Evaluation et optimisation du mécanisme de Handhover dans un Réseau Local Sans Fil dédié aux applications à trafic contraint par le temps

Sébastien Hernandez

N° d'ordre DU : 1682
E D S P I C : 356

UNIVERSITÉ BLAISE PASCAL - CLERMONT II
ECOLE DOCTORALE SCIENCES POUR L'INGÉNIEUR

THESE

présentée par

Sébastien HERNANDEZ

pour obtenir le grade de

DOCTEUR D'UNIVERSITE
SPECIALITE INFORMATIQUE

Evaluation et Optimisation du mécanisme de "Handover" dans un Réseau Local Sans Fil dédié aux applications à trafic contraint par le temps

Soutenue publiquement le 20 octobre 2006 devant le jury :

Pr. Michel SCHNEIDER	Président	Université de Clermont-Ferrand II
Pr. Michel MISSON	Directeur de Thèse	Université de Clermont-Ferrand I
Pr. Thierry VAL	Rapporteur	Université de Toulouse II
Dr. Philippe FRAISSE	Rapporteur	Université de Montpellier II
Dr. Vincent LECUIRE	Examinateur	Université de Nancy I
Dr. Antonio FREITAS	Examinateur	Université de Clermont-Ferrand I

Remerciements

Je tiens tout d'abord à remercier Monsieur Michel MISSON, Professeur à l'université de Clermont I, pour m'avoir proposé ce sujet, m'avoir encadré tout au long de ce travail et m'avoir encouragé pendant les périodes de doutes.

Je remercie Monsieur Michel SCHNEIDER, Professeur à l'université de Clermont II, pour m'avoir accueilli dans son laboratoire.

Je remercie Monsieur Thierry VAL, Professeur à l'université de Toulouse II et Monsieur Philippe FRAISSE, Maître de Conférences à l'université de Montpellier II, pour avoir accepté d'être les rapporteurs de mon travail et y apporter des critiques constructives, ainsi que pour nos collaborations au sein du groupe de travail L2I.

J'adresse mes remerciements à Monsieur Vincent LECUIRE, Maître de Conférences à l'université de Nancy I, pour avoir accepté d'être membre du jury.

Je remercie tout particulièrement Monsieur Antonio FREITAS, Maître de Conférences à l'univesité de Clermont I, pour avoir accepté de participer à mon jury, mais surtout pour nos différentes collaborations aussi bien au sein de l'université qu'en dehors.

Je tiens également à remercier toutes les personnes de l'équipe Réseaux et Protocoles, en particulier Frédérique, Nadir, Sabri, Walid, Patrick, Philippe, Bruno, Damien, Frank, Rachid, Gérard, Ali, Richard. Ainsi que mes collègues de l'IUT, en particulier François, Joël, Florence, Nathalie, Patrick, Lindsay, Jerzy, David, Laurent que j'ai côtoyé avec plaisir.

Pour terminer je remercie ma famille : mes parents, ma soeur, mes grands-parents, Paul, ainsi que tous mes amis, pour être à mes cotés depuis de nombreuses années.

Table des matières

Introduction **1**

Partie I État de l'art **7**

Chapitre 1
Les réseaux sans fil

1.1 Le médium radio 10
1.2 Éléments de Transmission 13
1.2.1 Modulations 13
1.2.2 Méthodes de transmission 13
1.3 Notion de Portée 16
1.4 Partage du médium 18
1.4.1 Introduction 18
1.4.2 Les principales méthodes d'accès 18
1.5 Notion de cellule et de couverture cellulaire 23
1.6 Les réseaux cellulaires 26
1.6.1 GSM 27
1.6.2 GPRS 33
1.6.3 UMTS 38
1.6.4 La norme 802.11 42

Chapitre 2
Gestion de l'itinérance dans les réseaux cellulaires

2.1 Le changement de cellule dans GSM 57
2.1.1 Gestion de l'itinérance dans GSM 57
2.1.2 Le Handover GSM 58
2.2 Le changement de cellule dans 802.11 59

Partie II Étude du handover **65**

Chapitre 1
Problème traité

1.1 Rappel des étapes du Handover 68
1.2 Description détaillée et estimation du temps du mécanisme de Handover 70
1.3 Le Handover dans le projet Waves. 72

Chapitre 2
État de l'art pour l'optimisation du Handover de 802.11

2.1 Solutions en exploitant les paramètres de la norme 78
2.1.1 ChannelList 78
2.1.2 MinChannelTime et MaxChannelTime 78
2.1.3 Envoi de données pendant le Handover 80
2.1.4 Réduction de la période de scan par réseaux de capteurs 80
2.2 Optimisation du handover au niveau IP 81
2.3 Gestion du Handover Inter-AP 83
2.3.1 IAPP : Inter Access Point Protocol 83
2.3.2 Tap-Dance 85

Chapitre 3
Le projet Waves

3.1 Application Générique 88
3.1.1 Hypothèses sur le trafic 89
3.1.2 Notion de voisinage 91
3.2 Choix d'un pseudo PCF pour les échanges intra-cellulaires 92
3.3 Première plateforme du projet Waves 92

3.4 Résultats concernant le trafic intracellulaire 93
3.4.1 Nature du trafic intracellulaire 93
3.4.2 Rappel sur le pseudo PCF 94
3.4.3 Choix d'une stratégie de mise à jour cyclique 95
3.4.4 Etude des différentes stratégies de diffusion 95
3.4.5 Conditions Expérimentales de la comparaison 99
3.4.6 Résultats de la comparaison des stratégies 100
3.4.7 Calibrage du simulateur 101
3.4.8 Influence d'un trafic applicatif 102

Partie III Propositions et Résultats **103**

Chapitre 1
Solutions proposées

1.1 Suppression du scan 105
1.2 Solution avec deux cartes sans fil sur la même station 107
1.2.1 Présentation 107
1.2.2 Le problème ARP 110
1.3 Solution par sockets de niveau 2 112
1.4 Handover par l'infrastructure 114
1.5 Gestion de la continuité d'une transmission 118

Chapitre 2
Résultats

2.1 Plateforme de tests 121
2.1.1 Matériel utilisé 121
2.1.2 Ethereal 123
2.2 Le mode scan manuel 123
2.3 Handover par l'infrastructure 126
2.4 Solutions avec deux interfaces sans fil embarquées 129

Conclusion **131**

Bibliographie **135**

Annexes **141**

Annexe A
Trame 802.11

Annexe B
Paramètres pour les sockets RAW

Annexe C
Code Applications

Annexe D
Le driver HostAP

Table des figures

1 *Le spectre électromagnétique* 10
2 *Propagation des ondes électromagnétiques* 11
3 *Interférence intersymboles* 12
4 *Frequency Hopping Spread Spectrum [6]* 14
5 *Direct Sequence Spread Spectrum [6]* 15
6 *Frequency Division Multiple Access* 19
7 *Time Division Multiple Access* 20
8 *TDMA et FDMA combinés* 21
9 *Zone de couverture d'une station sans fil* 24
10 *Couverture cellulaire* 24
11 *Couverture cellulaire avec zone de recouvrement* 25
12 *Les canaux de la bande ISM 2.4 Ghz* 26
13 *Couverture cellulaire avec 3 canaux* 27
14 *Les entités du réseau GSM et son architecture [5]* 30
15 *Structure d'un réseau GPRS [28]* 36
16 *Les piles logicielles d'un système GPRS [28]* 37
17 *Structure d'un réseau UMTS [28]* 41
18 *Topologie avec Infrastructure* 43
19 *Topologie distribuée Ad-Hoc* 44
20 *Méthode d'accès DCF* 47
21 *Le problème du terminal caché* 48

22 *Le mécanisme de réservation RTS/CTS* 49
23 *Méthode d'accès PCF* 49
24 *La période sans contention de PCF* 50
25 *Le handover dans les réseaux GSM [5]* 60
26 *Trames échangées pendant le handover* 69
27 *Etapes d'un Handover en scan actif* 70
28 *Temps de Handover 802.11* 73
29 *Capture des trames échangées pendant le handover* 75
30 *Réseau de capteurs (source [51])* 81
31 *Handover par interrogation de capteurs (source [51])* 82
32 *Temps de Handover au niveau IP* 86
33 *Application générique* 89
34 *Les différents types de trafic* 90
35 *Première plateforme pour le projet Waves* 93
36 *Broadcast-Broadcast* 97
37 *Broadcast-Unicast* 98
38 *Unicast-Broadcast* 99
39 *Unicast-Unicast* 99
40 *Résultats obtenus par le simulateur et avec des stations réelles* 101
41 *Etapes d'un Handover en scan manuel* 107
42 *Trames échangées lors d'un handover sans phase de scan* 108
43 *Handover avec 2 cartes embarquées* 109
44 *Architecture du Handover par le haut* 115
45 *Cas d'une infrastructure switchée* 119
46 *Plateforme générique pour les expérimentations* 122

47 *Le logiciel Ethereal* 124
48 *Capture d'un Handover en mode scan manuel* 125
49 *Schéma de test des performances du Handover par le haut* 127
50 *Handover en mode monitor* 128

Glossaire

AMRF : Accès Multiple à répartition en Fréquence

AMRT : Accès Multiple à Répartition dans le Temps

AP : Access Point

ARP : Address Resolution Protocol

ART : Autorité de Régularisation de Télécommunications

ARCEP : Autorité de Régulation des Communications Electroniques et des Postes

AUC : Authentification Center

BSC : Base Station Controller

BSS : Basic Service Set (dans 802.11), Base Station Sub-system (dans GSM)

BSSID : Basic Service Set IDentifier

BTS : Base Transceiver Station

CEPT : Conférence Européenne des Postes et Télécommunications

CNAM : Conservatoire National des Arts et Métiers

CSMA : Carrier Sense Multiple Access

CSMA/CA : CSMA with Collision Avoidance

CSMA/CD : CSMA with Collision Detection

CW : Contention Window

DCF : Distributed Coordination Function

DSSS : Direct Sequence Spread Spectrum

EDCF : Enhanced DCF

ESS : Extended Service Set

ESSID : Extended Service Set IDentifier

FDMA : Frequency Division Multiple Access

FHSS : Frequency Hopping Spread Spectrum

FRMA : Frame Reservation Multiple Access

GSM : Global System for Mobile communications (à l'origine Groupe Spécial Mobile)

HLR : Home Location Register

IAPP : Inter Access Point Protocol

IBSS : Independent Basic Service Set

IEEE : Institute of Electrical and Electronic Engineers

IFS : Inter-Frame Spaces delay

IP : Internet Protocol

ISM : Industrial, Scientific and Medical radio frequency

LAN : Local Area Network

MAC : Medium Access Control

MS : Mobile Station

MSC : Mobile Switching Center

NAV : Network Allocation Vector

NSS : Network Sub-System

OFDM : Orthogonal Frequency Division Multiplexing

OMC : Operation and Maintenance Center

OSS : Operation Sub-System

PCF : Point Coordination Function

QoS : Quality of Service

RADIUS : Remote Authentification Dial In User Service

RSSI : Receive Signal Strength Indicator

RTS/CTS : Request To Send / Clear To Send

SNR : Signal to Noise Ratio

TCP : Transmission Control Protocol

TDMA : Time Division Multiple Access

UDP : User Datagram Protocol

VLR : Visitor Location Register

WEP : Wired Equivalent Privacy

WI-FI : WIreless Fidelity

WLAN : Wireless Local Area Network

Introduction

La mobilité des entités communicantes, la rapidité de déploiement, la disponibilité de la technologie rendent tout à fait crédible la candidature des réseaux locaux sans fil pour des applications de type industriel. Le choix d'une telle solution pour une application industrielle de grande envergure nécessite de connaître comment se comporte un véritable réseau cellulaire dans un environnement industriel.

En 2002, un projet est proposé à l'équipe Réseaux et Protocoles. Il concerne l'étude du comportement de mobiles guidés, sur rail, qui ont différents besoins en communications, parmi lesquelles des communications utilisées pour faire collaborer des mobiles entre eux (par exemple évitement de collisions, transport d'une charge par plusieurs mobiles). Ces applications sont critiques et les communications sont fortement contraintes par le temps. L'objectif du projet est de proposer une solution de communication, qui respecte les contraintes temporelles fixées, et basée uniquement sur des réseaux locaux sans fil (WLAN pour Wireless Local Area Network).

Dans le cadre du projet, une plateforme a été mise en oeuvre pour évaluer les performances d'un WLAN. Nous avons rapidement opté pour une solution avec infrastructure c'est à dire que la plateforme est composée de stations de base fixes et de stations mobiles. Chaque station de base étant capable de gérer un certain nombre de mobiles dans une zone géographique délimitée, appelée cellule. Dans chaque cellule les mobiles vont communiquer via la station de base. Les caractéristiques et surtout la disponibilité nous a conduit à choisir des produits conformes au standard 802.11 [8] pour nos besoins en communications. En effet nous avons privilégié des communications réelles à des communications simulées pour la plateforme de test.

Quand l'espace nécessaire à l'application dépasse la taille d'une cellule, il est nécessaire d'étendre notre réseau en ajoutant de nouvelles stations de base. Les besoins en mobilité d'une station peuvent l'amener à changer de cellule. Ce processus induit une période de recherche d'une nouvelle station de base, qui implique du traffic autre que le trafic de collaboration entre les mobiles. De plus, pendant ce processus, la station ne pourra plus

communiquer avec les autres. Ce problème est à l'origine du travail étudié dans cette thèse et présenté dans ce manuscrit. Il consiste en l'étude détaillée du phénomène de changement de cellule, appelé handover (ou handoff) ou itinérance (roaming en anglais) pour ensuite proposer des solutions permettant de minimiser ses effets néfastes sur une application. Il existe 2 définitions pour le roaming. La première concerne un changement de réseau (par exemple le passage d'un réseaux IP à un autre ou un changement de réseau téléphonique si on part à l'étranger). La deuxième définit un changement de cellule à l'intérieur d'un même réseau, c'est cette deuxième définition que nous garderons pour la présentation de ce travail.

La première partie de ce manuscrit présente les réseaux sans fil de manière générale, et leur utilisation en réseaux cellulaires. Ensuite deux normes sont présentées, 802.11 car c'est le standard que nous avons choisi pour notre plateforme et GSM car c'est le réseau cellulaire le plus utilisé et dont l'efficacité n'est plus à démontrer. De plus il intègre une gestion très complète du changement de cellule. Ces fonctionnalités ainsi que celles du changement de cellule 802.11 font l'objet d'un chapitre.

La deuxième partie présente le contexte de l'étude. En commençant par une étude détaillée du problème du handover 802.11, au niveau du trafic engendré, du temps pris par ce processus et donc des effets que cela implique une application à contraintes temporelles. Cette partie se poursuit par la présentation de travaux proposant des solutions pour optimiser le changement de cellule dans 802.11 et la présentation de protocoles mettant en oeuvre une collaboration entre les stations de base pour une meilleure gestion du handover. Nous terminerons par la présentation du projet Waves qui occupe une part importante dans l'activité de l'équipe Réseaux et Protocoles. Nous y verrons la plateforme que nous avons définie ainsi que des premiers résultats concernant les performances d'un réseau sans fil pour notre application.

La troisième et dernière partie décrit différentes solutions proposées pour l'optimisation du handover en 802.11. Ces solutions peuvent avoir une influence sur le temps du processus

de changement de cellule ou sur le trafic qu'il engendre. Nous terminerons par les résultats obtenus en évaluant les performances de ces solutions, les effets néfastes qui persistent et des propositions pour l'intégration de ces solutions dans le projet final.

Première partie

État de l'art

Chapitre 1

Les réseaux sans fil

Sommaire

1.1 Le médium radio 10

1.2 Éléments de Transmission 13

1.2.1 Modulations 13

1.2.2 Méthodes de transmission 13

1.3 Notion de Portée 16

1.4 Partage du médium 18

1.4.1 Introduction 18

1.4.2 Les principales méthodes d'accès 18

1.5 Notion de cellule et de couverture cellulaire 23

1.6 Les réseaux cellulaires 26

1.6.1 GSM 27

1.6.2 GPRS 33

1.6.3 UMTS 38

1.6.4 La norme 802.11 42

1.1 Le médium radio

La mise en oeuvre d'un réseau suppose l'utilisation d'un médium de communication. Dans le cadre des réseaux locaux sans fil, deux sous ensembles du spectre électromagnétique sont utilisés : les infrarouges et les ondes radioélectriques.

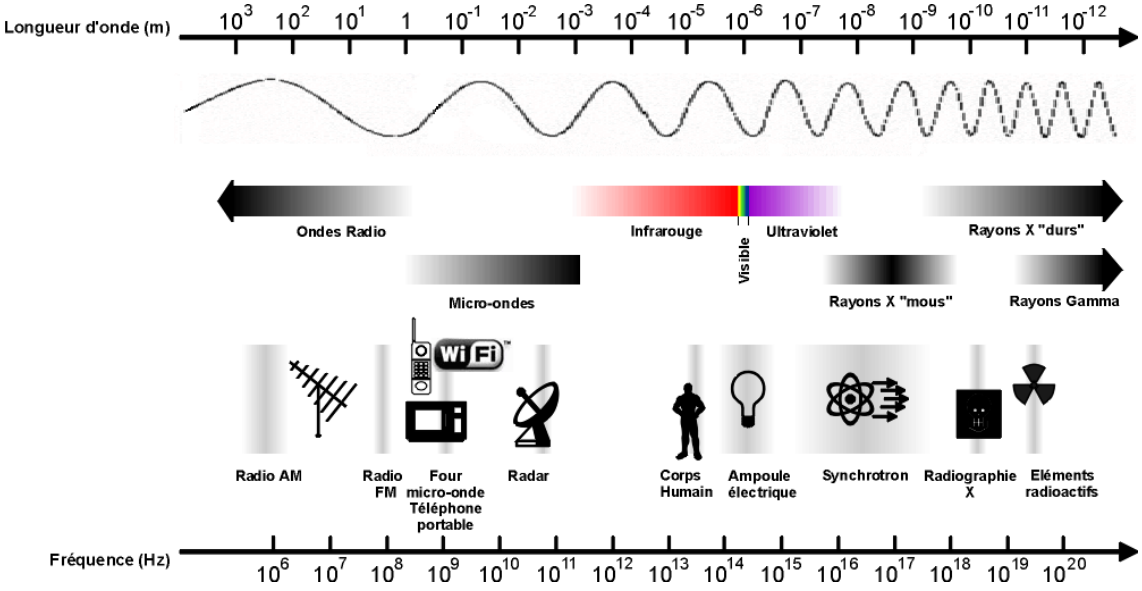


FIG. 1 – *Le spectre électromagnétique*

Dans notre étude, nous nous intéresserons uniquement aux ondes radioélectriques, leur fréquence est comprise entre 30 Khz et 300 Ghz. L'utilisation des ondes radio est très réglementée. En France c'est l'Autorité de Régulation des Communications Électroniques et des Postes (ARCEP nouveau nom depuis Mai 2005 de l'Autorité de Régularisation de Télécommunications(ART)) [3] qui est chargée de cette tâche. Les limitations imposées concernent aussi bien les bandes de fréquences, que les puissances d'émission des produits du marché. Certaines bandes de fréquences ne sont pas soumises à réglementation, elles sont utilisables sans avoir à demander de licence. Par exemple, les bandes ISM (Industriel, Scientifique et Médicale) parmi lesquelles les bandes 433,05 à 434,79 MHz, 868 à 870

MHz, 902 à 928 MHz, 2.4 à 2.5 GHz, 5,725 à 5,875 GHz. Ce sont ces bandes qui sont usuellement exploitées pour les matériels de réseaux sans fil commerciaux dont "Wifi" et les périphériques informatiques (claviers, souris...).

Les ondes électromagnétiques se propagent sur le médium, l'environnement (milieu, objets, personnes) a une influence sur les conditions de propagation. Plusieurs phénomènes peuvent être observés : la réflexion, la diffusion, la diffraction et l'absorption [29] [36] [45], ils sont résumés sur la figure 2. Ces mécanismes de propagation ont pour effet de "dupliquer" l'onde originale. Les ondes résultantes, quasiment identiques à l'original, vont emprunter des trajets différents pour atteindre le récepteur. Le récepteur va donc recevoir plusieurs composantes de la même onde. Ce phénomène est appelé trajets multiples. Ceci explique le fait qu'un onde puisse être reçue par le récepteur même si l'émetteur n'est pas en vue directe.

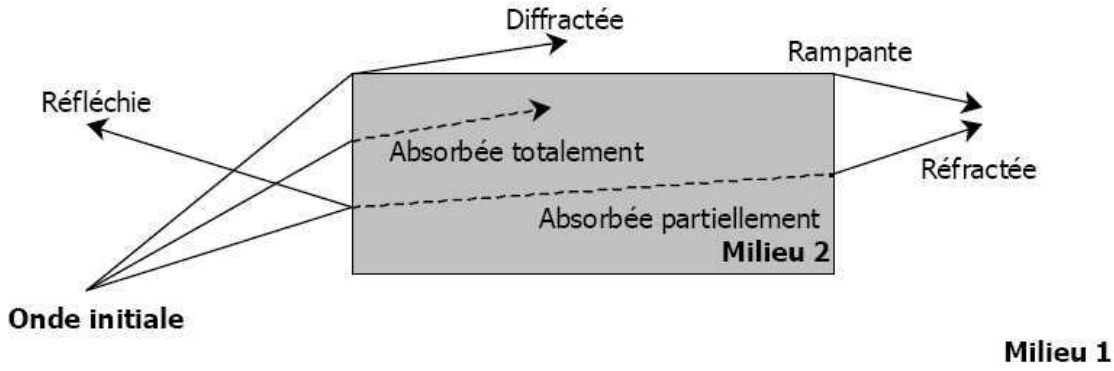


FIG. 2 – *Propagation des ondes électromagnétiques*

Ces phénomènes induisent plusieurs conséquences néfastes que nous allons voir brièvement.

La dispersion de puissance : La puissance du signal reçu varie en fonction des milieux traversés et de la distance entre l'émetteur et le récepteur. Donc, la plupart du temps, la puissance d'un signal provenant d'un émetteur lointain est inférieure à celle

d'un signal provenant d'un émetteur proche. De la même façon, quand une station émet des données, elle est aveuglée par son propre signal et ne perçoit pas l'information en provenance des autres stations. Ce problème est communément appelé *near-far effect*, ou effet d'aveuglement.

La dispersion du délai de propagation : L'onde emprunte plusieurs chemins de longueurs différentes avant d'atteindre le récepteur. Par conséquent, ce dernier reçoit plusieurs "copies", de l'information émise, espacées dans le temps. Ces copies forment un signal étalé à la réception. Ce phénomène est appelé *delay spread*. Ceci a des conséquences néfastes, en particulier quand le débit devient important. Le délai de propagation peut provoquer des recouvrements entre des symboles transmis successivement. Ce phénomène, schématisé sur la figure 3 est appelée interférences intersymboles. Ce problème peut être résolu en espaçant l'émission des symboles, par exemple en diminuant le débit de la liaison ou en réduisant volontairement la portée.

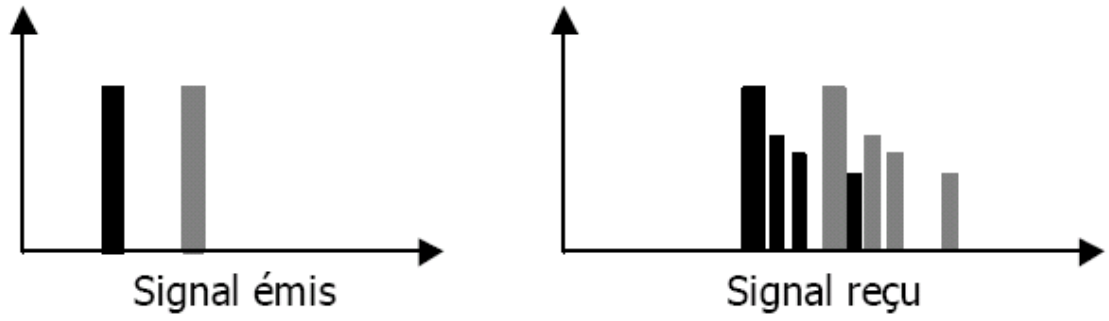


FIG. 3 – *Interférence intersymboles*

La distorsion de fréquence : Cet effet est également connu sous le nom d'effet Doppler. Il s'agit d'un décalage des fréquences de l'onde transmise dû au déplacement du mobile. Quand un mobile se déplace en cours de réception, la distance à parcourir par l'onde varie. Il peut également être observé avec un émetteur et un récepteur fixes, si

d'autres éléments sont en mouvement entre ces deux entités [40].

La distorsion d'amplitude : Les différentes composantes des ondes émises suivent des chemins différents pour atteindre le récepteur. A chaque instant, ce dernier capte la somme algébrique des différentes composantes de l'onde originale et perçoit donc une puissance variable du signal. L'addition algébrique de signaux en opposition de phase fait apparaître des creux très importants au niveau de la puissance reçue. Ce phénomène est appelé évanouissement (en anglais *fading*) de Rayleigh.

1.2 Éléments de Transmission

1.2.1 Modulations

Un signal est transmis sous la forme d'une onde. Ce signal est caractérisé par une amplitude, une fréquence et une phase. Des déformations, appelées modulations, lui sont appliquées afin de distinguer les différents éléments d'un message. Plusieurs types de modulations existent. On peut distinguer les modulations traditionnelles qui peuvent s'appliquer aux différentes caractéristiques du signal : modulation d'amplitude (AM), modulation de fréquence (FM), modulation de phase (PM), ou une combinaison de ces caractéristiques. Ces méthodes traditionnelles sont surtout exploitées pour le transport d'informations analogiques. Les modulations par étalement de spectre sont basées sur l'utilisation d'une bande passante plus large que celle nécessaire pour transmettre les mêmes informations au moyen d'une modulation traditionnelle. Ceci rend la transmission moins sensible aux défauts du médium radio.

1.2.2 Méthodes de transmission

Pour les transmissions radio dans les applications actuelles, plusieurs techniques sont exploitées. Parmi les plus utilisées, on en trouve deux basées sur l'étalement de spectre :

FHSS (Frequency Hopping Spread Spectrum), utilisé par Bluetooth par exemple, et DSSS (Direct Sequence Spread Spectrum) que l'on peut retrouver dans 802.11b. Elles sont couramment utilisées dans les applications utilisant les bandes ISM (Industrielles, Scientifiques et Médicales) qui sont des bandes de fréquences souvent sans contraintes de licences d'utilisation, les réseaux cellulaires (par exemple : GSM), les réseaux locaux sans fil (WLAN). Une autre technique, OFDM (Orthogonal Frequency Division Multiplexing), utilisant un spectre de fréquence de façon différente a été plus récemment exploitée. Elle est plus performante que les précédentes et est utilisée pour les extensions a et g de 802.11.

FHSS : Frequency Hopping Spread Spectrum

Son fonctionnement est basé sur l'étalement de spectre avec sauts de fréquence. La bande de fréquence allouée est divisée en plusieurs canaux plus étroits. Pour une transmission donnée, un sous ensemble de ces canaux est alloué. Au cours de cette transmission, les informations vont être envoyées successivement sur chacun des canaux de ce sous ensemble dans un ordre pseudo aléatoire. Ceci impose évidemment une synchronisation entre les entités communicantes. Il existe deux variantes pour le FHSS selon que le saut de fréquence intervient entre chaque trame ou à intervalle de temps réguliers.

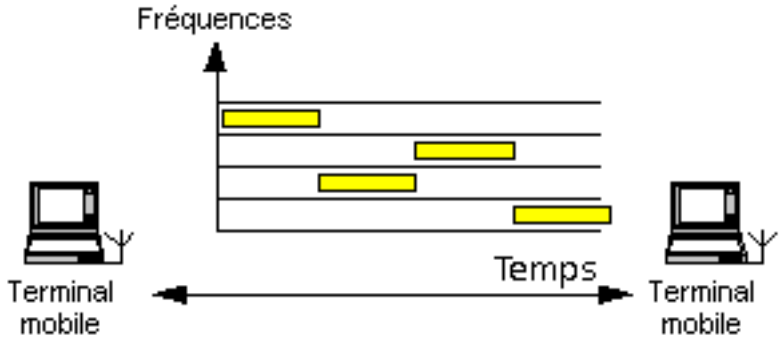


FIG. 4 – *Frequency Hopping Spread Spectrum [6]*

Cette technique a un inconvénient majeur. Le fait d'envoyer le signal sur une bande réduite oblige l'utilisation d'une puissance plus forte pour garder un taux d'erreur accep-

table. Les sauts de fréquences consomment également de l'énergie. Le FHSS est donc une technique défavorable si on est exigeant sur l'économie d'énergie.

DSSS : Direct Sequence Spread Spectrum

DSSS est également une technique à étalement de spectre à séquence directe. Le signal envoyé occupe l'intégralité de la bande passante allouée à la transmission. Par rapport au FHSS, le signal est envoyé sur tous les sous-canaux du canal courant. Cette redondance permet la diminution du taux d'erreur, donc de meilleures performances. Le DSSS est également moins sensible aux perturbations.

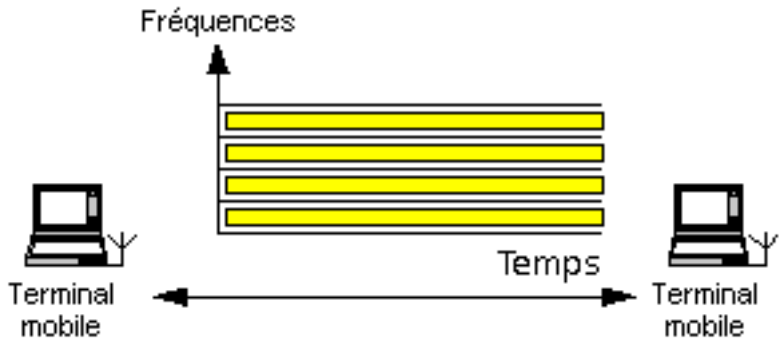


FIG. 5 – *Direct Sequence Spread Spectrum [6]*

OFDM : Orthogonal Frequency Division Multiplexing

OFDM signifie accès multiple à répartition dans le temps ou les fréquences. Cette technique date des années 1950 mais elle n'a commencé à être exploitée que dans les années 1980. Cette technique de transmission est basée sur l'émission simultanée sur n bandes de fréquence, de N porteuses sur chaque bande. Le signal est réparti sur les porteuses. Si l'une d'elles est atténuée, le signal passera quand même grâce à l'émission simultanée. Le débit est ajusté en fonction du nombre de porteuses. Au lieu d'envoyer les données à un débit de D symboles par secondes, on transmet sur chacune des N porteuses à D/N

symboles par secondes. L'émission à débit plus faible sur plusieurs porteuses permet la réduction des interférences dues aux trajets multiples que peut emprunter une onde radio.

1.3 Notion de Portée

Pour tout système de communication, le signal reçu est différent du signal émis. Ceci est dû aux différentes dégradations qui peuvent se produire lors d'une transmission. Les principales sources de dégradations les plus significatives sont l'affaiblissement en espace libre, le bruit, l'absorption atmosphérique, la propagation multitrajet et la réfraction [46].

Une transmission radio va donc s'effectuer sur une distance limitée. Pour les transmissions sans fil, l'affaiblissement est une fonction complexe qui dépend de l'environnement, même en espace libre la puissance du signal chute avec la distance. Le signal reçu est composé du signal émis altéré par des signaux aléatoires perturbateurs, que l'on appelle bruit. Ce signal reçu doit avoir assez de puissance pour être détecté et interprété par un récepteur.

Plusieurs notions sont utilisées pour juger la qualité d'une transmission. Tout d'abord le rapport signal sur bruit (noté S/B ou SNR pour *Signal to Noise Ratio* en anglais). Il s'exprime en décibels. On divise la valeur du signal par le bruit, qui est le signal non utile, composé de parasites provoqués par des perturbations externes ou les circuits électroniques.

$\mathrm{SNR} = 10 \log_{10} \frac{PuissanceSignal}{PuissanceBruit}$

Plus la valeur du S/B est élevée, plus le bruit est faible comparé au signal et meilleure est la qualité du signal. En règle générale, c'est l'augmentation de la distance entre l'émetteur et le récepteur qui va entraîner la chute du rapport signal sur bruit.

L'expression E_b/N_0 est le rapport de l'énergie du signal par bit à la densité du bruit par Hertz. Avec un débit R, $E_b = ST_b$ où S est la puissance du signal et T_b le temps nécessaire à l'envoi d'un bit. Le débit est alors $R = \frac{1}{T_b}$

$\frac{E_b}{N_0} = \frac{S/R}{N_0} = \frac{S}{kTR}$

Le taux d'erreur binaire (TEB) est une fonction de ce rapport E_b/N_0. Il est utilisé pour caractériser un canal de communication. Il représente le rapport entre le nombre de bits erronées et nombre de bits transmis. C'est un taux statistique : l'erreur affecte aléatoirement n bits consécutifs et non un bit tous les x bits. Des taux d'erreurs de 10^{-5} ou 10^{-4} sont considérés comme bons pour le sans fil. En filaire on peut avoir des valeurs de 10^{-6} à 10^{-14} pour la fibre optique, 10^{-3} est une valeur encore acceptable, au delà la transmission est dégradée.

Quand au niveau d'une station réceptrice, le SNR calculé est trop bas ou que le taux d'erreur devient important, on va considérer que la qualité de la liaison n'est plus acceptable et donc que la station n'est plus à portée radio de l'émetteur. On va alors considérer qu'il y a rupture de la communication, on peut alors éventuellement essayer de faire transiter les informations d'une autre manière, par exemple en utilisant une ou plusieurs stations relais situées entre les deux stations communicantes. La portée peut être augmentée en augmentant la puissance de l'émetteur ou en diminuant le bruit au niveau du récepteur.

Le type d'antenne (dipôle, parabole...) et leur gain [46] est également impliqué dans la portée entre un émetteur et un récepteur.

Dans le cas des réseaux cellulaires que nous allons voir à la fin de ce chapitre, le fait de ne plus être à portée d'une station de base, selon un des paramètres précédents, va provoquer le changement de cellule (handover).

1.4 Partage du médium

1.4.1 Introduction

Au cours des années 1980, les réseaux locaux se sont fortement développés. Les communications entre les entités d'un réseau étaient jusqu'alors réalisées par des connexions point à point, complexes à mettre en oeuvre. L'idée d'utiliser une ressource commune comme médium de communication vient de Bob Metcalf avec le protocole Ethernet, normalisé en 1983 par l'IEEE sous le nom de 802.3 [16], qui propose l'utilisation d'un même médium filaire pour les échanges de données. L'exploitation d'un médium commun pose différents problèmes liés à la bande passante qui pourra être allouée et à l'équité entre les stations pour accéder à ce médium. En filaire, la gestion est plus simple du fait que le médium est maitrisé (câble, fibre optique). Les spécificités du médium radio entraînent plus de contraintes : deux stations à portée radio l'une de l'autre propagent des ondes radio dans une zone géographique finie. Pour qu'un échange se déroule correctement entre ces deux stations, une seule transmission à la même fréquence doit être réalisée au même instant dans l'ensemble de deux zones. Plusieurs méthodes ont été proposées pour que le médium puissent être partagé entre différentes stations, elles sont principalement basées sur le partage des bandes de fréquences disponibles et le temps pendant lequel une station qui a accédé au médium a le droit d'émettre.

1.4.2 Les principales méthodes d'accès

Nous allons détailler dans les paragraphes suivants quelques méthodes d'accès utilisées à l'heure actuelle dans les réseaux sans fil. Les méthodes présentées sont celles qui sont exploitées par les réseaux présentés à la fin de ce chapitre.

FDMA

FDMA (Frequency Division Multiple Access, en français AMRF pour Accès Multiple à Répartition en Fréquence) est une méthode d'accès où plusieurs stations utilisant le même canal se partagent la bande passante. Il s'agit de multiplexage en fréquence. Le canal est divisé en plusieurs sous-canaux plus étroits. Quand un utilisateur souhaite communiquer, un de ces sous-canaux lui est alloué, il peut alors envoyer et recevoir des données sur la fréquence donnée et aucun autre utilisateur ne pourra émettre sur ce canal pendant la durée de la communication.

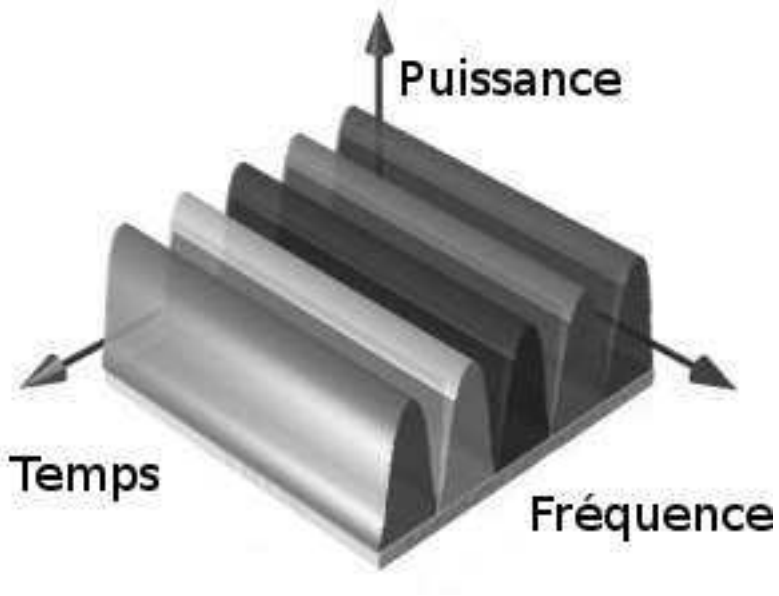


FIG. 6 – *Frequency Division Multiple Access*

TDMA

TDMA (Time Division Multiple Access, en français AMRT pour Accès Multiple à Répartition dans le Temps) est une méthode où tous les utilisateurs émettent sur le même canal chacun à leur tour. Cela s'appelle aussi du multiplexage temporel. Le temps est divisé en intervalles de temps (appelés slots). Quand une station a besoin d'émettre un

slot lui est alloué, pendant cette période elle est la seule à avoir le droit d'émettre. Sur la figure 7 deux stations ont chacune un message à envoyer (GO et HI), un slot est alloué à une première station, ce qui lui permet d'envoyer une partie de son message (le G dans notre exemple) sur le canal commun, ensuite un slot est alloué à la deuxième station qui va envoyer le H etc.

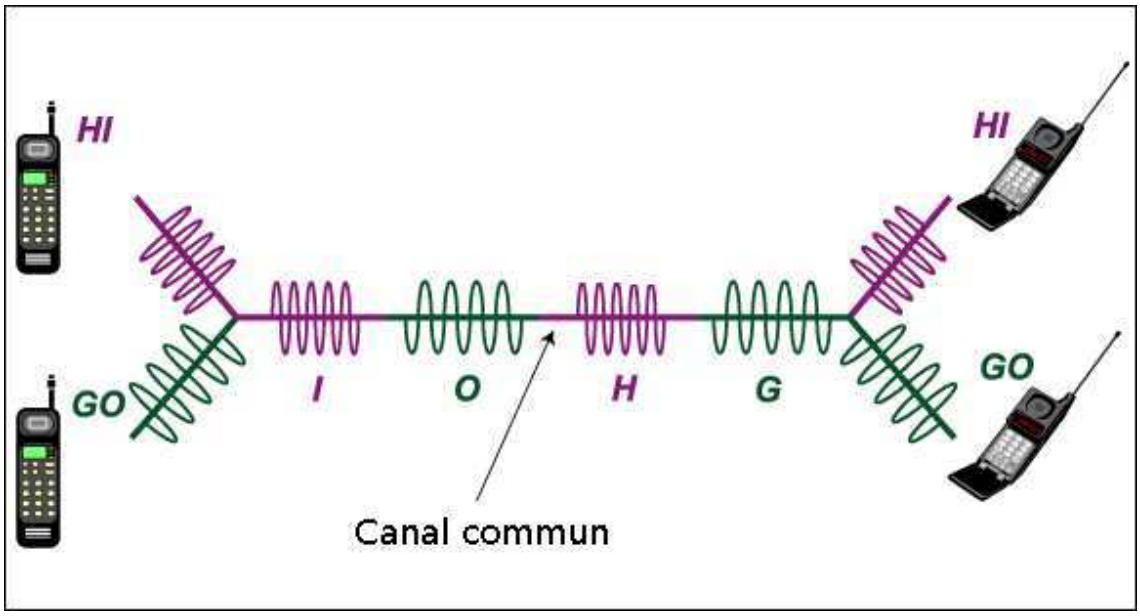


FIG. 7 – *Time Division Multiple Access*

Pour réduire le nombre d'utilisateurs sur un canal, le TDMA est souvent couplé à FDMA, comme le montre la figure 8. C'est notamment le cas dans les réseaux GSM.

CSMA

La méthode d'accès CSMA (Carrier Sense Multiple Access) est une méthode d'accès aléatoire pour laquelle chaque station va écouter le médium avant toute transmission de données, ce qui permet de s'assurer qu'aucune transmission n'est en cours. Le but de cette technique est d'éviter que deux stations tentent d'accéder au médium simultanément.

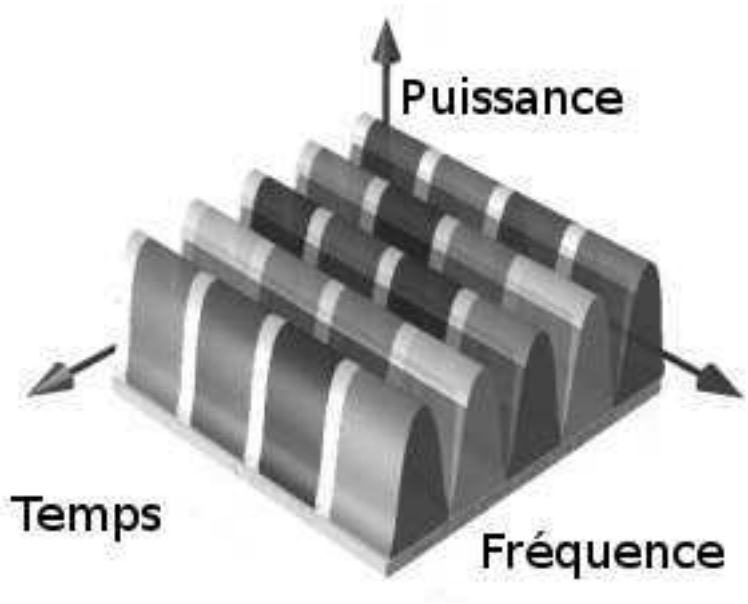


FIG. 8 – *TDMA et FDMA combinés*

La méthode n'est pas infaillible, il peut arriver que deux stations émettent une trame en même temps. Ceci est possible dans le cas où ces deux stations écoute le médium au même instant, détectent qu'il est libre puis émettent leur trame. On parle alors de collision. L'information contenue dans ces trames est alors perdue. Plusieurs variantes de CSMA sont disponibles, nous allons décrire la variante CD adaptée au réseaux filaires et CA qu'on retrouve dans les réseaux sans fil.

CSMA/CD : Dans un réseau filaire, une station qui envoie des données est capable de détecter les collisions. La communication dans ce type de réseau (Ethernet par exemple) se fait à l'aide de la méthode CSMA/CD (Carrier Sense Multiple Access with Collision Detection pour écoute de porteuse avec accès multiple et détection de collision). Avec cette méthode, toutes les machine sont autorisées à émettre sur la ligne libre à n'importe quel moment et sans notion de priorité entre les machines. Cette communication se fait de façon simple :

- Chaque machine vérifie qu'il n'y a aucune communication sur la ligne avant d'émettre
- Si deux machines émettent simultanément, alors il y a collision (c'est-à-dire que plusieurs trames de données se trouvent sur la ligne au même moment). La collision est détectée car chaque station écoute le médium en même temps qu'elle émet, si les informations lues sont différentes de celles émises alors la station en déduit qu'elle n'est pas seule à émettre et qu'il y a collision.
- Les deux machines interrompent leur communication et attendent un délai aléatoire, puis la première ayant passé ce délai peut alors retenter d'émettre

Plusieurs contraintes sont prises en compte : les paquets de données doivent avoir une taille maximale et il doit y avoir un temps d'attente entre deux transmissions.

Le temps d'attente varie selon la fréquence des collisions : après la première collision la machine attend une unité de temps. Après la seconde collision, la machine attend deux unités de temps, après la troisième collision la machine attend quatre unités de temps... On ajoute également à ces temps un délai supplémentaire aléatoire.

CSMA/CA La méthode d'accès CSMA/CD n'est pas applicable dans un environnement sans fil. La détection de collision n'est pas possible car la transmission n'est pas full-duplex, c'est à dire qu'une station ne peut pas émettre et écouter le médium simultanément. De plus deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée. Ce problème, appelé terminal caché, est décrit à la fin de ce chapitre dans la partie présentation de la norme 802.11. Ainsi la norme 802.11 propose un protocole similaire appelé CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance pour écoute de porteuse avec accès multiple et évitement de collision).

Le protocole CSMA/CA utilise un mécanisme d'esquive de collision basé sur un principe d'accusé de réceptions entre l'émetteur et le récepteur.

La station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission

est différée. Dans le cas contraire, si le média est libre pendant un temps donné, alors la station peut émettre. A réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK). Toutes les stations avoisinantes patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.

La méthode d'accès peut être complétée par un mécanisme de réservation du médium pour éviter les collisions entre deux stations n'étant pas à portée l'une de l'autre et souhaitant toutes deux communiquer avec une troisième station. Nous détaillerons ce point dans la partie suivante avec la présentation du mécanisme RTS/CTS, qui est une option de la méthode d'accès DCF de 802.11.

1.5 Notion de cellule et de couverture cellulaire

Une station munie d'une carte réseau sans fil va pouvoir émettre sur une certaine distance autour d'elle. Cette zone dans laquelle d'autres stations sont susceptibles de recevoir les informations venant de cette station est appelée zone de couverture (voir figure 9.

En mode infrastructure, toutes les communications passent par une station appelée point d'accès ou station de base, Dans cette configuration c'est la zone de couverture de ce point d'accès qui doit être prise en compte, on parle alors de cellule. Si toutes les stations communicantes sont à portée d'un point d'accès, alors une seule cellule est nécessaire. Par contre si la zone de communication est étendue, il faut prévoir plusieurs point d'accès de manière à ce que toutes les stations appartiennent à une cellule. Les point d'accès devront être reliés de manière à ce que les communications soient possibles entre des stations de cellules différentes comme on peut le voir sur la figure 10.

Dans la figure 10, les deux stations peuvent bien communiquer entre elles via leurs points d'accès respectifs et l'infrastructure. Par contre, dans cette configuration, la mo-

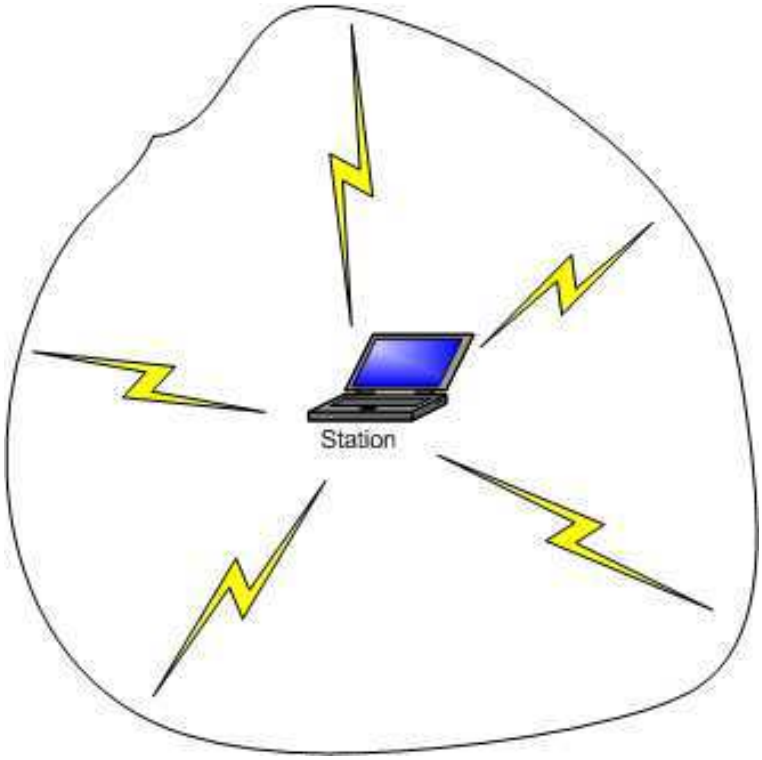


FIG. 9 – *Zone de couverture d'une station sans fil*

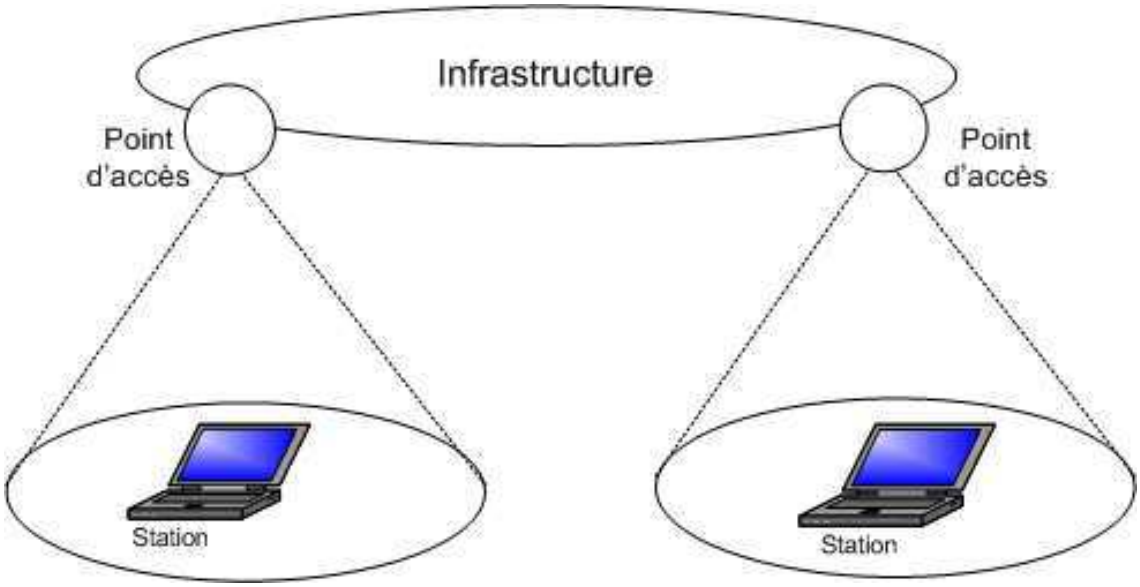


FIG. 10 – *Couverture cellulaire*

bilité des stations entre les cellules n'est pas possible sans perte de communication (la situation est similaire à un passage sous un tunnel lors d'une communication téléphonique). Pour que cela devienne possible, il est nécessaire que l'intersection de la zone de couverture des deux points d'accès ne soit pas nulle comme dans la figure 11 [49]. Cette zone commune aux deux cellules est appelée zone de recouvrement, c'est dans les zones de recouvrement que se négocient et s'effectuent les changements de cellule (handover). Pour que ce processus se déroule sans problème, il faut que la zone de recouvrement soit assez importante. Il est recommandé que sa largeur fasse environ 15% du diamètre de la cellule. Le but est de permettre un changement de cellule transparent pour l'utilisateur (seamless handover).

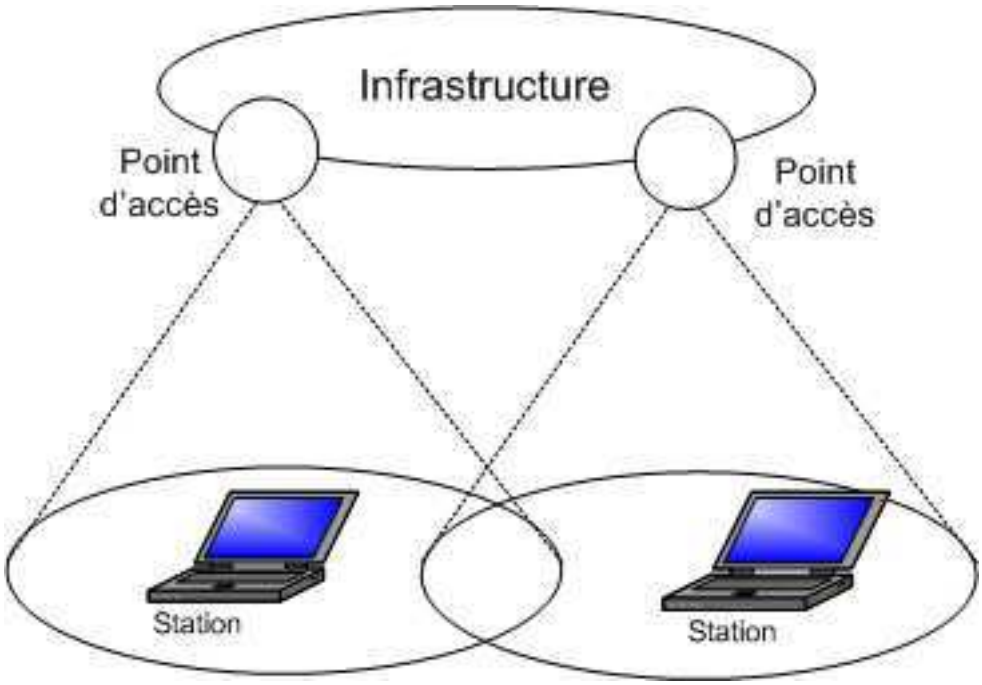


FIG. 11 – *Couverture cellulaire avec zone de recouvrement*

Pour éviter les interférences, deux cellules adjacentes ne doivent pas utiliser le même canal, c'est à dire fonctionner à des fréquences suffisamment éloignées. Pour obtenir une couverture cellulaire, il est nécessaire d'avoir un minimum de trois canaux de communications. Prenons par exemple l'utilisation du DSSS dans la bande ISM 2.4 Ghz comme c'est

la cas de la norme 802.11b. On dispose de 14 canaux espacés de 5 Mhz, dont le premier est à 2.412 Ghz, le deuxième à 2.417 Ghz etc, comme on peut le voir sur la figure 12. La technique par étalement de spectre fait que le signal envoyé sur le canal 1 va être étalé sur 22Mhz autour de la fréquence 2.412 Ghz, c'est à dire de 2.401 Ghz à 2.423 Ghz. On constate que les canaux 2 et 3 sont compris dans cet intervalle, il n'est donc pas possible d'utiliser les canaux 1 et 3 dans un même environnement. Les canaux 4 et 5 débordent également sur le canal 3, ils ne sont pas non plus utilisables avec le canal 1. Le premier canal possible pour être utilisé dans une cellule adjacente à une cellule fonctionnant sur la canal 1 est donc le canal 6. Avec le même raisonnement on voit que le canal 11 peut être utilisé.

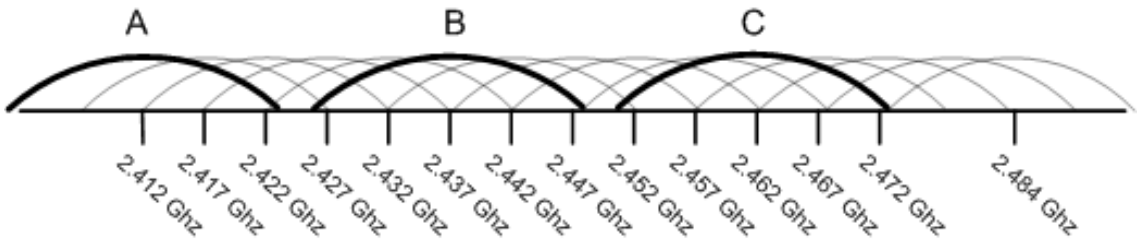


FIG. 12 – *Les canaux de la bande ISM 2.4 Ghz*

On dispose donc de 3 canaux indépendants, notés A, B et C sur les figures 12 et 13. La figure 13 représente une couverture cellulaire fonctionnelle avec 3 canaux qui sont représentés par les différents niveaux de gris.

1.6 Les réseaux cellulaires

Les réseaux cellulaires utilisent les ondes hertziennes pour transmettre les informations. Ces réseaux ont pour but de permettre la communication sur un territoire étendu. Il est découpé en petites zones indépendantes, les cellules. Comme vu plus haut dans deux cellules adjacentes, les stations ne pourront pas utiliser les mêmes fréquences pour communiquer. Au centre de chaque cellule se trouve une station de base (également appe-

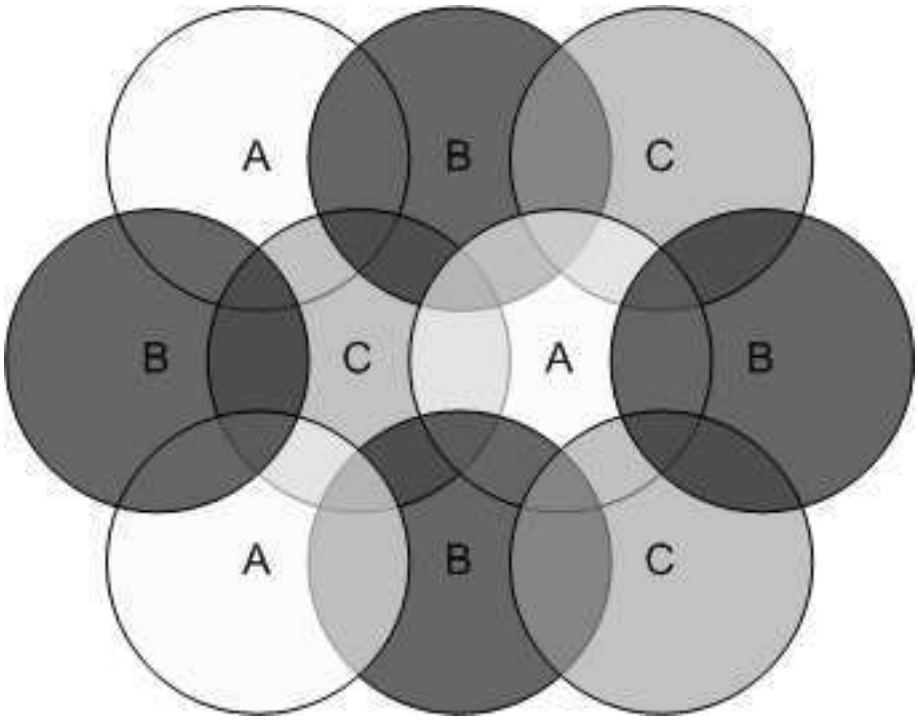


FIG. 13 – *Couverture cellulaire avec 3 canaux*

lée point d'accès) par laquelle passent toutes les communications entre les stations de la cellule. Les stations de bases d'un même réseau cellulaire sont reliées entre elles par une infrastructure. Cette dernière est utilisée pour la transmission de données entre stations se trouvant dans des cellules différentes. Voyons maintenant plusieurs exemples de réseaux cellulaires GSM et son évolution GPRS, UMTS et 802.11.

1.6.1 GSM

GSM [22] est la première norme de téléphonie cellulaire qui soit pleinement numérique. C'est la référence mondiale pour les systèmes radio mobiles.

Le réseau GSM offre à ses abonnés des services qui permettent la communication de stations mobiles de bout en bout à travers le réseau. La téléphonie est le plus important des services offerts. Ce réseau permet la communication entre deux postes mobiles ou entre un poste mobile et un poste fixe. Les autres services initialement proposés sont la

transmission de données et la transmission de messages alphanumériques courts.

Le GSM présente des services supports sans restriction sur le type des données utilisées par l'utilisateur. Il transporte les informations sans modification de bout en bout en mode circuit dans le réseau GSM, ce qui garantie la chronologie des informations échangées. Dans le réseau GSM, les données de l'utilisateur et la signalisation du réseau sont transportées dans des canaux de communication différents.

GSM en quelques dates

- 1979 : La Conférence Administrative Mondiale des Radio-communications (CAMR) décide d'affecter la bande de fréquence des 900 MHZ aux services mobiles terrestres et maritimes.
- 1982 : Apparition en Europe des premiers services commerciaux nationaux de radiotéléphonie cellulaire analogique. La Conférence Européenne des Postes et Télécommunications (CEPT) réserve deux sous-bandes de 25 MHz chacune : 890-915 MHz et 935-960 MHz. La CEPT crée un groupe de travail baptisé "Groupe Spécial Mobiles" qui a pour rôle d'élaborer et de formuler les spécifications nécessaires à l'établissement de ce futur réseau.
- 1985 : Le programme GSM reçoit l'appui de la Commission des Communautés européennes, décidée à imposer la future norme unique aux états membres.
- 1986 : Choix d'une technologie numérique plutôt qu'analogique. Le Groupe Spécial Mobiles doit donc élaborer un système numérique qui doit être aussi performant qu'un système analogique. Les premiers prototypes sont conçus et testés à la fin de cette année, à la fois en laboratoire et sur 1e terrain.
- 1987 : Treize pays européens s'accordent sur les options de la future norme. L'option numérique est définitivement adoptée. En matière de transmission radio, la solution adopte le principe d'un Accès Multiple à Répartition dans le Temps (AMRT, en anglais TDMA). Le GSM retient également l'idée des "sauts de fréquence" : émetteur

et récepteur changent de fréquence à intervalles définis au début de la communication.

- 1988 : Ratification d'une Charte européenne du GSM (Memorandam of Understanding ou MoU) par 17 organisations européennes de télécommunications. Les signataires s'engagent à introduire un système cellulaire numérique respectant les spécifications du GSM dans la bande des 900 MHz.
- 1991 : Le 1er juillet a lieu en France la première communication entre un mobile GSM et le réseau téléphonique fixe. Mais aucun opérateur européen n'est encore en mesure de lancer un service GSM commercial grandeur nature., en phase commerciale.
- 1992 : Le sigle GSM est modifié et devient Global System for Mobile communications.

Architecture du réseau GSM

Le réseau GSM est composé des 3 éléments suivants que nous allons ensuite décrire de manière plus détaillée :

- Le sous-système radio BSS (Base Station Sub-system) qui assure les transmissions radioélectriques et gère la ressource radio.
- Le sous-système d'acheminement, appelé aussi réseau fixe, NSS (Network Sub-System) qui réalise les fonctions d'établissements des appels et de la mobilité.
- Le sous-système d'exploitation et de maintenance OSS (Operation Sub-System) qui permet à l'exploitant d'administrer son réseau.

Cette architecture peut être représentée par la figure 14.

Sous-système radio (BSS) : Il est constitué des éléments radio du réseau.

Les stations mobiles (MS pour Mobile Stations), sont les équipements de l'abonné au réseau (comme par exemple le téléphone muni d'une carte SIM) et permettant l'accès aux

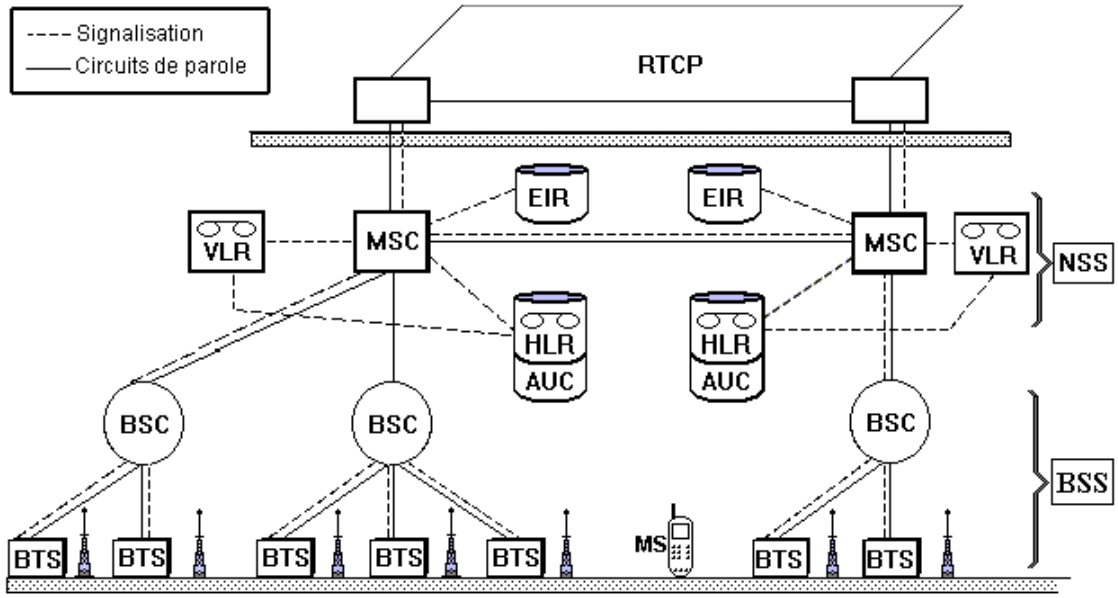


FIG. 14 – *Les entités du réseau GSM et son architecture [5]*

services fournis par le réseau. Chaque mobile a un identifiant unique. Ces station mobiles ont plusieurs fonctions, parmi lesquelles la mesure des signaux émis par les stations de base des cellules environnantes, dont les résultat permettent de faire les choix les plus judicieux en cas de besoin de changement de cellule. Nous appellerons également "terminal" une station de ce type.

Les stations de bases (BTS pour Base Transceiver Station) assurent le lien entre l'infrastructure du réseau et les MS. Chacune d'elle définit une zone de couverture (cellule). Elle fournit un point d'entrée au réseau téléphonique pour tous les abonnés présents dans sa cellule, ce qui permet de recevoir ou transmettre des appels. Une station de base gère simultanément huit communications grâce au multiplexage AMRT utilisé.

Les contrôleurs de stations de bases (BSC pour Base Station Controller) gèrent les BTS et assurent la fonction de concentration du trafic. Un BSC gère une ou plusieurs stations et remplit différentes missions pour les fonctions de communication et d'exploitation. Pour le trafic venant des stations de base, c'est un concentrateur ; pour le trafic issu de

l'infrastructure, c'est un aiguilleur vers la station du destinataire.

Sous-système fixe (NSS) : C'est l'infrastructure fixe du réseau. Il regroupe toutes les fonctions de routage et de communication.

Il est constitué des éléments suivants :

Le centre de communication du service mobile (MSC pour Mobile Switching Centre) assure le fonctionnement entre le système cellulaire et le réseau RTC. Il prend en compte les spécificités introduites par la mobilité, le transfert intercellulaire, la gestion des abonnés visiteurs. Le commutateur est un noeud important du réseau, il donne accès vers les bases de données du réseau et vers le centre d'authentification qui vérifie les droits des abonnés.

L'enregistreur de localisation des visiteurs (VLR pour Visitor Location Register) mémorise les données des abonnés présents dans la zone géographique considérée. C'est une base de données associée à un commutateur MSC. Sa mission est d'enregistrer des informations dynamiques relatives aux abonnés de passage dans le réseau. Cette gestion est importante car on doit connaître dans quelle cellule se trouve un abonné pour l'acheminement d'appel. La spécificité des abonnés GSM étant la mobilité, il faut en permanence localiser tous les abonnés présents dans le réseau et suivre leurs déplacements. A chaque changement de cellule d'un abonné, le réseau doit mettre à jour le VLR du réseau visité et le HLR de l'abonné, d'où un dialogue permanent entre les bases de données du réseau.

L'enregistreur de localisation nominal (HLR pour Home location register) est une base de données contenant les informations relatives aux abonnés du réseau. Dans cette base de données, un enregistrement décrit chacun des abonnements avec le détail des options souscrites et des services supplémentaires accessibles à l'abonné. A ces informations statiques, sont associées d'autres, dynamiques, comme la dernière localisation connue de l'abonné, l'état de son terminal (en service, en communication, en veille, hors service, etc). Un abonné est reconnu par les informations contenues dans sa carte d'abonnement (carte SIM). Les informations dynamiques relatives à l'état et à la localisation de l'abonné sont

particulièrement utiles lorsque le réseau achemine un appel vers l'abonné, car il commence par interroger le HLR avant toute autre action. Le HLR contient aussi la clé de l'abonné qui permet au réseau de l'identifier.

Le centre d'authentification (AUC pour Authentification Center) génère et stocke les paramètres d'authentification pour l'identification de l'abonné. C'est une base de données qui stocke des informations confidentielles. Il contrôle les droits d'usages possédés par chaque abonné sur les services du réseau. L'enregistreur des identités des équipements EIR contient les identités des terminaux. Le centre d'exploitation et de maintenance (OMC pour Operation and Maintenance Center) est l'entité de gestion et d'exploitation du réseau. Elle regroupe la gestion administrative des abonnés et la gestion technique des équipements.

Quelques caractéristiques techniques

Le GSM utilise deux techniques pour l'accès au médium, la première à multiplexage temporel (TDMA) et la deuxième à multiplexage fréquentiel (FDMA). L'utilisation de FDMA divise, en 124 canaux de 200 KHz chacun, les deux plages de fréquences utilisées pour le GSM 900Mhz, 890-915 Mhz pour les communications allant des stations mobiles aux stations de bases et 935-960 Mhz pour les communications allant des stations de bases aux stations mobiles. Le GSM 1800 utilise la bande 1710-1785 MHz pour l'envoi des données et la bande 1805-1880 MHz pour la réception des informations. Le multiplexage temporel partage une voie de transmission en 8 communications différentes. Ceci définit les canaux physiques de communication.

Sur ces canaux physiques, le GSM définit deux types de canaux logiques : les canaux de trafic, qui vont servir au transports des données (voix, SMS) et les canaux de signalisation, qui servent à la gestion des transmissions (diffusions d'informations par une station de base, appel d'une station mobiles, etc).

La puissance pour une station de base en France est comprise entre 2 et 8 Watts ,

celle d'une station mobile ne dépasse pas 2 Watts. Le rayon d'une cellule peut varier de 200 mètres à une trentaine de kilomètres. La topologie du réseau dépend de la densité de population dans un zone géographique. La puissance d'émission entre une station de base et un mobile est réglée en permanence (toutes les 60ms) en fonction de la qualité du signal, de manière à limiter les interférences, optimiser le rendement du médium radio et pour des raisons d'économie d'énergie (en particulier pour les stations mobiles).

1.6.2 GPRS

Présentation

Le GPRS ne constitue pas à lui tout seul un réseau mobile à part entière, mais une couche supplémentaire rajoutée à un réseau GSM existant. Il peut donc être installé sans aucune licence supplémentaire. Ceci signifie que tous les opérateurs qui disposent d'une licence GSM peuvent faire évoluer leur réseau vers le GPRS. Il utilise les bandes de fréquences attribuées au GSM. C'est à dire une bande dans les 900 MHz, une autre dans les 1800 MHz et enfin une troisième pour les USA, dans les 1900 MHz. Les opérateurs GSM actuels ont de fait un quasi monopole sur le GPRS, ce qui n'est pas le cas pour l'UMTS.

Le GPRS, appelé aussi GSM 2+, repose sur la transmission en mode paquet. Ce principe permet d'affecter à d'autres communications les "temps morts" d'une première communication (attente d'une réponse à une requête Internet par exemple).

Conçu pour réutiliser au maximum les infrastructures GSM existantes, le déploiement du GPRS nécessite la mise en place d'une infrastructure réseau basée sur la commutation de paquets et l'introduction de passerelles pour s'adosser aux réseaux GSM existants.

Cette technologie, capable de fournir des débits par utilisateur allant jusqu'à 115 kb/s (contre 9,6 kb/S pour le GSM), offre des fonctionnalités intéressantes :

- plusieurs canaux peuvent être alloués à un utilisateur,
- ces mêmes utilisateurs peuvent partager un même canal,

– le débit est indépendant des liens montant et descendant.

En France, les premiers services basés sur GPRS ont été mis en place fin juin 2000.

Services, possibilités et limitations

Trois domaines d'application : Alors que le GSM version WAP s'arrête à la consultation des pages Internet, le GPRS permet d'élargir l'offre de services. Outre l'accès à Internet (ou Intranet), à partir des mobiles traditionnels, il permet un meilleur accès aux e-mails comportant des fichiers joints. Le mobile, dans ce cas, est considéré comme un modem, et doit être associé à un ordinateur portable ou un assistant personnel.

Le troisième domaine concerne les applications professionnelles de transfert de données et de sécurité. La connexion ouverte en permanence du GPRS et le mode de taxation offrent à ceux qui font de la télémaintenance, de la télésurveillance et de la téléalarme, des opportunités intéressantes. On trouvera donc la norme GPRS dans les horodateurs, dans les ascenseurs (télésurveillance), dans les distributeurs de boissons ou de billet (vente, télésurveillance, gestion des stocks, réactualisation des prix), pour surveiller les sites industriels ainsi que les locaux professionnels et privés.

Débit : Avec le GPRS, on dispose d'un débit compris entre 40 et 115 kbit/s. Tout dépend du nombre de canaux virtuels ou "time slots" utilisés, et du schéma de codage. Ce dernier agit sur la compression des données comme un multiplicateur de débit. En mode multislots 3+1 (trois slots pour la transmission dans le sens réseau vers portable, et un slot pour le sens portable vers réseau), on atteint un débit de 40 kbit/s. En multislots (8+1), on atteint en pratique 115 kbit/s (en théorie 175 kbit/s).

L'accès immédiat et fiable : Le GPRS offre un accès immédiat. Le mode de fonctionnement du GPRS et son mode de facturation au volume de données transmises, permet de laisser le canal de transmission ouvert en permanence. Ainsi, pour télécharger un e-mail par GPRS on économise, par rapport à une connexion par GSM, lors de la première

connexion, le temps d'initialisation du modem, soit 30 secondes environ. Sur les autres e-mails, l'avantage est encore plus flagrant, les téléchargements se font immédiatement, sans numérotation préalable alors qu'en GSM il faut recommencer la procédure de numérotation pour chaque consultation.

Trois types de terminaux : Trois types de terminaux ont été définis pour répondre aux besoins du GPRS : le modèle de base est prévu pour la voix et les données en mode non simultané. Le modèle professionnel ou industriel est destiné aux données exclusivement (le terminal est utilisé comme un modem). Enfin le haut de gamme est compatible voix/données simultanément.

Fonctionnement et caractéristiques techniques

Mode connecté ou accès virtuel : Le premier avantage du GPRS est de permettre une meilleure utilisation des ressources radio et techniques. Alors que le GSM actuel fonctionne en mode "connecté", appelé également mode "circuit", le GPRS utilise pour sa part le mode de connexion virtuel. En mode "virtuel", les ressources sont partagées. Le canal de transmission n'est jamais affecté à un utilisateur unique, mais partagé entre un certain nombre d'utilisateurs. Chaque utilisateur en dispose lorsqu'il en a besoin et uniquement dans ce cas. Le reste du temps elles sont disponibles. Le mode "connecté" quant à lui correspond au fonctionnement d'une ligne GSM ou encore d'une ligne téléphonique standard. Il consiste à établir un lien physique entre deux points ou deux correspondants. Une fois le numéro d'appel composé, un circuit est affecté en permanence à la communication, sans aucun partage avec les autres clients. Ce mode de fonctionnement qui ne tient pas compte des périodes de silence, lorsque aucune donnée n'est transmise, n'optimise pas au mieux les ressources radio.

Le GPRS met en évidence le rôle plus important du gestionnaire de réseau. Dans une infrastructure GSM le rôle du gestionnaire se résume à affecter des ressources physiques

au début de chaque communication. Avec le GPRS, son rôle est plus important. Il consiste à allouer en temps réel des ressources physiques (mémoires et circuits électroniques), à gérer les ressources radio, et à les affecter en fonction de la demande.

Le GPRS s'installe sur le réseau GSM existant : L'implantation du GPRS peut être effectuée sur un réseau GSM existant. Les stations de base ne subissent aucune modification si ce n'est l'adjonction d'un logiciel spécifique. Plus en amont, le contrôleur de stations de base doit être doublé par un contrôleur de paquets (PCU pour Packets Controler Unit). Vient ensuite, la chaîne destinée aux données par paquets, constituée du commutateur (SGSN) ou Switch spécifique GPRS, équivalent du Mobile Switch Controler (MSC), contrôleur qui a pour fonction de vérifier l'enregistrement des abonnés, de les authentifier et d'autoriser les communications, et du module d'accès (GGSN) au monde IP (Internet ou Intranet). Le GGSN et le SGSN sont expliqués dans la partie suivante.

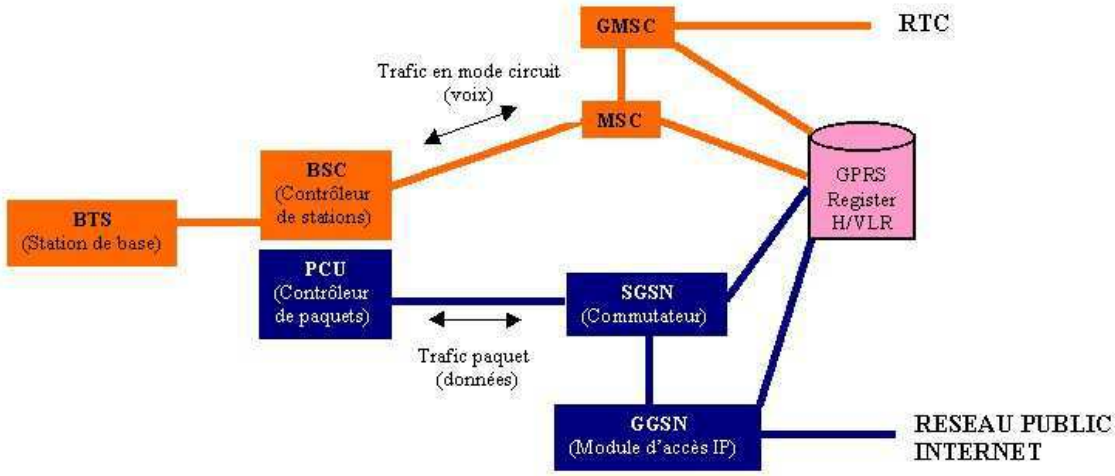


FIG. 15 – *Structure d'un réseau GPRS [28]*

Structure du réseau

Les composantes du réseau GPRS : La figure 16 Voici l'architecture des piles logicielles dans chacun des éléments d'un réseau GPRS.

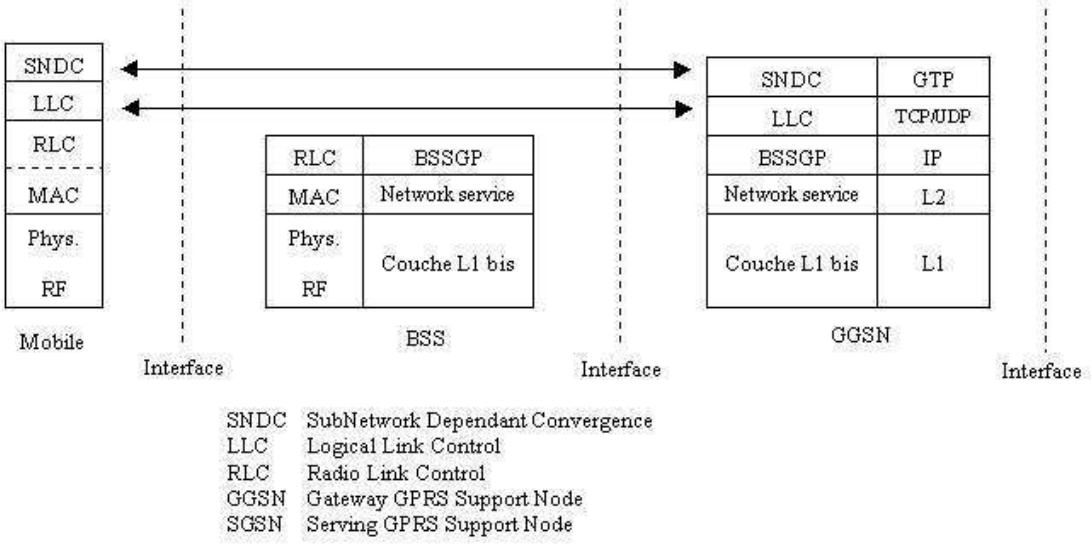


FIG. 16 – *Les piles logicielles d'un système GPRS [28]*

Dans le terminal mobile, nous trouvons de bas en haut les couches suivantes :

- La couche physique, qui se décompose en deux sous-couches fonctionnelles ;
  - La sous-couche RF, qui gère les fonctions radio du terminal. Elle émet les informations reçues de la couche physique. Elle décode les informations reçues de la station de base et les transfère pour interprétation vers la couche physique ;
  - La couche physique produit les trames, qui seront émises par la couche radio ; pour les trames reçues du réseau, elle détecte et corrige les erreurs de transmission ;
- La couche MAC (ou RLC pour Radio Link Control) pilote la liaison radio entre le terminal et la station de base, c'est-à-dire les mécanismes de retransmission en cas d'erreur, la fonction de contrôle d'accès aux ressources radio quand plusieurs terminaux sont en concurrence. Le RLC peut demander la retransmission d'un bloc de données ;
- La couche supérieure SNDC (SubNetwork Dependant Convergence) gère la mobilité, le cryptage et la compression de données.

GGSN : Gateway GPRS Support Node ou Routeur IP s'interfaçant avec les autres

réseaux. Le GGSN est la fonctionnalité d'interconnexion dans le centre de communication (MSC), qui permet de communiquer avec les autres réseaux de données par paquets extérieurs au réseau GSM. Le GGSN masque au réseau de données les spécificités du GPRS. Il doit supporter le protocole utilisé sur le réseau de données avec lequel il est interconnecté.

SGSN : Serving GPRS Support Node ou Routeur IP gérant les terminaux pour une zone. Le SGSN (Serving GPRS Support Node) est la fonctionnalité du service dans le centre de commutation (MSC), qui permet de gérer les services offerts à l'utilisateur. Le SGSN est l'interface logique entre l'abonné GSM et un réseau de données externe. Ses missions principales sont, d'une part la gestion des abonnés mobiles actifs (mise à jour permanente des références d'un abonné et des services utilisés) et d'autre part le relais des paquets de données. Quand un paquet de données arrive d'un réseau externe au réseau GSM, le GGSN reçoit ce paquet et le transfert au SGSN qui le retransmet vers la station mobile. Pour les paquets sortants, c'est le SGSN qui les transmet vers le GGSN.

Le routage des paquets : Le routage de chaque paquet est indépendant de celui qui le précède ou de celui qui le suit. Pendant la phase de connexion d'un terminal dans un réseau GSM, les échanges de signalisation sont nombreux, et pour faire face aux contraintes du mode paquet, les informations de routage obtenues pour acheminer le premier paquet vers un terminal GSM sont stoquées dans le GGSN. Ainsi la route pour les paquets suivants est sélectionnée à partir du contexte stoqué dans le GGSN (le Temporary Logical Link Identity ou TLLI).

1.6.3 UMTS

Présentation

L'UMTS (Universal Mobile Telecommunications System) [24] est la version européenne définie par l'ETSI (Institut Européen de Normalisation des Télécommunications) de la

troisième génération des services mobiles (3G). Les débits proposés doivent atteindre 2 Mb/s. En fait, cette norme est un membre de famille du projet IMT-2000 (International Mobile Telecommunication System 2000) défini par l'UIT (Union Internationale des Télécommunications). Les réseaux UMTS constitueront les systèmes de télécommunications mobiles et sans fil de troisième génération, capables d'offrir au grand public des services de type multimédia à débit élevé. Les objectifs sont les suivants :

- Pour les services :
  - Capacités multimédia et mobilité sur une très grande étendue géographique,
  - Accès efficace à Internet, aux intranets et aux autres services basés sur le protocole IP,
  - Transmission vocale de grande qualité, comparable à celle des réseaux fixes,
  - Portabilité des services dans les environnements UMTS différents,
  - Fonctionnement en mode GSM / UMTS à l'intérieur, à l'extérieur et dans des endroits extérieur éloignés, sans solution de continuité, permettant une itinérance totale entre les réseaux GSM et entre les éléments terrestres et satellitaires des réseaux UMTS.
- Pour les terminaux :
  - Terminaux GSM / UMTS bimodaux et à deux bandes,
  - Terminaux UMTS bimodaux terrestres / satellite.

Services

De nombreux services orientés données sont supportés par le GSM. En particulier les évolutions du GSM, telle que le GPRS, permettront une première étape vers la transmission haut débit, et vers d'autres services tels que le courrier électronique, le télépaiement, le transfert de fichiers, l'accès Internet. Toutefois, l'UMTS avec ses débits allant jusqu'à 2 Mbs propose un meilleur compromis capacité/coût.

Pour le grand public l'UMTS doit proposer des contenus multimédia (exemples : jeux,

loisirs, visioconférence) tout en répondant au besoin de mobilité des personnes.

Du GSM à l'UMTS

Interopérabilité GSM/UMTS : Les normes de deuxième génération permettent une couverture presque globale des territoires. Pour ce faire, trois types de cellules sont utilisées : des macro-cellules de 30 km de rayon environ, des micro-cellules de 500 m de rayon et des pico-cellules de 100 m.

L'UMTS, parce qu'il opère à une fréquence plus élevée et avec des débits à la fois variables et importants, nécessite des cellules de taille nettement plus petite que les macro-cellules actuelles, qui pourraient être de quelques centaines de mètres. Cela conduit à un réseau au coût plus élevé, onéreux en infrastructures. Par conséquent, le déploiement de l'UMTS sera progressif. La 3ème génération s'appuie donc sur la 2ème génération pour la couverture globale. L'objectif est d'obtenir une couverture maximale, telle qu'en tous lieux, les services UMTS soient accessibles à haut débit dans les zones UMTS ou en mode dégradé lorsque le mode GSM prend le relais. Cela implique une interopérabilité maximale avec le GSM, de façon transparente, et l'utilisation de terminaux GSM/UMTS.

Interface radio : Pour le réseau UMTS, l'interface radio terrestre reposera sur une nouvelle interface radio - UTRA (UMTS Terrestrial Radio Access)- distincte de celle du système GSM. Une décision de compromis a été prise par l'ETSI (Institut Européen de Normalisation des Télécommunications) :

Le débit de l'interface dépend de l'environnement d'utilisation :

- Dans une zone rurale : au moins 144 kbit/s, l'objectif étant de 384 kbit/s,
- Dans un espace urbain : au moins 384 kbit/s, l'objectif étant de 512 kbit/s,
- Dans un immeuble : au moins 2 Mbit/s.

L'interface UTRA doit offrir une négociation des attributs de services (type de support, débit, taux d'erreur, délai de transmission de bout en bout, etc.), des supports de services

orientés circuits et paquets, la gestion de priorité sur l'interface radio, l'adaptation de la liaison à la qualité et à la charge du réseau.

L'interface UTRA doir offrir un hand-over sans coupure du réseau d'un opérateur UMTS vers celui d'un autre opérateur UMTS, mais aussi vers un réseau GSM de la seconde génération.

Le réseau UMTS

L'introduction de l'UMTS est possible en gardant le même réseau que GSM. Il faut néanmoins installer de nouvelles stations de base (BS pour Base Station). La figure 17 montre la structure du réseau UMTS.

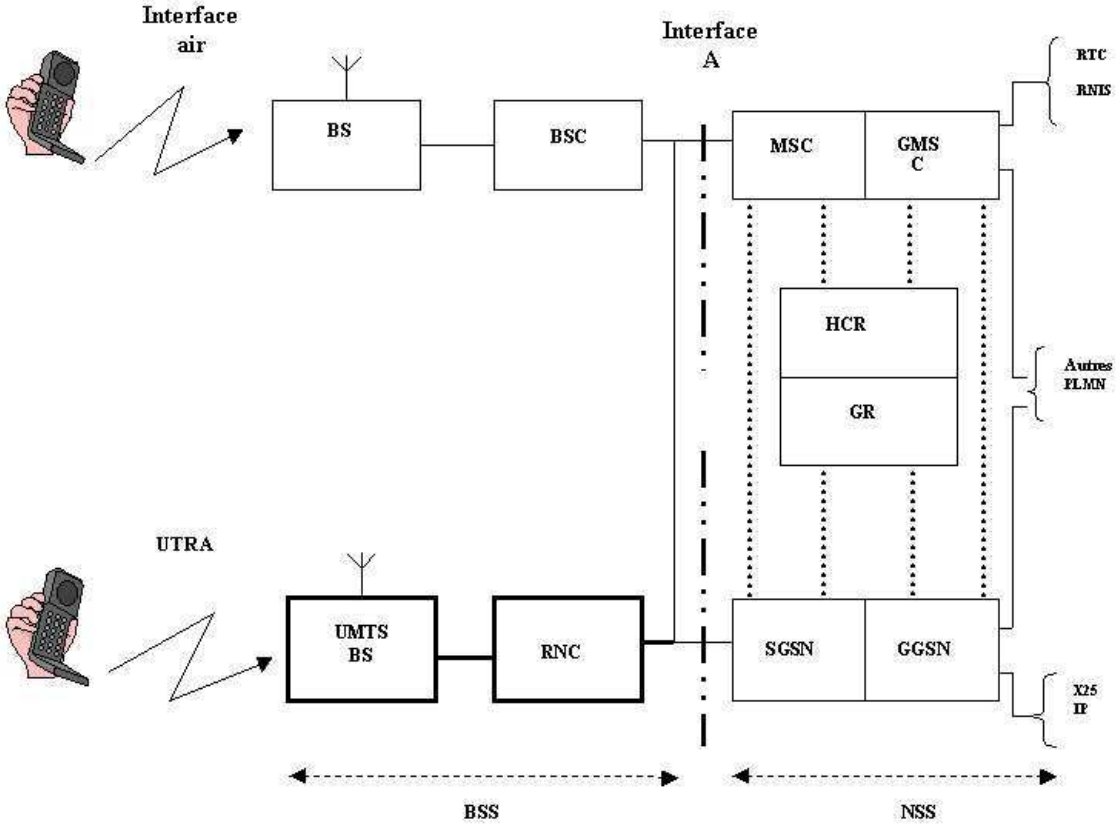


FIG. 17 – *Structure d'un réseau UMTS [28]*

1.6.4 La norme 802.11

Le 802.11 est une norme de réseaux sans fil qui date des années 1990. La première version est normalisée en 1997 [8] et propose des débits de 2Mbits/s au maximum. A cette époque le matériel est surtout professionnel. Par la suite des évolutions de la norme proposent des débits plus intéressants de 11Mbit/s. L'extension 802.11b [9] est normalisée en 1999. Les produits commercialisés sous le nom de Wifi deviennent accessibles au grand public. En 2003, la norme 802.11g [12] est disponible et propose des débits allant jusqu'à 54Mbits/s théorique.

Architectures

Le standard 802.11 définit deux topologies : le mode infrastructure et le mode ad hoc.

En mode infrastructure, le réseau sans fil consiste au minimum en un point d'accès (que nous noterons AP pour Access Point) et un ensemble de postes réseaux sans fil. Cette configuration est nommée Basic Service Set (BSS pour ensemble de services de base), il est identifié par le BSSID qui est en fait l'adresse MAC de l'interface réseau sans fil du point d'accès. Un Extended Service Set (ESS, ou ensemble de services étendu) est un ensemble d'au moins deux BSS formant un seul sous-réseau, il est identifié par un ESSID qui est un nom de réseau choisi par l'administrateur de l'ESS. La liaison entre les BSS se fait par une infrastructure, le plus souvent filaire, appelée DS (Distribution System pour système de distribution). Ce DS peut également être réalisé en sans fil, on parle alors de WDS (Wireless Distribution System). La plupart des WLAN devront pouvoir accéder aux services pris en charge par le LAN filaire (serveurs de fichiers, imprimantes, accès Internet). Aussi fonctionneront-ils en mode infrastructure. Dans cette configuration le WLAN est une extension du LAN destinée aux postes ayant des besoins de mobilité.

Quand on utilise ce type d'architecture, toutes les communications d'une cellule passent par le point d'accès. D'ailleurs, dans la trame 802.11, un champs supplémentaire est prévu pour l'adresse MAC du point d'accès en plus des champs adresses des stations communi-

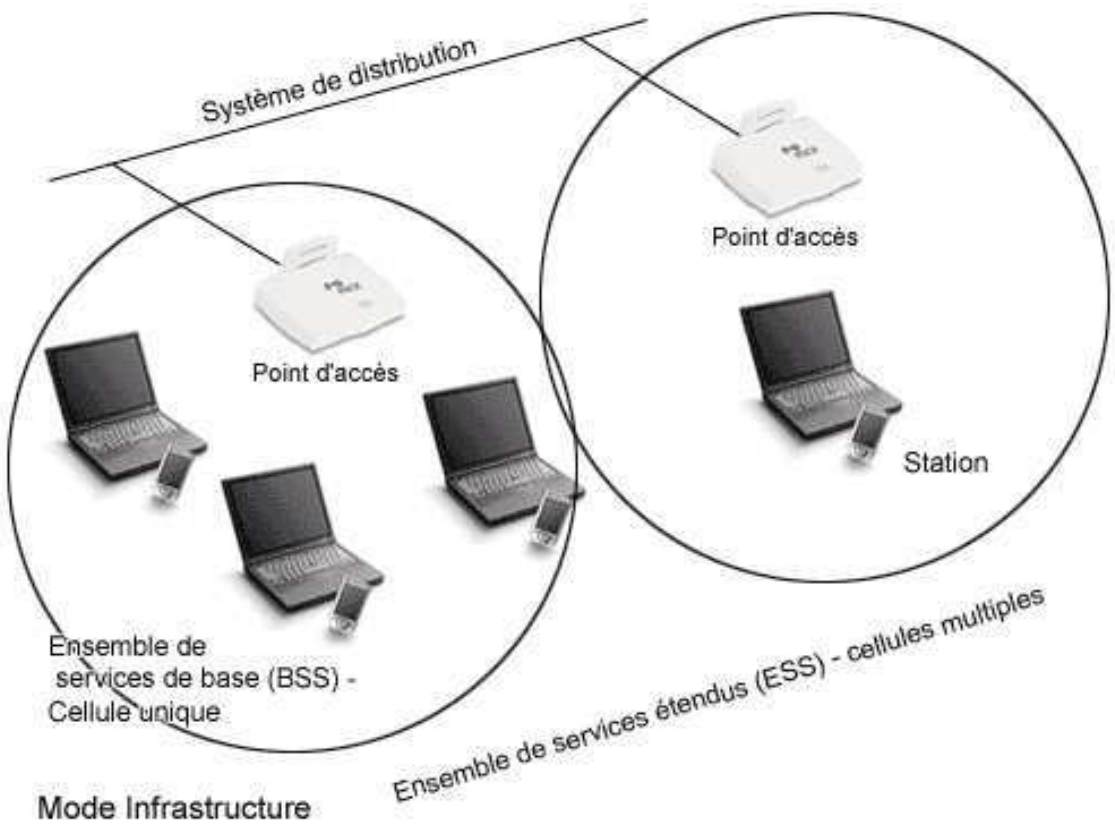


FIG. 18 – *Topologie avec Infrastructure*

cantes. Une trame en provenance d'un station sera donc capturée par le point d'accès puis répétée dans la cellule si la station destination s'y trouve. Il l'enverra sur le système de distribution si le destinataire se trouve ailleurs. Même si deux stations affiliées au même point d'accès sont à portée radio l'une de l'autre, les informations transitent par le point d'accès.

Pour connaître la liste des stations affiliées, chaque point d'accès gère une liste appelée table d'affiliation. Dans celle-ci, les stations sont identifiées par leur adresse MAC. La liste est mise à jour, soit quand une nouvelle station s'affilie, soit quand une station demande à quitter la cellule (Deauthentication présentée dans le chapitre 2 de cette partie). Le point d'accès peut également supprimer une station de sa liste si celle-ci reste inaccessible pendant un certain délai (Time Out).

Le mode ad hoc (voir figure 19 est défini par un ensemble de stations indépendantes appelées Independent Basic Service Set (IBSS pour ensemble de services de base indépendants). Ces stations communiquent en 802.11 directement entre elles sans passer par un point d'accès. Ce mode permet de créer rapidement et simplement un réseau sans fil là où il n'existe pas d'infrastructure filaire ou encore là où une telle infrastructure n'est pas nécessaire pour les services attendus.

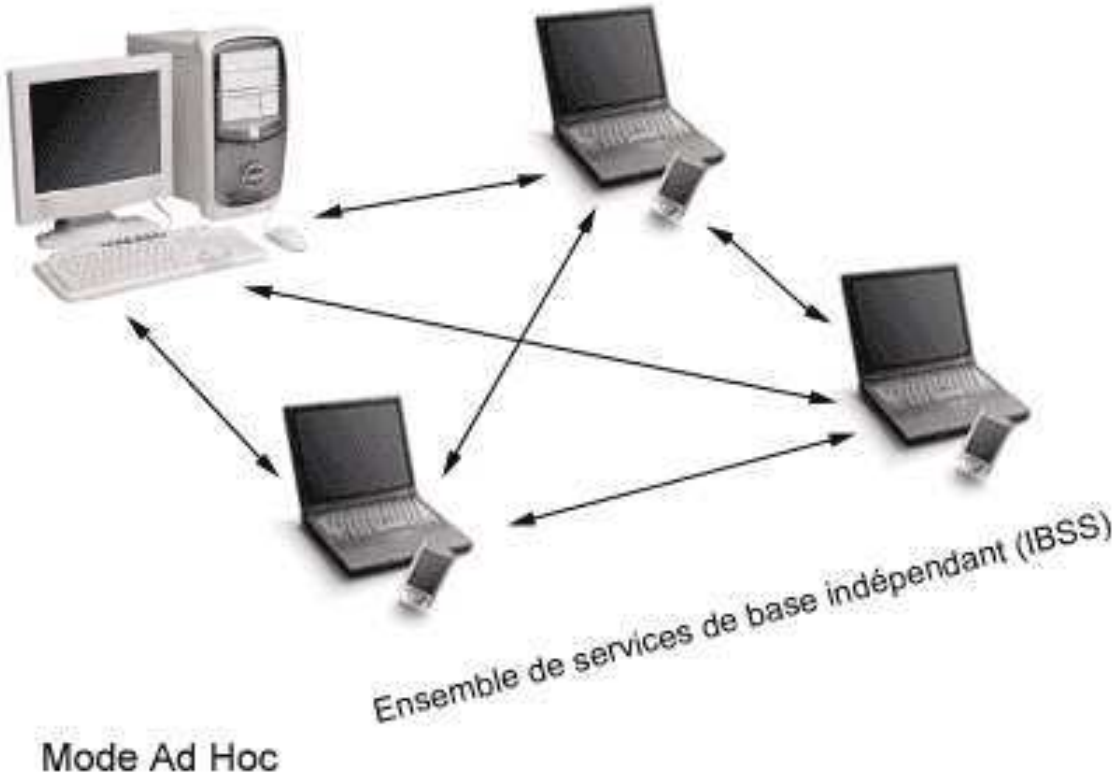


FIG. 19 – *Topologie distribuée Ad-Hoc*

Les méthode d'accès de 802.11 : DCF et PCF

La norme IEEE 802.11 définit deux méthodes d'accès au médium, qui proposent des qualités de service différentes. La méthode d'accès DCF (Distributed Coordination Function) est la méthode d'accès de base de la norme IEEE 802.11. La méthode d'accès au médium sans contention PCF (Point Coordination Function) est une option à la norme

IEEE 802.11. Les constructeurs de cartes réseaux sans fil ne sont pas tenus de la proposer dans leur matériel pour être conforme à la norme.

Avant de rentrer dans le détail des deux méthodes, il est nécessaire d'introduire les notions d'IFS et de contention :

Les IFS : Les IFS (Inter-Frame Spaces) sont des temps inter-trames utilisés dans les méthodes d'accès, ils ont des valeurs différentes qui permettent de donner des priorités différentes à différents types de trames. 4 sont définis par 802.11 :

- le SIFS (Short IFS) est l'IFS le plus court et est utilisé dans trois cas. Tout d'abord, c'est le temps au bout duquel une station doit envoyer l'acquittement en réponse à une trame qui lui est destinée et qui n'est pas erronée. C'est également le temps au bout duquel une trame CTS doit être émise par une station après réception d'une trame RTS. Enfin, c'est le temps qui sépare deux trames dans la méthode d'accès PCF.
- Le PIFS (PCF IFS) est quant à lui utilisé par les points d'accès pour débuter une période d'accès sans contention PCF.
- Le DIFS (DCF IFS) est le temps d'inactivité sur le médium au bout duquel une station peut débuter la période de contention, que nous allons décrire dans le paragraphe suivant.
- L'EIFS (Extended IFS) est l'IFS le plus long. Il est utilisé par une station lorsque sa couche Physique reçoit une trame erronée. Cela permet éventuellement à une autre station d'acquitter la trame avant que cette station n'ait eu le temps d'envoyer des informations sur le médium. La réception d'une trame correcte par la couche Physique de cette station a pour effet d'annuler l'EIFS. Dans ce cas, la station pourra à nouveau émettre au bout d'un temps DIFS, auquel s'ajoute la période de contention.

La contention : Dans le mécanisme présenté précédemment, on a vu qu'après l'envoi d'une trame, les stations attendent pendant un certain temps (par exemple un temps DIFS en DCF). On va ajouter à ce temps un délai appelé période de contention ou backoff. Sa valeur est choisi de manière aléatoire, par chaque station souhaitant communiquer, dans un intervalle qui va de 0 à CW (Contention Window qui est lui même compris dans un intervalle [CWMin, CWMax]). Durant la période de contention, à chaque intervalle de temps (noté slot) durant lequel aucune activité n'est enregistrée sur le réseau, les stations décrémentent la valeur de leur période de contention. Si une activité est enregistrée sur le réseau, la station arrête le décompte, attend un temps DIFS, avant de le recommencer. Quand la valeur devient nulle, la station émet sa trame, puis attend de nouveau un temps (DIFS, EIFS...) avant de retirer une valeur au hasard et ainsi de suite, un exemple de ce mécanisme est montré sur la figure 20 pour la méthode d'accès DCF. Le tirage aléatoire de la valeur permet d'éviter statistiquement que plusieurs stations tentent d'émettre au même moment. Quand une trame est envoyée et non acquittée, la station double la valeur CW, ce qui étend l'intervalle de tirage aléatoire ce qui permet d'éviter les collisions dans les réseaux chargés.

Après ces quelques précisions, revenons aux méthodes d'accès de 802.11 en commençant par le DCF.

DCF : Distributed Coordination Function : C'est une méthode distribuée, l'accès au médium est aléatoire, c'est à dire que les stations sont en compétition pour transmettre des données. Elle est adaptable à la fois au mode ad-hoc et au mode avec infrastructure. C'est une méthode d'accès, utilisant la contention, qui est en fait une adaptation de la méthode CSMA/CA, où chaque trame émise doit immédiatement être acquittée par le destinataire.

Avec cette méthode toutes les stations ont la même probabilité d'accéder au médium mais le tirage de la période de contention étant aléatoire, il n'est pas possible de garantir

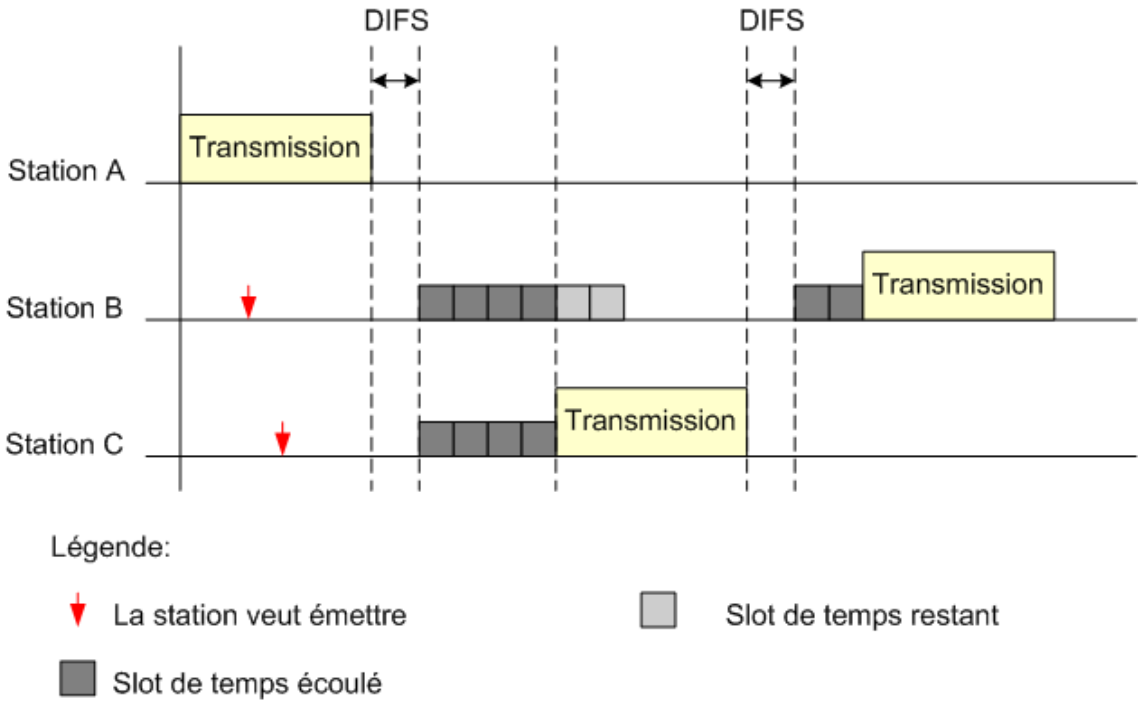


FIG. 20 – *Méthode d'accès DCF*

un délai minimal d'accès au médium. Le DCF ne propose pas la qualité de service, qui pourrait être nécessaire pour des applications à trafic contraint par le temps.

Le terminal caché : Parmi les différents problèmes liés aux réseaux sans fil, on trouve celui du terminal caché. Il survient quand deux stations souhaitent communiquer en même temps avec une troisième et que ces deux stations ne sont pas à portée radio l'une de l'autre. La méthode d'accès présentée ci-dessus n'est donc pas suffisante pour éviter les collisions. On va lui ajouter un mécanisme, le RTS/CTS (Request To Send/Clear To Send). Le principe de base est qu'une station souhaitant émettre des données va demander un délai pendant lequel le médium lui sera alloué, c'est à dire que toutes les autres stations auront l'obligation de "se taire".

La résolution du problème du terminal caché avec le RTS/CTS est représentée par la figure 21. Une station désirant émettre, diffuse une trame courte RTS vers la station destinataire, en spécifiant la durée nécessaire à l'émission de la trame. La station desti-

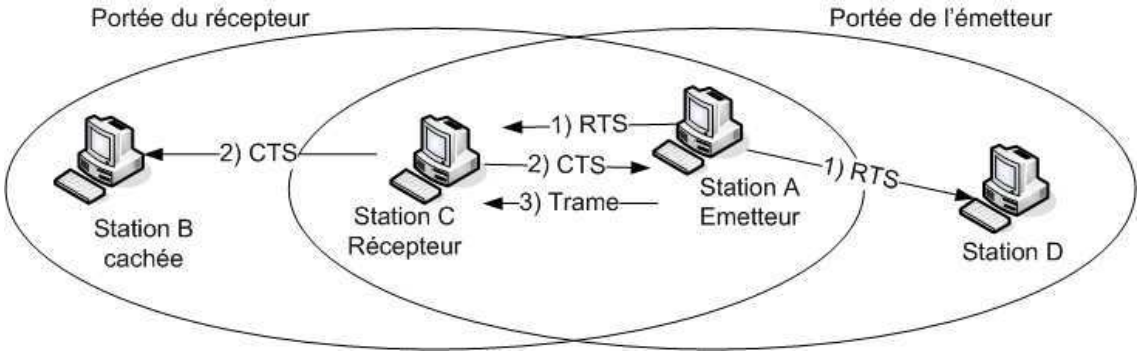


FIG. 21 – *Le problème du terminal caché*

nataire répond après un temps SIFS par une trame CTS en spécifiant à nouveau la durée d'émission de la trame. Aussi bien l'émetteur que la (ou les) station cachée vont recevoir la trame CTS. La station cachée ne va donc pas émettre pendant la durée spécifiée et l'émetteur va émettre pendant la période qui lui est réservée.

Le mécanisme de réservation utilise une temporisation, le NAV (Network Allocation Vector). Les stations à portée de l'émetteur (station D sur le la figure 22) vont initialiser le NAV avec une valeur égale au temps nécessaire à l'envoi du CTS et de la trame de donnée. Les stations à portée du récepteur vont initialiser le NAV avec la valeur contenue dans le CTS. Le NAV de chaque station va alors être décrémenté et elles ne pourront émettre qu'après que ce champs soit revenu à 0. Sauf évidemment la station émettrice qui envoie sa trame après un temps SIFS comme on peut le voir sur la figure 22.

PCF : Point Coordination Function : C'est une méthode d'accès centralisée, contrairement à DCF. Elle repose sur un système de polling simple. C'est à dire qu'une station maître peut interroger une à une les stations qui sont à sa portée, donc décider quelle station a le droit d'émettre dans la cellule. En 802.11 c'est le point d'accès qui intègre cette fonction. C'est pourquoi cette option n'est pas disponible pour le mode ad-hoc.

Quand on utilise le PCF, l'accès au médium se déroule en 2 période consécutives (voir

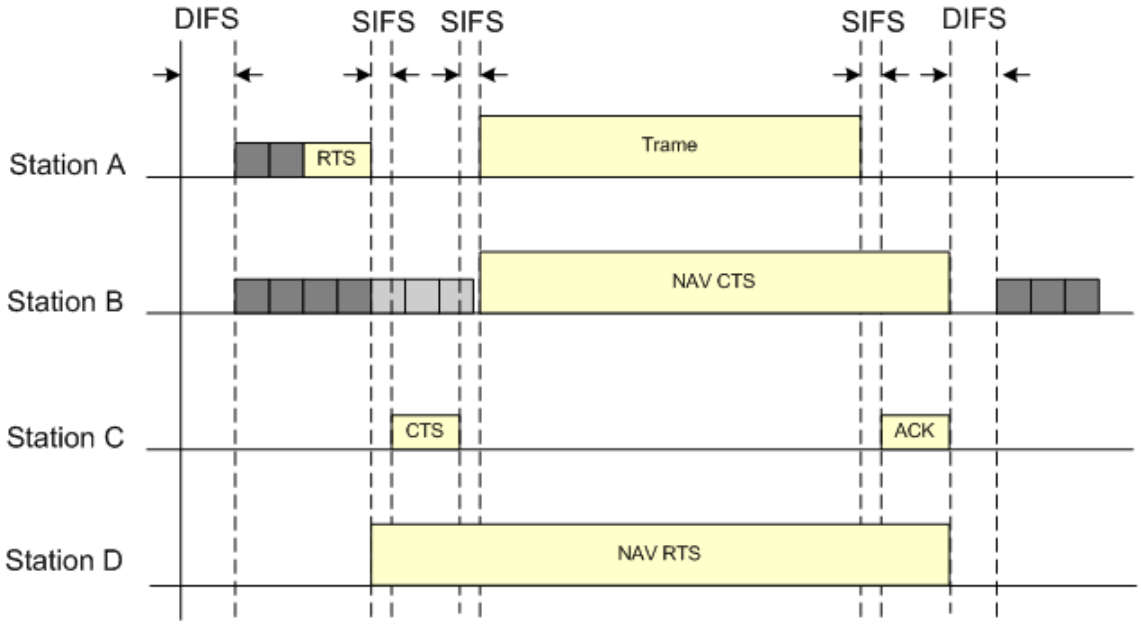


FIG. 22 – *Le mécanisme de réservation RTS/CTS*

figure 23). Pendant la première, le polling est initié par le point d'accès, cette période est dite sans contention. La deuxième, dite avec contention, utilise la méthode DCF décrite au-dessus. La phase de polling est prioritaire par rapport à la phase avec contention, cette priorité est réalisé grâce à l'utilisation d'un délai PIFS dont la valeur est comprise entre le SIFS utilisé pour l'acquittement de trames et le DIFS utilisé entre la transmission de deux trames.

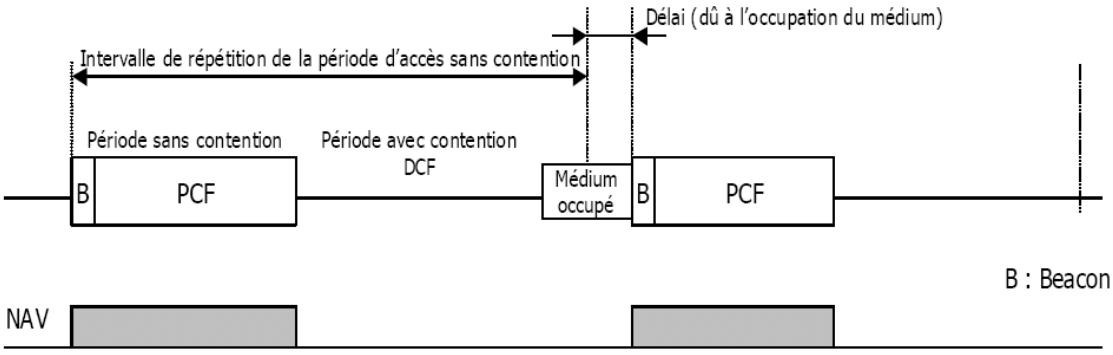


FIG. 23 – *Méthode d'accès PCF*

Le point d'accès débute la période sans contention en diffusant un Beacon spécifique (trame de gestion 802.11, c'est une balise qui permet de synchroniser les stations d'une cellule et de "réveiller" les éventuelles stations en mode économie d'énergie) après un délai PIFS.

Durant le polling, le point d'accès interroge à tour de rôle les stations qui lui sont affiliées. Seule la station sollicitée est autorisée à émettre. Le délai inter-trames utilisé est normalement le SIFS. Une station qui n'aurait pas de données à envoyer répond au point d'accès par une trame vide.

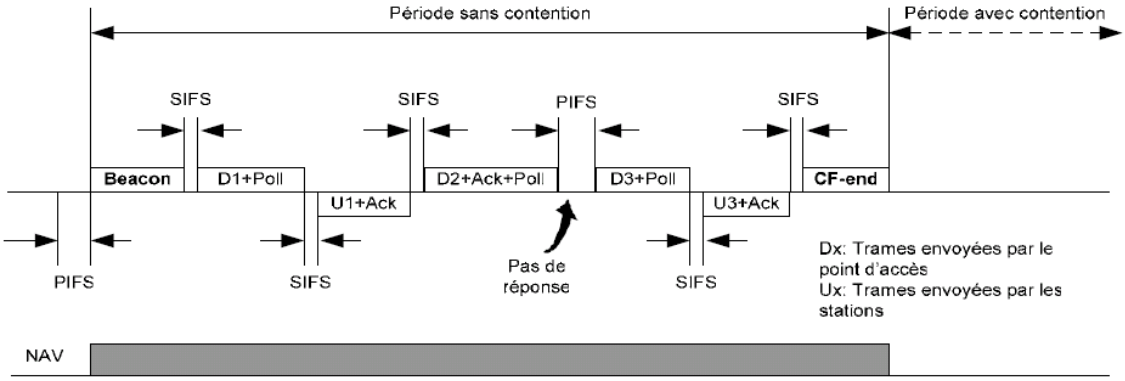


FIG. 24 – *La période sans contention de PCF*

De ces deux méthodes de base de la norme, seul le DCF est disponible dans tous les produits 802.11. Le PCF est optionnel et très peu de constructeurs ont décidé de l'implémenter. Pourtant, cette méthode pourrait être intéressante en terme de qualité de service puisqu'on peut donner une priorité à certaines communications et garantir un accès au médium sans compétition entre les stations affiliées à un même point d'accès. C'est d'ailleurs un système de polling similaire que nous avons mis en oeuvre pour l'interrogation des mobiles dans notre projet, qui sera décrit dans la deuxième partie de ce manuscrit.

De nombreux travaux ont été initiés pour améliorer ces deux méthodes d'accès, notamment pour résoudre des problèmes de qualité de service. C'est par exemple le cas de l'extension 802.11e [10] qui propose une amélioration de DCF, le EDCF (Enhanced DCF).

Les extensions de la norme 802.11

La norme 802.11 a beaucoup évolué et propose différentes extensions. Certaines sont des normes de communications à part entière (a, b et g) qui proposent des débits et des fréquences d'utilisation différents. D'autres sont plutôt des composants qui seront ajoutés selon les besoins des utilisateurs en sécurité ou qualité de service (i et e par exemple).

Parmi ces extensions, certaines sont encore au stade de groupe de travail et ne sont donc pas normalisées : 802.11n qui doit proposer des débits supérieurs à 100Mbits/s, 802.11r qui traite du Fast Roaming. Cette dernière dont le groupe de travail n'existe que depuis le printemps 2004, est proche de la thématique abordée dans le projet Waves.

Les principales extensions sont décrites dans le tableau suivant :

Nom de la norme	**Nom**	**Description**
802.11a	Wifi5	La norme 802.11a permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	Wifi	La norme 802.11b est la norme la plus répandue actuellement en Europe. Elle propose un débit théorique de 11 Mbps (6 Mbps rééls) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.

802.11c	Pontage 802.11 vers 802.1d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau liaison de données).
802.11d	Interopérabilité internationale	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche liaison de données. Ainsi, cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo.

802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (ou roaming en anglais)
802.11g		La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b
802.11h		La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, doù le h de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.

802.11i		La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11Ir		La norme 802.11Ir a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme 802.11j est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne. Ses caractéristiques techniques sont celles de 802.11a
802.11n		La norme 802.11n proposera des débits beaucoup plus rapides (plus de 100 Mb/s) utilisant la technologie MIMO (Multiple Input Multiple Output).
802.11r	Fast Roaming	La norme 802.11r traite du changement de cellule rapide en s'attachant au niveau du contenu, afin de ne pas perdre d'informations lors de la transmission de flux continus comme la vidéo ou la voix sur IP
802.11s	Réseaux Mesh	La norme 802.11s propose d'exploiter n'importe quel type d'équipement WiFi, afin d'acheminer des données d'un point à un autre.

Chapitre 2

Gestion de l'itinérance dans les réseaux cellulaires

Sommaire

2.1 Le changement de cellule dans GSM 57

2.1.1 Gestion de l'itinérance dans GSM 57

2.1.2 Le Handover GSM 58

2.2 Le changement de cellule dans 802.11 59

Une station mobile (téléphone portable, ordinateur de poche, etc) peut être amenée à se déplacer en différents points de la zone couverte par le réseau sans fil. Malgré cette mobilité, elle doit pouvoir garder sa connectivité avec le réseau : pouvoir atteindre une station voisine qui servira de relais avec l'infrastructure par exemple. C'est la notion d'itinérance (*roaming*).

Pendant une communication, le mobile est en liaison radio avec une station de base déterminée. Il est souhaitable d'assurer la continuité du service alors que l'utilisateur se déplace. Il est peut être nécessaire de changer la station de base avec laquelle le mobile est relié tout en maintenant la communication : c'est le transfert inter-cellulaire ou handover.

Le rôle principal d'un mécanisme de gestion de l'itinérance est de permettre au réseau

de connaître à tout moment la position d'un mobile. Cette fonction est nécessaire pour qu'il puisse joindre n'importe quel mobile du réseau. Dans la gestion de la localisation des mobiles, deux mécanismes de base interviennent :

- la localisation qui consiste à savoir où se trouve un mobile et ce à tout moment,
- la recherche de mobile qui consiste à émettre des messages d'avis de recherche dans les cellules où le système a précédemment localisé le mobile.

Systèmes sans localisation : Dans certains systèmes cellulaires de première génération, dans les réseaux radio de couverture peu étendue et dans pratiquement tous les systèmes de radio-messagerie unidirectionnelle, aucune gestion de l'itinérance des usagers n'est assurée. Aucune poursuite des mobiles n'est réalisée et lorsqu'un utilisateur est appelé, le système lance des avis de recherche sur toute la couverture radio du système. Les réseaux 802.11 n'utilisent pas de zones de localisations géographiques pour situer les stations contrairement aux réseaux GSM.

Cette méthode a l'avantage de la simplicité de gestion. En contrepartie, elle ne peut s'appliquer qu'à des systèmes où les taux d'appels entrants sont relativement faibles ou bien à des systèmes de transport de messages courts, en raison de la charge du réseau que ces opérations provoquent. Ceci est incompatible dans le cas des systèmes de communications bidirectionnelles et/ou desservant des populations importantes d'usagers .

Utilisation de zones de localisation Pour palier les inconvénients de la méthode décrite précédemment, des zones de localisation regroupant un certain nombre de cellules sont définies. Le système connaît la zone de localisation d'un mobile, c'est à dire la dernière zone géographique dans laquelle le mobile s'est signalé mais ignore la cellule précise où se trouve le mobile à l'intérieur de la zone de localisation. De cette manière, lorsque l'usager reçoit un appel, le système va le rechercher dans la zone de localisation courante en émettant un avis de recherche dans les cellules de cette zone. Et ainsi, la consommation

de ressources radio sera réduite à celle nécessaire à la recherche de l'abonné dans la zone de localisation concernée.

La mise à jour sur changement de zone de localisation est la méthode la plus utilisée par les systèmes cellulaires dans le domaine de la radio téléphonie (par exemple le GSM). Chaque station de base diffuse périodiquement sur une voie balise le numéro de la zone de localisation à laquelle elle appartient. Le mobile de son côté écoute périodiquement la voie balise et stocke en permanence le numéro de sa zone de localisation courante. Si le mobile s'aperçoit que le numéro de la zone dans laquelle il se trouve est différent du numéro stocké, il signale sa nouvelle position au réseau. C'est le mécanisme de mise à jour de localisation, appelé aussi inscription ou enregistrement. Les bases de données de localisation vont ainsi être mises à jour au niveau du réseau.

2.1 Le changement de cellule dans GSM

2.1.1 Gestion de l'itinérance dans GSM

Le réseau GSM utilise le principe des zones de localisation évoqué précédemment. Nous avons vu précédemment que deux bases de données sont utilisées pour stocker les informations concernant les mobiles : HLR et VLR. Pendant un changement de cellule, il y aura mise à jour des informations de ces bases, éventuellement des échanges d'informations entre elles.

Un VLR est associé à un MSC, il peut gérer plusieurs zones de localisation. En revanche, une zone de localisation ne peut pas comprendre des cellules dépendant d'un autre VLR. Pour éviter les transferts inutiles de signalisations, seul le VLR mémorise la zone de localisation courante de l'ensemble des mobiles qu'il gère. Le HLR mémorise l'identité du VLR courant de chaque abonné et non pas sa zone de localisation. Quand un appel est émis vers un abonné GSM, on interroge son HLR de manière à localiser l'abonné, du moins la dernière localisation connue ainsi que l'état de son terminal. S'il est disponible,

on interroge alors le VLR pour connaître la zone de localisation et le BSC correspondant qui lui peut atteindre l'abonné par l'intermédiaire des BTS qu'il contrôle.

2.1.2 Le Handover GSM

Le Handover permet de conserver une liaison continue entre le réseau et une station mobile se déplaçant au voisinage de la frontière séparant les cellules. Le changement de cellule (BTS) doit bien évidemment être transparent pour la plupart des applications de radio téléphonie. Nous allons voir une façon très courante de décider du déclenchement d'un handover, illustrée pour le cas du GSM de deuxième génération : durant la communication, le mobile utilise le temps laissé libre (slot) par l'AMRT (Accès Multiple à Répartition dans le Temps) pour scruter les canaux de signalisation (BCCH : Broadband Control CHannel) des cellules proches de sa propre cellule. Ces mesures sont envoyées au BSC afin d'y être analysées. Sur le canal courant, la station mobile mesure le niveau de signal reçu noté RXLev, et la qualité du signal de la cellule courante noté RXQual sur :

- la cellule avec laquelle elle communique.
- les cellules voisines qu'elle peut recevoir.

Les mesures sont classées par RxLev croissant. Si RxLev $<$ RxLev min et RxQual $>$ RxQualmin alors la BSC décide de faire un Handover.

L'architecture du réseau GSM nous permet de distinguer trois types de Handover :

Le handover intra BSC : C'est le type le plus fréquent. Ceci indique typiquement que la MS est sur le bord de la cellule.

Détaillons rapidement l'échange de message au sein du BSS pendant l'exécution du handover.

La BSC établit, parallèlement à la liaison existante, une seconde voie de signalisation vers la nouvelle BTS. Puis la BSC commande au mobile de se porter sur la BTS nouvel-

lement élue et commute la communication simultanément. Enfin, lorsque le transfert est réalisé, la BTS en informe la BSC qui commande la libération des ressources employées dans la cellule quittée.

Le handover inter BSC : Nous décrivons ici le déroulement du handover entre deux cellules d'un même MSC mais de BSC différents. Par action conjuguée du BSC quitté et du MSC, on établit un canal de signalisation vers la BTS cible au travers de la nouvelle BSC. Après un accord du BSC cible, le mobile est invité à se porter sous cette dernière. Alors, la MSC commute la communication. Après acquittement du Handover par la BTS cible, le MSC libère les anciens liens.

Si le BSC doit effectuer un handover hors de sa zone de gestion (c'est à dire dans une cellule qui n'est pas gérée par une BTS qu'il contrôle), il communique au MSC de rattachement les données nécessaires.

Le handover inter MSC : Le MSC1 (voir la figure 25) établit une liaison à travers le MSC2 vers la BTS cible.

Le MSC2 informe le MSC1 de l'accord du BSC cible. Le MSC1 commande le mobile à travers la BSC de la MSC1 à se porter sur la BTS cible.

Le MSC1 commute alors la communication vers la BTS cible via le MSC2 et le BSC de la MSC2.

De même, après acquittement du Handover, le MSC1 libère les anciens liens.

2.2 Le changement de cellule dans 802.11

Dans un réseau 802.11 en mode infrastructure, les stations sont affiliées à un point d'accès qui fait partie de cette infrastructure. Dans un contexte où les stations sont mo-

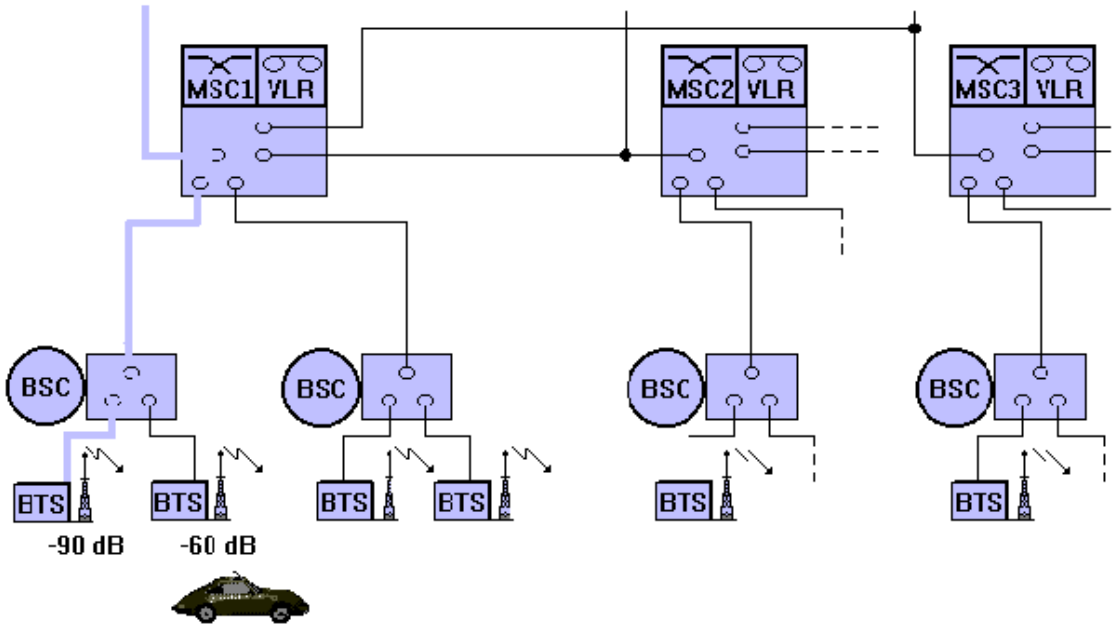


FIG. 25 – *Le handover dans les réseaux GSM [5]*

biles, il est parfois nécessaire qu'une station change de cellule, ce qui signifie qu'elle doit s'affilier à un autre point d'accès.

Dans la norme 802.11 [8], on ne trouve pas une réelle gestion du handover comme on a pu le voir dans le GSM. On trouve uniquement les conditions à partir desquelles une station va décider de changer de point d'accès d'affiliation ainsi que les différentes étapes qui vont lui permettre de choisir et de s'affilier à un nouveau point d'accès.

Le mécanisme peut être divisé en plusieurs étapes.

Phase de détection/déclenchement : Le changement de cellule est en principe décidé suite à une détérioration de la qualité de la liaison radio définie grâce à la puissance du signal, le rapport signal sur bruit (SNR : Signal to Noise Ratio) ou à une perte de connexion avec le point d'accès. Pour chaque trame reçue, la carte réseau est capable de mesurer la puissance du signal reçu, un indicateur le RSSI (Receive Signal Strength Indicator) est utilisé. Sa valeur peut aller de 0 à 255, 0 pour un signal très faible et 255 pour un signal

très satisfaisant.

Phase de Désauthentification : Une trame de gestion 802.11 appelée "Deauthentication" est envoyée, soit par la station avant de changer de canal de communication ce qui permet au point d'accès de mettre sa table d'affiliation à jour, soit par le point d'accès pour demander à une station de quitter la cellule.

Phase de recherche d'un nouveau point d'accès : Une fois que la décision concernant le handover est prise, la station doit chercher un point d'accès offrant des conditions de communications plus performantes selon les mêmes critères que le point d'accès précédent. Deux méthodes existent pour rechercher les point d'accès potentiels :

- Le scan actif : dans ce mode, la station va prendre l'initiative de la recherche d'un point d'accès à rejoindre. La station cherche à joindre les AP environnants en envoyant des trames sondes appelées Probe Request. Si un point d'accès reçoit ce type de trame, il va répondre avec une autre trame de gestion appelée Probe Response. Grâce à la mesure du signal effectuée à la réception de cette trame, la station va pourvoir juger si ce point d'accès potentiel est un bon candidat, c'est après comparaison des résultats de tous les "probe response" reçus que la station entamera la phase d'affiliation à un nouveau point d'accès.
- Le scan passif : la station n'émet plus et change de canal à intervalles réguliers selon le paramètre ChannelTimer. Il est nécessaire de rester sur chaque canal pour un délai supérieur au délai inter-beacon des AP. Tous les canaux seront scrutés, on retrouve ensuite la phase de Probe mais seulement pour l'AP choisi.

Le groupe 802.11k [14] travaille sur l'amélioration du choix de l'AP destination en tenant compte de la charge du réseau et plus seulement de la puissance du signal.

Phase d'Authentification : Une fois qu'une station a trouvé un Point d'Accès et a décidé de rejoindre une cellule, le processus d'authentification s'enclenche. Celui-ci consiste

Alg. 1 Scan Actif

```
1: Pour Tout canal dans ChannelList Faire
2:    Passer sur le canal courant ;
3:    Attendre Activité ou Expiration du délai ProbeDelay ;
4:    Envoi ProbeRequest ;
5:    Attendre Expiration du délai MinChannelTime
6:    Si Aucune réponse reçue Alors
7:       Passer au canal suivant
8:    Fin Si
9:    Si Traffic détecté ou Reception d'un Probe Response Alors
10:      Traiter les informations des Probe Response
11:      Passer au canal suivant après expiration du délai MaxChannelTime
12:   Fin Si
13: Fin Pour
```

en l'échange d'informations entre le point d'accès et la station en mode infrastructure (entre deux stations pour le mode ad-hoc), où chacun des deux partis prouve son identité. Cette phase est gérée par la couche MAC et est indispensable pour effectuer des communications au niveau supérieur. Il peut s'agir d'une authentification à système ouvert, un simple échange de 2 trames permet aux entités communicantes de s'authentifier entre elles. On peut également avoir une authentification utilisant des clés partagées, cette solution est moins performante (plus de trames à échanger) mais permet une meilleure sécurité.

Phase d'association ou réassociation : Une fois la station authentifiée, le processus d'association s'enclenche. Celui-ci consiste en un échange d'informations sur la cellule : l'ESSID et les vitesses de transmission supportées. Seulement après le processus d'association, la station fait partie du BSS et peut transmettre et recevoir des trames de données. Ce processus est de type hand-check : requête puis réponse à la requête. Il est réalisé par l'échange d'une trame Association Request envoyée par la station qui souhaite s'associer,

à laquelle le point d'accès répond par une trame Association Response, qui contient un code statut qui précise si l'association a été acceptée.

La réassociation est utilisée dans le cas d'un changement de cellule à l'intérieur d'un même ESS ou pour une modifications des conditions de la cellules, par exemple les vitesses de transmission. Les informations sont les même que pour l'association, avec en plus un champs comprenant le BSSID du point d'accès que l'on quitte.

Une fois l'affiliation terminée, l'identifiant de la station, c'est-à-dire l'adresse MAC de la carte réseau, sera contenue dans la table d'affiliation du point d'accès. Avec cette information, le point d'accès transmettra dans sa cellule (donc sur son interface radio) toutes les trames venant de l'infrastructure destinée à cette station.

Cette première partie nous a permis de voir les bases des réseaux sans fil, ainsi que leur fonctionnement en tant que réseaux cellulaires. Ceci permet de poser le problème du changement de cellule dans un réseau de type 802.11, puisque c'est cette norme qui est utilisée dans notre projet. Dans le chapitre précédent nous avons vu les mécanismes du changement de cellule dans un réseau 802.11. La deuxième partie du manuscrit est consacrée au contexte de l'étude. Nous commencerons par détailler les mécanismes du handover de 802.11, évaluer leur coût en temps, en trafic et donc leur influence sur une application telle que la notre. Nous verrons ensuite les solutions existantes pour améliorer le handover et nous terminerons par une présentation du projet Waves dans lequel s'inscrit ce travail de thèse.

Deuxième partie

Étude du handover

Chapitre 1

Problème traité

Sommaire

1.1 Rappel des étapes du Handover 68

1.2 Description détaillée et estimation du temps du mécanisme de Handover 70

1.3 Le Handover dans le projet Waves. 72

La problématique de cette thèse traite du changement de cellule, handover, dans les réseaux sans fil pour des applications à fortes contraintes de temps. Ce mécanisme va provoquer l'envoi de trames de gestion 802.11 échangées entre la station et les points d'accès environnants (celui auquel la station est affiliée et les point d'accès potentiels pour la nouvelle affiliation), ce trafic sera en compétition avec le trafic émis par les différentes entités du réseau. Le mécanisme va prendre un certain temps, pendant lequel le mobile ne pourra plus communiquer, avec l'infrastructure ou avec d'autres mobiles. Il est primordial pour une application contrainte par le temps que le temps du handover soit le plus minime possible, pour réduire au maximum la rupture de liaison entre la station et l'infrastructure. Nous devons donc chercher des solutions pour améliorer le processus de changement de cellule.

Dans un premier temps, nous allons rappeler les étapes du mécanisme de handover,

puis nous ferons une évaluation théorique du temps nécessaire au handover et nous terminerons ce chapitre par une évaluation pratique.

1.1 Rappel des étapes du Handover

Phase de détection/déclenchement : Le handover est en principe décidé suite à une détérioration de la qualité de la liaison radio qui peut être détectée grâce à la puissance du signal, rapport signal sur bruit (SNR : Signal to Noise Ratio) ou à une perte de connexion avec le point d'accès (qui peut être détectée par exemple par la non réception des beacons émis périodiquement par le point d'accès).

Phase de désauthentification : La station signale au point d'accès qu'elle va quitter la cellule avant de chercher un nouveau point d'accès auquel s'affilier. Cette étape a lieu dans le cas où la station est affiliée et décide de changer de cellule, dans le cas d'une perte de connexion complète (panne du point d'accès, station hors de portée...) c'est l'étape suivante qui sera exécutée immédiatement. Cette étape permet au point d'accès quitté de mettre sa table d'affiliation à jour.

Phase de recherche d'un nouveau point d'accès, le "scan" : Le handover ayant été déclenché, la station doit se mettre à la recherche d'un point d'accès offrant des conditions de communications plus performantes que celles constatées dans la cellule courante selon certains critères tels que la puissance du signal.

Il existe deux types de recherche. Pour la première la station est active (Scan actif), elle cherche à joindre des AP en envoyant des trames de gestions (Probe Request) et en attendant les réponses des points d'accès (Probe Response). Pour la deuxième méthode, la station est passive, c'est à dire qu'elle n'envoie aucune trame sur le réseau, elle se contente de passer d'un canal radio à un autre (dans la liste contenue dans le paramètre ChannelList de la norme). Elle reste sur chaque canal un temps égal au paramètre ChannelTimer et

enregistre les informations des éventuels trames beacon qu'elle reçoit. Une fois tous les canaux scrutés, la station fait le bilan des informations qu'elle a reçues et choisit un point d'accès auquel s'affilier.

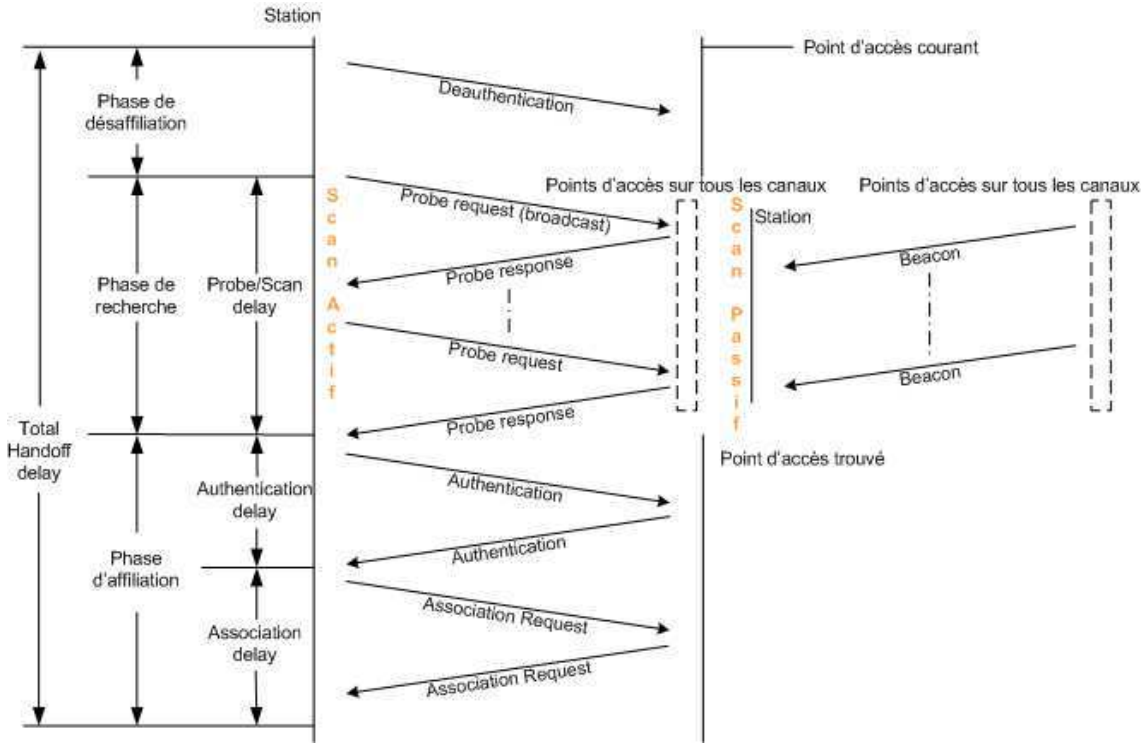


FIG. 26 – *Trames échangées pendant le handover*

Phase d'authentification : C'est un échange d'informations entre le point d'accès et la station, où chacune de ces deux entités prouve son identité.

Phase d'association : Une fois la station authentifiée, le processus d'association s'enclenche. Celui-ci consiste en un échange d'informations sur les différentes stations et les capacités de la cellule. Seulement après le processus d'association, la station peut transmettre et recevoir des trames de données.

La figure 26 rappelle l'ensemble de ces étapes et montre les différents types de trames échangées pendant ce processus.

1.2 Description détaillée et estimation du temps du mécanisme de Handover

Le processus de handover avec scan actif peut être décrit par le séquencement donné par la figure 27.

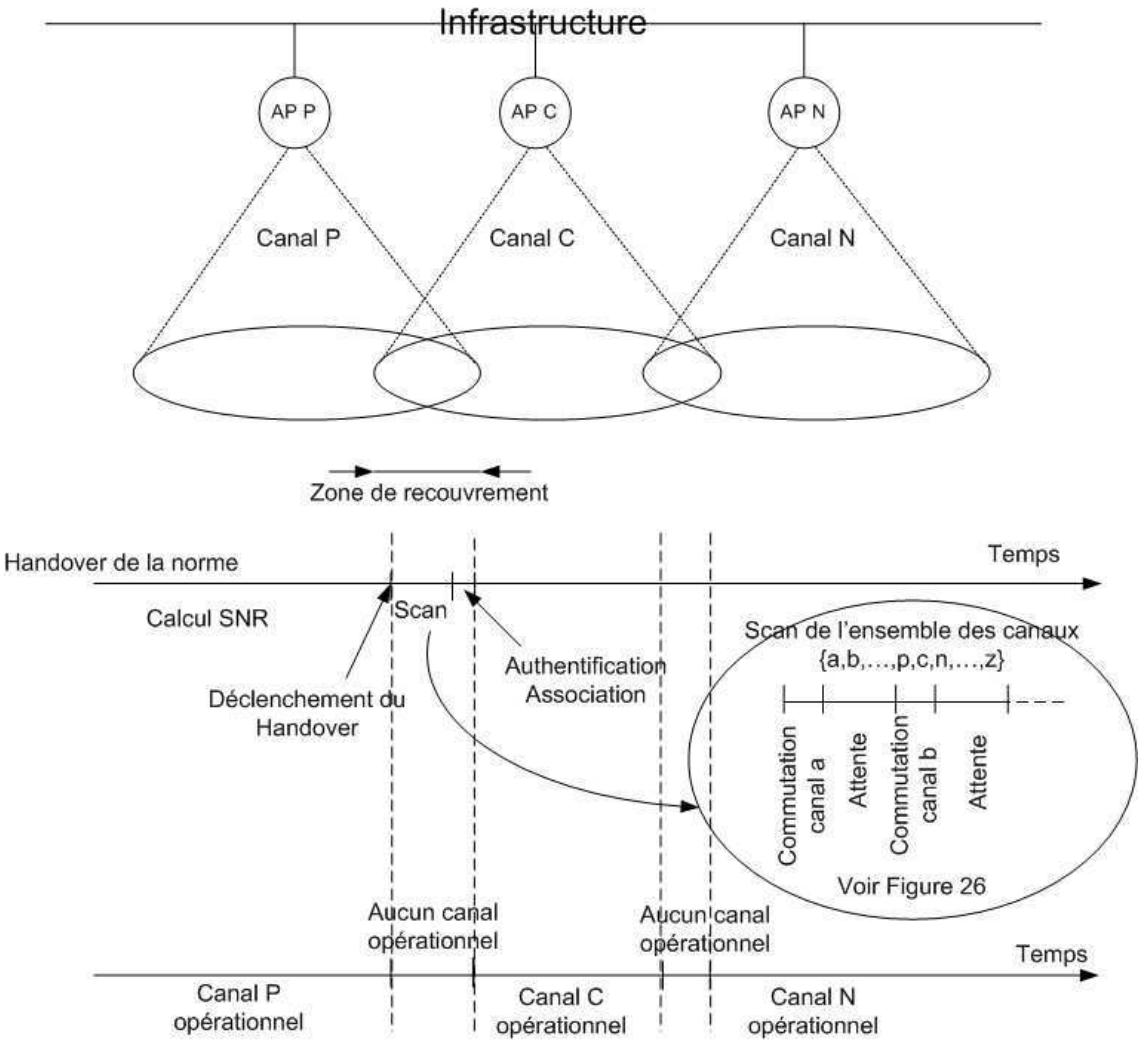


FIG. 27 – *Etapes d'un Handover en scan actif*

Le temps de la phase de Désauthentification est très faible, puisqu'il comprend uniquement l'envoi d'une trame "Deauthentication" entre la station et le point d'accès, suivie immédiatement de son acquittement qui est une trame prioritaire. De plus, tant que la

trame "Deauthentication" n'a pas été envoyée on considère que le handover n'est pas commencé, donc le temps que passe la station pour obtenir l'accès au médium ne fait pas partie du temps de handover. On peut également dire que cet échange rajoute peu de charge au réseau sans fil et a donc peu d'effet sur le trafic de la cellule quittée.

La phase de recherche d'un point d'accès est la plus coûteuse en temps. Elle peut être divisée en plusieurs sous-étapes. Chaque canal possible va être scruté, ce qui entraîne une commutation de canal, puis un temps d'attente sur ce canal. En scan actif, ce dernier temps est l'attente de trames Probe Response pouvant venir des points d'accès potentiels. On peut donc définir la formule suivante pour le temps de handover :

$T_{Handover} = k * (T_{Commutation} + T_{Attente}) + T_{Authentification} + T_{Association}$

Avec k le nombre de canaux scrutés (ceci dépend du paramètre ChannelList de la norme, par défaut k=13 en 802.11b), le temps d'attente est borné par les paramètres MinChannelTime et MaxChannelTime (ces 2 paramètres peuvent varier d'un modèle de carte à un autre, pour un modèle j'ai pu trouver comme valeurs par défaut 16ms pour MinChannelTime et 63ms pour MaxChannelTime).

La phase d'authentification permet une vérification d'identité d'une station. Selon la sécurité utilisée, ce processus peut être plus ou moins long. Dans un système non sécurisé, seules 2 trames Authentication seront échangées, avec leur acquittements 802.11. En utilisant un système sécurisé, par exemple WEP, plusieurs trames devront être échangées. Notre but étant de minimiser le trafic induit par le handover, nous nous plaçons dans le cas d'un système non sécurisé.

La phase d'association terminant le processus s'effectue par l'échange de deux trames (Association Request et Association Response), toutes deux acquittées. Le temps de cette phase comme celui de la précédente se limite au temps d'accès au médium, qui est dépendant du trafic dans la cellule car ces trames de gestions n'ont pas de priorités particulières, et du temps d'émission de ces trames. Par expérimentation, on peut évaluer à moins de 4ms le temps de ces deux dernières phases (voir figure 29) si il n'y pas de trafic dans la

cellule.

1.3 Le Handover dans le projet Waves.

Le projet Waves est un projet d'étude du comportement de mobiles pilotés par un réseau sans fil. Le projet est présenté de manière plus détaillée à la fin de cette partie de manuscrit. Le plateforme mise en oeuvre dans le cadre du projet servira de plateforme pour l'évaluation du handover et des propositions d'amélioration que nous apporterons.

Notre application est une application industrielle dans laquelle les mobiles, circulant sur une voie, ont une connaissance de leur position, de leur environnement et de la tâche/mission qu'ils ont à effectuer. Dans un tel contexte, le mobile peut connaître à l'avance le point d'accès qu'il devra rejoindre pour éviter le temps nécessaire à la phase de scrutation permettant de choisir le meilleur point d'accès, phase qui est la plus longue dans le processus de Handover. Les points d'accès devront réaliser une couverture cellulaire sur toute la zone où peuvent circuler les mobiles. Pour qu'il n'y ait pas de rupture de communications, il est nécessaire qu'il y ait une zone de recouvrement pour passer d'une cellule à l'autre. Pour le projet Waves, nous explorons l'intérêt d'un handover déclenché sur un critère applicatif : franchissement d'une balise ou constatation d'une surcharge d'un point d'accès (si l'objectif est de faire de l'équilibrage de charge). D'une façon générale, l'élément déclenchant sera appelé balise même quand il s'agit d'un "événement immatériel". Ces balises de déclenchement de handover doivent évidemment être dans une zone de recouvrement.

Le déclenchement du Handover au franchissement d'une balise consiste à forcer le changement de canal de la carte sans fil. Avec les paramètres par défaut de la norme, cette opération va provoquer l'envoi de la trame de Deauthentication. La station est par défaut en mode scan actif, elle envoie un Probe request sur les différents canaux et attend les Probe Response d'un AP potentiel. Les différentes étapes sont décrites sur la figure

27.

On distingue sur la figure 29 les différentes phases d'un Handover 802.11 classique. C'est une capture d'écran du logiciel Ethereal qui permet de capturer des trames sur un réseau. Les différentes colonnes qui apparaissent sont le numéro de la trame capturée, la station émettrice, la station réceptrice, le protocole réseau (ici 802.11) et le type de trame. Le processus commence par la phase de désauthentification (trames 3 et 4), puis vient la phase de scan (trames 5 à 48), ensuite nous trouvons la phase d'authentification (trames 49 et 50) et on termine par la phase d'association (trames 51 à 56). On voit bien sur cet exemple que la période de scan est de très loin la plus coûteuse en temps et en trafic.

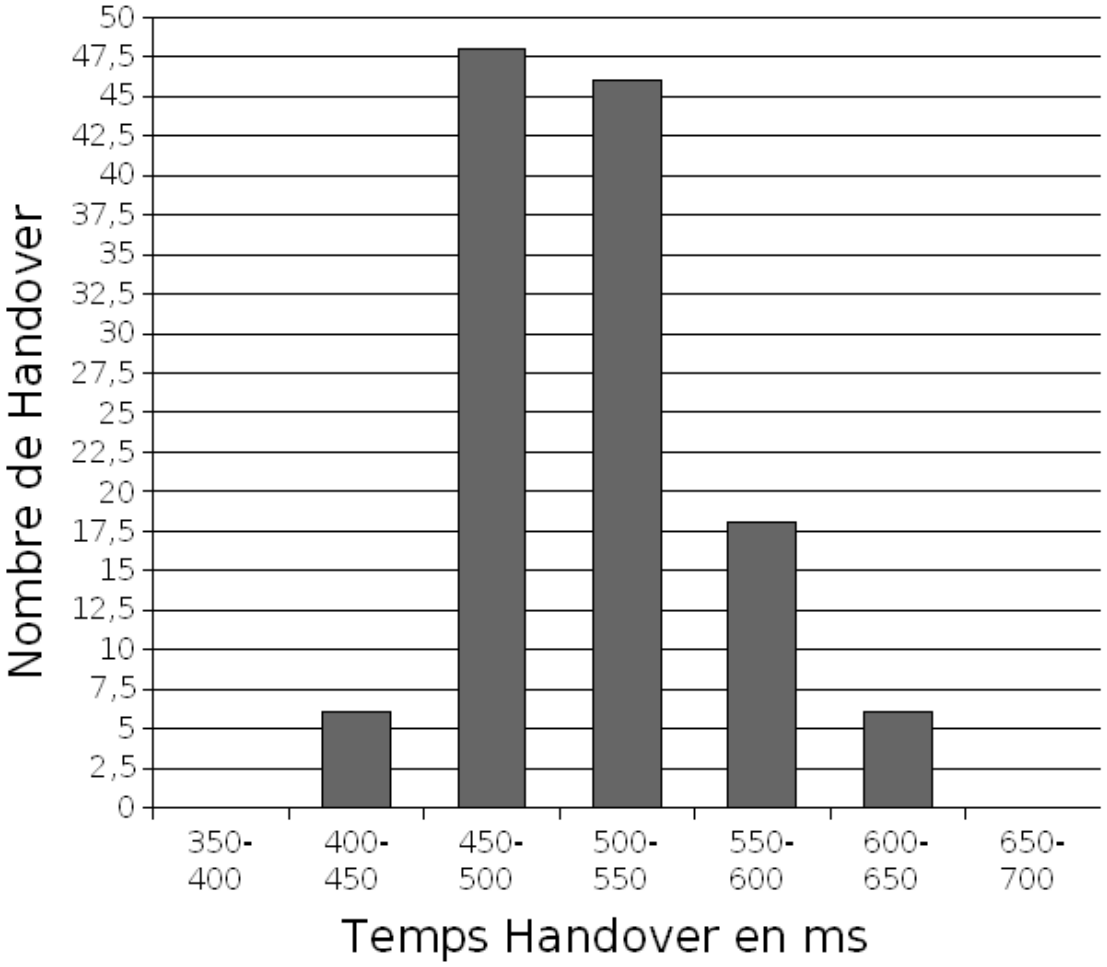


FIG. 28 – *Temps de Handover 802.11*

Le temps nécessaire est variable selon les conditions et le matériel utilisé. La figure 28 montre les résultats d'une série de mesure de temps de handover classiques 802.11, les mesures ont été réalisées avec des cartes Micronet 802.11b et Peabird 802.11b/g pour un temps moyen de handover de 520ms. On peut voir combien de handover ont été obtenu pour chaque tranche de temps.

Pendant le temps du handover, la station n'est affiliée nulle part et ne peut donc pas communiquer avec un élément de l'infrastructure. Au niveau applicatif, elle n'est pas joignable pendant un temps légèrement supérieur. On constate que les améliorations en modifiant les paramètres par défaut de la norme proposés dans [50] sont efficaces puisqu'ils obtiennent un temps de scan environ 4 fois inférieur. Mais leurs résultats sont obtenus par simulation des communications réseaux, alors que nous travaillons sur une plateforme où les communications réseaux se font réellement. Et nous ne pouvons malheureusement pas évaluer l'influence de ces modifications car il n'est pas possible avec le driver dont nous disposons de modifier les paramètres MinChannelTime et MaxChannelTime.

Selon le type d'application, ce temps où la station n'est pas joignable peut avoir des conséquences néfastes. Nous allons donc chercher à améliorer ce mécanisme aussi bien au niveau du temps nécessaire que du traffic généré. Dans le chapitre suivant, nous allons présenter une étude bibliographique des solutions existantes pour mieux gérer et optimiser le handover.

1	0.000000	Trend_b5:1e:f6	Broadcast	IEEE 802.11	Beacon frame
2	0.027153	BromaxCo_32:5d:45	Broadcast	IEEE 802.11	Beacon frame
3	*REF*	BromaxCo_32:5d:a7	Trend_b5:1e:f6	IEEE 802.11	Deauthentication
4	0.000256		BromaxCo_32:5d:a7 (RA)	IEEE 802.11	Acknowledgement
5	0.062824	BromaxCo_32:5d:a7	Broadcast	IEEE 802.11	Probe Request
6	0.063383	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
7	0.064582	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
8	0.065457	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
9	0.068736	BromaxCo_32:5d:45 (TA)	BromaxCo_32:5d:a7 (RA)	IEEE 802.11	Request-to-send
10	0.072150	Trend_b5:1e:f6	Broadcast	IEEE 802.11	Beacon frame
11	0.125419	BromaxCo_32:5d:a7	Broadcast	IEEE 802.11	Probe Request
12	0.126517	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
13	0.126791		BromaxCo_32:5d:45 (RA)	IEEE 802.11	Acknowledgement
14	0.174562	Trend_b5:1e:f6	Broadcast	IEEE 802.11	Beacon frame
15	0.187921	BromaxCo_32:5d:a7	Broadcast	IEEE 802.11	Probe Request
16	0.188780	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
17	0.189051		BromaxCo_32:5d:45 (RA)	IEEE 802.11	Acknowledgement
18	0.201762	BromaxCo_32:5d:45	Broadcast	IEEE 802.11	Beacon frame
19	0.267668	BromaxCo_32:5d:a7	Broadcast	IEEE 802.11	Probe Request
20	0.284106	BromaxCo_32:5d:a7	Broadcast	IEEE 802.11	Probe Request
21	0.284788	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
22	0.303837	BromaxCo_32:5d:45	Broadcast	IEEE 802.11	Beacon frame
23	0.347542	BromaxCo_32:5d:a7	Broadcast	IEEE 802.11	Probe Request
24	0.364779	BromaxCo_32:5d:a7	Broadcast	IEEE 802.11	Probe Request
25	0.365391	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
26	0.365658		BromaxCo_32:5d:45 (RA)	IEEE 802.11	Acknowledgement
27	0.379382	Trend_b5:1e:f6	Broadcast	IEEE 802.11	Beacon frame
28	0.406328	BromaxCo_32:5d:45	Broadcast	IEEE 802.11	Beacon frame
29	0.427987	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
30	0.429997	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
31	0.432373	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
32	0.434419	BromaxCo_32:5d:45 (TA)	BromaxCo_32:5d:a7 (RA)	IEEE 802.11	Request-to-send
33	0.439895	BromaxCo_32:5d:45 (TA)	BromaxCo_32:5d:a7 (RA)	IEEE 802.11	Request-to-send
34	0.481795	Trend_b5:1e:f6	Broadcast	IEEE 802.11	Beacon frame
35	0.490806	BromaxCo_32:5d:a7	Broadcast	IEEE 802.11	Probe Request
36	0.508078	BromaxCo_32:5d:a7	Broadcast	IEEE 802.11	Probe Request
37	0.508568	BromaxCo_32:5d:45	Broadcast	IEEE 802.11	Beacon frame
38	0.509208	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
39	0.509468		BromaxCo_32:5d:45 (RA)	IEEE 802.11	Acknowledgement
40	0.510789	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
41	0.511055		BromaxCo_32:5d:45 (RA)	IEEE 802.11	Acknowledgement
42	0.570126	BromaxCo_32:5d:a7	Broadcast	IEEE 802.11	Probe Request
43	0.570766	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
44	0.571972	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Probe Response
45	0.572241		BromaxCo_32:5d:45 (RA)	IEEE 802.11	Acknowledgement
46	0.584195	Trend_b5:1e:f6	Broadcast	IEEE 802.11	Beacon frame
47	0.611025	BromaxCo_32:5d:45	Broadcast	IEEE 802.11	Beacon frame
48	0.670041		BromaxCo_32:5d:a7 (RA)	IEEE 802.11	Acknowledgement
49	0.670876	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Authentication
50	0.671156		BromaxCo_32:5d:45 (RA)	IEEE 802.11	Acknowledgement
51	0.671604	BromaxCo_32:5d:a7 (TA)	BromaxCo_32:5d:45 (RA)	IEEE 802.11	Request-to-send
52	0.671871		BromaxCo_32:5d:a7 (RA)	IEEE 802.11	Clear-to-send
53	0.672259	BromaxCo_32:5d:a7	BromaxCo_32:5d:45	IEEE 802.11	Association Request
54	0.672544		BromaxCo_32:5d:a7 (RA)	IEEE 802.11	Acknowledgement
55	0.673131	BromaxCo_32:5d:45	BromaxCo_32:5d:a7	IEEE 802.11	Association Response
56	0.673412		BromaxCo_32:5d:45 (RA)	IEEE 802.11	Acknowledgement
57	0.686613	Trend_b5:1e:f6	Broadcast	IEEE 802.11	Beacon frame

FIG. 29 – *Capture des trames échangées pendant le handover*

Chapitre 2

État de l'art pour l'optimisation du Handover de 802.11

Sommaire

2.1 Solutions en exploitant les paramètres de la norme 78

2.1.1 ChannelList 78

2.1.2 MinChannelTime et MaxChannelTime 78

2.1.3 Envoi de données pendant le Handover 80

2.1.4 Réduction de la période de scan par réseaux de capteurs . . 80

2.2 Optimisation du handover au niveau IP 81

2.3 Gestion du Handover Inter-AP 83

2.3.1 IAPP : Inter Access Point Protocol 83

2.3.2 Tap-Dance 85

L'optimisation du Handover est un problème qui se pose pour tous types de réseaux sans fil avec une couverture cellulaire. Le but est de passer d'une cellule à l'autre sans perdre la connexion avec l'infrastructure ou de réduire le temps de perte de connexion de manière à ce qu'il ne perturbe pas la communication (en téléphonie par exemple on souhaite que l'utilisateur ne détecte pas une interruption dans le flux audio). Dans cette

partie, nous allons présenter plusieurs solutions existantes dans le cas des réseaux qui nous intéresse, c'est à dire 802.11.

2.1 Solutions en exploitant les paramètres de la norme

Parmi les différentes phase du handover, celle qui est la plus coûteuse en temps et également en trafic est la phase de recherche d'un nouveau point d'accès, le scan. Ceci a été démontré dans de nombreux travaux, le plus célèbre est le travail de Mishra, Shin et Arbaugh [37]. Dans cet article, ils proposent une étude très détaillée du processus de handover dans laquelle ils donnent des mesures pour chacune des phases de ce phénomène. Pour cette raison, beaucoup des travaux proposant une optimisation du handover traitent de l'amélioration de la phase de scan.

2.1.1 ChannelList

Ce paramètre définit la liste des canaux scrutés par une station lorsqu'elle recherche un point d'accès auquel s'affilier, aussi bien en scan actif qu'en scan passif. Il est possible de réduire le nombre de canaux scrutés si on a connaissance de la configuration de l'infrastructure à laquelle on essaye de se connecter. Par exemple, les couvertures cellulaires 802.11b utilisent généralement les trois canaux indépendants 1, 6 et 11. On peut réduire la recherche à ces 3 canaux aux lieu des 13 possibles, ce qui réduit considérablement le temps de scan.

2.1.2 MinChannelTime et MaxChannelTime

MinChannelTime définit un temps minimum pendant lequel une station va rester sur un canal donné et attendre des trames de gestions (beacon, probe response) d'éventuels points d'accès. Ce temps doit être assez long pour ne pas manquer ces trames.

Ce paramètre devra respecter la formule suivante : MinChannelTime $\geq$ DIFS + CW* aSlotTime

Ce temps représente le temps maximum d'envoi d'une trame. Une fois ce temps écoulé, on devrait avoir reçu une réponse du point d'accès. Dans le cas contraire, soit il n'y a pas de point d'accès sur le canal, soit on aura détecté d'autres types de traffic en concurrence avec les trames de gestions attendues. Dans ce cas on attend jusqu'au temps MaxChannelTime.

L'unité de temps utilisée est notée : TU pour Time Unit. La valeur d'1 TU est de 1024 μsecondes. Les valeurs des différents délais MinChannelTime, MaxChannelTime sont exprimées en TU. La valeur d'un temps DIFS est généralement de 50 μsec, CW représente la fenêtre de contention qui sera tirée aléatoirement entre 0 et CWmin, c'est à dire dans l'intervalle]0,32[. La valeur maximum sera donc de 31 slots de temps, dont la valeur aSlotTime est égale à 20 μsec.

D'après la formule ci-dessus, on peut donc déduire que MinChannelTime devra être supérieur à 670 μsec. Cette valeur n'est pas possible puisqu'on utilise TU comme unité, on arrondit donc à 1 TU.

Il n'y a pas de formule pour évaluer MaxChanneltime. Il doit aussi être assez court pour ne pas perdre de temps sur un canal trop encombré.

Dans [50], les auteurs ont fixé MinChanelTime à 1ms et suite à leurs expérimentations, ils ont jugé qu'une valeur de 10ms pour MaxChannelTime était efficace. Il ont pris pour paramètres, le nombre de stations dans une cellule, la charge en traffic et le nombre de canaux sur lesquels fonctionnent des points d'accès. Leur résultats sont obtenus par simulation du standard 802.11b. Ceci leur permet d'obtenir un temps de scan total, pour 13 canaux utilisés mais sans aucune charge de trafic, égal à 160ms. Dans une étude préalable réalisée avec différents modèles de cartes sans fil 802.11b, ils ont constaté que les temps de scan peuvent être très différents selon les constructeurs (87ms à 288ms).

2.1.3 Envoi de données pendant le Handover

Dans [30], Gonzalez, Perez et Zarate proposent une nouvelle méthode pour mesurer le temps de handover dans les réseaux 802.11. Leur but est de mieux séparer les phases du handover. Pour cela, ils se sont rendu compte qu'il était possible pour une carte réseau d'envoyer des trames de données pendant le handover, plus précisément entre la fin de la phase de scan et le début de la phase d'authentification ou entre la fin de l'authentification et le début de la phase d'association. En capturant l'intégralité des trames de gestion et de données pendant cette période, ceci leur permet d'évaluer plus précisément le temps de toutes les phases du handover. On peut envisager d'utiliser cette faille dans le fonctionnement des cartes 802.11 pour perdre moins de temps dans l'envoi de trames de données.

2.1.4 Réduction de la période de scan par réseaux de capteurs

La période de recherche de points d'accès (scan) est la plus coûteuse dans le mécanisme de handover. Sonia Waharte, Kevin Ritzenthaler et Raouf Boutaba proposent une solution pour optimiser cette recherche [51]. Leur solution est basée sur l'utilisation de capteur fonctionnant en 802.11, disposés dans les cellules et espacés de 50 à 150 mètres comme le montre la figure 30.

Ces capteurs ont pour rôle d'écouter le réseau et grâce aux beacons envoyés par les différents points d'accès, chaque capteur va être capable d'identifier les points d'accès environnants. Quand un mobile de notre réseau devra changer de cellule, il va commencer par une opération de pre-scan qui consiste à envoyer une requête d'interrogation aux capteurs. Les capteurs ayant reçus cette requête répondent en envoyant la liste des point d'accès qu'ils ont pu identifier. Chaque capteur répond en utilisant une fenêtre de contention calculée grâce à la puissance du signal de la requête. De cette manière, les capteurs les plus proches du mobile, qui doivent avoir la liste de points d'accès la plus significative pour ce mobile, répondront les premiers. Les réponses obtenues permettront au mobile d'avoir

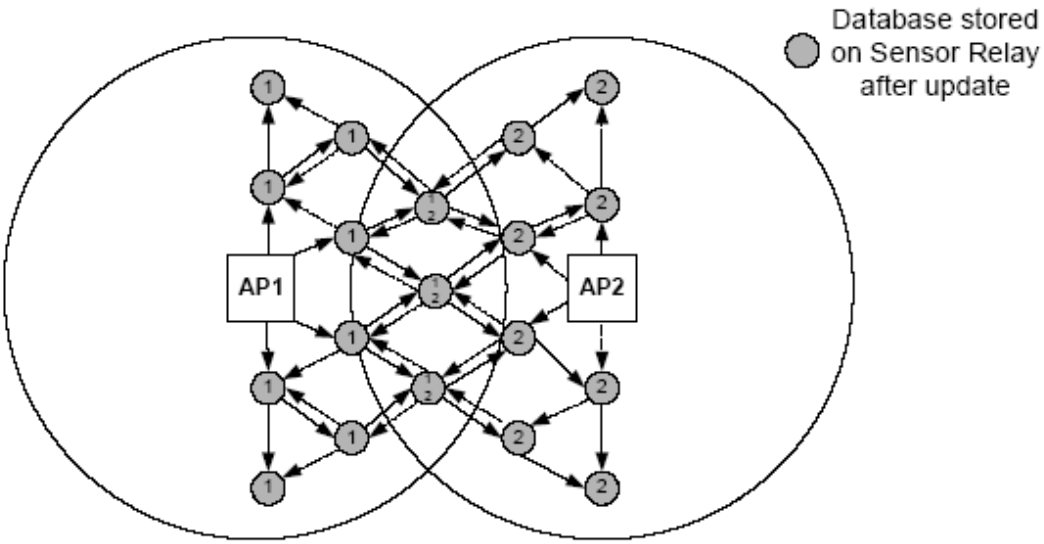


FIG. 30 – *Réseau de capteurs (source [51])*

une liste de points d'accès potentiels avec des informations telles que le BSSID (adresse MAC du point d'accès), le canal utilisé, la puissance du signal. Il effectuera ensuite le scan classique de 802.11 mais en se limitant aux canaux des points d'accès potentiels. La figure 31 présente ce mécanisme de handover.

2.2 Optimisation du handover au niveau IP

Les solutions précédentes traitent du handover au niveau 2. Dans le cas d'un réseau IP, il est possible que les points d'accès appartiennent à des réseaux IP différents. Pour qu'un mobile changeant de réseau puisse rester en contact avec d'autres machines en étant toujours identifié de la même manière, il est nécessaire d'utiliser le protocole "mobile IP", proposé par l'IETF (Internet Engineering Task Force) [33]. Avec ce protocole les noeuds mobiles doivent être identifiés par un agent, ce qui permet de localiser dans quel réseau se trouve le mobile. Lorsqu'un handover est effectué, les informations concernant le mobile doivent être modifiées au niveau de l'agent pour permettre la continuité d'une

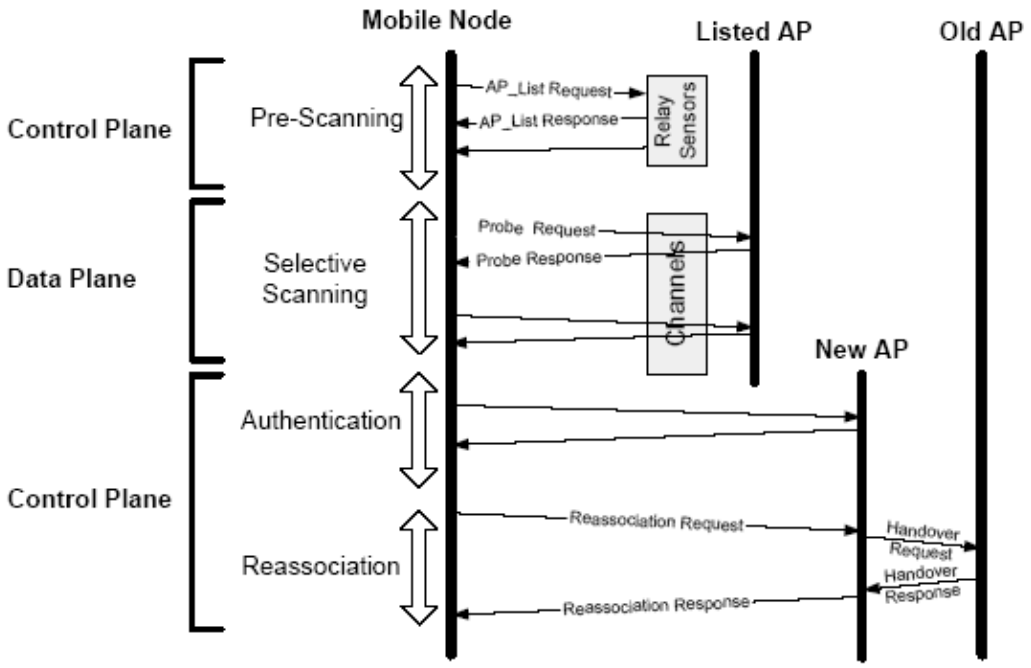


FIG. 31 – *Handover par interrogation de capteurs (source [51])*

communication. Ce mécanisme doit être optimisé pour que la rupture de communication soit la plus faible possible.

Nicolas Montavont et Thomas Noel proposent une solution d'optimisation du handover au niveau IP par anticipation des déplacements [39][38].

Quand le mobile effectue un handover, certains paquets qui lui sont destinés peuvent être perdus. Tandjaoui [47] propose une solution permettant de stocker les paquets destinés au mobile durant la période où il n'est plus accessible.

Le temps du handover de niveau 3 est au minimum égal au temps de handover de niveau 2.

2.3 Gestion du Handover Inter-AP

Nous avons vu jusqu'à présent la gestion du changement de cellule dans un réseau 802.11 au niveau des échanges entre la station et les point d'accès, c'est à dire comment une station indique qu'elle quitte une cellule et comment elle cherche un nouveau point d'accès et s'y affilie. Quand une station mobile est en train d'effectuer un transfert de données avec une autre station mobile ou une entité de l'infrastructure, les trames sont relayées à cette station par le point d'accès auquel elle est affiliée. Quand un handover est effectué, le point d'accès servant de relais va changer et rien n'est prévu dans la norme pour effectuer un "suivi" du parcours de la station. Ceci peut avoir pour conséquence des retards ou pertes de trames de données, ce qui peut être gênant par exemple dans le cas d'une utilisation de téléphonie sur Wifi par exemple. Dans ce chapitre, nous allons aborder des solutions qui apportent des fonctionnalités au niveau de l'infrastructure du réseau pour assister la gestion du handover 802.11. Le problème peut être traité à différents niveaux, le niveau 2 (MAC) si les stations et les point d'accès sont dans le même réseau, le niveau 3 (IP) si les stations sont dans un réseau différent. Dans notre étude, nous nous placerons plutôt dans le cas de stations à l'intérieur d'un même réseau local. Pour remédier à ce problème, des solutions ont été proposées pour améliorer la gestion du handover au niveau des point d'accès. Ces solutions sont souvent propriétaires, elles sont donc implémentées seulement sur les produits du constructeur qui la propose. Nous allons voir la solution Tap-Dance qui est un protocole propriétaire proposé par le constructeur ATMEL et le protocole IAPP proposé par l'IEEE.

2.3.1 IAPP : Inter Access Point Protocol

Ce protocole est défini dans une extension de la norme 802.11, 802.11f [11] qui a été ratifiée en juillet 2003. L'IAPP est un protocole de communication permettant l'interopérabilité entre des point d'accès appartenant au même système de distribution. Il utilise

les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) sur IP pour échanger les paquets du protocole IAPP entre les point d'accès.

Il a deux fonctions principales :

- l'association unique d'un client à un réseau (ESS Extended Service Set). Il permet la vérification qu'un seul utilisateur est connecté au réseau sous une identité donnée. IAPP peut exploiter un serveur RADIUS (Remote Authentification Dial In User Service) [19] pour gérer l'authentification des stations.
- l'échange proactif du contexte d'une station effectuant un handover aux point d'accès voisins, ce qui a pour but de réduire le temps de latence lors de la nouvelle association.

On peut distinguer 3 familles d'évènements :

- ADD : Il se produit quand un point d'accès reçoit une trame Association Request. Un envoi de trame contenant l'adresse MAC de la station va être effectué sur l'infrastructure, ce qui va permettre la mise à jour des tables des éléments réseaux de niveaux 2 se trouvant sur l'infrastructure (par exemple les Switchs qui doivent mettre à jour leur tables d'adresses MAC), ce qui leur permettra de commuter les trames dans la direction du nouveau point d'accès alors qu'en temps normal, cette mise à jour n'aurait été effectuée qu'après le premier envoi de trame de la station.
- MOVE : Il se produit quand un point d'accès reçoit une trame Reassociation Request. Une station va utiliser ce type de trame plutôt que l'Association Request quand elle a déjà été affiliée à un autre point d'accès du même ESS. La trame Reassociation Request a pour avantage d'inclure un champs "Point d'accès courant" qui permet d'indiquer au point d'accès auquel on est en train de s'affilier et quel point d'accès on quitte. Les deux points d'accès vont alors pouvoir échanger le context de cette station. Un exemple de contenu du contexte peut être les informations concernant l'authentification de la station ce qui permettra une phase d'authentification plus rapide.

– CACHE : Le principe est pour un point d'accès de transmettre le contexte d'une station aux points d'accès auxquels il est possible qu'elle s'affilie quand elle quittera sa cellule, ces point d'accès sont appelés voisins. Pour cela, grâce aux différents échanges de trames, les points d'accès vont maintenir un graphe qui définit une sorte de topologie de l'infrastructure en référençant les points d'accès voisins qui les entourent.

IAPP, implémenté sur tous les points d'accès d'une infrastructure, permet d'effectuer un handover sans rupture de communications (Seamless Handover). Il a l'inconvénient de fonctionner seulement au niveau 2, c'est à dire dans un même ESS et dans une même classe d'adresse IP. Au niveau 3 la solution la plus couramment utilisée est "Mobile IP" [20]. Voyons maintenant une solution permettant d'améliorer les performances de mobile IP.

2.3.2 Tap-Dance

Tap-Dance est une solution propriétaire proposée par ATMEL [23]. Cette solution a pour but d'améliorer les performances du handover par rapport aux performances obtenues avec mobile IP qui ne sont pas satisfaisantes pour des applications avec contraintes de temps. Il est basé sur le principe d'IAPP mais à un niveau supérieur puisqu'IAPP fonctionne sur un même réseau IP. Le but de Tap-Dance est de pouvoir garder une connexion quelque soit le réseau traversé pendant le déplacement d'un mobile.

La figure 32 montre les temps de handovers obtenus par ATMEL en mettant en oeuvre la solution Tap-Dance. Les tests ont été effectués sur un réseau local dans des conditions "normales" d'utilisation. Ils montrent le temps de handover au niveau IP obtenus en effectuant 150 changement de cellules.

On observe que peu de handovers dépassent les 30ms avec un maximum de 38ms. Ces temps sont très intéressants en particulier pour des applications à fortes contraintes temporelles par exemple la voix sur IP. Malheureusement, du fait que cette solution est

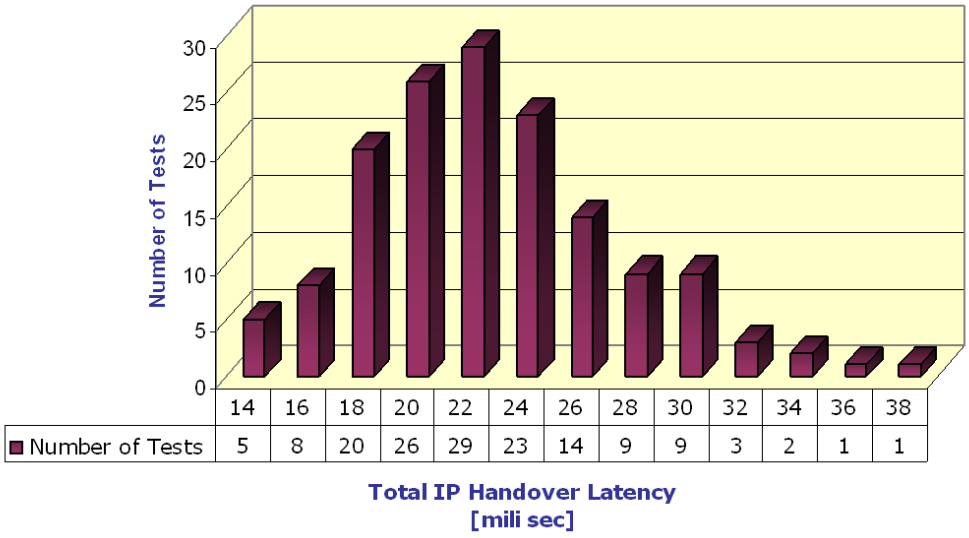


FIG. 32 – *Temps de Handover au niveau IP*

propriétaire, nous n'avons pas accès aux détails du fonctionnement de ce protocole. Il nous est donc impossible de savoir ce qui est mis en oeuvre pour obtenir des résultats si satisfaisants.

Chapitre 3

Le projet Waves

Sommaire

3.1 Application Générique 88

3.1.1 Hypothèses sur le trafic 89

3.1.2 Notion de voisinage 91

3.2 Choix d'un pseudo PCF pour les échanges intra-cellulaires 92

3.3 Première plateforme du projet Waves 92

3.4 Résultats concernant le trafic intracellulaire 93

3.4.1 Nature du trafic intracellulaire 93

3.4.2 Rappel sur le pseudo PCF 94

3.4.3 Choix d'une stratégie de mise à jour cyclique 95

3.4.4 Etude des différentes stratégies de diffusion 95

3.4.5 Conditions Expérimentales de la comparaison 99

3.4.6 Résultats de la comparaison des stratégies 100

3.4.7 Calibrage du simulateur 101

3.4.8 Influence d'un trafic applicatif 102

Le problème de l'optimisation du handover est une composante du projet WAVES (Wifi for Automated guided VehiclES). Ce projet a été initié fin 2002 au sein de l'équipe

Réseaux et Protocoles du LIMOS (Laboratoire d'Informatique, de Modelisation et d'Optimisation des systèmes. Il concerne l'évaluation des solutions IEEE 802.11b, 802.11a ou 802.11g pour des applications utilisant des mobiles coopérants guidés (AGV pour *Automated Guided Vehicles*) dont les trajectoires sont modélisables. Ces mobiles peuvent être à priori nombreux (plusieurs dizaines par cellule) et éventuellement groupés puisqu'ils sont censés collaborer. L'application générique qui sert de support à ce projet est une flotte de mobiles chargée de transporter des marchandises, leur coopération se limite essentiellement à la connaissance de leur position et de leur vitesse pour assurer une circulation sans collision.

Ce chapitre présente le projet Waves dans sa globalité, les contraintes temporelles, les choix d'implémentation ainsi que la stratégie utilisée pour que les mobiles coopèrent de la meilleure façon possible. Les contraintes de temps seront importantes pour évaluer les conséquences d'un changement de cellule sur cette application.

3.1 Application Générique

Cette application générique est représentative d'une classe d'applications industrielles utilisant des robots mobiles. Les représentants de cette classe diffèrent principalement dans le comportement individuel des mobiles, dans la mission globale qu'ils réalisent et dans leur façon de coopérer. Sur ce dernier point, nous allons considérer que les robots coopérants sont des robots voisins qui exploitent la mise à jour périodique de variables élémentaires indiquant leur état, notamment, leur position et leur vitesse. Cette connaissance qu'ils partagent par l'usage est utilisée pour déterminer leur comportement lors de missions élémentaires du type transport de fret. La figure 33 illustre une plateforme représentant l'application qui nous intéresse. Notre centre d'intérêt étant dans les communications réseau, nous utiliserons un réseau sans fil réel pour les échanges entre mobiles alors que les déplacement des mobiles seront simulés. Nous avons fait ce choix car nous tenions

à ce que les échanges réseaux soit réellement effectués, de manière à avoir des résultats significatifs. Par contre les mobiles sont simulés car il nous est impossible de disposer d'une flotte de mobile réels assez importante.

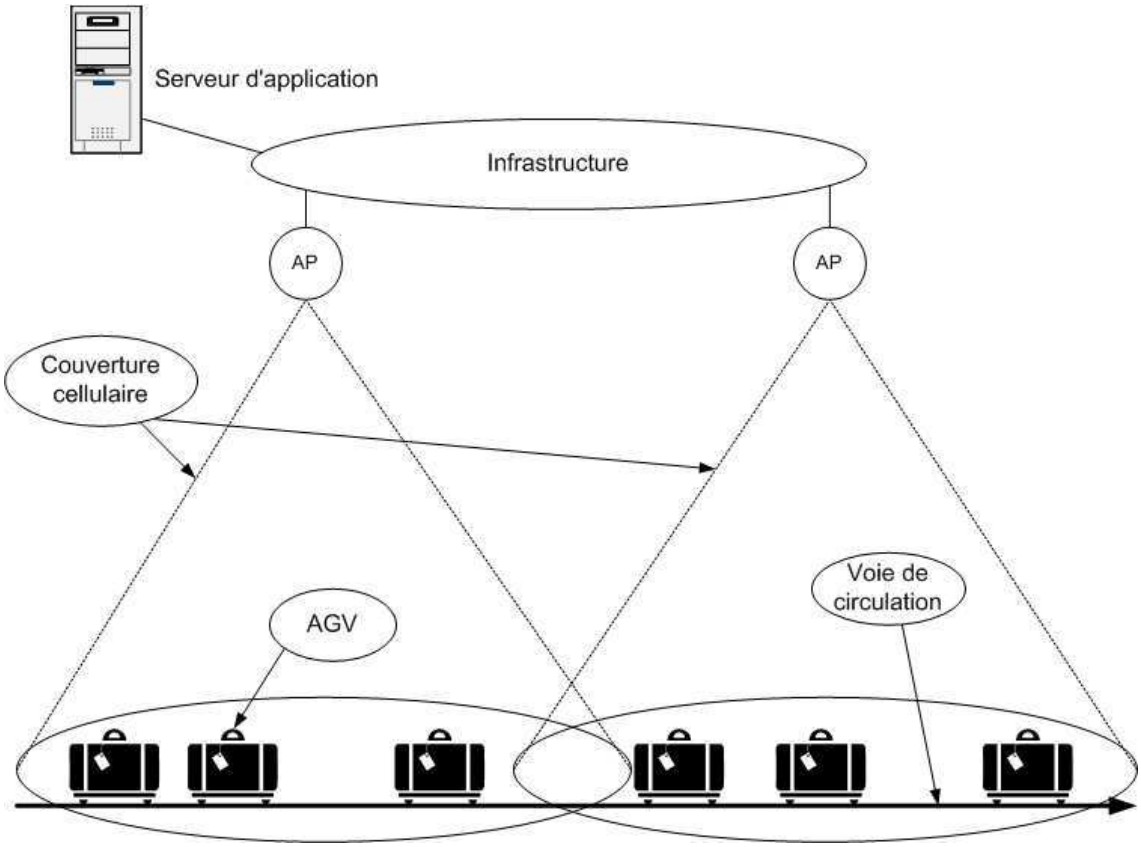


FIG. 33 – *Application générique*

3.1.1 Hypothèses sur le trafic

Cette classe d'applications industrielles génère trois types de trafic (voir figure 34) que nous pouvons désigner par trafic applicatif, trafic de coopération et trafic local.

Le trafic applicatif est composé de tous les échanges d'informations entre les organes de supervision de l'application et les acteurs que sont les robots mobiles. Les missions décidées au niveau de la supervision, transmises aux exécutants (les mobiles) constituent une partie de ce trafic.

Le trafic de coopération ou trafic inter-mobiles, donne la capacité à chaque mobile d'échanger avec les mobiles avec lesquels il coopère, des variables élémentaires telles que sa position, son état, sa vitesse. Pour ce type de trafic, nous visons un comportement du réseau sans fil le plus proche possible de celui d'un bus de terrain, car dans le cadre d'un travail coopératif, la fréquence des échanges de données et la stabilité de cette fréquence sont des paramètres fondamentaux pour l'implémentation des algorithmes d'asservissement entre mobiles. L'usage de 802.11b en DCF, qui exploite des délais de longueur aléatoire pour désigner, durant la phase de contention, celui qui a le droit d'accéder au médium, introduit malheureusement des retards variables dans les données destinées à alimenter les asservissements.

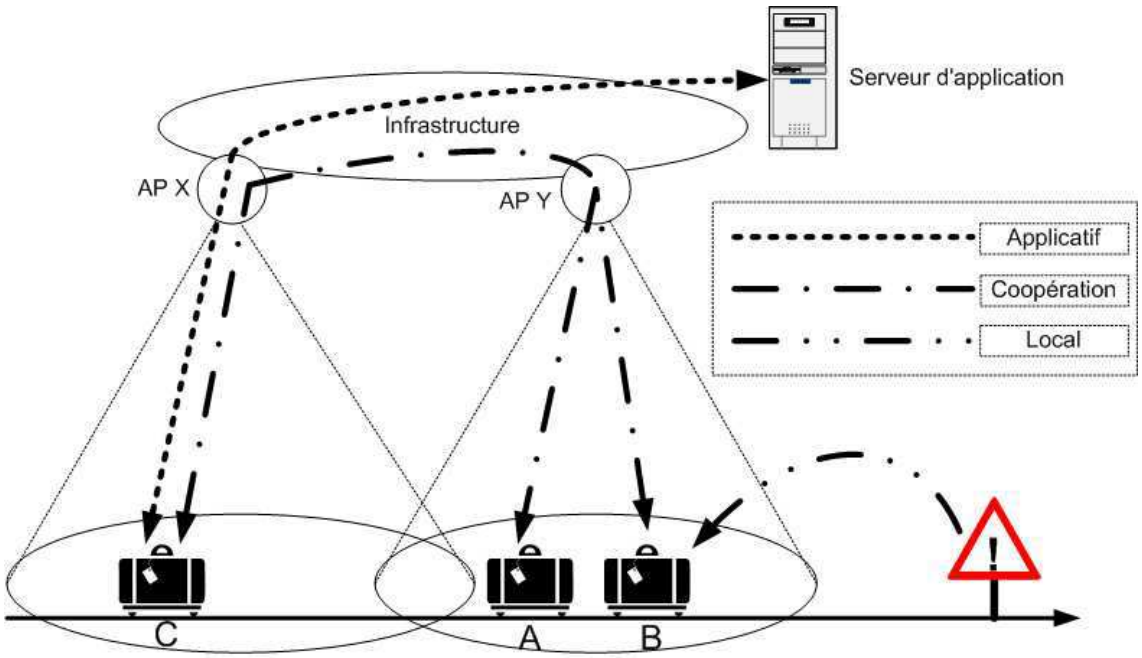


FIG. 34 – *Les différents types de trafic*

La démarche relative au projet Waves a pour but d'évaluer les caractéristiques temporelles de ce type d'échanges qui permettront à des mobiles voisins de coopérer. L'objectif est de caractériser la périodicité de la mise à jour de la connaissance nécessaire aux robots coopérants, et les écarts engendrés par la charge du réseau sur cette fréquence. Ces

résultats sont nécessaires aux concepteurs des tâches de coopération. Dans cette étude, les échanges seront réduits dans un premier temps aux variables nécessaires à la gestion de la bonne circulation de mobiles voisins.

Le trafic local correspond aux échanges de données faits le long des trajectoires, en des points particuliers du site entre un mobile et son environnement. Il peut s'agir de la prise de connaissance d'un panneau de circulation, de la génération d'un ordre d'ouverture de porte ou de commande d'aiguillage, etc. Dans une première approche, le volume de ces échanges ne sera pas pris en compte dans l'évaluation des performances.

3.1.2 Notion de voisinage

Dans la figure 34, le mobile du milieu (A) a deux voisins très proches :

- l'un devant lui et dans la même cellule (B)
- l'autre derrière lui et encore dans la cellule mitoyenne (C), dans ce cas, nous parlerons alors de voisins étrangers car ils dépendent d'autres Points d'Accès (AP).

Ce mobile doit donc échanger des informations avec :

- son voisin de devant, dans un réseau 802.11 avec infrastructure, ces échanges passent par le point d'accès qui leur est commun,
- mais aussi avec le voisin qui le suit (voisin étranger), dans ce cas les échanges doivent passer par l'infrastructure via les points d'accès X et Y des deux cellules mitoyennes. Si ces échanges ont la même finalité, ils n'auront pas les mêmes caractéristiques temporelles. [48]

3.2 Choix d'un pseudo PCF pour les échanges intracellulaires

Le choix d'une mise à jour pseudo périodique de variables d'états entre mobiles coopérants nous amène directement à faire jouer au point d'accès le rôle de contrôleur d'accès au médium dérivé du Polling Selecting. La norme 802.11 prévoit pour ce type d'application l'option PCF qui permet de donner un accès cyclique au canal à un lot de stations affiliées, mais cette option n'est implémentée par aucun des fournisseurs de drivers 802.11 que nous connaissons. L'idée d'émuler cette option PCF au-dessus de la couche MAC d'un driver DCF (option de base) n'est pas nouvelle [43]. Compte tenu du domaine applicatif, les échanges dans une cellule seront véritablement cadencés par le point d'accès.

3.3 Première plateforme du projet Waves

Une première plateforme (voir figure 35) a été mise en place pour évaluer les performances d'un trafic intracellulaire pour l'interrogation des mobiles [32].

Ne disposant pas d'une flotte de mobiles conséquente, toute la partie de notre étude concernant les informations de déplacement des mobiles et leurs voies de circulation sera simulée. Par contre la partie concernant les communications réseaux sera effectuée réellement. Le développement a été réalisé par Patrick Lafarguette dans le cadre de son stage d'ingénieur CNAM [34].

Le serveur d'application fait partie de l'infrastructure, il peut être chargé de la supervision des mobiles. Il pourra être utilisé pour communiquer à chaque mobile sa mission. Le point d'accès de la cellule gère la liste de mobiles affiliés et les interroge cycliquement (Pseudo PCF) de manière à diffuser à chaque mobile de sa cellule les informations concernant ses voisins (position, vitesse par exemple). Il sert également de relais entre les mobiles et l'infrastructure pour la transmission du trafic entre les mobiles et le serveur

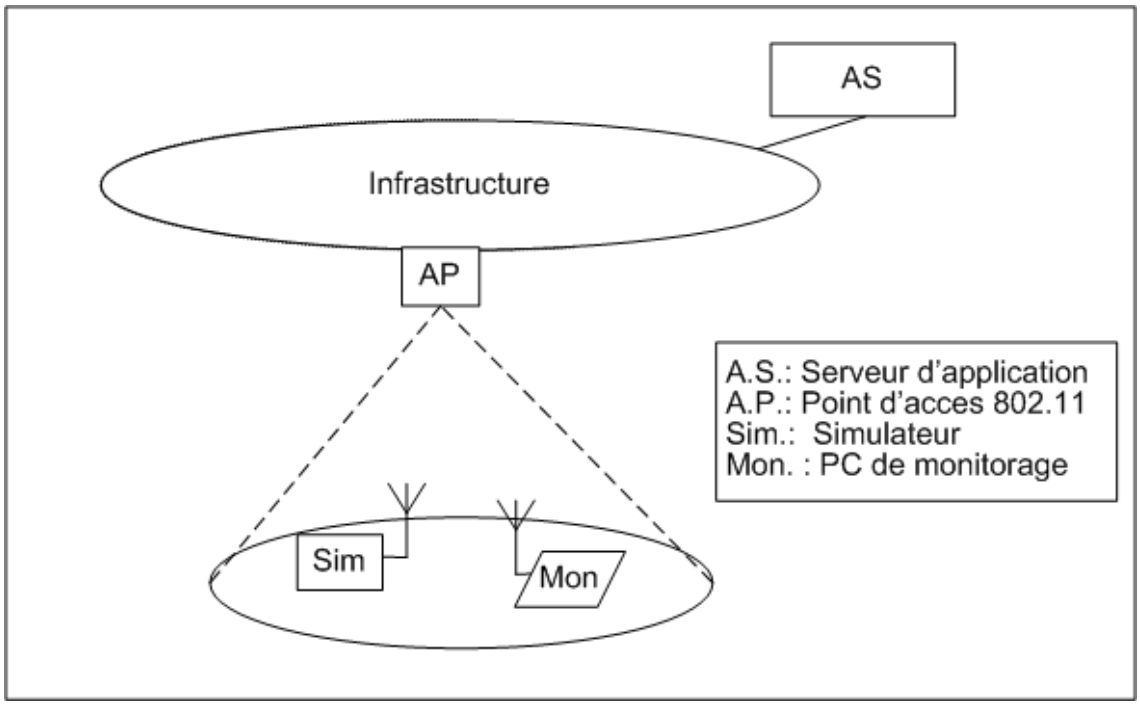


FIG. 35 – *Première plateforme pour le projet Waves*

d'application. Le simulateur représente les différents mobiles de la cellule, il connaît la trajectoire et calcule la position de chacun d'eux en tenant compte de la position et la vitesse de ses voisins. Il répond aux interrogations du point d'accès à la place de chacun des mobiles.

L'outil de monitorage sert à la supervision des échanges réalisés en radio dans la cellule. En utilisant le driver HostAP [7] on peut capter l'ensemble des trames radio échangées, y compris les trames de gestion 802.11.

3.4 Résultats concernant le trafic intracellulaire

3.4.1 Nature du trafic intracellulaire

La première version du simulateur nous permet de générer l'activité d'une flotte de mobiles se déplaçant dans une même cellule. Les premières mesures envisagées sont des-

tinées :

- au choix d'une stratégie de mise à jour cyclique des variables devant être partagées entre les mobiles voisins (trafic de coopération de la figure 34),
- au calibrage et à l'initialisation du simulateur pour la stratégie de mise à jour retenue,
- à l'évaluation des perturbations dues au trafic applicatif sur la périodicité de cette mise à jour.

3.4.2 Rappel sur le pseudo PCF

Quand il s'agit d'installer un réseau IEEE 802.11 ou 802.11b, les composants disponibles n'implémentent pas l'intégralité de la norme, seule la méthode d'accès DCF (Distribution Coordination Function) basée sur CSMA/CA est disponible. L'accès au médium radio est donc sujet à compétition de la part des stations qui souhaitent émettre une trame. Cela implique une faible possibilité de collision et par conséquent la ré-émission de trames, mais surtout cela ne permet pas d'envisager sans artifice un accès au médium pseudo périodique de la part des stations.

La partie de la norme IEEE 802.11 qui concerne la version réseau avec infrastructure que nous avons retenue propose en option une méthode d'accès garantissant une certaine périodicité aux échanges de trames, il s'agit du mode PCF (Point Coordination Function). Dans ce cas, le point d'accès alloue systématiquement un temps de parole aux stations qui le souhaitent. Chaque station dispose alors tour à tour du canal et peut émettre sans interférence. Cette option du standard IEEE 802.11 n'étant pas implémentée dans les pilotes des cartes disponibles, il a été décidé d'instaurer une gestion des cycles d'échange (un pseudo PCF), implémentée au dessus du niveau MAC.

3.4.3 Choix d'une stratégie de mise à jour cyclique

Notre objectif est de garantir un accès quasi périodique aux stations mobiles de la cellule qui le désirent. Le principe de gestion d'un pseudo PCF est relativement simple : le point d'accès stimule une des stations qui lui est affiliée. Cette station émet alors une trame de réponse destinée à la diffusion dans la cellule. Le point d'accès traite alors la station suivante de la liste des stations souhaitant un accès périodique. Le cycle se termine lorsque la dernière station de cette liste a répondu et que cette réponse a été diffusée. Ce fonctionnement permet au point d'accès de diriger le partage du médium dans sa cellule, en initiant les émissions de toutes les trames de données. De ce fait, le risque de collision dû au trafic des mobiles est quasiment nul car seule l'émission des trames de services (Probe et Beacon) n'est pas contrainte par cette forme de Polling Selecting.

3.4.4 Etude des différentes stratégies de diffusion

Il s'agit maintenant d'étudier comment les informations obtenues en réponse d'une sollicitation de l'AP vont être connues des stations voisines dans la cellule. Généralement, une trame émise par une station d'un réseau local peut être destinée à une adresse unique (Unicast), à une adresse représentant une classe de stations (Multicast), ou à l'ensemble des stations (Broadcast), dans ce dernier cas on parle de diffusion générale. La méthode la plus séduisante est d'utiliser cette diffusion pour communiquer immédiatement dans toute la cellule la réponse de chaque mobile. Ainsi, l'information la plus récente est immédiatement disponible pour toutes les stations de la cellule.

Adressage dédié ou Unicast : S'agissant de diffuser périodiquement l'information générée par les voisins d'une station, ce mode d'adressage est utilisable sous réserve de fournir à chaque stimulation d'une station, l'ensemble des réponses les plus récentes des autres stations. Ceci augmente notablement la quantité d'information à transmettre pour chaque cycle.

Diffusion générale ou Broadcast : La diffusion en mode infrastructure ne se fait pas de façon directe d'une station vers toutes les autres, mais en deux étapes, le Point d'Accès jouant le rôle d'intermédiaire :

- une trame diffusée par une station est placée dans une file d'attente par son Point d'Accès.
- ce Point d'Accès vide cette file en émettant les trames qu'elle contient, à la suite de chaque émission d'un " beacon ". Ce comportement est également valable pour le Multicast.

Ce fonctionnement décevant d'un point de vue temporel, découle de la possibilité de placer une station en mode "économie d'énergie". Dans ce mode, une station est en sommeil, périodiquement un beacon la réveille pour lui préciser si des trames en file d'attente lui sont destinées. Le même principe est employé pour les trames diffusées. En effet, une diffusion est destinée à être reçue par toutes les stations de la cellule, sans exception. C'est seulement après l'émission d'un beacon que toutes les stations sont à même d'effectuer cette réception. Il est donc évident que la diffusion sera pénalisante temporellement dans notre application car la réception des trames sera différée et soumise à la génération des beacons par le Point d'Accès. Une autre difficulté caractérisant la diffusion réside dans le fait que ces trames ne sont pas acquittées contrairement aux trames dédiées. Il n'existe donc pas de moyen simple de s'assurer de la bonne réception par l'ensemble des stations.

Sur la base de ce qui précède, nous avons décidé de tester quatre stratégies permettant une diffusion cyclique d'information :

	Interrogation par le Point d'Accès	Réponse de la Station
Trames	Broadcast	Broadcast
	Broadcast	Unicast
	Unicast	Broadcast
	Unicast	Unicast

Broadcast-Broadcast : Le Point d'Accès diffuse une trame contenant la liste des stations ordonnées, destinée à initier le cycle d'interrogation. Dès réception, la première station de cette liste diffuse sa réponse. Dès réception, la station suivante diffuse à son tour sa réponse et ainsi de suite jusqu'à la dernière station de cette liste. A réception de la réponse de la dernière station, le Point d'Accès recommence le processus. Si une station ne reçoit pas la réponse de la station précédente, le cycle est interrompu. Il est possible de mettre en place un mécanisme (basé sur la gestion d'une temporisation) pour remédier à ce problème, au prix d'une plus grande complexité.

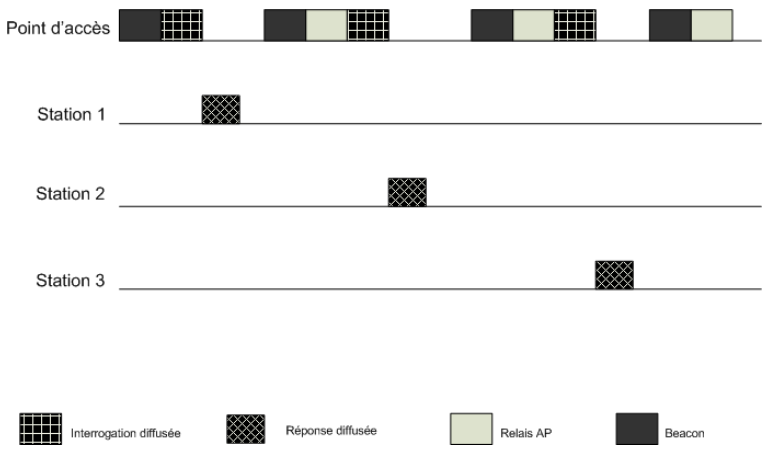


FIG. 36 – *Broadcast-Broadcast*

Broadcast-Unicast : Le point d'accès diffuse une trame qui contient la réponse de la station i et indique qu'il souhaite une réponse de la station j. Dès réception, la station j émet sa réponse destinée (Unicast) au point d'accès. A réception, le point d'accès traite la station suivante jusqu'à la fin du cycle et recommence.

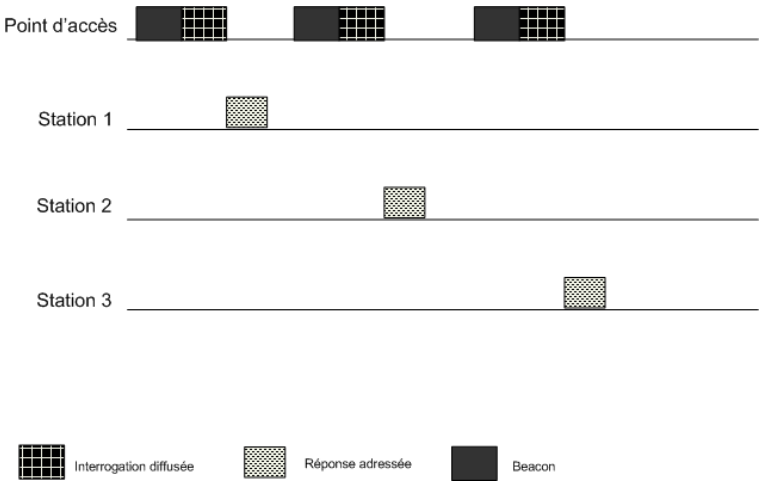


FIG. 37 – *Broadcast-Unicast*

Unicast-Broadcast : Le point d'accès adresse une trame d'interrogation à une station. Dès réception, la station diffuse sa réponse. A réception, le point d'accès traite la station suivante jusqu'à la fin du cycle et recommence. Les remarques faites sur le rôle du beacon dans la diffusion s'appliquent ici également.

Unicast-Unicast : Le point d'accès adresse une trame d'interrogation à la station i. Cette trame comporte les informations qu'il connaît des autres stations de sa cellule. Dès réception, la station i émet sa réponse au point d'accès. A réception, le point d'accès rafraîchit les informations qu'il connaît par celles de la station i et traite la station suivante jusqu'à la fin du cycle et recommence. L'avantage de cette stratégie est que chaque trame bénéficie pour son acheminement des dispositifs du standard tels que l'acquittement et la

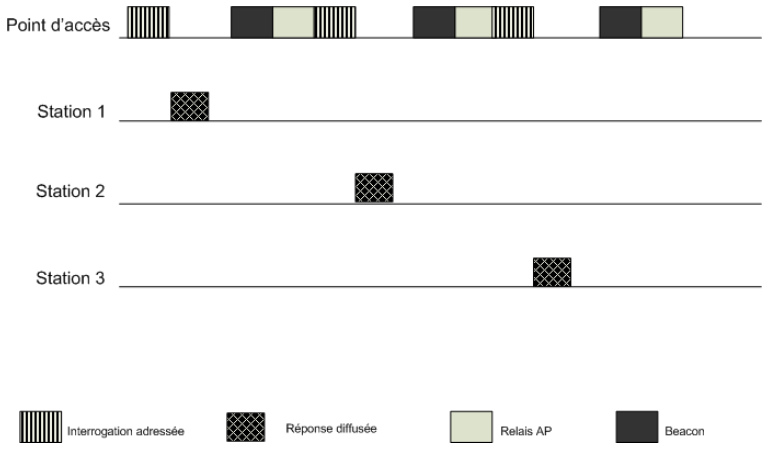


FIG. 38 – *Unicast-Broadcast*

ré-émission. L'inconvénient est l'augmentation du volume des informations à transmettre et le retard introduit par cette forme de diffusion.

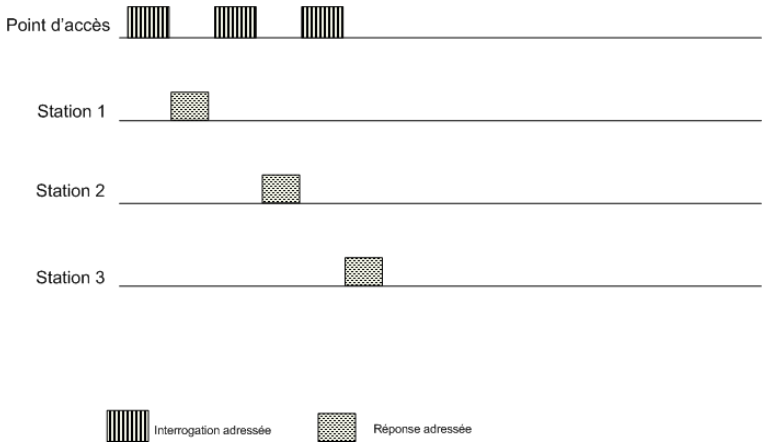


FIG. 39 – *Unicast-Unicast*

3.4.5 Conditions Expérimentales de la comparaison

Chacune des stratégies a été expérimentée dans des configurations comprenant un point d'accès, un moniteur et de une à quatre stations. Le point d'accès est un ordinateur

sous Linux équipé d'une carte 802.11b contenant le composant PRISM II. HostAP [7] est le pilote de la carte réseau, il offre la particularité d'exploiter le mode Soft AP des composants PRISM, de manière à faire fonctionner la carte en point d'accès. Le moniteur est un ordinateur équipé de manière similaire, qui exploite une autre particularité de la carte et du pilote. Un mode de " monitorage " est implémenté qui, couplé au logiciel Ethereal, permet de capturer une image des trames émises sur un canal et d'analyser ces trames. Le logiciel reconnaît les différents types de trames du standard 802.11. Il est ainsi possible de visualiser les trames de gestion (beacons, probes) et les trames de données (trafic applicatif). Ces captures sont enregistrées dans un fichier qui, après une étape de transformation, est importé dans Excel pour l'analyse finale. Les stations sont des ordinateurs équipés du même type de cartes et du même pilote. Les cartes sont toutefois configurées en mode "managed". Pour comparer les différentes stratégies, la même quantité d'information a été échangée pour chaque station soit 48 octets correspondants à un trafic de coopération plausible correspondant à la configuration de la figure 34.

3.4.6 Résultats de la comparaison des stratégies

Les résultats des expérimentations sont synthétisés dans la figure 40 et détaillés dans [34].

L'interprétation de ces résultats nous indique clairement que la stratégie la plus performante est l'Unicast-Unicast. Il apparaît donc qu'augmenter la taille des trames générées par le point d'accès n'est pas très pénalisant. Prasad et Munõz [44] ont montré que le coût temporel de l'émission d'une trame 802.11 est fortement lié à l'encapsulation des données (délai d'accès au canal évalué à 310 μs en moyenne, préambule émis à 1 Mbit/s en 192 μs). Dans ces conditions, il est évident qu'émettre deux trames de N octets dure plus longtemps que d'émettre une seule trame de 2*N octets. Broadcast-Broadcast et Broadcast-Unicast ont quasiment les mêmes performances et celles-ci sont liées au délai qui sépare l'émission de deux beacons, qui est par défaut de 102,4 millisecondes. Les résultats de la stratégie

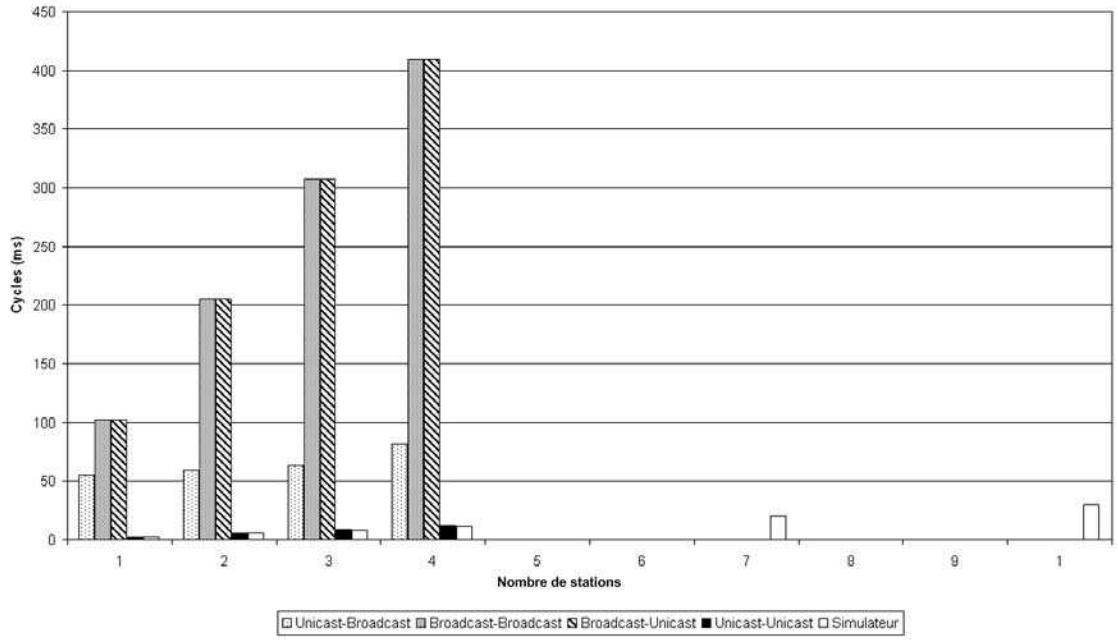


FIG. 40 – *Résultats obtenus par le simulateur et avec des stations réelles*

Unicast-Broadcast sont intermédiaires mais se dégradent sensiblement en terme d'écart type de la durée du cycle dès que le nombre de stations dépasse trois.

3.4.7 Calibrage du simulateur

La stratégie retenue pour la diffusion périodique à l'intérieur de la cellule est donc l'Unicast-Unicast. Il s'agit ici de comparer pour cette stratégie les performances obtenues avec N stations mobiles réelles à celles obtenues quand le simulateur se charge de répondre au nom de N stations simulées. Ceci représente l'étape de calibrage du simulateur. Le Moniteur permet de capturer les trames émises sur un canal et d'en déduire la longueur d'un cycle. Le simulateur a été utilisé pour obtenir les résultats correspondants à l'usage de 1, 2, 3 et 4 stations mobiles. Ces résultats sont très proches de ceux obtenus en utilisant de 1 à 4 stations mobiles réelles, les graphes qui leurs correspondant sont confondues sur la figure 40. Les points pour 7 et 10 mobiles ont été obtenus par simulation uniquement.

3.4.8 Influence d'un trafic applicatif

Dans le projet, il est prévu que les stations reçoivent des informations autres que celles venant des trames d'interrogation du point d'accès. Ces informations peuvent être par exemple la mission que la station mobile doit effectuer. Ce trafic est beaucoup moins fréquent que le trafic d'interrogation, nous avons fait une hypothèse de 2 trames par secondes pour chaque mobile. Dans [31], nous montrons que pour 20 mobiles dans une cellule, le trafic applicatif a peu d'influence sur les cycles d'interrogation. Dans le cas d'un envoi plus important de données venant de l'infrastructure, une solution est proposée par Philippe Llamas [35]. Sa solution est une modification du driver HostAP pour bloquer tout le trafic venant de l'infrastructure et l'intégrer au corps des trames d'interrogation cyclique en utilisant la notion de container : un pour le traffic coopératif et l'autre pour le traffic applicatif quand il existe.

La problématique du handover étant posée, nous allons proposer dans la partie suivante des solutions pour améliorer le processus de handover, dans le cadre une application à trafic contraint par le temps, telle que celle décrite dans le projet Waves.

Troisième partie

Propositions et Résultats

Chapitre 1

Solutions proposées

Sommaire

1.1 Suppression du scan 105

1.2 Solution avec deux cartes sans fil sur la même station . . 107

1.2.1 Présentation 107

1.2.2 Le problème ARP 110

1.3 Solution par sockets de niveau 2 112

1.4 Handover par l'infrastructure 114

1.5 Gestion de la continuité d'une transmission 118

1.1 Suppression du scan

Le mode utilisé par défaut dans 802.11 est un scan automatique, c'est-à-dire que c'est la station qui gère le choix de son AP destination. On a vu précédemment les effets induits par ce mode de fonctionnement.

Dans notre application, les trajectoires des mobiles et la topologie du réseau sont fixes et connus. On sait donc quand une station va quitter une cellule et dans laquelle elle va se rendre (c'est à dire le point d'accès auquel elle va devoir s'affilier)

Une première façon d'optimiser le temps de Handover va donc être la suppression de la phase de recherche du point d'accès puisqu'on est capable de le déterminer par l'application. Ceci est possible grâce à l'utilisation d'un mode de scan dit "manuel". En fait il n'y aura pas de scan effectué par la station, il est activé en donnant la valeur 2 au paramètre host-roaming du driver hostap). Dans ce mode, le handover n'est décidé ni par le point d'accès ni par la station, on le déclenche au niveau applicatif avec une commande dans laquelle on va spécifier l'identifiant du réseau (SSID), le canal sur lequel fonctionne le point d'accès de la cellule d'accueil et pour finir le BSSID c'est à dire l'adresse MAC du point d'accès. Pour cela, on peut utiliser les Wireless Tools [25], qui proposent les commandes *iwconfig* et *iwpriv* qui permettent la gestion des interfaces sans fil d'un PC sous Linux, *iwconfig* permet de modifier les paramètres généraux (ESSID, canal de communication, mode utilisé), *iwpriv* permet de modifier des paramètres plus fins au niveau du driver (par exemple le délai inter-beacon).

Exemple iwconfig wlan0 channel 11 essid Waves ap 00 :60 :1D :01 :23 :45.

Le fait de donner ces informations en paramètres, nous permet d'être sûr que c'est le point d'accès qui a l'adresse MAC spécifiée, auquel la station va s'affilier (si bien sûr il existe et est à notre portée).

La figure 41 permet de visualiser le fonctionnement d'un handover manuel. Le handover est déclenché dans la zone de recouvrement. Puisque le scan est "manuel" il n'y a pas de phase de recherche d'un nouveau point d'accès, la phase de scan se limite donc à la commutation sur le canal voulu. La figure 42 répertorie les trames qui seront échangées en utilisant le mode scanning manuel.

Il n'est pas possible de réduire plus le nombre de trames échangées lors d'un handover si on utilise des cartes respectant le standard 802.11.

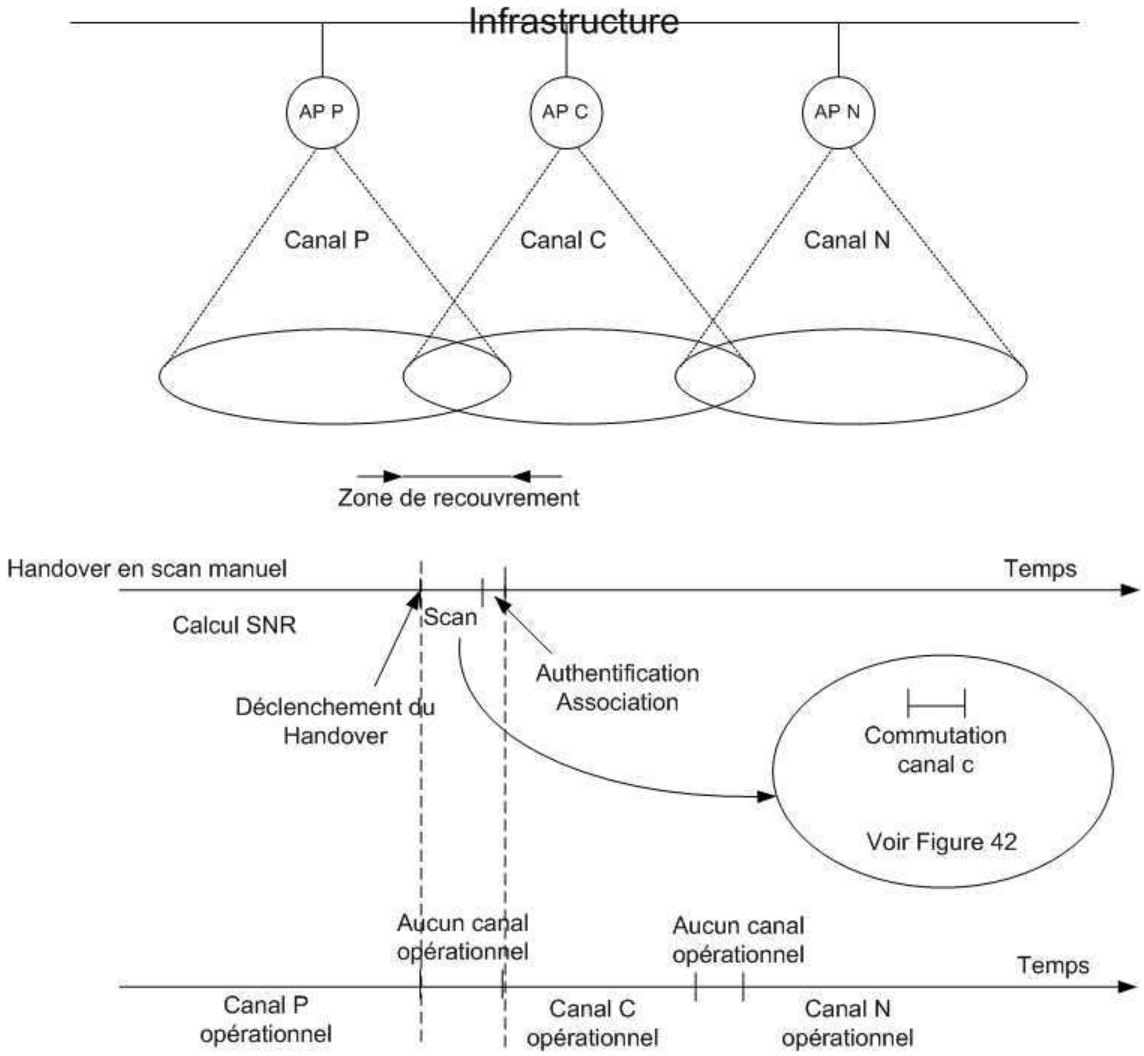


FIG. 41 – *Etapes d'un Handover en scan manuel*

1.2 Solution avec deux cartes sans fil sur la même station

1.2.1 Présentation

Il est évident que même si on optimise au maximum le temps de handover, il ne sera jamais nul car il faut assurer au minimum une commutation de canal. La station va forcément être inaccessible pendant un certain temps pour les autres entités du réseau.

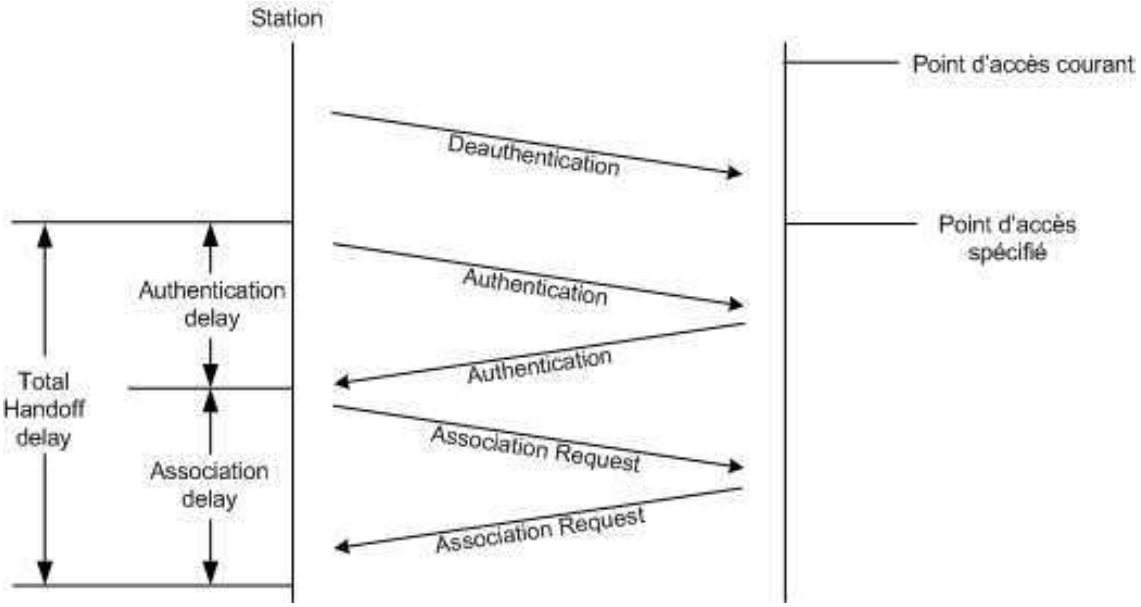


FIG. 42 – *Trames échangées lors d'un handover sans phase de scan*

Nous proposons donc l'installation d'une deuxième interface réseau sans fil sur les stations, de manière à supprimer la phase durant laquelle le mobile n'est affilié à aucun point d'accès. Nous avons à faire à un scénario de commutation de carte avec échange de rôles.

Dans la cellule, la première carte, dite active, est utilisée pour interroger le mobile. Quand une balise de déclenchement du Handover est rencontrée, on déclenche l'affiliation de la carte additionnelle au point d'accès cible, dont les caractéristiques ont pu être récupérées par exemple par la lecture de cette balise sur la voie. Une fois la station affiliée à ce nouveau point d'accès, elle peut être interrogée. On peut alors déclencher la désaffiliation (puis la mise en veille) de la première carte, la carte additionnelle devient alors la carte active (voir figure 43).

Avantages de cette solution :

– Elle permet à la station d'être interrogée de manière permanente ce qui est important dans une application où plusieurs mobiles doivent coopérer et risquent d'entrer en collision.

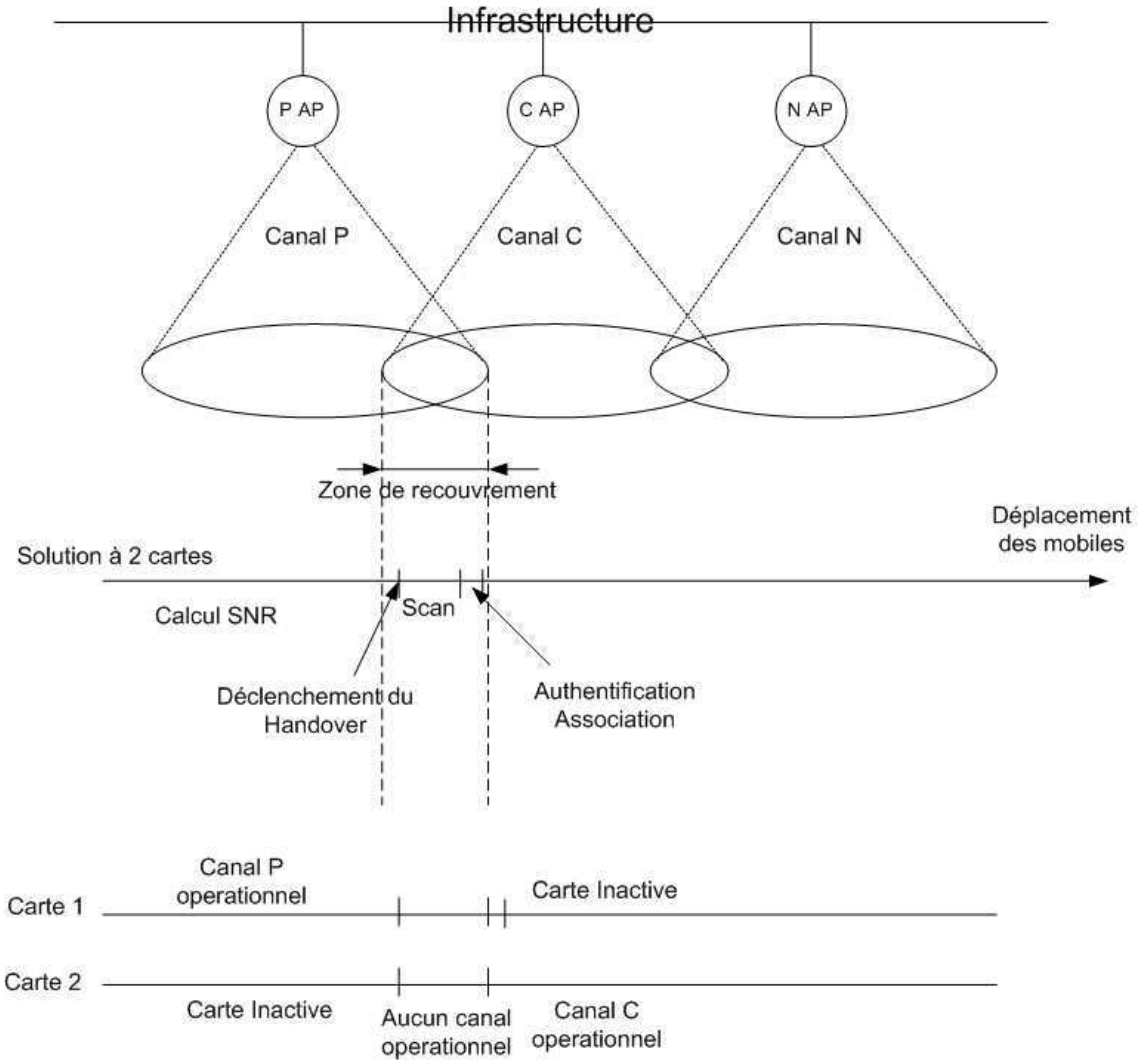


FIG. 43 – *Handover avec 2 cartes embarquées*

– Elle doit permettre d'éviter la perte de trames applicatives, par exemple un fichier mission provenant d'un serveur d'application.

Inconvénients :

– Elle n'apporte rien au niveau du nombre de trames échangées pour effectuer le handover.
– Quand la station est affiliée à 2 point d'accès simultanément, elle peut recevoir des informations concernant certains de ses voisins par ces deux points d'accès. Selon le

taux de rafraîchissement des informations dans les AP, il est possible qu'il y ait des incohérences dans les informations reçues. Il faut donc faire en sorte de ne prendre en compte que l'information la plus récente, par exemple en datant les informations ce qui nécessite une synchronisation des stations.

– Jusqu'à présent, nous avons fait le choix d'une application compatible IP. Chaque mobile est donc identifié de manière unique grâce à une adresse IP. Si on veut garder une continuité dans un transfert (par exemple un échange FTP entre la station et un serveur sur l'infrastructure), il faut donner aux deux cartes embarquées la même adresse IP, par contre chaque carte a une adresse physique(MAC), fixée par le constructeur. Cette adresse est codée sur 48 bits dont 24 sont un identifiant unique pour le constructeur, et les 24 autres sont attribués de manière séquentielle aux cartes produites. Ces adresses sont donc normalement uniques dans le monde. Chaque mobile a donc une seule adresse IP mais 2 adresses MAC, ce qui pose problème car en communication IP dans un réseau local Ethernet, l'adresse IP est évidemment utilisée mais on doit aussi préciser l'adresse MAC du destinataire dans l'en-tête de la trame, c'est ce qui permet à une carte réseau de détecter si une trame capturée sur le réseau lui est destinée ou non. Si l'adresse MAC dans la trame est identique à la sienne, elle traite la trame et la transmet aux couches protocolaires supérieures, sinon elles est ignorée.

1.2.2 Le problème ARP

Le fait d'avoir une seule adresses IP pour identifier deux cartes va provoquer l'envoi de requête ARP (Address Resolution Protocol) [1]. Ce protocole fait partie de TCP/IP, il est utilisé pour récupérer l'adresse MAC d'une station à partir de son adresse IP. Toutes les stations utilisant ARP vont garder en mémoire une table qui contient les couples (adresse IP, adresse MAC) obtenus grâce au protocole ARP, cette table est appelée cache ARP.

L'algorithme de fonctionnement du protocole est le suivant :

Alg. 2 Protocole ARP

```
1: Réception d'un paquet dans le module ARP
2: Si l'adresse IP destination est contenu dans le cache Alors
3:     Utiliser l'adresse MAC correspondante ;
4: Sinon
5:     Envoyer une requête ARP
6:     Attendre la réponse
7:     Réception de la Réponse ARP
8:     Utiliser l'adresse MAC reçue
9:     Mettre à jour le cache ARP
10: Fin Si
```

Les requêtes ARP sont des trames particulières qui vont contenir quatre champs d'adresses, l'adresse IP et l'adresse MAC de la station émettant la requête, et l'adresse IP du destinataire. Le dernier champs doit correspondre à l'adresse MAC du destinataire, qui est l'inconnue au moment de l'envoi de la requête. L'adresse contenue dans le champ est alors une adresse MAC de diffusion (FF-FF-FF-FF-FF-FF) pour que toutes les stations du réseau traitent la requête.

Ces requêtes ARP constituent un trafic indésirable puisqu'elles vont s'intercaler avec nos trames d'interrogations cycliques. De plus, elles sont diffusées et nous avons pu observer que les trames diffusées ne sont envoyées dans une cellule qu'après l'envoi d'une trame "Beacon" de manière à ce que les éventuelles stations en mode économie d'énergie passent en mode normal et puissent recevoir la trame. Ceci provoquerait donc un retard dans l'envoi de trames à la station en question.

Il faut également noter que les réponses obtenues par ARP sont stockées dans le cache de manière provisoire. Le délai est assez long pour qu'il ne soit pas nécessaire de renvoyer des requêtes ARP si on envoie de nombreuses trames consécutives à une même station. Mais ce délai ne doit pas être trop long pour éviter des incohérences si par exemple

on change la carte réseau d'un PC, dans ce cas l'adresse MAC changera puisqu'elle est contenue dans le matériel mais l'adresse IP restera souvent la même.

Une solution possible pour remédier à ce problème serait de manipuler le cache ARP de manière statique : ce qui est relativement simple au niveau de la station effectuant le handover mais plus difficile au niveau d'un serveur d'application car il faut lui faire remonter l'information quand le Handover est effectué. Tant qu'il n'a pas effectuée la mise à jour les trames qu'il enverra à la station seront perdues.

Avec les systèmes d'exploitations que nous utilisons (Linux ou Windows), il est possible de "tromper" une carte réseau en lui affectant une autre adresse MAC. Pour résoudre notre problème, il est envisageable de travailler avec un cache ARP statique, pour toutes les stations du réseau (qu'elles soient mobiles ou fixes sur l'infrastructure), dans lequel on mettrait pour chaque mobile une adresse IP et l'adresse MAC de la première carte. Cette adresse MAC sera ensuite affectée à la 2ème carte de manière à avoir une adresse MAC identique pour les deux cartes. Les 2 cartes réseaux ayant la même adresse IP et la même adresse MAC, toutes les stations du réseau ayant cette information de manière statique dans leur cache ARP, on ne devrait plus avoir de requêtes ARP sur notre réseau.

1.3 Solution par sockets de niveau 2

Une autre solution possible pour éviter le problème ARP serait de ne plus utiliser le protocole IP et de traiter toutes les communications au niveau inférieur, c'est à dire au niveau liaison de données (couche 2 du modèle OSI). C'est alors les adresses MAC qui seraient utilisées pour identifier les mobiles de manière unique.

Au niveau applicatif, cela implique l'utilisation de socket de niveau 2, appelée socket RAW. Ces sockets permettent de passer outre la manière dont un système gère les paquets TCP/IP. Il n'y a plus de traitement du paquet, au lieu de traverser les différentes couches traditionnelles (par encapsulation ou decapsulation) de la pile protocolaire TCP/IP, le

paquet sera transmis directement à l'application qui le traite. Ce type de paquet est appelé paquet RAW. C'est à l'application qui va recevoir le paquet d'effectuer toutes les opérations nécessaires sur ce dernier.

Cet outil permet de créer des paquets respectant des protocoles existants comme Ethernet ou IP. Il suffit pour cela de créer des structures conformes aux entêtes de ces protocoles et de les positionner en début d'un buffer (mémoire tampon) qui sera ensuite envoyé par la socket, le contenu de ce buffer est donc le contenu de notre paquet. Les sockets RAW sont habituellement utilisées pour implémenter de nouveaux protocoles, pour développer des applications de gestion de réseaux, par exemple un logiciel d'analyse de réseau ou encore pour faire du tunneling et passer au travers d'un firewall.

Pour notre application, l'utilisation de sockets RAW peut nous permettre de supprimer le problème d'envoi de requêtes ARP. Pour cela, il faut utiliser une structure respectant le format de l'entête 802.11. Le reste de l'espace mémoire disponible dans le buffer d'envoi servira à l'envoi de données appllicatives, dans notre cas cela pourra être les informations concernant les mobiles

Avantages :

- Le fait d'éviter la pile de protocole TCP/IP permet un léger gain de temps pour l'envoi de trames et le traitement de trames reçues. Des tests d'interrogation cycliques réalisées dans les même conditions que celles présentées par Patrick Lafarguette [34] ont donné des résultats entre 52 et 56 ms avec des sockets de niveau 2 (pour 20 stations avec des trames de 800 octets dans le sens AP $\rightarrow$ station et 40 dans le sens station $\rightarrow$ AP) contre 60 ms pour des sockets TCP/IP.
- On peut également utiliser une solution à deux cartes comme vu dans la section précédente. Comme au niveau IP, il faudra donner aux deux cartes la même adresse MAC pour qu'il n'y ait pas de coupure lors d'un transfert initié dans la cellule courante et devant se terminer dans la nouvelle cellule.

Inconvénients :

- Cette solution nécessiterait de passer toutes nos applications, développées en utilisant des sockets UDP, au niveau 2
- Il n'y a toujours pas de gain au niveau des trames de gestion du handover.
- Il y a une possibilité de duplication de trames. Il faut prévoir une gestion de ce type de problème au niveau applicatif.

1.4 Handover par l'infrastructure

Les problèmes d'identification des stations pour permettre la continuité des transmissions étant traités, il reste un point à aborder : la suppression de toutes les trames échangées lors d'un Handover.

Ceci est rendu possible par l'utilisation du mode monitor et des sockets RAW. Le mode monitor est un mode passif, on l'utilise généralement pour effectuer des captures de trames sur un réseau. Une carte en mode monitor n'est pas utilisable par des protocoles classiques (TCP/IP par exemple). En revanche il est possible d'envoyer des trames en utilisant les sockets RAW comme dans le point précédent.

Pour une communication au niveau 2, en langage C on va créer la socket grâce à la commande socket(PF_PACKET, SOCK_RAW, htons(ETH_P_ALL)) dont les paramètres sont :

- SOCK_RAW signifie qu'on utilise des sockets RAW, c'est à dire qu'on va éviter le traitement des trames par les piles protocolaires classiques comme TCP/IP, elles seront ainsi traitées par nous même au niveau des applications,
- AF_PACKET est le sous-type utilisé,
- ET_P_ALL signifie que les trames seront reconnues comme des trames ethernet.

Pour envoyer ces trames en mode monitor, il faut identifier la carte réseau souhaitée par son index au niveau du système. Comme on court-circuite les piles protocolaires, il

va donc être nécessaire de construire nous même la trame, c'est à dire ajouter en début de trames les informations de l'en-tête Ethernet dans notre cas. Le reste de la trame contiendra les informations relatives à l'application comme celles de coopération entre les stations, les missions provenant des serveurs d'applications dans notre cas.

Dans ce mode on constate, qu'il n'y a plus d'envoi de trames de gestion (Deauthentication, Association Request/Response, Authentication Request/Response) lors du Handover. L'idée de base du Handover par l'infrastructure peut être résumée par la figure 44.

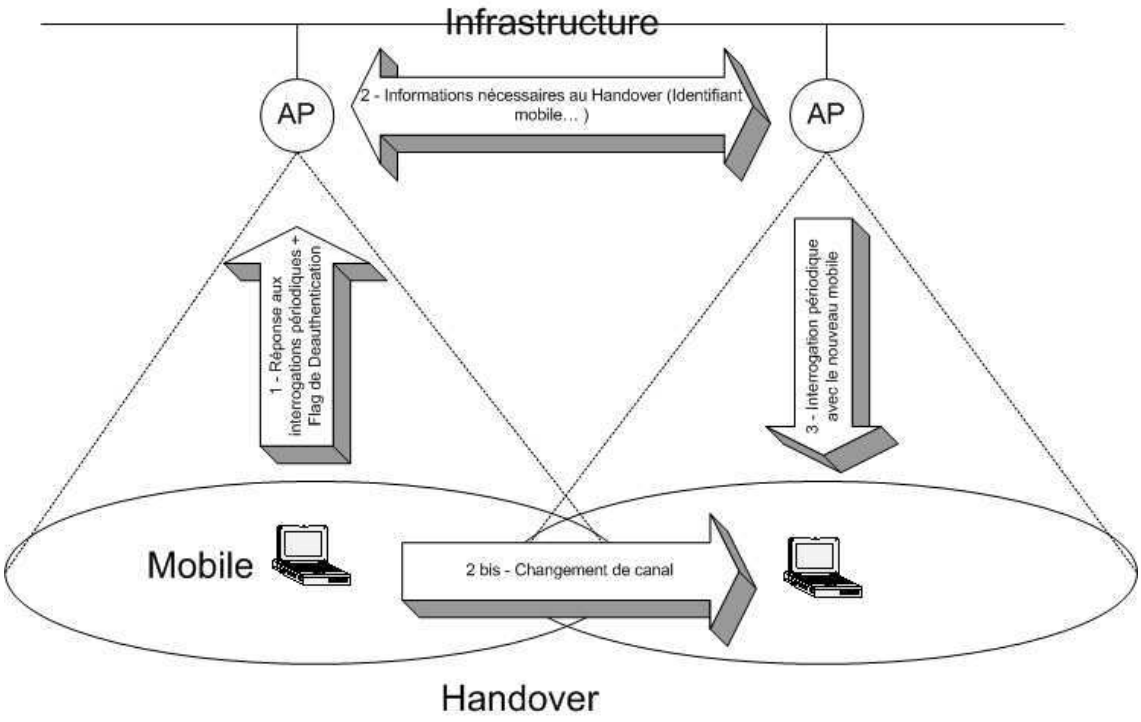


FIG. 44 – *Architecture du Handover par le haut*

Il faut un moyen pour indiquer à l'AP que la station va quitter la cellule et donc qu'il doit supprimer son identifiant de la table d'affiliation et la sortir de son cycle d'interrogation. Pour cela il suffit d'ajouter un flag dans les trames de réponses aux interrogations cycliques verticales et de positionner ce flag quand on va changer de cellule (c'est à dire

quand on vient de rencontrer une balise de Handover). Cette étape (1 sur la figure 44) remplace la trame de Deauthentication.

Le reste du handover concerne le trafic horizontal. Le point d'accès de la cellule quittée va transmettre les informations concernant la station au prochain point d'accès sur la trajectoire (étape 2), et ainsi lui indiquer qu'il doit ajouter ce mobile à son cycle d'interrogation (étape 3).

Au niveau de la station, elle va juste changer de canal. En mode monitor, la phase classique d'affiliation 802.11 ne s'effectue pas. La carte va capter tout le trafic transmis sur le canal donné. Le tri doit être effectué au niveau applicatif selon le type des paquets captés. Le système reconnaît différents types de paquets. Par exemple PACKET_HOST correspond aux paquets destinés à la station, PACKET_BROADCAST pour les paquets diffusés, etc. Dans notre cas les paquets intéressants sont ceux de type PACKET_HOST qui contiennent l'adresse MAC de la station dans le champs adresse MAC destination.

Avec cette solution, on a pu supprimer tout le trafic du Handover. On gagne donc le temps d'envoi de ces trames et le temps de handover dans ce cas se limite au temps qu'il faut au système d'exploitation pour déclencher le changement de canal sur le carte réseau et le temps de commutation de la carte du canal courant vers le nouveau canal.

Cette solution présente la contrainte de développer des applications complètes pour plusieurs raisons :

- le mode monitor n'étant pas prévu pour l'envoi de données, aucun contrôle n'est effectué. La norme 802.11 n'est plus complètement respectée. Il faut donc prévoir les contrôles d'intégrité des trames de données (CRC par exemple), définir une politique d'acquittement (en a-t-on besoin ? si oui quels délais prévoir ? etc). Ceci peut être vu comme un inconvénient mais peut également présenter des avantages au niveau des délais de traitements des trames et éventuellement de la méthode d'accès. En effet nous avons pu constater qu'en envoyant des trames en mode monitor,

l'envoi s'effectue sans qu'une période de contention soit respectée. En réalisant un générateur de trames en continu, on a pu constater qu'aucune autre station ne pouvait envoyer de trames, sauf dans le cas où les trames étaient adressées à une station particulière fonctionnant en mode managed. Dans ce cas, on pouvait voir les acquittements 802.11 ce qui laisse penser que l'envoi en mode monitor respecte quand même les délais inter-trames (IFS). Les acquittements étant prioritaires, ils sont envoyés après un temps SIFS plus court que le temps DIFS utilisé pour les trames de données en mode DCF,

– les applications utilisant la pile TCP/IP classique ne pourront pas utiliser la carte réseau. Il peut être envisagé le développement d'une application qui ferait l'interface entre la carte réseau et ces applications.

Cette solution présente d'autres avantages que ceux liés au handover. Elle pourrait nous permettre d'améliorer la façon dont nous réalisons le cycle d'interrogation des mobiles. Pour le moment, il est fait grâce à des trames unicast aussi bien pour les trames d'interrogation venant du point d'accès que pour les trames de réponses des stations. Une trame unicast n'est prise en compte que par la station à qui elle est adressée. L'utilisation du mode monitor pourrait nous permettre d'exploiter toutes les trames qui sont échangées dans la cellule. Même en gardant le principe d'interrogation actuel, en prenant en compte toutes les trames d'interrogation venant du point d'accès, une station aurait accès à des informations plus récentes concernant ses voisins, on peut aussi imaginer que les stations prennent en compte les réponses des différentes stations de la cellule.

Une autre méthode serait de diffuser une seule trame d'interrogation qui serait exploitée par toutes les stations, puis chacune répondrait dans un ordre défini par l'AP dans la trame d'interrogation. Ceci nous permettrait d'avoir des cycles d'interrogation plus courts et donc plus fréquents. On résoudrait en fait le problème lié au trames diffusées, qui le sont seulement après l'émission d'un Beacon, rencontré dans les tests du simulateur de mobiles présentés dans la partie précédente. Par contre, cette solution n'est envisageable qu'à la

condition que toutes les stations soient à portée les unes des autres car il est nécessaire que chacune capte les réponses des autres pour respecter le cycle de réponses.

1.5 Gestion de la continuité d'une transmission

Les solutions précédentes traitent de l'optimisation du trafic généré par le handover et du temps nécessaire à l'exécution de ce mécanisme. Un point reste à voir : la gestion d'une transmission de plusieurs données qui aurait été initiée avant le changement de cellule et qui devrait se terminer une fois la station affiliée à un nouveau point d'accès.

Pour qu'il n'y ait pas rupture dans la transmission, il est nécessaire d'agir au niveau des point d'accès et des éléments de l'infrastructure. On a vu que quand une station s'affilie à un nouveau point d'accès il ajoute l'adresse MAC de cette station dans sa table d'affiliation et qu'il va alors transmettre dans sa cellule toutes les trames destinées à cette station. Dans le cas où tous les points d'accès concernés voient le même trafic sur l'infrastructure (par exemple si ils sont sur un même segment Ethernet) alors il n'y a pas de problème puisque toutes les trames seront vues par tous les points d'accès). Par contre dans le cas d'une infrastructure commutée (par exemple un switch Ethernet) il y aura un problème de commutation des trames vers le nouveau point d'accès.

Sur la figure 45 on peut voir la configuration du switch à un instant donné. Considérons un transfert FTP entre le serveur et la station qui a l'adresse MAC2. Suite à des échanges préalables le switch connaît cette adresse MAC et grâce à sa table d'adresse MAC il va commuter les trames venant du serveur vers le port du switch auquel est relié le point d'accès qui gère la cellule de cette station, ici l'AP1. Quand la station va effectuer son handover, l'AP1 va supprimer l'adresse MAC2 de sa table d'affiliation et l'AP2 va l'ajouter à la sienne, mais ceci ne va pas avoir d'influence sur le comportement du switch, il va continuer de faire transiter les trames destinées à l'adresse MAC2 vers son port 4 alors qu'il faudrait désormais les envoyer sur le port 6. Normalement, pour que le switch mette

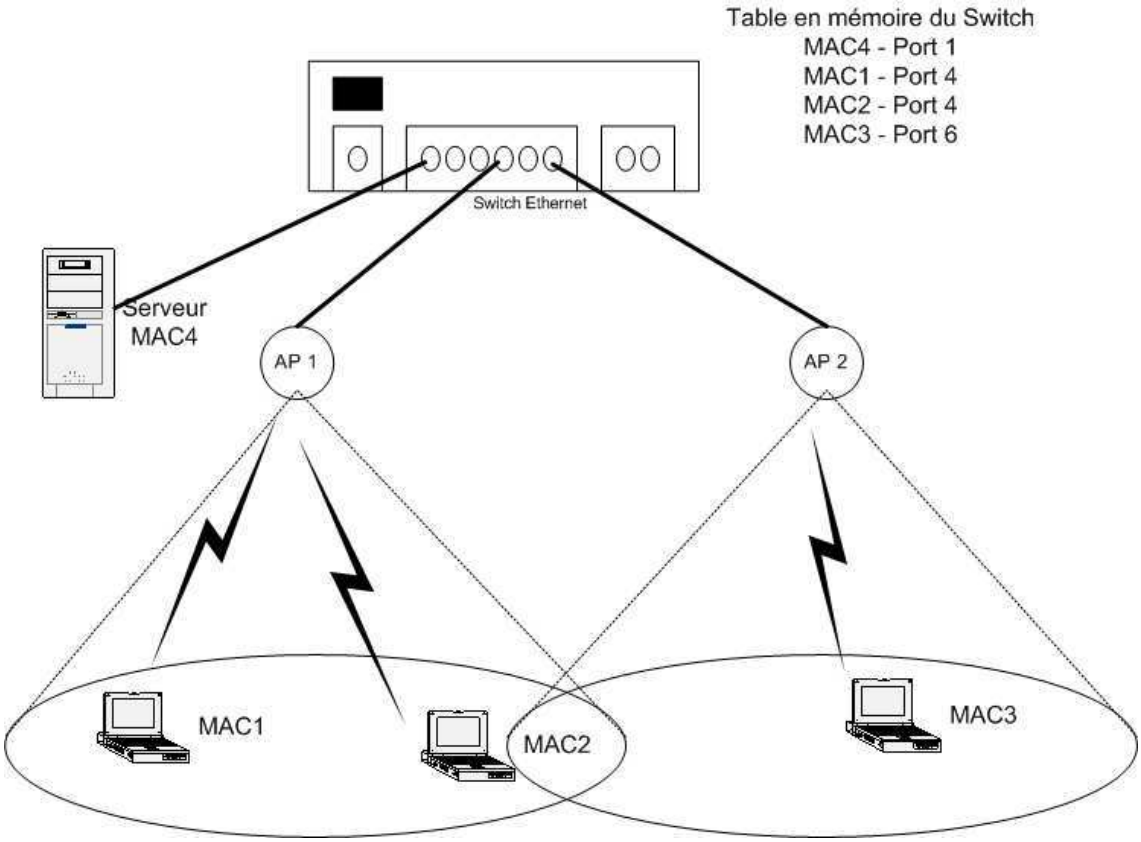


FIG. 45 – *Cas d'une infrastructure switchée*

sa table à jour, il faut qu'il reçoive sur le port 6 une trame venant de la station d'adresse MAC2. Si ceci n'est pas fait le transfert FTP va s'interrompre. Une solution possible est de mettre en oeuvre au niveau des points d'accès un protocole tel qu'IAPP. Dans le projet Waves, nous avons déjà prévu des échanges entre les AP pour la gestion de la collaboration des mobiles. On peut ajouter à cela des informations concernant le handover, comme proposé par exemple dans l'étape 2 du handover par l'infrastructure (voir figure 44).

Il faut alors mettre en oeuvre un mécanisme qui va permettre au switch de mettre à jour sa table d'adresses MAC. Quand le point d'accès reçoit une information lui indiquant qu'une nouvelle station va rejoindre sa cellule on peut provoquer l'envoi d'une trame Ethernet sur l'infrastructure, avec comme adresse MAC source l'adresse MAC de cette

station, ce qui est possible en utilisant une socket RAW. Ceci provoquera immédiatement la mise à jour de la table d'adresse MAC du switch avant même que la station qui vient de changer de cellule n'ait envoyer une trame sur le réseau et qui permettra au switch de commuter les trames dans la bonne direction et ainsi permettre un transfert de données sans rupture. Ce mécanisme doit être utilisé aussi bien avec une solution à une carte embarquée sur le mobile, qu'avec une solution à deux cartes.

Chapitre 2

Résultats

Sommaire

2.1 Plateforme de tests 121

2.1.1 Matériel utilisé 121

2.1.2 Ethereal 123

2.2 Le mode scan manuel 123

2.3 Handover par l'infrastructure 126

2.4 Solutions avec deux interfaces sans fil embarquées 129

Dans cette partie nous allons voir les résultats obtenus pour les différentes solutions proposées ainsi que des propositions de prolongements pour ce travail. Tous d'abord voyons les conditions expérimentales.

2.1 Plateforme de tests

2.1.1 Matériel utilisé

Les points d'accès et stations sont des ordinateurs de bureau ou portables équipés de processeurs relativement récents. Les communications sont réalisées avec des cartes sans fil de type PCMCIA et PCI équipées de chipsets Prism respectant les normes 802.11b ou

802.11g. Les drivers utilisés sont hostap (cartes 802.11b avec chipset Prism 2) ou prism54 (cartes 802.11g avec chipset Prism GT).

Ces deux drivers permettent d'utiliser les cartes sans fil dans différents modes :

- Managed (mode station) : c'est le mode de fonctionnement classique d'une carte équipant une station
- Master (mode point d'accès) : la station va réaliser toutes les fonctions d'un point d'accès
- Monitor (mode écoute) : la carte est alors inactive en émission, elle n'émet plus aucune information mais elle remonte toutes les trames qu'elle peut capturer aux couches supérieures, on peut donc les récupérer dans un logiciel d'analyse de réseau.

HospAP et Prism54 présentent également l'avantage d'être libres, ils sont donc récupérables gratuitement et open source. Ils ont été développés pour les systèmes Linux (noyau 2.2 au minimum).

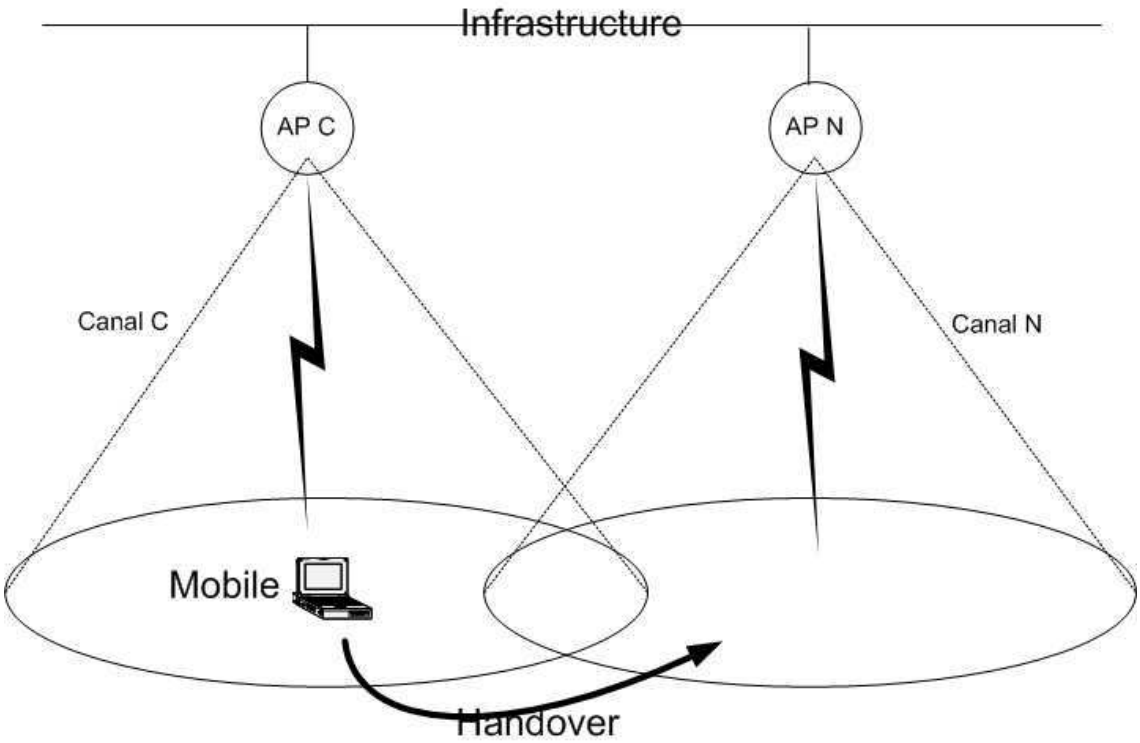


FIG. 46 – *Plateforme générique pour les expérimentations*

Pour nos tests, nous avons utilisé la configuration illustrée par la figure 46, avec deux points d'accès fonctionnant sur deux canaux différents, l'intersection des deux cellules ne sera évidemment pas nulle et la station effectuant le handover est positionnée dans la zone de recouvrement.

2.1.2 Ethereal

Pour bien étudier un processus réseau tel que le Handover, il est intéressant de pouvoir visualiser les différentes trames échangées. Pour cela on a utilisé un analyseur réseau, nous avons choisi Ethereal [4] qui est un des plus connus dans ce domaine. Couplé à une carte sans fil en mode monitor, on va capturer toutes les trames échangées dans une ou plusieurs cellules. En effet, contrairement au mode station, le mode monitor de HostAP permet de capturer également les trames de gestion de 802.11 (Acquittements, Beacons, Probes...).

L'interface du logiciel (voir figure 47) est composé de la manière suivante. La zone supérieure permet de visualiser la liste des tames capturées, avec quelques informations telles que les adresses (IP ou MAC), le type de trame car Ethereal reconnaît la plupart des protocoles courants, le temps auquel la trame est capturée. La zone centrale permet de visualiser les entêtes d'une trame sélectionnée dans la zone supérieure. Comme le logiciel reconnaît les protocoles il est capable de faire un découpage des différents champs de l'entête de la trame en question. La dernière zone permet de visualiser le contenu de la trame au format hexadécimal.

Après cette brève présentation des moyens passons aux expérimentations qui ont permis d'évaluer les performances des différentes solutions que nous proposons.

2.2 Le mode scan manuel

Le scan manuel est le mode pour lequel les informations concernant le point d'accès que nous souhaitons rejoindre vont être spécifiées par l'application. La phase de recherche

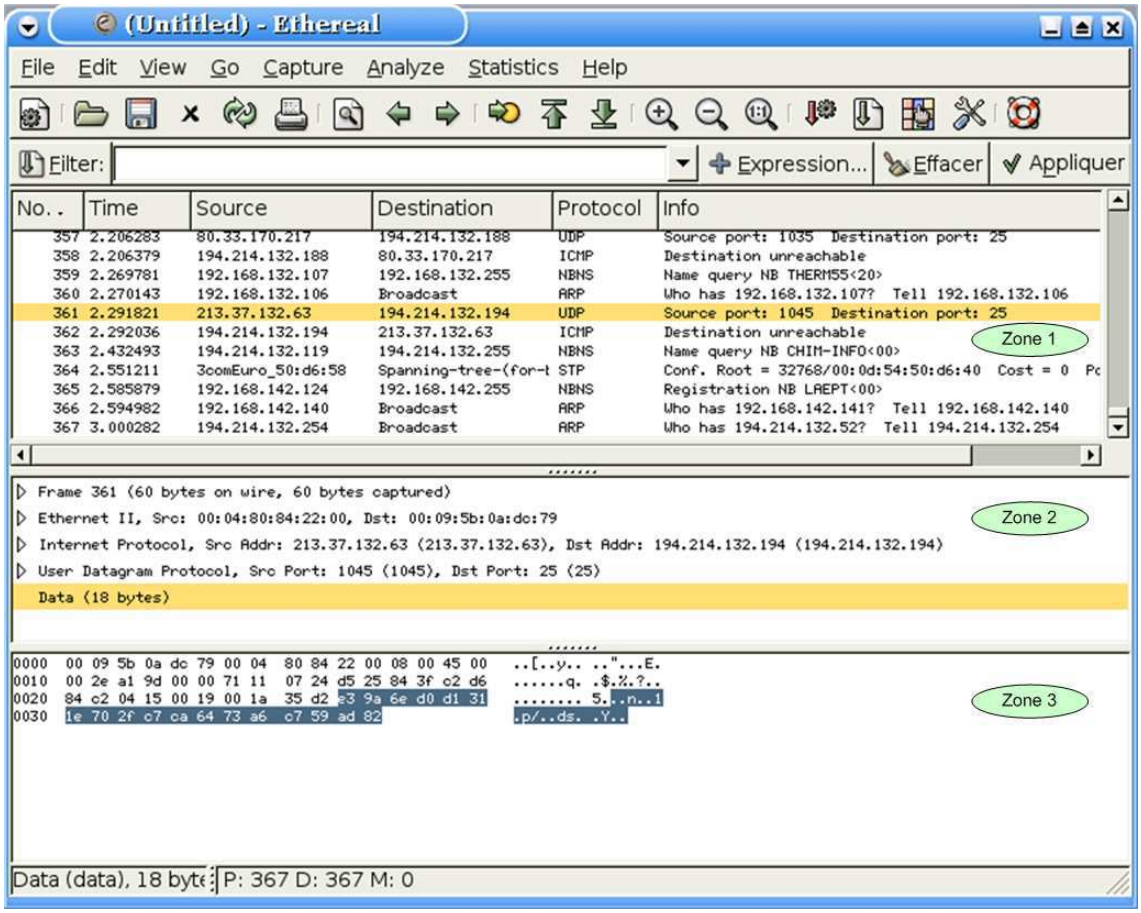


FIG. 47 – *Le logiciel Ethereal*

de point d'accès est donc supprimée. La figure 48 nous permet de voir les trames échangées pendant ce handover.

Le handover déclenché par l'application après le passage sur une balise, commence par l'envoi d'une trame "Deauthentication" par la station qui a l'adresse MAC terminant par 32-5E-AA, qui indique au point d'accès auquel elle est affiliée, qui a l'adresse 32-5E-A6, qu'elle quitte la cellule. Cette trame est acquittée puis la station change de canal pour passer sur celui spécifié par l'utilisateur ou l'application. La phase d'affiliation au nouveau point d'accès, qui a l'adresse MAC 32-5D-45, est initiée. Elle commence par la phase d'authentification et est suivie de la phase d'association. Elle se termine par l'acquittement de la trame Association Response.

14	1.125082	BromaxCo_32:5d:45	Broadcast	IEEE 802.11	Beacon frame
15	1.227280	BromaxCo_32:5d:45	Broadcast	IEEE 802.11	Beacon frame
16	*REF*	BromaxCo_32:5e:aa	BromaxCo_32:5e:a6	IEEE 802.11	Deauthentication
17	0.000285		BromaxCo_32:5e:aa (RA)	IEEE 802.11	Acknowledgement
18	0.010154	BromaxCo_32:5e:a6	Broadcast	IEEE 802.11	Beacon frame
19	0.095210	BromaxCo_32:5e:aa	BromaxCo_32:5d:45	IEEE 802.11	Authentication
20	0.095493		BromaxCo_32:5e:aa (RA)	IEEE 802.11	Acknowledgement
21	0.096205	BromaxCo_32:5d:45	BromaxCo_32:5e:aa	IEEE 802.11	Authentication
22	0.096491		BromaxCo_32:5d:45 (RA)	IEEE 802.11	Acknowledgement
23	0.097200	BromaxCo_32:5e:aa	BromaxCo_32:5d:45	IEEE 802.11	Association Request
24	0.097478		BromaxCo_32:5e:aa (RA)	IEEE 802.11	Acknowledgement
25	0.098070	BromaxCo_32:5d:45	BromaxCo_32:5e:aa	IEEE 802.11	Association Response
26	0.098349		BromaxCo_32:5d:45 (RA)	IEEE 802.11	Acknowledgement
27	0.112162	BromaxCo_32:5e:a6	Broadcast	IEEE 802.11	Beacon frame
28	0.214966	BromaxCo_32:5e:a6	Broadcast	IEEE 802.11	Beacon frame

FIG. 48 – *Capture d'un Handover en mode scan manuel*

Le temps de handover va donc être le temps entre l'envoi de la trame Deauthentication et l'acquittement de la trame Association Response. Dans la capture, le temps est exprimé en secondes, pour cet exemple il est de 0.098349, soit 98,349 ms. Plusieurs tests consécutifs donnent des résultats similaires, on peut donc considérer que le temps de handover en mode scan manuel est aux alentours de 100ms.

Ce temps est beaucoup plus satisfaisant qu'en mode scan automatique (temps compris entre 600ms et 700ms). Le cycle d'interrogation des mobiles d'une cellule que nous effectuons étant légèrement supérieur à 50ms, on risque de manquer deux trames d'interrogation venant des points d'accès, voire plus puisque le temps pendant lequel la station ne reçoit plus de trames au niveau application est légèrement supérieur au temps calculé avec les trames de gestion du handover. Dans notre application, nous avons fixé à 7 mètres par secondes la vitesse maximum des mobiles. En 100ms, un mobile peut donc parcourir 70cm, il faut donc prévoir une distance de sécurité supérieure à cette valeur entre les mobiles. Cette distance est à adapter selon la vitesse maximum des mobiles. Pour des collaborations plus contraintes par le temps et pour des applications concernant la voix sur IP cette solution ne sera pas forcément satisfaisante. Elle présente néanmoins l'avantage d'être simple à mettre en oeuvre et elle permet de rester compatible avec toute

application TCP/IP classique.

2.3 Handover par l'infrastructure

Cette solution permet la suppression complète des trames de gestion du handover en utilisant le mode monitor pour les cartes réseaux comme le permettent les drivers HostAP ou Prism54. Les informations concernant ce changement de cellule sont soit incluses dans les trames d'interrogation et les réponses échangées entre les points d'accès et les stations (ceci concerne le déclenchement du handover), soit échangées entre le point d'accès de la cellule quittée et celui de la cellule rejointe.

Le test de cette solution a nécessité le développement d'une application en C utilisant les sockets RAW qui permettent de passer outre les piles de protocoles classiques telles que TCP/IP. Nous allons utiliser l'entête de trame 802.11 qui inclue les adresses MAC des entités communicantes, c'est donc les adresses MAC qui serviront d'identifiant unique pour nos mobiles. Les paramètres nécessaires pour la création des sockets, et le code complet de l'application sont fournis dans les annexes B et C.

Pour les mesures, une application a été placée sur chaque point d'accès. Elles envoient toutes les deux des trames en permanence. Une application de réception et de traitement des trames est installée au niveau de la station, celle-ci permet de trier les trames destinées à cette station et pourrait être inclue dans une application de gestion des mobiles comme celle du projet Waves. La figure 49 résume la manipulation effectuée pour tester ce type de handover.

Plusieurs handovers successifs sont provoqués et on observe les résultats grâce à Ethereal. Dans ce cas, la carte étant en mode monitor aucune trame de gestion n'est envoyée, ni pour le handover ni pour acquitter les trames de données. Seules les trames générées par les applications et envoyées de manière continuelle par le point d'accès fonctionnant sur le même canal que la station apparaissent.

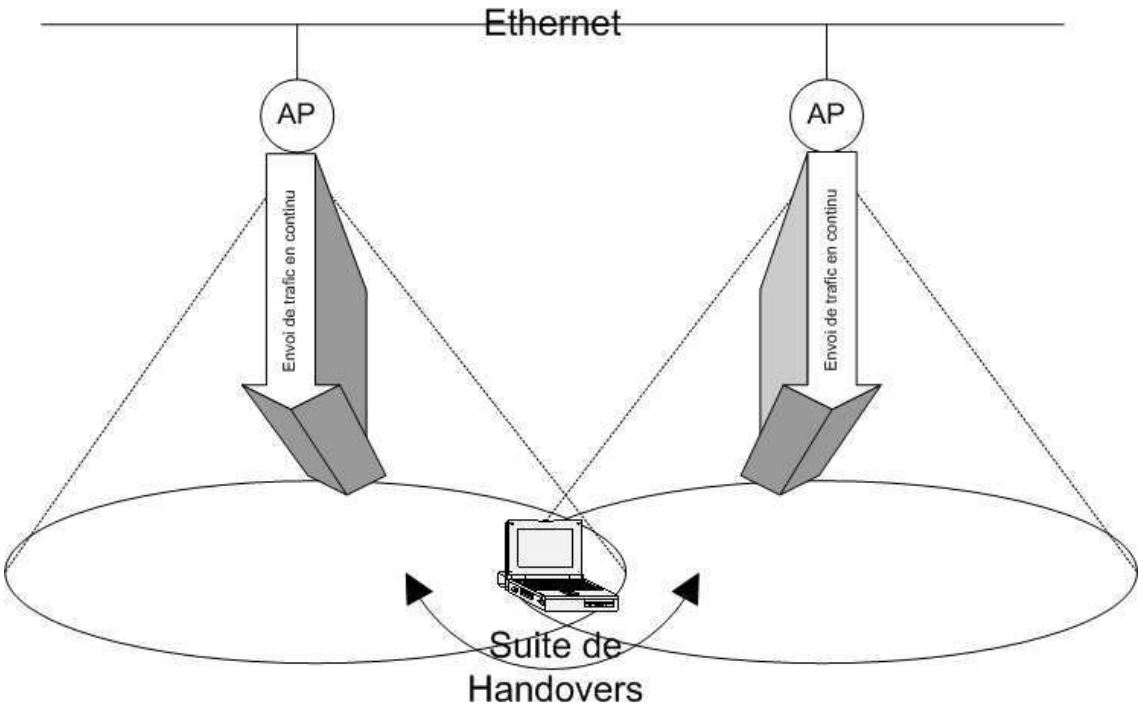


FIG. 49 – *Schéma de test des performances du Handover par le haut*

Notre trace Ethereal est donc composée d'une suite de trames provenant de l'AP1, puis au changement de canal d'un certain nombre venant de l'AP2, puis lors d'un nouveau changement de canal de trames venant de l'AP1, etc. Le temps de handover peut donc être évalué en détectant les changements de canal et en calculant la différence entre le moment où la dernière trame dans la cellule courante est reçue et la première qui est capturée quand la station passe dans la cellule suivante.

La figure 50 montre la répartition des résultats de cette manipulation. Le temps moyen obtenu pour le handover en mode monitor est de 45,7ms, ce qui est deux fois plus rapide que la solution précédente, de plus il s'agit là d'un temps de handover au niveau application. Ce temps est la somme du temps qu'il faut au système pour envoyer l'ordre à la carte de changer de canal et du temps nécessaire à chaque carte pour changer réellement de canal de transmission.

On peut considérer ce temps comme très satisfaisant puisque le cycle d'interrogation

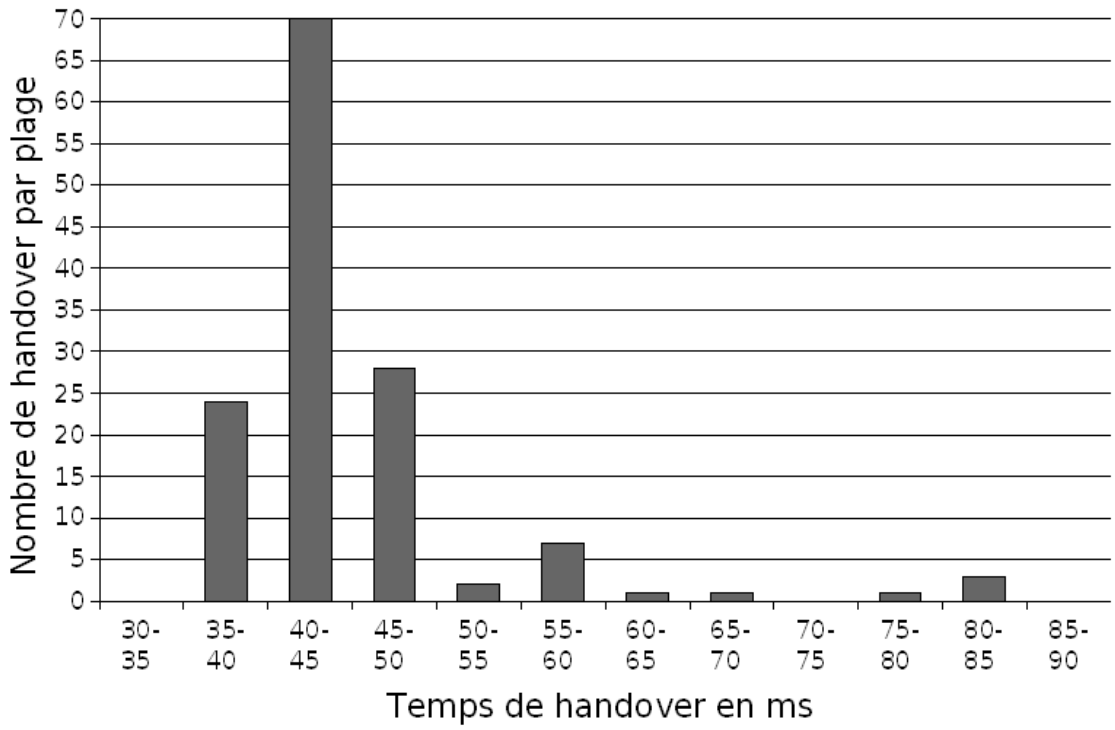


FIG. 50 – *Handover en mode monitor*

que nous avons fixé pour le projet est de 50ms. La station ne participerait pas, au plus, à un cycle d'interrogation du point d'accès. Pour d'autres applications à fortes contraintes de temps comme la voix ce serait également satisfaisant, le groupe de travail 802.11r [15], qui travaille à l'optimisation du handover pour la voix sur WiFi, a comme objectif un temps de handover inférieur à 150ms, en dessous de cette valeur l'homme n'est pas capable de détecter une rupture dans la conversation.

Ce temps pourrait peut-être être amélioré, en effet une carte réseau sans fil n'a pas besoin de tant de temps pour passer d'un canal à un autre. On peut penser qu'ici c'est le système d'exploitation qui allonge le temps total de la procédure. On pourrait sûrement obtenir des temps plus intéressants en utilisant des systèmes temps réel tels que RTLinux, RTAI...

2.4 Solutions avec deux interfaces sans fil embarquées

La solution à deux cartes n'est pas une solution à part entière, elle doit être combinée avec une des deux solutions précédentes, chaque carte devant utiliser soit le mode managed soit le mode monitor. Avec cette solution, on va affilier la carte inactive dont le mobile est équipée au point d'accès de la cellule que nous allons rejoindre au moment où une balise de handover va être détectée sur la voie. Pendant ce temps, la station continue d'être accessible par le point d'accès de la cellule courante via la carte active. On ne peut donc pas considérer le temps de handover comme étant le temps où la carte réseau recherche un nouveau point d'accès et s'y affilie comme nous l'avons fait précédemment, puisqu'il n'y devrait pas y avoir de temps où la station est inaccessible. Pendant un certain temps elle sera même accessible par ses deux interfaces réseaux. Les deux points d'accès ayant tous deux la station dans leur table d'affiliation chacun transmettra dans sa cellule les trames venant de l'infrastructure qui lui sont destinées. Il y aura alors redondance au niveau de la station, ce qui ne pose aucun problème dans le cas d'un transfert utilisant TCP/IP, puisque la duplication de trames est gérée par la pile de protocole. Dans le cas d'une application propriétaire que nous pourrions développer avec des sockets RAW il serait nécessaire de traiter ce problème de duplication.

L'avantage principal de cette solution est sa robustesse puisque que la station sera toujours joignable par l'infrastructure, il est préférable que la station soit affiliée à deux endroits à la fois plutôt qu'être inaccessible pendant un certain temps. Les possibles problèmes engendrés, comme la redondance peuvent être considérés comme mineurs par rapport aux besoins liés aux applications contraintes par le temps.

Le problème lié aux incohérences d'informations évoqué dans le chapitre proposant cette solution doit être traité au niveau des points d'accès. Dans le projet Waves ceci est réalisé par des échanges cycliques entre les points d'accès. Ce problème de collaboration entre les points d'accès est traité par Sabri Benferhat dans le cadre de son travail de

thèse[26].

Conclusion

Le travail présenté est une composante du projet Waves initié en 2002 dans l'équipe Réseaux et Protocoles du LIMOS de Clermont-Ferrand. Ce projet a pour but l'étude du comportement d'un réseau local sans fil dans un cadre industriel, c'est à dire pour des applications à fortes contraintes de temps, dans notre cas la supervision de mobiles coopérants, communiquant via un réseau sans fil en mode infrastructure, composé de produits respectant la norme IEEE802.11. L'étendue géographique de l'application peut nécessiter une couverture cellulaire ce qui nous a mené au sujet traité dans cette thèse : les effets d'un changement de cellule pour une telle application.

Après avoir étudié le fonctionnement du changement de cellule dans 802.11 et après l'avoir évalué expérimentalement, nous avons constaté que le trafic induit par le handover, qui est en compétition pour l'accès au médium avec le trafic lié à l'application, était très important et donc pénalisant. Le temps est le deuxième paramètre que nous avons pris en compte. Le handover 802.11 est composé d'une phase de recherche d'un nouveau point d'accès, d'une phase d'authentification et d'une phase d'association. Pendant ces différentes étapes le mobile n'est pas capable de communiquer. Avec les valeurs par défaut de la norme, une station pouvait rester inaccessible pour toute autre entité du réseau, pendant près d'une seconde, ce qui est inacceptable pour ce type d'application.

Plusieurs solutions ont donc été étudiées pour permettre de réduire à la fois le temps et le trafic généré par le handover. Le première est réalisée par un simple paramétrage du driver, qui permet de supprimer la phase de recherche du point d'accès qui est la plus longue du processus de changement de cellule. Elle implique une connaissance, par la station, du point d'accès de la cellule suivante. Dans le projet Waves, ces informations sont contenues dans des balises de déclenchement du handover, disposées le long de la voie de circulation et sont lues par les mobiles quand ils passent à proximité de la balise. La deuxième solution propose d'embarquer deux cartes réseaux sans fil sur chaque mobile. Pendant que la première carte, affiliée au point d'accès de la cellule courante, est utilisée pour contacter le mobile, la deuxième s'affiliera, au moment souhaité, au point d'accès

de la cellule suivante. Ceci permet à la station d'être contactée par deux point d'accès simultanément pendant un certain temps, ensuite la première carte sera désactivée et jouera le rôle de la deuxième carte au passage devant la prochaine balise de handover. Cette solution permet de ne plus avoir à prendre en compte le temps du handover, par contre le trafic généré sera le même. La dernière solution permet de supprimer totalement le trafic du handover, ce qui est rendu possible grâce à un mode de fonctionnement spécifique du driver de la carte sans fil. Ce mode est normalement destiné à l'analyse de réseau, mais nous avons constaté qu'il est possible de l'utiliser en communication grâce à l'utilisation de sockets RAW. Ce mode a pour effet de supprimer l'envoi de toutes les trames de gestion 802.11, mais aussi de passer outre la pile TCP/IP que nous utilisons normalement pour nos communications. L'implémentation de cette solution nécessiterait donc la prise en charge de tous les contrôles par notre application. Concernant le trafic du handover, l'idée est de le remplacer par des échanges inter-AP sur l'infrastructure filaire, qui propose un débit plus important. Pour toutes les solutions proposées il peut être nécessaire, suivant le type d'infrastructure utilisé, d'effectuer un traitement au niveau des point d'accès pour éviter une rupture de communication, dans le cas d'un transfert de données inter-cellulaire initié dans une cellule et devant continuer dans une autre.

Les résultats obtenus sont beaucoup plus satisfaisants que ceux obtenus en utilisant le handover classique de 802.11, en particulier pour les deux dernières solutions. La solution par l'infrastructure permet une suppression du trafic et un temps de changement de cellule inférieur à 50ms qui est le délai entre deux interrogations du mobile par le point d'accès, pour récupérer ses informations et lui communiquer celles des mobiles avec lesquels il coopère. La solution à deux cartes embarquées est intéressante pour sa robustesse puisqu'elle devrait permettre à un mobile d'être en permanence accessible.

Plusieurs prolongements peuvent être proposés parmi lesquels :

– l'implémentation des solutions proposées dans la plateforme générale du projet Waves.

- l'évaluation du comportement de l'application dans le cas où l'infrastructure serait sans fil (WDS)
- l'évaluation des performances de l'application en général et du handover en particulier en utilisant des technologies réseaux plus récentes, par exemple les extensions a et g de 802.11. Ceci peut être réalisé en exploitant le driver MadWifi [17] qui propose les mêmes fonctions qu'HostAP pour les cartes 802.11a et 802.11g à base de chipsets Atheros [2].
- le nombre de stations dont nous disposons étant limité, il serait intéressant de simuler une plateforme avec un nombre importants de mobiles. Ceci impliquerait l'utilisation de logiciels de type OPNET [21] ou NS2 [18].

Bibliographie

[1] Arp, rfc826, an ethernet address resolution protocol, ftp ://ftp.rfc-editor.org/in-notes/rfc826.txt.

[2] Atheros, http ://www.atheros.com.

[3] Autorité de régulation des communications electroniques et des postes, http ://www.arcep.fr.

[4] Ethereal, network protocol analyzer, http ://ethereal.com/.

[5] Exposé sur le fonctionnement du gsm phase 1 sur le plan traitement numérique du signal (modulation gmsk), http ://membres.lycos.fr/amalbert/.

[6] Guill.net, la page des réseaux, http ://www.guill.net/.

[7] Host ap driver, http ://hostap.epitest.fi/.

[8] Ieee80211, standard ieee, spécification de la méthode d'accès (mac) et de la couche physique(ph) pour réseau local sans fil, http ://grouper.ieee.org/groups/802/11.

[9] Ieee80211b, extension du standard 802.11 à 11 mbit/s, 2.4 ghz, http ://grouper.ieee.org/groups/802/11.

[10] Ieee80211e, standard ieee, quality of services, http ://grouper.ieee.org/groups/802/11.

[11] Ieee80211f, standard ieee, inter-ap protocol, http ://grouper.ieee.org/groups/802/11.

[12] Ieee80211g, standard ieee, extension du standard 802.11 à 54 mbit/s, 2.4 ghz, http ://grouper.ieee.org/groups/802/11.

[13] Ieee80211i, standard ieee, extension de standards de réseaux locaux sans fil, 802.11, pour le support de mécanisme de confidentialité et de sécurité de liaison sans fil, http ://grouper.ieee.org/groups/802/11.

[14] Ieee80211k, radio ressource management, http ://grouper.ieee.org/groups/802/11.

[15] Ieee80211r, standard ieee, fast roaming, http ://grouper.ieee.org/groups/802/11.

[16] Ieee802.3, standard ieee, csma/cd.

[17] Madwifi, http ://www.madwifi.com.

[18] Network simulator - ns2, http ://www.isi.edu/nsnam/ns/.

[19] Radius, rfc 2865 et 2866, http ://www.ietf.org/rfc/rfc2865.txt, http ://www.ietf.org/rfc/rfc2866.txt.

[20] Rfc2002, ip mobility support, ftp ://ftp.rfc-editor.org/in-notes/rfc2002.txt.

[21] Simulateur opnet (optimum network performance), http ://www.opnet.com/.

[22] Standard gsm, etsi, http ://www.etsi.org/services_products/freestandard/home.htm.

[23] Tapdance, http ://www.atmel.com.

[24] Umts - universal mobile telecommunications system, http ://www.etsi.org.

[25] Wireless tools, http ://www.hpl.hp.com/personal/jean_tourrilhes/linux/tools.html.

[26] Sabri Benferhat, Frederique Jacquet, and Michel Misson. Etude d'une architecture de communication pour des échanges intercellulaires entre mobiles coopérants. *CFIP*, 2005.

[27] Pat R. Calhoun. Minimal latency secure hand-off. 2000.

[28] Romain David. Réseaux cellulaires, http ://www.hds.utc.fr/ ducourth/tx/cel/.

[29] D. Devarsirvatham and T.S. Rappaport. Radio-wave propagation measurements and modelling for personal communications. *IEEE ICC International Conference on Communications, Tutorial 4, Geneva, Switzerland, May 1993*, 1993.

[30] F.A. Gonzalez, J.A. Perez, and V.H. Zarate. Layer 2 handoff accurate measurement strategy in wlans 802.11. *Workshop on Wireless Network Measurements*, 2005.

[31] Sebastien Hernandez, Patrick Lafarguette, Antonio Freitas, and Michel Misson. First evaluations of a simulation architecture of the use of a ieee 802.11 wlan in industrial context. *WCNC Atlanta*, 2004.

[32] Sebastien Hernandez, Patrick Lafarguette, and Michel Misson. Spécification d'une plateforme pour l'evaluation de 802.11 : Echanges inter mobiles dans une cellule. *CNRIUT*, 2003.

[33] IETF. Mobile ip : http ://www.ietf.org/html.charters/mobileip-charter.html.

[34] Patrick Lafarguette. Evaluation des capacités temps réel d'un réseau 802.11 dans un contexte industriel. *Mémoire de diplôme d'ingénieur CNAM*, 2003.

[35] Philippe Llamas. Adaptation d'un point d'accès 802.11b pour des applications temps réel. *Mémoire de diplôme d'ingénieur CNAM*, 2005.

[36] P. Mühlethaler. 802.11 et les réseaux sans fil. *Editions Eyrolles Août 2002*, 2002.

[37] Arunesh Mishra, Minho Shin, and William Arbaugh. An empirical analysis of the IEEE 802.11 MAC layer handoff process. *ACM Computer Communication Review*, 33(2) :93–102, 2003.

[38] Nicolas Montavont and Thomas Noël. Anticipation des handovers dans les réseaux sans fils. *16em congrès DNAC, Paris*, 2002.

[39] Nicolas Montavont and Thomas Noël. Fast handover protocol over ieee 802.11b wlans. *IEEE International Symposium on advances in Wireless Communications (ISWC'2002), Victoria, Canada*, 2002.

[40] A. Neskovic and G. Paunovic. Modern approaches in modelling of mobile radio systems propagation environment. *IEEE Communications Surveys http ://www.comsoc.org/pubs/surveys*, 2000.

[41] Diane Orr. Trade-off analysis (802.11e versus 802 .15.3 qos mechanism). 2002.

[42] K. Pahlavan and P. Krishnamurthy. Principles of wireless networks - a unified approach. *Editions Prentice Hall*, 2001.

[43] Se Hyun Park, Aura Ganz, and Zvi Ganz. Security protocol for IEEE 802.11 wireless local area network. *Mobile Networks and Applications*, 3(3) :237–246, 1998.

[44] R. Prasad and L. Munoz. Wireless ip, tutorial.

[45] T.S. Rappaport. Wireless communications - principles and practice. *Editions Prentice Hall*, 2002.

[46] William Stallings. Réseaux et communication sans fil - 2ème édition. *Editions Pearson Education*, 2005.

[47] D. Tandjaoui, N. Badache, H. Bettahar, A. Bouabdallah, and H. Seba. Towards a smooth handoff for tcp and real time applications in wireless network. 2002.

[48] Thierry Val. Etude d'un réseau local hybride d'intérieur permettant l'interconnexion de stations fixes et de stations mobiles. *Mémoire de Doctorat*, 2004.

[49] Thierry Val and Michel Misson. Multipath redundancy induced by the emitter/receiver distribution for the overlapping coverage in an infrared wireless communication area. *Conference record of EFOC&'N93, The Hague, The Netherlands*, pages 115–118, 1993.

[50] Hector Velayos and Gunnar Karlsson. Techniques to reduce ieee 802.11b mac layer handover time. 2003.

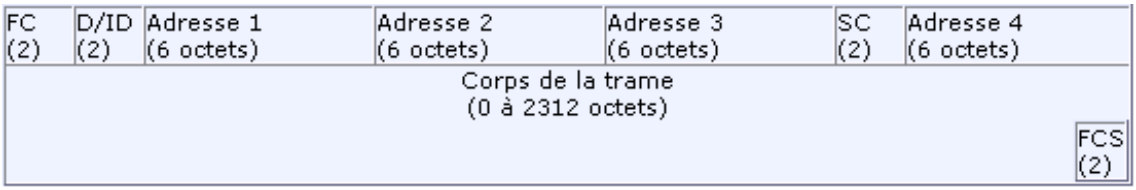
[51] Sonia Waharte, Kevin Ritzenthaler, and Raouf Boutaba. Selective active scanning for fast handoff in wlan using sensor networks. 2004.

Annexes

Annexe A

Trame 802.11

Voici le format d'une trame 802.11, ainsi suivant du détail du champs Frame Control et des différents type de trames possible (source pour les figures www.commentcamarche.net).



- FC (Frame Control) : décrit plus bas.
- D/ID (Duration ID) Il y a deux cas possibles pour ce champs suivant le type de trame. Pour les trames de polling en mode d'économie d'énergie, c'est l'identifiant de la station. Pour les autres trames, il contient la valeur utilisée pour le calcul du NAV.
- Adresse 1 : adresse MAC du récepteur. Si ToDS est à 1 alors c'est l'adresse du point d'accès, sinon, c'est l'adresse de la station.
- Adresse 2 : adresse MAC de l'émetteur. Si FromDS est à 1, c'est l'adresse du point d'accès, sinon, c'est l'adresse de la station émettrice.
- Adresse 3 : adresse MAC de l'émetteur original quand le champ FromDS est à 1. Sinon, et si ToDS est à 1, c'est l'adresse destination.

- SC (Sequence ontrol) : ce champ utilisé pour représenter l'ordre des différents fragments appartenant à une même trame, et pour reconnaître les paquets dupliqués. Il est composé de deux sous-champs, le numéro de fragment et le numéro de séquence qui définissent le numéro de trame et le numéro du fragment dans la trame.
- Adresse 4 : adresse MAC utilisée pour le WDS (infrastructure sans fil) et qu'une trame est transmise d'un point d'accès à un autre. Dans ce cas, ToDS et FromDS sont tous les deux à 1 et il faut donc renseigner à la fois l'émetteur original et le destinataire.
- Corps de la trame : Données provenant des couches supérieures.
- FCS (Frame Control Sequence) : contrôle d'intégrité de la trame.

Version de protocole (2 bits)		Type (2 bits)		Sous-Type (4 bits)			
To DS (1 bit)	From DS (1 bit)	More Frag (1 bit)	Retry (1 bit)	Power Mgt (1 bit)	More Data (1 bit)	WEP (1 bit)	Order (1 bit)

- Version de protocole : prévue pour différencier les différentes version de 802.11.
- Type et sous-type : les 6 bits définissent le type et le sous-type des trames (voir tableau ci dessous)
- ToDS : vaut 1 lorsque la trame est adressée au Point d'Accès pour qu'il la fasse suivre au système de distribution.
- FromDS : vaut 1 quand la trame vient du système de distribution.
- More Fragments (d'autres fragments) : ce bit est mis à 1 quand il y a d'autres fragments qui suivent le fragment en cours.
- Retry (retransmission) : ce bit indique que le fragment est une retransmission d'un fragment précédemment transmis.
- Power Management (gestion d'énergie) : vaut 1 si la station sera en mode de gestion d'énergie après la transmission de cette trame.
- More Data (d'autres données) : ce bit est également utilisé pour la gestion de l'énergie. Il est utilisé par le point d'accès pour indiquer que d'autres trames sont vont

suivre pour la station et éviter qu'elle repasse en mode économie d'énergie.

- WEP (sécurité) : vaut 1 si le corps de la trame est crypté suivant l'algorithme WEP.
- Order (ordre) : ce bit indique que cette trame est envoyée en utilisant la classe de service strictement ordonné (Strictly-Ordered service class). Cette classe est définie pour les utilisateurs qui ne peuvent pas accepter de changement d'ordre entre les trames unicast et multicast.

Type	Description du type	Sous-type	Description du sous-type
00	Management (gestion)	0000	Association request (requête d'association)
00	Management (gestion)	0001	Association response (réponse d'association)
00	Management (gestion)	0010	Reassociation request (requête ré-association)
00	Management (gestion)	0011	Reassociation response (réponse de ré-association)
00	Management (gestion)	0100	Probe request (requête d'enquête)
00	Management (gestion)	0101	Probe response (réponse d'enquête)
00	Management (gestion)	0110-0111	Reserved (réservé)
00	Management (gestion)	1000	Beacon (balise)
00	Management (gestion)	1001	Annoucement traffic indication message (*ATIM*)
00	Management (gestion)	1010	Disassociation (désassociation)
00	Management (gestion)	1011	Authentication (authentification)
00	Management (gestion)	1100	Deauthentication (désauthentification)
00	Management (gestion)	1101-1111	Reserved (réservé)
01	Control (contrôle)	0000-1001	Reserved (réservé)
01	Control (contrôle)	1010	Power Save (PS)-Poll (économie d'énergie)
01	Control (contrôle)	1011	Request To Send (RTS)
01	Control (contrôle)	1100	Clear To Send (CTS)
01	Control (contrôle)	1101	ACK
01	Control (contrôle)	1110	Contention Free (CF)-end
01	Control (contrôle)	1111	CF-end + CF-ACK
10	Data (données)	0000	Data (données)
10	Data (données)	0001	Data (données) + CF-Ack
10	Data (données)	0010	Data (données) + CF-Poll
10	Data (données)	0011	Data (données) + CF-Ack+CF-Poll
10	Data (données)	0100	Null function (no Data (données))
10	Data (données)	0101	CF-Ack
10	Data (données)	0110	CF-Poll
10	Data (données)	0111	CF-Ack + CF-Poll
10	Data (données)	1000-1111	Reserved (réservé)
11	Data (données)	0000-1111	Reserved (réservé)

Annexe B

Paramètres pour les sockets RAW

La création de la socket.

socket(PF_PACKET,SOCK_RAW,htons(ETH_P_ALL))

Il est nécessaire de préciser certains paramètres :

dest.sll_family=AF_PACKET ; // Mode paquet

dest.sll_pkttype=PACKET_HOST ; //Type du paquet host,broadcast...

dest.sll_halen=6 ; // Taille de l'adresse MAC en octets

dest.sll_protocol = htons(ETH_P_ALL) ; // Protocole Ethernet

dest.sll_ifindex = 3 ; //Index de l'interface sans fil

L'index est une valeur utilisée par le système d'exploitation pour numéroter les interfaces réseaux. Il est nécessaire d'identifier ce numéro pour que les informations envoyées ou reçues sur cette socket utilisent la bonne carte.

Un espace mémoire tampon (buffer) doit être créé pour que son contenu soit envoyé sur le réseau par l'intermédiaire de la socket. Etant donné que les piles de protocoles ne sont pas respectées on doit insérer au début du buffer les informations d'en-têtes appropriées, dans notre cas on utilise le format de la trame 802.11 (fourni dans l'annexe A). Voici la

structure créée dans l'application.

```
struct hostap_ieee80211_hdr
u16 frame_control;
u16 duration_id;
u8 addr1[6];
u8 addr2[6];
u8 addr3[6];
u16 seq_ctrl;
u8 addr4[6];
__attribute__ ((packed));
```

Le champs Frame Control permet en particulier de spécifier le type de trame (les différents types de trames : beacon, probe ou trames de données)

Les trois champs adresse sont les adresses MAC des stations communicantes et l'adresse du point d'accès dans le cas d'une communication en mode infrastructure.

Annexe C

Code Applications

Cette annexe présente quelques unes des applications utilisées pour effectuer les mesures de performances du handover. Une première application montre comment utiliser les sockets RAW, création et envoi d'une certaine quantité de données.

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h> // close
#include "sl2-send.h"

#include <features.h>    /* pour avoir la version GlibC */
#if __GLIBC__ >= 2 && __GLIBC_MINOR >= 1
#include <netpacket/packet.h>
#include <net/ethernet.h>     /* protocoles L2 */
#else
#include <asm/types.h>
#include <linux/if_packet.h>
#include <linux/if_ether.h>   /* protocoles L2 */
#endif


int main(int argc,char *argv[])
```

```
{
int sok,n,i;
struct sockaddr_ll dest,source;
char buf[800];
struct ethhdr ether_header;
char hw_source_addr[ETH_ALEN] = {0x00, 0xE0, 0x98, 0xB5, 0x1F, 0x14};
//char hw_dest_addr[ETH_ALEN] = {0x00, 0x30, 0xBD, 0x61, 0x0A, 0x59};

//Adresse MAC Eth0 PCFixe 00:0B:6A:52:72:08
//Adresse MAC Eth1 PCFixe 00:E0:98:B5:1F:14
//Adresse MAC Wlan0 Portable 00:30:BD:61:0A:59
//Adresse carte bruno 00 30 bd 61 0b 53
char hw_dest_addr[ETH_ALEN] = {0x00, 0x30, 0xBD, 0x61, 0x0B, 0x53};

//--------------------------------------------------------------------
//  DROITS D'UTILISATION
//--------------------------------------------------------------------

printf("User ID : %ld Group ID : %ld Effective UID : %ld GID : %ld\n",getuid(),getgid(),geteuid(),getegid());
if (setuid(0)!=0) // for UNIX
//if (setuid(544)!=0) // for WINDOWS
{
printf("Could not switch to Super User !!!\n");
exit(2);
}
printf("User ID : %ld Group ID : %ld Effective UID : %ld GID : %ld\n",getuid(),getgid(),geteuid(),getegid());


//-------------------------------------------------------------------------------
//  OUVERTURE DE LA SOCKET
//-------------------------------------------------------------------------------

    if ((sok=socket(PF_PACKET,SOCK_RAW,htons(ETH_P_ALL)))<0)
    {
        printf("Erreur socket !!!\n");
        exit(2);
    }

//-------------------------------------------------------------------------------
//  PARAMETRES D'ENVOI
//-------------------------------------------------------------------------------
```

```
dest.sll_family=AF_PACKET; // Mode paquet
//dest.sll_pkttype=PACKET_HOST; //Type du paquet host,broadcast...
dest.sll_halen=6; // Taille de l'adresse MAC en octets
dest.sll_protocol = htons(ETH_P_ALL);
//dest.sll_ifindex = 2; //Index de l'interface filaire
dest.sll_ifindex = 3; //Index de l'interface sans fil

memcpy(dest.sll_addr,hw_source_addr, ETH_ALEN);
memcpy (source.sll_addr, hw_source_addr, ETH_ALEN);

//Construction en-tete Ethernet
memcpy (ether_header.h_dest, hw_dest_addr, ETH_ALEN);
memcpy (ether_header.h_source, source.sll_addr,ETH_ALEN);

// Copie de l'en-tete ethernet dans le buffer d'envoi 14 octets
memcpy (buf, &ether_header, sizeof(ether_header));

//Ajout d'un message dans le buffer
buf[16]='t';buf[17]='o';buf[18]='t';buf[19]='o';

//---------------------------------------------------------------
//  ENVOI DU PAQUET
//---------------------------------------------------------------

     for(i=1;i<=1;i++)
     {
     n=sendto(sok,(char*)buf,sizeof(buf),0,(struct sockaddr*)&dest,sizeof(dest));
     //printf("Envoi de : %d octets\n",n);
     }

//---------------------------------------------------------------
//  RECPETION DU PAQUET
//---------------------------------------------------------------

close(sok);
}
```

Cette deuxième application est utilisée pour la réception de données. Elle récupère les trames reçues sur une carte réseau donnée et les tris selon le type de paquet (packet_host

si il s'agit d'un paquet destiné à cette station, packet_broadcast pour les trames de diffusion etc).

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h> // close
#include "sl2-recv.h"

#include <features.h>    /* pour avoir la version GlibC */
#if __GLIBC__ >= 2 && __GLIBC_MINOR >= 1
#include <netpacket/packet.h>
#include <net/ethernet.h>     /* protocoles L2 */
#else
#include <asm/types.h>
#include <linux/if_packet.h>
#include <linux/if_ether.h>   /* protocoles L2 */
#endif

int main(int argc,char *argv[])
{

int sok,n,count=0;
struct sockaddr_ll dest,source;
socklen_t len;
char buf[800];
char hw_dest_addr[ETH_ALEN] = {0x00, 0x0B, 0x6A, 0x52, 0x72, 0x08};
//--------------------------------------------------------------------
//  DROITS D'UTILISATION
//--------------------------------------------------------------------

printf("User ID : %ld Group ID : %ld Effective UID : %ld GID : %ld\n",getuid(),getgid(),geteuid(),getegid());
if (setuid(0)!=0) // for UNIX
//if (setuid(544)!=0) // for WINDOWS
{
printf("Could not switch to Super User !!!\n");
exit(2);
}
```

```
printf("User ID : %ld Group ID : %ld Effective UID : %ld GID : %ld\n",getuid(),getgid(),geteuid(),getegid());


//------------------------------------------------------------------------------
//  PARAMETRES RECEPTION
//------------------------------------------------------------------------------

dest.sll_family=AF_PACKET;
dest.sll_pkttype=PACKET_HOST;
//dest.sll_halen=6;
dest.sll_protocol = htons(ETH_P_ALL);
//dest.sll_ifindex = 2; //Index carte filaire
dest.sll_ifindex = 3; //Index carte sans fil
memcpy(dest.sll_addr,hw_dest_addr, ETH_ALEN);
memcpy (source.sll_addr, hw_dest_addr, ETH_ALEN);

//------------------------------------------------------------------------------
//  OUVERTURE DE LA SOCKET
//------------------------------------------------------------------------------

    if ((sok=socket(PF_PACKET,SOCK_RAW,htons(ETH_P_ALL)))<0)
    {
        printf("Erreur socket !!!\n");
        exit(2);
    }

//-----------------------------------------------------------------
//  RECEPTION DE PAQUETS
//-----------------------------------------------------------------

     len=sizeof(struct sockaddr);
     bind (sok,(struct sockaddr*)&dest,len);
     printf ("Index interface: %d\n", dest.sll_ifindex);
     printf ("Adresse Mac interface: %.2x %.2x %.2x %.2x %.2x %.2x %.2x %.2x \n",dest.sll_addr[0],dest.sll_addr[1],dest.s

     while(1)
     {
      if((n=recvfrom(sok,buf,800,0,(struct sockaddr*)&dest,&len))<0)
      {
printf("ERREUR \n");
      }
      else
```

```
      {


switch (dest.sll_pkttype)
{
       case PACKET_HOST:       {
printf("Host \n");

break;
}
       case PACKET_BROADCAST: printf("Broadcast \n"); break;
       case PACKET_MULTICAST: printf("Multicast \n"); break;
       case PACKET_OTHERHOST: printf("Other host \n"); break;
       case PACKET_OUTGOING:  printf("Outgoing \n"); break;
     default: printf("Autre type \n");break;
}
if(buf[40]=='t' && buf[41]=='o')
      {
//printf("Reception de: %d octets\n",n);
      printf("Buffer : %c %c %c %c \n",buf[40],buf[41],buf[42],buf[43]);
printf("Nombre de paquets toto: %d \n",count);
count++;
     }
      }
     } //Fin while

//---------------------------------------------------------------
//  FERMETURE SOCKET
//---------------------------------------------------------------

close(sok);

}
```

Ce dernier exemple utilise une structure conforme à l'entête 802.11 pour qu'on puisse créer des trames reconnues comme trames 802.11 par d'autres machines. On peut voir l'initialisation des différents champs, par exemple le champs FC qui permet de définir le type de trame 802.11 qu'on souhaite envoyer puisqu'il est possible de générer aussi bien

de trames de données que des trames de gestion (Beacon, Probe, Acquittements etc).

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h> // close
#include "send80211.h"

#include <features.h>    /* pour avoir la version GlibC */
#if __GLIBC__ >= 2 && __GLIBC_MINOR >= 1
#include <netpacket/packet.h>
#include <net/ethernet.h>     /* protocoles L2 */
#else
#include <asm/types.h>
#include <linux/if_packet.h>
#include <linux/if_ether.h>   /* protocoles L2 */
#endif

#include<hostap_80211.h>

#define ETH_P_80211_RAW        (ETH_P_ECONET + 1)

int main(int argc,char *argv[])
{
int sok,n,i;
struct sockaddr_ll dest,source;
char buf[800];
//struct ethhdr ether_header;
struct hostap_ieee80211_hdr ether_80211_header;
char hw_source_addr[ETH_ALEN] = {0x00, 0xE0, 0x98, 0xB5, 0x1F, 0x14};
//char hw_dest_addr[ETH_ALEN] = {0x00, 0x30, 0xBD, 0x61, 0x0A, 0x59};

//Adresse MAC Eth0 PCFixe 00:0B:6A:52:72:08
//Adresse MAC Eth1 PCFixe 00:E0:98:B5:1F:14
//Adresse MAC Wlan0 Portable 00:30:BD:61:0A:59
//Adresse carte bruno 00 30 bd 61 0b 53
char hw_dest_addr[ETH_ALEN] = {0x00, 0x30, 0xBD, 0x61, 0x0B, 0x53};
```

```
//u16 frame_c=0;
u16 frame_c=0x4818;
u16 dur_id=258;

ether_80211_header.seq_ctrl=0;

//---------------------------------------------------------------------
//  DROITS D'UTILISATION
//---------------------------------------------------------------------

printf("%d\n",sizeof(int));
printf("%d\n",sizeof(short int));
printf("%d\n",sizeof(long int));


printf("User ID : %ld Group ID : %ld Effective UID : %ld GID : %ld\n",getuid(),getgid(),geteuid(),getegid());
if (setuid(0)!=0) // for UNIX
//if (setuid(544)!=0) // for WINDOWS
{
printf("Could not switch to Super User !!!\n");
exit(2);
}
printf("User ID : %ld Group ID : %ld Effective UID : %ld GID : %ld\n",getuid(),getgid(),geteuid(),getegid());


//---------------------------------------------------------------------------------
//  OUVERTURE DE LA SOCKET
//---------------------------------------------------------------------------------

    if ((sok=socket(PF_PACKET,SOCK_RAW,htons(ETH_P_ALL)))<0)
    {
        printf("Erreur socket !!!\n");
        exit(2);
    }

//---------------------------------------------------------------------------------
//  PARAMETRES D'ENVOI
//---------------------------------------------------------------------------------

dest.sll_family=AF_PACKET; // Mode paquet
//dest.sll_pkttype=PACKET_HOST; //Type du paquet host,broadcast...
```

```
dest.sll_halen=6; // Taille de l'adresse MAC en octets
dest.sll_protocol = htons(ETH_P_ALL);
//dest.sll_ifindex = 2; //Index de l'interface filaire
dest.sll_ifindex = 3; //Index de l'interface sans fil

memcpy(dest.sll_addr,hw_source_addr, ETH_ALEN);
memcpy (source.sll_addr, hw_source_addr, ETH_ALEN);

//Construction en-tete Ethernet
//memcpy (ether_header.h_dest, hw_dest_addr, ETH_ALEN);
//memcpy (ether_header.h_source, source.sll_addr,ETH_ALEN);


//memcpy(ether_80211_header.frame_control,frame_c,sizeof(u16));
//memcpy(ether_80211_header.duration_id,dur_id,sizeof(u16));
ether_80211_header.frame_control=frame_c;
ether_80211_header.duration_id=dur_id;

memcpy(ether_80211_header.addr1,hw_dest_addr,ETH_ALEN);
memcpy(ether_80211_header.addr2,hw_dest_addr,ETH_ALEN);
memcpy(ether_80211_header.addr3,hw_dest_addr,ETH_ALEN);
//memcpy(ether_80211_header.addr4,hw_dest_addr, ETH_ALEN);


// Copie de l'en-tete ethernet dans le buffer d'envoi 14 octets
memcpy (buf,&ether_80211_header,IEEE80211_DATA_HDR4_LEN);



//Ajout d'un message dans le buffer
buf[40]='t';buf[41]='o';buf[42]='t';buf[43]='o';

//---------------------------------------------------------------
//  ENVOI DU PAQUET
//---------------------------------------------------------------

     for(i=1;i<=1;i++)
     {
     n=sendto(sok,(char*)buf,sizeof(buf),0,(struct sockaddr*)&dest,sizeof(dest));
     //printf("Envoi de : %d octets\n",n);
     }
```

```
//---------------------------------------------------------------
//  RECPETION DU PAQUET
//---------------------------------------------------------------

close(sok);
}
```

Annexe D

Le driver HostAP

Voici quelques extraits du fichier README fourni avec le driver HostAP. La version complète de ce document ainsi que le driver HostAP sont disponibles sur le site http ://hostap.epitest.fi.

```
Host AP driver for Intersil Prism2/2.5/3
========================================

Copyright (c) 2001-2002, SSH Communications Security Corp and Jouni Malinen
Copyright (c) 2002-2005, Jouni Malinen
Author: Jouni Malinen <jkmaline@cc.hut.fi>

This program is free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License version 2 as
published by the Free Software Foundation. See COPYING for more
details.


Installation and configuration
==============================


The driver supports Linux Wireless Extensions and certain configuration
items can be viewed and changed with iwconfig(8) and iwpriv(8) from
wireless utilities, e.g., mode (AP/station; iwconfig's 'mode'),
channel (iwconfig's 'freq' or 'channel'), WEP (encryption; iwconfig's
'key').
```

```
TODO: list example iwconfig commands and explain what they do

Current driver supports following iwpriv commands:

iwpriv wlan0 monitor <val>      [DEPRECATED]
    see 'IEEE 802.11 monitoring' below

iwpriv wlan0 prism2_param <param> <val>
    see list below for different parameters
    see prism2_param wrapper in hostap-utils package if using
    old version of iwpriv.

iwpriv wlan0 readmif <2*CR>
iwpriv wlan0 writemif <2*CR> <val>
    testing commands that allow low-level access to baseband processor
    configuration registers; do *NOT* use these, unless you are sure what
    you are doing; these do not have error checking and it may be
    possible to cause physical damage to your equipment by setting invalid
    values

iwpriv wlan0 reset <val>
    0: perform soft reset of the card
    1: perform COR sreset (almost hardreset ;-)
    2: perform port reset (disable and enable port 0)
    3: disable port 0
    4: enable port 0

iwpriv wlan0 inquire <val>
    use inquire command; debugging only

iwpriv wlan0 wds_add <mac addr>
iwpriv wlan0 wds_del <mac addr>
    add/remove WDS links (see WDS below)

iwpriv wlan0 set_rid_word <rid> <value>
    debug command for setting RIDs that are two bytes long; you may need
    to specify RID and value in decimal format (i.e. 64512, not 0xFC00)

iwpriv wlan0 maccmd <val>
    0: open policy for ACL (default)
    1: allow policy for ACL
    2: deny policy for ACL
```

```
    3: flush MAC access control list
    4: kick all authenticated stations

iwpriv wlan0 addmac <mac addr>
    add mac addr into access control list

iwpriv wlan0 delmac <mac addr>
    remove mac addr from access control list

iwpriv wlan0 kickmac <mac addr>
    kick authenticated station from AP

prism2_param
------------

prism2_param is an extentsion to private ioctls; it uses ioctl
sub-type to provide number of configuration items for the
driver. iwpriv from the latest version of Linux wireless tools and
receive Linux wireless extensions support these sub-ioctls
directly. Older versions can use prism2_param wrapper from the
hostap-utils package for setting these parameters.

Following parameters are currently supported. These can be set using
'iwpriv wlan# <param_name> <value>' or 'prism2_param wlan#
<param_name> <value>'. Most values can be read with 'iwpriv wlan#
get<param_name>' or 'prism2_param wlan# <param_name>'.

txratectrl:
    0 = use host driver based TX rate control (default),
    1 = use f/w based TX rate control
beacon_int: beacon interval (1 = 1024 usec)
dtim_period: DTIM period, i.e., number of beacon intervals between
    successive delivery traffic identification maps (DTIMs),
    used for power saving and multicast/broadcast delivery
pseudo_ibss:
    0 = use IEEE 802.11 IBSS mode (default),
    1 = use pseudo adhoc mode (no management frames)
other_ap_policy:
    0 = skip all beacons
    1 = accept beacons with our SSID
    2 = accept beacons from all APs
    3 = accept all beacons (even from IBSS)
```

```
dump: set RX/TX/TXEXC debug dump header bitfield
    0 = do not dump frame headers
    1 = dump RX frame headers
    2 = dump TX frame headers
    4 = dump TX error frame headers
    (these values can be bitwise ORed; e.g. 3 = both RX and TX)
ap_max_inactivity: Time (in seconds) after which inactive stations
    can be removed from AP's station list
ap_bridge_packets:
    0 = do not bridge packets between associated stations, i.e.,
        just pass them to upper layers for handling
    1 = bridge packets directly between associated stations, i.e.,
        upper layers do not even see these packets
ap_nullfunc_ack:
    0 = let station firmware take care of data::nullfunc ACKs
    1 = send "extra" ACKs for data::nullfunc frames to workaround
        problems with stations using PS mode
    (default 1 if STA f/w version is 0.8.0, otherwise 0)
max_wds: maximum number of allowed WDS connections (default 16)
autom_ap_wds:
    0 = add WDS connections manually
    1 = add WDS connections automatically to all recorded APs
        (based on other_ap_policy)
ap_auth_algs: allowed authentication algorithms
    0 = none (no authentication will succeed)
    1 = only open
    2 = only shared key
    3 = open or shared key (default)
monitor_allow_fcserr:
    0 = drop frames with FCS errors in monitor mode
    1 = pass also frames with FCS errors
host_encrypt:
    0 = do not use host encryption unless in Host AP mode
    1 = use host encryption in all modes
host_decrypt:
    0 = use WLAN card firmware to decrypt frames
    1 = use host driver to decrypt frames
bus_master_threshold_rx:
    packet length threshold for using PCI bus master on RX
    (only used with hostap_pci.o and if PRISM2_BUS_MASTER is set)
bus_master_threshold_tx:
    packet length threshold for using PCI bus master on TX
```

```
    (only used with hostap_pci.o and if PRISM2_BUS_MASTER is set)
host_roaming:
    0 = use station firmware for roaming decision (default)
    1 = use host driver roaming decision (automatic scan)
    2 = manual scan and roaming
bcrx_sta_key:
    0 = use station specific key (WEP key mapping) to override
        default keys only for RX frames sent to unicast address
        ("individual RA") (default)
    1 = use station specific key also with broadcast RX frames
        (this is against IEEE 802.11, but makes it easier to use
        different keys with stations that do not support WEP key
        mapping)
ieee_802_1x:
    0 = do not use IEEE 802.1X specific functionality (default)
    1 = use IEEE 802.1X: require 802.1X auth, filter EAPOL packets
antsel_tx:
    0 = do not touch TX AntSel, i.e., use card default (default)
    1 = use antenna diversity
    2 = force TX AntSel pin low
    3 = force TX AntSel pin high
antsel_rx:
    0 = do not touch RX AntSel, i.e., use card default (default)
    1 = use antenna diversity
    2 = force RX AntSel pin low
    3 = force RX AntSel pin high
monitor_type:
    0 = IEEE 802.11 headers (ARPHRD_IEEE80211)
    1 = Prism2 + IEEE 802.11 headers (ARPHRD_IEEE80211_PRISM)
    2 = AVS monitor header + IEEE 802.11 headers
        (ARPHRD_IEEE80211_PRISM)
wds_type: WDS type bitfield
    0 = options disabled (default)
    1 = use broadcast RA (WDS frame destination) for broadcast and
        multicast frames
    2 = use AP client mode in 'Managed mode'
    4 = use standard compliant WDS (4 addr) frame also in Host AP
        mode (Note! This requires STA f/w ver 1.5.x or newer)
hostscan: perform non-destructive AP scanning (i.e., maintain current
      association state); this requires STA f/w ver 1.3.1 or newer
    1 = send Probe Request at 1 Mbps
    2 = send Probe Request at 2 Mbps
```

```
    3 = send Probe Request at 5.5 Mbps
    4 = send Probe Request at 11 Mbps
ap_scan: interval (in seconds) between passive AP scans on different
    channels, 0 = disabled (default)
enh_sec: "enhanced security" bitfield
    0 = options disabled (default)
    1 = hide SSID in beacon frames
    2 = ignore clients configured with "ANY" (broadcast) SSID
    (3 = both options)
    Note! This requires STA f/w ver 1.6.3 or newer
basic_rates: basic transmit rate bitmap
    bit 0: 1 M, bit 1: 2 M, bit 2: 5.5 M, bit 3: 11 M
    (default 3: 1 and 2 Mbps)
oper_rates: operational transmit rate bitmap
    bit 0: 1 M, bit 1: 2 M, bit 2: 5.5 M, bit 3: 11 M
    (default 15: 1, 2, 5.5, and 11 Mbps)
    Note! This changes the same value as iwconfig rate command, but
    as a bitfield.
hostapd: hostapd mode configuration
    0 = use kernel driver for IEEE 802.11 management
    1 = use user space daemon, hostapd, for IEEE 802.11 management
hostapd_sta: hostapd mode configuration
    0 = no extra STA interface
    1 = use hostapd to control extra STA interface (wlan#sta)



IEEE 802.11 monitoring
======================

Prism2/2.5/3 cards have a test mode that can be used for monitoring wireless
networks. In this mode the driver receives all raw IEEE 802.11 frames
(including management frames).

Monitor mode is enabled with 'iwconfig wlan0 mode monitor'. Monitor
mode was added to wireless tools version 25. With later versions, you
cannot use iwconfig, so please either upgrade wireless tools or use
old iwpriv monitor method described below.

'prism2_param wlan0 monitor_type <val>' can be used to select which
headers are included in the monitored frames (0: IEEE 802.11,
```

1: Prism2 + IEEE 802.11).

Previously, monitoring mode was started using iwpriv(8). This is now deprecated and it is currently implemented as a backward compatibility wrapper for iwconfig mode command. It may be removed in the future versions of the driver.

iwpriv wlan0 monitor 2
    start monitor mode and send received frames (including 802.11 header) to user space using normal netdevice. This changes the device type to ARPHRD_IEEE80211 so that user space programs know how to handle different header type.
iwpriv wlan0 monitor 3
    start monitor mode and send received frames (including Prism2 RX data and 802.11 header) to user space using normal netdevice. This changes the device type to ARPHRD_IEEE80211_PRISM so that user space programs know how to handle different header type.

iwpriv wlan0 monitor 0
    disable monitor mode and return to Host AP mode

Example program in 'sniff', wlansniff.c, is a simple 802.11 frame parser that shows both the Prism2/2.5/3-specific data from the RX frame and parsed contents of the 802.11 frame.

Latest versions of libpcap and Ethereal support ARPHRD_IEEE80211 and ARPHRD_IEEE80211_PRISM, so monitor modes 2 and 3 can be used with them for real time IEEE 802.11 network monitoring.

Roaming in station mode
=======================

Host AP driver supports three different modes for roaming in station modes (Managed/Ad-hoc). These are configured with prism2_param host_roaming.

Firmware-based roaming (mode 0; default)

```
Station firmware decides when to scan channels for APs and which AP to
use. Host AP driver only configured SSID and possible WEP keys, but
does not control AP selection in any other ways.

Host-based roaming (mode 1)
---------------------------

Station firmware decides when to scan channels for APs and informs
Host AP driver about scan results. Host AP driver will then select
which AP to use. Current version of the selection code is quite
simple, the driver just selects the first entry in the list of APs
(which should be sorted by signal quality). In addition, this mode
allows user to specify preferred AP with 'iwconfig wlan0 ap
<bssid>'. This preferred AP will be used if it is in the list of scan
results. User will also need to set SSID.

Manual scan and roaming (mode 2)
--------------------------------

Both scanning and AP selection are left to user; neither firmware nor
Host AP driver initialize scanning automatically. User space programs
can use Linux wireless extensions to initialize scanning and joining
an AP. Active IEEE 802.11 scanning is not required; any other external
mean can be used to get knowledge about the AP configuration.

Example commands:

# enable manual scan and roaming in managed (infra/BSS) mode
iwpriv wlan0 host_roaming 2
iwconfig wlan0 mode managed

# scan channels; set broadcast SSID ('Any') to accept all SSIDs in scan
# results. Optionally, could also set WEP keys, if needed.
iwconfig wlan0 essid any
iwlist wlan0 scan

# Select AP with SSID foobar and BSSID 00:11:22:33:44:55
iwconfig wlan0 essid foobar
iwconfig wlan0 ap 00:11:22:33:44:55

Note: both SSID and BSSID must be set in order to make association
```

work. Setting BSSID with 'ap' command must be done after SSID is set since this commands triggers join request for Prism2 firmware.

Note: scanning is limited to current SSID. If information about other APs is required, SSID must be set to 'Any'. However, this will remove current association. Alternatively, host scan command, 'iwpriv wlan0 hostscan 1', can be used without breaking the connection. This command requires STA f/w version 1.3.1 or newer. In addition, current version of the driver shows hostscan results only in the kernel log ('dmesg').