I. Introduction :

En ce début du 21eme siècle, les réseaux locaux informatiques connaissent deux évolutions importantes. D'une part, l'utilisation courante du réseau local chez les particuliers, due en grande partie à internet, et d'autre part, l'arrivée en masse des ordinateurs et autres matériels mobiles. Pour cela il faut trouver une technologie permettant de simplifier le câblage du réseau chez un particulier et de préserver la mobilité des produits portables. Un seul principe permet de concilier les deux, le sans fil. [13]

IEEE 802.11 est un standard de réseau sans fil local proposé par l'organisme de standardisation Américain IEEE. La technologie 802.11 est généralement considérée comme la version sans fil de 802.3 (Ethernet). [14]

L'objectif de ce chapitre est de présenter en détail le standard 802.11 qui est le plus utilisé dans les réseaux locaux sans fil. Pour cela, nous commencerons dans une première partie par décrire les topologies suivant lesquels les WLAN 802.11 fonctionnent. Ensuite, nous présenterons les différentes versions du standard et les caractéristiques liées à l'architecture logique de la norme (couche physique et couche MAC).

II. Le standard IEEE 802.11 :

II.1 Généralités :

La première version de la norme IEEE 802.11 est définie en 1997. Des transmissions infrarouges étaient envisagées, les versions les plus récentes du standard sur la base desquelles sont construites l'essentiel des cartes d'interface commercialisées, s'adressent principalement à des transmissions radiofréquences.

Pour définir cette norme, les concepteurs ont pris en considération les points suivants :

- Robustesse et simplicité de la technologie contre les défauts de communication, de pouvoir transmettre dans les meilleures conditions, tenant compte des considérations que le canal de transmission, en l'occurrence l'air, n'est pas aussi fiable que le câble, et qu'il est plus difficile à gérer. Ces caractéristiques ont été vérifiées par l'utilisation d'une approche distribuée du protocole de la couche MAC.
- Utilisation du WLAN mondialement. C'est-à-dire le respect des différentes règles en usage dans les différents pays du monde.

- Totale compatibilité avec les anciens produits et les produits actuels qui composent les réseaux LAN. C'est-à-dire que le passage du WLAN au LAN et vice-versa devra être transparent à l'utilisateur.
- Une sécurité acceptable pour le passage de l'information dans l'air. (WEP).

Cette technologie très intéressante pourra prendre la relève des LAN au sein des entreprises, mais seulement le principal problème vient de la qualité de transmission, puisque le problème de capacité tend de plus en plus à être réduit, par l'augmentation des débits de transmission. Ce problème vient du fait que le canal de transport du WLAN n'est autre que l'air et il va être étudié d'une manière détaillé dans le chapitre suivant. [16], [19]

II.2 La famille IEEE 802 et les standards 802.11:

Le 802.11 est issu de la famille 802, qui est une série de spécifications pour les réseaux locaux. La figure montre la relation entre les différents composants de la famille 802 et leurs emplacements dans le modèle OSI.

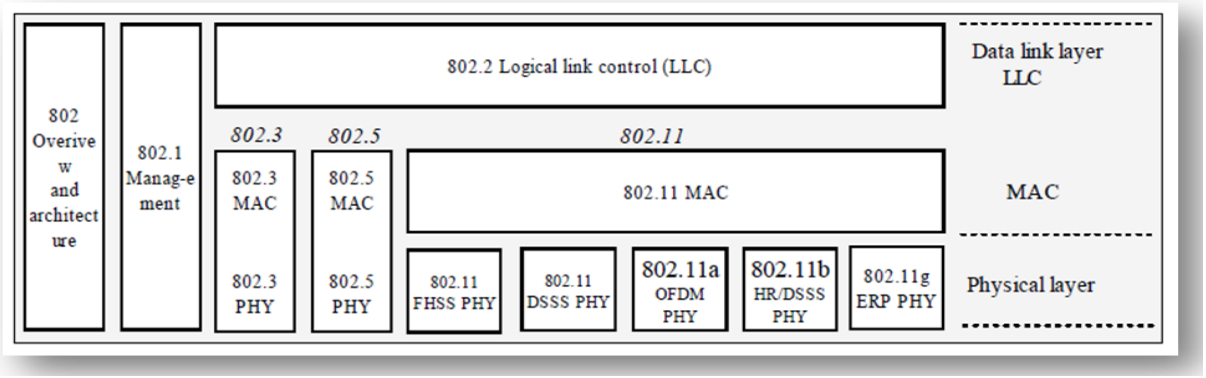

Figure 2.1 : la famille IEEE 802.11

Comme les spécifications 802, le standards IEEE 802.11 couvre les deux couches inferieures du modèle OSI : la couche liaison et la couche physique. La couche MAC définit un ensemble de règles permettant d'accéder au médium et d'envoyer des données, les détails de la réception et de la transmission, sont traiter au niveau de la couche physique. [13]

Actuellement au sein du 802.11 plusieurs groupes de travail ont été crées afin d'améliorer ou de proposer des nouveaux mécanismes régissant divers aspect. Des révisions donc ont été apportées à la norme originale (avec un débit de 1 ou 2 Mbps) afin d'optimiser le débit (c'est le cas des normes 802.11 physiques à savoir les normes 802.11a, 802.11b, 802.11g) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité. [17]

Les différentes révisions de la norme 802.11 sont citées ici : [14], [18]

- **802.11 (norme initiale) :** Dans sa version initiale de 1997, 802.11 proposait trois couches physiques : Radio a étalement de spectre par utilisation de séquences directes (DSSS3), débit bande de base 1 Mbits/s et 2 Mbits/s, Radio a étalement de spectre par utilisation de sauts de fréquences (FHSS3) a 1,6 Mbits/s, Infrarouge, 1 ou 2 Mbits/s.
- **802.11 a :** propose 8 canaux dans la bande des 5 GHz. Cette proposition permet d'atteindre un débit bande de base de 54 Mbits/s sur une portée d'une vingtaine de mètres environ.
- **802.11 b :** propose une amélioration de la norme initiale en introduisant la modulation CCK3 dans la bande des 2,4 GHz. Deux nouveaux débits sont alors disponibles : 5,5 Mbits/s et 11 Mbits/s sur une portée de quelques dizaines de mètres environ. Ratifiée en septembre 1999, 802.11b est l'amendement de 802.11 qui a donné sa popularité au Wifi. Bien que 802.11b soit encore largement utilisé, il est maintenant supplanté par 802.11g.
- **802.11 c :** propose une modification de la norme 802.1d existante pour les réseaux filaires afin de la transposer a 802.11. Elle permet une normalisation de l'interconnexion de niveau 2 (pont) entre un réseau filaire et un réseau Wifi.
- **802.11 d :** propose un protocole d'échange d'informations sur les fréquences et les puissances d'´emission en vue d'une utilisation dans chaque région du monde, quelque soit le pays d'origine du matériel.
- **802.11 e :** propose des outils de Qualité de Service. Les travaux spécifiques de ce groupe de travail seront détaillés et cette norme sera étudiée plus loin dans le chapitre 3.
- **802.11 f :** est une recommandation qui propose une extension pour la communication entre points d'accès compatibles 802.11 par le protocole IAPP en introduisant des capacités de changement de cellules et d'équilibrage des charges (load-balancing).
- **802.11 g :** constitue une amélioration directe de 802.11b en proposant un débit bande de base de 54 Mbits/s sur la bande des 2,4 GHz. Ce gain en débit est réalisé en reprenant le concept de l'´etalement de spectre par OFDM utilisé dans 802.11a. Toutefois, 802.11g garde une compatibilité avec 802.11b, ce qui

signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b.

- **802.11 h :** propose des améliorations pour pallier au futur problème de la sur-utilisation des fréquences dédiées à 802.11. Ce groupe de travail propose d'une part une possibilité de sélection dynamique de fréquence appelée DFS, qui permet de choisir le canal le moins perturbé, et d'autre part le contrôle de puissance TP pour Transmit Power Control, qui permet a l'émetteur de réduire sa puissance d'´emission au minimum nécessaire.
- **802.11 i :** met en place les mécanismes afin de garantir la sécurité. Cette norme définit des techniques de chiffrage telles que l'AES.
- **802.11 n :** son but est d'étendre le standard 802.11 pour atteindre un débit de 540 Mbit/s tout en assurant une rétrocompatibilité avec les trois précédents amendements (a, b et g). Sa porté est d'une centaine de mètre.il utilise les deux bandes 2.4 et 5GHz.
- **802.11 x :** sécurisation de divers médias y compris le lien sans fil par le biais de mécanismes d'authentification fort et de serveur RADIUS avec une distribution dynamique des clés.

II.3 Topologies: [14], [16]

Le réseau sans fil utilisant la norme 802.11 peut être déployé de deux manières différentes : Avec infrastructure ou sans infrastructure (mode Ad Hoc).

II.3.1 Réseaux WLAN avec Infrastructure :

Le réseau à infrastructure comprend des points d'accès ou Access Point qui gèrent l'ensemble des communications dans une même zone géographique sous la forme de cellule. Ce mode de gestion géographique ressemble un peu au modèle GSM ou UMTS. D'ailleurs il fonctionne de façon presque similaire, car les stations munies de carte WLAN peuvent se déplacer dans la zone de couverture de l'AP et effectuer un roaming entre les différents AP si la topologie le permet (chevauchement des cellules). Il faut remarquer que chaque AP possède une connexion LAN, ou un autre type de connexion lui assurant la connexion avec le réseau fixe.

Le réseau est alors formé de plusieurs BSS qui forment ensemble un unique EBSS.

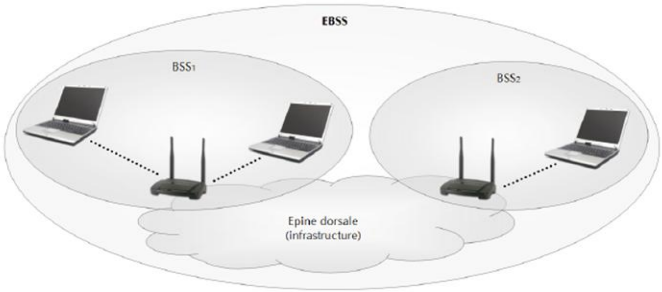

Figure 2.2 : Réseau WLAN avec infrastructure

II.3.2 Réseau WLAN Ad Hoc :

Un réseau Ad Hoc ou encore IBSS (Independent Basic Service Set) est un ensemble de stations possédant une carte WLAN sans la présence d'un AP. Contrairement au réseau à infrastructure, les stations dans un réseau Ad Hoc communiquent directement entre elles.

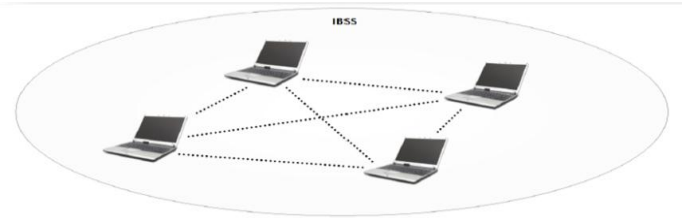

Figure 2.3: Réseau WLAN Ad Hoc

II.4 Architecture de la norme IEEE 802.11: [15], [22]

La norme IEEE 802.11 définit les deux premières couches (basses) du modèle OSI, à savoir la couche physique et la couche liaison de données. Elle introduit des modifications sur la couche basse du niveau lien (donc niveau MAC) et sur le niveau physique avec le support de plusieurs méthodes d'accès radio (donc la définition de plusieurs couches physiques). Il est à noter que la nouvelle couche MAC est commune à toutes les couches physiques. La figure2.4 illustre l'architecture en couches de la norme IEEE 802.11.

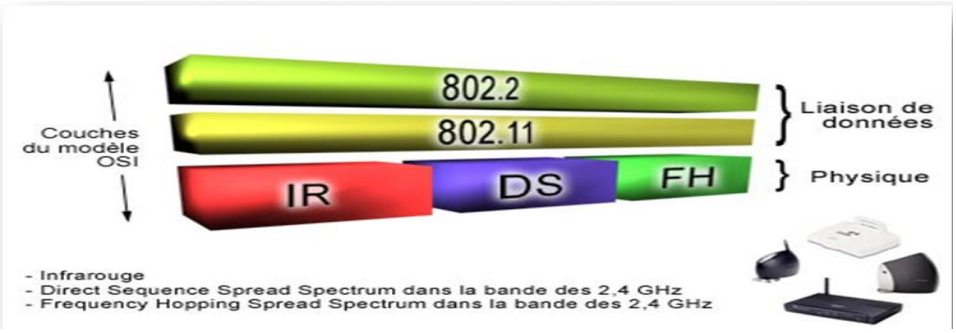

Figure 2.4 : Description des couches IEEE 802.11

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations. [20]

II.4.1 La couche physique :

La norme IEEE 802.11 définit deux sous-couches physiques :

- PMD (Physical Media Dependant) : gère l'encodage des données et la modulation.
- PLCP (Physical Layer Convergence Procedure): s'occupe de l'écoute du support et est directement reliée à la couche MAC pour lui signifier que le support de transmission est libre.

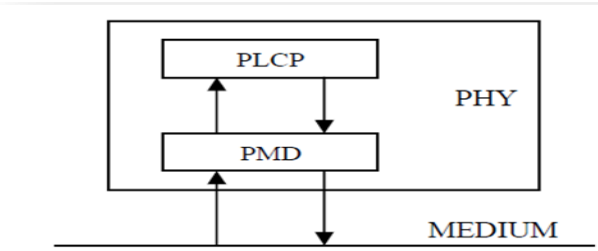

Figure 2.5 : Les deux sous couches physique du standard 802.11

Le standard 802.11 d'origine a défini trois couches physiques de base, FHSS, DSSS, IR, auxquelles ont été rajoutées trois nouvelles couches physiques Wifi (avec deux variantes au sein de la solution 802.11b) et Wi-Fi5 (802.11a/g).la figure suivante illustre ça :

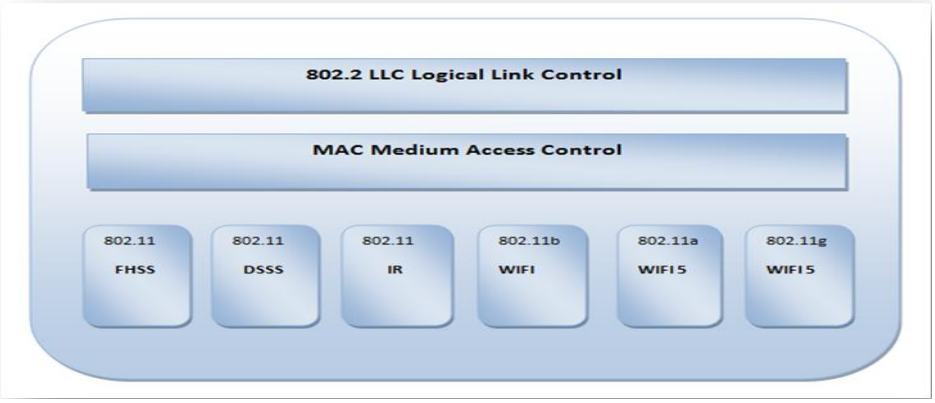

Figure 2.6 : Les couches physique du standard 802.11

i. Les couches physiques de base :

- **FHSS (Frequency Hopping Spread Spectrum):** [15] , [20], [22], [23]

La technique **FHSS** (Frequency Hopping Spread Spectrum, en français étalement de spectre par saut de fréquence ou étalement de spectre par évasion de fréquence) 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 est ainsi réalisée 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. L'émetteur et le récepteur s'accordent sur un schéma de saut, et les données sont envoyées sur une séquence de sous-canaux. Chaque conversation sur le réseau 802.11 s'effectue suivant un schéma de saut différent, et ces schémas sont définis de manière à minimiser le risque que deux expéditeurs utilisent simultanément le même sous-canal.

L'étalement de spectre par saut de fréquence a originalement été conçu dans un but militaire afin d'empêcher l'écoute des transmissions radio. En effet, une station ne connaissant pas la combinaison de fréquence à utiliser ne pouvait pas écouter la communication car il lui était impossible dans le temps imparti de localiser la fréquence sur laquelle le signal était émis puis de chercher la nouvelle fréquence. Aujourd'hui les réseaux locaux utilisant cette technologie sont standards ce qui signifie que la séquence de fréquences utilisées est connue de tous, l'étalement de spectre par saut de fréquence n'assure donc plus cette fonction de sécurisation des échanges.

FHSS est désormais utilisé dans le standard 802.11 de telle manière à réduire les interférences entre les transmissions des diverses stations d'une cellule.

Les techniques FHSS simplifient -- relativement -- la conception des liaisons radio, mais elles sont limitées à un débit de 2 Mbps, cette limitation résultant essentiellement des réglementations de l'ETSI qui restreignent la bande passante des sous-canaux à 1 MHz. Ces contraintes forcent les systèmes FHSS à s'étaler sur l'ensemble de la bande des 2,4 GHz, ce qui signifie que les sauts doivent être fréquents et représentent en fin de compte une charge importante.

En mode FHSS les données sont émises au moyen d'une modulation GMSK.

L'un des avantages du FHSS est qu'il permet, théoriquement, de faire fonctionner simultanément 26 réseaux 802.11 FHSS (correspondant aux 26 séquences) dans une même zone, chaque réseau utilisant une des séquences prédéfinies.

Un autre avantage du FHSS est sa résistance face aux interférences, comme le système saute toutes les 300 ms d'un canal à un autre sur la totalité de la bande, si des interférences surviennent sur une partie de la bande ISM (un ou plusieurs canaux), cela n'engendre pas de trop importantes pertes de performances.

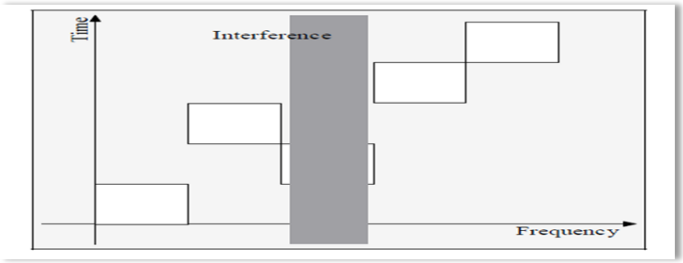

Figure 2.7 : Changement de fréquence dans FHSS

Une trame au niveau physique est composée de trois parties. Elle débute par un préambule, suivi d'un entête et terminée par la partie donnée :

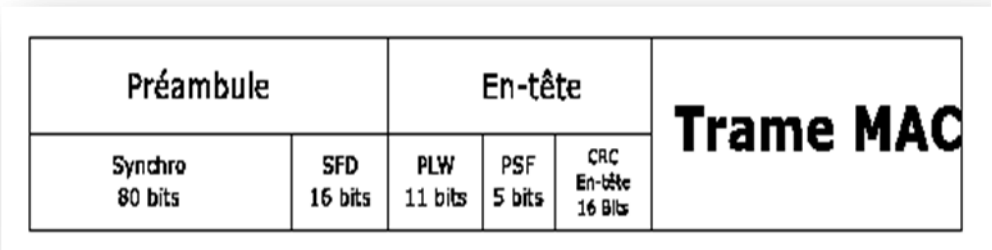

Figure 2.8 : Structure de la trame 802.11 au niveau physique pour le FHSS

Chaque champ de chaque partie possède un rôle spécifique :

- **Le préambule :**
  - La synchro est une séquence de synchronisation qui est composée d'une suite de 80 bits constitués en alternance de 0 et de 1. Elle permet à la couche physique de détecter la réception d'un signal. Elle permet accessoirement aussi, de choisir la meilleure antenne de réception si le choix existe.
  - Le Start Frame Delimiter (SFD) est l'identificateur de trame. Il est constitué par la suite de bits suivants : 0001100101101101.
- **L'entête :**
  - Le PSDU Length Word (PLW) est un paramètre passé par la couche MAC qui indique la longueur de la trame. C'est donc la longueur de la partie de donnée dans cette trame.

- Le PSF est un champ sur 5 bits qui permet de définir la vitesse de transmission. Le premier bit est toujours à 0. Les bits 1, 2 et 3 sont réservés et définis par défaut à zéro. Le 4ème et dernier bit, indique la vitesse de transmission. A 1Mb/s s'il est à 0 et à 2Mb/s s'il est à 1.
- Le CRC de l'entête est le champ de contrôle d'erreur de l'entête, composé de 16bits.

▪ **La partie donnée :** La Trame MAC contient les données relatives à la couche MAC.

- **DSSS (Direct Sequence Spread Spectrum):** [13], [15], [22], [20], [23]

Dans le but de lutter contre les interférences importantes mais n'affectant que des plages de fréquences assez étroites, il existe la technique de l'étalement de spectre.

Comme le FHSS, le DSSS divise la bande ISM en sous bandes. Cependant la division se fait ici en 14 canaux de 20 MHz chacun. La transmission ne se fait que sur un canal donné. La largeur de la bande ISM étant égale à 83.5 MHz, il est impossible d'y placer 14 canaux adjacents de 20 MHz. Les canaux se recouvrent donc, comme illustré à la figure suivante.

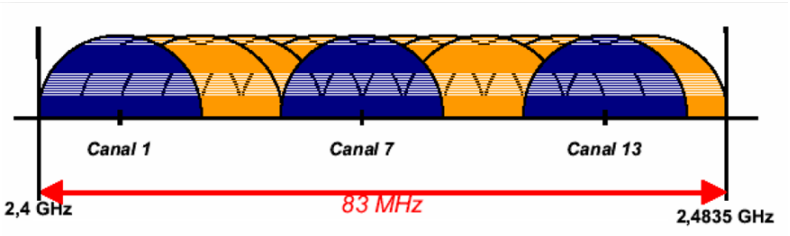

Figure 2.9 : Décomposition de la bande ISM en sous canaux

Comme le montre le tableau suivant, les fréquences centrales de chaque sous-canal sont espacées de 5 MHz.

Canal	Fréquence centrale (GHz)	Canal	Fréquence centrale (GHz)
1	2.412	8	2.447
2	2.417	9	2.452
3	2.422	10	2.457
4	2.427	11	2.462
5	2.432	12	2.467
6	2.437	13	2.472
7	2.442	14	2.477

Tableau 2.1: Fréquences centrales des sous canaux du mode DSSS

Comme la transmission ne se fait que sur un canal, les systèmes DSSS sont plus sensibles aux interférences que les systèmes FHSS, qui utilisent toute la largeur de bande.

L'utilisation d'un seul canal pour la transmission est un inconvénient si différents réseaux 802.11 DSSS se superposent.

Lorsqu'un canal est sélectionné, le spectre du signal occupe une bande comprise entre 10 et 15 MHz de chaque coté de la fréquence centrale. La valeur 15 MHz provient de la décroissance non idéale des lobes secondaires de la modulation utilisée. Il n'est donc pas possible d'utiliser dans la même zone géographique les canaux adjacents à ce canal.

Pour permettre à plusieurs réseaux d'émettre sur une même cellule, il faut allouer à chacun d'eux des canaux appropriés, qui ne se recouvrent pas. Par exemple, considérons deux réseaux utilisant DSSS. Si l'un d'eux utilise le canal 6, le canal 5 et 7 ne peut pas être utilisé par le deuxième réseau, car trop proche. Il en va de malheureusement de même pour les canaux 2, 3,4, 8, 9 et 10, qui ne peuvent non plus être alloués du fait de l'étalement de la bande passante du canal 6. Les canaux qui peuvent être utilisés sont les canaux 1, 11, 12, 13 et 14. Sachant que la largeur de bande n'est que de 83.5 MHz, il ne peut donc y avoir au maximum que trois réseaux 802.11 DSSS émettant sur une même cellule sans risque d'interférences.

Dans le standard 802.11 DSSS, La technique du « chipping sur 11 bits » aide à compenser le bruit généré par un canal donné, cette technique consiste à transmettre pour chaque bit une séquence Barker (parfois appelée bruit pseudo-aléatoire, noté PN) de bits. Ainsi chaque bit valant 1 est remplacé par une séquence de bits et chaque bit valant 0 par son complément. La couche physique de la norme 802.11 définit une séquence de 11 bits (*10110111000*) pour représenter un 1 et son complément (*01001000111*) pour coder un 0. On appelle *chip* ou chipping *code* (en français *puce*) chaque bit encodé à l'aide de la séquence *Barker*.

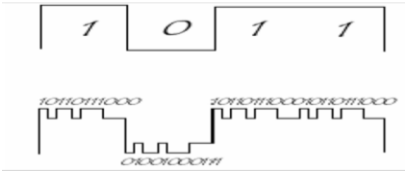

Figure 2.10 : Technique du chipping

Grâce au chippin*g*, de l'information redondante est transmise, ce qui permet d'effectuer des contrôles d'erreurs sur les transmissions.

Pour supporter les environnements plus bruyants et étendre la portée des équipements, les WLAN 802.11b utilisent la variation dynamique du débit, qui permet d'ajuster les taux de transmission automatiquement pour compenser les variations du canal radio. Dans une situation idéale, les utilisateurs se connectent à un taux de 11 Mbps plein.

Les caractéristiques du DSSS varient selon chaque pays, notamment ce qui concerne le nombre de sous canaux utilisés, ce qui peut remettre en cause la superposition de réseaux. Le tableau suivant montre ça :

Pays	**Etats-Unis**	**Europe**	**Japon**	**France**
Nombres de sous canaux utilisés	1 à 11	1 à 13	14	10 à 13

Tableau 2.2 : Nombre de canaux disponibles pour le DSSS en fonction du pays

Une trame au niveau physique est composée, comme pour la technique précédente, de trois parties : un préambule, puis un entête et enfin la partie données :

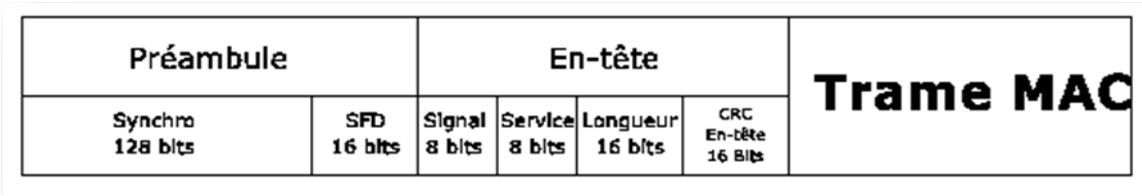

Figure 2.11 : Structure de la trame 802.11 au niveau physique pour le DSSS

- **Le préambule :**
  - La synchro est une séquence de synchronisation pseudo-aléatoire. Elle sert à la synchronisation au niveau récepteur.
  - Le Start Frame Delimiter (SFD) permet au récepteur de détecter le début de la trame. ce champ de deux octets vaut en hexadécimal F3A0.
- **L'entête :**
  - Le signal permet d'indiquer la vitesse de transmission sélectionnée. Si la valeur de ce champ est à 0A (en hexadécimal) la transmission se déroulera à 1Mb/s et si celle ci est à 14 (en hexadécimal), la transmission se déroulera à 2Mb/s. Il faut savoir qu'en fonction de la vitesse de transmission, une modulation différente est appliquée. Le differential binary phase shift

keying est utilisé lors d'une transmission à 1Mb/s et en opposition au Differential quadrature phase shift keying lors d'une transmission en 2Mb/s.

- Le service est réservé pour un usage futur La valeur 00 signifie que le transmetteur est conforme à la norme IEEE 802.11.
- La longueur indique la valeur de la longueur de la partie de données. Sa valeur peut varier entre 4 et 2^{16}.
- Le CRC de l'entête : est le champ de contrôle d'erreur de l'entête.

- **La partie donnée :**
  - La Trame MAC contient les données de la trame physique. Elles sont transmises selon la modulation sélectionnée dans le champ signal.
  - **IR (Infra Rouge):**

Le standard IEEE 802.11 prévoit également une alternative à l'utilisation des ondes radio : la lumière infrarouge. La technologie infrarouge a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission de données. [21]

Ainsi les transmissions se font de façon unidirectionnelle, soit en "vue directe" soit par réflexion. Le caractère non dissipatif des ondes lumineuses offre un niveau de sécurité plus élevé.

Il est possible grâce à la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelé **PPM**.

La modulation *PPM* consiste à transmettre des impulsions à amplitude constante, et à coder l'information suivant la position de l'impulsion. Le débit de 1 Mbps est obtenu avec une modulation de *16-PPM*, tandis que le débit de 2 Mbps est obtenu avec une modulation *4-PPM* permettant de coder deux bits de données avec 4 positions possibles

La méthode IR se base sur la diffusion d'une lumière infrarouge de longueur d'onde comprise entre 850 et 950 nm (nanomètres). Grâce aux caractéristiques réflectives de l'infrarouge, les stations appartenant au réseau ne doivent pas nécessairement être dirigées les unes vers les autres. Cependant, vu la portée très faible de l'infrarouge, les stations ne peuvent être éloignées les unes des autres de plus d'une dizaine de mètres. Un réseau 802.11 IR ne peut donc être déployé que dans un espace ayant la dimension d'une pièce. [22]