ SÉMANTIQUE

Carbonaro et al. [Car18] exploitent des technologies du Web Sémantique pour décrire explicitement la signification des données des capteurs et pour faciliter l'interopérabilité et l'intégration des données entre différents appareils. Il utilise ensuite les ontologies, une spécification explicite lisible par les machines qui partagent les mêmes concepts. Ces ontologies offrent une infrastructure générique pour l'échange, l'intégration et la réutilisation de données structurées, et proposent une approche informatique cognitive pour mieux accéder aux connaissances. Toutefois, il faut souligner que les modèles de données doivent être décrits, à partir de structures de données totalement différentes, représentant un important travail lors de l'intégration de nouveaux capteurs, et ne proposant pas de solution lorsque les données sont stockées à différents endroits.

Pour répondre à cette dernière problématique, et sur le même principe de l'interopérabilité sémantique, Desai et Al. [Des15] proposent une passerelle sémantique et une architecture IoT compatible avec le Web sémantique. L'objectif est d'assurer l'interopérabilité entre les systèmes et la connectivité entre les silos de données, en utilisant des normes de communication et de données établies. La passerelle permet la traduction entre des protocoles d'échanges tels que XMPP, CoAP et MQTT. Elle utilise l'ontologie SSN (*Semantic Sensor Network*) du W3C pour les annotations sémantiques des données des capteurs, qui offre une interopérabilité sémantique entre les messages et prend en charge le raisonnement sémantique pour obtenir des connaissances exploitables. L'architecture de la passerelle est représentée sur la figure 2.21.

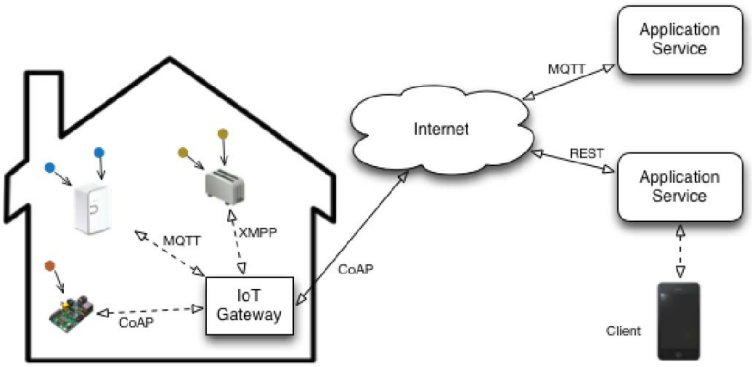


FIGURE 2.21 – Architecture IoT de la passerelle sémantique - issue de[Des15].

2.2.2/ INTÉGRATION AUX TERMINAUX MOBILES

Google Fit et Apple HealthKit

Les applications de santé mobile prolifèrent, en lien avec les objets connectés de santé ou les dispositifs médicaux connectés. Elles sont développées parfois par les constructeurs des objets connectés, mais également parfois par des développeurs tiers dont l'objectif est d'analyser une ou plusieurs sources de données. Dans tous les cas, les données sont stockées bien souvent sur un serveur cloud propre au constructeur de l'objet (architecture en silos). Les grands groupes à l'origine des systèmes d'exploitation mobiles, tels que Google, Apple ou encore Samsung, se placent depuis quelques années comme intermédiaires à la communication et au stockage des données de santé et de fitness des applications mobiles [Tol14]. Ces applications mobiles étant le point final d'un service supervisé plus vaste impliquant de nombreuses parties prenantes, ces grands groupes ont développé des boîtes à outils (toolkits) propres à chacun, comme le montre la figure 2.22, dont les objectifs sont :

- de faciliter la programmation des développeurs d'applications mobiles tierces pour l'analyse ou le partage de données,
- de standardiser au niveau de la boîte à outils les données,
- de regrouper les données au même endroit.

Les principaux toolkits des constructeurs sont : **Apple HealthKit**, **Google Fit**, **Samsung Digital Health**, **Huawei Health**.

Afin que les données soient récupérées dans les systèmes de stockage des toolkits, il est nécessaire que les constructeurs des objets connectés de santé et des dispositifs médicaux intègrent dans leur application mobile une association de données vers ces toolkits, et que l'utilisateur accepte de partager les données avec ces derniers. Les autorisations peuvent se faire directement depuis les applications tierces, et ce, sans que l'utilisateur ne comprenne qu'il va partager ses données de santé personnelles avec des géants de l'informatique, et implicitement, n'importe quelle autre application qui pourra exploiter ses données.

Les données supportées, en constante évolution, sont : le nombre de pas, la distance quotidienne parcourue, les calories dépensées, le type d'activité pratiqué, la taille, le poids, la fréquence cardiaque, le pourcentage de graisse, le taux de glucose, le sexe, la date de naissance, la nutrition (calories, poids, insaturés, polyinsaturé, cholestérol, sodium, sucre, vitamine, eau...), les dates de début et fin d'effort...

La sauvegarde des données se fera soit en local (comme chez Apple) ou encore sur un cloud (comme chez Google). Il y a également des restrictions d'utilisation de ces données. Par exemple Apple interdit aux développeurs d'application tiers de vendre les données médicales personnelles aux annonceurs ou de stocker les données médicales sur la plateforme iCloud (restriction liée au piratage). La question du stockage de données est importante du point de vue législatif, car les serveurs non certifiés HDS (*Hébergeur de Données de Santé*) ne sont pas autorisés à stocker des données de santé. Google, qui jusque-là se contentait d'utiliser son outil uniquement dans un cadre de fitness, a obtenu la certification HDS mi-2019 pour son Cloud, ce qui l'autorise à stocker des données de santé en Europe. Notons qu'il y a interdiction de la revente de données aux publicitaires, courtiers ou sociétés de données.

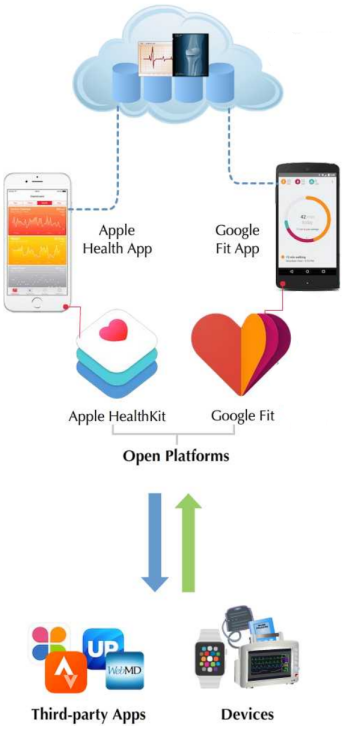


FIGURE 2.22 – Schéma de fonctionnement des toolkits de santé Google Fit et Apple Health Kit - issue de [Tol14].

Dans l'immédiat, les applications développées ne doivent pas être considérées comme des dispositifs médicaux. Il n'est pas possible d'utiliser ces outils en relation avec un quelconque service pouvant être qualifié de dispositif médical (*DM*).

2.2.3/ LE STANDARD CONTINUA POUR L'INTEROPÉRABILITÉ DES DISPOSITIFS MÉDICAUX CONNECTÉS

La *Personal Connected Health Alliance* (ou PCHA) [Car07] [War10] est un groupe international à but non lucratif et ouvert, de près de 240 prestataires de soins de santé développant le standard Continua. L'alliance estime que la santé est personnelle et s'étend au-delà des soins de santé. Ses membres sont des fabricants d'équipements et de solutions, des groupements hospitaliers, des représentants des pouvoirs publics (gouvernements), des laboratoires pharmaceutiques ou encore des établissements universitaires.

Le standard Continua a pour objectif principal de faciliter et de sécuriser l'intégration de nouveaux modèles de capteurs de santé communiquant avec les systèmes d'information des hôpitaux et les plateformes de télémédecine. Cela aboutira implicitement à une facilité de développement de programmes de télésurveillance aux domiciles des patients, au sein desquels sont mis en œuvre les dispositifs médicaux connectés.

Les bénéfices de ce standard en sont multiples :

- déploiement à grande échelle de la télésurveillance médicale,
- intégration des dispositifs médicaux des patients télésurveillés et des données résul-

tantes avec les dossiers patients,

- sécurisation des échanges,
- économies et gain de temps pour tous les acteurs dans une prise en charge : le patient, les professionnels de santé, ou encore les développeurs d'applications.

Le standard Continua est l'unique standard pour la santé connectée reconnu internationalement et soutenu par les institutions européennes (DG santé et DG Connect) et depuis début 2017 par l'ONC (*Office of the National Coordinator*) aux Etats-Unis. Les directives de conception Continua sont reconnues par l'Union Internationale des Télécommunications des Nations Unies (*UIT-T*) comme la norme internationale pour l'échange sûr, sécurisé et fiable de données vers et depuis les appareils de santé personnels : la sécurité et la confidentialité sont assurées de bout en bout grâce à une combinaison de gestion des identités, de l'intégrité, des consentements, des authentifications des entités et de la non-répudiation des données.

Ce standard permet également une intégration beaucoup plus rapide et beaucoup moins onéreuse de nouveaux capteurs (*« Plug & Play »*) à condition qu'il soit respecté. Pour cela, le standard définit la structure des données échangées, le moyen de communication, les étapes d'appareillage des objets ainsi que la sécurité des dispositifs. Il s'appuie sur des normes existantes, telles que IEEE 11073 pour les capteurs personnels de santé, *HL7 et HL7 FHIR* (nomenclature des termes cliniques dans le milieu médical), ainsi que la transaction PCD-01 d'IHE [Pch17] [Lee18].

2.2.3.1/ IEEE 11073

IEEE 11073 [Pch17] est une famille de normes de dispositifs de santé personnels pour la représentation et l'échange des données de santé entre les dispositifs médicaux (de santé et/ou de bien-être) et les systèmes informatiques externes (passerelle). Ces normes sont réparties en 4 partitions principales : les données sur les dispositifs, les services d'application, les normes d'interconnexion et de passerelle et le transport des messages.

Leurs objectifs sont :

- une interopérabilité « Plug & Play » en temps-réel pour les appareils médicaux, de santé et de bien-être pour les utilisateurs, peu importe l'endroit où ils se situent,
- des échanges efficaces de données sur les dispositifs de soins dans tous les environnements de soins, en temps-réel.

Pour le standard Continua, l'utilisation de ces normes se situe au niveau de l'interface des dispositifs de santé personnels (*Personnal Health Device Interface - PHDI*) visible sur la figure 2.23. Cette interface permet les échanges entre les dispositifs personnels de santé (*Personnal Health Device - PHD*) et la passerelle personnelle de santé (*Personnal Health Gateway - PHG*). Les concepts d'agents et de gestionnaires sont définis dans cette norme. L'agent est le dispositif médical personnel qui fournit les données. Le gestionnaire conserve une copie des données de l'agent, il réagit aux événements de mise à jour et enfin il déclenche des événements sur l'agent. Le gestionnaire est utilisé pour surveiller, afficher à distance les données des agents, et acheminer des informations de façon autonome depuis la source vers

la cible, mais il peut également contrôler à distance les agents pour demander d'effectuer les mesures.

Un message 11073 typique transporte différents types de mesures, avec des attributs communs sur le dispositif (fabricant, modèle...), des attributs spécifiques au dispositif (unité, date...) et des événements de dispositif (mise à jour, configuration, demande de mesure). Continua travaille à déterminer des profils d'utilisation contenant pour chacun d'eux un sous-ensemble d'attributs suffisants pour des mesures spécifiques : comme le tensiomètre ou la surveillance de la thérapie respiratoire de l'apnée du sommeil. Le nombre de profils est de 23 aujourd'hui.

Cette famille de normes garantit que les informations critiques ne sont pas perdues lors de leur transport du capteur vers la passerelle puis vers le dossier du patient. En outre, elle s'exécute au-dessus des protocoles de transport USB, Bluetooth, BLE (*Bluetooth Low Energie*), NFC et ZigBee. Ces technologies de communication peuvent donc être utilisées dans l'architecture Continua lors des échanges entre les dispositifs personnels de santé (PHD) et la passerelle personnelle de santé (PHG). Ce seront également ces technologies qui assureront la confidentialité, l'intégrité et l'authentification des données à travers l'interface des dispositifs de santé personnels.

2.2.3.2/ HL7 V2 ET HL7 FHIR

Health Level 7 (*HL7*) [Pch17] définit les spécifications techniques au niveau de la structure des messages échangés pour les échanges informatisés entre systèmes d'information hospitaliers. Ces spécifications sont définies par *Health Level Seven International* (une organisation internationale de normalisation) et tendent à devenir un standard international pour ce type d'application. Par exemple, le Dossier Médical Personnel (*DMP*) est alimenté, depuis 2010, dans le respect de la norme HL7.

Le L7 de HL7 indique qu'il fonctionne uniquement au niveau de la couche 7 du modèle OSI : la couche application (cf chapitre 3). Il ne prend donc pas en compte l'aspect transport ou la sécurité des échanges. Dans le standard Continua, ces normes sont utilisées pour représenter les données lors des transactions entre une passerelle (*Personnal Health Gateway - PHG*) de santé personnelle et des services de santé et de fitness. Ils interviennent donc sur l'interface de services (*Service Interface*) comme le présente la figure 2.23.

Depuis peu, le standard Continua est compatible avec l'utilisation de *HL7 FHIR* (*Fast Healthcare Interoperability Resources*). Ce dernier utilise une suite Web moderne de technologie, notamment les *API RESTful* basées sur le protocole HTTP, les authentifications *OAuth* et du *JSON* pour la représentation des données (à la place de XML). Il est donc plus facile à mettre en œuvre, plus ouvert et plus extensible que la V2 ou la V3. Les directives de conception Continua spécifient comment mapper les attributs *IEEE 11073* reçus d'un capteur aux ressources *FHIR*.

Les directives de conception Continua spécifient comment les transactions entre la passerelle (*PHG*) et les services de santé et de fitness peuvent s'effectuer par ces ressources *HL7 FHIR* (via *REST* et l'authentification *OAuth*), mais également par le profil *IHE PCD-01* (via *SOAP*, l'authentification *SAML* et *HL7 V2.6* pour les données).

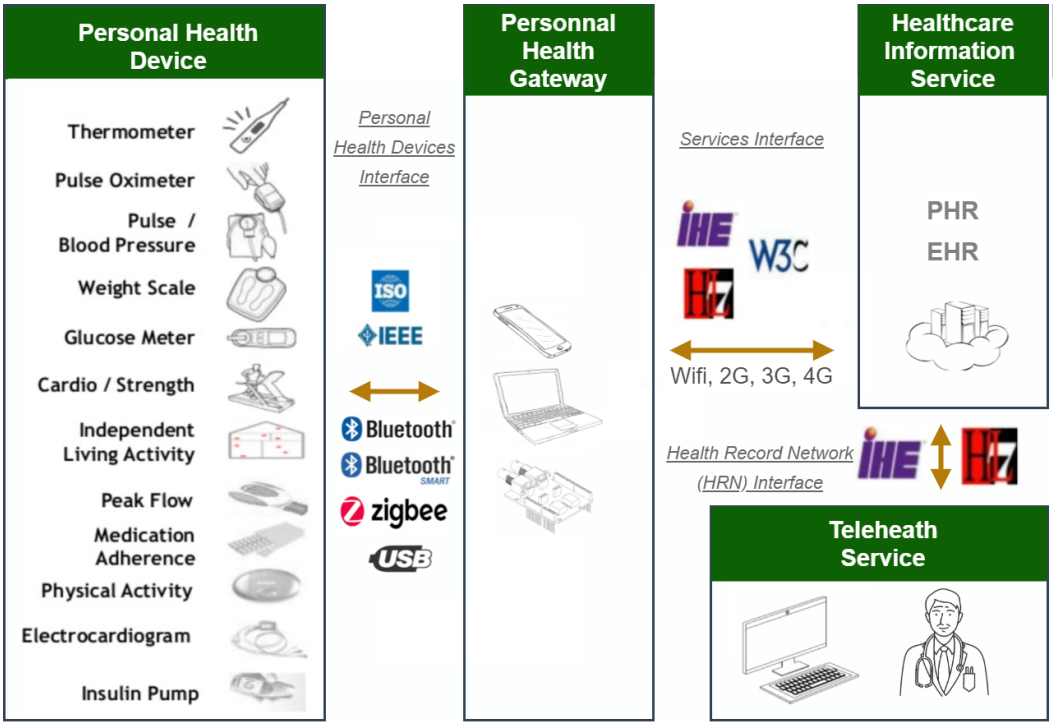


FIGURE 2.23 – L'architecture de Continua sur les différents acteurs.

2.2.3.3/ IHE PCD-01

IHE (*Integrating the Healthcare Enterprise*) [Lee18] est une organisation américaine à but non lucratif dont l'objectif est d'améliorer la façon dont les systèmes informatiques partagent les informations. Elle développe notamment des profils de partage d'informations standardisées dans les systèmes d'informations sur les soins de santé. En particulier, l'*IHE* a publié le profil *Patient Care Device (PCD)* pour la transmission des données d'observations enregistrées par les appareils médicaux. Les transactions *PCD-01* sont généralement transportées selon le protocole *SOAP (simple-object access protocol)* basé sur HTTP pour le transport, l'authentification SAML pour la sécurité et XML pour la représentation des données. Les messages utilisés dans les transactions *PCD-01* sont issus de la norme de message *HL7 v2.6*.

Dans l'architecture Continua, la transaction *IHE PCD-01* est utilisée pour communiquer entre la *Personal Health Gateway* et les services consommateurs au niveau de l'interface de services (2.23).

2.2.3.4/ ADOPTION

La *PCHA* met ainsi à disposition des directives de conception (*Continua Design Guidelines - CDG*) [Gui19], développées et révisées régulièrement en collaboration ouverte entre l'industrie et les fournisseurs. Elle propose également aux fabricants une certification Continua, qui confirme la conformité de leurs appareils et des systèmes avec les *CDG*. Pour finir elle met à disposition une bibliothèque de code source et des logiciels de tests pour simuler des dispositifs (*PHD*) ou une passerelle (*PHG*) qui suivent la ligne directrice.

Actuellement environ 70 objets connectés et dispositifs médicaux possèdent la certification

Continua [Sho20] comme le glucomètre *CareSens® N Premier* (figure 2.24). Également, certains fabricants commercialisent des passerelles (*PHG*) sur mobile via des applications ou des environnements de développement (SDK), ou encore des applications qui jouent le rôle de service de soins et fitness.

FIGURE 2.24 – Glucomètre *CareSens® N Premier* utilisant le standard Continua.

L'adoption du standard Continua se fait progressivement depuis 2012. Voici les exemples les plus marquants qui lui ont permis d'avancer :

- depuis 2012, le gouvernement du Danemark a adopté en 2012 les lignes directrices de Continua comme base pour ses services de télésanté.
- depuis 2014, en Norvège, le ministre de la santé a décrété que les technologies de bien-être seront normalisées pour se conformer aux lignes directrices de conception Continua.
- depuis 2015, le gouvernement Autrichien prévoit de déployer des services de surveillance à distance du diabète, des maladies cardiaques et des patients porteurs de dispositifs cardiaques implantés qui comprendront des références aux lignes directrices de conception Continua.
- depuis 2017, en Catalogne, pour se connecter au système de dossier de santé électronique de la région, les glucomètres personnels doivent respecter les exigences basées sur les directives de conception Continua de *PCHAlliance*. Le gouvernement a fait un achat de 50 millions d'euros de glucomètres.
- depuis 2017, en Suède, l'Association suédoise des pouvoirs locaux et des régions (*SALAR*) a recommandé des lignes directrices de conception Continua pour la transmission des données personnelles sur la santé.

Malgré tous les bénéfices de l'adoption du standard Continua, et en raison principalement des forces du marché, l'adoption universelle de ces lignes directrice est loin d'être une réussite. Le marché reste fragmenté par des protocoles propriétaires qui dominent le domaine, et aucune norme n'a émergé. Par ailleurs, le manque de demandes réelles sur des appareils conformes au standard Continua n'incite pas les fabricants à en commercialiser. Les petits fabricants, startup, ou chercheurs sont rapidement désorientés devant la complexité des 700 pages du *CDG*, et ne peuvent pas mettre en œuvre rapidement des cas d'utilisation (comme le développement d'une passerelle). L'offre limitée rend difficile pour les acheteurs publics d'imposer le respect des normes internationales dans leurs achats. Seuls les gros acheteurs peuvent faire évoluer le marché vers des normes ouvertes : les gouvernements et les autres systèmes de santé publics, ce qui n'est pas le cas actuellement.

Synthèse du chapitre 2

SYNTHÈSE

Dans cette section, nous avons pu définir les contraintes réglementaires, les différentes classes de risques, et le marquage CE sur les dispositifs médicaux connectés (*DMCs*) afin de différencier des objets connectés de santé (*OCSs*).

Il était important de définir et de donner des exemples concrêts de *DMCs* (oxymètres, glucomètres, stéthoscopes...), et d'*OCSs* (bracelets, montres, balances,...), ainsi que de leurs fonctionnalités et de leurs finalités.

Pour terminer, nous avons détaillé leur intégration dans une plateforme de télésurveillance, dont l'interopérabilité en est la principale difficulté : à l'aide du web sémantique, des toolkits des fabricants de mobiles ou encore l'adoption des lignes directrices du standard Continua pour la santé connectée.

Pour Continua, nous avons pu analyser les différentes normes de santé qui le compose, et nous avons cherché à comprendre les raisons pour lesquelles il n'était pas adopté par une communauté plus importante.

Le chapitre suivant est consacré à l'aspect réseau de l'internet des objets ainsi qu'à l'étude des différents protocoles qui le composent.

3

Les réseaux de l'Internet des Objets

Afin de transmettre les données de santé à un serveur distant, les dispositifs médicaux utilisent des stratégies et des technologies de communication différentes. Pour certains, les données sont retransmises au serveur par l'intermédiaire d'un smartphone. Pour d'autres, cela se réalise directement à l'aide de protocoles sans fil longue distance tels que les LTE (2G, 3G ou 4G), ou encore les LPWANs (*Low-Power Wide-Area-Network*).

Il existe de nombreuses technologies de communication. En fonction de l'application, de la portée, des besoins en données, de la puissance, de la sécurité ou encore de la durée de vie des batteries, les combinaisons de technologies seront différentes.

Les protocoles les plus utilisés actuellement dans les technologies de communication (sur ordinateur, ou smartphone généralement) ne conviennent pas parfaitement aux nouveaux dispositifs de l'Internet des Objets. Pour la plupart, ils entraînent une consommation excessive en énergie, des besoins en ressources réseau ou mémoire trop importants ou des contraintes de mise en place impossibles à tenir. L'Internet des Objets a donc conduit à l'émergence de nouveaux protocoles dont les caractéristiques sont adaptées à son domaine :

- une faible consommation en énergie,
- une grande portée,
- des débits de données faibles,
- des coûts moins élevés,
- une facilité de mise en œuvre,
- ...

Dans ce chapitre nous aborderons les réseaux sans fil destinés à l'Internet des Objets. Nous exposerons le fonctionnement des réseaux sans fil, les attentes de ces réseaux pour l'IoT et les différents types de réseaux par étendue spatiale. La majeure partie de ce chapitre sera consacrée ensuite à la description des différents réseaux destinés à l'IoT classés en deux parties bien distinctes : les réseaux longue portée d'une part et les réseaux courte portée d'autre part.

Ce chapitre a nécessité un très gros travail de synthèse parmi la masse très importante et dispersée d'informations sur ces réseaux. Il a abouti en particulier au tableau comparatif 3.3.

3.1/ QUELQUES FONDAMENTAUX

3.1.1/ LES RÉSEAUX SANS FIL

Une des définitions de L'IoT est la suivante [Sur15] : *« c'est un réseau de réseaux qui permet, via des systèmes normalisés et unifiés d'identification électronique, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter les données s'y rattachant, sans discontinuité entre les mondes physiques et virtuels.»*. Les réseaux sont donc au cœur de l'Internet des Objets, et particulièrement les réseaux sans fil.

Il existe différentes technologies de communications sans fil :

1. les communications radio et micro-onde véhiculent des informations en modulant les propriétés des ondes électromagnétiques transmises dans l'espace,
2. la communication optique en espace libre (FSO : *Free Space Optics*) utilise la lumière se propageant dans l'espace libre. Un exemple largement utilisé est celui des appareils infra-rouge grand public tels que les télécommandes et le réseau IrDA (*Infrared Data Association*),
3. la communication sonique, en particulier ultrasonique à courte portée, implique la transmission et la réception du son,
4. l'induction électromagnétique pour la communication à courte portée et la transmission de puissance est utilisée par exemple dans les étiquettes RFID à courte portée ou les stimulateurs cardiaques.

Nous ne disserterons dans ce chapitre que des communications radio impliquant les ondes électromagnétiques. Leur propagation, en particulier grâce leur grande longueur d'onde, a la capacité de traverser l'atmosphère et la plupart des matériaux de construction par diffraction et en se déformant autour des obstacles. De plus, elles ont tendance à être dispersées plutôt qu'absorbées par des objets plus grands que leur longueur d'onde, contrairement aux autres ondes électromagnétiques, ce qui les rend plus utilisables pour la télécommunication [Ell16].

Voici une chronologie simple de l'évolution des technologies sans fil au cours du temps :

- 1886 : Heinrich Hertz identifie pour la première fois les ondes radio.
- 1896 : Guglielmo Marconi développe le premier système télégraphique sans fil.
- 1927 : Premier service de radiotéléphonie commercial exploité entre la Grande-Bretagne et les États-Unis.
- 1946 : Premier téléphone mobile basé sur une voiture installé à Saint-Louis, utilisant la technologie *«push-to-talk»*.

- 1950 : TD-2, le premier système de télécommunications hertzien terrestre, installé pour prendre en charge 2400 circuits téléphoniques.

- 1962 : Premier satellite de communication, Telstar, lancé en orbite.

- 1968 : Début du développement de l'ARPANET (*Advanced Research Projects Agency Network*), le père de l'Internet moderne.

- 1968 : Premier réseau sans fil professionnel développé sous la marque ALOHAnet en 1969 à l'Université d'Hawaï.

- 1977 : Installation du système de téléphonie mobile avancé (AMPS : *Advanced Mobile Phone System*), inventé par Bell Labs, aux États-Unis avec des régions géographiques divisées en «cellules» (Téléphone cellulaire).

- 1977 : Invention d'Internet et des normes 802 de l'IEEE,

- 1987 : Lancement du *Global Positioning System* : GPS.

- 1991 : Réseau de téléphonie mobile 2G et premier SMS,

- 1993 : Protocole Internet version 4 (*IPv4*) établi pour une transmission fiable sur Internet conjointement avec le protocole de contrôle de transport (TCP :*Transmission Control Protocol*).

- 1998 : Arrivée des technologies sans fil Wi-Fi et Bluetooth.

- 2000 : Premiers accès à Internet en mobilité pour tous avec la 3G.

- 2010 : Arrivée de la 4G.

- 2015 : Mise sur le marché des LPWANs (Sigfox, LoRaWAN...).

- 2020 : Commercialisation de la 5G.

Les ondes radio sont émises par des charges électriques en cours d'accélération [Ell16]. Ce sont les courants électriques qui génèrent artificiellement ces ondes en variant dans le temps. Ceux-ci sont constitués d'électrons qui circulent d'avant en arrière dans un conducteur métallique : l'antenne.

Une communication radio peut être ainsi résumée en quatre étapes comme le montre la figure 3.1 :

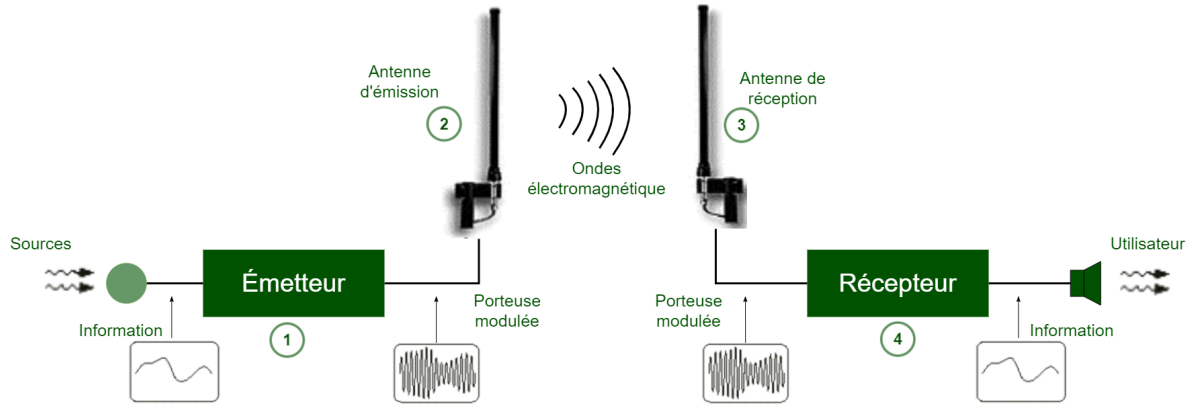


FIGURE 3.1 – Les étapes d'un communication radiofréquence [Ond20]

① L'émetteur génère un courant alternatif de radiofréquence qui est appliqué à une antenne.

② L'antenne émet la puissance de ce courant sous la forme d'ondes radio. On parle d'ondes porteuses quand elles transportent de l'information.

③ Les ondes frappent l'antenne d'un récepteur radio et poussent les électrons dans le métal d'avant en arrière, induisant un minuscule courant alternatif.

④ Le récepteur radio connecté à l'antenne détecte ce courant oscillant et l'amplifie puis le démodule (extraction de signal de modulation d'origine grâce à l'onde porteuse).

Les ondes radio se propagent dans l'air, et à mesure qu'elles s'éloignent de l'antenne d'émission, la force de leur signal (intensité en watts par mètre carré) diminue. Les transmissions radio ne peuvent donc être reçues que dans une portée limitée de l'émetteur en fonction de plusieurs paramètres : puissance de l'émetteur, diagramme de rayonnement de l'antenne, sensibilité du récepteur, niveau de bruit (interférences), présence d'obstacles...

La fréquence représente le nombre d'oscillations par seconde. Par exemple une fréquence de 868 MHz compte 868 millions d'oscillations par seconde. La longueur d'onde représente quant à elle la distance en mètres entre les crêtes adjacentes de l'onde. Dans l'air, les ondes radio se propagent à une vitesse très proche de la lumière. La longueur d'onde sera donc inversement proportionnelle à sa fréquence. En d'autres termes, plus la fréquence est élevée, plus la longueur d'onde sera petite.

On parle d'antenne omnidirectionnelle quand celle-ci reçoit des ondes radio dans toutes les directions, au contraire de l'antenne directionnelle. Ce sont ces premières qui sont les plus utilisées dans les systèmes de télécommunications sans fil. L'antenne de réception capte généralement les signaux radio de nombreux émetteurs. Le récepteur utilise des circuits dits *accordés* pour sélectionner le signal radio souhaité parmi tous les signaux captés par l'antenne et rejeter les autres.

Le signal électrique transportant l'information variant dans le temps est appelé signal de modulation. Suivant les méthodes de modulation et son signal analogique ou numérique, il

fait intervenir différents paramètres comme la variation de l'amplitude et la fréquence. Le type de modulation choisi a un impact significatif sur la consommation énergétique. Les méthodes de modulation les plus connues sont les suivantes :

- AM : modulation de l'amplitude utilisée pour la radiodiffusion,
- FM : modulation de la fréquence utilisée pour la radiodiffusion,
- FSK (*Frequency-shift keying*) : modulation par déplacement de fréquence (utilisé pour le GSM), c'est l'équivalent à la modulation FM en signal numérique,
- OFDM (*Orthogonal Frequency-Division Multiplexing*), modulation par répartition en fréquences orthogonales sous forme de multiples sous-porteuses (utilisée par la 4G, ou encore LTE-M et NB-IoT) mais consommatrice d'énergie,
- PSK (*Phase-Shift Keying*) : modulation par changement de phase de la porteuse (utilisé par Sigfox et NB-IoT),
- CSS (*Chirp spread spectrum*) modulation à étalement de spectre pour la technologie LoRa.
- ...

Ainsi, une onde radio modulée, transportant un signal d'information, occupe une gamme de fréquences. On parle de largeur de bande (*Bandwidht ou BW*), en hertz, la gamme de fréquences occupée par le signal radio. La largeur de bande requise par une transmission radio dépend du débit de données des informations (signal de modulation) envoyées et de l'efficacité spectrale de la méthode de modulation utilisée.

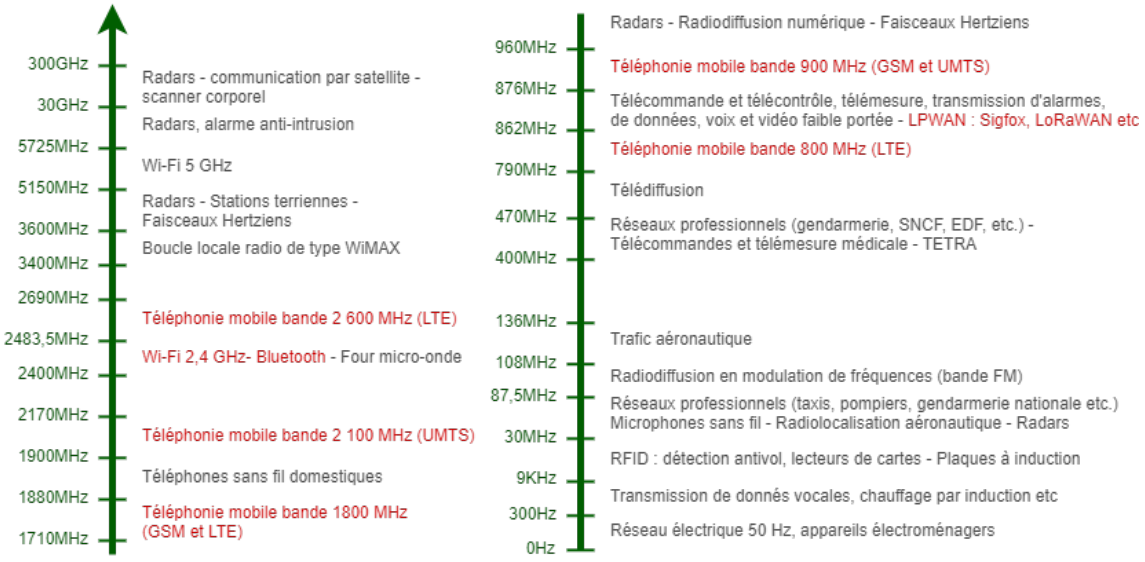


FIGURE 3.2 – Les applications par bandes de fréquences - [Ans15].

Le spectre radioélectrique, la gamme totale de fréquences radioélectriques pouvant être utilisée pour la communication dans une zone donnée, est une ressource limitée. Chaque

transmission radio occupe une partie de la bande passante totale disponible. La conséquence est que l'utilisation de certaines parties du spectre radioélectrique se vend très cher (par exemple + de 2,17 milliards pour la bande 3490 et 3800 Mhz destinée à la 5G en France). C'est l'Union Internationale des Télécommunications (*UIT*), qui est en charge de l'attribution de ces bandes de fréquences dans le spectre radioélectrique. Elle définit, avec les états, la réglementation sur l'émission d'ondes radio. L'un des objectifs est d'éviter les interférences entre les utilisateurs. Le spectre radioélectrique utilisable pour la communication se situe entre 30 hertz (Hz) et 300 gigahertz (GHz). La figure 3.2 montre l'utilisation du spectre par rapport aux différentes applications. Les applications en rouge représentent les applications les plus intéressantes dans l'IoT : les technologie cellulaires (LTE, GSM...), les LPWANs (LoRaWAN, Sigfox...) et les réseaux courte portée (Wi-Fi, Bluetooth...).

3.1.2/ LES TYPES DE RÉSEAUX INFORMATIQUES PAR ÉTENDUE SPATIALE

La télésurveillance médicale et, d'une manière générale, la télémédecine font intervenir différents types de réseau, et ce au sein même d'une plateforme. Selon la taille des réseaux, leur portée, leur capacité physique ou encore leur finalité, il est possible de les catégoriser suivant des types de réseaux. La figure 3.3 montre les principaux types de réseaux informatiques par étendue spatiale définis dans la littérature.

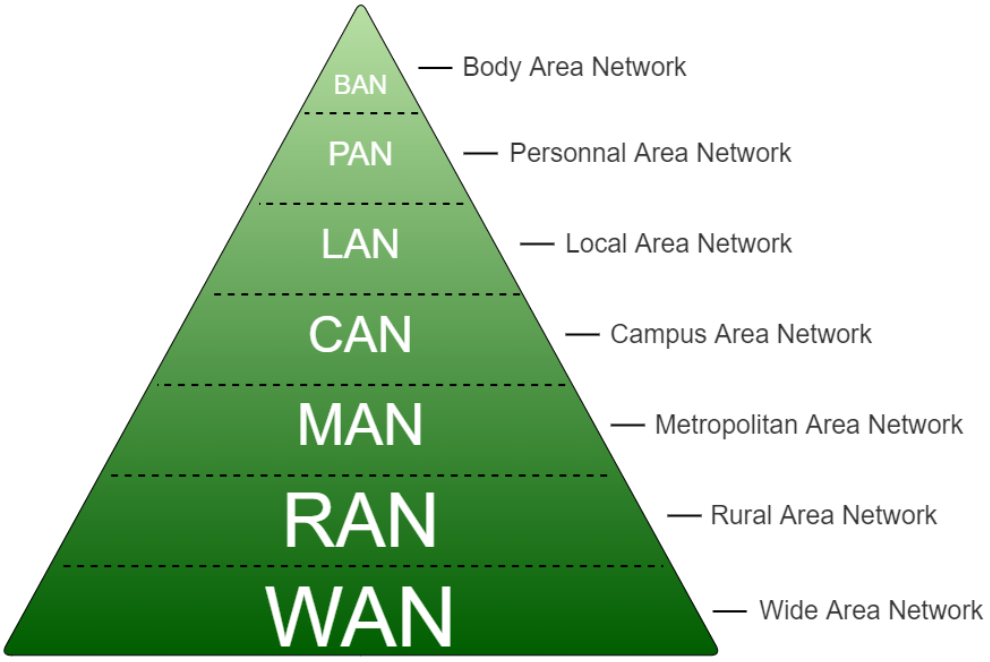


FIGURE 3.3 – Types de réseaux informatiques par étendue spatiale.

Dans le domaine des plateformes de télésurveillance, les types de réseaux utilisés seront :

- *Body Area Network* (BAN) : réseau de dispositifs (capteurs et actionneurs) intégrés dans ou sur le corps des personnes mais également dans les poches de vêtements, à la main, ou dans divers supports... Nous reviendrons sur ce type de réseau particulièrement intéressant dans nos recherches, @section 3.4.

- *Local Area Network* (LAN) ou *Home Area Network* (HAM) : réseau local, souvent au domicile des personnes, avec des dispositifs comme des objets connectés disposés dans la maison, des caméras ou des capteurs...
- *Wide Area Network* (WAN) : réseau qui couvre une grande zone géographique telle une ville ou un pays. Les lignes téléphoniques ou les câbles sont des exemples de supports pour ces réseaux étendus. Mais également, les ondes radio sont utilisées avec les technologies de communication sans fil longue portée comme la 3G, 4G, les LPWANs (Sigfox, LoRaWAN)...
- Internet : réseau particulier car unique et sans espace géographique. C'est l'ensemble des réseaux mondiaux interconnectés (gouvernementaux, universitaires, entreprises, publics et privés...).

Dans l'IoT, chacun de ces types de réseaux possède une couche technologique adaptée en fonction de son besoin (en portée, en énergie, débit, prix ou encore accessibilité). Dans la suite de cette section nous étudions, toujours dans un contexte de télésurveillance des patients, quels sont les protocoles les plus prometteurs à chacun des niveaux ainsi que les axes de recherche.

3.1.3/ Le modèle OSI appliqué aux protocoles de l'IoT

Afin de présenter les nouveaux protocoles de l'Internet des Objets, il est important de savoir à quel niveau ils se situent. Nous allons utiliser le modèle OSI (*Open Systems Interconnection*) pour catégoriser ces protocoles. Ce modèle est une norme qui décrit comment les dispositifs devraient communiquer entre eux. Son objectif est de normaliser les communications pour garantir une évolutivité et une interopérabilité entre ceux-ci. Le modèle est représenté en 7 couches qui ont chacune un rôle défini comme le montre le tableau 3.1 :

Couche	*Rôle*
7-Application	Point d'accès aux services réseaux.
6-Présentation	Chiffrement et conversion de données entre machines.
5-Session	Communication inter-host, gestion de sessions entre applications.
4-Transport	Connexion end-to-end et contrôle de flux.
3-Réseau	Détermine le parcours des données et l'adressage logique. Elle utilise un algorithme de routage ad hoc pour router les paquets entre les différents nœuds d'un réseau maillé mobile sans connaître la topologie du réseau ou la qualité des liens.
2-Liaison	Adressage physique. Dans les réseaux sans fil, c'est elle qui reconnaît et délimite le début et la fin des trames, assure l'adressage des stations de destination, détecte les erreurs de transmission, filtre les trames non destinées...
1-Physique	Transmission des signaux. Elle gère, entre autres, la génération de la fréquence porteuse, la détection des signaux, la modulation/démodulation et le chiffrement/déchiffrement des informations.

TABLE 3.1 – Les couches du modèle OSI.

Les protocoles les plus utilisés dans l'Internet des Objets ont été retenus suivant leur apparition dans la littérature et selon nos besoins dans le cadre de cette thèse. Ils ont été catégorisés (figure 3.4) en fonction des 7 couches précédemment présentées et séparés en quatre usages :

- les protocoles catégorisés dans les réseaux corporels (BAN), avec des technologies à ultra-faible portée et très peu consommatrices : IEEE 802.15.6, RFID,
- les protocoles catégorisés dans les réseaux locaux (LAN), avec des technologies faible portée : IEEE 802.15.4, ZIgbee, Bluetooth, Wi-Fi, Thread...
- les protocoles catégorisés dans les réseaux de grande étendue (WAN), avec des technologies grande portée ou filaires, et plus ou moins consommatrices d'énergie selon les besoins : LoRaWAN, Sigfox, NB-IoT, LTEM-M, Ingenu...
- les protocoles multi-niveaux appartenant aux couches hautes du modèle OSI et pouvant être utilisés dans différents types de réseaux : IP, TCP, UDP, HTTP...

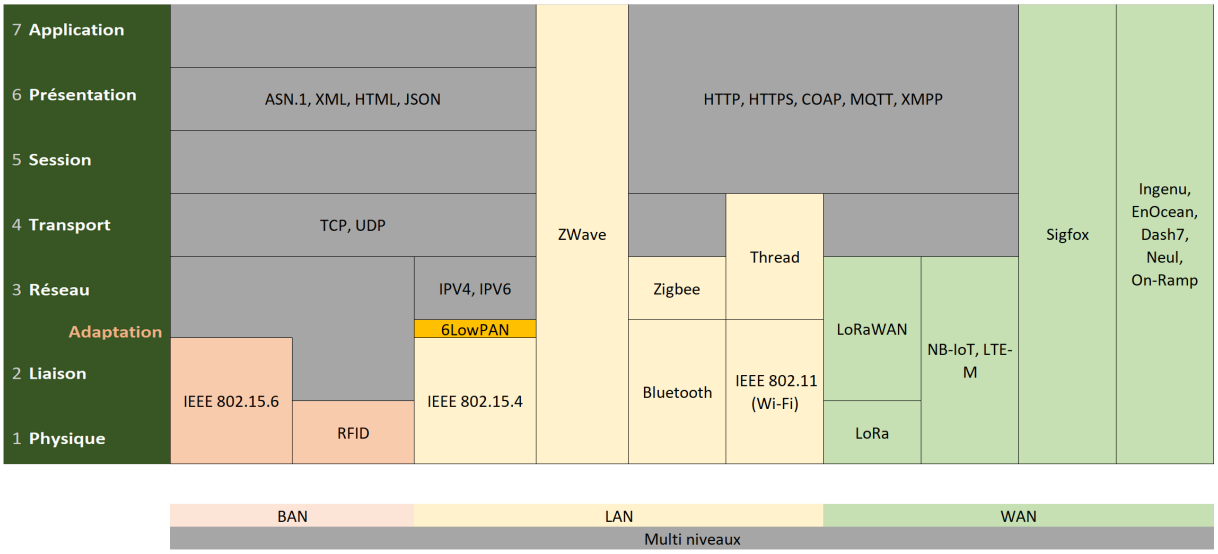


FIGURE 3.4 – Les protocoles de l'Internet des Objets en fonction des couches du modèle OSI.

Les nouveaux protocoles de l'Internet des Objets se situent principalement au niveau des réseaux étendus (WAN). Bien que certains protocoles soient ouverts ou open sources, les opérateurs se placent souvent en fournisseurs d'applications et contrôlent toute la couche du modèle OSI, de la puce jusqu'au service. Les raisons sont les performances énergétiques, la sécurité, la facilité d'utilisation et d'installation, ou tout simplement la compatibilité avec une technologie innovante. Au niveau des protocoles destinés aux réseaux locaux, c'est une évolution des protocoles existants pour l'IoT qui semble prendre le dessus, comme le *Bluetooth Low Energy*.

Dans la suite de ce document, nous décrivons et comparons ces protocoles suivant les étendues spatiales, en nous attardant particulièrement sur ceux des réseaux étendus (WAN). C'est sur ce point que nous orientons principalement nos recherches.

3.2/ Les technologies des réseaux étendus (WAN)

Pour le déploiement d'objets dans un environnement plus vaste comme dans la nature, d'autres moyens de communication entrent en jeu. Les réseaux cellulaires sont massivement utilisés dans le monde pour connecter les smartphones en dehors de la maison et participer à l'Internet des Objets. Les opérateurs téléphoniques proposent, en échange d'un abonnement, une couverture du territoire par les différentes technologies cellulaires : 2G, 3G, 4G et prochainement 5G. L'utilisation de la 2G est particulièrement intéressante pour les capteurs autonomes sur batterie car relativement économe en énergie par rapport aux autres technologies. Des initiatives sont en cours par le consortium 3GPP (*3rd Generation Partnership Project*) pour standardiser ce type de connexion et proposer des versions adaptées aux objets, avec une faible consommation énergétique. La 5G intégrera notamment un mode à faible consommation énergétique. Toutefois, le facteur clé des communications *IoT* est l'arrivée des *Low-Power Wide-Area-Networks*, ou LPWANs : des réseaux étendus à faible consommation énergétique.

3.2.1/ Les bandes de fréquences ISM : *Industrielle, Scientifique et Médicale*

Les protocoles LPWANs utilisent généralement des bandes de fréquences dites ISM [Ism17] : ce sont des bandes de fréquences qui peuvent être utilisées pour des applications industrielles, scientifiques, médicales, domestiques ou similaires à l'exception des applications de radiocommunication et de radio-repérage.

Elles peuvent être utilisées gratuitement à condition de respecter :

- La puissance d'émission : puissance maximale qu'un émetteur peut utiliser sur le canal lorsqu'il communique. Elle est habituellement de 25 mW pour LPWAN.
- Le *duty cycle* : coefficient d'utilisation ou *temps de vol limite*. Il est défini comme le rapport maximum de temps de transmission par heure. Un duty cycle de 1% signifie que l'on peut communiquer au maximum 36 secondes par heure. Le cycle de service est applicable à la sous-bande.

Ces limitations ont pour but de ne pas saturer la bande de fréquence radio. La norme EN 55011 définit les bandes de fréquences pour l'Union Européenne. Elle définit notamment les bandes suivantes :

- 433 MHz : utilisée pour des liaisons domestiques à faibles performances comme les télécommandes de voitures ou de portails,
- 868 MHz : utilisée dans les réseaux M2M [1] comme Sigfox et LoRa ou encore les réseaux d'équipements domotiques comme EnOcean [2] et Z-Wave,
- 2,4 GHz : utilisée par les réseaux WLAN [3] (comme le Wi-Fi), les dispositifs Bluetooth et des réseaux LoRa locaux.
- 5,8 GHz : également utilisée par des réseaux et dispositifs WLAN.

1. Machine-to-Machine
2. technologie radio sans pile courte portée en utilisant des cristaux piézoélectriques
3. Wireless Local Area Network

La bande de fréquence 868MHz, utilisée en Europe, est une bande passante publique européenne LPWAN (*Low Power Network*) que LoRaWan utilise pour la communication. Cette bande passante est régulée par différentes normes comme ERC-REC-70-3E [Erc18] définie par le CEPT [1] pour l'Europe ainsi que par des applications par pays, comme l'ARCEP [2] 2014-1263 pour la France. Cette bande de fréquences, qui s'étale de 865MHz à 870MHz, est découpée en 6 canaux avec des réglementations différentes par canal (figure 3.5).

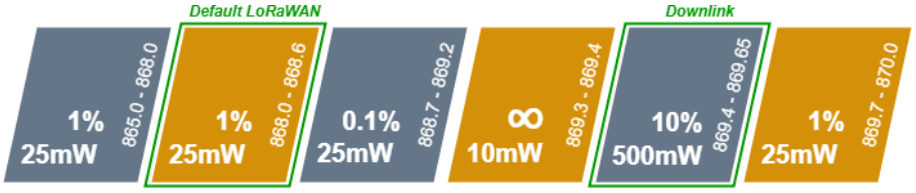


FIGURE 3.5 – Le découpage de la bande de fréquences publiques européennes 868 MHz - [Ism17].

Le premier canal 865-688 MHz et le dernier canal 869,7-870 MHz sont des zones non utilisées par défaut par le protocole LoRaWAN, mais elles peuvent être étendues pour des canaux LoRa.

Le second canal est utilisé par défaut dans le protocole LoRaWan. C'est sur cette bande de fréquences que se trouvent les 3 sous-canaux LoRaWan standardisés de 125 kHz chacun. C'est sur la largeur de ces sous-bandes que sera utilisé l'étalement de spectre lors de la communication radio.

Le troisième canal 868,7-869,2 MHz est une zone dans laquelle le coefficient d'utilisation est de 0,1%. Cette zone est intéressante lorsqu'un objet émet très peu par jour : le risque de collision est réellement plus faible et la fiabilité de communication est accrue. Ainsi cette sous-bande est intéressante pour espérer conserver l'énergie disponible ou pour communiquer un message prioritaire.

La quatrième sous-bande 869,3-869,4 MHz n'est pas utilisable pour LPWAN longue portée car la puissance maximale est seulement de 10 mW, mais sans *duty cycle* c'est une bonne zone pour la communication d'objets locaux sans limitation de message.

Le canal 869,4-869,65 MHz est particulièrement intéressant car vous pouvez communiquer avec 500mW et un *duty cycle* de 10%. Un objet ne serait pas capable d'utiliser une telle puissance lorsqu'il fonctionne sur batterie, mais du point de vue du réseau central, c'est un très bon canal pour les communications descendantes. Le fait d'avoir une plus grande puissance permet de maximiser les chances au *device* de recevoir un message de la passerelle, l'antenne de celui-ci étant moins performante que celle de la passerelle pour intercepter le signal.

3.2.2/ LES RÉSEAUX LPWAN

Les réseaux LPWAN [Dal18] [Ikp19] ouvrent la voie aux nouvelles technologies sans fil (ondes radio) conçues spécifiquement pour les applications IoT bas débit. Les deux enjeux majeurs sont :

1. Une communication très longue portée : elle couvre plusieurs dizaines de kilomètres

1. European Conference of Postal and Telecommunications Administrations
2. Autorité de régulation des communications électroniques et des postes

quand un réseau GSM est de l'ordre de 1 à 2 kilomètres et offre une couverture large pour un faible coût de réseau. Pour cela Les LPWANs utilisent principalement une bande de fréquences dite Sub-1GHz (juste en dessous de 1 GHz) leur permettant d'atteindre des récepteurs plus éloignés. L'équation de Friis montre la relation entre la distance séparant deux antennes et la fréquence :

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2 \tag{1}$$

Où :

- P_t est la puissance en watts (W) délivrée à l'antenne d'émission,
- P_r est la puissance en watts (W) collectée sur l'antenne de réception,
- G_t est le gain linéaire de l'antenne d'émission,
- G_r est le gain linéaire de l'antenne de réception,
- R est la distance en mètres (m) séparant les deux antennes,
- λ est la longueur d'onde en mètres (m) correspondant à la fréquence de travail.

De plus, les signaux sont moins atténués par des obstacles comme le béton (le *multi-path fading* est moins important). En outre, les débits de données (*data rate*) sont très faibles ce qui permet de transmettre chaque bit avec une énergie plus importante et ainsi de réduire considérablement la sensibilité des récepteurs à -130 dBm (1000 fois moins que les réseaux faible portée).

2. Une consommation d'énergie très faible : facteur 10 par rapport à la Wifi ou la 3G. Avec la possibilité de veille prolongée (mode non connecté). L'utilisation des fréquences Sub-1GHz nécessite moins de puissance d'émission (et donc moins d'énergie) pour atteindre un récepteur (une antenne) dans les mêmes conditions de réception qu'avec des fréquences plus élevées.

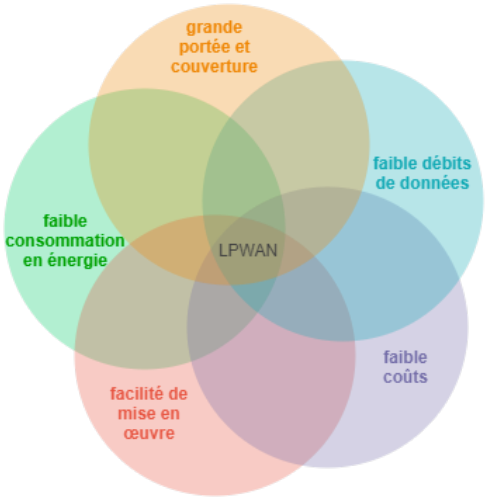


FIGURE 3.6 – Les caractéristiques des réseaux LPWAN.

Mais d'autres caractéristiques induites viennent s'ajouter : la faible consommation d'énergie entraîne inévitablement des faibles débits de données. Mais également, les coûts d'utilisation peu élevés sont un prérequis pour une utilisation massive, et avec une facilité de déploiement des opérateurs via la longue portée des LPWANs. La figure 3.6 montre les caractéristiques qui constituent les LPWANs.

Bien que la connectivité dans l'IoT ait été dominée par les technologies à courte portée pendant de nombreuses années, une étude [Dri17] prévoit que d'ici 2025, 25% des connexions IoT industrielles sans fil seront équipées de technologies LPWAN.

Le marché des LPWANs est fragmenté en de nombreuses technologies d'accès et de solutions. Les solutions d'accès les plus connues sont LoRa, Sigfox, LTE-M ainsi que NB-IoT. Mais, il en existe de nombreuses autres telles que Ingenu ou encore WavIoT. Le résultat est que, malgré le potentiel de l'IoT, les organisations et les utilisateurs finaux sont confrontés à des choix complexes.

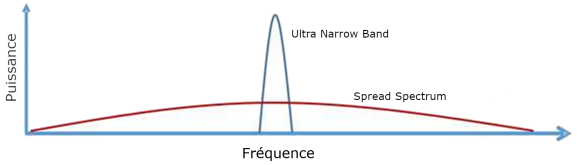


FIGURE 3.7 – L'utilisation du spectre de fréquences par les LPWANs - [Emb14].

Il n'existe que peu d'études comparatives car les technologies sont parfois très différentes, et bon nombre des technologies de pointe reposent sur des protocoles propriétaires dont les spécifications détaillées ne sont pas librement disponibles dans le domaine public [Ikp19]. Par exemple, certaines technologies comme Sigfox ou NB-IoT utilisent les technologies *Narrow Band* et *Ultra Narrow Band* qui consistent à minimiser la plage de fréquences lors de l'envoi d'un message pour "surpasser" les collisions éventuelles comme le montre la figure 3.7 [Emb14].

Au contraire LoRa et Ingenu utilisent la technologie *Spread Spectrum* qui consiste à étaler le signal sur une grande plage de fréquences afin de "contourner" les éventuelles collisions. D'autres technologies possèdent différentes variantes de propriétés sur les couches physiques ou MAC. Par conséquent, aucune pile de protocole LPWAN grand public n'est actuellement entièrement ouverte.

L'ensemble des LPWANs ont le point commun d'utiliser les mêmes acteurs lors des échanges de messages [Lpw17] (figure 3.8) :

- des nœuds terminaux (*end devices*), les capteurs et les actionneurs. Ce sont nos objets connectés de santé par exemple.
- une ou plusieurs passerelles distantes (appelées souvent stations de base ou *gateways*). Ce sont les antennes disposées pour couvrir une zone ou un territoire.
- un cœur de réseau (ou *backend server*) pour traiter les messages qui arrivent des antennes. Il gère l'identification des nœuds (les objets connectés), la sécurité, la duplication de données (lorsque plusieurs antennes captent le même message) ou encore l'envoi de messages descendant vers les objets. Les transmissions descendantes (*downlink* ou DL) sont utilisées, par exemple, pour signifier à l'objet qu'une mesure a bien

FIGURE 3.8 – Les différents acteurs des réseaux LPWAN.

été reçue (acquittement), pour envoyer des informations de reconfiguration, ou pour transmettre une commande quand l'objet est un actionneur.

- des serveurs de données propres aux applications, comme par exemple les serveurs de télémédecine qui stockent les dossiers médicaux des patients suivis et offrent les services de télésurveillance. Les données transitent du cœur de réseau vers les serveurs applicatifs généralement par des requêtes Http sur Internet.

Il est possible de classer les LPWANs en deux catégories :

1. Les réseaux qui évoluent sur des bandes de fréquences ISM sans licence, dites libres, permettant un déploiement à coût réduit et l'arrivée de nouveaux opérateurs sur le marché comme Sigfox, LoRaWAN, Ingenu, Telensa, IEEE 802.15.4k, IEEE 802.15.4g, Weightless-W / Weightless-N / Weightless-P ou encore DASH7.
2. Les réseaux utilisant des bandes licenciées correspondant aux réseaux cellulaires pour l'IoT comme LTE-M, NB-IoT ou EC-GSM-IoT.

3.2.3/ LES LPWANS SUR LES BANDES DE FRÉQUENCES SANS LICENCE

L'utilisation des bandes de fréquences sans licence a vu émerger de nombreuses technologies de LPWAN plus ou moins ressemblantes. Cependant, en France, seules les technologies Sigfox et LoRaWAN se sont démarquées aujourd'hui avec un déploiement significatif par les opérateurs.

3.2.3.1/ LORAWAN

LoRaWAN (*Long Range Wide-Area Network*) est un protocole de télécommunication permettant la communication à bas débit, par radio, d'objets à faible consommation électrique communiquant selon la technologie LoRa. C'est une alternative rentable et moins coûteuse en énergie aux réseaux cellulaires pour transmettre de très petites quantités de données. Le protocole met en relation des objets à faible consommation électrique et des passerelles distantes reliées à l'Internet, participant ainsi à l'Internet des Objets.

La technologie LoRa

Le protocole LoRaWAN utilise une modulation à étalement de spectre de type *Chirp spread spectrum* propriétaire appelée LoRa. LoRa, pour *Long Range*, est le nom donné à la couche physique radiofréquence. Le protocole de type *Chirp* a été développé pour les applications sonar et radar au cours de la 2ème guerre mondiale et utilise une modulation de fréquence à amplitude fixe. Cette modulation s'effectue sur les bandes radios ISM 868 MHz en Europe et 915 MHz en Amérique du Nord et permet une distance entre une passerelle et un équipement jusqu'à 5 km en zone urbaine et 15 km en zone rurale.

Par défaut le fonctionnement repose sur le type *ALOHA*. L'équipement envoie des données sans contrôler si le canal qu'il utilise est disponible. Il retransmet le message après un temps aléatoire s'il a été perdu. Bien que plusieurs transmissions LoRa émises simultanément puissent être traitées par une seule passerelle distante (antenne), la nature de l'accès au support ALOHA entraîne inévitablement la présence de collisions de transmission et donc de perte de messages. Une procédure d'écoute avant transmission LBT (*Listen Before Talk*) peut être utilisée au préalable, garantissant un RSSI (*Received Signal Strength Indication*) mesuré inférieur à 90 dBm avant n'importe quelle transmission de données, ce qui permet de réduire les collisions.

La nature du protocole *ALOHA* entraîne également le fait que les nœuds ne sont pas associés à une passerelle spécifique. Les données transmises peuvent être reçues par plusieurs passerelles (antenne). Chaque passerelle transmet le paquet reçu au serveur de réseau qui se chargera de filtrer les paquets en double. Ainsi, si un nœud est mobile ou en mouvement, aucun transfert (ou nouvelle connexion) n'est nécessaire pour passer d'une passerelle à une autre.

LoRaWan se base, par ailleurs, sur le protocole nommé *LoRaMAC* qui définit l'interaction entre les nœuds et les passerelles distantes. Ce protocole propose plusieurs mécanismes intéressants comme la synchronisation temporelle des nœuds, une gestion de clés d'identification du nœud ainsi qu'une gestion d'adaptation des paramètres de transmission.

Les différentes classes d'utilisation

Les envois de données avec la technologie LoRa consomment peu d'énergie. Cependant l'économie d'énergie la plus importante est réalisée entre les envois : ce réseau gère un mode asynchrone, c'est-à-dire que l'équipement peut passer en veille entre deux envois et ne plus être en écoute permanente. Suivant ce principe de veille, le protocole *LoRaWAN* propose plusieurs types de fonctionnement sous le nom de classes (A, B, et C). Avec la classe A, l'équipement peut envoyer des données à volonté mais le réseau ne peut lui envoyer des données que dans une courte fenêtre après la liaison montante. À l'opposé pour la classe C, plus gourmande en énergie, l'équipement est toujours en écoute. La classe B est située entre les deux classes précédentes : l'équipement ouvre des fenêtres de réception périodiquement.

L'équipement peut donc se réveiller à intervalles réguliers pour envoyer des données. À ce moment, il pourra alors rester en écoute quelques secondes pour attendre, soit un message de confirmation de réception, soit la réception d'un message descendant. L'attente, après l'envoi d'un message montant, est appelée *fenêtre de réception*.

Les messages descendants permettent de communiquer dans l'autre sens, c'est-à-dire de la passerelle distante vers la passerelle locale. Il sont donc envoyés par les passerelles distantes,

soit à tout moment dans le cas d'un objet en classe C, soit après la réception d'un message montant en classe A et B. Les messages descendants sont gérés et stockés en attente d'envoi par le serveur *backend*.

L'étalement de spectre LoRa

L'étalement du spectre est une technique consistant à étaler le message transmis sur une grande largeur de bande, en répétant le signal de nombreuse fois. LoRa utilise alors une très grande bande passante pour fonctionner avec un signal faible ou avec beaucoup de bruit. LoRa utilise trois largeurs de bande : 125 kHz, 250 kHz et 500 kHz. Le facteur d'étalement (*Spreading Factor*, SF), défini entre 7 et 12, représente de manière simplifiée la durée du *chirp*.

La relation entre le débit de données et le débit du chirp dans la technologie de modulation LoRa est définie ainsi :

$$\text{Le débit binaire de modulation LoRa } R_b = SF * [\frac{1}{[\frac{2^{SF}}{BW}]}] bits/s \quad (2)$$

Où :

- SF est le facteur d'étalement,
- et BW est la largeur de bande de modulation (Hz).

Le débit de données R_b est donc directement proportionnel au facteur d'étalement SF.

Avec l'utilisation d'un facteur d'étalement plus élevé, il faut alors plus de temps pour envoyer la même quantité de données : cela implique une augmentation du temps d'émission (*Time On Air, ToA*).

Par ailleurs, l'utilisation d'un plus grand facteur d'étalement augmente la période de modulation, ce qui permet d'augmenter la portée, au détriment du débit de données (bande passante) qui sera alors réduit. Par conséquent une communication plus longue implique une consommation d'énergie plus importante et donc une autonomie réduite des devises.

Dans ce contexte, l'algorithme ADR (*Adapative Data Rate*) est un mécanisme adaptatif dont le principal objectif est d'économiser de l'énergie.

L'algorithme ADR

Cet algorithme est important et sera une base pour une part de nos travaux.

L'algorithme ADR est un mécanisme d'optimisation du débit ou de la puissance d'émission permettant, entre autres, d'économiser de l'énergie, de gagner en temps de transmission et de réduire les interférences [Sem16] [Voj17]. Il est basé sur le fait que LoRaWAN permet aux objets de modifier individuellement les paramètres de transmission, le facteur d'étalement ou la puissance d'émission. Ainsi, l'algorithme ADR permet de déterminer, par l'intermédiaire d'un historique, les paramètres minimaux de communication entre le périphérique et la passerelle. L'ADR peut être activé lorsqu'un terminal dispose de conditions radiofréquence RF suffisamment stables, et donc généralement pour des périphériques statiques.

En revanche, l'algorithme ADR ne peut pas être utilisé dans des systèmes continuellement en mouvement. Plus la mobilité est rapide, plus l'efficacité de l'ADR diminue [Kon19]. Il se révèle inefficace et peut même être un facteur de surconsommation d'énergie important, tout en dégradant la fiabilité des transmissions. L'ADR ne doit pas non plus être activé si les trafics sont saturés, car les nœuds vont modifier leur SF et saturer encore davantage le réseau (goulot d'étranglement) [Hax19].

Lorsque le mode débit de données adaptatif de l'appareil est activé, le débit de données utilisé est dicté par le serveur via une commande MAC ADR dédiée, documentée dans les spécifications LoRaWAN.

La bande de fréquence 868 MHz disponible pour l'Union Européenne est en fait définie de 863 MHz à 870 MHz. Sur cette bande, 8 débits de données (DR) sont définis par la spécification des paramètres régionaux LoRaWAN (RPS) [Lor16]. Les valeurs des débits de données de 0 à 5 correspondent à la modulation LoRa avec des SF 12 à 7 respectivement, en utilisant une bande passante de 125 kHz. Les autres DR ne sont pas utilisés dans l'algorithme ADR. Ils utilisent une bande passante plus large comme DR6 ou ne ne peuvent tout simplement pas être pris en charge dans ADR (DR 7). Le tableau 3.9 des DR est défini ci-dessous. Plus le DR sera grand, plus un *Spreading Factor* petit sera utilisé, ce qui entraînera une diminution de la portée, mais une augmentation du débit physique. Par conséquent, le temps de communication sera réduit, et la consommation en énergie réduite également. Par ailleurs, la portée étant moins grande, le risque d'interférence sera réduit.

DR	Type	SF	Bande	Débit physique
0	LoRa	SF12	125 kHz	250 bit/s
1	LoRa	SF11	125 kHz	440 bit/s
2	LoRa	SF10	125 kHz	980 bit/s
3	LoRa	SF9	125 kHz	1 760 bit/s
4	LoRa	SF8	125 kHz	3 125 bit/s
5	LoRa	SF7	125 kHz	5 470 bit/s
6	LoRa	SF7	250 kHz	11 000 bit/s
7	FSCK	50kbits/s		50 000 bit/s

FIGURE 3.9 – Définition des Data Rate DR pour LoRaWAN sur la bande 868 MHz.

De plus, le RPS (*Regional Parameters specification*) définit 6 niveaux de puissance de sortie (TX) 0 à 5 correspondant respectivement à 20 dBm, 14 dBm, 11 dBm, 8 dBm, 5 dBm et 2 dBm. Pour se conformer à la réglementation [Erc17] l'ADR se limite aux puissances d'émission 1 à 5. Naturellement, plus la puissance de sortie *TX* est élevée, plus la consommation en énergie sera importante.

Le tableau 3.10 résume ce qu'implique une modification du DR sur la portée, le débit et la consommation énergétique (en utilisant toujours une même bande de fréquence, en l'occurrence ici 125 kHz).

Faible DR	Fort DR
+ spreading factor	- spreading factor
+ portée	- portée
- débit physique	+ débit physique
+ temps de communication	- temps de communication
+ consommation d'énergie	- consommation d'énergie

FIGURE 3.10 – Implication du DR dans la consommation d'énergie

Ainsi le principe de l'algorithme ADR 3.11 est l'ajustement du DR et du TX afin d'optimiser l'économie d'énergie et de causer moins d'interférences [Voj17]. La baisse de la puissance d'émission TX n'apporte pas forcément un gain énergétique pour le endpoint (tableau 3.2), mais lui permet surtout une diminution des nuisances envers

les nœuds voisins en cas de transmission simultanée sur le même canal. Pour ajuster ces paramètres, l'algorithme a besoin d'enregistrer les 20 liaisons montantes les plus récentes. Ces mesures contiennent le compteur de trames, le rapport signal sur bruit (*SNR*) et le nombre de passerelles ayant reçu chaque liaison montante. Pour chacune de ces mesures, nous prenons le SNR de la meilleure passerelle et calculons la «marge». Celle-ci est la différence entre le SNR mesuré et le SNR requis pour extraire un message en fonction du débit de données. Cette marge sert à déterminer dans quelle mesure le débit de données peut être augmenté et si la puissance de transmission peut être augmentée ou réduite [Sem16]. L'algorithme ne diminuera en revanche jamais le DR car cela pourrait avoir un effet domino sur le réseau dans le cas de saturation [Hax19]. L'algorithme présentée ici est tiré du réseau communautaire « The Things Network ». La version de ADR « Chirpstack » prend en compte également le nombre de retransmission du message (qui peut varier de 1 à 15 dans la spécification).

```
1:  i ← 0
2:  history[j] ← 0 for ∀j ∈ [0, 19]
3:  offset = 10
4:  threshold = {−20.0, −17.5, −15.0, −12.5, −10.0, −7.5}
5:  DR ← −1, TX ← 1
6:
7:  function RECEIVEPACKET(mSNR, mDR)
8:      if DR = −1 then
9:          DR ← mDR
10:     end if
11:
12:     history[i] ← mSNR
13:     i ← i + 1
14:
15:     if i = 20 then
16:         ADJUSTADR
17:         i ← 0
18:     end if
19: end function
20:
21: function ADJUSTADR
22:     margin ← max(history) − threshold[DR] − offset
23:     steps ← round(margin/3)
24:
25:     if steps > 0 then
26:         increase DR by steps until DR = 5
27:         decrease TX by remaining steps until TX = 0
28:     else if steps < 0 then
29:         increase TX by steps until TX = 5
30:     end if
31: end function
```

FIGURE 3.11 – Algorithme ADR classique.

Par ailleurs, les périphériques doivent mettre en œuvre une décroissance automatique du débit de données. En cas de déconnexion du réseau, ils augmenteront leur puissance d'émission TX puis réduiront leur débit de données DR pas à pas, jusqu'à ce qu'ils soient reconnectés.

En revanche, l'algorithme ADR ne peut pas être utilisé dans des systèmes continuellement

en mouvement. Plus la mobilité est rapide, plus l'efficacité de l'ADR diminue [Kon19]. Il peut donc être un facteur de surconsommation d'énergie important, tout en dégradant la fiabilité des transmissions. La raison est qu'un environnement instable ne permet pas de calculer les paramètres de communication optimaux (DR et TX) car les conditions sont très variables, et l'algorithme ADR ne gère pas les prédictions de déplacement. Il ne permet pas toujours de prendre en compte la dégradation du signal due à la mobilité des nœuds ou à la présence d'obstacles mobiles. De plus, la technologie LoRaWAN n'est pas adaptée aux flux de données continus en raison de sa conception et de la limitation du rapport cyclique (*duty cycle*) sur sa bande de fréquences ISM 868 MHz (au maximum entre 6 et 20 messages/heure environ suivant le *Time On Air, TOA*).

L'algorithme ADR ne permet pas une modification rapide des paramètres optimaux, car il se fait de manière incrémentale jusqu'à ce que la communication soit rétablie, en utilisant un historique des derniers messages. Si les nouvelles conditions environnementales sont très différentes des précédentes, cela peut prendre beaucoup de temps : par exemple, après un changement environnemental et un temps de 10 minutes entre chaque message envoyé, les paramètres seraient, à nouveau, optimaux après 20 nouveaux messages, soit plus de 3 heures. L'adaptation des paramètres de communication est donc trop lente et il ne peut pas être utilisé lors d'un déplacement.

Sur cette problématique, Benkahla et al. ont proposé l'algorithme E-ADR [Ben19]. Il est basé sur une estimation de la trajectoire d'un appareil mobile et de sa position lors du prochain envoi de paquet. L'objectif est de réduire la consommation d'énergie, le temps d'occupation du canal et le taux de perte, dû au temps d'adaptation de ADR ainsi qu'à la limitation du *duty cycle*. E-ADR utilise la méthode de trilatération avec un paquet LoRa pour géolocaliser le dispositif. Le serveur estimera la position prédictive de celui-ci et calculera le RSSI (*Received Signal Strength Indication*) afin d'attribuer, en fonction d'un tableau de correspondance, un ensemble de paramètres de communication à utiliser. L'estimation de la position dans ce contexte doit être très précise, et nécessite d'utiliser un réseau personnel local, à l'échelle d'une habitation par exemple.

La géolocalisation avec LoRaWAN

Il existe plusieurs techniques permettant d'estimer la position d'un appareil. Chacune de ces techniques présente des caractéristiques et des prérequis différents. Les trois méthodes les plus couramment utilisées pour réaliser la géolocalisation sont la triangulation, la trilatération et la multilatération. Il est important, lors de l'utilisation de la géolocalisation, de sélectionner celle qui convient le mieux en fonction des besoins et des conditions d'utilisation :

- La triangulation utilise les angles d'incidence des signaux reçus par au moins deux stations de réception. La position de l'objet est alors estimée en prenant la positions des deux antennes, les angles d'incidence et en appliquant une formule trigonométrique.
- La trilatération n'utilise pas d'angles pour positionner un point. Cette méthode est basée sur la distance entre l'émetteur et le récepteur, qui peut être obtenue à partir de l'heure d'arrivée (TOA), l'heure d'envoi (TOF) et la vitesse de propagation des ondes. Par conséquent, il est nécessaire d'avoir une synchronisation entre l'émetteur et le récepteur. Un cercle de rayon égal à la distance calculée pourra alors être tracé

sur chaque antenne réceptrice. La position de l'objet sera alors définie par l'intersection des trois cercles. Par conséquent, il sera nécessaire qu'au moins trois antennes reçoivent le signal.

- La multilatération est assez similaire à la trilatération. Cependant, la principale caractéristique permettant de calculer l'emplacement est la différence d'heure d'arrivée (TDOA). Les émetteurs sont synchronisés entre eux, alors que le récepteur n'a pas besoin de l'être.

Les objets connectés indépendants sur batterie qui utilisent la technologie LoRaWAN ne peuvent pas être synchronisés avec les stations distantes. En revanche, ces stations peuvent quant à elles être synchronisées entre elles, qu'elles soient déployées par un particulier ou par un opérateur de télécommunications. La seule information connue sera donc l'heure de réception des signaux qu'il sera possible d'utiliser dans l'algorithme de multilatération pour positionner un objet.

Le modèle de la consommation énergétique

Pour toutes ces explications, nous avons choisi de conserver les termes anglo saxon sans traduction systématique de ces termes très compréhensibles.

Afin de calculer l'énergie consommée lors d'un envoi d'un paquet [Bou19], nous devons tout d'abord calculer le *Time On Air* (en ms), T_{Packet}, il est représenté sous la somme du *preamble duration* et du *payload duration* :

$$T_{Packet} = T_{Preamble} + T_{Payload} \tag{3}$$

Le *preamble duration* $T_{Preamble}$ est sous la forme :

$$T_{Preamble} = (4.25 + NP) * T_{Symbol} \tag{4}$$

Où :

- NP est le *preamble symbol number*,
- et T_{Symbol} est le *symbol period*.

Le *payload duration* $T_{Payload}$ est de la forme :

$$T_{Payload} = N_{Payload} * T_{Symbol} \tag{5}$$

Où :

- $N_{Payload}$ est le *number of symbols*,
- et T_{Symbol} est le *symbol period*.

Le *symbol period* T_{Symbol} est sous la forme :

$$T_{Symbol} = \frac{2^{SF}}{BW} \tag{6}$$

Où :

- *BW* est la bande passante (125kHz ou 250kHz en Europe),
- et *SF* le *Spreading Factor*.

Le *payload symbol* (nombre de symboles qui composent la charge utile et l'en-tête du paquet) est calculé par l'équation :

$$N_{Payload} = 8 + max\left(ceil\left(\frac{\Theta(PL,SF)}{\Gamma(SF)}\right) * \frac{1}{CR}, 0\right) \tag{7}$$

Où :

- *ceil* représente la fonction de *ceiling* (arrondi supérieur),
- PL est le *payload size* (in bytes),
- $\Theta(PL,SF) = 8PL - 4SF + 16 + 28 - 20H$, avec $H = 1$ si le header est activé, et $H = 0$ s'il n'est pas présent,
- $\Gamma(SF) = SF - 2DE$, avec $DE = 1$ si le *low data rate optimization* est activé et $DE = 0$ sinon. Le *coding rate* est modélisé sous la forme $CR = [\frac{4}{4+n}]$ avec n entre 1 et 4, qui représente respectivement les 5, 6, 7 ou 8 bits utilisés pour l'encodage.

Nous pouvons ensuite calculer l'énergie consommée par envoi (en μJ) avec l'équation suivante :

$$E_{Cons} = P_{Cons}(P_T) * T_{Packet} \tag{8}$$

Où :

- $P_{Cons}(P_{Tr})$ est la puissance totale consommée qui dépend de la puissance de transmission,
- et T_{Packet} est le *time on air*.

La puissance totale consommée est calculée par l'équation suivante :

$$P_{Cons}(P_{Tr}) = Tr_{Tx} * SV \tag{9}$$

Où :

- Tr_{Tx} est l'intensité de transmission en fonction de la puissance d'envoi TX (en mA),
- et *SV* le *supply power* (généralement 3,3 V pour les puce SX1272 et SX1276).

Un outil *Semtech* est également disponible pour calculer le *time on air* et la consommation pour les puces LoRa SX1272 et SX1276 [Sem15]. Cet outil nous permet de définir le tableau 3.2 pour la puce SX1276 que nous utilisons et ainsi nous permet de calculer la puissance totale consommée $P_{Cons}(P_{Tr})$ en fonction de TX.

Transmission Power TX (dBm)	2	5	8	11	14	20
Intensity (mA)	24	25	25	32	44	125

TABLE 3.2 – Consommation d'énergie en fonction de la puissance de transmission TX.

Le déploiement de LoRaWAN

Depuis 2017, de nombreux déploiements de réseaux ont été réalisés un peu partout dans le monde dans le but de couvrir un territoire à l'échelle d'un pays ou d'une ville. En France, c'est l'opérateur ***Objenious***, filiale de Bouygues Télécom, qui a fait le premier pas, suivi d'Orange. Ce premier se targue de couvrir 95% de la population française et 86% de la surface en extérieur. Il propose, par ailleurs, un abonnement par défaut à 20 euros par capteur par an, ainsi qu'une plateforme *backend* pour la gestion des objets et la redirection vers des serveurs tiers.

Par ailleurs, un réseau communautaire open source interpays nommé *The Things Network* a vu le jour. Il est basé entièrement sur les passerelles que les particuliers déploient chez eux. Il est possible d'y accéder librement en respectant les contraintes des bandes ISM, mais également d'y contribuer avec de nouvelles passerelles. Il est largement présent sur les pays d'Europe à forte densité de population comme le Danemark, les Pays-Bas et la Belgique, mais également dans les grandes villes comme Paris et Londres. En revanche il n'est quasiment pas disponible sur le territoire français.

3.2.3.2/ SIGFOX

Sigfox [Fou20] [Sig17] est à la fois le nom de la technologie, du réseau et de l'opérateur mondial. Il a été créé en 2009 à Labège, commune de la banlieue toulousaine en France. L'entreprise a procédé à des levées de fonds entre 2012 et 2016 à hauteur de 275 millions d'euros. Cela lui a permis d'investir sur ses propres solutions et ainsi d'accélérer son développement afin de devenir un opérateur mondial indépendant. La startup pourrait bien rejoindre le cercle fermé des licornes avec une valorisation d'1 milliard de dollars ou plus, comme BlaBlaCar, Dataiku, OVH et Doctolib...

Des antennes Sigfox sont disposées dans 48 pays, comme les États Unis, le Brésil, l'Australie, et une grande partie de l'Europe (figure 3.12). Aujourd'hui, plusieurs millions d'objets connectés utilisent ce réseau comme :

- Des puces pour tracer les colis,
- Des détecteurs d'intrusion dans les maisons,
- Des puces pour gérer panneaux publicitaires.

Sigfox déploie et exploite le réseau mais fournit librement la spécification du protocole aux fabricants de puces. Il utilise la technologie *Ultra Narrow Band* pour communiquer sur de longues distances sans être affecté par le bruit.

La technologie *Ultra Narrow Band*

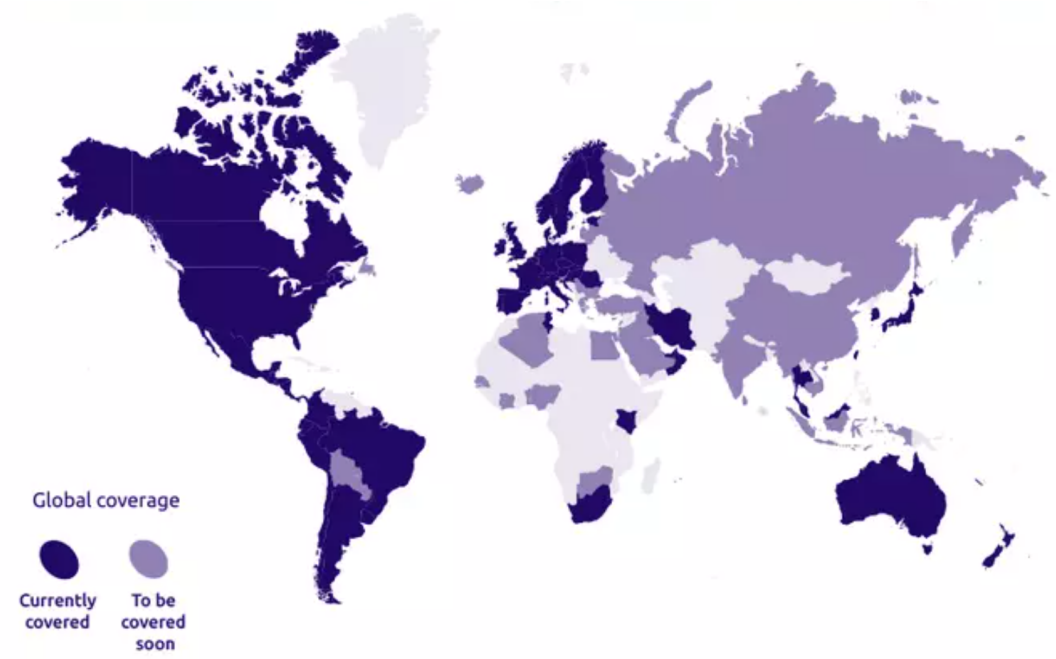


FIGURE 3.12 – Couverture Sigfox mondiale - [Sig19].

Sigfox utilise la technologie d'émission à bande ultra étroite UNB (*Ultra Narrow Band*) sur les bandes de fréquences ISM [Lav19]. L'avantage d'une telle approche est que le niveau de bruit présent dans un canal de communication à bande étroite est minime. En conséquence, la technologie UNB permet d'obtenir une portée de transmission très large, jusqu'à 50km.

La modulation utilisée par le protocole est DBPSK (*Differential Binary Phase Shift-Keying*) [Srp17]. C'est la forme la plus simple du PSK (*Phase-Shift Keying*) avec deux phases possibles d'onde : les bytes 0 ou 1 sont représentés par une onde montante ou descendante. Bien que ce type de modulation soit robuste, une déformation du signal, par exemple lors d'interférences, peut inverser les symboles. La meilleure façon de fiabiliser l'onde est donc de répéter le signal sur une même phase plusieurs fois pour chaque byte. Par exemple, avec un débit de 100 bytes par seconde, chaque byte est envoyé sur une période de 10 ms. Sur cette période, la même phase sera répétée 8.6 millions de fois. L'émetteur choisira ensuite la phase la plus probable entre 0 et 1. Pour effectuer ce découpage, une synchronisation est nécessaire en début de communication. Elle est réalisée grâce à une émission alternativement de 0 et 1 permettant au récepteur de synchroniser son horloge et ainsi de connaître le début de chaque byte.

La bande utilisée est différente suivant les zones géographiques :

- entre 868 et 868,2 MHz dans les pays suivants les normes ETSI [1],
- entre 902 et 928 MHz dans le reste du monde, notamment la zone FCC [2], avec des restrictions applicables selon la réglementation locale.

La taille d'un canal lors de l'envoi d'un message est de 100 Hz en zones ETSI (Europe) ou

1. The European Telecommunications Standards Institute
2. Federal Communications Commission : agence indépendante du gouvernement des États-Unis

de 600 Hz en zones FCC (Amérique du nord) dont le débit est respectivement 100 et 600 bits par seconde.

Le principal avantage de la technologie est, par sa résistance aux interférences et aux collisions, rendue possible par la mise en œuvre d'un mécanisme de « diversité temporelle et fréquentielle ». Ainsi la transmission n'est pas synchronisée entre l'objet et le réseau, mais les capteurs envoient les paquets de données sur trois canaux de communication différents de manière pseudo-aléatoire dans le temps sans vérifier l'occupation du canal (figure 3.13).

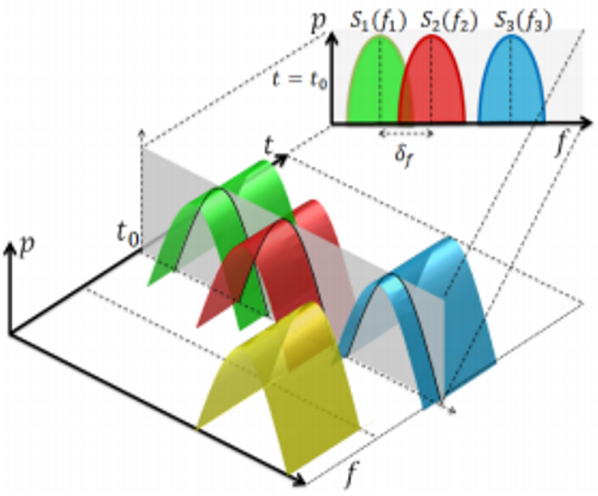


FIGURE 3.13 – Accès multiple au canal par répartition aléatoire de fréquence et de temps - [Min15].

L'accès multiple au canal par répartition aléatoire de fréquences et de temps se nomme *Random-FTDMA*. Son utilisation [Min15] se justifie notamment par :

- l'impossibilité pour le transmetteur d'avoir une précision inférieure à 400 Hz dans le choix de la fréquence, dépassant ainsi la largeur de la bande UNB.
- la suppression de la charge de trafic nécessaire pour la synchronisation et la gestion du réseau réduit le coût et la complexité des transmetteurs.

Lors de chaque communication, l'objet envoie le message puis deux répliques successives sur des fréquences aléatoires différentes. Ce message sera reçu par n'importe quelle station de base à proximité (on parle de diversité spatiale).

Le chevauchement avec le bruit est très faible dans la modulation UNB. Le signal doit être au moins 8 dB supérieur au bruit de fond pour être reçu par la passerelle (figure 3.14) [Sto17].

Lavric et al. [Lav19] ont montré que le niveau de performance du réseau Sigfox est relativement élevé mais très dépendant de la densité du réseau. Pour garantir un haut niveau de performance, avec un PER [1] inférieur à 10%, le nombre le plus élevé de capteurs pouvant communiquer simultanément est d'environ 1100, lorsque les 1920 canaux de Sigfox sont disponibles. Au-delà de ce nombre, un effet d'avalanche se déclenche qui détermine la baisse drastique du niveau de performance. En ce qui concerne Sigfox [Sig17], pour assurer

1. Packet Error Rate

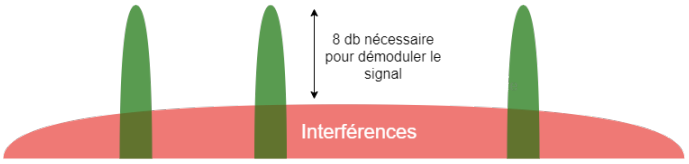


FIGURE 3.14 – Résistance aux interférences [Sto17].

une qualité de service à 99,99%, la charge du réseau ne doit pas dépasser les 270 objets en parallèle sur la même station de base.

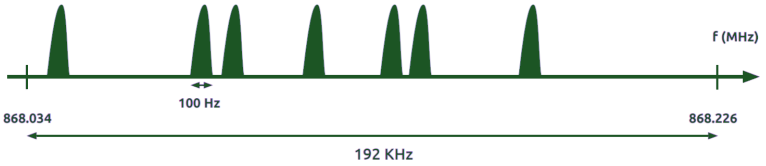


FIGURE 3.15 – UNB sur la bande de fréquence 868 MHz (zone ETSI) [Sto17].

La figure 3.15 représente le choix du canal pseudo-aléatoire sur la bande de fréquence 868 MHz. Le spectre complet de 192 kHz est surveillé en permanence par les stations de base Sigfox afin de rechercher les signaux UNB à démoduler.

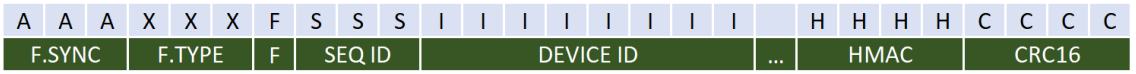
Les trames Sigfox

Le protocole Sigfox est uniquement conçu pour des transferts de très petites données. La charge utile (*payload*) des messages montants (*uplink*) est comprise entre 0 et 12 octets [Srp17]. À titre de comparaison, les coordonnées GPS avec une précision de 3m peuvent être codées sur 6 octets, soit la moitié de la taille maximale. Il est possible de gagner en temps de communication en réduisant la taille de la charge utile des messages (4, 8 ou 10 octets). Cependant, cette charge utile ne prend que peu de place par rapport à la trame entière, et le gain est minime (environ 10% maximum).

Sigfox dispose d'une communication bi-directionnelle. Les messages descendants ont une charge utile fixe de 8 octets. Il sont déclenchés par l'envoi d'un message montant (comme la classe A de LoRaWAN) : une fois émis, l'objet se met en veille pendant 20 secondes, puis se réactive pendant 25 secondes afin de recevoir le message descendant envoyé par la passerelle. À une vitesse de 100 bps, l'envoi d'un message avec une charge utile de 12 octets nécessite 2.08 secondes. Le message étant répété deux fois ensuite, environ 6 secondes de *duty cycle* sont utilisés. Il est donc possible d'envoyer 6 messages par heure au maximum, soit 144 messages par jour. Sigfox n'a pas la responsabilité de jeter les messages en cas de dépassement du *duty cycle*. La limitation du canal destiné aux messages descendants, envoyés par la passerelle, est de 10%. Théoriquement, et en fonction de la densité du réseau, il est possible de recevoir plus de message. Sigfox ne garantit cependant que 4 messages descendants par objet et par jour.

Le protocole ne dispose pas de chiffrement par défaut sur la couche de données. C'est à l'utilisateur d'implémenter son propre mécanisme cryptographique s'il le souhaite. Il ne peut cependant pas utiliser de génération de clés à la volée comme LoRaWAN car aucun

appairage et aucune synchronisation entre l'objet et la station de base ne sont réalisés avant la transmission.



F.SYNC	Début de la tram AAA pour la synchronisation.
F.TYPE	Élément qui permet de déterminer laquelle des 3 trames de data possibles est utilisée.
F	Information précisant laquelle des 3 émissions de Sigfox est utilisée.
SEQ ID	Numéro de séquence : compteur de tram envoyés (jusqu'à 2048 envois puis repart à 0). Permet de détecter les problèmes.
DEVICE ID	Identifiant du device.
...	Données de la tram (payload).
HMAC	Signature de la trame pour vérifier l'intégrité. Clé privée à l'intérieur du device. Le hash de la trame est envoyé ici.
CRC16	Permet de s'assurer que toutes les bytes reçus sont bien corrects, pour éviter des erreurs pendant la transmission

FIGURE 3.16 – Trame Sigfox - [Srp17].

La sécurité est tout de même renforcée. La technologie assure l'authentification, l'intégrité et la non-réexécution des messages diffusés sur le réseau. En fonction du cas d'usage et de la sensibilité, le fabricant ou le fournisseur d'applications peut décider de stocker les données d'identification dans l'objet, une zone logicielle protégée ou un élément sécurisé. La composition des trames Sigfox est illustrée sur la figure 3.16.

Efficacité énergétique

Les puces électroniques Sigfox consomment de 10 à 50 mA en transmission, selon le partenaire et la puce utilisée. Par exemple, la consommation du module *AX-SIGFOX ON* est d'environ 19 mA pour une puissance de sortie de 0 dBm et 49 mA en sortie maximale de 14 dBm. Aux États-Unis, une puissance de 22 dBm est requise. Mais avec une durée d'émission six fois inférieure (débit de 600 bps), la durée de vie de la batterie est approximativement la même.

La consommation énergétique des objets utilisant la technologie Sigfox est faible grâce aux deux facteurs suivants :

- les objets passent la plupart de leur temps en veille (plus de 99%), avec une consommation négligeable (environ 6 nA),
- il n'y a pas de synchronisation entre les objets et les stations de base avant la communication.

Dans un scénario d'un envoi de 140 paquets par jour avec le module module *AX-SIGFOX ON* sur 14 dBm, un objet possédant une batterie de type 2xAAA (capacité de 1500mAh) peut fonctionner jusqu'à 6,5 ans [Lav19]. Au final, Sigfox offre un service relativement fonctionnel, fiable et qualitatif de façon simple et avec peu de paramètres.

3.2.4/ LES LPWANS : DES RÉSEAUX CELLULAIRES

Le 3GPP (*3rd Generation Partnership Project*) est l'organisation internationale en charge de la standardisation dans le secteur des télécommunications. Elle normalise les communications, ce qui permet l'interopérabilité, et permet à nos téléphones de fonctionner aussi bien dans notre pays que dans les autres pays (itinérance des communications). Le 3GPP a été chargé, par les opérateurs téléphoniques, de définir de nouveaux protocoles pour concurrencer LoRaWAN et Sigfox sur le marché des LPWANs. Il a donc établi différentes normes, avec notamment NB-IoT, LTE-M et EC-GSM-IoT.

EC-GSM-IoT est une extension aux réseaux 2G GPRS (utilisée historiquement dans la communication M2M - *Machine-to-Machine*). Cependant, de nombreux pays ont décidé d'arrêter la 2G afin de récupérer les bandes de fréquences. Cependant aucun opérateur Français ne le propose.

3.2.4.1/ NB-IOT

La norme *Narrow-Band IoT (NB-IoT)* a été introduite dans LTE (*Long Term Evolution*) Rel-13 (tout comme le LTE-M). Elle est basée sur des fréquences licenciées (fréquence 900-1800 en France) à la différence des bandes de fréquences ISM utilisées par la concurrence (Sigfox et LoRaWAN par exemple) [Rat16].

Le NB-IoT s'appuie sur les infrastructures de communication existantes des opérateurs téléphoniques et des équipementiers de réseaux pour couvrir de grands territoires et communiquer efficacement. Cependant le déploiement de NB-IoT est limité aux stations de base 4G et LTE. Il ne convient donc pas aux régions rurales qui n'ont pas de couverture 4G [Sin17].

Bien qu'il soit intégré dans la norme LTE, il est considéré comme une nouvelle interface radio. Son coût d'infrastructure est faible, le NB-IoT requiert seulement l'ajout de modems à faible coût pour les opérateurs (15000$ par station de base [Sin17]). Pour économiser de l'énergie, il supprime de nombreuses fonctionnalités du LTE comme la surveillance de la qualité du canal, l'agrégation de porteuses, la double connectivité...

Le NB-IoT tire son nom de la technologie à bande étroite (*Narrow-Band*) qu'il utilise afin de "surpasser" les collisions éventuelles. on parlera de PRB (*Physical Resource Block*) d'une largeur de 180 kHz, contenu dans un canal utilisé par NB-IoT de 200 kHz (comme Sigfox) [Lan16].

NB-IoT peut être déployé dans trois modes de fonctionnement différents illustrés sur la figure 3.17 :

1. être autonome des fréquences porteuse dédiée sur un des canaux de la bande de fréquences GSM,
2. se placer dans un canal, en réservant un ou plusieurs PRB, sur une bande large occupée LTE (GPRS). Dans cette région, les signaux NB-IoT ne doivent pas être transmis dans des ressources temps-fréquence réservées au LTE,
3. se placer entre les bandes LTE, dans les bandes d'arrêts d'urgence (ou bandes de garde). Ces dernières permettaient jusque-là d'éviter les collisions entre les différentes bandes LTE.

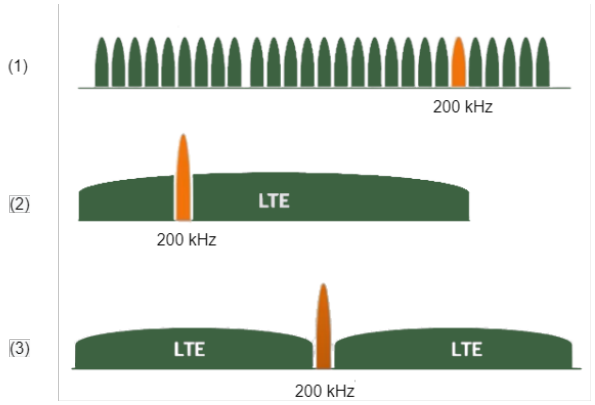


FIGURE 3.17 – Implémentation du NB-IoT dans les canaux GSM / GPRS existants - [Lan16].

NB-IoT utilise la modulation QPSK (*Quadrature Phase Shift Keying*) appelée également 4-PSK. C'est une modulation à 4 états (4 points, à équidistance autour d'un cercle). Avec ses quatre phases, QPSK peut coder deux bits par symbole. Cela a pour conséquence de multiplier le débit binaire par deux ou de réduire la bande passante utilisée par deux avec le même débit binaire (toutefois le taux d'erreurs par symbole augmente). Le débit de données théorique maximum est de 204.8 kb/s en liaison montante (*uplink*) en utilisant SC-FDMA (*Single-Carrier Frequency Division Multiple Access*) et 234.7 kb/s en liaison descendante (*downlink*) en utilisant OFDM (*Orthogonal Frequency-Division Multiplexing*). Cela représente environ 10 fois moins que le débit de données de LTE-M (avec une consommation moindre cependant), mais 10 à 100 fois plus que les LoRa et Sigfox. La latence pour NB-IoT est d'environ 1 à 7,6 secondes [Lan16].

Au contraire de LoRa, les objets utilisant NB-IoT ne peuvent pas se mettre en veille indéfiniment sans perdre la connectivité. Une synchronisation peu fréquente mais régulière est nécessaire, ce qui engendre une consommation supplémentaire d'énergie. Cela a pour conséquence un gain en robustesse des communications bidirectionnelles. Les technologies OFDM ou FDMA, utilisées par NB-IoT, nécessitent également plus de courant de crête pour fonctionner (120/130mA par rapport à 32 mA pour LoRa). Par conséquent, NB-IoT consomme plus d'énergie que ses concurrents directs LoRa et Sigfox, mais reste compétitif.

NB-IoT offre une qualité de service (QoS) supérieure à LoRa et Sigfox. Il utilise un spectre sous licence et son protocole (synchrone à créneaux temporels) est optimal pour la QoS. Il nécessite en revanche des bandes sous licence du spectre Sub-1GHz. Ce qui représente un coût énorme pour les opérateurs (généralement plus de 500 millions de dollars par MHz). En revanche, le NB-IoT ne supporte pas actuellement le handover [1]. Une reconnexion au

1. mécanisme permettant à un équipement de changer de cellule radio sans interrompre la conversation ou le transfert des données

réseau est nécessaire. Et de par la taille de ses cellules, plus petites que sur LoRa et Sigfox, cette reconnexion se fera plus régulièrement. Le NB-IoT est donc peu approprié dans des cas d'usages en mobilité constante (camions de livraison, véhicules autonomes...).

En France, seul l'opérateur SFR a choisi de déployer un réseau NB-IoT sur le territoire depuis 2019. En 2020, SFR ne communique pas encore sur l'avancée du déploiement du réseau NB-IoT. Dans le monde, des géants de la télécommunication tels que Huawei, Qualcomm, Vodafone et T-Mobile ont également choisi cette technologie.

3.2.4.2/ LTE-M

Le LTE-M (*Long Term Evolution, category M1*) également appelé eMTC (*enhanced Machine Type Communication*) est un système de communication utilisant le réseau 4G existant. Il dérive de l'itération 12 de standard LTE (*Long Term Evolution*) du 3GPP, et est amélioré dans l'itération 13 (LTE-M13) [Rat14]. Il constituera une des « briques » de la 5G au cours des années à venir, au niveau des projets IoT qui nécessitent des consommations énergétiques faibles mais également une qualité de service.

Son avantage principal est un débit largement supérieur à ses concurrents directs, avec environ 1 Mbit/s maximum grâce à une occupation spectrale de 1,4 MHz. Cela lui permet d'intégrer des données plus volumineuses comme la voix ou l'envoi de fichiers (images ou vidéos par exemple). La gestion de la mobilité (support du handover) et une latence réduite (environ 10ms) ont également été améliorés par rapport à NB-IoT, ce qui le rend plus utilisable que les autres protocoles pour des applications critiques [Bor20]. En contrepartie, la consommation énergétique est plus importante.

Pour réduire sa consommation énergétique, il ne conserve que le strict nécessaire de la pile de protocoles LTE pour la connexion des objets connectés, et il intègre le PSM (*Power Saving Mode*), un nouveau mode de fonctionnement de veille prolongée pendant un temps indéfini, au contraire de NB-IoT qui doit se synchroniser régulièrement [Bor20]. Il intègre également le mécanisme eDRX (*extended Discontinuous Reception*), permettant à l'équipement de planifier des temps de repos plus longs (*Paging Cycle*) en informant le réseau. Le LTE-M est particulièrement adapté dans le cadre d'application de suivi de déplacements, par exemple le traçage d'animaux dans la nature ou de véhicule en mouvement.

En France, seul l'opérateur Orange a lancé le déploiement du LTE-M sur le territoire. Il couvre, depuis 2019, environ 98 % de la population française en LTE-M13. Le déploiement est facilité par le faible coût d'infrastructure sur les réseaux existants : il ne nécessite qu'un changement au niveau de la couche logicielle des stations de base. L'ensemble des pays Européens, avec au moins un opérateur par pays sera couvert, ou en cours de déploiement, courant 2020. Des accords de roaming entre les pays permettront l'itinérance. La plateforme *Live Objects* d'Orange, se place en tant que coeur de réseau sur l'infrastructure du réseau Orange. Elle s'occupe, entre autres, de la gestion du parc, l'authentification, l'envoi de messages descendants et la notification d'alertes, pour les capteurs LTE-M mais aussi LoRa (Orange possède également son réseau LoRaWAN en France). Dans le monde, LTE-M a été choisi par 9 des plus grands opérateurs tels qu'AT&T et Verizon.

3.2.4.3/ 5G

La première génération (1G) de réseaux de communication mobiles n'offrait que des communications vocales analogiques. La deuxième génération (2G) était la première génération

numérique en offrant des messages texte avec des débits de données allant de 9,6 kbps à 19,2 kbps. La troisième génération (3G) intégrait des services Internet voix et mobile, offrant des débits de données allant de 144 kbps à 2 Mbps. La quatrième génération (4G) prend en charge les applications multimédia de grande capacité avec des débits de données allant de 100 Mbps à 1 Gbps [Bri16].

La 5G est la cinquième génération des standards pour la téléphonie mobile [Jon18]. Comme les générations précédentes, la 5G prolongera la norme LTE (*Long Term Evolution*). Elle est la prochaine étape dans l'évolution des communications mobiles. Son objectif principal est de répondre aux futures exigences des appareils mobiles en passant par :

- une connectivité pour tout type d'appareils,
- une augmentation de l'ordre de grandeur du débit de données jusqu'à 100 fois plus rapides que la 4G,
- une latence plus faible de l'ordre de 1ms, soit environ 10 à 20 fois moins que la 4G,
- une efficacité énergétique plus élevée pour l'IoT,
- une compatibilité avec les technologies précédentes.

Pour être en mesure d'atteindre ces objectifs, diverses technologies 5G sont en cours de développement. Le partenariat public-privé européen 5G (5GPPP) a, par exemple, financé des projets dans des domaines allant de la couche physique à l'architecture globale, à la gestion de réseau et aux réseaux logiciels. C'est une initiative conjointe entre la Commission Européenne et l'industrie européenne des TIC [1] (fabricants de TIC, opérateurs de télécommunications, prestataires de services, PME [2] et institutions de recherche). Son objectif secondaire est de renforcer l'industrie européenne et ouvrir de nouvelles opportunités d'innovation pour réussir à rivaliser sur les marchés mondiaux.

En plus des demandes de débit et de capacité élevées de trafic xMBB (*extreme Mobile BroadBand*) classiques, de nouvelles exigences ont vu le jour avec les cas d'utilisation de l'IoT comme : une faible latence, une grande fiabilité, une utilisation massive, une économie d'énergie.

Dans le contexte des nouveaux cas d'utilisation de la 5G, les applications de la 5G ont été définies en trois classes [Sch17] [Sin17] (figure 3.18) :

- les communications ultra haut débit xMBB : le débit de la 5G atteint 10 Gbit/s et 100 Mbit/s en bordure de cellule [Als18]. Cela va engendrer une quantité massive de données, il faudra prévoir des solutions pour stocker ces données. Un exemple d'application sera la surveillance en temps réel ou encore les vidéos immersives d'événements.
- les communications ultra-fiables à faible latence uRLLC [3] (ou parfois appelé uMTC [4]) : elles concernent les applications critiques, dans lesquelles l'échange de données ininterrompu et robuste est de la plus haute importance. Les temps de latence prévus sont de 1ms, contre 15ms pour la technologie LTE. Cette faible latence

1. Technologies de l'Information et de la Communication
2. Petite ou Moyenne Entreprise
3. ultra-reliable low-latency communications
4. ultra-reliable machine-type communications

est obtenue en déplaçant la puissance de calcul vers la périphérie du réseau, possible avec une approche de virtualisation dans l'architecture de réseau 5G [Zha18]. Cette virtualisation permet des transitions fluides entre technologies ou opérateurs. Un exemple d'application est la sécurité des voitures autonomes avec les piétons, ou la prise en charge d'opérations de patients à distance.

- les communications massives de type machine mMTC [1] : grand nombre d'appareils à faible coût avec des exigences élevées en matière d'évolutivité et de durée de vie accrue des batteries. Ce type de service sera donc utilisé pour les communications avec les capteurs et actionneurs. Ces communications seront assurées principalement par les réseaux LTM-M et NB-IoT évoqués précédemment, qui seront directement intégrés dans l'ensemble des technologies 5G.

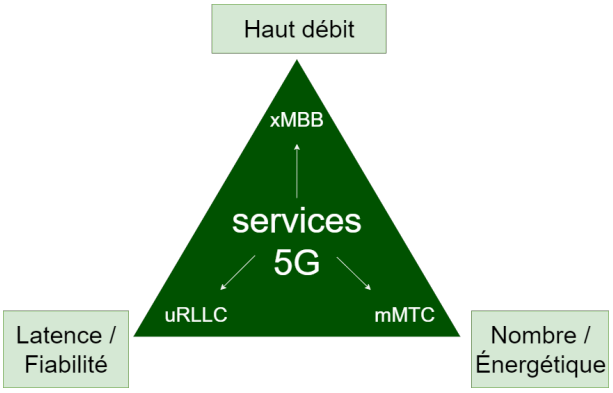


FIGURE 3.18 – Les différents services de la 5G.

La 4G utilise la modulation OFDM [2] (multiplexage par répartition orthogonale de la fréquence). Cependant, l'OFDM ne peut pas répondre aux exigences des réseaux 5G en raison de plusieurs problèmes [Bri16] :

- Sur-débit élevé dû au préfixe cyclique [3]. Cela entraîne un sur-débit élevé, ce qui réduit l'efficacité du spectre et augmente la consommation d'énergie.
- Émissions hors bandes élevées, limitant l'agrégation de porteuses [4].
- La synchronisation est un processus qui consomme du temps et de l'énergie dans un système OFDM. Elle est un facteur clé pour obtenir de bonnes performances, mais n'est pas forcément nécessaire (du moins pas régulièrement) dans les applications IoT.
- L'OFDM utilise des symboles longs et une trame longue, ce qui augmente la latence de la liaison radio.

1. massive machine-type communications
2. Orthogonal Frequency Division Multiplexing
3. Mécanisme qui permet principalement d'éliminer les interférences à la réception en recopiant les derniers échantillons du bloc au début de celui-ci.
4. Attribution de plusieurs bandes de fréquences à un utilisateur pour augmenter la vitesse maximale de transfert des données.

Pour permettre l'utilisation massive d'objets connectés, il convient d'adapter les réseaux et les qualités de service. Diverses solutions ont été proposées :

- le *Network Slicing* [Fou17] : concept qui découpe virtuellement un réseau en plusieurs tranches, afin de fournir des performances différentes selon l'usage de chaque tranche. Une tranche pour les voitures autonomes pourrait donc être dédiée en favorisant tout particulièrement la fiabilité et le niveau de latence. Ce concept nécessite la virtualisation des éléments de réseaux.
- le Radio Cognitive : technologie de gestion opportuniste du spectre, pour utiliser le meilleur canal disponible dans un temps et un lieu donné. Il nécessite de détecter dans quel état est l'environnement radio en mesurant les activités électromagnétiques (comparable à la procédure LBT, *Listen Before Talk* de LoRaWAN) puis d'analyser le spectre pour identifier les *"trous de spectre"*.
- l'utilisation massive des antennes MIMO (*Multiple Input Multiple Output*) : exploitation de l'effet multi-trajets, le signal radio se propageant par plusieurs chemins pour une réception sur une même antenne, dans les cellules urbaines.
- l'IoT daemon : modèle de couches basé sur une architecture distribuée pour permettre le dialogue massif, et la délégation des services de traitements entre les objets connectés...

3.2.5/ Comparaison des technologies longues portées

Dans la course aux LPWANs, nous avons montré que les différentes technologies réseaux ne sont pas conçues de manières identiques malgré des similarités au niveau des acteurs, ou des technologies de la couche physique et radio pour certaines.

Ces différences s'expliquent notamment par des objectifs différents en matière d'usage potentiel, ou encore en terme de coût d'installation et de déploiement. Au final, chacune des technologies se place sur une partie du marché des technologies longues portées et toutes celles-ci sont capables de cohabiter. Paul Pinault, expert sur les réseaux LPWAN et ambassadeur Sigfox, que nous avons contacté par téléphone en début de thèse, l'explique très bien dans cet article [Lpw19].

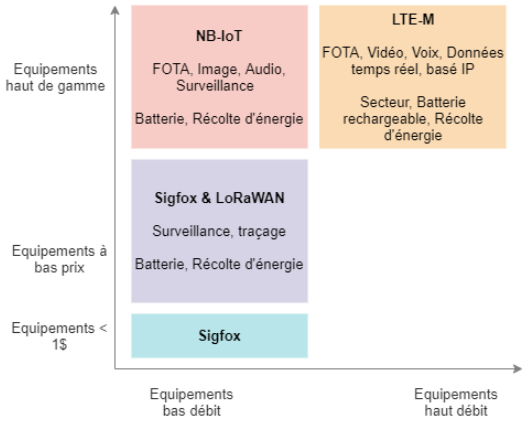


FIGURE 3.19 – La cohabitation des LPWANs sur le marché - [Lpw19].

Il y argumente que l'industrie des télécoms se plaçait au début de l'émergence technologique dans un océan rouge, c'est-à-dire une forte concurrence jusqu'à que l'une des technologies prenne le pas sur les autres en ciblant des cas d'utilisation et clients identiques à la concurrence.

Au lieu de ça, c'est un océan bleu (tiré du livre *Blue Ocean Strategy* [Mau07]) qui s'est installé, avec des technologies LPWAN qui cohabitent ensemble grâce à des cas d'utilisation et des clients différents. La figure 3.19 montre cette cohabitation.

À partir des recherches effectuées dans ce chapitre, nous avons réalisé un travail de synthèse sur la comparaison des technologies LPWAN. L'objectif est de :

- faciliter la prise de décision sur le choix d'une technologie plutôt qu'une autre,
- définir les points faibles et les points forts des technologies,
- et apporter des points techniques complémentaires sur l'utilisation des technologies.

Dans le tableau comparatif 3.3, nous avons comparé les technologies LTE-M, Nb-IoT, Sigfox et LoRaWAN (réseau objenious, réseau personnel et The Things Network) selon les critères suivants : la consommation énergétique, le coût global (installation, déploiement et matériel), la facilité d'utilisation, la couverture à l'échelle d'un territoire, la couverture aux endroits difficiles d'accès (deep-indoor), la possibilité de créer un réseau privé, la bidirectionnalité des données, l'itinérance (entre pays), la mobilité et enfin la densité maximale des réseaux.

Le tableau comparatif a été présenté manière empirique, avec des cases de couleur verte, orange et rouge pour une évaluation qualitative respectivement bonne, moyenne et mauvaise. Des explications supplémentaires ont été ajoutées en dessous du tableau comparatif pour préciser certains points intéressants.

	Consommation	Coûts	Facile	Couverture	Deep-indoor	Réseau privé	Bidirectionnel	Itinérance	Mobilité	Densité
LoRaWAN personnel			*C1*	*D1*	*E1*			*H1*		
LoRaWAN Objenious		*B2*	*C2*		*E2*	*F2*		*H2*		
LoRaWAN TTN			*C3*	*D3*		*F3*		*H3*		
Sigfox		*B4*					*G4*	*H4*		*J4*
Nb-IoT					*E5*		*G5*	*H5*	*I5*	
LTE-M									*I6*	

B2	20 euros par capteur par an (offre standard).
B4	Les prix peuvent varier entre 1 et 9 euros par an et par capteur.
C1	Il faut mettre en place les différentes antennes locales, le cœur de réseau, étudier la portée des objets, les canaux à utiliser…
C2	Nécessite de comprendre comment fonctionne la couche LoRaWAN (Spreding Factor, ADR…). Si la puce ne possède pas son propre microcontrôleur, cela nécessite d'utiliser une librairie externe.
C3	Nécessite de comprendre comment fonctionne la couche LoRaWAN (Spreding Factor, ADR…). Si la puce ne possède pas son propre microcontrôleur, cela nécessite d'utiliser une librairie externe.
D1	Couverture uniquement près de ses propres antennes.
D3	La couverture n'est pas bonne en France, mais elle est meilleure dans d'autres pays européens comme les Pays-Bas (pays plus petit et pas d'opérateur privé en avant.)
E1	Possibilité de couvrir les lieux les plus difficiles d'accès avec des antennes relais, mais cela reste coûteux.
E2	La technologie LoRa et la couverture actuelle ne permettent pas de couvrir en intérieur profond (sous-sols, pièces isolées…). La couverture en intérieur n'est effective principalement qu'en zone urbaine pour l'instant.
E5	Le réseau Nb-IoT possède une meilleure couverture en intérieur profond (+20 dB) notamment avec la multitude des antennes et l'utilisation de la bande de fréquences 900-1800 MHz.
F2	Les données sont stockées sur le cœur de réseau privé. Elles peuvent cependant être chiffrées depuis l'objet, et transiter jusqu'au serveur d'application nous appartenant. Les serveurs d'objenious ne sont pas Hébergeur de Données de Santé (HDS), ils n'ont théoriquement pas le droit de conserver des données de santé, même chiffrées.
F3	Pas d'opérateur, mais réseau partagé entre les particuliers.
G4	Il est possible de recevoir un message uniquement après un envoi (pas d'équivalent de classe C à LoRaWAN).
G5	Il est possible de recevoir un message uniquement après un envoi (pas d'équivalent de classe C à LoRaWAN).
H1	Il est maintenant possible de faire du Roaming (actif, passif) avec LoRaWAN.
H2	Le Roaming commence à se développer sur LoRaWAN et sera peut-être pris en compte prochainement pour ce réseau.
H3	Le réseau TTN, conçu sur des antennes collaboratives, est le même partout dans le monde.
H4	Comme Sigfox est un opérateur mondial, il est possible de l'utiliser dans n'importe quel pays qui est couvert.
H5	Cela dépend des opérateurs et des partenariats avec les autres opérateurs des autres pays. Cependant cela est techniquement possible, c'est un des objectifs de sa normalisation 3GPP.
I5	Après une mise en veille, il faut établir une nouvelle connexion avec le réseau (attribution d'une nouvelle adresse IP).
I6	Le "handover" est supporté.
H2	Jusqu'à 40 000 appareils par cellule.
J4	Jusqu'à 1 millions d'appareils par cellule.

TABLE 3.3 – Tableau comparatif des LPWANs.

Après cette étude comparative, nous pouvons effectuer un premier tri des technologies susceptibles de nous intéresser par la suite.

Sigfox, est facile d'utilisation à très faible coût par capteur et sa couverture est extrêmement développée. Cependant, il n'est pas réellement adapté à un monitoring médical de par son débit très faible, sa limitation en nombre de messages par jour, son réseau extrêmement fermé et sa faible capacité à couvrir à l'intérieur des bâtiments.

Nb-IoT est intéressant dans sa capacité à être économe en énergie, tout en ayant un débit de données plus important, une qualité de service plus importante et pas de limitation de nombre de messages par jour. Il n'est toutefois pas assez représenté en France et pas encore opérationnel à l'heure actuelle. LTE-M est lui mieux développé en France avec l'opérateur Orange malgré sa plus forte consommation en énergie.

La technologie LoRa est très intéressante par la possibilité de créer son propre réseau local (à l'échelle d'un hôpital par exemple) avec de nombreux paramètres de transmissions adaptables et la possibilité de contrôler le côté serveur *backend* avec des algorithmes personnalisés. Mais elle a également, la possibilité d'utiliser la couverture des opérateurs téléphoniques comme Objenious. L'inconvénient majeur de ce réseau est lié à la bande de fréquences ISM 868 Mhz, qui limite le *duty cycle* et donc le nombre de transmissions par jour avec un débit relativement faible.

Pour conclure, la technologie LoRa est probablement la plus adaptée dans la personnalisation de réseau en fonction de nos besoins. Nous retenons également Nb-IoT pour sa qualité de service, mais en l'attente d'une meilleure couverture, LTE-M se montre comme un choix alternatif, mais plus énergivore.

3.3/ LES TECHNOLOGIES DES RÉSEAUX LOCAUX (LAN)

De nombreux protocoles ont été pensés pour une faible consommation énergétique dans un environnement restreint, à l'échelle d'une maison, d'une entreprise, ou d'un établissement de santé par exemple. C'est le cas des protocoles tels que *Bluetooth Low Energy* (BLE), IEEE 802.15.4, ZigBee, Zwave ou encore IEEE 802.11n (version économique en énergie du WiFi). Différentes technologies, comme l'utilisation de canaux plus étroits, l'étalement de spectre, le mode veille, ou la compression de données ont permis de diminuer considérablement la consommation d'énergie de ces protocoles, en relation avec la diminution de la taille des paquets et du débit physique au strict minimum.

Nous détaillons, dans cette section, les protocoles des réseaux locaux les plus prometteurs, et qui sont déjà, ou peuvent être appliqués au domaine de la santé. Nous aborderons principalement BLE et IEEE 802.15.4, en détaillant particulièrement les implémentations de ce dernier telles que ZigBee et 6LowPAN.

3.3.1/ BLUETOOTH LOW ENERGY

La technologie BLE (*Bluetooth Low Energy*), également appelée *Bluetooth Smart* ou *Bluetooth 4.0* est une évolution de Bluetooth (IEEE 802.15.1) qui possède de meilleures spécifications pour les communications sans fil à faible consommation [Gom12] [Kuo14]. Les premières versions du BLE (sous le nom de *Wibree*) ont été introduites par Nokia en 2006 sous la forme d'un standard ouvert, qui complète, sans remplacer, le Bluetooth classique. La conception

et la commercialisation de la technologie est maintenant effectuée par le *Bluetooth Special Interest Group* (Bluetooth SIG).

Bluetooth Low Energy utilise les mêmes fréquences radio que le Bluetooth classique, à bande ISM 2,400-2,4835 GHz, ce qui permet aux appareils de partager une seule antenne radio. Il utilise cependant un système de modulation plus simple : l'étalement de spectre par saut de fréquence FHSS avec 43 canaux de largeur de bande de 2 MHz (alors que le Bluetooth classique se place sur 79 canaux de 1 MHz) pour une portée d'environ 100 mètres [Sie12]. Il existe deux types de canaux BLE : les canaux publicitaires et les canaux de données. Les canaux publicitaires sont utilisés pour la découverte des appareils, la connexion et la diffusion. Les canaux de données sont utilisés pour la communication bidirectionnelle entre les appareils connectés. La modulation par saut de fréquence est utilisée pour éviter les interférences, pour empêcher les écoutes et permettre les communications à accès multiple par répartition en code (CDMA). Son débit de 1 Mb/s le place dans le même ordre de grandeur que le Bluetooth classique, avec cependant une consommation d'énergie 10 à 20 fois moindre que ce dernier.

Le principe de conception a été orienté vers les appareils à très basse consommation, ce qui le rend idéal pour les nœuds de capteurs autonomes alimentés par batterie. Cette technologie est largement utilisée dans le domaine des objets connectés de santé (montres connectées, appareils de surveillance médicale...). Les systèmes d'exploitation mobiles comme iOS, Android, Windows Phone et BlackBerry, ainsi que le système d'exploitation macOS, Linux, Windows, prennent en charge de manière native *Bluetooth Low Energy*.

Les profils d'utilisation

Afin de répondre au besoin de fonctionnement d'un appareil dans une application particulière, le Bluetooth SIG définit plusieurs profils d'utilisation pour les appareils à faible consommation d'énergie, en se basant sur le *Generic Attribute Profile* (GATT). Les fabricants peuvent mettre en œuvre les spécifications appropriées d'un ou plusieurs profils pour leur appareil. On retrouve des profils pour toutes sortes d'applications, comme des profils audio pour véhiculer le son, des profils de notification d'alerte ou d'alarme, des profils de claviers et souris d'ordinateurs, des profils pour la connectivité internet ou encore des profils de maillage par exemple pour éteindre plusieurs appareils en même temps par retransmission de l'information entre les équipements. Également, il existe des profils dédiés pour les soins de santé et des profils dédiés au sport et au fitness : ce sont les profils les plus susceptibles de nous intéresser dans les applications de télésurveillance. Ils sont réalisés par le Bluetooth SIG en coopération étroite avec la *Personnal Connected Health Alliance* (cf section 2.2.3). Les premiers profils étaient spécifiques à un usage particulier comme BLP (*Blood Pressure Profile*), HTP (*Health Thermometer Profile*), GLP (*Glucose Profile*) ou encore CGMP (*Continuous Glucose Monitor Profile*). Dans le domaine du fitness, c'était également le cas avec par exemple BCS (*Body Composition Service*), HRP (*Heart Rate Profile*) ou RSCP (*Running Speed and Cadence Profile*). Il existe maintenant un unique profil HDP (*Health Device Profil*), basé sur la norme IEEE 11073-20601, qui permet de répondre à l'ensemble des usages. C'est sur ce profil que se base maintenant le standard *Personnal Connected Health Alliance* pour les dispositifs de santé connectés.

Les spécifications ISO / IEEE 11073 contiennent, entre autres, la spécification décrivant les outils pour représenter et transmettre des données de santé. Elles contiennent également un ensemble de spécialisations de données de périphérique, avec des détails pour des

applications spécifiques.

Il existe les spécialisations de données suivantes [Blu19] :

- IEEE 11073-10404 – Pulse Oximeter,
- IEEE 11073-10406 – Basic ECG (heart rate),
- IEEE 11073-10407 – Blood Pressure Monitor,
- IEEE 11073-10408 - Thermometer,
- IEEE 11073-10415 – Weighing Scale,
- IEEE 11073-10417 – Glucose Meter,
- IEEE 11073-10418 – International Normalized Ratio (INR) Monitor,
- IEEE 11073-10420 – Body Composition Analyzer,
- IEEE 11073-10421 – Peak Flow Monitor,
- IEEE 11073-10441 – Cardiovascular Fitness and Activity Monitor, Step Counter,
- IEEE 11073-10442 – Strength Fitness Equipment,
- IEEE 11073-10471 – Independent Living Activity Hub, Fall Sensor, Personal Emergency Response Sensor, Smoke Sensor, Carbon Monoxide (CO) Sensor, Water Sensor, Gas Sensor, Motion Sensor, Property Exit Sensor, Enuresis Sensor, Contact Closure Sensor, Usage Sensor, Switch Sensor, Medication Dosing Sensor, Temperature Sensor,
- IEEE 11073-10472 – Medication monitor,
- IEEE 11073-10427 – Power Status Monitor.

L'utilisation du profil HDP présente un certain nombre d'avantages [Sil9] :

- une meilleure interopérabilité : c'est un profil spécialisé conçu pour permettre l'interopérabilité entre les applications médicales, de santé et de fitness de différents fournisseurs. L'utilisation du protocole d'échange optimisé ISO / IEEE 11073-20601 fournit une approche structurée lors des échanges d'informations entre les dispositifs de santé communicants.
- un appareillage spécifique : il fournit une méthode de recherche de périphérique par type d'appareil et type de donnée. Cette recherche de périphérique est réalisée à l'aide de la procédure de découverte inclue dans le profil d'accès générique (GAP) et du protocole SDP (*Service Discovery Protocol*).
- une meilleure fiabilité : la source et le récepteur sont capables de détecter la rupture de la connexion pour réagir en fonction, par exemple lorsque les deux équipements s'éloignent trop. La couche *Reliable Data Channel* est également capable de détecter et retransmettre les paquets corrompus par des interférences sur la liaison radio, avec une séquence de vérification de trame (FCS). Cette vérification est importante lorsque le périphérique évolue à proximité d'un réseau Wi-Fi par exemple. HDP définit également un protocole de synchronisation d'horloge (CSP) permettant une synchronisation précise entre les appareils de santé.

- un mode repos : HDP permet aux appareils de conserver leur état pour éliminer les étapes de configuration redondantes lors des reconnexions. Cette procédure permet une déconnexion des appareils quand ceux-ci ne sont pas en transmission afin de réduire la consommation électrique. La latence, en partant d'un état non connecté, est par la même occasion réduite lors de l'envoi : environ 6 ms au lieu de 100 ms pour le Bluetooth classique.
- des configurations de canaux flexibles suivant l'application : chaque canal peut être configuré indépendamment pour offrir un niveau de fiabilité plus ou moins important. Les canaux plus fiables utilisent un mode de retransmission améliorée, tandis que les canaux de données utilisent le mode streaming.

3.3.2/ IEEE 802.15.4 ET SES IMPLÉMENTATIONS

IEEE 802.15.4 est une norme technique ouverte, établie en 2003, qui définit le fonctionnement des réseaux personnels sans fil à bas débit LRWPAN (*Low Rate Wireless Personal Area Network*) maintenue par le groupe de travail IEEE 802.15 [Erg04] [Han10]. Il spécifie la couche Physique et le contrôle d'accès au support avec un accent sur la communication à très faible coût des appareils à proximité dans l'intention de réduire la consommation d'énergie.

Cette norme est une base pour d'autres technologies ou protocoles comme Zigbee, Thread, 6LoWPAN, ISA100.11a, WirelessHART ou encore MiWi. Ceux-ci étendent la norme en développant les couches supérieures (les couches hautes du réseau) qui ne sont pas définies dans IEEE 802.15.4. Ce sont donc toutes des technologies complémentaires à IEEE 802.15.4. Les spécifications de la norme IEEE 802.15.4 sont disponibles sur internet et son implémentation est ouverte à tout le monde.

Bande (MHz)	*Modulation*	*Étalement*	*Débit (bit/s)*	*Norme*
868/915	BPSK	DSSS	20 k à 868 MHz / 40k à 915 MHz	IEEE 802.15.4-2003
2400	OQPSK	DSSS	250k	
868/915	BPSK	DSSS	20 k à 868 MHz / 40k à 915 MHz	EEE 802.15.4-2006
868/915	OQPSK	DSSS	100 k à 868 MHz / 250k à 915 MHz	
868/915	BPSK/ASK	PSSS	250 k	
2400	OQPSK	DSSS	250 k	
2400	DQPSK	CSS	1 M	IEEE 802.15.4a-2007
250-750	UWB		110 k à 850 k	
3244-4742	UWB		110 k à 850 k	
5944-10234	UWB		110 k à 850 k	
780	OQPSK	-	250 k	IEEE 802.15.4c-2009
780	MPSK	-	250 k	
950	GFSK	-	100 k	IEEE 802.15.4d-2009
950	BPSK	DSSS	20 k	

TABLE 3.4 – Caractéristiques des couches PHY définies par IEEE 802.15.4.

Le cadre de base de la norme a été conçu pour une portée de communication de 10 mètres et un débit de transfert de 250 kbits/s. Depuis, de nouvelles définitions de la couche physique ont vu le jour pour répondre aux exigences des dispositifs embarqués à faible puissance. Notamment, la norme a évolué pour utiliser la bande de fréquences ISM 868/915 MHz avec un débit de 40 kbits/s et une portée d'environ 75 mètres. Le tableau 3.4 récapitule les caractéristiques des couches physiques PHY définies dans les différentes versions de la norme IEEE 802.15.4 (une couche PHY possible par ligne).

La norme définit l'architecture des couches Physique (PHY) et Liaison. La couche PHY gère l'émetteur-récepteur RF physique, les fonctions de sélection de canal et la gestion de l'énergie et du signal. Elle fonctionne sur les trois bandes possibles sans licence : 868.0 MHz (Europe), 928 MHz (Amérique du nord) et 2400 MHz (monde entier) (voir tableau tableau 3.4). La version originale utilisait un spectre étalé DSSS (*Direct Sequence Spread Spectrum*) et une modulation BPSK/OQPSK. De nouvelles couches PHY sont apparues par la suite en utilisant notamment les étalements UWB (*Ultra-WideBand*) et CSS (*Chirp Spread Spectrum*), ainsi que les techniques de modulations ASK, OQPSK, MPSK ou GFSK. Au final, selon les différentes couches, le débit se situe entre 20 et 250 kbits/s, pour une portée entre 10 et 75 mètres environ. La taille maximale des paquets est de 127 octets.

La couche Liaison supporte la mise en place de réseaux de type étoile ou mesh. Le contrôle d'accès au support (MAC) permet la transmission de trames MAC via l'utilisation du canal physique. Il gère, entre autres, le service de données, la validation des trames, les intervalles de temps entre les envois/réceptions et les associations de nœuds. Enfin, il propose des points d'accroche pour des services sécurisés.

La norme 802.15.4 définit deux types de dispositifs [Sal10] :

- RFD (*Reduced Function Device*) : c'est un simple dispositif communicant pour signaler l'état d'un capteur ou contrôler l'activation d'un actionneur,
- FDD (*Full Function Device*) : il assure, en plus du RFD, la coordination au sein d'un réseau PAN comme l'initialisation du réseau, l'ajout de nouveaux dispositifs ou l'interface avec d'autres réseaux.

Le réseau pourra ensuite choisir un mode de fonctionnement parmi deux possibles :

- le mode *non-beacon* : le coordinateur (FDD) se met en attente permanente de données, sans temps de repos. Lorsque le coordinateur veut transmettre quelque chose au dispositif, il doit attend que le dispositif entre en contact avec lui. Les dispositifs peuvent envoyer des données quand ils le souhaitent, après avoir vérifié que le canal est libre (protocole CSMA/CA). Ce mode est utilisé généralement pour les capteurs qui sont en repos la plupart du temps.
- le mode *beacon* : les stations sont synchronisées sur le coordinateur (RFD) qui émet ou reçoit à intervalles réguliers. Les intervalles de temps sont appelés supertrames et sont divisés en 16 slots temporels appelés GTS (*Guaranteed Time Slot*). Les stations et surtout le coordinateur peuvent donc être en repos pendant ces intervalles de temps.

Les couches supérieures ou sous-couches d'interopérabilité ne sont pas définies dans la norme. Mais il existe d'autres spécifications, certaines propriétaires, qui s'appuient sur cette norme comme ZigBee, 6LowPAN ou encore Thread.

ZigBee

Zigbee [Erg04] [Gis08] a été conçu en 1998, normalisé en 2003 et enfin révisé en 2006. C'est une spécification basée sur la norme IEEE 802.15.4 pour une suite de protocoles de communication de haut niveau. La norme Zigbee a été initialement conçue pour des applications de domotique. Cependant, dans le domaine de santé, il a été mis en avant par la *Personnal Connected Health Alliance* comme un des protocoles sans fil retenu dans le standard Continua, avec le Bluetooth et BLE (cf section 2.2.3). La ZigBee Alliance a été crée en 2002 avec notamment les membres Ikea, Legrand, Samsung ou Amazon. C'est un groupe de sociétés qui maintient et publie la norme ZigBee basée sur IEEE 802.15.4, à l'image de la Wi-Fi Alliance avec la norme IEEE 802.11.

Les modes de fonctionnements des dispositifs Zigbee héritent de IEEE 802.15.4, avec trois types [Yen08] : le coordinateur ZC (équivalent du FDD), les *end devices* ZED (équivalent des RFD), et les routeurs ZR (uniquement la fonction routage du FDD). Les protocoles Zigbee prennent en charge également les réseaux en mode *beacon* et *non-beacon* de la norme. En mode *beacon*, les intervalles de temps dépendent du débit de données : ils s'étalent de 15,36 millisecondes à 786,432 secondes pour un débit de 20 kbits/s à 250 kbits/s. Cependant, un fonctionnement à faible cycle de service avec de longs intervalles de balise nécessite une synchronisation précise, ce qui peut être problématique lorsque les dispositifs sont peu performants et à faible coût.

ZigBee définit sa propre couche réseau avec un protocole de routage nommé AODV (*Ad-hoc On-demand Distance Vector*) qui permet un routage dans un réseau maillé. Pour trouver le périphérique de destination, AODV diffuse une demande d'itinéraire à tous ses voisins, qui feront de même jusqu'à trouver la destination. Le retour via une transmission *unicast* se fera par le chemin le moins coûteux grâce à la sauvegarde de l'itinéraire. La source pourra ensuite enregistrer, elle aussi, l'itinéraire vers la destination dans une table de routage [Alg14]. La couche application, quant à elle, constitue l'interface du système ZigBee avec les utilisateurs finaux. Cette couche initie les envois des messages entre les périphériques liés, gère les adresses de groupe, réassemble les paquets, transporte également les données et gère le ZDO (*ZigBee device object*). Le ZDO est un protocole responsable de la gestion globale des périphériques, des clés de sécurité, des politiques, des rôles des équipements en tant que coordinateur ou terminal, et de la découverte de nouveaux équipements.

6LowPAN

6LoWPAN est un acronyme d' *IPv6 over Low-Power Wireless Personal Area Networks*. Le concept est né, en 2007, de l'idée que le protocole IP pourrait et devrait être appliqué même au plus petit des appareils [Mul07]. IP est déjà utilisé actuellement pour l'accès Internet avec le Wi-Fi et Ethernet de nos ordinateurs portables, smartphones, tablettes... 6LoWPAN est donc une option de plus pour utiliser IP pour les objets intelligents dans l'IoT, et leur fournir une intégration Internet directe de bout en bout.

L'objectif initial était de définir une couche d'adaptation, sur des réseaux basés sur IEEE 802.15.4, pour répondre aux exigences de IPv6. Ce dernier est reconnu comme la dernière version du protocole de communication IP développé pour résoudre le problème attendu de l'épuisement des adresses IPv4.

Les spécifications 6LoWPAN définissent les mécanismes d'encapsulation et de compression

d'en-tête qui permettent aux paquets IPv6 d'être envoyés et reçus sur les réseaux. La spécification de base RFC 4944 a été développée par le groupe 6LoWPAN IETF, puis mise à jour successivement par RFC 6282 pour compression d'en-tête et par RFC 6775 pour l'optimisation de découverte de voisins.

De base, IPv6 impose une taille de paquets minimal de 1280 octets. Or nous avons vu que la taille maximale des paquets IEEE 802.15.4 est de 127 octets. Pour s'adapter, la solution est de fragmenter un paquet IPv6 en plusieurs trames. Cependant, divers problématiques s'ajoutent à cela :

- les fragmentations/réassemblages excessifs entraînent des surconsommations de mémoire et CPU,
- l'entête IPv6 de 40 octets n'offre que peu de place à la charge utile, il a fallu trouver des mécanismes de compression d'entête (actuellement LOWPAN_IPHC pour UDP),
- le routage sur des réseaux de type mesh ou étoile a dû être géré (protocole LOADng et RPL),
- ...

Une couche adaptation pour 6LoWPAN est donc apparue entre la couche réseau (paquets IPv6 de 1280 octets) et la couche liaison (trames 802.15.4). 6LoPWAN ne définit pas explicitement la couche application. Cependant, des travaux récents, à partir de 2016, suggèrent d'utiliser le protocole COAP (*Constrained Application Protocol*) en remplacement de son homologue HTTP. COAP est un protocole RESTful défini par l'IETF avec une complexité réduite basée sur UDP.

Nous pouvons évoquer également la technologie *Thread* pour les réseaux maillés spécialisés dans la domotique, qui est basée sur 6LoWPAN. Ces dernières années, l'alliance *Thread Group* a réuni diverses sociétés telles que Nest Labs (Google), Apple, Samsung, Qualcomm, Silicon Labs, Somfy et d'autres afin d'établir une technologie efficace pour la maison connectée, en renforçant notamment la sécurité.

Au final, 6LoWPAN offre une simplicité de communication et d'interopérabilité meilleure que Zigbee. Cependant, ce dernier bénéficie d'une meilleure expérience, avec notamment une sécurité renforcée.

3.4/ LES TECHNOLOGIES DES RÉSEAUX CORPORELS (BAN)

Bien que ZigBee ou Bluetooth Low Energy (BLE) soient souvent utilisés pour les communications entre capteurs à proximité du corps, en répondant aux attentes pour les réseaux corporels (comme Wong et al. [Won13]), le standard IEEE 802.15.6 a été créé exclusivement pour les types d'applications qui environnent le corps humain. C'est aujourd'hui le seul standard reconnu pour cela. Il permet également d'éviter la bande 2,4 GHz principalement dédiée au trafic WLAN (avec le Wi-Fi et Bluetooth) et sensible aux interférences.

3.4.1/ 802.15.6 (BAN)

Le standard IEEE 802.15.6 a été publié en février 2012. C'est une norme internationale pour les communications sans fil à faible puissance, à courte portée et extrêmement fiable dans la zone environnante du corps humain [Kwa10] [Sal16] : les BANs (*Body Area Networks*), appelés également WBANs (*Wireless Body Area Networks*) ou BSNs (*Body Sensor Networks*). Cette norme prend en compte différents facteurs propres au corps humain comme :

- les effets causés par la présence d'une personne sur les ondes et les antennes à proximité (interférences...),
- la configuration du diagramme de rayonnement pour minimiser le taux d'absorption spécifique (SAR) dans le corps,
- la mobilité des utilisateurs.

Les applications WBAN visées par la norme IEEE 802.15.6 sont divisées en applications : les applications médicales (collecte continue d'informations vitales sur un patient pour la télésurveillance) et les applications non médicales (l'armée, les jeux, les réseaux sociaux, le transfert de données ou la surveillance des objets oubliés...) Le protocole utilise les bandes ISM (*Industrielle, Scientifique et Médicale*) ainsi que les bandes de fréquences approuvées par les autorités médicales et réglementaires nationales. Il est possible de différencier trois types de bandes (figure 3.20) :

- la bande MICS (*Medical Implant Communications Service*) est une bande sous licence utilisée pour la communication bas débit avec les implants. Elle possède la même gamme de fréquences (402-405 MHz) dans la plupart des pays.
- la bande WMTS (*Wireless Medical Telemetry Services*) est une bande sous licence utilisée pour le système de télémétrie médicale. Tout comme MICS, la bande WMTS ne prend pas en charge les applications à haut débit.
- la bande ISM (*Industrielle, Scientifique et Médicale*) prend en charge les applications à haut débit et est disponible dans le monde entier. Cependant, les risques d'interférences sont élevés car de nombreux appareils sans fil, y compris IEEE 802.1 et IEEE 802.15.4, fonctionnent sur la bande ISM.

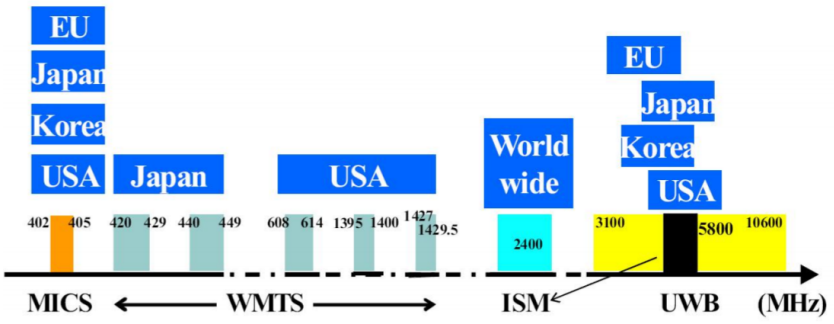


FIGURE 3.20 – Bandes de fréquences pour 802.15.6 - [Kwa10].

La norme actuelle IEEE 802.15.6 définit trois couches physiques (PHY) [Li12]. La sélection de chaque PHY dépend des exigences de l'application.

Human Body Communication (HBC)

Frequency	Bandwidth
16	4
27	4

Narrowband Communication (NB)

Frequency	Bandwidth
402-405	300
420-450	300
863-870	400
902-928	500
956-956	400
2360-2400	1
2400-243805	1

Ultra-Wideband communication

Frequency	Bandwidth
3.2-4.7	499
6.2-10.3	499

FIGURE 3.21 – Bandes de fréquence et bande passante des couches physiques - [Sal16].

La figure 3.21 présente le découpage des bandes de fréquences des couches physiques en canaux. Les trois couches sont :

- la couche physique à bande ultralarge (UWB) pour des applications de divertissement à haut débit. Elle fonctionne dans deux bandes de fréquences (bande basse et bande haute) divisées en canaux de 499,2 MHz. Une trame UWB contient une en-tête de synchronisation (SHR), une en-tête PHR nécessaires au décodage et un PSDU (corps du message).
- la couche physique de la communication corps humain (HBC) qui utilise le corps humain comme un canal. Elle utilise la technologie de communication de champ électrique (EFC). Elle fonctionne dans deux bandes de fréquences centrées sur 16 MHz et 27 MHz avec une bande passante de 4 MHz.

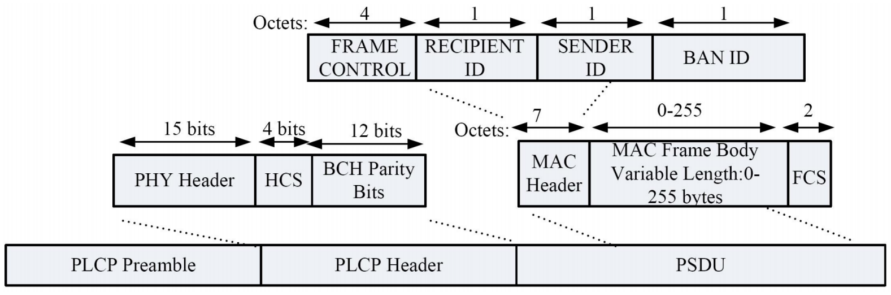


FIGURE 3.22 – Structure de la trame PPDU pour la couche PHY NB - [Sal16].

- la couche physique à bande étroite (NB) optimisée pour les applications biomédicales comme la biotélémétrie à très faible débit (capteurs placés sur le corps humain ou implantés). C'est principalement cette couche qui nous intéresse dans les applications de télésurveillance médicale. Cette couche gère la transmission / réception des données, l'activation / désactivation de l'émetteur-récepteur radio, et du CCA (*Clear Channel Assessment*), l'évaluation si le canal est libre ou déjà en cours d'utilisation. La figure 3.22 montre la trame PPDU (*PHY Protocol Data Unit*) de la couche NB. Elle est composée, en autres, d'un préambule PLCP (*PHY Layer Convergence Protocol*) pour la synchronisation et le décalage de porteuse, une en-tête PLCP (*PHY Layer Conformance Procedure*) avec les informations nécessaires au décodage et un composant PSDU (*PHY Service Data Unit*) qui contient le corps du message (body). Dans cette couche, la norme utilise différentes techniques de modulation suivant la bande de fréquences utilisée : DBPSK, DQPSK, D8PSK ou encore GMSK.

  Avec une puissance d'émission TX de -10dBm, la portée pour la couche NB est d'environ 40 mètres, et jusqu'à 110 mètres en condition optimale. [Won13].

La couche de Liaison MAC prépare la transmission et la réception des trames afin de gérer les délais de réponse, d'acquittement des trames et de contrôler les collisions (avec des retransmissions en cas de besoin). La norme définit également 3 niveaux de sécurité, du niveau 0 le plus faible (non sécurisé), au niveau 2 le plus fort (authentification et chiffrement AES-128 bits).

Synthèse du chapitre 3

SYNTHÈSE

Dans ce dernier chapitre très dense d'état de l'art, nous avons pu aborder le cœur de la thèse avec les réseaux de l'Internet des Objets. Tout d'abord, l'étude des transmissions par ondes radiofréquences ainsi que leur fonctionnement ont été présentés. Le modèle OSI permet de mieux comprendre le fonctionnement des technologies et des protocoles de l'IoT sur les couches basses : les couches physiques et liaisons essentiellement.

Nous avons montré la différence entre les réseaux longues portées destinés à un usage sur les espaces étendus (WAN) et les réseaux courtes portées destinés à un usage local (LAN), ou même sur le corps (BAN). Nous avons étudié en détails chacun des protocoles les plus prometteurs, à tous les niveaux, tels que Bluetooth Low Energy, IEEE 802.15.4, ZigBee, 6LowPAN, IEEE 802.15.4, Sigfox, NB-IoT, LTE-M, et tout particulièrement LoRaWAN.

Le premier travail de comparaison des technologies LPWAN que nous avons réalisé dans ce chapitre nous permet de définir les meilleures technologies qui pourront répondre à nos besoins pour la création d'une plateforme de télésurveillance, ce que nous développerons dans le chapitre suivant.
Nous avons notamment retenu la technologie LoRa adaptée dans la personnalisation de réseau en fonction de nos besoins, mais également LTE-M en choix alternatif de Nb-IoT pour sa qualité de service en attendant une meilleure couverture en France.
Nous avons également décrit en détails ADR de LoRaWAN, un algorithme qui adapte dynamiquement les paramètres de transmissions (facteur d'étalement, débit ou encore largeur de bande) lorsque les conditions le permettent, afin de réduire encore davantage la consommation énergétique. Nous utiliserons cet algorithme dans nos travaux, en relation avec de nouveaux mécanismes que nous introduirons dans les contributions pour fonctionner en mobilité.

Le chapitre suivant est consacré à nos contributions autour de l'élaboration de la nouvelle plateforme de télésurveillance que nous avons nommée I^{2}PHEN (**I**oT **I**nteroperable **P**latform for **HE**alth mo**N**itoring low power), en utilisant les technologies, les objets et les dispositifs médicaux, ainsi que les standards de l'Internet des Objets que nous avons détaillés dans ces trois premiers chapitres de l'état de l'art.

II

CONTRIBUTION

Cette partie détaille notre contribution qui s'articule principalement autour de notre plateforme de télésurveillance médicale I^{2}PHEN (**I***oT* **I***nteroperable* **P***latform for* **HE***alth mo***N***itoring low power*).

Cette plateforme a été conçue et réalisée à l'aide des technologies de l'Internet des Objets que nous avons définies précédemment telles que les réseaux longue portée et économes en énergie, les dispositifs et les standards de la santé connectée.

Dans le chapitre 4, nous développerons les défis que la plateforme devra relever, tels que la qualité des données, la sécurité ou l'interopérabilité, et nous étudierons comment elle sera en mesure de les réaliser. Nous aborderons l'économie d'énergie, l'ubiquité, la fiabilité, l'adaptabilité, le coût, la réglementation, ..., et tout cela dans l'objectif de définir la meilleure plateforme de télésurveillance possible.

Notre premier prototype de plateforme est prometteur mais certains objectifs sont encore perfectibles et nous évoquerons ces points et les possibilités d'amélioration. Nous détaillerons également des méthodes alternatives pour répondre à des besoins spécifiques, tels que l'amélioration de la fiabilité avec l'utilisation des réseaux cellulaires.

Enfin, dans le chapitre 5, nous aborderons l'algorithme ADR (*Adaptive Data Rate*) de LoRaWAN, pour l'adaptation des paramètres d'émission dynamiquement afin de réduire la consommation énergétique principalement. Puisque celui-ci n'est pas performant en cas de mobilité, nous proposerons un mécanisme original, COMMA (**C***ommunication* **O***ptimisation* **M***echanism for* **M***obility* **A***daptation*), plus adapté aux cas de mobilité quotidienne pour les patients actifs. Celui-ci se basera notamment sur une adaptation plus rapide des paramètres d'émission en cas de changement d'environnement, grâce à la localisation et l'historisation des lieux déjà rencontrés par l'objet.

Pour finir, nous étudierons le modèle énergétique des algorithmes ADR et COMMA avec des calculs de la consommation théorique. Nous pourrons alors comparer ces mesures avec la consommation théorique dans les meilleures et les pires conditions en faisant varier les paramètres de transmissions. Tout cela nous donnera également un aperçu de la durée de vie théorique des batteries dans les différentes conditions.

4

NOTRE NOUVELLE PLATEFORME DE TÉLÉSURVEILLANCE MÉDICALE I²PHEN

Ce chapitre est le premier de la partie contribution, il est consacré à la présentation de notre nouvelle plateforme de télésurveillance médicale : I²PHEN (**I***oT* **I***nteroperable* **P***latform for* **HE***alth mo***N***itoring low power**). La réalisation de cette dernière a été possible grâce aux connaissances acquises dans les chapitres précédents : l'Internet des Objets, les dispositifs médicaux, les réseaux courte ou longue portée mais également l'aspect réglementaire et qualitatif de la e-Santé. Tous ces éléments seront repris dans ce chapitre.

Cette plateforme répond à des challenges, il est donc important pour nous de synthétiser nos besoins, et de lister les exigences fonctionnelles d'une telle plateforme dans un contexte d'utilisation sur le terrain. Les choix, de technologies notamment, en découleront. Nous pourrons alors établir l'architecture de la plateforme puis en définir les acteurs. Nous décrirons longuement ces acteurs un à un, avec tous leurs éléments techniques, mais aussi fonctionnels.

Ce chapitre se termine par une description de la sécurité pour notre plateforme de bout en bout, c'est-à-dire pour chaque communication qui sera effectuée entre les différents acteurs.

4.1/ LES CHALLENGES DE NOTRE NOUVELLE PLATEFORME DE TÉLÉSURVEILLANCE

Pour qu'une plateforme de télésurveillance soit fonctionnelle, de nombreuses exigences sont nécessaires. Nous devons prendre en compte de très nombreuses problématiques. Afin de bien comprendre les enjeux d'une telle plateforme de télésurveillance, nous devons lister les challenges que nous devrons relever.

La figure 4.1 résume les dix challenges qui devront être relevés pour qu'une plateforme de télésurveillance soit fonctionnelle, et qui sont ainsi détaillés :

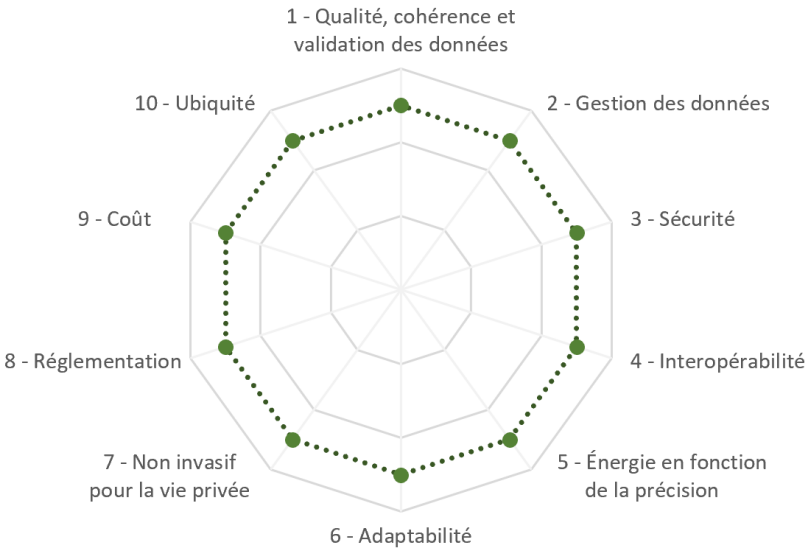


FIGURE 4.1 – Les challenges d'une plateforme de télésurveillance.

1 - Qualité, cohérence et validation des données

Les données générées et collectées jouent un rôle clé dans le processus de soins aux patients. Il est essentiel que la qualité de ces données soit d'un niveau élevé pour s'assurer que les décisions prises reposent sur les meilleures informations possibles.

Les données vitales des patients ne doivent, à terme, pas être fragmentées sur plusieurs nœuds ou dispositifs, mais centralisées afin de ne pas dégrader la qualité des soins en ne disposant pas de toutes les informations connues. Les mesures des capteurs doivent être précises et calibrées, même lorsque les dispositifs sont éteints puis rallumés. Les liaisons sans fil doivent être robustes et fonctionner dans les divers environnements des utilisateurs pour assurer des performances constantes.

L'utilisation des liaisons réseau sans fil non fiables, avec des interférences et des puissances limitées peut entraîner la transmission de données erronées à l'utilisateur final. Il est donc nécessaire que toutes les collectes et transmissions de données soient validées. Des mécanismes de validation de trames, d'acquittement et de retransmission le cas échéants seront indispensables.

2 - Gestion des données

Étant donné que les réseaux de capteurs et la télésurveillance médicale peuvent générer de gros volumes de données, la nécessité de gérer et de maintenir ces ensembles de données est de la plus haute importance. Ces données doivent être centralisées, règlementées, et accessibles par les membres de l'équipe de prise en charge du patient, comme le médecin

traitant, au moyen de services externes de visualisation, d'analyse et de traitement des données.

3 - Sécurité

La confidentialité, l'authentification, la disponibilité, l'intégrité, la traçabilité et l'actualité des données sont des exigences de sécurité sur une plateforme de télésurveillance. Les dispositifs et capteurs portables sont limités en termes de puissance, de mémoire, de débit de communication et de capacité de calcul : les solutions de sécurité proposées pour ces dispositifs et les technologies liées ne sont souvent pas suffisantes pour une utilisation médicale. Nous devrons évaluer les risques, pour chaque acteur, et redéfinir la sécurité, notamment au niveau des échanges de données. La sécurité des objets et dispositifs médicaux en eux-mêmes, par exemple en cas de perte, sera évaluée en fonction de leur certification (marquage réglementaire CE par exemple).

4 - Interopérabilité

La non-interopérabilité entre les composants de l'écosystème est le principal obstacle qui empêche les acteurs du marché de composer des solutions de télésurveillance intégrales. Une interopérabilité sur les dispositifs médicaux est indispensable afin de faciliter et de sécuriser l'intégration de nouveaux modèles de dispositifs et objets connectés de santé (***Plug and Play PnP***), sans devoir réaliser de nouveaux développements. L'utilisation de standards entre les dispositifs émetteurs et récepteurs de données, par exemple sur les protocoles de communication ou les mécanismes d'authentification, nous permet de réaliser cette interopérabilité, mais introduit de nouvelles contraintes comme la limitation des dispositifs compatibles avec ceux-ci.

Une interopérabilité des données au niveau du serveur centralisé est également intéressante. Elle permet de faciliter la communication et le partage d'informations structurées avec d'autres systèmes d'informations des hôpitaux ou encore avec des plateformes de télémédecine.

Une interopérabilité de bout en bout évite la réalisation de silos verticaux de systèmes propriétaires, qui limiterait l'évolutivité d'une telle plateforme, avec de nouvelles perspectives d'intégration par exemple.

5 - Énergie en fonction de la précision

L'économie d'énergie est au cœur des problématiques, et notamment au centre de l'Internet des Objets. Nous avons détaillé, dans le chapitre précédent, la consommation énergétique des réseaux courte ou longue portée en fonction des protocoles de transmission (et des puces). Mais cette problématique se situe également sur les capteurs, les dispositifs et les passerelles locales, avec par exemple la prise de mesure, le décodage de l'information, le chiffrement de sécurité, les mécanismes d'authentification ou encore le stockage de données.

Dans un environnement mobile, les acteurs de la plateforme seront principalement alimentés par des batteries. Une autonomie, la plus conséquente possible, sera de rigueur, allant de plusieurs jours à un objectif de plusieurs mois voire d'années. La récolte d'énergie

(*energy harvesting*), processus par lequel l'énergie est tirée de sources externes (solaire, éolienne, thermique, vibratoire ou encore cinétique) pourrait être une solution pour recharger automatiquement les batteries des objets ne nécessitant que peu d'énergie au quotidien.

Des mécanismes de mise en repos/éveil des appareils, y compris la plateforme locale, peuvent être mis en œuvre. Il faudra, dans ce cas, organiser la synchronisation des échanges et prévoir, en cas de nécessité, des mécanismes pour la bidirectionnalité des messages lorsque les objets sont en repos.

6 - Adaptabilité

Les utilisateurs peuvent avoir besoin de différents niveaux de surveillance. Par exemple la prise de mesure d'un patient atteint de diabète sera d'environ 4 fois par jour, tandis que pour un patient atteint de maladie cardiovasculaire, la prise devra être beaucoup plus régulière. Des compromis sur la régularité des mesures peuvent être trouvés en fonction des besoins. Mais la régularité des mesures peut également évoluer suivant l'état de santé du patient, ou la probabilité de dégradation de ce dernier.

D'une manière générale, une observation plus précise et plus fréquente de l'état de santé du patient se traduit par une consommation d'énergie plus élevée et vice-versa.

7 - Non invasion de la vie privée

L'adhésion massive de la télésurveillance par la population est encore loin d'être acquise et d'entrer dans les mœurs. Une gêne au quotidien, une utilité négligeable ou une menace potentielle pour la liberté sont autant de craintes potentielles pour les patients. L'acceptation sociale est la clé pour que la télésurveillance médicale trouve une application plus large. Cela va de pair avec la nécessité que l'utilisation du dispositif soit transparente pour l'utilisateur. Elle ne doit ni altérer ni gêner les activités quotidiennes de l'utilisateur. Cela se traduit par des capteurs avec une batterie qui dure dans le temps, peu complexes, petits, légers et reconfigurables à distance (afin d'éviter un déplacement inutile). Enfin, le fonctionnement en dehors du domicile est considéré comme un facteur favorisant la transparence d'utilisation pour le patient suivi.

8 - Réglementation

Le serveur de données centralisées doit être sécurisé mais également certifié *Hébergeur de Données de Santé* pour stocker à long terme des données médicales. Les données qui y seront stockées, devront être tracées.

Les données stockées ou utilisées par les capteurs et les dispositifs intermédiaires devront être anonymisées, c'est-à-dire qu'il ne sera pas possible en cas de perte ou de vol de données de remonter jusqu'au patient : les identifiants de dispositifs en fonction des patients pourront être stockés sur le serveur pour répondre à cette contrainte. De plus, ces données transitoires ne devront logiquement pas être stockées indéfiniment sur les dispositifs intermédiaires, mais supprimées une fois transmises au serveur centralisé.

9 - Coût

Les consommateurs, mais également les développeurs de la plateforme, attendent des solutions de surveillance médicale à faible coût, tout en offrant des fonctionnalités élevées. L'utilisation du réseau d'un opérateur téléphonique entraîne des coûts d'abonnement variables selon les opérateurs et les technologies, en plus des coûts des dispositifs médicaux relativement élevés.

Bien qu'une partie de la télémédecine, comme la téléconsultation, soit remboursable par la sécurité sociale, la télésurveillance médicale n'est que peu concernée. Il existe toutefois des prestations remboursables comme les prothèses cardiaques.

10 - Ubiquité

La plateforme devra, pour tous les acteurs, être accessible partout et n'importe quand. C'est un des challenges les plus compliqués à relever. Cela se traduit notamment par la possibilité, pour les capteurs et dispositifs portés par le patient, de transférer des données en mouvement ou non, depuis leur domicile, leur travail ou encore leur voiture à n'importe quel moment de la journée. Et parfois, le transfert doit être effectué depuis un intérieur profond (*deep indoor*) comme l'intérieur d'un grand bâtiment (un sous-sol et un ascenseur dans la mesure de l'acceptable).

La possibilité de transfert, à n'importe quel moment, peut être perturbée par les interférences, ou *l'effet Doppler*[1] par exemple. Il faut prendre cette problématique en compte afin de réduire les interférences et d'augmenter la coexistence des périphériques entre eux sur les réseaux disponibles. L'adaptation de paramètres de transmission est une des possibilités pour réduire les interférences et les effets boules de neige sur les réseaux (ou effets que nous appelons "*Openspace*" qui consistent à parler de plus en plus fort lorsque l'on n'entend plus son voisin, obligeant les autres à parler encore plus fort).

Dans le cas d'une plateforme de télésurveillance, l'ubiquité se traduit également pour les professionnels, par l'accès aux services externes de visualisation, l'analyse et aux traitements des données depuis *n'importe où*, au moyen d'une connexion Internet et d'un ordinateur par exemple.

En prenant en compte l'ensemble de ces challenges, et en se basant sur les connaissances que nous avons étudiées dans l'état de l'art, nous proposons notre nouvelle plateforme de télésurveillance nommée I^{2}PHEN (**I***oT* **I***nteroperable* **P***latform for* **HE***alth mo***N***itoring low power*).

1. décalage de fréquence d'une onde, observé lorsque la distance entre l'émetteur et le récepteur varie au cours du temps.

4.2/ L'ARCHITECTURE DE NOTRE PLATEFORME I²PHEN

Dans un premier temps, nous avons besoin de définir l'architecture globale de la plateforme et les différents acteurs qui entrent en jeu et que nous décrirons dans la suite de ce document.

Cette plateforme utilise les technologies des LPWAN pour les communications longue distance, son architecture est ainsi fortement liée à l'architecture des LPWAN (cf section 3.2.2) que nous avons étudiée dans l'état de l'art. Les acteurs, que nous observons sur la figure 4.2 sont les suivants :

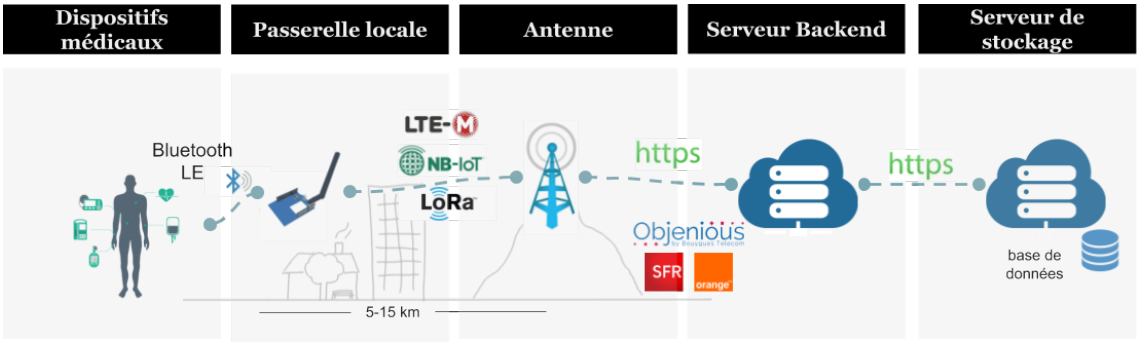


FIGURE 4.2 – La plateforme I²PHEN et ses différents acteurs.

- des nœuds terminaux (*end devices*) : les objets connectés de santé et les dispositifs médicaux qui contiennent des capteurs et des actionneurs. Dans la contrainte d'interopérabilité, de qualité et de validation de données, nous avons décidé de forcer l'utilisation du standard Continua pour les dispositifs médicaux. Nous reviendrons sur ce point dans la section 4.3.1. Toutefois, nous pouvons déjà affirmer que la communication des dispositifs Continua sera réalisée à l'aide des protocoles pris en charge par le standard : USB, Zigbee, Bluetooth et Bluetooth Low Energy, ce dernier étant largement privilégié à l'heure actuelle pour ces appareils.

- une passerelle locale : en l'absence de liaison sans-fil longue distance pour les nœuds terminaux, ceux-ci doivent communiquer localement avec une passerelle locale. La passerelle locale peut être un téléphone portable, ou une carte électronique de type Arduino ou Raspberry Pi par exemple. C'est cette passerelle locale, qui transmettra l'information au serveur médical par l'intermédiaire d'Internet, directement ou indirectement au travers d'antennes relais. La communication avec les antennes relais est réalisée avec les technologies LPWAN que nous avons comparées dans l'état de l'art. Nous avons retenu la technologies LoRaWAN, LTE-M et Nb-Iot.

- une ou plusieurs passerelles distantes (appelées souvent stations de base ou *gateways*) : ce sont les antennes disposées pour couvrir une zone ou un territoire. De par la contrainte de couverture à l'échelle d'un territoire, nous devons utiliser les réseaux privés des opérateurs téléphoniques tels que Objenious, Orange ou SFR.

- un cœur de réseau (ou *serveur backend*) : il sera en charge de traiter les messages qui arrivent des antennes des opérateurs privés. Le cœur de réseau gère l'identification des nœuds (les objets connectés), la sécurité, la duplication de données (lorsque plusieurs antennes captent le même message) ou encore l'envoi de messages descendant vers les objets. Les transmissions descendantes (*downlink* ou DL) sont utilisées, par

exemple, pour signifier à l'objet qu'une mesure a bien été reçue (acquittement), pour envoyer des informations de reconfiguration, ou pour transmettre une commande quand l'objet est un actionneur.

- un serveur de stockage de données médicales : les données transitent du cœur de réseau vers les serveurs applicatifs généralement par des requêtes Http sur Internet.

4.3/ LES ACTEURS DE LA PLATEFORME I²PHEN

Cette section nous permet de décrire chacun des acteurs ainsi que la manière dont ils communiquent entre eux.

4.3.1/ LES DISPOSITIFS MÉDICAUX

Nous avons décidé d'utiliser le standard Continua de la *Personal Connected Health Alliance* pour les dispositifs médicaux utilisés dans la plateforme de télésurveillance. Nous avons montré dans la section 2.2.3 que le standard Continua a pour objectif principal de faciliter et de sécuriser l'intégration de nouveaux modèles de capteurs de santé.

Voici les raisons qui ont guidé ce choix :

- C'est l'unique standard pour la santé connectée reconnu internationalement et soutenu par les institutions européennes (*DG santé* et *DG Connect*) et par l'ONC (*Office of the National Coordinator*) aux États-Unis.
- Avec l'utilisation d'un standard, l'interopérabilité des dispositifs et des données est acquise par défaut. Au contraire, sans l'utilisation d'un standard, l'interopérabilité devient extrêmement difficile. L'interopérabilité sémantique qui est une solution alternative permettrait d'unifier les modèles de données. Cependant, elle serait très difficilement applicable au niveau des dispositifs ainsi qu'au niveau de la gestion d'une utilisation *plug and play*, en plus de la nécessité d'une description fastidieuse de nombreux modèles de données propriétaires. L'utilisation des toolkits *Google Fit* et *Apple HealthKit* serait également possible. Cependant, elle implique une utilisation d'un smartphone, ainsi qu'un stockage des données de santé par ces constructeurs (point négatif bien qu'ils soient maintenant certifiés Hébergeur de Données de Santé et aient de grandes restrictions sur l'utilisation de ces données).
- Les dispositifs certifiés Continua sont testés en laboratoires reconnus par la *Personal Connected Health Alliance* et attestent d'une qualité. Le système d'évaluation de la conformité (*CAS*) de Continua est une méthode complète et rigoureuse pour garantir que les appareils répondent aux exigences fonctionnelles déclarées, avec des preuves pour démontrer l'efficacité des dispositifs et une attestation tierce des résultats des tests.

En outre, les dispositifs non certifiés peuvent être démontrés comme *Continua Compliant* dans un laboratoire de fournisseur à l'aide de l'outil de test Continua (outil gratuit). On peut donc parler de validation des dispositifs, contrairement à l'utilisation d'autres objets connectés de fitness ou de santé non certifiés (ou non marqués CE).

- l'utilisation de Continua renforce la protection, la confidentialité et la sécurité des données. Elle assure un échange sûr et sécurisé des données de santé des patients vers les plateformes de santé, sans intermédiaires tiers : les constructeurs des dispositifs ne stockent pas de données sur un serveur *cloud* privés contrairement à la plupart des autres dispositifs. En outre, les mécanismes de validation de trames, d'acquittement et de retransmission sont gérés par le standard Continua et les différents modes de transport. La confidentialité sera, quant à elle, renforcée par l'anonymisation des données : aucune information relative au patient ne sera stockée ou utilisée lors des communications, ni sur les dispositifs médicaux, ni sur la passerelle.

Le standard Continua possède tout de même quelques inconvénients : il est difficile à mettre en place côté passerelle réceptrice (c'est un point qui sera abordé dans la suite de ce document cf section 4.3.2) et il n'est pas beaucoup utilisé aujourd'hui dans le monde, et particulièrement en France.

D'après le *showcase* de la *PCHA* [Sho20], le nombre de dispositifs certifiés Continua dans la catégorie *Personal Health Device* est de 55 entre 2011 et mai 2020. Parmi ces dispositifs, il y a des lecteurs de glycémie, pompes à insuline, lecteurs de bêta-cétonémie, lecteur de coagulation sanguine, oxymètre de pouls, tensiomètre, thermomètre, balance, centre d'activités / capteur de mouvement, analyseur de composition corporelle, compteur de pas... Les principales marques de dispositifs sont i-SENS, Ascensia, UTECH, Roche Diagnotics, Philips, A & D Medical et Brunel. Ces dispositifs médicaux sont alimentés par des piles ou des batteries rechargeables, dont la durée de vie dépend de l'utilisation et varie de quelques jours à plusieurs mois.

Il existe également une dizaine de modules (microcontrôlers ou cartes électroniques à embarquer) certifiés Continua, qui comprennent la couche transport (BLE principalement) comme le module oxymètre de pouls de RENESAS (figure 4.3).

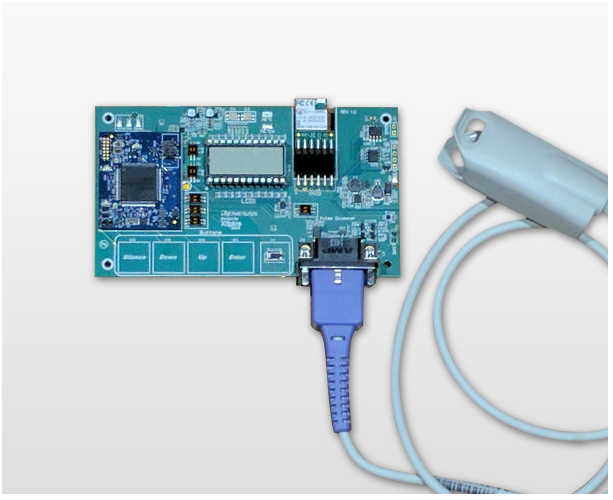


FIGURE 4.3 – Module oxymètre de pouls *RENESAS*.

Pour notre plateforme, nous utilisons le logiciel CESL (*Continua Enabling Software Library*) qui fonctionne sous Windows. Il comprend un simulateur de passerelle de santé personnelle, mais surtout une large gamme de simulateurs d'agent ISO / IEEE 11073 c'est-à-dire les dispositifs médicaux. Nous utilisons le mode de transport BLE des agents pour transférer les données. Pour les ordinateurs qui n'ont pas nativement le BLE, nous utilisons une clé ou *dongle USB CSR 4.0* permettant d'utiliser ce mode. Deux *dongles* sont nécessaires pour effec-

tuer nos tests de transfert entre les dispositifs virtuels et la passerelle virtuelle.

4.3.2/ La passerelle locale

La passerelle locale, ou *gateway*, joue un rôle primordial dans notre plateforme de télésurveillance. Elle échange des informations à la fois avec les dispositifs et le serveur médical, dans le sens montant comme dans le sens descendant. La passerelle locale ne peut pas stocker les informations à long terme. En revanche, elle peut stocker des informations en attente d'envoi.

Nous avons fait le choix de ne pas utiliser de smartphone dans notre plateforme, notamment par le fait que les téléphones portables doivent être rechargés trop régulièrement, et que les personnes les plus susceptibles d'utiliser la télésurveillance, les personnes âgées, n'en possèdent généralement pas (44 % pour les plus de 70 ans).

Nous nous sommes orientés vers les cartes électroniques libres de la marque Arduino. Ce sont des plateformes de prototypage *open source*, composées notamment d'un microcontrôleur permettant de réaliser des objets électroniques. Le modèle que nous avons utilisé pour nos tests est l'Arduino *UNO* (figure 4.4). Nous avons développé les programme en C/C++ avec l'aide du logiciel Eclipse et du plugin Arduino. Celui-ci est plus performant que l'IDE officiel de Arduino pour détecter les erreurs de développement avec une vérification de la syntaxe à chaud et une auto-complétion. Ce dernier est toutefois intéressant avec le *Library Manager* pour rechercher et installer des dépendances, comme la *ArduinoBLE library* que nous avons utilisé pour la gestion du *Bluetooth LE*.

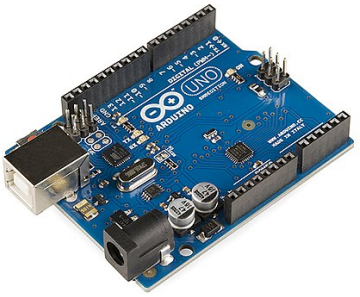


FIGURE 4.4 – *Arduino UNO.*

La carte *Arduino Uno* n'intègre pas, par défaut, la technologie *Bluetooth LE* contrairement à d'autres modèles comme le Arduino *Nano 33 BLE*. Nous avons donc associé, à la carte *Arduino Uno* , un *dongle USB CSR 4.0*, permettant d'utiliser *Bluetooth LE* et d'échanger des messages avec les objets connectés certifiés Continua. Le *Nano 33 BLE* est également intéressant pour sa petite taille de 45*x*18 mm.

FIGURE 4.5 – Dongle USB CSR 4.0.

Communication entre le dispositif et la passerelle locale

L'utilisation du standard Continua entre les dispositifs et la passerelle locale se situe au niveau de l'interface des dispositifs personnels de santé (*Personnal Health Device Interface - PHDI*). Cette interface permet les échanges entre les dispositifs personnels de santé (*Personnal Health Device - PHD*) et la passerelle personnelle de santé (*Personnal Health Gateway -*

PHG) avec le concept d'agents et de gestionnaires. Sur cette interface, c'est la norme IEEE 11073 qui est utilisée. Elle s'exécute au-dessus des protocoles de transport USB, Bluetooth, BLE (*Bluetooth Low Energie*), NFC et ZigBee. Nous retiendrons uniquement le protocole BLE, qui est le plus utilisé sur les dispositifs les plus récents. C'est lui qui assure la confidentialité, l'intégrité et l'authentification des données à travers l'interface des dispositifs de santé personnels et le protocole Bluetooth L directement (au contraire Bluetooth classique qui utilise le protocole d'échange IEEE 11073-20601 et le Health Device Profil).

Le schéma 4.6 représente un envoi standard de données entre un dispositif et la passerelle. Lorsque le dispositif est en veille, celui-ci doit au préalable effectuer une requête d'association (ou de liaison), tandis que la requête de fin d'association permet au dispositif d'y retourner. Si le périphérique n'est pas connu par la passerelle, un processus d'appareillage est nécessaire au préalable. La découverte de service, afin de rechercher les appareils compatibles, est ainsi requise pour tous les appareils Continua *Bluetooth LE*.

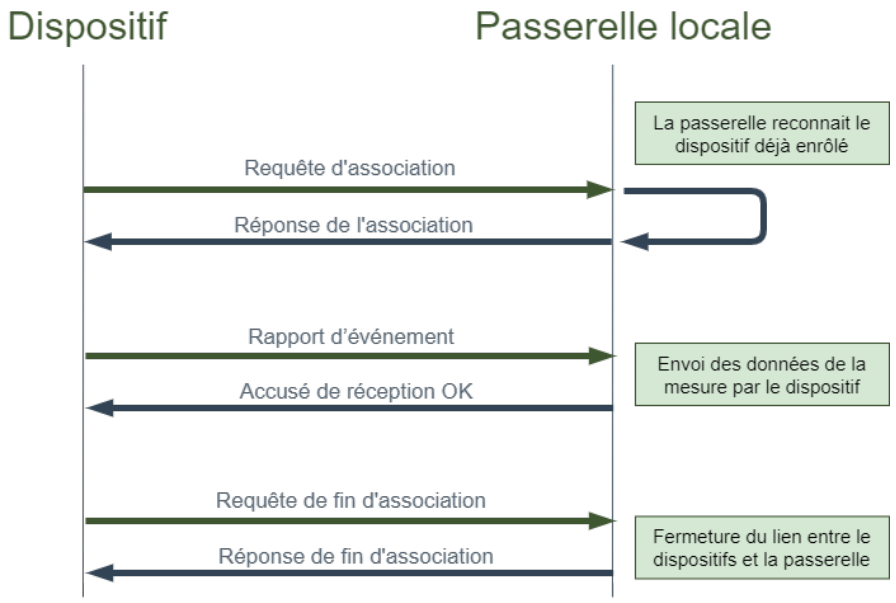


FIGURE 4.6 – Échange de données entre un dispositif et la passerelle locale via ISO-IEEE 11073.

Les données médicales à ce stade sont définies par IEEE 11073-20601 (suivant les différents profils d'utilisation) sous le format de structures de données ASN.1 (*Abstract Syntax Notation One*). Dans le standard Continua, le document technique CDG (*Continua Design Guidelines*) indique que l'interface PHG *Personnal Health Gateway* doit communiquer avec le système d'information HIS (*Health Information Service*) avec HL7 (ou IHE PCD-01) et la couche transport SOAP ou REST. Il faudrait alors effectuer le mapping des attributs ISO-IEEE 11073-20601 vers *FHL7* ou *FHL7 FHIR* (*Fast Healthcare Interoperability Resources*) sur la passerelle locale. Pour des raisons de difficultés techniques, de ressource en mémoire, d'économie d'énergie et puisque de toute manière nous allons utiliser les LPWAN, les données seront conservées en ISO-IEEE 11073-20601 jusqu'au serveur de données. Elles seront ensuite *mappées* sur celui-ci en *FHL7 FHIR*, la version la plus récente de *FHL7* en format de données *JSON*.

Les modes d'utilisation

Dans la problématique d'adaptabilité aux cas d'usages, la passerelle possède trois modes de fonctionnement en fonction des différentes utilisations des dispositifs de santé et de leur degré d'urgence :

- Le mode *ALL+* : la passerelle est en éveil permanent. Elle est donc capable de recevoir des données d'un dispositif de santé connecté en permanence. Nous pouvons ainsi prendre en charge les dispositifs de santé qui monitorent en permanence le patient. Nous obtiendrons dans ce cas un réseau de type MBAN (Medical Body Area Network). La passerelle sera également en mesure de recevoir un message de la passerelle distante à tous moments. La passerelle pourra donc à tous moments demander des mesures au dispositif de santé connecté, les renvoyer en temps réel et recevoir un retour d'analyse par le serveur et/ou l'avis d'un spécialiste. Ce mode de fonctionnement a pour seul désavantage d'être très gourmand en énergie, et par conséquence de ne pas pouvoir fonctionner sur batterie.
- Le mode *ALL-* : Ce mode se base sur le même fonctionnement que *ALL+*, à la différence que le dispositif n'est pas en écoute permanente sur la communication longue distance avec le serveur médical. Cependant, un message sera envoyé toutes les x minutes à la passerelle distante dans le but de recevoir des messages descendants sur une courte fenêtre de temps (cf principe de la classe A de LoRaWAN de la section 3.2.3.1). Ce message pourra également garantir au serveur que la passerelle locale est toujours en place.
- Le mode *MANUEL* : Ce mode entre dans le cadre où le dispositif de santé n'est pas en permanence sur le patient, et les mesures se font manuellement (comme un tensionmètre par exemple). Au moment de la mesure manuelle avec le dispositif de santé, la passerelle devra être réveillée manuellement. Les données de santé pourront alors être transférées à cette dernière qui transmettra à la passerelle distante.

Le choix d'un mode particulier plutôt qu'un autre est lié aux différents cas d'utilisation de la plateforme selon le suivi médical recherché pour le patient. Par exemple, dans le cas d'une prise de glycémie 2 fois par jour par un patient atteint de diabète, il sera judicieux d'utiliser un mode manuel. Dans le cas d'une mesure d'un rythme cardiaque automatique, le mode *ALL+* sera fortement conseillé pour une surveillance en temps réel. En l'absence d'algorithme de détection d'alerte côté serveur, il est impossible d'adapter dynamiquement la fréquence des prises de mesure en fonction de l'état de santé du patient.

Pour le mode *ALL-* et *MANUEL*, la plateforme est alimentée sur batterie, avec une batterie de $9V$ rechargeable, et la possibilité de la laisser sur secteur si le monitoring est constamment au domicile du patient. La passerelle locale est en repos la plupart du temps et consomme très peu d'énergie. La durée de vie de la batterie dépend principalement du nombre de mesures par jour, du protocole de communication longue portée, de la distance à l'antenne la plus proche ou encore de la mobilité quotidienne du patient. La récolte d'énergie (solaire, éolienne, thermique, vibratoire ou encore cinétique) ne sera pas utilisée dans cette première version.

Dans un souci *d'awareness* (prise de conscience), la passerelle locale est dotée d'une LED multicouleurs : orange lors du transfert longue distance et verte pendant quelques secondes

une fois l'accusé de réception reçu, la LED deviendra rouge en cas de problème de connectivité.

Communication entre la passerelle locale et le serveur médical

Nous avons retenu des technologies LoRaWAN et LTE-M/Nb-IoT pour la communication entre la passerelle locale et le serveur de stockage de données médicales. Ces deux technologies différentes entraînent des conceptions différentes pour cette étape. Nous allons décrire les deux possibilités séparément.

4.3.2.1/ UTILISATION DE LORAWAN

Pour utiliser LoRaWAN, nous avons choisi un module *Dragino LoRa Shield* qui est un émetteur-récepteur longue portée compatible avec les *Arduino UNO*. Il est basé sur une bibliothèque open source. Le *LoRa Shield* comprend une puce Semtech SX1276, un émetteur à spectre étendu à faible consommation d'énergie permettant d'envoyer des messages LoRa sur la bande la bande 868 MHz. La puce possède les caractéristiques suivantes (description par Semtech) :

- un bilan de liaison maximal de 168 dB,
- une sensibilité jusqu'à -148 dBm,
- une puissance d'émission jusqu'à +20 dBm (maximale de +14dBm autorisée en Europe),
- une consommation de 10,3 mA en réception, et de 200 ηA en repos,
- une prise en charge des modulations FSK, GFSK, MSK, GMSK, LoRaTM et OOK,
- un débit binaire jusqu'à 300 kbps.

Nous avons utilisé la bibliothèque *arduino-LMIC* issue de IBM LMIC (*LoraMAC-in-C*), légèrement modifiée pour fonctionner dans l'environnement Arduino et permettant d'utiliser le transpondeur *SX1276*. Cette bibliothèque permet d'envoyer et de recevoir des messages LoRa à n'importe quel cœur de réseau avec les avantages du protocole LoRaMAC.

La figure 4.7 présente la passerelle locale constituée du module *LoRa Shield* de Dragino (en rouge) et de son antenne, montés sur un Arduino UNO (en bleu), et relié à un capteur de température/humidité DHT11 et une LED multicouleurs.

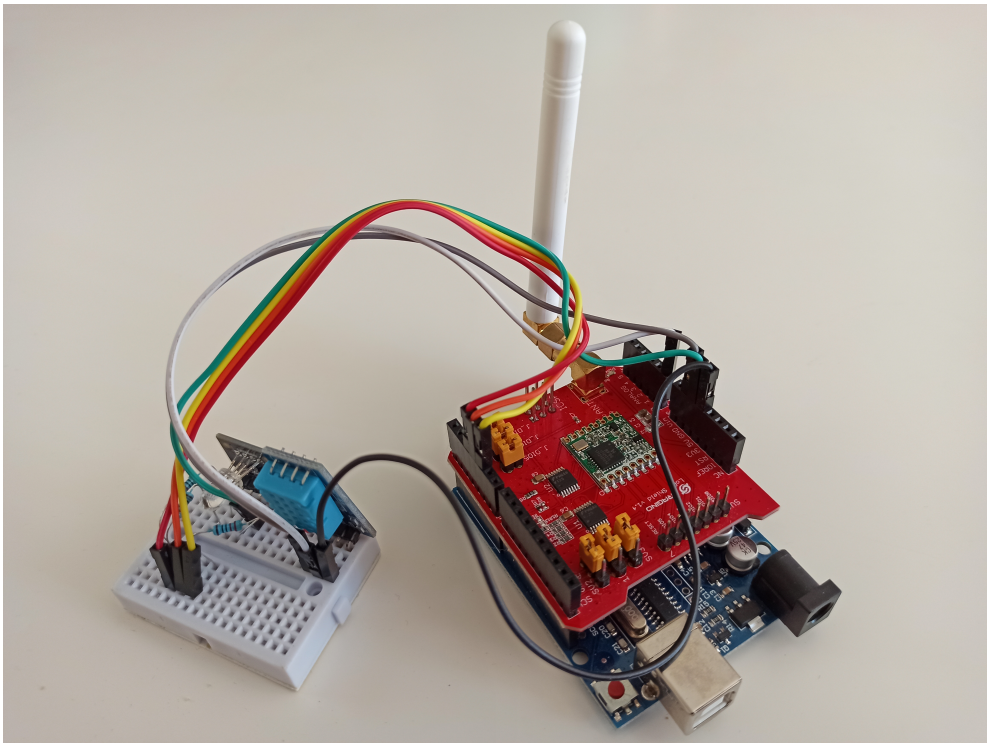


FIGURE 4.7 – Module *Dragino LoRa* monté sur un *Arduino Uno*.

Nous avons choisi d'utiliser le réseau LoRa mis à disposition par *Objenious* (filiale de Bouygues Telecoms), qui est le réseau ayant la plus grande couverture à l'heure actuelle avec de nombreuses antennes disposées sur l'ensemble du territoire Français. Le cœur de réseau, représenté par la plateforme *SPOT*, est une interface web sur laquelle sont déclarés les capteurs LoRa (notre passerelle locale dans notre cas). Elle offre la possibilité de gérer la flotte, à l'échelle d'un projet ou d'une application par exemple, avec entre autres :

- L'ajout ou la suppression de capteurs LoRa : ceux-ci seront ajoutés sur le cœur de réseau par nos soins en fonction des clés *AppEUI, AppKey et DevEUI. AppEUI* sera l'identifiant de l'application commune aux différentes passerelles locales, tandis que *DevEUI* permettra d'identifier la passerelle. La clé *AppKey* permettra quant à elle de sécuriser la transaction avec la génération des clés de sessions à la volée (mode *OTAA*). L'envoi de données, sera donc toujours précédé par une procédure de *JOIN* pour l'échange des clés. Les données seront également chiffrées à nouveau, au niveau de la passerelle, avec une clé AES 128 bits. La vérification de trame côté cœur de réseau permettra quant à elle d'assurer l'intégrité des données (le fait que les données ne subissent pas d'altération ou destruction).

- L'envoi des messages descendants (*downlink*) et accusés de réception. Le cœur de réseau gère les différentes classes LoRaWAN (A, B et C). Les messages descendants peuvent être initiés par un serveur tiers via *l'API REST* exposée par la plateforme *SPOT*. Les messages descendants seront stockés sur le cœur de réseau jusqu'à la détection d'une fenêtre de réception pour le dispositif.

- Le routage des paquets en temps réel vers un serveur tiers, à l'aide de requêtes *HTTP, AZURE, Google, Aws ou MQTT*. Nous utilisons les requêtes HTTP sécurisées avec un

certificat. Les informations du RSSI (*Received Signal Strength Indicator*), du signal, du bruit, et du SNR (*Signal on Noise*) seront également transmises lors du routage. Ces informations sont mesurées par les antennes lors des réceptions de messages.

- D'autres fonctionnalités comme le déchiffrage (avec des codecs), la visualisation des paquets LoRa ou la configuration d'alertes en fonction des données et des statuts des capteurs (capteur inactif par exemple) que nous n'utiliserons pas à ce niveau car les données seront chiffrées.

La consommation liée au transfert de données sera largement réduite avec la solution LoRaWAN et son algorithme ADR (*Adaptive Data Rate*) pour l'adaptation des paramètres de transmission (section 3.2.3.1). L'algorithme permet d'augmenter le *Spreading Factor* et de réduire la puissance d'émission *TX* au fur et à mesure des échanges afin de réduire la consommation énergétique lorsque les conditions environnementales le permettent. Dans le cas de mobilités quotidiennes, qui peuvent être un facteur important de consommation énergétique, l'algorithme ADR ne peut pas être utilisé. Nous avons alors mis en place l'algorithme *COMMA* (**C***ommunication* **O***ptimisation* **M***echanism for* **M***obility* **A***daptation* auquel le chapitre 5 est consacré) pour les patients considérés comme actifs (au moins 5 déplacements par semaine), afin de réduire la consommation énergétique en cas de mobilités quotidiennes.

La disponibilité de la plateforme dépendra en grande partie de la disponibilité des réseaux LPWAN. Il est nécessaire d'activer l'option d'acquittements sur le cœur de réseau *Objenious* afin d'être certain que le message soit transmis jusqu'à lui. En cas de problème, et si le message d'acquittement n'arrive pas jusqu'au dispositif, nous avons mis en place une procédure de retransmission du message : jusqu'à que la connectivité soit retrouvée, le message est retransmis avec des intervalles de 1, 2, 5, 10, 30 puis 60 minutes. Les intervalles s'espacent au fur et à mesure afin de ne pas consommer toute l'énergie restante si le dispositif est hors connexion.

Pour finir, le coût des abonnements LoRa avec la plateforme Objenious est relativement faible. Il est, pour l'offre de base, à 20 euros par an et par capteur (notre passerelle locale), mais négociable avec l'opérateur en fonction du nombre de capteurs.

4.3.2.2/ Utilisation de LTE-M et Nb-IoT

Pour des applications nécessitant une qualité de service (QoS) plus forte, comme un suivi critique des paramètres vitaux des patients, la qualité de service est nécessaire. Les technologies cellulaires *LTE-M* et *Nb-IoT* offrent, en utilisant des bandes de fréquences propriétaires, une QoS supérieure à LoRa, avec un débit plus important, et une latence plus faible (section 3.2.4). Ils sont également une solution plus intéressante pour une meilleure pénétration dans les bâtiments.

Nous avons choisi le module *dragino Nb-IoT Shield QG96* (figure 4.8), compatible avec l'arduino UNO, pour la communication cellulaire. Il prend en charge les multibandes pour NB-IoT, mais il est également compatible avec LTE-M. Il contient une puce *Quectel BG96* et un emplacement pour carte micro SIM. Cette dernière est fournie par les opérateurs téléphoniques correspondants (Orange et SFR en France).

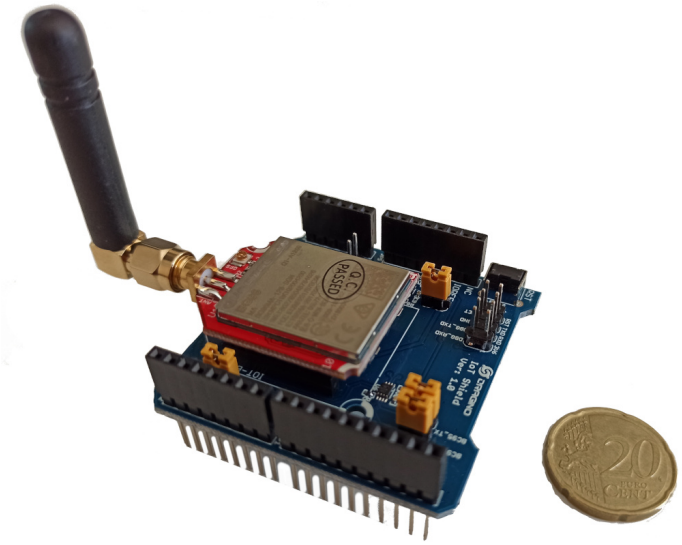


FIGURE 4.8 – Module *Dragino LTE-M* et *Nb-Iot* pour *Arduino Uno*.

L'utilisation des cœurs de réseaux de ces opérateurs pour la gestion des capteurs est possible. Cependant, ces technologies permettent également une connectivité directe avec Internet, et nous laissent la possibilité de requêter directement notre serveur médical via son adresse IP. L'envoi de données consiste à *mapper* les ports 10 et 11 du module *Quectel* avec la librairie native *SoftwareSerial* puis d'envoyer des commandes en mode texte en précisant le contenu des messages ainsi que l'adresse IP et le port cible.

La consommation énergétique sera en revanche, plus importante que la solution avec LoRaWAN. Une synchronisation régulière pour la technologie *Nb-IoT* et l'envoi de données plus consommateur avec *LTE-M* (malgré le *Power Saving Mode*) feront chuter la durée de vie des batteries : environ 3 à 6 mois avec 1 message par jour, contre 1-2 ans pour LoRaWAN en bonne condition.

4.3.3/ LE SERVEUR DE STOCKAGE

Le serveur de stockage d'I²PHEN concerne des données de santé, et doit être conforme aux directives propres aux pays (en France certification HDS de l'ASIP Santé *Agence des Systèmes d'Informations Partagés en Santé*). C'est lui qui stockera, en relation directe avec une base de données locale, l'ensemble des données de santé des patients suivis par les dispositifs de télésurveillance. Les données ne seront donc pas fragmentées pour l'analyse afin d'éviter les erreurs d'interprétation par manque de données. Nous avons donc retenu la société française OVH qui possède la certification HDS et offre des solutions basées sur le système d'exploitation *centOS* sur lequel notre système pourra stocker les données et héberger les services du serveur médical.

Le serveur médical de la plateforme I²PHEN est basé sur une architecture micro-service et développé en Java. La base de données associée est une base *elasticSearch*. C'est une base de données non relationnelle (*noSQL*) qui stocke l'information sous forme de fiches en format *JSON*, et qui permet de créer de puissants index de recherche pour améliorer la visualisation de gros volumes de données. Pour visualiser les données dans une interface graphique, nous utilisons l'application web *Grafana* reliée à la base de données *elasticSearch*. Les données sont visibles sous forme de graphiques et de tableaux, et organisées dans des tableaux de

bord (*dashboards*). Cela nous donne une vue d'ensemble des informations remontées par les capteurs ainsi que la possibilité de générer des statistiques. La figure 4.9 montre un exemple de graphiques présentant la température remontée par tous les acteurs de la plateforme, et ce sur une période de quelques heures. La figure 4.10 nous montre, sur cette même période, les informations relatives à la qualité du signal (RSSI, bruit et SNR) mesurées par les antennes et le cœur de réseau. Ces dernières informations nous serviront dans le chapitre 5 à estimer la qualité de la liaison.

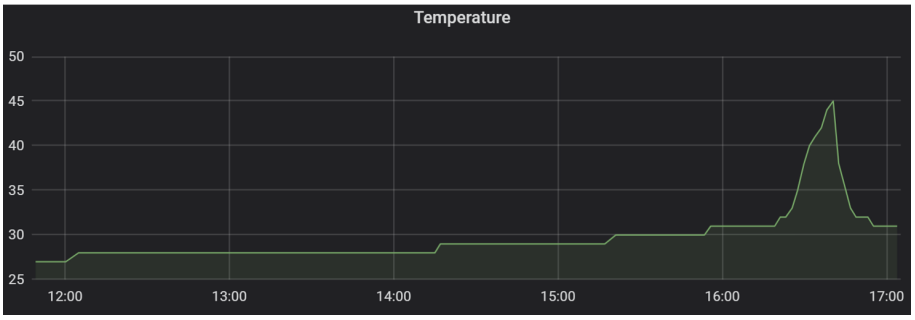


FIGURE 4.9 – Visualisation des données de température d'un capteur sur *Graphana*.

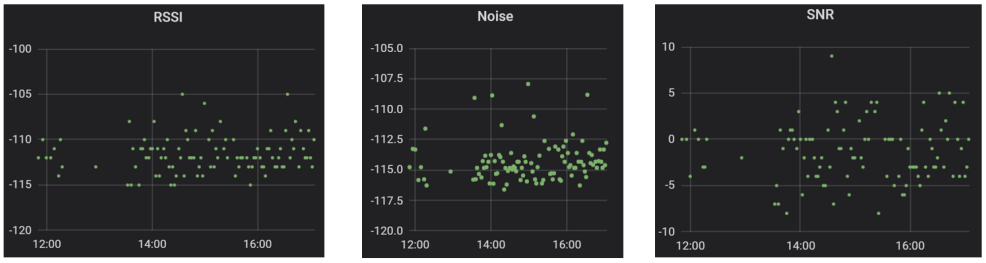


FIGURE 4.10 – Visualisation des données du RSSI, bruit et SNR mesurées par les antennes et le cœur de réseau.

Toutefois, l'application n'est en aucun cas un moyen d'administrer des dispositifs de santé ou de gérer les équipes de prise en charge des patients. Pour effectuer ces tâches, un service de e-Santé basé sur les parcours des patients et le suivi de maladies chroniques doit être associé. L'intégration, ou l'association, d'un tel service sera simplifiée par l'interopérabilité mise en place sur les données. Les données arrivant sous le format standardisé défini dans IEEE 11073-20601, il est nécessaire pour nous de mettre en place un *mapping* vers le format de données *HL7 FHIR*. Ce dernier est le standard de données défini au niveau de l'interface de service par la *PCHA*. La librairie *Hapifhir* possède tous les objets *FHIR* en Java afin de simplifier la manipulation.

Dans le cas où le cœur de réseau gère la redondance de données de son côté, et si plusieurs antennes interceptent le même message envoyé, comme c'est le cas avec Objenious ou encore Orange, il n'est pas nécessaire de gérer à nouveau la redondance. Il faut cependant mettre en place les services pour récupérer les données sur un serveur médical. Ces données seront retransmises par le cœur de réseau. Nous avons mis en place une *API REST* basée sur HTTP et un *endpoint POST*. Elle permet également de récupérer des données depuis l'extérieur pour les applications qui viendront s'interfacer. L'API est réalisée avec l'aide de *Swagger* pour documenter les points d'entrées, de *Grizzly* pour l'exposition de ceux-ci avec une serveur HTTP et de *Jersey* pour la sérialisation des données au format *JSON*.

4.4/ COMMUNICATION SÉCURISÉE DE BOUT EN BOUT

La communication entre les différents acteurs et par les différents protocoles de communication est sécurisée de bout en bout sur la plateforme I^{2}PHEN. La figure 4.11 expose la sécurité à chaque niveau de la communication.

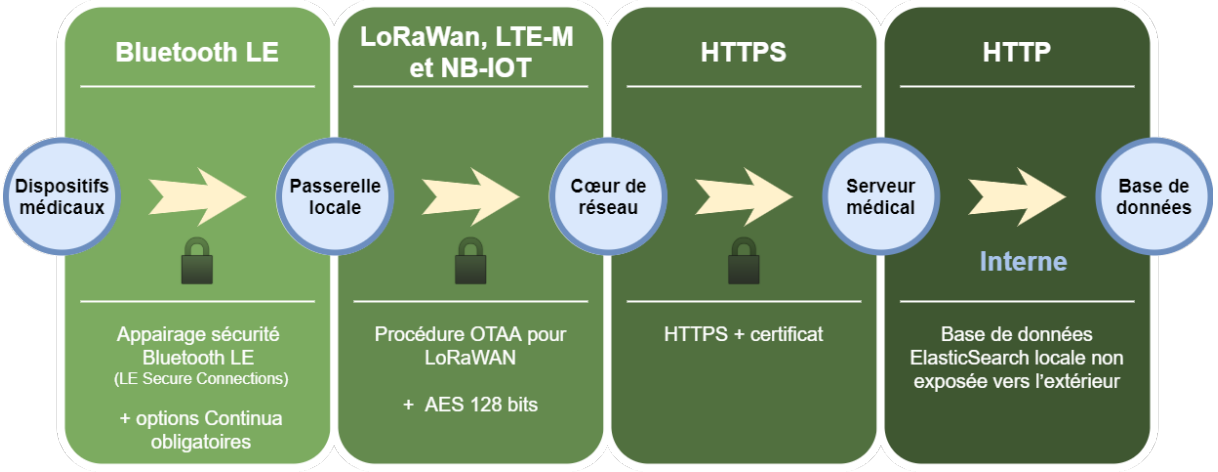


FIGURE 4.11 – La communication sécurisée de bout en bout entre les différents acteurs.

La connexion *Bluetooth LE*, établie entre les dispositifs et la passerelle locale, est sécurisée selon le standard Continua. Ce dernier impose l'utilisation au minimum de la version 4.2 du BLE, dotée d'une sécurité grandement améliorée (*LE Secure Connections*). Alors que dans *BLE*, il existe diverses options d'authentification, Continua propose des exigences plus strictes en matière de sécurité, d'authentification et de confidentialité :

- la possibilité de prendre en charge les fonctionnalités de sécurité du profil *Bluetooth LE* appropriées au type de périphérique. C'est le service, dans notre cas sur la passerelle locale, qui dicte les fonctionnalités que le dispositif devra suivre. Parmi ces fonctionnalités, il y a :
  - L'échange d'une clé secrète obtenue hors bande : les clés publiques sont échangées à l'aide d'une technologie sans fil différente comme le *NFC* (communication en champ proche, *Near Field Communication*). Ces clés sont utilisées pour créer une clé à court terme (STK, *SIM Application Toolkit*) qui servira à chiffrer la connexion. Si le canal de communication hors bande est protégé contre les attaques *MITM* (*Man In The Middle*), alors la connexion BLE est également protégée contre les attaques *MITM*. Ces attaques se produisent lorsqu'un troisième appareil malveillant usurpe l'identité des deux autres afin qu'ils se connectent à lui. Il pourra alors intercepter les communications sans que les autres appareils puissent le voir. Dans notre cas, n'ayant pas de second modèle de communication local, nous n'utiliserons pas cette fonctionnalité dans la première version de la plateforme.
  - L'authentification *Just Work* (version 4.2) : après l'échange de clés publiques, chacun des périphériques génère, puis envoie à l'autre, une valeur de confirmation *Cb* générée elle-même à partir d'un *nonce* commun (nombre arbitraire unique). Si les valeurs de confirmation correspondent, la connexion se poursuit. Bien

que cette méthode ne permette pas à l'utilisateur de vérifier l'authenticité de la connexion et de résister aux attaques *MITM*, celle-ci a une résilience nettement plus élevée à l'écoute passive que dans les précédentes versions.

- La prise en charge du modèle d'association par code PIN à 6 chiffres, entré dans chacun des appareils. Ce mot de passe est utilisé, avec les clés publiques échangées précédemment et un *nonce* de 128 bits pour authentifier la connexion. Cette méthode de clé d'accès, disponible uniquement en version 4.2, permet une résistance aux attaques *MITM* beaucoup plus importante que dans les versions inférieures.
- La comparaison numérique : à la fin de l'authentification *Just Work*, les deux appareils génèrent et affichent indépendamment une valeur de confirmation finale à 6 chiffres (générée à partir des deux *nonce* créés sur chaque dispositif). L'utilisateur doit ensuite vérifier que les valeurs correspondent afin d'accepter la connexion. Dans la première version, nous n'utiliserons pas non plus cette fonctionnalité difficile à mettre à place.

- La modification aléatoire de l'adresse *MAC* du périphérique pour éviter qu'un utilisateur soit suivi (confidentialité de la couche de liaison). Cela réduit grandement les possibilités d'attaques de suivi d'identité : le risque qu'une entité malveillante soit capable d'associer l'adresse d'un périphérique BLE à un utilisateur spécifique, et de le suivre physiquement par la présence du périphérique BLE.

Au niveau de la communication LoRa entre la passerelle locale et les antennes, nous utilisons la procédure d'activation *OTAA (Over the Air)* définie par LoRAWAN. Elle est basée sur les clés d'identification (*DevEUI et AppEui*) attribuées et stockées dans l'appareil ainsi que la clé *AES* de sécurité (*AppKey*) de 128 bits.

Les appareils exécutent d'abord une procédure de jointure avec le réseau, au cours de laquelle un *DevAddr* dynamique est attribué. L'appareil utilise ensuite la réponse de jointure pour dériver les clés de session *NwkSKey et AppSKey* à partir de la clé *AppKey*. Celles-ci seront utilisées par l'appareil pour chiffrer les données tout au long du trajet, d'abord par la clé de session réseau (*NwkSKey*), puis avec la clé de session d'application (*AppSKey*). Le chiffrement des données permet d'assurer que le paquet ne peut pas être lu ou modifié au cours du trajet : si le paquet n'est pas déchiffrable au niveau du serveur il sera rejeté. De plus, puisque les clés de chiffrement *NwkSKey et AppSKey* sont générées au niveau de l'objet (avec la réponse de jointure), elles ne circulent à aucun moment sur le réseau. Elles ne peuvent donc pas être interceptées par une entité malveillante qui se servirait de celles-ci pour envoyer de faux paquets par exemple.

L'appareil peut stocker ces clés et continuer à les utiliser pour communiquer jusqu'à ce qu'elles soient perdues ou que le réseau ait choisi de les placer comme expirées. Afin d'assurer la meilleure sécurité sur la plateforme, notre dispositif ne conservera pas les clés *NwkSKey et AppSKey* entre chaque envoi. Il se reconnectera et génèrera de nouvelles clés à chaque nouvel envoi.

Au final, la procédure d'activation à la volée *OTAA* est le meilleur moyen d'obtenir une connexion sécurisée permettant d'éviter les attaques de type *MITM* ou l'écoute passive des paquets. Elle est surtout plus sécurisée que la seconde procédure d'échange ABP (*Activation By Personalisation*) qui utilise directement les clés de session *NwkSKey et AppSKey* préprogrammées dans l'appareil.

Par ailleurs, puisque la plateforme utilise le réseau d'un opérateur privé dans la communication, il semble important que celui-ci ne puisse pas avoir accès aux données médicales qui transitent. Un chiffrement supplémentaire programmé est mis en place sur le message (*paylaod*) par une clé ***AES*** de 128 bits, partagée uniquement entre la passerelle locale et le serveur médical. Les données seront ainsi indéchiffrables au niveau du cœur de réseau et non interprétables par celui-ci.

Pour finir, le cœur de réseau et le serveur IoT communiquent par requêtes HTTPS (***HyperText Transfer Protocol Secure***) chiffrées (couche de chiffrement SSL et TLS), auxquelles s'ajoute un certificat partagé au format ***PEM*** entre ces deux acteurs. Ce dernier garantit la légitimité de l'émetteur en chiffrant toutes les données transmises. Les entités extérieures ne pourront donc pas interroger l'API ***RESTFul*** du serveur médical sans certificat valide pour envoyer ou récupérer des données.

Synthèse du chapitre 4

SYNTHÈSE

Dans cette section nous avons défini notre nouvelle plateforme de télésurveillance médicale I²PHEN (**I***oT* **I***nteroperable* **P***latform for* **HE***alth mo***N***itoring low power*).

Nous avons, dans un premier temps, synthétisé nos besoins avec l'élaboration des exigences fonctionnelles d'une plateforme de télésurveillance en 10 points : la qualité, cohérence et validation des données, la gestion des données, la sécurité, l'interopérabilité, la consommation d'énergie en fonction de la précision, l'adaptabilité, la non-invasion de la vie privée, la réglementation, le coût et pour terminer l'ubiquité.

Nous avons ainsi introduit l'architecture de I²PHEN, puis nous avons décrit chacun des acteurs impliqués (les dispositifs médicaux, la passerelle locale, les cœurs de réseau et le serveur médical).

Chacun des choix technologiques a été justifié, tel que l'utilisation du standard Continua et des LPWAN (LoRaWAN, LTE-M et NB-IoT), puis les différentes fonctionnalités implémentées pour répondre aux besoins d'une telle plateforme ont été détaillées : les différents modes d'utilisation, les acquittements et les procédures de retransmissions, l'utilisation d'ADR ...

Pour finir, nous avons consacré une section à la sécurité lors des échanges entre les acteurs.

Le chapitre suivant est consacré à notre protocole ***COMMA*** sur une base de l'algorithme ADR utilisé pour l'adaptation des paramètres dans la technologie LoRaWAN. Notre objectif est de proposer une adaptation qui permette un fonctionnement de l'algorithme ADR dans notre cas spécifique de mobilité quotidienne d'un individu.

5

COMMA : Communication Optimisation Mechanism for Mobility Adaptation

Comme nous l'avons détaillé au cours de la section 3.2.3.1, l'algorithme *ADR*, tel que défini dans la littérature, permet une économie d'énergie significative dans des systèmes statiques avec un environnement relativement stable.

Cependant, dans le cadre d'une utilisation quotidienne par une personne active et mobile, nous constatons que la mobilité est relative : les individus se déplacent régulièrement, mais passent la plupart de leur temps dans des environnements statiques et connus. Par exemple, une personne *lambda* passera la plupart de son temps à la maison, puis au travail. L'utilisation de l'algorithme *ADR* dans la mobilité quotidienne est donc possible. Toutefois, une adaptation sur chaque lieu de vie et tous les jours représente :

- une perte d'énergie lorsque l'on transmet des paquets en condition sur-optimisée,
- un risque de perte de paquets, et donc de retransmission et de surconsommation, en condition sous-optimisée, le temps que les paramètres de communications soient augmentés pour atteindre l'antenne (dans ce cas, si le dispositif s'attend à recevoir un *ACK*, il peut implémenter tout de même une procédure de retransmission, avec diminution du *Spreading Factor* pour retrouver la connectivité).

Les travaux sur *E-ADR* [Ben19] permettent d'améliorer l'adaptation des paramètres de communication dans un cadre de mobilité continue en se basant sur les prédictions. Mais cela ne correspond pas du tout à nos besoins en mobilité quotidienne.

Nous proposons dans ce chapitre, un mécanisme d'adaptation rapide des paramètres de communication dans le cas de mobilités quotidiennes, avec des changements brusques d'environnement provoqués par des déplacements, et des temps de stabilisation des paramètres dans des lieux connus ou inconnus. Il fonctionnera en complément de l'algorithme *ADR* pour stabiliser les paramètres sur chaque lieu.

5.1/ Le concept de l'algorithme

Le principe de l'adaptation et de l'amélioration, que nous présentons, repose sur une condition importante, la mobilité quotidienne. Entre les déplacements d'un individu au cours

de sa journée, les conditions minimales qui doivent être retrouvées sur chaque lieu sont les suivantes :

- Un environnement statique c'est-à-dire que les conditions doivent être relativement stables pour utiliser l'algorithme *ADR* normalement,
- Un environnement connu c'est-à-dire que le lieu a déjà été visité par l'individu dans l'utilisation de l'algorithme, ou que celui-ci est resté assez de temps pour avoir un historique des communications (20 historiques recommandés). Chaque environnement connu est défini par une aire, représentée par un positionnement moyen dans l'espace (une géolocalisation) et un rayon de limitation (figure 5.1).
- L'appareil doit écouter les messages de liaison descendante après chaque transmission, ce qui correspond aux classes A, B et C. Il est donc préférable d'utiliser autant que possible la classe A qui est la moins gourmande en énergie.

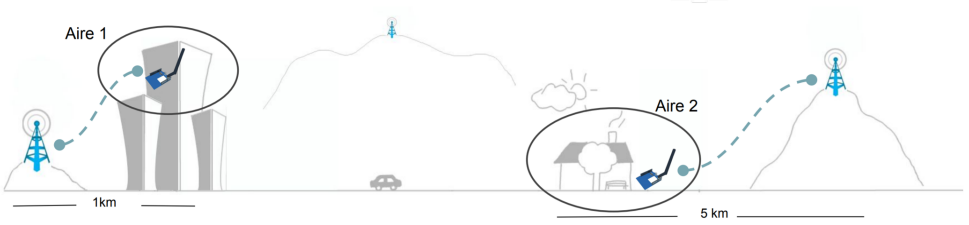


FIGURE 5.1 – Les aires en fonction du lieu dans l'algorithme COMMA.

L'originalité proposée est basée sur une utilisation des différents historiques de communication des aires, dans le but de trouver une adaptation plus rapide des paramètres optimaux de communication. Pour réaliser une adaptation rapide en fonction de l'environnement dans lequel l'objet se situe, les étapes suivantes sont nécessaires :

- Conservation des différents historiques de communication pour les différents environnements rencontrés par l'objet,
- Détection des changements d'environnement ou des déplacements de l'objet qui nécessiteraient une adaptation rapide des paramètres de communication,
- Association d'un environnement à un des historiques de communication enregistrés, ou définition d'une nouvelle aire et d'un nouvel historique.

Nous détaillons ces problématiques dans les sections suivantes. Le schéma 5.2 représente la suite logique de notre protocole.

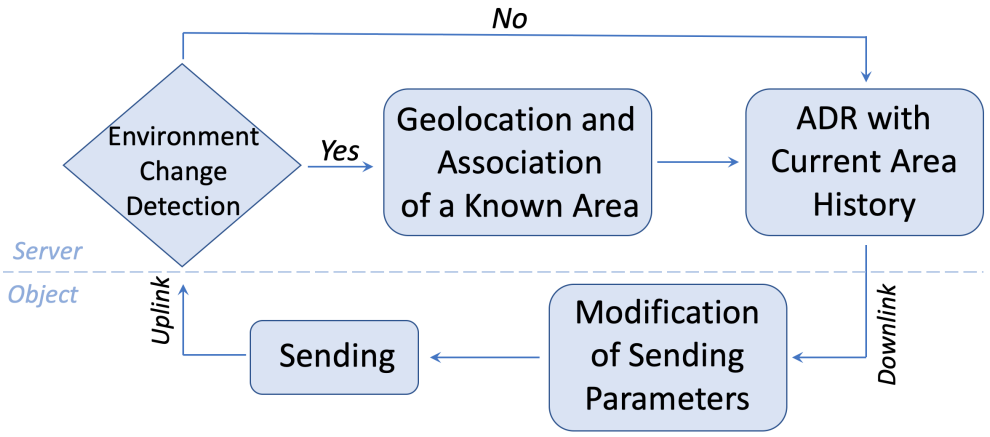


FIGURE 5.2 – Étapes de l'algorithme COMMA.

5.2/ LA DÉTECTION D'UN CHANGEMENT D'ENVIRONNEMENT

La détection d'un changement d'environnement est réalisée à la fois au niveau du serveur et du périphérique.

Lorsque le périphérique ne reçoit pas le message de confirmation de réception du serveur, cela signifie que le message montant ou que le message de confirmation (*ACK*) n'est jamais arrivé. Cela peut se produire dans le cas d'une interférence, ou si le périphérique est en condition d'envoi sous-optimal : par exemple, lors d'un éloignement du périphérique avec la passerelle distante la plus proche. Dans ce cas, le périphérique pourra alors modifier ses paramètres de transmission pas à pas (*TX* puis *DR*) jusqu'à retrouver la connectivité.

Le problème est que, dans le cas d'un dispositif de santé connecté et d'une urgence potentielle, il est important que l'objet ne soit pas hors connexion trop longtemps. Les retransmissions se font avec un certain temps de latence, et ne peuvent avoir lieu que toutes les minutes environ. Il est donc important, pour nous, d'utiliser un mécanisme pour retrouver rapidement la connectivité avec le serveur. Nous utiliserons donc la puissance maximale et le *DR* minimum pour maximiser les chances que le message puisse atteindre une passerelle distante. L'envoi d'un message avec des paramètres non-optimaux permettra probablement d'atteindre plusieurs passerelles distantes. Le serveur pourra alors géolocaliser le périphérique et associer un environnement.

D'autre part, nous devons détecter également les changements d'environnement lorsque l'environnement s'améliore pour l'objet, par exemple lorsqu'il se rapproche de la passerelle. Cette fois, la détection ne se fera pas du côté de l'objet, qui arrive toujours à envoyer les messages et à recevoir les *ACK*, mais du côté du serveur. Si la différence entre les *SNR* (*Signal to Noise Ratio*) des nouveaux et des anciens messages est trop élevée, nous pouvons en déduire qu'il y a eu un changement d'environnement. Nous utilisons le SNR_{dif} qui est la différence entre le *SNR* minimal et le *SNR* maximal enregistrée sur les 30 dernières minutes.

Si $SNR_{dif} > 5$, nous considérons que cela est le signe d'une rupture d'environnement. Dans ce cas, le serveur enverra dans le prochain message de confirmation de réception une demande de géolocalisation. Cela permettra de procéder ensuite à une tentative d'association d'environnement.

5.3/ L'ASSOCIATION D'ENVIRONNEMENT

La fonction d'association d'environnements connus peut s'effectuer de différentes manières. Nous avons choisi de retenir comme critère principal la géolocalisation.

Actuellement, ce sont les récepteurs GPS associés à un réseau GSM qui sont les plus utilisés pour effectuer la géolocalisation d'un objet. Il existe actuellement sur le marché des récepteurs GPS à des prix abordables, mais le principal problème est la consommation énergétique et la durée de vie des batteries. La consommation d'un récepteur GPS est d'environ 30 à 50 mA, ce qui représente un besoin en énergie considérable pour la plupart des appareils IoT à faible consommation. Par exemple, un module LoRaWAN fonctionnant dans une bande de fréquences de $868\,MHz$ consomme $2,8\,mA$, à l'état activé, des données de transmission de $38,9\,mA$ et des données de réception de $14,2\,mA$ [Lib16].

Il existe également une solution sans GPS utilisant un accéléromètre et une boussole [Zhu13]. Cependant, l'erreur se cumule dans le temps, et nous ne pourrons pas distinguer le même lieu visité à deux moments différents.

Il existe plusieurs techniques permettant d'estimer la position d'un appareil. Chacune de ces techniques présente des caractéristiques et des pré-requis différents. Les trois méthodes les plus couramment utilisées pour réaliser la géolocalisation sont la triangulation, la trilatération et la multilatération. En l'absence d'une synchronisation temporelle entre les passerelles et les périphériques, la seule méthode utilisable avec LoRaWAN est la multilatération : l'emplacement est calculé avec la différence d'heure d'arrivée $TDOA$ (*Time Difference Of Arrival*) [Pod18] [Bak17] sur les antennes. Un minimum de 3 antennes atteignables par l'objet et synchronisées temporellement entre elles est donc requis.

La tâche d'association d'environnement de l'objet sera réalisée sur le serveur, qui conserve les historiques des communications sur les différentes aires rencontrées. Chaque aire sera définie sur le serveur par un seul point $AREA_{POS}$, qui sera la moyenne des 20 dernières positions des messages associés à celle-ci. Pour associer une géolocalisation à une aire, nous définissons $RADIUS$, soit la distance maximale entre le point nouvellement calculé et le point moyen de l'aire pour effectuer une association.

Si la distance entre les deux points est supérieure à $RADIUS$, le nouveau point formera une nouvelle aire. Il a été montré [Pod18] que la géolocalisation LoRaWAN n'est pas réellement précise. Pour des nœuds stationnaires, la précision moyenne est évaluée à environ 100 m en atteignant 4 antennes. La géolocalisation avec LoRa n'est donc pas très précise, mais suffisamment pour distinguer les différents lieux (maison, travail...). Il sera donc nécessaire de prendre un $RADIUS$ suffisamment grand.

Lorsqu'une aire déjà existante est retrouvée après une détection de changement d'environnement, le meilleur couple DR et TX sur les 20 dernières communications sera envoyé au périphérique comme nouveau paramétrage à utiliser. Sans nouvelle rupture d'environnement, l'algorithme ADR sera de nouveau utilisé pour faire varier les paramètres de communication dans l'environnement statique.

Dans le cas où la requête de géolocalisation ne permet pas d'atteindre 3 antennes, la géolocalisation ne peut pas avoir lieu. Nous appliquerons l'algorithme ADR classique pour stabiliser pas à pas les paramètres de communication.

L'algorithme 2 montre les procédures à mettre en œuvre sur le serveur pour la détection de changements d'environnements, l'association d'un environnement existant et la demande

de géolocalisation. L'algorithme 1 montre la gestion côté client.

Algorithm 1 Algorithme au niveau de l'objet.

```
1:  TX_MAX ← 20
2:  DR_MIN ← 0
3:
4:  procedure RECEIVEGEOLOCREQUEST(message)
5:      TX ← TX_MAX
6:      DR ← DR_MIN
7:      send empty request
8:  end procedure
9:
10: procedure RECEIVEAJUSTPARAMETERS(TX, DR)
11:     TX ← TX
12:     DR ← DR
13: end procedure
14:
15: procedure LOOPDATAREQUEST
16:     send data request
17: end procedure
```

Algorithm 2 Algorithme au niveau du serveur.

```
1: TX_MAX ← 14
2: DR_MIN ← 0
3: RADIUS ← 100
4: SNR_MaxDif ← 5
5: last_SNR, areas_Histories[], currentArea
6:
7: function FINDAREA(msg)
8:     for all a of areas_Histories do
9:         r ← |a.AREA_pos − msg.position|
10:        if r < RADIUS then
11:            last_SNR ← a.last_SNR
12:            return a
13:
14:        end if
15:    end for
16:    ▷ no areas were found, we create a new area
17:    newArea ← new Area
18:    newArea.addHistory(TX_MAX, DR_MIN)
19:    areas_Histories.add(newArea)
20:    return newArea
21: end function
22:
23: procedure RECEIVEGEOLOCREQUEST(msg)
24:    currentArea ← findArea(msg)
25:    currentArea.adjustPosition(msg)
26:    TXmax ← max TX in history of currentArea
27:    DRmin ← min DR in history of currentArea
28:    send parameters TXmax and DRmin to object
29: end procedure
30:
31: procedure RECEIVEREQUEST(msg)
32:    if last_SNR = UNDEFINED then                    ▷ new area
33:        last_SNR ← msg.SNR
34:    else
35:        SNR_dif ← |msg.SNR − last_SNR|
36:        last_SNR ← msg.SNR
37:        ▷ environment change detection
38:        if SNR_dif > SNR_MaxDif then
39:            send geolocation request to object
40:        else
41:            currentArea.addHistory(msg.TX, msg.DR)
42:            apply ADR algorithm with currentArea history
43:
44:        end if
45:    end if
46: end procedure
```

5.4/ L'IMPLÉMENTATION ET LES RÉSULTATS

5.4.1/ TESTS

Afin de comparer les algorithmes d'adaptation du débit, nous avons réalisé des tests de l'algorithme *ADR* décrit par Semtech [Sem16] [Voj17] ainsi que du nouvel algorithme COMMA (*Communication Optimisation Mechanism for Mobility Adaptation*) dans des conditions de mobilité quotidienne (domicile et travail) sur une période de 3 jours. L'ensemble des intervenants (dispositif, réseau et serveurs) sont décrits dans la plateforme IPHEN [Pic19] : nous utilisons le réseau LoRaWAN de l'opérateur Objenious qui couvre l'ensemble du territoire Français avec de nombreuse antennes. C'est Objenious qui réalise la géolocalisation *TDOA*, avec l'aide de *machine-learning* pour améliorer la précision. Nous n'avons pas d'information supplémentaire car l'opérateur privé ne souhaite pas en divulguer davantage. Le dispositif est un *ArduinoUNO* et un module *Dragino LoRa Shield* qui possède une puce *Semtech SX1276*.

Les messages sont envoyés toutes les 10 minutes afin de respecter le *duty cycle* de la bande 868 MHz. La tableau 5.3 donne les distances approximatives entre l'objet et l'antenne au différents moments de la journée. Il faut prendre en compte le fait que des trajets ont été effectués entre les différents emplacements de l'objet au cours des 3 journées de tests.

Hour	*Antenna distance*
8h-12h	$\approx 1000m$
12h-14h	$\approx 2000m$
14h-18h	$\approx 1000m$
18h-8h	$\approx 5000m$

FIGURE 5.3 – Distance avec l'antenne la plus proche au cours des journées de tests.

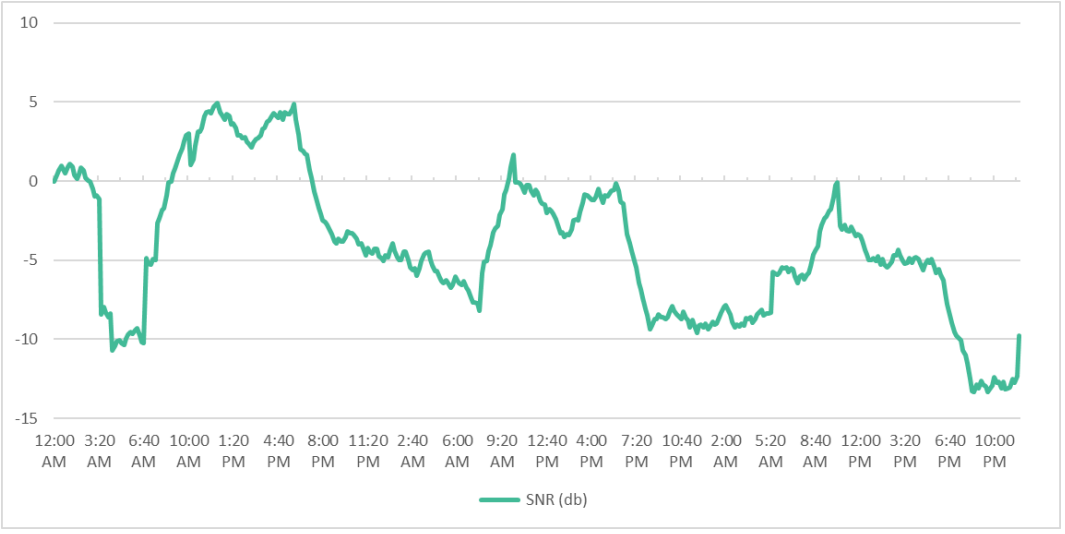


FIGURE 5.4 – Variation du *SNR* (en db) avec *ADR*.

Le graphique 5.4 montre les variations du *Data Rate* et de la puissance d'émission *TX* de l'objet en utilisant l'algorithme *ADR*. Le *SNR* est calculé par le serveur *Backend*, ici Objenious, c'est le rapport entre le signal et le bruit que les antennes mesurent lors de la

réception d'un message.

Les pics de *SNR* correspondent aux changement d'environnement brusques durant la journée. À mesure que l'objet se rapproche de la passerelle la plus proche, son signal reçu sera plus intense et son *SNR* augmentera rapidement. En appliquant la décroissance des paramètres de transmission de l'algorithme *ADR* (visible sur la figure 5.5), le *SNR* aura alors tendance à redescendre un certain temps jusqu'à ce qu'une pseudo-stabilisation des paramètres se produise.

Lorsque l'objet s'éloigne de la passerelle la plus proche, le *SNR* diminuera et le pic sera inversé après l'application de l'algorithme. Avec un message toutes les 10 minutes, l'algorithme *ADR* devra attendre 20 messages, soit presque 3 heures, pour commencer à adapter les paramètres de transmission. Par exemple, nous pouvons observer sur cette figure le changement d'environnement à 8 heures pour les 3 jours : l'objet se rapproche de l'antenne et le pic de *SNR* est rapidement atteint vers 10h environ. Les paramètres d'envoi seront ajustés de manière incrémentale, en priorité sur le débit *DR* puis sur la puissance d'envoi *TX* (lorsque *DR* est au maximum). Cet ajustement, visible sur la figure 5.5, prendra plusieurs heures.

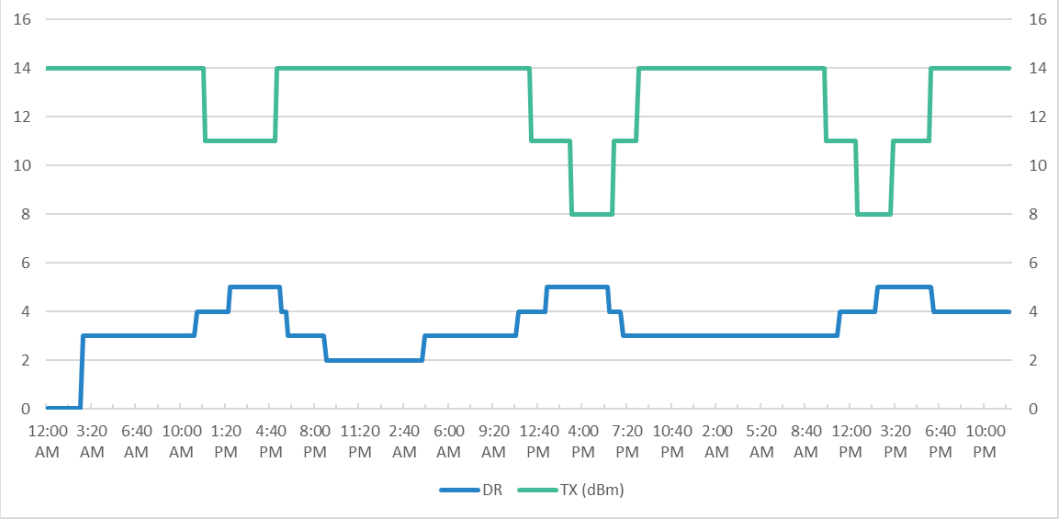


FIGURE 5.5 – Variation de *Data Rate* et de la puissance d'émission *TX* (en dBm) avec *ADR*.

Nous pouvons voir également, lorsque l'objet s'éloigne de l'antenne (dans notre exemple à la sortie du travail), que le paramètre *DR* diminue. Cela signifie que l'objet a perdu sa connectivité et qu'il a, lui-même, diminué ce paramètre pour la retrouver. Quelques messages seront donc retransmis plusieurs fois, impliquant une consommation d'énergie plus importante.

Au final, lorsque l'objet se rapproche de la passerelle, l'algorithme passe une grande partie de la journée à effectuer des ajustements des paramètres de communication et ainsi à être en surconsommation d'énergie, alors que très peu de déplacements sont effectués. L'algorithme COMMA permet d'ajuster les paramètres de communication plus rapidement et de faire redescendre rapidement les pics de *SNR*. Cela aura ainsi pour conséquence de diminuer la latence du traitement et d'économiser de l'énergie principalement, tout en gardant une qualité de service semblable.

La figure 5.6 montre les variations du *Data Rate* et de la puissance d'émission *TX* de l'objet

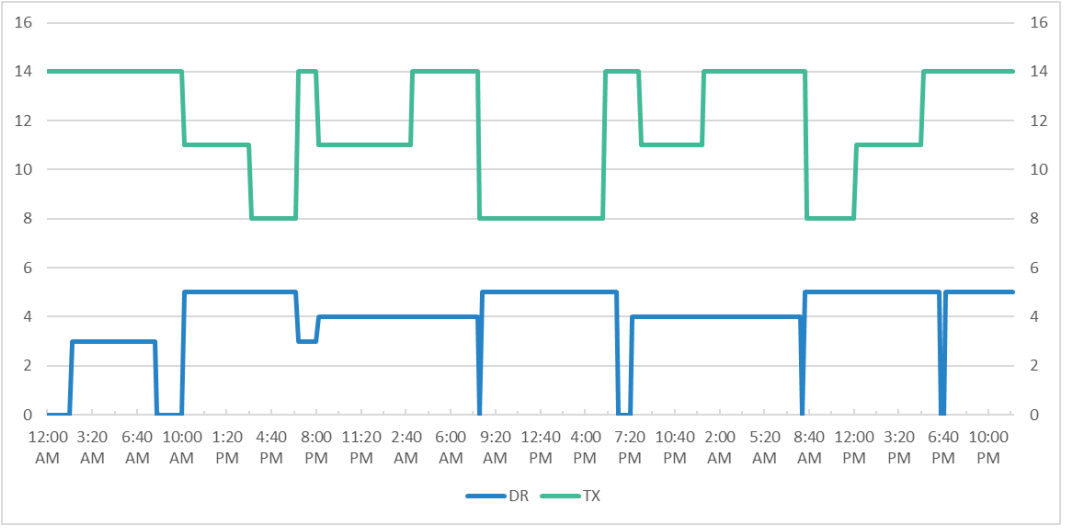


FIGURE 5.6 – Variation du débit *DR* et de la puissance d'émission *TX* (en dBm) avec COMMA.

en utilisant l'algorithme COMMA. Nous pouvons voir la détection de rupture d'environnement, visible sur la figure à 8h05 et à 18h30 le premier jour et 8h25 et 18h30 le deuxième jour. À 8h05 le premier jour, l'environnement est inconnu pour l'objet : le *DR* sera réinitialisé à 0 et la *TX* à 20 *dBm*. À 18h, l'environnement est connu : les précédents *DR* et *TX* seront réutilisés et l'adaptation des paramètres de communication se fera rapidement.

5.4.2/ LA COMPARAISON ÉNERGÉTIQUE

Pour comparer l'algorithme *ADR* et COMMA, nous devons évaluer la consommation énergétique des envois en nous basant sur le modèle de consommation énergétique de la section 3.2.3.1.

Pour tous les envois que nous effectuons, seule la puissance d'émission *TX* et le *Data Rate* *DR* varieront (*SV*, *CR*, *PL*, *NP*, *BW*, *H* et *DE* seront toujours les mêmes dans nos tests).

Voici un exemple avec $DR = 0$ (soit $SF = 12$ d'après 3.9) et $TX = 11$ (soit $Tr_{Tx} = 32\,mA$ d'après la figure 3.2) :

On calcule la puissance $P_{Cons}(P_{Tr})$ en fonction de la puissance d'émission Tx :

$$P_{Cons}(P_{Tr}) = Tr_{Tx} * SV = 32 * 3,3V = 105.6\,mW$$

$3,3\,V$ est la consommation du SX1276.

$$T_{Symbol} = \frac{2^{SF}}{BW} = \frac{2^{12}}{125kHz} = 32,768\,ms$$

On calcule $N_{Payload}$, le nombre de symboles utilisé pour transmettre la charge utile à l'aide de $\Theta(PL,SF)$ et $\Gamma(SF)$:

$$\Theta(PL,SF) = 8PL - 4SF + 16 + 28 - 20H = 60\ symboles$$

$$\Gamma(SF) = SF - 2DE = 12\ symboles$$

$$N_{Payload} = 8 + max\left(ceil\left(\frac{\Theta(PL,SF)}{\Gamma(SF)}\right) * \frac{1}{CR}, 0\right) = 13\ symboles$$

avec $CR = 1$, $H = 0$ car pas de header, PL = 8 bytes et $DE = 0$ car pas de *low data rate optimization*.

On calcule ensuite la durée de la charge utile $T_{Payload}$ puis la durée du préambule $T_{Preamble}$:

$$T_{Payload} = N_{Payload} * T_{Symbol} = 425,984\ ms$$

$$T_{Preamble} = (4.25 + NP) * T_{Symbol} = 335,872\ ms$$

avec NP le nombre de symboles du préambule = 6 symboles.

Enfin, on calcule le temps de vol T_{Packet} puis la consommation énergétique E_{Cons} (en fonction de la puissance d'émission) :

$$T_{Packet} = T_{Preamble} + T_{Payload} = 761,856\ ms$$

$$E_{Cons} = P_{Cons}(P_T) * T_{Packet} = 80451,994\ \mu J \approx 0,0805\ J$$

L'énergie consommée est donc d'environ $0,0805\ J$ pour $DR = 0$ et $TX = 11$. Nous reproduisons cette formule pour l'ensemble des paquets envoyés depuis les dispositifs sur les trois jours de tests afin de produire un graphique des *time on air* cumulés et un graphique de la consommation énergétique cumulée (cf figure 5.7) lors des envois.

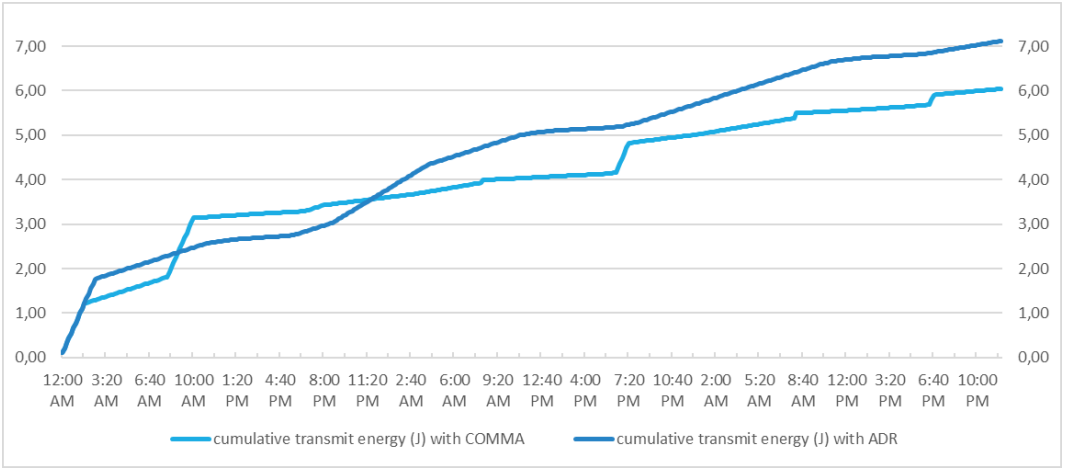


FIGURE 5.7 – Énergie cumulée (en joules) avec *ADR* et COMMA.

Nous constatons que l'énergie totale consommée lors des envois, en relation avec le *time on air*, est plus faible sur les trois jours de tests avec le mécanisme d'adaptation rapide en mobilité quotidienne COMMA.

Nous pouvons observer, sur la figure 5.7, que l'énergie totale consommée lors de la transmission, est plus faible sur les deux derniers jours de tests avec le mécanisme d'adaptation rapide en mobilité quotidienne COMMA. Sur ce laps de temps, l'énergie cumulée est de $3,49\ J$ avec l'algorithme *ADR* et de $2,47\ J$ avec l'algorithme COMMA, soit un gain d'environ 41,3 %. Par jour, cela donne une consommation énergétique de $1,05\ C$ (en coulombs) pour l'*ADR* et $0,748\ C$ pour COMMA (en divisant les résultats précédent par une tension de $3,3\ V$ et par le nombre de jours).

Énergie totale

Nous pouvons maintenant estimer la consommation totale en énergie en prenant en compte la consommation en réception et en repos. L'outil de calcul *Semtech* [Sem15] sur les puces LoRa SX1272 et SX1276 nous indique plusieurs points qui nous aiderons pour l'estimation :

- la consommation en repos de la puce SX1276 est de $100\,\eta A$, soit $0,0001\,mA$,
- le temps de réception est égal au T_{Packet},
- la consommation énergétique lors de la réception est toujours de $13\,mA$.

Avec ces informations, nous pouvons calculer $E_{TotalCons}$, la consommation totale (en mAh) entre deux transmissions qui comprend la consommation énergétique d'une transmission, d'une réception et du temps en repos.

$$E_{TotalCons} = (Tr_{Tx} + 13) * T_{PacketHour} + E_{sleep} * T_{sleep}\ en\ mAh$$

Où :

- E_{sleep} la consommation au repos (en mA),
- T_{sleep} le temps entre deux transmissions,
- $T_{PacketHour}$ le temps de vol T_{Packet} en heures.

Nous n'avons pas tenu compte du premier jour, qui est un jour d'adaptation, et qui n'est pas représentatif à long terme. Nous avons donc calculé cette consommation énergétique sur les deux derniers jours du test. $E_{TotalCons}$ est d'abord calculée pour chaque intervalle de 10 minutes, à partir de T_{Packet} convertis en heures et Tr_{Tx} collectés ainsi que $E_{sleep} = 0,0001\,mA$ et $T_{sleep} = 0,167\,h$.

Afin de comparer ces résultats, nous avons fait la même chose avec la consommation théorique dans les meilleures et les pires conditions (selon la réglementation Européenne de puissance maximale). Nous avons donc fait varier le *Spreading Factor* du meilleur ($SF = 7$) au pire ($SF = 12$) ainsi que la TX de meilleure ($TX = 8$) à la pire ($TX = 20$). Cela nous donne 4 nouvelles valeurs comparatives :

1. meilleur SF et meilleure TX,
2. meilleur SF et pire TX,
3. pire SF et meilleure TX,
4. pire SF et pire TX.

Nous pouvons maintenant cumuler les valeurs obtenues sur les deux jours de tests. La figure 5.8 nous donne l'énergie totale cumulée en mAh pour COMMA, ADR ainsi que les quatre courbes de comparaison sur deux jours. Les résultats donnent une consommation totale de $0,2832\,mAh$ pour COMMA contre $0,3938\,mAh$ pour ADR.

Cependant, en observant le graphique nous remarquons que :

- Dans les pires conditions (pire SF et pire TX), la technologie LoRaWAN est beaucoup plus consommatrice en énergie. Le facteur est d'environ 35 par rapport aux meilleures conditions (meilleur SF et meilleure TX).
- la courbe 3 augmente beaucoup plus rapidement que la courbe 2 : cela nous indique que la variation de la puissance d'émission TX ne joue que relativement peu dans la consommation énergétique par rapport à la variation du *Spreading Factor* et donc implicitement du temps de vol T_{Packet}. Les courbes 2 et 3 nous donnent respectivement un total cumulé de $E_{TotalCons1} = 0,143\,mAh$ et $E_{TotalCons2} = 2,320\,mAh$ sur les deux jours. Le facteur d'importance du paramètre SF par rapport au paramètre TX est calculé par $F_{SF/TX} = E_{TotalCons2}/E_{TotalCons1}$. Il est donc d'environ 16 sur la technologie LoRa. En d'autres termes, pour économiser de l'énergie, il est vraiment préférable de faire varier d'abord le *Spreading Factor* prioritairement avant de faire varier la puissance d'émission.

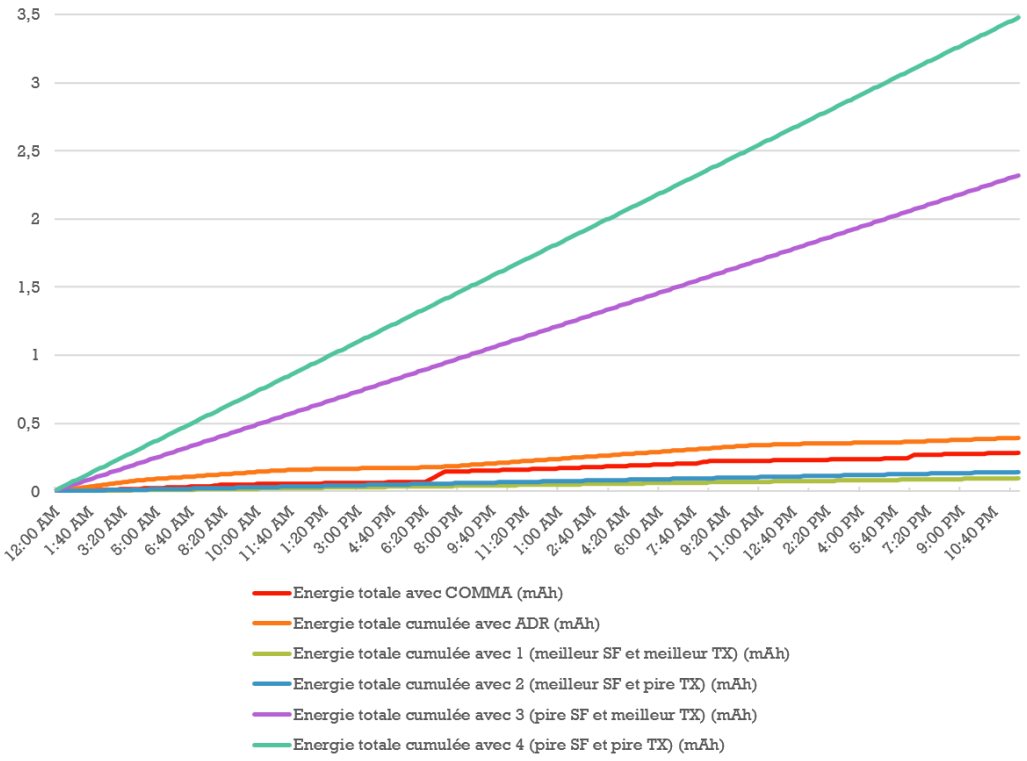


FIGURE 5.8 – Énergie totale théorique cumulée (en *mAH*) sur deux jours, avec des intervalles entre deux transmissions de 10 minutes.

Capacité de la batterie

À partir de la consommation calculée précédemment, il est possible d'estimer théoriquement la durée de vie d'une batterie. Cela ne prend pas en compte l'énergie consommée par les capteurs lors de la prise de mesure, du microcontrôler, de la RAM ou encore du déchargement de la batterie dans le temps.

La figure 5.9 montre la durée de vie estimée d'une batterie d'une capacité totale de $300\,mAh$ avec les algorithmes COMMA et *ADR*, ainsi que les courbes de comparaison dans les

meilleures et les pires conditions. Nous pouvons remarquer que la durée de vie est relativement importante lorsque les conditions le permettent avec des paramètres de transmission efficaces, mais qu'elle décroît vertigineusement si les paramètres de transmission ne sont pas efficaces.

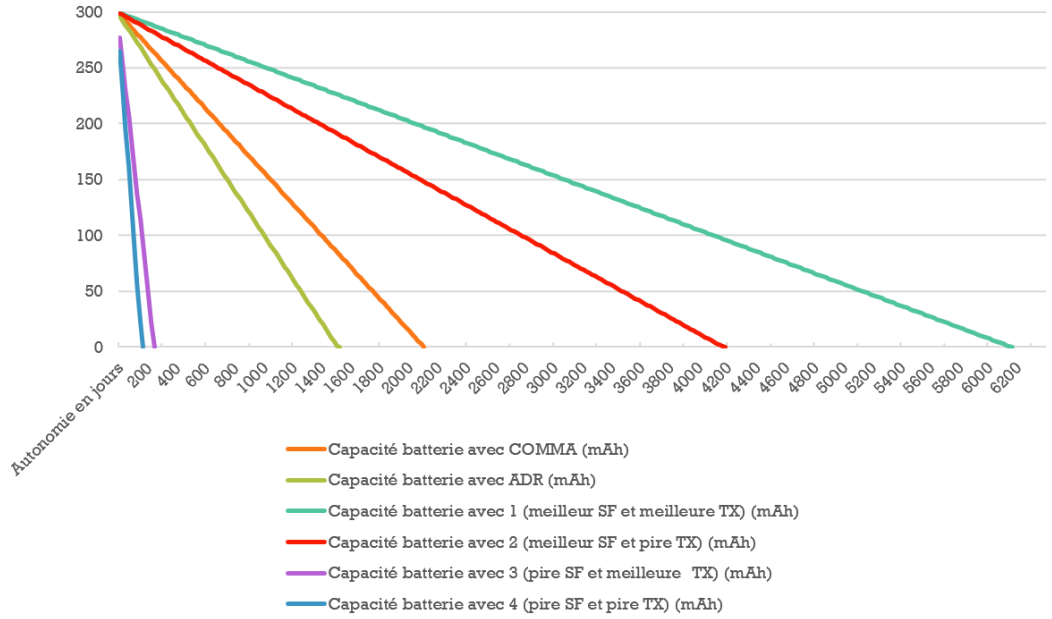


FIGURE 5.9 – Capacité théorique d'un batterie (en *mAH*) avec des transmissions toutes les 10 minutes.

En conclusion, nous pouvons affirmer que l'adaptation des paramètres de transmission, (et particulièrement le *Spreading Factor*), que ce soit avec *ADR* ou avec le mécanisme COMMA, a une incidence importante sur la consommation énergétique et la durée de vie des batteries.

Synthèse du chapitre 5

SYNTHÈSE

Dans cette section, nous avons détaillé COMMA (*Communication Optimisation Mechanism for Mobility Adaptation*) : un nouveau mécanisme d'adaptation des paramètres d'émission dans le cas de mobilité quotidienne. Il est basé sur l'algorithme *ADR*, mais utilise la détection et l'association d'environnement connu afin d'adapter plus rapidement les paramètres de transmission que ne peut le faire l'algorithme *ADR*.

Le mécanisme COMMA utilise, entre autres, le suivi du paramètre *SNR* au niveau du serveur pour la détection de rupture d'environnement, et la géolocalisation via LoRaWAN, afin d'effectuer l'association d'environnement. Nous avons ensuite comparé l'algorithme *ADR* à COMMA et ses mécanismes d'adaptation, en étudiant la consommation énergétique des deux solutions.

Bien que difficilement applicable pour des restrictions techniques et technologiques, le protocole COMMA permet un gain significatif si les conditions environnementales sont relativement stables.

Ce premier prototype est une preuve de concept significative et essentielle dans la poursuite des travaux communs du Laboratoire Femto-st et de l'entreprise *Maincare Solutions*. Le suivi en mobilité des patients, grâce à l'*IoT* est l'un des enjeux majeurs dans le domaine *eHealth & Telemedicine*.

Conclusion et perspectives

Conclusion générale

Les réseaux LPWAN comme LoRaWan sont des alternatives très intéressantes dans le monde de l'Internet des Objets. Avec leur faible consommation en énergie, leur grande portée et leur utilisation en mobilité, cela fait d'eux des acteurs principaux dans le développement de dispositifs connectés et participe grandement à l'Internet des Objets dans les différents secteurs d'activité comme l'environnement et l'industrie.

Cependant, ces réseaux ont aussi leurs faiblesses, de par leur limitation d'utilisation (temps d'utilisation maximal sur les bandes de fréquences libres et tailles des messages très restreints entre autres), ainsi que leur fiabilité relativement faible (perte de messages due à l'interférence ou à la couverture réseau, peu de qualité de service par défaut). Toutefois, il est intéressant pour nous d'utiliser ces réseaux ainsi que leurs principales caractéristiques (économie d'énergie, faible coût et mobilité notamment) dans le domaine critique de la santé, et plus particulièrement de la télésurveillance médicale.

Pour qu'une plateforme de suivi médical de patients, hors de l'hôpital, soit réellement utilisable au quotidien et à long terme, il est important que celle-ci soit économe en énergie tout en gardant une bonne fiabilité : c'est **le premier verrou** scientifique. C'est pourquoi, il est nécessaire de se tourner vers les nouvelles technologies que sont les IoTs et plus particulièrement les réseaux LPWAN.

C'est pourquoi, après avoir présenté notre première partie sur l'état de l'art, dans ce mémoire, nous avons exposé I^{2}PHEN (**I***oT* **I***nteroperable* **P***latform for* **HE***alth mo***N***itoring low power*), notre nouvelle plateforme de télésurveillance médicale à distance qui se distingue par sa capacité à être mobile et économe en énergie en utilisant la technologie de l'Internet des Objets. Nous avons synthétisé au mieux les besoins de la plateforme avec l'élaboration des exigences fonctionnelles en 10 points : la qualité, la cohérence et la validation des données, la gestion des données, la sécurité, l'interopérabilité, l'énergie en fonction de la précision, l'adaptabilité, la non-invasion de la vie privée, la réglementation, le coût et pour terminer l'ubiquité. Nous avons ainsi introduit l'architecture de la plateforme I^{2}PHEN avec une description de chacun des acteurs impliqués (les dispositifs médicaux, la passerelle locale, les cœurs de réseau et le serveur médical).

En se basant sur les connaissances acquises dans l'état de l'art, nous avons dû faire des choix technologiques et les justifier tels que l'utilisation des LPWAN (LoRaWAN, LTE-M et NB-IoT) et du standard Continua. Ce dernier offre une solution d'interopérabilité à la plateforme.

L'utilisation des différentes recommandations du standard permet, entre autres, de :

- pouvoir utiliser facilement plusieurs centaines de dispositifs médicaux connectés qui existent déjà sur le marché,
- renforcer la sécurité et d'uniformiser les données médicales récoltées.

Afin de répondre aux exigences liées à la télésurveillance de patients, dans le domaine critique de la santé, il était nécessaire, pour nous, d'apporter une qualité de service ainsi qu'une sécurité suffisante afin d'assurer et de protéger les échanges de données médicales. Différentes fonctionnalités ont été implémentées et détaillées : les différents modes d'utilisation, les acquittements et les procédures de retransmissions, l'utilisation d'ADR ...

Un **deuxième verrou** scientifique important est celui de la mobilité, car les patients atteints de maladies chroniques ne souhaitent pas changer leurs habitudes de vie.

Dans l'état de l'art, nous avons montré que l'algorithme ADR (*Adaptive Data Rate*) utilisé avec LoRaWAN peut réduire davantage la consommation d'énergie et les interférences en adaptant sa puissance de transmission et son débit de données. Toutefois, le principal défi est de pouvoir utiliser cet algorithme dans les cas où les patients sont mobiles et poursuivent leurs activités quotidiennes.

Nous avons proposé le nouveau protocole COMMA (Communication Optimisation Mechanism for Mobility Adaptation) : un nouveau mécanisme d'adaptation des paramètres d'émission dans le cas de mobilité quotidienne. Il est basé sur l'algorithme ***ADR*** de LoRaWAN, mais utilise la détection et l'association d'environnement connu afin d'adapter plus rapidement les paramètres de transmission que ne peut le faire l'algorithme ***ADR***. Le mécanisme COMMA utilise, entre autres, le suivi du paramètre ***SNR*** au niveau du serveur pour la détection de rupture d'environnement, et la géolocalisation via LoRaWAN, afin d'effectuer l'association d'environnement. Nous avons ensuite comparé l'algorithme ***ADR*** à COMMA et ses mécanismes d'adaptation, en étudiant la consommation énergétique des deux solutions. Nos premiers résultats sont très encourageants et montrent qu'il est vraiment possible de proposer des mécanismes qui intègrent cette mobilité tout en économisant de l'énergie. En outre, la diminution de la puissance d'envoi génère moins de collisions dans un réseau dense en objets LoRa, et augmente ainsi la fiabilité des échanges. Pour finir, nous avons montré que l'adaptation de paramètres d'émission est très importante pour économiser de l'énergie, et que s'en priver est une mauvaise stratégie.

Au final, nous proposons une plateforme de télésurveillance médicale à distance, I^2PHEN, économe en énergie et mobile. Cette plateforme peut répondre à des besoins spécifiques pour beaucoup de patients dans le monde. Elle favorise, de par sa mobilité, la continuité des soins en dehors du domicile comme le lieu de travail, les activités diverses ou les temps de déplacements, tout ce qu'une plateforme de télésurveillance classique ne peut pas assurer. L'économie d'énergie permet, quant à elle, de proposer une solution la moins contraignante possible, en évitant les recharges quotidiennes des batteries. De plus, l'aspect interopérabilité offre une large gamme de dispositifs médicaux connectés (tensiomètre, glucomètre, oxymètre...) et une facilitation d'intégration de nouveaux dispositifs. Cela permet de proposer une solution de soin pour les patients atteints de maladies chroniques multi-pathologiques pour lesquels les suivis de différentes mesures de constantes sont nécessaires. Enfin, nous avons proposé une solution adaptative pour les patients actifs, qui continuent à vivre avec

leur maladie et changent régulièrement de lieu et d'environnement. Nous avons montré que cette adaptation de paramètres est cruciale et qu'elle est forte consommatrice en énergie des objets.

Ce premier prototype de la plateforme s'inscrit dans un contexte de travaux communs entre le laboratoire Femto-st et l'entreprise *Maincare Solutions*. Le suivi des patients, atteints de maladies longue durée, est l'un des enjeux les plus importants avec un axe de développement majeur dans le domaine très évolutif de la télémédecine. Des financements institutionnels continuent à soutenir cet objectif, comme le projet *ETAPES* qui encourage et soutient financièrement le déploiement de projets de télésurveillance. Le contexte de la COVID-19 pourrait également accélérer la mise en œuvre. Un suivi au domicile des patients atteints du virus aurait pu participer au désengorgement des centres de soins. De plus, le développement massif de la téléconsultation pendant cette période a été un succès.

PERSPECTIVES

Ces travaux offrent différentes perceptives qui nous paraissent très intéressantes. Notre plateforme I^{2}PHEN est une plateforme de télésurveillance de *bout en bout* qui s'étend sur une large plage de technologies, standards ou protocoles de communications différents. De nombreuses améliorations peuvent être apportées à tous les niveaux : sur la plateforme en elle-même (au niveau hardware ou électronique), au niveau des réseaux de communication (algorithmiques, qualité de service, ou choix technologiques) ou encore au niveau du serveur de récupération de données médicales.

A, La communication directe (sans passerelle locale)

Le premier axe est la possibilité de se passer d'une passerelle locale pour transférer les données médicales vers la passerelle distante. En effet, il serait possible d'intégrer une puce LoRa directement dans le dispositif médical. Toutefois, se passer de la plateforme locale dans un cas multi-pathologique engendrerait une multiplication des puces LoRa et donc une multiplication des abonnements au réseau. De plus, intégrer des dispositifs médicaux propriétaires, utilisant la technologie LoRa, ferait perdre l'aspect interopérable de la plateforme qui fonctionne avec tous les objets certifiés Continua. La meilleure solution serait donc de faire évoluer le standard Continua de la *Personnal Connected Health Alliance* pour prendre en charge le mode de communication LoRaWAN.

C'est globalement ce que la *startup Medisanté*, basée en Suisse, a imaginé. Toutefois elle a utilisé les technologies cellulaires, fortes de leurs expériences et leurs déploiements massifs, pour commencer. La startup a tout d'abord développé un hub d'objets connectés servant de cœur de réseau. Puis, elle a sélectionné des objets connectés de santé qui utilisent des technologies cellulaires (avec carte SIM), et elle a intégré la transformation des données propriétaires dans le hub. Enfin, elle a passé un partenariat avec l'opérateur de télécommunications *Vodafone*. Elle propose ainsi d'intégrer le hub dans des solutions existantes, et avec des objets connectés de santé existants. Cependant, elle a pu constater que l'interopérabilité de cette solution n'était pas optimale. C'est pourquoi, Medisanté est devenue membre innovateur de la *PCHAlliance* afin de participer au développement de la connectivité *Direct2Cloud*, un mode de communication cellulaire intégré à Continua en 2020.

Il semble donc tout à fait possible que le standard Continua puisse évoluer pour prendre en compte la technologie LoRaWAN.

B, La plateforme locale à un établissement de santé ou une ville

La technologie LoRaWAN permet de créer son propre réseau librement (au contraire des concurrents comme Sigfox ou les Nb-IoT...) avec des passerelles distantes à disposer soi-même (c'est entre autres pour cela que cette technologie a été retenue). Cela permet de couvrir facilement un établissement de santé comme un hôpital ou une maison de retraite à moindre coût (une centaine d'euros par antenne).

Les antennes peuvent rediriger les données médicales directement vers le serveur médical dans un réseau local. Une solution alternative serait d'utiliser le cœur de réseau open source *The Things Network* (ou *TTN*) si le principe du réseau communautaire n'est pas un problème. En effet, les antennes disposées seront utilisables par n'importe qui, ce qui peut poser des problèmes de sécurité (notamment sur la disponibilité). Cependant, cela simplifie grandement la gestion du parc des dispositifs médicaux, les messages descendants, les redirections...

Dans tous les cas, l'utilisation de la bande de fréquences libre reste inchangée (bande 868 MHz en Europe), ce qui rend l'utilisation de celle-ci toujours limitée en temps et en puissance. Si les passerelles sont assez proches des dispositifs médicaux, la quatrième sous-bande $869,3 - 869,4\ MHz$ est très intéressante (cf figure 3.5). Le canal de la bande de fréquences est limité à $10\ mW$, donc réservé à une faible portée, mais illimité en temps d'utilisation (sans *duty cycle*).

Au final, il serait possible de créer un parc de dispositifs médicaux connectés dans un établissement à moindre coût avec cette technologie, et ce sans modification importante de la plateforme I^2PHEN.

C, La qualité et perceptives des réseaux IoT

La France possède certainement l'une des couvertures IoT les plus encourageantes au monde. Alors que d'autres pays se reposent sur un développement collaboratif des technologies IoT qui peine à avancer (avec notamment *The Things Network* et *Helium*), les opérateurs privés français (Sigfox, Bouygues Telecom, Orange et SFR) ont décidé de déployer massivement des antennes afin de couvrir une grande partie de la France sur les technologies Sigfox, LoRaWAN, Nb-IoT et LTE-M.

En conséquence, le développement des technologies est plus rapide, avec une plus grande couverture notamment en zone rurale. Cependant, le coût d'utilisation est plus important et la couverture *indoor* est un peu délaissée.

Une troisième solution de déploiement pourrait se développer dans les prochaines années. Cette solution se situe entre le réseau communautaire et le réseau privé, avec la dynamique de développement de la maison intelligente. *Semtech* a annoncé une association avec *Amazon* pour collaborer sur un nouveau réseau, *Amazon Sidewalk*, qui utilisera la technologie LoRa (mais pas LoRaWAN). La conception de ce réseau est différente, puisqu'elle va utiliser les objets connectés des maisons pour créer un réseau partagé avec les personnes qui seront

proches de la maison (voisins, passants ...). Les objets connectés de domotique tels que les caméras de surveillance, les portails ou les alarmes intégreront directement les antennes LoRa afin de partager le réseau. De proche en proche, un réseau collaboratif mondial se formera sur les lieux de vie des personnes, sans que ces personnes ne le sachent ou ne le réalisent.

Bien que le réseau *Amazon Sidewalk* ne prenne pas en charge LoRaWAN mais uniquement la technologie LoRa, il sera peut-être envisageable dans les années à venir de s'appuyer dessus pour utiliser un réseau IoT à moindre coût, plus faible consommation (due à la proximité des antennes), meilleure couverture et plus grande fiabilité.

D, L'améliorations du mécanisme COMMA

L'algorithme COMMA peut être une solution intéressante dans le cas de mobilités quotidiennes. Toutefois, il possède certaines limitations techniques qui ne lui permettent pas d'être utilisé dans tous les cas.

Tout d'abord, le nombre d'antennes, que peut atteindre le périphérique, doit être au minimum de 3, ce qui est pour l'instant rare en zone rurale. La détection d'environnement n'est pas non plus optimale lorsque la géolocalisation est réalisée car celle-ci n'est pas précise et peut même être erronée [Pod18]. Utiliser l'Intelligence Artificielle avec un algorithme d'apprentissage côté serveur pourrait dans ce cas améliorer la détection et l'association d'environnement grâce aux habitudes de déplacement des personnes. Une analyse prédictive des déplacements, au niveau du serveur, pourrait même avoir lieu (en fonction des habitudes régulières, du jour, de l'heure ...), ce qui permettrait un gain en énergie supplémentaire. Par ailleurs, un nouvel émetteur-récepteur LoRa *LR1110* de Semtech a été mis sur le marché en 2020. Il intègre une fonction géolocalisation GNSS à faible consommation énergétique qui pourrait remplacer la triangularisation avec LoRa.

L'introduction de nouveaux capteurs, comme le podomètre ou l'accéléromètre, pourrait également nous aider pour détecter les mouvements et les changements d'environnement. Enfin, questionner régulièrement les réseaux Wi-Fi et Bluetooth disponibles pourrait nous aider à effectuer l'association d'environnement plus précisément que la géolocalisation avec LoRa ou quand cette dernière ne le permet tout simplement pas. Les réseaux seront enregistrés et associés à des aires. Les reconnaissances de ces dernières seront alors plus faciles les fois suivantes. L'émetteur-récepteur LR1110 permet de scanner les réseaux Wi-Fi avec une très faible consommation énergétique.

Dans tous les cas, il serait intéressant d'intégrer une solution en mode dégradée qui permettra de faire une adaptation plus rapide que l'algorithme ADR classique lorsque les conditions nécessaires au fonctionnement du mécanisme COMMA ne sont pas réunies.

Par ailleurs, les conditions environnementales changent pour un même lieu au cours du temps, par exemple lors du déplacement d'objets autour d'appareils créant un effet Doppler ou une collision de paquets, ce qui ne nous permet pas d'assurer un envoi avec des paramètres d'émissions utilisés au préalable. Une marge d'erreur pourrait alors être acceptée pour éviter les conditions environnementales sous-optimales.

Pour finir, l'algorithme ne fonctionne qu'avec des accusés de réception pour chaque message envoyé. Cela consommera une quantité d'énergie non négligeable supplémentaire. Une

idée pourrait être de réaliser des accusés de réception groupés. Toutefois, une réaction instantanée lors d'une rupture d'environnement ne serait alors plus possible.

E, Le nouvel algorithme MARC (*Monitoring Algorithm Real-time for Connected health*

La dernière brique essentielle à la télésurveillance de patients à distance se trouve dans le monitoring en temps réel des données médicales récoltées.

Notre nouvel algorithme MARC permettrait de générer des alertes en cas de détection de valeurs anormales, et d'interagir avec le cercle médical du patient. Il aiderait à améliorer les conditions de monitoring des patients en fournissant au serveur médical une Intelligence Artificielle (IA) permettant de :

- Demander des nouvelles mesures automatiquement lorsqu'une anomalie est détectée afin de la confirmer,
- Détecter des mesures anormales ou le manque de mesures et déclencher des alertes auprès de l'équipe de prise en charge du patient,
- Faire redescendre des informations, avec validation, et confirmations de réception issues de l'IA et/ou de l'équipe de prise en charge au patient (via la passerelle locale et un écran par exemple),
- Gérer le duty cycle pour garantir le temps de communication en cas de problème.

L'algorithme, se trouvant sur le serveur IoT, peut connaître l'historique des données de santé du patient, mais également des paramètres de prise en charge (médecin traitant et équipe de prise en charge, parcours du patient, niveau de criticité et paramètre de déclenchement d'une alerte). Il doit également être en mesure de connaître le mode de fonctionnement des passerelles locales des patients. C'est en recoupant toutes ces données que l'algorithme peut, lors de la réception d'une nouvelle mesure, détecter si celle-ci est anormale, en utilisant des ontologies [Hri14] et en déclenchant soit :

- Une demande de nouvelle mesure directement à l'objet connecté ou au patient : pour envoyer un message descendant, le serveur contacte le cœur de réseau qui se charge de renvoyer le message. Dans le cas d'un mode de fonctionnement *ALL-* ou *MANUEL*, il faudra alors faire attention à retourner le message rapidement après réception : dans la plage de temps où la passerelle locale sera en écoute d'un message descendant. Il est donc nécessaire d'avoir un algorithme rapide dans l'analyse des nouvelles mesures.
- Une assistance médicale (équipe de prise en charge) : dans ce cas, une intervention humaine pourra alors a voir lieu comme un appel téléphonique, ou une intervention des pompiers par exemple.

Enfin, dans le chapitre 4, nous avons abordé la notion d'adaptabilité de la plateforme. L'algorithme MARC serait en mesure de trouver des compromis sur la régularité des prises de mesures en fonction des besoins, et pourrait, suivant l'état de santé du patient, ou la prédiction de dégradation de santé de ce dernier, adapter en temps réel cette régularité.

MA BIBLIOGRAPHIE PERSONNELLE

ARTICLE EN REVUE RÉFÉRENCÉE

[Pic20a] Picard, Alexis and Lapayre, Jean-Christophe and Hanna, Fouad and Muthada Pottayya, Ronnie. *COMMA : a new LoRaWAN Communication Optimisation Mechanism for Mobility Adaptation of IoT.* IET Wireless Sensor Systems - Q2 - IF 2.52. en cours de soumission July 2020.

PUBLICATIONS EN CONFÉRENCES INTERNATIONALES AVEC COMITÉ DE LECTURE D'AUDIENCE INTERNATIONALE, DONT LES ACTES SONT PUBLIÉS

[Pic20b] Picard, Alexis and Muthada Pottayya, Ronnie and Hanna, Fouad and Lapayre, Jean-Christophe. *COMMA : a New Protocol Used by IoT for Mobile Health Monitoring.* Proceedings of the IEEE 4th International Conference on Computer Supported Cooperative Work in Design (CSCWD 2020) - (classée B dans Core). Dalian, China (2020).

[Pic19] Picard, Alexis and Muthada Pottayya, Ronnie and Hanna, Fouad and Lapayre, Jean-Christophe. *I2PHEN : A Novel Interoperable IoT Platform for Medical Telemonitoring.* Proceedings of the 16th International Conference on Cooperative Design, Visualization, and Engineering (CDVE 2019) - Series Lecture Notes in Computer Science (LNCS) - (classée C dans Core). pages 84 - 97 - Mallorca, Spain - 2019.

BIBLIOGRAPHIE

[Aga10] Sparsh Agarwal and Chiew Tong Lau. Remote health monitoring using mobile phones and web services. Telemedicine and eHealth, pages 603–607, 2010.

[Alg14] Malek Al-Gabri, Chunlin LI, and Layuan Li. Improving ZigBee AODV mesh routing algorithm topology and simulation analysis. TELKOMNIKA Indonesian Journal of Electrical Engineering, 12(2), February 2014.

[Als18] Mashael M. Alsulami and Nadine Akkari. The role of 5g wireless networks in the internet-of- things (IoT). In 2018 1st International Conference on Computer Applications & Information Security (ICCAIS). IEEE, April 2018.

[And16] E. Andrès et al. Development and experimentation of a new digital communicating and intelligent stethoscope. European Research in Telemedicine / La Recherche Européenne en Télémédecine, 5(4) :145–155, December 2016.

[Ans19] ANSM. Définition des dispositifs médicaux. https://ansm.sante.fr/Glossaire/(filter)/D#term_16195. Accessed : 2019-11-04.

[Ans15] de l'environnement et du travail Agence nationale de sécurité sanitaire de l'alimentation. Compatibilité électromagnétique des dispositifs médicaux exposés à des sources radiofréquences. Rapport d'expertise collective, 2015.

[Bak17] Wafae et al. Bakkali. Kalman filter-based localization for internet of things lorawa end points. Personal, Indoor, and Mobile Radio Communications, pages 1–6, October 2017.

[Ban07] IEEE. Ieee 802.15 wpan task group 6 (tg6) body area networks. http://www.ieee802.org/15/pub/TG6.html, 2007. Accessed : 2020-01-13.

[Bar12] Deena M. Barakah and Muhammad Ammad-uddin. A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture. Proceedings - Third International Conference on Intelligent Systems Modelling and Simulation, pages 214–219, February 2012.

[Ben19] Norhane BENKAHLA, Hajer TOUNSI, Ye-Qiong SONG, and Mounir FRIKHA. Enhanced ADR for LoRaWAN networks with mobility. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). IEEE, June 2019.

[Bii16] BI Intelligence. The global market for iot healthcare tech will top $400 billion in 2022. BI Intelligence, 2016.

[Blu19] Bluetooth SIG. Health device profile implementation guidance whitepaper. https://www.bluetooth.com/bluetooth-resources/health-device-profile-implementation-guidance/, 2009. Accessed : 2020-07-20.

[Bol16] Jan Bolinder et al. Novel glucose-sensing technology and hypoglycaemia in type 1 diabetes : a multicentre, non-masked, randomised controlled trial. The Lancet, pages 2254–2263, September 2016.

[Bor20] Suresh R. Borkar. Long-term evolution for machines (LTE-m). In LPWAN Technologies for IoT and M2M Applications, pages 145–166. Elsevier, 2020.

[Bou19] Taoufik Bouguera, Jean-François Diouris, Jean-Jacques Chaillout, Randa Jaouadi, and Guillaume Andrieux. Energy consumption model for sensor nodes based on LoRa and LoRaWAN. Sensors, 18(7) :2104, June 2018.

[Bov19] Giampaolo Bovenzi, Domenico Ciuonzo, Valerio Persico, Antonio Pescapè, and Pierluigi Salvo Rossi. IoT-enabled distributed detection of a nuclear radioactive source via generalized score tests. In Communications in Computer and Information Science, pages 77–91. Springer Singapore, 2019.

[Bri16] Jose Marcos Camara Brito. Trends in wireless communications towards 5g networks — the influence of e-health and IoT applications. 2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech), pages 1–7, July 2016.

[Car07] Carroll et al. Randy. Continua : An interoperable personal healthcare ecosystem. IEEE Pervasive Computing, pages 90–94, November 2007.

[Car18] Antonella Carbonaro, Filippo Piccinini, and Roberto Reda. Semantic description of healthcare devices to enable data integration. In Advances in Intelligent Systems and Computing, pages 627–630. Springer International Publishing, 2018.

[Cha17] Subhajit Chatterjee et al. Internet of things and body area network-an integrated future. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), pages 396–400, October 2017.

[Che10] Min Chen et al. Body area networks : A survey. Mobile Networks and Applications, 16(2) :171–193, August 2010.

[Chr15] Dimitri A. Christakis. Potential utility of a smart thermometer to predict and avert epidemics. JAMA Pediatrics, 169(11) :1067–8, November 2015.

[Ciu19] Domenico Ciuonzo, Giacinto Gelli, Antonio Pescape, and Francesco Verde. Decision fusion rules in ambient backscatter wireless sensor networks. In 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, September 2019.

[Cos15] Susana E. P. Costa et al. Integration of wearable solutions in AAL environments with mobility support. Journal of Medical Systems, 39(12), October 2015.

[Dal18] Ismail Dali, Rahman Mahbubur, and Saifullah Abusayeed. Low-power wide-area networks : Opportunities, challenges, and directions. ICDCN Workshops, pages 1–6, January 2018.

[Des15] Pratikkumar Desai, Amit Sheth, and Pramod Anantharam. Semantic gateway as a service architecture for IoT interoperability. In 2015 IEEE International Conference on Mobile Services. IEEE, June 2015.

[Dri17] Drivesnccontrol. in 4 wireless iiot connections will use lpwa by 2025. https://drivesncontrols.com/news/fullstory.php/aid/5553/1_in_4_wireless_IIoT_connections_will_use_LPWA_by_2025.html. Accessed : 2020-04-07.

[Ell16] S.W. Ellingson. Radio Systems Engineering. Cambridge University Press, 2016.

[Emb14] Embedded Staff. Using sub-gigahertz wireless for long range internet of things connectivity. https://www.embedded.com/using-sub-gigahertz-wireless-for-long-range-internet-of-things-connectivity/, 2014. Accessed : 2019-04-20.

[Erc17] ERC. Erc recommendation 70-03 relating to the use of short range devices. CEPT, 2017.

[Erc18] CEPT member. Relating to the use of short range devices. ERC RECOMMENDATION 70-03, 2018.

[Erg04] Sinem Coleri Ergen. Zigbee/ieee 802.15. 4 summary. UC Berkeley, September, 10(17) :11, 2004.

[Fet14] Gerhard P. Fettweis. The tactile internet : Applications and challenges. IEEE Vehicular Technology Magazine, 9(1) :64–70, March 2014.

[Fou17] Xenofon Foukas, Georgios Patounas, Ahmed Elmokashfi, and Mahesh K. Marina. Network slicing in 5g : Survey and challenges. IEEE Communications Magazine, 55(5) :94–100, May 2017.

[Fou20] Christophe Fourtet and Benoît Ponsard. An introduction to sigfox radio system. In LPWAN Technologies for IoT and M2M Applications, pages 103–118. Elsevier, 2020.

[Fre18] James Freed et al. Telemedicine : is it really worth it ? a perspective from evidence and experience. Journal of innovation in health informatics, pages 1–14, March 2018.

[Gis08] D. Gislason. Zigbee Wireless Networking. Elsevier Science, 2008.

[Gom12] Carles Gomez, Joaquim Oller, and Josep Paradells. Overview and evaluation of bluetooth low energy : An emerging low-power wireless technology. Sensors, 12(9) :11734–11753, August 2012.

[Gui19] PCHA. Continua design guidelines. https://www.pchalliance.org/continua-design-guidelines, 2019. Accessed : 2020-04-27.

[Hal17] Julian P.J. Halcox et al. Assessment of remote heart rhythm sampling using the AliveCor heart monitor to screen for atrial fibrillation. Circulation, 136(19) :1784–1794, November 2017.

[Han10] Dae man Han and Jae hyun Lim. Smart home energy management system using IEEE 802.15.4 and zigbee. IEEE Transactions on Consumer Electronics, 56(3) :1403–1410, August 2010.

[Hao18] Zijiang Hao, Raymond Ji, and Qun Li. FastPay : A secure fast payment method for edge-IoT platforms using blockchain. In 2018 IEEE/ACM Symposium on Edge Computing (SEC). IEEE, October 2018.

[Hax19] Jetmir et al. Haxhibeqiri. A survey of lorawan for iot : From technology to application. Sensors, page 3995, November 2018.

[Hri14] Hristoskova et al. Anna. Ontology-driven monitoring of patients vital signs enabling personalized medical detection and alert. Sensors 2014, pages 1598–1628, January 2014.

[Ikp19] Augustine Ikpehai, Bamidele Adebisi, Khaled M. Rabie, Kelvin Anoh, Ruth E. Ande, Mohammad Hammoudeh, Haris Gacanin, and Uche M. Mbanaso. Low-power wide area network technologies for internet-of-things : A comparative review. IEEE Internet of Things Journal, 6(2) :2225–2240, April 2019.

[Ism17] Paul Pinault. All what you need to know about regulation on rf 868mhz for lpwan. https://www.disk91.com/2017/technology/sigfox/all-what-you-need-to-know-about-regulation-on-rf-868mhz-for-lpwan/, 2017. Accessed : 2019-04-13.

[Ist11] H. Istepanian, S. Hu, Y. Philip, and A. Sungoor. The potential of internet of m-health things m-iot for non-invasive glucose level sensing. 33rd Annual International Conference of the IEEE EMBS, pages 5264–6, August 2011.

[Itu14] Internatinal Telecommunication Union. The tactile internet. ITU-T Technology Watch Report, September 2014.

[Jis17] R.C. Jisha, Aiswarya Jyothindranath, and L Sajitha Kumary. Iot based school bus tracking and arrival time prediction. In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, September 2017.

[Jon18] Richard W. Jones and Konstantinos Katzis. 5g and wireless body area networks. 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pages 373–378, April 2018.

[Jov05] Emil et al. Jovanov. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. Journal NeuroEngineering and Rehabilitation, April 2005.

[Kha16] Ahmed Khattab, Ahmed Abdelgawad, and Kumar Yelmarthi. Design and implementation of a cloud-based IoT scheme for precision agriculture. In 2016 28th International Conference on Microelectronics (ICM). IEEE, December 2016.

[Kir15] Richard Kirk. Cars of the future : the internet of things in the automotive industry. Network Security, 2015(9) :16–18, September 2015.

[Kla16] B.J.F.van Beijnum B. Klaassen and H.J.Hermens. Usability in telemedicine systems-a literature survey. International Journal of Medical Informatics, pages 56–69, September 2016.

[Kon19] Kousias et al. Konstantinos. Empirical analysis of lorawan adaptive data rate for mobile internet of things applications. Mobile Computing and Networking (MobiCom), October 2019.

[Kuo14] Kuor-Hsin Chang. Bluetooth : a viable solution for IoT ? [industry perspectives]. IEEE Wireless Communications, 21(6) :6–7, December 2014.

[Kwa10] Kyung Sup Kwak, Sana Ullah, and Niamat Ullah. An overview of IEEE 802.15.6 standard. In 2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010). IEEE, November 2010.

[Lan16] S Landström, J Bergström, Erik Westerberg, and David Hammarwall. Nb-iot : A sustainable technology for connecting billions of devices. Ericsson Technology Review, 4 :2–11, 2016.

[Lav19] Alexandru Lavric, Adrian I. Petrariu, and Valentin Popa. Long range SigFox communication protocol scalability analysis under large-scale, high-density conditions. IEEE Access, 7 :35816–35825, 2019.

[Lee18] Sungkee Lee and Hyoungho Do. Comparison and analysis of ISO/IEEE 11073, IHE PCD-01, and HL7 FHIR messages for personal health devices. Healthcare Informatics Research, 24(1) :46, 2018.

[Li12] Miaoxin Li and Mingjie Zhuang. An overview of physical layers on wireless body area network. In Anti-counterfeiting, Security, and Identification. IEEE, August 2012.

[Lib16] Libelium. Waspmote lorawan networking guide. Comunicaciones Distribuidas S.L, page 56, 2016.

[Liu19] Yi Liu, Chao Yang, Li Jiang, Shengli Xie, and Yan Zhang. Intelligent edge computing for IoT-based energy management in smart cities. IEEE Network, 33(2) :111–117, March 2019.

[Lor16] LoRa Alliance. Lorawan regional parameters. LoRa Alliance Technical committee, 2016.

[Lpw17] Paul Pinault. Sigfox & lorawan network architecture and network kernels. https://www.disk91.com/2017/technology/internet-of-things-technology/sigfox-lorawan-network-architecture-and-network-kernels/, 2017. Accessed : 2020-03-23.

[Lpw19] Paul Pinault. Lpwan is not red ocean market. https://www.disk91.com/2019/news/lpwan/lpwan-is-not-red-ocean-market/, 2019. Accessed : 2020-08-13.

[Mam19] MarketsAndMarkets. Iot in healthcare market by component (medical device, systems & software, services, and connectivity technology), application (telemedicine, connected imaging, and inpatient monitoring), end user, and region - global forecast to 2024. https://www.marketsandmarkets.com/Market-Reports/iot-healthcare-market-160082804.html? Accessed : 2019-10-04.

[Mas18] et al. Guy G. Massa. Evaluation of the freestyle libre flash glucose monitoring system in children and adolescents with type 1 diabetes. Hormon Research in Pediatrics, pages 189–199, March 2018.

[Mil17] Richard V. Milani et al. Improving hypertension control and patient engagement using digital tools. The American Journal of Medicine, 130 :14–20, 2017.

[Min15] Minh Tien Do, Claire Goursaud, and Jean-Marie Gorce. Optimisation du nombre de retransmissions dans un réseau à bande ultra étroite basé sur R-FTDMA. In ALGOTEL 2015 - 17èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications, June 2015.

[Mau07] Renée Mauborgne and W Chan Kim. Blue ocean strategy. Gildan Media, 2007.

[Mul07] Geoff Mulligan. The 6lowpan architecture. In Proceedings of the 4th workshop on Embedded networked sensors. ACM Press, 2007.

[Ond20] Jean-Philippe Muller. Ondes et antennes. http://www.ta-formation.com/acrobat-modules/ondes-antennes.pdf. Accessed : 2020-08-05.

[Par17] et al. Mazoteras Pardo. The qardioarm app in the assessment of blood pressure and heart rate : Reliability and validity study. JMIR Mhealth Uhealth, page e198, December 2017.

[Pch17] PCHA. Fundamentals of data exchange. https://www.pchalliance.org/sites/pchalliance/files/ctools/Fundamentals_Data_Exchange_20171001.pdf, 2017. Accessed : 2020-04-27.

[Pic19] Alexis Picard, Jean-Christophe Lapayre, Ronnie Pottayya, and Eric Garcia. I^2phen : A novel interoperable iot platform for medical telemonitoring. Cooperative Design, Visualization, and Engineering, pages 84–97, 2019.

[Pod18] Nico et al. Podevijn. Tdoa-based outdoor positioning with tracking algorithm in a public lora network. Wireless Communications and Mobile Computing, pages 1–9, May 2018.

[Rag12] G. Ragesh and Baskaran Kaliaperumal. An overview of applications, standards and challenges in futuristic wireless body area networks. International Journal of Computer Science Issues 1694-0784, 9 :180–186, January 2012.

[Rat14] Rapeepat Ratasuk, Nitin Mangalvedhe, Amitava Ghosh, and Benny Vejlgaard. Narrowband LTE-m system for m2m communication. In 2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall). IEEE, September 2014.

[Rat16] Rapeepat Ratasuk, Benny Vejlgaard, Nitin Mangalvedhe, and Amitava Ghosh. NB-IoT system for m2m communication. In 2016 IEEE Wireless Communications and Networking Conference. IEEE, April 2016.

[Rgp18] CNIL. Qu'est-ce ce qu'une donnée de santé ? https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante. Accessed : 2019-28-01.

[Rod13] Joel JPC Rodrigues et al. Mobile health platform for pressure ulcer monitoring with electronic health record integration. Health Informatics Journal, 19(4) :300–311, November 2013.

[Sal10] N. Salman, I. Rasool, and A. H. Kemp. Overview of the IEEE 802.15.4 standards family for low rate wireless personal area networks. In 2010 7th International Symposium on Wireless Communication Systems. IEEE, September 2010.

[Sal16] S. Ahmad Salehi, M. A. Razzaque, Inmaculada Tomeo-Reyes, and Nasir Hussain. IEEE 802.15.6 standard in wireless body area networks from a healthcare point of view. In 2016 22nd Asia-Pacific Conference on Communications (APCC). IEEE, August 2016.

[Sur15] A. Surrallés, P.J. Benghozi, S. Bureau, F. Massit-Folléa, D. Diminescu, and F. Thibault. L'Internet des objets / The Internet of Things : Quels enjeux pour l'Europe ? / What Challenges for Europe ? Collection praTICs. Éditions de la Maison des sciences de l'homme, Paris, 2015.

[Sch17] Philipp Schulz et al. Latency critical IoT applications in 5g : Perspective on the design of radio interface and network architecture. IEEE Communications Magazine, 55(2) :70–78, February 2017.

[Sem15] Semtech. Sx1272 lora calculator. https://sx1272-lora-calculator.software.informer.com/download/, 2015. Accessed : 2020-05-27.

[Sem16] Semtech Corporation. Lorawan - simple rate adaptation recommended algorithm. Lora networks Rate adaptation, 2016.

[Sha17] Syed Ahmar Shah et al. Exacerbations in chronic obstructive pulmonary disease : Identification and prediction using a digital health system. Journal of Medical Internet Research, 19(3) :e69, March 2017.

[Sho20] PCHA. Continua certified product showcase. https://www.pchalliance.org/product-showcase, 2020. Accessed : 2020-04-27.

[Sie12] Matti Siekkinen, Markus Hiienkari, Jukka K. Nurminen, and Johanna Nieminen. How low energy is bluetooth low energy ? comparative measurements with ZigBee/802.15.4. In 2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). IEEE, April 2012.

[Sig17] Sigfox. Présentation technique de sigfox. https://www.fun-mooc.fr/asset-v1:univ-toulouse+101001+session02+type@asset+block/Presentation_technique_de_Sigfox_Juillet_2017.pdf, 2017. Accessed : 2020-06-29.

[Sig19] eMind. Sigfox inaugure à paris une quatrième hacking house. http://emind.be/sigfox-inaugure-a-paris-une-quatrieme-hacking-house/, 2019. Accessed : 2020-06-29.

[Sil9] Silicon Labs. An988 : Health device profile. https://www.silabs.com/documents/public/application-notes/AN988.pdf, 2019. Accessed : 2020-07-21.

[Sin17] Rashmi Sharan Sinha, Yiqiao Wei, and Seung-Hoon Hwang. A survey on LPWA technology : LoRa and NB-IoT. ICT Express, 3(1) :14–21, March 2017.

[Srp17] Paul Pinault. The sigfox radio protocol. https://www.disk91.com/2017/technology/sigfox/the-sigfox-radio-protocol/, 2017. Accessed : 2019-09-24.

[Sto17] Sigfox. Sigfox technical overview. https://www.disk91.com/wp-content/uploads/2017/05/4967675830228422064.pdf, 2017. Accessed : 2020-05-29.

[Sur18] Arthur Surville. Objets connectés et dispositifs médicaux connectés : Principaux outils disponibles à la pratique de la médecine générale en France en 2018. PhD thesis, Université Paul Sabatier - Toulouse, 9 Octobre 2018.

[Swa19] K. Narendra Swaroop, Kavitha Chandu, Ramesh Gorrepotu, and Subimal Deb. A health monitoring system for vital signs using IoT. Internet of Things, 5 :116–129, March 2019.

[Szy05] Hervé Szymczak. Classification des dispositifs médicaux. http://www.technologies-biomedicales.com/index.php?mod=articles&ac=commentaires&id=10, June 2005. Accessed : 2019-12-12.

[Tha17] Oscar Thabouillot, Kevin Bostanci, Francois Bouvier, Nicolae Dumitrescu, Maria Stéfuriac, Philippe Paule, and Nicolas-Charles Roche. Syncope during competitive events : Interrogating heart rate monitor watches may be useful ! Prehospital and Disaster Medicine, 32(6) :691–693, August 2017.

[Tol14] Touchapp. Are apple healthkit and google fit ready to revolutionize healthcare ? http://www.touchapp.co.uk/blog/2014/12/04/are-apple-healthkit-and-google-fit-ready-to-revolutionize-healthcare/, 2014. Accessed : 2019-04-21.

[UE17] Le parlement européen et le conseil de l'union européenne. Règlement (ue) 2017/745 du parlement européen et du conseil. http://nosobase.chu-lyon.fr/Reglementation/2017/reglement/05042017.pdf, April 2017. Accessed : 2019-12-07.

[Ver14] M. Vervloet et al. Short- and long-term effects of real-time medication monitoring with short message service (SMS) reminders for missed doses on the refill adherence of people with type 2 diabetes : evidence from a randomized controlled trial. Diabetic Medicine, 31(7) :821–828, April 2014.

[Voj17] Vojtech Hauser and Tomas Hegr. Proposal of adaptive data rate algorithm for lorawan-based infrastructure. International Conference on Future Internet of Things and Cloud, pages 85–90, August 2017.

[War10] Wartena et al. Frank. Continua : The reference architecture of a personal telehealth ecosystem. The 12th IEEE International Conference on e-Health Networking, Applications and Services, pages 1–6, August 2010.

[Wil14] Daryl J. Wile, Ranjit Ranawaya, and Zelma H.T. Kiss. Smart watch accelerometry for analysis and diagnosis of tremor. Journal of Neuroscience Methods, 230 :1–4, June 2014.

[Won13] Alan Chi Wai Wong, Mark Dawkins, Gabriele Devita, Nikolaos Kasparidis, Andreas Katsiamis, Oliver King, Franco Lauria, Johannes Schiff, and Alison J. Burdett. A 1 v 5 mA multimode IEEE 802.15.6/bluetooth low-energy WBAN transceiver for biotelemetry applications. IEEE Journal of Solid-State Circuits, 48(1) :186–198, January 2013.

[Woo01] Richard Wootton. Telemedicine. British Medical Journal, 2001.

[Xia11] Xiao Ming Zhang and Ning Zhang. An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and telemedicine. International Conference on Computer and Management (CAMAN), 2011.

[Yen08] Li-Hsing Yen and Wei-Ting Tsai. Flexible address configurations for tree-based ZigBee/IEEE 802.15.4 wireless networks. In 22nd International Conference on Advanced Information Networking and Applications (aina 2008). IEEE, 2008.

[Zha11] Min Zhang, Tao Yu, and Guo Fang Zhai. Smart transport system based on "the internet of things". Applied Mechanics and Materials, 48-49 :1073–1076, February 2011.

[Zha18] Haijun Zhang, Na Liu, Xiaoli Chu, Keping Long, Abdol-Hamid Aghvami, and Victor C. M. Leung. Network slicing based 5g and future mobile networks : Mobility, resource management, and challenges. IEEE Communications Magazine, 55(8) :138–145, August 2017.

[Zhu13] Xiaojun Zhu, Qun Li, and Guihai Chen. APT : Accurate outdoor pedestrian tracking with smartphones. In 2013 Proceedings IEEE INFOCOM. IEEE, April 2013.

[Zim96] T. G. Zimmerman. Personal area networks : Near-field intrabody communication. IBM Systems Journal, 35 :609–617, February 1996.

TABLE DES FIGURES

Liste des tables

Document réalisé avec LaTeX et :
le style LaTeX pour Thèse de Doctorat créé par S. Galland — http://www.multiagent.fr/ThesisStyle
la collection de paquets `tex-upmethodology` — http://www.arakhne.org/tex-upmethodology/

Résumé :

La télésurveillance médicale est un domaine encore en plein développement en France. C'est une branche de la télémédecine qui a pour vocation de permettre à un médecin de recueillir et d'interpréter à distance les données nécessaires au suivi médical d'un patient. Elle permet, entre autres, d'améliorer le suivi médical à distance des personnes âgées en perte d'autonomie ou atteintes de pathologies chroniques (insuffisance cardiaque, diabète et hypertension artérielle par exemple), et ainsi elle favorise leur maintien à domicile et prévient au plus tôt d'éventuelles hospitalisations. Cette Thèse CIFRE au sein de l'entreprise Maincare Solutions (éditeur majeur de solutions digitales pour le monde de la santé) nous a permis de proposer la nouvelle plateforme I^{2}PHEN (**I***oT* **I***nteroperable* **P***latform for* **HE***alth mo***N***itoring low power*) au sein de laquelle le suivi des paramètres de santé du patient est réalisé à l'aide d'objets connectés (tensiomètre, thermomètre, glucomètre, ...) qui communiquent avec la plateforme distante (monitoring de données distribuées). Le serveur de récupération peut alors déclencher des alertes, définies au préalable avec les équipes médicales. Le choix technologique des réseaux utilisés est un point majeur. En effet, les réseaux LPWAN (Low-Power Wide Area Network) offrent une alternative rentable et moins coûteuse en énergie que les réseaux cellulaires pour transmettre des petites quantités de données, sur des distances importantes et à partir de capteurs et d'objets faible puissance alimentés sur batterie. Ce domaine étant nouveau, et encore peu dédié au domaine médical, il a été nécessaire de développer de nouveaux axes de recherche comme COMMA, notre nouvel algorithme adaptatif pour réduire la consommation énergétique et les interférences en mobilités quotidiennes. Le premier verrou a été la consommation énergétique, en relation avec la qualité de service, de ces nouveaux réseaux dans le domaine critique de la santé. Le second verrou, et probablement le plus difficile, a été de proposer des solutions d'interopérabilité pour que les objets connectés puissent dialoguer via ces nouveaux réseaux avec la plateforme distante, par l'intermédiaire d'une passerelle locale (basée sur Arduino). Au final, la plateforme que nous proposons dans cette thèse permet le télémonitoring des patients de bout en bout, et sera interopérable et économe en énergie.

Mots-clés : Télémédecine, Télésurveillance, Objets Connectés, Réseaux, LPWAN, LoRaWan, Energie, Interopérabilité

Abstract:

Medical telemonitoring is an area still in full development in France. It is a branch of telemedicine which aims at enabling a doctor in collecting and interpreting remotely the data necessary for the medical follow-up of a patient. It enables, among others, in improving remote medical monitoring of seniors with loss of autonomy or suffering from chronic diseases (heart diseases, diabetes and high blood pressure for example). Hence it encourages their stay at home and to warn as soon as possible of any hospitalizations. We propose in this PHD our novel platform I^{2}PHEN (**I***oT* **I***nteroperable* **P***latform for* **HE***alth mo***N***itoring low power*) in which the monitoring of a patient's health parameters is done using connected objects (sphygmomanometer, thermometer, glucometer, ...) which communicates with the remote platform (distributed data monitoring). The central server can then trigger alerts which are defined beforehand with the medical teams. The technological choice of the networks used is a major concern. LPWAN networks (Low-Power Wide Area Network) offer a cost-effective alternative and are less expensive in terms of energy than cellular networks to transmit small amounts of data from sensors and energy efficient objects powered on batteries over important distances. This field being new, and still little dedicated to the medical field, it is necessary to develop new focus of research such as COMMA, a new adaptive algorithm to reduce energy consumption and interference in daily mobility. Hence, the first lock is the energy consumption, in relation to the quality of service (QoS), of these new networks in the critical area of telemedecine. The second lock, and probably the most difficult, is to propose interoperable solutions in which connected objects can interact, through these new networks, with the remote platform through a local gateway (based on Arduino). In the end, the platform that we propose in this PHD allows the telemonitoring of patients from end to end, is interoperable and energy efficient.

Keywords: Telemedicine, Medical Telemonitoring, Connected Objects, Network, LPWAN, LoRaWan, Energy, Interoperability

■ École doctorale SPIM 16 route de Gray F - 25030 Besançon cedex

■ tél. +33 (0)3 81 66 66 02 ■ ed-spim@univ-fcomte.fr ■ www.ed-spim.univ-fcomte.fr