

Réseaux Avancés

- Support de cours -

Élaboré par

Dr. Alioua Ahmed

Maître de Conférences A

Département d'Informatique

Faculté des Sciences Exactes et Informatique

Université Mohammed Seddik Benyahia - Jijel

Juin 2022



Avant-propos

Ce support de cours est destiné principalement aux étudiants en première année préparant un diplôme du Master en informatique. Il concerne le module "Réseaux Avancés" de la spécialité réseaux et sécurité (RS). Le présent document peut être également utilisé par les étudiants en fin de cycle de la formation de master pour préparer la partie état de l'art de leurs projets de fin d'étude. Comme il peut être utile pour d'autres étudiants suivant des spécialités similaires qui tournent ou qui se rapprochent des réseaux informatiques, ainsi qu'à toute personne désireuse de s'initier ou élargir ces connaissances sur les différents types des réseaux informatiques sans fil et les nouvelles avancées dans ce domaine.

Cette matière vise à introduire l'étudiant aux divers concepts, caractéristiques et types des réseaux sans fil. Ce cours est aussi une opportunité pour l'étudiant d'apprendre les grandes tendances dans les nouvelles générations des réseaux informatiques.

Les étudiants désirant suivre ce cours doivent avoir un minimum de connaissances sur les réseaux informatiques traditionnelles. À la fin de ce cours, les étudiants sont censés apprendre les concepts de bases des différents types des réseaux sans fil, identifier les cas d'utilisation de chaque type et savoir et identifier les nouvelles tendances des réseaux informatiques modernes.

TABLE DES MATIÈRES

Table des Matières	i
Table des figures	iv
Liste des tableaux	vi
1 Introduction et généralités sur les réseaux informatiques.	1
1.1 Introduction	1
1.2 Définition	1
1.3 Apport des réseaux	2
1.4 Composants de base d'un réseau	2
1.4.1 Composants matériels	2
1.4.2 Composants logiciels	2
1.5 Classification des réseaux	3
1.6 Modèle OSI (Open System Interconnexion)	5
1.7 Modèle TCP / IP (Transmission Control Protocol / Internet Protocol)	7
1.8 Technique de l'encapsulation / décapsulation	8
1.9 Adressage de réseau	9
1.9.1 Adresse physique (l'adresse MAC (Medium Access Control))	9
1.9.2 Adressage logique (l'adresse IP (Internet Protocol))	10
1.9.2.1 Adresse IPv4	10
1.9.2.2 Adresse IP version 6 (IPv6)	12
1.9.3 Adressage des applications (les ports)	13
1.10 Conclusion	14
2 Notions fondamentales des réseaux sans fil.	15
2.1 Introduction	15
2.2 C'est quoi un réseau sans fil (Wireless Network)?	15
2.3 Apports et défis des réseaux sans fil	16
2.3.1 Points forts	16
2.3.2 Défis	16
2.4 Support de communication sans fil (Onde électromagnétique)	17

2.4.1	Définitions	17
2.4.2	Caractéristiques	17
2.4.3	Spectre électromagnétique	18
2.4.4	Cas d'utilisation	19
2.4.5	Phénomènes perturbateurs des ondes électromagnétiques	19
2.4.6	Technique de modulation / démodulation	20
2.4.7	Technique d'accès au support de communication sans fil	21
2.5	Classification des réseaux sans fils	22
2.6	Conclusion	24
3	Réseaux sans fil avec infrastructure fixe (Réseaux mobiles cellulaires).	25
3.1	Introduction	25
3.2	Définition	25
3.3	Architecture Générale	26
3.4	Concept de base	27
3.4.1	Division cellulaire	27
3.4.2	Réutilisation des fréquences	28
3.4.3	Gestion de la mobilité	29
3.4.3.1	Transfert intercellulaire (ou handover)	29
3.4.3.2	Itinérance (ou Roaming)	29
3.5	Évolution et génération des réseaux mobiles cellulaires	30
3.6	Conclusion	32
4	Réseaux sans fil sans infrastructure (Réseaux Mobiles Ad-Hoc).	33
4.1	Introduction	33
4.2	Réseaux sans fil mobiles ad-hoc (Mobile Ad-hoc NETworks, MANETs)	33
4.2.1	Définition	33
4.2.2	Caractéristiques	34
4.2.3	Domaines d'application	35
4.2.4	Principaux défis	36
4.2.5	Classification des protocoles de routage	36
4.3	Réseaux sans fil de capteurs (Wireless Sensor Networks, WSNs)	37
4.3.1	Pourquoi et comment ?	37
4.3.2	Définition	38
4.3.3	Architecture	38
4.3.4	Architecture d'un nœud capteur	39
4.3.5	Caractéristiques	40
4.3.6	Modèle de communication en couches	40
4.3.7	Topologie	41
4.3.8	Méthodes de collecte d'informations	41
4.3.9	Domaines d'applications	41
4.3.10	Protocoles de routage	42
4.3.11	Défis opérationnels	42
4.3.12	Comparaison entre WSNs et MANETs	43
4.4	Réseaux sans fil ad hoc de véhicules (Vehicular Ad hoc NETworks, VANETs) .	44
4.4.1	Pourquoi ?	44

4.4.2	Définition	44
4.4.3	Composants	45
4.4.4	Véhicule intelligent (Smart Vehicle)	45
4.4.5	Mode de communication	45
4.4.6	Environnement de déploiement	46
4.4.7	Applications	46
4.4.8	Caractéristiques et défis	47
4.4.9	Technologies de communication	47
4.5	Réseaux sans fil ad-hoc de drones (Flying Ad-hoc NETworks, FANETs)	48
4.5.1	Pourquoi et quoi ?	48
4.5.2	Anatomie d'un mini-drone	48
4.5.3	Classification des drones	49
4.5.4	Architecture typique	50
4.6	Architecture de communication	50
4.6.1	Caractéristiques	50
4.6.2	Principaux défis	51
4.6.3	Applications	52
4.6.4	Comparaison entre les réseaux de drones (FANETs) et les réseaux ad-hoc (MANETs)	52
4.7	Conclusion	53
5	Introduction à l'Internet des objets.	54
5.1	Introduction	54
5.2	Définition	54
5.3	Objet connecté	55
5.3.1	Définition	55
5.3.2	Type	56
5.3.3	Défis	56
5.3.4	Interaction	56
5.3.5	Architecture matérielle	57
5.4	Composants	57
5.5	Modèle de référence	58
5.6	Domaines d'applications	59
5.7	Caractéristiques	60
5.8	Défis	61
5.9	Cloud / Edge (Fog) Computing	61
5.9.1	Cloud Computing	61
5.9.2	Edge / Fog computing	61
5.10	Conclusion	63
6	Réseaux de nouvelles générations (Les réseaux définis par logiciel).	64
6.1	Introduction	64
6.2	Architecture de contrôle d'un équipement de réseau	64
6.3	Vers des réseaux définis par logiciel (Software-Defined Networking)	65
6.3.1	Définition	65
6.3.2	Architecture logique de SDN	65

6.3.3	Apports de SDN	67
6.3.4	Principaux défis	67
6.3.5	Domaines d'applications	68
6.4	Network Function Virtualization (NFV)	68
6.4.1	Pourquoi NFV ?	68
6.4.2	Définition	68
6.4.3	Architecture	69
6.4.4	Apports	69
6.5	Software-Defined WAN (SD-WAN)	70
6.5.1	Pourquoi SD-WAN ?	70
6.5.2	Définition	70
6.5.3	Apport	71
6.6	Conclusion	71
Bibliographie		vii

TABLE DES FIGURES

1.1	le modèle OSI vs. le modèle TCP/IP.	7
1.2	le principe de l'encapsulation et décapsulation [7].	9
1.3	la composition d'une adresse IPv4.	10
2.1	un exemple illustratif d'un réseau sans fil.	16
2.2	les caractéristiques d'une onde électromagnétique.	18
2.3	le spectre électromagnétique [6].	19
2.4	des exemples de phénomènes perturbateurs des ondes électromagnétiques. . . .	20
2.5	la technique de modulation / démodulation [9].	21
2.6	les techniques d'accès au canal de communication sans fil.	22
2.7	classification des réseaux mobiles sans fil selon l'infrastructure fixe.	24
3.1	l'architecture générale d'un réseau mobile cellulaire.	26
3.2	la hiérarchie des cellules dans un réseau cellulaire.	27
3.3	le concept de la réutilisation des fréquences.	29
3.4	le transfert intercellulaire dans les réseaux mobiles cellulaires.	29
3.5	une chronologie de l'évolution historique des réseaux cellulaires.	30
4.1	un exemple illustratif d'un réseau mobile ad-hoc (MANET) [15].	34
4.2	des exemples illustratifs des domaines d'application des réseaux ad-hoc. . . .	36
4.3	l'architecture générale d'un réseau de capteurs sans fil [21].	38
4.4	l'architecture générale d'un nœud de capteur. [23].	39
4.5	le modèle de communication en couche de WSNs [23].	40
4.6	les topologies d'un réseau de capteurs [21].	41
4.7	un exemple illustratif d'un réseau ad-hoc de véhicules.	44
4.8	les modes de communications dans les réseaux ad-hoc de véhicules [58]. . . .	46
4.9	l'anatomie d'un mini-drone [40].	49
4.10	un exemple de l'architecture typique d'un réseau de drones [39].	51
5.1	l'Internet des objets.	55
5.2	l'architecture matérielle d'un objet.	57
5.3	le modèle de référence de l'Internet des objets selon CISCO [46].	59
5.4	le concept de Cloud computing.	62

5.5	le concept d'Edge / Fog computing [48].	62
6.1	l'architecture traditionnelle d'un équipement de réseau [55].	65
6.2	l'architecture des réseaux traditionnels vs. software-defined networking [54]. . .	66
6.3	l'architecture logique de SDN [58].	66
6.4	l'architecture des réseaux traditionnels vs. l'architecture des réseaux NFVs [64].	69
6.5	l'architecture de SD-WAN [67].	71

LISTE DES TABLEAUX

1.1	un tableau comparatif entre les catégories des réseaux filaires selon l'étendue [1,12]	4
1.2	un résumé sur les principales caractéristiques des couches de modèles OSI [8]. .	6
1.3	un résumé des caractéristiques des couches de modèles TCP/IP.	8
1.4	les classes des adresses IPv4 [12].	11
1.5	l'organisation hiérarchique de l'adresse IPv6.	13
2.1	un aperçu taxonomique sur une classification des réseaux sans fil selon l'étendue ou la taille de réseau.	23
3.1	une récapitulation sur quelques caractéristiques des types de cellules.	28
3.2	un tableau récapitulatif et comparatif des générations des réseaux cellulaires [10].	31
4.1	un tableau comparatif entre les réseaux WSNs et les MANETs.	43
4.2	la classification des drones selon la rotation des ailes [34,38]	49
4.3	la classification des drones selon la méthode de contrôle.	50
4.4	une comparaison entre les réseaux FANETs et MANETs [32,36].	53

CHAPITRE 1

INTRODUCTION ET GÉNÉRALITÉS SUR LES RÉSEAUX INFORMATIQUES.

1.1 Introduction

Historiquement, les acteurs du digital, en cherchant à échanger des informations entre différents ordinateurs, ont rapidement compris l'intérêt qu'ils pouvaient tirer de relier ces machines entre eux. Les réseaux informatiques sont nés du besoin de faire communiquer différents ordinateurs distants les uns avec les autres pour transporter et échanger des données [12].

Dans un premier temps, les réseaux étaient réservés principalement aux entreprises. De nos jours, l'utilisation des réseaux a été démocratisée et généralisée pour toucher tous les utilisateurs des machines informatiques équipées d'une interface de communication. Aujourd'hui, les réseaux ne cessent de se développer en offrant une riche panoplie de services de plus en plus innovantes, telles que : l'échange des données, le partage de ressources, les jeux en réseau, etc.

1.2 Définition

Un réseau informatique est un système complexe de machines (les ordinateurs, les imprimantes, les smartphones, etc.) interconnectées via des supports de communications (les câbles à paires torsadées, la fibre optique, lignes téléphoniques, les ondes électromagnétiques, etc.). Un réseau permet la communication entre différentes machines afin de transporter des informations, échanger des fichiers, partager des ressources, etc.

Il y a deux grandes catégories des réseaux selon la nature de support de communication : les réseaux filaires et les réseaux sans fils. Un réseau filaire est composé d'un ensemble de machines reliées via des câbles tel que : le câble coaxial, le câble à paire torsadée, la fibre optique, etc. Un réseau sans fil relie les machines en utilisant des liens sans fil à l'instar des ondes électromagnétiques.

Exemple : le réseau téléphonique, les réseaux mobiles cellulaires, Internet, etc.

1.3 Apport des réseaux

Les réseaux informatiques ont été conçus pour offrir plusieurs services. Parmi ces services les plus importants, il y a les suivants :

- Le partage des ressources (que ce soit logicielles ou matérielles).
- La communication à distance entre les utilisateurs et/ou les applications.
- L'échange des informations et le transfert des données.
- La collaboration à distance.
- L'accès à distance aux ressources centralisées.
- La réduction des coûts et la tolérance aux pannes
- L'amélioration de la rapidité et de la productivité.
- Etc.

1.4 Composants de base d'un réseau

Un réseau informatique est principalement composé de plusieurs éléments que ce soit matériels ou logiciels.

1.4.1 Composants matériels

Les principaux composants matériels d'un réseau sont [1] :

- **Les terminaux et les nœuds** : les différents types des machines informatiques qui sont équipés d'une interface de communication.
Exemple : les ordinateurs, les serveurs, les tablettes, les imprimantes, etc.
- **Les medias ou les supports de communication** : les liens de communication qui sert à transporter les données et les informations.
Exemple : le câble à paire torsadée, la fibre optique, les supports hertziens, etc.
- **Les équipements d'interconnexion** : l'ensemble des équipements qui relient les différents composants de réseau (les nœuds et les terminaux) entre eux.
Exemple : le hub, le switch, le routeur, le modem, le firewall, etc.

1.4.2 Composants logiciels

Les principaux composants logiciels d'un réseau sont [12] :

- **Les protocoles de communication** : il s'agit de l'ensemble des logiciels qui permettent aux différentes machines de communiquer et échanger des données.
Exemple : TCP, IP, HTTP, FTP, etc.
- **Les applications de réseau** : il s'agit principalement du système d'exploitation, les applications des utilisateurs, etc.

1.5 Classification des réseaux

Les réseaux informatiques peuvent être classifiés selon différents critères dont les plus importants sont les suivants :

- **Le support de communication** : il existe deux catégories principales des réseaux selon le type de support de communication : (i) les réseaux filaires qui utilisent des câbles pour permettre la communication entre les machines et; (ii) les réseaux sans fils qui utilisent les ondes électromagnétiques.
Exemple : le réseau de téléphonie filaire, les réseaux sans fil mobiles cellulaires.
- **L'architecture d'organisation** : ce critère représente la méthode d'organisation des nœuds de réseau ainsi que les différents liens entre eux [12]. Il existe deux catégories principales : (i) l'architecture client / serveur, où une machine puissante (le serveur) fournit un ensemble de services à la demande à d'autres machines dites clients, (ii) et l'architecture point à point (Peer to Peer, P2P), dans ce type toutes les machines de réseau sont égales, c'est-à-dire, chaque machine est à la fois un client et un serveur.
- **Le type de la topologie** : la topologie représente la méthode dont les nœuds sont distribués et interconnectés. Il y a deux types de topologie : (i) la topologie physique, qui définit comment les nœuds sont physiquement distribués et interconnectés, et (ii) la topologie logique, qui définit comment l'information circule et transite dans le réseau.
Exemple : la topologie en bus, étoile, anneau, arbre et maillée.
- **L'ouverture** : il y a différents types de réseau selon l'ouverture aux utilisateurs tels que : Intranet (un réseau interne à un organisme), Internet (un réseau public), Extranet (un réseau interne d'un organisme avec en plus la possibilité d'accès à distance via un canal sécurisé).
- **L'envergure** : selon ce critère, les réseaux sont classifiés selon l'étendue ou la taille de réseau.
Exemple : les réseaux personnels, les réseaux locaux, les réseaux métropolitains, les réseaux étendus, etc.
- Etc.

Le tableau 1.1, présente un résumé sur une classification taxonomique des principales caractéristiques des catégories des réseaux filaires selon l'étendue :

Type	Etendue	Rôle	Support de transmission	Exemple	Technologie
Réseaux personnels (Personal Area Networks, PANs)	Une dizaine de mètres.	Pour relier des appareils personnels.	Le câble USB (Universal serial Bus).	Un réseau entre un ordinateur et un smartphone reliés via un câble USB.	-
Réseaux locaux (Local Area Networks, LANs)	Une centaine de mètres.	Pour relier des appareils au sein du siège d'une entreprise par exemple.	Le câble coaxial, la paire torsadée, etc.	Un réseau entre les différents équipements informatique au sein d'une entreprise.	Ethernet, Token Ring, etc.
Réseaux métropolitains (Metropolitan Area Networks, MANs)	Une dizaine de kilomètres.	Pour relier des réseaux locaux distants (à l'échelle d'une ville).	La paire torsadée, la fibre optique, etc.	Un réseau qui relie des bâtiments (des réseaux locaux) au sein d'une ville.	Metro-Ethernet, FDDI, etc.
Réseaux étendus (Wide Area Networks, WANs)	Une centaine de kilomètres.	Pour relier des réseaux métropolitains distants (à l'échelle d'un pays).	La fibre optique, etc.	Un réseau qui relie les agences d'une banque située dans plusieurs villes du même pays.	ATM, MPLS, etc.
Réseau mondiale (Global Area Network, GAN)	Plusieurs milliers de kilomètres.	Pour relier des réseaux étendus distants (à l'échelle continentale).	La fibre optique, le câble sous-marin, etc.	Un réseau qui relie les sièges d'une multinationale situés dans différents pays ou même dans différents continents.	Internet

TABLE 1.1 – un tableau comparatif entre les catégories des réseaux filaires selon l'étendue [1, 12]

Dans un réseau informatique, ils peuvent exister une variété de protocoles et logiciels, une hétérogénéité des technologies de communication et une diversité des équipements communicants de différents constructeurs, etc. Pour garantir l'interopérabilité et la compatibilité entre ces différents systèmes. Différents organismes de normalisation ou standardisation à l'instar d'ISO (International Organisation for standardisation) proposent de définir des spécifications, des exigences, des lignes directrices pour imposer certaines contraintes techniques de fabrication aux industriels. Parmi les modèles les plus connus, ISO a proposé un modèle pour permettre l'interopérabilité et la comptabilité entre les systèmes informatiques ouverts connu sous le nom d'OSI pour Open System Interconnexion, en anglais.

1.6 Modèle OSI (Open System Interconnexion)

Le modèle OSI est une norme de communication entre ordinateurs interconnectés. Il a été proposé en 1984 par ISO. OSI propose un modèle standard composé de sept couches d'abstraction afin de normaliser l'interconnexion des systèmes ouverts. Quatre couches dites basses (la couche physique, liaison, réseau et transport) qui sont orientées vers l'acheminement de l'information et trois couches dites hautes (la couche session, présentation et application) qui sont orientées vers le traitement de l'information [8, 12]. Le tableau 1.2 donne un résumé récapitulatif sur les principales caractéristiques des sept couches de modèle OSI.

Comme toute technologie, le modèle OSI présente des avantages et souffre de quelques inconvénients.

- **Avantages** : le modèle OSI est un modèle ouvert, ce qui permet,
 - Une réduction de la complexité des communications entre les systèmes hétérogènes.
 - Une homogénéité du matériel entre les différents constructeurs.
 - Une standardisation des interfaces de communication.
 - Des réseaux compatibles les uns avec les autres.
 - Etc.
- **Inconvénient** : le modèle OSI est basé sur sept couches, ce qui le rendre,
 - Un modèle complexe.

Couches		Unité de données	Rôle	Protocoles
Couches Basses → Orientées vers l'acheminement de l'information	Couche 1 - Physique	Bit	• Gestion de média et de signal. • Transmission des bits.	DSL, 802.11, RJ45, etc.
	Couche 2 - Liaison	Trame	• Adressage physique (MAC/LLC). • Détection et correction des erreurs.	Ethernet, MAC/LLC, Frame Relay, CSMA/CD, etc.
	Couche 3 - Réseau	Paquet	• Adressage logique (IP). • Routage.	IP, ARP, ICMP, IGMP, OSPF, etc.
	Couche 4 - Transport	Segment	• Connexion de bout en bout. • Contrôle de flux (TCP).	TCP, UDP, SSL, TLS, etc.
Couches Hautes → Orientées vers le traitement de l'information	Couche 5 - Session	Donnée	• Gestion des sessions entre les hôtes. • Synchronisation des échanges distants.	SIP, RPC, NetBios, AppleTalk, etc.
	Couche 6 - Présentation	Donnée	• Conversion, compression et chiffrement des données.	HTML, MP3, JPEG, etc.
	Couche 7 - Application	Donnée	• Point d'accès aux services de réseau.	DNS, HTTP, POP, FTP, etc.

TABLE 1.2 – un résumé sur les principales caractéristiques des couches de modèles OSI [8].

1.7 Modèle TCP / IP (Transmission Control Protocol / Internet Protocol)

Le modèle TCP / IP a été proposé par DARPA (Defense Advanced Research Projects Agency), une agence de recherche et de développement du ministère de la défense des États-Unis, chargée du développement de technologies émergentes destinées à être utilisées par l'armée. Ce modèle a été inspiré du modèle OSI, mais il est plus simple par ce qu'il se base sur quatre couches au lieu des sept couches de modèle OSI [12], voir la figure 1.1.

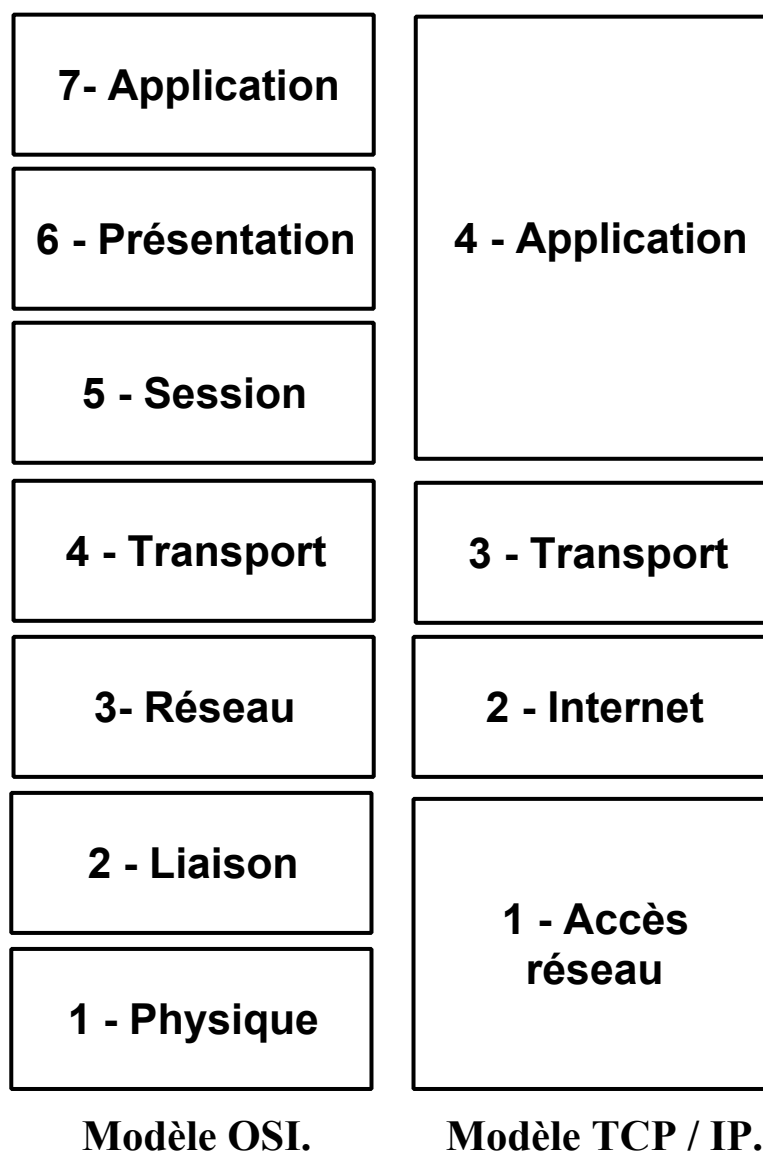


FIGURE 1.1 – le modèle OSI vs. le modèle TCP/IP.

Le tableau 1.3 résume les principales caractéristiques des couches de modèle TCP/IP.

Couche	Unité de donnée	Rôle	Protocoles
Couche 1 – Accès réseau	Trame	• Acheminement physique des données. • Conversion des signaux.	Ethernet, token ring, Frame Relay, FDDI, etc.
Couche 2 – Internet	Data-gramme	• Définition des data-grammes. • Gestion de l'adressage IP.	IP, ARP/RARP, ICMP, IGMP, OSPF, EIGRP etc.
Couche 3 - Transport	Segment	• Acheminement des données.	TCP, UDP.
Couche 4 – Application	Message	• Point d'accès aux applications réseau.	HTTP, DNS, DHCP, FTP, SMTP, POP, IMAP, etc.

TABLE 1.3 – un résumé des caractéristiques des couches de modèles TCP/IP.

Le modèle OSI et TCP/IP servent comme une guide pour indiquer à l'ordinateur ce qu'il est censé faire lorsque des données doivent être envoyées ou lorsqu'elles sont reçues. La technique de l'encapsulation / décapsulation décrit les transformations que les paquets des données subissent lorsqu'ils transitent à travers le modèle OSI ou TCP/IP.

1.8 Technique de l'encapsulation / décapsulation

La technique de l'encapsulation consiste à ajouter un bloc de données (un entête) à une unité de donnée d'un protocole (Protocol Data Unit (PDU)) à chaque passage par une couche d'abstraction. La décapsulation est l'opération inverse [1].

La technique de l'encapsulation est exécutée lors de l'envoi par l'émetteur. Tant dit que la décapsulation est exécutée lors de la réception par le récepteur. Les données passent de la couche la plus haute vers la couche la plus basse lors de l'encapsulation. Le contraire se passe lors de la décapsulation où les données passent de la couche la plus basse vers la couche la plus haute [1], voir la figure 1.2.

Selon le type de l'équipement de réseau et la couche sur laquelle il fonctionne, les données n'atteignent pas toujours la couche la plus supérieure de modèle. Par exemple pour le cas d'un routeur, la couche la plus haute c'est la couche réseau dans le modèle OSI et la couche Internet dans le modèle TCP/IP. Cela veut dire que uniquement de la couche de fonctionnement de l'équipement et les entêtes des couches inférieure à cette couche qui seront ajoutés lors de l'envoi.

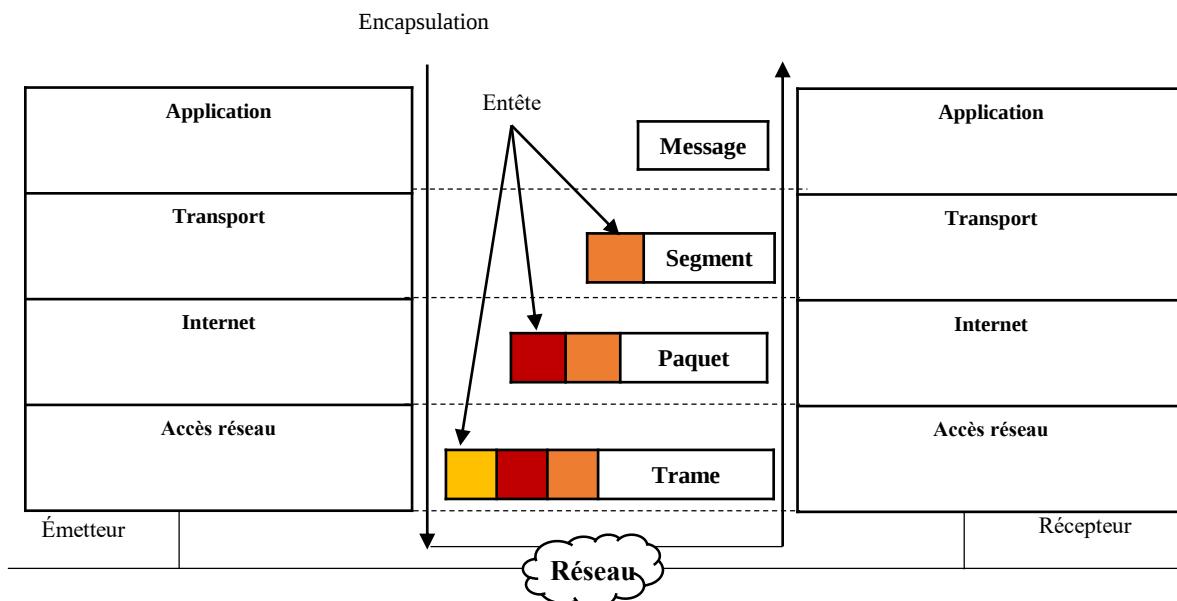


FIGURE 1.2 – le principe de l’encapsulation et décapsulation [7].

1.9 Adressage de réseau

La technique d’adressage consiste à affecter à chaque machine sur le réseau un identifiant dédié afin de pouvoir l’identifier de manière unique sans aucune ambiguïté. Il existe deux types d’adresses utilisées dans les réseaux informatiques : les adresses physiques et les adresses logiques.

1.9.1 Adresse physique (l’adresse MAC (Medium Access Control))

L’adresse MAC (Medium Access Control) représente l’adresse physique d’un équipement et elle se caractérise par les points suivants [2] :

- Elle est unique et elle est souvent gravée sur la carte réseau de l’équipement.
- Elle est codée en 48 bits (6 octets) notés en hexadécimal :
 - 24 premiers bits : ils identifient le constructeur de l’interface réseau et ils sont appelés OUI (Organizationally Unique Identifier).
 - 24 derniers bits : ils sont laissés à la discrétion du constructeur pour l’identifiant de la carte réseau.
- Elle a une représentation en Hexadécimale de six blocs séparés par des deux points (:).
Exemple : 5E :FF :56 :A2 :AF :15.
- L’adresse FF :FF :FF :FF :FF :FF représente l’adresse MAC de diffusion.

Remarque

- Les commandes *ipconfig /all* sous windows et *ifconfig* sous linux permettent d’afficher l’adresse MAC d’une machine.
- IEEE avec les constructeurs assure l’unicité de l’attribution des numéros des adresses MAC.

1.9.2 Adressage logique (l'adresse IP (Internet Protocol))

L'adresse IP (Internet Protocol) représente l'adresse logique d'un équipement. Elle se caractérise par les points suivants :

- Elle est utilisée pour identifier une machine sur Internet ou dans un réseau local.
- Elle est unique sur le réseau.
- Il existe deux versions : l'adresse IP version 4 (IPv4) sur 32 bits et l'adresse IP version 6 (IPv6) sur 128 bits.

Remarque : la commande *ipconfig* sous windows ou *ifconfig -a* sous linux permettent d'identifier l'adresse IP d'une carte réseau.

1.9.2.1 Adresse IPv4

Les principales caractéristiques des adresses IPv4 sont résumées dans les points suivants [8] :

- Taille : 32bits (4 octets).
- Composition : elle se compose de deux parties (voir la figure 1.3) :
 - Un identifiant de réseau (NET-ID) : il identifie un réseau de machines connectées.
 - Un identifiant d'hôte (HOST-ID) : il identifie une machine au sein du réseau.
- Notation : il y a deux notations possibles,
 - En binaires : l'adresse IPv4 peut être représentée sur 32 bits.
Exemple : 1001011 01100100 0000010 1000000001
 - En décimale : l'adresse IPv4 peut être aussi représentée par quatre nombres décimaux entiers (entre 0 et 255) séparés par des points (.).
Exemple : 192.168.1.12

Remarque : toutes les machines du même réseau physique doivent avoir le même identifiant de réseau.

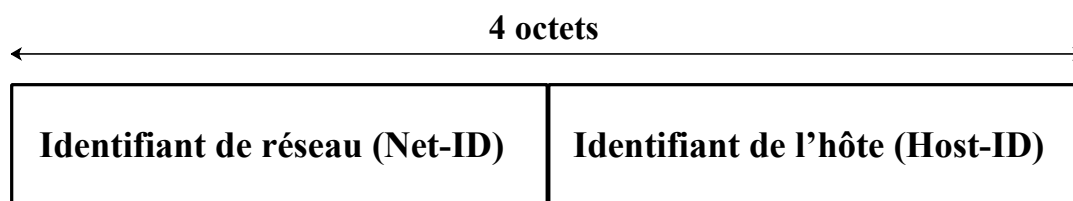


FIGURE 1.3 – la composition d'une adresse IPv4.

A) Classes d'adresses IPv4

Les classes des adresses IPv4 sont résumées dans le tableau 1.4 [12] :

Classe	Premiers bits	Sous-mask	Début	Fin	Nombre max de réseaux	Nombre max de machines
A	0	255.0.0.0	0.0.0.0	126.255.255.255	127 réseaux (8 bits)	Plus de 16 millions de machines (24 bits)
B	10	255.255.0.0	128.0.0.0	191.255.255.255	Plus de 16000 réseaux (16 bits)	Plus de 65000 machines (16 bits)
C	110	255.255.255.0	192.0.0.0	223.255.255.255	Plus de 2 millions de réseaux (24 bits)	254 machines (8 bits)
D	1110	255.255.255.240	224.0.0.0	239.255.255.255	-	-
E	11110	255.255.255.240	240.0.0.0	255.255.255.255	-	-

TABLE 1.4 – les classes des adresses IPv4 [12].

Remarques

- La classe D est réservée pour la diffusion de groupe.
- La classe E est réservée pour un usage futur.

Les adresses IPv4 peuvent être aussi classifiées en deux catégories :

- **Les adresses IPv4 privées** : elles représentent toutes les adresses IPv4 utilisées dans un réseau local (LAN). Ces adresses ne sont pas routables et elles ne peuvent pas être utilisées sur Internet. Elles sont visibles et uniques uniquement à l'intérieur des réseaux locaux. Les adresses IPv4 privées de chaque classe sont [8] :
 - **La classe A** : de 10.0.0.0 à 10.255.255.255
 - **La classe B** : de 172.16.0.0 à 172.31.255.255
 - **La classe C** : de 192.168.1.0 à 192.168.255.255
- **Les adresses IPv4 publiques** : elles représentent toutes les adresses IPv4 non privées qui sont routables et utilisables sur Internet. Une adresse IPv4 publique est unique dans le monde.

Pour permettre la correspondance entre les adresses IPv4 privées et publiques, il y a deux techniques :

- **La technique NAT (Network Address Translation)** : elle permet de faire correspondre une adresse IPv4 privée et une adresse IP publique [8].
- **La technique PAT (Port Address Translation)** : elle est une NAT qui fait correspondre plusieurs adresses IP privées à une adresse publique en utilisant différents ports [8].

B) Les adresses IPv4 particulières

Ils existent d'autres adresses IPv4 particulières qui sont résumés dans les points suivants [7] :

- **L'adresse 0.0.0.0** : elle représente tous les réseaux non connus (une adresse non valide).
- **L'adresse 127.0.0.1** : elle représente l'adresse de boucle locale (loopback) qui sert souvent à tester le bon fonctionnement de la carte réseau.
- **L'adresse 255.255.255.255** : elle représente l'adresse de diffusion (broadcast) qui sert à adresser toutes les machines de réseau.
- **Une adresse avec la partie réseau à x et la partie machine tout à 1** : elle représente une adresse de diffusion dirigée vers le réseau en cours.
Exemple : 192.168.32.255, une diffusion vers toutes les machines de réseau 192.168.32.0.
- **Une adresse avec la partie réseau tout égale à 0 et la partie machine tout à x** : elle représente l'adresse de la machine x sur le réseau en cours.
Exemple : 0.0.0.23 représente l'adresse de la machine 23 sur le réseau en cours.
- **Une adresse se terminant par 0 (x.x.x.0)** : elle représente l'identifiant d'un réseau.

Remarques

- La notation CIDR (Classless Inter-Domain Routing) : elle permet d'exprimer l'identifiant du réseau par un slash ("/") et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau.
Exemple : 186.15.0.0/16. L'adresse a un masque de 255.255.0.0 (11111111.11111111.00000000.00000000) ce qui peut être écrit en notation CIDR comme suit : /16 (c'est-à-dire 16 bits à 1).
- L'adresse de réseau : elle peut être obtenue en appliquant un *ET logique* entre l'adresse IP le masque de réseau [8].

1.9.2.2 Adresse IP version 6 (IPv6)

À cause de la grande augmentation de nombre des machines connectées, le nombre des adresses IPv4 arrivent à ses limites. Pour cela, une nouvelle version d'adresses IP a été proposée pour augmenter le nombre des adresses IPs [8]. Il s'agit de l'adresse IP version 6 (notée IPv6) codée sur 128 bits, dont les principales caractéristiques sont résumées dans les points suivants [8] :

- **Taille** : 128bits (8 octets).
- **Notation** : elle est représentée sur 8 groupes de 16 bits représentés par 4 chiffres en hexadécimal et séparés par (:).
Exemple : 5800 :10C3 :E3C3 :F1AA :48E3 :D923 :D494 :AAFF
- **Notation abrégée** : dans une adresse IPv6, les zéros à gauche de chaque groupe peuvent être omis. Aussi, un ou plusieurs groupes de zéros consécutifs peuvent être remplacés par " : ". Il faut bien noter que cette règle est à utiliser une seule fois [7].

Exemple : 2001 :0660 :7401 :0200 :0000 :0000 :0edf :bdd7
 → 2001 :660 :7401 :200 : :edf :bdd7

Remarque : l'adresse IPv6 est compatible avec l'adresse IPv4.

A) Adresses IPv6 particulières

Les adresses IPv6 particulières sont :

- **L'adresse IPv6 0000 :0000 :0000 :0000 :0000 :0000 :0000 :0001 ou : :1 :** elle représente l'adresse de boucle locale (LoopBack). Cette adresse est équivalente à l'adresse 127.0.0.1 en IPv4.
- **L'adresse IPv6 0 :0 :0 :0 :0 :0 :0 :0 ou : : :** elle représente l'adresse indéterminée ou le cas d'absence de l'adresse lors de l'initialisation d'un équipement.

Remarque : l'adresse IPv6 utilise une représentation à l'aide de la notation CIDR pour la représentation des masques de sous-réseaux.

Exemple : l'adresse fe80 : :20d :61ff :fe22 :3476 /64 a un masque de 64 bits.

B) Organisation d'une adresse IPv6

Comme il est illustré dans le tableau 1.5, une adresse IPv6 est hiérarchisée en trois niveaux :

- Le préfixe de réseau (48 bits).
- Le préfixe de sous-réseau (16 bits).
- L'identifiant de l'interface de la machine (64 bits).

Préfixe de réseau (Network prefix)		Identifiant de l'interface (Interface ID)
5800 :10C3 :E3C3	:F1AA	:48E3 :D923 :D494 :AAFF
Préfixe de réseau / Topologie publique	Préfixe de sous-réseau (subnet) / Topologie du site	
48 bits	16 bits	
64 bits		64 bits
Le préfixe de réseau définit l'@ de réseau et de sous-réseau.		L'ID de l'interface définit une machine donnée.

TABLE 1.5 – l'organisation hiérarchique de l'adresse IPv6.

1.9.3 Adressage des applications (les ports)

Un port de connexion (ou un port de service) c'est l'identifiant logiciel unique de l'application émettant ou recevant le message associé à une communication. Il est représenté par 16 bits. Une application sur une machine sur le réseau est adressée par le *Socket* qui représente un identifiant unique formé par le couple : l'adresse IP et le numéro de port.

Notation : *adresse_src :port_src / adresse_dst :port_dst*

Exemple : 212.195.198.187 :2256 / 78.109.84.60 :80

Remarque : la commande pour afficher le statut des sockets (ports ouverts) sous windows est :
netstat -an | netstat -a

1.10 Conclusion

De nos jours, les réseaux informatiques ne cessent plus de se développer en bénissant des énormes avancées technologiques dans divers domaines tels que : la micro-électronique, le traitement de signal, les technologies de communication, etc. Actuellement, les réseaux informatiques sont omniprésents et ils ont changé notre manière de communiquer en offrant des services de plus en plus innovants tels que : la communication à distance, le partage de ressources, les jeux en réseau, etc.

Plus récemment, les utilisateurs des réseaux informatiques sont souvent mobiles et ils exigent de pouvoir communiquer à partir de n'importe quel endroit et à tout moment. Suite à cette demande, les réseaux informatiques ont dû s'adapter et ils sont rapidement convergés vers des communications sans fil.

Dans la suite des chapitres, nous allons focaliser sur la présentation des concepts de base des différents types des réseaux sans fil.

CHAPITRE 2

NOTIONS FONDAMENTALES DES RÉSEAUX SANS FIL.

2.1 Introduction

L'apparition des réseaux filaires a révolutionné le monde de l'informatique en permettant la communication entre des machines distantes. Cela en offrant une panoplie d'avantages allant de simple partage de ressources aux calculs parallèles. Cependant, les réseaux filaires souffrent d'un coût élevé de déploiement et de gestion de l'infrastructure filaire en plus des capacités limitées des câbles. De même, les utilisateurs expriment de plus en plus des besoins de mobilité et souhaitent pouvoir communiquer tout en se déplaçant.

Dans ce contexte, la technologie des réseaux mobiles sans fil a apparu pour subvenir au besoin de joindre la mobilité à la communication. Depuis, la technologie des réseaux sans fil n'a pas cessé de se développer et elle est devenue de plus en plus populaire du fait de sa facilité de déploiement et grâce aux développements technologiques dans divers domaines liés à la micro-électronique. Les réseaux sans fils offrent une grande flexibilité d'emploi, ils permettent aux utilisateurs de se déplacer librement tout en continuant normalement leurs communications.

2.2 C'est quoi un réseau sans fil (Wireless Network) ?

Un réseau sans fil (Wireless network) est, comme son nom l'indique, un réseau dans lequel les terminaux peuvent se déplacer librement et communiquer sans le besoin d'une liaison filaire. Un réseau sans fil doit assurer toutes les fonctionnalités et tous les services d'un réseau classique. En effet, il s'agit d'un système composé de nœuds mobiles généralement connectés à un point d'accès sans fil, voir la figure 2.1. Ce système permet à ses utilisateurs d'accéder à l'information indépendamment de leurs positions géographiques [3]. Les technologies de communication sans fil utilisent les ondes électromagnétiques, l'infrarouge, etc. Les terminaux des réseaux sans fil peuvent être tout équipement muni d'une interface sans fil comme par exemple : Laptops, Tablets, Smartphones, etc.

Remarques

— Un réseau est dit sans fil, si au moins deux terminaux communiquent via un lien sans fil.

- Les réseaux sans fil sont considérés comme une extension des réseaux filaires.

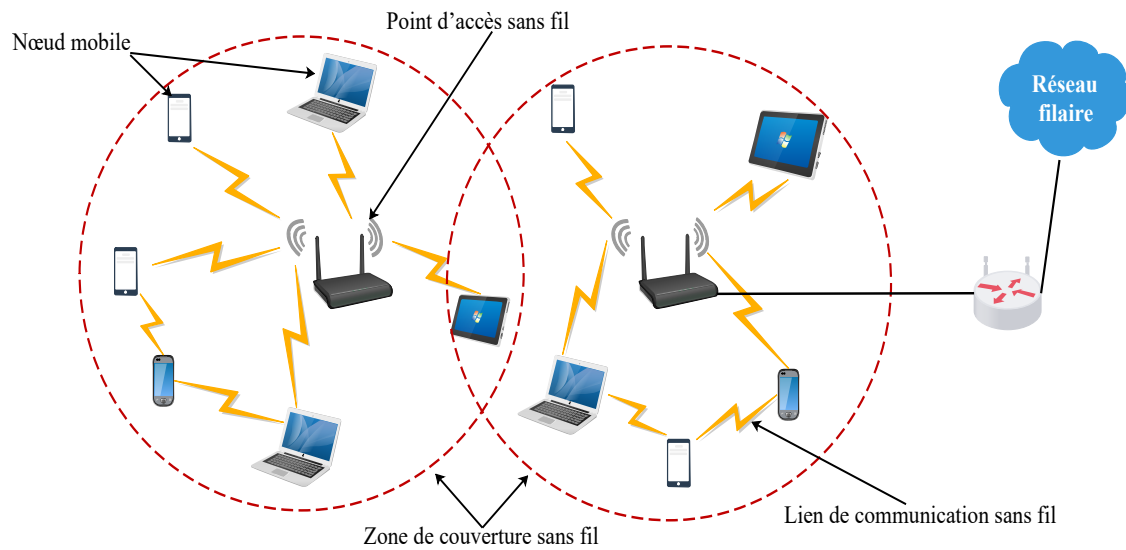


FIGURE 2.1 – un exemple illustratif d'un réseau sans fil.

2.3 Apports et défis des réseaux sans fil

Les principaux points forts et défis des réseaux sans fil sont résumés dans les points suivants [4].

2.3.1 Points forts

- Le support de la mobilité et la liberté de mouvement.
- La facilité et la rapidité de déploiement.
- La flexibilité et la souplesse de l'utilisation.
- La simplicité et la rapidité de l'extension et de la maintenance.
- Plus économiques et ne nécessite pas un gros investissement.
- Moins ennuyeux en infrastructure et en équipements.

2.3.2 Défis

- La sécurité.
- Les contraintes liées à l'énergie.
- Les problèmes liés à la mobilité tels que : la localisation, le transfert intercellulaires (handover), l'adressage mobile, etc.

2.4 Support de communication sans fil (Onde électromagnétique)

Les réseaux sans fils utilisent les onde-électromagnétiques pour permettre la communication entre les équipements mobiles.

2.4.1 Définitions

Qu'est-ce qu'une onde ?, Une onde est le phénomène de propagation résultat d'une oscillation (une vibration) ou d'une perturbation, au sein d'un milieu.

Exemple : les ondes résultats de jet d'une pierre dans l'eau.

Qu'est-ce qu'une onde électromagnétique ?, Une onde électromagnétique est le phénomène de propagation résultat d'une perturbation qui a eu lieu dans un champ de forces électrique et magnétique [5] :

- Le champ électrique (Volt / mètres) : il est le résultat de la différence des charges électriques.
- Le champ magnétique (Tesla) : il est le résultat du déplacement des courants électriques.

Remarque : les ondes électromagnétiques se propagent à travers la plupart des matériaux et aussi dans le vide.

2.4.2 Caractéristiques

Les principales caractéristiques des ondes électromagnétiques sont [5] :

- a) **La longueur (λ)** : elle représente la distance parcourue par l'onde pendant une période de temps (T) à la vitesse (v), voir la figure 2.2. La longueur de l'onde, notée λ , est donnée par :

$$\lambda(m) = \frac{v(m/s)}{f(Hz)}$$

Tel que f est la fréquence : $f = 1/T$.

Remarques

- L'unité de mesure de la longueur est le mètre.
 - La vitesse de l'onde électromagnétique dans le vide est égale à la vitesse ou la célérité de la lumière (3×10^8 m/s).
- b) **La fréquence (f)** : elle représente le nombre de fois qu'un cycle se répète par seconde. La taille de motif d'un cycle d'une onde se représente graphiquement par la différence entre deux crêtes (pics) successives, voir la figure 2.2.

Remarques

- L'unité de la fréquence est le hertz (Hz). $1Hz = onde/sec$.
- Une onde à faible fréquence se propage plus loin que celle avec une fréquence élevée.
- Plus la fréquence est élevée, plus elle peut transmettre plus de données et d'énergie.

- Une onde avec une longueur élevée correspond à une faible fréquence.
- Une onde à petite longueur correspond à une onde avec une fréquence élevée.

c) **L'amplitude** : elle représente la hauteur de l'onde, c'est-à-dire, la distance entre la crête supérieure et la crête inférieure de l'onde, voir la figure 2.2. L'amplitude représente la quantité d'énergie injectée dans le signal et elle est communément utilisée pour mesurer la force du signal.

Remarques

- Une onde avec une grande amplitude est générée par un signal fort par contre une onde avec une petite amplitude est générée par un signal faible.
- Une force électrique élevée va générer une large amplitude avec une forte énergie.

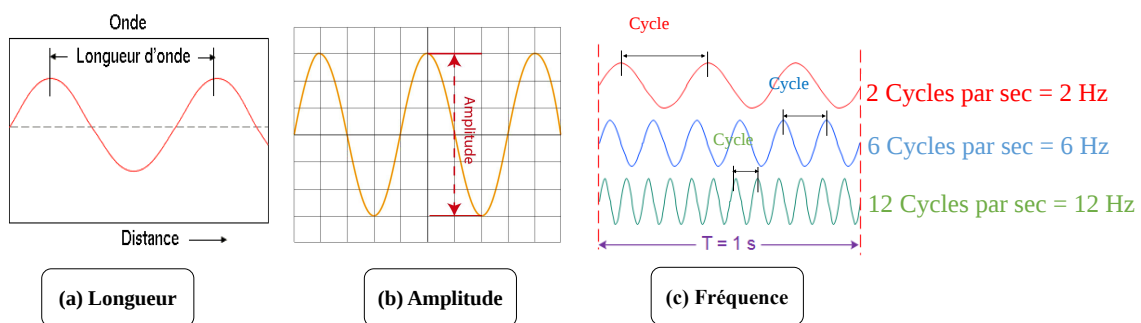


FIGURE 2.2 – les caractéristiques d'une onde électromagnétique.

2.4.3 Spectre électromagnétique

Comme il est illustré à la figure 2.3, le spectre électromagnétique est découpé en plusieurs catégories selon la fréquence et la longueur des ondes [5] :

- **Les ondes visibles** (la lumière) et **les ondes invisibles** (l'onde-radio, la micro-onde, l'infrarouge, l'ultraviolet, le rayon X et le rayon gamma).
- **Les ondes ionisantes** (elles ont des fréquences élevées (les rayons X ou gamma)) et **les ondes non-ionisantes** (les autres fréquences).
- **Les ondes radios des réseaux sans fil** : elles sont des micro-ondes électromagnétiques dont la fréquence est comprise entre 9 kHz et 300 GHz avec des longueurs d'onde allant de 33 km à 0,1 mm.

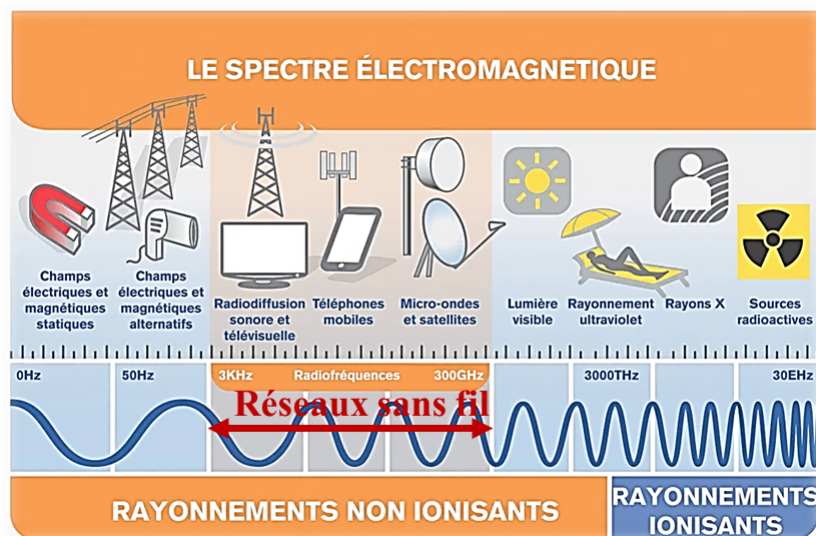


FIGURE 2.3 – le spectre électromagnétique [6].

2.4.4 Cas d'utilisation

Les ondes électromagnétiques sont utilisées dans divers domaines et pour différentes objectives. Les cas d'utilisation les plus répandus sont les suivants [6] :

- Le transport de l'énergie (les réseaux 50Hz/60Hz).
- La communication (AM/FM, WIFI, 4G, 5G, etc.).
- La télédétection (les radars).
- Les soins médicaux (l'imagerie médicale).
- Le réchauffement des aliments (les micro-ondes).
- etc.

2.4.5 Phénomènes perturbateurs des ondes électromagnétiques

Une onde électromagnétique est assujettie à différents phénomènes perturbateurs, les plus importants sont résumés dans les points suivants :

- **L'atténuation** : ce phénomène est dû à la diminution de l'amplitude résultant de l'absorption de l'énergie par le milieu traversé lorsque l'onde s'éloigne de la source.
- **Les interférences** : ce phénomène se produit lorsque plusieurs ondes de même fréquence se rencontrent, ce qui entraîne une déformation du signal.
- **L'effet de fading** : ce phénomène représente la disparition du signal des ondes due à son atténuation à cause de la météo ou son élimination à cause des interférences destructives.
- **L'effet de masque (Shadowing)** : il représente des variations du canal radio mobile ou l'atténuation de la puissance du signal due aux obstacles entre l'émetteur et le récepteur.

- **La réflexion et la réfraction** : c'est le phénomène qui caractérise une onde électromagnétique lorsqu'elle passe par une surface de séparation entre deux milieux de propagation. En effet, une partie de l'onde est déviée vers le milieu d'origine et il s'agit de phénomène de la réflexion. Tant dit que l'autre partie traverse la surface de séparation en changeant de direction, en effet, il s'agit de phénomène de réfraction, voir la figure 2.4, voir la figure 2.4.
- **La diffraction** : un phénomène qui se manifeste par la déviation (l'étalement) de la direction d'une onde lorsqu'elle est obstruée par un obstacle ou un passage d'une ouverture, voir la figure 2.4.
- **La diffusion** : ce phénomène se produit lorsqu'une onde électromagnétique rencontre un obstacle, elle se diffuse dans toutes les directions, voir la figure 2.4.
- **Le bruit ambiant** : il correspond à la somme des fréquences qui peuvent être reçues en un point précis.

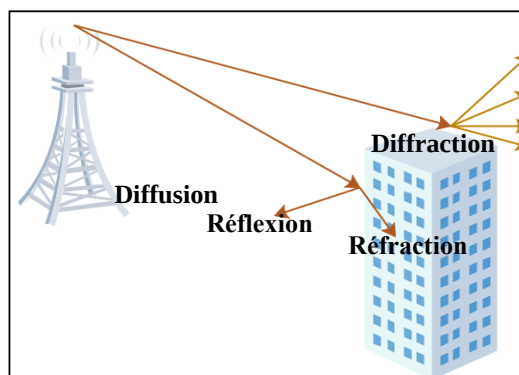


FIGURE 2.4 – des exemples de phénomènes perturbateurs des ondes électromagnétiques.

2.4.6 Technique de modulation / démodulation

Le signal de l'onde électromagnétique est rarement adapté à la transmission directe par le canal de communication sans fil. En effet, il est impossible de [7, 12] :

- a) Transmettre des ondes à basse fréquence sur une grande distance, et
- b) Distinguer les ondes avec des fréquences proches ou identiques par le récepteur.

La solution à ce problème consiste à utiliser une autre onde à haute fréquence (dite *porteuse*) pour transporter l'onde initiale en utilisant la technique de la modulation / démodulation, voir la figure 2.5.

La modulation est une technique qui consiste à transformer une onde (un signal) source à une autre forme adaptée au canal de transmission en utilisant une autre onde de haute fréquence. La modulation consiste à varier l'amplitude (Amplitude Modulation, AM), la fréquence (Frequency Modulation, FM) ou la phase (Phase Modulation, PM) [7].

La démodulation est l'opération inverse qui permet d'extraire l'onde originale de la porteuse.

Remarques

- Le dispositif physique responsable de ces deux opérations est le modem (modulator-demodulator).
- Il existe deux formes de signal : le signal numérique (0 et 1) et le signal analogique.

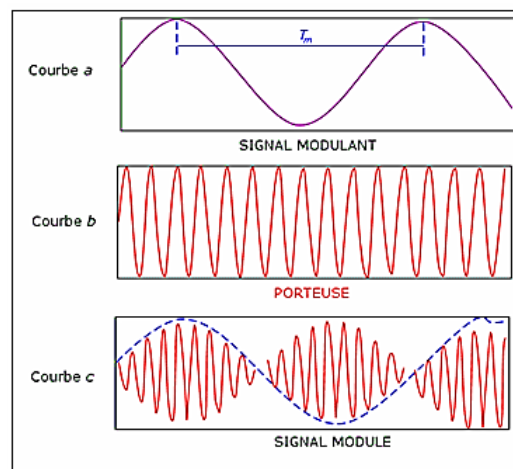


FIGURE 2.5 – la technique de modulation / démodulation [9].

À cause de la nature partagée du canal de communication sans fil, les messages (ou les paquets) envoyés en même temps sur la même fréquence sont constamment subits au problème de collision de signaux. Pour remédier à ce problème, plusieurs techniques de gestion d'accès au canal de communication sans fil ont été proposées.

2.4.7 Technique d'accès au support de communication sans fil

Les principales techniques de base de la gestion d'accès au canal sans fil sont [8] :

- FDMA (Frequency Division Multiple Access)** : cette technique consiste à diviser la fréquence en sous-bandes (sous-fréquences) et chaque sous-fréquence est associée définitivement à un utilisateur, voir la figure 2.6. Cette technique présente l'avantage d'être simple à implémenter par contre elle génère une sous-exploitation de la bande de fréquence. Autrement dit, une sous-fréquence est allouée définitivement à un utilisateur donnée, et même si elle est libre, elle ne peut pas être utilisée par un autre utilisateur.
- TDMA (Time Division Multiple Access)** : cette technique consiste à diviser la bande de fréquences en plusieurs slots (ou tranches) de temps et chaque slot est associé à un utilisateur, voir la figure 2.6. Les utilisateurs communiquent à tour de rôle. TDMA permet d'augmenter le nombre d'utilisateurs par contre elle est complexe et nécessite la synchronisation des communications.
- CDMA (Code Division Multiple Access)** : cette technique consiste à affecter à chaque utilisateur un code unique, déterminant la fréquence et la puissance, voir la figure 2.6. Les utilisateurs peuvent communiquer en même temps sur la même fréquence avec des codes différents. Le récepteur distingue les signaux sources grâce à leurs codes. CDMA permet de réutiliser les mêmes fréquences par contre lorsque le nombre d'utilisateurs augmente, le bruit augmente ce que risque de dégrader la qualité de service (Quality of Service (QoS)).

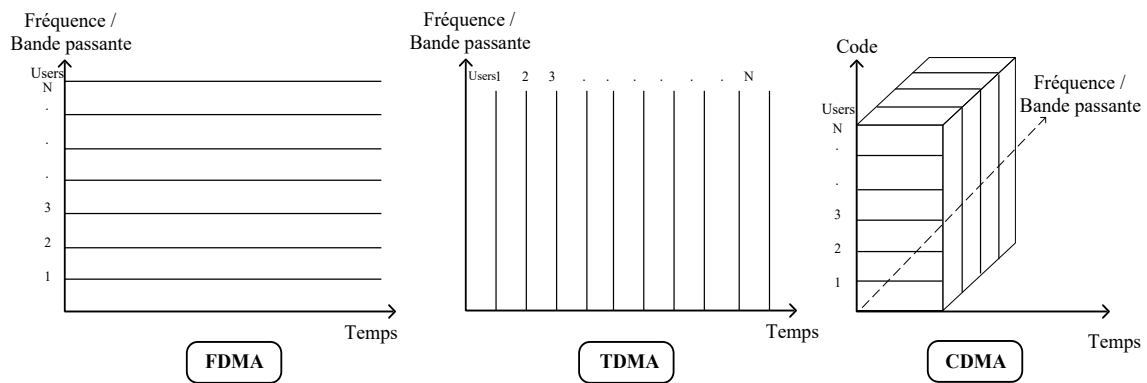


FIGURE 2.6 – les techniques d'accès au canal de communication sans fil.

2.5 Classification des réseaux sans fils

Les réseaux sans fil peuvent être classifiés selon différents critères à l'instar de la taille, la technologie de communication, l'utilisation de l'infrastructure fixe, etc.

Le tableau 2.1 présente un aperçu taxonomique sur une classification des réseaux sans fil selon l'étendue ou la taille de réseau.

Type	Portée	Norme	Technologie	Rôle	Exemple
Les réseaux sans fil personnels - WPAN (Wireless Personal Area Network)	Faible (maximum une dizaine de mètres)	IEEE 802.15	Bluetooth, ZigBee, IrDA, NFC, etc.	Relier des machines non éloignées via un lien sans fil (le niveau individuel ou personnel).	Un réseau entre une souris sans fil et un ordinateur.
Les réseaux sans fil locaux - WLAN (Wireless local Area Network)	Moyenne (maximum une centaine de mètres).	IEEE 802.11	WiFi, Hi-perLan2 (Europe), etc.	Relier des machines moyennement éloignées via des liens sans fil (le niveau d'un bâtiment).	Un réseau local d'une entreprise entre équipements connectés via un point d'accès.
Les réseaux sans fil métropolitains - WMAN (Wireless Metropolitan Area Network)	Large (maximum une dizaine de kilomètres).	IEEE 802.16	WiMax	Relier des réseaux WLANs éloignés via des liens sans fil (le niveau d'une ville ou d'un campus).	Un réseau WiMax entre des sièges éloignés d'une entreprise dans la même ville.
Les réseaux sans fil étendus - WWAN (Wireless Wide Area Network)	Très large (Plusieurs centaines (milliers) de kilomètres).	UMTS, LTE, etc.	Les réseaux cellulaires (GSM, 3G, 4G), les réseaux satellitaires.	Relier des réseaux très éloignés via des liens sans fil (le niveau régional, national, ou continental).	Un réseau 4G entre les sièges éloignés d'une entreprise situés dans plusieurs villes.

TABLE 2.1 – un aperçu taxonomique sur une classification des réseaux sans fil selon l'étendue ou la taille de réseau.

Les réseaux mobiles sans fil peuvent être classés aussi selon l'architecture de communication adoptée en deux grandes catégories :

- Les réseaux cellulaires avec infrastructure fixe ou les réseaux cellulaires.
- Les réseaux Ad hoc sans infrastructure fixe ou les réseaux mobiles ad hoc.

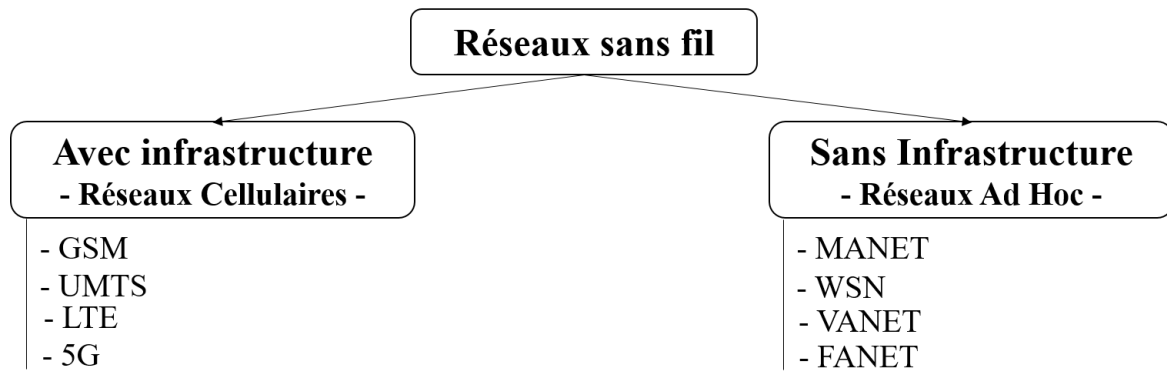


FIGURE 2.7 – classification des réseaux mobiles sans fil selon l’infrastructure fixe.

Comme il est illustré à la figure 2.7, plusieurs technologies sont apparentées aux réseaux cellulaires comme : GSM, WiMax, GPRS, UMTS, etc., et aux réseaux mobiles Ad Hoc comme les MANETs, WSNs, VANETs et les réseaux de drones (FANETs).

2.6 Conclusion

Les réseaux mobiles sans fil ont connu un énorme succès. L’avantage de tels systèmes est la possibilité de communiquer de n’importe où, même en se déplaçant sans le besoin d’une liaison filaire. Actuellement, les plus grandes avancées dans les domaines des réseaux sont principalement consacrées pour les réseaux mobiles sans fil tel que la cinquième génération des réseaux cellulaires, l’Internet des objets et prochainement l’Internet mobile via le satellite à l’instar du projet Starlink de SpaceX. Les réseaux sans fil doivent faire face aussi à de nombreux défis tels que les risques liés à la sécurité et aux contraintes liées à l’énergie.

Dans le chapitre suivant, nous allons présenter les concepts de base des réseaux sans fil avec infrastructure (les réseaux mobiles cellulaires).

CHAPITRE 3

RÉSEAUX SANS FIL AVEC INFRASTRUCTURE FIXE (RÉSEAUX MOBILES CELLULAIRES).

3.1 Introduction

Historiquement, l'invention du premier téléphone fixe en 1876 par le physicien américain *Alexander Graham Bell* a offert le premier moyen qui permet aux gens de se parler librement sur de longues distances. Les réseaux de téléphonies fixes ont rapidement connu un énorme succès et un large déploiement propulsés par différentes innovations tel que l'échange pratique (the workable exchange) en 1879, qui permet de commuter les appels entre les abonnés au lieu d'avoir des lignes directes, et le début de la désignation des abonnés par des numéros et non plus par leurs noms. Cependant, les réseaux de téléphonies fixes souffrent d'un coût élevé pour déployer les câbles et sécuriser les installations. Ils sont rigides et manquent de portabilité et mobilité qui limitent beaucoup la capacité de communication tout en se déplaçant.

Les réseaux de téléphones mobiles sans fil ont progressivement émergé. Ainsi, l'année 1946 a connu la mise en service du premier service commercial de téléphonie mobile au monde. Il permet de relier des véhicules en mouvement à un réseau téléphonique par onde-radio. Motorola par la suite a produit le premier téléphone portable (Motorola Dyna TAC 8000 X) en 1984. Initialement, dédiés exclusivement pour le transfert de la voix, les données ont été introduites progressivement. Depuis les réseaux de téléphones mobiles (plus connu actuellement sous l'appellation des réseaux mobiles cellulaires) ont connu une énorme évolution durant les dernières décennies.

3.2 Définition

Un réseau mobile sans fil cellulaire (Wireless mobile cellular network) est un réseau sans fil avec infrastructure fixe dans lequel les terminaux sont mobiles, peuvent se déplacer librement et communiquer indépendamment de leurs positions géographiques sans le besoin d'une liaison filaire. Il s'agit des réseaux structurés, basés sur des équipements d'interconnexion faisant office de ponts entre un réseau radio et un réseau câblé, permettant ainsi à de nombreux utilisateurs mobiles d'accéder à des ressources informatiques en utilisant une liaison radio [10].

3.3 Architecture Générale

Un réseau mobile cellulaire se compose de plusieurs éléments de base [10], voir la figure 3.1 :

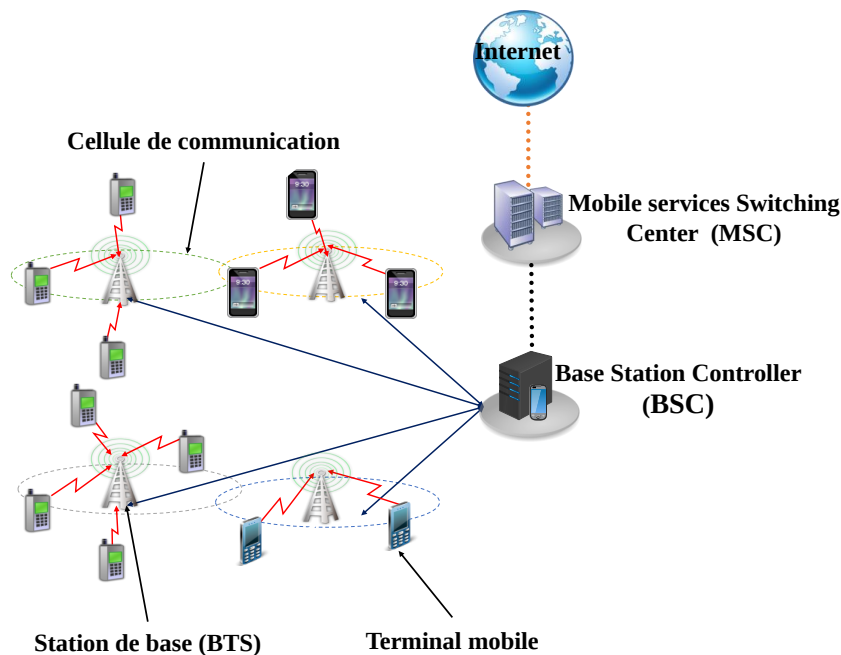


FIGURE 3.1 – l'architecture générale d'un réseau mobile cellulaire.

- a) **Le terminal mobile** : il permet à l'abonné d'accéder aux services du réseau. Il est généralement composé de :
 - i) **L'équipement portable** : qui contient son identité internationale IMEI (International Mobile Equipment Identity) ; et
 - ii) **La carte SIM (Subscriber Identity Mobile)** : qui gère une série d'informations caractérisant un abonné, ainsi que ses droits. Tel que : le numéro de téléphone de l'utilisateur (MSISDN, Mobile Station ISDN Number), l'identité internationale de l'abonné (IMSI, International Mobile Subscriber Identity) et une clé pour l'authentification et le chiffrement de la liaison radio (Ki, Individual Subscriber Authentication Key). En plus de code PIN et PUK, le nom de l'opérateur, les contacts, etc.
- b) **La station de base ou BTS (Base Transceiver Station)** : elle intègre l'antenne ¹ qui assure la communication entre les terminaux des abonnés et le réseau de l'opérateur sur une zone de couverture définie. Elle s'occupe de la modulation, de codage/décodage, de l'adaptation du débit, etc.
- c) **Le contrôleur de stations de base ou BSC (Base Station Controller)** : il gère les ressources radios et les bandes passantes des stations de base associées.
- d) **Le BSS (Base Station Subsystem)** : le BSC et l'ensemble des BTS qui lui sont raccordés constituent le sous-système radio BSS.

1. **Antenne** : il s'agit d'un ensemble des émetteurs/récepteurs appelés TRX (Transceiver) qui assurent la communication sur une zone bien définie. On distingue trois grands types : antennes omnidirectionnelles (360°), antennes bi-sectorielles (180°) et antennes tri-sectorielles (120°).

- e) **Le MSC (Mobile services Switching Center)** : les BSCs sont tous raccordés à des commutateurs du service mobile, appelés MSC.

3.4 Concept de base

Les réseaux mobiles cellulaires reposent sur deux principes fondamentaux à savoir : le découpage en cellules (ou la division cellulaire) et la réutilisation de fréquences.

3.4.1 Division cellulaire

La division cellulaire consiste à découper le territoire ou l'environnement de communication en cellules hiérarchiques afin de mieux supporter la mobilité des utilisateurs, voir la figure 3.2.

- a) **Le concept de cellule** : une cellule est une zone géographique couverte par une antenne de transmission et desservie par la station de base. Une cellule est caractérisée par :

- i) Une puissance d'émission : qui représente sa zone de couverture ; et
- ii) La fréquence de l'onde porteuse : utilisée pour l'émission électromagnétique.

Remarque : une cellule est généralement modélisée par un hexagone (cette forme n'existe pas dans la réalité).

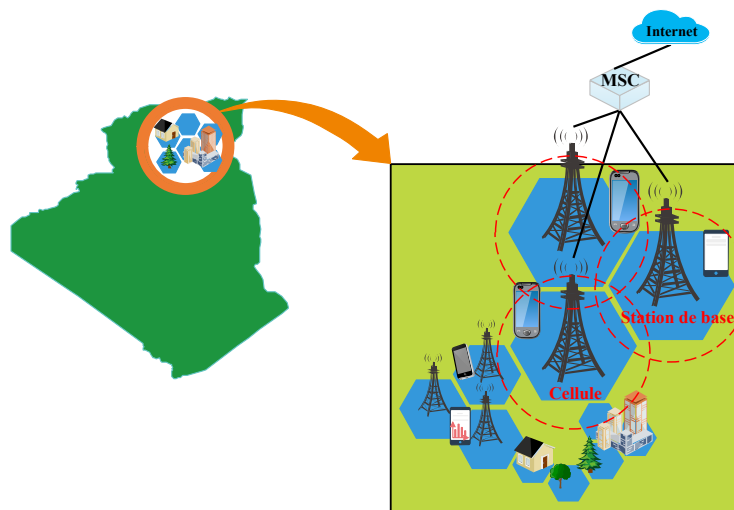


FIGURE 3.2 – la hiérarchie des cellules dans un réseau cellulaire.

- b) **Taille de la cellule** : elle représente l'étendue de la zone de couverture de la station de base. La taille d'une cellule peut varier en fonction de relief de territoire (la plaine, la montagne), la localisation (urbaine, rurale, suburbaine), la densité d'abonnés, la nature des constructions (maisons, pavillons, tours), etc. Il y a plusieurs types de cellules selon la taille :

- i) **La cellule globale (Umbrella Cell)** : elle couvre une région pouvant atteindre le tiers du globe grâce aux satellites.

- ii) **La macro-cellule** : elle a un rayon de couverture important allant jusqu'à 35 Km, adaptées aux zones rurales faiblement peuplées.
- iii) **La micro-cellule** : elle a un rayon de couverture de quelques centaines de mètres, adaptées aux zones urbaines denses.
- iv) **La pico-cellule** : elle a un rayon de couverture de quelques dizaines de mètres, adaptées aux petits espaces très denses.
- v) **La femto-cellule** : elle a un rayon de quelques mètres, adaptés aux locaux fermés.

Remarque : plus la taille de la cellule est plus petite, plus le nombre d'utilisateurs est plus grand.

Types de cellules	Distance	Milieu
Macro-cellule	2 Km à 35 km	Rural
Micro-cellule	500 m à 2 km	Urbain
Pico-cellule	moins de 500 m	Bâtiments
Femto-cellule	10 à 20 m	Locaux fermés

TABLE 3.1 – une récapitulation sur quelques caractéristiques des types de cellules.

3.4.2 Réutilisation des fréquences

La réutilisation des fréquences permet d'augmenter la capacité de réseau par le découpage d'une cellule en plusieurs cellules plus petites. Les fréquences utilisées par une cellule peuvent être réutilisées par une autre cellule suffisamment éloignée, grâce à la propriété d'atténuation des ondes radio-magnétiques. Ainsi, au lieu d'utiliser une seule cellule pour tout le réseau, la zone de couverture est divisée en petites cellules regroupées en cluster (ou motif cellulaire) dont la taille dépend du système [10].

- i) **Le motif cellulaire (cluster)** : il représente le plus petit groupe de cellules où l'ensemble de fréquences sont utilisées une seule fois.
- ii) **La distance de réutilisation (D)** : elle représente la distance minimale entre deux cellules pour pouvoir réutiliser une fréquence. Cette distance doit être suffisamment grande pour ne pas causer d'interférences et elle peut être calculée via la relation suivante : $D = R\sqrt{3N}$, tel que, R est le rayon de la cellule et N est la taille du motif (le facteur de réutilisation), voir la figure 3.3.
- iii) **Le nombre de communications** : ils peuvent avoir $K \times N$ communications simultanées. Tel que :
 - K représente le nombre de motifs : $K = i^2 + i \times j + j^2$ (i et j sont des entiers); et
 - N est le nombre de cellules par motif : $N = D^2 / (3 \times R^2)$.

Remarque : le but est de trouver la plus petite valeur de N donnant un seuil d'interférence minimal pour obtenir une utilisation maximale de la bande passante.

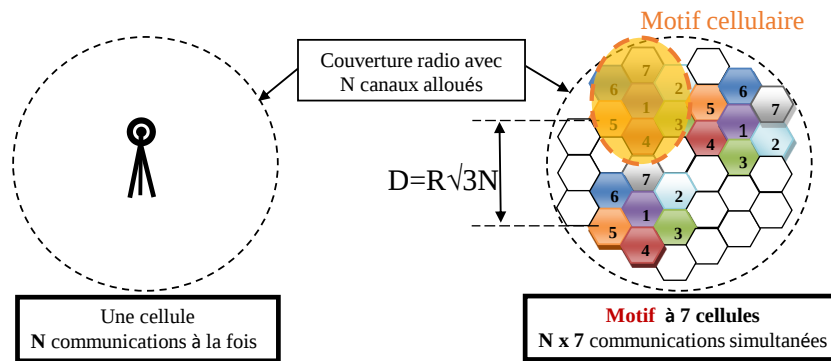


FIGURE 3.3 – le concept de la réutilisation des fréquences.

3.4.3 Gestion de la mobilité

La gestion de la mobilité vise à assurer la connectivité des abonnés lors des déplacements grâce à deux fonctionnalités de base : le transfert intercellulaire (Handover) et la gestion de l'itinérance (Roaming).

3.4.3.1 Transfert intercellulaire (ou handover)

Le transfert intercellulaire ou handover représente le processus par lequel une communication est maintenue lors du déplacement du terminal mobile dans le réseau mobile cellulaire d'une cellule à une autre. Ce maintien est possible grâce au changement du canal radio utilisé. Le handover est exécuté dans la zone de handover (la zone de chevauchement entre deux cellules), voir la figure 3.4. Une station mobile (SM) est connectée à une station de base 1 (SB 1), et se déplace vers la SB2 pendant son appel. Le handover sera effectué dans la zone de chevauchement (la zone de handover) entre les deux SBs où la SM peut recevoir le signal à partir des deux SBs [12], [13].

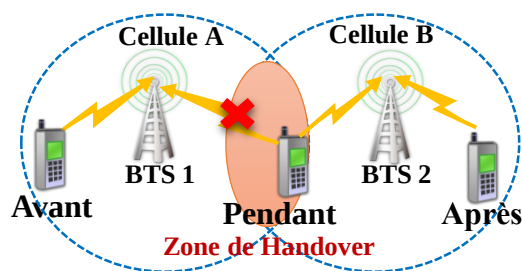


FIGURE 3.4 – le transfert intercellulaire dans les réseaux mobiles cellulaires.

3.4.3.2 Itinérance (ou Roaming)

L'itinérance (ou Roaming) vise à permettre à l'abonné de communiquer hors de la zone de couverture de réseau de son opérateur cellulaire. En effet, le roaming désigne le procédé qui permet à un utilisateur de communiquer, en passant par le réseau d'un opérateur qui n'est pas le sien (qui a signé auparavant un contrat de roaming) lors de son déplacement hors de la zone de couverture de son opérateur d'origine.

3.5 Évolution et génération des réseaux mobiles cellulaires

Depuis, la première génération (notée 1G) apparue dans la fin des années 70 principalement basée sur un fonctionnement analogique et la technique FDMA, les réseaux mobiles cellulaires ont connu un développement extraordinaire au fil des années. La seconde génération (notée 2G) est apparue au début des années 90. L'apparition de cette génération a marqué la rupture avec la 1G grâce au passage de l'analogique au numérique et aussi l'utilisation de TDMA. La norme permet la transmission de la parole numérique de très bonne qualité et aussi de petits volumes de données avec des vitesses modestes. En effet, presque à chaque décennie, on voit l'arrivée d'une nouvelle génération avec des capacités et des caractéristiques plus avancées, voir la figure 3.5.

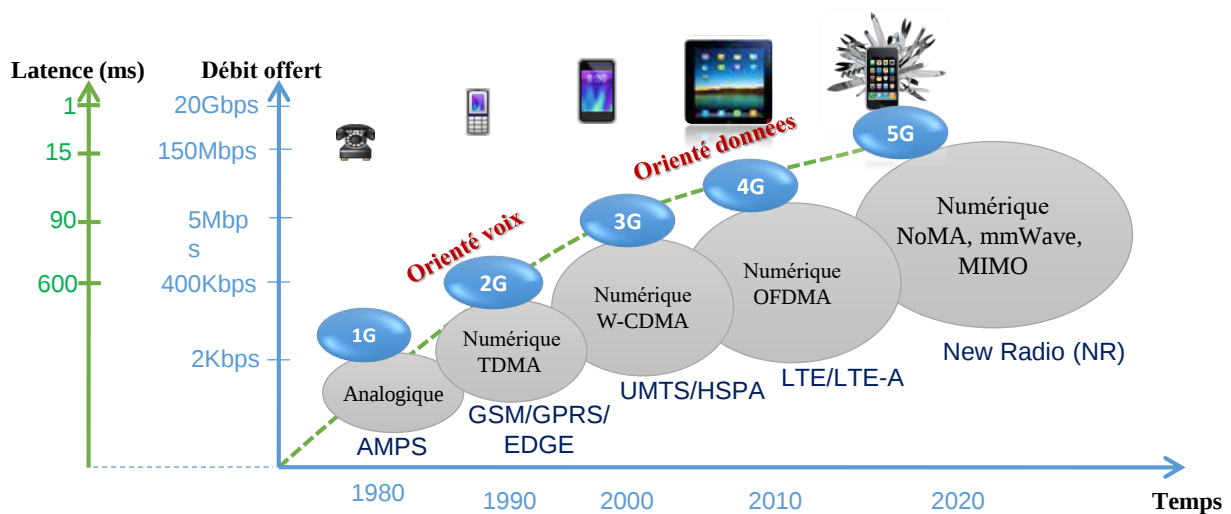


FIGURE 3.5 – une chronologie de l'évolution historique des réseaux cellulaires.

La deuxième génération (la 3G) des réseaux cellulaires apporte les données mobiles avec des vitesses de transmissions plus rapides. La 3G permet la transmission de la voix et des données simultanément. Plus tard, la quatrième génération (la 4G) a introduit l'accès à l'Internet mobile à très haut débit avec une faible latence. Plus récemment, la cinquième génération (la 5G) propose des connexions mobiles à très haut débits (qui voisine les giga-bytes) avec des très faibles latences et des ondes millimétriques. Actuellement, la sixième génération (la 6G) – Internet for machines-enabled IA - des réseaux cellulaires est en cours de standardisation. La fin de spécification des pré-requis est prévue en 2022 avec des débits s'approchant de Terabytes / s. La date de début de déploiement de la 6G est prévue pour le début de l'année 2030.

Le tableau 3.2 présente un résumé comparatif et récapitulatif des principales caractéristiques des générations des réseaux mobiles cellulaires.

Génération	Standard	Année de déploiement	Débit	Service	ère
1G	AMPS (USA) / TACS (EU) / ETACS (UK)	Fin 1970	2 kbps	la voix analogique.	le téléphone pour la voix analogique.
2G	GSM (Eu) CDMA IS-95 (USA)	1990 (fin 91)	9,6 kbps	la voix numérique, les données de faible volume, etc.	le téléphone pour la voix numérique.
2G+ ou 2.5G	GPRS	2001	21,4 171,2 Kbit/s	le transfert de la voix ou des données de volume modéré.	-
2G++ ou 2.75G	EDGE	2003	43,2 345,6 Kbit/s	le transfert simultané de la voix et des données.	-
3G	UMTS	2004	entre 384 kb/s et 2 Mb/s	la Vidéo HD, la visiophonie, VoD, etc.	le téléphone pour les données.
+ ou 3.5G	HSPA	2006	14 Mb/s (Download) + 5.76 Mb/s (Upload)	Pareil comme la 3G.	-
3G++ ou 3.75G	HSPA+	2008	168 Mb/s (download) - 22 Mb/s (upload)	Pareil comme la 3G.	-
4G	LTE	2010	100 Mb/s (download) - 50 Mb/s (upload)	le streaming HD, etc.	le téléphone pour l'Internet.
4G+ ou 4.5G	LTE-A	Après 2014	Jusqu'à 1 Gbit/s	les objets connectés, etc.	-
5G	NR (New Radio)	2020	entre 1 Gb/s et 20 Gb/s (download)	la réalité augmentée, la voiture autonome, l'IoT, etc.	le téléphone pour l'internet des objets.

TABLE 3.2 – un tableau récapitulatif et comparatif des générations des réseaux cellulaires [10].

3.6 Conclusion

Les réseaux mobiles cellulaires, sont sans aucun doute, ceux qui ont connu la plus grande évolution ces dernières années. Cela est principalement dû à l'explosion du nombre d'abonnés, la demande sans cesse croissante de débit plus élevés et l'apparition des applications multimédias. Ces réseaux sont basés sur l'utilisation de l'interface radio et la réutilisation de fréquences, ainsi que sur la technologie de la division cellulaire.

Il s'agit du déploiement de plusieurs générations successives de réseaux de télécommunications, essentiellement dédiées à la téléphonie ((1G, ETACS), (2G, GSM)) puis plus orientées vers le multimédia ((3G, UMTS), (4G, LTE)), et plus récemment orienté vers l'Internet mobile à haut débit (5G) et très prochainement orientés vers l'internet des objets augmentés par des techniques de l'intelligence artificielle (6G).

Dans le chapitre suivant, nous présentons les différents types des réseaux sans fil sans infrastructure (les réseaux mobiles ad-hoc).

CHAPITRE 4

RÉSEAUX SANS FIL SANS INFRASTRUCTURE (RÉSEAUX MOBILES AD-HOC).

4.1 Introduction

Au cours des dernières décennies, suite au grand développement des technologies de communications sans fil et le progrès dans les capacités des dispositifs mobiles, les réseaux sans fil mobiles ad-hoc, communément appelés MANETs pour Mobile Ad-hoc NETWORKs en anglais, ont émergé comme une nouvelle génération de réseau sans fil facilement et rapidement déployable avec un faible coût, sans aucune administration centralisée ni infrastructure préexistante. Ces réseaux sont particulièrement adaptés pour des applications dans des situations où la mise en place d'une infrastructure fixe n'est pas envisageable ou simplement non rentable économiquement.

Les réseaux mobiles ad-hoc offrent une grande flexibilité de déploiement et ils sont de plus en plus utilisés. Ils sont traditionnellement utilisés dans les applications militaires, les services d'urgence, les événements occasionnels, etc.

4.2 Réseaux sans fil mobiles ad-hoc (Mobile Ad-hoc NETWORKs, MANETs)

Aujourd'hui, les réseaux ad-hoc sont de plus en plus populaires du fait de leur facilité de déploiement et la diversité de leurs domaines d'applications.

4.2.1 Définition

Un réseau mobile ad-hoc, appelé aussi MANET (Mobile Ad-hoc NETWORK), est un réseau auto-organisé qui se compose d'un ensemble de nœuds mobiles et autonomes. Ces nœuds sont interconnectés via des technologies sans fil avec un système de communication distribué de nœud à nœud en multi-sauts sans l'aide de l'infrastructure fixe préexistante, ni d'administration centralisée, voir la figure 4.1. Du fait de cette absence d'infrastructure, la portée de communi-

cation est généralement limitée, et pour pouvoir communiquer entre eux chaque nœud mobile doit agir de manière autonome et jouer le rôle d'un routeur et d'un terminal en même temps. Un réseau ad-hoc a un modèle de mobilité libre, aléatoire et imprévisible [14].

Exemple de nœuds : les téléphones portables, les tablettes, les ordinateurs portables, les capteurs, etc.

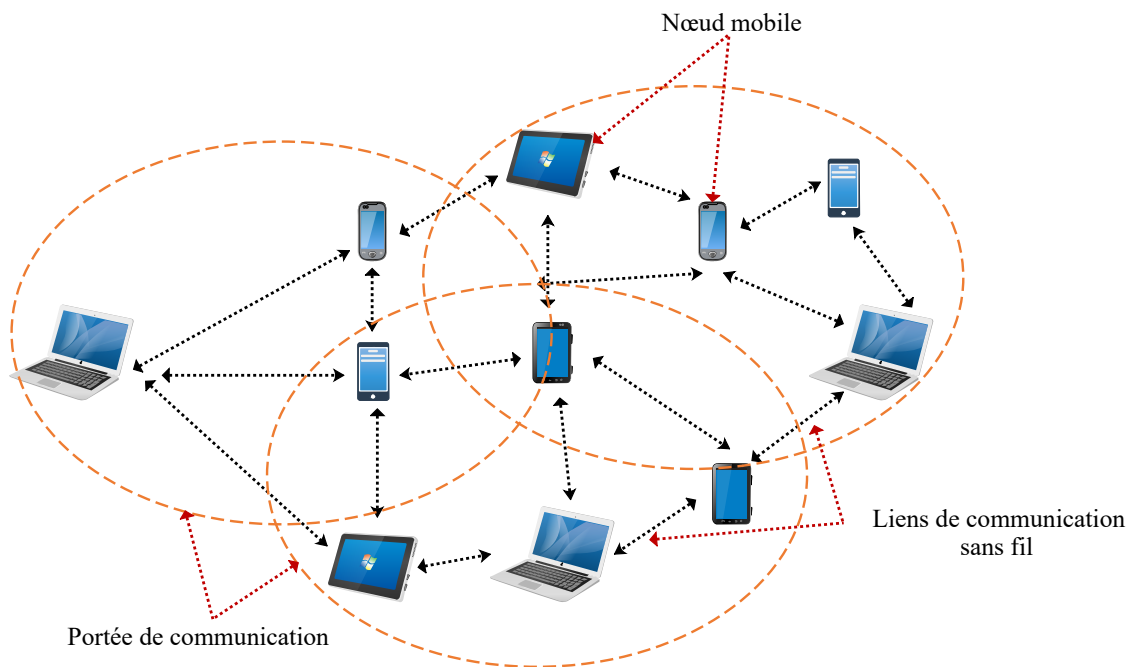


FIGURE 4.1 – un exemple illustratif d'un réseau mobile ad-hoc (MANET) [15].

Remarque : un réseau ad-hoc est un réseau dynamique et il est souvent temporaire.

4.2.2 Caractéristiques

Les principales caractéristiques des réseaux ad-hoc sont résumées dans les points suivants [16, 17, 20] :

- L'absence de l'infrastructure préexistante.
- Une architecture distribuée avec l'absence de tout genre d'administration centralisée.
- Chaque nœud du réseau est à la fois hôte et routeur.
- Une mobilité des nœuds aléatoire et imprévisible.
- Une topologie souvent très dynamique et non-prédictible.
- Une auto-organisation et une auto-adaptation.
- Un médium de communication sans fil et un mode de communication en multi-sauts.
- Une bande passante limitée à cause de médium de communication sans fil partagé.
- Une taille de réseau souvent limitée, mais parfois trop importantes.

- Un déploiement rapide et une résistance aux pannes grâce à la topologie distribuée.
- Des contraintes d'énergie à cause des sources d'alimentations limitées (batterie, etc.).
- Une sécurité physique limitée et des menaces de la confidentialité et de l'intégrité des données.
- Un taux d'erreur de transmission radio plus élevée due à la nature des liens sans fil et la topologie dynamique.
- La présence des interférences dues à l'utilisation de la même fréquence (ou des fréquences proches) des liens radios.
- Etc.

4.2.3 Domaines d'application

Comme il est illustré à la figure 4.2, les réseaux ad-hoc trouvent diverses applications dans différents domaines. Les domaines les plus importants sont résumés dans les points suivants [20] :

- **Les opérations stratégiques et tactiques** : les réseaux ad-hoc sont utilisés pour les communications militaires, les champs de batailles automatisées, etc.
- **Les services d'urgence** : les réseaux ad-hoc sont utilisés dans les opérations de recherche, d'exploration et de secours en cas de sinistres.
- **Le contrôle et la surveillance de l'environnement** : les réseaux ad-hoc sont utilisés pour la surveillance et la collecte des informations sur l'environnement (la température, l'humidité, etc.).
- **Les réseaux ad-hoc de véhicules** : les réseaux ad-hoc sont utilisés pour la surveillance de l'état de la route, le fonctionnement des véhicules, etc.
- **Le domaine sanitaire et médical** : les réseaux ad-hoc sont utilisés pour les opérations de suivi médical et les applications des réseaux WBANs (Wireless Body Area Network).
- **Les sites archéologiques et les événements occasionnels** : les réseaux ad-hoc sont utilisés dans les musées, les châteaux, les conférences, les séminaires, etc.
- **Les services civils et commerciaux** : les réseaux ad-hoc sont utilisés pour l'E-commerce (le paiement électronique), etc.
- **Les réseaux personnels et d'entreprise** : les réseaux ad-hoc sont utilisés dans les réseaux sans fil personnels (les écouteurs sans fil, etc.), les réseaux dans les locaux temporaires des entreprises et le Mobile office.
- **L'éducation** : les réseaux ad-hoc sont utilisés pour les communications ad-hoc durant les réunions, les conférences, etc.
- **Le divertissement** : les réseaux ad-hoc sont utilisés pour l'accès à Internet en extérieur, les jeux sous réseau en multi-joueurs, etc.
- Internet des objets, la ville intelligente, etc.
- Etc.

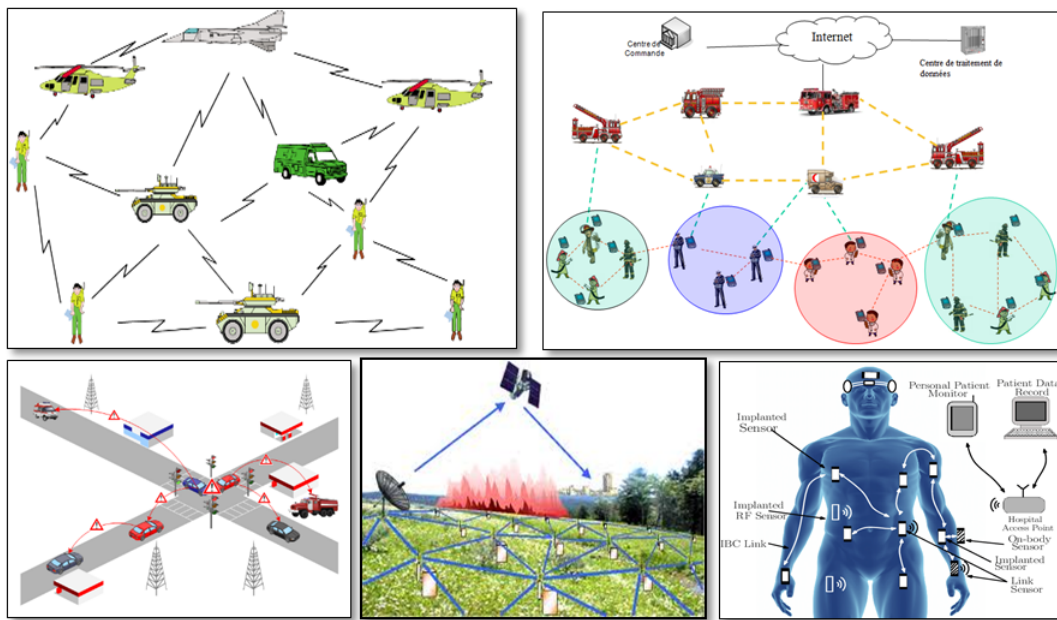


FIGURE 4.2 – des exemples illustratifs des domaines d’application des réseaux ad-hoc.

4.2.4 Principaux défis

Les réseaux ad-hoc héritent des problèmes traditionnels des réseaux sans fil. De plus, les MANETs ont des défis spécifiques, dont les plus importants sont résumés dans les points suivants [18] :

- Une difficulté d’assurer un partage équitable de canal de communication radio.
- Une faible sécurité due à la nature distribuée multi-sauts et le partage de canal radio.
- Des ressources limitées en termes d’énergie, de calcul, de stockage, etc.
- Une difficulté de conception des protocoles de routage efficace à cause de la forte mobilité, la topologie dynamique et la grande taille de réseau.
- Une difficulté d’assurer une bonne qualité de service faute de la topologie très dynamique, la nature intermittente des communications sans fil et la bande passante limitée.
- Etc.

4.2.5 Classification des protocoles de routage

Les protocoles de routage des réseaux ad-hoc peuvent être classifiés selon la méthode de préparation des routes en trois grandes catégories [18, 19] :

- a) **Les protocoles de routage proactifs** : ils sont caractérisés par la disponibilité à l’avance des routes et des mises à jour périodiques des tables de routage.
 - **Avantage** : la disponibilité immédiate des routes.
 - **Inconvénient** : la surcharge de réseau à cause des mises à jour périodiques.
 - **Exemple** : le protocole OLSR (Optimized Link State Routing).

- b) **Les protocoles de routage réactifs** : ils sont caractérisés par la création à la demande des routes et la non-utilisation de trafic de contrôle.
- **Avantage** : le trafic de contrôle est généré uniquement au besoin, ce qui permet de ne pas surcharger le réseau par de trafic inutile.
 - **Inconvénient** : un long délai d'attente pour l'établissement des routes.
 - **Exemple** : le protocole AODV (Ad hoc On-Demand Distance Vector).
- c) **Les protocoles de routage hybrides** : ils représentent un compromis avec une procédure de détermination à la demande et un coût de recherche limité. Il fonctionne avec un comportement proactif en local et un fonctionnement réactif pour les nœuds éloignés.
- **Exemple** : le protocole ZRP (Zone Routing Protocol).

Ils existent d'autres types de protocoles de routage pour les réseaux ad-hoc :

- a) **Les protocoles géographiques** : ils utilisent des informations sur la position des nœuds (les coordonnées géographiques) pour établir les routes.
- **Avantage** : une réduction significative du trafic de contrôle.
 - **Inconvénient** : la réduction de l'espace de recherche des routes peut mener à un échec de la découverte de la route même si elle existe.
 - **Exemple** : le protocole LAR (Location-Aided Routing), DREAM (Distance Routing Effect Algorithm for Mobility), etc.
- b) **Les protocoles hiérarchiques** : ils sont adaptés aux réseaux ad-hoc ayant une taille importante et une gestion difficile. Ils consistent à partitionner le réseau en sous-ensembles afin de faciliter le routage.
- Exemple** : le protocole HSR (Hierarchical State Routing).

Considérant les divers domaines d'application des réseaux ad-hoc (MANETs), plusieurs types particuliers des réseaux MANETs ont été plus tard apparus pour s'adapter aux différentes exigences d'utilisation dans les différents domaines d'application. Les types les plus répondus sont détaillés dans la suite de ce chapitre.

4.3 Réseaux sans fil de capteurs (Wireless Sensor Networks, WSNs)

4.3.1 Pourquoi et comment ?

Récemment, il y a un besoin de plus en plus croissant pour de petits équipements qui sont capables de :

- Surveiller de grandes zones dans des endroits dangereux et/ou difficilement accessibles ;
- Fonctionner dans les conditions extrêmes ; et
- Collecter des données en temps réel, ainsi que collaborer et communiquer.

Suite à ce besoin, les avancées dans les domaines de la micro-électronique et des technologies sans-fil ont accéléré l'apparition de capteurs de petites tailles consommant peu d'énergie et qui sont capable de collecter, traiter et communiquer les données collectées. Quelques types de ces capteurs sont très robustes et peuvent opérer dans des conditions très difficiles [26].

Dans ce contexte, un nouveau type de réseau ad-hoc a vu le jour, communément connu sous le nom des réseaux de capteurs sans fil (RCSFs), plus souvent appelés WSNs pour Wireless Sensor Networks en anglais.

4.3.2 Définition

Les réseaux sans fil de capteurs communément appelés, WSNs pour Wireless Sensor Networks en anglais, sont un type particulier des réseaux ad-hoc MANETs composé d'un grand nombre de micro-capteurs qui sont [21, 26] :

- Éparpillés aléatoirement.
- Autonomes, auto-organisables et collaboratifs.
- Facilement et rapidement déployable avec un faible coût.
- Capable de capter et de traiter des données sur des grandeurs physiques (la chaleur, l'humidité, etc.) en temps réel.
- Capable de communiquer via différentes technologies sans fil (Bluetooth, Infrarouge, Zigbee, etc.).

4.3.3 Architecture

Comme il est illustré à la figure 4.3, un réseau de capteurs est principalement composé de deux types de nœuds [24, 26] :

- a) **Plusieurs nœuds de capteurs** : ils sont chargés de relever, collecter, analyser et transmettre des informations sur l'environnement vers le point de collecte aussi appelé puits ou (sink).
- b) **Le(s) puits (station de base ou sink)** : il(s) est(sont) responsable(s) de la collecte des informations à partir des capteurs et les transmettre au centre de traitement. Généralement, le puits est plus performant que les autres capteurs et il peut être fixe ou mobile, comme il peut être relié à Internet ou même contrôlé à distance.

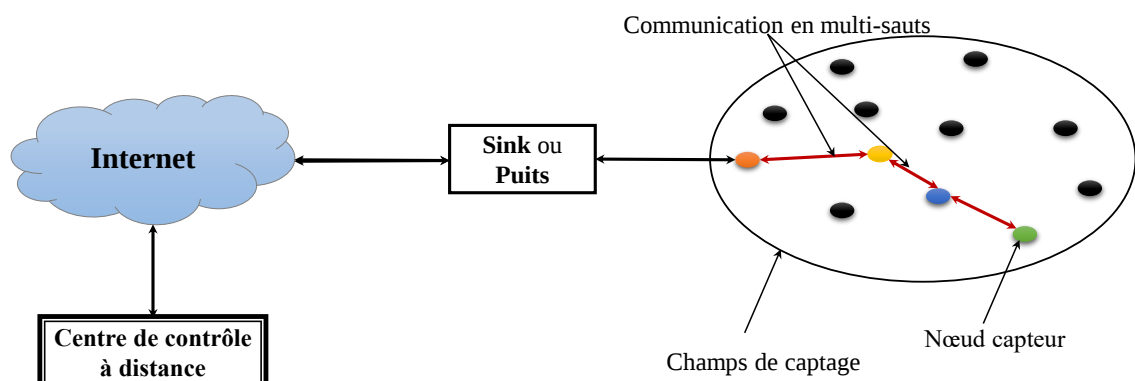


FIGURE 4.3 – l'architecture générale d'un réseau de capteurs sans fil [21].

Les capteurs sont disposés de manière aléatoire formant la zone de couverture (ou le champ de captage). Aussi, l'acheminement des données entre les nœuds de capteurs et le sink se fait en multi-sauts.

4.3.4 Architecture d'un nœud capteur

Un nœud capteur est composé essentiellement de quatre éléments de base [22, 23] :

- 1) **L'unité de captage ou d'acquisition (Sensing unit)** : elle est composée de deux sous-unités :
 - i) Un capteur : il collecte des mesures sur l'environnement (la température, la pression, etc.);
 - ii) Un convertisseur analogique-numérique (Analog to Digital Converter (ADC)) : il convertit l'information analogique en numérique et assure la transmission de cette dernière à l'unité de traitement.
- 2) **L'unité de traitement (Processing unit)** : elle est responsable de l'exécution des tâches. Elle est composée de :
 - i) Un microprocesseur avec un système d'exploitation à l'instar de TinyOS.
 - ii) Une unité de stockage qui représente la mémoire de capteur.
- 3) **L'unité de transmission (Transmission unit)** : elle est responsable de l'émission/réception des informations.
- 4) **L'unité d'énergie (Power unit)** : elle est responsable de l'alimentation de capteur en énergie.

Un capteur peut avoir d'autres éléments selon le type d'applications. Parmi ces éléments il y a :

- Un système de localisation : il utilise le système GPS (global positioning system) pour localiser le capteur.
- Un générateur d'énergie : comme par exemple les panneaux solaires.
- Un mobilisateur : il permet de déplacer le capteur.
- etc.

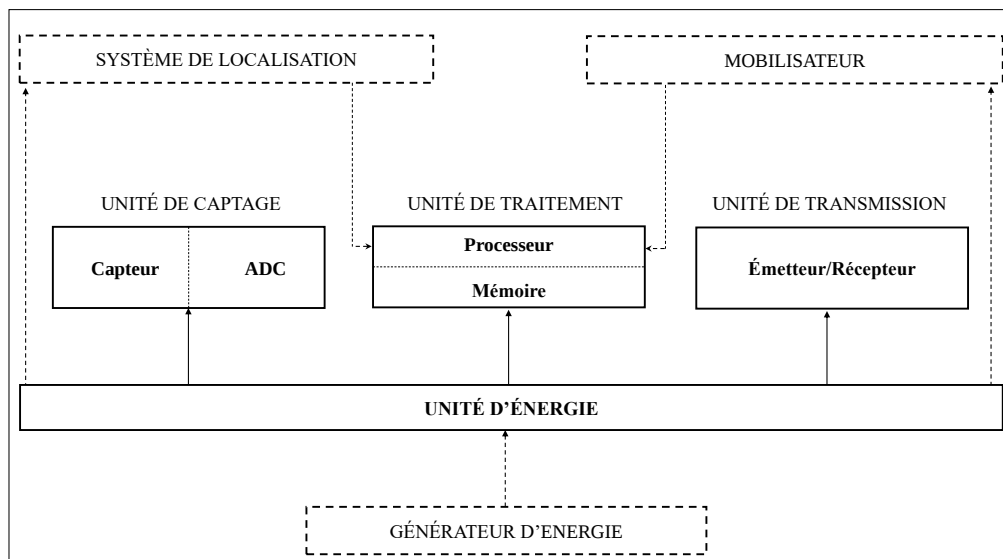


FIGURE 4.4 – l'architecture générale d'un nœud de capteur. [23].

4.3.5 Caractéristiques

Les réseaux de capteurs sont considérés comme un type particulier des réseaux MANETs et ils héritent de beaucoup de leurs caractéristiques. Cependant, ils possèdent des caractéristiques particulières, dont les plus importantes sont résumées dans les points suivants [25] :

- Un grand nombre de nœuds capteurs.
- Une auto-organisation, structuration et configuration.
- Une facilité et une rapidité de déploiement avec un faible coût.
- Une capacité de déploiement dans des milieux hostiles, difficiles et \ou inaccessibles.
- Une forte résistance aux conditions extrêmes avec une forte tolérance aux pannes.
- Une haute capacité de captage, grâce à la collaboration entre les capteurs.
- Une capacité limitée en énergie, stockage et calcul.
- Une durée de vie limitée.
- Une taille petite des capteurs.
- Un passage à l'échelle difficile face au grand nombre des nœuds capteurs.
- etc.

4.3.6 Modèle de communication en couches

Le modèle de communication des réseaux de capteurs est structuré en cinq couches traditionnelles de modèle OSI : la couche application, transport, réseau, liaison et physique. Il définit aussi trois plans de gestion : d'énergie, de la mobilité et de celui des tâches [23], voir la figure 4.5. Ce modèle fait la combinaison entre le routage, la gestion d'énergie et il favorise la coopération entre les nœuds.

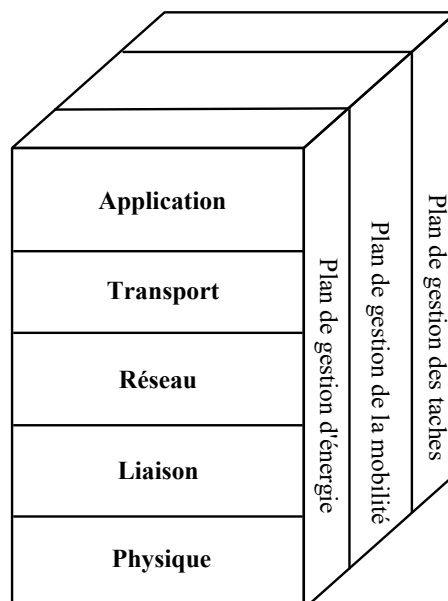


FIGURE 4.5 – le modèle de communication en couche de WSNs [23].

4.3.7 Topologie

Comme il est illustré à la figure 4.6, les topologies des réseaux de capteurs peuvent être classifiées en trois grandes catégories [21] :

- a) **La topologie en étoile** : dans cette topologie, une seule station de base centralise l'envoi/la réception et la collection des informations pour un ensemble de capteurs.
- b) **La topologie maillée** : dans ce type de topologie, tous les nœuds peuvent communiquer les uns avec les autres en utilisant des communications multi-sauts.
- c) **La topologie hybride** : dans ce type de topologie, les nœuds avec un niveau d'énergie plus élevé peuvent effectuer des communications multi-sauts quand les autres nœuds avec un niveau d'énergie moins élevé ne sont pas autorisés à faire de multi-sauts.

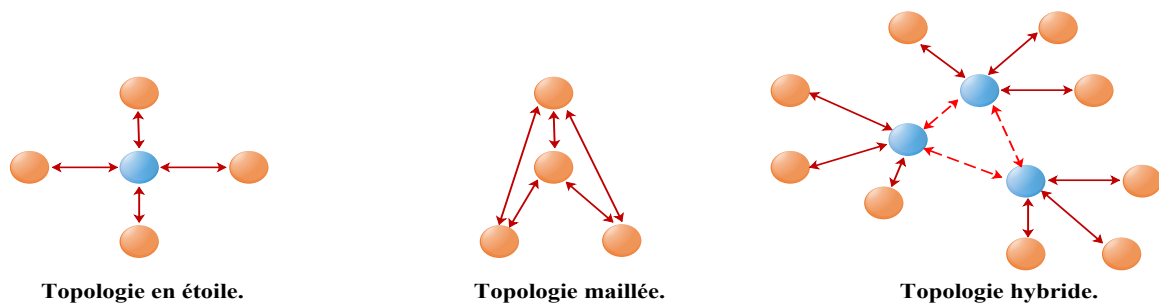


FIGURE 4.6 – les topologies d'un réseau de capteurs [21].

4.3.8 Méthodes de collecte d'informations

Dans un réseau de capteurs, il y a deux types principaux de méthode pour collecter les informations :

- a) **La collecte cyclique** : les nœuds chargés de la collecte des données transmettent des messages à des intervalles réguliers, après ils rentrent en veille afin de conserver leurs énergies.
- b) **La collecte à la demande** : la collecte et la transmission des données peuvent être déclenchées suite à :
 - Un évènement (event-driven) : une source ne transmet des données que lorsqu'un évènement est détecté, sinon elle reste en veille.
 - Une requête (on-demand) : la source ne transmet les données que lorsqu'un autre nœud va les demander, autrement elle reste toujours en veille.

4.3.9 Domaines d'applications

Les réseaux de capteurs ont connu de grands succès dans différents domaines. Les domaines les plus importants sont cités dans les points suivants [22–24] :

- Le secteur militaire : les capteurs sont utilisés pour la surveillance des champs de bataille, la détection d'agents chimiques, etc.

- La surveillance et la détection de l'environnement : les capteurs sont utilisés pour la détection et la signalisation des événements (la pression, la chaleur, l'humidité, etc.), la surveillance des volcans et des incendies, etc.
- La surveillance des structures : les capteurs sont utilisés pour surveiller les ponts et les tunnels, etc.
- Le transport : les capteurs sont utilisés pour la surveillance en temps réel de trafic et de l'état de la route, etc.
- La santé et le domaine médical : les capteurs sont utilisés pour la télésurveillance des données physiologiques des patients, le diagnostic des malades, etc.
- Le secteur agricole : les capteurs sont utilisés pour automatiser l'irrigation, surveiller le d'érosion du sol, localiser les animaux, etc.
- Les applications domestiques et commerciales.
- Les réseaux personnels ou corporels (Wireless body Area Network (WBAN)).
- etc.

4.3.10 Protocoles de routage

Les protocoles de routage des réseaux de capteurs peuvent être classés selon la structure de réseau, en trois grandes catégories [25, 26] :

- a) **Le routage à plat (Flat-based Routing)** : dans cette catégorie, tous les nœuds ont des rôles et des fonctionnalités égaux.
Exemple de protocole : SPIN, DD, etc.
- b) **Le routage hiérarchique (Hierarchical-based Routing)** : dans cette catégorie, les nœuds jouent des rôles différents dans le réseau.
Exemple de protocole : PEGASIS, APTEEN, etc.
- c) **Le routage géographique (Location-based Routing)** : dans cette catégorie, les positions des nœuds sont utilisées pour acheminer les données dans le réseau.
Exemple de protocole : Gear, etc.

Les protocoles de routage des réseaux de capteurs peuvent aussi être classés selon d'autres critères tels que la qualité de service, la multiplicité de chemins, etc.

4.3.11 Défis opérationnels

Ils existent plusieurs défis liés au déploiement des réseaux de capteurs. Parmi les contraintes les plus contraignantes ceux résumés dans les points suivants [21, 23] :

- **La tolérance aux pannes** : les capteurs sont vulnérables, limités en énergie et vivent dans des milieux hostiles.
- **Le passage à l'échelle** : les protocoles des réseaux de capteurs doivent être capables de supporter le grand nombre des capteurs.
- **Le coût de production** : principalement à cause de grand nombre de nœuds et la nature un peu jetable des capteurs.

- **Les contraintes liées aux matériels** : il faut bien équilibrer les fonctionnalités des capteurs avec les contraintes de coût.
- **La maintenance de la topologie de réseau** : il faut assurer une bonne maintenance de la topologie de réseau.
- **La résistance aux conditions de l'environnement** : les capteurs doivent pouvoir fonctionner de manière autonome dans des régions géographiques éloignées et des milieux difficiles.
- La collaboration distribuée face à l'hétérogénéité des capteurs et le traitement en temps réel des données.
- **L'optimisation de la consommation énergétique** : la plupart des défis des réseaux de capteurs tournent autour de la limitation des sources énergétiques principalement causée par la petite taille de capteur.

4.3.12 Comparaison entre WSNs et MANETs

Les réseaux de capteurs sont considérés comme un type particulier des réseaux MANETs. Pour cela, ils héritent de plusieurs points en commun. Cependant, ils possèdent des caractéristiques spécifiques qui les distinguent. Le tableau 4.1 donne un petit aperçu comparatif entre les deux types de réseaux ad-hoc :

	WSNs	<i>MANETs</i>
Nœuds	Petits micro-capteurs	Portables, PDA, etc.
Mode de communication	Plusieurs à un (many to one)	Plusieurs à plusieurs (many to many)
Communication	Diffusion /Aggregation	Point à point
Topologie	Mobilité faible	En constante évolution et mobilité forte
Relation entre les nœuds	Collaborer pour le même objectif	Chaque nœud à son propre objectif
Identification des nœuds	Très grand nombre de nœuds n'ayant pas tous une ID (data-centric)	Présence de la notion d'ID
Objectif du réseau	Objectif ciblé	Générique / communication
Contrainte clé	Ressource énergétiques	Débit /QoS

TABLE 4.1 – un tableau comparatif entre les réseaux WSNs et les MANETs.

Récemment, un autre type particulier des réseaux ad-hoc a submergé principalement propulsés par les longs embouteillages et les nombreux accidents de la route. Il s'agit bien des réseaux ad-hoc de véhicules qui ont émergé dans le but d rendre l'expérience de voyage plus agréable, la route plus sûre et le système de transport plus efficace.

4.4 Réseaux sans fil ad hoc de véhicules (Vehicular Ad hoc NETWORKs, VANETs)

4.4.1 Pourquoi ?

De nos jours, nous passons de plus en plus de temps dans les transports, que ce soit dans des véhicules personnels ou dans des transports en commun. Cela a vite causé une grande croissance du parc automobile ce qui a engendré de longs embouteillages et une forte augmentation du nombre d'accidents. De plus, nos usages des moyens de communication sont devenus de plus en plus nomades surtout avec les grandes avancées des technologies d'information et de communication (TIC).

Le concept des réseaux ad hoc de véhicules a donc vu le jour suite à cette évolution dans le but d'offrir une large variété de services, allant de l'amélioration de la sécurité routière à l'optimisation du trafic, en passant par le divertissement du conducteur et des passagers. En permettant la communication entre les véhicules et/ou entre les véhicules et l'infrastructure au bord des routes, le développement des réseaux de véhicules a contribué massivement dans le succès des systèmes de transports intelligents (STIs).

4.4.2 Définition

"Les réseaux ad-hoc de véhicules souvent appelés VANETs, pour Vehicle Ad-hoc NETWORKs, sont une technologie émergente déployée pour permettre la communication entre les véhicules mobiles les uns avec les autres par l'intermédiaire d'une communication véhicule à véhicule (Vehicle to Vehicle, V2V) aussi bien qu'avec l'infrastructure fixe au bord de la route par l'intermédiaire d'une communication véhicule à infrastructure (Vehicle to Infrastructure, V2I)" [27,58], voir la figure 4.7. Les réseaux de véhicules visent principalement à améliorer la sécurité sur les routes, le confort des voyageurs et l'efficacité de la gestion du trafic routier.

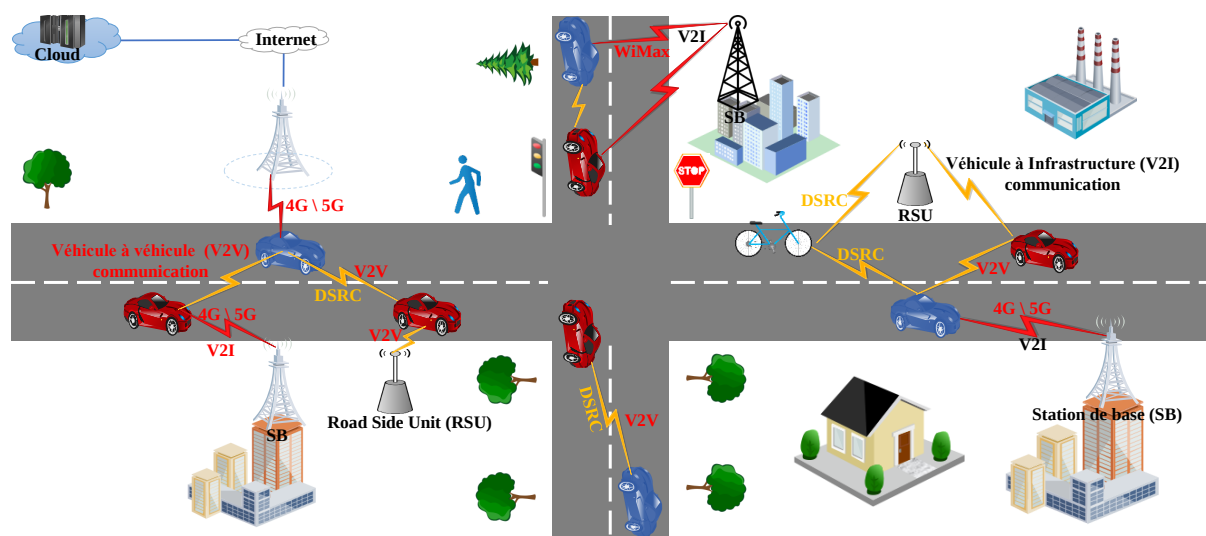


FIGURE 4.7 – un exemple illustratif d'un réseau ad-hoc de véhicules.

4.4.3 Composants

Un réseau de véhicules repose principalement sur trois éléments de base : les véhicules intelligents, les équipements à bord de véhicule et les équipements au bord de la route. En plus de la communication entre les véhicules [28].

- 1) **Les véhicules intelligents (Smart Vehicle)** : ils représentent des véhicules traditionnels équipés de différents types de capteurs et de technologies de communication. Des véhicules munis d'une capacité de calcul, de stockage et de communication.
- 2) **Les équipements à bord de véhicule (On Board Units, OBUs)** : ce sont des équipements mobiles (e.g., radars/ Lidars, capteurs, unité de calcul, etc.) installés sur les véhicules qui peuvent enregistrer/collecter, calculer, surveiller, localiser et envoyer des messages, etc.
- 3) **Les équipements au bord de la route (Road Side Unit, RSU)** : ce sont les équipements placés au bord des routes qui représentent l'infrastructure fixe du réseau. Ils jouent le rôle de station de base pour connecter deux véhicules éloignés, des organes de diffusion des informations sur les conditions du trafic, météorologiques ou de la route (la vitesse maximale, etc.).

En plus de ces trois éléments de base, il s'ajoute les équipements embarqués dans les véhicules qui représentent tous les terminaux et les appareils intelligents des passagers.

4.4.4 Véhicule intelligent (Smart Vehicle)

Un véhicule intelligent est un véhicule traditionnel équipé de différents systèmes embarqués et de technologies de communication sans fil, qui est capable de communiquer, collecter les informations, les stocker et / ou de les traiter. Sur un véhicule intelligent, on peut trouver :

- Des dispositifs de communication sans fil (WiFi, DSRC, Bluetooth, 5G, etc.).
- Des plateformes de traitement et de stockage et des systèmes d'aide à la conduite.
- Des capteurs de toute catégorie (Caméras, Capteurs, Radars, LiDAr, etc.).
- Des systèmes de localisation (GPS, etc.).
- etc.

4.4.5 Mode de communication

Dans les réseaux de véhicules, on peut distinguer principalement trois modes de communication [28, 29] : le mode avec infrastructure, le mode ad-hoc et le mode hybride, voir la figure 4.8.

- 1) **Le mode avec infrastructure** : dans ce mode, les véhicules communiquent de manière centralisée avec l'infrastructure fixe du réseau, c'est-à-dire, les RSUs, par l'intermédiaire d'une communication véhicule à infrastructure (Vehicle to Infrastructure, V2I).
- 2) **Le mode ad-hoc** : ce mode représente une architecture ad-hoc où les véhicules communiquent de manière distribuée directement les uns avec les autres par l'intermédiaire d'une communication véhicule à véhicule (Vehicle to Vehicle, V2V).
- 3) **Le mode hybride** : ce mode combine les deux premiers modes. Il utilise les communications V2V pour étendre la zone de couverture limitée des infrastructures au bord de la route.

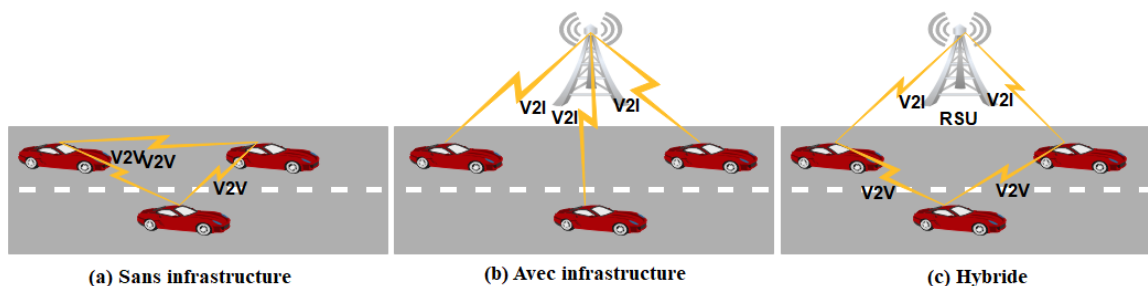


FIGURE 4.8 – les modes de communications dans les réseaux ad-hoc de véhicules [58].

4.4.6 Environnement de déploiement

Dans un réseau avec une topologie aussi large et dynamique comme celui des réseaux de véhicules, il y a différents environnements de déploiement et chaque environnement a ses propres caractéristiques. Ces environnements peuvent être classifiés principalement en trois grandes catégories : urbain, rural et autoroute.

- **Urbain** : ce type d'environnement se caractérise par une dense infrastructure routière (intersections, feux tricolores, stops, etc.), un modèle de mobilité complexe, une forte densité et une diversité de véhicules qui se déplacent généralement avec une vitesse réduite qui ne dépassent pas généralement 60 km/h. Il y a aussi une forte perturbation des ondes radio par les obstacles (les bâtiments, etc.).
- **Rural** : ce type d'environnement se caractérise par une vitesse moyenne de déplacement des véhicules, une faible densité et une difficulté de déploiement des RSUs.
- **Autoroute** : ce type d'environnement se caractérise par une forte vitesse de déplacement de véhicules qui est généralement à l'entour de 120 km/h, une forte densité et un coût élevé de déploiement des RSUs.

4.4.7 Applications

Les applications des réseaux de véhicules peuvent être classées en trois grandes catégories : les applications de sécurité, les applications de gestion du trafic routier et les applications du confort [28, 30, 31].

- **Les applications de sécurité** : cette catégorie d'application a comme principal objectif, l'amélioration de la sécurité des conducteurs et/ou des passagers sur les routes en avisant les véhicules de toute situation dangereuse afin de réduire le nombre des accidents sur les routes.
Exemple : les applications d'aide aux dépassements de véhicules, des alertes de freinage d'urgence, des avertissements de collision et d'accidents, etc.
- **Les applications de gestion de trafic routier** : ce type d'application vise à améliorer la fluidité de la circulation des véhicules, prévenir la congestion et garantir une utilisation efficace des capacités des routes dans le but de réduire les embouteillages.
Exemple : la surveillance du trafic, l'ordonnancement des feux de signalisation, la prédiction des embouteillages, la proposition des itinéraires alternatifs, etc.
- **Applications de confort ou divertissement** : cette catégorie d'application a comme principal objectif d'assurer aux usagers de la route un voyage convivial et agréable.

Exemple : les jeux en réseau, le partage de la musique et de la vidéo, les offres des restaurants, les annonces des hôtels et sites touristiques, le péage à distance, etc.

4.4.8 Caractéristiques et défis

Les réseaux de véhicules sont un type particulier des réseaux MANETs et ils héritent de la plupart de leurs caractéristiques et défis. Cependant, les réseaux de véhicules ont des caractéristiques spécifiques dont les plus importants sont résumés dans les points suivants [28,31] :

- Une forte mobilité et une topologie hautement dynamique du réseau.
- Une grande capacité de traitement, d'énergie et de communication.
- Un modèle de mobilité limité par l'infrastructure routière et un mouvement des véhicules prédictibles.
- Une évolutivité (scalability) à cause de la taille de réseau et la diversité de la densité.

Comme toute autre technologie les réseaux de véhicules font face à quelques défis dont les plus importants sont cités dans les points suivants [28,31] :

- Un risque de sécurité et d'anonymat.
- La dégradation de la qualité de service face à l'augmentation de nombre de véhicules et la variation de leurs vitesses.
- Le partitionnement de réseau faute de la faible densité des véhicules dans les zones rurales, et même le faible taux de pénétration des véhicules intelligents.

4.4.9 Technologies de communication

Pour satisfaire les exigences particulières des applications véhiculaires, de nombreuses normes ont été développées telles que la technologie DSRC (Dedicated Short-Range Communication), connue aussi sous le nom IEEE 802.11p, et le standard WAVE (Wireless Access in Vehicular Environment), appelé aussi IEEE 1609.x. Ces deux technologies sont considérées comme une adaptation de la technologie de WiFi (la couche MAC) pour supporter des communications à petite latence et aussi la forte vitesse de déplacement des véhicules. Plus récemment, il y a une nouvelle alternative de communication qui profite des avancées des nouvelles générations des réseaux cellulaires (4G et 5G) pour améliorer les communications inter-véhiculaires connues sous le nom de Cellular-Vehicular to Everything (C-V2X) [28].

Plus récemment, un autre type particulier des réseaux ad-hoc a vu le jour. Il s'agit des réseaux ad-hoc de drones qui se caractérisent principalement par une simple méthode de déploiement et un modèle de mobilité très fluide et flexibles.

4.5 Réseaux sans fil ad-hoc de drones (Flying Ad-hoc Networks, FANETs)

4.5.1 Pourquoi et quoi ?

Récemment, les grandes avancées dans le domaine de la robotique, les capteurs et les technologies de communication sans fil, ont accéléré la démocratisation de l'utilisation des mini-drones civils avec un faible coût. Ils ont aussi facilité l'apparition des nouvelles applications civiles des drones.

Un Drone ou système aérien sans pilote (Unmanned Aerial Vehicle, UAV), est un aéronef (avion) capable de voler sans pilote ni passagers à bord. Il se caractérise par un modèle de mobilité agile et flexible et un déploiement facile et rapide [32, 34].

Un réseau ad-hoc de drones communément appelé, FANETs pour Flying ad-hoc Networks en anglais, est composé d'un ensemble de drones permettant une grande mobilité qui communiquent et collaborent pour réaliser une mission commune [32, 33].

4.5.2 Anatomie d'un mini-drone

Comme il est illustré dans la figure 4.9, les principaux composants de base d'un mini-drone sont [40] :

- 1) **Le châssis** : il représente la base ou le squelette du drone.
- 2) **Le système de propulsion** : il est composé de :
 - a) **Un moteur** : il produit et fournit la puissance de rotation aux hélices.
 - b) **Les hélices** : elles produisent de la poussée.
 - c) **Les contrôleurs de vitesse électrique** : ils gèrent la vitesse, la direction et la rotation des moteurs.
 - d) **La batterie** : elle alimente en énergie les autres composants de drone. L'autonomie de la batterie détermine le temps de vol.
- 3) **Le contrôleur de vol** : il interprète les signaux et les convertit en actions qui permettent de régler la vitesse par exemple.
- 4) **L'immersion** : elle permet la prise de vue aérienne en temps réel. Le drone est équipé par :
 - a) **La charge utile** : Mini-caméra, émetteur vidéo, capteurs, etc.
 - b) **Le récepteur vidéo et l'appareil d'affichage de la vidéo** : des moniteurs LCD, smartphone, etc.

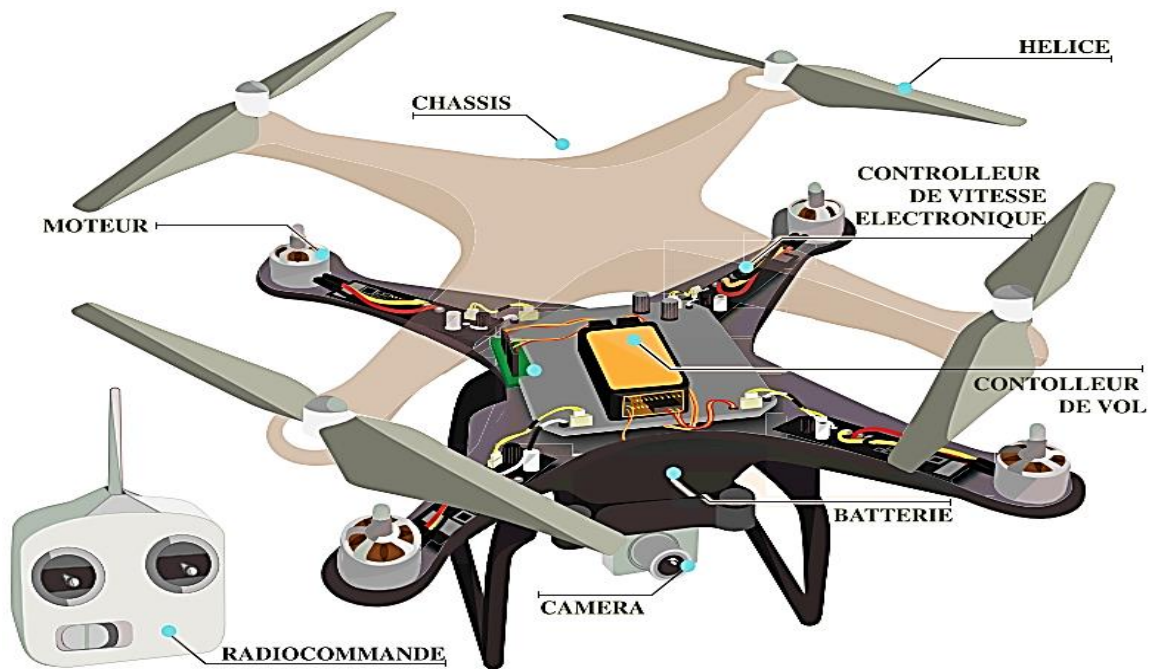


FIGURE 4.9 – l'anatomie d'un mini-drone [40].

4.5.3 Classification des drones

Les drones peuvent être classifiés selon la rotation des ailes (les voilures) en deux types [34,38,42] : drones avec des voilures fixes et drones avec des voilures rotatives (voir le tableau 4.2) :

	Aile-fixe	Aile-rotative
Mécanisme	Levée à l'aide d'ailes avec vitesse d'avancement.	Levée générée par des hélices tournant autour d'un axe de rotation.
Avantage	Structure plus simple, charge utile généralement plus importante, vitesse et altitude plus élevée.	Peut voler en stationnaire, peut se déplacer dans n'importe quelle direction, décollage et atterrissage vertical.
Limitation	Nécessité de maintenir le mouvement vers l'avant, besoin d'une piste pour le décollage et l'atterrissage.	Habituellement, chargement plus faible, vitesse plus faible, portée plus courte.

TABLE 4.2 – la classification des drones selon la rotation des ailes [34,38] .

Les drones peuvent être classifiés selon la méthode de contrôle en plusieurs types, voir le tableau 4.3 :

Pilotage humain à distance	Contrôle en temps réel par un pilote à distance.
Opérateur humain à distance	L'opérateur fournit les paramètres de vol permettant d'invoquer les fonctions intégrées pour le contrôle du drone.
Semi-autonome	Initiation et destination contrôlées par l'opérateur, exécution autonome des missions.
Autonome	Opération automatisée après initiation humaine
Contrôle par la flotte	Accomplissement coopératif de la mission par le contrôle des drones.

TABLE 4.3 – la classification des drones selon la méthode de contrôle.

4.5.4 Architecture typique

Comme illustré à la figure 4.10, une architecture typique des réseaux de drones doit contenir les éléments suivants [34, 38] :

- **La flotte de drones** : ils sont souvent équipés d'une charge utile (l'ensemble des systèmes embarqués qui lui permettent de réaliser sa mission (l'appareil photo, la caméra vidéo, les sondes, les capteurs, etc.)).
- **Les liens de communication sans fil** : le trafic de commande et de contrôle C2 (Control and Command) et celui de transfert des données.
- **La station de contrôle et/ou le centre de contrôle au sol** : c'est l'ensemble d'entités physiques et de logiciels qui permettent de contrôler le mouvement des drones.
- **L'équipement des utilisateurs** : il est muni d'une interface homme-machine qui permet de recevoir en temps réel les données captées.

Remarque : Certains types de drones ont besoin en plus d'un système de lancement pour le décollage.

4.6 Architecture de communication

Les drones dans les réseaux de drones peuvent communiquer en utilisant différents modes de communication [37, 38] :

- Une communication centralisée avec un seul centre de contrôle terrestre.
- Une communication en passant par une connexion via le satellite.
- Une communication en passant par les stations de base de réseau cellulaire.
- Une communication en multi-sauts en mode ad-hoc en passant de manière directe d'un drone à un autre.

4.6.1 Caractéristiques

En plus des caractéristiques héritées des réseaux MANETs, les réseaux de drones se caractérisent par les points suivants [33, 38, 42] :

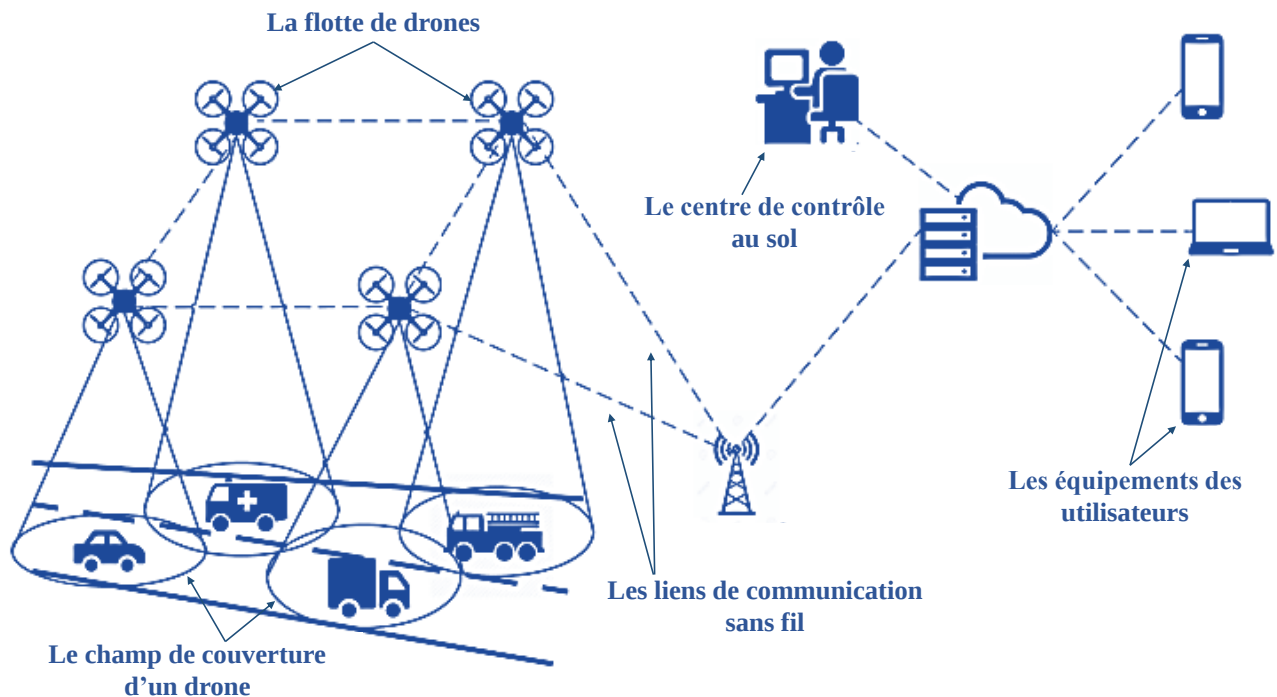


FIGURE 4.10 – un exemple de l'architecture typique d'un réseau de drones [39].

- L'agilité : la plupart de mini-drones n'ont pas besoin de piste ou de grande vitesse pour le décollage.
- Un déploiement dynamique, facile et rapide : les drones sont flexibles et peuvent être facilement déployés d'une manière dynamique en fonction des besoins en temps réel.
- La flexibilité : les drones peuvent atteindre un environnement hostile et/ou non accessible.
- Un vaste champ de couverture : elle est due à la capacité de voler en haute altitude et la vue dégagée de drone.
- Une transmission sans fil très fiable : ils existent peu d'obstacles dans le champ de transmission en plus de la capacité d'ajustement de la position de drone pour améliorer la fiabilité de la qualité de lien sans fil.
- La collaboration entre la flotte de drones : les drones sont une solution facilement réalisable pour récupérer ou établir un réseau de communication de manière très rapide et efficace.
- Un support aérien efficace : les drones peuvent fonctionner comme un support aérien pour l'infrastructure du réseau terrestre.
- Une utilisation plus sûre et sécurisée.

4.6.2 Principaux défis

Les réseaux de drones doivent faire face à un ensemble de défis dont les plus importants sont résumés dans les points suivants [35,38,41] :

- La connectivité intermittente : elle est principalement causée par la rapide vitesse de déplacement des drones, les conditions climatiques, etc.

- La faible densité des nœuds : un réseau de drones est généralement composé d'un nombre réduit de drones.
- La consommation énergétique : la durée de vie du réseau de drones dépend de l'autonomie de la batterie et de la consommation énergétique des différents capteurs.
- Le modèle de mobilité : il est le plus souvent prévisible, mais, dans la majorité des cas dynamiquement modifié à cause de la vitesse des drones, des conditions climatiques, géographiques et topographiques.
- L'environnement de déploiement : les drones circulent dans l'air libre.
- Les délais stricts : les flux de contrôle et de commande des réseaux de drones doivent arriver et être traités en temps réel par les drones afin d'éviter une perte de contrôle de l'aéronef et une meilleure gestion des applications en temps réel.
- La sécurité.
- Etc.

4.6.3 Applications

Les applications des réseaux de drones les plus connus sont résumées dans les points suivants [32, 35, 41, 42] :

- Les missions militaires.
- L'agriculture.
- Les missions de secours, de recherche dans les zones inaccessibles.
- L'inspection et l'entretien des grandes infrastructures.
- La cartographie et la topographie.
- La livraison des paquets.
- L'audiovisuel (la photographie aérienne, la cinématographie, etc.).
- La couverture omniprésente de réseau grâce aux drones.
- Le support aérien à l'infrastructure fixe terrestre des réseaux de communication.
- La connexion des segments isolés d'un réseau.
- L'accès à Internet.
- Etc.

4.6.4 Comparaison entre les réseaux de drones (FANETs) et les réseaux ad-hoc (MANETs)

Les réseaux de drones sont considérés comme un type particulier de MANETs. Le tableau 4.4 résume les principales différences entre les deux technologies :

	FANET	MANET
Mobilité des nœuds	très rapide	lente (suivant les nœuds)
Modèle de mobilité	modèles spéciaux	généralement aléatoire
Densité des nœuds	faible	forte (suivant le type d'application)
Modification de la topologie	rapide	lente
Modèle de propagation radio	en altitude	généralement au sol
Type de flux	temps réel	non-temps réel

TABLE 4.4 – une comparaison entre les réseaux FANETs et MANETs [32, 36].

4.7 Conclusion

Les réseaux ad-hoc offrent des solutions de communications sans fil auto-déployables pour fournir la mobilité là où le déploiement de l'infrastructure fixe est trop contraignant, non intéressant économiquement ou parce que la durée d'utilisation du réseau ne justifie pas la persistance du câblage.

Les réseaux ad-hoc ont connu un grand succès dans différents domaines d'applications et des adaptations de ces réseaux aux exigences particulières de différents domaines d'application ont très rapidement émergés. Depuis le temps, les réseaux de capteurs, les réseaux de véhicules et les réseaux de drones font les cas d'application des réseaux ad-hoc les plus avancés.

Avec la démocratisation de l'utilisation de l'Internet mobile et les grandes avancées dans les technologies de communications sans fil, de nouvelles générations des réseaux sans fil commencent à émerger avec des capacités très avancées. Les deux chapitres suivants détaillent les concepts de base de ces nouvelles générations des réseaux, autrement dit, les réseaux d'Internet de véhicules et les réseaux définis par logiciel.

CHAPITRE 5

INTRODUCTION À L'INTERNET DES OBJETS.

5.1 Introduction

Le grand progrès des technologies de communication, la démocratisation de l'utilisation de l'Internet mobile, l'augmentation exponentielle de nombre d'appareils connectés, en plus de l'évolution spectaculaire des technologies des micro-capteurs, ont contribué massivement à l'apparition et la prolifération de la technologie de l'Internet des objets (IdOs), plus connus sous l'acronyme de l'IoTs pour Internet of Things, en anglais.

La technologie de l'Internet des objets est une nouvelle ère d'Internet et elle est considérée comme le Web 3.0. Le terme IoT est apparu la première fois en 1999 dans un discours de *Kevin ASHTON* (un ingénieur britannique). En effet, elle offre une multitude de nouveaux services afin de rendre la vie de tous les jours plus facile et plus confortable. Cela passe par l'augmentation des différents objets du monde physique (un réfrigérateur, une montre, un bracelet, etc.) avec une certaine sorte d'intelligence (des capacités de calcul de stockage et de communication) qui exploite une diversité de données (la températures, la pression, etc.) et sont connectés entre eux grâce à une connexion Internet [43].

En général, l'Internet des objets fournit une sorte de jonction entre les objets de monde numérique, (c'est-à-dire, tous les systèmes manipulant des données numériques et les réseaux d'échange des données (e.g., les calculateurs, les microcontrôleurs, les serveurs, les bases de données, les réseaux)), et ceux du monde physique (c'est-à-dire, tous les systèmes vivants ou artificiels qui interagissent entre eux par divers effets physiques (e.g., les animaux, les végétaux, les véhicules, les objets du quotidien, etc.)) .

5.2 Définition

Il n'existe pas de définition standard et unifiée de l'Internet des objets. Cependant sémantiquement, l'Internet des objets est une expression composée de deux mots [45] :

- Internet qui représente le réseau mondial des réseaux informatiques interconnectés, et
- Objets qui désignent tout objet du monde physique non précisément identifiable.

Tandis que techniquement, l'IoT est un réseau mondial de réseaux composé d'un ensemble (milliers / millions) d'objets intelligents (physiques ou virtuels) du monde physique muni de capteurs, qui sont interconnectés via Internet, voir la figure 5.1. Chaque objet possède la capacité de récupérer, stocker, transférer et traiter les données s'y rattachant. Tout objet communique, peut être interrogé, envoie de l'information et interagit avec son environnement [43].

L'Internet des objets est considérée comme le future d'Internet et fournit un réseau omniprésent (ubiquitous network) qui permet à tout personne /objet de se connecter de n'importe où à n'importe quel moment avec n'importe quoi à travers n'importe quel chemin relié à Internet pour tout service, d'où la notation IoT = Anytime, Anywhere, Anyone, Anything [44].

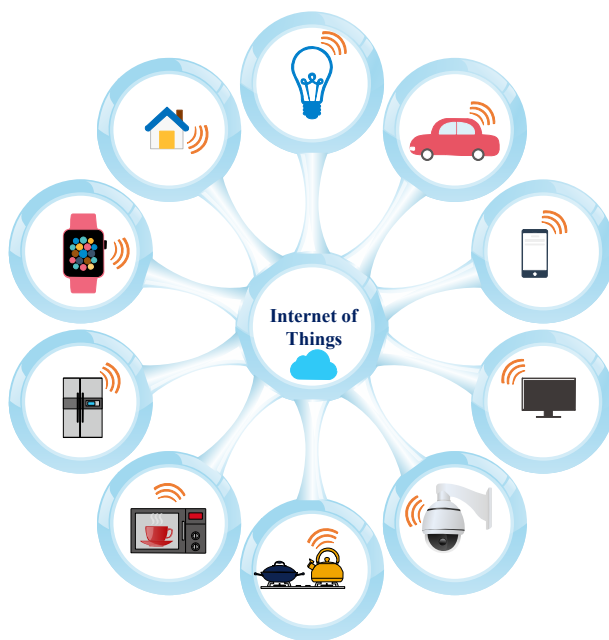


FIGURE 5.1 – l'Internet des objets.

5.3 Objet connecté

L'objet est considéré comme le composant élémentaire principal de la technologie d'Internet des objets. Cette section détaille les concepts de base des objets connectés.

5.3.1 Définition

Un objet connecté est tout dispositif intelligent (physique ou numérique) du monde réel capable de se connecter à Internet. Un objet connecté se caractérise par les points suivants [51] :

- Il est adressable de manière unique.
- Il possède la capacité d'interagir et d'échanger des données avec d'autres entités physiques ou numériques.

- Il a la capacité de collecter des informations sur l'environnement et de les envoyer via le réseau Internet.
- Il est autonome et peut agir sans l'intervention d'un tiers.
- Il peut être programmé et piloté à distance.
- Un objet physique possède des technologies embarquées (des capteurs intelligents).
- Les objets constituent un réseau généralement composé d'un nombre potentiellement élevé de nœuds.
- Les objets sont hétérogènes en termes de puissance de calcul, de stockage, de communication et d'énergie.

Quelques exemples d'objets connectés : la montre connecté, le bracelet connecté, la voiture connectée, la maison intelligente, l'être humain, etc.

5.3.2 Type

Les objets peuvent être classés selon le critère de la mobilité en deux grands types :

- i) **Les objets fixes** : ce type d'objet est statique et il ne change pas de position.
Exemple : la maison intelligente.
- ii) **Les objets mobiles** : ce type d'objet a la capacité de se déplacer et il change constamment sa position.
Exemple : le véhicule mobile, le smart phone, etc.

5.3.3 Défis

Les objets connectés souffrent de plusieurs défis tels que les problèmes liés à [51] :

- La sécurité.
- La mobilité.
- La robustesse.
- Les ressources limitées (en termes d'énergie, de stockage et de traitement).
- Etc.

5.3.4 Interaction

Les objets sont capables d'interagir de manière autonome les uns avec les autres et aussi avec leur environnement comme :

- i) **Des capteurs** : ils permettent de recueillir des informations depuis le monde physique et de les transmettre vers le système informatique.
Exemple : un capteur de température, de vitesse ou de l'humidité.
- ii) **Les actionneurs** : ils permettent au système informatique d'agir en exécutant des actions sur le monde physique (les objets) en modifiant son état.
Exemple : un actionneur peut allumer un appareil à distance.

5.3.5 Architecture matérielle

Comme il est illustré à la figure 5.2, un objet connecté est généralement composé de :

- L'unité de traitement : un microprocesseur (Arduino, Raspberry, etc.).
- L'unité de communication : une interface de réseau, le plus souvent sans fil et reliée à Internet.
- L'unité de stockage : une mémoire de stockage.
- L'unité de perception : l'ensemble des capteurs.
- L'unité d'énergie : une source passive (comme la batterie) ou une source active (l'énergie à partir d'un autre élément (comme la technologie NFC pour Near Field Communication)).

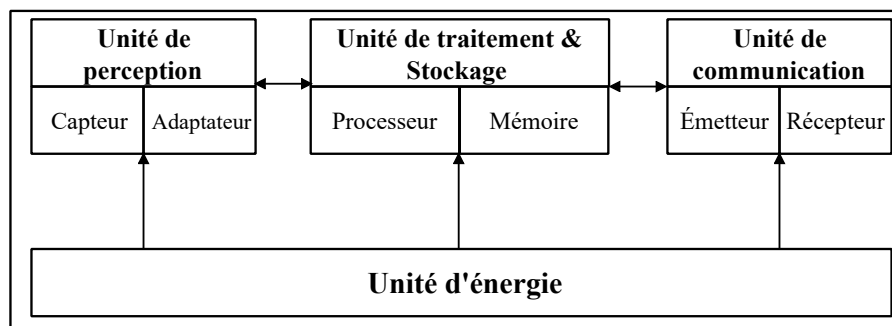


FIGURE 5.2 – l'architecture matérielle d'un objet.

5.4 Composants

Un système d'Internet des objets s'articule autour de 7 composants essentiels qui sont [53] :

- 1) **Les objets** : ce sont tous les équipements (les capteurs) pouvant générer et capter des données exploitables pour les utilisateurs.
- 2) **Les capteurs** : un dispositif intelligent qui transforme une grandeur physique à une information numérique.
- 3) **Le réseau** : il permet l'interconnexion des objets et la transmission des données en utilisant différentes technologies de communications telles que : M2M (Machine-to-Machine), LoRA, SigFox, RFID, Bluetooth, 3G/4G, etc.
- 4) **Les données** : il s'agit essentiellement des éléments récoltés depuis les objets.
- 5) **Les informations** : ils sont souvent le résultat de traitement et de l'analyse des données.
- 6) **Les applications d'exploitation** : il s'agit de l'ensemble des IHM (Interfaces Homme-Machine) pour visualiser les données.
- 7) **L'intelligence** : les outils qui améliorent la capacité à décrire, prédire, traiter et exploiter les informations captées. Cette composante est souvent déployée dans le Cloud.

5.5 Modèle de référence

Cisco Systems a proposé en 2014 un modèle de référence pour l'Internet des objets en sept couches hiérarchiques, voir la figure 5.3. Chaque couche correspond à un niveau d'abstraction d'une fonction particulière dans le processus de traitement. Le modèle de référence a pour but de bien définir la méthode suivant laquelle les différents composants de l'Internet des objets interagissent entre eux [46]. Les détails des couches sont résumés dans les points suivants :

- **Niveau 1 (la couche des dispositifs physiques et des contrôleurs)** : ce sont les "objets" de l'IoT qui collectent, envoient et reçoivent des données. Ainsi que les contrôleurs pour gérer ces objets. Un contrôleur peut contrôler plusieurs objets.
- **Niveau 2 (la couche de la connectivité et la communication)** : cette couche s'occupe de la transmission fiable et opportune de l'information, soit : (i) entre les objets (de niveau 1) et le réseau, (ii) entre le réseau (de niveau 2) et le traitement des informations de niveau 3, ou (iii) à travers divers types de réseau.
- **Niveau 3 (la couche d'edge computing)** : cette couche est responsable de l'analyse sur place de grands volumes de données ainsi que leurs transformations en informations appropriées pour le stockage et le traitement au niveau 4.
- **Niveau 4 (la couche d'accumulation des données)** : cette couche assure la conversion des données en mouvement dans le réseau en données dit « au repos » ou « en veille » qui seront stockés par la suite sur des mémoires ou sur des disques. Ces données peuvent être utilisées après par des applications en temps réel.
- **Niveau 5 (la couche d'abstraction des données)** : le principal rôle de cette couche est axé sur l'abstraction et le rendement des données à travers un stockage de manière qui à permettre le développement d'applications plus simples et plus performantes.
- **Niveau 6 (la couche application)** : cette couche représente l'endroit où l'interprétation de l'information se produise en se basant sur les données au repos de niveau 5.
- **Niveau 7 (la couche collaboration et processus)** : dans cette couche, les personnes communiquent et collaborent en utilisant différents processus pour produire des actions de valeur. Elle permet aux personnes de mieux faire leur travail en leur fournissant les bonnes données (de niveau 6), au bon moment, afin qu'ils puissent prendre la bonne décision.



FIGURE 5.3 – le modèle de référence de l'Internet des objets selon CISCO [46].

Remarque : il est important de noter que dans l'Internet des objets, les données circulent dans les deux sens. Dans un modèle de contrôle, les informations de contrôle circulent à travers un flux descendant du haut du modèle (niveau 7) vers le bas (niveau 1). Dans un modèle de surveillance, le flux d'informations est un flux montant (de la couche 1 à la couche 7). Dans la plupart des systèmes, le flux sera bidirectionnel [46].

5.6 Domaines d'applications

L'Internet des objets fournit une diversité d'applications et de services innovants dans différents domaines, dont les plus importants sont cités dans les points suivants [43,45] :

- La domotique (Smart Home) : IoT est utilisée dans,
 - ✓ Le contrôle à distance des appareils domestiques et les systèmes de détection d'intrusion.
 - ✓ La surveillance de la consommation d'énergie et de l'eau.

- Les villes intelligentes (Smart Cities) : IoT est utilisée dans,
 - ✓ La gestion intelligente de l'éclairage public et la consommation de l'énergie.
 - ✓ La gestion de circulation, le stationnement, la logistique et le transport.
- L'industrie du futur (Industrie 4.0) : IoT est utilisée dans,
 - ✓ La commande intelligente des moyens de production et approvisionnements.
 - ✓ La maintenance prédictive et la gestion automatisée des alertes.
- La cyber-santé (Smart Health) : IoT est utilisée dans,
 - ✓ La télésurveillance des patients et les soins à distance.
 - ✓ Le contrôle et le suivi des signes cliniques (la tension, le rythme cardiaque, etc.).
- L'agriculture intelligente (Smart Agriculture) : IoT est utilisée dans,
 - ✓ Le contrôle de l'humidité et des niveaux de température.
 - ✓ L'arrosage automatique intelligent et l'épandage d'engrais.
- Le transport et la logistique : IoT est utilisée dans,
 - ✓ L'optimisation de flux de trafic et l'optimisation des tournées de livraison.
 - ✓ La détection et la signalisation des incompatibilités de stockage.
- Les environnements intelligents : IoT est utilisée dans,
 - ✓ La prédiction des séismes et la détection d'incendies.
 - ✓ La surveillance de la qualité de l'air et les glissements de terrain.
- Les compteurs intelligents : IoT est utilisée dans,
 - ✓ La surveillance de la pression et des fuites de l'eau, les niveaux des réservoirs.
 - ✓ La grille intelligente et la gestion intelligente de la consommation d'énergie.
- Etc.

5.7 Caractéristiques

Les principales caractéristiques des réseaux d'Internet des objets sont résumées dans les points suivants [50] :

- Une auto-organisation et une auto-adaptation.
- Une structure flexible et dynamique des objets.
- Un mode de fonctionnement orienté événement (event-driven).
- Une disponibilité omniprésente de la connexion et de l'intelligence.
- Une grande hétérogénéité des objets, des technologies et des protocoles.
- Une architecture maillée avec un grand nombre d'objets connectés.
- De petits objets de monde physique largement distribués.
- Un contrôle instantané en temps réel dans des systèmes très complexes.
- Une capacité de stockage et du traitement limitée.
- Une diversité des domaines d'applications (smart city, industry 4.0, smart Health, etc.).

5.8 Défis

Comme toute nouvelle technologie, les réseaux d'Internet des objets font face à de nombreux défis, dont les plus importants sont décrits dans les points suivants [49, 52] :

- Une gestion complexe et une difficulté de la standardisation et de la normalisation face à la diversité des objets et l'hétérogénéité des technologies de communication.
- Des contraintes de sécurité et de confidentialité.
- Une difficulté pour supporter l'évolutivité, garantir la disponibilité et la tolérance aux pannes.
- La difficulté de l'interopérabilité pour faciliter la communication des différents objets et technologies.
- Une connectivité de bout en bout difficile face aux variétés des normes et technologies de communication.
- L'absence de la gouvernance centralisée et la difficulté d'assurer une connexion Internet omniprésente.
- Un coût de mise en œuvre élevé pour déployer un grand nombre d'objets avec un faible coût.
- La difficulté pour gérer l'énorme nombre et volume des données générées par les objets qui nécessitent souvent des calculs intensifs.
- Des capacités de calcul et de stockage limitées des objets connectés.

Le paradigme de Cloud Computing est présenté comme une solution prometteuse pour assister l'Internet des objets à surmonter un nombre non-négligeable parmi les défis précédents.

5.9 Cloud / Edge (Fog) Computing

5.9.1 Cloud Computing

Le paradigme de Cloud computing consiste à fournir de puissantes ressources informatiques de calcul et/ou de stockage à la demande pour des utilisateurs distants via Internet grâce à des serveurs distants, voir la figure 5.4. Le Cloud computing permet d'améliorer le travail collaboratif, la souplesse, la disponibilité et la réduction des coûts, etc. Cependant, il souffre d'un temps de réponse (délai de latence) élevé et il est moins adapté pour les applications sensibles aux délais, faute des serveurs distants [47], [48].

Une des solutions les plus prometteuses pour réduire les délais de réponse est l'Edge computing.

5.9.2 Edge / Fog computing

Le paradigme d'Edge computing consiste à déplacer les capacités du Cloud computing (calcul et/ou stockage) à la périphérie du réseau (au niveau de réseau d'accès), dans les emplacements les plus efficaces entre les objets connectés et le Cloud, voir la figure 5.5. Il vise à réduire le temps de réponse et la latence de Cloud. En plus de réduire le trafic des données sur les liens de

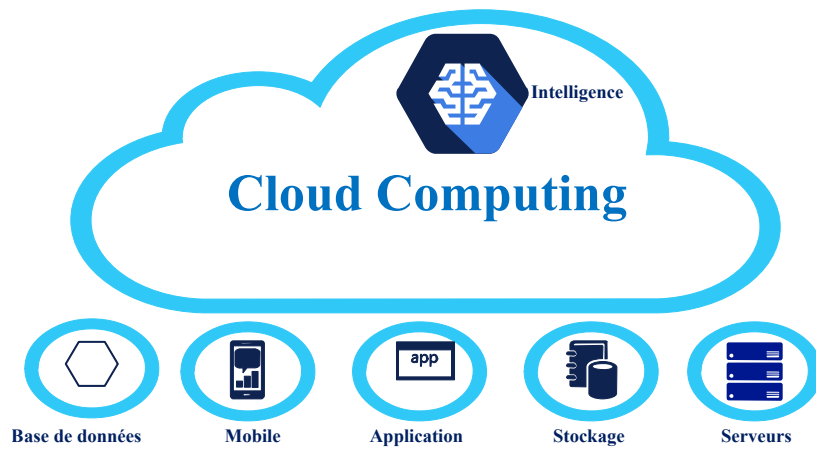


FIGURE 5.4 – le concept de Cloud computing.

réseau cœur [47], [48].

Elle existe une technologie similaire à celle d'Edge computing, connue sous le nom de Fog computing avec comme principale différence entre les deux technologies, l'endroit où les données sont traitées. En effet, dans la technique de Fog computing, les données sont transférées pour être traitées sur des serveurs à la périphérie de réseau. Tant dit que dans celle d'Edge computing, les données sont traitées en local par les objets connectés [47], [48].

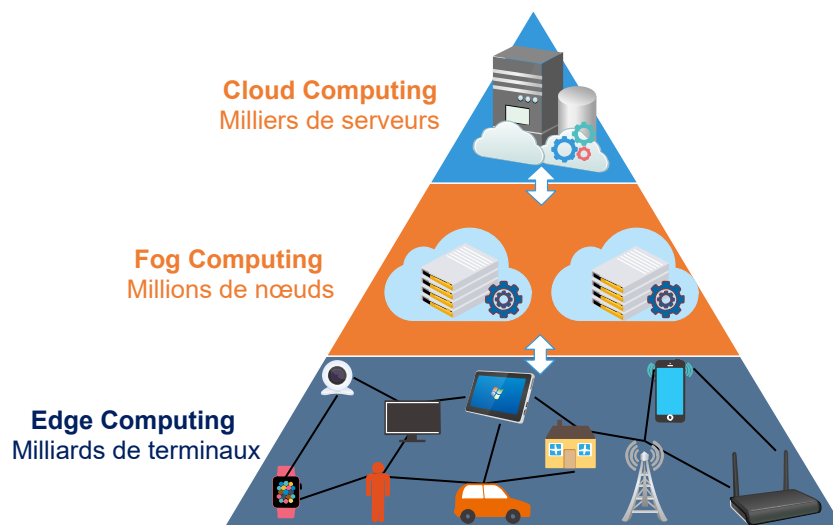


FIGURE 5.5 – le concept d'Edge / Fog computing [48].

5.10 Conclusion

L'Internet des objets est considéré comme la troisième évolution de l'Internet qui construit pour un monde où tout objet physique sera connecté et doté d'une certaine intelligence. L'IoTs fournit plusieurs services innovants avec des capacités avancées. Cependant, la démocratisation de cette technologie doit faire face à plusieurs défis tout en particulier l'énorme quantité des données générées par les capteurs, les nouvelles exigences des services connectés en terme de débit et de délai et les capacités limitées des réseaux traditionnels.

Dans le chapitre suivant, nous présentons les concepts fondamentaux des réseaux définis par logiciel (Software Defined Networking, SDN).

CHAPITRE 6

RÉSEAUX DE NOUVELLES GÉNÉRATIONS (LES RÉSEAUX DÉFINIS PAR LOGICIEL).

6.1 Introduction

Les architectures des réseaux traditionnelles souffrent d'un manque d'intelligence de programmabilité à cause de l'aspect propriétaires et non-programmable (fermé) des équipements qui dépendent des fournisseurs en développement. En plus de l'hétérogénéité des fabricants des équipements (Cisco, Juniper, Huawei, etc.). Cela a engendré des réseaux rigides qui sont difficilement modifiables et peu évolutifs [56].

En plus, ces réseaux souffrent d'un manque de flexibilité, d'adaptabilité et de scalabilité faute de la grande diversité des protocoles et multiplicités des solutions. Aussi, il est difficile de gérer et de configurer un réseau de grande taille avec un nombre élevé des équipements hétérogènes. En effet, il faut accéder et configurer chaque équipement de réseau individuellement. Les architectures des réseaux traditionnels sont donc difficiles à gérer et coûteuse à administrer. Ce qui va limiter les fonctionnalités du réseau, ralentir la créativité et entraîner la sous-exploitation des ressources [57].

De nouvelles architectures plus flexibles et évolutives sont plus que nécessaires pour affronter les défis des nouvelles générations des réseaux. Dans ce contexte, les réseaux définis par logiciel (software-defined networking) ont émergé comme une solution prometteuse pour surmonter les problèmes des réseaux traditionnels.

6.2 Architecture de contrôle d'un équipement de réseau

L'architecture de contrôle d'un équipement dans les réseaux traditionnels est composée de trois plans ou couches [55] (voir la figure 6.1) :

- 1) **Le plan de gestion (Management Plane)** : il représente l'ensemble des méthodes et des protocoles qui permettent d'accéder (physiquement ou à distance) et de configurer un équipement. Par exemple, le protocole Telnet et SSH.



FIGURE 6.1 – l'architecture traditionnelle d'un équipement de réseau [55].

- 2) **Le plan de contrôle (Control Plane)** : il représente l'intelligence de l'équipement (le cerveau) qui regroupe toutes les fonctionnalités et les protocoles responsables de la gestion et la prise de décision. Comme par exemple les protocoles de routage à l'instar d'OSPF et RIP.
- 3) **Le plan de données (Data Plane)** : il regroupe les fonctionnalités et les protocoles qui assurent la transmission / la réception des données et l'exécution des décisions du plan de contrôle comme par exemple les tables de routage.

Remarque : un "plan ou une couche" en réseau est une conception abstraite de l'endroit où se déroulent certains processus.

6.3 Vers des réseaux définis par logiciel (Software-Defined Networking)

6.3.1 Définition

Software-defined networking (SDN) ou les réseaux définis par logiciel est une nouvelle architecture émergente de réseau qui est basée sur deux concepts de base [59], voir la figure 6.2 :

- Une séparation physique entre le plan de contrôle, c'est-à-dire, l'ensemble des fonctionnalités intelligentes qui décident comment gérer le réseau, et le plan de données, c'est-à-dire, les fonctionnalités de réseau qui gèrent le traitement et l'acheminement des paquets.
- Une intelligence du réseau logiquement centralisée dans un (des) contrôleur(s) logiciel(s). Les autres équipements de réseaux deviennent peu intelligents et gèrent uniquement la transmission / réception des paquets et la surveillance des paramètres locales.

SDN permet des réseaux plus intelligents, faciles à gérer, flexibles, ouverts et programmables. SDN est considéré comme le socle des futures architectures des nouvelles générations des réseaux informatiques.

6.3.2 Architecture logique de SDN

L'ONF¹ (Open Networking Fondation) [62] a défini une architecture hiérarchique en trois couches pour les réseaux SDN [60], voir la figure 6.3 :

1. ONF est une fondation d'industriels (Facebook, Cisco, etc.) réunis pour promouvoir des équipements compatibles avec SDN afin de faciliter sa commercialisation.

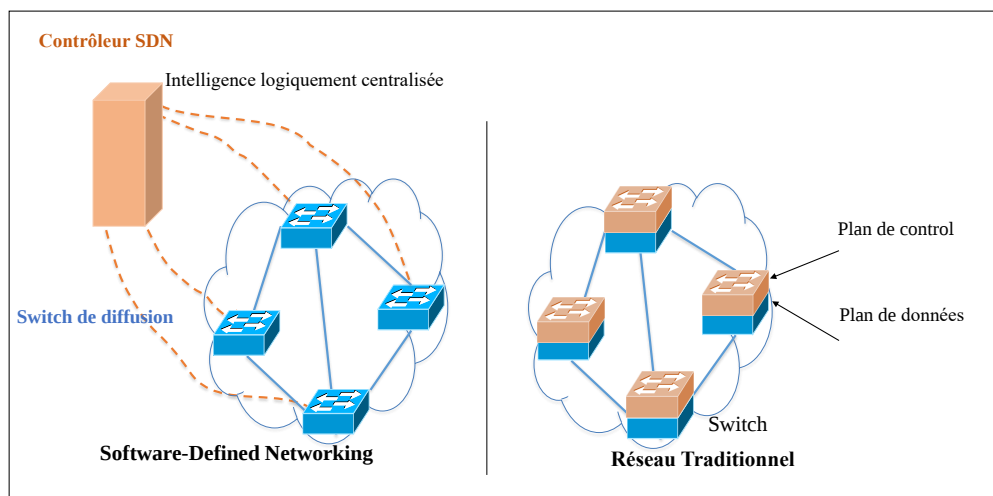


FIGURE 6.2 – l’architecture des réseaux traditionnels vs. software-defined networking [54].

- 1) **Le plan d’application** : il se compose des applications de l’utilisateur final.
- 2) **Le plan de contrôle** : il s’agit de(s) contrôleur(s) intelligent(s) de réseau qui décide(ent), contrôle(ent), programme(ent) et supervise(ent) le comportement des équipements du plan de données grâce à une interface ouverte à l’instar d’OpenFlow.
- 3) **Le plan de données** : il s’agit des équipements qui assurent la transmission des paquets. Il est responsable du transfert des données, la surveillance et la collecte des statistiques locales.

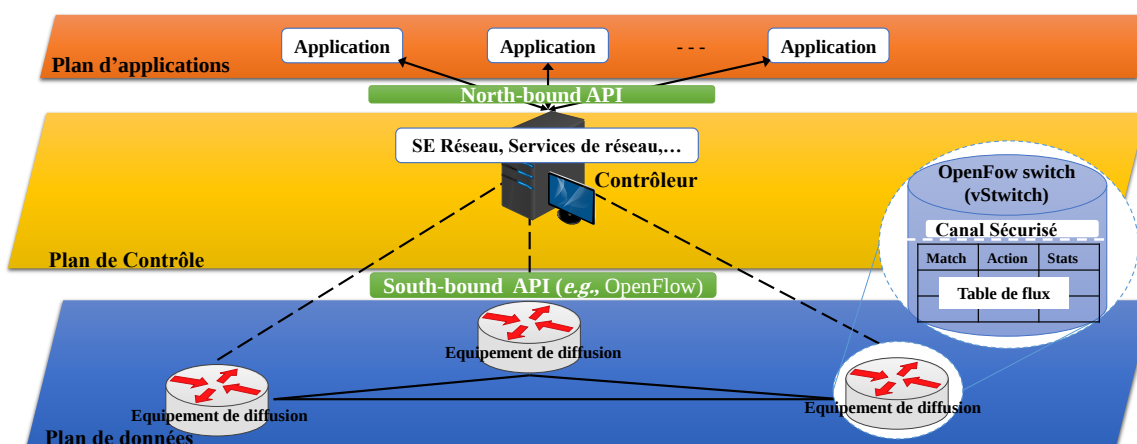


FIGURE 6.3 – l’architecture logique de SDN [58].

SDN utilise des interfaces ouvertes et standardisées sous-forme d’API (Application Programming Interface) pour permettre la communication entre les différents plans d’abstraction. En effet il y a les interfaces suivantes [60] :

- a) **North-bound API** : elle permet la communication et l'échange des données entre le contrôleur SDN sur le plan de contrôle et les applications du réseau. Il n'y a pas de standardisation pour cette interface.
- b) **South-bound API** : elle permet la communication entre les composants de plan de contrôle et ceux du plan de données. OpenFlow [61] est le standard SDN le plus utilisé pour les communications de cette interface.

OpenFlow définit deux types d'équipements du réseau [58] :

- a) **Le contrôleur OpenFlow** : un logiciel (une virtuelle machine) qui centralise toutes les fonctions de contrôle du réseau ;
- b) **L'OpenFlow vSwitch (OF Switch)** : qui s'occupe uniquement de transfert des paquets. Chaque vSwitch possède une table de flux contenant des entrées de flux du contrôleur.

Le contrôleur gère les vSwitchs en installant des règles de flux dans la table de flux via un canal sécurisé.

6.3.3 Apports de SDN

SDN promet de révolutionner la méthode de gestion et de contrôle des réseaux informatiques en apportant les avantages suivants [57] :

- Faciliter une gestion efficace et rapide du réseau : SDN permet de simplifier l'architecture de réseau et une configuration plus rapide du réseau.
- Exploiter plus efficacement les ressources, faciliter le passage à l'échelle et réduire les coûts : SDN utilise la vue globale en temps réel du contrôleur SDN pour identifier l'état actuel du trafic et rendre l'allocation des ressources plus efficace. Aussi que déployer les solutions les plus appropriées selon le contexte et les conditions de réseau en temps réel.
- Accélérer l'innovation et introduire de nouveaux services plus avancés : cela grâce à la programmabilité et les interfaces de communication unifiées de SDN. En effet, les équipements seront configurables avec des logiciels indépendants des fournisseurs.
- Mieux supporter l'abstraction, l'hétérogénéité et le découpage de réseau : cela grâce à la virtualisation des fonctionnalités et l'abstraction des interfaces de communications. En effet, le contrôleur peut créer plusieurs réseaux virtuels sur la même infrastructure physique.
- Améliorer les services de sécurité et réagir plus rapidement aux situations d'urgence : SDN est plus flexible et permet de réagir plus rapidement aux situations d'urgence.

6.3.4 Principaux défis

SDN doit faire face à un certain nombre de défis techniques et fonctionnels. Parmi les défis les plus importants il y a [57] :

- Le manque de sécurité.
- La standardisation.
- Le coût de déploiement.
- La fiabilité.
- Le passage à l'échelle (Scalability).

6.3.5 Domaines d'applications

Dans les dernières années, SDN a connu énormément de succès que ce soit dans le domaine académique ou dans l'industrie. En effet, SDN a été implémenté dans la plupart des nouveaux réseaux à l'instar de la 5G, comme il a été adopté par la quasi-totalité des fournisseurs des équipements et des équipements compatibles avec SDN sont disponibles actuellement sur le marché à l'instar de Cisco ACI comprises Cisco Nexus Switches from the 9000 Series et Huawei Agile Controller 3.0 (AC 3.0).

- **Académiques** : il a été développé initialement pour les réseaux filaires de campus. SDN a été massivement appliquée dans divers domaines [59] : les data-centers, smart transportation, network slicing, Cloud, les réseaux d'entreprises, WANs publique, réseaux cellulaires, etc. Aussi pour différentes problématiques comme l'équilibrage de charge des serveurs, la virtualisation des réseaux, energy-efficient networking, etc.
- **Industries** : les grands fournisseurs et fabricants des équipements de réseau à l'instar de Cisco, HP, Juniper et VMware, ont commencé à commercialiser des équipements compatibles avec SDN/OpenFlow. Google, par exemple, a déployé un SDN pour interconnecter ses centres de données à travers le monde. Ce réseau a permis à l'entreprise d'améliorer son efficacité opérationnelle et à réduire considérablement les coûts [59].

SDN est considéré comme une des technologies les plus prometteuse et fondamentales. Parmi les applications les plus connues de SDN déjà déployées actuellement, il y a la technologie de Network Function Virtualization (NFV) et celle de Software-defined WAN (SD-WAN).

6.4 Network Function Virtualization (NFV)

La technique de virtualisation des fonctions de réseaux (NFV) est considérée comme un des cas d'utilisation de la technologie de SDN dans le domaine des fournisseurs de services.

6.4.1 Pourquoi NFV ?

Dans les architectures des réseaux traditionnels, chaque fonction de réseau est exécutée sur un équipement matériel propriétaire et dédié. Ce qui rend la gestion de réseau difficile avec un coût élevé en termes de ressources.

Une solution prometteuse propose de séparer et de découpler les fonctions de réseau des matériels propriétaires et dédiés. Cette solution est connue sous le nom de NFV ou network function virtualization (la virtualisation des fonctions de réseau).

6.4.2 Définition

NFV est une nouvelle technologie d'abstraction des réseaux qui s'appuie sur les techniques de la virtualisation, le Cloud et le paradigme de SDN pour découpler les fonctions de réseau du matériel propriétaire et dédié. Les services de réseaux seront des logiciels qui s'exécutent sous forme de machines virtuelles (VMs) sur du matériel standard [63], voir la figure 6.4.

Exemple de service : les routeurs, les pare-feu, les équilibreurs de charge, etc.

Remarque : NFV est lancé en 2012 par le groupe de travail ISG de ETSI ISG (European Telecommunications Standards Institute) pour réduire les coûts de l'infrastructure matériel du réseau.

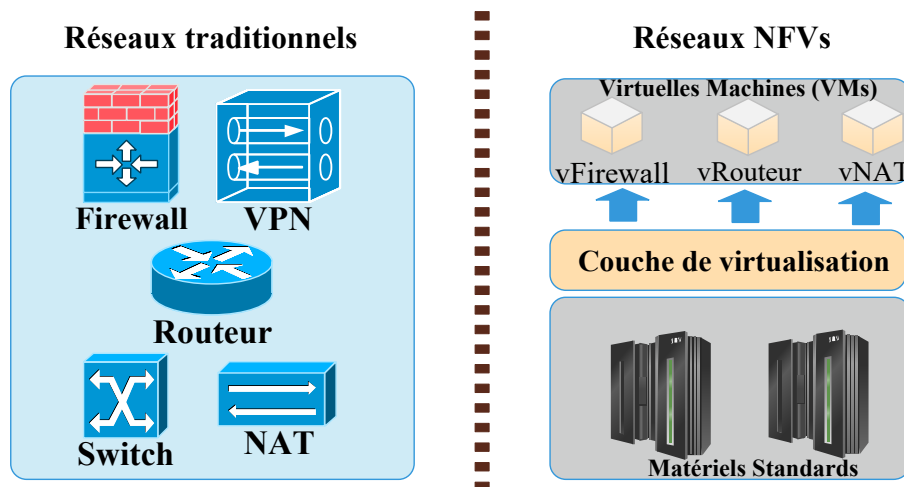


FIGURE 6.4 – l'architecture des réseaux traditionnels vs. l'architecture des réseaux NFVs [64].

6.4.3 Architecture

ETSI a défini une architecture hiérarchique pour le NFV de trois couches [65] :

- 1) **Les fonctions virtualisées de réseau (Virtual Network Function, VNF)** : elle représente les virtuelles machines des fonctions de réseau.
- 2) **L'infrastructure de NFV (NFV Infrastructure, NFVI)** : ce sont les ressources matériels/ logiciels (calcul, stockage, communication) où les VNFs sont exécutés. Exemple de serveur standard : COTS (Commercial Off The Shelf).
- 3) **La plateforme de gestion, d'automatisation et d'orchestration du réseau (NFV Management Orchestration, MANO)** : elle représente les fonctionnalités qui permettent de gérer les fonctions de réseau de bout en bout. Elle gère aussi les ressources de l'infrastructure NFVI (le stockage, la puissance de calcul) et la durée de vie des VNFs. Comme elle assure la gestion et l'orchestration des VNFs (la création et l'allocation des VMs).

6.4.4 Apports

La technologie de NFV permet de [66],

- Accélérer le déploiement de nouveaux services : des mises à jour à la demande sans ressources supplémentaire.
- Améliorer la communication et réduire les coûts en exécutant par exemple plusieurs NFVs sur un seul matériel standard.
- Améliorer la flexibilité et la scalabilité à travers par exemple le déplacement des VMs selon le besoin.

- S'adapter dynamiquement aux changements de trafic dans les centres de données.
- Améliorer l'évolutivité et la gestion des ressources.

Remarque : NFV simplifie théoriquement l'exploitation du réseau, mais pas toujours dans la pratique.

6.5 Software-Defined WAN (SD-WAN)

SD-WAN est considéré comme l'application de SDN dans les réseaux WAN d'entreprise.

6.5.1 Pourquoi SD-WAN ?

Dans les réseaux WANs traditionnels, les entreprises utilisent des réseaux MPLS (Multiprotocol Label Switching) dédiés et privés pour les communications depuis / vers leurs sièges, etc. Ainsi, les utilisateurs se connectent aux centres de données (data-centers) de l'entreprise pour accéder aux applications métiers. Cependant, la technologie MPLS est complètement gérée par le fournisseur de service et le client (l'entreprise) n'a pas de contrôle direct sur son WAN.

Plus récemment, les entreprises utilisent le Cloud computing et s'abonnent au logiciel en tant que service. Les utilisateurs accèdent désormais à ces mêmes applications sur le Cloud. Le problème qui se pose, c'est que le WAN traditionnel (MPLS) n'est plus adapté aux applications basées sur le Cloud. En effet, elle présente une forte latence, une bande passante limitée, de faible performance (applications), un coût élevé et peu de sécurité [67], [68].

Pour répondre à cette problématique, la technologie de SD-WAN (Software-defined WAN) a été proposée comme une nouvelle méthode pour accéder plus rapidement, avec des performances de qualité professionnelle et une disponibilité continue, à tous les autres sites du réseau Cloud. SD-WAN permet de simplifier la gestion des WANs d'entreprise avec des coûts réduits, une meilleure efficacité en termes de bande passante [67].

6.5.2 Définition

SD-WAN est une nouvelle architecture virtuelle pour améliorer la gestion des WANs d'entreprise. Elle consiste à découpler le matériel de réseau de son mécanisme de contrôle. Cette technologie utilise le contrôle centralisé de SDN pour mieux diriger le trafic WAN avec plus de sécurité et plus d'efficacité, et des contrôleurs sur le Cloud pour permettre un réseau WAN superposé et construire les tunnels cryptés [68], voir la figure 6.5.

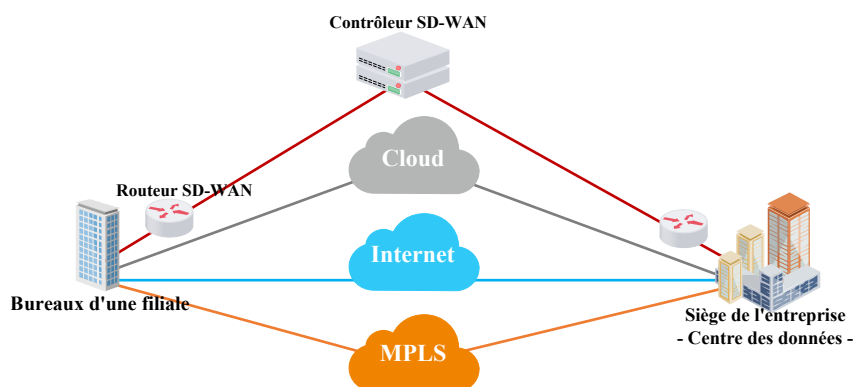


FIGURE 6.5 – l'architecture de SD-WAN [67].

SD-WAN permet d'optimiser, d'automatiser et de protéger le trafic entre divers emplacements du réseau WAN. Il permet aussi d'assurer une bonne qualité de service du bout en bout avec de meilleurs délais. Cela via l'équilibrage des charges et aussi la sélection de la technologie de communication avec les meilleures performances. Ce qui va permettre d'augmenter la productivité des entreprises (le coût) et d'améliorer la QoE (Quality of Experience) [68].

6.5.3 Apport

La technologie de SD-WAN permet [67, 68],

- Une meilleure agilité du réseau : il s'agit d'une solution logicielle sur le Cloud avec une adaptation rapide aux besoins dynamiques de WAN de l'entreprise.
- Une facilité de déploiement et de la gestion : SD-WAN est basé sur le Cloud et contrôlé et géré par un orchestrateur central.
- Une gestion et un contrôle centralisé : un orchestrateur centralisé surveille le réseau et permet la résolution à distance des problèmes.
- La réduction des coûts : le déploiement de SD-WAN est moins cher que les WANs traditionnels (une solution logiciel et une indépendance du transport de données (un choix dynamique selon les performances entre : MPLS, 4G/5G, Internet, etc.)).
- L'amélioration de la QoE (une meilleure disponibilité des services) ce qui va se répercuter par une meilleure productivité de l'entreprise.
- Une meilleure sécurité (un trafic sécurisé de bout en bout, une segmentation de réseau, etc.).

6.6 Conclusion

SDN est considérée comme le futur des architectures des nouvelles générations des réseaux de communication. Il promet de révolutionner le monde des réseaux en proposant des architectures des réseaux ouvertes, programmables, évolutives, flexibles et facile à gérer.

Initialement développé pour les réseaux filaires, SDN a connu un grand succès dans divers domaines et plusieurs applications basées sur SDN sont déjà en face de déploiement comme la technologie de NFV et celle de SD-WAN. Cependant, SDN semble toujours dans ces débuts et il a besoin de plus de temps pour se mûrir et se standardiser. Beaucoup de défis restent à relever avant d'espérer un large déploiement de SDN tels que : la scalabilité, la sécurité, etc.

BIBLIOGRAPHIE

- [1] G. Pujolle. *Initiation aux réseaux - Cours et exercices*. Éditions Eyrolles, 2001.
- [2] J. P. Arnaud C. Servin. *Réseaux et Télécoms (4e édition)*. DUNOD, 2013.
- [3] Piyush Gupta and Panganmala R Kumar. The capacity of wireless networks. *IEEE Transactions on information theory*, 46(2) :388–404, 2000.
- [4] Matthew Gast. *802.11 wireless networks : the definitive guide*. " O'Reilly Media, Inc.", 2005.
- [5] Gaëlle COUREAU. *Effets sanitaires des champs électromagnétiques et tumeurs du système nerveux central*. PhD thesis, UNIVERSITÉ BORDEAUX 2, 2013.
- [6] "guide emf uit", union internationale des télécommunications (itu), disponible sur : <https://emfguide.itu.int/>, consulté le : 7/8/2021.
- [7] D. Présent S. Lohier. *Réseaux et transmissions - 6e ed - Protocoles, infrastructures et services (6e édition)*. DUNOD, 2016.
- [8] S. Rackley. *Wireless networking technology from principles to successful implementation*. Newnes/Elsevier, 2007.
- [9] "transmission des informations, cours en ligne sur la platephorme maxicours", disponible sur <https://www.maxicours.com/se/cours/transmission-des-informations/>, consulté le : 8/9/2021., school = , year = , address = , month = , note = .
- [10] Ahmed Alioua. Modélisation et évaluation des performances des stratégies de contrôle d'admission avec rappel et canaux gardiens dans les réseaux mobiles cellulaires. *Memoire de Magister, USTHB*, 2014.
- [11] A. Alioua. Modélisation et évaluation des performances des stratégies de contrôle d'admission avec rappel et canaux gardiens dans les réseaux mobiles cellulaires. *Memoire de Magister, USTHB*, 2014.
- [12] G. Pujolle. Les réseaux (édition 2014). *EYROLLES*, 2014.
- [13] R. Venkatesha Prasad V. Quang Bien and I. G. Niemegeers. A survey on handoffs-lessons for 60ghz based wireless systems. *IEEE Communications Surveys and Tutorials*, 14(1) :64–86, 2012.
- [14] Fouzi MEKHALDI. *Partitionnement dans les réseaux mobiles Ad-hoc : Conception et évaluation de protocoles auto-stabilisants robustes*. PhD thesis, Université Paris-Sud 11, 2011.

- [15] AZZA Mohammed. *Sécurité des Réseaux AD HOC*. PhD thesis, Université Djillali Liabès de Sidi-Bel-Abbès, 2016.
- [16] R.P.Mahapatra Nishu Garg. Manet security issues. *International Journal of Computer Science and Network Security (IJCSNS)*, 9(8), 2009.
- [17] Ashish Srivastava, Atul Mishra, Bikash Upadhyay, and Akhilesh kumar Yadav. Survey and overview of mobile ad-hoc network routing protocols. In *2014 International Conference on Advances in Engineering Technology Research (ICAETR - 2014)*, pages 1–6, 2014.
- [18] Sunil Taneja and Ashwani Kush. A survey of routing protocols in mobile ad hoc networks. *International Journal of innovation, Management and technology*, 1(3) :279, 2010.
- [19] Changling Liu and Jörg Kaiser. Survey of mobile ad hoc network routing protocols. 2005.
- [20] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. An overview of mobile ad hoc networks : applications and challenges. *Journal-Communications Network*, 3(3) :60–66, 2004.
- [21] Mohammad Abdul Matin and MM Islam. Overview of wireless sensor network. *Wireless sensor networks-technology and protocols*, 2012.
- [22] Kazem Sohraby, Daniel Minoli, and Taieb Znati. *Wireless sensor networks : technology, protocols, and applications*. John wiley & sons, 2007.
- [23] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. Wireless sensor networks : a survey. *Computer networks*, 38(4) :393–422, 2002.
- [24] Qinghua Wang and Ilanko Balasingham. Wireless sensor networks-an introduction. *Wireless sensor networks : application-centric design*, pages 1–14, 2010.
- [25] Zill-E-Huma Kamal and Mohammad Ali Salahuddin. *Introduction to Wireless Sensor Networks*, pages 3–32. Springer New York, New York, NY, 2015.
- [26] J.N. Al-Karaki and A.E. Kamal. Routing techniques in wireless sensor networks : a survey. *IEEE Wireless Communications*, 11(6) :6–28, 2004.
- [27] S. Chakraborty Y. Liu, C. Chen. A software defined network architecture for geobroadcast in vanets. In *2015 IEEE International Conference on Communications (ICC)*, 2015.
- [28] Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui. A survey on pseudonym changing strategies for vehicular ad-hoc networks. *IEEE Communications Surveys Tutorials*, 20(1) :770–790, 2018.
- [29] Jerome Harri, Fethi Filali, and Christian Bonnet. Mobility models for vehicular ad hoc networks : a survey and taxonomy. *IEEE Communications Surveys Tutorials*, 11(4) :19–41, 2009.
- [30] Yacine Khaled, Manabu Tsukada, José Santa, JinHyeock Choi, and Thierry Ernst. A usage oriented analysis of vehicular networks : From technologies to applications. *J. Commun.*, 4(5) :357–368, 2009.
- [31] Rola Naja et al. *Wireless vehicular networks for car collision avoidance*, volume 2013. Springer, 2013.
- [32] Ilker Bekmezci, Ozgur Koray Sahingoz, and Şamil Temel. Flying ad-hoc networks (fanets) : A survey. *Ad Hoc Networks*, 11(3) :1254–1270, 2013.

- [33] Amartya Mukherjee, Vaibhav Keshary, Karan Pandya, Nilanjan Dey, and Suresh Chandra Satapathy. Flying ad hoc networks : A comprehensive survey. *Information and decision sciences*, pages 569–580, 2018.
- [34] Ozgur Koray Sahingoz. Networking models in flying ad-hoc networks (fanets) : Concepts and challenges. *Journal of Intelligent & Robotic Systems*, 74(1) :513–527, 2014.
- [35] Omar Sami Oubbati, Mohammed Atiquzzaman, Tariq Ahamed Ahanger, and Atef Ibrahim. Softwarization of uav networks : A survey of applications and future trends. *IEEE Access*, 8 :98073–98125, 2020.
- [36] Lav Gupta, Raj Jain, and Gabor Vaszkun. Survey of important issues in uav communication networks. *IEEE Communications Surveys & Tutorials*, 18(2) :1123–1152, 2015.
- [37] Muhammad Asghar Khan, Alamgir Safi, Ijaz Mansoor Qureshi, and Inam Ullah Khan. Flying ad-hoc networks (fanets) : A review of communication architectures, and routing protocols. In *2017 First International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT)*, pages 1–9, 2017.
- [38] Amira Chriki, Haifa Touati, Hichem Snoussi, and Farouk Kamoun. Fanet : Communication, mobility models and security issues. *Computer Networks*, 163 :106877, 2019.
- [39] Alexey V Leonov and George A Litvinov. Simulation-based packet delivery performance evaluation with different parameters in flying ad-hoc network (fanet) using aodv and olsr. In *Journal of Physics : Conference Series*, volume 1015, page 032178. IOP Publishing, 2018.
- [40] S. Michael. Drone anatomy 101. 2018.
- [41] Hazim Shakhatreh, Ahmad H Sawalmeh, Ala Al-Fuqaha, Zuochao Dou, Eyad Almaita, Issa Khalil, Noor Shamsiah Othman, Abdallah Khreishah, and Mohsen Guizani. Unmanned aerial vehicles (uavs) : A survey on civil applications and key research challenges. *Ieee Access*, 7 :48572–48634, 2019.
- [42] Mohammad Mozaffari, Walid Saad, Mehdi Bennis, Young-Han Nam, and Mérouane Deb-bah. A tutorial on uavs for wireless networks : Applications, challenges, and open problems. *IEEE communications surveys & tutorials*, 21(3) :2334–2360, 2019.
- [43] S. Zhao S. Li, L.D. Xu. The internet of things : a survey. *Inf Syst Front*, 7 :243–259, 2015.
- [44] ITU Strategy ITU, The Internet of Things and November 2005. Policy Unit (SPU).
- [45] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things : A survey. *Computer Networks*, 54(15) :2787–2805, 2010.
- [46] The internet of things reference model, cisco white paper, 2014.
- [47] Rajkumar Buyya and Vahid Amir Dastjerdi. *Internet of Things : Principles and Paradigms*. Morgan Kaufmann, 1 edition, 2016.
- [48] Simar Preet Singh, Anand Nayyar, Rajesh Kumar, and Anju Sharma. Fog computing : from architecture to edge computing and big data processing. *The Journal of Supercomputing*, 75(4) :2070–2105, 2018.
- [49] Suryadevara N.K. S.C. Mukhopadhyay. Internet of things : Challenges and opportunities. *Smart Sensors, Measurement and Instrumentation*, 9, 2014.

- [50] Keyur K. Patel and Sunil M. Patel. Internet of things-iot : Definition, characteristics, architecture, enabling technologies, application future challenges. *International Journal of Engineering Science and Computing*, 6, 2016.
- [51] H. Kopetz. Internet of things. *Real-Time Systems. Real-Time Systems Series*, 2011.
- [52] Michele Nitti, Virginia Pilloni, Giuseppe Colistra, and Luigi Atzori. The virtual object as a major element of the internet of things : A survey. *IEEE Communications Surveys and Tutorials*, 18(2) :1228–1240, 2016.
- [53] Nallapaneni Manoj Kumar and Pradeep Kumar Mallick. The Internet of Things : Insights into the building blocks, component interactions, and architecture layers. pages 109–117. Elsevier BV, 2018.
- [54] R. Venkatesha Prasad V. Quang Bien and I. G. Niemegeers. A survey of software-defined networking : Past, present, and future of programmable networks. *IEEE Communications Surveys and Tutorials*, 16(3) :1617–1634, 2014.
- [55] Paul Goransso and Chuck Blackn. Software defined networks : A comprehensive approach. *Elsevier Morgan Kaufmann*, 2017.
- [56] J. Cao Z. He and X. Liu.n. Sdvn : enabling rapid network innovation for heterogeneous vehicular communication. *IEEE Network*, 30(4) :10–15, 2016.
- [57] M. Gerla R. L. Gomes F. Ongaro I. Ku, Y. Lu and E. Cerqueira. Towards software-defined vanet : Architecture and services. In *2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*, 2014.
- [58] Ahmed Alioua. Intégration du software-defined networking (sdn) dans les réseaux de véhicules (vanets). *These de doctorat, Université des sciences et technologies - houari Boumediane* -, 2019.
- [59] Diego Kreutz, Fernando M. V. Ramos, Paulo Esteves Veríssimo, Christian Esteve Rothenberg, Siamak Azodolmolky, and Steve Uhlig. Software-defined networking : A comprehensive survey. *Proceedings of the IEEE*, 103(1) :14–76, 2015.
- [60] Yuan Zhang, Lin Cui, Wei Wang, and Yuxiang Zhang. A survey on software defined networking with multiple controllers. *J. Netw. Comput. Appl.*, 103(C) :101–118, February 2018.
- [61] H. Balakrishnan G. Parulkar L. Peterson J. Rexford S. Shenker N. McKeown, T. Anderson and J. Turner. Open flow : enabling innovation in campus networks. *SIGCOMM Comput. Commun.*, 38(2) :69–74, 2008.
- [62] <https://www.opennetworking.org/>. Open networking fondation.
- [63] Yong Li and Min Chen. Software-defined network function virtualization : A survey. *IEEE Access*, 3 :2542–2553, 2015.
- [64] Ahmed M. Alwakeel, Abdulrahman K. Alnaim, and Eduardo B. Fernandez. Toward a reference architecture for nfv. In *2019 2nd International Conference on Computer Applications Information Security (ICCAIS)*, pages 1–6, 2019.
- [65] Bo Yi, Xingwei Wang, Keqin Li, Sajal k. Das, and Min Huang. A comprehensive survey of network function virtualization. *Computer Networks*, 133 :212–262, 2018.
- [66] Van-Giang Nguyen, Anna Brunstrom, Karl-Johan Grinnemo, and Javid Taheri. Sdn/nfv-based mobile packet core network architectures : A survey. *IEEE Communications Surveys and Tutorials*, 19(3) :1567–1602, 2017.

- [67] P. Segeč, M. Moravčík, J. Uratmová, J. Papán, and O. Yeremenko. Sd-wan - architecture, functions and benefits. In *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pages 593–599, 2020.
- [68] S. Rajagopalan. A study on mpls vs sd-wan. In *Computer Networks, Big Data and IoT, Lecture Notes on Data Engineering and Communications Technologies*, 2021.