Premier Rapport INF6404A : Développement des Couches Dispositifs, Communication et Réseaux

Alexandre Mao
David Johannès
Philippe Troclet
Fabien Berquez
Département Génie Informatique et Génie Logiciel
École Polytechnique de Montréal, Québec, Canada
alexandre.mao@polymtl.ca
david.johannes@polymtl.ca
philippe.troclet@polymtl.ca
fabien.berquez@polymtl.ca

11 mai 2016

1 Introduction

Le progrès établi dans les domaines scientifiques et technologiques a permis l'apparition et le développement de nouveaux objets, similaires à ceux que nous connaissons actuellement, mais avec la faculté supplémentaire d'être connectés à Internet. Ce déploiement d'Internet aux objets physiques est appelé Internet Of Things, ou IoT.

IoT représente donc une nouvelle manière de voir notre monde d'aujourd'hui, à savoir un monde où les objets communiquent entre eux, et sont interconnectés. Plus précisément, IoT est un « réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et sans fil, d'identifier et de communiquer numériquement avec des objets physiques afin de pouvoir mesurer et échanger des données entre les mondes physiques et virtuels » [1]

Bien évidemment, IoT a vu le jour afin de répondre à des problématiques importantes, notamment avoir la possibilité de fournir une mesure en continue de certaines variables, tout en minimisant les coûts technologiques, de maintenance, et en ressources humaines.

L'IoT peut ainsi être appliqué au Smart Health, à savoir être utilisé dans les soins cliniques où les patients, dont le statut physiologique nécessite une attention particulière, peuvent être surveillés en permanence en utilisant des

outils non invasifs et dirigés par l'IoT. Cela nécessite par conséquent des capteurs sans fils pour recueillir de l'information physiologique précise et complète, et implique d'utiliser des routeurs hybrides, permettant d'identifier les capteurs ne pouvant pas accueillir d'adresse IP, des passerelles (gateways) et le Cloud pour analyser et stocker les informations, puis pour envoyer (de manière sans fil) les données analysées aux aides-soignants et aux médecins pour une analyse et des examens plus approfondis.

Ces techniques permettraient d'améliorer la qualité des soins grâce à une surveillance constante et de réduire le coût des soins en éliminant la nécessité d'avoir activement et systématiquement un aide-soignant pour collecter et analyser les données.

En outre, la technologie peut être utilisée pour la surveillance à distance à l'aide de petites solutions connectées sans fil à travers l'IoT. Ces solutions peuvent être utilisées pour capturer des données en toute sécurité sur la santé des patients à partir d'une variété de capteurs, pour appliquer des algorithmes complexes pour analyser les données, puis pour les partager grâce à la connectivité sans fil avec les professionnels médicaux qui peuvent faire des recommandations de soins appropriées.

Il faut donc permettre aux applications de surveillance dans le domaine de la santé de collecter des données provenant de capteurs, de fournir un support pour les interfaces et les affichages de l'utilisateur, d'avoir une connexion au réseau pour l'accès aux services de l'infrastructure, et bien évidemment d'être robuste, durable, précis, fiable, et faible en consommation d'énergie [2].

Pour en revenir aux objectifs principaux de tels hôpitaux « intelligents », ils se résument à améliorer la qualité de vie des personnes qui ont besoin de surveillance permanente, à diminuer les barrières concernant la surveillance d'importants paramètres de santé, à éviter les coûts et les efforts de santé inutiles, et à fournir un support médical juste et approprié au bon moment.

Dans le cadre de nos laboratoires, nous nous intéresserons donc aux hôpitaux, et plus particulièrement aux services de soins intensifs qui nécessitent une surveillance permanente de patients (qu'ils soient animés ou inanimés, et l'utilisation de hautes technologies de mesure. Le but de nos laboratoires sera alors d'apporter une solution IoT face à la congestion des hôpitaux, et plus précisément dans les services de soins intensifs, en distinguant plusieurs cas d'utilisation (patients inanimés ou non). Notre premier laboratoire consistera à décrire les différents dispositifs qu'il est possible d'utiliser dans notre cas, ainsi que les protocoles de réseau et de communication qu'il faudra appliquer pour permettre à nos dispositifs de communiquer entre eux. Aussi, nous établirons en dernier lieu les problématiques liées à notre solution.

2 Les Dispositifs

Les hôpitaux fournissent à la population un service essentiel et vital, mais de nombreux problèmes se présentent à eux. Ils peuvent faire faceà des périodes de fortes affluences, ce qui peut amener à une congestion au niveau du traitement des patients. L'un des défis majeurs que rencontrent les hôpitaux est donc la gestion de ces périodes, ce qui passe par la gestion efficace du temps de son personnel et l'optimisation du service qu'il fournit. Et dans certains départements, le personnel médical doit être omniprésent auprès des patients pour un suivi de l'évolution des cas les plus critiques, ce qui a pour conséquence une augmentation du besoin de personnel et ainsi un sur-coût non-négligeable pour l'hôpital. L'IoT a déjà permis de grande économie dans le domaine de la santé grâce au télésuivi des malades chroniques, avec des économies dépassant les 30 milliards de dollars.[3]

Nous allons nous intéresser dans notre cas, à un département de l'hôpital qui requiert une forte présence humaine et gestion très attentive et minutieuse. Ce département est celui des soins intensifs :

≪ Les unités de soins intensifs (ou USI) sont des services hospitaliers spécialisés dans la prise en charge des patients inanimés ou particulièrement malades nécessitant une surveillance permanente. De manière générale, les services de soins intensifs ont pour mission de maintenir en vie des patients en état critique dont le pronostic vital est engagé dans la mesure où leurs fonctions vitales sont affectées. En soins intensifs, les malades sont surveillés par des équipes spécialisées disposant d'un matériel de haute technicité. ≫ [4]

Le système que nous allons proposer va avoir pour but de surveiller l'état des patients de manière continue et de telle sorte à ce que ces informations soient transmises rapidement au personnel médical et permettent ainsi un suivi de l'évolution de la santé du patient plus facile. Le système que nous proposons a pour but d'optimiser le temps passé par le personnel médical auprès du patient et de s'occuper de surveiller certaines fonctions vitales et environnementales du patient tout en permettant d'indiquer au personnel médical toute anomalie détectée. Il a aussi pour but de réduire les erreurs médicales liées aux fautes humaines.

Nous présentons dans ce qui suit un ensemble d'appareils connectés destinés à surveiller le patient lors de sa présence dans les unités de soins intensifs jusqu'à sa sortie de celui-ci (transition d'un service à un autre par exemple) en fournissant un ensemble de capteurs et d'autre dispositifs pour permettre ce suivi lors de son séjour à l'hôpital. On décrira donc dans un premier temps les différents dispositifs nécessaires pour surveiller le patient et son environnement (les diverses conditions de sa chambre). Une telle mise en place de ces dispositifs est illustrée sur la Figure 1. Les capteurs spécifiques représentent les capteurs qui ne sont appropriés que pour certains cas particuliers d'état du patient (coma, diabète, blessure grave, cancer).

On décrira ensuite les dispositifs nécessaires à mettre en place sur le patient pour le surveiller lors de son passage du service de soins intensifs à un autre service, jusqu'à sa sortie de l'hôpital. Cette situation est illustrée par la Figure

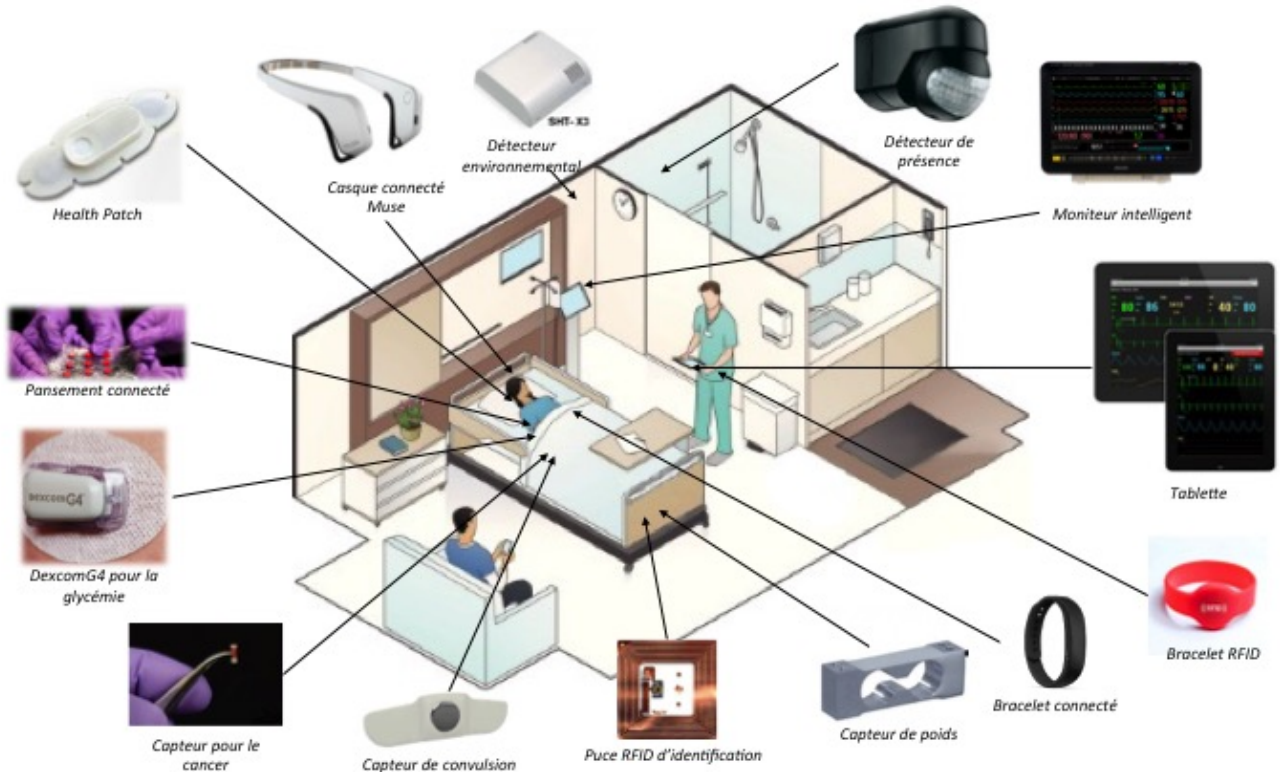

FIGURE 1 – Dispositifs dans la Chambre du Patient

2. En effet, une fois que le patient peut sortir de l'unité des soins intensifs, il est nécessaire de continuer à le surveiller encore quelques temps avant de lui permettre de sortir de l'hôpital.

Nous allons tout d'abord définir les capteurs généraux qui pourront être utilisés sur tous les patients admis dans le département de soins intensifs. Un patient présent en soin intensif nécessite une surveillance accrue. Pour cela, nous avons mesuré certains paramètres vitaux spécifiques comme la fréquence respiratoire, le rythme cardiaque, la température du corps et la pression sanguine, avec des capteurs qui nous permettront d'obtenir ces informations essentielles sur l'état du patient. Dans notre recherche des technologies IoT actuelles, il s'avère que le patch Health Patch [5] permet de mesurer toutes ces variables, ainsi que de surveiller les phases de sommeil du patient, ce qui a pour avantage de regrouper plusieurs capteurs en un seul élément (ici sur un seul patch). Du fait de la surveillance nécessaire de certains paramètres vitaux en continu et en temps réel (notamment la fréquence respiratoire et le rythme cardiaque), nous avons réfléchi à une récupération des données à chaque demie seconde, pour être rapidement prévenu en cas d'anomalie et de permettre au personnel soignant

FIGURE 2 – Dispositifs pour un patient classique

d'intervenir rapidement en cas d'urgence.

A ces capteurs qui seront mis sur chaque patient, nous allons nous intéresser à des cas plus spécifiques.

Pour les patients souffrant de cancer et recevant un traitement approprié, il est intéressant de pouvoir mesurer l'efficacité de celui-ci. Ainsi, un capteur qui permettrait de suivre l'évolution d'un cancer [6] pourrait être placé sur cette catégorie de patients , et serait alors placé au cœur de la tumeur. Grâce à un système de communication sans fil, le capteur récolterait des informations sur la tumeur, à savoir sa concentration en oxygène et son acidité. Il les enverra en temps réel à un récepteur. Ces deux informations permettront aux médecins de savoir si le traitement administré au patient fonctionne ou non. En effet, si une tumeur s'acidifie de plus en plus, alors le traitement marche. Une hausse du taux d'oxygène est aussi un bon indicateur car elle révèle que la tumeur ne peut pas se développer (celle-ci se développant dans un milieu faible en oxygène). Il n'est pas nécessaire de relever les mesures très fréquemment, étant donné la faible évolutivité d'une tumeur. Par conséquent, une transmission de ces variables toutes les heures est suffisante.

Certains patients en soins intensifs peuvent souffrir de diabète. Il est alors nécessaire de pouvoir relever le taux de glycémie dans le corps du patient. Alphabet a développé le DexCom [7] qui est un pansement connecté permettant de surveiller le taux de glycémie à travers la peau. Il possède l'avantage de ne pas piquer le patient pour effectuer cette mesure. Il pourra ainsi aider le personnel

soignant à administrer les quantités d'insuline appropriées tout en apportant un confort d'utilisation au patient. Au niveau de la fréquence de la mesure du taux de glycémie, une collecte d'informations chaque quart d'heure est suffisante, car le taux de glycémie peut varier modérément dans le temps.

Un autre de nos objectifs pour améliorer l'efficacité et la qualité de la surveillance du patient est de permettre d'avoir des capteurs qui puissent évaluer la cicatrisation de diverses blessures. Un pansement connecté et autonome [8], qui est un objet flexible et présentant une bonne adhésion grâce au matériau le constituant, semble approprié. Ainsi, il serait possible d'intégrer des capteurs à l'intérieur du pansement, situé à la surface de la peau du patient. Ces capteurs permettront de vérifier l'état des blessures et l'évolution de la cicatrisation. Il pourra aussi signaler une infection sur la plaie. Une mesure toutes les 10 minutes est suffisante, car une blessure cicatrise assez lentement dans le temps.

Il est fréquent de recevoir dans le service des soins intensifs des patients inanimés ou dans le coma. Il devient alors nécessaire de mesurer l'activité cérébrale de ces patients et de surveiller en continu, c'est-à-dire à un interval de l'ordre de la seconde . Un capteur peut alors être mis en place pour suivre l'activité cérébrale du patient. Nous avons vu l'exemple du casque Muse [9], qui « utilise des capteurs pour identifier les ondes générées par l'activité du cerveau. Les algorithmes de Muse détectent les changements subtils dans le cerveau et montrent l'activité en temps réel ». Cependant, ce dispositif est utilisé actuellement pour le divertissement. On peut néanmoins supposer qu'un tel type de capteur peut être modifié à des fins médicales.

Une autre variable qui pourrait intéresser le médecin est le poids du patient tout au long de son séjour à l'hôpital. C'est pourquoi un capteur de force, placé au niveau du lit, et permettant de relever le poids du patient régulièrement, serait utile. Il serait suffisant de relever le poids du patient dans des intervalles de temps assez larges, par exemple toutes les 12 heures, étant donné que cette variable évolue très peu d'un jour à l'autre (dans des conditions normales d'alimentation).

Afin de vérifier à n'importe quel moment où se situe le patient, il est important de pouvoir permettre sa localisation et traçabilité [10] assez fréquemment (toutes les 5 secondes, étant donné que le patient va passer une grande partie de son séjour dans le lit), cela pourrait être fait à l'aide d'un bracelet qui serait placé au niveau de son poignet.

Nous pouvons aussi voir si le patient peut présenter des convulsions, avec un capteur [11] qui peut être posé pour mesurer les mouvements du patient toutes les secondes (ce capteur déclencherait une alarme s'il relève une trop forte variabilité du mouvement du patient sur une petite période).

Il serait possible également de placer des capteurs de présence dans la chambre et les diverses pièces de la zone du patient (salle de bain, toilettes) afin de détecter la présence d'un patient dans ces pièces et le localiser dans sa zone. Ces capteurs n'auraient besoin de relever les données qu'à des intervalles de temps de plusieurs secondes, étant donné que l'on considère que le patient va se déplacer lentement tout au long de son séjour. Cela permettrait aussi à l'hôpital de connaître en quasi-temps réel l'occupation de ces chambres.

Tous les dispositifs décrits jusqu'à présent peuvent être reliés à un moniteur principal intelligent, qui va centraliser toutes les informations récupérées de ces dispositifs pour les relayer au serveur de l'hôpital. Ce moniteur central pourra également agir sur la perfusion possiblement reliée au patient afin d'administrer automatiquement et précisément un certain traitement, qui dépend des informations qu'il aura collecté ou en fonction des indications du personnel médical. Par exemple, en collectant des informations sur le taux de glycémie du patient, le moniteur pourrait contrôler l'injection d'insuline nécessaire pour la santé du patient. Dans le cas où certains dispositifs devraient envoyer des informations directement sur le réseau, des routeurs hybrides pourraient être mis en place pour faire la traduction des identifiants qui seraient attribués aux dispositifs ne pouvant pas accueillir d'adresses IP, tout en permettant le routage classique par IP.

Une puce RFID (Radio Frequency Identification) [12] pourrait également être placé au pied du lit du patient afin de permettre au médecin qui vient dans la chambre de pouvoir le scanner pour un accès rapide au dossier du patient. La puce RFID sera mise à jour chaque fois qu'un lecteur RFID essayera de la lire et lui enverra éventuellement les nouvelles données qui ont été modifiées.

Des capteurs pourront être placés pour surveiller l'environnement du patient (toutes les minutes) afin de lui procurer un environnement optimal dans sa phase de guérison. Pour cela, proposons de placer des capteurs d'humidité, de température, de luminosité, [13] et de fumée qui vont servir à surveiller l'environnement de la chambre du patient.

Une fois que l'état du patient s'est améliorée et que celui-ci lui permet de quitter le service des soins intensifs, et dans un contexte de suivi optimal du patient, certains dispositifs pourraient lui être appliqués, comme à tout patient dans l'hôpital, pour suivre son état en phase de rétablissement. Il peut être nécessaire de surveiller encore certaines variables, pour vérifier que son état de santé est normal, et ce jusqu'à sa sortie de l'hôpital.

Dans ce but, nous proposons de maintenir la mesure de la fréquence respiratoire, du rythme cardiaque, de la température du corps, et de la pression sanguine, à savoir avoir un dispositif similaire à Health Path qui fournit ces mesures à des intervalles de temps de la seconde. D'après les technologies actuelles, Vital Patch [14], qui se base sur la même technologie que Health Patch, propose de fournir ces mesures, et est approprié pour cette situation où le patient sera plus libre de ses mouvements et pourrait se déplacer plus régulièrement dans l'hôpital.

Certains dispositifs pourraient être gardés ou mis en place selon les caractéristiques de santé du patient. Par exemple si le patient est diabétique, le même capteur de glycémie que décrit précédemment (DexCom) peut être maintenu pour avoir une mesure régulière de son taux de glucose.

Enfin, afin de permettre de localiser approximativement le patient, mais aussi permettre aux médecins d'avoir accès au dossier du patient, un bracelet muni d'une puce RFID (avec l'architecture appropriée pour proposer la localisation et les données du patient) peut être placée, sous forme de bracelet, au poignet du

patient. Ainsi, nous aurions des lecteurs RFID disséminés un peu partout dans l'hôpital pour détecter les bracelets RFID des patients, et ainsi les localiser. Plus précisément, les lecteurs RFID seront placés un peu partout dans les couloirs de l'hôpital, et à l'entrée de chaque chambre, et reliés au réseau de l'hôpital.

Certains appareils ou capteurs pourraient intervenir dans l'amélioration du travail du personnel médical pour leur apporter une aide supplémentaire, par exemple du côté du personnel soignant, et en particulier des médecins, des bracelets RFID [15] pourraient leur être fournis (comme pour les patients), dans le but de les localiser et permettre, en cas d'alerte sur un patient, de prévenir l'aide-soignant ou le médecin le plus proche (et maîtrisant la spécialité ou les compétences correspondant au problème détecté).

3 Protocoles de Communication et Réseaux

L'internet des objets est étroitement lié à Internet, les réseaux de communications mobiles et les capteurs sans fil. L'IoT est un réseau qui interconnecte des objets physiques avec des adresses identifiables pour fournir un service supplémentaire. Il n'est pas seulement constitué d'ordinateurs, de smartphones, etc.. mais aussi d'appareils de plus en plus petits comme des étiquettes ou puces RFID, des capteurs et d'autres appareils qui n'ont pas forcément les capacités d'accueillir les moyens d'adressage classique par IP. Nous avons pour cela étudié différents protocoles de communication possibles pour ces appareils. La Figure 3 illustre les protocoles de communication que nous avons choisi pour notre solution IoT de Smart Health.

Nous avons commencé par l'évaluation de différents protocoles physiques de communication, correspondant aux couches 1 (physique) et 2 (liaison) du modèle standard OSI. Les tableaux 1, 2, et 3 [16] [17] résument les caractéristiques de ces protocoles (et proposent une comparaison de ceux-ci) pour les différentes couches (réseau, application, et physique).

Protocoles	**Avantages**	**Inconvénients**
IPv6	- Nombre presque illimité d'adresses - Protocole éprouvé - Permet une communication simple	- Protocole lourd, beaucoup de capteurs ne peuvent l'utiliser
6LoWPan	- Faible consommation énergétique - Offre des fonctionnalités similaires à IPv6	- Toujours tributaire de l'énergie pour la sécurité

Table 1 – Protocoles pour la Couche Réseau

L'utilisation de nombreux capteurs, sur un patient susceptible de bouger à la fois dans son lit voire dans la pièce impose l'utilisation de protocoles sans fils, pour que la mobilité de la personne soit prise en compte. Les différents protocoles sans fil existants sont décrits ci-dessous.

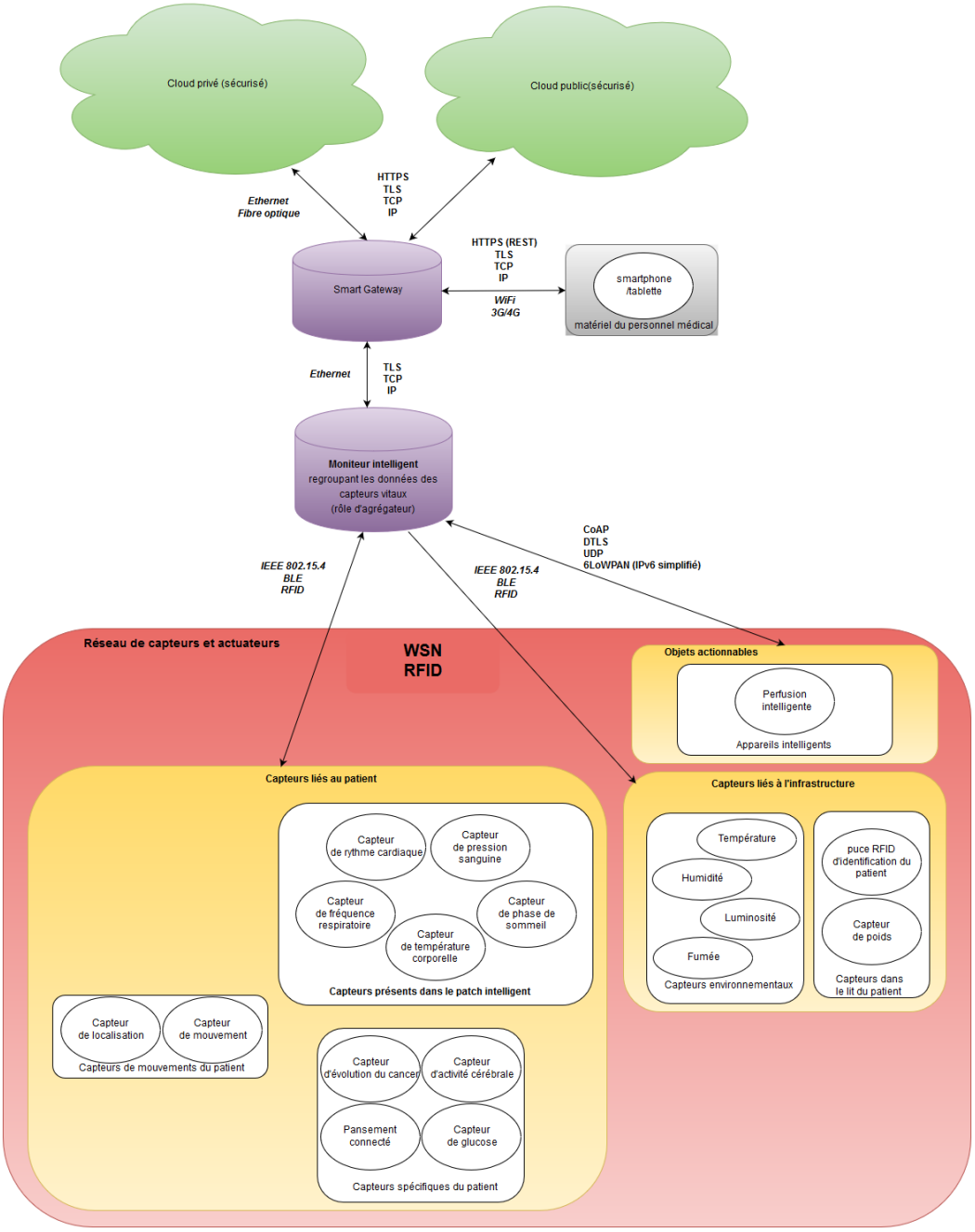

FIGURE 3 – Protocoles de Communication et Réseaux de notre Système

Protocoles	Avantages	Inconvénients
CoAP	- Support pour le multicast - Compatible avec une interface web - Permet le “machine to machine” - Mode d’adressage simple - Économe - Permet de communiquer le contexte d’un message - Support natif de PUT, POST, GET	- Mode de communication Request/Respond pas adapté pour la récupération fréquente de données
XMPP	- Adressage simple - Économe - Mécanisme publisher/suscriber pratique pour la récupération des données - Protocole extensible - S’interface facilement avec du web	- Pas de support natif pour le multicast (se base sur une extension) - Peu évoqué dans les articles - Pas de support pour QoS
MQTT	- Économe - Publish/suscrib - Machine to machine(M2M)	- Pas de support pour le multicast - Pas mentionné dans la littérature

Table 2 – Protocoles de Communication pour la Couche Application

Caractéristique	Zigbee	Bluetooth Low Energy	Bluetooth	Wi-Fi
IEEE	802.15.4	802.15.1	802.15.1	802.11a/b/g/n/ac
Besoins mémoire	4-32 ko		250 ko +	1 Mo +
Autonomie avec pile	Années	Années	Mois	Jours
Nombre de nœuds	65000+	illimité	255	256+
Vitesse de transfert	20-250 kb/s	1 Mb/s	1-3 Mb/s	11-54-108-320-1000 Mb/s
Portée (environ)	10 m	10 m	10 m	100 m

Table 3 – Protocoles pour la Couche Physique

Le WiFi (Wireless Fidelity) [18], normalisé sous la forme IEEE 802.11 permet la communication sans fil des différents composants dans des réseaux ad-hocs ou plus centralisés, suivant le protocole IP. Cependant, le WiFi soulève un certain nombre de problèmes, le plus important étant l’utilisation des ressources énergétiques pour la transmission, qui n’est pas supportable pour de petits capteurs.

Le Bluetooth [19], normalisé IEEE 802.15.1, est également un protocole de communication sans fil possible, mais présente certains inconvénients majeurs : la dépense énergétique associée à la transmission est assez importante, et donc peu supportable pour de petits capteurs, et ses limitations intrinsèques (un périphérique maître Bluetooth ne peut avoir que 7 périphériques esclaves) ne lui donnent pas la propriété de scalabilité recherchée dans l’IoT, où le nombre de capteurs peut augmenter fortement. Ce procédé de communication n’a donc pas été retenu dans notre architecture.

Une fois ces protocoles trop consommateurs en énergie exclus, nous avons

conservé trois protocoles sans fil majeurs.

La transmission radio-fréquence (IEEE 802.15.4) [20] [21] est une possibilité, relativement peu coûteuse en énergie, proposant un faible débit (de 20 à 250 kbit/s) et un mécanisme d'évitement des collisions lors de la transmission. Par ailleurs, la faible portée des émissions (de 10 à 25 m) est intéressante dans une optique de réseau très localisé (autour du lit du patient) s'appuyant sur un point central. Par ailleurs le protocole IEEE 802.15.4 propose un mécanisme d'allocation automatique d'adresses de 16 ou 64 bits, ce qui est pratique pour offrir une flexibilité d'adressage avec un nombre de capteurs variable.

Le Bluetooth Low Energy (BLE) [22] est une variante du Bluetooth offrant des débits raisonnables tout en pouvant fonctionner sur des appareils de faible puissance et avec une faible batterie. Par ailleurs, BLE revient sur certaines limitations du Bluetooth comme le nombre de noeuds pouvant être connectés à un même appareil. Cette limite passe de 7 à plus de 65 000, ce qui laisse une marge appréciable pour des réseaux de capteurs. Un inconvénient de ce système est sa non compatibilité avec des appareils Bluetooth standard.

RFID est un protocole et un appareil sans fil à faible portée qui peut être ajouté à n'importe quel appareil pour le rendre "intelligent". On peut alors interagir avec ces objets via un lecteur RFID, qui peut généralement également écrire. L'avantage principal de ce système est que la puce RFID n'a absolument pas besoin d'une source d'énergie. L'énergie nécessaire à la lecture est fournie par les ondes provenant du lecteur.

Le protocole Zigbee se base sur des ondes radios (norme IEEE 802.15.4), est à basse consommation d'énergie et permet une communication à courte distance, comme Bluetooth mais de manière moins complexe et moins cher.

Enfin, NFC [23] se base sur un mélange entre RFID et BLE. NFC peut être couplé avec un système d'authentification renforcé pour offrir une plus grande sécurité d'accès, tout en permettant la lecture de ses informations comme on pourrait le faire pour une puce RFID classique. Cependant son inconvénient principal est la portée de lecture, qui impliquerait au lecteur d'être très proche (pas plus de quelques centimètres) de l'appareil comportant la puce NFC.

En se basant sur ce comparatif, nous avons choisi pour le système de notre Smart Hôpital de ne pas utiliser certains protocoles qui ne nous semblent pas adapter à notre architecture : WiFi et Bluetooth pour des raisons énergétiques, NFC pour des raisons de portée et Zigbee auquel on a préféré BLE pour des raisons d'homogénéité dans notre architecture. Nous avons également choisi, dans un soucis de laisser une bonne diversité de capteurs possibles, que notre système de Smart Hôpital pourrait gérer différents protocoles parmi les plus répandus : IEEE 802.15.4 (radio), BLE et RFID, qui sont tous les trois prometteurs vis-à-vis des restrictions des capteurs, tout en offrant un certain nombre de mécanismes de sécurité (particulièrement BLE).

Après avoir étudié les protocoles physiques, intéressons nous aux protocoles de la couche 3.

Le protocole classique de la couche 3 est bien entendu le protocole IP. IPv4

n'est pas envisageable pour l'IoT, en raison du manque d'adresses disponibles par rapport à la quantité croissante d'objets à connecter, et donc à adresser. IPv6 [24] résout ce problème, avec un nombre d'adresses virtuellement illimité, et représente un protocole éprouvé et adapté à de nouvelles problématiques. Cependant, les besoins d'IPv6 en calcul et en stockage, notamment du fait de ses différents entêtes le rend inutilisable en tant que tel sur de nombreux capteurs.

Face à l'IPv6 classique, une alternative a été développée afin de tenir compte de ressources limitées des différents capteurs utilisés sur IoT, mais également des possibilités de transmission limitées de certains protocoles, comme IEEE 802.15.4 dont les trames sont beaucoup plus petites que celles d'IPv6. Cette alternative est 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network) [25], un protocole venant au dessus d'IEEE 802.15.4 consistant en une simplification d'IPv6 par la diminution des entêtes nécessaires (toutes celles pouvant être déduites par le contexte ne sont pas transmises), et une meilleure gestion de la fragmentation des trames IPv6 par les protocoles de la couche inférieure. Ceci le rend utilisable sur des capteurs qui ne pourraient pas autrement utiliser IPv6. Par ailleurs, la diminution du stockage et du calcul nécessaire entraîne également une baisse du coût énergétique de transmission du paquet. Compte tenu de l'utilisation que nous avons prévu des émetteurs et récepteurs radio (IEEE 802.15.4), nous avons retenu ce protocole comme protocole de couche 3.

Enfin, le système que nous concevons est destiné à fonctionner grâce à des applications à la fois pour téléphones ou tablettes, sur des serveurs ou des agrégateurs. Nous aurons donc besoin de prendre en compte la communication au niveau applicatif, c'est à dire la couche 7 du modèle OSI, et de choisir de façon adéquate les protocoles applicatifs utilisés afin de simplifier le travail de développement des applications.

Dans notre recherche dans la littérature académique sur IoT, un certain nombre de protocoles ont été proposés. Nous nous intéresserons ici à trois protocoles particuliers, XMPP, MQTT et enfin Constraint Application Protocol (CoAP).

XMPP [26] est un protocole ouvert permettant l'échange de messages. Présenté comme un protocole phare de l'IoT, il permet un adressage simple des capteurs, via une adresse proche des adresses mail. Une de ses forces est la présence d'un mécanisme de type "Publish-Subscribe", c'est-à-dire un mécanisme où une application intéressée s'enregistre (subscribe) auprès du capteur (publisher) afin d'être notifiée lorsque la valeur du capteur évolue. Ceci permet de limiter la bande passante utilisée, par rapport à un envoi périodique des informations. Un de ses inconvénients est sa faible utilisation dans des exemples concrets de systèmes ce qui nous ne permet de vérifier sa fiabilité en situation réelle.

MQTT (Message Queue Telemetry Transport) [27] est un autre protocole applicatif offrant un mécanisme de type publish-subscribe. Il gère également la communication Machine to Machine, mais est là aussi assez peu présent dans la littérature et dans les systèmes réels.

Constraint Application Protocol (CoAP) [28] est un protocole applicatif qui possède de nombreux points communs avec HTTP, bien qu'étant bien plus léger.

En particulier, il supporte l'adressage des capteurs et appareils par une adresse de type URI, et il fonctionne sur un système de requêtes/réponses, supportant comme HTTP quatre méthodes de requêtes : GET, PUT, POST et DELETE. Ces deux caractéristiques facilitent l'utilisation d'API de type REST (fréquentes dans les applications mobiles), et la traduction de HTTP vers CoAP et inversement. De plus, CoAP permet de préciser un type de données transmis, comme le type MIME avec HTTP, ce qui facilite la connaissance du contexte et améliore la sémantique des données transmises. Enfin, CoAP est peu exigeant en capacité de stockage et en énergie, efficace grâce à des entêtes réduites (meilleur ratio de charge utile), et, pouvant s'appuyer sur UDP et DTLS, ce qui permet une sécurisation des données.

Compte tenu de ces avantages, et la possibilité que nous souhaitons fournir aux médecins et au personnel hospitalier de voir les différentes informations fournies par les capteurs à travers des applications, nous avons donc choisi CoAP pour la communication applicative avec nos capteurs.

4 Considérations en Sécurité, privacité et Quality of Service (QoS)

Les informations issues des divers capteurs peuvent, dans une certaine mesure, représenter un risque pour la vie privée des patients. De ce fait, des mesures doivent être prises pour assurer la confidentialité de ces données. De même, si de fausses informations venaient à être transmises au moniteur, ou à la "smart gateway" voire à la base de données, cela pourrait avoir de graves conséquences. L'intégrité des données est donc primordiale. En effet, si une personne mal intentionnée envoyait de fausses informations au moniteur cela pourrait déclencher des alarmes qui entrainerait une mauvaise gestion du temps du personnel hospitalier qui serait réquisitionné inutilement, ou pourrait modifier ou actionner certains appareils qui, mal utilisés, pourraient nuire au patient. De plus, si les données envoyées sur le cloud ne sont pas contrôlées, il y a possiblement un risque pour le patient. Par exemple, si une personne parvient a supprimer du dossier du patient les allergies de ce dernier, il devient alors possible que le personnel lui donne des médicaments ou aliments dangereux pour sa santé.

Par ailleurs, il est évident que l'accès au dossier du patient doit être restreint afin que seules les personnes impliquées puissent le consulter. Certains travaux évoquent la potentielle nécessité de contrôler l'accès afin que seul le médecin attribué à la personne soit en mesure de lire les informations du patient. Toutefois, notre étude se fait au sein d'un service de soins intensifs. Aussi, en cas d'urgence, il est nécessaire que tous les médecins puissent intervenir. Ainsi, le médecin ou l'infirmier le plus proche pourrait prendre le patient en charge. Un contrôle aussi fin n'est donc pas approprié dans notre cas.

Il serait donc nécessaire d'avoir un contrôle d'accès et un chiffrement des données. On peut aussi souligner qu'une certaine qualité de service (QoS) est nécessaire pour que le système soit utilisable. En cas d'anomalies, les médecins

doivent être prévenus dans un bref délai puisque nous sommes en présence de capteurs récupérant des données vitales.

Nous allons donc étudier les caractéristiques des protocoles présentés auparavant.

Dans notre architecture, les patients pourraient avoir un bracelet ou une puce RFID qui permettrait de récupérer leurs informations afin d'améliorer le traitement. Le médecin pourrait récupérer l'historique du patient et les bracelets RFID des médecins permettraient de les situer et de connaître leur domaine de compétence (la fatigue du médecin pourrait également être déduite via le nombre d'heures de travail enregistrées). En cas d'urgence, le médecin ayant le bon domaine de compétences ou le plus proche pourra être envoyé pour la traiter. Les lecteurs utiliseraient les ondes électromagnétiques pour communiquer avec les puces RFID. Mais, il n'y a aucun moyen de sécuriser un tel canal (par exemple, l'authentification est impossible). C'est pourquoi le stockage des informations ne se fera pas directement sur les puces RFID, où l' on stockera un id qui permettra d'obtenir ces informations depuis la base de données dont l'accès sera, lui, sécurisé. Cet id, devra, de préférence n'avoir aucun rapport avec des informations personnelles de la personne. Cette base de données ne serait accessible que par une certaine application (sur tablette, smartphone ou via une interface web) qui serait la base pour un contrôle d'accès strict.

Par ailleurs, afin de garantir une bonne QoS, il faudra limiter les interférences entre les différents éléments RFID et s'assurer qu'ils sont sur une structure adéquate. Pour cela, on peut imaginer des antennes orientées de puissances variables.

BLE pour Bluetooth Low Energy, peut chiffrer ses données via AES-128 et possède des mécanismes d'authentification (par exemple : passkey, ou encore recopier des séquences depuis un écran). Afin d'éviter une attaque "man in the middle", il est nécessaire d'effectuer cette étape. Elle devra être faite manuellement par le personnel hospitalier.

La sécurité sur 6LoWPAN reste un challenge. En effet les divers mécanismes de protection sont gourmands en ressources (IPSec, TLS) et pas nécessairement applicables à un capteur. De plus, l'algorithme d'échange de clés n'est pas précisé par le standard. Notons que des mécanismes éprouvés sont présents au niveau application (exemple : DTLS). De plus, au niveau de la couche MAC, il y a la possibilité d'utiliser le chiffrement AES. Pour résumer, des mécanismes de sécurité sont présents mais la faible capacité des capteurs pose problème. Et, le fait de devoir diviser le paquet IPV6 augmente le nombre de pertes potentielles.

Le protocole TLS (Transportation Layer Security) utilisé pour sécuriser une connexion, pourrait, dans notre cas, garantir la sécurité lors des échanges entre le moniteur et la "smart gateway", et serait sûrement un des éléments essentiels de la sécurité lors d'envois sur la base de données (via HTTPS par exemple). Ce protocole permet d'identifier les deux partis (via des certificats), puis d'établir

une session sécurisée en créant une clé de session. Dans notre cas, l'identification des deux membres étant obligatoire : on identifie le serveur pour éviter des attaques type "man in the middle" et le client pour interdir l'envoi de données falsifiées. Ainsi, le moniteur doit posséder un certificat racine de l'hôpital qui serait utilisé pour certifier l'ensemble des dispositifs de ce dernier.

Concernant la QoS, une première mesure afin d'améliorer la disponibilité et donc de permettre aux médecins d'être notifiés rapidement en cas de variations anormales, serait de connecter les moniteurs via Ethernet au réseau de l'hôpital. Cela permettrait une plus grande capacité et limiterait le nombre d'interférences liés aux ondes. Par ailleurs, une telle méthode permettrait de ne pas causer de dysfonctionnement avec d'autres appareils sensibles comme un scanner. Une autre mesure serait l'utilisation d'UDP (avec sa surcouche DTLS) pour l'envoi de données fréquentes au Smart Gateway depuis le moniteur. Par données fréquentes, nous entendons des données qui sont fréquemment mises à jour. Ainsi, pour de telles données, la perte de quelques paquets de manière épisodique n'est pas pénalisante en soi, car un nouveau paquet sera envoyé très peu de temps après, mais un mécanisme applicatif devra détecter les pertes consécutives et déclencher des avertissements afin qu'un membre du personnel de l'hôpital aille vérifier l'état du capteur concerné. En revanche, pour les mesures prises de façon plus rares, il est nécessaire d'avoir un mécanisme d'accusé de réception (comme par exemple celui offert par TCP) afin de ne pas perdre de données.

Enfin, le système doit être disponible et fiable. Dès qu'une mesure anormale est détectée, il faut connaître la raison de cette anomalie. Si elle provient de l'appareil il faut que celui-ci soit vérifié et changé si besoin est. Pour cela, on pourrait s'appuyer sur la fabrication d'un appareil qui intégrera certains cas de défaillance et en avertira un technicien, qui pourra être envoyé pour vérifier les capteurs pour des valeurs non conformes. Pour les autres anomalies détectées, un membre du personnel médical sera envoyé sur place. Ce serait alors à lui de vérifier que les données sont bien reliées au patient et non une erreur du dispositif, et d'appeler un technicien le cas échéant. Par ailleurs, il est nécessaire de mettre un place un timeout afin de lancer une alerte en l'absence de données durant un certain laps de temps. Selon les informations que caractérisent ces données, l'alerte ne sera pas la même. En effet, le dysfonctionnement d'un capteur selon ce qu'il mesure (fréquence cardique, température de la salle) n'a pas le même impact. Aussi, il y a une hiérarchisation du signal envoyé (alerte, avertissement, notification) selon la gravité de la panne afin que les pannes les plus graves soient traitées en premier. Cette hiérarchisation est illustrée sur la Figure 4.

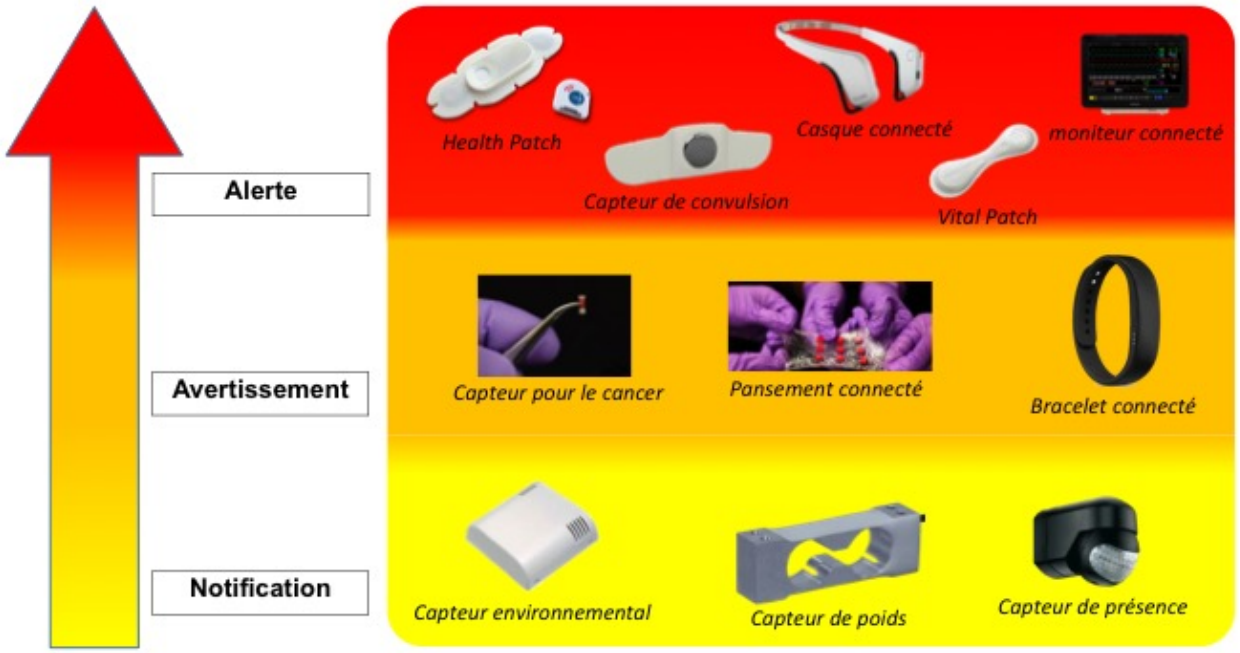

FIGURE 4 – Hiérarchie du Signal en fonction du Dispositif

5 Conclusion

Références

[1] Pierre-Jean Benghozi, Sylvain Bureau, and Françoise Massit-Folléa. *L'Internet Des Objets/The Internet of Things : Quels Enjeux Pour L'Europe ?/What Challenges for Europe ?* Les Editions de la MSH, 2009.

[2] Ovidiu Vermesan and Peter Friess. *Internet of Things-From research and innovation to Market Deployment*. River Publishers, 2014.

[3] [infographie] la transformation digitale de l'hôpital. `http://www.orange-business.com/fr/blogs/e-sante/hopital-numerique/infographie-la-transformation-digitale-de-l-hopital`.

[4] Soins intensifs - définition, 2016. `http://sante-medecine.journaldesfemmes.com/faq/45101-soins-intensifs-definition`.

[5] Healthpatch® md, 2016. http://www.vitalconnect.com/healthpatch-md.

[6] Santé : suivre l'évolution d'un cancer grâce à un capteurd, 2015. http://www.objetconnecte.net/sante-cancer-capteur-2108/.

[7] Alphabet et dexcom ensemble contre le diabète, 2015. http://www.objetconnecte.net/alphabet-dexcom-diabete-2608/.

[8] Le pansement connecté futuriste et autonome, 2015. http://www.objetconnecte.net/pansement-connecte/.

[9] Muse, le bandeau capteur d'activité cérébrale, 2014. http://webdesobjets.fr/muse-le-bandeau-capteur-dactivite-cerebrale/.

[10] Localisation et traçabilité des patients, 2016. http://www.hellopro.fr/localisation-et-tracabilite-des-patients-10290-fr-1-feuille.html.

[11] Ces 2016 – tucky, le patch qui surveille les enfants malades, 2016. http://www.lesnumeriques.com/objet-connecte/e-takescare-tucky-p30533/ces-2016-tucky-patch-qui-surveille-enfants-malades-n48553.html.

[12] Radio-identification, 2016. https://fr.wikipedia.org/wiki/Radio-identification.

[13] Capteur humidité, température et luminosité - gce electronics, 2016. http://www.planete-domotique.com/capteur-humidite-temperature-et-luminosite-gce-electronics.html.

[14] Vitalpatch^{TM}, 2016. http://www.vitalconnect.com/vitalpatch.

[15] Système de localisation du personnel hospitalière par rfid active. http://www.kimaldi.com/kimaldi_fre/secteurs/geriatriques_et_centres_sanitaires/systeme_de_localisation_du_personnel_hospitaliere_par_rfid_active.

[16] Zigbee. https://fr.wikipedia.org/wiki/ZigBee.

[17] Luca Catarinucci, Danilo De Donno, Luca Mainetti, Luca Palano, Luigi Patrono, Maria Laura Stefanizzi, and Luciano Tarricone. An iot-aware architecture for smart healthcare systems. *Internet of Things Journal, IEEE*, 2(6) :515–526, 2015.

[18] Wi-fi, 2016. https://fr.wikipedia.org/wiki/Wi-Fi.

[19] Bluetooth, 2016. https://fr.wikipedia.org/wiki/Bluetooth.

[20] Internet of things : 802.15.4, 6lowpan, rpl, coap, 2010. https://www.utwente.nl/ewi/dacs/colloquium/archive/2010/slides/2010-utwente-6lowpan-rpl-coap.pdf.

[21] Ieee std. 802.15.4, 2005. http://www.cs.berkeley.edu/~prabal/teaching/cs294-11-f05/slides/day21.pdf.

[22] Bluetooth low energy, 2016. https://en.wikipedia.org/wiki/Bluetooth_low_energy.

[23] Communication en champ proche, 2016. https://fr.wikipedia.org/wiki/Communication_en_champ_proche.

[24] Antonio J Jara, Latif Ladid, and Antonio F Gómez-Skarmeta. The internet of everything through ipv6 : An analysis of challenges, solutions and opportunities. *JoWUA*, 4(3) :97–118, 2013.

[25] 6lowpan tutorial. http://voip.netlab.uky.edu/~fei/teaching/cs687/slides/4.6LoWPAN-tutorial.pdf.

[26] Michael Kirsche and Ronny Klauck. Unify to bridge gaps : Bringing xmpp into the internet of things. In *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*, pages 455–458. IEEE, 2012.

[27] Mqtt, 2016. https://fr.wikipedia.org/wiki/MQTT.

[28] Coap, 2014. http://coap.technology.