Institut Supérieur
d'Informatique, de
Modélisation et de
leurs Applications

1 rue de la Chebarde
63178 Aubière CEDEX

Rapport d'ingénieur
Projet de 3e année
Filière *Réseaux et Sécurité informatique*

À déterminer

Présenté par : **Loïc Guillaume**
Lucien Guimier

Responsable entreprise : **Pascal Mouchard**
Responsable ISIMA : **Patrice Laurencot**

Soutenance le **À déterminer**
Projet de **120 heures**

Remerciements

Table des figures

Résumé

Abstract

Table des matières

Introduction

L'Internet des Objets (**IdO** ou **IoT** pour *Internet of Things* en anglais) représente la jonction entre Internet et le monde des capteurs qui ne sont généralement pas directement reliés à des équipements actifs des réseaux, comme un routeur par exemple. En effet, usuellement les données passent plutôt par une phase de traitement sur un ordinateur avant d'être potentiellement envoyées sur le réseau.

Tous les concepts derrière l'IoT soulèvent plusieurs problématiques telles que l'accroissement exponentiel du volume de données sur le réseau, dû à l'explosion du nombre d'objets connectés, mais aussi des problèmes de nature énergétiques, car les capteurs sont rarement alimentés en continue via une prise électrique.

C'est pourquoi plusieurs protocoles ont été créés en prenant en compte ces contraintes, l'un d'eux étant **6LoWPAN**. Il nous fût demandé d'effectuer une étude sur ce protocole car il présente une particularité que son principal concurrent ne possède pas (**ZigBee**), celle de pouvoir router l'information depuis n'importe quels nœuds (*node* en anglais). Cela ne nous oblige pas à avoir une topologie Maître/Esclave, mais plutôt un réseau maillé ce qui permet de couvrir de plus grandes superficies.

Notre projet consista en une étude de 6LoWPAN ainsi qu'à son expérimentation grâce à des cartes achetées par notre tuteur, le but ultime étant de pouvoir router de l'information via n'importe quelle carte. Aussi ce projet était à vocation exploratoire pour préparer d'autres projets sur l'IoT dans les années futures. La question était donc :

Comment router de l'information grâce à 6LoWPAN ?

Pour répondre, nous allons, dans un premier temps, vous présenter plus en détails l'IoT, certains protocoles et bien sûr 6LowPAN. Ensuite nous reviendrons sur le travail technique que nous avons effectués sur les cartes puis nous dresserons un bilan de ce projet.

1 L'IoT et ses protocoles

Dans cette première partie, nous allons définir plus en détail quelles sont les implications et les spécificités de l'IoT ainsi que de l'approche au niveau des réseaux via la présentation de quelques protocoles et bien évidemment celle de 6LoWPAN.

1.1 L'IoT

L'Internet of Things, que nous appellerons maintenant IoT pour le reste de ce rapport, se traduit littéralement comme l'Internet des Objets, mais qu'est-ce-qu'un objet ? Dans le monde de l'IoT les objets peuvent se référer à des biens (comme des meubles ou de l'électroménager), des machines, des véhicules, des immeubles ou bien même à quelque chose d'organique comme un être vivant (Homme ou animal), une plante, des sols (pour les cultures).

Alors la question est : Comment pouvons nous tous connecter ? En effet, comment faire en sorte qu'une plante possède un accès réseau. C'est cela que l'IoT veut définir et représente, une connectivité pour tout.

Mais d'abord que veut dire le mot connecter ? Prenons l'exemple d'une chaise, le fait qu'elle soit connectée veut dire que je peux avoir accès à de l'information la concernant, depuis n'importe où, grâce à un accès à Internet, par exemple, est-elle occupée ? Si oui, qui est assis dessus ? Pour cela nous avons besoin de donner certains attributs de cette chaise, comme un numéro d'identification unique, une manière de la distinguée d'un autre objet.

Grâce à **IPv6**, nous pouvons maintenant affecter une adresse unique à tout sans limite réel car l'espace adressable est sans limite pratique (mais il y a bien sur une limite physique). IPv4 est déjà dépassée en terme de capacité d'adressage depuis longtemps mais grâce à des mécanismes comme le NAT/PAT, IPv4 est encore utilisé. Nous reviendrons sur IPv6 un peu plus tard dans ce rapport lors de notre présentation de 6LoWPAN.

Ensuite, nous avons besoins de donner à la chaise un moyen de communiquer avec le monde, soit de manière filaire ou sans fil grâce à des antennes. D'où la nécessiter des protocoles réseaux qui vont devoir transporter les informations, malheureusement ceux que nous utilisons dans la vie tous les jours ne sont pas vraiment adaptées (IPv4, IPv6, Wi-Fi, ...) à l'IoT, de part leur consommation électrique ou de bande-passante. C'est pourquoi de nouveaux protocoles ont vu le jour, spécialement adaptés à ces besoins. Certain se concentre sur la puissance d'émission et d'autre sur la fiabilité dans les milieux bruités, mais tous prennent en compte certaines contraintes de l'IoT.

Aussi, nous parlons d'information et de données mais il faut bien les générer, pour cela nous utilisons différents types de capteurs, comme par example de pression pour savoir si notre chaise est occupé. Un autre type de capteur pourrait être une puce de localisation, ou bien même un capteur d'identification qui pourra nous dire qui est assis sur notre chaise et qui l'a été. De nos jours les capteurs sont extrêmement petits mais ont quand même certaines capacités comme de la mémoire, ce qui est très pratique en cas de coupure temporaire du réseaux, en effet, les données ne sont pas forcément perdue.

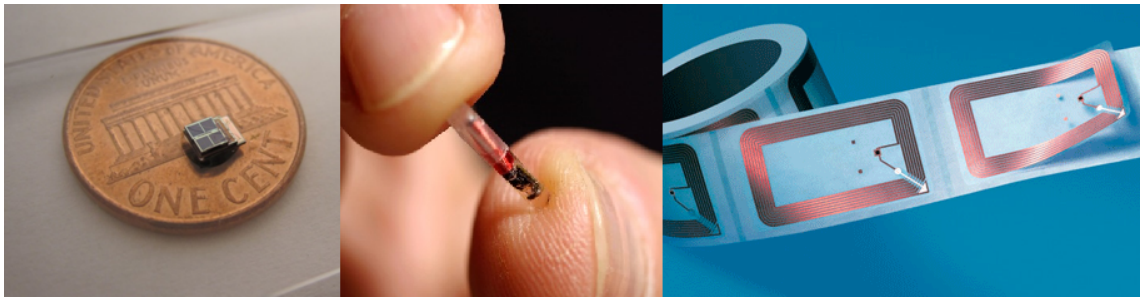

FIGURE 1 – Exemple de capteurs

Quelles seront les impacts et les possibilités de l'IoT ? Nous ne sommes limités seulement par notre imagination car nous changeons l'approche de voir et de connecter les objets.

Prenons quelques exemples pour montrer l'intérêt de l'IoT. Le *monitoring* ne se résume pas aux réseaux et aux machines, nous pouvons aussi l'appliquer pour surveiller l'état

d'un patient en médecine. Imaginons quelqu'un avec un problème cardiaque, il possède un pacemaker qui est "connecté", cela veut dire qu'une application sur son téléphone peut dire à cette personne l'état de son cœur, mais aussi à son hôpital. Dans le cas d'une défaillance, une alerte est lancée à l'hôpital qui peut envoyer immédiatement une ambulance, quant à la localisation ils peuvent utiliser un tracker GPS intégré au tout.

Grâce à des algorithmes puissants, nous pourrons même prédire un potentiel problème sans que le patient vienne faire des visites de contrôles régulières, son pacemaker enverra les données pour lui. Avec le nombre de personnes de plus de 65 qui va doubler dans peu de temps, la e-santé et la télé-médecine vont devenir un des plus gros secteurs de l'IoT.

Les tracas de quotidiens comme la perte de ses clefs ne seront plus un problème, en effet, dans le monde de l'IoT vos clés sont géo-localisables. Cela peut s'appliquer à plein de choses, si ce n'est à toutes, vous ne perdrez plus jamais rien.

Si nous savons où les choses sont et dans quels états elles sont, nous pouvons mieux les manager. Prenons le cas du trafic en ville, si nous savons où les voitures se situent et où elles vont, nous pouvons potentiellement éliminer les bouchons, optimiser les trajets et rediriger les flux plus facilement. Il en va de même pour l'énergie, si nous savons où l'énergie est requise, nous pouvons adapter la production et optimiser les coûts.

L'IoT permet aussi de déléguer du contrôle, toujours dans une optique d'optimisation énergétique, nous pouvons déléguer l'heure de départ d'une machine à laver, d'un lave-vaisselle à un contrôleur distant qui lancera le programme au moment où l'énergie sera la moins chère.

Un autre marché que l'IoT va investir est la réalité augmentée (en particulier les jeux vidéo). En effet, en utilisant la réalité augmentée, nous pouvons superposer la réalité (filmée par une caméra) et le monde virtuel grâce à un traitement logiciel. L'IoT va simplement étendre le panel de fonctionnalité de manière infinie en permettant d'interagir avec l'environnement. Par example, il suffirait de lancer son application de réalité augmentée et de toucher l'objet avec lequel nous voulons interagir pour se voir proposer des actions. Le panel d'action se limite seulement à ce que le développeur veut laisser les gens

faire.

FIGURE 2 – Réalité augmentée + IoT

Le fait est qu'avec l'IoT, la notion de "privé" devient très floue. Nous tenons à évoquer ce point car l'IoT va quelque peut bousculer certaines habitudes. Reprenons notre chaise, comme dit précédemment, nous pouvons facilement savoir qui était assis dessus grâce à notre identifiant unique. Les risques liés à la protection de notre vie privée augmentent avec l'IoT qui collecte agrège des bouts de données liées aux services que l'appareil propose. Le recoupement d'informations peut assez vite convertir des données banales en données personnelles car les événements (action de l'utilisateur) possèdent un lieu, une heure, une récurrence, etc. L'achat régulier de différents types de nourriture peut révéler la religion ou des problèmes de santé. C'est un véritable enjeu lié au Big Data que l'exploitation des données générées par l'IoT. Le volume de données produit va pouvoir permettre aux exploitants de convertir ces données "public" en "privé".

Maintenant, il faut aussi se placer du côté de l'exploitant qui va vouloir protéger ses informations, c'est pour cela que la sécurisation des transmissions est l'un des enjeux essentiels de l'IoT. L'inconvénient est que la plus part du temps, les capteurs n'ont aucune puissance de calcul pour crypter l'information, actuellement les capteurs se concentre plus sur l'intégrité du message et à établir une connexion sécurisée. Plus la technologie

évoluera, plus la sécurité de l'information se rapprochera de l'appareil, pour ultimement devenir embarquée.

Il est vrai qu'un simple sniffer réglée sur la bonne fréquence permettra de pouvoir intercepter les informations si celles-ci sont transmisses sans-fil. En effet sans cryptages elles sont envoyées en clair. Cela ne pose pas trop de problème pour des données non-confidentielles mais peut vite devenir problématique si les informations recueillies sont de nature plus sensibles.

Nous avons parlé précédemment de traitement de l'information, mais aux vues des volumes de données générées ce n'est pas sur un simple pc de bureau que nous pourrons analyser les données. Avec 20 Milliards d'objets connectés en 2020, les datacenters feront face à des charges de travails inédites. Le volume de données traités n'aura jamais était aussi important et ne fera que grossir aux fils des années. Dès aujourd'hui les fournisseurs commencent à désigner leur datacenters en prévision de l'IoT qui arrive à grand pas.

Mais revenons à un niveau plus bas, celui de la transmission entre les capteurs. Nous ne sommes pas encore sur les infrastructures des FAI mais dans notre réseau local. Ce même réseau est celui qui est le plus proche de l'utilisateur.

1.2 Les différents protocoles et topologies

1.2.1 Les différentes topologies

Un réseau local (**LAN** pour *Local Area Network*) est un réseau où les terminaux peuvent communiquer sans avoir besoin d'un accès Internet. Mais il existe un autre type de réseau plus proche de nos contraintes, le réseau personnel (**PAN** pour *Personal Area Network).* Dans ce type de réseau le but est de faire aboutir les échanges entre les divers éléments du réseau avec des puissances assez faible pour garantir une autonomie correcte. Ce qui correspond bien à nos besoins avec les capteurs. Ils ont besoins d'être autonome le plus longtemps possible tout en évitant une interaction humaine physique direct.

Dans le monde des réseau, nous utilisons le terme topologie pour définir l'arrangement des différents nœuds dans un réseau. Avec les réseaux PAN, on se limite assez souvent à deux topologies : maillage partielle (**mesh**) et en étoile (**star**).

La topologie en étoile est extrêmement repandue car c'est celle qui est utilisée dans le modèle maître-esclave(s). Le maître est le point névralgique du réseau, toutes les communications sont obligées de passer par lui. Cela se révèle assez pratique dans le cas de la collecte de données car le maître est le point de convergence en plus d'être le point de sortie du réseau.

Cette topologie est en parfaite opposition au maillage partielle. En effet dans cette dernière topologie chaque nœuds est potentiellement un routeur, et chaque routeur un potentiel point de sortie. Ces routeur sont appelés des *Edge Router* ou *Border Router*, ils font le lien entre le PAN et d'autres réseaux. Les End Devices ne routent pas l'information.

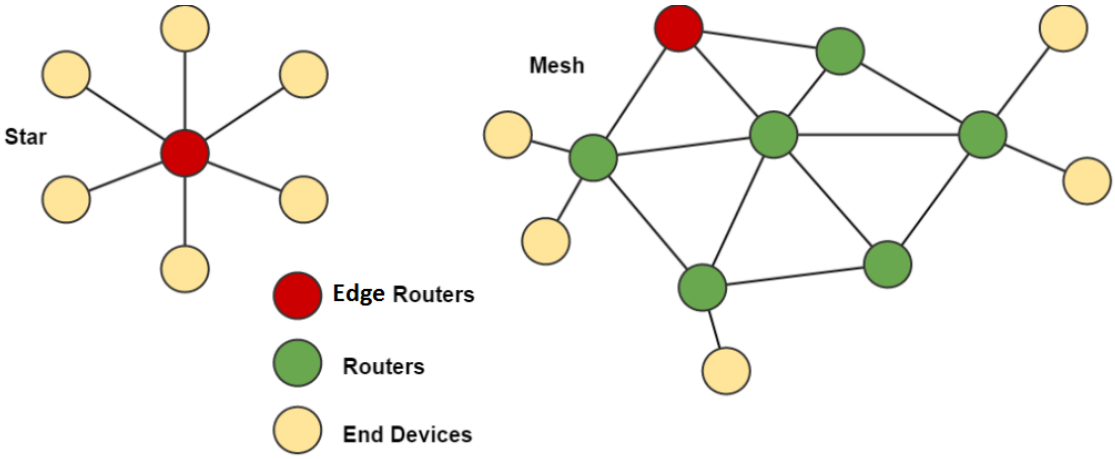

FIGURE 3 – Topologies

Le fait est que comme cette technologie est explorée par plusieurs constructeur et organisme, plusieurs protocoles ont vu le jour, mais sans réel standard, chacun utilise celui qu'il veut. Cela pose pas mal de problème avec l'interopérabilité des éléments dans le réseau qui est pourtant une des caractéristiques phare de l'IoT. Voici une liste succincte de ces divers protocoles.

1.2.2 les différents protocoles

Dans cette partie nous allons vous présenter divers protocoles orientés basse consommation. Ces protocoles sont développées par divers organismes ce qui fait qu'aucun n'est un standard, les constructeurs implémentent ceux qui veulent. Cela peut poser certains problèmes d'interopérabilités, et augmenter fortement le prix des appareils.

Bluetooth : protocole sans-fil opérant dans la bande 2.4 GHz. Il a été conçue pour l'échange de données sur de courtes distances mais ne tenait pas bien compte de la consommation. Généralement, un dongle USB permettait l'ajout du bluetooth à son PC mais la technologies est devenue tellement commune qu'elle est maintenant complètement intégrée dans l'hardware de nos équipements. Bluetooth utilise exclusivement une topologies en étoiles ce qui n'est pas très pratique pour l'établissement de grand réseau (en terme de nombre et de surface).

Le groupe travaillant sur Bluetooth changea la donne avec la version 4 de leur protocole avec l'introduction du Bluetooth Low Energy (aussi connue sous le nom de Bluetooth Smart). Cette version du protocole prend mieux en compte les besoins et contraintes de l'IoT comme la consommation. Par contre la topologie étoile est toujours obligatoire mais un groupe d'étude a été lancé par Bluetooth **SIG** (*Special Interest Group*, les personnes en charge du développement de Bluetooth), nommée Smart Mesh, il a pour but de définir un standard pour pouvoir utiliser BLE avec une topologie mesh.

Wi-Fi : technologie sans-fil permettant d'obtenir de gros débit, on l'utilise majoritairement pour donner un accès réseau à des équipements sans fil. Certaine variantes existent, comme Wi-Fi Direct qui permet le transfert de fichier à haute vitesse entre 2 équipements. Actuellement le protocole est très énergivore ce qui fait de cette technologie un mauvais candidat pour l'IoT, mais des groupes de travails cherche à faire évoluer la norme (débit / bande-passante / consommation / vitesse d'association) en correspondance avec l'IoT pour gagner des parts de marché.

Zigbee : ce protocole repose sur les couches basses définis par **802.15.4** (aussi utilisé

par 6LoWPAN et défini dans la partie suivante). Il supporte des topologies en étoiles et maillées (*mesh*), mais pour cela, un des équipements doit avoir le rôle de "coordinateur". Le coordinateur est généralement l'appareil avec le plus de puissance et il est la racine du réseau, il peut avoir plusieurs rôles comme faire la liaison entre réseaux ou bien un aire de stockage pour les clés de sécurités. Il ne peut y avoir qu'un seul coordinateur par réseau et dans le cas d'un réseau en étoile il est forcément au centre.

La technologie utilisant ce protocole est conçue comme une alternative plus simple et moins chère que celles des autres WPANs, comme Bluetooth ou Wi-Fi. La portée varie beaucoup en fonction de la bande de fréquence utilisé mais à titre d'exemple, la portée à 2.4 GHz en intérieur varie en 10 et 20 mètres. Les débits sont aussi relativement faible : 20 kbit/s si l'on opère dans la bande 868 MHz et 250 kbit/s à 2.4 GHz. Les faibles débits permettent de maintenir une consommation extrêmement faible, ce qui fait en sorte que les équipements tiennent plusieurs années.

Z-Wave : protocole orienté domotique (automatisation dans les bâtiments), chaque réseau peut comporter jusqu'à 232 noeuds, la majorité sont des esclaves et les autres sont des contrôleurs. La topologie maillé implémente un système de saut (hop), jusqu'à 4, ce qui fait qu'avec une portée de base de 100 m plus les sauts, la couverture en terme de surface est très grande.

Dans les dernières version de Z-Wave, un système d'*explorer frame* (trame exploratoire) permet de réparer des routes quand un appareil est défectueux ou enlever du réseau. Par contre, comme le protocole est routé statiquement, Z-Wave suppose que tous les appareils dans le réseau reste à leur place originelle. Les appareils mobiles, comme les télécommandes, sont donc impossibles à router.

Il existe beaucoup d'autres protocoles que nous ne développerons pas car leur usages restes assez limité.

1.3 6LoWPAN

Cette partie à pour but de présenter le protocole 6LoWPAN ainsi que la norme 802.15.4 utiliser dans les couches basses de 6LoWPAN.

1.3.1 802.15.4

Ce standard de l'**IEEE** est définie sur 2 couches du **modèles OSI**, la couche physique et la couche MAC. Il est à la base de différents protocoles IoT (ZigBee notamment) qui implémentent des couches supérieurs différentes.

Le framework de base prévoie un rayon de communication de 10 mètres pour un débit allant jusqu'à 250 kbit/s. Il est bien sur possible de réduire la puissance d'émission (le rayon) et de diminuer le débit pour réduire la consommation électrique. L'idée derrière cette réduction drastique est de quand même de conserver une bonne fiabilité.

Comme Wi-Fi (802.11), 802.15.4 utilise au niveau 2 **CSMA/CA** pour éviter les collisions et intègre plusieurs mécanisme pour la sécurisation des communications. Certains appareils peuvent aussi intégrer des modules d'optimisation de la consommation, de détection de la qualité de la liaison ainsi que la puissance de réception.

Les appareils conforme à la norme 802.15.4 peuvent désormais se caler sur 3 bandes de fréquences : 868, 915 et 2450 MHz. Cela permet de se conformer plus facilement au norme en vigueur dans chaque pays qui ont des lois en la matière différente. Il n'y a pas de législation mondiale a ce propos.

Le standard défini deux types de nœud :

le premier est le *Full-Function Device* (FFD). Il peut servir de coordinateur dans le PAN tout comme il peut fonctionner en tant que simple nœud. Ils sont doté d'un module de communication qui permet de pouvoir retransmettre des trames (faire du routage).

Le second est le *Reduced-Function Devices* (RFD). Ils sont prévues pour être ex-

trêmement simple et possèdent peut de ressource. A cause de cela, il ne peuvent que communiquer avec les FFD et ne peuvent pas être les coordinateurs.

Dans le réseau chaque équipement se voit attribuer un identifiant de 16 bits unique qui permet de faire du routage de niveau 2.

1.3.2 6LoWPAN

6LoWPAN est l'acronyme d'*IPv6 over Low power Wireless Personal Area Networks*, ce veut dire Ipv6 au dessus de réseau personnelle sans-fil basse consommation. l'idée principale derrière ce protocole était d'amener IP à tous types d'appareils.

Aussi, 6LoWPAN n'est spécifié qu'avec IPv6, ce qui fait que l'utilisation d'IPv4 dans un réseau utilisant 6LoWPAN est impossible. Grâce à cela les *edge routers* peuvent utiliser des mécanisme de transition pour connecter des réseaux 6LoWPAN et IPv4 comme **NAT64**.

Sur un réseau 6LoWPAN le *border/edge router* réalise 3 actions :

1. L'échange de données en les appareils du réseau local et l'Internet (une autre réseau IP).
2. L'échange de données en local
3. la génération et la maintient du réseau

Ensuite l'un des énormes avantages de 6LoWPAN, du fait de l'utilisation d'IP, est le routage de niveau 3 (couche réseau). Avec 6LowPAN il n'y pas besoin de maintenir une connexion au niveau applicatif, au contraire de ZigBee, Z-Wave ou Bluetooth qui requiert des passerelles applicatives pour accéder à Internet. En d'autre terme, l'équivalent du *edge router* doit comprendre les protocoles utilisés au niveau applicatif. Cela réduit fortement la charge de travail du routeur.

Voici un comparaison des différentes stack utilisés par les protocoles cités précédem-

ment :

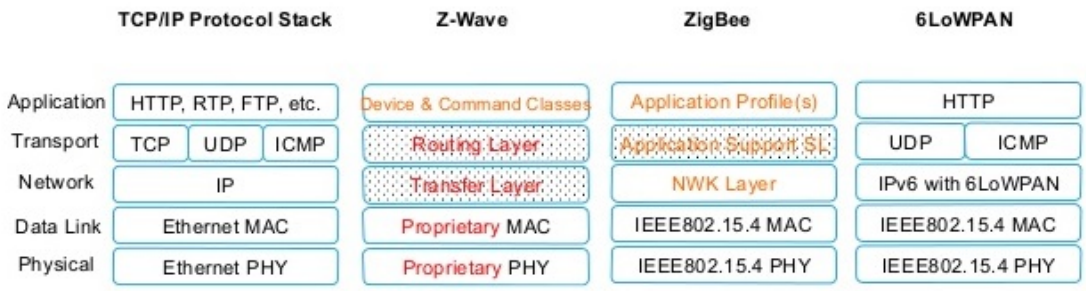

FIGURE 4 – Comparaison de différents protocoles IoT

——-Mettre des observations pour zigbee et z-wave ?——-

En réalité IPv6 est plus une couche 2.5 que 3, en effet la couche 3 est IPv6. En fait, dans le cas de 6LowPAN la stack réseau ressemble plus à cela :

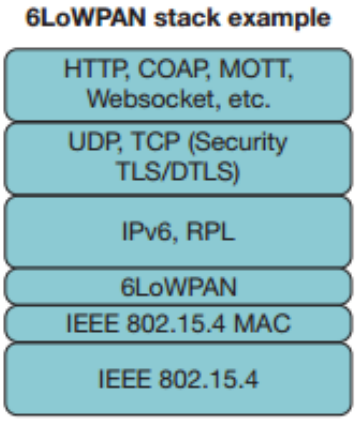

FIGURE 5 – Stack 6LoWPAN

Comme nous pouvons voir, 6LoWPAN fait la liaison entre 802.15.4 et IPv6. Au niveau transport, 6LoWPAN supporte UDP et TCP mais ce dernier n'est pas beaucoup utiliser. En effet, TCP étant un protocole connecté les en-tête sont très grandes (à cause de l'ajout de numéro de séquence par exemple) et donc pas vraiment pratiques pour les appareils basse consommation. Le trafic supplémentaire, avec les ACK, rend son utilisation délicate. On privilégiera plutôt UDP et sa propre version de TLS, DTLS.

Au niveau applicatif, il est bon de noter que 6LoWPAN supporte HTTP, mais ne l'utilise que très peux a cause de la verbosité du langage. L'industrie a développé un protocole de messagerie plus adapté au nom de **COAP** (*COnstrained Application Protocol*) qui est beaucoup plus adapté aux appareils basse consommation.

Dans le cas de 6LoWPAN il existe 2 types de routage, celui de niveau 3 et celui de niveau 2. l'un utilisant l'adresse IPv6 et le second l'adresse de niveau 2 (l'identifiant 802.15.4).

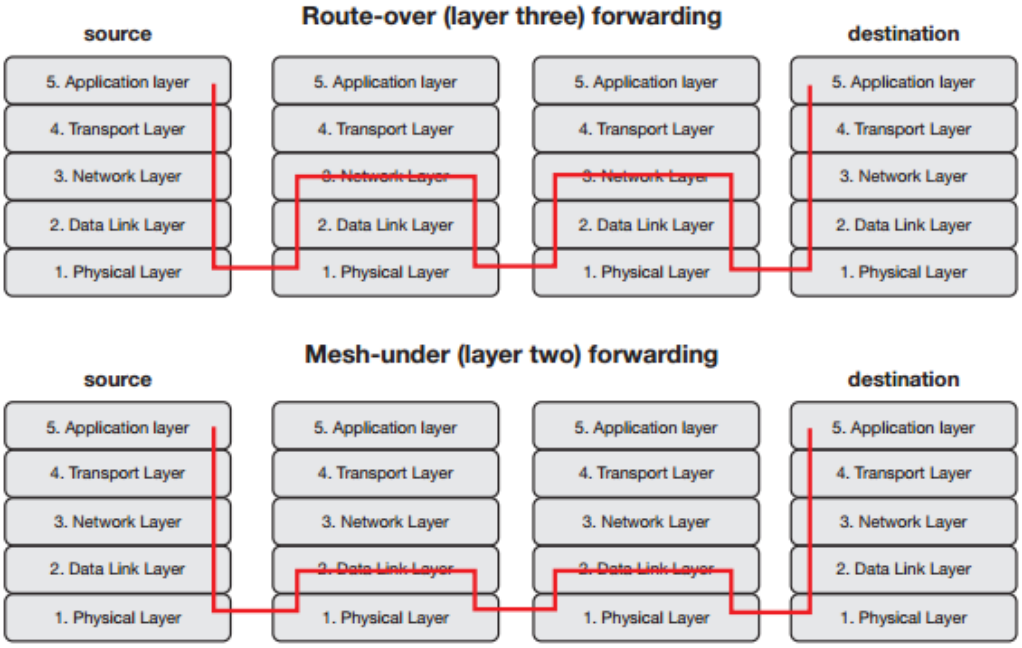

FIGURE 6 – Les 2 type de routage avec 6LoWPAN

L'un des avantages d'IPv6 est l'auto-gestion des adresses, un appareil peut générer automatiquement son adresse sans avoir recours à un DHCP. Le protocole **NDP** (*Neighbor Discovery Protocol*) permet d'obtenir cette adresse unique dans le réseau, ce qui évitera les conflits.

La sécurité dans l'IoT est un véritable challenge, en effet, à cause du nombre de nœuds avec des performances assez faible, il y beaucoup de point d'entré pour les attaques de l'extérieur. Aussi l'un des points critiques dans l'IoT est la nature des données, qui dans certains cas peuvent être cruciale sur elles servent à commander des alarmes ou des portes

d'accès.

Du coup, 6LoWPAN tire partie de l'**AES-128** qui est définie dans 802.15.4. Avec l'utilisation de TLS ou de DTLS on peut aussi sécuriser les échanges au niveau de la couche transport. Mais cela implique d'avoir des équipements avec une certaine puissance. Les cartes TI fournis par notre tuteur ont été développé spécialement dans cette optique de sécurité (**cc2538**).

2 Bilan

2.1 Travail accompli

2.2 Difficultés rencontrées

2.3 Perspectives

Conclusion