REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE D'ORAN

-MOHAMED BOUDIAF-

Polycopié

Cours

Réseaux Avancés destiné aux étudiants Master 2

Option RSID UT231

Présentée par : Mme Khalifa Fatiha

Année universitaire 2022-2023

Intitulé du Master : Réseaux et Systèmes Informatiques Distribués RSID
Semestre : 3
Intitulé de l'UE : UT231
Intitulé de la matière : Réseaux Avancés
Crédits : 2
Coefficients : 2

Objectifs de l'enseignement du cours :

Les évolutions techniques et technologiques bouleversent le domaine des réseaux par la demande d'utilisation intensive, l'augmentation des débits, l'exigence d'une certaine qualité de service, la nature de l'information transportées, la mobilité et la protection de la vie privée.
L'interconnexion et l'intégration d'objets multiples et variés font que l'étudiant doit être au moins sensibilisé sur le futur et les changements attendus.

Connaissances préalables recommandées

Connaissances acquises durant le cursus de formation de la licence : Systèmes informatiques (SI) ou Ingénierie des Systèmes d'information et du Logiciel (ISIL)

Contenu de la matière

1. Introduction
    - Les nouveaux usages et leurs impacts sur la vie quotidienne
    - L'explosion du digital
    - Domotique personnelle, Smart Cities & Internet des Objets
    - Les technologies associées : Réseaux de capteurs, Smart Grid
2. Les problématiques (Développement économique, recherche technologique et mise à disposition des données)
3. Interconnexion et intégration de plusieurs objets connectés
    - Bluetooth Low Energy
    - Plateformes logicielles (Android, Ios)
    - Solution SaaS
4. Digitalisation à grandes échelle
    - Multiplication des points d'accès
5. Documents Web dynamiques et technologie CGI
6. Documents Web actifs et technologie Java
7. Les réseaux du futur/Extensions de WIFI

Table des matières

Chapitre 1

Introduction

L’histoire des réseaux mobiles est jalonnée par trois étapes principales, auxquelles on donne couramment le nom de *génération*. On parle des première, deuxième et troisième générations de réseaux mobiles, généralement abrégées respectivement en 1G, 2G et 3G. Ces trois générations diffèrent principalement par les techniques mises en œuvre pour accéder à la ressource radio.

L’évolution de ces techniques est guidée par la volonté d’accroître la *capacité* ainsi que les *débits* offerts par le système dans une bande de fréquences restreinte. En effet, les fréquences sont des ressources très rares car convoitées par de multiples applications (télévision, radio, faisceaux hertziens, liaisons satellites, réseaux privés, communications militaires, etc.). Dans les différents pays du monde, le spectre disponible au début des années 1980 était déjà très limité. Aussi le développement des réseaux mobiles a été, et est toujours, principalement conditionné par la capacité des ingénieurs à tirer le meilleur parti des ressources spectrales disponibles. Initialement, la capacité des réseaux mobiles se traduisait par le nombre maximal de communications téléphoniques pouvant être maintenues simultanément sous couverture d’une même cellule. De nos jours, avec le développement de l’usage des services de données, la capacité d’un réseau se matérialise aussi par le nombre d’utilisateurs pouvant être connectés simultanément aux services de données, ainsi que par le débit moyen par utilisateur lors d’une session de transfert de données. Plus généralement, la capacité d’un réseau peut être représentée par le débit total maximal pouvant être écoulé par une cellule fortement chargée.

Types de réseau

Les réseaux modernes peuvent être complexes. Il existe de nombreux types de réseaux caractérisés par leur taille géographique, par le nombre d'appareils ou de réseaux qui s'y connectent et par le fait qu'ils prennent en charge ou non des terminaux mobiles. Les réseaux sont également caractérisés par leur fonction et leur but.

Réseau personnel (PAN)

Les réseaux personnels sont des réseaux de petite taille où les appareils sans fil connectés sont proches d'une personne. La connexion de votre Smartphone à votre voiture via Bluetooth est un exemple de réseau personnel.

Réseau local (LAN)

Les réseaux locaux sont généralement des réseaux dans une zone géographique de petite envergure ou locale, comme une maison, une PME ou un département dans une grande entreprise. Les réseaux locaux peuvent connecter au moins deux appareils, dont des ordinateurs, des imprimantes et des appareils sans fil. Les réseaux locaux permettent d'accéder à de plus grands réseaux étendus (WAN) et à Internet.

Réseaux étendus (WAN)

Le terme WAN désigne généralement un ensemble de LAN qui assure une connectivité inter-LAN et Internet pour les entreprises et les administrations.

Internet

Internet est un réseau mondial à plusieurs couches qui relie des centaines de millions d'ordinateurs. Internet n'appartient pas à une seule personne ou une seule entreprise. Cet immense système se compose de plusieurs réseaux locaux et mondiaux qui servent les intérêts privés et publics, mais aussi ceux des entreprises, des établissements scolaires et des agences gouvernementales. Il permet d'échanger des données entre plus d'une centaine de pays connectés à Internet dans le monde entier. Internet transporte donc diverses informations et divers services pour une multitude d'utilisateurs. On peut citer, par exemple, le texte, les données multimédias, les e-mails, les conversations en ligne, la VoIP, les transferts et les partages de fichiers, le commerce électronique et les jeux en ligne.

Réseaux sans fil

Les réseaux sans fil sont des réseaux informatiques qui utilisent des ondes électromagnétiques à la place des câbles pour transporter des signaux sur les diverses parties du réseau. Les réseaux sans fil peuvent être des PAN, des LAN ou des WAN, selon leur envergure.

Étant donné que la navigation sur Internet est une activité quotidienne normale, les points d'accès sans fil sont devenus monnaie courante dans les infrastructures de communications d'aujourd'hui. Parmi les lieux publics connectés à Internet, on compte les bibliothèques, les aéroports, les cafés, les hôtels et les cybercafés spécialisés. Grâce à la technologie Wi-Fi, tout le monde peut désormais accéder à Internet à condition de posséder un ordinateur portable, une tablette ou un smartphone. La Figure 4 présente les différentes catégories de réseaux sans fil disponibles.

Le cloud

Le terme « cloud » est utilisé de bien des manières. Le cloud n'est pas vraiment un type de réseau, mais plutôt un ensemble de data centres ou des groupes de serveurs connectés qui permettent de stocker et d'analyser des données, d'accéder à des applications en ligne et de fournir des services de sauvegarde à des fins personnelles et professionnelles. Plusieurs entreprises proposent des services cloud.

Fog computing

Vu le nombre croissant de capteurs utilisés par l'Internet des objets, il est souvent nécessaire de stocker en toute sécurité les données du capteur à proximité de l'endroit où elles seront analysées. Ces données analysées servent alors à mettre à jour ou modifier rapidement les processus d'une entreprise. Le fog computing est situé à la périphérie d'une entreprise ou d'un réseau d'entreprise. Les serveurs et les programmes informatiques assurent le prétraitement des données pour assurer une utilisation immédiate. Puis, les données prétraitées peuvent être envoyées vers le cloud pour une étude plus approfondie, si nécessaire.

1.1 Les nouveaux usages et leurs impacts sur la vie quotidienne

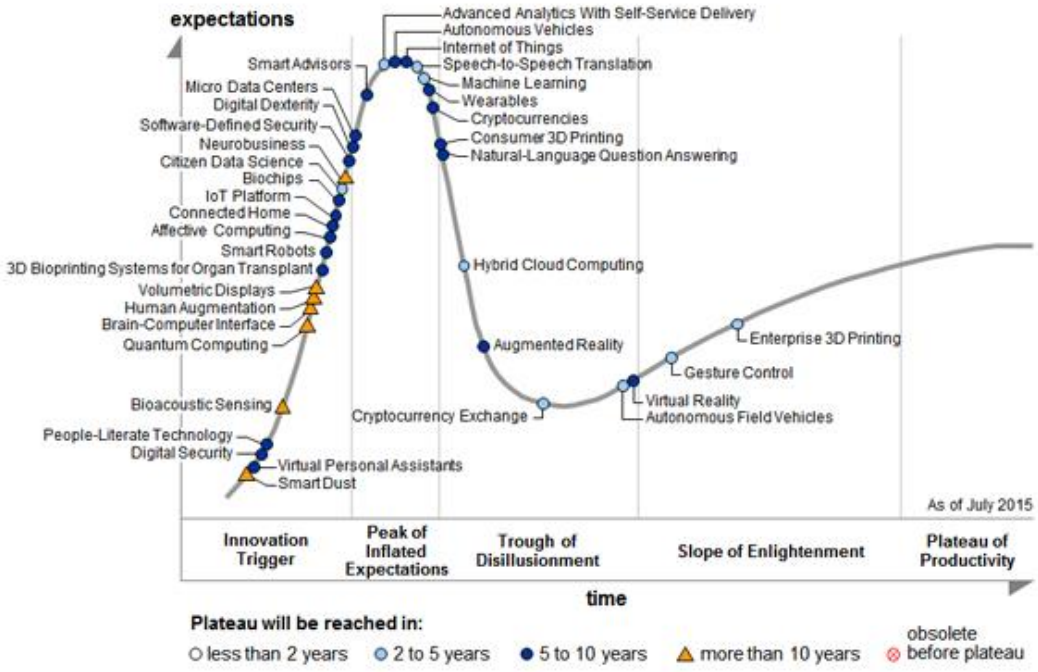


Figure 1.1 : Hyper Cycle sur l'émergence des Technologies, (Gartner 2015)

Selon L'édition 2015 du Hype Cycle des technologies émergentes du cabinet Gartner

le cycle des innovations est découpé en cinq étapes-clés, par niveau d'attente. Première étape, les technologies naissantes («technology trigger»), suivie par un pic inflationniste d'attentes («peak of inflated expectations»), le trou d'air inévitable («trough of disillusionment»), la relance («slope of enlightenment»), et enfin la phase d'industrialisation et d'adoption par le grand public («plateau of productivity»).

En 2014, l'institut Gartner distinguait l'internet des objets («internet of things»), les technologies de questions-réponses en langage naturel («natural-language question answering»), ainsi que les interfaces utilisateur portables («wereable user interface») au sommet du «peak of inflated expectations». Les changements majeurs pour 2015? Cette année, le Hype Cycle reflète «l'émergence de technologies qui soutiennent un 'humanisme digital' – la notion selon laquelle les hommes sont au centre des innovations», souligne Gartner dans son communiqué. D'où l'apparition des notions de «people literate technology» et de «citizen data science».

1.2 L’explosion du digital (Les réseaux du futur)

Les réseaux connectent désormais des milliards de capteurs. Via les logiciels, les données de ces capteurs peuvent modifier les environnements physiques sans intervention humaine.

Comme mentionné précédemment, tous les appareils numériques exploitent des programmes informatiques et les données fournies. Les termes « intelligence artificielle » impliquent que ces appareils sont capables de penser par eux-mêmes. S'ils sont correctement programmés, les appareils intelligents sont capables d'évaluer les données qui leur sont fournies, et de modifier des processus ou des paramètres immédiatement. Si on leur fournit suffisamment de données, ils peuvent « apprendre » et modifier leur propre code sur la base de ces nouveaux paramètres.

Que se passe-t-il ensuite ?

Nous savons que les logiciels peuvent être écrits de sorte que les données puissent modifier des paramètres du code afin d'ajuster la température de votre domicile ou la vitesse à laquelle votre adolescent peut conduire votre véhicule. Pourquoi ne pourrions-nous pas fournir aux logiciels des règles, des instructions ou des objectifs pour permettre aux données de modifier le réseau, les fonctionnalités de l'infrastructure ou les fonctions de sécurité sur le réseau ? En fait, c'est déjà possible. C'est ce qu'on appelle le réseau basé sur l'intention (IBN).

Prenons un exemple simple pour mieux comprendre le concept de réseau basé sur l'intention : une entreprise peut déterminer qu'un collaborateur contractuel n'a le droit d'accéder qu'à un ensemble spécifique de données et d'applications. C'est ce qui correspond à l'objectif (l'intention). Sur un réseau IBN, tous les appareils seront automatiquement configurés pour respecter cette condition sur tout le réseau, peu importe l'endroit d'où se connecte le collaborateur. Le VLAN, le sous-réseau, la liste de contrôle d'accès et toutes les autres informations seront automatiquement définis et configurés dans le respect des bonnes pratiques. Vous ne devez définir l'objectif qu'une seule fois dans une console de gestion centralisée, puis le réseau s'y conformera en permanence, même en cas de modifications.

1.3 Domotique personnelle (Smart Cities & Internet des Objets)

Les technologies domestiques intelligentes sont devenues très populaires et leur popularité augmente chaque année à mesure que la technologie évolue. Comment ne pas être ébahi à l'idée de pouvoir allumer ou éteindre votre thermostat personnel alors que vous êtes au bureau, ou de recevoir les courses que votre réfrigérateur a commandées ? N'est-il pas génial de voir comment va votre chien ou de vérifier que vos adolescents font bien leurs devoirs après l'école en activant vos caméras de sécurité domestiques ?

Alors que nous installons toujours plus de capteurs intelligents dans nos maisons, nous augmentons notre vulnérabilité. Les capteurs sont souvent connectés au même réseau que nos appareils domestiques ou ceux de notre PME, si bien qu'une faille visant l'un de ces appareils peut se propager et affecter l'ensemble des appareils

connectés. Les capteurs peuvent également fournir un moyen aux hackers d'accéder à notre réseau domestique et d'obtenir l'accès à tous les PC et toutes les données qui y sont connectés.

Même les assistants virtuels tels qu'Apple SIRI, Amazon Echo ou Google Home peuvent présenter des risques de sécurité. Les particuliers utilisent ces appareils notamment pour mettre de la musique, ajuster la température ambiante, commander des produits en ligne ou demander un itinéraire. Cela peut-il être dangereux ? Des informations personnelles telles que les mots de passe ou les numéros de carte de crédit pourraient être compromises.

L'Internet des objets (IoT) désigne l'interconnexion de millions d'appareils et de capteurs intelligents connectés à Internet. Ces capteurs et ces appareils connectés collectent et partagent des données qui seront utilisées et analysées par plusieurs organismes, dont des entreprises, des villes, des gouvernements, des hôpitaux et des particuliers. L'avènement de l'IoT a été possible, en partie, grâce à l'apparition des processeurs bon marché et des réseaux sans fil. Des objets jusqu'à présent inanimés (comme des poignées de porte ou des ampoules électriques) peuvent désormais être équipés d'un capteur intelligent qui collecte des données ou les transfère à un réseau.

Les chercheurs estiment que 3 millions de nouveaux terminaux se connectent à Internet chaque mois. Dans les quatre prochaines années, ce chiffre devrait atteindre les 30 milliards d'appareils connectés dans le monde entier.

Environ un tiers des appareils connectés seront des télévisions intelligentes, des smartphones, des tablettes et des ordinateurs. Les deux tiers restants correspondront à des « objets » : des capteurs, des actionneurs et des appareils intelligents innovants qui surveillent, gèrent, analysent et optimisent notre monde.

Voici quelques exemples de capteurs connectés intelligents : les sonnettes intelligentes, les portes de garage, les thermostats, les vêtements de sport, les pacemakers, les feux de circulation, les places de stationnement et bien d'autres. Votre imagination est la seule limite quant aux objets qui peuvent devenir des capteurs intelligents.

Comment les appareils connectés à l'IoT se connectent-ils au réseau ?

Un capteur doit être connecté à un réseau pour que les données collectées puissent être stockées et partagées. Vous aurez donc besoin d'une connexion Ethernet filaire ou d'une connexion sans fil à un contrôleur. Les contrôleurs sont chargés de collecter les données des capteurs et de fournir la connectivité réseau ou Internet. Ils peuvent être à même de prendre des décisions immédiates ou ils peuvent envoyer les données à un ordinateur plus puissant en vue d'une analyse. Cet ordinateur peut se trouver dans le même réseau local que le contrôleur ou n'être accessible que par l'intermédiaire d'une connexion Internet.

Les capteurs fonctionnent souvent ensemble à l'aide d'un appareil appelé actionneur. Les actionneurs reçoivent une entrée électrique et la transforment en action physique. Par exemple, si un capteur détecte une chaleur excessive dans une salle, il envoie la température mesurée au microcontrôleur. Le microcontrôleur peut envoyer les données à un actionneur qui activerait, à son tour, le système de climatisation.

La majorité des nouveaux appareils, comme les vêtements ou équipements de sport, les pacemakers implantés, les dispositifs de mesure de l'air dans une mine et les compteurs d'eau dans un champ agricole nécessitent tous une connectivité sans fil. Étant donné que de nombreux capteurs sont « sur le terrain » et sont alimentés par des batteries ou des panneaux solaires, il convient de tenir compte de la consommation électrique. Il est indispensable d'utiliser des options de connexion basse tension pour optimiser et prolonger la disponibilité du capteur.

1.4 Les technologies associées : Réseaux de capteurs, Smart Grid

Les technologies associées à la révolution des réseaux de nouvelles générations reposent sur le concept des réseaux de capteurs sans fil (ces derniers seront traités en détail dans les chapitres qui suivent) et les réseaux type smart grid.

Un smart grid désigne « *un réseau d'énergie qui intègre des technologies de l'information et de la communication, ce qui concourt à une amélioration de son exploitation et au développement de nouveaux usages tels que l'autoconsommation, le véhicule électrique ou le stockage* » Il est souvent question de ces réseaux intelligents ou « smart grids » au sujet des réseaux d'électricité qui, grâce à des technologies informatiques, ajustent les flux d'électricité entre fournisseurs et consommateurs.

En collectant des informations sur l'état du réseau, les smart grids contribuent à une adéquation entre production, distribution et consommation.

Les réseaux intelligents peuvent être définis selon quatre caractéristiques en matière de :

- flexibilité : ils permettent de gérer plus finement l'équilibre entre production et consommation ;
- fiabilité : ils améliorent l'efficacité et la sécurité des réseaux ;
- accessibilité : ils favorisent l'intégration des sources d'énergies renouvelables sur l'ensemble du réseau ;
- économie : ils apportent, grâce à une meilleure gestion du système, des économies d'énergie et une diminution des coûts (à la production comme à la consommation).

Au sens large, un réseau intelligent associe l'infrastructure électrique aux technologies numériques qui analysent et transmettent l'information reçue. Ces technologies sont utilisées à tous les niveaux du réseau : production, transport, distribution et consommation.

- **Un contrôle des flux en temps réel** : des capteurs installés sur l'ensemble du réseau indiquent instantanément les flux électriques et les niveaux de consommation. Les opérateurs du réseau peuvent alors réorienter les flux énergétiques en fonction de la demande et envoyer des signaux de prix aux particuliers pour adapter leur consommation (volontairement ou automatiquement).
- **L'interopérabilité des réseaux** : l'ensemble du réseau électrique comprend le réseau de transport et le réseau de distribution. Le premier relie

les sites de production d'électricité aux zones de consommation : ce sont les grands axes qui quadrillent le territoire. Le réseau de distribution s'apparente aux axes secondaires. Il achemine l'électricité jusqu'aux consommateurs finaux. Par l'échange instantané d'informations, les smart grids favorise une interopérabilité entre les gestionnaires du réseau de transport et ceux du réseau de distribution.

- **L'intégration des énergies renouvelables au réseau** : les réseaux intelligents reposent sur un système d'information qui permet de prévoir à court et à long terme le niveau de production et de consommation. Les énergies renouvelables qui fonctionnent souvent par intermittence et de façon peu prévisible (ex : l'éolien) peuvent ainsi être mieux gérées.
- **Une gestion plus responsable des consommations individuelle** : les compteurs communicants (ou compteurs évolués, « Linky » pour l'électricité) sont les premières versions d'application du réseau intelligent. Installés chez les consommateurs, ils fournissent des informations sur les prix, les heures de pointe de consommation, la qualité et le niveau de consommation d'électricité du foyer. Les consommateurs peuvent alors réguler eux-mêmes leur consommation au cours de la journée. De leur côté, les opérateurs du réseau peuvent détecter plus vite les pannes.

Chapitre 2

Les problématiques (Développement économique, recherche technologique et mise à disposition des données)

2.1 Introduction

Dans le domaine des sciences de l'information, l'expression *Big Data* (ou données massives) a pris ces dernières années une importance croissante. En premier lieu, c'est l'augmentation importante du volume des données produites par les géants de l'Internet, mais aussi par certaines disciplines scientifiques (la génomique et l'astronomie, en particulier) qui a favorisé ce phénomène. Les progrès intervenus dans les techniques de stockage et dans le traitement de données volumineuses de natures variées (notamment en format texte ou image), souvent produites en flux continu (d'où la dénomination des « trois V » (pour Volume, Variété et Vélocité) qui est souvent citée et mise en avant) sont à l'origine de gigantesques gisements de données. Leur existence même a permis la mise en œuvre d'outils et de méthodes spécifiques (par exemple, de certains algorithmes de recommandation pour des sites de vente en ligne), mais elle a aussi donné la possibilité de disposer d'une information

2.2 Le Développement économique et le Big Data

Les données sont des informations issues de diverses sources, telles que des personnes, des images, du texte, des capteurs et des sites web. Elles proviennent également d'appareils technologiques comme les téléphones portables, les ordinateurs, les kiosques, les tablettes et les caisses enregistreuses. Récemment, le volume de données générées par les capteurs a connu une importante augmentation. Les capteurs sont désormais installés dans de plus en plus de lieux et dans un nombre croissant d'objets, y compris les caméras de sécurité, les feux de circulation, les voitures intelligentes, les thermomètres et même les vignes.

Le terme Big Data désigne une grande quantité de données, mais qu'entend-on par « grande quantité » ? Personne ne sait exactement à partir de quel volume les données entrent dans la catégorie du « Big Data ». Voici trois caractéristiques qui indiquent qu'une entreprise peut être confrontée au Big Data :

1) Elle doit faire régulièrement face à la nécessité d'accroître l'espace de stockage afin de pouvoir gérer quantité élevée de données (volume).
2) Elle doit faire face à une croissance rapide et exponentielle de la quantité de données (vitesse).
3) Elle doit faire face à des données générées dans différents formats (variété).

Quelle est la quantité de données collectées par les capteurs ? Voici quelques estimations possibles :

- Les capteurs d'une voiture autonome peuvent générer 4 000 gigaoctets (Go) de données par jour.

- Un moteur d'Airbus A380 génère 1 pétaoctet (Po) de données sur un vol reliant Londres à Singapour.

- Les capteurs de sécurité dans le secteur des opérations minières peuvent générer jusqu'à 2,4 téraoctets (To) de données toutes les minutes.

- Les capteurs d'une « maison connectée » peuvent produire jusqu'à 1 gigaoctet (Go) de données par semaine.

Bien que le Big Data représente un réel défi pour les entreprises en matière de stockage et d'analytique, il peut également fournir des informations précieuses pour ajuster leur mode de fonctionnement et améliorer la satisfaction client.

Quels sont les défis du Big Data ?

Selon les estimations d'IBM en matière de Big Data IBM « chaque jour nous créons 2,5 quintillions d'octets de données ». Pour mettre cet élément en contexte, chaque minute de chaque jour :

- Nous chargeons plus de 300 heures de vidéos YouTube.
- Nous envoyons plus de 3,5 millions de messages texte.
- Nous recevons en flux continu plus de 86 000 heures de vidéos Netflix.
- Nous « aimons »plus de 4 millions de publications Facebook.
- Nous demandons plus de 14 millions de prévisions de La chaîne météo.

La croissance rapide des données peut être un avantage ou un obstacle à la réalisation des objectifs des entreprises. Pour réussir, celles-ci doivent être en mesure d'accéder à leurs données et de les gérer aussi facilement que possible.

Compte tenu de la création constante d'énormes quantités de données, les technologies et les entrepôts de données traditionnels ne parviennent pas à faire face aux besoins de stockage. Même avec les installations de stockage cloud qui sont fournies par des entreprises comme Amazon, Google, Microsoft et bien d'autres, la sécurité des données stockées devient un gros problème. Les solutions Big Data doivent être sécurisées, avoir une tolérance aux pannes élevée et utiliser la réplication afin d'éviter toute perte de données. La question n'est pas seulement de stocker les gros volumes de données, mais aussi de les gérer.

Le Big Data pose cinq problèmes majeurs en matière de stockage des données.

Où peut-on stocker le Big Data ?

Le Big Data est généralement stocké sur plusieurs serveurs, habituellement hébergés dans des data centers. Pour la sécurité, l'accessibilité et la redondance, les données sont généralement distribuées et/ou répliquées sur de nombreux serveurs différents dans de nombreux data centers distincts.

2.2.1 Fog computing

Le fog computing est une architecture qui utilise les clients ou les appareils de « périphérie » des utilisateurs finaux pour réaliser une portion substantielle du

prétraitement et du stockage dont une entreprise a besoin. Le fog computing a été conçu pour maintenir les données au plus près de la source pour le prétraitement.

Les données de capteur, en particulier, peuvent être préalablement traitées près de l'endroit où elles ont été collectées. Les informations recueillies avec le traitement préalable peuvent être retransmises au système de l'entreprise afin de modifier les processus, le cas échéant. Étant donné que les données de capteur sont préalablement traitées par des terminaux au sein de ce système, les communications entre les serveurs et les terminaux sont plus rapides. Cette opération nécessite moins de bande passante que l'accès continu au cloud.

Une fois que les données ont été préalablement traitées, elles sont souvent stockées à long terme, sauvegardées ou analysées plus en détail via le cloud.

2.2.2. Le cloud et le cloud computing

Comme indiqué précédemment, le cloud est un ensemble de data centres ou des groupes de serveurs connectés. L'accès aux logiciels, au stockage et aux services disponibles sur les serveurs est obtenu via une interface de navigateur Internet. Les services cloud sont fournis par de nombreuses grandes entreprises comme Google, Microsoft et Apple. Les services de stockage cloud sont fournis par différents fournisseurs, dont Google Drive, Apple iCloud, Microsoft OneDrive et Dropbox.

Du point de vue des particuliers, les services cloud permettent les actions suivantes :

- Stocker toutes les données, telles que les images, la musique, les vidéos et les e-mails, libérant ainsi de l'espace sur le disque dur local
- Accéder à de nombreuses applications au lieu de les télécharger sur un appareil local
- Accéder aux données et aux applications de n'importe où, à tout moment et sur n'importe quel appareil

L'un des inconvénients liés à l'utilisation du cloud est que vos données peuvent tomber entre de mauvaises mains. Vos données sont à la merci de la robustesse de la sécurité du fournisseur de cloud que vous avez choisi.

Du point de vue des entreprises, les services cloud et le cloud computing répondent à divers problèmes en matière de gestion des données :

- Il permet d'accéder aux données de l'entreprise partout, à tout moment.
- Il rationalise les opérations IT d'une entreprise en s'abonnant uniquement aux services nécessaires.

- Il élimine ou réduit le besoin d'équipements IT, de maintenance et de gestion sur site.

- Il réduit le coût des équipements, de l'énergie, des installations physiques requises et le besoin en formation du personnel.

- Il permet de répondre rapidement aux exigences liées au volume croissant des données.

2.2.3 Le traitement distribué

En matière de gestion des données, le traitement analytique ne posait pas de problème lorsque seuls les humains créaient des données. Le volume de données était gérable et relativement facile à répartir. Toutefois, avec l'explosion des systèmes d'automatisation et la croissance exponentielle des applications web et des données générées par les machines, l'analytique est de plus en plus difficile à gérer. En effet, 90 % des données actuellement disponibles ont été générées au cours des deux dernières années. Une telle augmentation de volume dans un si court laps de temps est un signe révélateur d'une croissance exponentielle. Il devient difficile de traiter et d'analyser une si grande quantité de données dans un délai raisonnable.

Au lieu de traiter de grandes bases de données avec de gros ordinateurs grand public puissants et de les stocker sur des baies de disques géantes (montée en charge verticale), le traitement distribué des données récupère un grand volume de données et les divise en ensembles plus petits. Ces volumes de données plus petits sont distribués dans de nombreux emplacements où ils sont traités par de nombreux ordinateurs équipés de processeurs plus petits. Dans l'architecture distribuée, chaque ordinateur analyse sa partie de l'image du Big Data (montée en charge horizontale).

La plupart des systèmes de fichiers distribués sont conçus pour ne pas être visibles par les programmes client. Le système de fichiers distribué localise les fichiers et déplace les données, mais les utilisateurs n'ont aucun moyen de savoir de quelle manière les fichiers sont distribués sur les différents serveurs et nœuds. Les utilisateurs accèdent aux fichiers comme si ces derniers étaient stockés sur leur propre machine. Tous les utilisateurs disposent de la même vue du système de fichiers et peuvent accéder simultanément aux mêmes données.

Hadoop a été créé pour gérer ces volumes de Big Data. Au départ, le projet Hadoop se composait de deux entités : HDFS, un système de fichiers distribué insensible aux pannes, et MapReduce, une solution de traitement des données axée sur la

distribution. Aujourd'hui, Hadoop est à lui seul un écosystème très complet de logiciels pour la gestion du Big Data.

Ce logiciel open source permet le traitement distribué des grands ensembles de données stockés dans des clusters d'ordinateurs et dont la taille peut atteindre plusieurs téraoctets. Hadoop est conçu pour pouvoir prendre en charge tant des serveurs individuels que des milliers de machines, offrant chacune le stockage et le calcul au niveau local. Pour gagner en efficacité, Hadoop peut être installé et exécuté sur plusieurs machines virtuelles. Celles-ci peuvent toutes fonctionner en parallèle afin de traiter et de stocker les données.

Hadoop se divise en deux principales fonctionnalités qui sont devenues une référence dans le domaine de la gestion du Big Data :

- Évolutivité : la taille plus importante des clusters améliore les performances et offre des fonctions de traitement de données plus performantes. Avec Hadoop, la taille de cluster est facilement ajustable. Vous pouvez passer d'un cluster à cinq nœuds à un cluster à mille nœuds sans augmenter excessivement les tâches d'administration.

- Tolérance aux pannes : Hadoop réplique automatiquement les données entre tous les clusters afin d'éviter toute perte. Si un disque, un nœud ou un rack entier tombe en panne, les données sont en sécurité.

2.3 Pourquoi les entreprises analysent-elles les données ?

Dans le monde numérique d'aujourd'hui, toutes les entreprises doivent rivaliser d'ingéniosité pour rester compétitives et ne pas tomber dans l'oubli. L'IoT est désormais partie intégrante de cette quête d'efficacité et d'innovation.

De nombreuses entreprises ont pour objectif de collecter et d'analyser les énormes quantités de données d'utilisation des nouveaux produits pour en tirer une vue d'ensemble utile. L'analyse des données permet aux entreprises de mieux comprendre l'impact de leurs produits et services, d'ajuster leurs méthodes et leurs objectifs, et de fournir à leurs clients de meilleurs produits plus rapidement. La possibilité de transformer leurs données en informations exploitables leur offre un réel avantage.

Les données sont le nouveau carburant des entreprises. Comme le pétrole brut, elles sont précieuses, mais difficilement utilisables lorsqu'elles ne sont pas raffinées. Le pétrole brut doit être transformé en essence, en plastique, en produits chimiques et en d'autres substances pour créer un produit de valeur. Il en est de même pour les données. Pour avoir de la valeur, les données doivent être décomposées et analysées.

La valeur provient de deux principaux types de données traitées : les données transactionnelles et les données analytiques. Les informations transactionnelles sont capturées et traitées à mesure que les événements se produisent. Elles sont utilisées pour analyser les rapports de vente et les calendriers de production quotidiens afin de déterminer le stock à prévoir. Les informations analytiques sont utilisées pour les tâches d'analyse de la direction. Elles permettent par exemple de déterminer si

l'entreprise doit construire une nouvelle usine ou recruter d'autres représentants commerciaux.

Quelles sont les Sources d'informations ?

La source de données des grands ensembles de données varie. Outre les informations issues des capteurs, les autres données proviennent de tout ce qui a été analysé, saisi et publié sur Internet depuis des sources telles que :

- Les sites de médias sociaux comme Facebook, YouTube, eHarmony et Twitter
- Les pages HTTP, les pages web et les moteurs de recherche sur Internet
- Les données historiques des archives publiques et privées
- Les métadonnées associées aux e-mails, aux documents transmis et aux images
- Les formulaires médicaux, les formulaires d'assurance et les formulaires d'impôt
- La recherche sur le génome avec l'ADN

Les données collectées sont classées comme étant structurées ou non structurées.

Les données structurées sont créées par des applications qui utilisent une saisie au format « fixe » comme des feuilles de calcul ou des formulaires médicaux. Même si les données sont considérées comme structurées, des applications distinctes créent des fichiers dans différents formats qui ne sont pas nécessairement compatibles entre eux. Les données structurées doivent parfois être manipulées et converties dans un format commun tel que CSV.

Les fichiers de valeurs séparées par des virgules (CSV) sont un type de fichier en texte brut qui utilise des virgules pour séparer les colonnes dans une table de données et le retour chariot pour séparer les lignes. Chaque ligne représente un enregistrement. Bien que ces fichiers soient fréquemment utilisés pour importer et exporter des données dans les feuilles de calcul et les bases de données traditionnelles, il n'existe pas de norme spécifique. Les formats JSON et XML sont également des types de fichier en texte brut qui utilisent un processus standard pour consigner les enregistrements de données. Ces formats de fichier sont compatibles avec un large choix d'applications. Convertir les données dans un format commun est un moyen efficace pour combiner des données provenant de sources distinctes.

Les données non structurées sont générées dans un style « libre » : audio, vidéo, pages web, tweets, etc. Les données non structurées nécessitent des outils différents pour préparer leur traitement ou leur analyse. Voici deux exemples :

- Les pages web sont créées pour fournir des données aux humaines et non aux machines. Les outils de « web scraping » (en français, extraction de contenu web) extraient automatiquement les données des pages HTML. Ils fonctionnent de la même manière que le robot d'indexation d'un moteur de recherche. Ils parcourent le web pour en extraire des données et créer la base de données requise pour répondre aux critères de la recherche. Pour accéder à Internet, les

logiciels d'extraction de contenu web peuvent utiliser le protocole HTTP ou un navigateur web. L'extraction de contenu web est généralement un processus automatisé qui utilise un robot d'exploration pour le datamining. Des données spécifiques sont rassemblées et copiées à partir du web vers une base de données ou une feuille de calcul. Les données peuvent ainsi être facilement analysées.

- De nombreux fournisseurs de services web tels que Facebook proposent des interfaces standardisées pour collecter automatiquement les données via des API. L'approche la plus courante consiste à utiliser des API RESTful. Les API RESTful utilisent le protocole de communication HTTP et la structure JSON pour l'encodage des données. Les sites web tels que Google et Twitter regroupent de grandes quantités de données chronologiques et statiques. Les ingénieurs et analystes de données ont tout intérêt à se familiariser avec les API associées à ces sites afin de pouvoir accéder aux grands volumes de données générés en continu sur Internet.

2.4 Automatisation des données

Le terme automatisation désigne tout processus auto exécuté qui réduit, voire élimine, toute nécessité d'une intervention humaine.

Auparavant, l'automatisation était réservée au secteur de la fabrication. Les tâches très répétitives, telles que l'assemblage automobile, ont été confiées aux machines, ce qui a donné naissance aux chaînes d'assemblage modernes. Les machines présentent l'avantage de pouvoir répéter la même tâche sans jamais se fatiguer et sans commettre les erreurs auxquelles les humains peuvent difficilement échapper. La productivité est donc supérieure, car les machines peuvent fonctionner 24 heures sur 24, sans aucune pause. Elles fournissent également un produit plus uniforme.

Les réseaux du futur tels que l'internet des objets (IoT) et les réseaux de capteurs sans fil ouvrent tout un univers nouveau, où les tâches qui nécessitaient précédemment une intervention humaine peuvent être automatisées. Comme nous l'avons vu, l'IoT permet la collecte d'importants volumes de données qui peuvent être analysées rapidement afin de fournir des informations susceptibles d'orienter un événement ou un processus.

Avec l'adoption croissante de l'IoT, l'automatisation devient de plus en plus importante. L'accès à d'énormes quantités de données de capteur traitées rapidement a incité les têtes pensantes à réfléchir à la façon dont ils pourraient appliquer les concepts de l'apprentissage automatique et de l'automatisation aux tâches quotidiennes. De nombreuses tâches de routine sont automatisées afin d'améliorer leur précision et leur efficacité.

L'automatisation est souvent associée au domaine de la robotique. Les robots sont utilisés dans des conditions dangereuses comme l'exploitation minière, la lutte contre les incendies et le nettoyage des accidents industriels, réduisant ainsi les risques pour

les humains. Ils sont également utilisés dans des tâches telles que les chaînes d'assemblage automatisées.

De nos jours, l'automatisation est partout, des caisses en libre-service disponibles dans les magasins aux contrôles environnementaux dans les bâtiments, en passant par les voitures et les avions autonomes. À combien de systèmes automatisés avez-vous affaire en une seule journée ?

Tableau 1.1 : quelques exemples sur l'automatisation

	Automatisation	Pas d'automatisation
La température et l'éclairage de votre domicile ou de votre société sont ajustés en fonction de vos habitudes quotidiennes	✓	
Vous utilisez un appareil distant pour démarrer votre voiture		✓
Les robots sont utilisés dans des conditions dangereuses come l'exploitation minière, la lutte contre les incendies et le nettoyage des accidents industriels réduisant ainsi les risques pour la sécurité humains	✓	
Vous utilisez les services bancaires en ligne pour payer une facture		✓
Les niveaux de production sont automatiquement liés à la demande, éliminant ainsi les produit superflus tout en réduisant l'impact sur l »environnement	✓	
Vous réglez le volume de la télévision avec une télécommande		✓
Votre GPS recalcule la meilleure route vers la destination en fonction d'un embouteillage en cours	✓	
Un réfrigérateur détecte que vous n'avez plus de lait et en commande donc plus	✓	

2.5 Conclusion

La technologie, les données, le volume et la capacité des données, les big data peuvent être utilisés à différentes fins : pour faciliter la communication entre les acteurs (les machines, les serveurs, les réseaux informatiques ou même les capteurs). Tous ca pour faire circuler l'information utile aux activités économiques en zones rurales, pour améliorer des services existants, ou encore pour en créer de nouveaux.

Chapitre 3

Interconnexion et intégration de plusieurs objets connectés

3.1 Introduction

3.2 La technologie Bluetooth

Bluetooth est une technologie de réseau personnel sans fil WPAN (Wireless personal Area Network) qui a été créé par Ericsson en 1994. Ensuite a partir de 1998 elle a eter développée par l'organisation Bluetooth Special Interest Group (Bluetooth SIG). Cette organisation comporte des personnes de différentes sociétés dot font partie Ericson, Intel, IBM, Nokia, Toshiba, 3Com, Microsoft et Motorola

3.2.1 La topologie du réseau Bluetooth

a) Réseau piconet

Un piconet est un réseau qui se crée de manière instantanée et automatique quand plusieurs périphériques Bluetooth sont dans un même rayon (10 m).
Ce réseau suit une topologie en étoile : 1 maître / plusieurs esclaves. Un périphérique maître peut administrer jusqu'à 7 esclaves actifs ou 255 esclaves en mode parked (=inactif).
La communication est directe entre le maître et un esclave. Les esclaves ne peuvent pas communiquer entre eux.
Tous les esclaves du piconet sont synchronisés sur l'horloge du maître. C'est le maître qui détermine la fréquence de saut de fréquence pour tout le piconet.

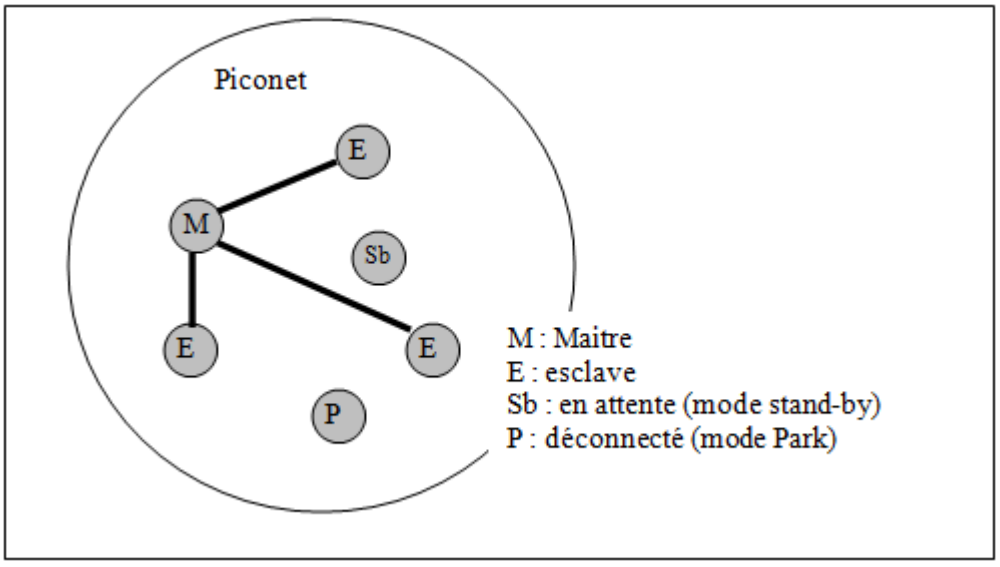


Figure 3.1 Réseau Bluetooth Piconet

b) Réseau Scatternet

Les Scatternets sont des interconnexions de Piconets (Scatter = dispersion).
Ces interconnexions sont possibles car les périphériques esclaves peuvent avoir plusieurs maîtres, les différents piconets peuvent donc être reliés entre eux.

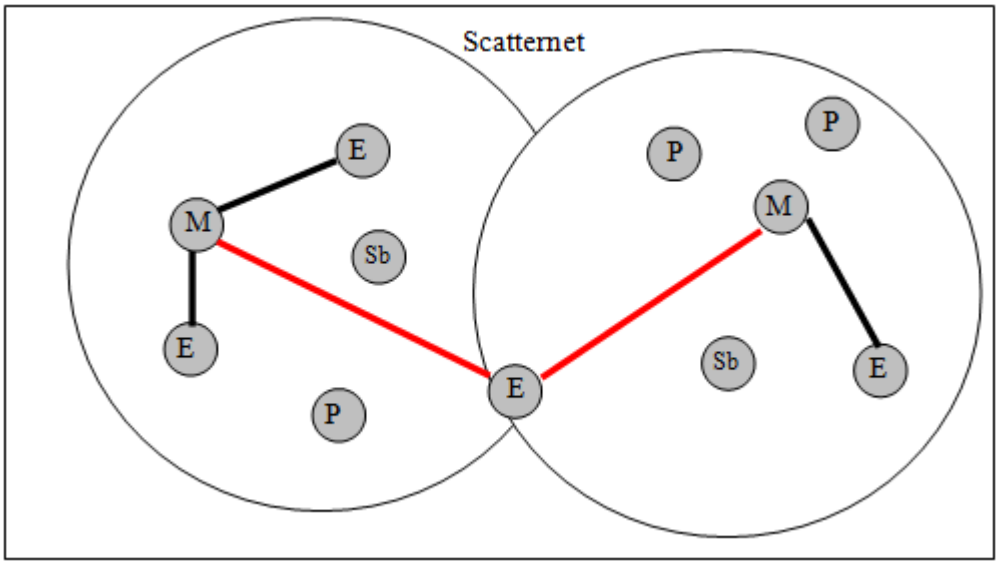


Figure 3.2 Réseau Bluetooth Scattenet

3.2.2 Types de communication dans Bluetooth

Les communications dan un réseau Bluetooth peuvent être synchrones ou asynchrones assurées moyennant deux types de lien :

- Synchronous Connection Oriented (SCO)
- Asynchonous connection Less (ACL)

1) Synchronous Connection Oriented (SCO)

Ce type de lien permet une connexion point à point symétrique entre le maitre et un esclave permettant la communication dans des slots réservés.
Les liens SCO sont généralement utilisés pour transporter des données avec contrainte de temps comme la voix. Le maître peut supporter jusqu'à trois connexions SCO avec un même esclave ou avec différents esclaves.

2) Asynchonous connection Less (ACL)

Dans les slots qui ne sont pas réservés pour les connexions SCO le maitre peut échanger des paquets avec n'importe quel esclave. On dit que le maitre a établie une connexion ACL avec les esclaves.
Entre un maitre et un esclave une seule connexion ACL peut exister.

De façon plus précise, le temps est découpé en tranches, ou slots, à raison de 1 600 slots par seconde. Un slot fait donc 625 µs de long, comme illustré à la figure 21.4.

La figure 2.5 illustre un scénario de transmissions simultanées de trafics CSO et ACL

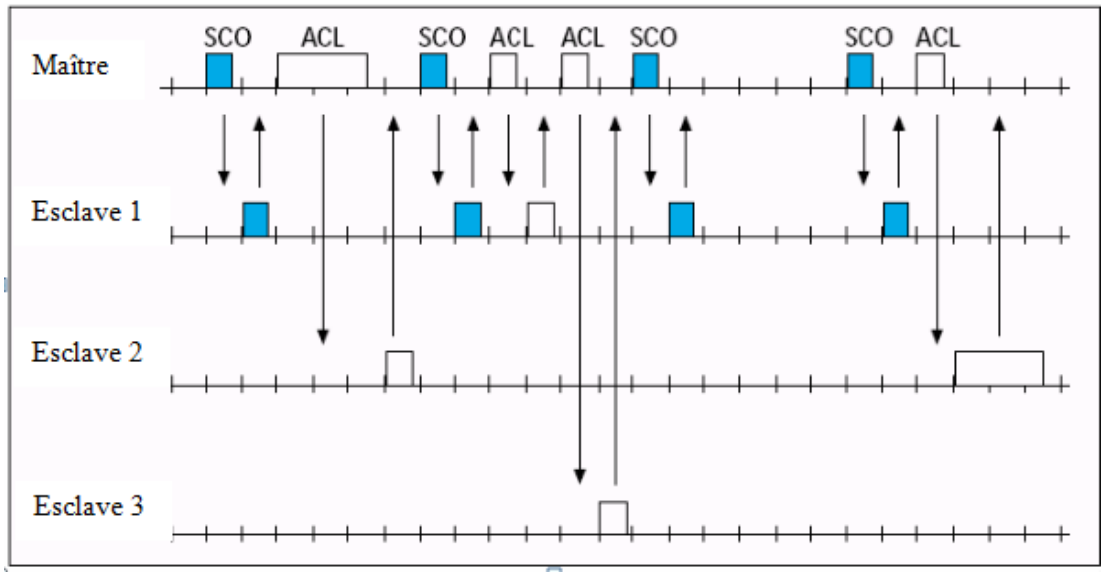


Figure 3.3 Exemple de transmissions simultanées SCO et ACL

2.1.3 Etats des terminaux Bluetooth

Lorsqu'aucune connexion n'est pas encore établie dans un réseau Piconet ou Scatternet , tous les périphériques sont en mode Standby (Fig 3.4). Dans ce mode, une unité non connectée « écoute » les messages périodiquement toutes les 1.28 secondes. A chaque fois qu'une unité rentre en mode actif, celle-ci écoute un ensemble de 32 sauts de fréquences qui lui est propre.

La procédure de connexion est initiée par n'importe quelle unité du réseau, celle-ci devenant alors Maître. Une connexion est établie par un message de type PAGE si l'adresse de l'unité à connecter (unité Esclave) est connue ou alors un message de type INQUIRY (demandant à toutes les unités de répondre) suivi d'un PAGE si l'adresse n'est pas connue.

Dans l'état initial PAGE, l'unité Maître envoie un train de 16 messages identiques de paging sur 16 différents sauts de fréquences spécifiques à l'unité pagée (Esclave). Ce train de message couvre la moitié de la séquence de sauts de fréquences que l'unité Esclave écoute en mode STANDBY et il est répété 128 fois, ce qui correspond à 1.28 s. Si aucune réponse n'est reçue après ce délai, le Maître retransmet le même train de message de paging dans les 16 sauts de fréquences restant de la période d'écoute de l'unité Esclave.

Le délai maximum pour que l'unité Maître atteigne une unité Esclave est donc de deux fois 1.28 s c'est à dire 2.56 s.

Le message INQUIRY est utilisé afin de communiquer avec des équipements dont on ne connaît pas l'adresse (par exemple des imprimantes ou des fax publics). Le message INQUIRY ressemble très fortement au message PAGE mais nécessite un train de paging supplémentaire pour collecter toutes les réponses.

Pour les unités connectées, trois modes d'économie d'énergie peuvent être utilisés si aucune donnée ne doit être transmise :

- Mode HOLD : l'unité Maître peut forcer les unités Esclaves en mode HOLD. Dans ce mode, il n'y a plus que l'horloge interne qui fonctionne. Les unités Esclaves peuvent aussi demander à passer en mode HOLD. Le transfert de données ne reprendra que lorsque l'unité aura quittée le mode HOLD.
  Le mode HOLD est typiquement utilisé dans le cas de connexions avec plusieurs piconets, ou encore lorsque les données ne sont pas envoyées très fréquemment. Une application possible serait un thermostat qui transmettrait ses données une fois toutes les minutes.

- Mode SNIFF : dans ce mode, une unité Esclave écoute les messages du réseau avec une plus grande périodicité en réduisant son cycle de travail. La périodicité est programmable et dépend de l'application ;

- Mode PARK : dans ce mode une unité est toujours synchronisée au réseau mais ne participe pas au trafic. Cette unité abandonne son adresse MAC et écoute occasionnellement le trafic de l'unité Maître pour se re-synchroniser.

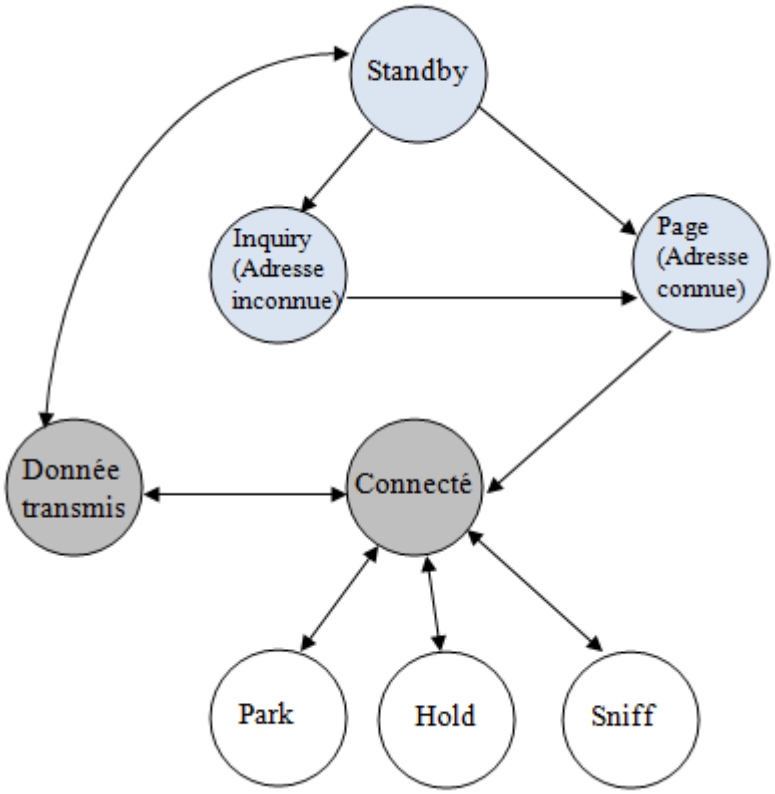


Figure 3.4 Etats des terminaux Bluetooth

3.2.4 Architecture Bluetooth

L'architecture Bluetooth est composée de trois grandes parties (fig 3.4)

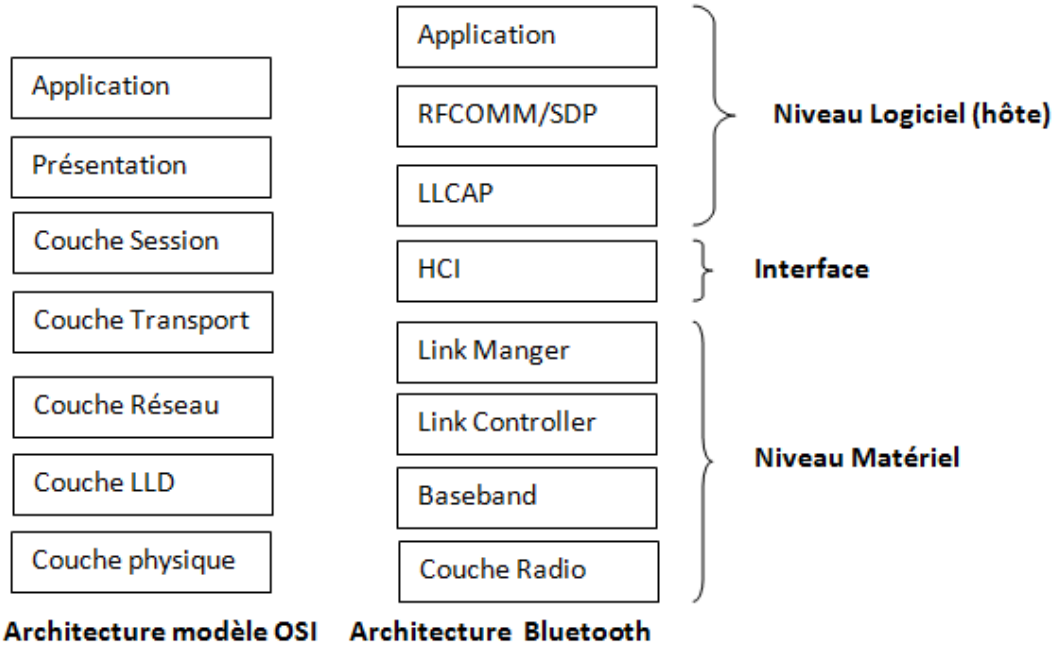


Figure 3.5 Architecture de la technologie Bluetooth

- Le Bluetooth core : composé de la couche radio du Baseband du link Manager et du Link controller.
  - La couche Radio : elle est en charge de l'émission et de la réception du flux de bits modulés.
  - Baseband : il est en charge de la synchronisation entre unité, le l'établissement de liaison, du multiplexage, des paquets, du contrôle de flux, de la détection et de la correction d'erreur.
  - Link Manager : il est en charge de la gestion des états , du contrôle des paquets et du flux sur le lien.
  - Logical Link Control and Management : il est en charge du multiplexage des protocoles utilisateurs.

- Les protocoles :

- RFCOMM : émulation d'un câble série entre deux périphériques Bluetooth. Ainsi, des applications fonctionnant directement sur un port série (Hyperterm par exemple dans le monde Microsoft), sont capables de communiquer entre elles via un lien Bluetooth ce qui permet entre autre d'effectuer un transfert de fichier.
- SDP Service discovery Protocol : il a pour rôle la recherche de services. La notion de service est très large : RFCOMM constitue un service, toute application utilisant ou s'appuyant sur RFCOMM est un service, SDP lui-même est un service. Retenons pour l'instant que plusieurs organismes sont en train de définir des normes permettant la découverte et la recherche de services (JINI, Salutation, UPNP). Il est probable que dans un futur assez proche, SDP sera utilisé par ces normes pour effectuer la découverte de services rendus par des périphériques Bluetooth.

Les profils : un profil définit un ensemble de composantes protocolaires nécessaires à la mise en œuvre d'applications Bluetooth. A l'heure actuelle, plusieurs profils ont été spécifiés par le Bluetooth SIG.

Couche physique (RF : radio Frequency)
Cette couche s'occupe de l'émission et la réception des ondes radio. Elle définit les caractéristiques de la transmission telles que la bande de fréquences, les canaux, la modulation, etc.
La transmission se fait dans la bande de fréquence 204GHZ ISM (Industriel science and Medecine)

Contrôleur de liens
La bande de base ou baseband est gérée au niveau matériel.
C'est au niveau de la bande de base que sont définit les adresses matérielles des périphériques (équivalent à l'adresse MAC d'une carte réseau), cette adresse est nommée BD-ADDR (Bluetooth Device Adress) est codée sur 48 bits.
C'est également la bande de base qui gère les différents types de communication entre les appareils.

Le contrôleur de liaison (link controler)
Cette couche gère la configuration et le contrôle de la liaison physique entre deux appareils.

Le gestionnaire de liaison (link manager)

Cette couche gère les liens entre les périphériques maitres et les esclaves, il gère aussi les types de liaisons (synchrones ou asynchrones)

- L'authentification
- Le pairage (relier deux machines entre elles)
- La création et la modification des lés
- cryptage

HCI (Interface de Contrôle de l'hôte)

Son rôle est de séparer le cote hard du coté soft
Les protocoles de transport suivants son supportés :

- USB
- PC Card
- RS-232
- UARI

L2CAP

LLCAP (Link Control & Adaptation Protocol)
Cette couche permet d'utiliser simultanément différents protocole de niveaux supérieurs

RFCOMM c'est un service basé sur les spécifications RS-232, il peut servir a faire passer une connexion IP par Bluetooth

SDP (Service Discovery Protocol)
Ce protocole permet a un appareil bluetooth de rechercher d'autre appareils

3.3 La norme 802.15.3 UWB (Ultra Wide Band)

La technologie Ultra Large Bande (Ultra Wide Band - UWB) est une technique de transmission radio utilisant des signaux à très large spectre. À ses débuts, cette technologie était réservée aux applications radar, puis elle a été élargie aux applications de communications. En 2002, la FCC (Federal Communication Commission), l'organisme américain de régulation des communications, a réglementé l'ULB. Elle donne une définition précise et fixe les niveaux de densité de puissance maximale autorisés (- 41 dBm /MHz pour la bande haute). La définition de l'ultra large bande donnée par la FCC en février 2002 est la suivant
Un signal est dit ultra large bande si :

- sa bande passante est au minimum de 500 MHz

$$BP_{relative} = 2\frac{f_h - f_l}{f_h + f_l} > 0,2$$

- Sa bande passante relative (Bprelative) est supérieur à 20%

Ou fh et fl désigne respectivement les fréquences limites hautes et basse du spectre du signal

3.3.1 Types applications visée par l'UWB

- Radar haute résolution : nombreuse information sur la cible
- Imagerie :
  - à travers les murs détection/identification présence des personnes (respiration, battement du cœur)
  - Médicale : meilleur que l'IRM possibilité de bouger
- Communication: application militaires
- Systèmes UWB pour équipements sur vêtements
- Localisation (Location Aware Communications)

3.3.3 Caractéristiques UWB

- Norme 802.15.3 et 802.15.3a
- Distances de couverture (km) : 0.010 (10 m)
- Bande de fréquence (MHz) : > 500 (3.1 Ghz -10.6 Ghz)
- Débits (kb/s) : 500
- Nombre de nœuds par réseau : NA

3.3.4 Techniques de transmission dans les UWB

Deux principales techniques de transmission sont utilisés dans la technologie UWB : la technique discontinue et la technique continue.
Pour la première, on trouve principalement la technique ultralarge bande par impulsion (IR-UWB). a seconde comprend les techniques classiques comme l‟OFDM (Orthogonal Frequency Division Multiplex) et la modulation de fréquence large bande

1) **Technique Continue: (OFDM)** le principe de l'OFDM consiste à répartir sur un grand nombre de sous-porteuses le signal numérique que l'on veut transmettre. Pour que les fréquences des sous-porteuses soient les plus proches possibles et ainsi transmettre le maximum d'information sur une portion de fréquences donnée

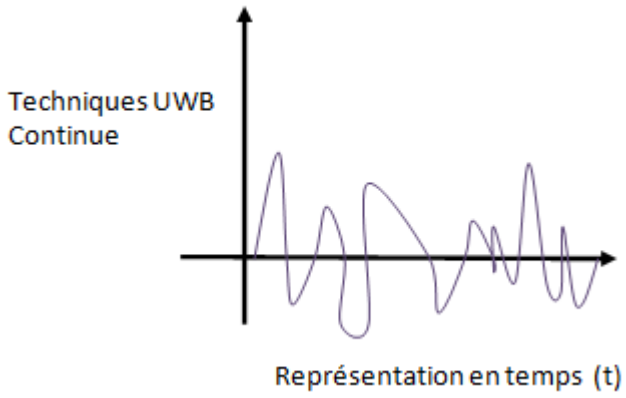


Figure 3.6 Technique OFDM

2) **Technique discontinue: (par impulsion IR-UWB)**
L'impulse Radio UWB (IR-UWB) propose d'utiliser des impulsions de très courte durée, occupant un spectre fréquentiel très large

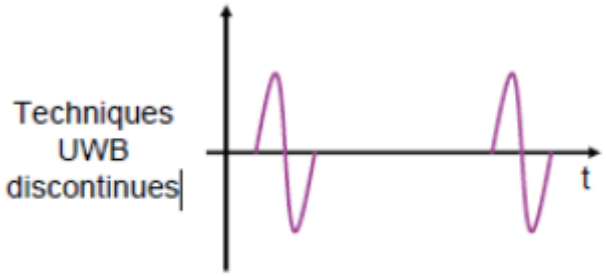


Figure 3.7 : Technique discontinue

3.3.5 Avantages et inconvénients de l'UWB

Les Avantages de l'UWB sont :

- une très grande capacité de canal de transmission. Puisque les données sont transmises sur une importante largeur de bande, cela fournit un débit très élevé pour les applications des réseaux multi-usagers.
- une faible probabilité de détection et d'interception . Cette faible distinction est due à la faible densité spectrale des signaux UWB, de même qu'à une puissance et un rapport signalant un bruit relativement faibles.
- une absence d'interférence. Les signaux des systèmes de communication UWB n ' interfèrent pas avec les autres signaux partageant avec eux le même spectre.
- une bonne capacité de pénétration. Les signaux UWB peuvent ainsi traverser différents types de surface.
- une accessibilité pour des applications de localisation. La détection et la précision du signa l UWB, grâce à leur résolution , rendent cette technologie accessible pour des applications de localisation.
- une faible consommation d'énergie. Grâce à la faible puissance de transmission et à l'utilisation d 'impulsions de très courte durée en émission et en réception , les systèmes UWB consomment peu d'énergie .

Les inconvénient de l'UWB :

- une faible couverture. La très large bande et la faible puissance du signal UWB limitent le type d'applications possibles qui utilisent cette technologie.
- Le haut débit induit l'utilité du traitement d'un signal très dense à la réception, avec une rapidité raisonnable, ce qui est difficile à réaliser.

3.4 La norme 802.15.4 ZIGBEE

ZigBee est une technologie de type LP-WPAN (Low Power– Wireless Personal AreaNetwork) qui est un réseau sans fil à bas débit et à courte portée qui utilise les ondes hertziennes pour transporter des messages entre deux ou plusieurs entités réseaux. Il est caractérisé par une portée comprise entre quelques mètres et quelques centaines de mètres et un débit faible (maximum 250 kbits/s). La différence entre ZigBee et la plupart des autres réseaux locaux et personnels sans fil (WiFi, Bluetooth) se situe au niveau de l'utilisation du médium hertzien :

ZigBee est optimisé pour une faible utilisation du médium partagé par tous, par exemple 0,1 % du temps. Typiquement, un module ZigBee occupera le médium pendant quelques millisecondes en émission, attendra éventuellement une réponse ou un acquittement, puis se mettra en veille pendant une longue période avant l'émission suivante, qui aura lieu à un instant prédéterminé. ZigBee est conçu pour interconnecter des unités embarquées autonomes comme des capteurs/actionneurs, à

des unités de contrôle ou de commande. De telles entités embarquées peuvent dès lors être alimentées pendant plusieurs mois par des piles classiques.

3.4.1 Caractéristiques du ZIGBEE

-Débit de 20 kb/s, 40kb/s et 250 kb/s suivant la fréquence.
-Méthode d'accès au support de type CSMA-CA (Carrier Sense Multiple Access – Collision Avoidance).
-Protocole avec acquittement et fiable.
-Faible consommation (alimentation sur pile de type AA).

3.4.2 Le modèle en couche ZigBee

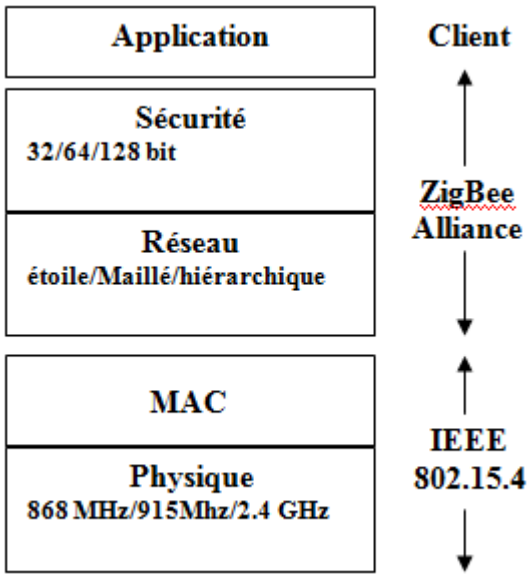


Figure 3.8 Le modèle en couche ZigBee

- **La couche physique**

Supporte la gestion des fréquences d'émission et de réception, le débit des données envoyées ou reçues, le type de modulation et le codage numérique des informations
La norme IEEE 802.15.4 a les caractéristiques générales suivantes :
3 bandes de fréquence de fonctionnement : 868 MHz (1 canal), 915 MHz (10 canaux) et 2,4 GHz (16 canaux).

Bande (MHZ)	Débits	Etalement, Modulation

	(Kbits/s)	
780	250	OQPSK/MPSK
950	20 100	GFSK DSSS – BPSK
868-868.6 (1 canal)	20 100	DSSS – BPSK/OQPSK PSSS – BPSK/ASK
902-938 (10 canaux)	40 250	DSSS – BPSK/OQPSK PSSS – BPSK/ASK
2400-2483.5 (16 canaux)	250 1000	DSSS – OQPSK CSS – DQPSK
250-750	110 à 850	ULB
3244-4742		
5944-10234		

Tableau 3.1 Ensemble des bandes possibles dans la norme IEEE 802.15.4 (toutes les bandes ne sont pas disponibles dans l'ensemble des régions du monde), débits attendus sur chaque bande et méthodes d'étalement et de modulation associées

- **La couche d'accès au médium ou MAC (Medium Access Control)**

La couche MAC s'appuie sur les ressources de la couche physique. C'est la couche principale pour les aspects logiciels qui définit la façon dont un nœud du réseau pourra dialoguer (transmettre ou recevoir). Ces mécanismes sont tous détaillés dans la spécification du standard IEEE 802.15.4.

La couche MAC gère les accès au médium radio, résolvant notamment les problèmes d'accès concurrents. 802.15.4 propose deux modes pour l'accès au médium :
Un mode non coordonné (totalement CSMA/CA) et un mode coordonné, ou beacon mode
Le mode coordonné est disponible uniquement dans une topologie étoile où le coordinateur de cette étoile envoie périodiquement des trames balises (beacon) pour synchroniser les nœuds du réseau

Le mode non coordonné (totalement CSMA/CA) fonctionne sans émission de beacon donc pas de synchronisation entre les différents nœuds du réseau. Les nœuds voulant émettre des données doivent utiliser le protocole CSMA/CA « non slotté », c'est-à-dire que le début d'une émission se fait dès que le médium est jugé libre,

- **La couche réseau**

Assure principalement les règles d'établissement d'un réseau, l'association et l'interconnexion de tous les nœuds dans le réseau, le transfert des informations entre les entités de ce réseau via une route, ainsi que la structure des messages (trames) qui seront échangés.

- **La couche application**

Utilise les couches inférieures pour une application communicante donnée. Elle donne entre autres une signification aux informations échangées dans le réseau

3.4.3 Topologie réseau du protocole ZigBee/la norme IEEE 802.15.4

La norme IEEE 802.15.4 supporte les topologies réseaux : étoile, maillé et Cluster, et utilisant 3 types d'équipements (les nœuds du réseau) qui peuvent être :

- ***Le coordinateur du réseau***.
  - Ne peut être qu'un et un seul dans un réseau
  - Tiers de confiance
  - Racine du réseau et passerelle vers les autres réseaux avec alimentation permanente
- ***L'équipement à fonctionnalités complètes FFD (Full Function Device)***
  - Le routeur
  - Equipement intermédiaire qui route les paquets au sein du réseau avec alimentation permanente
- ***.L'équipement à fonctionnalités réduites RFD (Reduced Function Device)***
  - Equipement terminal qui ne communique qu'avec un routeur ou le coordinateur

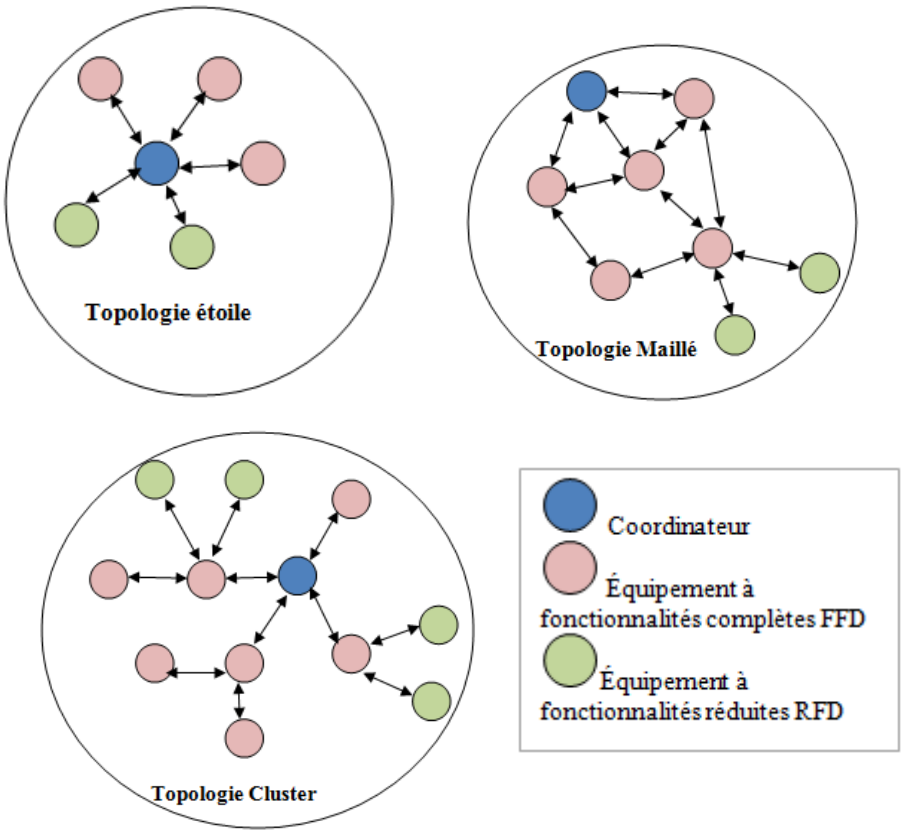


Figure 3.9 Topologie ZigBee/802.15.4

Tableau3.2 comparatif entre Bluetooth, UWB, Zigbee et WiFi.

Standard	**Bluetooth**	**UWB**	**Zigbee**	**Wifi**
Norme IEEE	802.15.1	802.15.3	802.15.4	802.11a/b/g/n
Bande de fréquence	2.4 Ghz	868/915 Mhz 2.4 Ghz	3.1 -10.6 Ghz	2.4 Ghz -5 Ghz
Besoins mémoire	250ko+		4-32 ko	1Mo+
Autonomie ave pile	Mois		Années	Heurs
Nombres de Nœuds	7	8	65000+	32
Vitesse de transfert	1-3 Mb/s	500 Mb/s-7.5 Gp/s	250kb/s	11-54-108-20Mb/s
Cellule de base	Piconet	Piconet	Etoile	BSS
Portée	10-50m	10m	1000m-1500m	300m
Sécurité (protection des données)	16 bit-CRC	32 bits-CRC	16 bits-CRC	32 bits-CRC

3.5 Les réseaux de capteurs sans Fil (RCSF)

3.5.1 Architecture d'un réseau de capteurs sans fil

Un Réseau de Capteurs Sans Fil (RCSF) ou Wireless Sensor Network (WSN) est un réseau informatique composé de petits dispositifs autonomes, fixés ou dispersés aléatoirement dans une zone d'intérêt (zone de captage), utilisant des capteurs coopérant pour surveiller des conditions environnementales ou physiques, comme la température, le son, les vibrations, la pression, le mouvement, etc. (fig4.1) et qui sont liés a une station de base applée aussi Sink ou Puits sa tâche est decollecter les données qui proviennent des autres nœuds (capteurs) du réseau, elle doit être toujours active

Pour les applications environnementales, les données recensées permettent une intervention beaucoup plus rapide et efficace des secours. Mais l'information fournie par le réseau est beaucoup plus utile s'il est possible de déterminer dans quelle partie de la zone surveillée cette information a été recensée. Supposons qu'un réseau de capteurs est déployé pour surveiller une forêt (détecter le feu en mesurant la température de l'air), des résultats utiles de ce réseau seraient non seulement le signal que la température de l'air est très élevé, mais également dans quelle partie de la forêt surveillée le feu a commencé, pour permettre de combattre le feu plus efficacement.

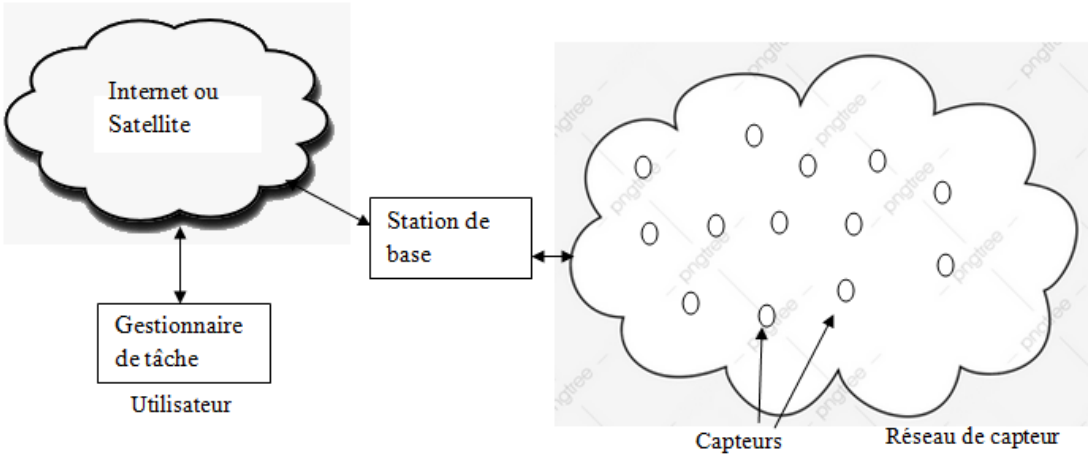


Figure 3.10 Architecture d'un réseau de capteurs sans fil

3.5.2 Les capteurs : Composants et caractéristiques

Les capteurs sont des dispositifs miniaturisés possédants des ressources énergétiques limités et autonomes, capables de traiter des informations et de les transmettre via des ondes radio. Les capteurs prélèvent une information sur le comportement de la partie opérative et la transforment en une information exploitable par la partie commande.

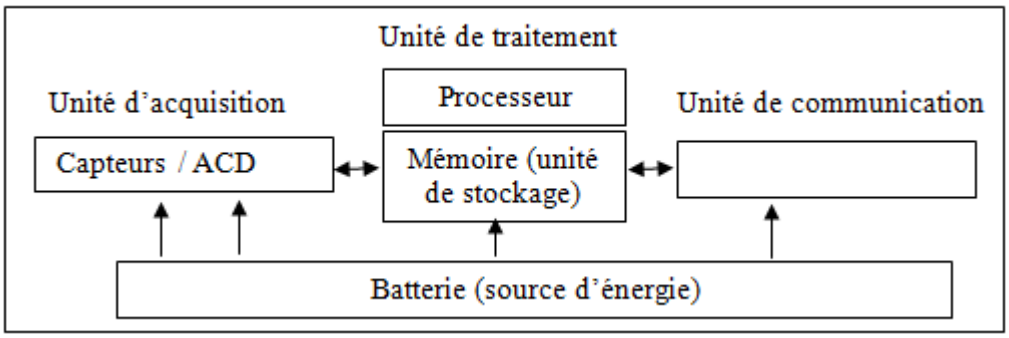


Figure 3.11 Architecture matérielle d'un capteur sans fil

Un capteur est composé de quatre unités de base représentée dans la figure 3.11 :

- **L'unité d'acquisition (ou unité de captage)**
  Elle est composée de deux sous unités : un capteur et un convertisseur ADC (Analog to Digital Converter) analogique –numérique. Les ADCs convertissent ces signaux analogiques aux signaux numériques.
- **L'unité de traitement**
  Elle est composée d'une petite unité de stockage des données et d'un processeur pour traiter les données.

- **L'unité de communication (Emetteur-Récepteur) :** c'est l'unité permettant aux nœuds du réseau de communiquer entre eux via un support de communication radio
- **Batterie :** elle sert à alimenter les autres unités

3.5.3 Pile protocolaires des réseaux de capteurs

La pile protocolaire utilisée par la station de base ainsi que par tous les capteurs du Réseau est illustrée par la Figure 3.2.3.Ce modèle comprend 5 couches (une couche application, une couche transport, une couche réseau, une couche liaison de données, une couche physique) qui ont les mêmes fonctions que celles du modèle OSI, ainsi que 3 niveaux (plans) qui sont: un plan de gestion d'énergie, un plan de gestion de mobilité et un plan de gestion des tâches

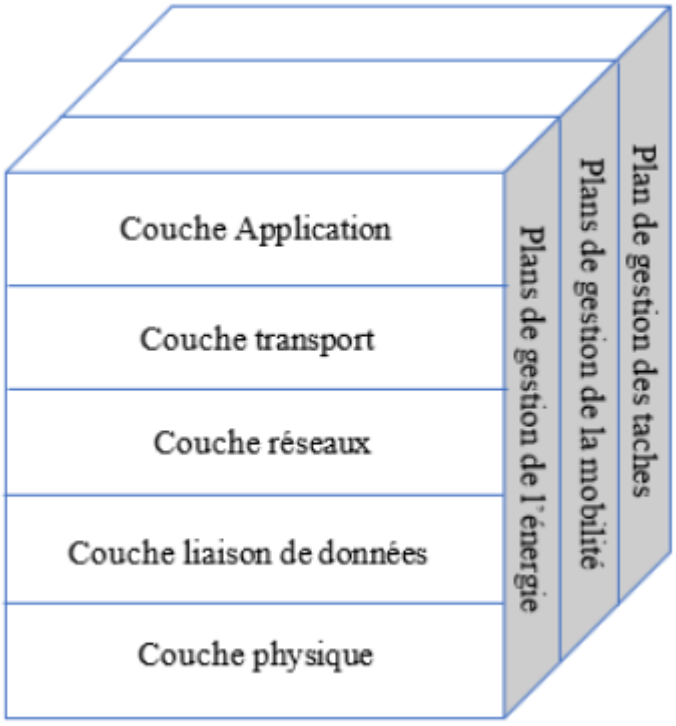


Figure 3.12 : Pile protocolaire dans les réseaux de capteurs sans fil

La couche physique: La couche physique est responsable de la bonne émission et réception de données, de la sélection des fréquences et de la détection du signal.

La couche liaison de données: Cette couche est responsable du multiplexage duflux de données, de la détection et du verrouillage des trames de données et du contrôle des erreurs. Elle assure une connexionfiable (point à point ou point-à-multipoints) selon la topologie du réseau de capteurs. La sous-couche MAC

(MediaAccessControl) de la couche liaison de données gère le contrôle d'accès au média, elle détermine, pour un nœud, la possibilité et le moment pour accéder au canal de communication.

La couche réseau: La couche réseau s'occupe de l'acheminement des données (trouver une route et une transmissionfiable des données) captées, des nœuds capteurs vers la station de base en optimisant l'utilisation de l'énergie des capteurs

La couche transport: Cette couche est chargée du transport des données sans ré-ordonnancement ou duplication, de leur découpage en paquets, du contrôle deflux et de la gestion des éventuelles erreurs de transmission.

La couche application: C'est le niveau le plus pro che de l'utilisateur, elle assure l'interface avec les applications. Selon les tâches de détection, différents types d'applications peuvent être implémentés et utilisés sur la couche application

Les niveaux (plans) intégrés dans la pile protocolaire dans les RCSFs, ils assurent les fonctions suivantes :
Le plan de gestion d'énergie: La vie du nœud montre une dépendance forte à l'égard de la vie de la batterie. Les fonctions intégrées à ce niveau consistent à gérer l'énergie consommée par les capteurs. Un capteur p eut par exemple éteindre son interface de réception radio dès qu'il reçoit un message d'un nœud voisin afin d'éviter la réception des messages dupliqués

Le plan de gestion de mobilité: Selon le type d'application, les nœuds capteurs peuvent être mobiles. Ce plan est responsable d'enregistrer les mouvements d'un nœud et de connaître sa localisation.

Plan de gestion de tâches: Le niveau de gestion des tâches assure l'équilibrage et la distribution des tâches sur les différents nœuds du réseau affin d'assurer un travail coopératif et efficace en matière de consommation d'énergie, ce qui permet de prolonger la durée de vie du réseau

Tableau 3.2 Réseaux de capteurs vs réseaux Ad-hoc

Capteurs	Ad-hoc
1. Objectif ciblé	1. Générique / communication
2. Nœuds collaborent pour remplir un objectif	2. Chaque nœud a son propre Objectif
3. Flot de données « Many-to-one »	3. Flot « Any-to-any »
4. Très grand nombre de nœuds n'ayant pas tous une ID	4. Notion d'ID
5. Energie est un facteur déterminant	5. Débit est majeur
6. Utilisation du broadcast	6. Communication point à point

3.6 Conclusion

Chapitre 4

Les réseaux du futur/Extensions de WI-FI

4.1 Introduction

Le monde a rapidement été couvert par des réseaux qui permettent aux appareils numériques de s'interconnecter et de transmettre des données. Nous vivons actuellement une transformation numérique, à mesure que les réseaux numériques continuent de gagner du terrain dans le monde entier et que les bénéfices économiques de la numérisation se multiplient. La transformation numérique consiste à appliquer la technologie numérique pour créer les bases de l'innovation dans les entreprises et le secteur de l'industrie.

Les capteurs sont désormais omniprésents et collectent et transmettent d'énormes quantités de données. Ces données peuvent être stockées et analysées à une date ultérieure, ou être analysées et exploitées immédiatement. Les capteurs peuvent être installés dans les maisons, sur les feux de circulation, dans les champs agricoles et sur nos corps. Les données des capteurs sont analysées et utilisées par les gouvernements, les villes, les entreprises et les particuliers pour mettre en place des changements, comme surveiller l'environnement, prévoir les tendances démographiques, contrôler la gestion des déchets ou sécuriser une maison.

Les réseaux constituent la base de l'univers du numérique. Il existe de nombreux types de réseaux caractérisés par leur taille géographique (fig **), par le nombre d'appareils ou de réseaux qui s'y connectent et par le fait qu'ils prennent en charge ou non des terminaux mobiles. Les réseaux sont également caractérisés par leur fonction et leur but.

- Internet des Objets
- Réseau 6LowPAN
- WAN : Internet, le cloud, le fog computing
- Sans fil : Wi-Fi, Li-FI

En général, un capteur se connecte à un contrôleur via une connexion sans fil. Les contrôleurs collectent les données des capteurs, et envoient des données pour stockage et analyse. Ils peuvent être à même de prendre des décisions immédiates ou de travailler en collaboration avec un appareil appelé actionneur. Les actionneurs reçoivent une entrée électrique et la transforment en action physique.

Les actionneurs connectent désormais des milliards de capteurs et peuvent modifier les environnements physiques sans intervention humaine. Les réseaux du futur tourneront autour de l'IA (intelligence artificielle) et de l'IBN (réseaux basés sur l'intention). S'ils sont correctement programmés, les appareils intelligents sont capables d'évaluer les données qui leur sont fournies, et de modifier des processus ou des paramètres. Si on leur fournit suffisamment de données, ils peuvent « apprendre » et modifier leur propre code sur la base de ces nouveaux paramètres.

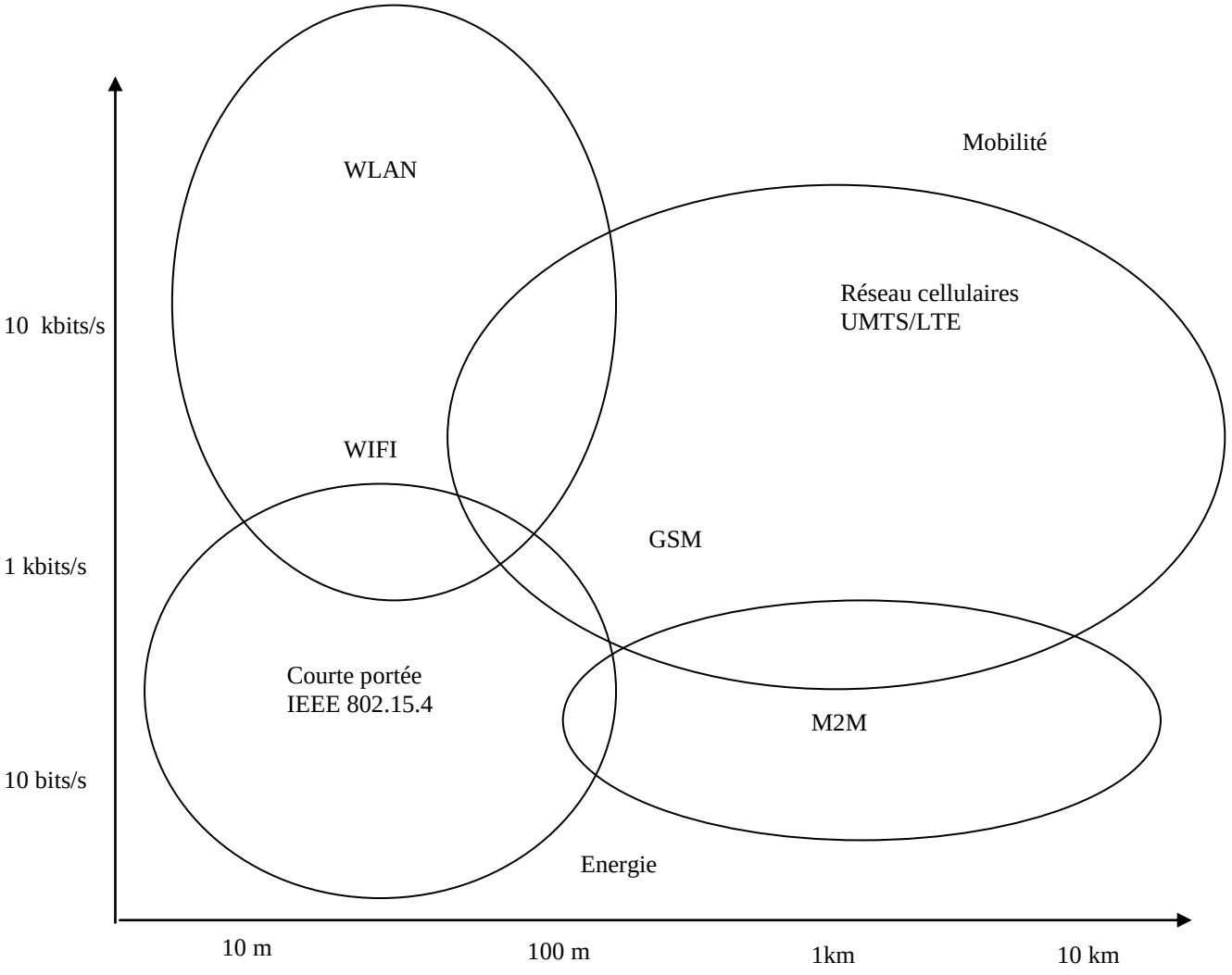


Figure 4.1. Les différents types de réseaux sans fils

4.2 Internet des Objets

L'Internet des objets (IoT) désigne l'interconnexion de millions d'appareils et de capteurs intelligents connectés à Internet. Ces capteurs et ces appareils connectés collectent et partagent des données qui seront utilisées et analysées par plusieurs organismes, dont des entreprises, des villes, des gouvernements, des hôpitaux et des particuliers. L'avènement de l'IoT a été possible, en partie, grâce à l'apparition des processeurs bon marché et des réseaux sans fil. Des objets jusqu'à présent inanimés (comme des poignées de porte ou des ampoules électriques) peuvent désormais être équipés d'un capteur intelligent qui collecte des données ou les transfère à un réseau.

Les chercheurs estiment que 3 millions de nouveaux terminaux se connectent à Internet chaque mois. Dans les quatre prochaines années, ce chiffre devrait atteindre les 30 milliards d'appareils connectés dans le monde entier.

Environ un tiers des appareils connectés seront des télévisions intelligentes, des smartphones, des tablettes et des ordinateurs. Les deux tiers restants correspondront à des « objets » : des capteurs, des actionneurs et des appareils intelligents innovants qui surveillent, gèrent, analysent et optimisent notre monde.

Voici quelques exemples de capteurs connectés intelligents : les sonnettes intelligentes, les portes de garage, les thermostats, les vêtements de sport, les pacemakers, les feux de circulation, les places de stationnement et bien d'autres. Votre imagination est la seule limite quant aux objets qui peuvent devenir des capteurs intelligents.

Les bâtiments intelligents

Les usines intelligentes

Les voitures intelligentes

L’autopilotage aérien

Le diagnostic médical et la chirurgie

Réseaux électriques intelligents

4.2.1 Définitions

Dans cette section, nous définissons les termes capteur, actionneur et objet connecté, Des termes qui sont relatifs à l'internet des objets.

- ***Capteur:*** Les capteurs sont des dispositifs électroniques composés de cellules sensorielles capables de mesurer des paramètres physiques de l'environnement tels que la luminosité, la température, les sons, les mouvements ou tout autre paramètre de l'environnement. En général, les capteurs sont associés à des passerelles pour transmettre les données capturées à la plate-forme de traitement et de stockage.

- ***Actionneur*** *:* un actionneur est un dispositif électronique et/ou mécanique qui produit des actions pour modifier l'état ou le comportement d'un système.

- ***Objet connectés*** *:* ou «objet intelligent» est tout objet ou produit qui, par le biais de technologies intégrées, est capable d'être identifié, de collecter des données sur l'état physique de son environnement, de prendre des décisions et de produire des actions (mécaniques ou par messages de contrôle), et de se connecter à un réseau (ex. Internet) pour échanger des données.

4.2.2 Architecture générales pour l'Internet des objets.

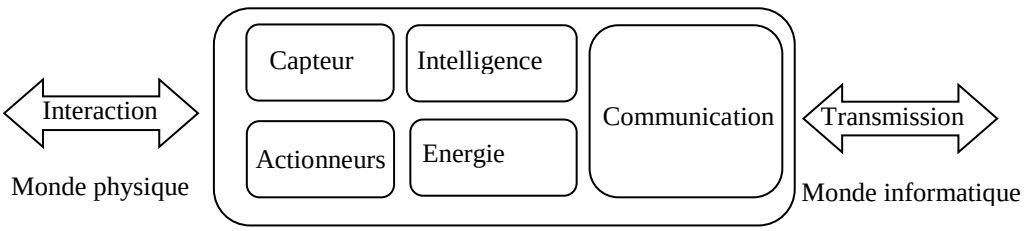


Figure 4.2 Composantes IoT

- ***Capteur :*** Traduction d'une grandeur physique en un signal électrique
- ***Actionneur*** : Modification d e l'état de l'environnement

- ***Intelligence*** : traitement des données
- ***Energie :*** Alimentation de la plateforme en énergie électrique. Doit être adaptée à l'application.
- ***Communication :*** Codage et transmission des données, protocoles standards ou dédiés, communication filaire ou sans fil.

4.2.3 Pile protocolaire IoT

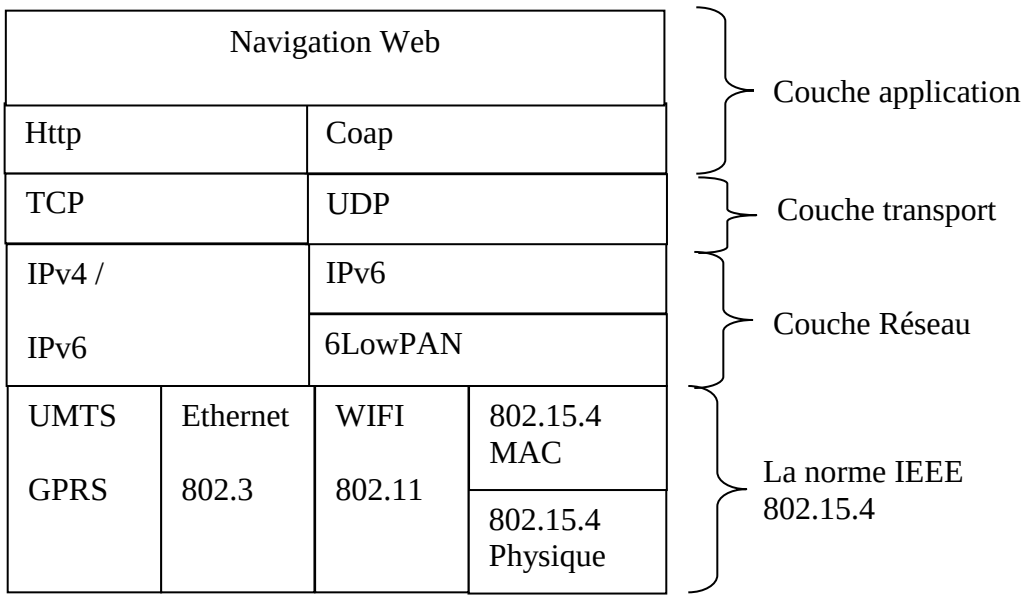


Figure 4.3. Pile protocolaire IoT

4.3 IPv6 Low power Wireless Personal Area Networks

IPv6 Low power Wireless Personal Area Networks (6LOWPAN) est une nouvelle couche protocole au niveau 2.5. Cette couche a été introduite dans les réseaux IEEE 802.15.4 afin d'adapter la taille des segments IPv6 (environ 1280 octets) à la taille maximale d'octet que peuvent supporter la trame IEEE 802.15.4 (128 octets).
Donc la couche 6LoWPAN a été ajouté comme une nouvelle couche entre la couche MAC et la couche IP permettant la fragmentation et aussi la compression des entêtes IP et UDP (TCP est en cours).

6LoWPAN est l'abréviation d'IPv6 Low Power Wireless Personel Area Network. Et pourquoi IPv6? La réponse est simple : Ce nouveau réseau à faible consommation d'énergie pourra utiliser dans les réseaux de capteurs donc la taille du champ adresse IPv4 ne permet d'avoir un réseau de grande taille et aussi on aura un grand problème d'adressage. C'est pour cette raison le groupe 6LoWPAN de IETF a opté pour l'utilisation de IPV6.

Le protocole 6LoWPAN assure une compatibilité IPv6 au dessus d'IEEE 802.15.4
Difficultés : taille importante des en-têtes IPv6, MTU IPv6 de 1280 octets, contraintes liées à 802.15.4 donc besoin de fragmentation et du réassemblage, compression, simplification du plan de contrôle (NDP)

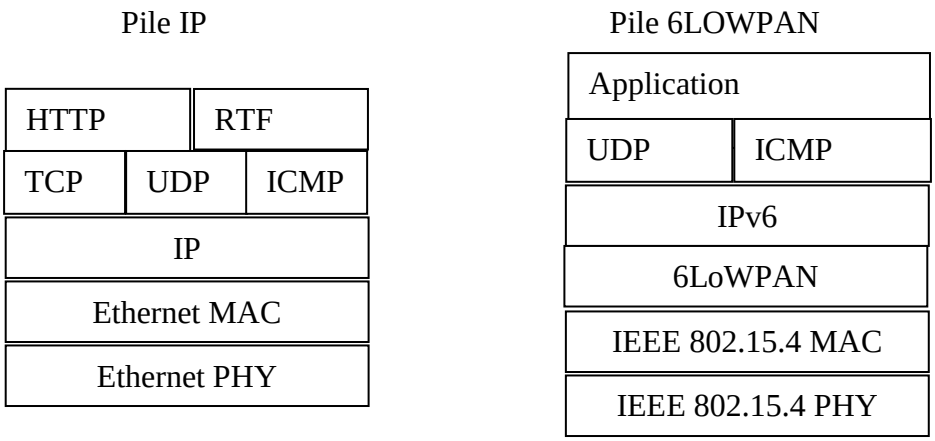


Figure 4.4. Comparaison de la pile IP et la pile 6LOWPAN

4.3.1 Architecture 6LOWPAN

Un réseau 6LoWPAN est formé par des équipements compatibles avec la norme IEEE 802.15.4. On distingue trois acteurs dans le réseau 6LoWPAN :

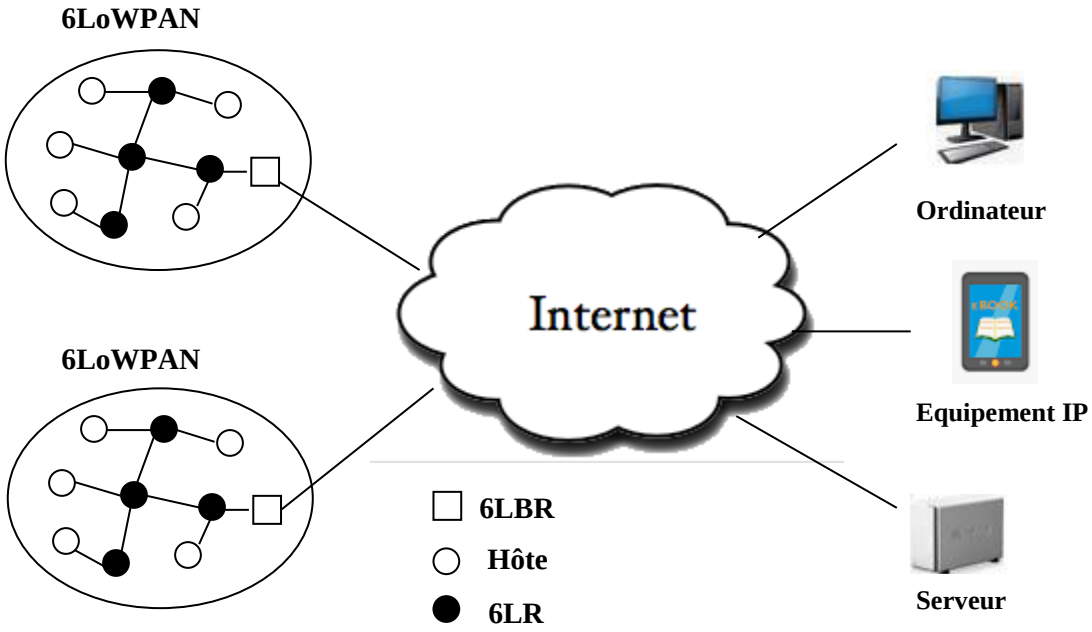


Figure 4.5 : Architecture 6LOWPAN

4.3.2 Adaptation de 6LOWPAN pour IPV6

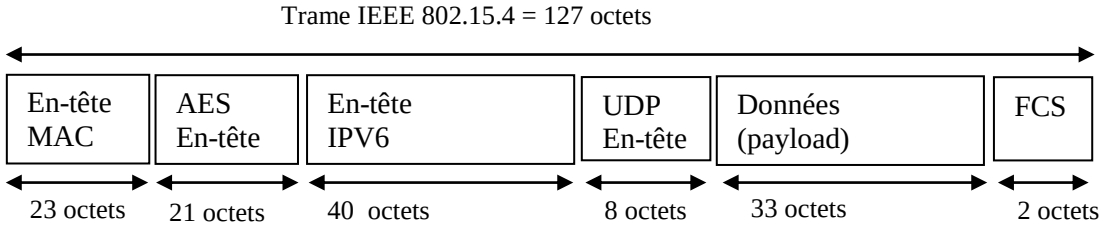
L'adaptation 6LOWPAN est une sous couche de la norme 802.15.4 introduite pour adapter la taille des segments IPV6 qui permet de faire :

- La fragmentation /Réassemblage
- La compression des entêtes IPv6-UDP-ICMPv6

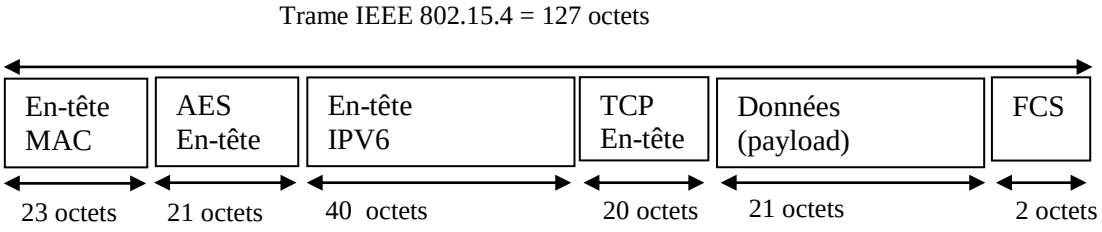
On a:

- Pour IPV6 la taille minimale des paquets est de =1280 Octets
- La taille de l'en-tête IPV6 =40 Octets min
- La norme 802.15.4 a pour MTU (Maximum transmission unit)= 127 Octets

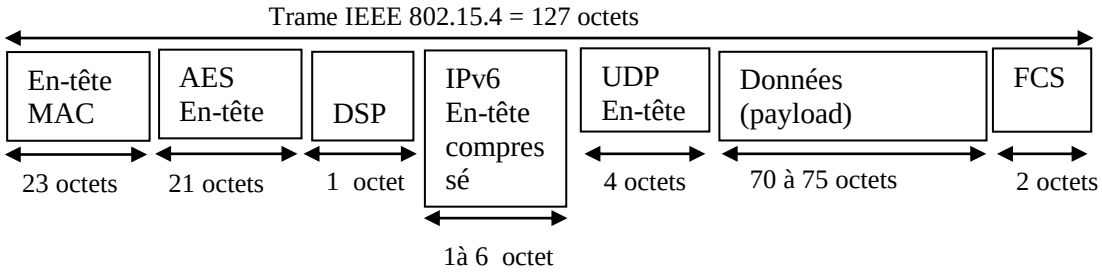
Un datagramme 802.15.4 avec le protocole UDP, non compressé :



Un datagramme 802.15.4 avec le protocole TCP, non compressé :



Un datagramme 802.15.4 avec le protocole UDP, compressé et non fragmenté:

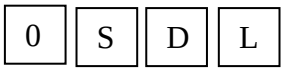


Pour Le champ DSP (Dispatch) sur 1 octet on trouve les différents types d'état concernant l'entête ipv6 (tableau 4.1)

Tableau 4.1 : Types d'états du champ dispatch

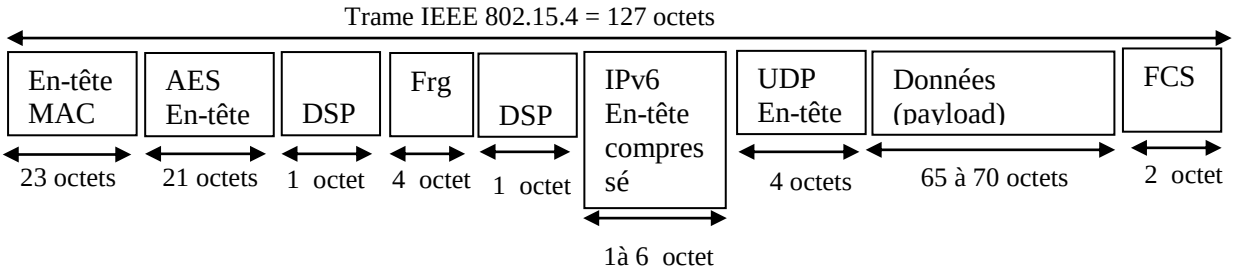
00 xxx xxx	NALP (Not a Low Pan Packet)
01 000 0001	Ipv6 non compressées
01 000 010	Ipv6 compressée HC1
01 010 000	Broadcast
01 111 111	Esc additional dispatch byte follows
10 xxx xxx	Mesh Header
11 000 xxx	Frag1
11 100 xxx	Frag n

Pour le champ UDP compressé est sur 4 octet :

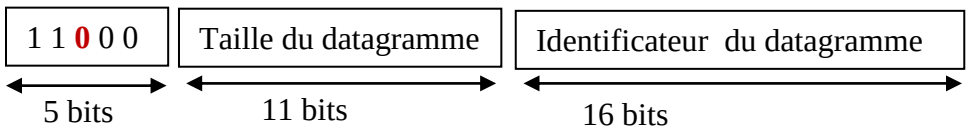


Le 1er octet =00000000
Le 2éme octet « S » :UDP port source
Le 3éme octet « D »: UDP port destination
« L » : UDP lenght ommitted

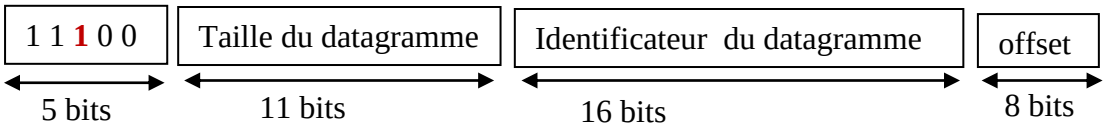
Un datagramme 802.15.4 avec le protocole UDP, compressé et fragmenté (premier fragment):



Le champ Frg pour le premier fragment du datagramme sur 4 octets = 32 bits détaillé comme suit :



Le champ Frg pour un fragment n du datagramme sur 5 octets détaillé comme suit :



4.3.3 La découverte des voisins (Neighbor Discovery : ND) avec 6LOWPAN

La découverte des voisins – Neighbor discovery (ND) est un protocole basé sur le protocole ICMPv6 il est utilisé pour déterminer l'adresse MAC des voisins attachés au lien et de découvrir d'autre nœuds sur le même lien, découvrir les routeurs, et détecter les adresses dupliquées.
Le ND utilise cinq messages différents :

- **Router Advertisement (RA):** utilisés par les routeurs pour signaler leur présence sur le lien ainsi que le préfixe et le MTU du lien.
- **Router dolicitations (RS) :** utilisés par les hôtes pour demander aux routeurs de signaler leurs présences par un message RA
- **Neighbor Solicitations (NS) :** utilisés pour les hôtes pour vérifier si une adresse existe, si elle est encore accessible et pour trouver l'adresse MAC d'un hôte voisin
- **Neighbor Advertisements (NA) :** utilisés pour répondre au message NS (remplace l'ARP)

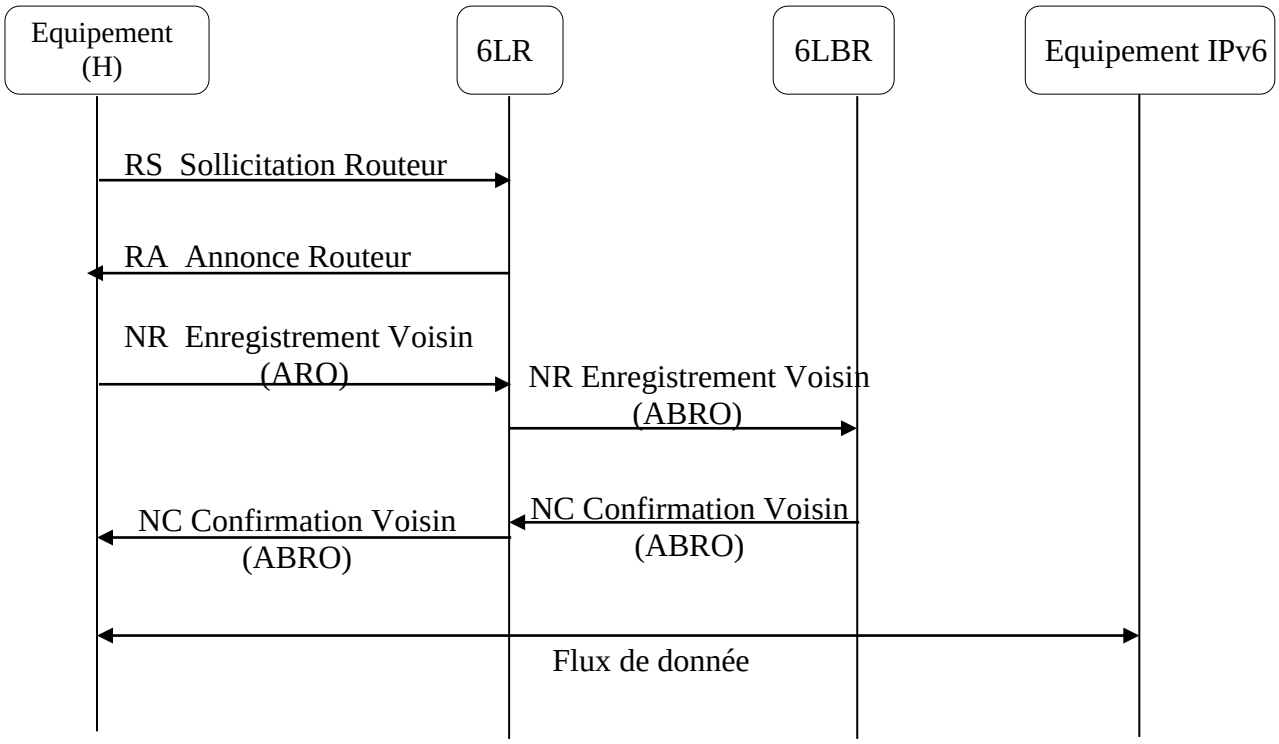


Figure 4.6 Neighbor 6LowPAN

4.4 Light Fidelity (LIFI)

Le LiFi (Light Fidelity) est une nouvelle technique de transmission de données sans fil qui utilise le spectre de la lumière visible, c'est-à-dire des ondes comprises entre 390 nm (bleu) et 780nm (rouge). Alors que le Wi-Fi utilise la partie radio du spectre électromagnétique (fréquence de 2.4 et 5 GHz), le LiFi utilise lui le spectre optique (fréquence entre 385 et 790 THz).

Existant depuis plusieurs années mais uniquement en version unidirectionnelle bas débit (VLC Visible Light Communication), cette lumière intelligente et connectée prend une nouvelle dimension via des luminaires LIFI nouvelle génération, bidirectionnel et haut-débit permettant un accès à internet par la lumière.

4.4.1 La norme IEEE 802.15.7

Le LiFi est défini par le standard IEEE 802.15.7, produit en 2010, il couvre les couche 1, physique (PHY) et 2, liaison de donnée (couche d'accès MAC), du modèle OSI. La couche MAC supporte actuellement trois topologies d'accès : Le peer-to-peer, la configuration en étoile et le mode de diffusion. La couche physique est divisé en trois types : PHY I, II et III, et ceux ci emploient une combinaison de différents schémas de modulation.

4.4.2 Topologies LIFI

La topologie en étoile implique l'existence d'un noeud central, appelé "coordinateur", qui est dédié au contrôle de la communication. Dans ce cas, un réseau indépendant sera créé, avec un identifiant de réseau personnel VLC unique.

Dans la topologie peer-to-peer, chaque appareil sera en mesure de communiquer directement avec tous les appareils dans son voisinage. Dans ce cas, un des deux nœuds impliqués agira comme coordonnateur, généralement le nœud qui initie la communication.

La topologie de diffusion implique la transmission de données, d'un nœud à un autre ou à plusieurs nœuds sans former un réseau. Ce type de communication est unidirectionnel et aucune adresse de destination n'est nécessaire.

4.4.3 Architecture d'un réseau LIFI

La conception Li-Fi est composée d'un grand nombre d'éclairages à LED utilisé pour la transmission optique en appliquant une tension constante et un courant constant. Les composants fondamentaux d'un tel système sont : Plusieurs éclairages à LED pour la transmission de données.
Un capteur de lumière pour la réception de données. Cela peut se faire par un

photodétecteur ou soit par une caméra, par exemple la caméra d'un téléphone mobile. Dans ce dernier cas, on parle de « Optical Camera Communication » (OCC). Comme illustré à la figure 4.4 , les terminaux peuvent se connecter à Internet via une

lampe à LED. Le driver (pilote à lampe) permet de contrôler la luminosité des LEDs selon l'environnement et les données reçues

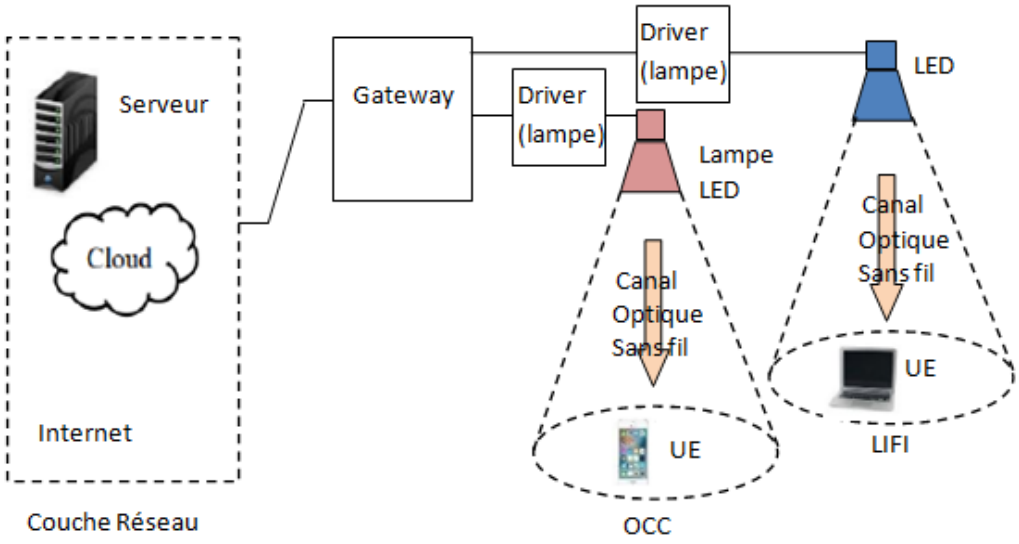


Figure 4.7 Architecture d'un système LIFI

4.4.4 Le LiFi VS WiFI

Le Li-Fi est un terme utilisé pour décrire la technologie de communication à lumière visible appliquée à la communication sans fil à haute vitesse. Il a acquis ce nom en raison de la similitude avec le Wi-Fi, en utilisant uniquement la lumière au lieu de la radio. Le Wi-Fi est idéal pour la couverture sans fil générale dans les bâtiments, tandis que la technologie Li-Fi est idéale pour la couverture de données sans fil haute densité dans des zones confinées et pour réduire les problèmes d'interférence radio. Les deux technologies peuvent donc être considérées comme complémentaires. Les fonctionnalités Li-Fi incluent des avantages en termes de capacité, d'efficacité énergétique, de sécurité et de sûreté d'un système sans fil. Elles présentent un certain nombre d'avantages essentiels par rapport au Wi-Fi, mais constituent par nature une technologie complémentaire.

Tableau 4.2 présente une comparaison rapide des différentes technologies de communication sans fil. Le LiFi et le WiFi offrent potentiellement les débits de données les plus élevés, tandis que le cellulaire offre les plus longues distances

	Cellulaire	WIFI	LIFI	Bluetooth	Zigbee	6LowPAN
Standard	GSM/GPRS/EDGE (2G), UMTS(3G), LTE(4G),5G	802.11a/b/g/n/ac	802.15.7	802.15.1	802.15.4	RFC6282
Fréquence	900,1800,1900 et 2100 MHZ 2.3, 2.6, 5.25, 26.4 et 58.68	2.4 GHZ et 5GHZ	400-800 THZ	2.4 GHZ	2.4 GHZ	2.4 GHZ et ~ 1GHZ
Portée	< 200 Km	~ 50m	< 10 m	50-150 m	10-100 m	< 20m
Débit	< 500 kps (2G) <2 Mps (3G) <10 Mps (4G) < 100 Mps (5G)	< 1Gbps	<224 Gbps	1Mbs	250kbps	20 - 250kbps

Chapitre 5

Les Nouveaux Paradigmes Réseaux

5.1 La technologie Software definde network (SDN)

Le concept de réseau défini par logiciel, largement connu sous le nom de Software Defined Networking (SDN), est un nouveau paradigme émerge d'architecture réseau conçue pour permettre une fonctionnalité réseau virtualisée qui peut être gérée, configurée et modifiée de manière centralisée par logiciel. basée sur :

- une séparation physique entre le plan de contrôle (i.e., les fonctionnalités qui assurent la gestion du réseau) et le plan de données (i.e., les fonctionnalités qui assurent le transfert des données)
- Un contrôle et une intelligence logiquement centralisés dans un ou plusieurs contrôleurs logiciels. Dans SDN, les contrôleurs détiennent une vue globale sur tout l'état de réseau et gèrent les autres équipements de plan de données de réseau. Ces derniers deviennent de simple transmetteur/récepteur des données avec une intelligence minimale. SDN promet d'apporter la flexibilité, l'évolutivité et la programmabilité aux architectures des réseaux de véhicules de nos jours. Ils facilitent également la gestion de réseau et introduisent de nouveaux services.

5.1.1 Définition du SDN

La définition académique, qui a depuis largement évolué, consistait à voir le SDN comme une architecture qui découplait les fonctions de contrôle et de transfert des données du réseau (data plane) afin d'avoir une infrastructure physique complètement exempte de tout service réseau. Il est possible de lire sur le site de l'open networking foundation la définition suivante
« Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services ».
Dans ce modèle, les équipements réseau se contentent d'implémenter des règles, injectées par les applications, de traitement des flux de données. Plus besoin d'avoir sur ces équipements de protocoles de routage, spanning-tree, etc. : une entité intelligente, appelée « contrôleur » voit le réseau dans sa globalité et injecte directement les règles de traitement des données sur chaque équipement.

5.1.2 Architecture SDN

SDN est basé sur une architecture hiérarchique de trois couches, voir la figure 5.1. :

1) Couche du plan de données : le plan de données représente tous les équipements du réseau, souvent appelés, les équipements de diffusion, tels que des commutateurs, des routeurs, des équipements virtuels etc. L'objectif d'un plan de données est de transmettre le trafic réseau sur une base d'un certain ensemble de règles de transmission ordonnée par le plan de contrôle.

La communication entre le plan de données et le plan de contrôle est assurée par des interfaces Sud qu'on appelle API Southbond.

2) Couche d'applications : elle regroupe tous les services et les applications des systèmes installés sur le contrôleur SDN.
3) Couche plan de contrôle : Le plan de contrôle est responsable de la prise de décision du trafic à travers le réseau, dépendamment des critères suivants: en fonction des exigences de l'application, selon les utilisateurs, et des politiques de communication du réseau résultant du plan de données. Le composant central d'un plan de contrôle est le contrôleur SDN. Un contrôleur SDN traduit les exigences des applications et les objectifs commerciaux tels que la nécessité de hiérarchiser le trafic (qualité de service), le contrôle d'accès (privilège), la gestion de la bande passante, ou autre. Ensuite, ces informations sont communiquées aux composants du plan de données.

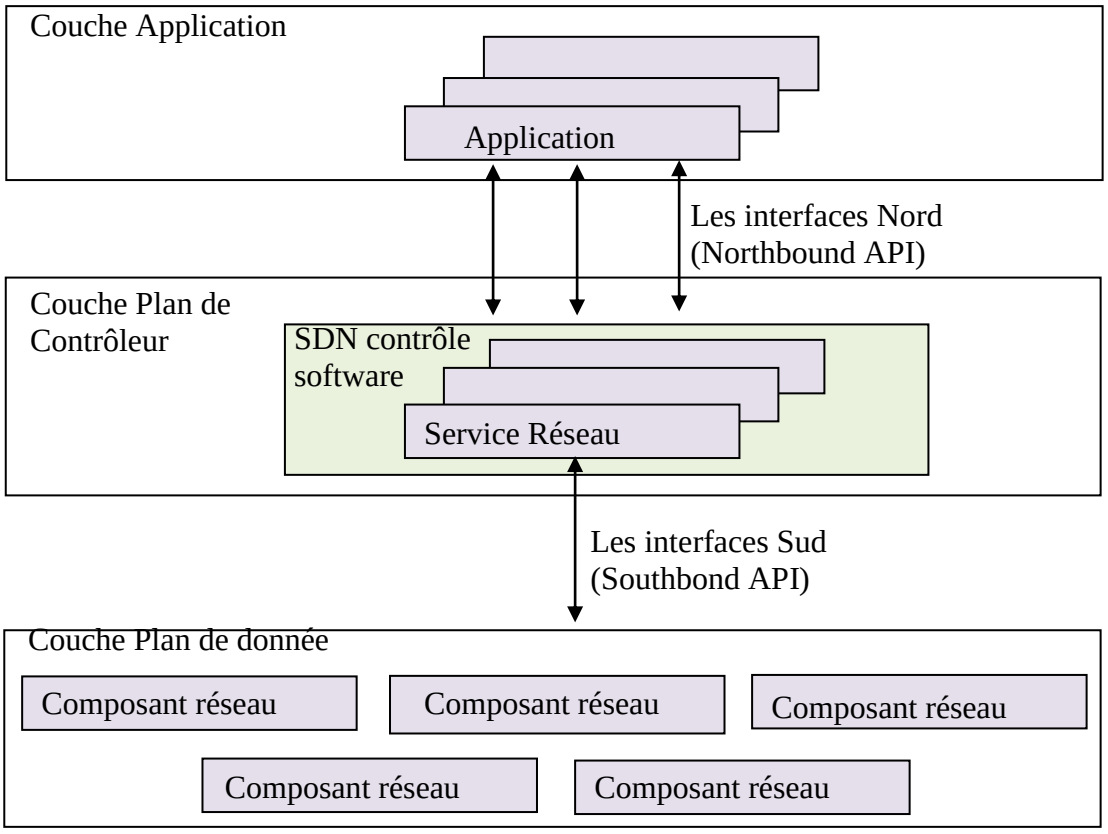


Figure 5.1. : Architecture SDN

5.1.3 Les interfaces SDN

Les flèches entre les couches représentent des interfaces. Une couche peut disposer de flèches allant vers une couche plus basse, on parlera alors d'interface de service

Sud. Elle peut disposer de flèches entrantes venant d'une couche supérieure, on parlera alors d'interface de service Nord.

Il existe des cas où des couches de même niveau discutent entre elles, c'est le cas notamment des plans de contrôle totalement ou partiellement distribués. On parlera alors d'interface de service Est/Ouest.

La figure 5.1 présente un exemple où un réseau est géré par deux plans de contrôle. Chaque plan de contrôle gère une partie des ressources réseaux. Une interface peut être nécessaire entre les deux plans de contrôle (besoin d'échange d'informations). C'est une interface de service Est/Ouest.

- **Les interfaces Sud (Southbond API)**

Les interfaces Sud constituent un protocole entre le contrôleur SDN et le plan de données. Elles contrôlent les opérations de transfert, les notifications d'événements, les rapports statistiques et annoncent également les capacités du réseau. Essentiellement, elles permettent à un contrôleur de définir le comportement du matériel dans le réseau.

- **Les interfaces Nord (Northbound API)**

Les interfaces nord permettent la communication et l'échange des données entre le contrôleur SDN sur le plan de contrôle et les applications du réseau. Le type d'informations échangées ainsi que leurs formes et fréquences dépendent de chaque application du réseau. Il n'y a pas de standardisation pour cette interface.

5.1.3 Différents modèles pour le SDN

Les modèles SDN sont classés selon la manière dont la couche contrôleur est connectée aux dispositifs SDN, le réseau SDN peut être divisé en quatre types différents:

- **SDN ouvert :** Le SDN ouvert possède un plan de contrôle centralisé et utilise OpenFlow pour l'API sud du trafic des commutateurs physiques ou virtuels vers le contrôleur SDN.

- **SDN Hybird :** Le modèle SDN hybride, également appelé SDN basé sur l'automatisation, mélange les fonctionnalités SDN et les équipements de réseau traditionnels. Il utilise des outils d'automatisation tels que des agents, Python, etc. et des composants prenant en charge différents types d'OS. Le modèle hybride SDN est souvent utilisé comme méthode de référence pour le SDN.

- **Overlay SDN**
  Modèle overlay SDN ne traite pas les réseaux physiques sous-jacents mais établit un réseau virtuel par-dessus le matériel actuel. Il fonctionne sur un

réseau superposé et offre des tunnels avec des canaux vers les centres de données pour résoudre les problèmes de connectivité des centres de données.

- **SDN API**
  Le SDN API, différent du SDN ouvert, qui nécessite un commutateur compatible OpenFlow, fonctionne bien avec les commutateurs traditionnels. Le SDN via les API existantes consiste à employer des fonctions pour les dispositifs de mise en réseau via une connexion à distance, en utilisant les méthodes traditionnelles telles que SNMP ou CLI, ou une méthode plus récente comme l'API REST. Bien que l'API SDN via l'API soit non propriétaire et ouverte, les API individuelles utilisées dans l'API SDN sont propriétaires de fournisseurs spécifiques. Et la transparence peut varier d'un fournisseur à l'autre.

5.2 La virtualisation des fonctions réseau (NFV)

5.2.1 Architecture de la virtualisation des fonctions réseau

L'architecture NFV proposée par l'Institut européen des normes de télécommunications (ETSI) aide à définir les normes pour la mise en œuvre de la virtualisation des fonctions réseau. Chaque composant de l'architecture repose sur ces normes afin d'offrir un niveau de stabilité et d'interopérabilité supérieur.

Une architecture NFV comprend les éléments suivants :

- Les fonctions réseau virtualisées (VNF) sont des applications logicielles qui fournissent des fonctions réseau, telles que le partage de fichiers, les services d'annuaire et la configuration d'IP
- L'infrastructure de virtualisation des fonctions réseau (NFVi) consiste en un ensemble de composants d'infrastructure (calcul, stockage, réseau) sur une plateforme, qui prend en charge des logiciels, par exemple un hyperviseur tel que KVM, ou une plateforme de gestion de conteneurs, nécessaire pour exécuter des applications réseau.
-
- Le composant de gestion, d'automatisation et d'orchestration réseau ou MANO (Management, Automation and Network Orchestration) fournit la structure permettant de gérer l'infrastructure NFV et le provisionnement de nouvelles fonctions réseau virtualisées.

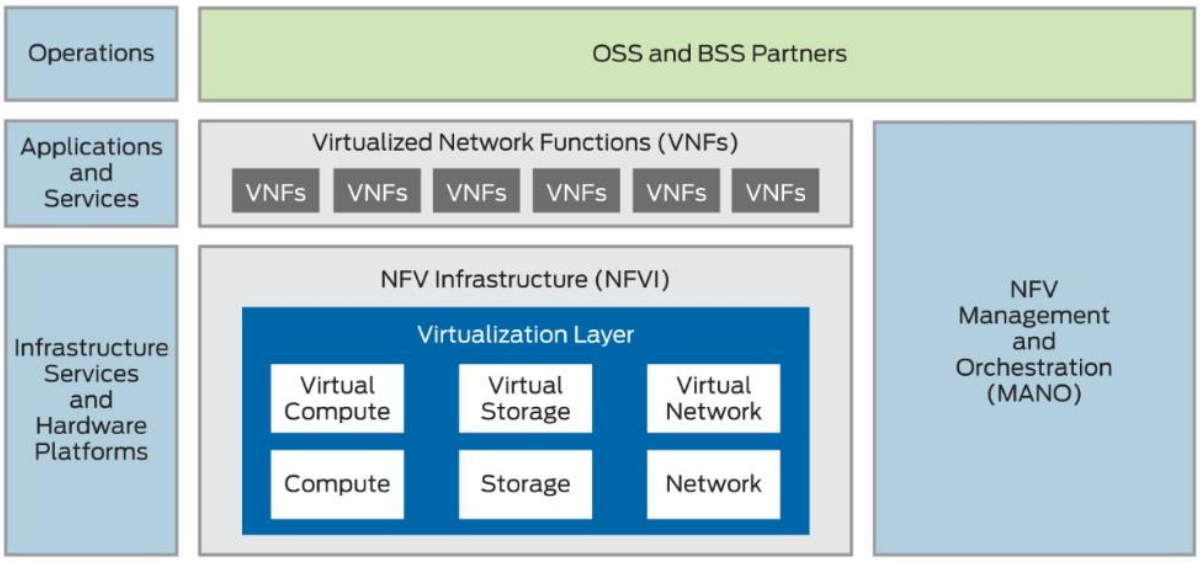


Figure 5.2. Architecture NFV

Les principaux composants de l'architecture sont les suivants :

- Le module d'infrastructure NFV (NFVI) : fournit la couche de virtualisation (hyperviseurs ou systèmes de gestion des conteneurs, comme Docker), ainsi que les composants physiques de calcul, de stockage et de mise en réseau hébergeant les VNF. Le module NFVI est géré via le gestionnaire d'infrastructure NFVI (VIM), qui contrôle l'allocation des ressources aux VNF. OpenStack est un exemple de gestionnaire VIM open source contrôlant les ressources physiques et virtuelles. La plate-forme Red Hat OpenStack est un exemple de VIM commercial.
- Les VNF : applications logicielles fournissant un ou plusieurs services réseau. Les VNF utilisent l'infrastructure virtualisée fournie par le module NFVI pour se connecter au réseau et fournir des services programmables et évolutifs. Les gestionnaires VNF prennent en charge le cycle de vie des instances VNF et la gestion du logiciel VNF.
- Le composant de gestion et d'orchestration (MANO) : fournit le processus de gestion et d'orchestration global des VNF au sein de l'architecture NFV. Le composant MANO exécute les services réseau via l'automatisation, le provisionnement et la coordination des flux de travail sur les gestionnaires VIM et VNF qui exécutent les fonctions VNF et superposent les chaînes de services de mise en réseau. Le composant MANO connecte l'architecture NFV aux systèmes OSS/BSS existants.

Référence :

1. Guy Pujolle : Cours réseaux et télécoms, Groupe Eyrolles, 2000, 2004, 2008, ISBN : 978-2-212-12414-9.
2. Jean-luc Montagnier : Réseau d'entreprise par la pratique, Edition Eyrolles,ISBN :2-212-112588-0.
3. Guy Pujolle : Les réseaux, Groupe Eyrolles, 2000, 2004, 2008, ISBN : 2-212-11437-0
4. Internet Protocol version 6 (IPv6): RFC 2460 https:// www.ietf.org/rfc/rfc2460.txt Yannick Bouguen, Eric Hardouin, François xavier Wolff : LTE et les réseaux 4G, Groupe Eyrolles, 2012, ISBN : 978-2-212-12990-8
5. Cisco, "L'Internet des objets (IoT)", 16 déc. 2015. http://www.cisco.com/web/FR/solutions/trends/iot/overview.html
6. http://mqtt.org/
7. Cristian Bude and Andreas Kervefors Bergstrand, "Internet of Things Exploring and Securing a Future Concept ", 15-06-2015.
8. 6LoWPAN Working Group. (2009, Mars 9). Neighbor Discovery for 6LoWPAN. Récupéré sur http://www.ietf.org/internet-drafts/draft-ietf-6lowpan-nd-02.txt