

Rapport de TIPE : L'interopérabilité des systèmes communicants dans le domaine de la domotique

Clément Guillemot, Kenan Terrisse, Florin Gogibus
Hugo Delannoy, Mickael Mendes de Carvalho
Encadrant : Julien Mercadal

17 juin 2016

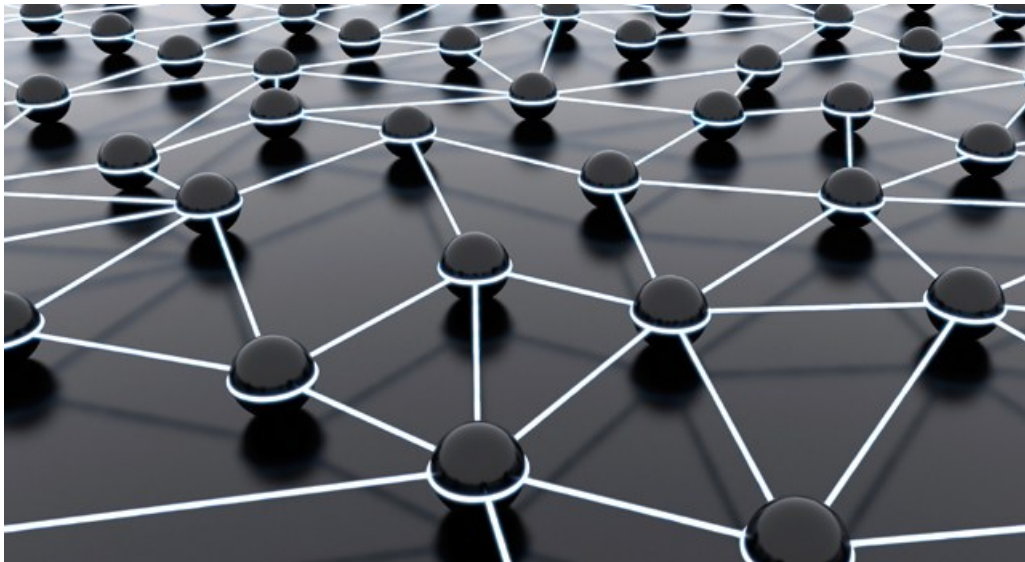


Table des matières

1	Introduction	1
1.1	Scénario	1
2	Pré-requis et définition	4
2.1	Principe d'abstraction et de modèle	4
2.2	Topologie des réseaux	6
2.2.1	Les réseaux en bus	6
2.2.2	Les réseaux en étoiles	7
2.2.3	Les réseaux en anneaux	7
2.2.4	Les réseaux en <i>mesh</i>	7
2.2.5	Le réseau étendu : WAN (Wide Area Network)	8
3	Principaux protocoles de communication domotique existant	8
3.1	EnOcean	8
3.2	Zigbee	9
3.3	Z-Wave	11
3.4	L'UPnP	11
3.4.1	Addressage	12
3.4.2	Découverte	12
3.4.3	Description	12
3.4.4	Contrôle	12
3.4.5	Notification d'évènement	12
3.4.6	Présentation	13
3.4.7	Application	13
3.5	Les passerelles et l'inter-opérabilité	14
3.5.1	Principe de passerelle	14
3.5.2	Exemple de passerelle/central domotique	14
4	Solution retenu pour la famille Dubois	16
	Références	17

1 Introduction

La domotique du latin *domus* et du grec *domos* (« maison ») avec le suffixe -tique qui fait référence à l'informatique, est un ensemble de techniques visant à automatiser les tâches quotidiennes dans l'habitat individuel et collectif. On commence à parler de domotique dans les années 1980 [14]. On remarque qu'elle évolue très vite et que la tendance est désormais de tout connecter avec des services extérieurs à la maison [3]. De manière simple il est possible de télécommander des ouvrants (portail, volet,...) ou programmer les heures d'allumage d'un chauffage *via* une télécommande.

Nous pouvons qualifier ces usages de classiques. Avec la démocratisation de *Internet of Thing* (IoT, pour Internet des Objets), nous assistons au développement exponentiel des objets connectés. N'importe quel système, même le plus simple, est désormais relié à Internet et peut communiquer avec d'autres systèmes. Un besoin se ressent désormais de connecter sa propre maison [9]. La majorité des personnes ont l'idée de la maison du future comme anticipant leur besoins. On a également que 31 pourcents des personnes interrogés voudraient investir dans la domotique pour les économies d'énergie.

1.1 Scénario

Pour illustrer les problématiques liée à la domotique, nous allons analyser les besoins d'une famille ordinaire désirant rendre sa maison connectée et plus intelligente. La famille Dubois fait donc son premier grand pas dans la domotique.

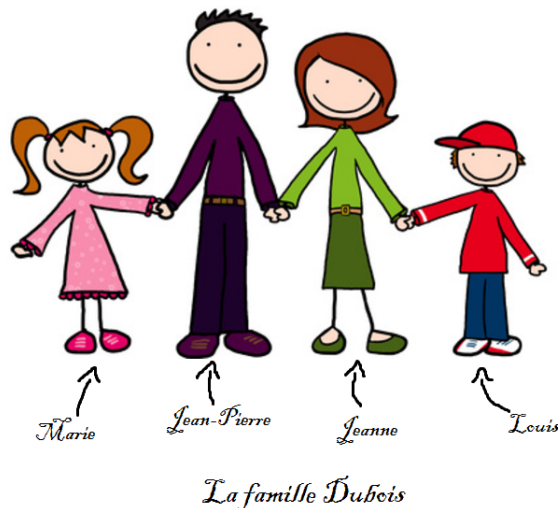


FIGURE 1 – La famille Dubois

Chaque membre de la famille a ses besoins en fonction de ses loisirs et de son activité professionnelle :

- Marie, 10 ans, CM2, est une jeune fille pleine de vie toujours prête à jouer avec des amis ou la famille. Elle adore aussi regarder ses dessins animés préférés.
- Louis, 15 ans, 3ème, est un adolescent très connecté. Dès qu'il n'est plus avec ses amis, il se connecte sur les réseaux sociaux. Il aime beaucoup les séries TV et les jeux vidéos. Son problème ? Il fait toujours trop chaud pour lui dans la maison, ce qui pose problème avec le ressenti de sa mère.
- Jeanne, 40 ans, professeur dans un lycée, est une mère très active. Elle peut avoir de temps en temps des oublis (elle est tête en l'air) : courses et aliments, lumières et TV allumées toute la journée alors que personne n'est là,... . Elle aime beaucoup son métier et voyager. Ce qui l'oppose à son fils c'est qu'elle a toujours froid... Les chauffages tournent donc à plein régime toute la journée pour par grand chose étant donné que toute la famille vaque à ses occupations en ville.
- Jean-Pierre, 42 ans, ingénieur, c'est un peu le papa geek. C'est lui qui veut introduire la domotique dans la maison familiale. Très attaché à son travail, qui est aussi sa passion, il a besoin dans la semaine d'être souvent connecté à ce dernier pour récupérer les dernières informations. Sinon il aime toutes sortes de gadgets connectés : montre, chaussure, vêtements, ect. Il aime également voyager avec sa femme mais ils ont encore trop peur de laisser les enfants seuls pendant leurs voyages. Il déplore les factures d'électricité et de gaz à cause de sa femme. Il fait également les courses pour la maison mais ne prend jamais ce qu'il faut.

De cette description ressortent certains besoins :

- Contrôle du chauffage
- Contrôle des lumières
- Surveillance de la maison
- Un point central de contrôle et d'organisation (planning, gestion du système, mémo de courses, ...)

Jean-Pierre a beaucoup de produits en tête permettant de répondre à tous ces besoins. Mais il ne voit pas comment toutes ses technologies peuvent fonctionner ensemble et se contrôler depuis l'îlot. Chacun propose son application, elle fonctionne avec les produits de la marque. Mais si je veux utiliser une autre marque ? Bon le constat est que Jean-Pierre est perdu. Nous allons faire une étude des différentes solutions techniques et des produits existants afin de répondre à son besoin : faire communiquer des éléments domotiques entre eux.



Diversité des systèmes Un système domotique est un ensemble de capteurs et d'actionneurs. Les capteurs (température, humidité, présence, ...) sont chargés de récolter des données sur l'environnement et les actionneurs (moteurs, chauffage, lumières, ...) sont chargés d'agir sur l'environnement. En fonction des données des capteurs et des consignes, les actionneurs réagiront de manière différente. Une VMC (ventilation mécanique), par exemple, peut-être contrôlé en fonction de capteur extérieur et intérieur de température. Cela permet de faire de la thermorégulation. La diversité des systèmes domotiques est problématique. Tout au long de cette étude, nous verrons que mettre en relation tous les éléments n'est pas facile pour un utilisateur. Les manières dont s'organise le système peuvent être très diverses, on parle de topologie. :

- Système centralisé, où un ordinateur récupère les données et commande les actionneurs. Les éléments du système ne communiquent donc jamais entre eux
- Système décentralisé, où chaque élément est indépendant. Les actionneurs peuvent par eux même aller chercher l'information auprès des capteurs

Il est évident que ces deux types d'organisation ont leurs avantages et leurs inconvénients. L'ensemble des topologies de reseaux seront étudiés dans la section 2.2.

L'organisation du système n'est pas le seul facteur de diversité. En effet, les capteurs sont tous très différents, tout comme les actionneurs. Ils n'ont pas forcément le même but, ils ne sont pas de même marque, de même génération. Pour faire ce constat, il suffit de se rendre dans un magasin spécialisé en informatique puis aller au niveau des ampoules connectées. Vous trouverez plusieurs marques, beaucoup font de la lumière que l'on peut commander, d'autres n'ont même plus cette fonction mais en gardent juste la forme. Si veux intégrer cette lampe Koninklijke Philips Electronics N.V.[©] à mon système domotique Somfy[©] TaHoma[®], est ce que je suis sûr que ma lampe s'intégrera dans ce dernier? Elle sera peut être juste contrôlable manuellement mais ne respectera pas les scénarios programmés. On se demande donc jusqu'où ira l'intégration de cette lampe totalement étrangère...

Ce type de scénario appelle à se développer de plus en plus avec l'expansion des objets connectés. Les systèmes domotiques deviendront de plus en plus complexes et les interactions d'autres systèmes seront un point important. L'utilisateur sera pris dans ce développement et sûrement perdu à cause des nombreuses technologies qui se développent en parallèle. En effet, aujourd'hui aucune norme universelle ne semble s'imposer et beaucoup de constructeurs intègrent la leur dans leurs produits. Par conséquent, peu de produits seraient compatibles entre eux. Existe-il donc des solutions techniques pour palier ce manque d'uniformité? Comment assurer l'interopérabilité des éléments?

2 Pré-requis et définition

Afin de mieux comprendre la suite du développement il est nécessaire de comprendre quelque notion un peu technique sur les réseaux comme le principe de couches ou la topologie des réseaux.

2.1 Principe d'abstraction et de modèle

La diversité des systèmes se fait principalement par leurs protocoles de communication. Il s'agit un ensemble de règles établies pour permettre à deux systèmes de communiquer. Les règles spécifie généralement la manière dont une connection est créée, dont les données sont échangées, la gestion du format des données, ect. On peut prendre pour exemple le modèle OSI ou encore le modèle TCP/IP qui sont comparés dans la figure 2. C'est modèles définissent des couches empilés appelé couche d'abstraction. Elle désigne un ensemble d'objets permettant d'être manipulé sans se soucier de sa vraie valeur. Les couches d'abstraction sont beaucoup utilisées en programmation afin d'unifier, d'uniformiser le développement. Pour prendre un exemple concret, lorsqu'un informaticien développe un jeu, il utilise une couche d'abstraction appelé API (DirectX par exemple) qui lui permet de programmer sans se soucier du matériel sous lequel tournera son jeu. Autrement dit, l'API lui donne des méthodes génériques pour développer, et l'API se charge de l'implémentation du code spécifique pour chaque matériel.

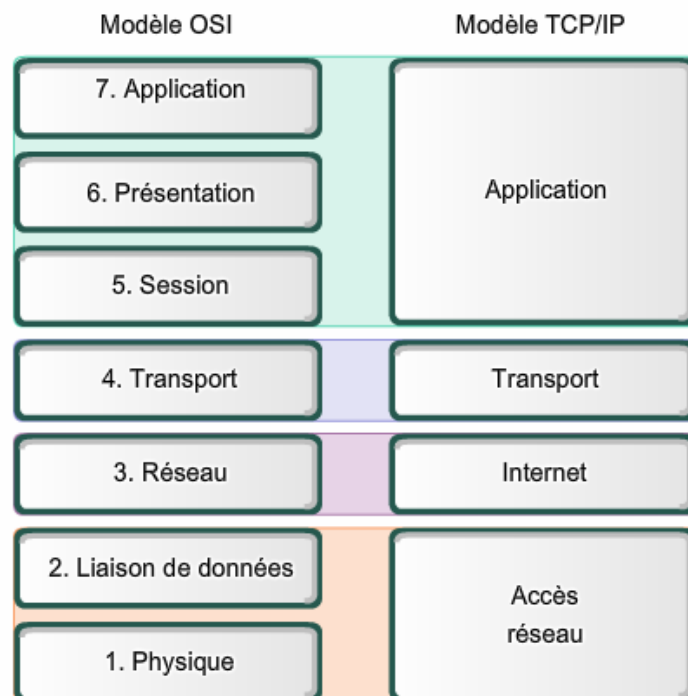


FIGURE 2 – Comparaison des modèles OSI et IP

Dans le monde des réseaux internet, cela veut signifie que une couche n n'aura pas besoin de se soucier de comment les données sont gérées par la couche $n - 1$. Cette même couche n sera donc elle chargé de fournir l'abstraction nécessaire la couche $n + 1$. La couche applicative n'a qu'a utiliser les services que lui fournit la couche inferieur. On peut voir ce cas dans la figure 3.

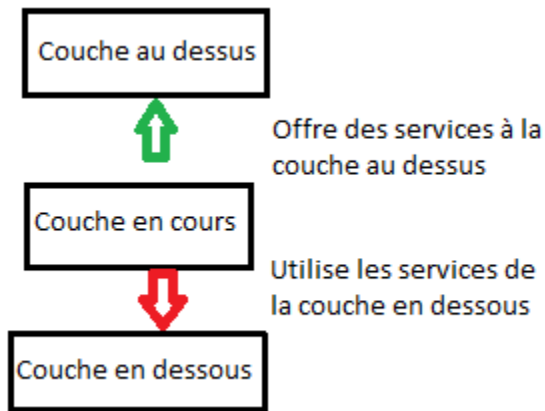


FIGURE 3 – Intéraction entre les couches

Les règles de communication imposé par les protocoles n’agissent en général que sur cette couche applicative. On dit que ce protocole est par dessus TCP/IP comme on peut voir avec l’UPnP à la figure 4.

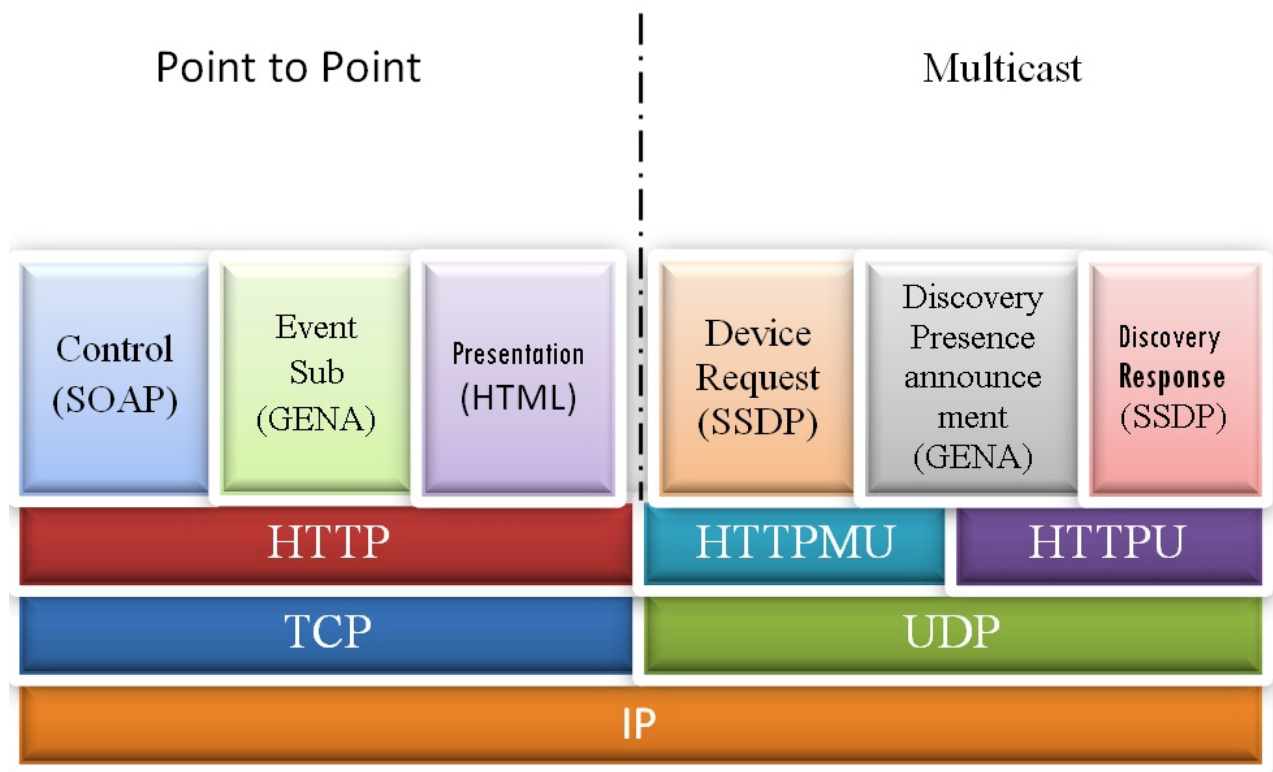


FIGURE 4 – L’UPnP au dessus du protocole TCP/IP

Le TCP/IP est aujourd’hui le protocole de communication omniprésent mais le modèle OSI est une référence pour la construction de norme car très détaillé. Pour une famille lambda voulant intégrer la domotique dans sa maison sur de nombreux niveaux (lumière, chauffage, contrôle de sécurité de surveillance de la maison, un point central de contrôle et d’organisation), il est nécessaire et plus pratique de trouver un système permettant de relier tous ces niveaux afin que la communication se fasse bien entre les différents modèles choisis. Il faut donc trouver

des systèmes utilisant des protocoles de communication pouvant se comprendre afin de faciliter l'intégration de tout le système domotique dans la maison.

Pour que l'utilisateur puisse intégrer plus facilement sont objet domotique, il faut que le protocole domotique soit capable de se mettre au dessus d'autre protocole de communication. Ainsi, on pourra s'assurer qu'il puisse utiliser des interfaces de communication varié (Wifi, bluetooth, Ethernet,...). Reste le problème de l'interopérabilité entre les protocole, il ne sont pas penser au départ pour être inter-opérable car ils n'implémentent pas de d'abstraction. Chacun à voulu s'imposer comme le "nouveau" protocole universel. Par contre il existe bien des passerelles, qui seront développer à la section 3.5.1 capable de passer d'un protocole vers un autre de manière transparente pour l'utilisateur. Les protocoles internet sont aujourd'hui bien assis sur des bases solide et les normes restent unifiés. Par contre dans le monde de la domotique, où les technologies sont très récentes et en plein boom, cette stabilité est peut présente. Nous allons donc, dans la partie qui suit, tenter de lister au mieux les différents protocoles de communications, les technologies sur les quelles ils reposent, les avantages et leur inconvénients. Puis dans une seconde partie, il sera question d'étudier leur interopérabilité, dans quelles mesurent peuvent ils communiquer ensembles dans un réseau domestiques.

2.2 Topologie des réseaux

La topologie est une représentation d'un réseau, en général celle-ci représente la disposition physique de l'ensemble des composants d'un réseau. On la représente la plupart du temps par un dessin qui réunit l'ensemble des postes, des périphériques, des câblages, des protocoles etc. Lorsque l'on veut créer un réseau il est important de d'abord choisir comment celui-ci va être structurer c'est pour cela qu'il faut connaître les différentes topologies de réseau qui existent. Nous allons donc montrer les différents types de topologies de réseau, les décrire et faire le point sur leurs avantages et sur leurs inconvénients.

2.2.1 Les réseaux en bus

On l'appelle aussi réseau en bus linéaire car les différents composants du réseau (postes) sont reliés à un seul et même câble (le bus) en série. Dans cette disposition les informations envoyés par une station sont transmises sur l'ensemble du bus à toutes les stations. De plus, aux extrémités du câble est fixé un bouchon de terminaison pour éviter les réverbérations des signaux transmis. L'information circulant dans le bus contient son adresse de destination c'est donc à la station de reconnaître cette information en comparant son adresse à l'adresse de destination de l'information. Deux stations ne peuvent pas émettre une information simultanément car celles-ci rentrent en collision et l'information peut être perdu dans ce cas là les stations en question vont renvoyer leurs informations respectives et l'information 'perdue' va être absorber par les bouchons de terminaison. Pour éviter ces collisions le débit du réseau est limité à 10 Mbit/s et le nombre de stations branchées au réseau est lui limité à 30. On dit aussi que cette topologie est passive car l'information transmise sous forme d'un signal électrique le long du bus n'est pas régénérée lorsqu'elle passe devant un composant du réseau. Ces réseaux ont pour avantages d'être simples et peu coûteux à mettre en place, de plus si une machine du réseau tombe en panne alors le reste du réseau continuera de fonctionner ce qui n'est pas forcément le cas d'autres topologies. Cependant ils ne sont pas dépourvus d'inconvénients par exemple si le câble venait à être défectueux alors le réseau tout entier ne pourrait plus fonctionner. Sa limitation à 10 Mbit/s est aussi un inconvénient majeur à ne pas négliger.

2.2.2 Les réseaux en étoiles

Dans un réseau en étoile, la topologie physique utilisé est le bus, toutes les machines sont interconnectées grâce à un SWITCH qui est une ‘multiprise’ pour les câbles réseaux. Les stations émettent vers ce SWITCH et celui-ci renvoie les données vers tous les autres ports réseaux ou alors uniquement au destinataire.

Cette topologie de réseau est la plus utilisée car elle dispose de beaucoup d’avantages. Par exemple la panne d’un élément du réseau ne perturbe pas le fonctionnement général du réseau, on peut aussi facilement déplacer un appareil dans le réseau car on n’a pas à se soucier de son emplacement tant que celui-ci est relié au concentrateur. Elle a de plus un avantage en plus par rapport aux réseaux en bus : le débit, en effet il n’est pas limité à 10 Mbps et peut aller jusqu’à 100 Mbps. Le seul inconvénient que l’on peut noté est le rôle essentiel du concentrateur si celui est défectueux c’est tout le réseau qui est alors hors-service.

2.2.3 Les réseaux en anneaux

Dans un réseau en anneau, la topologie physique utilisé est le bus, les machines sont disposées en cercle et forment une boucle, elles sont reliées par un bus renfermé sur lui-même, cependant contrairement au réseau en bus, la topologie logique utilisée est le token ring, ce système utilise une méthode anti-collision pour palier au problème de collisions de données que possède les réseaux en bus. En effet, cette méthode consiste à attribuer une autorisation de communiquer à une machine (représentée sous la forme d’un jeton). La machine peut alors transmettre son message et ses données et après avoir finit sa transmission c’est à dire lorsque ses données reviennent vers elle après avoir traversées toute la boucle, elle les élimine du réseau et elle peut alors donner son jeton à la machine suivante et ainsi de suite. Si la machine ne transmet pas de message, l’autorisation passe à la machine suivante. Cette topologie de réseau a pour avantage d’utiliser le plein potentiel de la bande-passante (le bus) car les données qui y circulent ne peuvent pas entrer en collisions. Malheureusement on retrouve dans ce réseau en anneaux le même inconvénient que dans le réseau en bus c’est à dire que si une machine du réseau tombe en panne alors c’est tout le réseau qui ne fonctionne plus.

2.2.4 Les réseaux en *mesh*

Dans un réseau en maille, la topologie physique utilisé est le bus ou sans fil, toutes les machines sont connectées de proche en proche sans hiérarchie spécifique (c’est un réseau décentralisé), elles forment ainsi une structure en forme de filet comme on peut le voir sur la figure /ref Comme les éléments du réseau sont connectés à tous les autres éléments du réseau à leur porté et que ceux-ci ont la possibilité de relayer des informations si l’un des éléments est défectueux alors la connexion entre l’élément défectueux et les autres éléments du réseau est coupée, et les autres éléments utiliseront une autre voie pour transporter les informations en question. C’est une technologie de rupture c’est à dire que c’est une technologie qui va de plus en plus dominer le marché car celle-ci n’a pas de réels défauts de par sa décentralisation elle ne dépend pas d’un coordinateur central comme peut nous le proposer la topologie en étoile qui occupe de nos jours une grosse part du marché. De plus, la mise en place d’un tel réseau est rapide et simple, il offre une forte tolérance aux interférences (car les informations se propagent de proche en proche sur de courtes distances) ce qui réduit fortement les coûts d’installation et d’exploitation des réseaux.

2.2.5 Le réseau étendu : WAN (Wide Area Network)

WAN (*Wide Area Network*) que l'on peut traduire en français par « réseau étendu » est un réseau longue distance, la plupart du temps publique, situé à l'échelle nationale et internationale. Ce sont généralement des réseaux de télécommunications qui sont gérés par des opérateurs comme par exemple France Telecom, ils ont pour mission d'assurer la transmission des données entre les villes et les pays à l'échelle de la planète. Les supports qui servent à la transmission de ces réseaux sont très variés (ondes hertziennes, fibre optique, ligne téléphonique ou encore satellite). Internet est par exemple le plus grand réseau WAN. Plus le réseau couvre une grande distance plus le taux d'erreur sur les bits transmis est élevé pour un réseau WAN on a donc un taux d'erreur de communication qui vaut le double de celui d'un réseau MAN. De plus, les débits sont généralement plus faible dans un réseau WAN, en effet ils dépendent des supports de transmission cités précédemment, ils vont de 56kbps à plus de 625Mbps.

3 Principaux protocoles de communication domotique existant

Après avoir bien défini c'est notion, nous allons désormais dans cette partie étudier trois des principaux que protocole domotique.

3.1 EnOcean

EnOcean [11] est une entreprise fondée en mars 2012, proposant un protocole de communication du même nom. Celui-ci est un protocole applicatif (agissant sur les couches hautes du modèles OSI)[4]. Il se superpose à la norme ISO/IEC 14543-3-1X [8] Celui est basé l'amplitude shift key (ASK) qui est une type de modulation numérique dans lequel l'amplitude varie afin d'offrir différent canaux de communication et éviter les interférences. La norme diffère en fonction du continent : en Europe la bande fréquence est de 868MHz, en revanche aux états unis celle est de 315 MHz avec une transmission des données de 125kb/s. La zone de transmission est de 30 mètres en intérieur et de 300 mètres en extérieur. La transmission peut être accrue par le biais de relais au nombre de 2 au maximum. Cette dernière est sécurisée, par le cryptage AES 128 (*Advanced Ecrption Standar*) apparu en 1997. Il est utilisé par le gouvernement des États Unis et est approuvé par la NSA (National Security Agency). C'est le cryptage le plus utilisé et le plus sécurisé. Contrairement au WiFi ou GSM, la technologie EnOcean ne dialogue que très peu, pas d'émission radio en continu ce qui en fait également un atout pour les réticents aux ondes. Il ne subit pas d'interférences liées aux environnement WiFi, 4G, DECT [11].

EnOcean s'impose de plus en plus dans le marché de la domotique, ses produit sont de plus en plus standardisé, possédant aussi bien des avantages que des inconvénients. Il est possible d'obtenir une central qui relis les informations du réseau EnOcean vers le cloud, aussi bien accessible sur Mac[©], sur Windows[©]. que sur smartphone, cela permet de paramétrer son environnement EnOcean à distance.

Les appareils EnOcean permettent une réduction du coût et du gaspillage [?], en effet la technologie EnOcean se trouve être une technologie verte. Elle utilise plusieurs procédés écologique telles que l'utilisation de panneaux photovoltaïque (récupération des photons et stockage de ceux ci), l'utilisation des propriétés fondamentales de la thermodynamique (utilisation de la

variation de température) ainsi que les propriétés fondamentales de électromagnétisme (capteur piézoélectrique). Ainsi les appareils EnOcean n'ont pas besoin de pile pour fonctionner.

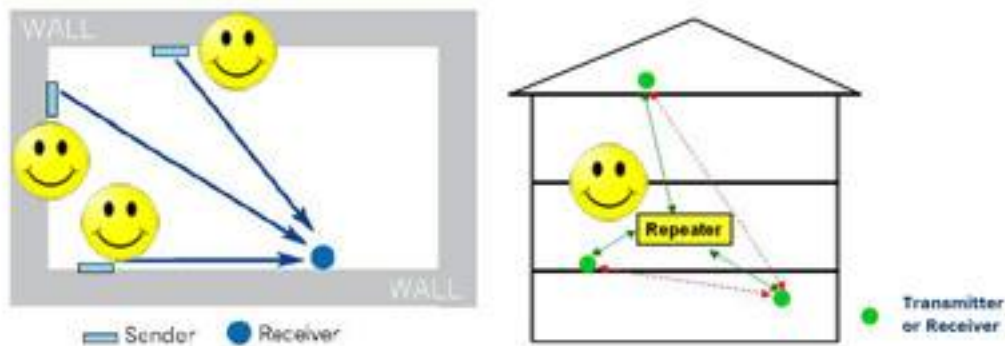


FIGURE 5 – Exemple de configuration Recepteur-Emetteur

Le protocole EnOcean configuré soit en maille, soit en étoile, permet d'affecter plusieurs fonctionnalités à un seul appareil. Par exemple un contact de fenêtre permet aussi bien de détecter une présence que de faire varier la température de la pièce car celle-ci est ouverte.

Pour revenir à la famille Dubois : “ Lors de la construction d’une maison traditionnelle, l’électricien doit passer nombre de fils dans les plafonds et dans les murs. Cela engendre bien évidemment un coût important... Pour une installation qui demeure complètement figée, c’est à dire qui est peu évolutive.” *extrait du site enocean.com*

Cela éviterai pour la famille de devoir faire moult travaux, la technologie EnOcean leur permettra de s’adapter à leur besoin tout en restant dans leur budget.



FIGURE 6 – L’EnOcean est un protocole applicatif s’ajoutant sur la norme ISO/IEC 14543-3-1X

3.2 Zigbee

ZigBee est un protocole de communication sans-fil, qui a été conçu par la ZigBee Alliance, est basé sur la norme IEEE 802.15.4 qui est destiné aux réseaux sans-fil LP-WPAN [5] (*Low-Power-Wireless Personal Area Network*) du fait de leur faible consommation, de leur faible portée ainsi que le faible débit des dispositifs utilisant ce protocole.

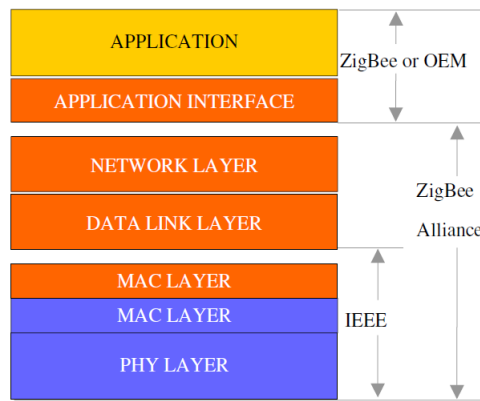


FIGURE 7 – La pile réseau pour le Zigbee

ZigBee est donc un standard de communication tout comme l'est le Wifi ou le Bluetooth par exemple. Pour communiquer et transporter des messages entre deux ou plusieurs éléments du réseau, Zigbee utilise des ondes hertziennes définies sur 3 bandes de fréquences disponibles, une disponible uniquement en Europe : 868 MHz, une disponible seulement aux États-Unis et en Australie : 915 MHz et une dernière disponible partout : 2,4 GHz. Cette dernière est la plus utilisée car elle permet d'obtenir un débit plus important comparé aux deux autres fréquences. Ce qui différencie ZigBee du Wifi ou du Bluetooth est l'utilisation des ondes hertziennes, en effet un module Zigbee occupera le médium pendant quelques millisecondes, le temps d'émettre et d'attendre éventuellement une réponse, puis il se mettra automatiquement en veille, ce qui veut dire que la majeure partie du temps c'est à dire 99,9 % du temps les modules ZigBee sont en veille. ZigBee a été conçu pour interconnecter des unités embarquées autonomes comme des capteurs ou des actionneurs à des unités de contrôle, de commande. Grâce à leur système d'activation et de mise en veille très rapide et peu coûteuse en énergie ces unités consomment très peu et peuvent être alimentés pendant des mois voir des années par de simples piles alcalines de 1,5V. ZigBee de par sa norme IEEE 802.15.4 prévoit deux types de topologies[1] : en étoile ou en point à point, et définit trois types d'éléments pour constituer un réseau :

- Le coordinateur ZigBee qui est le noeud le plus important car il s'agit du noeud qui est à l'origine de la création du réseau : c'est lui qui met à jour la liste des participants au réseau et qui attribue leurs adresses. Après la création du réseau il agit comme un simple routeur.
- Le routeur ZigBee qui est un noeud intermédiaire, il s'associe soit à un coordinateur soit à un autre routeur, il peut aussi avoir le même rôle qu'un coordinateur si plusieurs éléments s'associent à lui.
- Le terminal ZigBee qui est le noeud le plus simple, il s'associe soit à un routeur ZigBee soit à un coordinateur ZigBee car il finit les branches du réseau, il ne participe donc pas au routage des messages et aucun autre élément ne s'associe à lui.

Pour la famille Dubois, il pourrait être intéressant d'utiliser la technologie ZigBee, car celle-ci est peu coûteuse en terme de prix mais aussi en terme d'énergie, de plus ZigBee peut voir son débit monter jusqu'à 250 kb/s soit le double que ce que peut proposer d'autres technologies telle que EnOcean par exemple.

3.3 Z-Wave

Le Z-wave[7] [6] est un protocole domotique propriétaire sans fils créé par une petite société danoise nommée Zensis. Ce protocole est orienté vers le contrôle résidentiel et l'automatisation du marché. Afin d'optimiser la consommation électrique, il utilise la bande de fréquence des 868Mhz. La bande passante est donc limitée, d'un côté par la bande de fréquence mais aussi afin de réduire la consommation. Elle est de 9 à 40 kbit/s. Cette optimisation permet d'avoir des éléments domotiques (nœuds) fonctionnant uniquement sur pile par opposition au WiFi qui ne permet pas d'avoir ce type de design. La portée est de 50 mètres environ mais afin d'augmenter sa portée il utilise une typologie de réseau mesh. L'avantage est que chaque nœud est à la fois récepteur et émetteur. Il peut relayer l'information d'un élément vers un autre. Afin d'assurer l'interopérabilité des différents éléments, le Z-wave définit l'ensemble des couches réseaux et applicatives que nous allons décrire ensuite. De plus le protocole définit des classes (interrupteur binaire, capteur binaire, capteur multi-niveaux, moteur multi-niveaux, thermostat, alarme, ...). Un des avantages de ce protocole est de pouvoir être utilisé autant de manière centralisée avec une passerelle que de manière décentralisée (une prise et un interrupteur par exemple). L'utilisation de passerelle permet d'ouvrir le système Z-wave à internet ou d'autres systèmes.

Z-wave se trouve être le seul protocole de communication sur le marché de fournir une interopérabilité des applications de niveau et de maintenir une compatibilité dans toutes ces versions. Il peut supporter un nombre maximal de 232 nœuds. Il existe deux types de nœuds : les nœuds maîtres et les nœuds esclaves. Une alliance a été créée au sein du marché poussant des entreprises à collaborer avec Z-wave (Intermatic, Honeywell). Ce protocole utilise également un système de mise en veille, les données s'échangent entre deux nœuds en quelques millisecondes puis les sources deviennent passives.

3.4 L'UPnP

L'UPnP (Universal Plug and Play) est née de la technologie plug and play souvent abrégée PnP, est une technologie visant à rendre l'installation de divers appareils plus facile (ex : clé USB avec l'installation automatique du pilote). En effet le PnP est une procédure qui permet l'installation, l'intégration automatique de l'appareil dans un système informatisé voulu sans manipulation particulière à faire de la part de l'utilisateur. Ainsi une fois l'efficacité de cette nouvelle technologie constatée, l'UPnP est née. Comme vous l'aurez compris cette technologie consiste à faciliter l'installation d'un élément informatisé dans un réseau domotique dans nos cas. Les membres du forum UPnP ont défini un protocole utilisé par l'ensemble des constructeurs participant sur la majorité de leur produit permettant une interopérabilité entre ces produits simplifiées. En effet ce protocole se situant au niveau de la couche applicative, il n'y a pas de problème de communication avec les couches inférieures. Nous allons donc maintenant nous intéresser à ce protocole pour comprendre son fonctionnement et voir comment il pourrait être utile à la famille Dubois [10].

Le Protocole UPnP est composé de 6 étapes, ces 6 étapes ce :

- Addressage
- Découverte
- Description
- Contrôle
- Notification d'évènement
- Présentation

3.4.1 Addressage

C'est le moment où l'appareil qui cherche à rentrer dans le réseau va fournir à celui si sont adresse IP ou va chercher à en créer une, pour lui permettre de ce faire repérer par tout les appareille de ce réseau. Pour ce faire il va utiliser le protocole DHCP (*Dynamic Host Configuration Protocole*). le protocole DHCP est chargé de la configuration des paramétré ip.

3.4.2 Découverte

Dans cette étapes il va s'agir de faire en sorte que tout les objet connecté au réseau puisse communiquer avec le nouvel intervenant du réseau. Il va ainsi s'agir d'une description de l'équipement et des fonctionnalité fournit par l'objet. cette description va ce faire par le biais du protocole SSDP (*Simple service discovery protocol*).

Cette phase du protocole UPnP qui va se relancer périodiquement pour pouvoir vérifier la présence de l'élément dans le réseau.

3.4.3 Description

La découverte d'un équipement durant la phase précédente va permettre de pouvoir récupérer les information données par l'URL obtenu dans la phase précédente.

la description de l'onjet va ce présenter sous la forme d'un fichier XML et va contenir des informations telles que :

- numéro de série
- le modèle de l'appareil
- le constructeur
- liste des différentes actions exécutable par l'équipement (les commandes au quel va réagir le produit)
- les différents composant de l'appareil

Un exemple de document XML ce situe à la figure 8.

3.4.4 Contrôle

Une fois l'étape de la description terminée, la communication dans les deux sens enfin possible, c'est-à-dire que le réseau peut enfin envoyé des "ordres", à l'élément que l'ont souhaite ajouter au réseau, ces "ordres" restant dans la limites des différentes actions exécutable trouvée dans la description. toutes ces actions sont effectué grâce au protocole SOAP (*Simple Object Access Protocol*). Le protocole est un protocole qui permet la transmission d'information entre deux objet via le protocole http.

3.4.5 Notification d'évènement

L'étape contrôle effectué il va falloir mettre à jour les notification retourné par l'élément ces mises à jours prennent la forme de messages XML contenant les variables qui caractérisent le services à l'exécution. Les mises ne sont publié uniquement dans le cas de changement de variable.

```

<?xml version="1.0"?>
<root xmlns="urn:schemas-upnp-org:device-1-0">
  <specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>

  <device>
    <deviceType>urn:schemas-upnp-org:device:lighting.2</deviceType>
    <friendlyName>Dan's UPnP Device Host Test</friendlyName>
    <manufacturer>Microsoft</manufacturer>
    <manufacturerURL>http://www.microsoft.com/</manufacturerURL>
    <modelDescription>Dan's UPnP-X10 Light and Dimmer
control</modelDescription>
    <modelName>X-10L1</modelName>
    <modelName>L1</modelName>
    <modelURL>http://www.microsoft.com/</modelURL>
    <serialNumber>0000001</serialNumber>
    <UDN>DummyUDN</UDN>
    <UPC>00000-00001</UPC>

    <iconList>
      <icon>
        <mimetype>image/png</mimetype>
        <width>16</width>
        <height>16</height>
        <depth>2</depth>
        <url>icon.png</url>
      </icon>
    </iconList>

    <serviceList>
      <service>
        <serviceType>urn:schemas-upnp-org:service:pwrdim:2</serviceType>
        <serviceId>upnp:id:pwrdim</serviceId>
        <controlURL></controlURL>
        <eventSubURL></eventSubURL>
        <SCPDURL>SampleSCPD.xml</SCPDURL>
      </service>
    </serviceList>

    <presentationURL>sample.html</presentationURL>
  </device>
</root>

```

Information sur le produit

Champs concernant les contrôles et les services

FIGURE 8 – Exemple de fichier XML

3.4.6 Présentation

La présentation est la dernière étapes du protocole UPnP, celle si n'est pas toujours effectué car n'étant pas obligatoire, cette étapes consiste à charger l'URL fournis avec dans la description, ce qui permet à l'utilisateur de voir les différentes actions qu'il peut effectuer.[2]

3.4.7 Application

Ainsi pour nôtres familles Dubois l'application de la normes Upnp sur tout les élément domotique présent dans leur maison permettrai, une installation facile de n'importe quel de ces éléments. On peut d'ailleurs noté qu'une telle association de marques pour facilité l'insertion du plus d'objet informatiser possible, l'alliance DLNA(Digital Living Network Alliance) qui rassemble plus de 250 société. d'objet informatiser possible, l'alliance DLNA(Digital Living Network Alliance) qui rassemble plus de 250 société.



3.5 Les passerelles et l'inter-opérabilité

Nous allons désormais étudier les passerelles puis nous verrons des exemples de passerelle commercialisé aujourd'hui.

3.5.1 Principe de passerelle

Le terme de passerelle s'utilise dans différentes situations. Le terme de passerelle (ou proxy) fut employé pour la première fois à la conférence **ICDCS** (*International Conference on Distributed Computing Systems*) de 1986 par Marc Shapiro. Le proxy agit sur les couches hautes du modèles OSI. Initialement il se charge de transmettre les requêtes entre deux réseaux différents (typologie et protocole différents). Sachant qu'il est au milieu de deux réseaux, on l'utilise désormais pour contrôler le flux de données entre ces deux réseaux. On peut faire du *キャッシング* afin de fournir plus rapidement les contenus souvent demandé par les utilisateurs. On peut aussi faire du contrôle de contenu afin de limiter l'accès à certains sites web et pour éviter les infections informatiques dans les environnements de production par exemple. Avec la généralisation des réseaux TCP/IP, les réseaux locaux et les réseaux étendus n'ont plus besoin de proxy. Il reste néanmoins très utilisés pour ses autres fonctionnalités. Dans notre cas, son utilisation comme pont entre deux sera sa seule fonction.

On peut distinguer deux types de passerelle : les passerelles logicielles et les passerelles matérielles. Les passerelles logicielles font le lien entre deux protocoles de couche haute (partie applicative du modèle TCP/IP). On peut imaginer par exemple un pont entre les protocoles internet HTTP et REST. Un logiciel sur un serveur serait chargé de transcrire les requêtes HTTP vers la syntaxe REST. Les passerelles matérielles agissent sur les couches basses (partie accès réseau pour le TCP/IP). On peut prendre comme exemple une passerelle Ethernet/WIFI pour fournir un accès internet aux clients mobiles.

3.5.2 Exemple de passerelle/central domotique

MyFox Home Control 2 Il existe de nombreux produits tout-en-un sur le marché aujourd'hui. Le nom commercial de "box domotique" est souvent employé. A l'image des box internet, ces box domotiques font office de passerelle entre différents réseaux, de central domotique et de serveur applicatif pour l'interface utilisateur. Nous avons pris comme exemple le produit de la société Myfox[®] : Home Control 2. Elle est spécialisée dans la sécurité et la surveillance du domicile mais peut aussi contrôler des objets utilisant le protocole Chacon utilisant la bande de fréquence des 433Mhz. Ce protocole est très économique et simple à mise en place. La famille Dubois peut facilement trouver une prise contrôlable dans le commerce et l'associer dans son système domotique. Ce système possède son application mobile propriétaire permettant de gérer son système et d'associer des actions avec des services extérieurs.

Cette central est très intéressante et particulière car elle possède des slots d'extensions (voir figure 11). Cela permet de la rendre évolutive et de lui ajouter le support du EnOcean et de connectivité GSM.

Le plus gros inconvénient de cette box grand public est que tout le système est non libre. Autrement dit quelqu'un qui veut faire du DIY (*Do It Yourself*) et créer ses propres objets ou applications n'aura pas accès au API du constructeur. Une API (*Application Programming Interface*) est une bibliothèque de fonctions permettant l'interaction avec un objet ou un logiciel. Cela permet

d'insérer une couche d'abstraction entre le logiciel de la box domotique et l'application DIY du particulier.



FIGURE 9 – Slot d'extension

OpenPicus C'est une entreprise qui produit du matériel et du logiciel IoT pour la domotique. Leur modèle de développement ressemble énormément à celui de Arduino ou de Raspberry Pi. En effet l'ensemble des schémas électrique et des codes sources sont libre d'accès [13]. Leur produit principal s'appel FlyPort, c'est une plateforme évolutive dont les capacités peuvent être étendu [12] par les ports GPIO (*General Purpose Input/Output*). On peut imaginer une infinité de capteurs, d'actionneurs, et d'éléments communiquant. La carte électronique est également séparable en deux : d'un côté la partie "carte mère" et de l'autre processeur comme on peut le voir à la figure 10. La partie processeur peut être modifier pour obtenir soit une connectivité WIFI, GSM ou Ethernet.

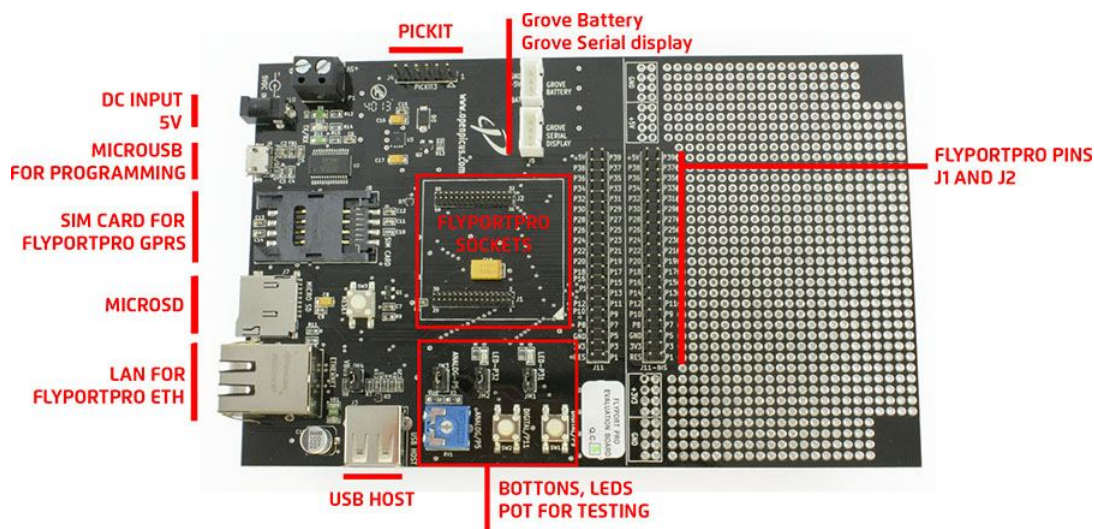


FIGURE 10 – La carte mère du FlyPort Pro

De nombreux tutoriels et documentation existe sur internet, et son capacité d'évolution en font une passerelle domotique de choix pour Jean-Pierre Dubois afin de passer d'un réseau EnOcean à un réseau wifi ou autre.

4 Solution retenu pour la famille Dubois

Après études des quartes protocoles et des passerelles dans la section 3 nous pouvons voir que la majorité des protocoles ne peuvent pas être interconnecté directement entre eux. Il est nécessaire d'insérer une ou plusieurs passerelle entre les différents réseaux. Cette passerelle nécessite d'être logiciel et matériel. En effet nous pu voir que les protocoles sont implémenter sur la couche applicatif (donc nécessite une passerelle logiciel) et sont au dessus de normes agissant sur la couche matériel : il faut donc une passerelle matériel pour changer de norme. Certains protocoles propose leur applications propriétaire. Rare sont les protocoles qui offre leur API afin de développer des services tierces. En conclusion, les services externes utilisable en parallèles des systèmes domotiques sont limités à ceux qui sont proposé par les constructeurs possédant les droit sur le protocole.

Pour la famille Dubois, nous allons créer un système domotique basé sur l'UPnP. Le fait est que aucun protocole de communication existant est aujourd'hui interopérable telle que on le trouve dans le commerce. Il est obligatoire de passer par des passerelles. On a pu voir qu'il en existe qui intègre différents protocoles nécessaire à la communication entre les modules incompatibles. Nous allons donc essayer de créer une connexion entre 2 éléments domotique et une central par le protocole réseau universelle UPnP. Le but de notre projet est de faire communiquer un capteur de lumière à base de carte Arduino avec une central domotique qui orchestra l'ensemble du système. Cette même central ira contrôler une lumière sur une autre carte Arduino. Nous aurons deux carte qui supporterons l'UPnP sur WiFi.

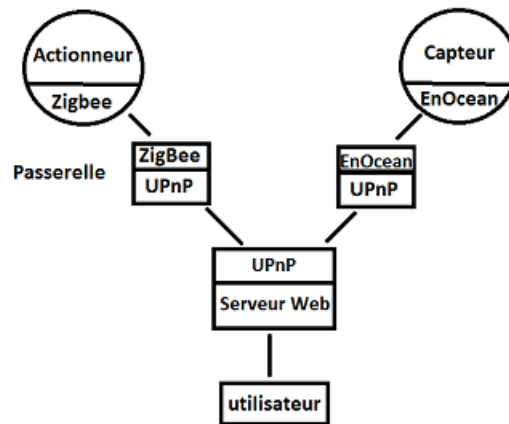


FIGURE 11 – Schéma décrivant le système domotique retenu

Références

- [1] *IEEE Std. 802.15.4 Enabling Pervasive Wireless Sensor Networks.*
- [2] Digital Living Network Alliance. Site web de l'alliance dnla, 2016.
- [3] Pascal Amphoux. Domotique domestique. 1990.
- [4] EnOcean. *The Easy Way to Energy Harvesting Wireless Products*, 06 2015.
- [5] Jackson Francomme, Ferial Virolleau, Jiamin Pang, Yan Xin Phang, and Thierry Val. Zigbee, de la théorie à la pratique : création d'un réseau zigbee avec transmission de données. *3EI*, 71 :1–18, 2013.
- [6] Mikhail T Galeev. Catching the z-wave. *Embedded Systems Design*, 19(10) :28, 2006.
- [7] Md Zahurul Huq and Syed Islam. Home area network technology assessment for demand response in smart grid environment. In *Universities Power Engineering Conference (AUPEC), 2010 20th Australasian*, pages 1–6. IEEE, 2010.
- [8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *Wireless Short-Packet (WSP) protocol optimized for energy harvesting — Architecture and lower layer protocols.*
- [9] le Credoc. Deuxième enquête "HABITANTS, HABITATS et MODES DE VIE". Technical report, Association Promotelec, 11 2014.
- [10] VINCENT Maxime. Profil upnp™ pour l'administration de plates-formes d'exécution hétérogènes. 2008.
- [11] Institute of Research Engineers and Doctors. *Comparison protocoles*, 2013.
- [12] OpenPicus. *FlyportPRO Wi-Fi 802.11G*, 11 2013. Rev. 1.
- [13] OpenPicus. Wiki pour les schémas et datasheet des produit openpicus, 2016.
- [14] Mercedes López Santiago. Étude du champ lexico-sémantique de domotique et de ses dérivés. In *Anales de filología francesa*, volume 18, pages 333–353, 2010.