



Université Sidi Mohamed Ben Abdellah
Faculté Des Sciences et Techniques
Fès



Livrable 2

Date début : 15/11/2013 Date Fin : 13/12/2013

Date prévue de soumission : 03/12/2013

Date Actuelle de soumission : 01/12/2013

Réalisé par :

- ZOUHAIRI Fouad
- EL GHOBACH Imad
- JIDA Safae
- KHARBAN Yahya
- TABTI Abdelhak

Année universitaire 2013/2014

Ce livrable contient un cours détaillé à propos des réseaux sans fils. Il parle surtout de la norme IEEE 802.11 et de son évolution.

Version	Date	Modifie par	Motif de la Modification
V1.0	01/12/2013	Groupe LIFISIR2014	Finalisation de livrable

Table des matières

I.	Introduction :	4
II.	Généralités sur la transmission :	4
1.	Les différents besoins :	4
2.	Contraintes de la transmission radio :	5
3.	Différents systèmes pour différent besoins :	5
4.	Nouveaux usages, nouvelles technologies :	6
III.	La Réglementation des Fréquences :	6
1.	Attribution de fréquence :	7
2.	Plans :	8
3.	Coordination :	9
IV.	Normalisation des WLANs :	9
4.	La norme 802.11 (Wi-fi) :	9
1.	La norme HIPERLAN :	11
V.	Le standards 802.11 :	12
5.	Application :	12
6.	Architecture :	13
VI.	La couche Physique 802.11 :	15
1.	DSSS (Direct Sequence Spread Spectrum): :	15
2.	FHSS (Frequency-Hopping Spread Spectrum): :	16
3.	OFDM (Orthogonal Frequency Division Multiplexing) :	16
4.	Comparatif des Trois Technique :	16
VII.	Technique d'accès :	17
1.	La DCF (Distributed Coordination Function) :	17
2.	La PCF (Point coordination Function) :	17
3.	CSMA/CA :	18
4.	Algorithme de backoff :	20
5.	RTC/CTC :	21
VIII.	Fonctions de la couche liaison :	22
IX.	Conclusion :	24

Liste de Figures

Figure 1 : Situation de la norme 802.11	12
Figure 2:Exemple De liaison inter-bâtiments	13
Figure 3 : Les canaux 1,7,13.....	15
Figure 4 : OFDM.....	16
Figure 5 : Le protocole CSMA/CA dans sa forme la plus simple.....	Error! Bookmark not defined.

I. Introduction :

La radio tient une place particulière dans les télécommunications. Utilisée initialement pour les services de communications à longue distance et de diffusion, peu de temps après transmission radio de l'italien Guglielmo Marconi en 1895, elle s'est progressivement étendue à tous les domaines des télécommunications, jusqu'à la téléphonie mobile d'aujourd'hui.

L'arrivée du numérique a permis d'améliorer les performances des systèmes radio grâce à la compression des données et à une meilleure protection contre les perturbations qu'autorise la numérisation des signaux. Dorénavant, de nombreux services sont numériques et l'évolution récente des services radio-mobiles vers les données et Internet mobile le montre bien.

II. Généralités sur la transmission :

1. Les différents besoins :

Parmi les différents besoins en communication, certains ne pourraient être satisfaits si les transmissions par ondes radio n'existaient pas. C'est le cas en particulier des communications en situation de mobilité, pour lesquelles il n'est pas possible de déplacer les infrastructures du réseau de communication pour garder l'accès aux services. Les services de défense et de sécurité, qui en ont tout de suite saisi l'intérêt, ont ainsi développé et utilisé différentes techniques et systèmes de transmissions radio pour leurs besoins propres, des faisceaux hertziens transportables aux réseaux mobiles tactiques en passant par les transmissions par satellites ou les transmissions ionosphériques. La plupart de ces techniques ont été étendues aux applications civiles et le grand public les utilise aujourd'hui dans la rue ou depuis son domicile par l'intermédiaire du téléphone sans fil ou de la réception de programmes télévisuels diffusés par satellite. Le Global System for Mobile communication (GSM, anciennement « Groupe spéciale mobile»), principale norme de téléphonie mobile numérique en Europe et dans le monde depuis 1992, est sans doute l'exemple le plus frappant de l'irruption de la radio dans les communications personnelles de la vie quotidienne.

Un autre intérêt des transmissions radio est leur capacité de couvrir facilement une grande zone géographique ou des zones difficiles d'accès pour des infrastructures classiques, c'est pourquoi les transmissions radio sont utilisées pour la plupart des services de diffusion où l'on n'émet qu'une seule fois le même signal destiné à de multiples usagers (radiophonie, télévision). De ce point de vue, la diffusion par satellite géostationnaire est très intéressante, puisque plusieurs pays peuvent être couverts simultanément par un seul satellite.

Les transmissions radio peuvent aussi servir de moyen pour accéder à l'utilisateur, en particulier dans les régions isolées ou montagneuses, lorsqu'il est plus économique.

2. Contraintes de la transmission radio :

La contrepartie des avantages des transmissions radio est de deux ordres, d'une part, ces transmissions radio nécessitent l'utilisation d'une ressource rare qu'il est nécessaire de partager avec d'autres utilisateurs : les fréquences radio. D'autre part, l'utilisation de cette ressource implique des contraintes opérationnelles qui se traduisent en termes de limitations en performance ou par des coûts d'équipements ou de déploiement plus élevés.

L'accès à la ressource spectrale est réglementé par des instances gouvernementales ou supranationales, avec en premier lieu le secteur radiocommunication de l'Union internationale des télécommunications (U.I.T.-R. ou I.T.U-R.). L'aspect de cette réglementation comme l'importance économique de l'attribution de ressources spectrales sur des secteurs concurrentiels tels que les mobiles se mesure au coût d'acquisition, de plus en plus élevé pour les opérateurs des autorisations d'émettre. Certains gouvernements n'hésitent pas à mettre aux enchères les bandes de fréquences, comme cela a été le cas pour les systèmes mobile de troisième génération *Universal Mobile Telecommunication System* (UMTS) dans certains pays européens.

Les limitations en performance ainsi que les contraintes opérationnelles sont quant à elles inhérentes à l'utilisation des fréquences radio. Selon les bandes de fréquences utilisées, ces contraintes pourront être différentes (très fortes atténuations du signal à certaines fréquences ou contraintes technologiques de réalisation). Une fois la bande de fréquence choisie, les limitations proviendront des conditions de propagation (réflexion, diffraction, atténuation et chemins multiples qui entraînent une distorsion et un affaiblissement du signal émis), de la puissance limitée des émetteurs radio (en particulier due aux contraintes de coûts et de taille des équipements terminaux) ainsi que des contraintes opérationnelles et de coûts du réseau d'accès radio. Un compromis technique et économique devra être trouvé afin de satisfaire des besoins exprimés par les utilisateurs en termes de service (débit, disponibilité et qualité) au moyen de ressources limitées en fréquences et avec des contraintes budgétaires fortes pour que le système soit rentable pour l'opérateur et d'un coût attractif pour l'utilisateur.

3. Différents systèmes pour différent besoins

Les besoins de services peuvent être très diversifiés, du simple message d'alerte qu'on souhaite recevoir partout dans le monde à la transmission bidirectionnelle de données multimédias à haut débit à domicile. Les utilisateurs peuvent aussi être très variés, allant du simple individu à la population entière d'un pays en passant par les différentes catégories de professionnels, les groupes fermés d'utilisateurs, ou les opérateurs de télécommunications eux-mêmes pour leurs propres besoins en transmissions. Cela a conduit à la conception de nombreux systèmes, chacun d'entre eux étant optimisé pour différentes catégories d'utilisateurs ayant des besoins spécifiques en termes de service, quelques exemples ont déjà été mentionnés, on pourrait compléter la liste, sans être exhaustif, en citant les systèmes de messagerie, de téléphonie d'entreprise sans fil, de téléphonie mobile dédiés pour flotte d'entreprise ou les services de sécurité, les constellations de satellite en orbite basse pour la voix ou les données. Ces différents systèmes peuvent être classés en : système de diffusion ou de communication ; systèmes fixes ou mobiles ; systèmes d'accès ou d'infrastructure ;

systèmes privés ou publics ; systèmes terrestres ou satellitaires ; systèmes unidirectionnels ou bidirectionnels.

4. Nouveaux usages, nouvelles technologies

Avec l'arrivée d'Internet dans la vie quotidienne et la démocratisation de la téléphonie mobile, de nouveaux usages se font à jour, qui nécessitent de faire évoluer les systèmes existants et de mettre en place de nouveaux systèmes plus performants. C'est le cas, en particulier, du GSM, lequel, de simple système de téléphonie cellulaire dédié uniquement à la transmission de paroles, évolue pour incorporer la transmission de données et l'Internet mobile. Ainsi, la mise en œuvre du protocole WAP (Wireless application Protocol) permet d'accéder aux services Internet pour les terminaux qui en sont équipés. La norme GPRS (General Packet Radio Service), mise en place à partir de 2001, autorise des transmissions non plus en mode circuit (cas de la téléphonie) mais en mode paquet. L'intérêt du mode paquet est qu'il est plus économique en ressources radio tout en permettant la facturation au volume et non plus à la durée. On utilise en effet les ressources uniquement lors de la transmission des données alors qu'en mode circuit celles-ci sont mobilisées pendant la durée de la communication (même lorsqu'on ne parle pas). Les nouveaux systèmes comme l'UMTS, ou les autres systèmes de la troisième génération de mobiles- regroupées avec l'UMTS dans la famille des systèmes IMT-2000 (International Mobile Télécommunication 2000) – sont bien sûr tous numériques et ont pris en compte dès leur conception les nouvelles demandes de services : débit plus élevés jusqu'à 2 mégabits par seconde (Mbits/s) en mode paquet, service multimédia, service de localisation performante, etc.

III. La Réglementation des Fréquences :

Avec le début d'exploitation es ondes radio comme un moyen de transmission d'informations il est devenu claire que les ondes radioélectriques ne respectent pas les frontières internationaux et constituent une ressource planétaire, donc pour éviter les brouillages préjudiciables entre les pays, il faut parvenir à un consensus au niveau mondial sur leur utilisation, dans ce but des études préliminaires de la réglementation international de la radiocommunication ont été lancés.

Les progrès rapides des techniques de radiocommunication qui ont eu lieu pendant la seconde guerre mondiale ont engendré une explosion de la demande de bandes de fréquences par les utilisateurs de tous les pays. Par ailleurs, les pressions accrues imposées aux ressources disponibles de la partie du spectre utilisable à des fins commerciales ont également eu pour effet d'augmenter la possibilité de brouillage préjudiciable entre les utilisateurs et les services.

Par conséquent, un groupe de pays s'est réuni à Moscou en 1946 et a pris certaines décisions qui ont été ensuite développées et approuvées à la Conférence administrative des radiocommunications et à la Conférence de plénipotentiaires de l'UIT qui, Cette dernière a élaboré une structure pour la gestion du spectre radioélectrique, fondée sur quatre principes fondamentaux:

- **Attribution de spectre:** la partie utilisable du spectre radioélectrique est divisée en petites bandes qui sont attribuées en exclusivité ou en partage à des services précis de radiocommunication.
- **Planification:** des plans d'assignation ou d'allotissement sont adoptés pour des services déterminés comme la radiodiffusion, le service mobile maritime ou encore le service mobile aéronautique, où l'émission et la réception ne sont pas nécessairement limitées au territoire d'un pays donné.
- **Coordination/accords:** dans certaines bandes, des procédures sont élaborées en vue de procéder à une coordination internationale supplémentaire vis-à-vis de services déterminés (comme les services de radiodiffusion spatiale ou de radiodiffusion en ondes courtes), lorsque les services d'un pays risquent de causer des brouillages à bon nombre d'autres pays.
- **Notification:** l'utilisation planifiée et coordonnée d'une fréquence, conformément aux dispositions du Règlement des radiocommunications, doit être notifiée à l'UIT. Le Bureau des radiocommunications de l'UIT a pour tâche d'examiner chaque fiche de notification, de veiller à ce que tous les pays Membres de l'UIT appliquent les dispositions du Règlement des radiocommunications concernant l'utilisation du spectre radioélectrique et de tenir à jour un Fichier de référence international des fréquences (souvent appelé simplement le Fichier de référence).

Suit a ce règlement La partie utilisable du spectre est en fait divisée en petites portions dont la largeur varie selon les besoins. Ces portions sont appelées "bandes de fréquences" et sont attribuées, dans le cadre d'un Tableau d'attribution (ci-dessus) des bandes de fréquences, aux différents services de radiocommunication soit en exclusivité, soit en partage. Toute modification à ce Tableau (ou au Règlement des radiocommunications dont il fait partie) ne peut être effectuée que par une Conférence mondiale des radiocommunications et uniquement à la suite de décisions adoptées par consensus, ou vote le cas échéant, à l'issue de négociations entre les délégations des pays, L'existence de plans et de procédures établis au niveau international facilite la mise en œuvre de nouveaux systèmes de radiocommunication, dans la mesure où ils permettent de garantir la stabilité des projets de conception qui ont servi à la planification de ces systèmes.

1. Attribution de fréquence :

Trois instruments sont utilisé pour procéder au partage international des fréquences: le tableau d'attribution des bandes de fréquences; des plans d'assignation ou d'allotissement et les procédures de coordination.

- **Tableau d'attribution des bandes de fréquences**

Des bandes de fréquences sont attribuées aux divers services de radiocommunication à titre exclusif ou en partage. On distingue trois catégories de service: primaire, secondaire et permis. Ces attributions peuvent être faites au niveau mondial ou être limitées à une région du monde.

Exemple : une partie du tableau d'attribution de fréquences

MHz 138 - 148			
Attribution aux services ^{Note}			
Région 1	Région 2	Région 3	
138 - 143.6	138 - 143.6	138 - 143.6	
MOBILE AÉRONAUTIQUE (OR)	FIXE MOBILE RADIOLOCALISATION Recherche spatiale (espace vers Terre)	FIXE MOBILE Recherche spatiale (espace vers Terre)	
S5.210 S5.211 S5.212 S5.214		S5.207 S5.213	
143.6 - 143.65	143.6 - 143.65	143.6 - 143.65	
MOBILE AÉRONAUTIQUE(OR) RECHERCHE SPATIALE (espace vers Terre)	FIXE MOBILE RADIOLOCALISATION Recherche spatiale (espace vers Terre)	FIXE MOBILE Recherche spatiale (espace vers Terre)	
S5.211 S5.212 S5.214		S5.207 S5.213	
143.65 - 144	143.65 - 144	143.65 - 144	
MOBILE AÉRONAUTIQUE (OR)	FIXE MOBILE RADIOLOCALISATION Recherche spatiale (espace vers Terre)	FIXE MOBILE Recherche spatiale (espace vers Terre)	
S5.210 S5.211 S5.212 S5.214		S.5207 S5.213	
144 - 146	AMATEUR S5.120 AMATEUR PAR SATELLITE S5.216		
146 - 148	146 - 148	146 - 148	
FIXE MOBILE sauf mobile aéronautique (R)	AMATEUR	FIXE MOBILE	
	S5.217	S5.217	

2. Plans

Pour certains services les bandes de fréquences d'émission et de réception ne sont pas limitées au seul territoire d'un pays ce qui fait pour ces types de service des conférences adoptent des Plans d'assignation ou des Plans d'allotissement, selon le cas. Des plans d'assignation attribuent, sur la base des besoins exprimés par chaque pays, des fréquences pour chaque station d'un service donné, des plans d'allotissement accordent à chaque pays des fréquences destinées à être utilisées par un service donné, fréquences que le pays assigne ensuite, selon les besoins, aux stations qui relèvent de sa juridiction.

3. Coordination

Lorsque des plans ne peuvent être établis, des procédures sont élaborées pour une coordination internationale qui vise à ce que le pays projetant d'utiliser une fréquence donnée obtienne l'assentiment de tous les pays qui pourraient être affectés par cette utilisation.

IV. Normalisation des WLANs

Un réseau sans fil est un réseau dans lequel au moins deux terminaux peuvent communiquer sans utiliser de liaison filaire. Il offre la possibilité de se déplacer, tout en restant connecté, dans un périmètre géographique plus ou moins étendu, grâce à sa liaison qui utilise les ondes radioélectriques.

Le réseau local sans fil, noté WLAN (Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre eux les terminaux présents dans la zone de couverture. On cite parmi ses technologies concurrentes le Wi-Fi et Hiperlan.

1. La norme 802.11 (Wi-fi)

La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom Wi-Fi (contraction de Wireless Fidelity, parfois notée à tort WiFi) correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau Wifi est en réalité un réseau répondant à la norme 802.11. Les matériels certifiés par la Wi-Fi Alliance bénéficient de la possibilité d'utiliser le logo suivant :



La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. Voici un tableau présentant les différentes révisions de la norme 802.11 et leur signification :

Nom de la norme	Nom	Description
802.11a	Wifi5	La norme 802.11a (baptisé <i>WiFi 5</i>) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	Wifi	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.
802.11c	Pontage 802.11 vers 802.1d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau <i>liaison de données</i>).
802.11d	Internationalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche <i>liaison de données</i> . Ainsi cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo.
802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole <i>Inter-Access point roaming protocol</i> permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée <i>itinérance</i> (ou <i>roaming en anglais</i>)
802.11g		La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels

		conformes à la norme 802.11g peuvent fonctionner en 802.11b
802.11h		La norme <i>802.11h</i> vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, dont le <i>h</i> de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme <i>802.11i</i> a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l' <i>AES (Advanced Encryption Standard)</i> et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11r		La norme <i>802.11r</i> a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme <i>802.11j</i> est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

2. La norme HIPERLAN

HiperLAN (ou HIGH PERFORMANCE radio LAN) est un standard européen de télécommunications créé par l'ETSI (European Telecommunications Standards Institute) dans but de créer des environnements sans fil flexibles à haut débit Permettant un fonctionnement ad-hoc, cette norme est Composé de 2 version : HiperLAN1 et HiperLAN2.

- HiperLAN1 : Cette première version est initiée et créé en 1998 par l'ETSI (European Télécommunication Standard Institute), cette version permettait la connexion ad-hoc à l'intérieur des bâtiments sur des distances d'environ 50 m par borne, avec un débit théorique de débit de 20 Mbits/s.
- HiperLAN2 : Cette version daté de 1999 et a été définie par le groupe H2GF (Hiperlan 2 global Forum) différemment au première version, celle-ci permet une connexion réseaux en mode infrastructure avec un débit théorique de 50 Mbits/s.

V. Le standards 802.11

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- la couche physique (notée parfois couche PHY), proposant trois types de codages de l'information.
- la couche liaison de données, constitué de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC).
- A l'instar des autres normes 802.x, 802.11 couvre les couches physique et liaison de données. Le schéma suivant présente les couches en question, positionnées par rapport au modèle de référence OSI de l'ISO :

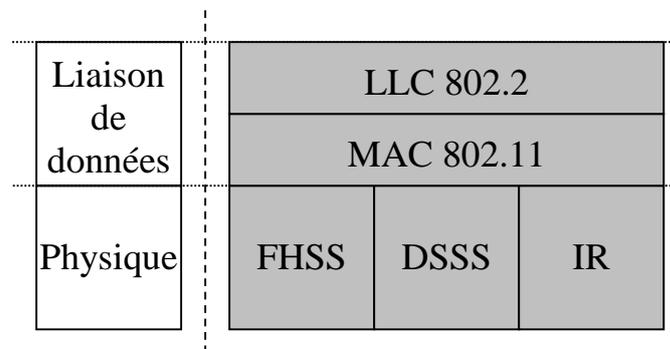


Figure 1 : Situation de la norme 802.11

4. Application

▪ Mobilité de l'utilisateur et/ou du terminal

Comme exemple de services offrant la mobilité à l'utilisateur et aux terminaux, on cite : l'accès internet haut débit via les hot spots publics, et donc les services vidéo, le mail, le chat, les forums et le travail collaboratif. Aussi à domicile, via les boîtiers multi Play (free box, live box...).

▪ Mise en place d'un réseau dans un temps très court

Ad-hoc est un exemple d'implémentation d'un réseau sans fil dans des temps minimale. Ce type de réseau est utilisé pour permettre la création d'un réseau locale en s'appuyant sur le wifi. À titre d'exemple, on peut citer le cas des jeux FPS qui utilisent souvent ce dernier.

- **Éviter le câblage des locaux, des liaisons inter-bâtiments**

Parmi les points forts des réseaux sans fil est la possibilité de lier deux bâtiments distants possédant chacun un réseau interne décrites sur la figure suivante :

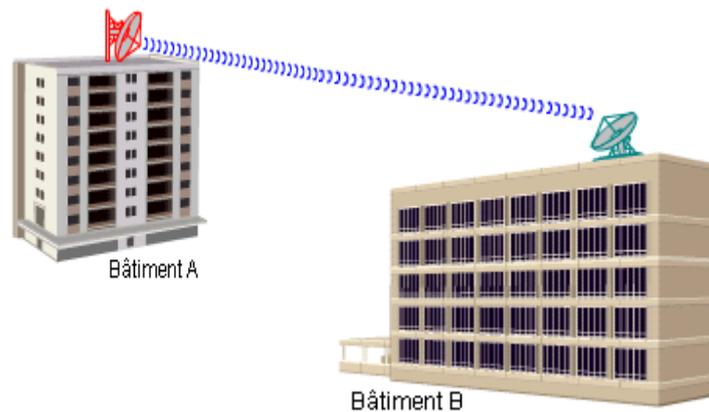


Figure 2:Exemple De liaison inter-bâtiments

Comme exemple de liaison inter bâtiments, on cite le réseau MARWAN permettant la liaison de la FSTF avec la présidence d'Université Sidi Mohamed Ben Abdellah.

- **Création des infrastructures dans des bâtiments classés :**

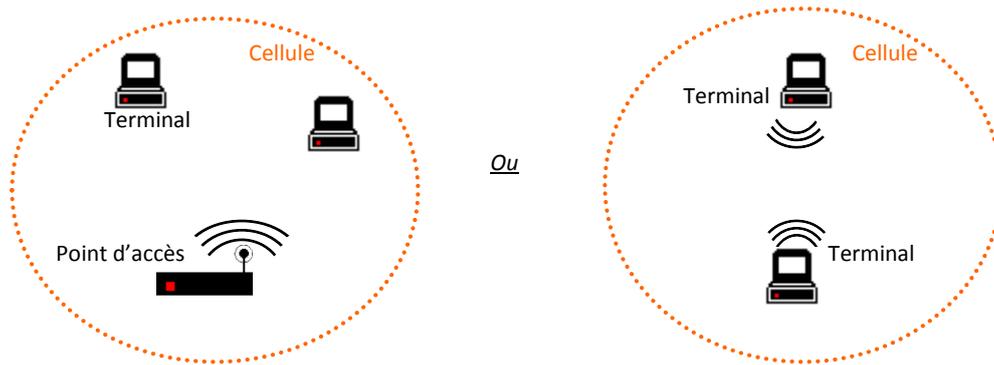
Le sans-fil permet de mettre en place une installation réseau dans des bâtiments classés, c'est le genre de bâtiments possédant une infrastructure faible, qui ne supporte pas la mise en place d'un réseau câblé. Comme exemple on peut citer l'implémentation des réseaux sans fil dans des bâtiments considérés comme patrimoine historique tel que : Al Quaraouiyine.

- **Réalisation des installations temporaires :**

Avec le réseau sans-fil on peut réaliser des installations temporaires, par exemple les installations faites lors des conférences, festival, ou bien les installations réseaux implémentées lors des cérémonies internationales telles que la coupe du monde.

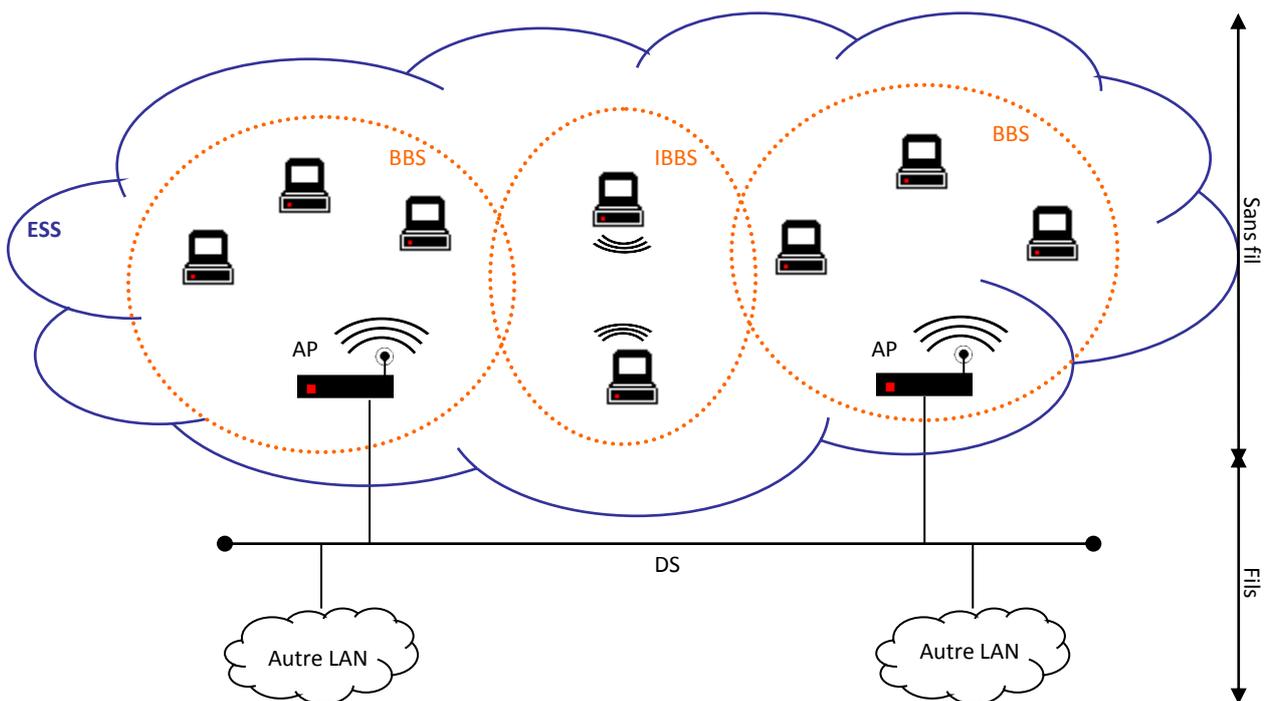
5. Architecture

Le principe de la cellule est au centre de l'architecture 802.11. Une cellule est la zone géographique dans laquelle une interface 802.11 est capable de dialoguer avec une autre interface 802.11.



Le plus souvent, une cellule est contrôlée par une station de base appelée point d'accès. Ce mode est encore appelé mode infrastructure car les terminaux proches d'un point d'accès vont pouvoir utiliser un ensemble de services fournis par l'infrastructure du réseau 802.11 via un point d'accès. Il est cependant possible d'établir des communications ad-hoc permettant une communication directe entre terminaux, sans passer par l'infrastructure centrale.

Une vue complète des éléments architecturaux proposés par l'IEEE 802.11 peut se résumer par le schéma suivant :



On distingue les éléments suivants :

- la cellule de base appelée BBS (Basic Service Set)
- la cellule de base en mode ad-hoc appelée IBBS (Independent Basic Service Set)
- le point d'accès appelé AP (Acces Point)
- l'ensemble du réseau sans fil appelé ESS (Extented Service Set) :

- L'ESS peut aussi fournir aux différentes stations mobiles une passerelle d'accès vers un réseau fixe, tel qu'Internet
- l'épine dorsale appelée DS (Distribution System) : Le système de distribution (DS) est responsable du transfert des paquets entre différents BSS d'un même ESS il est implémenté de manière indépendante de la structure hertzienne de la partie sans fil.

Typiquement, chaque cellule est contrôlée par un AP, toutes les cellules (encore appelées BBS) sont reliées à une épine dorsale DS qui permettra le transfert de données au sein d'un même ESS ainsi que la communication avec des réseaux filaires.

En mode ad-hoc, un groupe de terminaux forment un IBSS et communiquent au sien de cet IBSS sans avoir recours à des tiers.

VI. La couche Physique 802.11

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, elle propose plusieurs types de codage de l'information : DSSS, FHSS, IR, OFDM.

1. DSSS (Direct Sequence Spread Spectrum):

C'est une méthode de modulation de signal, qui permet un étalement de spectre en séquence directe. La bande des 2,4 GHz est divisée en 14 canaux de 22 MHz espacés de 5 MHz. Les canaux adjacents se chevauchent partiellement (en cas où deux points d'accès utilisant les mêmes canaux ont des zones d'émission qui se recoupent, des distorsions du signal risquent de perturber la transmission) et seuls trois canaux sur les 14 étant entièrement isolés sont généralement utilisés pour éviter les interférences (ex. 1, 6, 11 ou 1, 7, 13 comme le montre la figure ci-dessus). Les données sont transmises intégralement sur l'un de ces canaux de 22 MHz, sans saut.

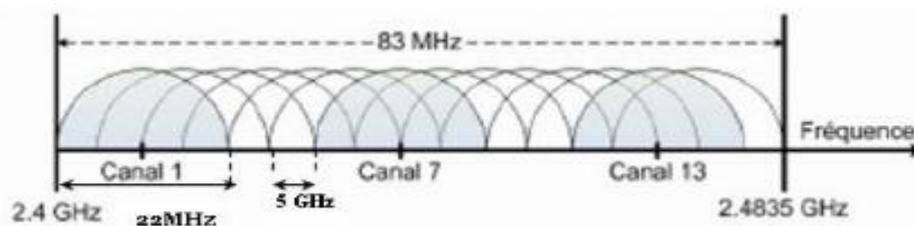


Figure 3 : Les canaux 1,7,13

2. FHSS (Frequency-Hopping Spread Spectrum):

Cette méthode consiste à découper la large bande de fréquence en un minimum de 75 canaux (hops ou sauts d'une largeur de 1MHz), puis de transmettre en utilisant une combinaison de canaux connue de toutes les stations de la cellule. Dans la norme 802.11, la bande de fréquence 2.4 - 2.4835 GHz permet de créer 79 canaux de 1 MHz. La transmission se fait ainsi en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (d'environ 400 ms), ce qui permet à un instant donné de transmettre un signal plus facilement reconnaissable sur une fréquence donnée.

3. OFDM (Orthogonal Frequency Division Multiplexing)

Le principe de cette technique consiste à diviser le signal que l'on veut transmettre sur différentes bandes porteuses, comme si l'on combinait ce signal sur un grand nombre d'émetteurs indépendants, fonctionnant sur des fréquences différentes. Un canal est constitué de 52 porteuses de 300 KHz de largeur, 48 porteuses sont dédiées au transport de l'information utile et 4 pour la correction d'erreurs appelées *porteuses pilote*, Huit canaux de 20 MHz sont définis dans la bande de 5 GHz.

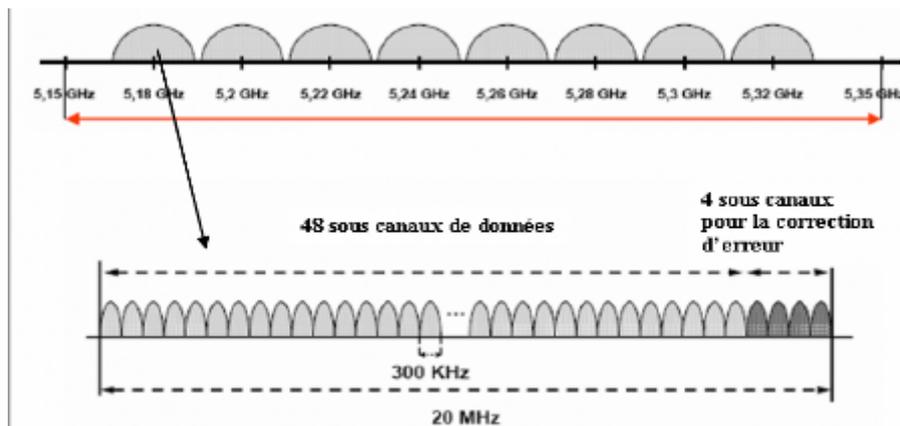


Figure 4 : OFDM

4. Comparatif des Trois Technique :

Le tableau suivant illustre un comparatif entre les avantages et les inconvénients de chaque méthode :

Technique de transmission	Avantages	Inconvénients
DSSS	<ul style="list-style-type: none"> Elle propose des vitesses de transmissions plus importantes [14]. 	<ul style="list-style-type: none"> L'utilisation d'un seul canal pour la transmission, rend le système DSSS plus sensibles aux interférences.
FHSS	<ul style="list-style-type: none"> Elle empêche une perte totale du signal, grâce à la technique de transmission par saut. Elle constitue une solution efficace dans un environnement où il y a beaucoup de multitrajets. 	<ul style="list-style-type: none"> faible largeur de bande par canal ne lui permettant pas d'atteindre des vitesses de transmissions élevées. Utilisation de toute la largeur de bande, ce qui implique une charge supplémentaire sur le réseau.
OFDM	<ul style="list-style-type: none"> Permet d'atteindre des vitesses de transmission jusqu'à 54 Mbps pour la 802.11a et la 802.11g. Elle offre un mécanisme de correction d'erreurs sur l'interface physique. 	

1. Technique d'accès

Les stations partagent un même support de transmission (les ondes hertziennes en 802.11, le support filaire en 802.3) et doivent obéir à une politique d'accès pour l'utiliser. Dans 802.11, deux méthodes d'accès sont proposées :

2. La DCF (Distributed Coordination Function) :

C'est un mode qui peut être utilisé par tous les mobiles, et qui permet un accès équitable au canal radio sans aucune centralisation de la gestion de l'accès (mode totalement distribué). Il met en œuvre un certain nombre de mécanismes qui visent à éviter les collisions et non pas à les détecter. Ce mode peut aussi bien être lorsqu'il n'y a pas de station de base (mode ad hoc) que lorsqu'il y en a (mode infrastructure).

Cette méthode sera illustré dans les schémas expliquant la CSMA/CA par la suite.

3. La PCF (Point coordination Function) :

Le (PCF) appelée mode d'accès contrôlé, est fondé sur l'interrogation à tour de rôle des stations, contrôlées par le point d'accès qui indiquera à chacun des mobiles qui lui

sont rattachés quand ils doivent émettre leurs paquets. Durant la phase où le point d'accès impose l'ordre des transmissions, il n'y a pas de contention pour l'accès au canal. Une station ne peut émettre que si elle est autorisée et elle ne peut recevoir que si elle est sélectionnée. Cette méthode est conçue pour les applications temps réel (vidéo, voix) nécessitant une gestion du délai lors des transmissions de données. Cette méthode est optionnelle et ne fonctionne qu'en mode infrastructure.

4. CSMA/CA

Contrairement à CSMA/CD (Carrier Sense Multiple Access with Collision Detection) la méthode CSMA/CA met en avant le principe d'évitement des collision. Au lieu d'un contrôle des collisions à posteriori, on adopte une politique de contrôle à priori. En effet, la technique de détection de collision CD ne peut pas s'appliquer sur un réseau physique sans fil pour les raisons suivantes :

- pour détecter des collisions, il serait nécessaire de disposer d'une liaison radio full duplex (émission et réception simultanées possibles), ce qui n'est pas envisageable compte tenu des coûts induits
- le fait qu'une station détecte que le support est libre autour d'elle ne signifie pas forcément que le support l'est autour du récepteur. En effet, deux stations ne sont pas forcément en relation directe et donc le principe d'écoute de la porteuse n'est pas utilisable au sens strict du terme.

Il résulte de cet état de fait l'utilisation du principe CA (qui permet d'éviter les collisions) et d'un mécanisme d'acquiescement appelé Positif Acknowledge. Les autres éléments importants sont les espaces intertrames et le temporisateur d'émission.

Les espace intertrames, ou IFS (Inter Frame Spacing), correspondent à un intervalle de temps entre l'émission de deux trames. Il en existe trois types selon 802.11 :

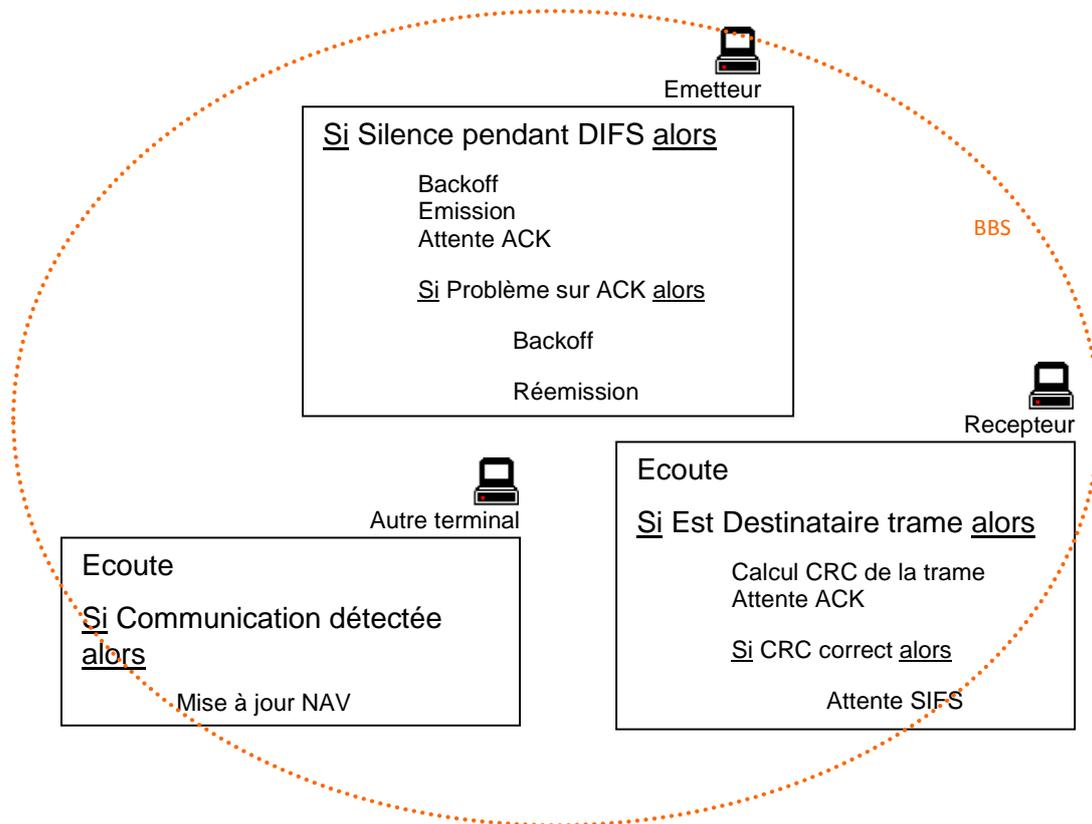
- SIFS (Short IFS), utilisé pour séparer les transmissions d'un même dialogue
- PIFS (PCF IFS), utilisé par le point d'accès pour effectuer le polling dans la méthode PCF
- DIFS (DCF IFS), utilisé en DCF (c'est à dire en CSMA/CA) lorsqu'une station veut initier une communication

La temporisation d'émission, appelé NAV (Network Allocation Vector) permet d'éviter les collisions en retardant les émissions de toutes les stations qui détectent que le support est occupé.

Le principe général de la méthode CSMA/CA est donc : une station qui souhaite émettre explore les ondes et, si aucune activité n'est détectée, attend un temps aléatoire (appelé DIFS, Distributed Inter Frame Space), vérifie à nouveau si le support est libre et le cas échéant transmet. Les stations en écoute constatent une émission et déclencheront pour une durée fixée leur indicateur de Virtual Carrier Sense (appelé NAV pour Network Allocation Vector) et utiliseront cette information pour retarder toute transmission prévue. Si le paquet est intact à la réception (calcul d'un CRC), la station réceptrice émet une trame d'acquiescement (ACK)

qui, une fois reçue par l'émetteur, met un terme au processus. Si la trame ACK n'est pas détectée par la station émettrice (parce que le paquet original ou le paquet ACK n'a pas été reçu intact), une collision est supposée et le paquet de données est retransmis après attente d'un autre temps aléatoire.

Le schéma suivant résume une communication réussie dans le cas où aucune collision ne se produit :



Toujours dans ce même cas de figure basique, les trames échangées sont les suivantes :

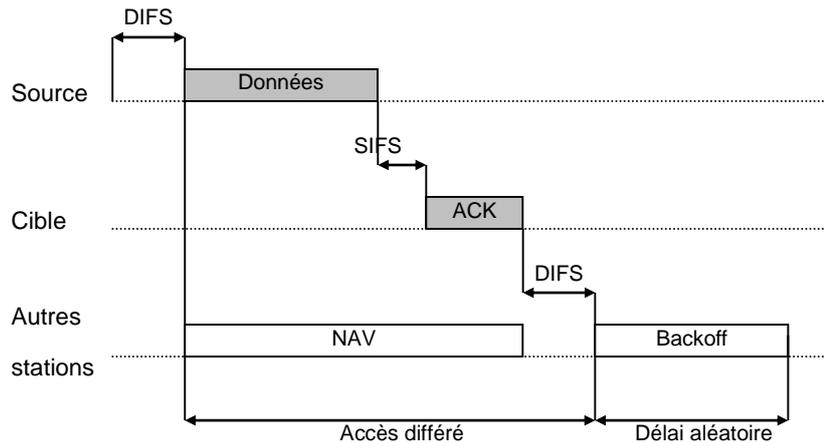


Fig. 5 : La transmission des données dans CSMA/CA (forme simple)

On peut noter dès à présent que ce mécanisme d'accusé de réception explicite à 802.11 une charge inconnue sous 802.3, aussi un réseau local 802.11 aura-t-il des performances inférieures à un LAN Ethernet équivalent par exemple.

5. Algorithme de backoff

Le backoff est une méthode bien connue pour résoudre les différences entre plusieurs stations voulant avoir accès au support. Cette méthode demande que chaque station choisisse un nombre aléatoire n entre 0 et un certain nombre, et d'attendre ce nombre de slots avant d'accéder au support, toujours en vérifiant qu'une autre station n'a pas accédé au support avant elle.

La durée d'un slot (Slot Time) est définie de telle sorte que la station sera toujours capable de déterminer si une autre station a accédé au support au début du slot précédent. Cela divise la probabilité de collision par deux. Le backoff exponentiel signifie qu'à chaque fois qu'une station choisit un slot et provoque une collision, le nombre maximum pour la sélection aléatoire est augmenté exponentiellement. Le standard 802.11 définit l'algorithme de backoff exponentiel comme devant être exécuté dans les cas suivant :

- Quand la station écoute le support avant la première transmission d'un paquet et que le support est occupé.
- Après chaque retransmission
- Après une transmission réussie

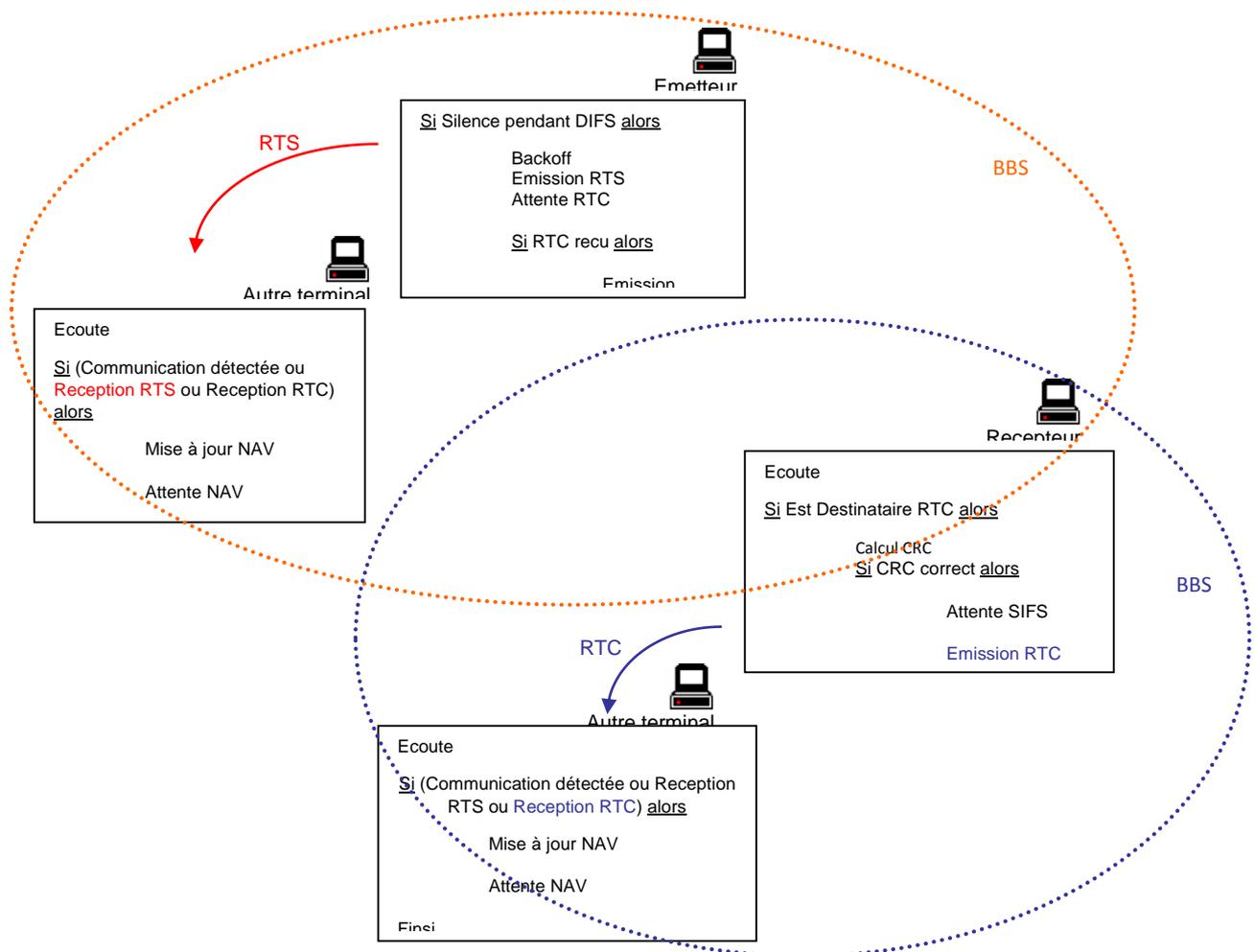
Le seul cas où ce mécanisme n'est pas utilisé est quand la station décide de transmettre un nouveau paquet et que le support a été libre pour un temps supérieur au DIFS.

6. RTC/CTC

Un autre problème spécifique au sans-fil est celui du "nœud caché", où deux stations situées de chaque côté d'un point d'accès peuvent entendre toutes les deux une activité du point d'accès, mais pas de l'autre station, problème généralement lié aux distances ou à la présence d'un obstacle. Pour résoudre ce problème, le standard 802.11 définit sur la couche MAC un mécanisme optionnel de type RTS/CTS (Request to Send/Clear to Send) appelé mécanisme de Virtual Carrier Sense (sensation virtuelle de porteuse).

Lorsque cette fonction est utilisée, une station émettrice transmet un RTS et attend en réponse un CTS. Toutes les stations du réseau recevant soit le RTS, soit le CTS, déclencheront pour une durée fixée leur indicateur NAV pour retarder toute transmission prévue. La station émettrice peut alors transmettre et recevoir son accusé de réception sans aucun risque de collision.

Schématiquement, on a :



Dans ce cas de figure, les trames échangées sont les suivantes :

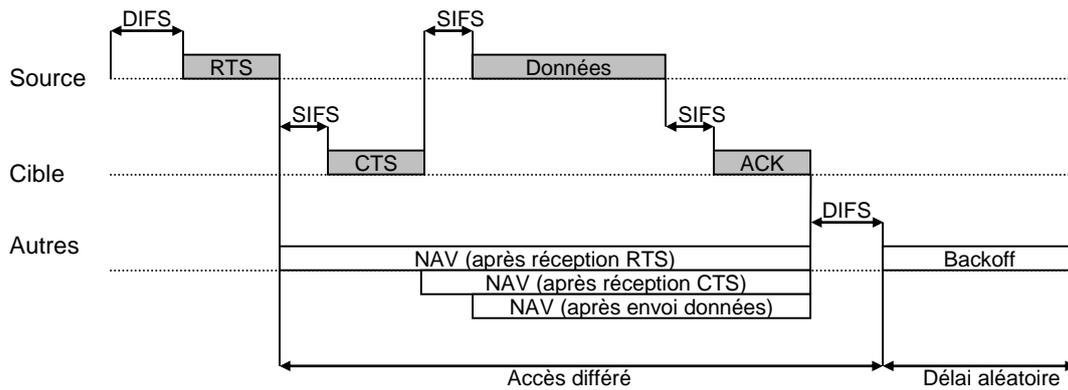


Fig. 6 : La transmission des données dans CSMA/CA (forme RTS/CTS)

Cependant, les trames RTS/CTS ajoutent à la charge du réseau en réservant temporairement le support donc on utilise cette technique seulement pour les gros paquets à transmettre.

Le point négatif de cette politique d'accès est qu'elle est probabiliste : il n'est pas possible de garantir un délai minimal avant l'accès au support, ce qui est problématique pour certaines applications (voix, vidéo, ...).

VII. Fonctions de la couche liaison

La couche liaison c'est l'ensemble des équipements et des logiciels fournissant les moyens fonctionnels nécessaires pour acheminer des données avec un taux d'erreurs garanti dans le but fiabiliser la transmission physique et offrir un service à la couche RESEAU pour acheminer les bits remis par le processus réseau vers leur destination.

La couche liaison de données en 802.11 est composée, à l'instar d'autres normes des familles 802.x, des deux sous-couches LLC 802.2 et MAC 802.11.

- La couche LLC (Logical Link Control) normalisée 802.2 permet de relier un WLAN 802.11 à tout autre réseau respectant l'une des normes de la famille 802.x.
- La couche MAC 802.11 est comparable à la couche MAC 802.3 : elle implante la politique d'accès. Cependant, cette couche MAC est spécifique à l'IEEE 802.11 car elle offre d'avantages de fonctions par rapport à une couche MAC classique (allocation du support, adressage, formatage des trames). Ces fonctions supplémentaires offertes sont normalement confiées aux protocoles supérieurs, comme les sommes de contrôle de CRC, la fragmentation et le réassemblage (très utile car le support radio a un taux d'erreur important), les retransmissions de paquet et les accusés de réception. Cela ajoute de la robustesse à la couche MAC 802.11.

Dans la rubrique précédente on a décrit plusieurs fonctionnalités de cette couche, dans ce qui suit on citera d'autres fonctionnalités :

Les sommes de contrôle et fragmentation :

Dans un réseau sans fil, puisque le taux d'erreur est plus élevé qu'en transmission filaire, les concepteurs ont mis en place un contrôle d'erreur intégré au niveau de la couche liaison de données. Le contrôle d'erreur est basé sur le polynôme de degré 32 suivant :

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

D'autre part le taux d'erreur de transmission sur les réseaux sans fils augmente généralement avec des paquets de taille importante, c'est la raison pour laquelle Wi-fi offre un mécanisme de fragmentation, permettant de découper une trame en plusieurs morceaux, appelés fragments

▪ Etude de trame wi-fi

Les paquets IP composés dans les terminaux du réseau sans fils doivent être transmis sur le support hertzien. Pour cela, ils doivent être placés dans une trame Ethernet. De plus, pour contrôler et gérer la liaison, il est nécessaire d'avoir des trames spécifiques.

Les trois types de trames disponibles dans Wi-fi sont les suivants:

- trame de données, pour la transmission des données utilisateurs;
- trame de contrôle, pour contrôler l'accès au support (RTS, CTS, ACK: cf image précédente)
- trame de gestion, pour les associations ou les désassociations d'une station avec un point d'accès, ainsi que pour la synchronisation et l'authentification.

Toutes les trames sont composées de la manière suivante:

Préambule | PLCP | Données MAC | Corps | FCS

Le préambule est dépendant de la couche physique et contient deux séquences suivantes:

- **Synch**, de 80 bits alternant 0 et 1, qui est utilisée par le circuit physique pour sélectionner la meilleur antenne et se synchroniser dessus.
- **SFD** (Start Frame Delimiter) de 16 bits (000 1100 1011 1101) indique le début de la trame.

Structure d'une trame de données

Contrôle de trame	Durée / ID	Adresse 1	Adresse 2	Adresse 3	Contrôle de séq.	Adresse 4	Données	CRC
2 octets	2 octets	6 octets	6 octets	6 octets	2 octets	6 octets	0 - 2312 octets	4 octets

L'en-tête **PLCP** (Physical Layer Convergence Protocol) contient les informations logiques utilisées par la couche physique pour décoder la trame:

- **FC** (Frame Contrôle): ce champ de deux octets est constitué, entre autres, des informations suivantes:
- To DS (1 bit) et From DS (1 bit), permet de savoir le destinataire et émetteur de la trame,
- More Fragment (1 bit), indique si il reste d'autres fragments dans la trame.
- La zone de données MAC indique la durée d'utilisation du canal, jusqu'à 4 adresses, et un contrôle de séquence
- Un **CRC** assurant l'intégrité du fragment

Cette décomposition de la trame permet de limiter les risques de collision entre les différentes stations.

- **Handover**

Le handover est défini par le Passage d'une cellule à une autre sans interruption de la

Communication. Lorsqu'un terminal se déplace d'une cellule à une autre sans interrompre la communication, cela se fait à peu près de la même manière que dans la téléphonie mobile, mais dans les réseaux sans fil, le handover se fait entre 2 transmissions de données et non pas au milieu d'un dialogue. Le standard IEEE 802.11 ne fournit pas un mécanisme de handover à part entière, mais définit quelques règles :

- Synchronisation.
- Écoute active et passive.
- Mécanismes d'association et de réassociation, qui permettent aux stations de choisir l'AP auquel elles veulent s'associer.

Au niveau d'un BSS, les stations synchronisent leur horloge avec l'horloge du point d'accès, Pour garder la synchronisation, le point d'accès envoie périodiquement des trames balisées appelées Beacon Frames, qui contiennent la valeur de l'horloge du point d'accès. Lors de la réception de ces trames, les stations mettent à jour leurs horloges pour rester synchronisées avec le point d'accès.

VIII. Conclusion

Les réseaux sans fil sont des technologies intéressantes souvent utilisées dans plusieurs domaines tels que l'industrie et le domaine militaire. Les différents avantages qu'apportent ces technologies comme la mobilité et la simplicité d'installation sont la cause de la diversification de ces derniers. Cependant la sécurité reste vulnérable car plusieurs failles ont été détectées dès la première utilisation de ce réseau.

Référence :

Les sites web :

http://www.memoireonline.com/07/09/2324/m_Les-technologies-sans-fil-Le-Wi-Fi-et-la-Securite.html

<http://www.nantes-wireless.org/pages/wiki/index.php>

<http://www.itu.int/newsarchive/press/WRC97/Sharing-the-spectrum-fr.html>

http://fr.wikipedia.org/wiki/Couche_liaison_de_donn%C3%A9es

Les Livres :

Livre sur la norme 802.11 et l'HyperLan : **802.11 vs Hyperlan** par Renaud Garelli –Nicolas Royères –Christian Tschopp

Livre sur les Réseaux sans fil :Cours 2 : **réseaux sans fil**

Livre sur l'HyperLan : **HiperLAN**

Livre sur le Wifi : **WiFi** par Michel Terré

Livre sur La couche liaison du WIFI : **La couche liaison de données** par P.Sicard