

TPs de radio- communications

P. CLERC
J.M. GORCE
J. VERDIER
G. VILLEMAUD,

SOMMAIRE

<i>TP 1-2 : outil d'aide à la planification des réseaux mobiles</i>	3
1. Introduction	3
2. Questions préalables.....	3
3. Prise en main du logiciel	4
4. Etude de propagation et dimensionnement.....	7
<i>TP 3 : Mesures du lien radio en GSM</i>	13
1. Matériel	Erreur ! Signet non défini.
2. caractérisation spectrale des fréquences GSM.....	14
3. étude du gsm sur le campus.....	15
<i>TP 4 : caractéristiques radio des réseaux locaux d'accès sans fil</i>	16
1. Matériel	16
2. analyse de couverture.....	17
3. Relation entre le niveau de signal et le taux de transmission	19
4. Interférences entre plusieurs réseaux.....	20
5. Planification	Erreur ! Signet non défini.
<i>Le GSM : planification et dimensionnement</i>	21
6. introduction.....	21
7. La norme GSM.....	21
8. Contraintes radio.....	22
9. Contraintes de trafic	27
10. Dimensionnement du réseau GSM	28
11. Planification du réseau	31
12. Prédiction de couverture radio	32
<i>Les réseaux locaux sans fil (RLANs)</i>	33
1. Introduction : la norme IEEE802.11b	33
2. Topologies des réseaux IEEE 802.11b	34
3. Anatomie d'un LAN sans-fil 802.11b	37
4. La couche physique : le modem radiO	40
5. La couche MAC.....	45

TP 1-2 : outil d'aide à la planification des réseaux mobiles

1. INTRODUCTION

Ce TP est réparti sur 2 séances. Il s'agit de prendre en main un logiciel d'aide à la planification de réseaux mobile de 2^{ème} génération : le GSM.

Le logiciel utilisé Atoll©, commercialisé par la société Forsk, est un logiciel professionnel à destination des opérateurs. Ce TP utilise une version de démonstration, distribué gratuitement, mais qui est relativement complète. L'inconvénient majeur est qu'il est impossible de sauvegarder une configuration donnée. Toutefois, ce TP permet de comprendre les problématiques réelles de déploiement de réseau mobile.

Les problématiques abordées ici recouvrent les antennes, la propagation, la couverture radio, et l'architecture cellulaire.

La partie 2 contient quelques questions dont vous trouverez les réponses dans le cours ou dans les annexes. Il est souhaitable d'y répondre avant de venir en TP.

La partie 3 contient un ensemble de questions destinées à vous aider à prendre en main le logiciel. Il est souhaitable de ne pas y passer plus de 2 heures. Les questions sont là pour vous aider, mais ne devront pas être rendues dans le rapport.

La partie 4 contient le cœur du travail qui vous est demandé. Un rapport devra être rendu à la fin des 2 séances, dans lequel vous proposerez un déploiement cellulaire exploitant uniquement une sous-bande de la bande de fréquences GSM. Vous expliquerez les étapes par lesquelles vous êtes passés pour établir la solution que vous préconisez. Vous donnerez des résultats en terme de taux de blocage, de pourcentage de couverture, etc...

Il vous est conseillé de finir la partie 4-2 à la première séance (premier dimensionnement) et d'effectuer l'optimisation du réseau à la deuxième séance (vous veillerez à sauvegarder proprement votre configuration pour pouvoir facilement reprendre à la deuxième séance).

2. QUESTIONS PREALABLES

2.1 QUESTIONS D'ORDRE GENERAL

- Quelle est la bande de fréquence utilisée en GSM ?
- Quel est le nombre de canaux disponibles pour chaque opérateur sur la bande GSM et sur la bande DCS1800.

2.2 COUVERTURE ET ANTENNES

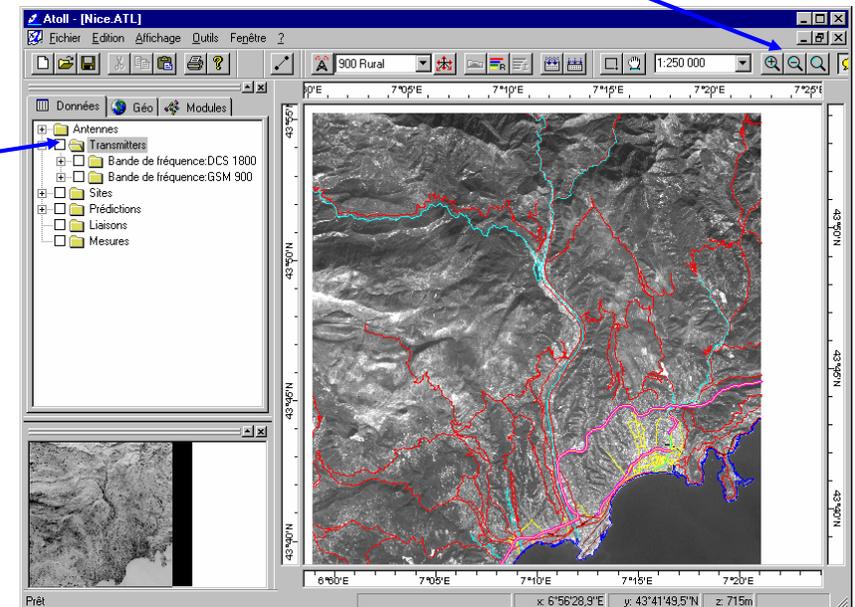
- A quoi correspondent les termes suivant : dBm, dBW, dBi, PIRE.
- Rappelez quelles sont les principales méthodes de prédiction de couverture radio. Quels sont les différents paramètres qui peuvent être pris en compte pour améliorer la prédiction de couverture ?
- Qu'entend-on par 'dégagement du 1^{er} ellipsoïde de Fresnel' ?
- Que calcule à votre avis une prédiction de lien radio en visibilité directe ?

3. PRISE EN MAIN DU LOGICIEL

3.1 DEMARRAGE

Pour démarrer dans une configuration exploitable directement vous devez effectuer les opérations suivantes :

- 1- Après avoir démarré le logiciel, chargez l'exemple Nice.ATL, localisé dans C:\Program Files\Forsk\Atoll\Samples.
- 2- Dans la fenêtre de paramétrage, sélectionnez l'onglet Données, et décochez tous les répertoires (Transmitters, Sites, Prédiction...).
- 3- Utilisez les boutons de zoom pour visualiser l'ensemble de la carte
- 4- Vous devez obtenir la représentation ci-dessous :



3.2 DONNEES GEOGRAPHIQUES

Dans la fenêtre de paramétrage, sélectionnez l'onglet 'Geo'.
Repérez les différents types de données présents et leur rôle.
Vous avez la possibilité, sur chacun des items des menus, de cliquer dessus avec le bouton droit de la souris (ou de double-cliquer avec le bouton de gauche pour appeler un menu contextuel).
Faites-le notamment pour les items «Traffic Density» et «Clutter», et étudiez les tableaux de données.
☺ Quelle est leur utilité pour la planification ?

3.3 MODELES DE PREDICTION

Dans la fenêtre de paramétrage, sélectionnez l'onglet 'Modules'.
Développez le menu 'Modèles de propagation'.
Développez les menus du modèle d'Okumura-Hata, et repérez les différents modèles existants.
Qu'est-ce qui change entre les différents modèles ?
Cliquez avec le bouton de droite sur l'item 'Okumura-Hata', et étudiez la configuration.
Repérez le lien les différents champs du tableau et les 'clutter', définis dans les données géographiques.
Repérez en visualisant les clutter sur la carte :
☺ Le paramétrage d'Okumura-Hata le plus utilisé en zone rurale.
☺ Le paramétrage d'Okumura-Hata le plus utilisé en zone urbaine.

3.4 DIMENSIONNEMENT DU SYSTEME

3.4.1 Utilisation des menus pour les sites et les émetteurs

Dans la fenêtre de paramétrage, revenez à l'onglet 'Données'.
Visualisez les sites (cochez le bon item), et zoomez convenablement sur la zone de terrain que l'on cherche à couvrir.
Pour les émetteurs, comme pour les sites, il est possible d'appeler un menu contextuel en cliquant avec le bouton de droite (ou 2x avec le bouton de gauche pour appeler la fenêtre des propriétés).
De même, en cliquant 2 fois avec le bouton de gauche sur les répertoires sites ou émetteurs on obtient la liste avec les paramètres correspondant.
Deux types de sites sont affichés, représentés par une couleur verte ou rouge.
☺ Qu'elle est la différence entre ces 2 types de sites ?
Visualisez les émetteurs associés. Cliquez 2 fois avec le bouton gauche sur l'item 'Bande de fréquences :GSM900', dans le menu 'transmitters'.
☺ Recensez les informations auxquelles vous avez accès et qui vous semblent intéressantes pour la planification.

☺ Analysez la répartition des émetteurs sur le terrain (entre GSM900 et DCS1800), et justifiez la répartition faite entre les 2 bandes de fréquences.
☺ Combien y a-t-il d'émetteurs par site ? Recensez les différentes antennes utilisées et donnez pour chacune l'angle d'ouverture. Regardez pour cela les caractéristiques des émetteurs.
Résumez les propriétés des émetteurs, et allez chercher les caractéristiques d'antennes dans le menu antennes, en sélectionnant l'antenne correspondante.

A chaque transmetteur, il est possible d'associer une méthode de calcul de propagation spécifique. Toutefois, en la paramétrant 'par défaut', la méthode utilisée sera celle qui est précisée lors du calcul, globalement (voir plus loin).
☺ Quel est le modèle de propagation associé à chaque type d'émetteur ?

Sélectionnez, dans le menu 'site', un des sites GSM. Faites afficher la 'zone en visibilité' en ligne directe. Vérifiez la prise en compte de la géographie de terrain en affichant les données terrain d'élévation. Utilisez l'icône de visualisation de profil.

☺ A quoi peut servir cette représentation ?

3.5 PREDICTION DE COUVERTURE

3.5.1 Analyse de couverture

Repérez les différentes études qui sont faites en terme de couverture hertzienne. (dans l'item prédictions)
Dans l'item propagation, en cliquant 2x, on obtient la fenêtre des propriétés. La méthode de calcul de prédiction (par défaut Okumura-Hata), est définie. Cependant, le moteur de prédiction peut être adapté émetteur par émetteur et est défini dans les propriétés de chaque émetteur, ou groupe d'émetteur (comme précisé ci-dessus). Dans ce cas, c'est la méthode qui est précisée dans les propriétés des émetteurs qui est prépondérante. Pour éviter toute confusion, mettez le modèle de propagation de chaque émetteur à une valeur 'par défaut'.
☺ Etudiez les différentes propriétés paramétrables pour le calcul de prédiction.
☺ Affichez les couvertures GSM et DCS.
☺ Quels sont les différents paramètres associés à chaque type de résultat (Interférences, Signal Level, Coverage).
☺ Quel est l'intérêt de chacune de ces estimations ?

3.5.2 Analyse du plan fréquences

☺ Recherchez quels sont les canaux BCCH (voix balise) associés à chaque Tx, et représentez-les sur le diagramme de couverture. Donnez une vision schématique du plan de fréquences BCCH. Représentez l'identificateur de chaque émetteur (BSIC). Quelles sont les fréquences balises réutilisées ?
Le BSIC (Base Station Identity Code), est un code de 'couleur' qui permet de distinguer des émetteurs utilisant la même fréquence de voix balise. Un mobile à mi-distance entre ces 2 stations de base risque de recevoir simultanément les voix balises des 2 stations. Pour permettre de les dissocier, les signaux émis sur la voix balise sont codés différemment. Il y a 8

codes possibles par voix balise. Dans le tableau donné dans Atoll, le premier chiffre est un code standard par pays (1), et le 2^{ème} est un code de couleur compris entre 0 et 7.

3.5.3 Analyse d'interférences

- ☉ Etudiez les interférences. Quel est le principe de calcul d'interférences? Quel niveau de signal limite est défini ? Est-ce que ça vous paraît judicieux ? Comment sont-elles calculées ? Comment expliquez-vous ce faible taux d'interférences ?
- ☉ Recalculez les interférences pour le GSM900, en changeant le paramètre de niveau de brouillage à 18dB au lieu de 10dB. Relancez le calcul d'interférences.
- ☉ Analysez pour les sites 48, 52, 55, les sites voisins qui brouillent le plus. Utilisez pour cela le bouton 'interférences' du menu principal.

4. ETUDE DE PROPAGATION ET DIMENSIONNEMENT

4.1 MANIPULATIONS PREALABLES

4.1.1 Suppression du déploiement initial

Sélectionnez successivement, dans l'onglet «données», chaque émetteur puis supprimez-le. Supprimez ensuite les différents sites. Sélectionnez alors chaque item de prédiction, puis supprimez-le également.

4.1.2 Réglage par défaut transmetteurs

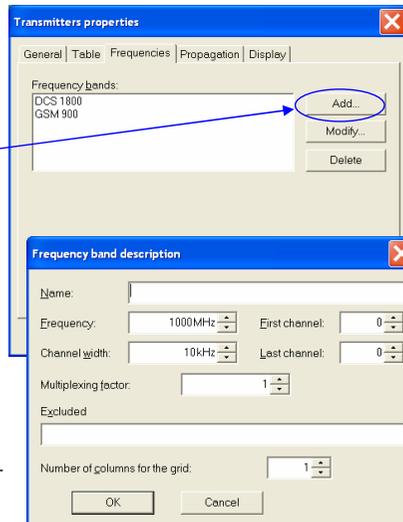
Par clic droit sur l'item 'transmetteurs' dans la fenêtre 'data', vous obtenez un menu contextuel de paramétrage des transmetteurs. Cliquez sur 'propriétés'. On s'intéresse aux onglets 'fréquences', et 'propagation'.

→ Fréquences :

- vous supposez être un opérateur disposant de 62 canaux en fréquence : soit les canaux de 1 à 62 → Effectuez ce paramétrage.
- Paramétrez correctement le facteur de multiplexage (cf section 10.1).

→ Propagation :

- différents modèles de propagation sont disponibles. Il est possible d'en choisir un spécifiquement. Il est en fait préférable de régler ici la valeur 'par défaut'. Le modèle utilisé sera alors spécifié au moment du calcul de propagation.



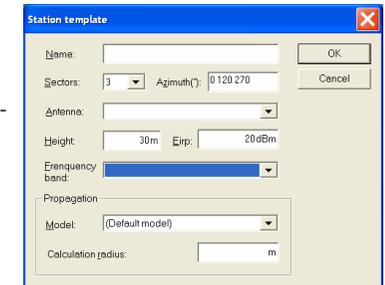
4.1.3 Création d'un site type

Pour faciliter le déploiement de plusieurs sites identiques, il est possible de définir plusieurs sites types. Ils sont visibles dans le menu déroulant présentant par défaut la valeur «rural». Cliquez sur ce menu, et sélectionnez «paramétrage». Vous pouvez alors définir un nouveau type de site qui aura les propriétés suivantes :

Pour faciliter le déploiement de sites, vous utiliserez le bouton spécifique, dans le menu principal.

Il faut donc configurer correctement le site par défaut. Créez un nouveau type de site.

- Créez ce site de type omnidirectionnel (1 secteur).
- Sélectionnez une antenne adéquate.
- Sélectionnez une PIRE de 35dBm.
- Choisissez la bonne bande de fréquence (définie ci-dessus)
- Réglez le modèle de propagation par défaut.



Pour déployer ce site type, il vous suffit de cliquer sur le bouton du menu principal, situé à côté de ce menu déroulant.

4.2 DIMENSIONNEMENT

Vous avez maintenant tous les éléments de départ pour commencer la planification de votre réseau. Pour démarrer il va vous falloir dimensionner : c'est-à-dire calculer la taille et le nombre de cellules qu'il va falloir positionner.

Dans une phase de déploiement initial d'un réseau, on raisonne à partir d'un modèle de répartition des cellules GSM selon le schéma hexagonal (ou nid d'abeille), voir annexe.

Vous disposez de 64 fréquences.

4.2.1 Facteur de réutilisation

- Calculez le facteur de réutilisation à utiliser (voir annexe). Déduisez-en le nombre maximal de fréquences que vous pouvez allouer à une cellule pour limiter les interférences. Vous prendrez un modèle d'affaiblissement en $n=3$, et vous chercherez à garantir 12dB de C/I.

4.2.2 Taille des cellules

→ Déduisez-en la taille maximale des cellules à déployer en zone urbaine, pour absorber le trafic voix, avec un taux de blocage inférieur à 2% (on pourra ensuite essayer d'améliorer ce taux de service).

→ Calculez alors le rayon maximal de ces cellules.

4.2.3 Réglage des émetteurs

→ Vous pouvez maintenant améliorer vos sites en choisissant une puissance d'émission peut-être différente de 35dBm, en réglant le tilt et la hauteur de l'antenne. Vous pouvez positionner un ou plusieurs sites et regarder les simulations de couverture. Pensez qu'un recouvrement minimal est nécessaire entre cellules voisines pour permettre le handover.

4.2.4 Déploiement régulier

→ 1 fois les réglages faits, vous pouvez effectuer un premier déploiement régulier, selon un modèle hexagonal, en respectant les distances que vous avez calculées. Pour vous aider à positionner les antennes, vous pouvez afficher une grille autour de chaque site, de taille égale aux cellules maximales que vous souhaitez avoir. Pour cela : clic droit sur l'item 'site' de la fenêtre principale, et ouvrez le menu 'grilles'.

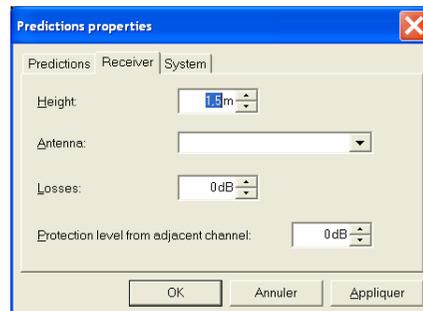
4.3 ETUDE DE COUVERTURE

Une fois les sites positionnés, il faut maintenant simuler le comportement du réseau. Pour cela, il faut effectuer un calcul de couverture radio. On s'intéressera plus particulièrement aux zones urbaines.

4.3.1 Paramétrage global des prédictions

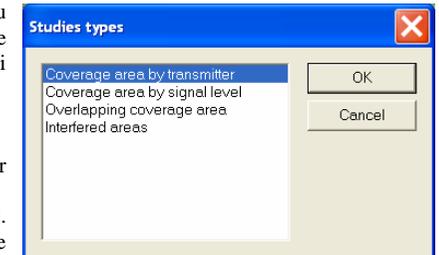
Par un clic droit sur l'item 'prédictions' du menu principal, accédez au menu 'propriétés', et réglez les 3 onglets 'prédictions', 'récepteur' et 'système' → Justifiez tous vos choix.

Remarque : la résolution, paramétrable dans l'onglet 'prédictions', permet de régler le pas des simulations. Un pas trop grossier vous fournira des résultats trop approximatifs, alors qu'un pas trop fin alourdira très fortement les temps de calcul. Vous pouvez le modifier au fur et à mesure de votre travail, en affinant les prédictions une fois les réglages faits, par exemple.



4.3.2 Calculs de couverture

Par un clic droit sur l'item 'prédictions' du menu principal, vous pouvez lancer une nouvelle prédiction en cliquant sur l'item 'nouveau' qui vous ouvre le menu suivant :



Etudiez rapidement ces 4 types de prédiction.

On va s'intéresser au calcul de couverture par transmetteur.

→ Réglez la simulation et lancez le calcul.

Analysez votre résultat et évaluez la qualité de votre simulation : trous de couverture ? Sur-recouvrement ? Cellules trop grandes ? Trop petites ? Vous donnerez cette analyse, avec une figure bien choisie, dans le compte-rendu.

Remarquez en particulier les problèmes de bords.

Vous pouvez utiliser le bouton de visualisation des niveaux de signal de réception (bouton 'R' du menu principal), pour évaluer le niveau de signal reçu en tout point.

Vous pouvez également lancer une simulation de couverture par niveau de champ, pour repérer les anomalies, en combinant les 2 visualisations.

4.4 OPTIMISATION DU DEPLOIEMENT

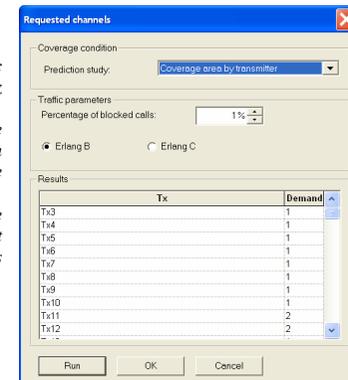
4.4.1 Réglages des sites

A partir des observations faites dans la partie précédente, proposez des améliorations de votre réseau (réglage de la puissance d'émission, tilt, déplacement sur un point haut (menu site), ajout/suppression de sites, changement de l'antenne, sélection de différents modèles de propagation, ...).

→ Vous détaillerez votre démarche, et les différentes améliorations proposées, et comparerez la solution finale à la solution obtenue dans la partie précédente.

Quelques remarques :

- Vous rendrez un document précisant la configuration choisie avec l'illustration de la couverture, en niveaux et par émetteur. Vous justifierez vos choix et vous décrierez la méthode employée pour arriver à cette solution.
- Vous noterez précisément le paramétrage des sites en sauvegardant la liste des sites et des émetteurs, que vous rendrez avec le compte-rendu : donnez en annexe de votre document, les tableaux listant les sites et les émetteurs que vous avez positionnés
- Pour accélérer les calculs de prédiction, vous réglerez de façon appropriée la portée supposée des émetteurs, ainsi que le pas de calcul. (cf onglet prédiction/propriétés). Attention, à ne pas trop réduire la portée, sinon vous n'aurez plus aucune interférence dans la suite ...



4.5 EVALUATION DE LA QoS

4.5.1 Nombre de canaux requis

Le logiciel est capable de calculer le nombre de canaux requis pour chacune des cellules, en fonction de sa zone de couverture et du trafic associé.

Lancez ce calcul à l'aide du menu disponible sur l'item 'transmetteurs'.

Réglez les différents paramètres et justifiez vos choix.

En fonction du résultat obtenu, vous pouvez éventuellement modifier le réseau obtenu à l'étape précédente → détaillez vos modifications.

4.5.2 Affectation des code BSIC

→ Lancer l'affectation automatique des codes BSIC, et modifiez au besoin votre configuration de façon à obtenir une répartition des codes vérifiant les contraintes. Quel est leur rôle ???

4.5.3 Affectation des fréquences

→ Lancer l'affectation automatique des fréquences. Modifiez progressivement votre réseau de façon à obtenir une configuration permettant un taux de blocage inférieur à 1% .

→ Vous chercherez à vous en approcher le plus possible, et in fine, vous choisirez une solution pour laquelle vous donnerez les résultats en termes de QoS.

Quelques remarques :

- Vous rendrez un document précisant la configuration choisie avec l'illustration de la couverture, en niveaux et par émetteur. Vous ferez une étude d'interférences, que vous donnerez. Vous détaillerez les étapes de votre travail.
- Vous noterez précisément le paramétrage des sites en sauvegardant la liste des sites et des émetteurs, que vous rendrez avec le compte-rendu : donnez en annexe de votre document, les tableaux listant les sites et les émetteurs que vous avez positionnés
- Cela vous permettra de reconstruire rapidement votre configuration à la deuxième séance.

4.5.4 Affectation automatique des voisines

→ Lancer le calcul automatique de voisines. A quoi cela sert-il ? Analysez vos résultats. Si il y trop de voisines, comment peut-on les réduire ? Au contraire si le nombre est trop faible, comment les augmenter ? Un nombre de voisine moyen de 5 serait assez réaliste.

4.6 DEPLOIEMENT DE SITES TRI-SECTORIEL

→ Afin d'améliorer le réseau, remplacez certains sites par des sites tri-sectoriels :

- soit vous remplacez un site omni par un site tri-sectoriel, et vous augmentez le nombre de cellules (valable si vos cellules sont trop grandes).
- Soit vous remplacez 3 sites omni, par un site tri-sectoriel, positionné approximativement à l'intersection de ces 3 cellules. Quel sera l'avantage ?
- Refaites tout le processus jusqu'à l'évaluation de la QoS

4.7 BILAN DE LIAISONS POUR LES FAISCEAUX HERTZIENS

4.7.1 Conditions

Pour permettre au réseau de fonctionner correctement, il faut que les différents émetteurs soient reliés entre eux via des liaisons hertziennes qui permettent de garantir l'interconnexion.

4.7.2 Mise en œuvre

A l'aide des menus de l'item 'liaisons', Etablissez quelques liaisons entre les sites. Vous utiliserez l'outil de repérage de stations voisines et vous tiendrez compte de la qualité des liens radios. Vous choisirez une antenne appropriée (fréquence élevée et ouverture angulaire faible).

→ Vous donnerez dans le compte-rendu un bilan de liaison associé à une liaison et vous détaillerez les différents termes.

TP 3 : Mesures du lien radio en GSM

1. OBJECTIF

Ce TP a pour but l'analyse de traces GSM réelles, en provenance des stations de base installées sur le campus.

Vous disposez d'un récepteur RF sélectif en fréquence, CA47, associé à un logiciel de traitement de données « log47V1.0 ». La connexion entre le récepteur RF et le PC portable est assurée par une liaison série.

Vous disposez également d'un analyseur de spectre ESA d'Agilent à partager entre les 2 binômes.

Remarque : L'autonomie des appareils est à prendre fortement en considération notamment celle du PC portable. Aussi, nous vous conseillons de lire attentivement, en début de séance, la documentation technique de l'analyseur et de réaliser les premiers tests avec l'analyseur et le logiciel « log47V1.0 » en branchant les 2 appareils sur le réseau électrique. Vous pouvez également fixer le temps de veille du PC au minimum (ne pas l'éteindre en cours de TP !), et vérifier régulièrement l'état de charge des accumulateurs du PC portable.

1.1 ETUDE DE L'APPAREIL DE MESURES CA.47

A partir du logiciel de mesures, effectuez un SCAN d'une partie des fréquences descendantes du GSM. Repérez les canaux utilisés et non utilisés.

Question 1. Calculez pour différentes tailles de filtres, le niveau de bruit (en dBm) présent sur ces canaux. C'est un bruit blanc lié au récepteur. Comparez les différentes valeurs de bruit (en fonction de la largeur du filtre) et calculez la densité de bruit par Hertz (No, cf. p.5). Calculez la figure de bruit de l'amplificateur en réception.

Question 2. Etudiez les différents paramètres de réglage de l'appareil.

1.2 ETUDE DE L'APPAREIL ESA

Question 3. Effectuez le même genre de SCAN, qu'avec le CA47, et comparez les mesures que vous obtenez avec cet appareil.

2. CARACTERISATION SPECTRALE DES FREQUENCES GSM

2.1 ETUDE GLOBALE DES CANAUX GSM

Vous devez étudier l'ensemble des fréquences caractérisant le lien descendant et le lien montant des systèmes GSM. Il s'agit de scanner l'ensemble des fréquences en prenant soin de choisir et de tester différentes configurations de l'analyseur (filtre, moyennage, pas de mesure, puissance de réception...).

Après avoir étudié le fonctionnement de l'appareil CA47, et le document sur la norme GSM :

Question 4. L'analyse de spectre repose sur l'étude, après mélangeur, de la puissance disponible dans une bande de fréquence donnée. Est-il possible avec cet appareil de reconstituer les trames GSM ? Expliquez pourquoi.

Question 5. A partir des informations données, estimez la taille de la fenêtre d'analyse ?

Question 6. Quelles sont les périodicités d'analyse maximale, et minimale que l'on peut choisir ?

Question 7. Peut-on se synchroniser sur les trames GSM ?

Question 8. Effectuez un SCAN des bandes de fréquences utilisées en GSM et donnez les figures correspondantes.

Question 9. Donnez tous les réglages que vous aurez faits, en justifiant. En particulier, largeur du filtre, type de mesure, périodicité.

Question 10. Vous analyserez et commenterez ce spectre : niveau de bruit, canaux, etc...

2.2 RECHERCHE DE VOIX BALISES

Il s'agit de l'étude des canaux associés au lien descendant et correspondant à des voies balises. Il est donc nécessaire de réfléchir à la méthodologie de mesure appropriée.

Question 11. A partir d'une trace des canaux GSM, repérez les voies balises. Donnez les numéros des canaux correspondants. Procédez de même pour la gamme de fréquence DCS1800.

Question 12. Sachant que les opérateurs Orange et SFR se partagent la bande GSM900 sur le campus, estimez le nombre de voies balises disponibles par opérateur visibles sur place.

Question 13. Estimez le nombre de cellules susceptibles de servir un mobile à votre point de mesure.

2.3 ETUDE D'UNE VOIX BALISE

Choisissez la voie balise qui présente le niveau de signal le plus élevé.

Question 14. Effectuez une estimation de la Densité Spectrale de Puissance (DSP) du canal correspondant, en utilisant le filtre le plus fin possible. Estimez la précision de vos mesures en effectuant plusieurs mesures successives et en calculant l'écart-type à la moyenne.

3. ETUDE DU GSM SUR LE CAMPUS

3.1 ETUDE DE COUVERTURE

Question 15. A l'aide du plan de campus donné ci-joint, et avec l'appareil de mesure, vous chercherez à repérer les différents sites GSM localisés sur le campus. Pour chaque site vous déterminerez si il s'agit d'un site omnidirectionnel ou tri-sectoriel. Vous en déterminerez les voies balises.

Vous donnerez les réglages précis de l'appareil.

Question 16. Vous choisirez un site tri-sectoriel et vous dresserez une carte de couverture la plus précise possible.

Chaque point de mesure sera repéré sur la carte, et pour chaque point vous effectuerez une série de 10 mesures sur un rayon de 5m autour du point de mesure, pour chacune des 3 voies balises. Vous donnerez la puissance moyenne et l'écart-type à la moyenne.

Question 17. A partir de vos points de mesure, judicieusement choisis, vous établirez une estimation de l'orientation des antennes en angle, et de la zone angulaire couverte par chacune des antennes.

Question 18. Pour un des secteurs, vous vous déplacerez d'une distance au sol d'environ 10m à 150m et vous tracerez l'affaiblissement en fonction de la distance.

Question 19. Vous tenterez de donner les canaux descendants observés, associés à chacune des 3 cellules.

TP 4 : caractéristiques radio des réseaux locaux d'accès sans fil

1. OBJECTIFS

Ce TP vous permettra d'évaluer les performances des technologies WiFi, dans différentes configurations. Il est basé sur l'utilisation de cartes 802.11b, mais la généralisation des notions étudiées aux normes plus récentes 802.11g, ou 802.11a, est immédiate.

Ce TP a également pour but de vous familiariser avec la prise de mesure, en radiocoms, et en particulier avec l'analyse des résultats de mesure. Vous porterez un soin particulier à la prise de mesures et à l'analyse.

Le WiFi est principalement dédié au déploiement de réseau en environnement confiné, même si dans certains cas, on l'utilise en extérieur. Même si les standards donnent une estimation de la portée de ces technologies, il est très difficile de prédire la couverture que l'on peut obtenir à cause de l'impact de l'environnement sur les performances réelles.

2. MATERIEL

Le travail est effectué par binômes. Chaque binôme utilise 2 PC portables, équipés de cartes réseau sans fil. Vous pouvez utiliser :

- soit les PC fournis en TP, qui permettent de relever avec le logiciel Orinoco Manager, les niveaux de signal reçu, ainsi que le débit moyen
- soit vos PC portables, en utilisant le même logiciel (si compatible), ou netstumbler, ou tout autre logiciel fourni avec le PC.

Pour les études avec les PC de la salle TP, vous disposez de 2 utilitaires.

«client manager» : c'est un utilitaire fourni par Lucent, livré avec les cartes, ou téléchargeable sur leur site. Il permet de configurer en partie les paramètres des cartes WLAN. Il propose également un outil d'analyse du lien radio entre 2 éléments du réseau.

Vous le trouverez dans le menu démarrage, dans l'onglet «ORINOCO».

« Qcheck » c'est un utilitaire « freeware », qui permet d'effectuer des tests de transmission avec différents protocoles réseau : temps de réponse moyen, débit utile réel (throughput) entre 2 machines. Pour fonctionner le logiciel doit être démarré sur les 2 machines.

**Rem : attention les batteries n'ont pas une durée de vie éternelle...
Laissez l'alimentation secteur lorsque vous travaillez en fixe.**

3. ANALYSE DE COUVERTURE

3.1 PROPAGATION EN EXTERIEUR

3.1.1 Etude théorique

→ Rappelez quelle est l'expression de la puissance reçue (en dBm), en fonction de la distance entre l'émetteur et le récepteur (formule de Friis).

→ Sous Matlab, ou Excel, ou tout autre programme de votre choix, tracez-la, en utilisant des valeurs numériques réalistes pour la longueur d'onde, la puissance d'émission, les gains d'antenne, ...

Cette courbe sert de référence et représente l'affaiblissement en espace libre.

→ Modifiez cette courbe pour tenir compte de l'effet de sol, avec une modélisation à 2 rayons (réflexion au sol), ou modèle à 2 pentes. Concluez sur l'intérêt de ce modèle dans le cas du WiFi.

→ Calculez le plancher de bruit No des récepteurs WiFi. Comparez à la valeur donnée par le logiciel de mesure.

3.1.2 Etude expérimentale du path-loss

Les mesures sont faites à l'aide de 2 PC portables et du « client manager » dans un endroit extérieur, sur le campus, et suffisamment ouvert.

→ Prenez un point fixe (premier PC), et positionnez le 2^{ème} à la limite de la portée : vous ne pouvez pas faire de mesures plus éloignées. Représentez ces 2 points sur le plan du campus le plus précisément possible. Définissez ensuite entre ces 2 points, au moins une vingtaine de positions intermédiaires pour le 2^{ème} portable, que vous repérez en comptant vos pas, par exemple. Pour chacune des positions, vous effectuez un relevé de signal reçu.

Remarques :

1- Attention, à chaque position, il ne s'agit pas de relever une valeur, mais un ensemble de points, obtenus en déplaçant le PC autour du point de référence.

2- Lorsque vous déplacez le PC autour de la position de référence, vous avez 2 solutions :

- soit vous laissez toujours le PC orienté de la même façon vers l'autre PC, et dans ce cas vous n'êtes pas sensible aux variations de puissance reçue dues au gain de l'antenne.

- soit vous modifiez en permanence l'orientation du PC, ce qui intégrera l'effet du gain d'antenne dans les variations de puissance reçue.

3- choix des positions de référence : lorsque vous allez analyser ces résultats, vous allez tracer le signal reçu en fonction de la distance, sur une échelle semilog. Pour que vos résultats soient

intéressants et exploitables, il faut répartir les positions de mesure également selon une échelle log : par exemple si vous faites uniquement 5 mesures, un bon choix serait {100m 30m 10m 3m 1m} car réparties sur 2 décades, et non {100m, 80m, 60m, 40m, 20m}, réparties sur 1 seule décade.

→ Tracé : à partir de ces mesures, vous pouvez représenter ces points sur un plan (log(distance), P(dBm)) . Pour chaque position, donnez la valeur moyenne de la puissance reçue, et en barre verticale l'écart-type.

→ Régression linéaire : faites une régression linéaire de vos mesures, et donnez le coefficient d'affaiblissement ainsi obtenu. Comparez à l'espace libre.

3.1.3 Stabilité de ce modèle

→ Refaites 2 autres séries de mesure, selon le même principe, et à 2 autres endroits en extérieur. Recalculez un modèle pour chacune.

→ Comparez les modèles.

→ Proposez un modèle moyen à parti de ces 3 séries.

Remarque :

1- vous représenterez sur le plan du campus, les lignes de mesure que vous avez utilisées.

2- Vous rendrez le tracé des modèles théoriques et des mesures expérimentales sur une échelle semilog en x, représentant la puissance reçue (en dBm) en fonction de la distance (en m).

3.1.4 Etude expérimentale des variations de signal (fading)

→ Rappelez ce qu'est le fading.

→ Toujours en extérieur, choisissez une distance entre les 2 PCs, telle que le signal soit suffisamment bon, mais permettant toutefois d'avoir plusieurs chemins entre l'émetteur et le récepteur (donc pas trop près).

→ En vous déplaçant légèrement autour de cette position, relevez le signal au cours du temps.

→ Analysez l'histogramme des valeurs mesurées : conclusions ?

3.2 PROPAGATION EN ENVIRONNEMENT INDOOR

L'étude de la propagation en Indoor est bien plus complexe. Nous allons mesurer quelques effets liés à la présence d'obstacles.

3.2.1 Les murs et les obstacles.

→ Évaluez les pertes liées : à un mur, à une porte, à la présence humaine. Évaluez si la présence d'objets métalliques (armoires par exemple) génère des modifications de lien radio.

→ Pour quantifier correctement ces pertes, vous pourrez comparer vos mesures, aux mesures en espace libre : en positionnant les nouveaux points sur les mêmes figures que précédemment, et en évaluant la distance, vous pourrez évaluer l'affaiblissement lié à l'obstacle.

3.2.2 Effet couloir

→ A partir de mesures prélevées dans le couloir, comparez l'affaiblissement le long du couloir principal, à l'affaiblissement en espace libre : conclusions. Reprendre la méthodologie de la section 3.1.2.

3.2.3 Les effets du sol

→ Évaluez les pertes lors d'une liaison entre 2 étages voisins, dans un même bâtiment.

3.2.4 Stabilité du signal

→ Reprenez le travail de la partie 3.1.3, dans des conditions NLOS. Comparez les 2 cas.

4. RELATION ENTRE NIVEAU DE SIGNAL ET DEBIT

4.1.1 Relation entre débit théorique et niveau de signal

→ Tracez une courbe donnant l'évolution du 'débit théorique' (annoncé par le wave manager) en fonction du SNR. Vous effectuerez suffisamment de mesures (en Indoor). Vous donnerez le nuage de points de mesures, et vous en déduirez une courbe approximative (par paliers !).

Remarques :

- 1- En vous promenant dans le bâtiment, sélectionnez différentes positions, correspondant à différents SNR, et relevez le débit théorique (c'est-à-dire la vitesse de modulation choisie).
- 2- Tracez la courbe débit en fonction du SNR.

4.1.2 Relation entre débit théorique et débit utile

En combinant les informations fournies par les softs «client Manager» et «Qcheck», établissez la relation entre le SNR et le débit réel.

De même que pour la question précédente, donnez le nuage de points de mesures, et tracez une courbe représentant le débit réel en fonction du SNR.

5. INTERFERENCES ENTRE PLUSIEURS RESEAUX.

Cette partie du travail devra être effectuée par les 3 binômes travaillant sur ce TP. Proposez, pour différentes configurations, l'influence de la co-existence de plusieurs réseaux simultanés exploitant le même canal radio ou des canaux différents. Vous comparerez aux performances de transmission lorsqu'un seul réseau ad-hoc regroupe tous les utilisateurs qui communiquent simultanément. Concluez sur les précautions à prendre pour garantir un bon fonctionnement.

Pour cela, vous utiliserez soit le logiciel Qcheck, en synchronisant bien les émissions, soit vous effectuerez le transfert d'un gros fichier, après avoir installé un serveur de fichiers.

Le GSM : planification et dimensionnement

6. INTRODUCTION

Le dimensionnement des réseaux mobiles est un problème complexe qui met en jeu à la fois des aspects théoriques et pratiques.

Il s'agit de trouver la meilleure architecture cellulaire au regard de plusieurs critères que l'on peut résumer comme suit :

- Qualité de couverture : garantir un lien radio en tout point de la zone à couvrir.
- Absorption de la charge : le réseau doit être capable de fournir un nombre de canaux de communication adapté à la densité de trafic associée à chaque cellule.
- Mobilité : Faciliter le handover lors des changements de cellules. Chaque station de base doit connaître ses voisines pour permettre à un utilisateur de se déplacer sans perte de communication.
- Evolutivité : un réseau cellulaire de type GSM est en perpétuelle évolution, intégrant de nouvelles stations de bases, ou simplement de nouveaux TRX associés à chaque station de base.
- Déploiement du réseau fixe via un ensemble de faisceaux hertziens pour interconnecter les stations de base.

7. LA NORME GSM

Le tableau ci-dessous résume les principales propriétés de la couche radio GSM :

	GSM	DCS
Bande de fréquence	890-915 MHz (up) 935-960 MHz (down)	1710-1785 MHz (up) 1805-1880 MHz (down)
Nombre d'intervalles de temps par trame TDMA	8	8
Nombre de porteuses	124	374
Fréquences porteuses	$f_c = 935 + 0,2 \cdot n$, pour $1 \leq n \leq 124$	$f_c = 1805,2 + 0,2 \cdot (n - 512)$, pour $512 \leq n \leq 885$
Ecart Duplex	45 MHz	95 MHz
Rapidité de modulation	271 kbit/s	271 kbit/s
Débit de la parole	13 kbit/s (5,6 kbit/s)	13 kbit/s (5,6 kbit/s)
Débit après codage d'erreur	22,8 kbit/s	22,8 kbit/s
Débit max de données	12 kbit/s	12 kbit/s
Accès multiple	Multiplexage fréquentiel et temporel, duplexage fréquentiel	Multiplexage fréquentiel et temporel, duplexage fréquentiel
Rayon des cellules	0,3 à 30 km	0,1 à 4 km
modulation	GMSK	GMSK

remarque : la bande GSM a été étendue récemment et est aujourd'hui égale : 880-915 MHz, 925-960 MHz.

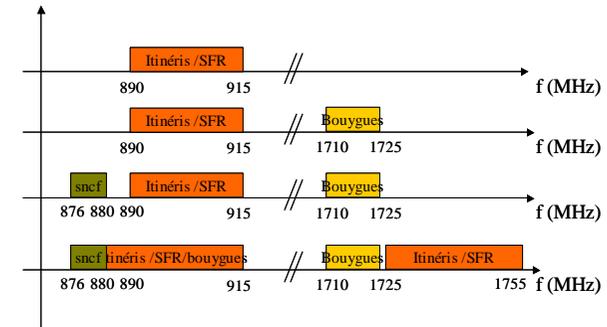


Figure 1 : évolution du partage des ressources spectrales sur le lien montant au cours de la dernière décennie

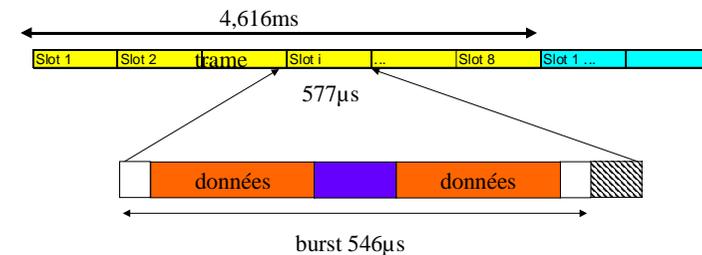


Figure 2 : durée des slots et des trames GSM

8. CONTRAINTES RADIO

8.1 RAPPORT SIGNAL A BRUIT C/N

Le premier objectif d'un déploiement cellulaire est de garantir un lien radio en tout point de la zone à couvrir. La qualité de ce lien est définie principalement par 2 paramètres : le rapport signal à bruit C/N (canal /noise) et le rapport signal sur interférences (C/I (canal/interférences)).

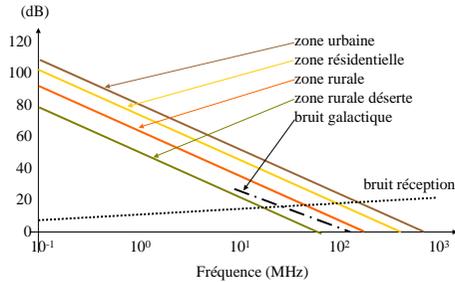


Figure 3 : niveau de bruit électromagnétique relativement au bruit thermique minimal des systèmes de réception

Le rapport signal à bruit est donné par le rapport entre la puissance du signal reçu et la densité de puissance du bruit en réception. Comme le montre la Figure 3, dans la gamme de fréquences utilisées en GSM, le bruit en réception est majoritairement un bruit thermique (ou bruit Johnson) lié à l'échauffement des électrons dans le système de réception. Ce bruit a des propriétés bien spécifiques : il est blanc, à moyenne nulle, gaussien, additif.

- Blanc veut dire qu'il est réparti sur l'ensemble des fréquences de façon uniforme : sa densité spectrale de puissance (DSP) est donc uniforme sur toutes les fréquences (sauf pour une fréquence nulle où il est égal à 0).
- Moyenne nulle : il n'y a pas de composante continue. Si l'on fait la somme (ou l'intégration) du bruit au cours du temps, elle tend vers 0.
- Gaussien : Ce signal aléatoire, a une distribution d'amplitude bien particulière : la probabilité d'avoir un bruit d'amplitude est régie par une loi normale (forme gaussienne). L'écart-type de la distribution σ est le seul paramètre à connaître pour caractériser le niveau de bruit. La puissance moyenne de ce bruit que l'on nomme N_0 est égale à la variance des échantillons :

$$E-1: \sigma^2 = N_0$$

- Additif : un bruit additif est un bruit dont le niveau ne dépend pas de l'amplitude du signal reçu. Statistiquement, le bruit est indépendant du signal reçu, et le signal observé est la somme du signal reçu et du bruit.

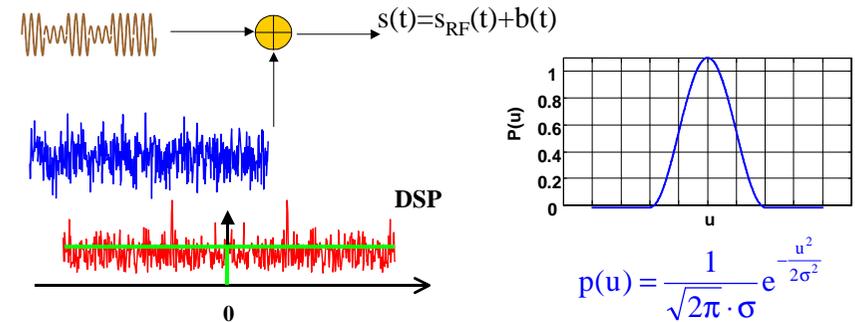


Figure 4 : représentation du bruit AWGN (Additive White Gaussian Noise) : aléatoire, additif, blanc et gaussien.

Le niveau de bruit en réception s'estime assez facilement à partir de la formule de Johnson :

$$E-2 \quad N_0 = \kappa \cdot T_K \text{ Watt/Hz}$$

Où κ est la constante de Boltzman ($1.38 \cdot 10^{-23}$ J/K) et T_K est la température en Kelvin ($T_K = 290^\circ\text{K}$, en référence). Finalement, comme le bruit est étalé sur tout le spectre, seule la partie qui est présente sur la bande spectrale utilisée par la transmission interfère avec le signal transmis. La puissance du bruit après filtrage est égale à :

$$E-3 \quad N = N_0 \cdot W = \kappa \cdot T_K \cdot W \text{ Watt}$$

Où W est la bande passante utilisée par le système.

On peut alors estimer le bruit minimal pour un récepteur GSM mobile à 1 température moyenne de 290K. La bande utile d'un canal GSM est estimée à $W=271\text{kHz}$ (c'est une approximation faite à partir de la vitesse de modulation, cf Figure 5) :

$$E-4 \quad N \approx 10^{-15} \text{ Watt ; soit } N_{dB} \sim -120\text{dBm}$$

Cette approximation permet de quantifier le niveau de bruit dans le récepteur. Sachant alors que la norme GSM préconise en réception un rapport signal à bruit d'au moins 8dB, et en prenant une marge de protection de 1 à 3dB (pertes liées à la présence du corps humain, facteur de bruit de l'amplificateur en réception), on obtient un niveau minimal en réception de l'ordre de :

$$E-5 \quad C_{dB} - N_{dB} > 10\text{dB} \quad \left(\text{soit } \frac{C}{N} > 10 \right) \text{ soit } C_{dB} > -110\text{dBm}$$

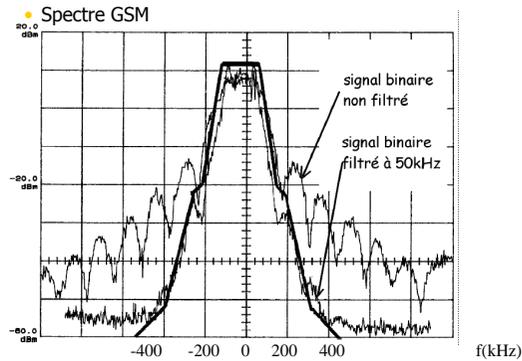


Figure 5 : DSP d'un signal GSM.

8.2 RAPPORT SIGNAL A BRUIT C/I

Les interférences sont de 3 types : les interférences inter-symboles (IIS), les interférences interférences (IIF, encore appelées interférences canaux-adjacents), et les interférences cocanal (ICC).

Les interférences inter-symboles caractérisent les interférences entre les impulsions successives d'une même source : lorsqu'un bit est émis, le récepteur en reçoit plusieurs échos étalés dans le temps à cause de la différence de temps de parcours entre les différents chemins Emetteur-Recepteur. Ces interférences (IIS), sont combattues par des techniques d'égalisation (l'égaliseur de Viterbi en GSM) et de codage canal et ne sont pas prises en compte dans la phase de planification.

Les interférences co-canal (ICC) sont forcément importantes en GSM et sont directement liées à la norme elle-même. Le choix d'un partage de ressources de type FTMA (Frequency and Time Division Multiple Access) impose une répartition des ressources en temps et en fréquence. Sur un canal en fréquence, on peut avoir jusqu'à 8 voix multiplexées en temps (8slots par trame). Pour augmenter la capacité globale d'un système, les fréquences sont réparties entre les cellules, avec un certain facteur de réutilisation. Ainsi, toutes les cellules et les stations de base associées qui utilisent un même canal en fréquence sont susceptibles d'interférer entre elles.

Le rapport C/ICC est donné par le rapport entre la puissance utile du signal reçu par un mobile en provenance de la station de base (BTS) à laquelle il est associé, et la somme des puissances des signaux reçus par le même mobile en provenance de toutes les BTS utilisant la même fréquence (cf. Figure 6).

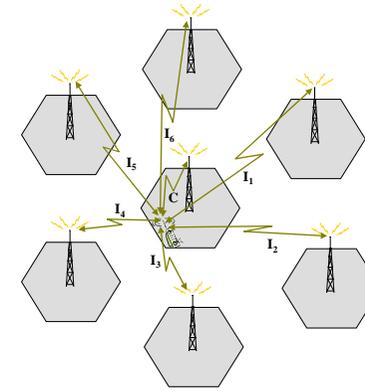


Figure 6 : Interférences entre cellules voisines réutilisant la même fréquence sur un modèle hexagonal

Les interférences canaux adjacents (IIF) sont liés à la réutilisation de canaux de fréquences adjacents. En effet la largeur réelle des canaux est supérieure aux 200kHz utilisés pour répartir les canaux en fréquence (cf. Figure 5). Ainsi, à puissance identique, 2 canaux voisins (f_i et f_{i+1}) ont un rapport C/I d'environ 18dB, 2 canaux voisins (f_i et f_{i+2}) un C/I de 50dB, et 2 canaux (f_i et f_{i+3}) un C/I de 58dB.

Pour garantir un C/I total supérieur à 9dB, la norme GSM définit un rapport de protection pour 2 canaux voisins, donné par le tableau suivant :

Interférences co-canal (fo)	C/lc	9dB
Interférences 1er canal adjacent	C/la1	-9dB
Interférences 2ième canal adjacent	C/la2	-41dB
Interférences 3ième canal adjacent	C/la3	-49dB

Finalement, le rapport C/I total est donné par :

$$E-6 \quad \frac{C}{I} = \frac{C}{\sum_{\text{cellcocanal}} I_i + R_1 \cdot \sum_{\text{celladjacent 1}} I_i + R_2 \cdot \sum_{\text{celladjacent 2}} I_i + R_3 \cdot \sum_{\text{celladjacent 3}} I_i}$$

Où R_i est le rapport de protection donné par :

$$E-7 \quad R_i = \frac{C/la_i}{C/lc}$$

D'après le tableau précédent, $R_1=0.015$; $R_2=10^{-5}$; $R_3 \sim 10^{-6}$.

9. CONTRAINTES DE TRAFIC

Dans un réseau GSM, il ne s'agit cependant pas seulement de garantir un lien radio, mais également de garantir un certain trafic. Le trafic est estimé statistiquement à partir de la densité de population et du type d'activité associée à chaque région. Par exemple, la probabilité d'appel dans une zone à forte densité d'habitation est très différente de la probabilité d'appel dans une zone à forte densité d'activité professionnelle.

Les lois d'Erlang sont utilisées pour caractériser le taux d'appels téléphoniques. Cette loi est paramétrée par 2 paramètres : le taux d'appel μ , et la durée moyenne d'appel H. L'intensité de trafic par utilisateur s'exprime par :

$$\text{E- 8 } A_U = \mu \cdot H \text{ erlang}$$

Connaissant la densité de population associée à une zone géographique, il est facile de déterminer la densité de trafic par le produit :

$$\text{E- 9 } A = A_U \cdot d_H \text{ erlang/km}^2$$

où d_H est la densité de population par km^2 .

Enfin, si l'on est capable de prédire la zone couverte par une cellule, il est alors possible d'estimer le trafic que la cellule doit absorber :

$$\text{E- 10 } A_{\text{tot}} = A \cdot S \text{ erlang}$$

où S est la superficie de la cellule.

Les lois d'Erlang permettent alors de déterminer le nombre de canaux nécessaires pour absorber ce trafic statistique avec un taux d'échec donné :

La loi d'Erlang B est donnée par la formule suivante :

$$\text{E- 11 } P_c = \frac{A^{N_c} \frac{1}{N_c!}}{\sum_{n=0}^{N_c} A^n \frac{1}{n!}}$$

Où N_c est le nombre de canaux voix.

Ainsi, à partir de la connaissance de la densité de trafic et de la surface couverte par un émetteur, il est possible de prédire le nombre de canaux à affecter à une cellule pour garantir un taux de blocage inférieur à un certain pourcentage (par exemple 1%).

On comprend bien alors que le déploiement d'un réseau GSM ne repose pas seulement sur une couverture radio mais sur une répartition intelligente des ressources radio sur un ensemble de stations de base.

10. DIMENSIONNEMENT DU RESEAU GSM

10.1 DEFINITION DES ZONES DE SERVICES

Le dimensionnement doit prendre en compte les contraintes radio et les contraintes de trafic.

Il est possible, dans un premier temps, pour une zone géographique donnée, d'estimer la capacité globale d'un système GSM, en exploitant le modèle hexagonal théorique.

Soit un système avec S canaux disponibles. Le nombre de canaux voix disponibles n'est pas égal au nombre de canaux en fréquences.

Pour chaque cellule, il faut réserver une voix balise qui contient les canaux de synchronisation (FCH SCH, BCCH) : ces canaux permettent aux mobiles de détecter la présence des stations de base. Lors de l'attribution d'un certain nombre de fréquences à une station de base, il faut donc éliminer une des fréquences pour compter les ressources radios.

D'autre part, chaque canal en fréquence est susceptible de fournir 8 canaux de données TCH (chaque trame contient 8 slots multiplexés) : le nombre total de canaux est donc égal à 8 fois le nombre de canaux en fréquence.

Cependant, certains canaux communs, et en particulier la voix balise, nécessitent des ressources. On considère en général, qu'1/8^{ième} des ressources est utilisé pour les canaux communs (y compris la voix balise).

Ainsi, pour N canaux attribués à une station de base, le nombre de TCH est donné par :

$$\text{E11 } N_{TCH} = N \cdot 7/8$$

Si N_f est le nombre de porteuses attribuées, alors le nombre de canaux physiques TCH disponibles est de :

$$\text{E- 12 } N_c = 7 \cdot N_f$$

En conséquence, le tableau ci-dessous donne le nombre de canaux voix en fonction du nombre de porteuses attribuées à une cellule, conformément à l'équation E- 11 :

Nb fréquences	1	2	3	4	5	6	7	8
Canaux physiques	8	16	24	32	40	48	56	64
Nb TCH	7	14	21	28	35	42	49	56

La figure ci-dessous représente le taux de rejet d'appel en fonction de la densité de trafic demandée, et pour un nombre de porteuses allant de 1 à 7.

Etude du taux d'erreur en fonction du nombre de canaux fréquences

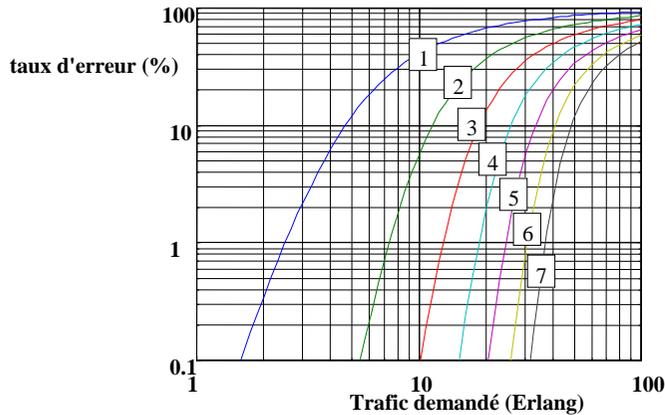


Figure 7 : Etude du taux de refus d'appel en fonction du trafic demandé, pour un nombre de porteuses attribué à la cellule variant de 1 à 8.

10.2 FACTEUR DE REUTILISATION DES RESSOURCES

Pour dimensionner un réseau cellulaire, on peut partir d'un modèle théorique hexagonal régulier. Dans ce cas, on cherche à répartir les ressources de façon régulière et optimale, minimisant les interférences. La théorie des graphes offre des résultats intéressants. Un graphe est un ensemble de nœuds et d'arêtes reliant ces nœuds. Dans notre cas, chaque nœud représente une cellule GSM, et les arêtes correspondent à une contrainte de non interférence. Le coloriage de graphe consiste à colorier les sommets du graphe avec un minimum de couleurs, sous la contrainte que 2 sommets voisins ne soient jamais de la même couleur. Dans notre cas, il s'agit donc de colorier les cellules. La notion de voisinage ne se résume pas uniquement aux cellules voisines géométriquement (qui ont un bord commun). On peut fixer une contrainte plus stricte de réutilisation des ressources afin de réduire les interférences.

On appelle distance de réutilisation la distance entre les cellules co-canales, telles qu'illustrées à la figure suivante :

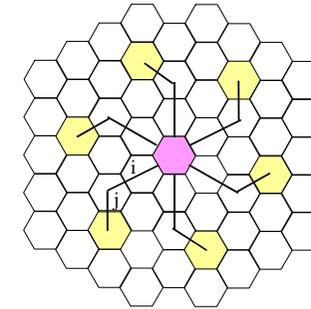


Figure 8 : représentation des cellules co-canal

On peut montrer que chacune des cellules du voisinage de la cellule centrale peut être coloriée avec une couleur différente, et que chaque cellule aura 6 premières voisines co-canales, comme sur le schéma. Ces 6 co-canales sont déterminées par les paramètres i et j , qui représentent le nombre de cellules que l'on traverse en 2 sauts comme illustré. La théorie des graphes montre que le nombre de couleurs nécessaire au coloriage complet de ce schéma est donné par la formule suivante :

$$N = i^2 + ij + j^2$$

Résumé dans le tableau :

i / j	1	2	3	4
1	3	7	13	21
2	7	12	19	28
3	13	19	27	37
4	21	28	37	48

On appelle $Q=D/R$ le facteur de réutilisation, où D est la distance entre 2 cellules co-canales, et R le rayon des cellules. Il est à peu près égal à :

$$E-13 \quad Q \approx \sqrt{3N}$$

On va maintenant calculer le rapport C/I en fonction de ce facteur de réutilisation. On tient compte ici uniquement des interférences co-canales. Le rapport C/I est alors donné par :

$$E-14 \quad \frac{C}{I} = \frac{C}{\sum_i I_i}$$

Considérons un mobile en limite de cellule. La puissance utile reçue, est donnée par :

$$E-15 \quad C = P_0 \left(\frac{R}{d_0} \right)^{-n},$$

où r est le rayon de la cellule.

La puissance en provenance de chacun des interférents peut être approchée par la distance entre les 2 stations de bases, soit la distance D . on a alors :

$$E-16 \quad \sum_i I_i = 6P_0 \left(\frac{D}{d_0} \right)^{-n},$$

Ce qui permet d'estimer le C/I par

$$E-17 \quad \frac{C}{I} = \frac{Q^n}{6} = \frac{\sqrt{3N}^n}{6}$$

Finalement, on pourra choisir N , en fonction de la contrainte de C/I et du modèle d'affaiblissement n .

Cependant, il est évident que ce genre de contrainte n'est qu'une approximation bien théorique de la réalité. En pratique, les cellules sont bien loin d'être hexagonales, et le nombre de cellules voisines, les niveaux d'interférence, et l'affectation des canaux nécessite une approche empirique basée sur plusieurs tests.

11. PLANIFICATION DU RESEAU

Dans la pratique, le déploiement d'un réseau GSM nécessite l'optimisation du placement des sites, sous les 2 contraintes de type radio et trafic. Il s'agit de tester, en fonction du type d'antenne, de sa puissance d'émission et de son orientation, la zone couverte par l'émetteur. Une approche pas à pas permet progressivement de faire converger le réseau vers une bonne configuration.

Le principe est le suivant (en simulation ☺) :

- répartir les émetteurs sur le terrain
- établir les zones de couverture, et les adapter en déplaçant les sites, en modifiant les puissances d'émission, en choisissant les orientations.
- Une fois la couverture assurée, il faut rechercher une répartition des fréquences en analysant les sites qui sont voisins.
- Il faut alors rechercher une répartition des fréquences entre les sites. On commencera par positionner les fréquences BCCH, puis les canaux de données.
- Dans le cas où la planification n'arrive pas à converger, il faut alors densifier le réseau : soit rajouter des sites, soit remplacer des émetteurs omnidirectionnels par des émetteurs tri-sectoriels.

Notons qu'en cours d'exploitation, l'augmentation du nombre d'abonnés impose à l'opérateur de faire évoluer son réseau, en tenant compte de l'évolution probable du nombre d'abonnés et des taux d'appel.

12. PREDICTION DE COUVERTURE RADIO

Il est impossible d'envisager le déploiement complet en phase de tests, et les opérateurs sont amenés à utiliser des logiciels de simulation qui permettent de prédire la couverture radio associée à chaque émetteur.

En effet, la prédiction de couverture est fondamentale car elle conditionne à la fois les critères radios (on peut prédire le taux d'interférence et le niveau de signal) et les critères trafic (dimensionnement du nombre de canaux).

Les méthodes de prédiction de couverture aujourd'hui utilisées mixent avantageusement les approches empiriques et déterministes.

Les méthodes empiriques, telle la méthode d'Okumura-Hata, utilise des résultats expérimentaux pour estimer la couverture radio. Elles nécessitent de grandes campagnes de mesure, et ne tiennent que très peu compte de la réalité géographique de terrain.

Au contraire, les méthodes déterministes intègrent les effets de relief (au niveau macro), sans tenir compte des propriétés locales.

Les méthodes utilisées (voir dans le logiciel) intègrent en général les 2 approches.

- Les méthodes empiriques intègrent en général la prise en compte des effets de masque et de diffraction sur le profil entre émetteur et récepteur, puis pondèrent ces prédictions par des coefficients déterminés par les formules empiriques d'Okumura et al, ou autres dérivées.
- Les méthodes déterministes procèdent soit par profil (comme pour les méthodes empiriques), et dans ce cas négligent l'effet des chemins latéraux et les effets liés à l'environnement 'micro' (immeubles, forêts,...) ; soit par des approches semblables au lancer de rayon mais avec dans ce cas un coût de calcul assez prohibitif.

Notons que ces prédictions nécessitent plusieurs type d'information : relief et type de terrain. Les opérateurs doivent donc acquérir ces bases de données. Les données de terrain proviennent en général des images satellites qui permettent aujourd'hui d'estimer l'élévation locale de terrain avec une résolution de l'ordre de 3m. Ces données coûtent relativement cher. D'autre part l'affectation des zones (forêt, zone urbaine, etc...) sont effectuées manuellement à partir des cartographies conventionnelles.

Les réseaux locaux sans fil (RLANs)

1. INTRODUCTION : LA NORME IEEE802.11B

1.1 INTERET DES LANs SANS FIL (RLANs)

Les LANs permettent de connecter des stations à un réseau numérique de données avec des débits assez élevés et un matériel de raccordement peu coûteux, aussi bien dans les secteurs publics que privés. De nos jours, pratiquement chaque entreprise dispose d'un LAN de type Ethernet, donc filaire. Ethernet (norme IEEE 802.3) est le protocole de base le plus fréquemment utilisé pour les LANs filaires. Cependant, ces LANs sont dépendants de l'infrastructure physique et câblée du bâtiment, ce qui est un problème pour les utilisateurs qui recherchent à être mobiles dans les entreprises.

Les LANs sans fil sont particulièrement sollicités par les hôpitaux (gestion des fichiers des patients), les universités (LANs extrêmement sollicités sur les campus), les aéroports, les chantiers de construction, les usines (gestion de la production, gestion des stocks, inventaires). En effet, tous ceux là trouvent dans les LANs sans fil des solutions particulièrement adaptées.

Pour les entreprises diverses, les LANs sans fil sont une bonne solution pour des applications telles que :

- extension à des LANs filaires
- sites difficiles à câbler (bâtiments anciens, musées, monuments historiques...)
- réalisations temporaires (pour des périodes de surcharge ou des projets spéciaux)
- mise en place rapide de réseaux
- environnement en évolution constante
- LAN préinstallés, prêts à l'emploi ou devant être évolutifs
- accès LAN aux utilisateurs d'ordinateurs mobiles
- liaisons par antennes extérieures pour remplacement rapide de ligne louée
- conférences...

1.2 LA NORME IEEE 802.11B

Il existe plusieurs normes indépendantes et incompatibles entre elles provenant de nombreux constructeurs, mais la plupart des constructeurs ont rejoint l'IEEE pour créer une norme pour les LANs sans-fil. Cette norme s'appelle IEEE 802.11b.

Les caractéristiques générales de la norme 802.11b sont :

- Famille technologique : technologie radio à étalement de spectre

- Plage de fréquence utilisée par cette norme : 2,4000-2,4970 GHz. En France, la gendarmerie se réserve une partie de cette plage de fréquence, faisant que la plage disponible est réduite à l'espace 2,4465-2,4835 GHz. Il est urgent en France de libérer plus de canaux sur la bande des 2,4GHz, car cela limite réellement les possibilités d'installation et d'évolution du LAN sans fil. Dans le monde la France est avec le Japon un pays très restrictif sur cette bande de fréquence. Paradoxalement 4 canaux seulement sont officiellement disponibles en France contre 11 à 13 dans la plupart des autres pays. L'utilisation de cette bande de fréquence est libre et ne nécessite donc pas de licence.

Pays	Plage de fréquence (en GHz)
USA	2,4000-2,4835
Europe	2,4000-2,4835
Japon	2,4710-2,4970
France	2,4465-2,4835
Espagne	2,4450-2,4750

Figure 9 : Bande de fréquence allouée en fonction du pays pour la norme 802.11

- 14 canaux distincts sont définis dans cette plage de fréquence
- Méthode d'étalement de spectre : FHSS ou DSSS (saut de fréquence ou séquence directe)
- Limite de la puissance effective d'émission à 100 mW ce qui ne permet d'établir des liaisons que sur 1 km au maximum en vue dégagée (et en étant optimiste !).
La norme IEEE 802.11b est entièrement définie par les 2 couches les plus basses du modèle OSI (voir plus loin).

Pour une description plus précise, vous pouvez trouver la norme complète sur le site IEEE : c'est un document rendu public pour favoriser l'utilisation de cette norme.

2. TOPOLOGIES DES RESEAUX IEEE 802.11B

Un LAN sans-fils peut être utilisé pour remplacer ou étendre un LAN filaire. Nous allons décrire quelles sont les différentes topologies de réseau possibles avec la norme 802.11.

2.1 RESEAU AD-HOC

La topologie basique d'un réseau 802.11 est représenté en Figure 2. Un BSS (Basic Service Set) consiste en 2 nœuds sans fil ou plus, ou en des stations qui se reconnaissent et qui communiquent chacune entre-elles. Ces stations peuvent être des PC portables ou des PC fixes. Dans la topologie la plus basique, les stations communiquent directement entre-elles en point à point (peer to peer), tout en partageant une certaine cellule radio limitée en espace. On appelle ce réseau un réseau ad-hoc, ou aussi un IBSS (Independent Basic Service Set).

Ce réseau ad-hoc simplifié permet de réaliser rapidement un petit réseau entre 2 stations sans fils comme par exemple 2 consultants sur le site d'un client qui ont besoin d'échanger des données.

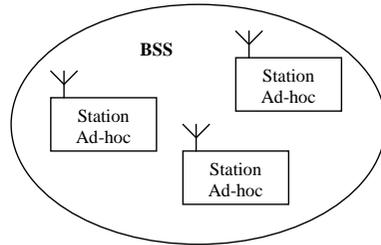


Figure 10 : Communication point à point dans un réseau Ad-hoc

2.2 RESEAU AVEC POINT D'ACCES

Dans la plupart des cas, le BSS renferme un Point d'Accès (AP). La fonction principale d'un AP est de former un pont entre le LAN filaire et le LAN sans-fil. Celui-ci est donc relié au LAN filaire par un câble Ethernet et aux stations du LAN sans fil par radio. Un point d'accès agit en fait comme une passerelle entre le protocole CSMA/CD d'Ethernet et le protocole CSMA/CA du sans fil.

En présence d'un AP, les stations ne communiquent plus en point à point : toutes les communications entre les stations ou entre une station et un LAN filaire passent par l'AP. Les APs ne sont pas mobiles, et font partie du réseau filaire.

Lorsqu'on regroupe une série de BSS qui se superposent (chacun contenant un AP), on forme un ESS (Extended Service Set), représenté en Figure 3. Les APs sont reliés entre eux par un Système de Distribution (DS). Ce DS est dans la majorité des cas un LAN Ethernet.

Les nœuds mobiles peuvent errer entre les différents APs, on parle alors de "roaming" ; couvrir un campus entier (par exemple) par un LAN sans fil, c'est à dire rester connecté au réseau en tout point du campus est ainsi possible.

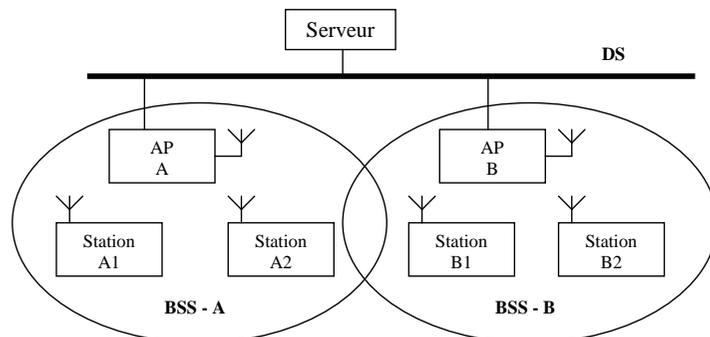


Figure 11 : ESS : Réseau avec points d'accès

2.3 FONCTIONNEMENT : COMMENT UNE STATION REJOINT-ELLE UN BSS ?

2.3.1 Synchronisation

Quand une station veut accéder à un BSS ou à un IBSS, soit après démarrage ou après un passage en mode de veille, la station a besoin d'informations de synchronisation de la part du point d'accès (ou des autres stations dans le cas d'un réseau ad-hoc). Les stations doivent obligatoirement rester synchronisées ; ceci est nécessaire pour garder la synchronisation au cours des sauts (dans le cas de la méthode d'étalement de spectre à saut de fréquence) ou pour d'autres fonctions comme l'économie d'énergie.

La station peut obtenir ces informations par une des 2 techniques suivantes :

- **Ecoute active** : dans ce cas, la station essaie de trouver un point d'accès en transmettant une trame de demande de synchronisation (Probe Request Frame) et attend une trame "balise" (Beacon Frame) de la part du point d'accès. La trame balise est une trame contenant les informations de synchronisation. Elles contiennent en fait la valeur de l'horloge du point d'accès au moment de la transmission (notons que c'est le moment où la transmission a réellement lieu, et non quand la transmission est mise à la suite des transmissions à faire. Puisque la trame balise est transmise selon les règles du CSMA, la transmission pourrait être différée significativement).
- **Ecoute passive** : dans ce cas, la station attend simplement de recevoir une trame "balise" (Beacon Frame), celle-ci étant envoyée périodiquement par le point d'accès toutes les 100ms par exemple. Les stations réceptrices vérifient la valeur de leur horloge au moment de la réception, et la corrigent pour rester synchronisées avec l'horloge du point d'accès. Ceci évite des dérives d'horloge qui pourraient causer la perte de la synchronisation au bout de quelques heures de fonctionnement.

La première technique est utilisée lorsque la station veut se connecter à un BSS pour la première fois (ou pour se reconnecter). La deuxième est utilisée pour garder la synchronisation avec le point d'accès une fois que la station a déjà été associée au BSS.

2.3.2 L'authentification

Une fois qu'une station a trouvé un point d'accès et une cellule (BSS) associée, le processus d'authentification s'enclenche (voir chapitre sur la sécurité).

2.3.3 L'association

Une fois la station authentifiée, le processus d'association s'enclenche. Celui-ci consiste en un échange d'informations concernant les différentes stations, les capacités de la cellule et enfin l'enregistrement de la position actuelle de la station par le point d'accès.

C'est seulement après la fin du processus d'association que la station peut transmettre et recevoir des trames de données.

Etant associée à une cellule, la station reste synchronisée avec le point d'accès par écoute passive. Le point d'accès transmet régulièrement les trames appelées trames "balises", qui

contiennent la valeur de son horloge interne et qui permettent aux stations de synchroniser leur horloge.

2.3.4 Le roaming

Le roaming est le processus de mouvement d'une cellule vers une autre sans perdre la connexion au réseau. Cette fonction est similaire au "handover" des téléphones portables, mais avec deux différences majeures :

- Sur un LAN, qui est basé sur une transmission par paquets, la transition d'une cellule à une autre doit être faite entre deux transmissions de paquets, contrairement à la téléphonie où la transition peut subvenir au cours d'une conversation. Ceci rend le roaming plus facile dans les LANs sans fil, mais...
- Dans un système vocal, une déconnexion temporaire peut ne pas affecter la conversation, alors que dans un environnement de paquets, les performances seront considérablement réduites à cause de la retransmission qui sera exécutée par les protocoles des couches supérieures.

Le standard 802.11 ne définit pas intégralement le processus de roaming, mais en définit cependant les règles de base (les processus sont différents selon les constructeurs). Celles-ci comprennent l'écoute active ou passive, le processus de ré-association (une station qui passe d'un point d'accès à un autre sera associée au nouveau point d'accès).

D'autre part le roaming n'est possible que si ces points d'accès sont configurés avec le même "Network ID" (le nom du réseau).

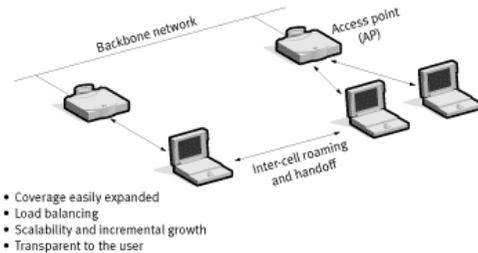


Figure 12 : Le roaming : passage d'un point d'accès à un autre

3. ANATOMIE D'UN LAN SANS-FIL 802.11B

3.1 LE MODELE OSI

Grâce au modèle de référence OSI de l'ISO, on peut facilement représenter ce que définit la norme 802.11. Comme tous les protocoles 802 de l'IEEE, le protocole 802.11 se situe dans les couches basses du modèle OSI. En l'occurrence, la norme 802.11 définit seulement les deux couches les plus basses du modèle OSI. Ainsi sont définies la couche physique PHY et la sous-couche MAC (Medium Access Control) de la couche liaison de données.

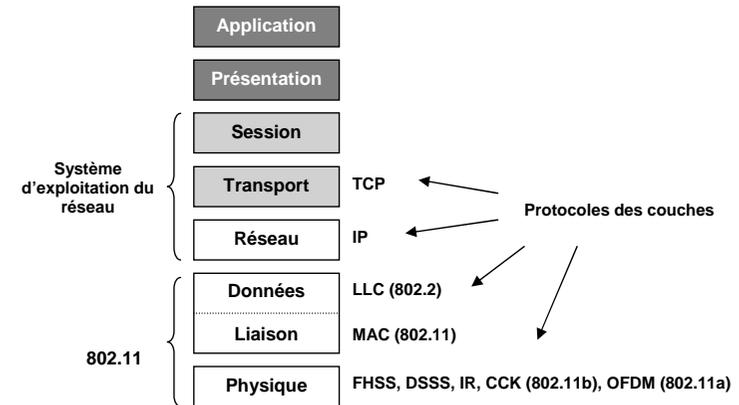


Figure 13 : 802.11 dans le modèle OSI

La **couche physique** gère essentiellement la transmission des bits sur le support de communication, les niveaux électriques et les modulations. Exemples de normes classiques pour la couche physique : protocole V24 (ou RS232C), protocole V11 (ou RS422)...

Notons ici que l'architecture de base, les caractéristiques et services du protocole **802.11b** sont définis par le protocole 802.11. Les spécifications du **802.11b** affectent seulement la couche physique en ajoutant un taux de transfert plus rapide et des connexions plus robustes.

La **couche liaison de données** gère la fiabilité du transfert des informations, le découpage en trames, la protection contre les erreurs, les trames d'acquiescement et la régulation du trafic. Cette couche se compose de 2 sous-couches :

- La **sous-couche liaison logique LLC** (Logical Link Control) : elle gère les erreurs, le trafic, le flux, et la liaison au support. Dans le cas d'un LAN 802.11, cette sous-couche est la même que pour un LAN filaire. Elle est définie par le protocole 802.2 (adressage 48 bits). Elle est reprise simplement pour permettre le pontage entre les LANs sans fil et les LANs filaires de l'IEEE. Exemples de protocoles LLC : SDLC, HDLC, LAP, LLC...
- La **sous-couche d'accès au support MAC** (Medium Access Control) : elle gère le partage du support. En plus des fonctions habituellement rendues par la couche MAC, la couche MAC 802.11 offre d'autres fonctions qui sont normalement confiées aux protocoles supérieurs, comme la fragmentation des données, les retransmissions de paquet et les accusés de réception. Exemples de protocoles MAC : ALOHA, 802.3 (CSMA/CD), CSMA/CA, 802.4 (bus à jeton), 802.5 (anneau à jeton)...

La **couche réseau** n'est pas gérée par 802.11. Détailler cette couche nous permet de voir ce que 802.11 n'intègre pas : la couche réseau gère l'acheminement des informations (routage, contrôle de flux), les adressages, l'interconnexion de réseaux hétérogènes et l'établissement et la libération des connexions. Exemples de protocoles de la couche réseaux : IP (Internet Protocol), X25...

3.2 SYNOPTIQUE GENERAL : DES ONDES AU FIL

Pour mieux comprendre comment fonctionne chaque élément d'un LAN sans fil, il est utile de détailler chaque partie constitutive d'un système sans fil 802.11 dont le synoptique général est représenté ci-dessous en figure 6.

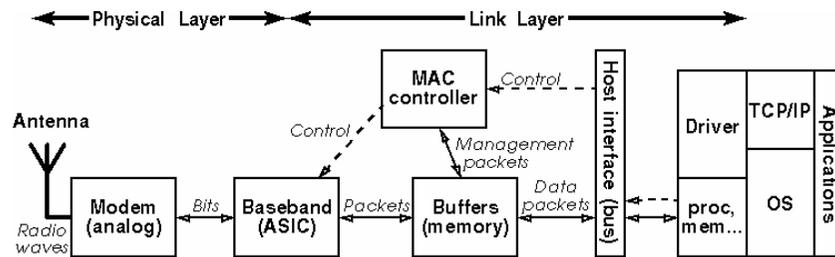


Fig. 14 : Synoptique général d'un système sans-fil 802.11

Nous allons décrire chaque partie séparément.

3.2.1 L'équipement radio

Un réseau radio est une multitude de nœuds appelés à communiquer en utilisant les ondes radioélectriques pour porter l'information grâce à des équipements radio. La plupart des équipements radio se présentent sous forme de carte (ISA, PCI ou PCMCIA) à brancher directement sur un PC.

Un équipement radio est composé de deux parties principales :

- le **modem** (modulateur/démodulateur) **radio**, qui constitue la partie devant transmettre à l'aide d'une modulation le signal sur la bonne fréquence et inversement recevoir l'information captée et donc effectuer la démodulation. Il est composé principalement de parties analogiques (antenne, amplificateurs, convertisseurs de fréquences, oscillateurs, filtres) et d'un démodulateur (généralement un ASIC). Tout ce petit monde est encapsulé dans un blindage métallique pour protéger le PC des radiations à haute fréquence. Les caractéristiques principales du modem sont : la bande de fréquence, le taux de transfert, la modulation et la puissance transmise.
- le **contrôleur MAC**. Le protocole MAC est principalement implémenté dans un ASIC et/ou un microcontrôleur sur la carte même, avec parfois certaines fonctionnalités gérées directement par le driver sur le PC. La carte contient aussi quelques blocs mémoire pour le contrôleur MAC afin de stocker les paquets entrants et sortants (buffers) et autres données (configuration, statistiques...). Les caractéristiques principales du contrôleur MAC sont le format des paquets (taille, en-têtes), la méthode d'accès au canal, et des fonctionnalités purement liées au management de réseau.

3.2.2 La "host interface"

On trouve ensuite la "host interface" qui fait le lien de la carte au PC par un de ses bus (ISA, PCI, Pcmcia...) ou de ses ports de transmission (séquentiel, parallèle, USB ou Ethernet). Cette

interface permet au logiciel (la plupart du temps le driver) de communiquer avec le contrôleur MAC et la majeure partie du temps directement avec la mémoire de la carte (le logiciel écrit des paquets à un emplacement spécifique, et le contrôleur les lit et les envoie). La caractéristique principale de l'interface est principalement la vitesse (E/S, mémoire partagée ou accès direct à la mémoire (DMA)) et la capacité de traiter des demandes en parallèle.

3.2.3 Le driver

Avec tous les systèmes d'exploitation modernes, l'application n'accède pas directement au matériel mais utilise un API standard. Le système d'exploitation a besoin d'un driver pour interfacer le matériel avec le protocole réseau (TCP/IP, NetBeui, IPX...). La fonction principale du driver est de gérer le matériel et de répondre à ses interruptions.

4. LA COUCHE PHYSIQUE : LE MODEM RADIO

Le standard définit actuellement une seule couche MAC qui interagit avec 3 couches physiques :

- FHSS Frequency Hopping Spread Spectrum
- DSSS Direct Sequence Spread Spectrum
- l'infrarouge

4.1.1 Le FHSS ou saut de fréquence

La bande des 2.4 GHz est divisée en 79 canaux de 1 MHz chacun. Cette technique est basée sur le saut de fréquence périodique de l'émetteur (toutes les 20 à 400ms), suivant un ordre cyclique prédéterminé. Le fait de ne jamais rester sur le même canal accroît fortement l'immunité au bruit. Dans le cas de canaux encombrés, cela permet d'avoir au final un bon moyennage et d'utiliser au mieux toute la bande passante allouée. Cette technique rend difficile l'interception de trames. L'avantage de cette technique est aussi que même en perdant quelques "sauts" (ou hop) suite à des interférences très localisées, on peut tout de même retrouver le signal. D'un autre côté, si le bruit de fond est plus puissant que le signal émis, il n'y a rien à faire. De plus, cette méthode de transmission est relativement simple mais elle est limitée par son débit maximum de 2 Mbits/s. Enfin, elle introduit une certaine complication au niveau MAC, ce qui se traduit en termes de multiplication d'en-têtes et donc de réduction de débit.

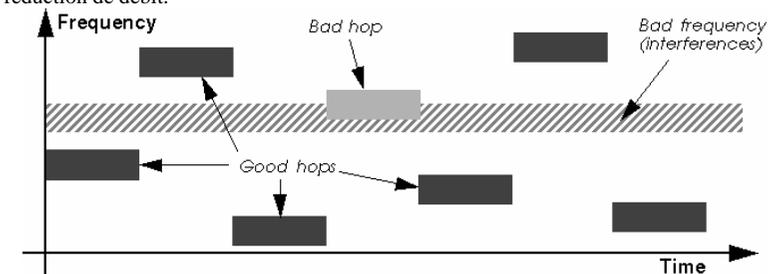


Figure 15 : FHSS

4.1.2 Le DSSS ou séquence directe

La technique de la séquence directe divise la bande des 2.4 GHz en 14 canaux de 22 MHz chacun. Les données sont envoyées uniquement sur l'un des 14 canaux. Pour minimiser le bruit de fond et les interférences locales, une technique dite de "chipping" est utilisée. Elle consiste à convertir les bits de données en une série de bits redondants. Le bit 1 sera remplacé par une succession de 11 bits 0 ou 1 (appelée code PN) pendant le même temps de transmission. Le bit 0 sera remplacé par le complémentaire de la succession de bits utilisée pour le bit 1 (voir ci-dessous).

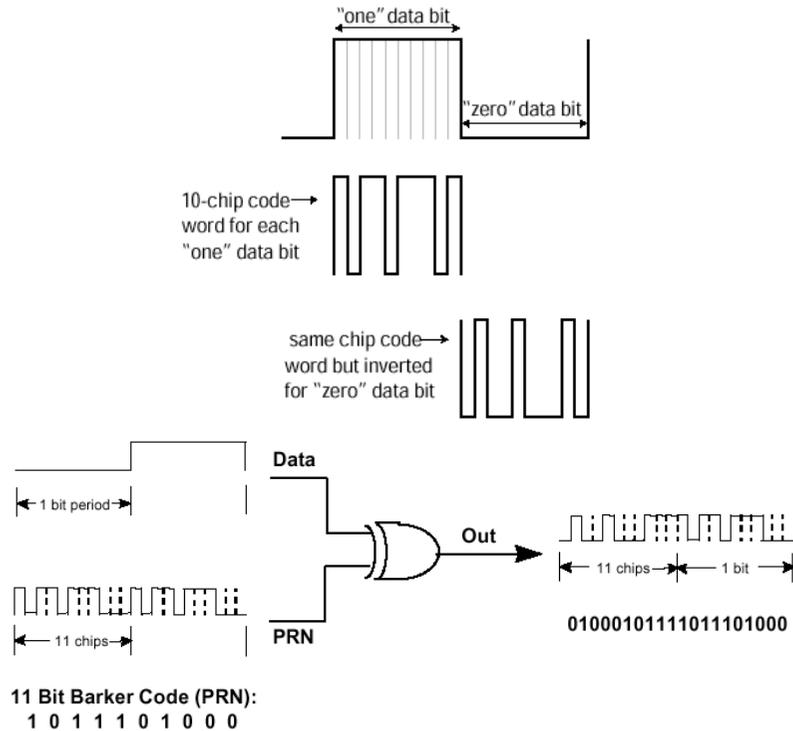


Figure 16 : code PN - chipping

On étale ainsi le signal sur une bande de fréquence plus large en sur-modulant chaque bit du paquet à transmettre par ce code PN répétitif. Au niveau du récepteur, le signal original est retrouvé en réceptionnant tout le canal étalé et en le démodulant avec le même code.

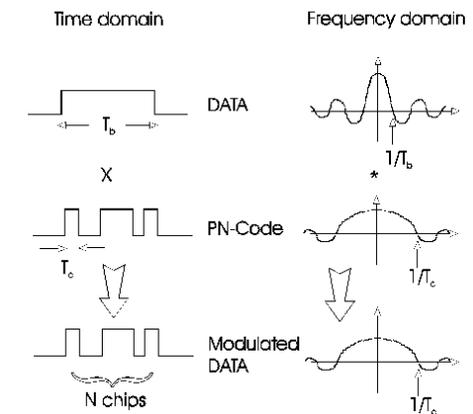
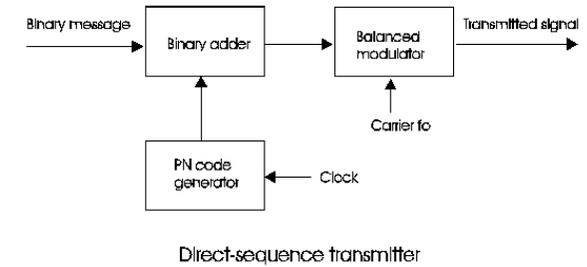


Figure 17 : code PN - étalement

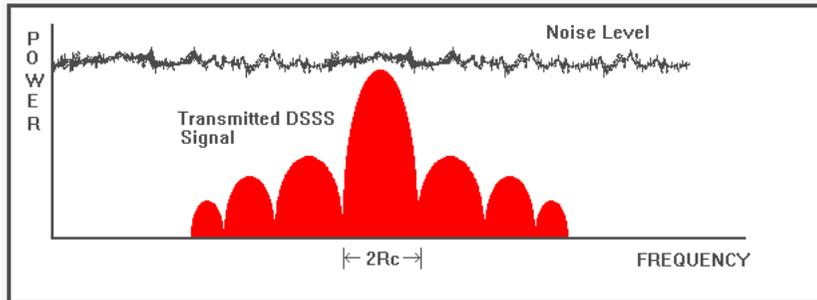


Figure 18 : DSSS

Le DSSS du protocole 802.11 spécifie donc un chipping de 11 bits appelé *Barker sequence*. Chaque séquence de 11 bits représente un bit (0 ou 1) de données. Elle est ensuite convertie en onde appelée *symbol* transmis à 1 MS/s (1 millions de Symboles par seconde). C'est la modulation utilisée qui permet d'avoir des débits différents. La BPSK (Binary Phase Shift Keying) pour un débit de 1 Mbit/s et la QPSK (Quadrature Phase Shift Keying) pour un débit de 2 Mbit/s.

Dans le protocole 802.11b, pour pouvoir supporter les 2 nouveaux débits 5.5 Mbit/s et 11 Mbit/s, seul le DSSS est utilisé. En effet, le FHSS ne pourrait pas supporter ces nouveaux débits sans violer les règles actuelles du FCC (Federal Communication Commission).

Cette augmentation des débits est faite grâce aux techniques de modulation et de codage comme le CCK (Complementary Code Keying). Mais quelle que soit le débit employé, et c'est d'ailleurs pourquoi ces techniques ont été autorisées, le signal est toujours étalé sur 22 MHz (=2*taille codage*vitesse de symbole).

Le tableau suivant récapitule la situation :

Débits	Codage ?	Modulation	Vitesse de symbole	Nb de bits/symbole
1 Mbit/s	11 (Barker Sequence)	BPSK	1 MS/s	1
2 Mbit/s	11 (Barker Sequence)	QPSK	1 MS/s	2
5.5 Mbit/s	8 (CCK)	QPSK	1,375 MS/s	4
11 Mbit/s	8 (CCK)	QPSK	1,375 MS/s	8

Figure 19 : Tableau récapitulatif des différentes techniques.

Ainsi, toute interférence à bande étroite apparaîtra très faible, d'autant plus que le démodulateur utilise le même code que l'émetteur pour retrouver le signal étalé, ce qui minimise encore les signaux aléatoires.

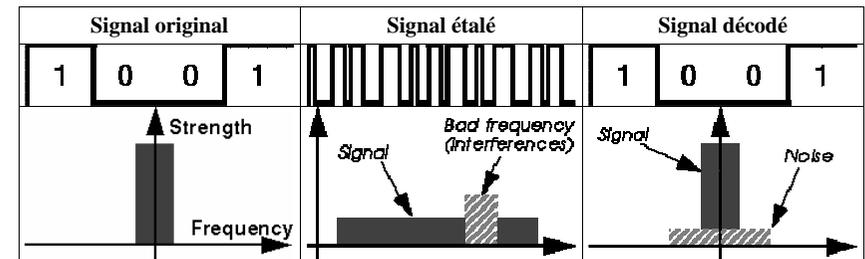


Figure 20 : Robustesse aux interférences

Mais par conséquent, dans cette technique où la bande passante de chaque canal est de 22MHz, ceci implique que seuls 3 canaux (sur les 14 prévus par la norme) peuvent être utilisés de manière adjacente si on veut totalement éviter le recouvrement de spectre. On pointe du doigt un problème latent en France qui limite l'intérêt du LAN sans fil : pour l'instant, seuls 4 canaux sont disponibles. On est donc contraint pour le moment à superposer plusieurs canaux, mais ceci tend à augmenter le bruit et diminuer ainsi les performances du système, car tous les produits opèrent avec le même code PN (et non un code par fréquence) !

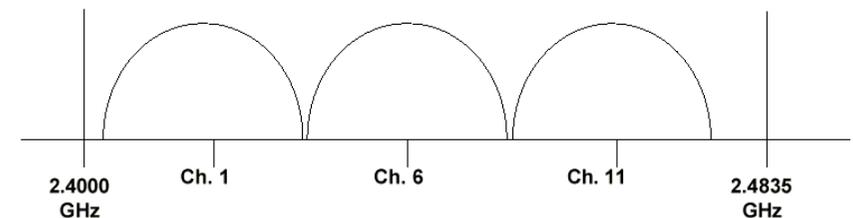


Figure 21 : Espacement des canaux adjacents pour limiter tout recouvrement spectral

Frequency Range	2400-2500 MHz ¹			
Channel ID	FCC	ETSI	France	Japan
1	2412	2412	-	2412
2	2417	2417	-	2417
3	2422	2422	-	2422
4	2427	2427	-	2427
5	2432	2432	-	2432
6	2437	2437	-	2437
7	2442	2442	-	2442
8	2447	2447	-	2447
9	2452	2452	-	2452
10	2457	2457	2457	2457
11	2462	2462	2462	2462
12	-	2467	2467	2467
13	-	2472	2472	2472
14	-	-	-	2484

Figure 22 : Fréquences des canaux alloués

4.1.3 Comparaison des deux techniques

Saut de fréquence	Séquence directe
<ul style="list-style-type: none"> faible débit (2Mbps maxi) + sûr du point de vue de la sécurité + grande portée cohabitation aisée entre LANs sans fil 30 à 50 stations par point d'accès pour un débit intéressant (8 ko/s mini) à condition d'avoir un petit réseau (peu de points d'accès car pas de partage de la bande) modulation plus simple moins onéreux 	<ul style="list-style-type: none"> débit élevé (11Mbps, et bientôt 22Mbps) + employé 10 à 20 stations par point d'accès pour un débit intéressant (8 ko/s mini), quelle que soit la taille du réseau moins d'interférences car pas de partage désordonné de la bande passante protocole MAC plus simple

5. LA COUCHE MAC

La norme IEEE 802.11 utilise les retransmissions au niveau MAC, le RTS/CTS et la fragmentation de paquets. La sous-couche MAC définit deux normes d'exécution : le mode distribué CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), le plus utilisé, et le mode par point.

Au niveau de la sécurité, le protocole MAC du 802.11 inclut l'authentification facultative et le cryptage des données (utilisant le WEP, Wired Equivalent Privacy, qui est du RC4 à 40 bits ; quelques constructeurs offrent du RC4 à 128 bits). Pour plus de détails sur ces points, voir le chapitre sur la sécurité.

5.1 LE CSMA/CA

5.1.1 Le CSMA et les collisions

Dans les réseaux filaires, on utilise les protocoles CSMA comme mécanisme d'accès de canal, c'est à dire un mécanisme qui indique comment chaque nœud peut utiliser le support (le canal) : quand écouter, quand transmettre... Le principal avantage du CSMA est qu'il est approprié aux protocoles de réseau tels que le TCP/IP, qu'il s'adapte tout à fait bien avec l'état variable du trafic et qu'il est tout à fait robuste aux interférences.

Le protocole CSMA fonctionne ainsi : une station voulant transmettre sonde le support de transmission. S'il est occupé (une autre transmission est en cours), alors la station reporte sa transmission pour plus tard. S'il est libre, alors la station peut émettre.

Ce type de protocole est très efficace lorsque le support n'est pas surchargé, dans la mesure où il permet aux stations d'émettre avec un minimum d'attente, mais il existe toujours un risque pour que deux stations émettent en même temps après avoir détecté un support libre et créent ainsi une collision.

Il faut alors détecter ces collisions pour que la couche MAC puisse retransmettre la trame sans avoir à repasser par les couches supérieures, ce qui engendrerait des retards significatifs. Pour Ethernet, les collisions sont repérées par les stations émettrices qui effectuent alors un algorithme de retransmission appelé algorithme de retour aléatoire exponentiel ("Algorithme de Back-off aléatoire exponentiel").

Si ces mécanismes de détection de collision sont bons sur un réseau local câblé, ils ne peuvent pas être utilisés dans un environnement sans fil, ceci pour deux raisons principales :

- Implémenter un mécanisme de détection de collision demanderait l'implémentation d'une liaison radio full duplex, capable de transmettre et de recevoir simultanément, ce qui augmenterait le prix.
- Dans un environnement sans fil, on ne peut pas être sûr que toutes les stations ont un lien radio entre elles (ce qui est l'hypothèse de base du principe de détection de collision), et le fait que la station voulant transmettre teste si le support est libre, ne veut pas forcément dire que le support est libre autour du récepteur.

Pour pallier ces problèmes, 802.11 utilise un mécanisme d'évitement de collision associé à un système d'accusé de réception : le CSMA/CA.

5.1.2 Le mécanisme d'accès de canal du DCF ou CSMA/CA

La couche MAC définit deux méthodes d'accès de canal différentes, la Fonction de Coordination Distribuée (DCF : Distributed Coordination Function) et la Fonction de Coordination par Point (PCF : Point Coordination Function).

Le mécanisme d'accès de base, le DCF, est typiquement le mécanisme CSMA/CA, qui est le mécanisme d'accès de canal employé par la plupart des LANs sans fil dans les bandes ISM. CSMA/CA est dérivé de CSMA/CD (Collision Detection), qui est la base d'Ethernet. Nous reparlerons du PCF plus loin.

Détection physique de porteuse :

Le mécanisme de base est l'écoute du canal avant transmission. Ce mécanisme est appelé détection physique de porteuse.

La station voulant transmettre commence par écouter le canal de transmission :

- Si le canal est occupé (une autre transmission est en cours), l'émetteur attend la fin de transmission du paquet et émet au bout d'une période aléatoire. Si le canal est encore occupé à l'émission, il utilise toujours le même algorithme. Puisque le temps d'attente avant émission est un nombre aléatoire pour chaque paquet, chaque nœud a la même probabilité d'accès au canal.
- Si le canal est libre au moins pendant un temps spécifié, appelé DIFS (Distributed Inter Frame Space), il émet le paquet. Après fin de transmission du paquet, le destinataire vérifie le CRC du paquet et renvoie un accusé de réception à l'émetteur, ce qui signifie à l'émetteur qu'il n'y a pas eu collision. Les collisions ne sont donc pas détectées, mais s'il y a collision, les deux stations qui l'ont provoquée ne reçoivent pas l'accusé de réception du destinataire, donc tentent de ré-émettre chacune au bout d'un temps aléatoire. Le premier à ré-émettre peut alors transmettre son paquet. En pratique, avec les cartes Orinoco, lorsqu'un accusé de réception n'est pas reçu, l'émetteur ré-émet le paquet. Si au bout de plusieurs fois, il n'y a toujours pas de réponse, la station ré-émet à un débit moins important.

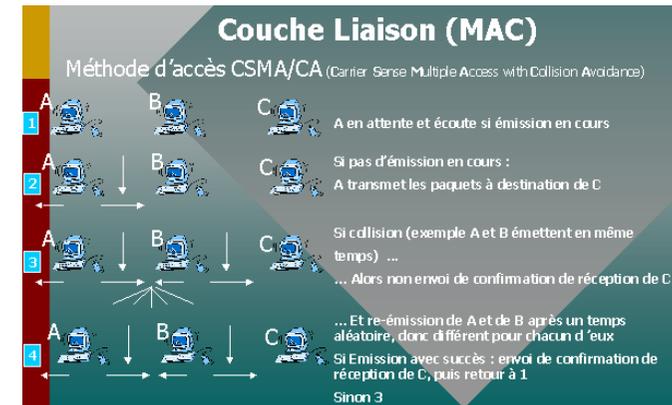


Figure 23 : Le mécanisme de détection physique de porteuse

Détection virtuelle de porteuse :

Pour réduire la probabilité de collision due au fait que deux stations sans fil appartenant au même réseau n'ont pas de liens radio entre-elles (elles sont trop éloignées), 802.11 utilise un mécanisme de détection virtuelle de porteuse. Nous allons nous servir de la figure 15 pour expliquer ce mécanisme.

Une station (A sur la figure) voulant transmettre commence par émettre un court message appelé RTS (Ready To Send), qui contient les adresses de l'émetteur et du destinataire et la durée du message. Si le canal est libre (donc après une non-détection physique de porteuse), le destinataire (B) émet alors un message CTS (Clear To Send) comportant les mêmes informations que le RTS, indiquant à l'émetteur que son paquet peut être envoyé.

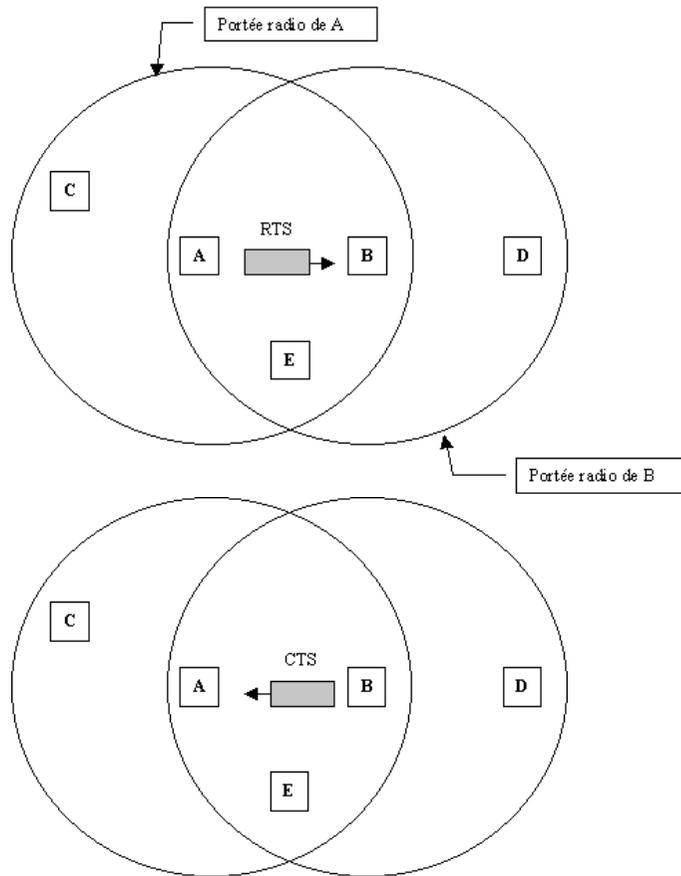


Figure 24 : Détection virtuelle de porteuse : le problème des stations "cachées"

Toutes les stations recevant ce message RTS ou/et CTS mettront à jour leur indicateur de détection virtuelle de porteuse (appelé NAV pour Network Allocation Vector : indique le temps minimal de report) pour la durée précisée dans ces messages et utiliseront ces informations en parallèle avec la détection physique de porteuse pendant le processus de détection avant d'émettre un message. Ainsi, sur la figure 16, la station C aura reçue le RTS, la station D le CTS et la station E le RTS et le CTS.

Ce mécanisme réduit la probabilité de collision par une station "cachée" de l'émetteur dans la zone du récepteur à la courte durée de transmission du RTS, parce que la station entend le CTS et considère le support comme occupé jusqu'à la fin de la transaction. L'information "durée d'occupation du canal" dans le RTS et le CTS protège la zone de l'émetteur des collisions pendant la transmission de l'accusé de réception (par les stations étant hors de portée de la station accusant réception).

Il est également important de noter que grâce au fait que le RTS et le CTS soient des trames courtes (30 octets), le nombre de collisions est réduit, puisque ces trames sont reconnues plus rapidement que si tout le paquet devait être transmis. Ceci est vrai si le paquet est beaucoup plus important que le RTS. Le standard autorise donc les paquets courts à être transmis sans l'échange de RTS/CTS, ceci étant contrôlé pour chaque station grâce au paramètre appelé *RTS Threshold*. (Voir documentation driver linux et tests sans RTS/CTS).

Le diagramme de la figure 17 résume les échanges entre les deux stations A et B et le vecteur NAV des stations voisines.

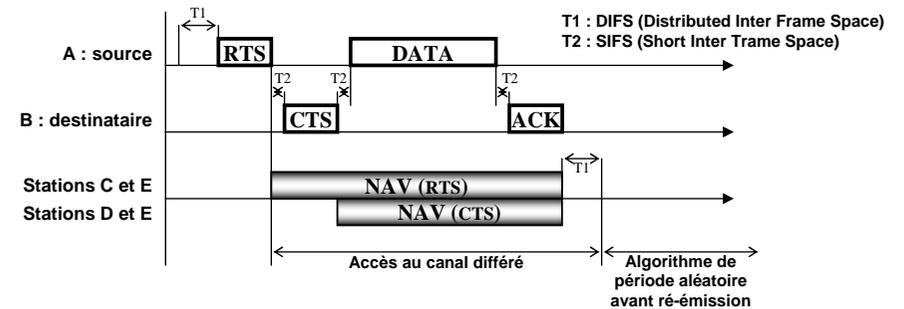


Figure 25 : Echanges entre 2 stations A et B et vecteur NAV des autres stations

5.1.3 La Fonction de Coordination par Point (PCF)

A l'opposé du DCF, où le contrôle d'accès au canal est distribué sur toutes les stations, le mode PCF définit le point d'accès comme seul contrôleur d'accès au canal.

Si le mode PCF est actif dans un BSS, le temps est partagé entre le mode PCF et le mode DCF pour permettre aux stations l'accès au canal. Dans le mode PCF, le point d'accès élit chaque station pour un temps déterminé et passe à la station suivante. Ainsi, chaque station n'est autorisée à transmettre ou à recevoir les données que si elle a été élue. Ce fonctionnement permet de garantir la qualité de service, mais sur un réseau important le fait de n'avoir qu'un seul point d'accès au canal et d'élire tour à tour chaque station peut-être un inconvénient. Notons que le PCF est très peu utilisé dans la couche MAC des LANs sans fil.

5.2 LA SECURITE

La sous-couche MAC définit un mécanisme de cryptage et de contrôle d'accès appelé WEP (Wired Equivalent Privacy) que nous allons décrire plus précisément dans le chapitre adéquat (sécurité).

5.2.1 L'accès aux ressources du réseau

L'accès aux ressources du réseau est obtenu en utilisant un mécanisme d'authentification où une station est obligée de prouver sa connaissance d'une clé, ce qui est similaire à la sécurité sur réseaux câblés, dans le sens où l'intrus doit entrer dans les lieux (en utilisant une clé physique) pour connecter son poste au réseau câblé.

5.2.2 L'écoute clandestine

L'écoute clandestine est bloquée par l'utilisation de l'algorithme WEP qui est un générateur de nombres pseudo-aléatoires initialisés par une clé secrète partagée par toutes les stations d'un LAN. L'algorithme WEP est un simple algorithme basé sur l'algorithme RC4 de RSA, qui a les propriétés suivantes :

- Plutôt performant : l'attaque par "force brutale" (essai de décodage par des clés aléatoires ou des listes de clés) de cet algorithme est difficile car chaque trame est envoyée avec un vecteur d'initialisation qui relance le générateur de nombres pseudo-aléatoires.
- Autosynchronisé : l'algorithme se resynchronise pour chaque message. Ceci est nécessaire pour travailler en mode non connecté, où les paquets peuvent être perdus, comme dans tout réseau local.

5.3 L'ECONOMIE D'ENERGIE

Les réseaux sans fil sont généralement en relation avec des applications mobiles, et dans ce genre d'application, l'énergie de la batterie est une ressource importante. C'est pour cette raison que le standard 802.11 donne lui-même des directives pour l'économie d'énergie et définit tout un mécanisme pour permettre aux stations de se mettre en veille pendant de longues périodes sans perdre d'information.

L'idée générale, derrière le mécanisme d'économie d'énergie, est que le point d'accès maintient un enregistrement à jour des stations travaillant en mode d'économie d'énergie, et garde les paquets adressés à ces stations jusqu'à ce que les stations les demandent avec une requête de polling, ou jusqu'à ce qu'elles changent de mode de fonctionnement.

Les points d'accès transmettent aussi périodiquement (dans les trames "balise") des informations spécifiant quelles stations ont des trames stockées par le point d'accès. Ces stations peuvent ainsi se réveiller pour récupérer ces trames balise, et si elles contiennent une indication sur une trame stockée en attente, la station peut rester éveillée pour demander à récupérer ces trames.

Les trames de multicast et de broadcast (trames destinées à toutes les stations du réseau) sont stockées par le point d'accès et transmises à certains moments (à chaque DTIM) où toutes les stations en mode d'économie d'énergie qui veulent recevoir ce genre de trames devraient rester éveillées.

5.4 CONCLUSION SUR LES FONCTIONNALITES DE LA COUCHE MAC

Donc la couche MAC :

- Décrit comment les trames "balise" sont envoyées à intervalles réguliers (par ex 100 ms) des APs aux stations pour permettre à celles-ci de gérer la présence ou non de l'AP.
- Donne une batterie de trames de management qui permettent aux stations de scanner régulièrement leur environnement en quête d'autres APs sur chaque canal disponible.
- Définit des fonctionnalités spéciales pour la retransmission de paquets non reçus, la fragmentation des paquets, la réservation du « médium » via RTS/CTS (Request To Send/Clear To Send) etc...
- Dans le cas des réseaux ad hoc, il n'y a pas de point d'accès, et une partie de ses fonctionnalités sont reprises par les stations elles-mêmes (comme les trames "balise" pour la synchronisation). D'autres fonctions ne sont pas utilisables dans ce cas : le relayage des trames et le mode d'économie d'énergie).

On ne peut pas faire de changements énormes au niveau MAC, comme par exemple « upgrader » son WLAN 802.11b à 802.11a en changeant le protocole, et ceci pour la simple raison que la majorité du protocole MAC est embarqué dans la carte (sur le microcontrôleur ou voire même sur un ASIC ou un FPGA pour les couches basses du protocole MAC) et que seulement quelques fonctions sont prises en charge par le driver. De plus, les constructeurs ne disent en général pas comment reprogrammer le driver de leurs produits mais même s'ils le faisaient, cela ne suffirait pas pour créer des émetteurs/récepteurs radios universels qui puissent être re-configurables facilement et à volonté pour recevoir n'importe quel standard radio. Pour cela, il faudrait re-concevoir toute la carte avec un bloc conséquent de logique re-programmable sur laquelle on téléchargerait une nouvelle configuration pour le protocole que l'on désirerait utiliser, afin de pouvoir s'adapter à n'importe quel modulation ou taux de transfert. Ce serait alors un produit implémenté entièrement en numérique et non plus principalement analogique comme c'est le cas actuellement. Il faudrait tout d'abord numériser toute la bande passante du signal capté, avec un convertisseur analogique numérique très rapide, et « envoyer » le tout dans un DSP ou un FPGA (Field Programmable Gate Array). Le problème principal serait, d'une part le coût d'un tel produit, mais aussi et surtout de gérer tout ce que cela implique de travailler avec des fréquences de l'ordre du GigaHertz !