# De l'exploitation des réceptions opportunistes dans les mécanismes de relayage pour les réseaux sans-fil

Lucien Loiseau

**N° d'ordre** : 2013telb0282

**Sous le sceau de l'Université européenne de Bretagne**

# Télécom Bretagne

**En habilitation conjointe avec l'Université de** Rennes 1

École Doctorale – MATISSE

---

# De l'exploitation des réceptions opportunistes dans les mécanismes de relayage pour les réseaux sans-fil

---

## Thèse de Doctorat

Mention : « Informatique »

Présentée par **Lucien Loiseau**

Département : Réseaux, Sécurité et Multimédia (RSM)

Laboratoire : IRISA

Directeur de thèse : Xavier Lagrange

Soutenue le 6 Décembre 2013

**Jury :**

M. VIHO César - Professeur à l'Université Rennes 1
M. NOEL Thomas - Professeur à l'Université de Strasbourg
M. CHAOUCHI Hakima - Professeur à Télécom SudParis
M. HEUSSE Martin - Professeur à l'Ensimag
M. LAGRANGE Xavier - Professeur à Télécom Bretagne
M. MONTAVONT Nicolas - Maître de conférences à Télécom Bretagne

# Résumé

Les réseaux sans-fil tels que IEEE 802.11 (Wifi) connaissent aujourd'hui une popularité sans précédent, offrant des connexions réseau à domicile, en entreprise ou dans des lieux publics sous forme de «*Hot spot*». Un nouveau concept a même vu le jour récemment, appelé réseau communautaire. Cette mouvance propose de partager les accès 802.11 entre plusieurs utilisateurs, afin d'étendre les couvertures radios jusqu'à couvrir des villes entières. Nous avons mesuré que plus de 90% des villes sont couvertes par ce type de réseau en France. Cependant, la technologie a ses limites : les stations clientes doivent être proches du points d'accès ; sinon, elles peuvent monopoliser le canal de transmission car elles adaptent leur modulation à leur qualité de lien et transmettent à bas débit.

Nous nous sommes alors intéressés aux mécanismes de relayage de trames entre les stations. L'objectif d'un relayage est de pouvoir compter sur des stations ayant une bonne qualité de lien pour relayer les trames des stations les plus lointaines. Ces mécanismes tendent à effacer la frontière entre les réseaux à infrastructure (avec points d'accès) et les réseaux sans-fil multi-sauts, où les stations communiquent directement entre elles. Nous avons analysé les mécanismes et les protocoles des réseaux sans-fil multi-sauts et plus particulièrement la façon dont ces protocoles appréhendent la variabilité du canal sans-fil pour le mécanisme de relayage. Nous étudions les différentes techniques permettant d'optimiser le relayage et nous fournissons une présentation de synthèse de cette large analyse.

Nous avons alors proposé une nouvelle méthode de relayage opportuniste pour les réseaux basés sur le CSMA/CA. La station qui prend en charge le relayage est choisie dynamiquement lors de la transmission des données, ce qui permet de tenir compte de la qualité intrinsèquement variable du canal radio et fournit méthode efficace pour exploiter la diversité spatiale et temporelle des réseaux sans-fil. En évitant l'inondation, et en réduisant au maximum la signalisation, nous proposons de légères modifications au standard IEEE 802.11 afin d'autoriser des stations intermédiaires de relayer des trames des autres stations. Les modifications apportées

portent simplement sur le traitement des trames à destination d'autrui, et une gestion différente des acquittements : lorsqu'une destination ne reçoit pas un acquittement, toutes les stations ayant reçu la trame considèrent qu'une retransmission est nécessaire. Ces dernières entreront en compétition pour retransmettre la trame si leur probabilité d'effectuer une transmission réussie est plus forte que la source. Nous avons implémenté et testé notre proposition dans le simulateur réseau NS-2, et les résultats démontrent que la connectivité des stations lointaines est fortement améliorée.

# Table des matières

CHAPITRE 1

# Introduction

## Sommaire

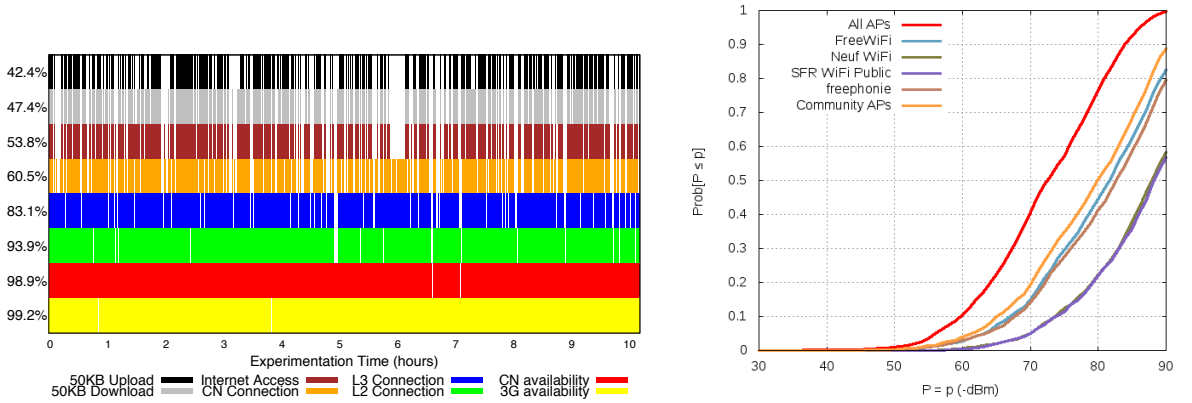


## 1.1 Contexte des travaux

Les réseaux sans-fil ont d'abord été introduits pour répondre à un besoin de mobilité dans nos télécommunications. Avec le développement d'Internet, ce besoin est devenu de plus en plus une nécessité du fait du rayonnement de ce réseau qui prend une place de plus en plus importante dans nos vie. Le succès d'Internet a nécessité le développement de réseaux d'accès plus ubiquitaires, motivant le développement de technologies sans-fil. Ce développement, couplé aux capacités industrielles de miniaturisation, a rendu le sans-fil omniprésent et a mené à l'élaboration de nombreux standards : ZigBee, Bluetooth, Wifi, GSM, 3G, LTE, DVS-B pour n'en citer que quelques-uns. La plupart de ces technologies permettent d'amener le support de la mobilité pour les appareils connectés mais se distinguent par la taille de la cellule offerte. Dans cette course, les **réseaux sans-fil locaux** tels que IEEE 802.11 jouent un rôle majeur grâce à leur faible coût de déploiement et aux débits élevés fournis par ce standard.

Cette technologie permet aux utilisateurs de déployer leur propre réseau sans-fil en le connectant directement à leur connexion Internet résidentielle. Différents fournisseurs d'accès à Internet offrent à leurs utilisateurs des points d'accès 802.11 qui ont la capacité de diffuser différents réseaux, appelés des *Service Set Identifier* (SSID).

Un de ces SSID est commun à tous les clients et est diffusé par tous les points d'accès (AP) de ce fournisseur d'accès Internet (FAI). Un client qui se trouve à portée de l'AP d'un autre client du même FAI peut ainsi bénéficier d'un accès Internet. Récemment, ces réseaux communautaires sont apparus comme une alternative viable aux réseaux $3G$ et $4G$ en fournissant un accès à Internet à bas coût et à haut débit. Dans le cadre du projet Wi2Me [CLM11], nous avons étudié le déploiement de ces réseaux communautaires dans la ville de Rennes en effectuant une campagne de recensement de ces réseaux. Cette campagne consistait à se déplacer dans la ville de Rennes muni d'un terminal mobile. Le terminal essayait continuellement de se connecter à ces réseaux communautaires et lorsque cela était possible, d'échanger des données avec un serveur que nous avions préalablement configuré.




(a) connectivité avec les AP communautaires le long du chemin

(b) Fonction de repartition (CDF) de la puissance reçue des AP

Figure 1.1 – Résultat de la campagne Wi2Me effectuée à Rennes

La figure 1.1 montre le résultat de cette campagne de test dans la ville de Rennes. Le temps (en heure) de l'expérimentation est donné en abscisse et le taux de connexion des différentes couches est donné en ordonnée. Chaque bande de couleur décrit une couche différente : la bande jaune indique la présence de la 3G ; la bande rouge indique la présence des réseaux communautaires (à la réception des *beacon*) ; les bandes vertes et bleues indiquent une connexion à un AP (couche MAC et IP) ; la bande orange indique une connexion réussie au portail communautaire et les bandes marrons, grises et noires indiquent une connexion réussie au serveur (*upload* et *download*). Cette figure montre que la présence des réseaux communautaires dans le centre ville est similaire à celle d'un réseau 3G. En revanche, du fait que ces points d'accès sont situés à l'intérieur des domiciles, l'atténuation du signal est importante, comme on peut le voir sur la figure 1.1b qui montre que dans $50\%$ des cas, la puissance reçue des AP communautaires est inférieure à $-80dBm$. Cette relative mauvaise qualité de lien avec les points d'accès impacte la capacité

des appareils connectés à être effectivement capables d'envoyer et de recevoir de l'information sur Internet. Cela est confirmé avec la figure 1.1a par la difficulté du terminal à maintenir une connectivité au niveau TCP. De $98.9\%$ de présence des réseaux communautaires, on passe à seulement environ $45\%$ de temps effectivement connecté. Ces résultats démontrent qu'il existe un potentiel très fort dans ces réseaux mais que l'état actuel de l'accès ne permet pas d'en profiter pleinement. Le problème vient sûrement du fait que les terminaux essaient de communiquer directement avec les AP, alors que les ceux-ci sont mal placés. Pour ce cas de figure, des protocoles existent pour faire du relayage entre des stations situées à proximité les unes des autres. Dans le reste de ce manuscrit, nous emploierons le terme station comme dans le standard IEEE 802.11, c'est-à-dire pour indiquer un terminal d'un réseau sans-fil.

Depuis près de $30$ ans, de nombreux travaux ont été effectués dans le cadre des réseaux sans-fil multi-sauts. Ces derniers reposent sur le relayage des paquets par les stations du réseau pour fournir une connectivité entre des stations qui ne seraient pas à portée autrement. En plus de gérer les contraintes liées à la technologie sans-fil, ces protocoles doivent faire face aux caractéristiques décentralisées et mobiles de ces réseaux. Les performances de ces réseaux dépendent directement de la capacité qu'ont ces protocoles à relayer les paquets efficacement. Les décisions de routage des paquets doivent ainsi s'adapter aux modifications de l'environnement en terme de topologie mais doivent également s'adapter à la variabilité des conditions du canal. Ces protocoles de routage servent donc deux fonctions que sont la construction de la topologie et la propagation des paquets par relayage successif de proche en proche jusqu'à la destination. Après plusieurs années d'étude par le milieu scientifique et académique, ces réseaux connaissent un nouvel essor avec le développement des réseaux de capteurs et de l'omniprésence des appareils mobiles rendant possible de nouveaux usages innovants. Ces nouveaux besoins industriels motivent le développement de protocoles plus performants qui répondent aux contraintes techniques.

## 1.2 Contributions

Notre principale contribution est la proposition d'un protocole de coopération pour les réseaux sans-fil qui efface la frontière entre réseaux d'infrastructure et réseaux sans-fil multi-sauts. Nous proposons un mécanisme original qui permet à des stations intermédiaires de relayer vers la destination des trames entendues de manière opportuniste. Notre protocole s'inscrit plus particulièrement dans le cadre des

réseaux basés sur le standard IEEE 802.11 mais pourrait s'appliquer à d'autres protocoles utilisant le mécanisme CSMA/CA comme 802.15.14 par exemple.

Dans un réseau de type CSMA/CA comme 802.11, une station retransmet plusieurs fois sa trame jusqu'à recevoir un ACK de sa destination. Dans le cas du mode infrastructure c'est le point d'accès qui envoie cet ACK, dans le cas d'un réseau multi-sauts il s'agit du prochain saut de routage. Si aucun ACK n'est reçu suivant une réception, la station émettrice fait l'hypothèse que la destination n'a pas reçu la trame et va donc tenter une retransmission après une phase de contention CSMA/CA. Une station 802.11 peut également utiliser un mode de transmission plus robuste face aux interférences mais offrant un débit moindre. Les retransmissions comme la diminution du débit ont pour effet de consommer plus de temps de canal et impactent le débit général de la cellule, et donc des autres stations. Nous mettons en évidence que l'usage d'un relais offre une contre-mesure plus efficace à la fois pour la station source qui peut transmettre à haut débit, mais aussi pour les stations environnantes. Nous proposons un nouveau protocole s'inscrivant dans la famille du routage opportuniste et tirant profit de la réception opportuniste des trames par des stations environnantes. Le relayage s'effectue de façon quasi-transparente et n'intervient que lorsqu'une trame n'a pas reçu d'acquittement et qu'une retransmission est nécessaire. Parce que le sans-fil est un support diffus, cette trame peut avoir été «entendue» par un certain nombre de récepteurs, certain pouvant même avoir une meilleure qualité de lien avec la destination que la source elle-même. Dans ce cas, notre protocole permet à ces stations de participer à la contention pour essayer de retransmettre la trame à la place de la destination. Ce protocole permet de tirer profit de la diversité des récepteurs plutôt que de se limiter à l'utilisation d'un seul relais. En déléguant ces dernières à des stations pouvant faire progresser la trame vers la destination de façon plus efficace que la source, nous visons à réduire le nombre de retransmissions totales effectuées sur le canal.

Premièrement, notre solution permet d'améliorer les performances d'une cellule 802.11 constituée de stations présentant des débits hétérogènes en motivant l'utilisation de plusieurs liens à haut débits *via* les relais. Deuxièmement, cette solution peut s'appliquer aux réseaux communautaires afin d'en améliorer l'accès en utilisant les stations proches d'un point d'accès comme relais. Cette application est d'autant plus viable que la densité des points d'accès et des utilisateurs est très forte dans les zones urbaines, comme nous l'avons montré dans notre expérimentation Wi2Me. Finalement, en optimisant le relayage, notre solution permet d'améliorer les performances

des réseaux sans-fil multi-sauts tel qu'un réseau *ad hoc* standard ou bien un réseaux de capteurs. Ces derniers sont souvent constitués d'une densité élevée de nœuds mais possédant des qualités de lien assez mauvaises. En réduisant le nombre de transmissions inutiles, notre solution permet d'économiser de l'énergie.

## 1.3 Plan de la thèse

Ce mémoire de thèse est organisé en trois chapitres. Dans le chapitre 2, nous discuterons des caractéristiques et des contraintes physiques du support de transmission sans-fil et nous décrirons les mécanismes d'accès au canal permettant d'assurer la communication dans cet environnement difficile. Nous étudierons avec plus d'attention le standard IEEE 802.11 sous l'angle de son déploiement réel mais également de ses limitations techniques. Nous mettrons en évidence l'intérêt du relayage dans ces réseaux pour améliorer les performances d'accès et des débits, ainsi que les différents facteurs limitant les performances des réseaux sans-fil locaux (mauvaise qualité de lien, adaptation de débit, retransmissions).

Dans le chapitre 3, nous étudierons les protocoles et stratégies existantes pour le routage dans le domaine des réseaux sans-fil mobiles et multi-sauts. Nous discuterons de ces stratégies sous l'angle des mécanismes de relayage et plus précisement de la rapidité de ces protocoles à réagir face aux modifications des conditions de l'environnement. Nous identifierons les caractéristiques pouvant répondre à la problématique posée, à la suite de quoi nous proposerons une taxonomie originale permettant de classifier les protocoles de routage suivant trois grandes familles.

Finalement, dans le chapitre 4, nous proposerons un nouveau mécanisme de relayage pour les réseaux sans-fil basés sur CSMA/CA qui vise à réduire le temps passé sur le canal pour transmettre une trame. Nous validerons notre proposition par simulation et analyserons l'impact de notre protocole sur les performances d'une cellule IEEE 802.11. Nous proposerons également une nouvelle métrique pour les protocoles de routage opportunistes.

CHAPITRE 2

# Les spécificités de la communication sans-fil

## Sommaire

## 2.1 Introduction

Les réseaux sans-fil permettent à au moins deux stations de communiquer à distance en utilisant les ondes électromagnétiques comme support de transmission de l'information. La diversité des gammes de fréquences disponibles permet un grand nombre de cas d'usages allant du fonctionnement d'une télécommande de télévision jusqu'aux satellites de télécommunications. De nos jours, ordinateurs portables, téléphone cellulaire, souris et clavier sans-fil, télévision numérique, le sans-fil est partout. Ceci s'explique par les propriétés très intéressantes qu'offrent les ondes électromagnétiques. C'est un support *immatériel*, pouvant *traverser* des obstacles, facile à déployer et offrant à des appareils connectés une aire de *mobilité* plus ou moins vaste (ex : GSM, WiFi). Ces gains ne sont pas cependant sans un ensemble de contraintes à prendre en compte lors de l'élaboration des protocoles de télécommunication. La forte *variabilité* du lien sans-fil entraîne une incertitude sur la fiabilité des transmissions effectuées. De plus, la nature *partagée* du support électromagnétique entraîne des possibilités de brouillage entre signaux de même nature et une rareté du spectre éléctromagnétique qui doit être géré de façon parcimonieuse pour éviter la saturation et la congestion du réseau. Ces caractéristiques rendent difficiles la transposition des techniques utilisées en filaire et ont nécessité l'élaboration de nouveaux mécanismes de codage du signal et d'accès au support. Dans ce chapitre nous nous intéresserons aux spécificités de la communication sans-fil d'un point de vue physique puis nous décrirons les problématiques liées aux méthodes d'accès au canal ainsi que les solutions existantes. Finalement, nous présenterons la norme IEEE 802.11 sur laquelle s'est basée notre travail.

## 2.2 Caractéristique du support radioélectrique

### 2.2.1 Bande de fréquence

Chaque technologie utilisant un support électromagnétique pour transmettre de l'information opère sur une (ou plusieurs) bande de fréquence qui lui est propre.

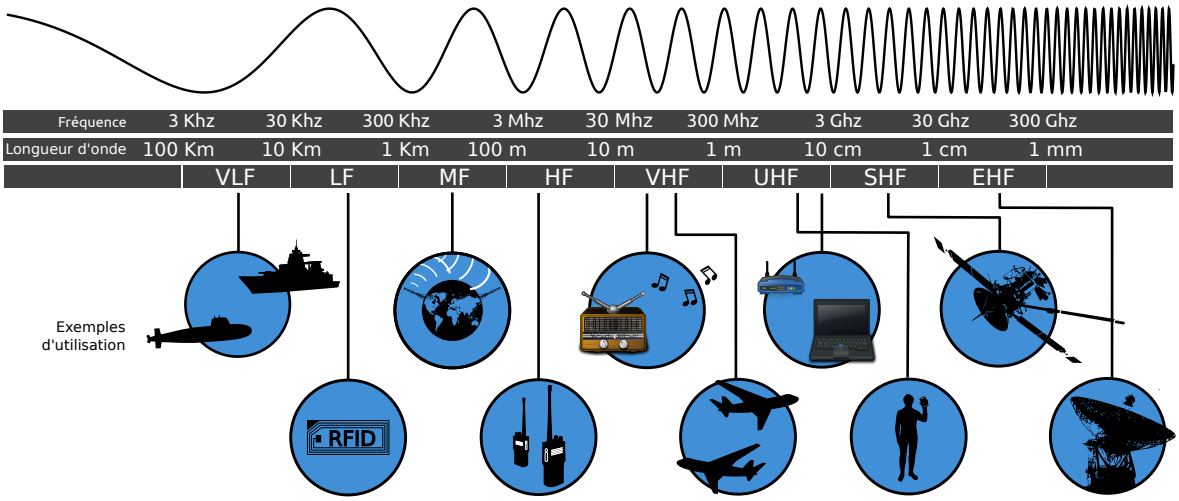



Figure 2.1 – Spectre Radioélectrique

En effet, chaque bande de fréquence a un mode de propagation privilégié se prêtant à des types de service particuliers. À titre d'exemple, le mode de propagation ionosphérique consiste à faire *rebondir* le signal radio contre la ionosphère. Cette propriété des ondes courtes, autour de 10 MHz, peut permettre d'atteindre un point à la surface du globe que l'on ne pourrait pas atteindre en ligne directe à cause de la courbure de la terre. Par ailleurs, plus la fréquence est élevée, plus l'atténuation du signal avec la distance est importante (l'atténuation du signal est plus «rapide») et moins le pouvoir de *pénétration* est important. Lorsque la fréquence de l'onde électromagnétique est inférieure à 300 GHz, on parle d'onde radioélectrique (ou onde radio). Dans cette thèse, notre travail se basant essentiellement sur la norme IEEE 802.11, notre travail s'effectuera autour des fréquences 2.4 GHz et 5 GHz, c'est-à-dire dans les ondes dites Ultra High Frequency (UHF)et Super High Frequency (SHF), comme le montre la figure 2.1 ci dessus.

Les technologies radioélectriques n'opèrent pas directement sur une fréquence pure mais sur un *canal* dont la largeur de bande (ou largeur de spectre) varie en fonction des besoins, et dont l'utilisation est régulée en France par l'Autorité de Régulation des Communications Électroniques et des Postes (ARCEP). L'expression du besoin en fréquence dépend donc de la richesse de l'information à véhiculer (voix, télévision, données), des paramètres techniques (fiabilité, codage) et des besoins ou des contraintes géographiques (niveaux de couverture, obstacles, mobilité des appareils connectés). La figure 2.1 présente quelques cas d'usage d'utilisation des fréquences. L'eau possédant un très fort pouvoir d'atténuation des ondes électromagnétiques, il a fallu utiliser des ondes très courtes dans la bande Very Low Frequency (VLF) pour

pouvoir communiquer avec des sous-marins jusqu'à 20 mètres sous la surface de la mer. Les radio-amateurs utilisent les bandes de hautes et moyennes fréquences (HF et MF) afin de profiter de la propagation ionosphérique pour pouvoir communiquer avec plusieurs points du globe. Les fréquences qui sont propices aux communications électroniques sont situées au voisinage de la bande UHF et sont utilisées par la télévision, le GSM, le Bluetooth, l'UMTS, le WiFi et bien d'autres encore.

### 2.2.2 Un lien évanescent, variable et asymétrique

Toute onde de nature électromagnétique subit une atténuation du signal qui est fonction inverse du carré de la distance. Si la distance est le principal facteur d'atténuation, il n'est pas le seul ; la température, l'humidité, la pression atmosphérique, les effets de multi-chemin (rebonds de l'onde contre un mur), la mobilité et les obstacles sont autant de facteurs influant sur la puissance du signal reçu par un récepteur. La qualité d'un signal radio se mesure par le rapport signal sur bruit appelé SNR (Signal Noise Ratio) qui est exprimé en décibel (dB)

La couverture d'une station sans-fil est l'aire autour de celle-ci dans laquelle la communication avec une autre station sans-fil est possible. Si cette aire est parfois schématiquement représentée par un cercle, ses contours sont en réalité flous et fluctuant avec le temps. Ce caractère aléatoire du sans-fil en fait un support particulièrement capricieux et difficilement prévisible. En particulier, la qualité d'un signal peut évoluer dans le temps de façon imprévisible. Aguayo *et al* [ABB+04] ont étudié ce phénomène sur des liaisons sans-fil WiFi avec des équipements fixes. La figure 2.2 empruntée à ces travaux montre bien que les liaisons sans-fil peuvent être très variables au cours du temps, même sur de toutes petites échelles comme on peut le voir par les micro-variations.

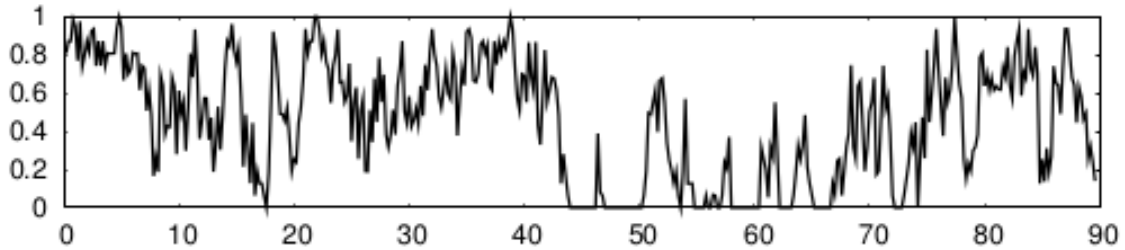



Figure 2.2 – Évolution du taux de perte (en ordonnée) au cours du temps (en secondes) sur une liaison 802.11 (Figure 7 dans [ABB+04])

De plus, les situations d'interférences (nœuds cachés, pollution électromagnétique) peuvent localement rendre difficile le décodage d'une trame. Comme l'environnement n'est pas le même entre deux stations communiquant ensembles, ces phénomènes peuvent provoquer une asymétrie de lien. Même lorsque des stations sont immobiles et dans un environnement similaire, ce phénomène existe et doit donc être pris en compte par les protocoles de télécommunication. Cerpa *et. al* [CBE03] en $2003$ a montré que dans une expérimentation effectuée en 802.11, le nombre de liens asymétriques pouvait monter jusqu'à $30\%$ (un lien étant déclaré asymétrique si la différence en terme de taux d'erreur dépassait $40\%$). Cela a été confirmé par une autre étude en $2007$, publié par Sang *et al* [SAZ07] qui montre que dans certains cas, $50\%$ des liens (sur 500 liens) présente des caractéristiques asymétriques parmi lesquels $7\%$ sont quasiment unidirectionnel (c'est-à-dire que la différence en terme de taux d'erreur dépasse $90\%$).

### 2.2.3 Une nature diffuse

En télécommunication, beaucoup de protocoles font abstraction de la nature du support électromagnétique donnant l'impression d'un lien point à point reliant deux stations. Cette abstraction cache cependant la nature diffuse des ondes électromagnétiques. Une antenne isotrope rayonne théoriquement uniformément dans toutes les directions formant ainsi naturellement une aire de réception autour de la station émettrice. La surface de cette aire est directement liée à l'atténuation du signal et donc de la fréquence et de la puissance à laquelle ce signal a été émis. Une station se trouvant à l'intérieur de cette aire, autour d'une station émettrice, peut ainsi recevoir le signal. Ce caractère diffus permet aussi bien à l'émetteur qu'au récepteur de se déplacer. La nature diffuse du support électromagnétique permet ainsi la mobilité aux stations connectées.

Mais cette nature diffuse va de paire avec le fait que deux stations émettant simultanément sur la même bande de fréquences peuvent brouiller leur signal, rendant toutes réception impossible. Il est possible de rendre plus directif un signal électromagnétique en utilisant des antennes plus spécifiques, réduisant l'angle de rayonnement dans laquelle la réception est possible (et donc la mobilité)

Aussi, afin d'éviter le brouillage involontaire des signaux, on utilise des méthodes d'accès au canal telles que celles décrites en 2.3.

### 2.2.4 Un lien half-duplex

Il n'est pas possible en sans-fil d'utiliser une seule antenne à la fois pour écouter et pour transmettre un signal simultanément sur la même fréquence. On peut établir une liaison full-duplex en utilisant au moins deux fréquences différentes, une pour le lien montant et une pour le lien descendant. Cette méthode est par exemple utilisée pour le GSM, mais cela nécessite d'opérer sur plusieurs plages de fréquence différentes.

Une communication sur une seule plage de fréquence impose d'attendre la réception d'un signal avant de pouvoir émettre. L'utilisation d'une deuxième antenne, sur la même fréquence, dédiée à la réception pour établir une liaison full-duplex n'est pas possible non plus car la proximité avec l'antenne émettrice provoque un phénomène d'aveuglement. En effet, la puissance reçue du signal émis par l'antenne émettrice au niveau de l'antenne réceptrice sera très importante, provoquant de très fortes interférences et aveuglant cette dernière complètement.

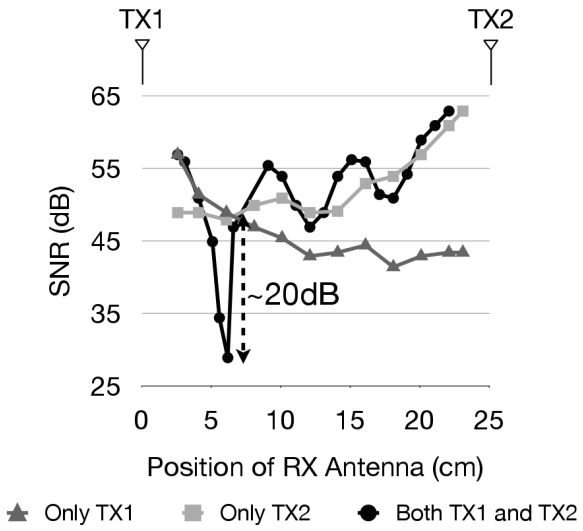



Figure 2.3 – puissance reçue d'un signal envoyé par deux antennes émettrices en fonction du placement de l'antenne réceptrice (Figure 4 dans [CJS+10])

On peut toutefois citer les travaux de Choi *et. al* [CJS+10] qui ont réussi à créer des liaisons full-duplex (sur une seule fréquence) en utilisant le principe de l'annulation d'antenne. Dans ces travaux, ils utilisent deux antennes pour transmettre et une antenne pour recevoir. Pour une longueur d'onde donnée $\lambda$, les deux antennes émettrices sont placées respectivement à une distance $d$ et $d + \frac{\lambda}{2}$ de l'antenne réceptrice. En plaçant les antennes ainsi, le même signal émis par les deux antennes s'annule au point de l'antenne réceptrice comme décrit la figure 2.3. À ce dispositif s'ajoutent des méthodes de traitement du signal permettant de finir de soustraire

le signal émis au signal reçu. Cette combinaison de deux techniques (création d'un *null spot* + traitement du signal) permet effectivement d'avoir un système capable de recevoir et d'émettre un signal en même temps, créant ainsi une liaison *full-duplex* avec une autre station. Cette approche est efficace pour *annuler* une fréquence pure mais reste toutefois limitée par la largeur de la plage de fréquence utilisée.

Ces techniques ne sont que rarement utilisées dans l'industrie et la plupart des standards de télécommunication existant (IEEE 802.11, UMTS, IEEE 802.15.4 etc.) n'implémente pas de lien sans-fil full duplex mono-fréquentielle. Dans la suite de cette thèse nous travaillerons sur IEEE 802.11 et ça ce titre, nous considérerons qu'un lien sans-fil n'est pas un lien full-duplex.

## 2.3 Les méthodes d'accès au canal

Les méthodes d'accès au canal décrivent l'ensemble des méthodes permettant de coordonner les accès au support partagé entre plusieurs stations. Plus spécifiquement, la couche MAC décrit les règles permettant à une station de transmettre et d'écouter. Ces règles sont écrites de façon à remplir un ensemble de services tels que l'équité (dans l'accès au canal ou dans les ressources utilisées), la fiabilité, le passage à l'échelle, la qualité de service et ce en maximisant les débits. Ce sont des protocoles de niveau 2 dans le modèle OSI et l'équivalent de la couche liaison dans le modèle TCP/IP. Ces protocoles sont critiques dans un environnement où les stations ne peuvent pas recevoir en même temps qu'elles émettent et dans lequel le support est partagé et en diffusion par nature.

### 2.3.1 Méthodes basées circuit

Les méthodes basées circuit permettent à deux stations d'établir un canal de communication dédié avant que la communication ne commence. Le circuit alloue ainsi des ressources qui ne seront libérées qu'à la fin de la communication. Ces méthodes permettent d'assurer une qualité de service mais limitent le nombre de stations qui peuvent se partager le canal simultanément. Il y a trois types de méthodes basées circuit que sont :

- Time Division Multiplexing Access (TDMA) permet de diviser le temps en une série de *time slots*, les *slots* étant ensuite distribués aux paires de stations voulant

communiquer. Cela permet ainsi à plusieurs stations de pouvoir communiquer sur une période de temps donnée.

- Frequency Division Multiplexing Access (FDMA) permet de diviser la largeur de bande disponible en petites plages de fréquence allouées indépendamment les unes des autres. Cela permet ainsi à plusieurs stations de communiquer simultanément, chacune opérant sur un canal différent.

- Code Division Multiplexing Access (CDMA) permet à plusieurs stations de se partager la même bande de fréquence, cependant leur signal est étalé au moyen d'un code particulier leur permettant d'être séparée par un récepteur au moyen de technique de décorrélation.

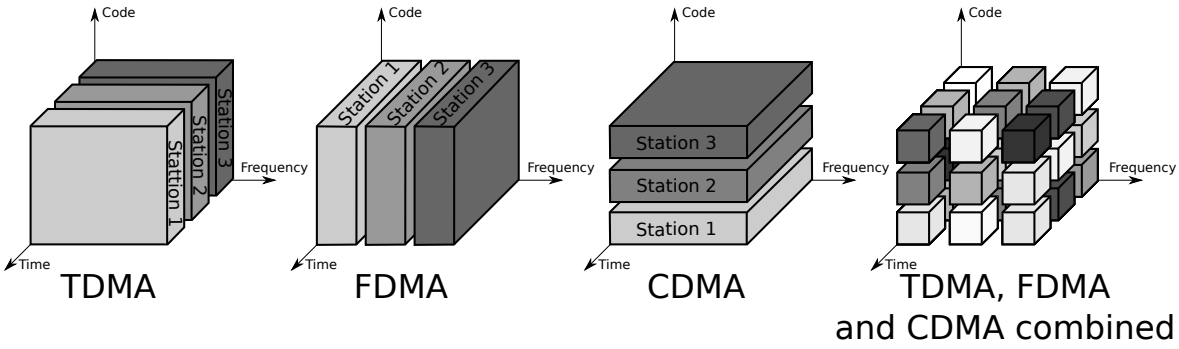



Figure 2.4 – Schéma de comparaison des techniques basées circuit TDMA, FDMA et CDMA

En théorie ces trois méthodes offrent exactement la même efficacité spectrale (bande passante), mais en pratique chacune de ces méthodes amène son lot de difficulté. Dans le cas de TDMA, les *timeslot* étant de l'ordre de la $\mu$s (576.9 $\mu$s pour le GSM), c'est la synchronisation temporelle des stations qui est l'aspect le plus important. Cette synchronisation est effectuée à l'aide de *beacons* envoyées périodiquement par la station de base. Avec FDMA, la difficulté se trouve au niveau du filtrage des fréquences. Dans le cas de GSM, la bande de fréquence de 25 MHz est divisé en 124 fenêtre de 200 Khz de largeur chacune. Et enfin CDMA se basant sur l'étalement de la puissance dans le spectre au moyen d'un code particulier, le contrôle de la puissance est l'aspect le plus important dans cette technique.

À titre d'exemple, le GSM utilise une combinaison de TDMA et de FDMA. Les réseaux de troisième génération tel que UMTS[1] utilisent CDMA en plus de FDMA et de TDMA.

[1] UMTS est connu sous le nom de **réseaux 3G**

### 2.3.2 Méthodes basées paquets

Dans les méthodes basées paquets, chaque trame est traitée individuellement et il n'y a pas de réservation de ressources. Les méthodes basées paquets sont similaires aux techniques de multiplexage temporelle mais ne s'effectuent pas de façon cyclique comme TDMA. Ces méthodes sont essentiellement basées sur une approche d'accès aléatoire au support avec des mécanismes supplémentaires permettant d'éviter des collisions ou de fournir un accès au support équitable parmi les stations compétitrices.

#### 2.3.2.1 Pure Aloha

Pure Aloha [Abr70] est une méthode d'accès au support très simple mise au point en 1968 à l'université de Hawaï pour ALOHAnet. L'idée d'ALOHAnet était de relier plusieurs îles dans une architecture de type *étoile* dans laquelle la station centrale était appelée le *Menehun*. Deux bandes de fréquences étaient dédiés pour la communication, une allant des stations vers le Menehun, le canal entrant, et une autre allant du Menehune vers les stations, aussi appelé canal sortant. Le protocole Aloha a ainsi été développé pour répondre au contrainte du canal entrant dans lequel plusieurs stations se partagent le même canal.

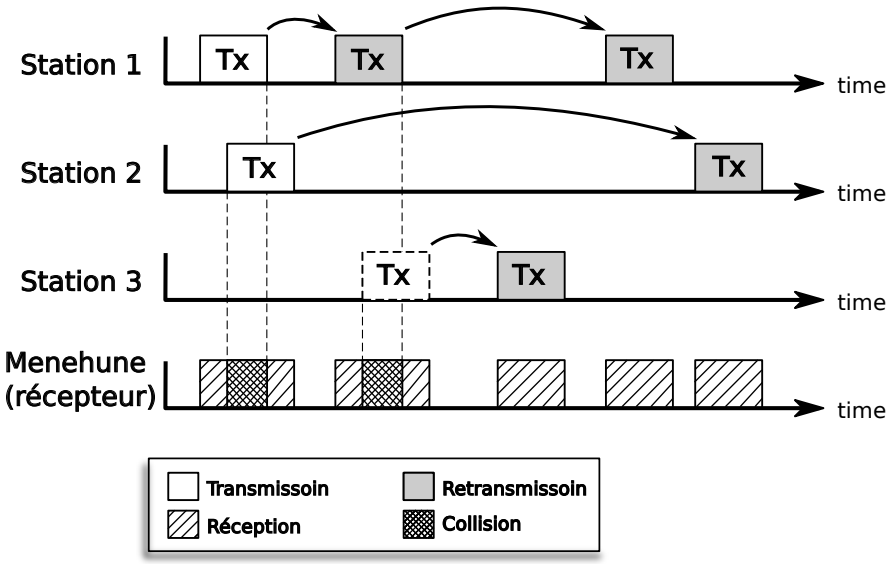



Figure 2.5 – Exemple de communication avec le protocole Pure Aloha

Lorsqu'une station souhaite émettre une trame, elle le transmet sur le canal entrant, quelles que soit les conditions de celui-ci. Chaque trame correctement reçue par la destination est alors acquittée (via le canal sortant) auprès de la source. Si

après un certain temps, la station émettrice n'a toujours pas reçu d'accusé, elle considère que la transmission a échoué et va retransmettre sa trame après un certain temps d'attente, choisi aléatoirement. La procédure est répétée autant de fois que nécessaire. Dans cette approche, plus le nombre d'émetteur est élevé, plus le nombre de collisions augmente. Comme les stations n'écoutent pas si le canal est libre avant d'émettre, une collision peut apparaître en milieu de transmission comme décrit sur la figure 2.5. Ce temps d'attente aléatoire entre la décision de retransmettre et la retransmission s'appelle le backoff, c'est un paramètre essentiel pour l'efficacité du protocole. Un protocole efficace est un protocole qui introduit peu de retransmission et qui ne perd pas de temps pour transmettre (afin d'optimiser la bande passante disponible). Plus le backoff est petit, plus la probabilité de collision entre deux retransmissions augmente. De la même façon, plus le backoff est long, plus une station passe de temps à attendre. La valeur du backoff doit donc être choisie en fonction des besoins.

#### 2.3.2.2 Slotted Aloha

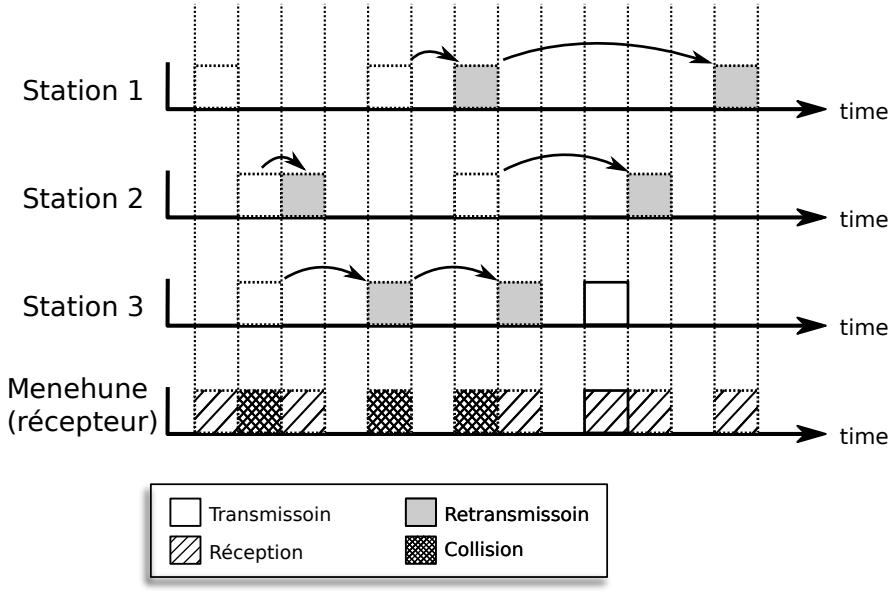



Figure 2.6 – Exemple de communication avec le protocole Slotted Aloha

Slotted Aloha est une amélioration de Pure ALOHA dans le but de réduire la probabilité de collision. Dans ce nouveau protocole, les stations sont synchronisées de telle façon qu'il n'est possible de commencer à émettre qu'au début d'un slot. Cela n'empêche pas les collisions de se produire puisque deux stations peuvent choisir le même slot pour émettre, mais cela évite qu'une collision commence durant la transmission d'une trame comme le montre la figure 2.6.

#### 2.3.2.3 CSMA/CA

Carrier Sense Multiple Access (CSMA) est une méthode d'accès au canal similaire à *Pure Aloha* mais dans laquelle une station souhaitant émettre va d'abord *écouter* le canal (*carrier sensing*) pour s'assurer que ce dernier est libre. Si le canal est déjà occupé, la station va attendre que le canal se libère avant d'émettre. Comme ALOHA, cela n'empêche pas les collisions de se produire si plusieurs stations souhaitent émettre alors que le canal est déjà occupé car elles tenteront simultanément d'émettre sitôt le canal libéré.

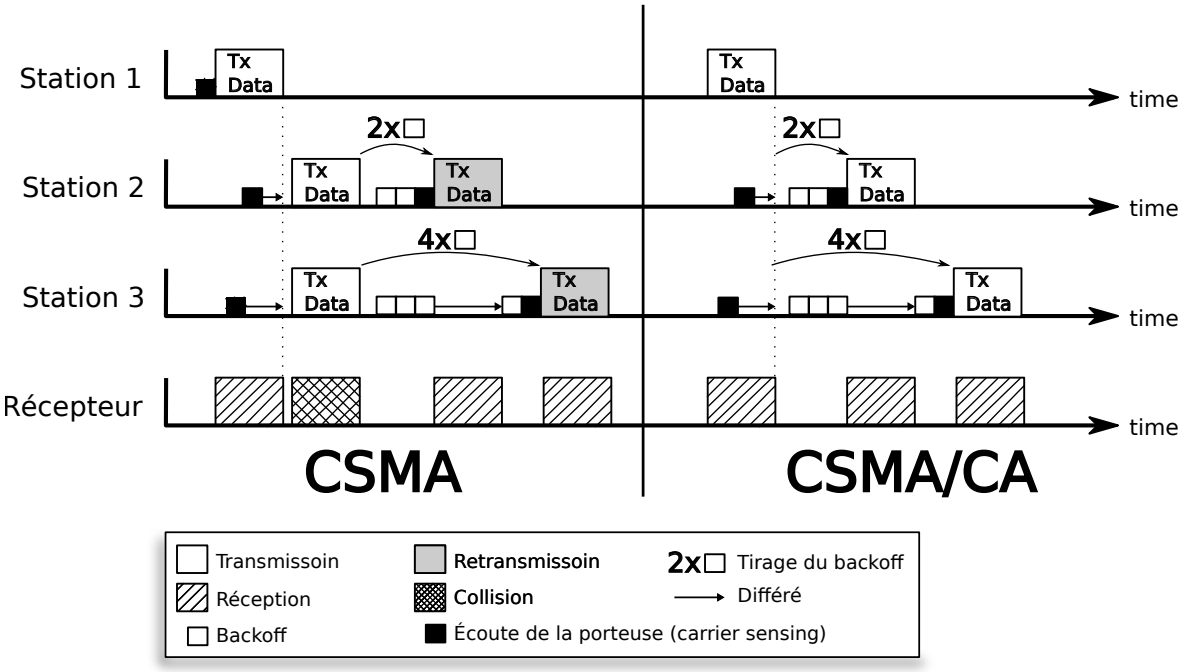



Figure 2.7 – Différence entre CSMA et CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) fut introduit dans le but de diminuer le nombre de collisions. La différence avec CSMA, tel que décrit sur la figure 2.7 est qu'une station ne va pas émettre sitôt le canal libéré, mais va tirer aléatoirement un *backoff* dans un intervalle avant d'émettre. Ce *backoff* est mis en pause chaque fois que le canal est de nouveau occupé. De plus, chaque fois qu'une transmission échoue, l'intervalle augmente exponentiellement et un nouveau *backoff* est tiré de cet intervalle.

CSMA/CA est à la base du standard IEEE 802.11 que nous allons décrire dans la section suivante.

## 2.4 Présentation de la norme IEEE 802.11

### 2.4.1 Présence et déploiement du WiFi

La technologie IEEE 802.11, plus connue sous son appellation commerciale Wireless Fidelity (WiFi), est la technologie sans-fil la plus populaire du fait de ses débits élevés et de son faible coût. En 2004, Jones *et. al* [JL07] ont étudié une base de donnée de plus de $5$ millions de points d'accès WiFi collecté par Skyhook Wireless, une entreprise fournissant un service de localisation géographique basé sur la présence des points d'accès. Cette étude a mis en évidence une densité de points d'accès (AP) entre 100 et 1800 AP par $km^2$ dans plusieurs grandes villes américaines (Las vegas, Atlanta, San Francisco, Seattle, Boston et Manhattan). Plus récemment, une étude en 2013 conduite par Achtzen *et. al* [AAM13] a ainsi recensée 800 *AP* par $km^2$ et 4 utilisateurs en moyenne par AP en zone résidentiel. En milieu urbain, c'est plus de 6000 APs par $km^2$ avec 1,4 utilisateurs en moyenne par AP. D'autres statistiques collectés collaborativement via la plate-forme wigle [WIG13] permet de suivre l'évolution du nombre d'AP dans le monde. La figure 2.8 (tirée du site web) représente le nombre d'AP découvert depuis 2002, la courbe en rouge représente le nombre total d'AP tandis que la courbe en bleu représente le nombre journalier d'AP découvert. Ces derniers ont repertorié plus de $111250587$ APs uniques (en Septembre 2013) dont $1944816$ rien qu'en France.

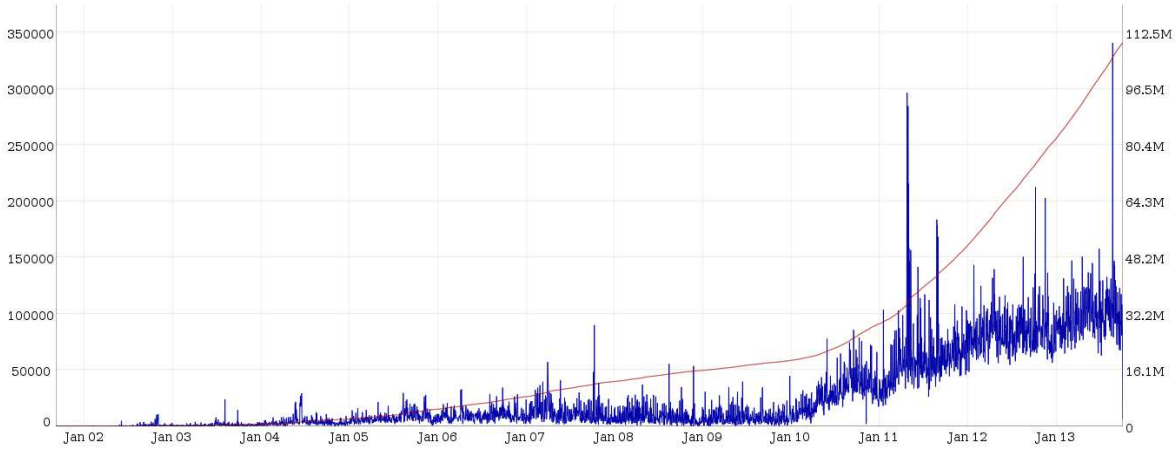



Figure 2.8 – Évolution de la présence du wifi depuis 2002 (source : wigle.net)

$10,5$ millions de foyers disposent en 2008 d'une *box* ADSL en France, soit deux foyers sur cinq et près des trois quarts des foyers connectés à l'Internet. Avec l'introduction de ces *box* ADSL chez les utilisateurs par les Fournisseur d'accès à Internet

(FAI), nous avons pu assister ces dernières années aux développement des réseaux WiFi communautaires (CN).

Les réseaux communautaires se caractérisent par le partage d'une connexion résidentielle à une communauté via un AP. Les FAI intègrent dans les *box* une puce IEEE 802.11 qui à la capacité de diffuser différents noms de réseau (ESSID). Un de ces ESSID est commun à tous les clients et est activé sur toutes les box du même FAI. En échange de partager sa connexion Internet, l'utilisateur peut lui même profiter de la connexion des autres membres de la communauté. Ainsi, un utilisateur qui se déplace au sein d'une ville ou même dans une autre ville peut bénéficier gratuitement d'un accès Internet en utilisant ses identifiants. FON est une des premières sociétés à avoir déployé un réseau communautaire et à avoir mis au point un modèle économique permettant d'inciter les utilisateurs à ouvrir leur connexion Internet. Ces réseaux communautaires apparaissent comme une alternative crédible pour fournir un accès à haut débit à Internet.

Du fait que ces AP sont reliés à une connexion Internet résidentielle, ces réseaux communautaires sont principalement déployés de façon décentralisée à l'intérieur des bâtiments et sans stratégie de déploiement. Afin d'évaluer la présence et la qualité de ce type de réseau, nous avons mis au point plusieurs expérimentations dans le cadre du projet Wi2Me à Telecom Bretagne. Ces expérimentations consistaient à effectuer des campagnes de mesure au centre ville de Rennes afin d'évaluer la qualité du déploiement de ces réseaux et la qualité d'une connexion basée uniquement sur ces réseaux communautaires.

#### 2.4.1.1 Description des expérimentations

Ce travail de recensement des réseaux WiFi a été effectué avec plusieurs doctorants et ingénieurs de l'école et s'est déroulé en deux temps.

• Durant l'été 2010, nous avons analysé le déploiement des points d'accès au centre ville de Rennes. Cette analyse consistait à identifier le nombre d'AP existant, la façon dont ils sont déployés et leur aire de couverture. Afin de répondre à ces questions, nous avons utilisé un ordinateur portable comme *sniffer* afin de capturer les trames IEEE 802.11 le long de l'itinéraire que nous nous étions définis. Le matériel était constitué d'un ordinateur portable de la marque Asus N10JB fonctionnant sur la distribution Ubuntu 9.04 (Jaunty Jackalope). La carte WiFi fonctionnait avec une version modifiée du driver *ath9k*. Nous avons également doté l'ordinateur portable d'une antenne externe possédant un gain de $5dBi$ pour pouvoir avoir

une meilleure réception. Afin de pouvoir localiser les traces, nous avons utilisé un récepteur GPS en USB ainsi que le logiciel osm-gps-map [NZJ13] pour afficher les captures sur une carte. Afin de maximiser la découverte d'AP, nous avons modifié le driver *ath9k* pour le forcer à effectuer un scanning actif toute les deux secondes (voir section 2.4.6.2). En même temps, la station capturait dans un deuxième fichier la localisation géographique toutes les secondes. Ce fichier et celui constitué des réponses du scanning ont ensuite été fusionnées et analysées sur notre poste de travail afin d'obtenir une vue complète de la campagne.

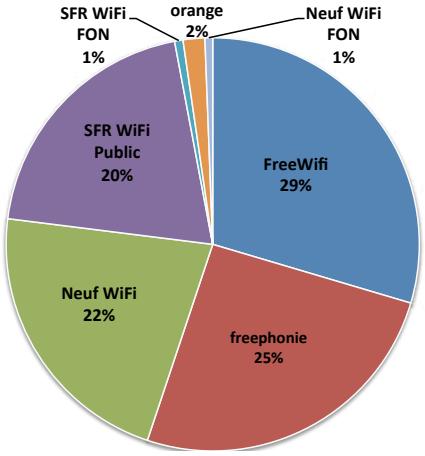
- Dans une deuxième expérimentation nous avons utilisé des téléphone Samsung Galaxy SII avec une application dédiée. Cette application, développée au sein de l'équipe, permet de faire du *scanning* de réseaux et tente de se connecter à l'un de nos serveurs lorsque cela est possible. Pour cela des scripts ont été développés afin d'entrer automatiquement les identifiants auprès des portails captifs des réseaux communautaires. Lorsque l'authentification auprès des portails captifs fonctionnait, l'application essayait de transmettre et recevoir des données via Internet auprès d'un serveur préalablement configuré.

#### 2.4.1.2 Résultats des expérimentations


Figure 2.9 – Déploiement des APs le long du chemin

La figure 2.9 représente les APs découvert le long du chemin sur une distance de 8 km. Nous avons découvert 6620 points d'accès différents et plus de 3305 ESSID différents. Parmi ces points d'accès découverts, 29% faisaient partie d'un réseau

communautaire. La figure 2.10 illustre la répartition des ESSID des réseaux communautaires. On peut ainsi voir qu'au moment de l'expérience, *FreeWifi* représentait la part la plus importante des réseaux communautaires avec 29%. Nous avons découvert qu'un utilisateur se déplaçant le long du chemin pouvait bénéficier d'un accès ininterrompu au réseau communautaire *FreeWifi* sur un chemin long de 292 mètres. En ayant accès à la fois aux réseaux communautaires FreeWifi et Neuf/SFR, l'utilisateur pouvait avoir un accès de 451 mètres sans interrompre la connexion. Cependant, la mobilité n'est pas implémentée entre les AP, ce qui signifie qu'un utilisateur doit se reconnecter entre deux AP, interrompant la connexion au niveau applicatif.

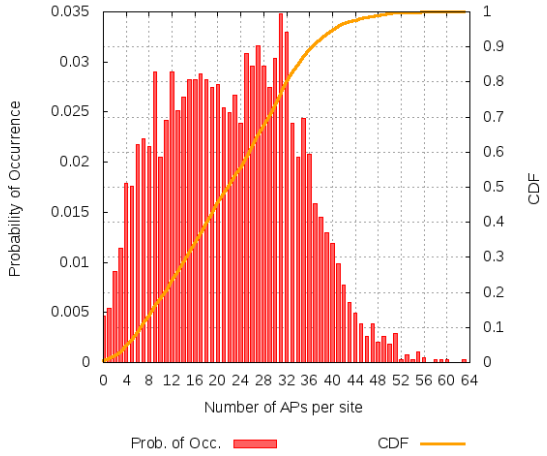



| Réseau Communautaire | Couverture globale (%) | Chemin le plus long (m) |
|---|---|---|
| FreeWiFi | 67.43 | 292.12 |
| FreePhonie | 63.52 | 283.18 |
| Neuf WiFi | 41.06 | 125.89 |
| SFR WiFi Public | 38.59 | 125.89 |
| All | 74.77 | 451.82 |

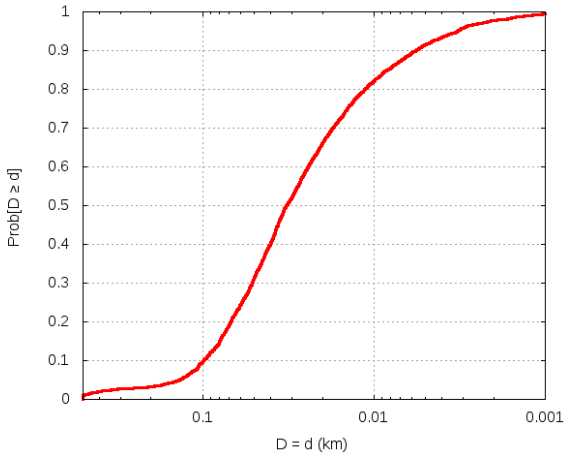
Figure 2.10

La figure 2.11a montre la fonction de répartition du nombre d'APs trouvés lors de chaque scan. Ainsi on observe que 22 APs sont découvert en moyenne par sondage. Ceci signifie que en tout point parcouru, l'utilisateur observe jusqu'à 32 points d'accès simultanément, cela démontre la présence très forte de la technologie IEEE 802.11 dans un environnement urbain. La figure 2.11b illustre la distribution de la couverture des AP découvert. On peut voir que la couverture moyenne est de 32.3 mètres.

La qualité d'une connexion basée sur ces points d'accès en terme de bande passante est donnée par la figure 1.1 en Introduction. On voit ainsi que malgré une présence quasi ininterrompue des CN tout au long des expérimentations, il n'était possible d'échanger des données avec le serveur que pour environ 50% de la durée. Ceci est en partie due au manque de support de la mobilité des terminaux mobiles qui impose de refaire toute une procédure de reconnexion à chaque changement d'AP (niveau 2, obtention d'une IP, connexion et authentification au portail, connection TCP au serveur). Une autre raison est la mauvaise qualité de signal entre le




(a) Nombre d'APs découverts par scan ; En orange la CDF et en rouge la PDF




(b) couverture (en km) des AP découverts

terminal et les AP, représentée par la figure 1.1b. Cette mauvaise qualité provoque de nombreuses pertes et oblige le terminal à changer plus fréquemment d'AP.

Comme nous avons pu l'observer les réseaux WiFi sont extrêmement populaires mais si on y prête un usage urbain (connexion dans la ville), de nombreuses améliorations sont à apporter. Notamment, comme nous le verrons dans le chapitre 4, nous décrirons un mécanisme de relayage qui se prête très bien à cette utilisation. Mais avant cela, comme notre solution de relayage est essentiellement pensée pour les réseaux IEEE 802.11, nous allons détailler dans les sections suivantes les spécificités techniques de ce standard pour asseoir les bases de notre travail.

### 2.4.2 Évolution technique de la norme IEEE 802.11

Cette norme a subi de nombreuses évolutions techniques ayant permis d'améliorer les débits mais également d'augmenter la sécurité ou les usages. Le tableau 2.1 ci-dessous retrace les différentes évolutions ayant permis d'améliorer les débits.

| Norme | Modulation | Fréquence | Débit (Mbit/s) | Largeur de canal |
|---|---|---|---|---|
| 802.11-1997 | DSSS / FHSS | 2.4 GHz | 1 – 2 | 22 MHz |
| 802.11b-1999 | DSSS | 2.4 GHz | 1 – 11 | 22 MHz |
| 802.11a-1999 | OFDM | 5 GHz | 6 – 54 | 20 MHz |
| 802.11g-2003 | OFDM / DSSS | 2.4 GHz | 1 – 54 | 20 MHz |
| 802.11n-2009 | OFDM | 2.4 / 5 GHz | 6 – 600 | 20 / 40 MHz |
| 802.11ac-2009 | OFDM | 5 GHz | 6 – 1000 | 20 / 40 / 80 / 160 MHz |

Tableau 2.1 – Évolution des débits de IEEE 802.11

**IEEE 802.11-1997** est la première norme 802.11 sortie en 1997 et qui permettait d'atteindre des débits de 1 ou 2 Mbps en utilisant des méthodes de codage basées sur Direct-Sequence Spread Spectrum (DSSS) et Frequency Hop Spread Spectrum (FHSS) dans la bande des 2.4 GHz.

**IEEE 802.11b-1999** a rapidement supplanté IEEE-802.11 en permettant d'atteindre des débits allant jusqu'à 11 Mbps. Pour atteindre de tels débits en utilisant la même méthode de codage DSSS, IEEE-802.11b remplace le Barker Code, la méthode de modulation utilisée dans IEEE-802.11 par la méthode Complementary Code Keying (CCK).

**IEEE-802.11a-1999** utilise la modulation Orthogonal Frequency Division Multiplexing (OFDM) sur la bande des 5 GHz pour atteindre des débits allant jusqu'à 54 Mbps par secondes. OFDM fonctionne en émettant sur $n$ fréquences simultanément. La norme 802.11a utilise 52 sous-fréquences (dont 48 pour de la data) pour une largeur de canal de 20 MHz. La bande de fréquence 5GHz étant moins utilisé que celle des 2.4 GHz, la norme IEEE-802.11a possède un avantage dans la mesure où elle subit moins d'interférence. Cependant cette fréquence élevée pénètre plus difficilement les murs et réduit l'aire de couverture des appareils.

**IEEE-802.11g-2003** fonctionne dans la bande 2.4 GHz (comme IEEE 802.11b) mais en utilisant les même techniques de modulation OFDM que IEEE 802.11a fournissant ainsi les même débits allant jusqu'à 54 Mbps.

**IEEE-802.11n-2009** amène les dernières modifications à ce jour pour atteindre des débits allant jusqu'à 600 Mbps. Ces débits sont possibles en utilisant plusieurs antennes à la place d'une seule, technologie connue sous le nom de Multiple Input, Multiple Output (MIMO) ainsi qu'en utilisant plus de sous-porteuses dans OFDM, en optimisant certains aspect d'OFDM et en augmentant la taille des canaux à 40 MHz.

**IEEE 802.11ac**, qui est la dernière amélioration apportée à IEEE 802.11n, permettra d'atteindre des débits de l'ordre du Gbps sur la bande des 5 GHz. Cette amélioration significative des débits est possible en utilisant des canaux de 80 MHz ou 160 MHz de large, en utilisant plus d'antennes pour le MIMO (8 contre 4 pour 802.11n) et en utilisant des techniques de modulation plus performantes (256-QAM contre 64-QAM pour 802.11n).

On peut également noter l'existence de travaux en cours tels que **IEEE 802.11ad** qui permettra d'atteindre des débits de 7 Gbps sur la bande des 60 GHz. À cette fréquence, le signal ne traverse plus les murs et les cas d'usage de cette norme sont principalement pensés pour des applications domestiques et multimédia telles que

le streaming de vidéo HD. La norme **IEEE 802.11y**, quant à elle, prévoit une aire de couverture de 5 km pour les réseaux métropolitains sur la bande 3.6 GHz. À l'heure d'écriture de cette thèse, la norme IEEE 802.11g est la plus utilisée à travers le monde et particulièrement en France. C'est sur cette dernière que nous avons basé nos travaux décrits dans cette thèse.

En plus des évolutions techniques ayant permis d'améliorer la qualité et la fiabilité du WiFi, d'autres évolutions sont apparues afin d'étendre l'utilisation du WiFi pour de nouveaux cas d'usage et répondre à de nouveaux besoins. Sans être exhaustif,le tableau 2.2 indique les évolutions les plus notables du WiFi ne constituant pas une amélioration des débits.

| Norme | description |
|---|---|
| 802.11i-2004 | introduit le chiffrement WPA1 et WPA2 afin de pallier les faiblesses du WEP |
| 802.11e-2005 | ajout de mécanisme de qualité de service |
| 802.11k-2008 | normalisation des mesures radio et introduction de mécanisme de gestion des ressources |
| 802.11s | définit la couche MAC et PHY pour des réseaux mesh. |

Tableau 2.2 – Évolution des services de 802.11

La sécurité Wireless Encryption Protection (WEP) standardisée depuis 1999 est basée sur la méthode de chiffrement de flux RC4, c'est-à-dire qu'elle peut traiter des données de longueur quelconque sans avoir besoin de les découper. Après la croissance et la popularité des réseaux WiFi, cette sécurité s'est très vite montrée insuffisante face aux attaques devenues de plus en plus rapides à mener (quelques minutes suffisent pour casser la clé de chiffrement). La norme **IEEE 802.11i-2004** introduit ainsi de nouveaux procédés de chiffrement appelés WPA en se basant sur des technologies de chiffrement par bloc plus robustes (AES-CCMP/PSK). WPA permet également de mettre en place des mécanismes d'authentification via une architecture type IEEE-802.1X c'est-à-dire via un serveur d'authentification type RADIUS.

La norme **IEEE 802.11e** modifie la couche MAC en proposant des mécanismes de qualité de service aux applications. Cette norme introduit dorénavant quatre files d'attentes contre une seule auparavant, chacune ayant une certaine priorité.

La norme **IEEE 802.11k** est un projet récent dont le but est de standardiser la façon dont les réseaux IEEE 802.11a, b et g peuvent présenter les mesures radio et les conditions du réseau au niveau des applications. Avant cette norme, chaque constructeur était libre dans la façon de présenter ces valeurs auprès des appli-

cations comme par exemple la puissance d'un signal reçu appelée Radio Signal Strength Indicator (RSSI). Le RSSI est exprimé en unité arbitraire et n'a pas de lien direct avec la puissance physique du signal reçu (exprimé en $mW$ ou $dB$). Son calcul et son domaine sont laissés à la discrétion du constructeur, par exemple le RSSI vaut entre $0$ et $100$ pour les cartes WiFi Cisco alors qu'il vaut entre $0$ et $127$ pour les cartes WiFi Atheros. Cette nouvelle norme entend normaliser ces valeurs afin de pouvoir introduire des mécanismes de radios cognitives.

### 2.4.3 Allocation des canaux

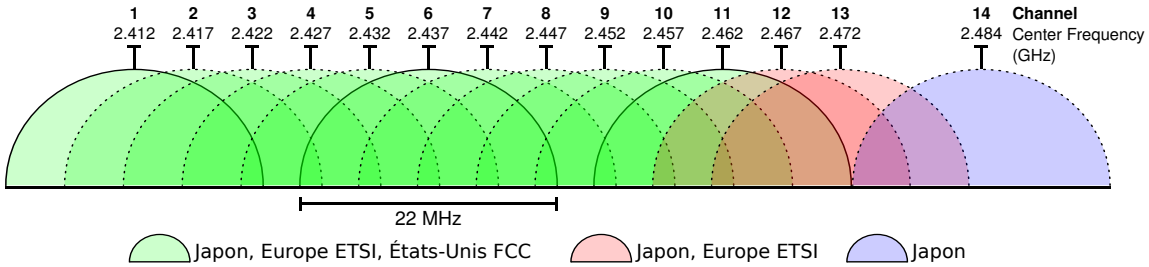



Figure 2.12 – Allocation des canaux WiFi sur la bande des 2.4 GHz selon les pays

L'allocation des bandes de fréquences ainsi que la puissance d'émission dépend des organismes de régulation de chaque pays, qui allouent ou autorisent l'utilisation de certaines bandes de fréquences en fonction de leur disponibilité. Le WiFi opère sur la bande ISM et plus particulièrement sur la bande des 2.4 GHz et 5 Ghz. En WiFi, La bande des 2.4 GHz est divisée en 14 canaux de 22 MHz séparés de 5 MHz chacun tel que décrit sur la figure 2.12. Tous les pays n'autorisent pas l'utilisation de ces canaux ; en France et en Europe, seul les 13 premiers canaux sont autorisés, aux États-Unis les canaux 12 et 13 sont autorisés à condition que la puissance d'émission soit faible et au Japon le canal 14 n'est autorisé qu'avec les modes de modulation DSSS et CCK (ce qui exclut l'utilisation de IEEE 802.11g). En Europe, la puissance d'émission (après calcul du gain de l'antenne) est limitée à $100mW$, c'est-à-dire $17dBm$ contre $1000mW$ aux États-Unis, soit $30dBm$. Le Japon utilise une méthode différente pour spécifier la puissance d'émission. Au lieu de spécifier une puissance maximale d'émission, ils mesurent la puissance par rapport à la bande passante. La valeur de la mesure s'exprime en milliwatt par mégahertz. Ainsi, la puissance d'émission au Japon est limitée à $10mW/MHz$ ce qui signifie que pour un canal de $22MHz$, la puissance d'émission maximale est de $220mW$, c'est-à-dire $23dBm$.

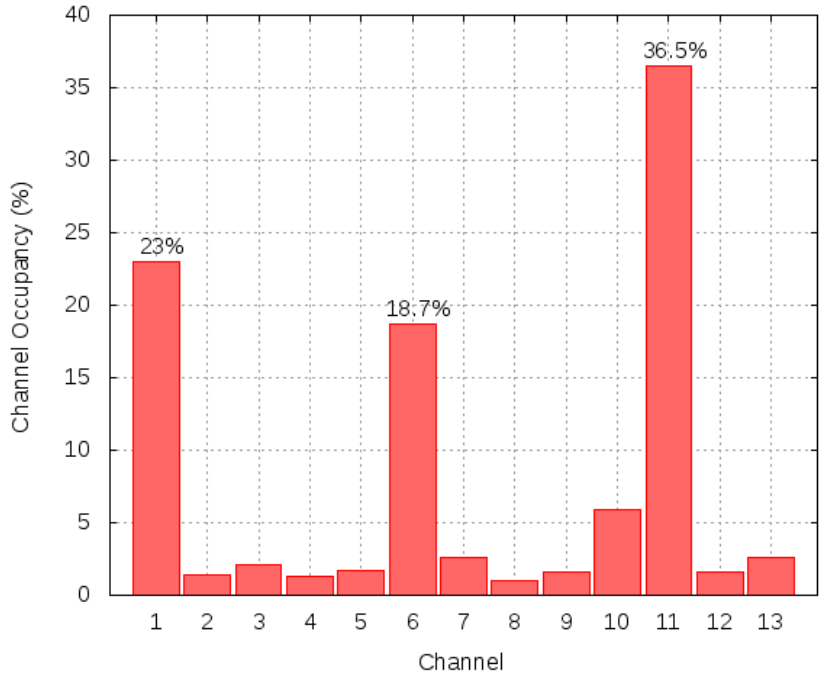



Figure 2.13 – Distribution des canaux dans l'expérimentation Wi2Me

La figure 2.13 représente la distribution des canaux telle que nous avons pu l'observer dans le projet Wi2Me. On s'aperçoit que les canaux 1,6 et 11 sont les plus utilisés. Cela est du au fait que ces trois canaux ne se chevauchent pas et n'interfèrent donc pas entre eux.

### 2.4.4 Les modes d'opération de IEEE 802.11

Le standard IEEE 802.11 décrit deux modes d'architecture : l'un appelé **mode infrastructure** ou *Basic Service Set* BSS et l'autre **mode ad hoc** ou sans infrastructure aussi appelé Independant Basic Service Set (IBSS). Les deux modes sont présentés ci-dessous.

#### 2.4.4.1 Le mode Ad Hoc

Le **mode ad hoc** ou Independant Basic Service Set (IBSS) permet à plusieurs stations de communiquer directement entre elles sans avoir besoin d'un AP central. En fonctionnant en mode *ad hoc*, les stations étant à portée les unes des autres peuvent se découvrir et communiquer directement, à condition qu'elles utilisent le même canal

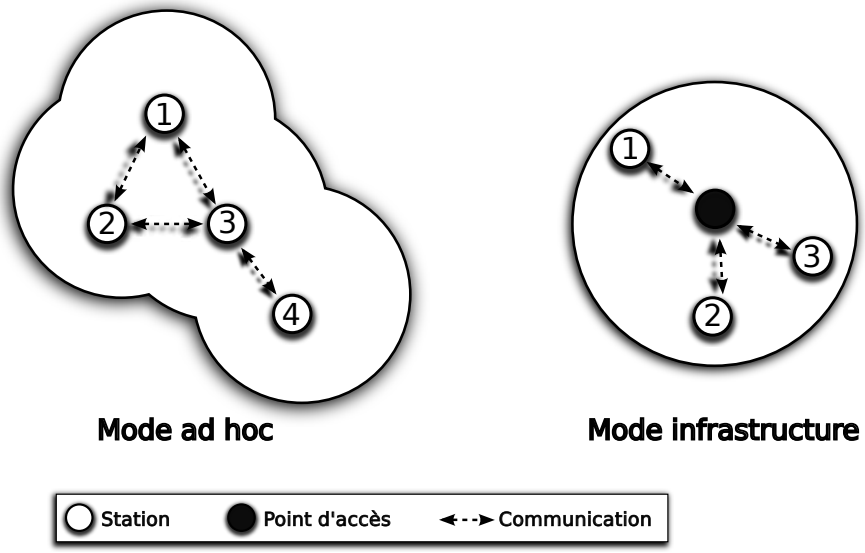



Figure 2.14 – Mode de fonctionnement *ad hoc* et infrastructure du WiFi

et le même SSID [2]. Il n'y a pas de limite dans le nombre de stations qui peuvent participer au réseau *ad hoc* autre que les limites techniques qui font que le canal peut rapidement être saturé lorsque le nombre de stations augmente. Chaque station participant au réseau *ad hoc* est donc une partie de l'infrastructure portant le réseau. Cependant, le mode *ad hoc* seul ne décrit pas les mécanismes de routage nécessaires au cas où deux stations appartenant au même réseau *ad hoc* ne sont pas à portée l'une de l'autre. Par exemple, sur la figure 2.14, les nœuds $(1)$ et $(4)$ ne peuvent pas communiquer directement et doivent utiliser le relais $(3)$ comme un nœud intermédiaire. Le routage doit être configuré manuellement ou en faisant fonctionner sur tous les nœuds un algorithme de routage qui permettra l'échange et la configuration automatique des routes (voir 3). La norme IEEE 802.11s introduite précédemment décrit un algorithme de routage permettant de mettre au point ces routes. Cela permet, dans un réseau connexe (c'est-à-dire qu'il existe au moins un chemin entre chaque paire de nœud), de rendre possible la communication d'un nœud à un autre.

#### 2.4.4.2 Le mode Infrastructure

Le **mode infrastructure** fonctionne avec une station particulière, un AP, dont le rôle est de coordonner et de centraliser les échanges. Lorsque plusieurs stations sont connectées à l'AP, elles peuvent communiquer entre elles via l'AP qui sert de passerelle obligatoire. Un AP avec toutes les stations associées forment un *Basic Service Set* BSS et annonce sa présence en diffusant périodiquement son Basic Service Set

[2] *Service Set Identifier*, c'est-à-dire le nom du réseau

IDentification (BSSID) ainsi qu'un Service Set IDentification (SSID). Le BSSID est une adresse MAC qui identifie la BSS uniquement tandis que le SSID est une chaîne de caractère compréhensible par les humains. Lorsque plusieurs BSS connectés au même réseau filaire diffusent le même SSID, cela forme un *Extended Service Set* ESS comme décrit sur la figure 2.15. Cela permet de pouvoir étendre la couverture de l'infrastructure sans-fil, une station ne se connecte qu'à un seul AP à la fois. Généralement, le ou les points d'accès sont connectés à un réseau filaire et font office de passerelle vers les ressources du réseau filaire, comme Internet par exemple.

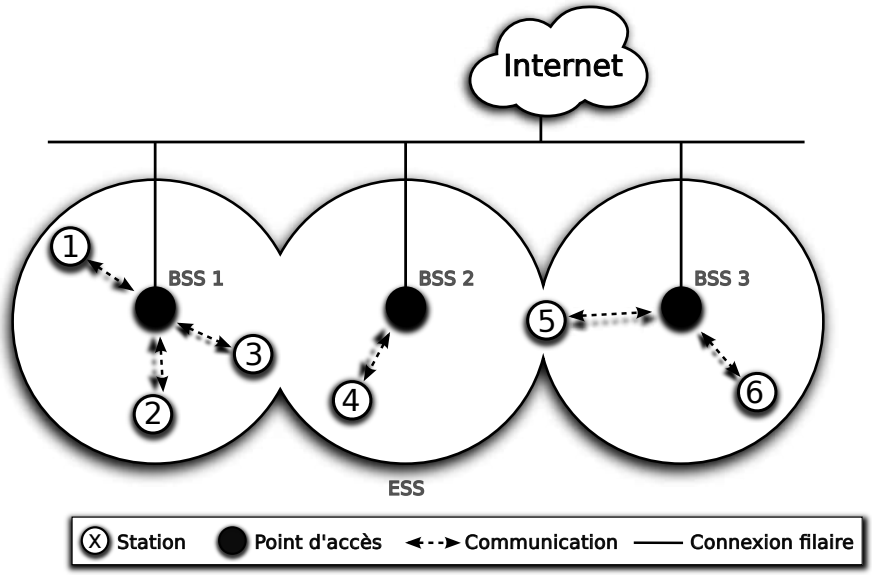



Figure 2.15 – Exemple d'architecture IEEE 802.11 d'un ESS constitué de 3 BSS

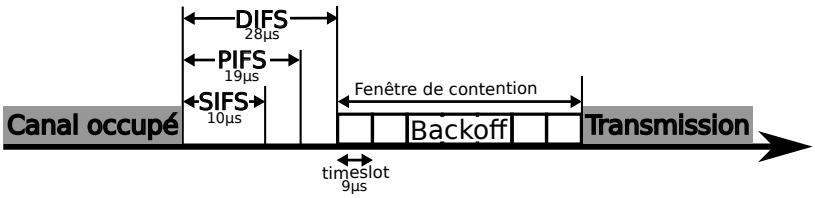
#### 2.4.4.3 Wifi Direct

Initialement appelé WiFi P2P, Wifi Direct est une initiative de 2010 de la WiFi Alliance dont le but est de connecter des appareils en WiFi sans avoir besoin de passer par un AP. Cela ressemble au mode *ad hoc* dans son mode de déploiement mais fonctionne en réalité en donnant à un appareil WiFi Direct la possibilité de se mettre en mode AP. La norme WiFi Direct décrit ainsi les mécanismes de découverte d'appareils et de services ainsi que les mécanismes de négociation du groupe (choisir quel appareil fonctionnera en mode AP). Comme WiFi Direct se base sur le mode infrastructure de la norme IEEE 802.11, il suffit qu'un seul appareil soit compatible WiFi direct pour rendre possible la communication directement entre deux stations. Ce choix technologique sur le mode infrastructure plutôt que le mode *ad hoc* est sûrement dû au fait que le mode *ad hoc* souffre d'un manque ou de mauvaises implémentations. WiFi Direct simplifie également la configuration de la sécurité en se

basant principalement sur le mode de sécurité WPS qui nécessite simplement d'appuyer simultanément sur un bouton situé sur l'AP et un bouton situé sur la station invitée. À terme cette norme pourrait bien remplacer le bluetooth car elle propose des services similaires mais à des débits beaucoup plus importants et un rayon plus important. Bien que récente, cette norme est déjà implémentée dans le noyau Linux et sur différents téléphones mobiles.

### 2.4.5 Les méthodes d'accès au canal (MAC)

La norme IEEE 802.11 est basée sur CSMA/CA pour l'accès au canal mais introduit également des *timers* appelés Inter-Frame Spacing (IFS) . Ces *timers* sont une caractéristique remarquable de IEEE 802.11 car ils permettent d'ajouter des notions de priorité à CSMA/CA, qui est normalement un protocole meilleur effort (*Best Effort*). Lorsque le canal est libéré, une station IEEE 802.11 doit attendre au moins l'écoulement d'un *timer* avant de pouvoir commencer une transmission. Dans la norme de base, quatre *timers* différents sont décrits de la façon représentée sur la figure 2.16. Sur le tableau de droite sont décrites les relations qu'entretiennent ces *timers* entre eux. Le *timer* SIFS et la durée d'un *slot* sont définis statiquement par la couche physique et sont différents pour chaque évolution de la norme. PIFS, DIFS et EIFS, en revanche, sont liés aux valeurs de SIFS et du temps d'un slot. Dans la figure de gauche, nous avons donné à titre indicatif leurs temps en $\mu$s tels que décrit dans la norme IEEE-802.11g-2003. L'existence de ces *timers* est due à la nature des données à transmettre sur le canal. Certaines trames nécessitent une transmission immédiate, tels que les accusés de réception par exemple, ou les réponses CTS à un RTS (décrit en section 2.4.5.4).




| Timer | Durée formelle |
|---|---|
| SIFS | décrit par la PHY |
| PIFS | SIFS + SLOT |
| DIFS | SIFS + 2xSLOT |
| EIFS | ACK + SIFS + DIFS |

Figure 2.16 – Relation entre les timers de IEEE 802.11

- Short Inter-Frame Spacing (SIFS) est le plus petit des *timers* IFS et est utilisé lorsqu'une trame doit être transmise immédiatement après une autre. En 802.11, Chaque trame envoyée en *unicast* doit nécessairement être suivie d'un ACK, l'absence d'accusé étant interprétée comme une transmission ayant échoué. Un

ACK est ainsi transmis directement après la réception d'une trame de données grâce à l'utilisation du timer SIFS. D'autres trames peuvent nécessiter l'utilisation du *timer* SIFS telle que dans un échange RTS/CTS ou pour la réponse à un CF-POLL dans le mode PCF.

- PCF Inter-Frame Spacing (PIFS) est le *timer* utilisé par le mode d'accès PCF et vaut un SIFS plus la valeur d'un seul *slot* (PIFS vaut $10 + 9\mu$s dans 802.11g). Du fait qu'il est inférieur à DIFS, le mode de communication PCF est prioritaire face à DCF mais compatible dans la mesure où il ne provoque pas d'interférences et que les deux modes peuvent cohabiter sur le même canal.
- DCF Inter-Frame Spacing (DIFS) vaut un SIFS plus la valeur de deux slots ($10 + 18\mu$s dans 802.11g). Il est destiné à la transmission d'une trame de données dans le mode DCF. Ce *timer* DIFS est immédiatement suivi d'une procédure de *backoff* constituée d'un nombre aléatoire de *slots*. Un *timeslot* constitue l'unité de temps fondamentale du *backoff*.
- Extended Inter-Frame Spacing (EIFS) est un *timer* utilisé lorsqu'une station reçoit une trame pour laquelle une erreur a été détectée (grâce au code de détection d'erreur). Dans ce cas, la station doit attendre un temps EIFS qui est suffisamment long pour permettre à une autre station, potentiellement la vraie destination de cette trame, d'envoyer un ACK au débit le plus faible.

En se basant sur ces *timers*, la norme IEEE 802.11 décrit deux méthodes d'accès au canal, la méthode PCF ainsi que la méthode DCF. L'amendement IEEE 802.11e introduit des mécanismes de QoS et décrit une troisième méthode d'accès, similaire à DCF, appelée Enhanced Distributed Coordination Function (EDCF).

#### 2.4.5.1 Le mode d'accès PCF

Le mode d'accès Point Coordination Function (PCF) est une méthode sans contention et qui ne fonctionne que dans le mode infrastructure. Ce mode nécessite un **coordinateur**, au niveau de l'AP, qui décide de qui à le droit d'émettre à un instant donné. Le mode PCF fonctionne en alternant des périodes sans contention, contrôlé par le coordinateur, avec des périodes avec contention utilisant le mode d'accès DCF. La durée des périodes sans contention est définie par l'AP. Durant les périodes sans contention, le coordinateur questionne une liste de stations pour leur donner l'autorisation de transmettre. Cela fonctionne en envoyant une trame particulière CF-POLL en *unicast* à une station qui doit répondre par une trame CF-Ack si

elle souhaite émettre ou bien CF-Null si elle ne le souhaite pas. Ainsi, durant les périodes sans contention, les stations ne peuvent émettre que si elles ont explicitement reçues l'autorisation du coordinateur.

Ce mode d'accès est extrêmement peu utilisé et est quasiment inexistant dans l'implémentation des cartes WiFi. Nous allons décrire plus en détail le fonctionnement des modes d'accès DCF et EDCF.

### 2.4.5.2 Le mode d'accès DCF

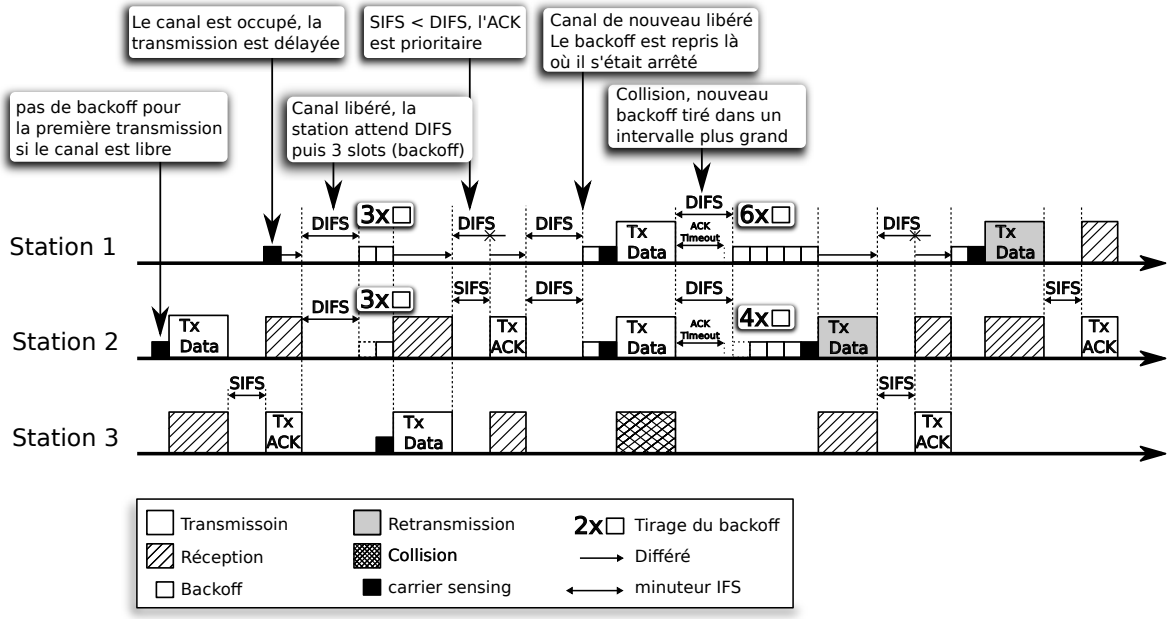



Figure 2.17 – Exemple d'accès au canal avec la méthode DCF dans IEEE 802.11

Distributed Coordination Function (DCF) est une méthode basée contention sur le modèle de CSMA/CA (voir section 2.3.2.3). Cette méthode est utilisée à la fois dans le mode *ad hoc* et dans le mode infrastructure. La figure 2.17 donne un exemple d'accès au canal avec cette méthode. Comme CSMA/CA, pour qu'une station puisse émettre, elle doit d'abord commencer par écouter la présence éventuelle d'une porteuse. Si le canal est libre alors la station a le droit d'émettre et peut procéder à la transmission de sa trame. Si le canal est déjà occupé, elle retarde sa transmission jusqu'à ce que le canal soit libre. Lorsque le canal est libre de nouveau, la station doit d'abord attendre un temps DIFS puis choisir un nombre aléatoire de *slots*. Ce nombre de slots choisis aléatoirement s'appelle le **backoff** et celui-ci est décrémenté tant que le canal reste libre. Si le canal est de nouveau occupé durant le décompte du *backoff*, celui-ci se met en pause jusqu'à ce que le canal soit de nouveau libre et

reprendra son décompte après un temps DIFS. Lorsque le *backoff* arrive à zéro, la station peut alors émettre sa trame.

Le **backoff** est un aspect essentiel de l'efficacité du protocole. Il est tiré dans une **fenêtre de contention** bornée par $0$ et *CWmin*. Si la taille de cette fenêtre est trop petite, alors plusieurs stations souhaitant accéder au canal risqueraient de tirer le même nombre de slots, ce qui provoquerait une collision. Si à l'inverse cette fenêtre de contention est trop grande, le canal risque d'être sous-utilisé, réduisant de fait l'efficacité du protocole. IEEE 802.11 a introduit un mécanisme de backoff dynamique qui s'adapte à la congestion du réseau en augmentant exponentiellement la fenêtre de contention. Chaque fois qu'une transmission n'est pas suivie par la réception d'un ACK, la station suppose qu'il y a eu collision, double sa fenêtre de contention et recommence une procédure de contention jusqu'à ce que la borne supérieure atteigne *CWmax*. En doublant la fenêtre de contention, la station augmente ses chances de tirer un *backoff* élevé, ce qui permet aux autres stations de bénéficier de l'accès au canal. En procédant ainsi, la méthode DCF contrôle la charge sur le canal en réduisant la contention, car les stations ayant raté leur transmission ont plus de chance d'accéder au canal plus tard. La figure ci-après donne un exemple de ce mécanisme de l'évolution exponentielle de la fenêtre de contention pour *CWmin* et *CWmax* valant respectivement $7$ et $255$. Dans la norme IEEE 802.11g, *CWmin* et *CWmax* valent respectivement $7$ et $1023$.

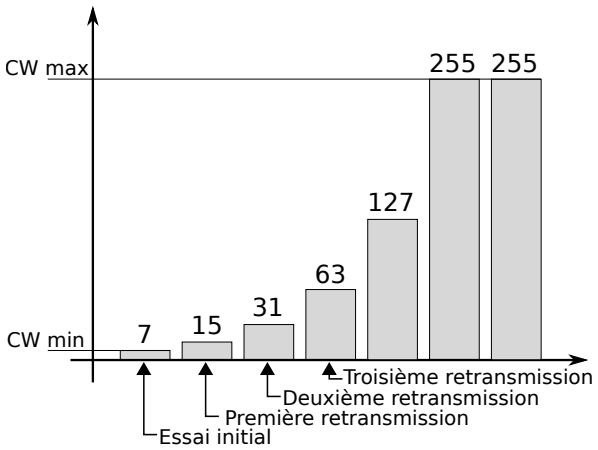



Figure 2.18 – Backoff exponentiel pour CWmin et CWmax valant respectivement $7$ et $255$

Lorsqu'une trame est transmise avec succès, c'est-à-dire qu'un accusé de réception a suivi la transmission, la fenêtre de contention est réinitialisée à *CWmin*. Si une trame est retransmise un nombre trop important de fois, c'est-à-dire que la fenêtre de contention à atteint *CWmax*, la trame est jetée, la fenêtre réinitialisée et une nouvelle trame est tirée de la file d'attente.

| Classe de service | CWmin | CWmax | AIFSN |
|---|---|---|---|
| AC_BK | $aCWmin$ (15) | $aCWmax$ (1023) | 7 |
| AC_BE | $aCWmin$ (15) | $aCWmax$ (1023) | 3 |
| AC_VI | $(aCWmin+1)/2-1$ (7) | $aCWmin$ (15) | 2 |
| AC_VO | $(aCWmin+1)/4-1$ (3) | $(aCWmin+1)/2-1$ (7) | 2 |
| DCF | $aCWmin$ (15) | $aCWmax$ (1023) | 2 |

Tableau 2.3 – Valeur par défaut des classes de services dans IEEE 802.11e

#### 2.4.5.3 Le mode d'accès EDCA

Enhanced Distributed Channel Access (EDCA) est une évolution apportée à DCF dans l'amendement IEEE-802.11e et dont l'objectif est de fournir différentes classes de service. Le but de EDCA est de donner une plus grande priorité d'accès au canal pour les trames prioritaires. Afin de rendre cela possible, EDCA joue principalement sur deux paramètres :

- *Arbitrary IFS* AIFS un nouveau timer variable
- *CWmin* et *CWmax* sont paramétrables

Le *timer* AIFS fonctionne en raccourcissant ou en augmentant la période d'attente après libération du canal. Un AIFS court signifie qu'une trame a une plus grande probabilité d'accéder au canal avec une latence faible. En fonction de la classe de service désirée, le *timer* AIFS sera différent et permettra par exemple de donner la priorité à de la voix plutôt qu'à de l'email. Le *timer* AIFS dépend du AIFSN qui est spécifique à une classe de service (qu'on note alors AIFSN[AC]). AIFS est calculé avec la formule :

$$AIFS = SIFS + AIFSN[AC] * SlotTime \tag{2.1}$$

On voit que AIFS est équivalent à DIFS pour un AIFSN valant 2. EDCA décrit ainsi quatre classes de services différentes, **AC_VO** pour la voix, **AC_VI** pour la vidéo, **AC_BE** pour le traffic Best Effort et **AC_BK** pour le traffic non prioritaire. Chaque classe de service (AC) personnalise le *timer* AIFS avec un AIFSN[AC] qui lui est propre, ainsi que ses paramètres *CWmin* et *CWmax*. Les valeurs par défaut sont présentées dans le tableau 2.3.

Dans ce tableau, les valeurs entre parenthèses de *CWmin* et *CWmax* sont données à titre d'exemple pour $aCWmin$ et $aCWmax$ valant respectivement $15$ et $1023$ (valeurs pour IEEE 802.11g). Contrairement à DCF qui ne gère qu'une seul liste d'attente, EDCA implémente quatre liste d'attentes, une pour chaque classe de service, indépendantes les unes des autres. Chaque liste d'attente gère indépendamment son backoff et ses paramètres de contention, de fait des collisions internes sont possibles.

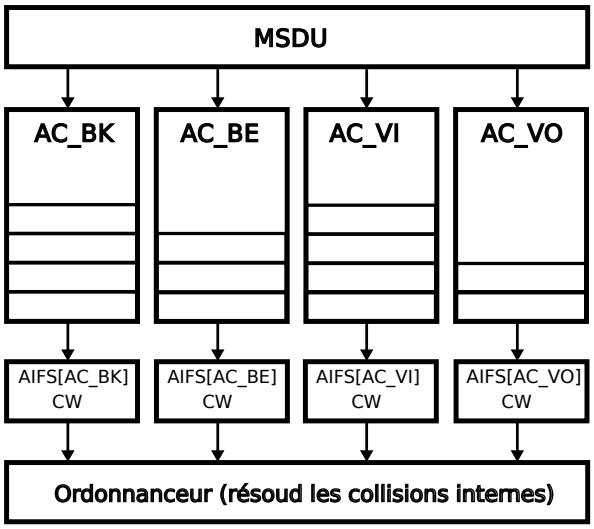



Figure 2.19

Au sein d'une même station, lorsque deux *backoffs* terminent en même temps, la trame provenant de la liste la plus prioritaire gagne l'accès au canal et le ou les autres sont jetées comme si il y avait eu une collision sur le canal.

#### 2.4.5.4 RTS/CTS

Une station émettrice ne connait pas les conditions radio dans lesquelles se trouve une station réceptrice. Cela amène, dans certain cas de figure, au problème du nœud caché dans lequel des stations qui ne s'entendent pas tentent d'émettre simultanément vers une destination. La figure 2.20 représente une situation de nœud caché avec un AP entouré de deux stations.

Dans ce cas de figure, les deux stations sont connectées à l'AP mais sont trop éloignées l'une de l'autre pour se détecter. Dans notre exemple, la station $1$ arrive à la fin de sa procédure de *backoff*, et transmet sa trame après avoir écouté le canal pour tenter d'y détecter une porteuse. Peu de temps après, et avant que la station $1$ n'ait terminé sa transmission, la station $2$ fait de même, et ne détectant pas la station $1$, transmet également sa trame. Il en résulte une collision et l'AP n'est pas capable de

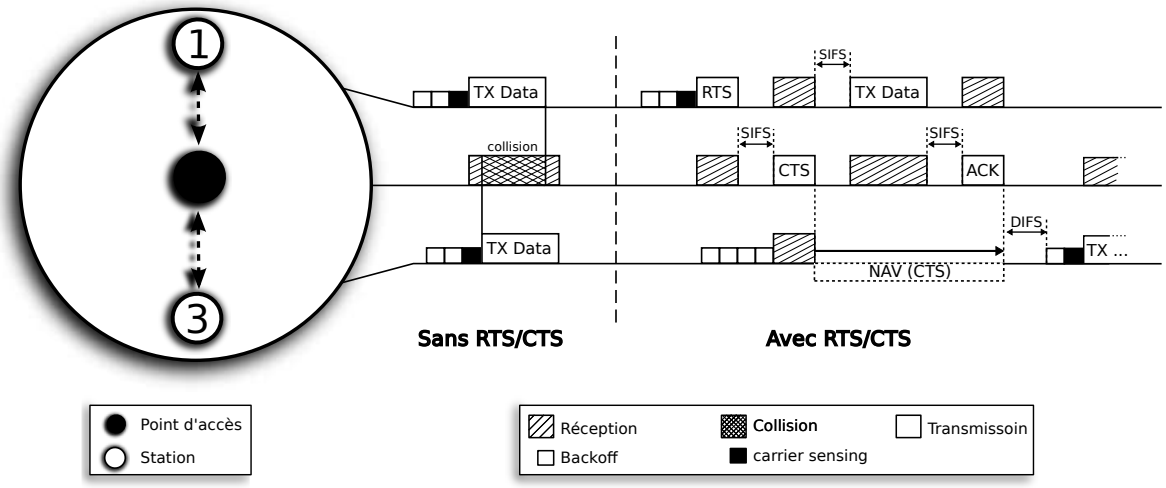



Figure 2.20 – Problème du nœud caché et solution avec RTS/CTS

décoder correctement l'une au l'autre station. Afin de pallier ce problème, la norme IEEE 802.11 décrit le mécanisme RTS/CTS permettant d'éviter ce type de situation.

Avec RTS/CTS, avant de transmettre sa trame de donnée, la station 1 envoie une trame de type Request-To-Sent (RTS) à l'AP. À la réception du RTS, l'AP répond avec une trame Clear-To-Send (CTS) qui sera reçue par l'ensemble des stations connectées à l'AP. Ce CTS donne le droit à la station ayant initié la requête de transmettre sa trame, mais indique également aux autres stations que le canal sera occupé pour une période de temps. Cela est représenté au niveau de la station 2 par un *timer* appelé Network Allocation Vector (NAV) qui démarre à la réception du CTS et qui dure le temps de la transmission de la station 1. Le NAV agit comme si le canal était occupé. En procédant ainsi, on évite les collisions au niveau de l'AP mais c'est une procédure coûteuse puisqu'elle rajoute des échanges de trames.

Le mécanisme RTS/CTS est optionnel et est généralement activé lorsqu'un seuil de sensibilité est franchi où lorsqu'une trame de données à transmettre est trop gros. Cela se configure au niveau des stations par l'administrateur de la machine.

### 2.4.6 Beacon, Scan et découverte de réseau

Un réseau, qu'il soit *ad hoc* ou infrastructure, est annoncé par la diffusion périodique de message appelé *Beacon*. Ces messages contiennent des information sur le réseau telle que le *timestamp* (pour la coordination des nœuds), le temps d'intervalle entre deux *beacon*, les débits possibles (en termes de débit), les informations d'identification (SSID, BSSID) et les paramètres de modulation. Dans le mode infrastructure, ces

*beacon* sont envoyés périodiquement par l'AP. L'intervalle est d'environ toutes les $100ms$ mais cela est configurable par l'administrateur de l'AP. La figure 2.21 donne un exemple d'émission périodique d'un *beacon* par un AP. Si à un instant donné l'AP ne peut pas émettre de *beacon* parce que le canal est déjà occupé, il diffère sa transmission et transmet le *beacon* dès que le canal est de nouveau libéré.

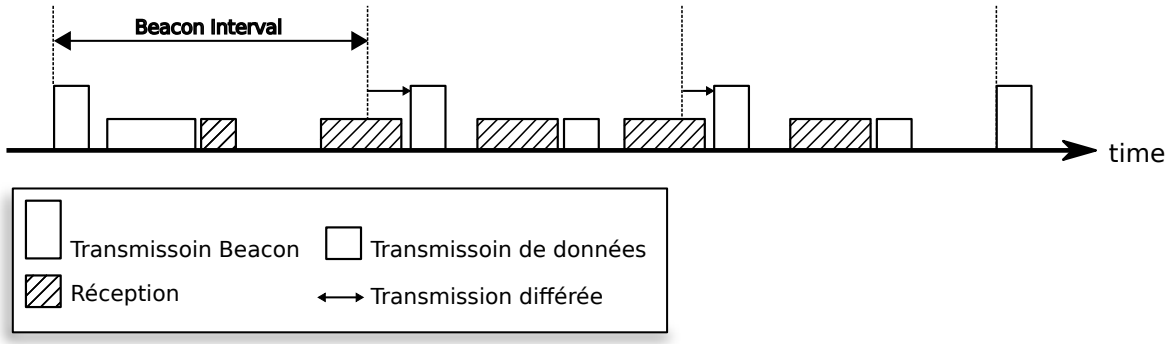



Figure 2.21 – Émission périodique de beacon par un AP IEEE 802.11

Dans le mode *ad hoc*, toutes les stations participent pour envoyer des *beacons*, mais pour éviter de surcharger le réseau, les stations n'envoient pas toutes des *beacons* en même temps. Comme pour le mode infrastructure, l'envoi des *beacons* est fait périodiquement en suivant l'intervalle défini par la première station à avoir créé le réseau *ad hoc*. Pour éviter que plusieurs stations n'envoient un *beacon* en même temps, le protocole utilisé est de type CSMA/CA c'est-à-dire qu'au moment où un beacon doit être envoyé, chaque station tire un *backoff* aléatoire. Le *beacon* est transmis par la première station pour laquelle le *backoff* arrive à zéro, les autres stations annulent leurs *backoff*. La figure 2.22 donne un exemple de fonctionnement dans un réseaux *ad hoc* constitué de deux stations.

La phase de *scanning* est une primitive de IEEE 802.11 permettant de recenser les ressources disponibles sur l'ensemble des canaux. Elle permet de remonter aux couches supérieurs la liste des points d'accès ou réseaux *ad hoc* environnants. La procédure de scanning doit être effectuée le plus rapidement possible afin de pouvoir avoir des algorithmes de *handover* efficaces. Le *handover* est le mécanisme permettant de se déconnecter d'un AP pour se raccrocher à un autre. Ce cas de figure arrive par exemple lorsqu'un utilisateur se déplace dans un immeuble et au fur à mesure qu'il se déplace, son ordinateur se connecte au meilleur AP disponible (appartenant au même ESS). Afin que cela se fasse le plus efficacement possible, il faut que la phase de *scanning* soit la plus courte possible, tout en recensant le maximum d'AP à la fois. Il existe deux façon de faire du *scanning*, une méthode appelée le **scan passif** et une autre appelée le **scan actif**.

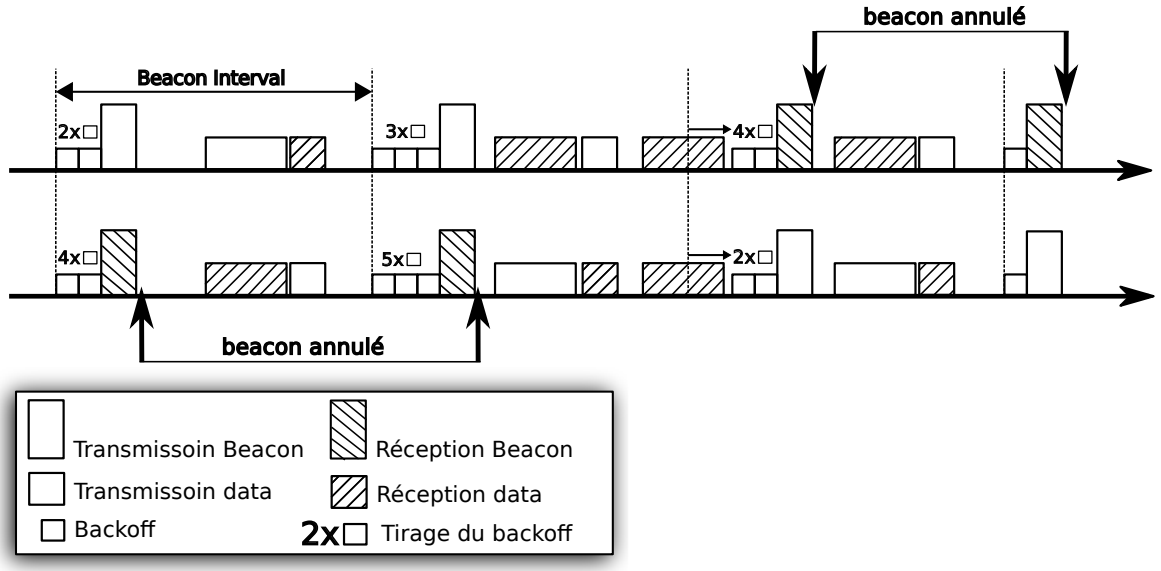



Figure 2.22 – Émission périodique de beacon dans le mode *ad hoc* de IEEE 802.11

#### 2.4.6.1 Scan passif

Le scan passif consiste à écouter chaque canal pour une période de temps donnée afin d'y détecter la présence éventuelle des *beacons* périodiques. Cet algorithme se base sur un *timer* appelé *Channel Time* qui est réinitialisé à chaque fois que la station écoute un nouveau canal. Lorsque le timer expire, la station passe au canal suivant et recommence.

#### 2.4.6.2 Scan actif

Le *scan* actif consiste à forcer la réception d'un *beacon* au moyen d'une trame appelé **probe request**. Lorsqu'une *probe request* est envoyée sur un canal, tous les points d'accès et les stations *ad hoc* environnantes doivent répondre avec une **probe response** en suivant la méthode DCF. Les *probe responses* ne peuvent pas être renvoyées après un temps SIFS car il peut y avoir plusieurs réponses et il faut donc utiliser le mécanisme de contention afin d'éviter les collisions. Cela implique que le moment où la station recevra les *probe responses* est indéterminé car il peut y avoir un certain nombre de trames de données entre l'émission du *probe request* et la réception des **probe responses**. La procédure du scanning actif se base sur deux timers au lieu d'un seul dans le scan passif. Le premier timer, appelé *Minimum Channel Time* est le temps minimum à passer sur un canal pour recevoir des *beacons* ou des *probe responses*. Si au-delà de ce temps aucun *beacon* ni *probe response* n'a été reçu, la station passe au canal suivant et recommence. Si au moins un *beacon* a été reçu, la station at-

tend alors jusqu'au deuxième *timer* appelé *Maximum Channel Time* pour en recevoir d'autres.

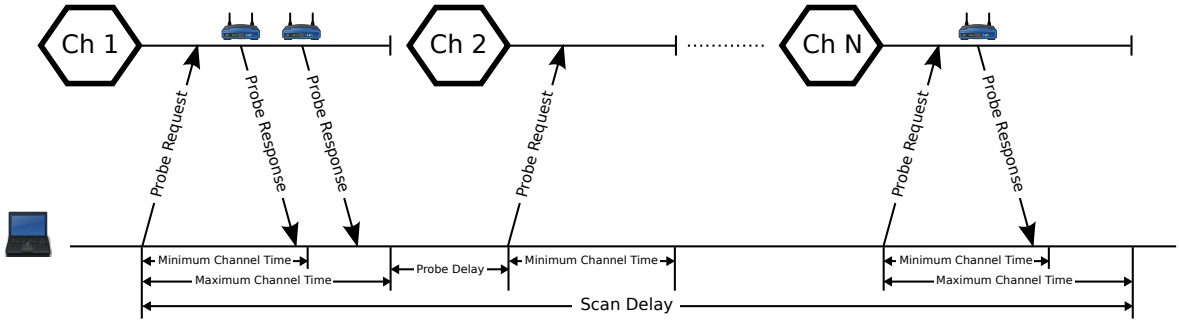


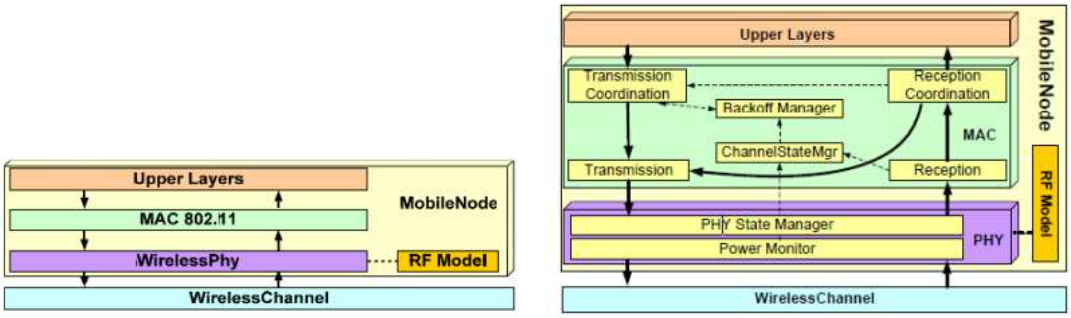

Figure 2.23 – Procédure de scan actif dans IEEE 802.11

La figure 2.23 donne un exemple de *scanning* actif. Dans le canal 1, la station reçoit un premier *probe response* avant la fin du premier timer et attend donc jusqu'à l'expiration du deuxième timer. On remarque d'une deuxième réponse à été reçue durant cette période, à l'expiration du deuxième timer la station passe au canal suivant. dans le canal 2 aucune *probe response* n'a été reçue, la station passe directement au canal suivant à la fin du premier *timer*. Dans le dernier canal, la station reçoit une première *probe response* durant le premier *timer* mais ne reçoit rien après, elle attendra donc le temps maximal pour rien.

## 2.5 IEEE 802.11 dans le simulateur NS-2

Network Simulator version 2 (NS-2) est un simulateur de réseau open source écrit en TCL et C++. Il existe deux principales implémentations de IEEE 802.11 dans ce simulateur appelées Mac80211 et Mac80211Ext [CSEJ+07]

La figure 2.24a et 2.24b montre l'architecture de ces deux modules. Le module original est la première implémentation de 802.11 et est assez simple dans sa façon de fonctionner. Cette implémentation se concentre plus particulièrement sur une représentation fidèle des mécanismes de la MAC et implémente toute la sous-couche de gestion (association, authentification, *beacon*, etc.). Étant la première implémentation, beaucoup de travaux dans la littérature se base sur cette implémentation. Cependant, cette implémentation possède un certain nombre de défauts à la fois dans l'architecture et dans les détails des modèles de la MAC et de la couche physique. La chaîne de transmission/réception est naïve et ne gère pas de façon fine les transmissions simultanées. Ce module n'implémente pas non plus le préambule et l'entête PLCP qui précède chaque transmission de trame dans 802.11. Le mo-




(a) Implémentation de 802.11 par le module Mac80211

(b) Implémentation de 802.11 par le module Mac80211Ext

Figure 2.24 – Architecture des deux architectures principales de NS-2 (figures empruntés à [CSEJ+07], Fig. 2 et Fig. 3)

dule 802.11Ext est une implémentations du standard IEEE 802.11g de l'université de Karlsruhe [CSEJ+07]. Le module 802.11Ext fournit à la fois une implémentation de la mac (mac-802.11Ext) mais également une modélisation de la couche physique (phy-802.11Ext). Le module physique de ce module inclut le calcul du SINR, du préambule, l'entête PLCP ainsi que des effets de capture. La couche MAC de ce module n'implémente en revanche pas les mécanisme de la sous-couche de gestion. Comme on peut le voir sur la figure 2.24b, cette implémentation décrit les mécanismes de réception/transmission, de backoff et de gestion de l'état du canal d'une façon modulaire.

Durant cette thèse, nous avons basé nos travaux sur le module 802.11Ext car nous avions besoin d'un modèle de canal détaillé. De plus, la modularité offerte par ce module a permis une prise en main rapide du code. Nous décrivons dans cette section les améliorations que nous avons apportées à ce module afin d'implémenter un modèle plus réaliste de Packet Error Rate (PER), basé sur un échantillonnage des valeurs de Bit Error Rate (BER) trouvé dans la littérature.

### 2.5.1 Implémentation d'un modèle réaliste de PER dans NS-2

La couche physique du module phy-802.11Ext modélise la sous-couche PLCP qui constitue la sous-couche logique de la couche physique de 802.11. Ce module maintient quatre états tel que représenté sur la figure 2.25.La transmission et la réception d'une trame dans ce module sont gérés de la façon suivante :

1. La trame est transmise par l'émetteur avec une puissance $P_t$ (état TXing sur l'émetteur)

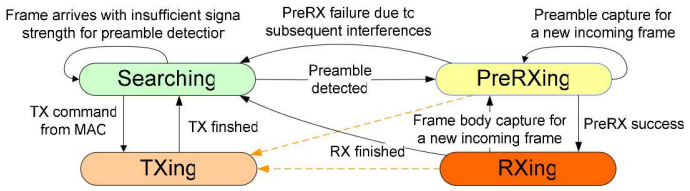



Figure 2.25 – Différents états de la couche physique 802.11 dans l'implémentation 802.11Ext

2. La trame est envoyée à la couche modélisant le canal qui envoie la trame à la couche physique de tous les récepteurs (état RXing sur les récepteurs). Chaque récepteur reçoit la trame avec une puissance $P_r$ différente par récepteur, calculé par le modèle de propagation *freespace* qui prend en compte les puissances, la distances et les gains des antennes.

3. Sur chaque récepteur, la couche phy-802.11Ext estime le SINR (en $dB$) de chaque signal reçu en fonction de la puissance reçu $P_r$, des transmissions environnantes et du bruit.

4. En fonction du SINR, un PER est déterminé après consultation d'un tableau (basé sur un seuil propre à la modulation utilisée), suite à quoi un tirage aléatoire détermine si la trame est reçue ou non de façon à ce que le taux de perte corresponde au PER déterminé.

Les modifications que nous avons apportées à la couche physique concerne le point 4. Le module 80211Ext actuel ne prend pas en considération la taille de la trame dans le calcul du PER. Ces valeurs de PER ont été pré-calculés et sont ensuite déterminé pendant la simulation en se basant sur un seuil de la valeur du SINR. Une telle limitation pourrait fortement biaiser les résultats puisqu'un ACK aurait les même chances d'être perdu qu'une trame de 1500 octets. Le modèle actuel est donc très pessimiste et surtout inexact.

Afin d'avoir une approche plus exact du problème, nous allons estimer le Bit Error Rate (BER) ce qui permettra de calculer le PER quelque soit la taille de la trame. IEEE 802.11g utilise la modulation OFDM pour fournir différents débit 6, 9, 12, 18, 24, 36, 48 et 54 Mbps. Chaque mode de transmission a ses propres caractéristiques tel que la valence $V$, le nombre de bits par symbol (NBPS), la modulation (BPSK, QPSK, QAM-16 ou QAM-64), le taux de codage et la distance de *hamming* $d$. Le BER est différent pour chacun de ces mode de transmission car il dépend de ces caractéristiques. Le tableau 2.4 indique la valeur de chaque paramètre OFDM pour chaque mode de transmission.

| PHY mode | Modulation | Valence | NBPS | Coding rate | Hamming | débit brut |
|---|---|---|---|---|---|---|
| 1 | BPSK | 1 | 48 | 1/2 | 10 | 6 Mbps |
| 2 | BPSK | 1 | 48 | 3/4 | 5 | 9 Mbps |
| 3 | QPSK | 2 | 96 | 1/2 | 10 | 12 Mbps |
| 4 | QPSK | 2 | 96 | 3/4 | 5 | 18 Mbps |
| 5 | QAM-16 | 4 | 192 | 1/2 | 10 | 24 Mbps |
| 6 | QAM-16 | 4 | 192 | 3/4 | 5 | 36 Mbps |
| 7 | QAM-64 | 6 | 288 | 2/3 | 6 | 48 Mbps |
| 8 | QAM-64 | 6 | 288 | 3/4 | 5 | 54 Mbps |

Tableau 2.4 – valeurs des paramètres OFDM pour chaque mode de transmission dans IEEE 802.11g

La Valence $(V)$ est le nombre de bits que peut coder une porteuse qui est dépendante de la modulation utilisée. Par exemple avec la modulation BPSK, $V$ est égale à $1$ et donc la modulation BPSK permet de transmettre $48$ bits par symbole car OFDM utilise $48$ sous-porteuses, d'où $NBPS = 48$. Afin d'être plus résistant aux perturbations, OFDM ajoute de la redondance pour rendre l'information plus robuste. C'est ce qu'on appelle le *coding rate*, exprimé sous la forme $x/y$, pour $x$ bits en entrée, $y$ sont transmis. Un *coding rate* de $1/2$ double donc la quantité d'information à transmettre. Sachant qu'un symbole met $4\mu$s pour être transmis, le débit brut en bits par secondes est donc calculé de la façon suivante :

$$\text{débit} = \frac{NBPS}{\textit{coding rate} \times 4 \times 10^{-6}} \tag{2.2}$$

Le Bit Error Rate (BER) dépend de la modulation et du codage utilisé. Nous avons utilisé un tableau d'échantillonnage des valeurs de BER en fonction de ces paramètres trouvé dans la littérature [Mil03].

Ces deux tableaux 2.26 et 2.27 donnent le BER étant donné $E_b/N_o$ qui est le rapport entre l'énergie d'un bit (bit utilisateur avant encodage) et la densité spectrale de bruit. Le calcul de $E_b/N_o$ peut être trouvé à partir du SINR grâce à la formule 2.3

$$E_b/N_o = SINR - 10log(V) + 10log(\frac{1}{\textit{coding rate}}) \tag{2.3}$$

De cette façon, nous pouvons calculer le BER étant donné un mode de transmission et le $SINR$. Pour une taille $L$ de trame donné et la distance de *hamming* $d$, on peut calculer le PER avec la formule suivante, obtenu depuis la littérature :

| $E_b/N_0$ (dB) | BPSK | | | | | | | | QPSK | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $r$ = 1/2, soft | | $r$ = 3/4, soft | | $r$ = 1/2, hard | | $r$ = 3/4, hard | | $r$ = 1/2, soft | | $r$ = 3/4, soft | | $r$ = 1/2, hard | | $r$ = 3/4, hard | |
| | # pkt | BER | # pkt | BER | # pkt | BER | # pkt | BER | # pkt | BER | # pkt | BER | # pkt | BER | # pkt | BER |
| 0.0 | 10,000 | 2.00E-1 | 5,000 | 3.21E-1 | 10,000 | 3.49E-1 | 10,000 | 3.76E-1 | 5,000 | 2.78E-1 | 5,000 | 4.10E-1 | 5,000 | 4.06E-1 | 5,000 | 4.51E-1 |
| 0.5 | | 1.49E-1 | | 2.88E-1 | | 3.13E-1 | | 3.60E-1 | | 2.13E-1 | | 3.81E-1 | | 3.77E-1 | | 4.36E-1 |
| 1.0 | | 1.01E-1 | | 2.42E-1 | | 2.75E-1 | | 3.38E-1 | | 1.51E-1 | | 3.38E-1 | | 3.42E-1 | | 4.20E-1 |
| 1.5 | 20,000 | 6.06E-2 | | 1.90E-1 | | 2.28E-1 | | 3.09E-1 | 10,000 | 9.22E-2 | | 2.81E-1 | | 2.94E-1 | | 3.92E-1 |
| 2.0 | | 3.31E-2 | | 1.31E-1 | | 1.80E-1 | | 2.73E-1 | | 4.88E-2 | | 2.08E-1 | | 2.38E-1 | | 3.54E-1 |
| 2.5 | 50,000 | 1.50E-2 | 10,000 | 8.21E-2 | | 1.32E-1 | | 2.27E-1 | 25,000 | 2.22E-2 | 10,000 | 1.34E-1 | | 1.77E-1 | | 3.10E-1 |
| 3.0 | | 6.04E-3 | | 4.05E-2 | | 8.80E-2 | | 1.79E-1 | | 8.54E-3 | | 7.14E-2 | | 1.22E-1 | | 2.53E-1 |
| 3.5 | 100,000 | 2.13E-3 | | 1.91E-2 | | 5.30E-2 | | 1.28E-1 | 50,000 | 2.71E-3 | | 3.05E-2 | | 7.43E-2 | | 1.89E-1 |
| 4.0 | | 6.23E-4 | | 6.35E-3 | | 2.91E-2 | | 8.30E-2 | 100,000 | 7.38E-4 | | 1.09E-2 | | 4.03E-2 | | 1.26E-1 |
| 4.5 | | 1.41E-4 | 20,000 | 2.20E-3 | 20,000 | 1.41E-2 | 20,000 | 4.93E-2 | | 1.78E-4 | 20,000 | 3.12E-3 | | 1.78E-2 | | 7.53E-2 |
| 5.0 | | 4.21E-5 | | 5.31E-4 | | 6.18E-3 | | 2.60E-2 | | 4.00E-5 | | 7.31E-4 | | 8.40E-3 | | 3.97E-2 |
| 5.5 | | 6.43E-6 | | 1.69E-4 | | 2.73E-3 | | 1.31E-2 | | 8.56E-6 | | 1.03E-4 | 10,000 | 3.11E-3 | | 1.78E-2 |
| 6.0 | | 7.14E-7 | 100,000 | 2.80E-5 | | 9.80E-4 | | 4.97E-3 | | 2.33E-7 | 100,000 | 3.62E-5 | | 1.27E-3 | | 7.41E-3 |
| 6.5 | | | | 6.21E-6 | | 2.49E-4 | | 1.91E-3 | | | | 1.06E-5 | 20,000 | 2.71E-4 | 10,000 | 2.50E-3 |
| 7.0 | | | | 6.06E-7 | 50,000 | 8.00E-5 | 50,000 | 5.89E-4 | | | | 1.59E-6 | | 6.83E-5 | 20,000 | 7.74E-4 |
| 7.5 | | | | | | 8.57E-6 | | 2.07E-4 | | | | | 50,000 | 2.16E-5 | | 1.59E-4 |
| 8.0 | | | | | 100,000 | 5.48E-6 | 100,000 | 4.52E-5 | | | | | | 5.11E-6 | | 4.09E-5 |
| 8.5 | | | | | | 2.62E-6 | | 1.02E-5 | | | | | 100,000 | 4.44E-7 | 50,000 | 9.57E-6 |
| 9.0 | | | | | | | | | | | | | | | | 4.64E-6 |
| 9.5 | | | | | | | | | | | | | | | | |
| 10.0 | | | | | | | | | | | | | | | | |

Figure 2.26 – Échantillonage des valeurs de BER pour les modulations BPSK et QPSK

| $E_b/N_0$ (dB) | 16-QAM | | | | | | | | 64-QAM | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $r$ = 1/2, soft | | $r$ = 3/4, soft | | $r$ = 1/2, hard | | $r$ = 3/4, hard | | $r$ = 2/3, soft | | $r$ = 3/4, soft | | $r$ = 2/3, hard | | $r$ = 3/4, hard | |
| | # pkt | BER | # pkt | BER | # pkt | BER | # pkt | BER | # pkt | BER | # pkt | BER | # pkt | BER | # pkt | BER |
| 0.0 | 5,000 | 4.39E-1 | | | 5,000 | 4.78E-1 | 5,000 | 4.90E-1 | 2,000 | 4.92E-1 | 2,000 | 4.93E-1 | | | | |
| 0.5 | | 4.22E-1 | | | | 4.73E-1 | | 4.87E-1 | | 4.90E-1 | | 4.92E-1 | | | | |
| 1.0 | | 3.98E-1 | 10,000 | 4.74E-1 | | 4.67E-1 | | 4.86E-1 | | 4.88E-1 | | 4.91E-1 | | | | |
| 1.5 | | 3.62E-1 | | 4.68E-1 | | 4.59E-1 | | 4.84E-1 | | 4.86E-1 | | 4.89E-1 | | | | |
| 2.0 | | 3.13E-1 | | 4.60E-1 | | 4.44E-1 | | 4.79E-1 | | 4.84E-1 | | 4.90E-1 | | | | |
| 2.5 | | 2.53E-1 | | 4.47E-1 | | 4.26E-1 | | 4.74E-1 | | 4.83E-1 | | 4.87E-1 | 2,000 | 4.91E-1 | | |
| 3.0 | | 1.83E-1 | | 4.29E-1 | | 4.00E-1 | | 4.65E-1 | | 4.77E-1 | | 4.83E-1 | | 4.89E-1 | | |
| 3.5 | 10,000 | 1.17E-1 | | 4.01E-1 | | 3.68E-1 | | 4.55E-1 | | 4.70E-1 | | 4.81E-1 | | 4.89E-1 | | |
| 4.0 | | 6.31E-2 | 20,000 | 3.60E-1 | | 3.25E-1 | | 4.39E-1 | | 4.62E-1 | | 4.77E-1 | | 4.85E-1 | | |
| 4.5 | | 2.89E-2 | | 3.03E-1 | 10,000 | 2.71E-1 | | 4.16E-1 | 5,000 | 4.49E-1 | | 4.70E-1 | | 4.80E-1 | | |
| 5.0 | 50,000 | 1.05E-2 | | 2.28E-1 | | 2.12E-1 | | 3.84E-1 | | 4.34E-1 | | 4.65E-1 | | 4.74E-1 | | |
| 5.5 | | 3.50E-3 | | 1.49E-1 | | 1.53E-1 | 10,000 | 3.48E-1 | | 4.09E-1 | 5,000 | 4.56E-1 | | 4.68E-1 | | |
| 6.0 | 100,000 | 9.36E-4 | 50,000 | 7.94E-2 | 20,000 | 1.00E-1 | | 2.95E-1 | | 3.74E-1 | | 4.40E-1 | | 4.59E-1 | | |
| 6.5 | | 2.19E-4 | | 3.39E-2 | | 6.04E-2 | | 2.36E-1 | 10,000 | 3.20E-1 | | 4.19E-1 | | 4.43E-1 | | |
| 7.0 | | 4.90E-5 | | 1.24E-2 | | 3.32E-2 | | 1.73E-1 | | 2.54E-1 | | 3.89E-1 | | 4.25E-1 | 5,000 | 4.55E-1 |
| 7.5 | 50,000 | 1.13E-5 | | 3.70E-3 | | 1.59E-2 | 20,000 | 1.14E-1 | | 1.75E-1 | 10,000 | 3.44E-1 | | 3.98E-1 | | 4.39E-1 |
| 8.0 | | 1.51E-6 | 100,000 | 1.02E-3 | 50,000 | 7.02E-3 | | 6.76E-2 | | 1.03E-1 | | 2.81E-1 | | 3.65E-1 | | 4.20E-1 |
| 8.5 | | | | 2.68E-4 | | 2.91E-3 | | 3.51E-2 | 20,000 | 5.07E-2 | | 2.04E-1 | | 3.23E-1 | | 3.92E-1 |
| 9.0 | | | 200,000 | 6.64E-5 | 100,000 | 1.09E-3 | | 1.66E-2 | | 2.02E-2 | | 1.26E-1 | | 2.76E-1 | | 3.59E-1 |
| 9.5 | | | 50,000 | 1.62E-5 | | 3.77E-4 | 50,000 | 7.01E-3 | | 6.57E-3 | 20,000 | 6.36E-2 | | 2.17E-1 | | 3.15E-1 |
| 10.0 | | | | 2.34E-6 | | 1.15E-4 | | 2.69E-3 | | 2.07E-3 | | 2.66E-2 | | 1.64E-1 | | 2.59E-1 |
| 10.5 | | | | | | 3.87E-5 | 100,000 | 9.19E-4 | 50,000 | 5.31E-4 | | 9.11E-3 | 5,000 | 1.10E-1 | 10,000 | 2.03E-1 |
| 11.0 | | | | | | 1.07E-5 | | 2.76E-4 | | 1.40E-4 | | 3.00E-3 | | 6.85E-2 | | 1.44E-1 |
| 11.5 | | | | | | 1.34E-6 | | 8.15E-5 | | 3.50E-5 | 100,000 | 8.24E-4 | | 3.78E-2 | | 9.38E-2 |
| 12.0 | | | | | | | | 1.80E-5 | 100,000 | 6.93E-6 | | 2.35E-4 | | 2.00E-2 | | 5.57E-2 |
| 12.5 | | | | | | | 200,000 | 3.05E-6 | | 1.19E-6 | | 6.67E-5 | | 9.21E-3 | | 3.01E-2 |
| 13.0 | | | | | | | 100,000 | 1.13E-6 | | 3.17E-7 | | 1.97E-5 | 10,000 | 3.94E-3 | 20,000 | 1.43E-2 |
| 13.5 | | | | | | | | 6.38E-7 | | | | 5.80E-6 | | 1.67E-3 | | 6.42E-3 |
| 14.0 | | | | | | | | | | | | 1.08E-6 | | 6.18E-4 | | 2.57E-3 |
| 14.5 | | | | | | | | | | | | | | 1.90E-4 | 50,000 | 9.37E-4 |
| 15.0 | | | | | | | | | | | | | 50,000 | 5.32E-5 | | 3.30E-4 |
| 15.5 | | | | | | | | | | | | | | 1.55E-5 | | 9.77E-5 |
| 16.0 | | | | | | | | | | | | | 100,000 | 3.86E-6 | | 2.85E-5 |
| 16.5 | | | | | | | | | | | | | | 8.47E-7 | 100,000 | 6.50E-6 |
| 17.0 | | | | | | | | | | | | | | 3.70E-7 | | 2.25E-6 |
| 17.5 | | | | | | | | | | | | | | | | 3.52E-7 |

Figure 2.27 – Échantillonage des valeurs de BER pour les modulations QAM-16 et QAM-64

$$\begin{cases} PER_1 = \frac{L.BER}{d}, \\ PER_2 = 1 - (1 - BER)^L, \end{cases} \tag{2.4}$$

$$PER = min(PER_1, PER_2). \tag{2.5}$$

Le $PER_2$ est une expression naïve du PER puisqu'il ne prend pas en compte la distance de hamming $d$ c'est-à-dire la capacité des mécanismes de codage de "réparer" un bit erroné. Le $PER_1$ est une approximation plus juste du PER pour une BER faible. Cependant, on remarque pour pour un BER élevé, $PER_1$ peut être supérieur à 1. L'expression du $PER$ est ainsi le minimum entre le $PER_1$ et le $PER_2$.

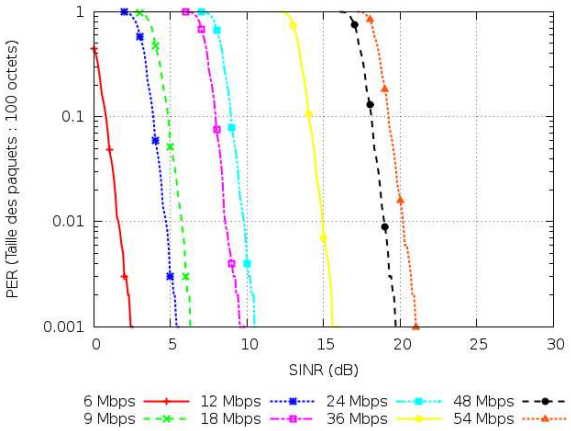
### 2.5.2 Validation de l'implémentation dans NS-2


Figure 2.28 – Scénario simple

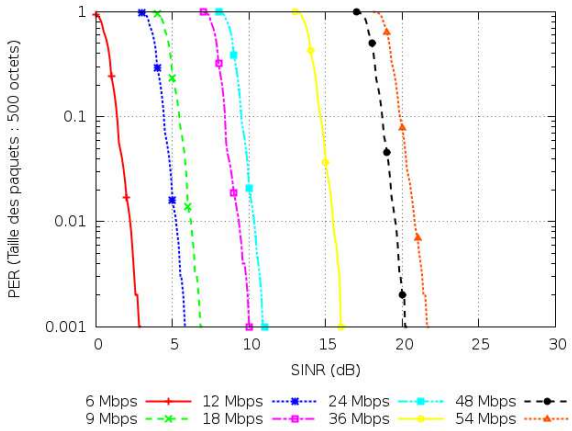
| MAC/802.11Ext | | PHY/802.11Ext | |
|---|---|---|---|
| **Paramètre** | **Valeur** | **Paramètre** | **Valeur** |
| CWMin | 15 | CSThresh | $6.30957e-13$ |
| CWMax | 1023 | Pt | 0.001 |
| SlotTime | 0.000009 | freq | $5.18e9$ |
| SIFS | 0.000016 | noise floor | $2.51189e-13$ |
| ShortRetryLimit | 0 | L | 1.0 |
| LongRetryLimit | 0 | PowerMonitorThresh | 0 |
| HeaderDuration | 0.000020 | HeaderDuration | 0.000020 |
| SymbolDuration | 0.000004 | PreambleCaptureSwitch | 1 |
| BasicModulationScheme | 0 | DataCaptureSwitch | 0 |
| RTSThreshold | 2000 | SINR PreambleCapture | 2.5118 |
| CSThresh | $6.30957e-13$ | SINR DataCapture | 100.0 |
| | | dist | $1e6$ |

Tableau 2.5 – Paramètre de simulation

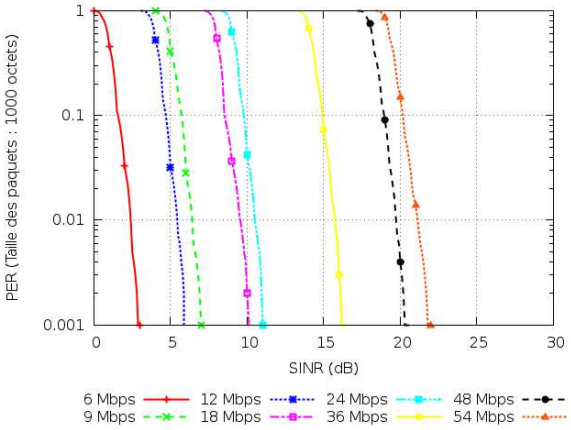
Afin de tester l'implémentation de la couche physique nous avons effectué quelques simulations dans le scénario décrit par la figure 2.28. Le tableau 2.5 donne les paramètres de simulation que nous avons utilisés. Nous avons effectué 120 simulations pour faire varier les 8 modes de transmissions possibles et pour 15 tailles de trame différentes (de 100 à 1500 octets). Les figures 2.29 montre le PER en fonction du SINR pour chaque mode de transmission et pour quatre différentes tailles de trame (100, 500, 1000 et 1500 octets). On peut voir que pour un SINR identique, plus le paquet est de petite taille, plus la probabilité de succès est élevée, ce qui correspond au comportement attendu.



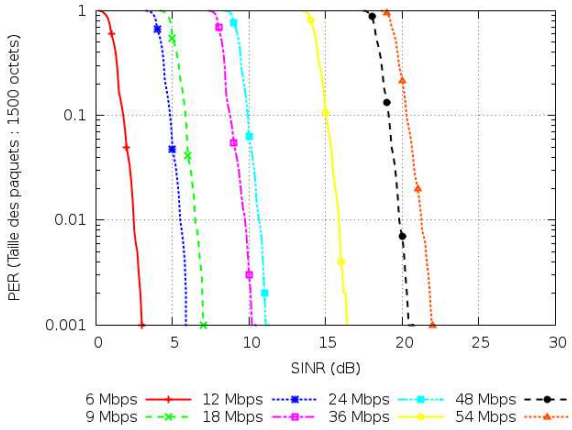

(a) PER pour chaque mode en fonction du SINR pour une trame de 100 octets




(b) PER pour chaque mode en fonction du SINR pour une trame de 500 octets




(c) PER pour chaque mode en fonction du SINR pour une trame de 1000 octets

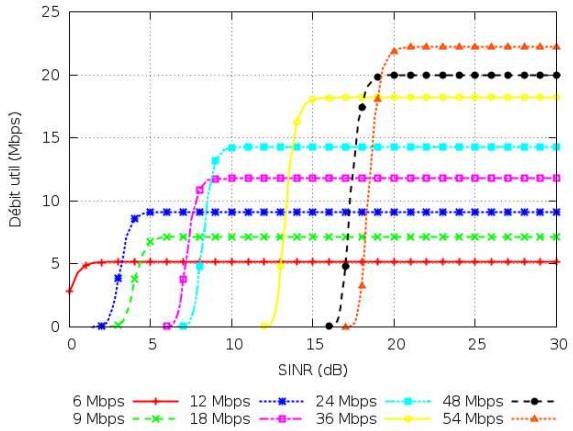



(d) PER pour chaque mode en fonction du SINR pour une trame de 1500 octets

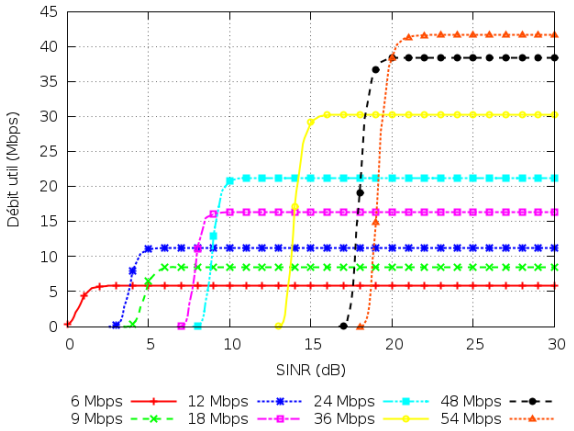
Figure 2.29 – PER en fonction du SINR et du mode de transmission pour différentes tailles de trames

Les figures 2.30 montre le *débit applicatif*[3] en fonction du SINR pour chaque mode de transmission et pour différentes tailles de trame ($100$, $500$, $1000$ et $1500$ octets). Par exemple, pour un mode de transmission de $54$ Mbps, on voit que le débit est plus important avec des trames de $1500$ octets ( 50mbps) qu'avec des trames de $100$ octets ( 22Mbps). La différence que l'on observe dans les débits pour les différentes tailles de trame est due au fait que chaque émission de trame est précédée d'un préambule de $20\mu$s. Cela n'est pas négligeable dans le cas d'une trame de 100 octets puisque le préambule à lui seul représente $12.8\%$ du temps d'émission ($100$ octets = $34$ symboles soit $34 * 4 = 136\mu$s,$20\mu$s représentant donc $12.8\%$).

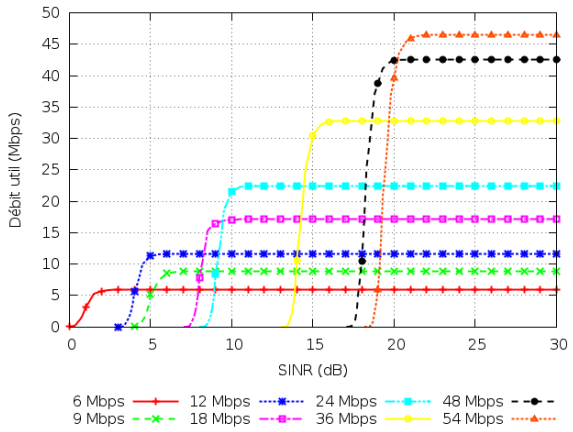
[3]on trouvera le terme de goodput dans la littérature



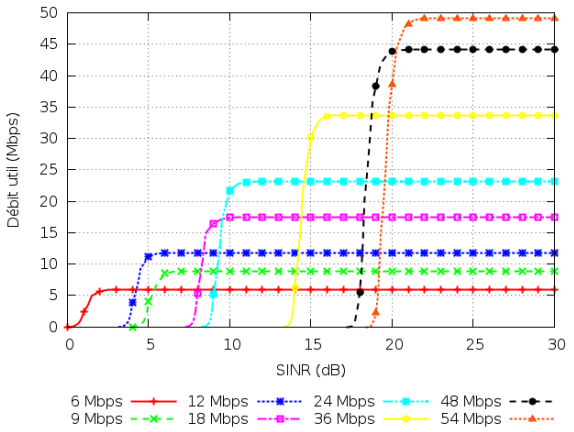

(a) débit pour chaque mode en fonction du SINR pour une trame de 100 octets




(b) débit pour chaque mode en fonction du SINR pour une trame de 500 octets




(c) débit pour chaque mode en fonction du SINR pour une trame de 1000 octets




(d) débit pour chaque mode en fonction du SINR pour une trame de 1500 octets

Figure 2.30 – Débit applicatif en fonction du SINR et du mode de transmission pour différentes tailles de trame

## 2.6 Adaptation du débit d'une station IEEE 802.11

### 2.6.1 Adaptation du débit dans les chipset 802.11

La norme IEEE 802.11 ne décrit pas de mécanisme d'adaptation du débit en fonction des conditions du réseau. On sait que plus le débit est important, plus il est sensible aux perturbations et se propage donc moins loin. D'une façon générale, lorsque le signal avec un AP est faible, plus le débit est important, plus le *Packet Error Rate* PER est important, ce qui implique un nombre tout aussi important de retransmissions. Les développeurs des drivers 802.11 ont été libres dans le choix de l'algorithme de sélection du débit. La plupart des drivers se basent sur la puissance du signal reçu, le

RSSI, et choisissent le débit à adopter en fonction de ce dernier. Mais cette approche est naïve et ne prend pas en compte la nature des interférences.

Une trame transmise a une certaine probabilité d'être reçue, dépendante d'un certain nombre de variables telles que la distance avec la destination, les effets de multi-chemins ou même les interférences avec d'autres appareils. Or on ne peut savoir à l'avance quelle variable va prédominer et on ne sait pas non plus quelles seront les interférences auxquelles une transmission sera sujette. Par exemple, si les interférences sont par *burst*, alors des trames envoyées rapidement ont plus de chance de traverser les intervalles silencieux et donc un débit élevé est préférable.

On peut distinguer un algorithme appelé minstrel, développé sous Linux par Derek Smithies pour le driver madwifi[4]. Cet algorithme se distingue par une approche heuristique se basant sur des échantillons réels de mesure de performance. Ce dernier offre la possibilité de choisir le meilleur débit pour un instant donné et de s'adapter automatiquement aux changements de l'environnement. Minstrel fonctionne en essayant tous les débits possibles et choisit celui qui offre les meilleures performances. La mesure de performance est le débit utile calculé pour chaque débit par la formule 2.6.

$$debit = \frac{P_{succes} * Mb_{transmis}}{T_{trame}} \tag{2.6}$$

La formule 2.6 calcule le débit utile, pour un débit donné, par la multiplication entre la probabilité de succès (approximé par les résultats passés) et le débit pour transmettre les données. Les performances de toutes les transmissions effectuées par la station mettent ainsi à jour un tableau contenant le débit utile pour chaque débit. Afin de connaitre la probabilité de succès pour tous les débits, $10\%$ des trames sont envoyées à des débits non optimaux afin de les tester, même lorsque les conditions ne changent pas. L'un des aspects les plus intéressants de minstrel est le fait que les résultats plus récents ont plus d'importance que les résultats anciens, grâce à l'usage d'une moyenne mobile exponentielle EWMA[Ph.07]. Dans le calcul de la moyenne pour la probabilité de succès, les résultats les plus récents ont un poids exponentiellement plus important que les résultats les plus anciens. Un résultat récent est un résultat obtenu dans les derniers $100ms$. Toutes les $10ms$, la table EWMA est mise à jour et minstrel sélectionne le meilleur débit.

En plus de choisir le meilleur débit étant donné une situation, minstrel définit également une liste de débit à utiliser en cas de retransmission. Ce procédé s'ap-

[4]Madwifi était le driver pour les cartes WiFi à chipset atheros. Ce projet est obsolète et a depuis été remplacé par le projet linux-wireless

pelle la *Retry Chain* ou chaîne de retransmission. La première transmission est ainsi effectuée avec le meilleur débit, la deuxième avec le deuxième meilleur débit, la troisième avec le débit offrant la meilleure probabilité de transmission et la quatrième retransmission est effectuée avec le débit le plus faible.

### 2.6.2 Implémentation de l'adaptation du débit dans NS-2

$NS-2$ ne dispose pas de base d'un mécanisme d'adaptation de débit. On peut trouver dans la littérature quelques implémentations, souvent pour le besoin de valider un nouveau mécanisme, mais ces implémentations sont souvent obsolètes ou mal supportées. Nous avons donc implémenté un mécanisme naïf d'adaptation de débit basée sur notre implémentation du PER. Nous avons fait l'hypothèse que les stations 802.11 ont accès à la valeur du SINR instantanément et pour toutes les modulations. En pratique cette valeur est difficile à estimer car elle requiert un échantillonnage et un échange de trame similaire à celui décrit pour minstrel. Cependant il est peut être justifier de faire l'hypothèse qu'une station choisit à un instant donné le meilleur débit possible afin de ne pas introduire de biais des résultats de simulation liés à ce mécanisme d'adaptation du débit. Notre algorithme choisit ainsi la meilleur modulation en calculant la meilleure modulation possible en fonction de la taille des trames et du SINR. Pour chaque mode de transmission $mode$, on calcul le débit possible $D_{mode}$ en fonction de la taille des trames $size$, du temps de transmission d'une trame $T_{trame}$, et du $PER$ (qu'une station peut estimer en fonction de son SINR grâce à la table précédente) avec la formule donnée en équation 2.7.

$$D_{mode} = \frac{size * (1 - PER)}{T_{trame}} \tag{2.7}$$

On en déduit le meilleur mode de transmission $B_{mode}$ comme étant celui offrant le meilleure débit (on rappel qu'il y a $8$ modes de transmission possible) :

$$B_{mode} = \{maxD_i; 0 < i < 7\} \tag{2.8}$$

Nous avons effectués des simulations avec la même topologie et les mêmes paramètres MAC et physique que présentés dans le tableau 4.1. La source génère un trafic vers l'AP de façon à ce qu'il sature son lien IEEE 802.11. Nous avons ensuite effectué différentes simulations en faisant varier la position de la source (sur 500 positions), chaque simulation étant lancée pour une durée de 20 secondes simulées. La figure 2.31 représente le débit atteint par la station pour ces différents emplacements,

l'algorithme de sélection de débit ayant automatiquement choisit la meilleure modulation en fonction de son SINR.

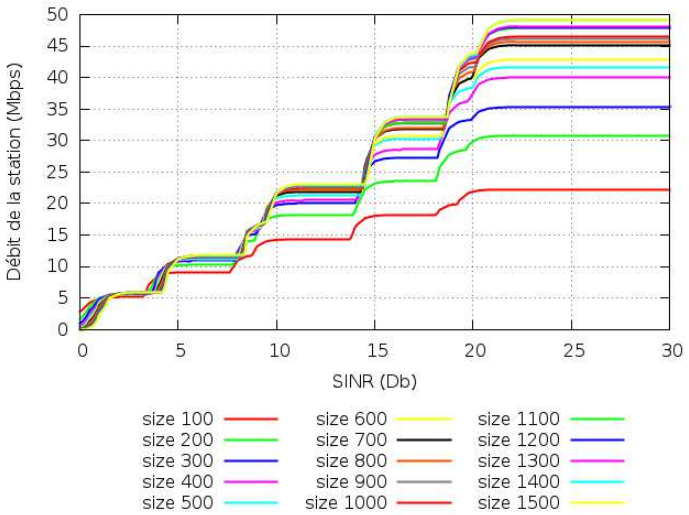



Figure 2.31 – Station 802.11 adaptant son débit automatiquement en fonction du SINR

### 2.6.3 Problème liés à l'adaptation du débit

Les réseaux IEEE 802.11 sont appelés réseaux *multi-rate* car plusieurs stations avec des débits différents peuvent co-exister au sein d'une même cellule. On sait qu'il existe de nombreuses raisons pouvant influencer la qualité d'un lien sans-fil en fonction du temps, comme les interférences, l'atténuation due à la distance, les trajets multi-chemins, les propriétés de propagation, le bruit ou la mobilité [ABB+04]. Pour ces raisons, et comme expliqué en section 2.6, une station peut adapter son débit en fonction des conditions du canal afin d'augmenter son débit utile. Une transmission à débit plus faible utilise une modulation plus robuste qui diminue le *Bit Error Rate* BER. Les transmissions prennent ainsi plus de temps mais cela est compensé par la diminution du taux d'erreur, qui permet globalement d'obtenir un meilleur débit utile. Dans les réseaux IEEE 802.11, cette adaptation de débit à des débit plus faible impact fortement le débit des stations environnantes. Heusse [HRBSD03] décrit ce problème en 2003 via une étude analytique du mécanisme DCF et validé par des simulations. En diminuant son débit, et donc en augmentant le temps de transmission de chaque trame, la station diminue le temps de canal disponible, impactant du même coup le débit des stations ayant un débit élevé. Ceci est du à l'objectif premier du mécanisme DCF qui recherche une équité en termes d'accès au canal mais pas en termes de temps passé sur le canal. Différentes approches ont été étudiées

pour pallier cette anomalie et peuvent être classifiées dans deux groupes. La première approche consiste à modifier la MAC pour fournir une méthode d'accès plus équitable en terme d'occupation du canal. La deuxième approche consiste à éviter que les stations éloignées diminuent leur débit en utilisant d'autres stations comme relais à haut débit. Cette deuxième approche sera étudiée plus en détail dans le chapitre 3 traitant des réseaux sans-fil multi-sauts. Pour permettre une équité en terme de temps d'occupation de canal, les approches sont généralement de faire varier en fonction du débit soit le temps d'occupation du canal, soit la probabilité d'accès au canal. Dans cette approche on propose aux stations ayant un débit plus élevé de transmettre plus longtemps pour compenser la lenteur de transmission des stations ayant un débit plus faible.

#### 2.6.3.1 Rendre 802.11 plus équitable

Pour permettre une équité en terme de temps d'occupation de canal, les approches sont généralement de faire varier en fonction du débit soit le temps d'occupation du canal, soit la probabilité d'accès au canal. Dans cette approche on propose aux stations ayant un débit plus élevé de transmettre plus longtemps pour compenser la lenteur de transmission des stations ayant un débit plus faible.

Sadeghi [SKSK05] propose en 2005 une méthode appelée Opportunistic Auto Rate (OAR) permettant à des stations ayant un débit élevé de garder le canal plus longtemps pour envoyer plusieurs trames à la suite. L'idée est de permettre à des stations d'occuper le canal aussi longtemps qu'elles le feraient si tout le monde communiquait au débit le plus bas. Par exemple si une station transmet à un débit de $11$ Mbps, et que le débit le plus bas est $2$ Mbps, cette station aurait le droit d'envoyer $\lfloor 11/2 \rfloor = 5$ trames au lieu d'une, sans avoir besoin de faire un backoff entre chacune. OAR utilise le mécanisme de fragmentation défini par 802.11 pour conserver l'accès au canal. Lorsqu'un paquet (niveau 3) est trop grand pour être transmis en une seule trame, IEEE 802.11 permet de fragmenter le paquet en plusieurs trames et de transmettre ces dernières les unes à la suite des autres. La transmission d'un paquet fragmenté doit être précédée d'un échange RTS/CTS afin que les autres stations configurent un NAV pour les empêcher de transmettre. Chaque fragment est acquitté comme une trame normale et met à jour le NAV des autres stations. La figure 2.32 représente la façon dont OAR exploite ce principe pour envoyer plusieurs trames à la suite. Le bit de fragmentation (indiquant que d'autres trames vont suivre cette transmission) est activé dans les trames de la séquence excepté pour la dernière. On voit que le canal ne peut pas être repris par une autre station à cause

du NAV d'une part, mais aussi parce que toutes les transmissions ne sont séparées que par un timer SIFS.

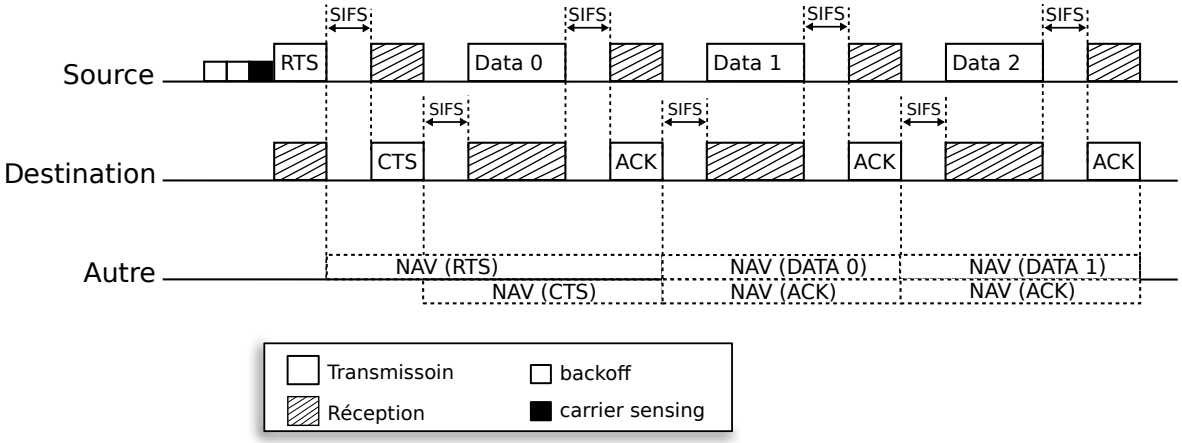



Figure 2.32 – Illustration du fonctionnement de OAR avec une station source envoyant plusieurs trames à la suite en utilisant le mécanisme de fragmentation de IEEE 802.11

Une deuxième façon de procéder pour introduire de l'équité en terme d'occupation du canal est de diminuer la probabilité d'accès au canal proportionnellement au débit. En procédant ainsi, on diminue la probabilité d'accès des stations lentes permettant aux stations rapides d'émettre plus de trames. Heusse [HRGD05] propose en 2005 le mécanisme *IdleSende* permettant de faire varier la fenêtre de contention en fonction du débit utilisé. Une station transmettant à un débit $r_{current}$ inférieur au débit maximal $r_{max}$ utilisera une fenêtre de contention plus importante calculée de la façon suivante :

$$CW' = CW \times \frac{r_{max}}{r_{current}}$$

En procédant de cette façon, les stations ayant un débit faible ont moins de chance d'accéder au canal, les empêchant ainsi d'occuper le canal trop longtemps. Il introduit également une deuxième amélioration à 802.11 pour optimiser DCF. Dans IEEE 802.11, une transmission ratée (non acquittée) est considérée comme une collision. Afin de s'adapter à la charge du réseau, la méthode DCF double la fenêtre de contention afin de réduire les probabilités de collision. Heusse affirme qu'il s'agit d'un indicateur biaisé puisque tous les échecs de transmission ne sont pas dus à des collisions et propose que toutes les stations partagent la même fenêtre de contention. Cela permet d'éviter d'introduire des délais importants dus à l'augmentation exponentielle de cette dernière qui pénalise les stations subissant des interférences.

Il décrit un mécanisme permettant d'adapter dynamiquement la taille de cette fenêtre à la charge du réseau de façon distribuée. Chaque station mesure la charge non plus sur le nombre successif d'échecs de transmission, mais sur un mécanisme d'échantillonnage permettant de mesurer la probabilité d'occupation du canal. Cet algorithme assure la convergence de la fenêtre de contention vers une taille identique pour toutes les stations.

#### 2.6.3.2 Utilisation de relais 802.11

Bahl [BCL+09] montre en 2009 que dans certains cas de figure, faire un saut de routage à haut débit plutôt que de transmettre en un saut à faible débit peut significativement augmenter les performances d'une cellule. Ce papier introduit un mécanisme de coopération appelé *SoftRepeater* pour les cellules IEEE 802.11 en mode infrastructure (avec un AP). L'approche décrite est de transformer une station en *SoftRepeater*, c'est-à-dire en relais, lorsqu'elle détecte que son temps d'accès canal est réduit car une station opère avec un débit plus faible. Pour détecter cette anomalie de débit, la station collecte des informations à propos des stations voisines. Elle maintient une table contenant pour chaque station voisine, le nombre de trames entendues, la taille moyenne des trames, le RSSI, le débit utilisé et le BSSID auquel est connecté cette station. À partir de ces informations, la station peut calculer le temps d'occupation du canal pour chaque station voisine. Si la station détecte qu'une station voisine envoie à peu près le même nombre de trames que la station courante avec un débit plus faible, elle initie la procédure de *SoftRepeater*. Cette procédure consiste à s'annoncer via un message UDP qui est envoyé à tout le réseau IP. Ce message contient également la liste des stations pour lesquelles la station émettrice offre le service de relayage. Les clients désignés calculent l'intérêt de passer par ce relais et lui renvoie un message contenant une estimation du débit qu'ils pourraient avoir avec le relais (estimé à partir du RSSI du relais). Le relais re-calcule alors l'utilité de son service et renvoie une nouvelle offre avec la liste des stations qu'il souhaite servir. À la réception de la seconde requête, les stations peuvent décider de joindre ou non le relais. Lorsque le relais reçoit la confirmation qu'une ou plusieurs station vont l'utiliser, il démarre un AP local. Les autres stations se déconnectent de l'AP et rejoignent celui du relais. Leurs expérimentations montre que la coopération entre les stations augmente non seulement le débit de la cellule de $200\%$ sans nécessiter de changements au standard IEEE 802.11, mais améliore également la stabilité des liens TCP. Cette approche a l'avantage de ne pas modifier la MAC et peut donc fonctionner dans n'importe quelle cellule 802.11. Cependant le temps de négocia-

tion est couteux et nécessite 4 échanges de messages plus le temps nécessaire au démarrage du *SoftRepeater*.

## 2.7 Conclusion

La technologie sans-fil est un support de communication flexible, à bas coût et offrant une aire de mobilité pour les appareils connectés. Nous avons d'ailleurs montré à travers le projet Wi2Me que ces atouts ont amenés à une très grande présence des réseaux IEEE 802.11 dans un environnement urbain et à la création de réseaux communautaires. L'omniprésence de ces réseaux communautaires rend possible la création d'un réseaux d'accès à haut débit, alternatif aux grands réseaux à infrastructure tel que l'UMTS. Cependant, la nature aléatoire, diffuse et évanescente du sans-fil peut provoquer des interférences et une forte atténuation du signal, créant ainsi des pertes sur le lien.

Le standard IEEE 802.11 gère ces caractéristiques en permettant aux stations de retransmettre leurs données si elles n'ont pas été acquittées par la destination, ou en faisant varier le mode de transmission à un débit plus faible pour le rendre plus robuste face aux interférences. Si la décision de retransmettre une trame est aisée, celle de changer de mode de transmission n'est pas trivial et nécessite des algorithmes évolués, à la fois pour choisir le meilleur débit mais également pour être réactif face aux changements de condition de l'environnement. Dans un premier temps, nous avons implémenté un modèle de canal pour la technologie OFDM réalisé dans le simulateur NS-2, que nous avons ensuite validé en simulation. Ce modèle nous a également permis d'implémenter un support d'adaptation de débit optimiste dans NS-2 qui n'existait pas précédemment.

Étant donné une station connectée à un AP, retransmettre des données ou décider de changer le mode de transmission permet de réduire les pertes avec l'AP mais réduit également les performances de la cellule entière. Les trames mettant plus de temps à être transmises, le temps de canal disponible diminue, réduisant de fait les performances de toutes les stations environnantes. Une première méthode pour réduire l'impact de ces contre-mesures est de modifier la MAC pour la rendre plus équitable en terme d'occupation du canal. Cette méthode permet d'améliorer les performances des stations environnantes mais n'améliore certainement pas le cas d'une station ayant eu recourt à ces contre-mesures. Bien au contraire, elles sont d'autant plus pénalisées de partager un temps de canal équitable en transmettant à une vitesse inférieure ou en devant faire des retransmissions. Une deuxième ap-

proche est de tirer profit des stations environnantes en les utilisant comme relais, cela permet de conserver un débit élevé et donc de réduire le temps d'occupation du canal.

Dans le chapitre 3 nous étudierons les mécanismes utilisés dans les réseaux sans-fil multi-sauts. Nous proposerons ensuite une nouvelles méthode pour les réseaux type 802.11 dans le chapitre 4.

CHAPITRE 3

# Les réseaux sans-fil multi-sauts

## Sommaire



## 3.1 Introduction

En même temps que ce sont développées les technologies sans-fil, les progrès de miniaturisation des composants électroniques ont rendu possible le développement de l'informatique embarquée. De nos jours, les appareils électroniques mobiles possèdent tous une ou plusieurs interfaces sans-fil comme le WiFi ou le Bluetooth. Ces appareils mobiles sont très répandus en particulier grâce au succès de l'Internet et à la démocratisation des *smartphones*. La proximité des ces appareils les uns avec les autres crée avec la technologie sans-fil un tissu de réseaux invisibles sur lequel la

communication serait possible, sans nécessairement passer par une infrastructure fixe. La mobilité, les déconnexions ou les contraintes d'énergies sont autant de caractéristiques rendant difficile voire impossible la transposition des protocoles de l'Internet. Ces réseaux ont ainsi amené de nouveaux paradigmes de communication ouvrant vers de nombreux sujets de recherche et vers de nouvelles applications. Les réseaux sans-fil multi-sauts sont ainsi nés de ces évolutions et opèrent sur ces réseaux dépourvus d'infrastructure fixe. La portée des stations étant limitée, le paradigme de communication de ces réseaux fonctionne sur un principe de coopération entre les nœuds. Chaque nœud du réseau peut ainsi être sollicité pour relayer des trames entre différents nœuds qui ne seraient pas atteignables autrement. Ainsi, de nouveaux protocoles ont été inventés pour organiser automatiquement le réseau de façon à rendre possible la communication entre les nœuds.

Les protocoles de routage servent une fonction essentielle dans ces réseaux car ils rendent possible la communication entre les nœuds. Les protocoles de routage servent deux fonctions que sont premièrement la construction des routes et deuxièmement la propagation des données le long de ces routes. En se basant sur une infrastructure qui n'est portée que par des appareils mobiles et sans-fil, la topologie de ces réseaux est très dynamique et peut fortement varier, même à des échelles de temps très petites (comme nous l'avons montré à la section 2.2.2). Cette dynamicité très forte entre les liens de ces réseaux multi-sauts provoque des fluctuations dans le voisinage des nœuds pouvant perturber voir couper la communication si les protocoles ne s'adaptent pas suffisamment vite à ces changements.

L'approche de la communauté scientifique sur ce type de réseau a beaucoup évolué et la littérature est très importante sur le sujet. Dans ce chapitre, nous allons étudier les différentes stratégies et évolutions qui ont eu lieu dans ce domaine depuis environ 30 ans que la communauté scientifique s'y intéresse. Dans un premier temps nous ferons une analyse de l'évolution des besoins et des tendances actuels concernant les recherches dans ce domaine. Après une étude fine des différentes stratégies existantes dans le domaine, nous proposerons une classification de ces protocoles sous l'angle de l'adaptation aux conditions du canal dans le processus de relayage.

## 3.2 Évolution des réseaux sans-fil multi-sauts et standardisation

### 3.2.1 Des réseaux MANETs...

Initialement, les réseaux sans-fil multi-sauts ont été conçus pour répondre à des applications militaires. En 1983, le DARPA a financé un projet appelé SURvivable rAdio Network (SURAN) [Bey90] (Survivable Radio Network) visant à développer des réseaux sans-fil auto-configurés et multi-sauts pour être déployés sur les champs de bataille. Dans ce type de réseau dépourvu d'infrastructure fixe, le routage doit être effectué par les stations elles-mêmes puisque la portée de chaque station est limitée à quelques dizaines de mètres. Les contraintes matérielles de l'époque ont cependant empêché les scientifiques d'aboutir à des systèmes réellement performants. Avec le développement des ordinateurs portables et des Personal Digital Assistant (PDA) (Personnal Digital Assistant) au milieu des années 90, la communauté scientifique s'est intéressée à construire et à tester ce type de réseaux. Un des premiers groupe de travail à standardiser des protocoles pour ce type de réseau fut l'internet Engineering Task Force (IETF) via le groupe de travail Mobile Ad hoc NETwork (MANET) (Mobile *ad hoc* NETwork). Ce groupe a contribué à l'élaboration de plusieurs protocoles comme OLSR [CJA+03], AODV [DBRP03], ou encore DSR [JMB+01] qui sont devenus des RFC ainsi qu'à de nombreux autres drafts tels que LANMAR [PGH00] ou TORA [PC97]. De très nombreux protocoles ont depuis été développés par la communauté scientifique. Bien que standardisés, voire même pour certains implémentés, ces protocoles ne sont pas beaucoup utilisés dans l'industrie et leur usage reste limité à des activités militaires ou associatives.

D'un point de vue opérationnel, ces réseaux se sont principalement développés via des structures associatives dans des régions où les infrastructures de télécommunication étaient absentes. De nombreuses associations à travers le monde déploient des réseaux mesh, certains pour être reliés à l'Internet ou pour constituer un réseau communautaire plus ou moins étendu. Ces réseaux sont pour des pays en voie de développement une vraie solution face à l'absence d'infrastructure de télécommunication. À ce titre nous pouvons citer le projet Village Telco (VT) [AGS11] qui vise à fournir aux régions reculées du monde un réseau téléphonique local à bas coût en se basant sur la technologie 802.11. VT procède en déployant dans un village donné des équipements sans-fil afin de former des liens point à point. Le protocole BATMAN [NALW08], issue des recherches sur les MANETs, permet de maintenir le réseau mesh et fournit une connectivité IP à tout le village. Les services sont ensuite

ajoutés au-dessus de la couche IP tel que SIP pour la voix sur IP, qui fournit donc le service téléphonique. Les nœuds étant majoritairement fixes et le réseau cœur essentiellement constitué de liens sans-fil point à point, on parle de réseau *mesh* plutôt que MANETs car la prise en compte de la mobilité n'est plus une caractéristique de l'ensemble des nœuds de l'architecture. Un réseau *mesh* désigne généralement un réseau sans-fil multi-sauts qui possède une partie fixe (telle que des points d'accès IEEE 802.11) et une partie mobile, celle-ci étant des clients de l'architecture. Les clients se connectent aux points d'accès comme dans un réseau à infrastructure, et un protocole de routage doit être implémenté dans le cœur du réseau sans-fil, entre les points d'accès. Akyildiz et al [AWW05] proposent une analyse détaillée des problématiques liées aux réseaux *mesh*.

Ces dernières années ont vu apparaître un certain nombre de projets mettant en place des réseaux sans-fil mesh communautaires, c'est-à-dire opérés par une communauté de volontaires plutôt que par une entreprise. Le mode de fonctionnement décentralisé des réseaux mesh se prête particulièrement bien à ce type d'initiative. En Europe on peut citer le réseau sans-fil communautaire espagnol Guifi [CA12] qui à ce jour est constitué de plus de 20 000 nœuds formant environ 40 000 kilomètres de liens sans-fil. En Allemagne le groupe Freifunk [JMS+07] est un groupe de passionnés qui participe activement au développement et à la promotion des réseaux mesh. Ils fournissent des firmwares pour les routeurs sans-fil linksys permettant à n'importe qui de déployer facilement un réseau mesh. Enfin, de nombreuses autres associations font la promotion des réseaux mesh comme étant une alternative libre et neutre face à un Internet de plus en plus centralisé et contrôlé.

D'un point de vue industriel, les recherches sur les MANETs connaissent un nouvel essor à travers les Vehicular Ad hoc NETwork (VANETs), qui constituent un cas d'usage prometteur pour les Intelligent Transport Service (ITS). Les réseaux VANETs sont une sous-classe des réseaux MANETs dans lesquels les terminaux mobiles sont essentiellement des véhicules (typiquement des voitures ou des bus). Le but des réseaux ITS est de fournir de nouveaux services innovants liés aux modes de transport et à la gestion du trafic. Par exemple, les ITS pourraient participer à augmenter la sécurité routière en informant les véhicules des conditions de la route en avance et en temps réel. Les VANETs constituent ainsi une solution potentielle crédible pour atteindre ces objectifs. Les VANETs décrivent trois modes de communication possibles, le Vehicule-to-Vehicule (V2V), le Véhicule-to-Roadside (V2R) et le Vehicule-to-Infrastructure (V2I). Le V2V relève directement des problématiques issue des MANETs puisqu'il s'agit d'une communication *ad hoc* entre véhicules mobiles. Le V2R et le V2I relèvent plutôt des problématiques d'association et de han-

dover auprès des bornes d'accès sans-fil situées sur les bords de la route. En 2007, le consortium CAR-2-CAR a écrit un manifeste [C+07] résumant les principales avancées dans les VANETs et poussant à l'écriture d'un standard industriel basé sur la norme IEEE 802.11p.

Les réseaux MANETs (ou mesh) ont généré de nombreux efforts de la communauté scientifique durant plus de vingt ans, et ont toujours une place importante dans la recherche contemporaine sur les réseaux. Initialement motivé et financé par des objectifs militaires, ce type de réseau de communications a reçu un écho tout à fait positif de la part des associations et des collectivités qui y voient une alternative à bas coût aux réseaux à infrastructure filaire. Par contre, ils n'ont reçu que peu d'intérêt de la part des industriels, de par les difficultés de mise en œuvre des aspects dynamiques de ce type de réseau (comme la gestion de la mobilité, ou de l'auto-configuration). Les ITS semblent toutefois être le cas d'usage le plus crédible aujourd'hui pour un développement industriel des MANETs.

### 3.2.2 ... aux réseaux de capteurs

Plus récemment on a vu apparaître un nouveau paradigme de communication dans l'Internet avec la notion d'Internet des objets et de réseau de capteurs [WMRD11]. Jusqu'à présent, l'information présente sur Internet est créée et exploitée majoritairement par les humains. Les progrès de la miniaturisation des composants et des technologies de la télécommunication rend possible l'interconnexion des *objets* avec l'Internet. Dans l'Internet des objets, l'information serait créée et manipulée par les objets eux-même. Un objet connecté serait capable de faire remonter de l'information pour alimenter des bases de données accessibles sur l'Internet. Ces objets pourraient également communiquer entre eux directement pour remplir des tâches, cela s'appelle le Machine to Machine (M2M). Contrairement aux réseaux MANET, le besoin provient dorénavant des industriels qui cherchent à automatiser des tâches sans intervention humaine, proposer des solutions automatisées pour le domicile, exploiter ces données pour proposer de nouveaux services innovants. Cette vision a changé la façon de percevoir les réseaux *ad hoc* en ne cherchant non plus un moyen d'établir la communication entre chaque paire de nœuds, mais en cherchant à organiser le réseau pour le connecter à l'Internet. Ainsi, les réseaux de capteurs diffèrent principalement des réseaux MANET dans les modèles de trafics que doivent supporter les protocoles. Malgré de grandes similarités avec les réseaux MANET, ces différences en termes de trafic et d'applicabilité ont motivé la création de nouveaux protocoles, plus adaptés à ces besoins.

Un des premiers cas d'usage ayant popularisé le terme d'Internet des objets est la maison connectée ou Wireless Home Ad hoc Network (WHAN). Un WHAN permet de contrôler et de gérer automatiquement une maison ou un bâtiment. Cela peut aller d'une lumière commandée par un capteur de présence jusqu'au contrôle et la gestion de la consommation des appareils électroménagers. Certains industriels ont développé des solutions propriétaires pour répondre à ces besoins telles que ZigBee [All06], Z-Wave [Gal06], Wavenis [wav01] ou Insteon [Dar05]. Wavenis a tenté de s'imposer en standard en 2008 en créant la Wavenis Open Standard Alliance.

En même temps que les industriels développent leurs solutions, la communauté scientifique au sein de l'IETF a travaillé sur l'élaboration de standards ouverts basés sur IP. Là où les humains représentent déjà une limite importante au développement d'Internet à cause de l'épuisement des ressources en IPv4, l'introduction des objets dans l'Internet est un réel défi en terme de passage à l'échelle de l'Internet. Le choix a alors été fait de développer de nouveaux standards directement autour d'IPv6, qui devient ainsi la brique de communication commune des objets connectés. En plus d'être la nouvelle version du protocole Internet qui est actuellement déployée, IPv6 permet d'adresser un nombre d'équipements qu'on estime aujourd'hui presque infini. L'objectif est alors d'adapter le protocole de base pour obtenir une implémentation compatible à l'IPv6 sur les supports de communications utilisés par les réseaux de capteurs, en prenant en compte les fortes contraintes des équipements. Cette approche a donné naissance aux groupes de travail ROLL, 6LowPan et CORE de l'IETF.

Le groupe Routing Over Low power and Lossy links (ROLL) a travaillé à l'élaboration de l'algorithme de routage IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) [Win12] pour les réseaux de capteurs (voir section 3.3.1.1.3). Ce protocole permet différents modèles de communication, dont la remontée d'informations depuis les capteurs vers des puits de données. Dans RPL, chaque capteur doit agir comme un routeur pour participer au routage des capteurs les plus lointain, vers la(les) racine(s) du réseau. RPL sera décrit un peu plus en détail dans la section 3.3.1.1.3.

Le groupe IPv6 over Low power Wireless Personal Area (6LowPan) adapte IPv6 pour les réseaux de capteurs, en prenant en compte les contraintes de puissance et de durée de vie qui sont cruciales dans cet environnement. Les missions de 6LowPan sont de proposer un ensemble de protocoles et d'algorithmes pour faire fonctionner les protocoles de l'Internet (IPv6) dans des objets très petits afin de pouvoir les faire participer à l'Internet des objets. Ce groupe de travail a ainsi créé le RFC

6282 [HT11] décrivant des mécanismes de compression d'entêtes IPv6 pouvant être supporté par des réseaux sans-fil à faible capacité de transport.

Le groupe Constrained RESTful Environments (CORE) a élaboré le protocole Constrained Application Protocol (CoAP), inspiré du protocole HTTP. Une fois que ces petits équipements sont accessibles depuis l'Internet grâce à RPL et 6LowPan, CoAP fournit un moyen de communiquer avec eux. Il a été conçu pour être facilement traduit en HTTP afin d'offrir une intégration aisée avec le web traditionnel. Des proxys permettent ainsi de fournir un accès à des ressources en CoAP depuis HTTP.

Ces trois protocoles forment ensemble des briques fondamentales au fonctionnement de l'Internet des objets. Bien que fortement inspirés des réseaux MANET, les réseaux de capteurs répondent principalement à un besoin industriel et la communauté scientifique s'est réorganisée afin de fournir des solutions adaptées à ces nouveaux défis.

### 3.2.3 Les réseaux DTN

Les réseaux Delay Tolerant Network (DTN) sont une classe de réseaux sans-fil multi-sauts très différente de ce qui a été décrit jusqu'à présent. Financé par la NASA au sein du Jet Propulsion Laboratory (JPL) , le projet InterPlanetary Networking (IPN) a posé en 1998 les premiers principes fondateurs des réseaux DTN sous la direction de Vint Cerf [BCD+02]. Ces recherches ont initialement été conduites pour répondre aux contraintes de la communication interplanétaire dans le contexte de l'exploration de Mars. Étant donné les très grandes distances séparant les planètes, les communications souffrent de délais importants. Par exemple, le temps d'aller-retour d'une communication entre la Terre et Mars varie entre 13 et 40 minutes. Si la pile TCP/IP fonctionne très bien sur Terre, et fonctionnerait sûrement bien sur Mars, elle n'est pas du tout adaptée aux délais imposés par la communication entre la Terre et Mars. De plus, certaines connexions sont régulièrement interrompues à cause des mouvements orbitaux. Par exemple, lorsqu'un satellite de télécommunication passe derrière une planète, il faut attendre qu'il revienne de l'autre côté avant de pouvoir rétablir la communication. Afin d'interconnecter la Terre avec Mars, il a fallu concevoir de nouveaux protocoles pouvant répondre aux contraintes de variabilité des délais et d'interruption des liens. Puisqu'à un instant donné aucun chemin de bout en bout n'existe entre deux nœuds, l'approche d'IPN est de conserver les données entre chaque saut le temps que la communication avec le prochain saut s'établisse. Le robot martien Spirit Rover (2004) conservait ainsi ses données en mémoire et les

envoyait à un satellite via un lien UHF ( 8 GHz) lorsque celui-ci était atteignable. Le satellite conservait également les données le temps d'orbiter autour de Mars puis les renvoyait sur Terre via le Deep Space Network (DSN). Cette façon de conserver les données en mémoire puis de les renvoyer lorsqu'une opportunité se présente est un nouveau paradigme de communication appelé le *Store, Carry and Forward*. En procédant ainsi, IPN s'affranchit des contraintes de délai et d'interruption et tire profit des opportunités de transmission plutôt que de construire et de maintenir un chemin de bout en bout.

En 2003, Kevin Fall [Fal03] reprend les principes d'IPN et impose le terme de DTN pour désigner des réseaux de communication tolérants aux délais et aux interruptions de service. Il voit dans cette architecture un moyen d'interconnecter des réseaux de natures différentes, c'est-à-dire fonctionnant avec des technologies et des caractéristiques différentes. À l'inverse de la tendance qui est d'unifier tous les réseaux avec IP, l'approche DTN est de définir des passerelles basées sur le paradigme du *Store, Carry and Forward* pour interconnecter ces réseaux. La figure 3.1 issue du papier [Fal03] donne un exemple d'architecture d'un réseau DTN. Sur cette figure, les différentes régions sont interconnectées via des *gateways DTN* faisant abstraction de la technologie utilisée dans chaque région. Le groupe de travail DTNRG (DTN Research Group) a depuis écrit plusieurs RFC telles que la RFC 4838 [CBH+07] qui décrit l'architecture des DTN, ou la RFC 5050 [SB07] qui spécifie le protocole de communication.

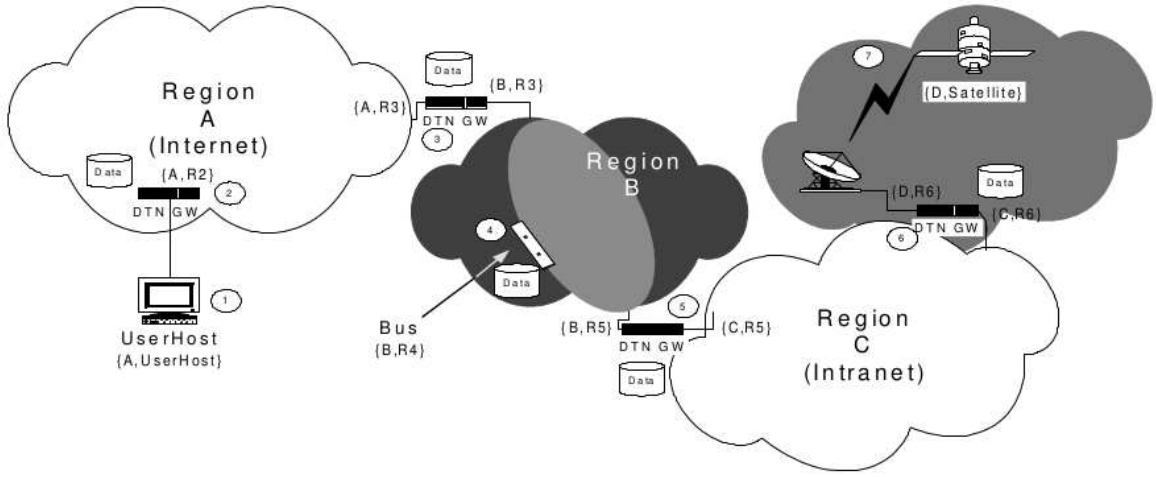



Figure 3.1 – Exemple d'une architecture DTN interconnectant quatre régions de natures différentes (figure empruntée à [Fal03])

De nombreux travaux ont depuis été effectués, basés sur les DTN eux-mêmes mais aussi en appliquant certains des concepts DTN aux MANETs et aux réseaux

de capteurs. En faisant tomber l'hypothèse d'existence d'un chemin de bout en bout dans les réseaux MANETs, l'approche DTN permet de s'affranchir des problèmes liés à la mobilité. La mobilité n'est alors plus vue comme une contrainte, mais comme une façon de rendre possible la communication entre des îlots déconnectés. Le terme de **routage opportuniste** a fait son apparition pour désigner un routage basé sur le principe du *Store, Carry and Forward* dans lequel le prochain saut de routage n'est pas connu à l'avance. Le routage opportuniste désigne donc le fait de tirer profit d'une opportunité de transmission pour router une trame. Il faut donc définir de nouvelles métriques permettant de prendre la décision de relayer une trame étant donnée une rencontre entre deux nœuds. Chiara Boldrini [BCJP07] ou Elizabeth Daly [DH07] exploitent ce principe pour router des trames dans un réseau MANET déconnecté. De la même façon, Tuomo Hyyryläinen [HKL+07] décrit un système où n'importe quel équipement mobile peut alors servir de *facteur* en relayant et distribuant des messages destinés à autrui de façon opportuniste, au gré des rencontres avec les autres équipements. Les réseaux DTN ont également reçu de l'intérêt pour une utilisation dans les réseaux de capteurs. L'agrégation des données pourraient être effectuée en utilisant un nœud DTN mobile appelé *mule* [HF04]. Ces *mules* se déplacent dans le réseau de capteurs, récupérant les données en passant à proximité des capteurs et les stockent jusqu'au retour à la base où elles peuvent les transférer jusqu'à un serveur central.

### 3.2.4 Conclusion

Les réseaux MANET ont initialement été étudiés par le monde académique pour des applications militaires (communication entre les unités sur le champs de bataille) et humanitaires (élaboration de réseaux alternatifs en cas de destruction ou d'absence d'infrastructure). Ces réseaux ont reçu énormément d'intérêt de la part de la communauté scientifique et ont abouti à l'élaboration de plusieurs dizaines de protocoles de routage. Les ITS semblent être un cas d'usage très prometteur pour le développement de ce type de réseau. Plus récemment, les réseaux de capteurs sont apparus avec les progrès de la miniaturisation de l'électronique et la diminution des coûts de production. Ces progrès ont permis d'imaginer de nouveaux scénarios et ces réseaux sont au cœur de l'engouement académique et industriel lié à l'Internet des objets.

Les protocoles de routage dans les réseaux sans-fil multi-sauts constituent ainsi un défi majeur pour le développement de ces nouveaux modes de communications et de ces nouveaux services. Dans la prochaine section, nous allons étudier les dif-

férentes stratégies élaborées par ces protocoles de routage dans un environnement non déconnecté.

## 3.3 Protocoles de routage pour les réseaux sans-fil multi-sauts

Les protocoles de routage servent deux fonctions. La première est la construction et la maintenance des routes pour certaines destinations. La deuxième consiste en l'acheminement des données le long de ces routes. La littérature sur les protocoles de routage dans les réseaux sans-fil multi-sauts est très importante et il serait impossible d'être exhaustif ici. Le plus grand défi des protocoles de routage est de trouver à un instant donné le meilleur chemin entre deux stations, c'est-à-dire la suite de nœuds pouvant acheminer les données le plus efficacement possible. Cependant, la mobilité et la variabilité du canal sans-fil étant ce qu'elle est (cf section 2.2), ces routes peuvent changer à tout moment et la difficulté est donc de s'adapter à ces changements afin de maintenir la communication, d'une part, mais de conserver un routage efficace d'autre part.

Nous distinguons ainsi trois principales approches liées à la façon de s'adapter à ces changements (cf 3.2) ; dans la première approche (routage traditionnel), le routage est effectué le long d'une route dont le calcul précède la transmission des données. Dans la deuxième approche (routage adaptatif), chaque saut de routage est déterminé en se basant sur les conditions quasi-instantanées du canal, la sélection du relais précède la transmission. Dans la troisième approche (routage opportuniste), les données sont transmise et la sélection du relais se fait à posteriori. Dans la figure 3.2, les protocoles sont représentés par des cercles et chaque flèche indique une nouvelle innovation (et donc une nouvelle famille). Par exemple, dans le routage traditionnel, on remarque qu'OLSR [CJA+03] appartient à la famille des protocoles pro-actifs . Les protocoles CGSR [CWLG97], HSR [PGHC99] et LANMAR [PGH00] sont également des protocoles pro-actifs mais ont un mode de fonctionnement hiérarchiques qui les distinguent des autres protocoles pro-actifs. Les flèches en pointillés indiquent une similitude de fonctionnement sans être toutefois une extension de la famille. Par exemple, les protocoles RBF [ALRS09b][ALRS09a] et SIF [CDV05] sont des protocoles de la famille de routage adaptatif et ont des similitudes dans leur fonctionnement avec le protocole CBF de la famille de routage opportuniste. Cependant RBF et SIF n'appartiennent pas pour autant à la famille de routage opportuniste. L'ordre vertical suit les années de publication.

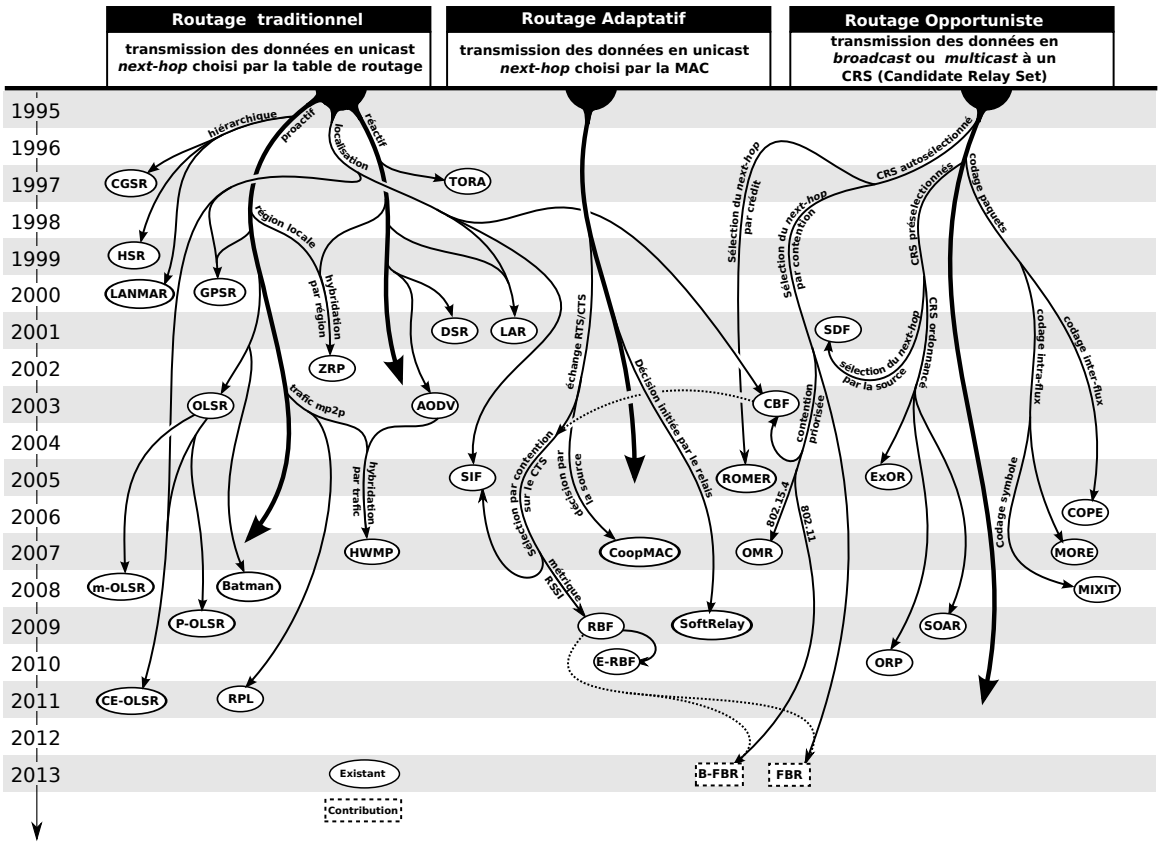



Figure 3.2 – Protocoles de routage pour les réseaux sans-fil multi-sauts

Nos contributions (FBR et B-FBR) sont indiquées avec un rectangle pointillé, on remarque qu'elles s'inscrivent dans la famille du routage opportuniste (nous détaillerons par la suite les différentes sous-familles) et offre des similitudes dans leur fonctionnement avec RBF.

### 3.3.1 Protocoles de routage traditionnels

Les protocoles de routage traditionnels construisent les routes avant de transmettre les données. Pour être opérationnel, un protocole de routage fonctionne en disséminant l'information de routage à travers le réseau. On distingue deux grandes sous-familles de protocoles liés à la façon dont l'information de routage est disséminée : les protocoles de routage **pro-actifs** et **réactifs**. Les protocoles de routage pro-actifs fonctionnent en disséminant périodiquement l'information de routage de façon à construire et maintenir les routes quel que soit le besoin. Les protocoles de routage réactifs fonctionnent à la demande en construisant les routes uniquement lorsqu'elles sont nécessaires. Nous présenterons également deux protocoles hybrides

qui proposent une approche mixte avec des mécanismes à la fois pro-actifs et réactifs.

#### 3.3.1.1 Protocoles de routage pro-actifs

Les protocoles de routage pro-actifs fonctionnent sur le principe que chaque nœud doit connaître une route vers n'importe quelle destination du réseau à tout instant. Un protocole de routage pro-actif désigne donc le fait de calculer les routes *avant* qu'il n'y en ait besoin. De cette façon, un nœud peut transmettre des données vers une destination après une simple consultation de sa table de routage et sans délai supplémentaire. Pour maintenir cette table de routage avec des informations valides, ces protocoles requièrent des mises à jour périodiques et permanentes, matérialisées par des messages envoyés par les nœuds du réseau. La fréquence d'émission doit être suffisamment importante pour prendre rapidement en compte les modifications de la topologie du réseau, mais suffisamment faible pour ne pas surcharger le réseau par ces messages de contrôle.

La topologie du réseau étant liée à la position des terminaux, une forte mobilité rend la topologie très dynamique. Face à une mobilité importante, les routes changent constamment et la diffusion des informations de routage peuvent fortement impacter les performances du réseau, voire empêcher de construire correctement les routes. Broch et al. [BMJ+98] montrent que les protocoles de routage pro-actifs fonctionnent bien tant que la mobilité est faible mais qu'ils ne convergent plus lorsque celle-ci devient trop importante.

Dans la suite de cette section nous allons décrire rapidement les protocoles pro-actifs OLSR, BATMAN et RPL. OLSR est un protocole de référence, possède de nombreuses implémentations (réelles et dans des simulateurs) et a fait l'objet d'un nombre important de contributions scientifiques (environ 1000 papiers avec le mot OLSR dans le titre entre 2003 et 2013). BATMAN présente quelques innovations intéressantes qui méritent d'être soulignées. RPL un protocole de routage ayant de fortes chances d'être massivement adopté pour les réseaux de capteurs.

**3.3.1.1.1 Optimized Link State Routing (OLSR)** [CJA+03] est un algorithme pro-actif à état de lien, standardisé par l'IETF en 2003 sous la RFC 3626[CJA+03]. Dans les algorithmes à état de lien, chaque station maintient une base de données décrivant la topologie entière du réseau et construit à partir de celle-ci un arbre des plus courts chemins vers toutes les destinations, dont il est la racine (avec l'algorithme dijkstra). Pour construire une vue complète du réseau, chaque station doit

découvrir ses voisins et ensuite diffuser cette information de voisinage à l'ensemble du réseau. Afin d'éviter de surcharger le réseau avec ces informations, OLSR tire profit de la nature diffuse du sans-fil pour optimiser cette diffusion.

Chaque station commence d'abord par s'annoncer auprès de son voisinage à l'aide des message *HELLO*, qui sont envoyés en diffusion (mais qui ne sont pas relayés). Lorsqu'une station reçoit un message *HELLO*, elle met à jour sa table de voisinage en y ajoutant l'émetteur du message s'il n'y est pas déjà. Ces messages *HELLO* sont envoyés périodiquement et contiennent également la liste des voisins immédiats de l'émetteur du message. Ces messages sont donc susceptibles d'évoluer entre deux transmissions du fait que chaque station apprend au fur et à mesure son propre voisinage à un saut. Après un certain temps de convergence, en connaissant ses voisins ainsi que les voisins de ses voisins (inclus dans les messages *HELLO*), chaque station peut alors construire la topologie du réseau à deux sauts.

La deuxième étape consiste à propager la table de voisinage à l'ensemble du réseau. Pour cela des messages *TC* sont diffusés et relayés par les voisins de proche en proche à l'ensemble du réseau. Afin d'optimiser l'inondation et d'éviter qu'une station ne reçoive trop de fois le même message *TC* (via deux routes différentes), chaque station va sélectionner un sous-ensemble de ses voisins qui seront les seuls responsables de relayer ses messages *TC*. Le calcul de ces voisins appelés Multi-Point Relay (MPR) est effectué de telle sorte que l'ensemble des voisins à deux sauts soit atteignable. Ce sous-ensemble est construit en choisissant successivement le voisin ayant le plus fort degré (nombre de voisins) et l'ajoute au sous-ensemble MPR, jusqu'à ce que tous les voisins à deux sauts soient atteignables. Chaque message *TC* est ensuite envoyé aux MPR et relayés par ces derniers de la même façon, jusqu'à ce que l'ensemble du réseau (et pas seulement les voisins à deux sauts) en ait connaissance.

Chaque station OLSR calcule ensuite localement le meilleur chemin pour chaque destination du réseau. Le moindre changement de topologie (une déconnexion entre deux nœuds) implique de réitérer le processus d'inondation et de recalculer les chemins sur l'ensemble des nœuds du réseau. Le protocole OLSR possède une implémentation stable dans le noyau Linux et est disponible par défaut dans le firmware fourni par Freifunk. Cette communauté (Freifunk) basée à Berlin a pu procéder à un certain nombre de tests réels et ont obtenu une certaine expérience liée au comportement de OLSR. Lorsque le réseau dépasse 300 nœuds, les opérateurs se sont rendus compte que OLSR provoquait un certain nombre de comportements problématiques dans un réseau pourtant fixe, comme des routes qui apparaissent et disparaissent,

des boucles de routages et des déconnexions. Ils ont par ailleurs développé un nouveau protocole baptisé BATMAN en réponse aux problèmes rencontrés avec OLSR.

**3.3.1.1.2 Better Approach To Mobile Ad hoc Networking (BATMAN)** [NALW08] est un protocole développé par Freifunk en réponse aux faiblesses de OLSR. C'est un protocole de routage pro-actif car il construit et maintient les tables quel que soit le trafic sur le réseau. Il a cependant un certain nombre de caractéristiques qui le rendent unique dans sa façon de fonctionner. Il est fondamentalement différent des algorithmes à état de lien ou à vecteur de distance. BATMAN n'essaye pas de construire ou de calculer des tables de routage, il cherche à détecter quel voisin offre la meilleure route pour chaque destination.

Dans BATMAN, les tables de routage ne sont pas échangées directement entre les nœuds. Chaque nœud diffuse à l'ensemble du réseau un message appelé OriGinator Message (OGM), dont le contenu est similaire au *HELLO* de OLSR. Cependant, les messages OGM sont petits car ils ne comportent aucune information de voisinage et la diffusion n'est pas optimisée pour passer par des MPR. La sélection du chemin pour une certaine destination est basée sur le voisin ayant relayé le plus d'OGM pour cette destination. La métrique utilisée par BATMAN est donc basée sur le taux de perte et conceptuellement similaire à la métrique ETX (voir section 3.3.1.4). La mise à l'échelle de BATMAN est liée au taux de perte du canal. Les messages OGM étant émis périodiquement environ toutes les secondes, ce protocole n'est pas adapté dans un environnement où les liens sont de bonne qualité car il souffrirait de cette diffusion massive.

Dans le protocole originel, BATMAN se basait sur des trames UDP. BATMAN a subi une évolution notable appelée *batman-adv* afin de le transformer en protocole de routage de niveau 2 (*mesh-under*). Ceci permet à BATMAN de se déployer automatiquement sans avoir besoin d'un adressage à priori des nœuds. Le papier [MDK10] montre que *batman-adv* offre de meilleures performances que BATMAN.

**3.3.1.1.3 IPv6 Routing Protocol for Low power and Lossy Networks (RPL)** [IET12] est un protocole de routage pro-actif, standardisé à l'IETF par le groupe de travail ROLL sous la RFC 6550. RPL est destiné aux réseaux de capteurs pouvant aller jusqu'à plusieurs milliers de nœuds. RPL fait également partie de la famille des protocoles *Route-Over*, c'est-à-dire qu'il fonctionne au-dessus d'IP et plus particulièrement d'IPv6. Chaque nœud s'attribue son adresse *link-layer* IPv6, basée sur son adresse MAC. Chaque message de contrôle RPL est un message ICMPv6 particulier.

RPL fonctionne en organisant le réseau pour construire Destination Oriented Directed Acyclic Graph (DODAG) dont la racine est le puits (un nœud particulier recevant le trafic des capteurs). Un DODAG est similaire à un arbre excepté qu'un nœud peut posséder plusieurs parents comme indiqué sur la figure 3.3. Le DODAG est construit de façon à optimiser une certaine fonction objective (*objective function*) sélectionnée par le puits. Cette fonction objective indique quelle est la métrique choisie, quel critère est utilisé pour déterminer la notion de meilleure route. Une fonction objective peut être la latence, le nombre de sauts, ou l'énergie par exemple. Chaque nœud possède un rang qui détermine sa profondeur dans le DODAG, le puits a un rang de 0 et le seul a en posséder un au début. RPL fonctionne sur la base d'un graphe orienté, aussi les routes qui vont vers la racine (*upward*) ne sont pas nécessairement les mêmes que celles qui descendent vers les nœuds (*downward*).

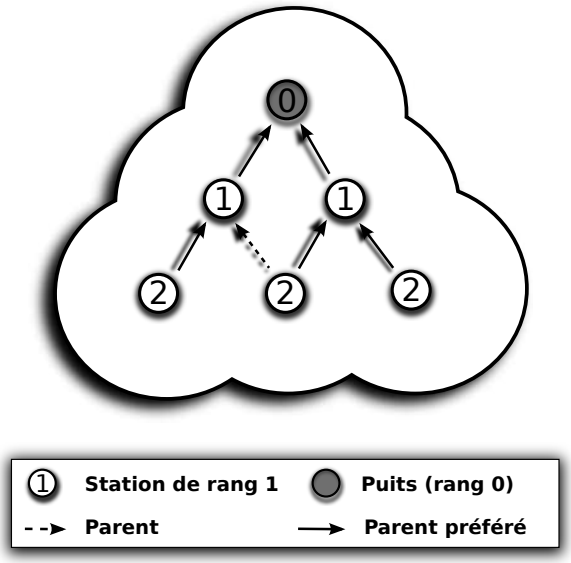



Figure 3.3 – RPL forme un DODAG dont la racine est le puits

RPL s'instancie au niveau de la racine (le puits) par l'émission de message Destination Information Object (DIO). Ces messages servent à construire et à maintenir les routes qui vont des nœuds vers la racine (*upward route*). Les DIO contiennent des informations telles que l'identité du DODAG, le rang de l'émetteur du DIO, le numéro de version du DODAG (*DODAGversionNumber*). Chaque station écoute les DIO provenant de ses voisins avant de rejoindre le DODAG. Il peut également forcer l'émission de DIO en envoyant un Destination Information Sollicitation (DIS). Il choisit ensuite un ensemble de parent parmi ses voisins en fonction du rang qu'ils communiquent et calcule finalement son propre rang (qui est nécessairement plus élevé que celui de ses parents). Une fois qu'une station a rejoint le DODAG et calculé son rang, il peut lui-même diffuser des DIO à son voisinage. De cette façon, la

construction du DODAG commence par la racine qui diffuse les premiers DIO, et se propage jusqu'à ce que tous les nœuds aient rejoint le DODAG. Même si un nœud maintient plusieurs parents, il n'en choisit qu'un seul pour envoyer ses messages à la racine. Les autres servent à basculer le trafic si la connexion avec le meilleur disparaît. La racine peut ordonner une reconstruction complète du DODAG en incrémentant le numéro de version du DODAG, cette opération est appelé le *DAG repair*. Les messages DAO servent à construire les routes allant de la racine vers les nœuds (*downward route*) et sont émis par les nœuds ayant rejoint le DODAG. Chaque fois qu'un nœud rejoint le DODAG, il émet un message DAO à destination de ses parents. À la réception du DAO, les parents vont créer la route inverse vers leur fils et le DAO va être propagé jusqu'à la racine. L'émission de DAO est également régie par un *timer* et par des événements comme la reconstruction du DODAG. RPL supporte trois modes de communication :

- *multipoint-to-point*, le trafic des nœuds vers la racine. Ce trafic suit les routes construites grâce aux messages DIO.
- *point-to-multipoint*, trafic depuis la racine vers les nœuds. Ce trafic suit les routes construites grâce aux messages DAO.
- *point-to-point*, le trafic d'un nœud vers un autre. S'ils ne sont pas directement à proximité, le trafic est routé jusqu'au premier nœud parent qu'ils ont en commun.

#### 3.3.1.2 Protocoles de routage réactifs

Les protocoles réactifs fonctionnent en construisant les routes à la demande et ne les maintiennent que si elles sont utilisées. L'avantage par rapport à une approche pro-active est qu'il n'y a pas besoin de maintenir de route lorsqu'il n'y a pas ou peu de trafic, cela permet d'être moins gourmand en ressources. Cependant, puisque la route n'existe pas avant d'être utilisée, un moment de latence est introduit avant que la route ne soit construite.

**3.3.1.2.1 Ad hoc On demand Distant Vector (AODV)** [DBRP03] est un protocole standardisé par l'IETF en 2003 par la RFC 3561. Ce protocole a suscité de très nombreuses contributions et modifications. Nous décrivons ici le fonctionnement de base de AODV.

Lorsqu'une station source souhaite envoyer des données à une destination, elle doit d'abord commencer par entamer une procédure de découverte de route. Celle-ci consiste à diffuser à tout le réseau un message Route Request (RREQ) propagé de proche en proche par tous les nœuds du réseau. Le message RREQ comporte dans son entête le nombre de sauts effectués depuis la source. Chaque nœud participant à la propagation de ce message met à jour sa table de routage vers la source et propage la requête en incrémentant le champ "hop count" de l'entête du message. Si la destination est accessible, le message finit par y arriver, éventuellement par plusieurs chemins. La destination répond à la requête avec un message Route Reply (RREP) à destination de la source. La figure 3.4 décrit un exemple de ce processus de découverte de chemin. Le nœud $E$ reçoit une première instance de *route request* qui a fait le chemin $S - B - E$. À sa réception, le nœud $E$ ajoute une entrée vers $S$ de taille $2$ avec $B$ comme prochain saut. Lorsque la deuxième instance de *route request* arrive depuis le chemin $S - A - D - E$, le nœud $E$ jette ce message car celui-ci provient d'une route moins bonne que la première instance.

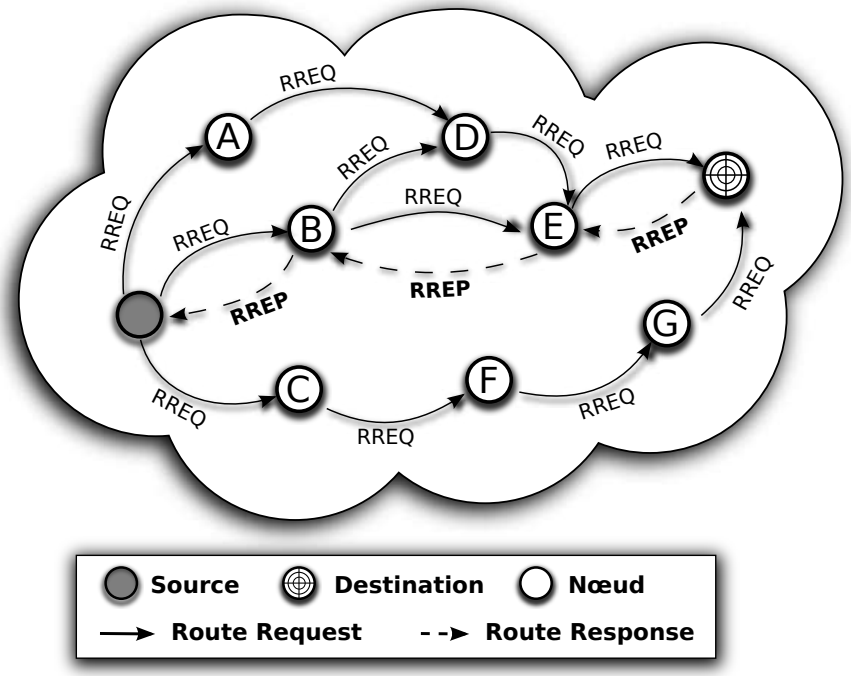



Figure 3.4 – AODV construit les routes via la diffusion d'une Route Request (RREQ) à qui la destination répond avec une Route Reply (RREP)

Tant que la route est utilisée, tous les nœuds intermédiaires doivent maintenir les informations de routage à jour. Chaque nœud intermédiaire maintient son voisinage à jour via la diffusion périodique de message *HELLO*. Si le voisinage change et impacte une des routes en cours d'utilisation, un message Route Error (RERR)

est envoyé à destination des sources impactées. Cette situation amène les sources impactées à initier une nouvelle procédure de découverte de route.

AODV possède beaucoup d'implémentations dans des simulateurs ainsi que dans des systèmes d'exploitation tel que Linux qui en offre une implémentation stable. Ces implémentations ont permis à AODV d'être testé et comparé à de nombreux autres protocoles.

**3.3.1.2.2 Dynamic Source Routing (DSR)** [JMB+01] est un protocole standardisé par l'IETF en 2007 sous la RFC 4728. Faisant partie de la famille des protocoles réactifs, il ne maintient pas une connaissance du réseau à priori. DSR fonctionne à la demande avec un premier mécanisme de **découverte de route** qui est initié suite à une requête, et un mécanisme de **maintenance de route**. il est assez similaire à AODV dans son mode de fonctionnement (routes construites à la demande) mais ne fait pas l'hypothèse que les liens sont symétriques.

Comme AODV, la procédure de découverte de route se fait via l'émission d'une Route Request (RREQ). Lorsqu'une station (source) veut établir une communication avec un certain nœud et qu'aucune route n'a encore été découverte, la source crée le message RREQ contenant l'adresse du nœud source et celle du nœud destination. Ce message est diffusé à tout le réseau en étant propagé de proche en proche. Avant de propager la requête, un nœud intermédiaire ajoute son adresse afin de construire la route au fur et à mesure de sa propagation. Lorsque la requête arrive finalement à la destination, la route est contenue dans la trame : elle contient la liste des nœuds intermédiaires traversés. La destination peut alors envoyer un message Route Reply (RREP) via la route inverse découverte lors de la propagation de la requête. À cause de l'asymétrie des liens sans-fil, la destination peut choisir de démarrer une procédure de découverte de route vers la source plutôt que d'utiliser la route inverse de la requête. Par conséquent, la route de la source vers la destination et de la destination vers la source peut être différente. Lorsque la source reçoit finalement le *Route Reply*, elle peut envoyer ses données en spécifiant dans l'entête de la trame la route à prendre. C'est pour cette raison que cela s'appelle *dynamic source routing*, car la route que doit prendre la trame est explicitement décrite dans son entête.

Tous les nœuds intermédiaires ayant participé à la propagation des requêtes et des réponses mettent ces dernières en cache afin de réduire le temps de découverte d'une route pour une prochaine procédure. Chaque fois qu'une nouvelle requête ou réponse est propagée, le cache est mis à jour si nécessaire. Lorsqu'une route est cassée et que le relayage des données échoue à un des maillons, le nœud détectant la rupture du lien prévient tous les nœuds concernés avec un message Route Error

(RERR). À la réception d'un tel message, les nœuds sources peuvent procéder à une nouvelle découverte de chemin si aucun autre chemin n'est connu.

#### 3.3.1.3 Protocoles Hybrides

Les protocoles de routage hybrides permettent de tirer parti des avantages de chacune des deux approches précédentes. Les protocoles de routage pro-actifs sont plus performants pour des réseaux ayant un faible nombre de nœud et peuvent à tout moment transmettre des données à n'importe quelle destination du réseau. Les protocoles de routage réactifs passent mieux à l'échelle mais introduisent un délai pour la construction de la route. Nous présentons ici deux protocoles de routage hybrides, ZRP et HWMP, chacun ayant une approche différente de l'hybridation. ZRP utilise l'hybridation comme un moyen de fournir un compromis entre délai et passage à l'échelle tandis que HWMP va utiliser l'hybridation pour optimiser ses différents services.

**3.3.1.3.1 Zone Routing Protocol (ZRP)** [HPS02b] est un protocole hybride ayant fait l'objet d'un draft IETF en 2002 mais n'a jamais atteint le stade de RFC. Il est le premier et le plus connu des protocoles hybrides. ZRP décrit autour de chaque nœud une zone de routage dans laquelle des mécanismes pro-actifs entretiennent la connaissance locale. Des mécanismes réactifs sont utilisés pour atteindre des nœuds en dehors de la zone. L'hybridation est donc effectuée de façon à offrir un compromis entre délai et passage à l'échelle.

La zone de routage est définie par l'ensemble des nœuds accessibles en $k$ sauts. Chaque nœud maintenant sa propre zone de routage, des nœuds voisins auront une zone qui se superpose mais qui ne sera pas identique. ZRP décrit le protocole Intra-zone Routing Protocol (IARP) [HPS02a] pour construire et maintenir les routes à l'intérieur de cette zone. Il s'agit d'un protocole de routage pro-actif à état de lien, similaire à OSPF dans son fonctionnement. Chaque nœud commence par apprendre son voisinage et s'y annoncer à l'aide de message "hello" . Cette information est ensuite propagée à ses $k$ plus proches voisins via des messages Neighbor Discovery Protocol (NDP). Afin de limiter la propagation aux $k$ plus proches voisins, un TTL est décrémenté à chaque nœud intermédiaire que traversent ces messages. Lorsque le TTL atteint $0$, le message est jeté. Comme OLSR, après un certain temps de convergence, chaque nœud peuvent construire la topologie de la zone et calculer la table de routage vers n'importe quel nœud de sa zone. Si une source et une destination sont

dans la même zone, la trame peut être transmise immédiatement après consultation du cache de la table de routage.

Pour joindre un nœud se trouvant en dehors de la zone de routage pro-active, ZRP utilise un algorithme réactif nommé Inter-zone Routing Protocol (IERP) [HPS01]. Cela est effectué en envoyant une requête à tous les nœuds de bordure de la zone. Chacun des nœud de bordure de la zone va regarder si la destination se trouve dans sa propre zone de routage. Si ce n'est pas le cas, ce nœud ajoute son adresse dans l'entête de la trame (comme DSR) et fait suivre la requête à ses propres routeurs de bordure. Si en revanche la destination se trouve dans la zone de routage, il envoie une *route reply* à la source via la route inverse indiquée dans la requête. La source peut alors utiliser la route contenue dans le *route reply* pour envoyer ses données à la destination.

**3.3.1.3.2 IEEE 802.11s** est une évolution du standard IEEE 802.11 afin d'y apporter un nouveau mode de déploiement multi-sauts. Il possède déjà une implémentation dans le noyau Linux (> 2.6.26) et est soutenu par des organisations comme Nortel, Cozybit, One Laptop Per Child (OLPC) et Google. Il a été conçu pour répondre à un certain nombre d'applications et doit pouvoir fonctionner normalement dans des réseaux avec plus de 50 nœuds [Eas07]. Les trois scénarios les plus important sont les réseaux résidentiels, les bureaux et les campus (universités). IEEE 802.11s décrit un protocole de routage mesh de niveau 2 appelé le Hybrid Wireless Mesh Protocol (HWMP) [Bah06] [Bah07]. C'est un protocole hybride offrant une partie pro-active similaire à RPL pour la communication avec les passerelles et une partie réactive similaire à AODV pour la communication entre les nœuds du réseau. HWMP utilise donc l'hybridation comme un moyen d'optimiser les différents services, faible délai pour la communication avec les passerelles qui constituent le trafic le plus important et routes à la demande pour la communication entre les nœuds.

HWMP introduit trois nouveaux types de nœuds en plus du mode AP et du mode STA :

- Mesh Point (MP) tous les nœuds participant au réseau mesh sont des MP. C'est le nœud mesh de base, il participe au relayage des trames et peut initier des procédures de découverte de chemin.
- Mesh Access Point (MAP) a les même fonctionnalités que le MP mais peut également servir d'AP pour des STAtion (STA) n'ayant pas de fonctionnalité mesh. C'est un MP et un AP en même temps.

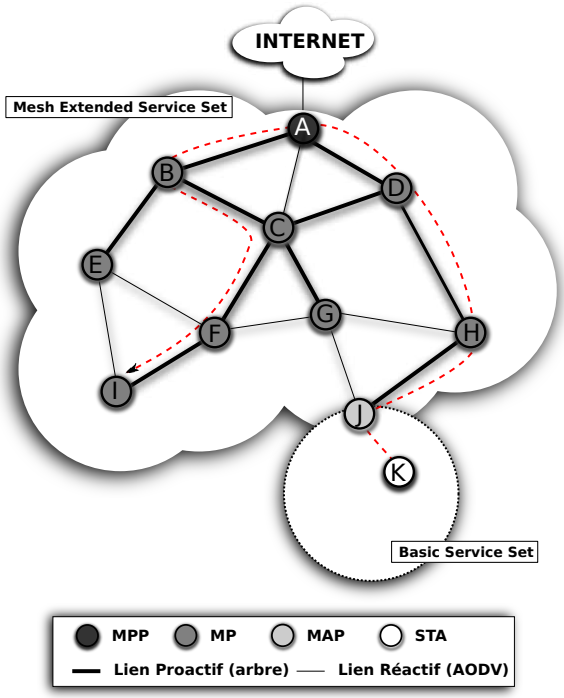



Figure 3.5 – Hybrid Wireless Mesh Protocol (HWMP) maintient pro-activement une structure d'arbre dont la racine est une passerelle vers un réseau. En attendant qu'une route soit découverte avec AODV, la structure d'arbre peut fournir du trafic *point-to-point*

- Mesh Portal Point (MPP) a les mêmes fonctionnalités que le MP mais est une passerelle vers un autre réseau. Il peut relayer les trames vers n'importe quel autre réseau 802, en particulier Ethernet pour l'accès à Internet.

La découverte de chemin à la demande (partie réactive) est effectuée grâce à une procédure très similaire à celle décrite par AODV. Un nœud ayant besoin d'un chemin vers une destination peut initier un Path Request (PREQ) qui sera diffusé au réseau mesh. À la réception de la requête, la destination peut répondre un Path Reply (PREP) à destination de la source. Les MP intermédiaires ayant déjà connaissance de la route peuvent répondre un PREP directement. La source peut également décider que seule la destination a le droit de répondre un PREP en plaçant le bit *Destination Only* à 1.

La partie pro-active de HWMP sert à maintenir une structure d'arbre et nécessite qu'un ou plusieurs nœuds se soient déclarés en tant que racine. Chaque arbre est indépendant des autres et un MP peut appartenir à plusieurs arbres en même temps. Un nœud qui se déclare en temps que racine devient un MPP tel que le nœud $A$ sur la figure 3.5. Il existe trois modes de fonctionnement du mode pro-actif. Le premier

mode consiste à maintenir pro-activement les routes *upward* (vers la racine) et *downward* (depuis la racine). Pour cela, la racine propage périodiquement des PREQ à destination du réseau en entier (broadcast) et place le bit *proactive PREP* à $0$. En procédant ainsi, chaque nouvelle PREQ va se diffuser à travers tout le réseau, créant du même coup les routes vers la racine, et chaque PREP renvoyé à la racine va créer les routes vers les nœuds du réseau. Le deuxième mode consiste à ne maintenir que les routes *upward* vers la racine. Cela est effectué en plaçant le bit *proactive PREP* à $1$. De cette façon, aucun PREP ne sera renvoyé à la racine et seul les routes *upward* seront maintenues. Ce mode permet de limiter la surcharge du réseau tout en permettant de maintenir des routes vers la passerelle. Le troisième mode consiste à ne maintenir aucune route vers la racine mais à propager uniquement des annonces. Cela permet à la racine de s'annoncer en distribuant périodiquement des Root Annoucement (RANN) sans pour autant construire et maintenir les routes pour y accéder. Les RANN permettent, en plus d'annoncer la passerelle à tout le réseau, de calculer la métrique pour y accéder. Dans ce troisième mode de fonctionnement, chaque MP est libre de construire à la demande la route pour accéder à la passerelle.

La structure d'arbre peut également fournir un chemin entre deux stations en attendant qu'un nouveau chemin soit découvert. Sur la figure 3.5, la station $K$ est connectée au MAP $J$, lui-même connecté au réseau mesh. Lorsque la station $K$ veut communiquer avec la station $I$, le MAP $J$ utilise le chemin $H-D-A-B-C-F-I$ déjà créé passant par la racine, mais peut en même temps démarrer une procédure de découverte de chemin. Lorsque cette dernière aura abouti, le nœud $J$ pourra alors basculer son trafic via le chemin $J-G-F-I$.

#### 3.3.1.4 Métriques pour les protocoles de routage traditionnels

Pendant longtemps les liens sans-fil ont été considérés comme étant soit très bon, soit très mauvais. On retrouve cette représentation simpliste du sans-fil dans les premiers modèles de propagation utilisés pour simuler les protocoles. Ces premiers modèles décrivaient un cercle autour d'une station à l'intérieur duquel la réception était de $100\%$ et de $0\%$ à l'extérieur. Il était ainsi généralement admis que si un message de contrôle traversait correctement un lien, alors le lien était utilisable pour transférer les données. Cette vision bimodale du lien sans-fil, hérité des réseaux filaires, a naturellement amené à utiliser le nombre de sauts comme métrique pour les réseaux sans-fil multi-sauts. Si cette métrique donne d'excellents résultats dans les réseaux filaires, elle n'est pas du tout adaptée aux réseaux MANETs. Le papier [DCACM03] en 2003 explora l'influence de cette métrique sur une plateforme réelle d'expérimentation appelée *RoofNet* [Cha02]. Les auteurs ont remarqué que cette mé-

trique, en privilégiant des chemins courts, privilégiaient du même coup les «longs» sauts et donc présentant une forte atténuation. Cette métrique donnaient ainsi des performances assez médiocres du fait des taux d'erreurs élevés que formaient ces chemins. La métrique de routage est donc un aspect essentiel des protocoles de routage dans un environnement sans-fil multi-sauts.

Cette même équipe a développé en 2005 une nouvelle métrique appelée Expected Transmission Count (ETX) [CABM05]. L'ETX d'un lien est l'estimation du nombre de transmissions nécessaires pour transmettre correctement une trame sur un lien en incluant les retransmissions. C'est une métrique cumulative, on peut calculer l'ETX d'un chemin en sommant les ETX pour chaque lien de la route. Par exemple, prenons un chemin constitué de trois sauts de routage dans lequel chaque lien a un taux d'erreur de $50\%$. La valeur de la métrique ETX sur ce chemin vaudra $6$ car en moyenne $2$ transmissions seront nécessaires pour chaque saut. L'ETX d'un lien entre une source et une destination est calculé en mesurant la probabilité $d_f$ qu'une trame soit correctement reçue par la destination ainsi que la probabilité $d_r$ que l'ACK envoyé par la destination soit correctement reçu par la source. Plus formellement, ETX répond à l'équation suivante :

$$ETX = \frac{1}{d_f \times d_r} \tag{3.1}$$

Afin de mesurer les probabilités du lien dans les deux sens, chaque station «teste» les liens en envoyant toutes les secondes une trame particulière appelée *probes*. La station se souvient de l'ensemble des *probes* envoyées et reçues les $10$ dernières secondes. L'avantage d'ETX par rapport au nombre de sauts est que cette métrique est basée sur le taux de succès du lien et que cela affecte directement le débit. De plus, ETX supporte les liens asymétriques puisque le calcul de la métrique est effectué par chaque station de chaque côté du lien.

Modified ETX (mETX) [KB06] est une évolution de ETX plus précise puisqu'elle se base sur le taux d'erreur bit plutôt que sur le taux d'erreur trame. Ceci est réalisé en comptant le nombre de bits erronés à la réception des *probes* qui contiennent une séquence de bit connu. Comme ETX, les $10$ dernières *probes* sont conservées mais afin de rendre la métrique plus réactive face à la variabilité des conditions du canal, mETX utilise une moyenne exponentielle à fenêtre glissante (EWMA). Le filtre EWMA permet d'accorder plus d'importance aux résultats récents en leur donnant plus de poids. Si ETX et mETX ont prouvé leur efficacité face au nombre de sauts, elle ne prennent cependant pas en compte la bande passante des liens. Certains terminaux peuvent transmettre à des *datarates* plus élevés que d'autres et certains

chemins peuvent être plus rapides que d'autres sans que ETX ne soit capable de les distinguer.

Expected Transmission Time (ETT) [ECM+08] est une métrique permettant de mesurer le temps de transmission nécessaire pour correctement transmettre une trame. Elle est fonction du taux d'erreur du canal obtenu avec la métrique ETX, de la taille $S$ des données à transmettre et de la bande passante $B$ du lien. ETT peut donc s'exprimer avec l'équation suivante :

$$ETT = ETX \times \frac{S}{B} \tag{3.2}$$

Contrairement à ETX, cette métrique n'est pas facilement cumulable sur un chemin multi-sauts à cause des interférences qu'introduit un saut de routage. Prenons l'exemple d'un chemin composé de deux liens sans-fil opérant sur le même canal. En faisant l'hypothèse que chaque lien à une bande passante de $B$, la bande passante sur le chemin ne pourra pas dépasser $B/2$ du fait qu'un seul nœud peut transmettre à la fois sur un même canal. Weighted Cumulativ ETT (WCETT) [DPZ04] est une métrique basée sur ETT et prenant en compte la diversité des canaux disponibles sur un chemin multi-sauts. En posant $k$ comme étant le nombre de canaux disponibles, WCETT s'exprime avec l'équation suivante :

$$X_j = \sum_{\text{le saut i est sur le canal j}} ETT_i \quad \text{avec } 1 \leq j \leq k, \tag{3.3}$$

$$WCETT = (1-\beta) * \sum_{i=1}^{n} ETT_i + \beta * \max_{1 \leq j \leq k} X_j \tag{3.4}$$

L'équation 3.4 est composée de deux parties. La première partie est une simple somme sur les ETT le long du chemin, cela reflète le temps d'occupation du canal le long du chemin. La deuxième partie reflète l'ensemble des sauts qui auront le plus d'impact sur le débit. $\beta$ est un paramètre configurable tel que $0 \leq \beta \leq 1$ permettant de choisir un compromis entre les deux, entre délai et débit. Autrement dit, WCETT permet d'estimer l'efficacité d'un chemin en se basant sur ETT et en prenant en compte les interférences générées par le flux lui-même[1]. De façon similaire, une autre métrique Interference Aware (iAWARE) [SBM06] estime l'efficacité d'un chemin en se basant sur ETT et en prenant en compte les interférences causées par les flux eux-mêmes le long du chemin (interférences intra-flux) ainsi que celles causées par les différents flux (interférences inter-flux). iAWARE fonctionne en estimant le SINR (*Signal Over Interference Noise Ratio*)sur chaque nœud du chemin.

Le papier [MLD07] introduit Expected Throughput (ETP) qui est une amélioration de ETT dans les réseaux 802.11. Ce qui fait la spécifité de cette métrique est

[1] on parlera dans la littérature de *intra-flow interferences*.

la prise en compte de l'anomalie de débit décrite dans la section 2.6.3. Une station transmettant à un débit plus faible impactera le débit de toutes les stations se trouvant dans son domaine de contention. La métrique ETP prend en compte ces anomalies liées à la diversité de débit le long du chemin pour calculer son coût. ETP peut être utilisé pour des réseaux multi-hops, multi-canaux et multi-rate.

#### 3.3.1.5 Conclusion

Les protocoles de routage traditionnels fonctionnent en décrivant des mécanismes pour construire les routes et transmettent ensuite les données le long de ces routes. Nous avons identifié plusieurs stratégies de construction de route (proactif, réactif et hybride) et avons décrit le fonctionnement de quelques protocoles. Ainsi, étant donnée une destination, les données sont acheminées de proche en proche le long de ce qui a été déterminé comme la meilleure route par la métrique. Ces métriques se basent pour la plupart sur des moyennes d'échantillonnage et ne reflète donc pas en temps réel l'état de la route. Pourtant, comme nous l'avons montré dans la section 2.2.2, les conditions du canal subissent des variations à toutes les échelles de temps (macro/micro variations) et dépendent de nombreux facteurs rendant impossible de prévoir son évolution au cours du temps. Les protocoles de routage traditionnels ne sont donc pas très réactifs face à ces variations car elles ne peuvent affecter instantanément les résultats de ces calculs. Augmenter la fréquence d'échantillonnage afin d'avoir une connaissance à jour des conditions du canal entraînerait une surcharge importante pour le réseau. Il en résulte que la sélection du prochain saut au sens traditionnel n'est pas optimale, car basée sur des informations obsolètes ou peu adaptés aux micro-variations des conditions du canal. Une approche pour optimiser le routage consiste donc à faire participer la couche de liaison dans la décision de sélection du prochain saut.

### 3.3.2 Protocole de routage adaptatif

Dans cette section, on ne s'intéresse plus à la façon dont les routes sont construites mais plutôt de la façon dont les données sont propagées jusqu'à la destination. Mettons que l'on ait une station dans un réseau multi-sauts qui souhaite envoyer une trame à une certaine destination. Il existe souvent plusieurs chemins possible pour atteindre une destination et donc il existe plusieurs relais permettant de faire progresser la trame jusqu'à la destination. Ces relais sont appelés relais potentiels ou *Candidate Relais Set* en anglais. Le choix du relais est déterminant pour les perfor-

mances d'un protocole et nécessite donc de réagir rapidement face aux variations des conditions du canal. L'idée du routage adaptatif est de baser le relayage sur l'état actuel du voisinage tel qu'il existe et non pas sur la façon dont la station le perçoit. Le routage adaptatif utilise donc des informations et des mécanismes de la MAC pour prendre sa décision de routage. La sélection du relais peut ainsi être fait de deux façons, soit depuis la source en se basant sur des informations à jour de la MAC, soit de façon distribuée par contention entre les relais potentiels.

#### 3.3.2.1 Sélection du relais par la source

**3.3.2.1.1 CoopMAC** [LTN+07] permet d'utiliser les informations de la MAC pour faire coopérer les stations afin d'optimiser la propagation d'une trame vers une certaine destination. Dans cette approche, toutes les stations maintiennent une table de voisinage et ne conservent que les stations voisines qui peuvent apporter un bénéfice à être utilisées en tant que relais (relais potentiels). Pour chacun de ces relais potentiels, la source calcule le temps de transmission que prendrait une trame en étant d'abord transmise au relais puis retransmise par le relais à la destination. Le relais utilise la formule suivante pour effectuer ce calcul : $L/R_{sr} + L/R_{rd}$ ; avec $L$ la taille des données, $R_{sr}$ le débit de la source au relais et $R_{rd}$ le débit du relais à la destination. La source a donc le choix d'envoyer sa trame soit directement à la destination, soit en passant par un relais si celui-ci est plus intéressant. CoopMac s'implémente dans IEEE 802.11 en modifiant la sémantique de l'échange RTS/CTS, une transmission via un relais s'effectue en quatre étapes :

- Si une source veut que sa transmission s'effectue en deux sauts via un relais, la source envoie un message RTS au relais qu'elle a sélectionné.
- Lorsque le relais reçoit un RTS, il répond par un Helper-To-Send (HTS) qui permet de prévenir la véritable destination qu'une transmission va être effectuée en deux sauts.
- À la réception d'un HTS, la destination renvoie un CTS pour réserver le canal le temps nécessaire pour que les deux transmissions soient effectuées.
- Si la source reçoit à la fois le HTS et le CTS, elle peut envoyer sa trame au relais qui sera ensuite directement transmise à la destination. Un ACK standard est envoyé pour acquitter la transmission, que celle-ci se soit effectuée en une seule ou en deux transmissions.

Il est crucial que chaque station maintienne la table de voisinage des relais afin que la décision de routage ne se fasse par avec des informations obsolètes. CoopMac maintient une table appelée *CoopTable* dans laquelle chaque entrée contient des informations sur un relais potentiel spécifique. Les informations maintenues sur ces relais potentiels incluent l'adresse MAC (48 bits), le temps écoulé depuis la dernière trame entendue envoyée par ce relais, et le débit utilisé par ce relais pour communiquer avec la destination. Un ensemble de protocoles est décrit par CoopMac pour maintenir cette table à jour.

#### 3.3.2.2 Sélection du relais par contention

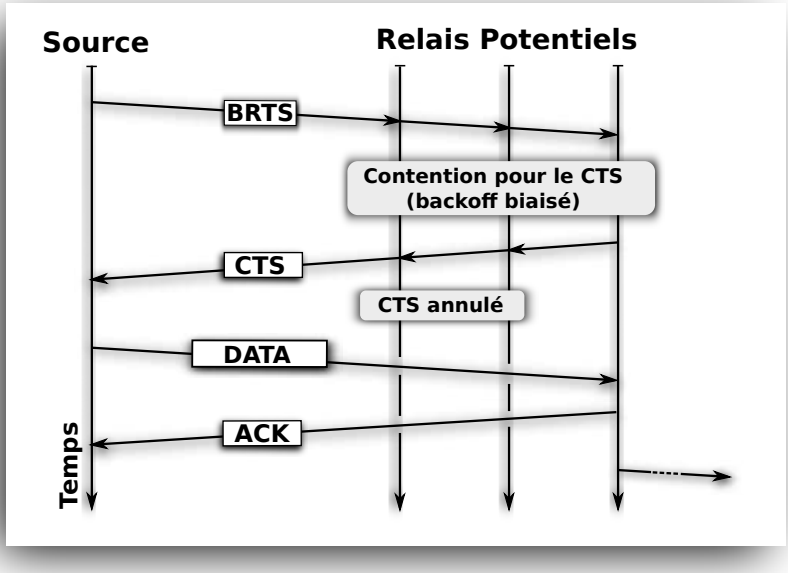



Figure 3.6 – routage adaptatif avec State-free Implicit Forwarding (SIF)

**3.3.2.2.1 State-free Implicit Forwarding (SIF)** [CDV05] décrit par Chen *et al* est un protocole de routage pour réseau de capteurs permettant de propager efficacement des informations vers le puits. SIF est un protocole sans-état, c'est-à-dire qu'il ne maintient pas de table de routage ni ne nécessite de disséminer une requête pour l'obtention d'une route. Ce protocole fait l'hypothèse que chaque station est munie d'un module GPS lui permettant de déterminer sa position géographique et connaît par ailleurs la position géographique de la destination. Étant donnée une station à une certaine position, il existe un certain nombre de relais potentiels permettant de faire progresser la trame vers la destination. La figure 3.6 montre un exemple de transmission avec SIF. Avant de transmettre sa trame de donnée, la source envoie

un message Broadcast RTS (BRTS), qui est un RTS en diffusion, contenant sa propre position géographique. Une station recevant ce RTS peut déterminer si elle est un relais potentiel en comparant la distance qui la sépare de la destination avec celle de la source. Si un récepteur détermine qu'il est plus proche de la destination que la source, il devient relais potentiel. Les relais potentiels entrent alors dans une phase de contention pour transmettre le CTS. Les données sont ensuite envoyées au relais ayant gagné la contention (le premier à transmettre un CTS).

**3.3.2.2.2 RSSI-Based Forwarding (RBF)** [ALRS09b][ALRS09a] décrit par Awang *et al* est un mécanisme similaire à SIF permettant de choisir le prochain saut dynamiquement pour chaque trame à l'intérieur d'une cellule 802.11. Comme toute cellule 802.11, l'AP propage périodiquement un *beacon* permettant à chaque station de connaître son RSSI (i.e. le niveau de puissance du beacon reçu). Dans RBF, chaque transmission est précédée par l'émission d'un RTS (voir section 2.4.5.4) envoyé en *broadcast* et comportant dans son entête le RSSI de l'émetteur. Les stations ayant reçu le RTS peuvent lire la valeur du RSSI contenu dans l'entête et la comparer avec la leur. Si le RSSI est plus important que celui contenu dans l'entête du RTS, la station peut déduire qu'elle est plus proche de l'AP que l'émetteur et devient un relais potentiel. Les relais potentiels participent ensuite à une procédure de contention pour transmettre le CTS auprès de la source. Le relais potentiel ayant le plus petit *backoff* transmet le CTS, annulant en même temps le *backoff* des autres relais potentiels. La source envoie finalement sa trame en unicast auprès du relais ayant gagné la contention. Cette approche permet de s'adapter aux conditions du canal à chaque transmission. Cette méthode de sélection basée sur la valeur du RSSI sera reprise pour notre travail sur FBR bien que notre approche du problème soit différente.

### 3.3.2.3 Conclusion

Les protocoles de routage adaptatifs permettent d'utiliser les informations et les mécanismes de la MAC pour optimiser le routage. Cela se base soit sur une mise à jour en temps réel des taux d'erreurs des liens rendu possible par l'écoute des trames environnantes (CoopMac), soit par la sélection d'un relais après une phase de contention sur le CTS. Ces deux approches permettent de choisir un relais en se basant sur des informations du canal beaucoup plus à jour que dans le cas du routage traditionnel. Cependant, cette approche est encore sous-optimale car cela suppose que les conditions du canal sont stables entre la sélection du relais et l'envoi des données vers ce relais. Même si les informations du canal sont très à jour, l'échange prélimi-

naire à la sélection du relais concerne une trame de petite taille et ces mécanismes ne peuvent assurer que la trame de données sera bien reçue par le relais sélectionné.

### 3.3.3 Protocole de routage opportuniste

Les protocoles de routages décrits dans les sections précédentes cherchent à déterminer le meilleur relais possible avant de transmettre les données sur le lien. En routage traditionnel comme en routage adaptatif, une fois que le relais est déterminé, les trames de données sont envoyés sur le chemin et arrivent à la destination après un certain nombre de sauts de routage unicast. Si au niveau d'un nœud intermédiaire une transmission échoue, c'est-à-dire que le *next hop* n'a pas acquitté la transmission, une retransmission est effectuée. La trame est retransmise jusqu'à la transmission d'un ACK ou si le nombre maximal de retransmissions a été atteint. Les algorithmes de routage font donc abstraction du lien sans-fil et le routage est construit comme une séquence de liens point à point.

Cependant, cette méthode de routage unicast ne tire pas tous les avantages de la communication en sans-fil. Comme expliqué dans le chapitre 2.2, le sans-fil est un support diffus et capricieux. Les conditions du canal peuvent varier dans le temps à cause de l'atténuation, des interférences, des effets de multi-chemin ou de la mobilité. En plus d'être imprévisible, une station émettrice ne connaît pas les conditions radio dans lesquelles se trouve une station réceptrice. De plus, due à la nature diffuse du sans-fil, une transmission envoyée en unicast peut-être reçue par plusieurs nœud en même temps, et pas nécessairement celui souhaité. Dans ces conditions, choisir le prochain saut à priori d'une transmission n'est pas la meilleure stratégie de routage. Cela signifie que le routage unicast, tel qu'il est implémenté en *hop-by-hop* est sous-optimal et peut être amélioré. Des recherches effectuées dans le domaine de la théorie de l'information démontrent l'avantage d'utiliser un canal de diffusion composé de plusieurs relais [VdM77].

Un routage optimal permettrait de choisir le prochain saut, c'est-à-dire celui qui sera responsable de retransmettre la trame, à posteriori d'une transmission. Une telle stratégie de routage consisterait d'abord à transmettre la trame en diffusion et choisir ensuite le meilleur relais parmi ceux qui ont correctement reçu la trame. Une telle approche permettrait dans un premier temps de profiter de la diversité des chemins offerts.

Considérons l'exemple de gauche de la figure 3.7. Cette figure est composée d'une source, d'une destination et de quatre relais intermédiaires ayant des pro-


Figure 3.7 – Le routage opportuniste exploite la diversité des chemins et peut faire des progrès vers la destination de façon plus efficace qu'en routage traditionnel

babilités de lien identique. Une approche traditionnelle choisirait un de ces relais, le nœud $B$ dans l'exemple, et routerait tout son trafic à travers ce dernier. Un rapide calcul nous montre qu'en moyenne $5$ transmissions sont nécessaires pour atteindre la destination, $4$ pour le premier saut et $1$ pour le deuxième saut. Une approche opportuniste permettrait de tirer profit de la diversité des relais, en supposant les probabilités indépendantes seules $2.5$ transmissions seraient nécessaires $(1/(1-\overline{0.25})^4+1)$.

De plus, une approche opportuniste permet de tirer profit de chaque transmission utile. Prenons l'exemple de droite de la figure 3.7. Dans cet exemple, le nœud source et destination sont séparés par une chaîne de nœuds intermédiaires avec des probabilités de réception décroissantes avec la distance. Une approche traditionnelle choisirait la séquence $src-B-D-dst$ qui offre le meilleur compromis en terme de nombre de sauts et taux de réception. Si une transmission depuis la source va moins loin que prévu et n'atteint que $A$ sans atteindre $B$, cette transmission est gâchée et la source va retransmettre la trame. Si à l'inverse la transmission va plus loin que prévu et atteint $C$, le routage traditionnel ne peut pas exploiter cette transmission et $C$ détruira la trame. Dans le routage opportuniste, $A$ aurait pu retransmettre la trame et permettre à celle-ci de progresser vers la destination un peu plus que si cette dernière était restée à la source. De la même façon, les « longues » transmissions peuvent être exploitées, permettant d'économiser une transmission.

Le routage opportuniste permet ainsi d'exploiter au maximum les caractéristiques du sans-fil mais pose en même temps de nouveaux défis. Afin d'arriver à un routage opportuniste optimal, il y a deux difficultés à prendre en compte :

- **Sélection** des relais potentiels parmi les récepteurs
- **Suppression** des candidats pour que seul le meilleur relais retransmette la trame

Du fait de la nature diffuse du sans-fil, une trame envoyée en diffusion va être reçu potentiellement par tous les nœuds du voisinage. Parmi les récepteurs, on appelle relais potentiels les récepteurs pouvant faire progresser la trame vers la destination [2]. La première difficulté est donc d'avoir un moyen permettant de **sélectionner** le sous-ensemble de nœuds parmi les récepteurs pouvant participer au relayage. Un mauvais discriminant risquerait de mettre à contribution des nœuds offrant une capacité de progression vers la destination moindre que la source elle-même.

En augmentant le nombre de relais potentiels, on augmente également le risque de provoquer plusieurs retransmissions de la même trame par des relais différents. Afin d'éviter une *tempête* de retransmission, il faut décrire un mécanisme permettant de coordonner les nœuds à la fois pour sélectionner un seul relais parmi l'ensemble des relais potentiel et supprimer les autres pour les empêcher de propager inutilement la trame. La **suppression** consiste donc à éviter les duplications de trames en retirant des relais potentiels non sélectionnés de la procédure. Cela doit être fait avec un coût minimum car un échange de messages trop important risquerait de neutraliser les avantages du routage opportuniste qui consiste justement à diminuer au maximum les transmissions inutiles.

La plupart des approches de routage opportunistes peuvent se distinguer en deux catégories : celles qui prédéterminent l'ensemble des relais potentiels avant la transmission (*multicast*) et celles qui ne les déterminent pas à l'avance (*broadcast*).

#### 3.3.3.1 Relais potentiels prédéterminés

**3.3.3.1.1 Extremely Opportunistic Routing (ExOR)** [BM05] est un protocole de routage opportuniste créé en 2004 au MIT par Biswas *et. al*. Ce protocole fonctionne en prédéterminant l'ensemble des relais potentiels avant la destination et en organisant la *suppression* en ordonnançant les transmissions des relais potentiels de façon à privilégier les meilleurs. ExOR fait l'hypothèse que toutes les paires d'ETX du réseau sont connues de chaque nœud. À partir de ces informations, lorsqu'une source souhaite transmettre des données à une destination, elle construit d'abord la *forwarder list*, la liste des relais pouvant participer au relayage des trames. Pour chaque relais de cette liste, un coût est associé désignant le nombre moyen de transmissions nécessaires pour aller jusqu'à la destination en passant par ce relais (calculé en sommant les ETX). Proportionnellement à ce coût, la source spécifie un *timer* pour chaque relais désignant à quel moment la transmission sera possible. La liste des relais et leurs *timers* sont placés dans les entêtes de chaque trame envoyée par la

[2] On trouvera le terme de Candidate Relay Set (CRS) dans la littérature

source. De cette façon, chaque relais attend son tour avant de commencer ses retransmissions en laissant la priorité aux meilleurs relais. Les trames ne sont pas acquittées directement auprès de la source avec un ACK car chaque trame est envoyée en *broadcast*, à la place ExOR utilise un mécanisme de *gossiping*. ExOR opère sur un lot de trames, la source envoie ses trames en diffusion à la suite, sans interruption, et la destination renvoie la liste des trames qu'elle a reçue. Les relais commencent ensuite à retransmettre ce qui est nécessaire, les meilleurs relais en premier. Chaque retransmission contient également dans son entête la liste des trames déjà reçues ou déjà retransmises. De cette façon, chaque relais met à jour la liste des trames restant à transmettre en écoutant les retransmissions des autres relais. Lorsque le dernier relais à fini ses retransmissions, la source retransmet toutes les trames n'ayant été ni reçues ni retransmises.

Des expériences réelles effectuées sur la plateforme d'expérimentation *RoofNet* [Cha02] ont montré qu'ExOR permettait d'augmenter le débit de plus de $35\%$. ExOR fonctionne encore mieux pour les nœuds éloignés en offrant une augmentation de $200\%$ à $400\%$. Si les résultats de ExOR sont très impressionnants, cet algorithme fait cependant l'hypothèse que toutes les paires de liens sont connues, ce qui constitue une hypothèse très forte. De plus, la sélection du meilleur relais se fait en se basant sur la métrique ETX qui n'est pas adaptée pour une approche opportuniste car elle ne prend pas en compte la diversité des chemins possibles.

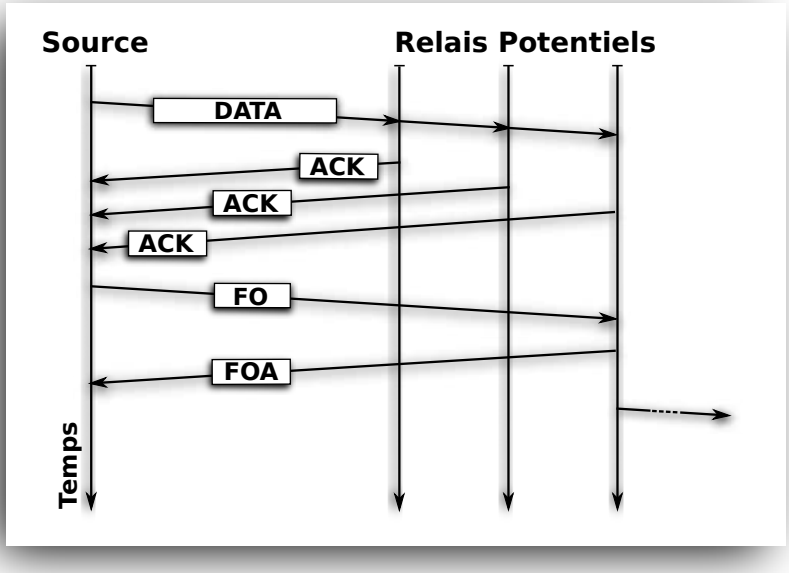



Figure 3.8 – routage opportuniste avec Selection diversity forwarding (SDF)

**3.3.3.1.2 Selection Diversity Forwarding** Selection diversity forwarding (SDF) [Lar01] est un algorithme élaboré en 2001 au MIT. La figure 3.8 donne un exemple de routage opportuniste avec SDF. La source souhaitant transmettre des données à une destination prédétermine un ensemble de relais potentiels appropriés auxquels elle envoie la trame (en multicast). La trame est transmise en une seule fois mais inclut dans son entête la liste des relais potentiels afin que chaque nœud concerné puisse la traiter. Parmi ces relais, ceux ayant reçu la trame renvoient un accusé de réception à la source, chacun leur tour dans l'ordre défini par la liste en entête de la trame. En recevant ces accusés de réception, la source peut déterminer lequel des candidats est le meilleur pour faire progresser la trame vers la destination. Elle envoie un message appelé Forward Order (FO) en unicast au candidat qu'elle pense être le meilleur. Finalement, le candidat termine la procédure en accusant auprès de la source la réception de cet ordre avec un Forward Order Acknowledgement (FOA). Cette procédure recommence jusqu'à ce que la trame atteigne la destination.Ainsi, 4 échanges sont nécessaires pour relayer une trame avec SDF, c'est similaire à l'échange RTS/CTS dans IEEE 802.11.

### 3.3.3.2 Relais potentiels non-déterminés à l'avance

**3.3.3.2.1 Contention-Based Forwarding (CBF)** [FWK+03] est un protocole de routage opportuniste qui ne prédétermine pas l'ensemble des relais à l'avance. Chaque trame est envoyée en diffusion à l'ensemble du voisinage et seules les stations pouvant faire progresser la trame vers la destination participent au mécanisme. Ce protocole appartenant à la famille des protocoles géographiques (voir figure 3.2), cette décision est basée sur la position des relais par rapport à celle de la source, vis-à-vis de celle de la destination. Un mécanisme de contention aléatoire, similaire au *backoff* de 802.11, est ensuite effectué entre ces relais potentiels pour sélectionner celui qui va effectivement relayer la trame. CBF introduit un biais dans la façon dont le *timer* est choisi en favorisant les «meilleures» stations en fonction de leur position par rapport à la destination. Afin d'éviter les duplications, CBF implémente un mécanisme de suppression des relais potentiels, c'est-à-dire le mécanisme qui permet de s'assurer qu'une seule copie de la trame est relayée. Lorsqu'un des relais gagne la contention, il relaie la trame vers la destination, les autres relais potentiels entendant cette transmission annulent leur procédure de relayage. Si à l'issue du *timer* un relais potentiel n'a pas entendu une autre station relayer la trame, il va lui-même la relayer. Les auteurs décrivent un mécanisme permettant de réduire le risque de duplication de trame en faisant une sélection plus exigeante des relais potentiels. Via une approche géographique du problème, seuls les relais potentiels

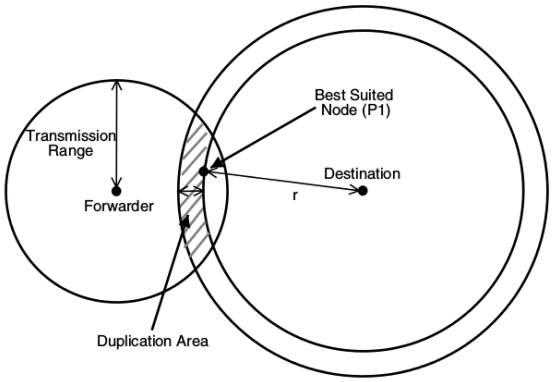



Figure 3.9 – Mécanisme de sélection des relais potentiels avec Contention Based Forwarding (CBF)

se trouvant à la frontière de l'aire de couverture de la source (c'est-à-dire ceux offrant le maximum de progression vers la destination) sont autorisés à participer à la contention. L'aire de couverture est modélisée par les auteurs avec un cercle centré sur la source, ainsi seuls les relais à proximité de la frontière du cercle sont autorisés à participer au relayage de la trame. Ce mécanisme est représenté par la figure 3.9 empruntée au papier [FWK+03] (Fig 2. dans le papier). La **suppression** des relais potentiels est donc effectuée par une combinaison d'informations géographiques et d'écoute du canal. Ce papier est le premier à offrir une vision basée sur la contention entre les relais, et cette idée sera au cœur du mécanisme FBR que nous proposons (voir 4).

**3.3.3.2.2 Opportunistic Multi-path Routing (OMR)** [DLC07] est un protocole de routage opportuniste pour les réseaux IEEE 802.15.4 destiné aux réseaux de capteurs. Comme CBF, les relais sont déterminés de façon opportuniste parmi les récepteurs en fonction de leur capacité à faire progresser la trame vers un puits. Dans OMR, les stations sont organisées en fonction du nombre de sauts pour atteindre la destination avec un algorithme de routage traditionnel donnant ainsi un «rang» à chaque station. Lorsqu'une source envoie une trame en diffusion, les stations voisines peuvent comparer leur « rang » avec celui de la source pour choisir de faire partie de l'ensemble des relais potentiels ou non. Les relais potentiels démarrent ensuite une phase de contention dans laquelle ils choisissent un *backoff* de façon à favoriser les stations ayant une plus forte probabilité $p_{relais}$ de faire progresser la trame vers la destination. Pour cela, les auteurs considèrent que les stations connaissent les ETX avec leurs voisins et calculent $p_{relais}$ comme étant la probabilité qu'au moins

une station $i$ de rang inférieur reçoive la trame

$$p_{relais} = 1 - (1 - q_i) \tag{3.5}$$

avec $q_i$ le taux de perte du canal entre le relais et la station $i$. Le relais qui gagne la contention transmet la trame, les autres se retirent de la procédure en entendant cette transmission mais conserve la trame en cache. Cependant, OMR permet dans certains cas à des relais ayant entendu la retransmission de relayer quand même la trame afin de promouvoir l'exploration de nouveaux chemins pour augmenter la probabilité qu'au moins une trame arrive à destination. Cette exploration n'est permise que si la probabilité $p_{relais}$ est inférieure à $90\%$, c'est-à-dire s'il y a de fortes chances qu'il n'arrive pas à progresser vers la destination. OMR décrit également un mécanisme d'acquittement négatif permettant au puits d'envoyer vers la source une demande de retransmission des trames perdues en chemin (en regardant les numéros de séquence manquants). Comme certaines de ces trames sont gardées en cache par les stations intermédiaires, cette requête ne revient pas nécessairement jusqu'à la source car ces nœuds intermédiaires peuvent prendre en charge la retransmission de ces trames s'ils les possèdent.

## 3.4 Conclusion

Les réseaux sans-fil multi-sauts sont une classe de réseaux distribués et sans infrastructure dans laquelle la communication est rendue possible par la coopération des nœuds pour le relayage des trames. Dans ces réseaux, les protocoles de routage jouent un rôle fondamental car ils sont responsables de construire les routes et de propager les trames le long de ces routes. À cause de la dynamique du réseau due aux caractéristiques des liens sans-fil et de la mobilité des nœuds, ces protocoles doivent pouvoir réagir face aux modifications de la topologie et de l'environnement pour maintenir la communication et les performances du réseau. La littérature sur les protocoles de routage dans ces réseaux est très importante et a ainsi mené à de nombreuses stratégies. Sans être exhaustif, nous avons classé ces différentes stratégies dans trois catégories en fonction de l'échelle de temps prise en compte pour la réactivité face aux modifications du voisinage d'un nœud dans les mécanismes de relayage.

Dans le **routage traditionnel**, les trames sont transmises le long des routes en étant relayées de proche en proche jusqu'à la destination. Ces sauts de routage sont effectués en *unicast* après consultation de la table de routage précédemment calculée lors de la phase de construction de route. Si des pertes ont lieu au niveau d'un nœud

intermédiaire, ce nœud retransmet la trame jusqu'à ce qu'elle soit correctement reçue par le prochain saut. L'efficacité de ce type de relayage est donc très dépendant de la pertinence du calcul de ces tables de routage. Pro-actif ou réactif, ce calcul est généralement effectué en suivant une moyenne cumulée sur les chemins permettant d'offrir une vue d'ensemble de la qualité d'un chemin. Ce mode de fonctionnement échoue cependant à offrir une vision réactive de l'environnement immédiat du nœud car cela nécessiterait un échantillonnage trop important du voisinage.

Le **routage adaptatif** est une approche qui permet de déléguer la tâche de relayage à la couche basse en prenant en compte l'environnement immédiat du nœud pour sa décision de routage. Dans cette approche, on distingue la création des routes calculées traditionnellement et qui permet d'offrir un gradient de convergence vers une destination, du mécanisme de relayage des trames le long de ces chemins qui est ici délégué aux couches basses. Il s'agit donc d'une approche *cross-layer* qui utilise les informations du routage traditionnel pour sélectionner un ensemble de relais pouvant faire progresser la trame vers la destination. La décision de choisir un relais parmi un ensemble de candidats est donnée à la MAC en fonction des conditions du canal. La trame est ensuite transmise en *unicast* vers le relais sélectionné par la MAC. En ne maintenant non plus un voisin, mais un ensemble de candidats, le routage adaptatif permet de s'adapter très rapidement aux changements de conditions de l'environnement.

Le **routage opportuniste** est une approche permettant de prendre en compte l'environnement immédiat d'un nœud tel qu'il est et non pas tel qu'il est perçu par ce nœud. Cette approche fonctionne en envoyant d'abord la trame de donnée, et en sélectionnant ensuite un relais parmi l'ensemble des stations ayant reçue cette trame. Comme pour le routage adaptatif, cette sélection peut-être effectuée en utilisant les informations du routage traditionnel pour créer le gradient de convergence. En embrassant la nature diffuse du sans-fil, cette approche supprime la signalisation nécessaire pour sonder l'environnement et permet de tirer profit de toutes les transmissions effectuées puisque la transmission n'est plus *unicast* mais en *broadcast* ou en *multicast*. La duplication des relais nécessite cependant de devoir contrôler la diffusion de la trame afin d'éviter la duplication des trames, ce qui consommerait inutilement les ressources du réseau.

Dans le chapitre 4, nous décrirons une solution de coopération dans une cellule 802.11 en se basant sur les mécanismes de routage opportuniste.

CHAPITRE 4

# Proposition d'un protocole de retransmission : FBR

**Sommaire**



## 4.1 Motivation

L'aire de réception autour d'une station sans-fil est délimitée par la capacité des récepteurs à décoder correctement un signal. Augmenter la puissance d'émission de l'émetteur permet d'augmenter l'aire de la cellule mais cela est coûteux car l'atténuation du signal est fonction carré de la distance. Cette solution est limitée par le

coût énergétique mais également par les législations en vigueurs limitant la puissance d'émission. Augmenter l'infrastructure du réseau d'accès tel que cela est fait dans les réseaux GSM ou les ESS de IEEE 802.11 (voir section 2.4.4.2) permet de couvrir une plus grande surface mais implique un coût de planification cellulaire. Cette solution n'est pas flexible et s'adapte difficilement aux besoins du réseau. L'usage de relais dans les réseaux sans-fil est intéressant car cela permet d'augmenter la couverture d'une cellule à moindre coût, en tirant parti de la présence des utilisateurs de la cellule. Dans cette thèse nous décrivons une méthode pour les réseaux basés sur CSMA/CA permettant de tirer parti de la présence d'un (ou plusieurs) relais dans un cellule. Cette méthode permet à une relais de relayer les trames d'une station ayant une mauvaise qualité de lien avec la destination. Notre protocole n'utilise aucune message de signalisation et profite de la réception opportuniste des trames pour les décisions de routages. Bien que pouvant s'adapter à n'importe quel technologie basée sur CSMA/CA, nous nous sommes concentré sur le cas de figure des réseaux IEEE 802.11 car ils offrent le plus de potentiels du fait de leur très vaste présence.

Dans le standard IEEE 802.11, une station source retransmet la trame tant qu'elle n'a pas reçue un ACK ou qu'elle n'a pas atteint le nombre maximum de tentatives. Les pertes peuvent être dues à des collisions ou à cause d'une mauvaise qualité de lien avec la destination. L'augmentation de la fenêtre de contention permet de diminuer les probabilités de collisions et donc d'augmenter les chance que la retransmission soit correctement reçu par la destination. Cette stratégie est cependant peu efficace dans le cas d'une mauvaise qualité de lien car la retransmission aura la même probabilité d'échec. IEEE 802.11 permet également de s'adapter aux conditions du canal en choisissant un débit moins élevé offrant un mode de transmission plus robuste. Cette diversité de débit provoque cependant certains effets de bord comme nous l'avons expliqué dans la section 2.6.3. Les stations choisissant un débit plus faible passent plus de temps à envoyer leur propres trames, affectant de fait le débit général de la cellule et donc celui des autres stations. Nous avons montré que dans certaines conditions, il est plus intéressant de faire plusieurs sauts de routage à des débits élevés plutôt que d'essayer de transmettre les trames en une seule transmission. Ces sauts de routages peuvent être effectués par d'autres stations IEEE 802.11 environnantes.

Dans le deuxième chapitre, nous avons étudié les différentes solutions de relayage développées au cours de ces vingt dernières années dans le domaine des réseaux sans-fil multi-sauts. Ces protocoles décrivent différentes stratégies de routage pour acheminer de l'information en utilisant les différentes stations comme relais. L'approche du routage opportuniste est séduisante car elle tire profit de la nature

diffuse du sans-fil en considérant tous les relais présents à l'instant de la transmission dans l'environnement de l'émetteur. Cette approche permet de s'adapter instantanément aux modifications de l'environnement du lien sans-fil et permet en plus de tirer parti des transmissions «chanceuses» en explorant tous les relais à un saut à la fois.

Dans ce chapitre, nous proposons un nouveau mécanisme de coopération appelé Forwarding By Retransmission (FBR) et basé sur la retransmission opportuniste des trames. Le but de ce mécanisme est de réduire le nombre de retransmission dans un réseau infrastructure, ou alors peut être utilisé pour relayer des trames dans réseau *ad hoc*. Ce mécanisme fonctionne en déléguant le mécanisme de retransmission à des stations ayant plus de chance de succès avec la destination que la source. En procédant ainsi, on résout les problèmes des pertes des stations lointaines en fournissant un mécanisme de relayage qui minimise la signalisation. Ce protocole efface la frontière du mode infrastructure et du mode *ad hoc* en empruntant des stratégies de routage similaires aux réseaux sans-fil multi-sauts et plus particulièrement du routage opportuniste. Dans un premier temps nous décrirons le fonctionnement du protocole en détail ainsi que son implémentation dans le simulateur NS-2. Nous validerons son fonctionnement par simulation et nous ouvrirons des pistes d'amélioration du protocole.

## 4.2 Conception

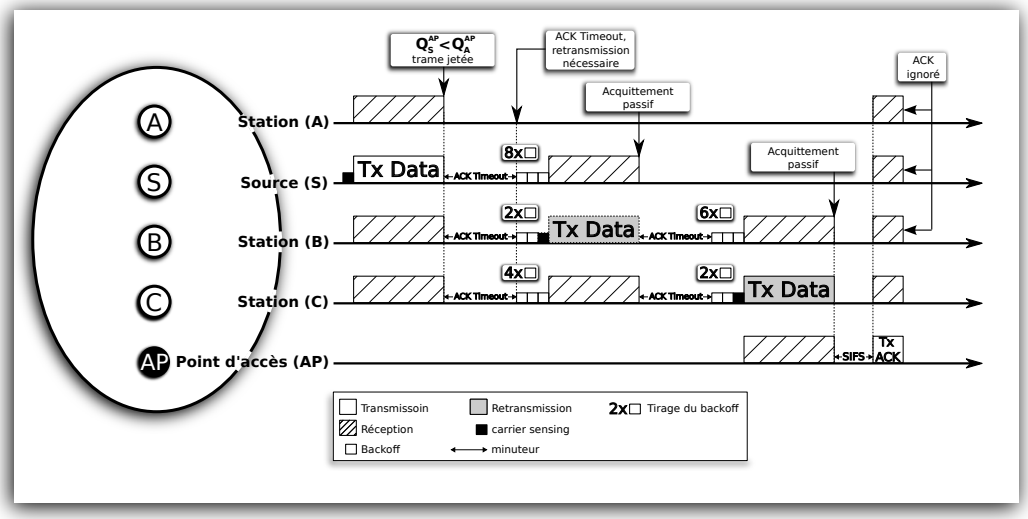



Figure 4.1 – Exemple de coopération dans une cellule IEEE 802.11 avec FBR

Due à la nature diffuse du sans-fil, chaque transmission effectuée par une station peut être reçue par un certain nombre de stations environnantes et pas nécessairement par la destination. Parmi ces récepteurs, certains peuvent fournir une meilleure capacité de progression vers la destination que la source (par exemple parce qu'ils ont une meilleure qualité de lien avec la destination). FBR permet à une telle station réceptrice de prendre la décision de retransmettre une trame à la place de la destination en se basant uniquement sur des informations locales (*i.e.* sans échanger d'informations avec les autres stations). Le relayage est donc vu comme une forme de retransmission, effectuée par une station ayant plus de chance de faire progresser la trame vers la destination que la source elle-même. Cet algorithme est indépendant du mode de fonctionnement (mode infrastructure ou mode *ad hoc*) mais nécessite que les stations aient accès à une métrique informant de leur qualité de progression vers une certaine destination afin de se comparer avec la source.

Dans le mode infrastructure, cette métrique peut être le RSSI du *beacon* transmis par l'AP, ou bien par la probabilité du lien fournis par le driver de la carte *wifi* (voir section 2.6.1). Dans le mode *ad hoc*, dans un réseau sans-fil multi-sauts cette information peut être obtenue avec n'importe quel métrique comme celles que nous avons vues dans la section 3.3.1.4. On note $Q_i^j$ la métrique donnant la qualité du lien ou du chemin entre la station $i$ et $j$.

La figure 4.1 montre un exemple de fonctionnement du protocole FBR dans le mode infrastructure. Ce scénario est composé d'un $(AP)$ et de $4$ stations dont une source $(S)$ et trois stations $(A)$,$(B)$ et $(C)$. Les stations sont placées à des distances croissantes de l'AP de telle sorte que $Q_A^{AP} > Q_S^{AP} > Q_B^{AP} > Q_C^{AP}$. La source $(S)$ envoie une trame vers l'AP qui est reçue par les stations $(A)$,$(B)$ et $(C)$ mais pas par l'AP. La source $S$ a également pris soin d'ajouter dans l'entête de la trame sa propre métrique $Q_S^{AP}$. De cette façon, les stations réceptrices sont en mesure de lire cette métrique et de la comparer avec la leur. La station $(A)$ possède une métrique $Q_A^{AP}$ plus mauvais que celle de la source et ne participe donc pas à la retransmission. Les station $(B)$, $(C)$ participeront à la retransmission (si besoin) car leur métrique est meilleure que celle de la source. À l'issue du *timer ACK timeout*, aucun ACK n'a été reçu et donc une retransmission est nécessaire. Les trois stations $(S)$, $(B)$ et $(C)$ sont en compétition pour retransmettre la trame et chacune tire un *backoff* aléatoire. Dans cet exemple, la station $(B)$ gagne la contention et retransmet la trame sans modifier les champs d'adresse source et destination et insère sa métrique $Q_B^{AP}$ dans l'entête de la trame. En entendant cette retransmission, la source $(S)$ sait que la trame à progressé vers la destination car $(B)$ a une meilleure métrique qu'elle. La source $(S)$ considère donc cette trame comme un accusé de réception. La station $(C)$ en

revanche a une meilleure métrique $Q_C^{AP}$ que la station $(B)$ et ne considère donc pas cette trame comme un accusé de réception. L'AP n'ayant pas reçu cette transmission, une retransmission est de nouveau nécessaire. À l'issue du *timer ACK timeout*, les stations $(B)$ et $(C)$ vont essayer de retransmettre la trame. La station $(C)$ gagne la contention et retransmet la trame. $(B)$ acquitte passivement la trame (car $(C)$ a une meilleure métrique que $(B)$) et la destination acquitte normalement la trame. Bien que l'accusé de réception soit envoyé à destination de la source $(S)$ (car les champs adresses n'ont pas été modifié par les relais), la source $(S)$ et $(B)$ ont déjà acquitté passivement la trame (en entendant respectivement la retransmission de $B$ et de $C$) et ignorent donc cet ACK. L'ACK termine la procédure de retransmission.

Ainsi, lorsque la source $s$ envoie sa trame à destination de $d$, FBR s'exécute de la façon suivante sur un récepteur $r$ :

**Algorithm 1** Algorithme FBR sur un relais $r$

```
1 : Une trame est entendue et reçue par la MAC (source s, destination d).
2 : if (Q_r^d < Q_s^d) then
3 :     La contention démarre.                          ▷ (r) est un relais potentiel
4 :     while (La contention n'est pas terminée) do
5 :         if (Acquittement passif || Acquittement retardé) then
6 :             abandon de la contention ;              ▷ (r) a perdu la contention
7 :             trame jetée ;
8 :             Exit
9 :         end if ;
10 :    end while ;
11 :    La trame est transmise.                         ▷ (r) a gagné la contention
12 :    if (SIFS timeout & pas d'ACK reçu) then
13 :        La trame nécessite une retransmission, go to line 3
14 :    end if ;
15 : else
16 :    La trame est ignorée ;                          ▷ (r) n'est pas un relais potentiel
17 :    Exit
18 : end if ;
```

Afin de rendre FBR opérationnel nous devons faire les modifications suivantes à IEEE 802.11 :

- Une métrique (e.g. ETX, RSSI, etc.) est ajoutée dans les entêtes de toutes les transmissions par l'émetteur de la trame

- Chaque station traite toutes les trames correctement reçues, même celles pour lesquelles elle n'est pas la destination (*monitor mode*)
- Nous introduisons deux nouveaux mécanismes d'acquittement appelés *acquittement passif* et *acquittement retardé*.

Les sous-sections suivantes détaillent les principes de fonctionnement de FBR.

### 4.2.1 Les relais potentiels

Nous définissons ainsi l'ensemble des *relais potentiels* (PF) comme étant l'ensemble des stations qui vont entrer en compétition avec la source pour retransmettre les trames nécessitant une retransmission (celles n'ayant pas été acquittées par la destination). Chaque transmission effectuée par une station est reçue par un ensemble de récepteurs. Les relais potentiels constituent le sous-ensemble de récepteurs permettant de faire progresser la trame vers la destination plus efficacement que l'émetteur. Ainsi lorsqu'une station entend une trame, elle doit pouvoir déterminer si elle fait partie de ce sous-ensemble ou non. Cela signifie que nous avons besoin d'une métrique et d'un mécanisme permettant à un récepteur de se comparer avec l'émetteur sur la capacité à faire progresser la trame vers la destination.

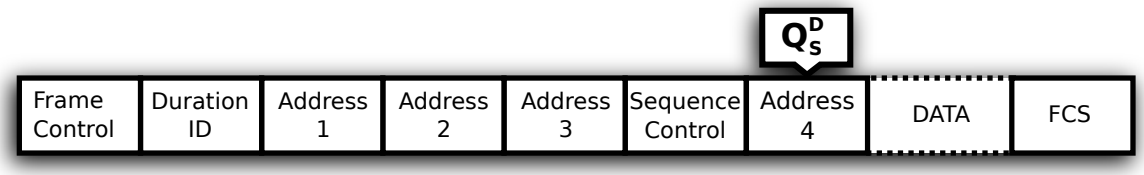



Figure 4.2 – le champ d'adresse $4$ de l'entête IEEE 802.11 est utilisé pour transporter la métrique de l'émetteur

Afin de permettre à une station réceptrice de comparer sa métrique avec celle de la station émettrice, chaque station ajoute la valeur de sa métrique (avec la destination) dans l'entête de chaque trame qu'elle envoie. Une trame IEEE 802.11 standard a un entête de $30$ octets tel que décrit dans la figure 4.2 et ne supporte pas de champs optionnels comme IPv4 ou IPv6. On ne peut donc pas étendre cette entête avec de nouveaux champs. Nous utilisons donc le quatrième champ d'adresse pour y insérer la métrique $Q_s^d$ de l'émetteur $s$ avec la destination $d$. C'est un champ de $6$ octets, cela nous laisse amplement la place d'y stocker la valeur d'une métrique ($4$ octets pour une métrique de type *int*). En faisant cela, nous limitons notre solution à un BSS ou un IBSS mais nous ne pouvons plus utiliser le mode de fonctionnement ESS

(voir section 2.4.4.2). Étant donné une source $s$ et une destination $d$ et l'ensemble $R$ des stations ayant entendue la trame, nous pouvons définir l'ensemble des relais potentiels les stations vérifiant :

$$Q_s^d \leq Q_i^d, \quad i \in R \tag{4.1}$$

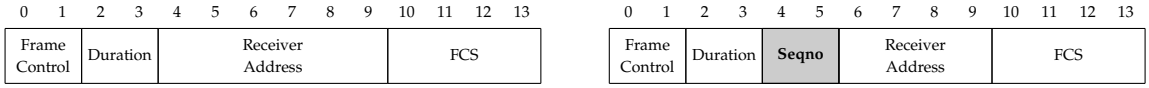
Si une station est un relais potentiel pour une trame qui vient d'être entendue, cette station attend maintenant l'ACK correspondant à cette transmission et démarre un *timer*. Si un ACK est reçu, aucune retransmission n'est nécessaire, le *timer* est annulé et la trame est jetée. Si aucun ACK n'est reçu, le *timer* expire et la station considère que la destination n'a pas correctement reçu la trame et qu'une retransmission est nécessaire. Chaque relais potentiel choisit alors un nombre aléatoire de *slots* dans sa fenêtre de contention (CW) et commence la procédure de contention avec la source. On notera au passage que dans la première phase de contention entre les relais potentiels et la source, les relais ont une fenêtre de contention minimum tandis que la source a déjà doublé sa fenêtre de contention. Les relais potentiels sont donc privilégiés par rapport à la source mais ont les même chances entre eux de gagner la contention (en ce qui concerne la première retransmission). Si un des relais potentiels accède au canal avant la source (et avant les autres), il est maintenant responsable de la bonne réception de la trame par la destination. À ce titre il doit recommencer la procédure de retransmission jusqu'à ce qu'il atteigne le nombre maximum de transmissions ou qu'il reçoive lui-même un acquittement (voir section 4.2.2). Lorsqu'un relais retransmet la trame, il conserve les champs d'adresse source et destination mais modifie la valeur de la métrique dans l'entête par la sienne.

Une version modifiée de FBR appelée Biased-FBR (B-FBR) privilégie les meilleurs stations lors de la phase de contention. L'idée dans B-FBR est de donner de meilleures chances de gagner la contention aux stations ayant une meilleure métrique. B-FBR fonctionne en modifiant la façon dont le *backoff* est tiré par les relais potentiels. Dans B-FBR, la taille de la fenêtre de contention d'un relais potentiel est fonction de la métrique de la source avec la destination et est calculée suivant la formule 4.2 :

$$CW' = \left\lceil CW * \frac{Q_{source}^{destination}}{Q_{current}^{destination}} \right\rceil \tag{4.2}$$

Ainsi si la métrique d'un relais potentiel avec la destination est deux fois plus importante que celui de la source, la taille de sa fenêtre de contention avec B-FBR sera divisée par deux.

### 4.2.2 Mécanisme d'ACK




(a) Entête d'un ACK

(b) Entête modifié d'un ACK

Figure 4.3 – Modifications apportées à l'entête ACK pour supporter les ACK retardés

Dans IEEE 802.11, chaque trame envoyée en *unicast* doit être acquitté par la destination. Une destination (par exemple l'AP) qui reçoit une trame doit attendre un temps SIFS et renvoyer un accusé de réception (ACK) qui permet d'acquitter la source. Nous ne modifions pas ce comportement mais nous introduisons deux autres types d'acquittement que nous appelons acquittement passif et acquittement retardé représenté sur la figure 4.4.

Un **acquittement passif** correspond au cas où une station, ou un relais potentiel, entend la retransmission d'une trame actuellement gérée par la MAC et effectuée par une station ayant une meilleure métrique. Par exemple, quand la source envoie une trame et ne reçoit pas d'ACK de la part de la destination, elle va tenter de retransmettre sa trame. Si cette trame est retransmise par un relais avant la source, et que la source entend cette retransmission, elle peut considérer celle-ci comme un acquittement passif. Il en résulte que la source peut jeter cette trame de la file d'attente. En effet, cela indique que la trame a progressé vers la destination et le relais a dorénavant la responsabilité de faire progresser cette trame jusque la destination. Toutefois, si la source gagne la contention et prend en charge la retransmission à la place du relais, le relais ne doit pas acquitter cette trame en l'entendant car la source a une métrique plus faible que le relais. De la même façon parmi les relais potentiels, seuls ceux ayant une moins bonne métrique que celle de l'émetteur peuvent acquitter passivement la trame en entendant la retransmission. Cette approche est similaire au *custody transfer* [FHM03] dans les réseaux DTN car une station n'a pas besoin de recevoir un acquittement direct de la destination, savoir que la trame est gérée par une autre station est suffisant.

Cependant, il peut arriver que la source, ou un relais potentiel, n'entende pas une retransmission effectuée par un autre relais. Ce cas de figure est problématique car cela risque de créer des duplications et des retransmissions inutiles. Afin d'éviter cela, nous introduisons le concept d'**acquittement retardé** qui consiste pour une station source à accepter un ACK (si il lui est destiné) même si celui-ci est reçu bien après la période de SIFS suivant une transmission. Comme la retransmission d'une trame par les relais ne modifie pas les champs d'adresse source et destination, l'ACK

envoyé par l'AP sera toujours à destination de la source originelle de la trame. Ainsi si une station source ou un relais potentiel reçoit un ACK pour une trame en file d'attente, elle peut en déduire qu'un autre relais à retransmis avec succès cette trame. Cependant, comme on peut le voir sur 4.3a, l'entête d'un ACK contient un champ d'adresse utilisé pour identifier la station source mais n'inclut pas le numéro de séquence de la trame qu'elle acquitte. Or les acquittements passifs peuvent provoquer des désynchronisations entre la trame actuellement gérée par une station et celle tout juste reçue par la destination. Pour éviter qu'une station n'acquitte par erreur une trame de sa file d'attente, nous avons modifié l'entête de l'ACK de façon à intégrer le numéro de séquence de la trame acquittée. Nous pensons que cela n'affecte pas significativement le risque de collision dans les adresses car ce sont surtout les trois derniers octets de l'adresse MAC qui assurent l'entropie, les trois premiers octets identifiant le constructeur du matériel.

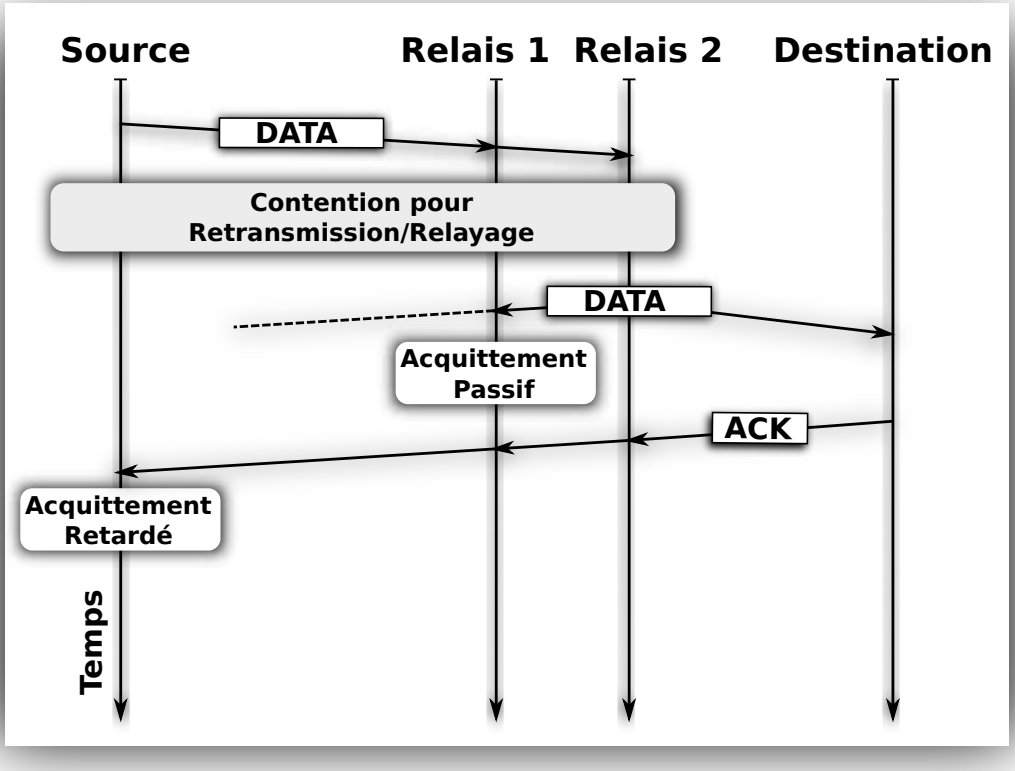



Figure 4.4 – Acquittement passif et acquittement retardé dans FBR

### 4.2.3 Gestion de la queue

Dans IEEE 802.11, chaque station gère une file d'attente pour ses trames de données nécessitant d'être envoyée sur le canal. Une trame entendue nécessitant une retransmission ne peut pas être placée à la fin de cette file d'attente car elle doit être traitée le plus rapidement possible si elle veut avoir une chance d'être retransmise par un relais potentiel. Cependant, si elle est placée en tête de la file d'attente, il est fort probable que cette station ne transmette jamais ses propres trames car elle sera constamment sollicitée pour retransmettre les trames d'une autre station. Nous avons donc introduit une deuxième file d'attente spécialement dédiée au relayage des trames d'une autre station.

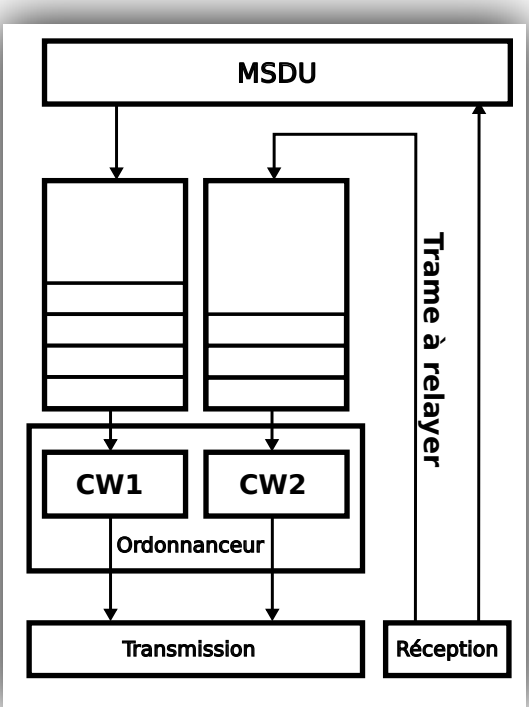



Figure 4.5 – Ajout d'une file d'attente pour FBR

Dans notre conception, chaque station maintient ainsi deux files d'attentes indépendantes, une pour ses propres trames et une autre pour les trames entendues nécessitant une retransmission. La figure 4.5 représente ces deux files d'attentes. Chaque file d'attente gère son propre *backoff* indépendamment de l'autre et gère également indépendamment sa fenêtre de contention (CW). Afin d'éviter les collisions entre les files d'attentes, l'ordonnanceur s'assure que les files d'attentes ne peuvent pas tirer le même *backoff*. Lorsque le canal est libre, le *backoff* de chaque file d'attente

est décrémenté en parallèle. En procédant ainsi, nous fournissons un mécanisme équitable qui minimise l'impact sur les données du relayeur tout en permettant aux relais potentiels d'être en compétition avec la source pour l'accès au canal.

### 4.2.4 Cas possibles

La figure 4.6 montre tous les scénarios possible si on considère une source souhaitant transmettre une trame vers la destination avec un relais FBR intermédiaire. Le même scénario s'applique dans le cas où il y a plusieurs relais car en fin de compte, seul un relais est sélectionné avec le mécanisme de contention. Les scénarios sont classifiés suivant $3$ états : L'état $A$ représente le cas où la source seule cherche à transmettre une trame. C'est le cas de la transmission initiale de la source, ou si une retransmission est nécessaire mais qu'aucun relais n'a reçu la première transmission. L'état $B$ représente le cas où la source et le relais sont en compétition pour retransmettre la trame initiale. C'est le cas lorsque la transmission initiale de la source a échouée mais que le relais l'a entendue. L'état $C$ représente le cas où le relais seule cherche à retransmettre la trame. C'est le cas lorsque la transmission par le relais à échouée à atteindre la destination mais à acquitté passivement la source. Les boîtes blanches ($A3$, $A8$, $A9$, $B1.3$, $B1.9$, $B2.2$, $B2.7$, $B2.8$, $C2$, $C7$, $C8$) représentent l'état finale, c'est-à-dire que le processus de transmission et de retransmission est terminé (la destination à reçu et a acquitté la trame, et la source et le relais n'essayent plus de retransmettre la trame). Étant un état, il existe plusieurs transition possibles correspondant à différents scénario. Par exemple, la transition $A1$ correspond à la source effectuant une transmission qui a échouée, dans ce cas on retourne dans l'état $A$ car la source va tenter une retransmission. La transition $A2$ correspond au cas de figure dans lequel la station source effectue une transmission qui échoue à atteindre la destination mais est entendu par le relais. Le prochain état est donc $B$ car la source et le relais essaieront de faire une retransmission.

Idéalement les transitions d'un état à un autre sont soit vers le même état, soit vers l'état *suivant*, (par exemple depuis $A$ vers $B$) c'est-à-dire que la trame progresse vers la destination. Les cas de figure $B1.5$, $B1.7$ et $B2.4$ sont problématiques car ils retournent à l'état $A$ et donc signifie qu'on est revenu «en arrière». Dans les deux cas de figure $B1.5$ et $B1.7$, la source et le relais veulent retransmettre la trame mais la source gagne la contention et retransmet la trame. Dans les deux cas, la destination a reçu la trame et envoie un ACK qui n'est reçu que par le relais. Ainsi, le relais jette la trame de sa file d'attente car il considère qu'il n'y a plus de retransmission nécessaire, cependant la source va essayer de retransmettre. Ces deux cas de figures

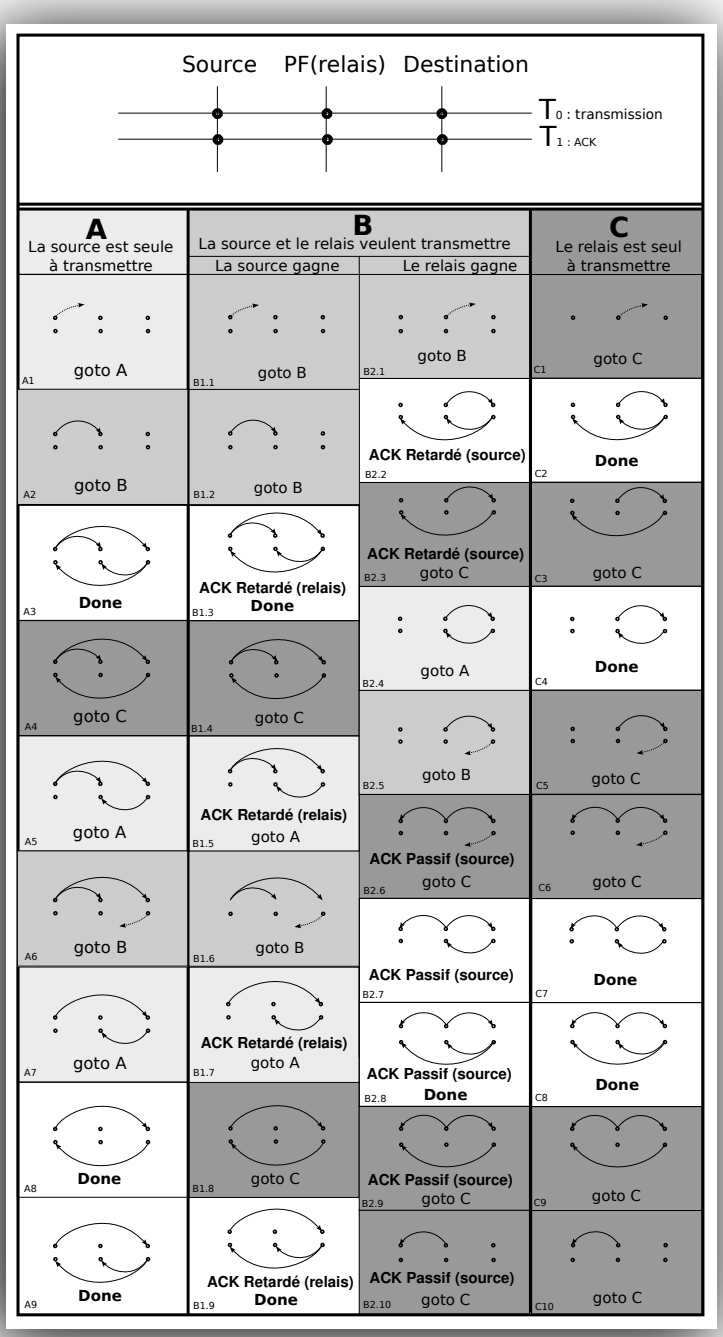



Figure 4.6 – Scénarios pour transmettre les données avec une source et un relais

sont assez rare car les accusés de réception sont des trames de petites tailles envoyés à un débit plus faible et donc moins sujet aux pertes et n'est certainement pas lié à notre algorithme. Dans $B2.4$, le relais et la source veulent retransmettre mais le relais gagne la contention et retransmet la trame qui est immédiatement acquittée par la

destination. Dans ce cas de figure, et de façon similaire aux deux précédents, seul le relais reçoit l'ACK et la source sera seule à retransmettre. Notons qu'ici la source n'a pas reçue non plus la retransmission effectuée par le relais. Ce cas de figure est également rare et ne provoquera qu'une seule retransmission inutile.

Dans les états $B1.\{3, 5, 7, 9\}$ et $B2.\{2, 3\}$, nous pouvons voir la présence d'un *ACK retardé* qui correspond à la réception d'un ACK suivant une retransmission effectuée par une autre station. Dans les états $B2.\{6, 10\}$, nous pouvons voir la présence d'un acquittement passif (ACK Passif) qui correspond au fait d'entendre la retransmission effectuée par une autre station d'une trame en file d'attente. Par exemple, dans l'état $B2.6$, le relais retransmet la trame et la source initiale considère cette retransmission comme un acquittement pour la trame qu'elle a transmise précédemment malgré qu'elle n'ait pas reçue d'ACK. Dans ce cas, la responsabilité de la transmission est délégué au relais. Nous détaillerons ces deux mécanismes d'acquittement dans la section 4.2.2.

## 4.3 Évaluation et Résultats

### 4.3.1 Implémentation dans NS-2

Network Simulator version 2 (NS-2) est un simulateur de réseau open source écrit en TCL et C++. Nous avons basé notre implémentation sur le module 802.11Ext qui est une implémentations du standard IEEE 802.11g de l'université de Karlsruhe [CSEJ+07]. Le module 802.11Ext fournis deux sous-modules appelé mac-802.11Ext et phy-802.11Ext. Nous avons modifié le module mac-802.11Ext pour implémenter notre solution FBR et avons amélioré la couche physique en implémentant un modèle plus réaliste du Packet Error Rate (PER) basé sur un échantillonnage des valeurs de Bit Error Rate (BER) trouvé dans la littérature.

Le module 802.11Ext est composé de plusieurs sous-modules, chacun coordinant des aspects internes des mécanismes de la MAC. Ces sous-modules sont les suivants :

- *Channel State Manager* Ce sous-module est responsable de maintenir l'état du canal physique et virtuel (NAV) pour le mécanisme IEEE 802.11 CSMA/CA
- *Reception Coordination (RxC)* Ce sous-module reçoit de la couche basse les trames de contrôle et de données adressées à cette station. Elle envoie un signal

au sous-module TxC lorsque des trames CTS et ACK arrivent. Elle est responsable d'envoyer les trames CTS et ACK lorsqu'une trame RTS ou de données arrive. Elle est également responsable de désencapsuler les trames de données avant de les passer à la couche supérieure.

- *Transmission Coordination (TxC)* Ce sous-module gère les accès au canal pour les trames arrivant de la couche supérieure.
- *Backoff Manager* Ce sous-module assiste le sous-module TxC dans la transmission des trames. Il maintient le compteur du *backoff* pour supporter le mécanisme de contention de IEEE 802.11.

Nous n'avons laissé le *Channel State Manager* en l'état et avons modifié Reception Coordination (RxC), Transmission Coordination (TxC) ainsi que le *backoff manager*.

#### 4.3.1.1 Modification du sous-module RxC

La figure 4.7 montre la modification apportée au sous-module RxC, le sous-module responsable de gérer les trames reçues ou entendues par la station. L'état *RXC_IDLE* correspond à l'état de repos, c'est-à-dire qu'aucune trame n'est traitée par ce sous-module. De cet état, le sous-module peut recevoir des trames de données, ACK, RTS ou CTS. Nous avons implémenté des fonctions supplémentaires pour le cas où une trame reçue est une trame de données et que l'adresse de destination ne correspond pas à l'adresse MAC de la station. Nous vérifions d'abord si cette trame reçue est une trame que la station a en file d'attente. Si c'est le cas, et que la trame reçue a été émise par une meilleure station (au sens du RSSI), nous supprimons cette trame de la file d'attente (ACK Passif). Sinon cette trame pourrait éventuellement nécessiter une retransmission. La station réceptrice vérifie si elle est un relais potentiel pour la station émettrice (*i.e.* si elle a plus de chance de transmettre cette trame vers la destination que la source), prépare la trame en conséquence si tel est le cas et attend de recevoir l'éventuel ACK (état *TXC WaitACKRelay*).

#### 4.3.1.2 Modification du sous-module TxC

La figure 4.8 montre les modifications apportées au sous-module TxC, le module responsable de traiter les trames devant être transmises par la station. Cette figure ne représente que la partie liée à FBR et commence avec l'état *TXC WaitACKRelay*. Cet état signifie que la station a entendu une trame de données unicast transmise

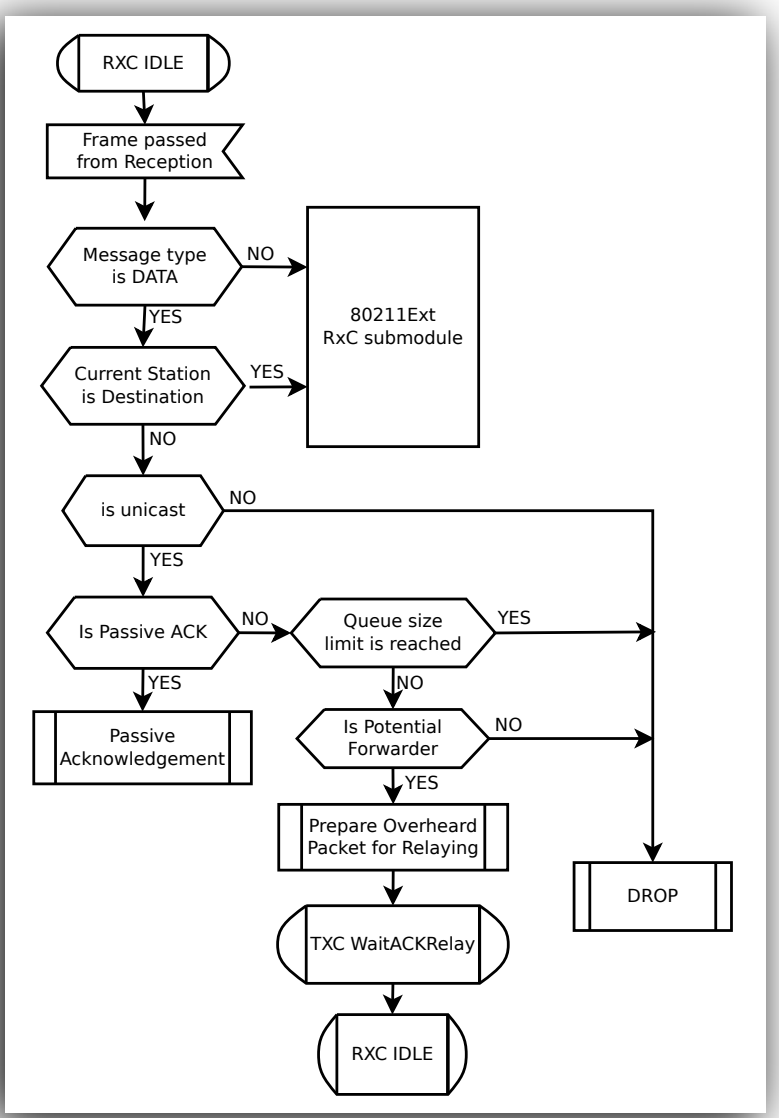



Figure 4.7 – Modifications apportées au sous-module RxC

par une station avec un RSSI moins bon que cette station. Si l'ACK est reçu avant l'expiration du *timer*, aucune retransmission n'est nécessaire et la trame est jetée. Si le *timer* expire, une retransmission est nécessaire et la station commence une procédure de *backoff* pour retransmettre la trame (état *RELAY PENDING*), deux issues sont alors possibles. Si la station reçoit un acquittement passif (voir section 4.2.2), le *backoff* est annulé et la trame supprimée. Sinon, le *backoff* termine et la station retransmet la trame, et attend une fois de plus un ACK (état *WaitACKRelay*). La station doit retransmettre cette trame autant de fois que nécessaire, c'est-à-dire jusqu'à ce

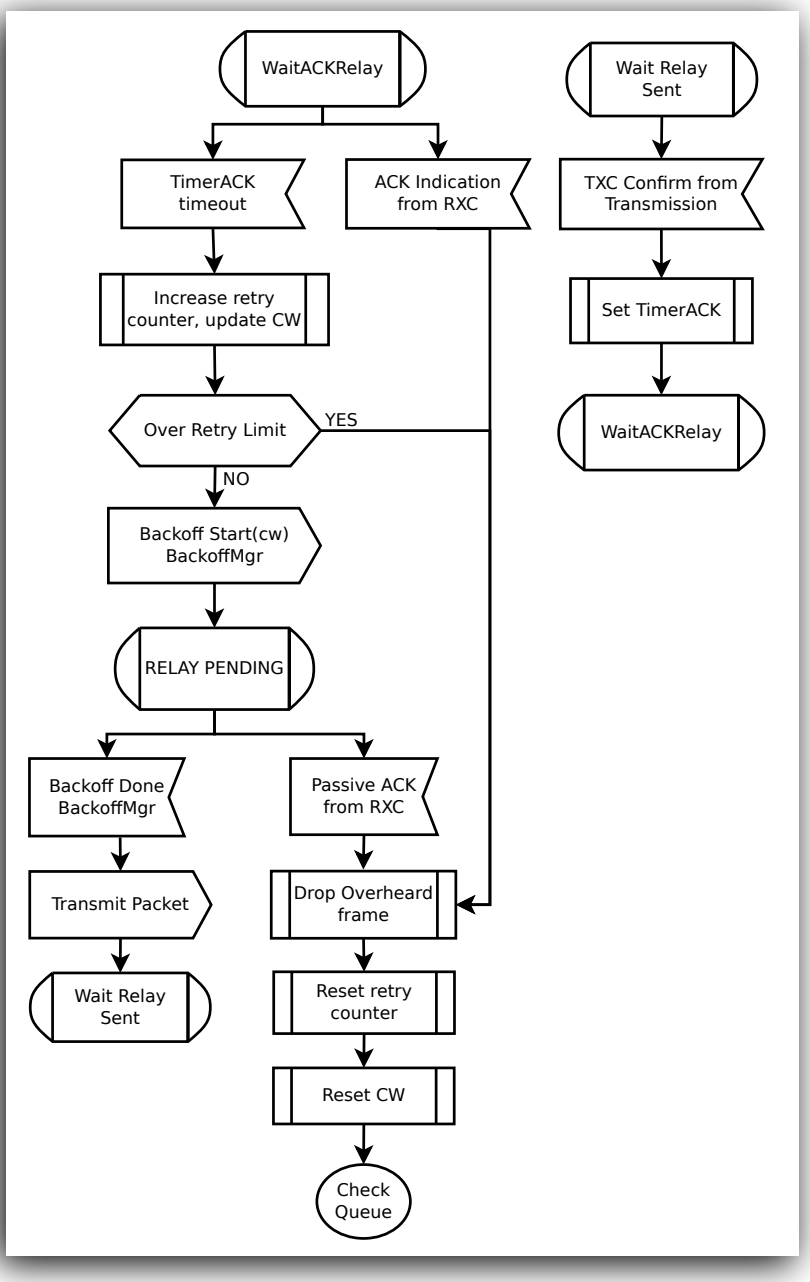



Figure 4.8 – Modifications apportés au sous-module TxC

qu'elle reçoive un acquitement (passif ou avec un ACK) ou s'il atteint le nombre maximum de retransmissions.

#### 4.3.1.3 Backoff

Nous avons modifié le sous-module de gestion du *backoff* afin de gérer deux *backoff* indépendants comme indiqué section 4.2.3. Chacun des deux *backoff* manipule sa propre fenêtre de contention et choisit un nombre aléatoire de *slots* en s'assurant qu'il n'y a pas de collision interne. Si durant le tirage du *backoff*, une des files d'attente choisie le même nombre de slot que l'autre file d'attente, une nouveau lancé est effectué, jusqu'à ce qu'un slot différent soit tiré.

#### 4.3.1.4 Métrique

Nous avons décidé d'utiliser le RSSI comme discriminant car des études ont montré une forte corrélation entre le taux de réception (PER) et le SNR [HHSW10]. De plus, la détermination du RSSI peut être obtenu instantanément donnant une information immédiate de la qualité du lien. Dans le simulateur, nous avons utilisé la valeur du SNR précédemment implémenté (voir section 2.5.1)

### 4.3.2 Impact du relayage FBR pour une source

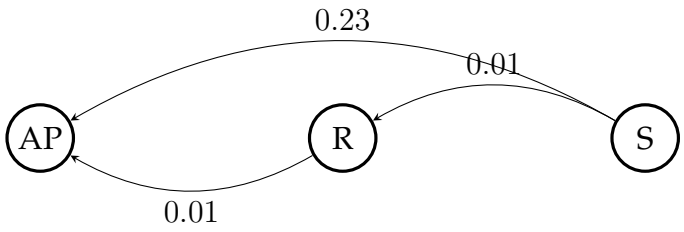



Figure 4.9 – Scénario dans lequel la source $S$ envoie du trafic vers l'$AP$, éventuellement retransmis avec FBR par le relais $R$. Chaque lien est labellisé avec son PER.

Le premier scénario tel que représenté sur la figure 4.9 est constitué d'un AP, d'une station source envoyant du traffic vers l'AP et d'un relais FBR entre les deux. La source est située à une certaine distance de l'AP de telle façon que son PER soit de $23\%$. Cela signifie que sur $100$ trames envoyées, $23$ ne seront pas reçues par le points d'accès et nécessiteront une retransmission. La station relais est placée entre la station source et l'AP de telle façon qu'elle ait un PER inférieur à $0.01\%$ avec les deux. Nous avons effectué deux séries de simulation, une première avec le mécanisme FBR désactivé et une deuxième avec FBR activé. Dans les deux cas, la source envoie du trafic Constant Bit Rate (CBR) à l'AP au débit maximal afin de saturer le canal.

| MAC/802.11Ext | | PHY/802.11Ext | |
|---|---|---|---|
| **Paramètre** | **Valeur** | **Paramètre** | **Valeur** |
| CWMin | 15 | CSThresh | $6.30957e-13$ |
| CWMax | 1023 | Pt | 0.001 |
| SlotTime | 0.000009 | freq | $5.18e9$ |
| SIFS | 0.000016 | noise floor | $2.51189e-13$ |
| ShortRetryLimit | 0 | L | 1.0 |
| LongRetryLimit | 0 | PowerMonitorThresh | 0 |
| HeaderDuration | 0.000020 | HeaderDuration | 0.000020 |
| SymbolDuration | 0.000004 | PreambleCaptureSwitch | 1 |
| BasicModulationScheme | 0 | DataCaptureSwitch | 0 |
| RTSThreshold | 2000 | SINR PreambleCapture | 2.5118 |
| CSThresh | $6.30957e-13$ | SINR DataCapture | 100.0 |
| datarate | 36 Mbps | dist | $1e6$ |
| **Autres paramètres** | | | |
| (relais) FBR queue size | | 1 | |
| (source) CBR packet size | | 1042 octets | |
| (source) CBR rate | | 30 Mbps | |
| temps de simulation | | 100 secondes | |

Tableau 4.1 – Paramètre de simulation

La figure 4.9 représente schématiquement ce scénario. Nous avons effectué des simulations pour valider l'implémentation et montrer que FBR améliore le standard IEEE 802.11. Les simulations ont été effectuées sous NS-2 avec le module 802.11Ext et l'implémentation décrite précédemment. Le tableau 4.1 indique les paramètres utilisés pour la simulation. Nous avons configuré la taille de la file d'attente pour les trames à retransmettre à 1. Le débit de transmission étant de 36 Mbps, un CBR de 30 Mbps permet de saturer le canal sans-fil à cause de la taille des entêtes et des temps de contention.

#### 4.3.2.1 Comportement de la source en présence d'un relais FBR

Dans un premier temps, nous nous intéressons au comportement de la source sans et avec FBR activé. Pour cela, nous avons généré à partir des logs de NS-2 les diagrammes de transition de la source représentés sur les figures 4.10 et 4.11. Ces diagrammes représentent les probabilités de transition entre les états de la source lorsqu'elle essaye de transmettre une trame vers l'AP. Les tableaux 4.2 explique la signification des états et des transitions.

| État | Signification |
|---|---|
| IDLE | La source n'est pas ou plus dans un processus de transmission/retransmission d'une trame |
| WAIT_RX_ACK | La source attend un ACK pour le premier essai de transmission qu'elle vient d'effectuer |
| WAIT_RX_ACK_RETRY(_$i$) | La source attend un ACK pour la ($i$ème) **retransmission** qu'elle vient d'effectuer |

| Transition | Signification |
|---|---|
| TX | Transmission d'une nouvelle trame, elle va de l'état *IDLE* vers *WAIT_RX_ACK*. La source à transmis une trame à l'AP (Tx) et attend maintenant un ACK de l'AP. |
| RX_ACK | Cette transition signifie que la station a reçu un ACK envoyé par l'AP pour acquitter la trame. Les retransmissions ne sont plus nécessaires pour cette trame et la station peut retourner à l'état *IDLE*. |
| TX_RETRY | Le *timer* a expiré et une retransmission a été effectuée, la station est maintenant en attente d'un ACK. |
| RETRY_LIMIT | Le nombre maximal de retransmissions a été atteint, la trame est détruite et la station retourne à l'état *IDLE*. |
| RX_DELAYED_ACK | Uniquement dans le mode FBR, un acquittement passif ou retardé a été entendu. |

Tableau 4.2 – Tableau des états et transitions possibles pour les diagrammes de transitions

Chaque diagramme indique en bleu pour chaque état la probabilité d'emprunter une transition sortante. Par exemple, on remarque que dans les deux cas (avec et sans FBR),la probabilité de succès de transmission d'une trame au premier essai est de $77\%$, ce qui est attendu puisque le PER est de $23\%$. Par ailleurs, sans FBR, on remarque que pour chaque nouvelle retransmission, la source a toujours entre $25$ et $30\%$ de chance de devoir retransmettre sa trame avec la transition *TX_RETRY*. Il en résulte que la source passe beaucoup de temps à retransmettre et atteint même plusieurs fois la limite maximale de retransmission (la transition *RETRY_LIMIT*). Avec FBR, la probabilité d'échec de la retransmission diminue à chaque retransmission passant successivement de $0,11$ à $0,04$ puis $0,03$. Elle n'est que de $0.11$ pour

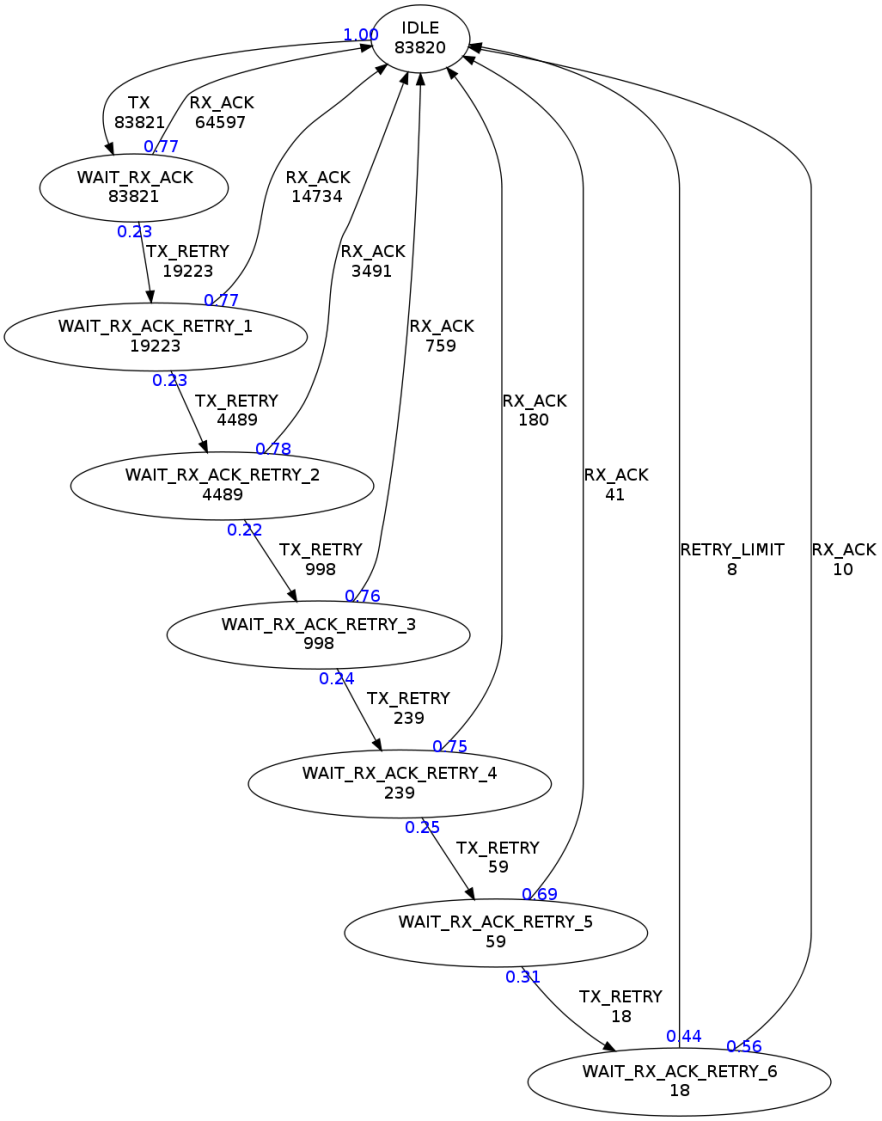



Figure 4.10 – Probabilité de transition sans FBR

la première retransmission (contre $0.23$ sans FBR) car le relais prend déjà en charge une partie des retransmissions. Cette probabilité diminue ensuite car chaque fois que la source doit retransmettre une trame elle double sa fenêtre de contention CW, donnant plus de chance au relais de retransmettre la trame. Ainsi, plus la source retransmet, plus le relais a de chance de gagner la contention et de retransmettre la trame, acquittant passivement la source du même coup.

Si on se concentre uniquement sur les trames nécessitant une retransmission (car c'est sur ce point qu'agit FBR), on voit que sans FBR, on a un surplus de $30\%$ de retransmissions inutiles. C'est-à-dire que pour $100$ trames nécessitant une retransmission $130$ seront nécessaires au total. Ce surplus n'est plus que de $12\%$ avec FBR ce qui signifie que nous réduisons les retransmissions inutiles de $60\%$. Si le relais

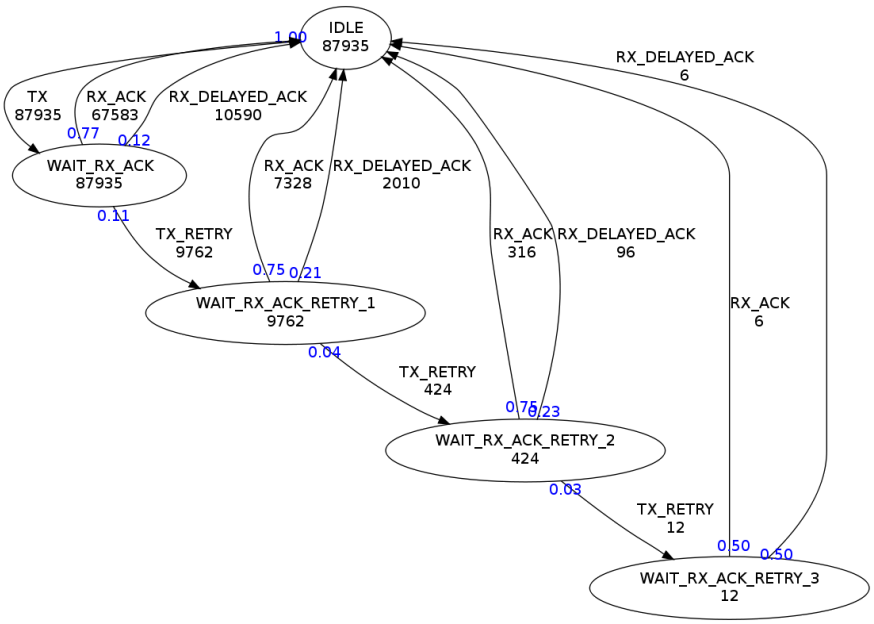



Figure 4.11 – Probabilité de transition avec FBR

gagnait chaque contention, une seule retransmission serait nécessaire pour chaque trame non acquittée ce qui aurait atteint $100\%$ de réduction (car le relais ne perd pas de trame). Le relais ne gagne pas tous les accès au canal mais est légèrement avantagé par rapport à la source car sa fenêtre de contention est plus petite.

De plus, en diminuant le nombre de retransmissions, cela crée plus d'opportunités pour la source pour envoyer plus de données. En effet, moins de retransmissions implique que la fenêtre de contention sera en moyenne plus petite, réduisant de fait la durée du *backoff*. En conséquence, la source attend moins longtemps et gagne la contention plus souvent et envoie donc plus de données, atteignant le débit de $7.03$ Mbps avec FBR contre $6.7$ Mbps sans FBR.

#### 4.3.2.2 Efficacité de FBR en fonction du PER

La figure 4.12 représente le nombre de trames (uniques) correctement reçues par l'AP (axe $y$) en fonction du PER entre la source et l'AP. Avec 802.11, on voit que plus la station s'éloigne, moins l'AP reçoit les trames, le nombre de retransmission augmentant proportionnellement avec le PER. En forçant un saut de routage via le relais, on voit qu'il n'est pas intéressant de l'utiliser tant que le PER est inférieur à $50\%$. Cela est de au fait qu'un saut de routage divise la bande passante par deux car chaque trame doit être transmise deux fois. Lorsque le PER est supérieur à $50\%$, il devient intéressant de relayer les trames car une transmission directe depuis la

source nécessite en moyenne plus de deux transmissions par trame. Avec le mécanisme FBR activé, on peut voir que les performances sont améliorées car le relais ne retransmet les trames que lorsque c'est nécessaire. Même avec un PER allant au delà de $50\%$, les performances sont tout de même améliorées car FBR permet de tirer parti des transmissions de la source réussies. Cependant, passé 80% de perte, FBR devient moins intéressant qu'un relayage traditionnel car le relais FBR ne gagne pas chaque contention pour la retransmission. En augmentant la probabilité du relais à gagner la contention, B-FBR permet d'atteindre une performance quasi-optimale en offrant de meilleurs résultats que le relayage traditionnel.

Ce simple scénario montre que FBR s'adapte automatiquement aux conditions du lien de l'émetteur. Sans échange de trame de contrôle, une troisième station (le relais dans notre cas) peut aider la source à retransmettre une trame seulement si cela est nécessaire, c'est-à-dire que la destination ne l'a pas correctement reçue. Ainsi FBR peut adapter dynamiquement la topologie du réseau en fonction des conditions radio. Ce mécanisme surpasse à la fois 802.11 seul et les mécanismes de routage traditionnels.

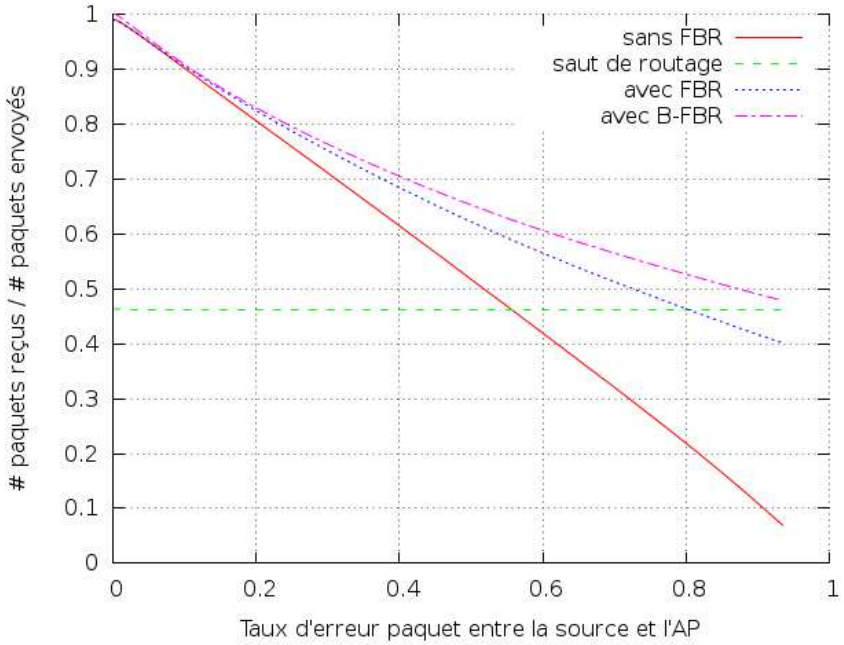



Figure 4.12 – Proportion de trames uniques reçues avec 802.11 seul (sans FBR), un saut de routage, FBR et B-FBR

#### 4.3.2.3 Impact du relayage en fonction des débits

Nous reprenons le scénario précédant en faisant cette fois varier le débit de la source. La source est placée à un emplacement de telle sorte que son PER au débit 48Mbps soit de 10% tandis que son PER pour le débit 54 Mbps est de 90% (comme on peut le voir sur la figure 2.29d, les PER chutent rapidement avec la distance). Nous avons comparé ici FBR avec le cas où il n'y a pas de relayage (IEEE 802.11) et le cas où on force le relayage par le relais. Les tableaux 4.3 et 4.4 donnent les résultats de simulation en terme de nombre de trame reçues et envoyées dans les différents cas de figure.

| **48 Mbps** | Nb trames envoyées par la Source | Nb trames retransmises par le Relais | Nb trames reçues par l'AP de la source | Nb trames reçues par l'AP du relais |
|---|---|---|---|---|
| IEEE 802.11 | 238508(unique) + 29042(dup) = **267550** | 0 | **238507** | 0 |
| FBR | 239929(unique) + 14677(dup) = **254606** | **17801** | **226473** | **15413** |
| Saut de routage | 153003(unique) + 19084(dup) = **172087** | 132105(unique) + 24314(dup) = **156419** | 0 | **132104** |

Tableau 4.3 – Nombre de trames uniques reçues par la source pour un CBR de 48 Mbps

| **54 Mbps** | Nb trames envoyées par la Source | Nb trames retransmises par le Relais | Nb trames reçues par l'AP de la source | Nb trames reçues par l'AP du relais |
|---|---|---|---|---|
| IEEE 802.11 | 16418(unique) + 64285(dup) = **70703** | 0 | **9800** | 0 |
| FBR | 106885(unique) + 57143(dup) = **164028** | **95876** | **19354** | **87706** |
| Saut de routage | 152652(unique) + 19296(dup) = **171948** | 132499(unique) + 24433(dup) = **156932** | 0 | **132499** |

Tableau 4.4 – Nombre de trames uniques reçues par la source pour un CBR de 54 Mbps

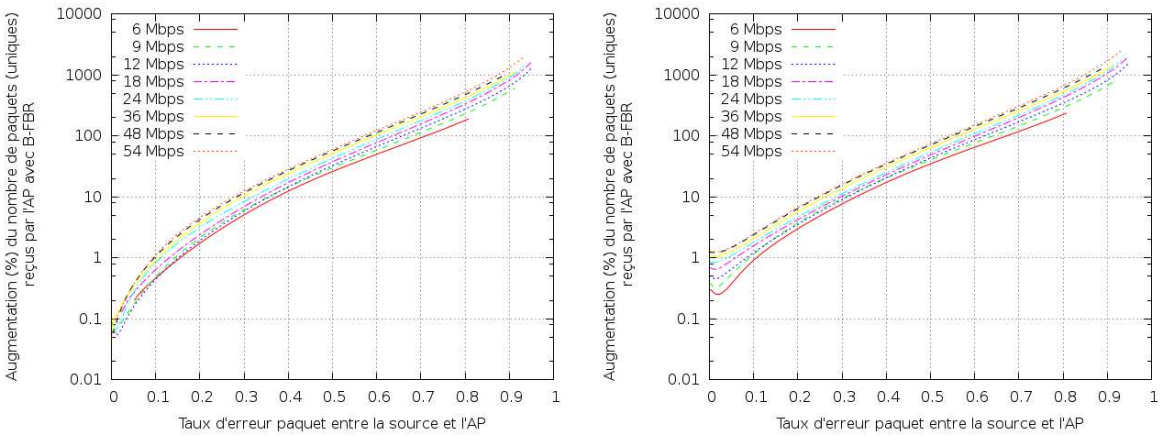
Pour le cas à 48 Mbps, on remarque que faire du relayage opportuniste permet d'optimiser les cas où une retransmission est nécessaire, ce qui représente un peu plus de 10% des transmissions de la source. Dans le cas sans relayage (IEEE 802.11), ces 10% sont tous retransmis par la source car FBR est désactivé. L'AP a ainsi correctement reçu **238507** trames de la source. Avec FBR d'activé à 48 Mbps, parmi ces 10% de trames nécessitant une retransmission, 57% sont retransmis avec succès par le relais. Ces retransmissions effectuées par le relais sont moins sujettes à des pertes et ceci explique l'amélioration par rapport au premier scénario puisque l'AP a reçu correctement un total de $\mathbf{226473} + \mathbf{15413}$ soit **241886** trames. Comme précédemment, le relais n'a pas pris pas en charge toutes les retransmissions, car il est en compétition avec la source pour la retransmission. Le taux de retransmissions est légèrement supérieur pour le relais (57%) car sa fenêtre de contention est plus petite. Dans le troisième scénario, on force le passage par le relais même si la trame a été reçu par la destination, ce qui arrive pourtant dans 90% des cas. On obtient donc de moins bonnes performances que dans les premier et deuxième scénarios puisqu'on multiplie pratiquement par deux le nombre de transmissions pour chaque trame.

Dans le cas à 54 Mbps, seulement 12% des transmissions de la source sont correctement reçues par l'AP. Dans le scénario sans relayage (IEEE 802.11), chaque retransmission est effectuée par la source, ce qui provoque de très nombreuses retransmissions. Comme la fenêtre de contention (CW) est doublée à chaque retransmission (avec un maximum de 7 retransmissions), le nombre de trames envoyées et reçues par l'AP est aussi faible. Le cas avec FBR activé améliore nettement les résultats puisque parmi les 88% de trames nécessitant une retransmission, 64% seront effectués par le relais, laissant la source retransmettre (pratiquement inutilement) dans 37%.

Ces deux cas de figure illustrent bien le problème de la sélection du relais. Le relayage n'est pas tout le temps nécessaire, et lorsqu'il l'est la difficulté est de choisir le bon relayeur entre la source et le relais. Idéalement, le relais devrait gagner la contention à chaque fois que le besoin de relayer existe. On observe cependant que notre algorithme adapte automatiquement la prise en charge des retransmissions par le relais en fonction de la qualité de lien de la source avec l'AP. Dans le cas à 48 Mbps, la part du relais sur les trames à retransmettre est de 57% alors qu'elle est de 64% dans le cas à 54 Mbps. Ceci s'explique par le fait que chaque fois que la source échoue une transmission (ou une retransmission), elle augmente sa fenêtre de contention (CW). Dans les deux cas la CW de la source est plus importante que celle du relais, ce qui donne au relais plus de chance de gagner la contention. Cependant, la CW dans le cas à 54 Mbps est souvent plus importante que dans le cas

à 48 Mbps car pratiquement aucune des retransmissions faites par la source ne sont correctement reçues par l'AP. En effet, le nombre moyen de retransmissions par la source dans le cas à 48 Mbps est de 1.12 contre 1.53 dans le cas à 54 Mbps. Il en résulte que FBR adapte automatiquement la charge de retransmission sur le meilleur relais grâce à l'augmentation de la fenêtre de contention des mauvaises stations.

Nous étendons maintenant le scénario précédent en faisant varier le débit utilisé par la source (6, 9, 12, 18, 24, 36, 48, 54) et en faisant également varier le PER entre la source et l'AP de 0 à 1. Le relais est fixe et placé dans toutes les simulations à une distance lui permettant d'obtenir un PER de 90%. Nous allons pour tous les scénarios calculer le nombre de trames (uniques) reçus par l'AP durant les 50 secondes de simulation avec et sans FBR activé. Le graphique 4.13a montre le pourcentage d'amélioration entre le cas sans relayage (mode de fonctionnement normal de 802.11) et avec FBR d'activé. Le graphique 4.13b montre le pourcentage d'amélioration entre le cas sans relayage et avec B-FBR activé. Dans les deux graphiques, l'échelle de l'ordonnée est logarithmique




(a) bénéfices apportés par FBR

(b) bénéfices apportés par B-FBR

Figure 4.13 – Bénéfices en pourcentage apportés par les protocoles FBR et B-FBR

Ce qu'on observe dans un premier temps sur ces deux figures est que les courbes n'augmentent pas de la même façon en fonction du débit. Ceci s'explique par que le fait que plus le débit est élevé, plus le temps « libre » sera utilisé efficacement. Le relayage opportuniste permet effectivement d'économiser des retransmissions pour la source. Cette économie permet de mieux profiter du canal de deux façons : d'abord sur le temps des retransmissions eux-mêmes, mais également sur le *backoff* car moins de retransmissions implique moins de temps d'attente. Le temps de retransmission gagné ne suffit pas seul à expliquer ces différences de performance entre les débits, car étant donné un certain débit, pour une retransmission économi-

sée on ne peut transmettre qu'une seule trame. En revanche l'économie faite sur le *backoff* étant un temps indépendant du débit de transmission, un débit plus élevé le réutilisera mieux. Concernant la figure 4.13a la deuxième chose qu'on observe est que le relais semble offrir de l'intérêt uniquement à partir d'un PER de 10%.

On remarque que B-FBR donne de meilleurs résultats que FBR dans toutes les situations. Cela est du au fait que B-FBR donne un avantage au relais et ce dès la première transmission. Bien que B-FBR surpasse FBR dans toutes les situations, cette amélioration est plus marquée pour un PER faible que pour un PER élevé. Comme on l'a remarqué précédemment, FBR s'adapte déjà automatiquement de façon à privilégier le relais lorsque le PER est élevé du aux échecs de retransmission de la source qui double sa fenêtre de contention.

### 4.3.3 Comportement de FBR avec 6 stations

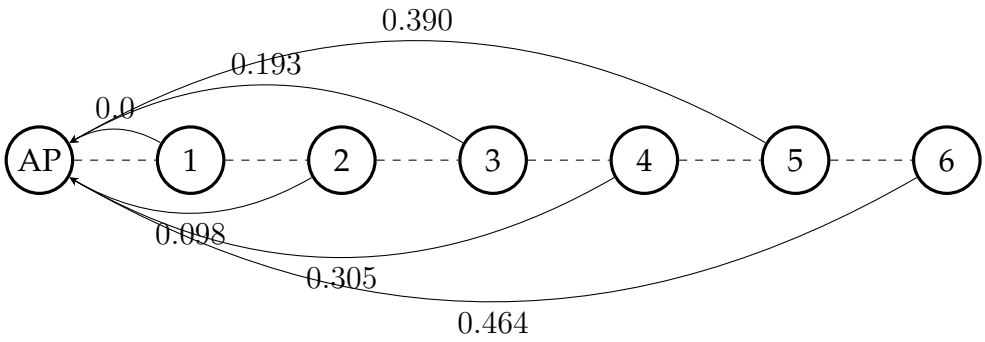



Figure 4.14 – Scénario dans lequel chaque station est une source vers l'AP. Les liens sont labellisés avec leurs PER.

| | Case 1 | | | Case 2 | | | Case 3 | | |
|---|---|---|---|---|---|---|---|---|---|
| | Dist. | PER | FBR | Dist. | PER | FBR | Dist. | PER | FBR |
| STA1 | 400 | 0 | x | 400 | 0 | x | 400 | 0 | ✓ |
| STA2 | 400 | 0 | x | 500 | 0.098 | x | 500 | 0.098 | ✓ |
| STA3 | 400 | 0 | x | 521 | 0.193 | x | 521 | 0.193 | ✓ |
| STA4 | 400 | 0 | x | 533 | 0.305 | x | 533 | 0.305 | ✓ |
| STA5 | 400 | 0 | x | 539 | 0.390 | x | 539 | 0.390 | ✓ |
| STA6 | 400 | 0 | x | 545 | 0.464 | x | 545 | 0.464 | ✓ |

Tableau 4.5 – Placement des stations pour le scénario où 6 stations envoient du trafic.

Dans ce scénario, nous avons configuré six stations, chacune étant la source d'un trafic CBR. Nous avons testé différents débits pour le CBR, de 64 kbps à 2048 kbps, en doublant cette valeur pour chaque expérimentation. Ces débits correspondent au débit utile au niveau applicatif, mais les entêtes des couches basses impliquent une

plus grande consommation de bande passante. Nous avons testé trois cas de figure comme indiqué dans le tableau 4.5. Dans le premier cas de figure, les six stations sont situées près de l'AP avec un PER de 0. Cela sert d'expérience témoin afin de voir comment les stations peuvent se partager la bande passante sans perte et sans mécanisme FBR. Dans le deuxième cas de figure, les 6 stations sont alignées avec l'AP, les valeurs de PER sont données dans le tableau 4.5. Le mécanisme FBR est désactivé pour ce deuxième scénario. Le troisième scénario a une topologie identique au deuxième scénario mais toutes les stations activent le mode FBR et peuvent donc être sollicitées pour retransmettre certaines trames.

Les paramètres de simulations sont les mêmes que dans le scénario précédent (voir 4.1) excepté pour le débit CBR qui est devenu ici un paramètre des scénarios. Nous avons choisi de conserver une taille de file d'attente CBR de 1 afin de ne pas inclure de biais lié à la gestion des files d'attente. Ainsi, si une station entend une trame nécessitant une retransmission mais que cette station est déjà en train de participer à un relayage, elle ignore cette réception.

#### 4.3.3.1 Impact de FBR sur la réception des trames auprès de l'AP

Les figures 4.15 montrent les résultats pour les débits applicatifs de 64 kbps à 2048 kbps. Chaque barre représente le pourcentage de trames reçues par l'AP pour une station source. Le cas 1 ne présente qu'une seule barre (sur la gauche des figures) car toutes les stations sont situées au même endroit et envoient le même nombre de trames à l'AP. Nous avons utilisé cette valeur comme une valeur de référence, c'est pourquoi le cas 1 atteint toujours 100%, les cas 2 et 3 étant normalisés par rapport au cas 1. Les résultats du cas 2 sont donnés par les six barres au milieu des figures (une barre par station). Chaque barre est composée de deux parties. La première partie (en vert sur les figures) représente le pourcentage de trames ayant correctement été reçues par l'AP dès la première transmission. Le reste est la proportion de trames ayant nécessité au moins une retransmission (qui ont été effectuées par la station elle-même puisque FBR est désactivé dans le cas 2). Les résultats du cas 3 sont représentés de façon similaire par les six barres à droite des figures. Chaque barre est constituée de plusieurs parties. Comme pour le cas 2, la première partie représente la proportion des trames ayant été reçues directement par l'AP dès la première transmission. Les autres parties correspondent aux contributions des autres stations dans la procédure de retransmission. Le tableau 4.6 donne le nombre moyen de transmission pour chaque trame de donnée pour les deux scénarios 512 kbps et 2048 kbps (1 signifie que la trame a été correctement reçue par l'AP à la première transmission).

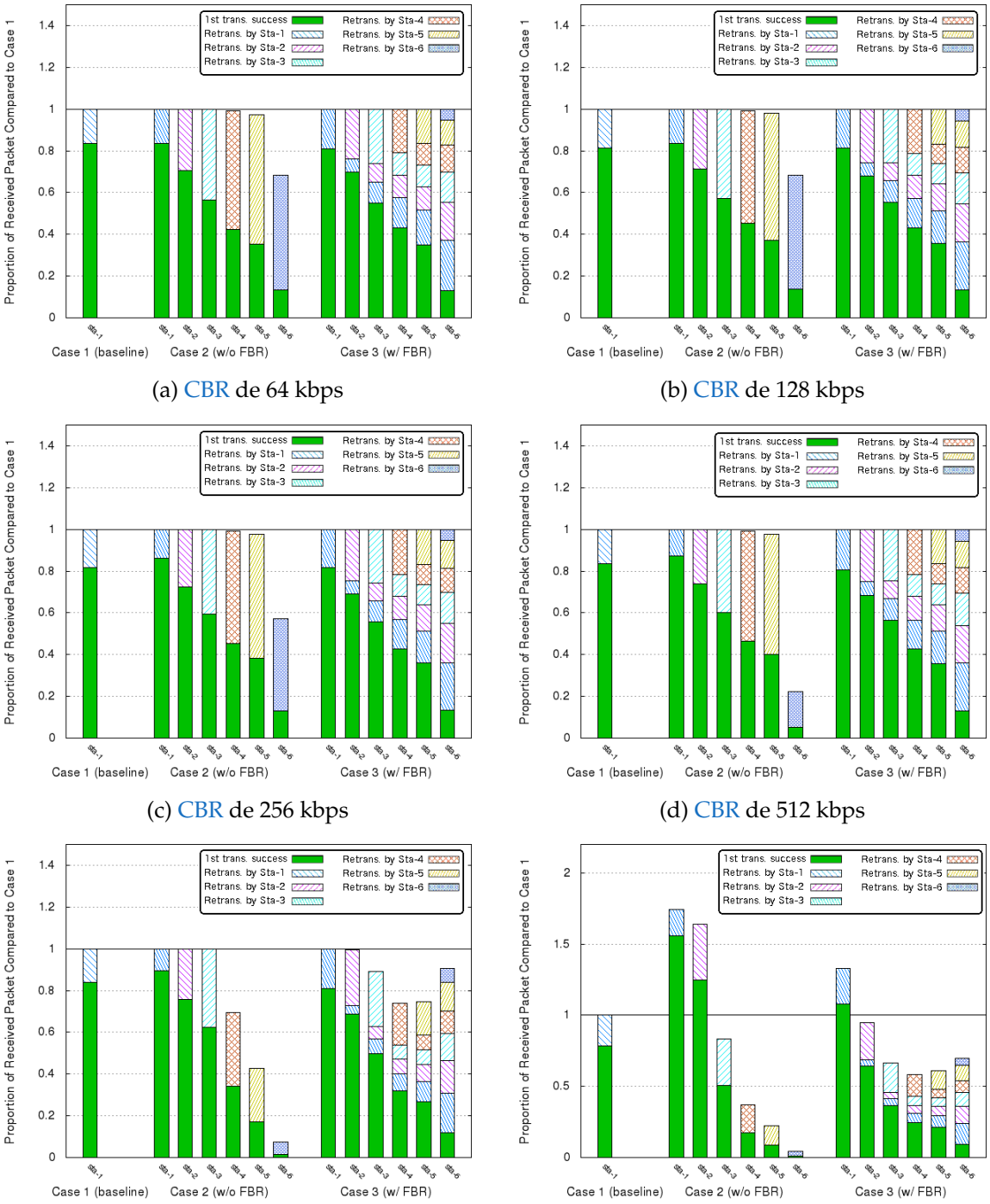
| | CBR 64 kbps | | CBR 128 kbps | | CBR 256 kbps | | CBR at 512kbps | | CBR at 1024 kbps | | CBR 2048kbps | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Case 2 | Case 3 | Case 2 | Case 3 | Case 2 | Case 3 | Case 2 | Case 3 | Case 2 | Case 3 | Case 2 | Case 3 |
| STA1 | 1.18 | 1.20 | 1.17 | 1.20 | 1.14 | 1.20 | 1.13 | 1.21 | 1.11 | 1.23 | 1.11 | 1.23 |
| STA2 | 1.37 | 1.37 | 1.35 | 1.39 | 1.34 | 1.38 | 1.32 | 1.39 | 1.31 | 1.44 | 1.32 | 1.46 |
| STA3 | 1.66 | 1.65 | 1.66 | 1.64 | 1.61 | 1.63 | 1.61 | 1.63 | 1.58 | 1.72 | 1.65 | 1.77 |
| STA4 | 2.11 | 1.92 | 2.08 | 1.93 | 2.07 | 1.92 | 2.05 | 1.93 | 2.03 | 2.02 | 2.13 | 2.12 |
| STA5 | 2.51 | 2.18 | 2.45 | 2.13 | 2.42 | 2.14 | 2.39 | 2.16 | 2.43 | 2.33 | 2.54 | 2.37 |
| STA6 | 4.57 | 2.74 | 4.53 | 2.76 | 4.42 | 2.76 | 4.42 | 2.78 | 4.52 | 3.06 | 4.62 | 3.1 |

Tableau 4.6 – Nombre moyen de transmission

Le tableau 4.6 donne le nombre moyen de retransmissions par station pour les cas $512$ kbps et $2048$ kbps (qui sont les plus significatifs).

Dans le cas $2$ (c'est-à-dire sans que FBR ne soit activé), on peut voir que plus une station est éloignée, plus la part de retransmission est importante. Les stations $1$ à $3$ sont toujours capables d'envoyer leur trafic $CBR$ à $100\%$ *i.e.* le même nombre de trames (uniques) que dans le cas $1$. En revanche, les stations $4$, $5$ et particulièrement $6$ sont trop loin et n'arrivent pas à transmettre toutes leurs données à cause des pertes. Dans le cas à $2048$ kbps, même la station $3$ n'arrivent plus à compenser les pertes avec les retransmissions. La station $6$ est la pire et la plupart du temps elle atteint le nombre maximum de retransmissions et jette la plupart de ses trames. On remarque ainsi que plus le débit applicatif est élevé, plus les stations éloignées (stations $4$, $5$ et $6$) ont du mal à transmettre la totalité de leur trafic CBR. Par exemple, la proportion de trafic envoyé par la station $6$ (par rapport au cas $1$) est de $81.48\%$ dans le cas à $64$ kbps et chute progressivement à $68.44\%$ ($128$ kbps), $22.4\%$ ($256$ kbps), $7.3\%$ ($1024$ kbps) et $4.26\%$ ($2048$ kbps). Cela est du au fait que le débit de la cellule se sature petit à petit.

Concentrons-nous sur les cas de figure de $64$ kbps à $512$ kbps dans lesquels la cellule n'est pas saturée. On remarque dans les cas $3$ que FBR arrive clairement à améliorer la situation puisqu'on obtient les mêmes performances que dans les cas $1$. On peut voir que toutes les stations, à part la station $6$, participent aux retransmissions. Bien sûr, les stations les plus proches de l'AP sont sollicitées plus souvent car ils sont des relais potentiels pour davantage de stations. Par exemple, la station $1$ relaie des trames de toutes les autres stations, tandis que la station $5$ ne relai que les trames de la station $6$. On remarque cependant que la part des retransmissions a légèrement augmenté pour les stations relais avec FBR. Par exemple, considérons la station $1$ dans le cas à $512$ kbps. Son taux de succès à la première transmission à diminué de $87.4\%$ à $80.57\%$. Cela est davantage détaillé dans la table 4.6 où on peut voir que les stations $1$, $2$ et $3$ ont besoin de plus de retransmissions dans le cas $3$ que dans le cas $2$. Cela est du au fait que les stations plus éloignées (avec de moins bonnes condi-




(a) CBR de 64 kbps

(b) CBR de 128 kbps

(c) CBR de 256 kbps

(d) CBR de 512 kbps

(e) CBR de 1024 kbps

(f) CBR de 2048 kbps

Figure 4.15 – Proportion des trames reçues à différents débits CBR

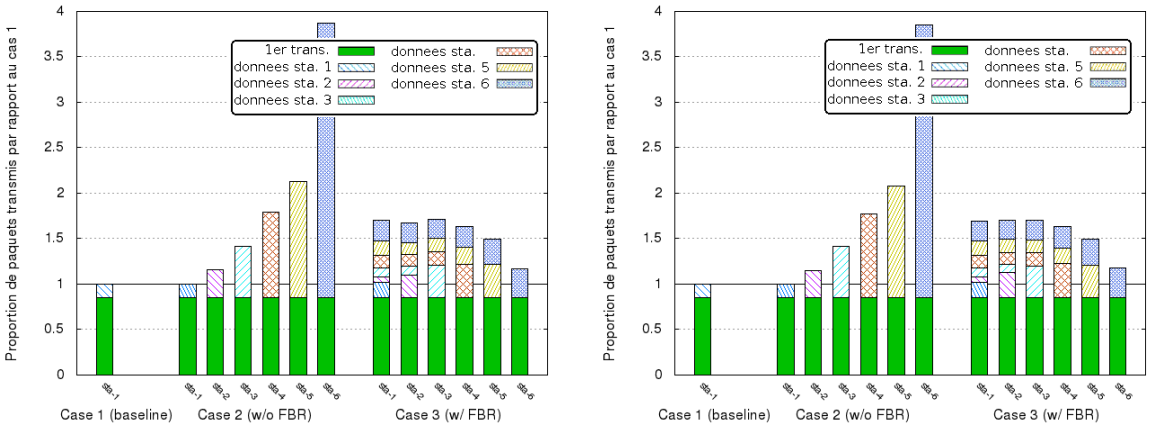
tions radio) injectent maintenant plus de trafic dans la cellule. Cette augmentation de trafic par les moins bonnes stations s'explique par deux faits : ces «mauvaises» stations reçoivent un acquittement plus rapide avec FBR que dans le cas 2 (car la trame est prise en charge par les relais), et cela leur permet ainsi de passer plus vite

à la prochaine trame CBR. Deuxièmement, parce que leurs trames nécessitent dorénavant moins de retransmissions de leur part (voir table 4.6), ces stations auront en moyenne un *backoff* plus petit que dans le cas 2 car la fenêtre de contention sera en moyenne plus petite. Ces stations éloignées perdent ainsi moins de temps à attendre d'avoir le droit de transmettre, injectant de fait plus de trafic dans le cellule et provoquant donc plus de collisions avec les «bonnes» stations. En dehors de cet effet de bord, les stations avec un PER faible (avec de bonnes conditions radio) peuvent quand même transmettre tout leur trafic CBR à l'AP et atteignent 100% par rapport au cas 1.

Concentrons-nous maintenant sur les cas de figure à 1024 kbps et 2048 kbps représentés par les figures 4.15e 4.15f. À ces débits, toute la cellule est saturée et les stations ne peuvent pas envoyer toutes leurs données CBR. Dans le cas 2 (sans FBR), les stations proches de l'AP envoient plus de trafic que lorsqu'elles étaient toutes à proximité de l'AP (cas 1). Ceci s'explique par le fait que les stations plus éloignées passent plus de temps à retransmettre leurs propres trames (on rappelle qu'une station double sa fenêtre de contention à chaque retransmission). Ces stations attendent ainsi plus longtemps avant de pouvoir accéder au canal, laissant la priorité aux stations ayant une meilleure qualité de lien. Ainsi, on peut voir que les stations 1 et 2 sont capables d'envoyer plus de trames CBR que dans le cas 1. En revanche, les stations 3, 4, 5 et 6 souffrent de leur PER plus élevé et jettent un nombre important de trames CBR du fait du nombre élevé de retransmissions. Dans le scénario à 2048 kbps, la station 6 n'est capable d'envoyer que 4.26% de ses données par rapport au cas 1, ce qui correspond à un débit de 64 kbps. Dans le cas 3, lorsque les stations utilisent FBR, la situation est plus équitable. On peut voir que le débit des stations éloignées devient acceptable alors que les débits des stations 1 et 2 ne sont pas radicalement impactés. La station 1 est toujours capable d'envoyer plus de trames que dans le cas 1 (132% pour le scénario 2048 kbps). Le comportement est cohérent avec le scénario observé dans le cas à 512 kbps. FBR permet d'augmenter significativement les performances des stations ayant un PER élevé. Comme le canal radio est une ressource partagée, dans un scénario où le débit de la cellule est saturé, lorsque le trafic d'une station augmente, le trafic d'une autre diminue. Comme le débit CBR est ici important, cet effet est exacerbé comparé au cas à 512 kbps, mais on peut apprécier le fait que le débit de chaque station est quand même plus qu'acceptable.

#### 4.3.3.2 Impact de FBR sur la retransmission des trames par les stations

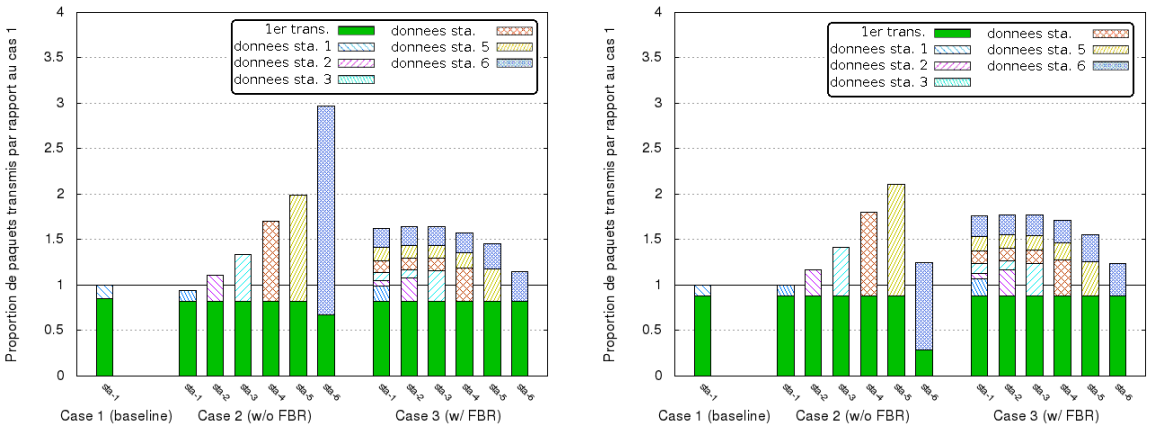
Les figures 4.16 représentent le nombre total de transmissions effectuées par chaque station, normalisé sur le cas 1. Ces figures permettent de mieux comprendre com-




(a) CBR de 64 kbps



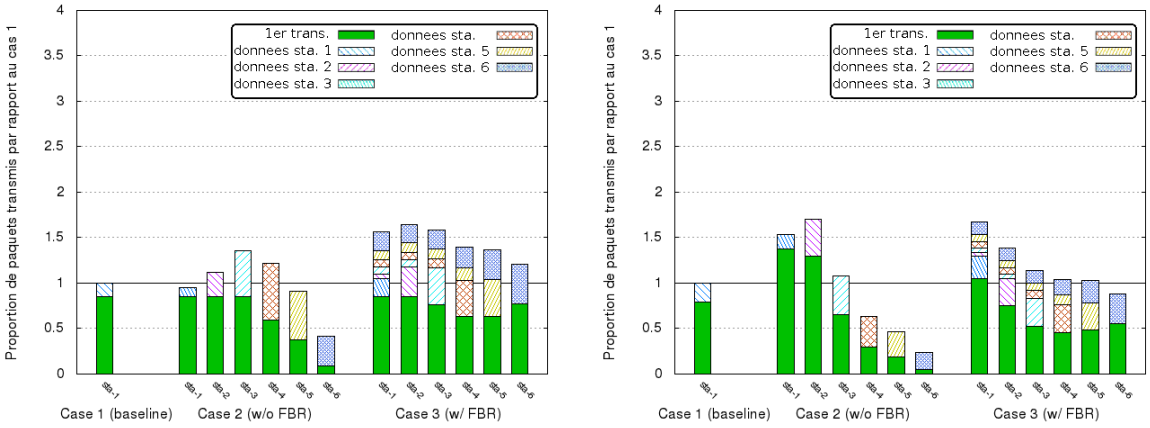

(b) CBR de 128 kbps




(c) CBR de 256 kbps




(d) CBR de 512 kbps




(e) CBR de 1024 kbps




(f) CBR de 2048 kbps

Figure 4.16 – Proportion des trames reçues à différents débits CBR

ment la charge des transmissions a été partagée parmi les différentes stations. Contrairement aux figures précédentes, chaque barre de l'histogramme représente le nombre total de transmission effectuées par une station (même celles ayant échoué). La première partie en vert correspond à la transmission d'une nouvelle

trame (pas une retransmission). Dans le cas 2 (les 6 barres au milieu des figures), la deuxième partie correspond aux retransmissions effectuées par la station (même celles ayant échoué). Le cas 3 (les 6 barres à droite de la figure) est similaire au cas 2 avec $FBR$ activé. La première partie (en vert) correspond également à la transmission d'une nouvelle trame (pas une retransmission). Les autres parties de la barre concernent les retransmissions et le relayage des trames des autres stations.

À titre d'exemple, pour bien comprendre ces figures, étudions la figure 4.16a. Le cas 1 représente le nombre de trames transmises par chaque station (transmission en vert, retransmission en hachuré) lorsqu'elles se trouvent toutes les 6 à proximité de l'AP. Le cas 2 représente le nombre de transmissions et retransmissions effectuées lorsque FBR n'est pas activé. On voit que plus une station est éloignée, plus elle effectue de retransmissions pour transmettre la totalité de son trafic CBR. Lorsque FBR est activé dans le cas 3, on remarque que la charge des retransmissions a été partagée entre les stations. La station 1 qui ne faisait pratiquement aucune retransmission s'occupe désormais de retransmettre les données des stations 2, 3, 4, 5 et 6. De cette façon, la station 6 n'a plus besoin de retransmettre ses propres trames.

Ces figures nous aident à mieux comprendre ce qu'on observait dans la section 4.3.3.1 précédente. En regardant la figure 4.16d, on constate que la station 6 sans FBR n'arrive plus à écouler son trafic CBR. On le voit avec la très forte diminution du nombre de *nouvelles trames* envoyées à l'AP. Ce nombre plus faible que dans le cas 1 signifie que la station a été obligée de jeter des trames car elle a atteint le nombre maximum de retransmissions et comme la cellule est presque saturée, elle ne peut plus rattraper son retard avec de nouvelles transmissions. On voit bien ici que grâce à FBR, la station 6 peut de nouveau écouler son trafic CBR.

#### 4.3.3.3 Impact de FBR sur les collisions

On s'intéresse ici aux collisions générées par FBR. Pour cela nous avons comparé le nombre de collisions dans les trois cas de figure. La figure 4.17 présente pour chaque débit la proportion de collisions avec et sans FBR (resp. les cas 2 et 3), normalisée sur le cas 1.

On remarque que la proportion de collisions dans le cas 2 par rapport au cas 1 diminue avec l'augmentation de débit. Cela s'explique par le fait que plus le débit est élevé, plus le nombre de collisions est important dans le cas 1. Cependant dans le cas 2, les stations éloignées provoquent moins de collisions du fait de leur fenêtre de contention qui est plus grande que les stations proches de l'AP.

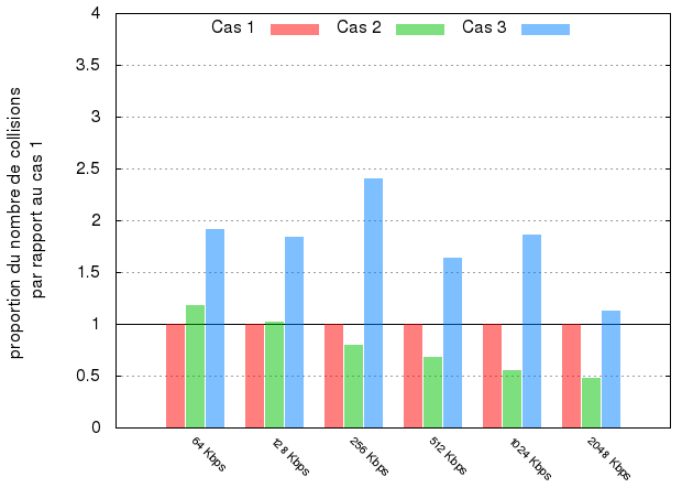
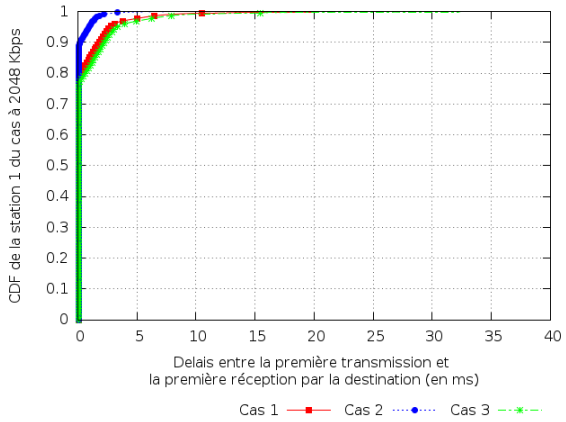



Figure 4.17 – Collisions normalisées sur le cas 1

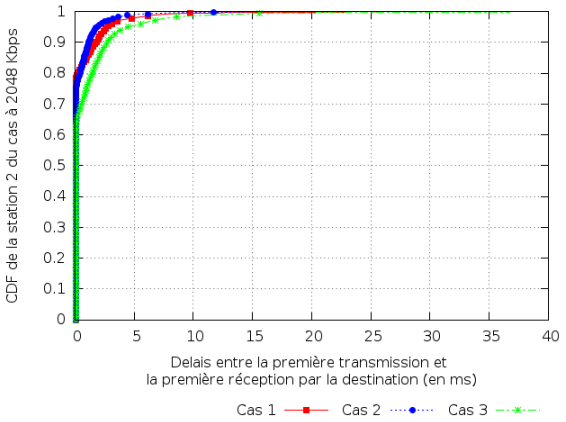
Comme on peut le voir sur la figure 4.17, FBR augmente significativement le nombre de collisions dans la cellule. Sur ces histogrammes on voit que FBR augmente jusqu'à deux fois et demi le nombre de collisions dans la cellule par rapport au cas 1. Cela s'explique simplement à cause de la façon dont FBR fonctionne. En effet, notre algorithme s'appuie sur la méthode de contention IEEE 802.11 pour sélectionner le relais, contrairement aux méthodes centralisées type SDF ou ExOR. Si notre méthode a l'avantage d'être entièrement distribuée et ne nécessite aucun échange de messages pour sélectionner le relais, il augmente en revanche les probabilités de collisions sur la contention. En effet, puisque chaque station possède deux files d'attentes et que ces dernières sont indépendantes l'une de l'autre, on peut doubler le nombre de compétiteurs à un instant donné. À titre d'exemple, lorsque la station 6 transmet une trame qui n'est pas reçue par l'AP, on passe de 6 *backoff* à 12 (dans le pire des cas).

#### 4.3.3.4 Impact de FBR sur les delais de réception

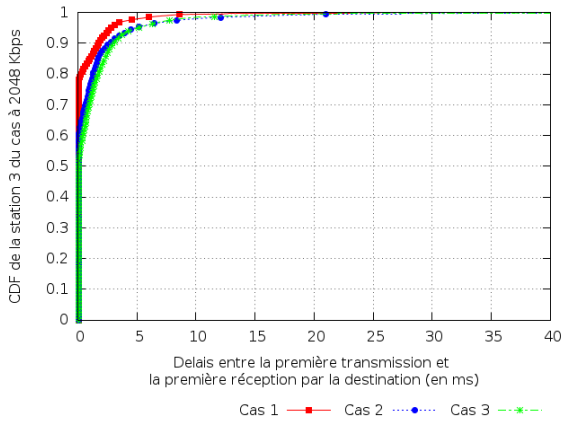
Le délai de réception correspond au temps écoulé entre la première transmission d'une trame et le moment où l'AP reçoit cette trame. Les pertes sur le canal ainsi que les collisions vont influencer ce délai puisque plus les retransmissions échouent, plus le délai sera important. Les figures 4.18 représentent les fonctions de répartition (CDF) des délais de réception (en $ms$) des trames transmises à un débit CBR de 2048 kbps pour chacune des 6 stations. Chaque figure est composée de trois CDF pour chacun des trois cas étudiés, c'est-à-dire le scénario où les 6 stations sont à proximité



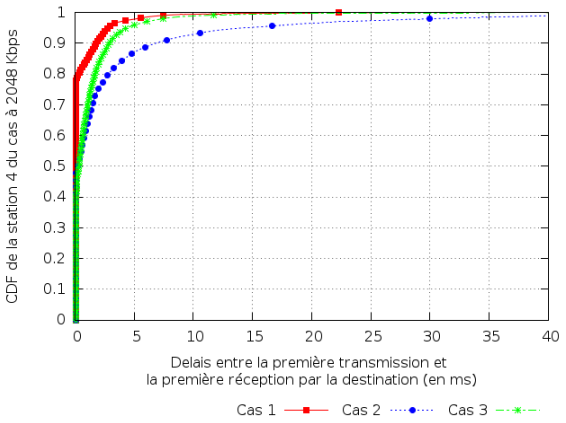

(a) CDF du délai des trames la station 1 à 2048 kbps



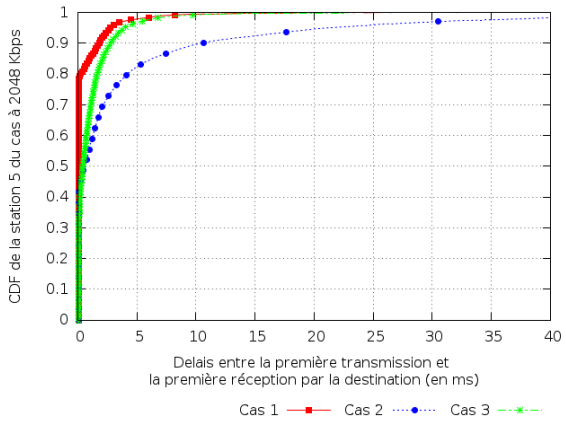

(b) CDF du délai des trames la station 2 à 2048 kbps



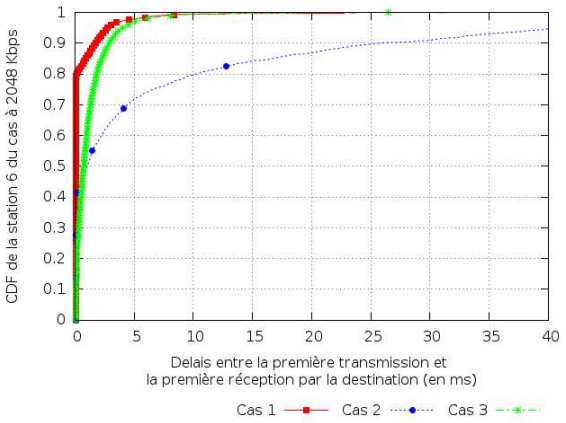

(c) CDF du délai des trames la station 3 à 2048 kbps




(d) CDF du délai des trames la station 4 à 2048 kbps




(e) CDF du délai des trames la station 5 à 2048 kbps




(f) CDF du délai des trames la station 6 à 2048 kbps

Figure 4.18 – Proportion des trames reçues à différents débits CBR

de l'AP (cas 1), les six stations en lignes sans FBR d'activé (cas 2) et les six stations en ligne avec FBR activé (cas 3).

Tout d'abord on remarque que la CDF du cas 1 ne change pas entre les stations car il correspond au cas où les stations partagent les mêmes conditions à proximité de l'AP. Cette courbe nous permet d'avoir un cas témoin pour mieux apprécier l'évolution des autres courbes. La CDF du cas 2 évolue fortement en fonction de la station. Plus la station est éloignée, plus son délai augmente à cause des pertes sur le canal qui obligent ces stations à retransmettre. On remarque également que le délai des trois premières stations a diminué dans le cas 2 par rapport au cas 1. Cela est du au fait que plus les «mauvaises» stations s'éloignent, plus leur *backoff* est élevé, ce qui diminue les collisions avec les «bonnes» stations qui réduisent leur retransmission, améliorant ainsi leurs délais.

Finalement on remarque ainsi que le délai pour les stations éloignées a très fortement diminué grâce à FBR, se rapprochant du cas 1. En revanche, le délai des stations proches de l'AP a très légèrement augmenté. Cela est du à l'augmentation des collisions que nous avons mis en évidence précédemment. Bien que le délai ait augmenté pour les stations 1 et 2, cette augmentation est très légère en comparaison avec le gain obtenu par les stations 4, 5 et 6.

Nous n'avons représenté ici que les résultats pour le cas à 2048 kbps mais nous avons observé les même comportements pour les autres débits.

## 4.4 Conclusion

Dans ce chapitre, nous avons décrit notre solution de relayage pour les réseaux IEEE 802.11 basée sur la retransmission opportuniste des trames n'ayant pas été acquittées par la destination. Dans FBR, La **sélection** de l'ensemble des relais potentiels (c'est-à-dire ceux pouvant faire progresser la trame vers la destination) se base sur la valeur du RSSI. La **suppression** des relais (c'est-à-dire le fait d'empêcher tous les relais potentiels de relayer) se base sur l'introduction de deux nouveaux acquittements ; les acquittements passifs qui correspondent au fait d'entendre une retransmission d'une trame en file d'attente ; et les acquittements retardés qui correspondent à la réception en retard – c'est-à-dire après le *timer* SIFS – d'un accusé de réception. Nous avons également introduit une version modifiée de FBR appelé B-FBR qui permet de biaiser le *backoff* des relais potentiels de façon à donner une plus grande chance aux meilleurs relais d'accéder au canal les premiers.

Dans un premier temps, nous avons montré par simulation que dans un scénario simple constitué d'une source et d'un relais, FBR améliore significativement les performances de la source. Sans nécessiter de signalisation supplémentaire, FBR permet de partager la charge de la retransmission avec le relais et diminue de fait le nombre d'échecs de retransmission de la part de la source, augmentant significativement les performances de la station. *B-FBR* permet d'atteindre des performances quasi optimales en permettant au relais de prendre en charge une fraction plus importante des retransmissions. FBR est ainsi capable d'adapter dynamiquement la topologie du réseau en fonction des conditions radio sans nécessiter d'échange de trames de contrôle. Ce mécanisme surpasse à la fois 802.11 seul en prenant en charge les retransmissions, et les mécanismes de routage traditionnels en exploitant les transmissions «chanceuses».

Dans un deuxième temps, nous avons testé FBR dans des conditions où plusieurs stations ayant une connectivité inégale avec un AP étaient source de trafic. les résultats démontrent que la connectivité des stations lointaines est fortement améliorée au prix d'une légère baisse de performance pour les stations les plus proches. Cette baisse de performance s'explique par un meilleur partage de la bande passante entre toutes les stations d'une cellule.

CHAPITRE 5

# Conclusion et Perspectives

## Sommaire



## 5.1 Conclusion

La principale contribution de cette thèse est la proposition d'un algorithme de relayage opportuniste (FBR) qui tire profit des réceptions opportunistes des trames pour améliorer le mécanisme de retransmission dans les réseaux CSMA/CA. Par la nature diffuse des communications sans-fil, une trame *unicast* est en réalité reçue par les stations voisines de la source. Nous avons proposé que ces dernières, en cas de non réception de la trame par la destination, participent à la retransmission. Cette participation est conditionnée par la qualité de lien de chaque station ; seules les stations ayant une meilleure qualité de lien avec la destination que la source entreront en compétition pour retransmettre ladite trame. Ce mécanisme est léger puisqu'il n'introduit pas de nouvelles signalisations, mais modifie la sémantique des trames et acquittements déjà utilisés. FBR est une approche originale, puisque contrairement aux solutions de relayage et routage existantes, l'ensemble de relais potentiels est auto-sélectionné après l'émission de la trame, et non *a priori*. Ceci permet de s'adapter efficacement aux perturbations subies par les communications sans-fil. Finalement, ce protocole FBR efface la frontière entre réseau à infrastructure – qui consiste en un accès sans-fil fourni par un AP – et le mode *ad hoc* – un réseau dé-

centralisé dont les fonctions de routage sont assurées par les stations elles-mêmes. En effet, le relayage proposé permet de relayer des trames vers un AP, ou tout autre destination du réseau.

Dans le chapitre 2, nous avons étudié les caractéristiques des technologies sans-fil et avons mis en évidence leur caractère diffus et aléatoire. Dans IEEE 802.11, une station ayant une mauvaise qualité de signal avec une destination subira des pertes qui sont dues à la mauvaise réception de ses trames. Dans un tel cas de figure, la station source peut soit retransmettre les trames non acquittées, soit réduire son débit de transmission pour utiliser une modulation plus robuste, mais ces deux stratégies ont des impacts négatifs. En effet, les retransmissions, en plus d'augmenter le délai à cause de l'augmentation de la fenêtre de contention, n'améliore pas les probabilités de réception si les pertes sont principalement dues au PER élevé du lien. La réduction du débit est efficace pour limiter les retransmissions mais implique une durée de transmission plus importante, ce qui diminue les performances des autres stations (car le temps de canal disponible est réduit). En proposant d'utiliser le relayage pour ces cas de figure, nous introduisons une troisième contre-mesure pour ces réseaux, basée sur la coopération de l'ensemble de la cellule.

Les techniques de relayage ont été beaucoup étudiées au cours de ces dernières années et c'est pourquoi nous étudions dans le chapitre 3 les différentes stratégies proposées dans la littérature. Ces techniques proviennent des protocoles des routage dans les réseaux sans-fil multi-sauts dans lesquels le relayage est la clé de voûte de la communication, car il n'y a pas d'infrastructure fixe commune aux stations permettant d'assurer la bonne réception des trames. Ces protocoles servent deux fonctions qui sont la construction des routes d'une part, et le relayage des trames entre les stations le long de ces routes d'autre part. Nous avons identifié et proposé une taxonomie permettant de classifier ces protocoles selon leur réactivité aux modifications locales de l'environnement dans la politique de relayage. En sélectionnant le prochain saut *a posteriori* de la transmission en diffusion d'une trame, le routage opportuniste permet de prendre en compte la topologie immédiate du réseau telle qu'elle est réellement et non pas telle qu'elle est perçue. Pour être complètement fonctionnelle, cette technique nécessite cependant de résoudre deux défis que sont la sélection des relais parmi les récepteurs et le contrôle des retransmissions pour éviter les duplications.

Nous présentons FBR dans le chapitre 4 qui permet de déléguer de façon opportuniste les retransmissions à des stations relais. En procédant ainsi, on évite qu'une station source avec de mauvaises conditions radio ne retransmette inutilement ses trames ou n'utilise un débit plus faible. Les stations, même avec une mauvaise qua-

lité de lien, effectuent ainsi leurs transmissions à haut débit et seuls les paquets nécessitant une retransmission (c'est-à-dire non acquittée par la destination) sont pris en charge par les relais opportunistes. Afin d'éviter les duplications de trames, les relais ne retransmettent pas une trame qui a déjà été retransmise par un autre relais. L'application de ces principes pour IEEE 802.11 nécessite d'ajouter deux nouveaux types d'acquittement que sont l'acquittement passif et l'acquittement retardé. Le premier considère comme un acquittement le fait d'entendre une retransmission effectuée par une «meilleure» station car cela signifie que la trame a pu progresser vers la destination. Le deuxième consiste à accepter un acquittement (ACK) même si celui-ci est reçu après la période SIFS car cela implique qu'une station a retransmis la trame et que la destination l'a reçue. Afin de valider cet algorithme, nous l'avons implémenté sous NS-2 après avoir amélioré la couche physique du simulateur. Les résultats de simulation montrent ainsi que l'exploitation des réceptions opportunistes permet à des stations de conserver l'utilisation de débits élevés même lorsque ces dernières sont éloignées de l'AP.

## 5.2 Travaux futurs

Afin d'étendre les contributions de cette thèse, il est évident qu'une implémentation réelle et des résultats empiriques permettront de garantir la pertinence de la solution proposée. L'homogénéisation de la prise en charge des pilotes dans la nouvelle architecture *mac80211* sous Linux permettrait de fournir une solution fonctionnant de façon générique. Une telle implémentation est prévue et actuellement en cours de développement.

Il serait également important d'étudier comment le mécanisme FBR impacte l'algorithme de sélection de débit dans 802.11 *minstrel*. Ce dernier fonctionne en enregistrant le résultat de toutes les transmissions effectuées afin de sélectionner le mode de transmission offrant le meilleur débit utile. En améliorant le taux de succès des transmissions (indépendamment du débit utilisé) FBR va nécessairement promouvoir l'utilisation de débits plus élevés en présence d'un voisinage apte à relayer les trames. Il faudra donc étudier l'influence du voisinage sur les performances et la pertinence des débits sélectionnés par *minstrel*. Il faudrait pour cela modifier l'algorithme *minstrel* pour prendre en compte les deux nouveaux types d'acquittements que nous avons introduit dans le calcul des statistiques.

Nous avons montré que face à une densité élevée de stations source, FBR à tendance à augmenter le nombre de collisions à cause de l'introduction de nouveaux

participants (les relais potentiels) dans le mécanisme de contention. Pour réduire les collisions, nous voyons deux pistes d'exploration qui ne sont pas nécessairement exclusives. La première consisterait à introduire un mécanisme permettant de limiter le nombre de relais potentiels sans toutefois introduire de signalisation supplémentaire. Chaque relais potentiel pourrait décider de se retirer de la contention en fonction de l'état actuel du voisinage. Si une station estime qu'il y a déjà un nombre «suffisant» de relais potentiels pour une certaine trame, elle pourrait décider de ne pas participer à la contention (via un tirage aléatoire dépendant du nombre de relais potentiels estimé par exemple). Chaque station pourrait ainsi maintenir la connaissance de son voisinage en écoutant toutes les trames pour calculer des statistiques sur le taux de succès des stations voisines (à la manière de *minstrel*). Une deuxième approche pour réduire le nombre de collisions serait d'effectuer la contention entre les relais sur les ACK plutôt que sur la retransmission de la trame. Lorsqu'une trame est entendue par un certain nombre de relais potentiels, ces derniers acquittent la source en suivant une procédure de contention afin de ne pas créer de collision sur les ACK (voir Annexe A.1). Le premier relais potentiel à transmettre l'ACK sera ainsi auto-sélectionné pour effectuer la retransmission de la trame. Cette approche apporte dans un premier temps le bénéfice de fiabiliser le processus de *suppression* puisque l'ACK a plus de chance d'être entendu par les relais potentiels que la retransmission de la trame de données. Deuxièmement, en réduisant la contention sur les trames de données, cela contribue à réduire le nombre de collisions des trames de données que nous avons observé section 4.3.3.3. Cette approche amène cependant deux nouveaux défis : comment augmenter l'intervalle SIFS de façon à limiter le risque de collision sur les ACK, sans introduire un délai trop important pour l'émission des trames de données ? Deuxièmement, en introduisant un risque (nouveau) de collision sur les ACK, on augmente le risque de retransmettre une trame quand ce n'est pas nécessaire (trame ayant progressée vers la destination mais pour laquelle l'ACK est perdu).

## 5.3 Perspectives

Les efforts de standardisation tels que IEEE 802.11s ou RPL vont dans le sens des thématiques développées dans cette thèse et permettent raisonnablement d'envisager que les réseaux de demain seront constitués en partie de réseaux sans-fil multi-sauts. L'Internet des objets décrit également de nombreux domaines d'application dans lesquels les réseaux sans-fil multi-sauts jouent un rôle prépondérant. Les ITS, le *home networking* ou encore les relevés de compteur sont autant de domaines d'appli-

cation, que de contraintes variables. Pour ces réseaux, FBR peut améliorer le processus de relayage jusqu'au puit dans le cas de RPL par exemple. L'ajout de FBR dans ces réseaux peut fortement améliorer les performances de transmission de saut en saut ; chaque saut de routage, c'est-à-dire chaque parent devant être un point de passage obligatoire pour les trames, peut être vu comme une tentative de transmission dans une cellule. Paradoxalement, pour profiter au mieux des mécanismes de FBR, il faut choisir une métrique privilégiant les sauts de routage « longs » de type nombre de sauts jusqu'à la destination. Le parent choisi doit donc être à portée du fils, mais le plus loin possible. La raison est que FBR n'exploite pas les transmissions ayant progressées au-delà de la destination (car l'ACK termine la procédure). Pour tirer le meilleur profit de FBR, il faut que la source soit à portée de l'ACK de la destination mais que cette dernière se trouve le plus « loin » possible pour profiter de tous les relais potentiels intermédiaires. Les contraintes énergétiques sont souvent au cœur de ces applications bien qu'on trouve des réseaux d'objets non limités en énergie. L'applicabilité de FBR dans des réseaux à forte contrainte énergétique n'est pas triviale. FBR se basant sur la présence de relais, cela implique que ces derniers doivent conserver leur interface sans-fil allumée même s'ils ne sont pas la destination prévue d'une trame. Ces réseaux de capteurs se basent souvent sur des notions de *duty cycle* (sommeil) pouvant rendre FBR inopérant dans cet environnement s'il est utilisé comme tel. Une perspective intéressante serait l'intégration de FBR aussi bien dans un protocole à préambule (un préambule annonce qu'une trame est envoyée pour indiquer qu'il faut se réveiller) que dans les protocoles à synchronisation (tout le monde se réveille soit par un beacon, soit par des périodes alternatives d'éveils).

ANNEXE A

## A.1 Interférence sur les ACK

Durant la conception de FBR, nous avons été amené à étudier l'éventualité de transmettre des ACK simultanément par plusieurs stations pour acquitter une station source. L'idée était d'acquitter une station dès que la trame réussissait à faire du progrès plutôt que d'attendre que la destination reçoive la trame pour émettre un ACK. Deux trames transmises simultanément sont susceptible de s'interférer provoquant une collision qui rend difficile pour un récepteur de correctement décoder le signal. Cependant, dans notre cas de figure les ACK sont rigoureusement identiques au bit près et transmis exactement au même moment (juste après la durée SIFS). Comme expliqué à la section 2.2.4, des signaux identiques peuvent s'additionner ou s'annuler en fonction du placement des antennes émettrices et de la longueur d'onde de la porteuse utilisée. Il n'est donc pas déraisonnable de faire l'hypothèse que dans certain cas de figure, un récepteur peut tout à fait être capable de décoder correctement un ACK transmis par deux stations simultanément. Le but de cette expérimentation est de tester cette hypothèse dans un environnement réel. L'hypothèse que nous souhaitions donc vérifier dans cette expérimentation était donc *«si plusieurs stations transmettent simultanément un ACK identique, un récepteur est-il capable de correctement le décoder ?»*

### A.1.1 Protocole expérimental

Afin de tester l'hypothèse, nous avons configuré un ordinateur portable (AP) sous la forme d'un point d'accès et deux ordinateurs portables (STA1,STA2) faisant office de stations. Le portable utilisé pour le point d'accès était un DELL Latitude D410 munie d'une carte WiFi NetGear WPN511 utilisant un *chipset Atheros*. Les deux stations étaient des Samsung NC10 avec une carte wifi utilisant également un chipset *Atheros*. Pour les trois ordinateurs, avons utilisé les drivers Linux *ath5k*. La figure

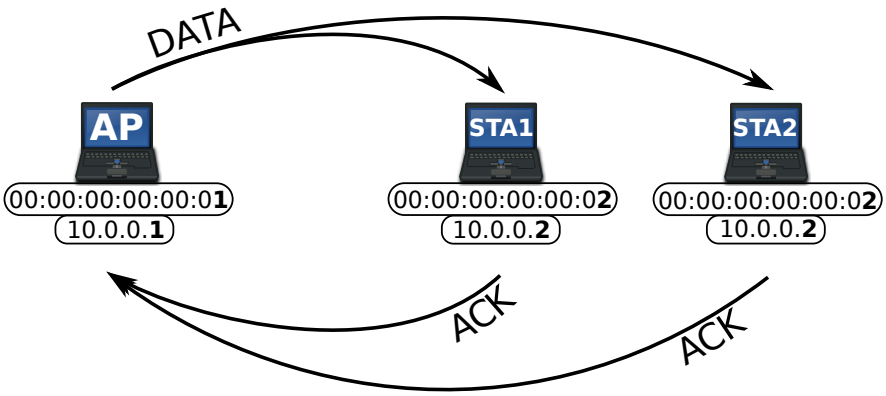



Figure A.1 – Scénario expérimental permettant de tester si les ACK simultanées s'interfèrent de façon significative

A.1 représente le scénario que nous avons mis en place pour tester si les ACK s'interfèrent. Nous avons fait plusieurs expérimentations en faisant varier la position des stations, pour chaque position le protocole expérimental était le suivant :

1. L'ordinateur AP configure un point d'accès avec l'adresse MAC `00:00:00:00:00:01` et se configure une IP statique `10.0.0.1`
2. Les deux stations sont configurés avec la même adresse MAC `00:00:00:00:00:02`, se connectent au point d'accès et s'attribuent statiquement la même IP `10.0.0.2`
3. les deux stations font tourner un programme *perl* qui attend une connexion UDP sur le port `1234`
4. le point d'accès envoie 200 trames UDP vers `10.0.0.2` et enregistre le nombre de retransmission nécessaire pour chaque trames.

Afin de mesurer l'efficacité de ce scénario, nous allons compter le nombre de retransmissions effectuées pour chaque trame envoyée par le point d'accès aux deux stations.

#### A.1.1.1 Configuration du point d'accès

Nous avons d'abord attribué manuellement une adresse MAC à l'interface sans-fil avec la commande arp :

```
1        # ifconfig wlan2 hw ether 00:00:00:00:00:01
```

Nous avons utilisé le logiciel HostAPD qui permet de gérer le mode AP de IEEE 802.11 sous Linux. Toute la partie authentification, gestion des clés, et les autres aspects du mode infrastructure sont gérés en *userspace* par le démon hostapd. Ce dernier lit la configuration du point d'accès dans un fichier passé en paramètre. Nous avons utilisé les paramètres suivants :

```
interface=wlan2
driver=nl80211
ctrl_interface=/var/run/hostapd
ctrl_interface_group=wheel
ssid=isacklost
country_code=FR
hw_mode=g
dtim_period=2
channel=6
beacon_int=100
supported_rates=480
basic_rates=10 20
```

Avec cette configuration, le point d'accès diffuse un SSID "isacklost" sans chiffrement et impose aux ACK d'être envoyés à 1 mbps, et aux stations d'utiliser un débit de 48 mbps. Nous avons ensuite attribué statiquement une IP au point d'accès avec la commande *ip* :

```
# ip addr add wlan2 10.0.0.1/32
```

Pour éviter que le point d'accès ne fasse de requête ARP auprès des stations, nous avons rempli manuellement la table avec la commande suivante :

```
# arp -s 10.0.0.2 00:00:00:00:00:02
```

### A.1.1.2 Configuration des stations

Comme pour le point d'accès, nous avons attribué manuellement une adresse MAC (la même) aux deux stations :

```
# ifconfig wlan0 hw ether 00:00:00:00:00:01
```

La connexion au point d'accès se fait sous linux avec la commande *iw* :

```
# iw dev wlan0 connect isacklost
```

Finalement, nous avons attribué une adresse IP statique pour les deux stations :

```
# ip addr add wlan0 10.0.0.2
```

En partageant ainsi la même adresse MAC et la même adresse IP, si les deux stations reçoivent en même temps une trame, elles transmettront simultanément un

ACK en direction de l'AP. Nous configurons ensuite les deux stations pour être à l'écoute sur un port UDP, nous utilisons pour cela l'utilitaire *netcat* disponible sous le système d'exploitation GNU/Linux en ligne de commande :

```
# netcat -l -u 1234
```

Cette commande ouvre une *socket* UDP (option -u) et écoute sur le port `1234` (option -l).

### A.1.1.3 Compter le nombre de retransmission

Le *driver mac80211* permet de récupérer un certain nombre de statistiques relatives à 802.11 dans le dossier `/sys/kernel/debug/ieee80211/`. Ce dossier contient des statistiques tel que le nombre de trames émises, reçues, retransmises etc. Nous avons donc fait un script qui envoie une trame UDP et regarde ensuite combien de retransmissions ont été nécessaires.

```
#!/usr/bin/perl

use IO::Socket;
my $sock = IO::Socket::INET->new(Proto => 'udp') or die "socket: $!";
$ipaddr = inet_aton("10.0.0.2");
$portaddr = sockaddr_in(1234, $ipaddr);

# on recupere les statistiques avant de transmettre
my $tx=`cat /sys/kernel/debug/ieee80211/phy0/stations/00:00:00:00:00:02/tx_packets`;
my $retry=`cat /sys/kernel/debug/ieee80211/phy0/stations/00:00:00:00:00:02/tx_retry_count`;

for($i = 0; $i < 200; $i++){
  my $MSG="ping $i\0";
  send($sock, $MSG, 0, $portaddr) == length($MSG)
    or die "cannot send: $!";
}

# on recupere les statistiques apres les transmissions
my $tx2=`cat /sys/kernel/debug/ieee80211/phy0/stations/00:00:00:00:00:02/tx_packets`;
my $retry2=`cat /sys/kernel/debug/ieee80211/phy0/stations/00:00:00:00:00:02/tx_retry_count`;

# on calcul les moyennes
my $total_tx_packets = $tx2 - $tx;
my $nb_retry_per_packet = $total_tx_packets/($retry2-$retry);
```

En comparant le nombre de trames totales transmises et retransmises avant et après l'émission des 200 trames UDP, on peut estimer le nombre moyen de retransmissions nécessaires pour chaque trame. Le nombre moyen de retransmissions par trame est donné par la variable `nb_retry_per_packet`

### A.1.2 Résultats d'expérimentation

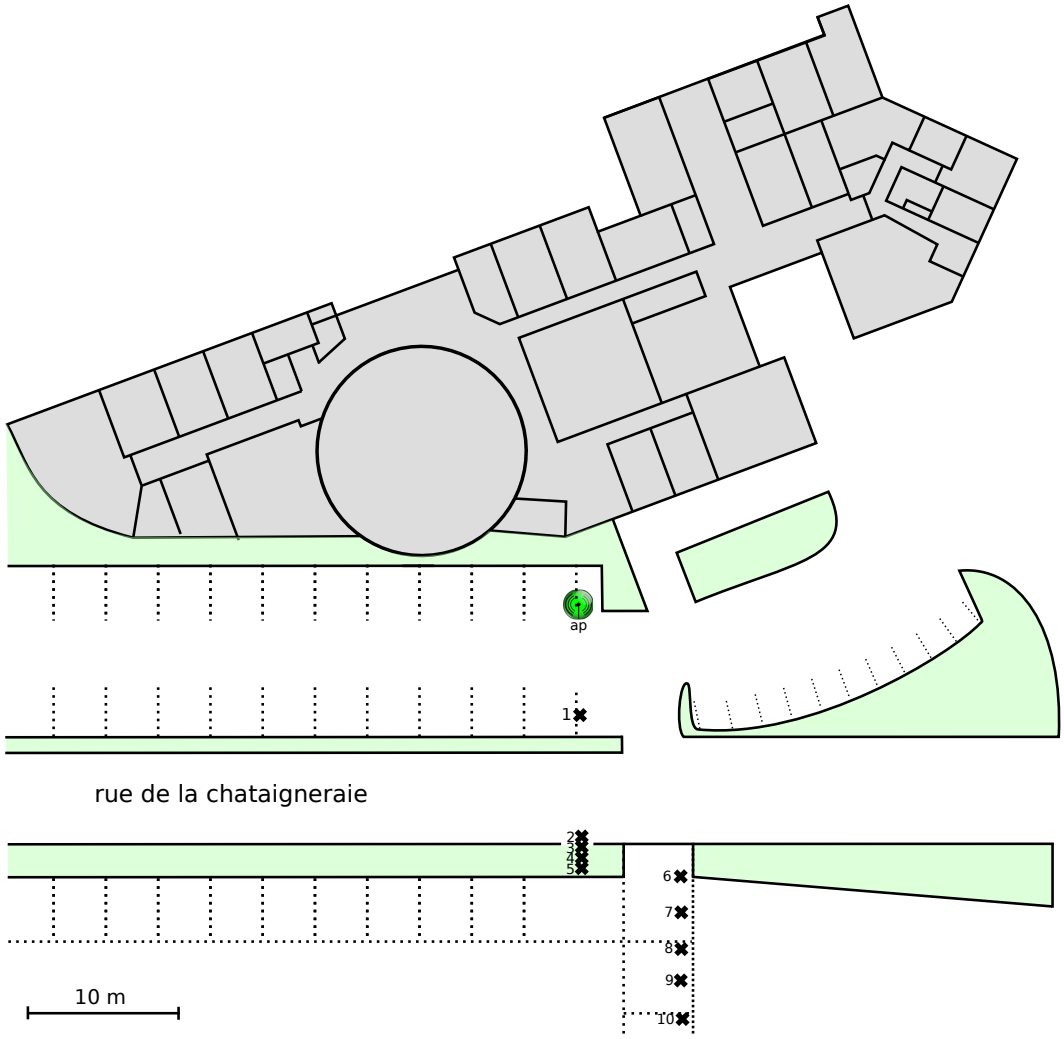



Figure A.2 – Carte du campus de Telecom bretagne (parking Sud) avec les marqueurs des position prises par les stations lors de l'expérimentation

Nous avons effectués les tests sur le parking sud du campus de Rennes Telecom Bretagne, les différentes positions sont représentés sur la carte de la figure A.2. Avant de testé la réception d'ACK simultannée, nous avons commencé par récupérer la qualité du lien entre l'AP et les différentes positions. Pour cela nous avons utilisé les configurations précédemment décrites mais en désactivant une des deux station pour obtenir la qualité réelle du lien. Ces résultats sont disponibles sur le tableau A.1a. Du fait de l'absence d'obstacle, on remarque que le nombre moyen de retransmission est extrêmement faible avec un minimum $0.005$ pour le cas où la station se trouve en position $6$ et un maximum de $0.479$ pour la position $10$.

Nous avons ensuite testé un certain nombre de configurations comme indiqué sur le tableau A.1b. Les valeurs de couleurs vertes signifient que le nombre moyen de retransmissions est similaires au cas témoin tandis que les valeurs de couleurs rouges indiquent un nombre élevé de retransmission (et donc de perte de l'ACK). On constate que les valeurs sont assez extrêmes, soit le signal s'additionne et l'ACK est bien reçu, soit le signal s'annule et cela implique un nombre très important de retransmissions. On remarque par exemple que lorsque la station 1 est en position 6 et la station 2 en position 10 on obtient de bons résultats. Cependant si la station 2 se déplace en position 7, les résultats deviennent subitement médiocres.

| | Cas témoin (STA2 seule) | | | | | |
|---|---|---|---|---|---|---|
| **Pos. AP** | 0 | 0 | 0 | 0 | 0 | 0 |
| **Pos. STA1** | X | X | X | X | X | X |
| **Pos. STA2** | 5 | 6 | 7 | 8 | 9 | 10 |
| **# Retrans. moyen** | 0.19 | 0.005 | 0.035 | 0.19 | 0.315 | 0.479 |

(a) Nombre moyen de retransmissions nécessaires pour les différentes positions avec une seule station émettant des ACK (cas témoin).

| | STA1 & STA2 positions différentes | | | | | | | | | | | STA1 & STA2 même position | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Pos. AP** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **Pos. STA1** | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 6 | 7 | 8 | 9 | 10 | 9 | 8 |
| **Pos. STA2** | 2 | 3 | 4 | 5 | 8 | 9 | 10 | 10 | 10 | 10 | 10 | 10 | 9 | 8 |
| **# Retrans. moyen** | 7.32 | 7.06 | 9.61 | 7.19 | 0.28 | 0.74 | 0.16 | 0.58 | 6.67 | 5.24 | 7.37 | 4.86 | 6.46 | 6.45 |

(b) Nombre moyen de retransmissions nécessaires en fonction du placement des stations. En vert les scénarios acceptables (performances similaires aux cas témoins) et en rouge les cas posant problèmes.

Tableau A.1 – Résultat d'expérimentation pour tester la faisabilité d'un système d'acquittement basé sur une transmission d'ACK simultanément par plusieurs stations

### A.1.3 Conclusion

Transmettre des ACK simultanément par plusieurs stations résulte en un très fort taux de perte malgré que les trames soient identiques et envoyées au même moment. Certains cas de figure confirment toutefois l'hypothèse que de tels ACK peuvent être correctement reçues par un récepteur mais ces cas de figures sont très sensibles à la position des stations et les performances peuvent dramatiquement chuter en bougeant un tout petit peu. Ce n'est donc pas utilisable de façon fiable dans un environnement mobile et même dans un environnement fixe, cette méthode demanderait trop de contrôle dans la position des stations.

# Publications

## Rapports et présentations

- Loiseau Lucien, Rapport Livrable numéro II, Projet pôle de compétitivité image et réseau Extrem, 2010
- Loiseau Lucien, Présentation orale, *Forwarding by Retransmission in IEEE 802.11 networks*, Journée Futur & Rupture, Poster, Telecom Paris, Janvier 2013
- Loiseau Lucien, Présentation poster, *Opportunistic Forwarding in Wireless Networks*, Journée Futur & Rupture, Poster, Telecom Paris, Janvier 2012
- Lucien Loiseau, Présentation poster, *Toward a modular protocol Stack*, écolé d'été RESCOM 2010, Presqu'île de Giens, Juillet 2010
- Lucien Loiseau, German Castignani, Présentation poster, *A Wireless network experiment*, école d'été RESCOM 2010, Presqu'île de Giens, Juillet 2010

## Conférences Internationales

- Nicolas Montavont, Safaà Hachana et Lucien Loiseau, *Opportunistic Social Network Experiment*, The 2nd IEEE International Workshop on Opportunistic Networking (WON-09), Bradford (EN), 29 Mai 2009
- Lucien Loiseau, German Castignani, Nicolas Montavont, *An Evaluation of IEEE 802.11 Community Networks Deployements*, International Conference on Information Networking (ICOIN 2011), Kuala Lumpur (MY), 28 Janvier 2011
- Lucien Loiseau, Nicolas Montavont et Xavier Lagrange, *Forwarding By Retransmission in IEEE 802.11*, Seventh IEEE International Conference on Advanced Networks and Telecommunication Systems, Chennay (IN) (ANTS) 2013

# Glossary

**broadcast** Une trame envoyée en *broadcast* désigne une trame envoyée à toutes les stations du lien. S'il s'agit d'une transmission de niveau 2 (MAC) il s'agit alors de l'ensemble des stations du lien. S'il s'agit d'une transmission de niveau 3 (IP), il s'agit de l'ensemble du sous-réseau IP. Ce terme est à opposer à une transmission unicast. 82, 86, 137

**débit** Le débit désigne le débit utilisé au niveau de la couche 3 du modèle OSI.. 77–79, 86

**datarate** Le *datarate* désigne le débit de transmission utilisé au niveau de la couche 2 du modèle OSI.. 77

**multicast** Une trame envoyée en *multicast* désigne une trame envoyée à une liste de stations. Ce terme est à opposer à une transmission unicast. 87, 137

**trame** Une trame désigne un bloc d'information véhiculé au niveau de la couche 2 (MAC) du modèle OSI. Elle inclut l'entête MAC et les données transportées. 77, 82, 83, 85, 87

**unicast** Une trame envoyée en *unicast* désigne une trame envoyée à une station en particulier. Ce terme est à opposer à une transmission broadcast ou multicast. 82, 83, 87, 137

# Acronymes

**6LowPan** IPv6 over Low power Wireless Personal Area. 60, 61

**ACK** ACKnowledgement. 4, 30, 32, 40, 80, 83, 86, 92, 94, 95, 97–99, 101, 103–106, 109, 130, 132

**ADSL** Asymmetric Digital Subscriber Line. 18

**AES** Advanced Encryption Standard. 24

**AIFS** Arbitrary Inter-Frame Spacing. 33

**AIFSN** Arbitrary Inter-Frame Spacing Number. 33

**AODV** Ad hoc On demand Distant Vector. 57, 71, 72, 74, 75, 148

**AP** Access Point. 2, 19, 49, 74, 93–95, 98, 99, 101, 107–109, 111, 113–118, 120, 122, 123, 125, 126, 131, 150

**ARCEP** Autorité de Régulation des Communications Électroniques et des Postes. 9

**ARP** Address Resolution Protocol. 133

**B-FBR** Biased-FBR. 65, 97, 112, 115, 116, 126, 149

**BATMAN** Better Approach To Mobile Ad hoc Network. 57, 66, 68

**BER** Bit Error Rate. 39, 41–44, 50, 103, 148

**BPSK** Binary Phase-Shift Keying. 41, 42, 148

**BRTS** Broadcast RTS. 82

**BSS** Basic Service Set. 26, 28, 96

**BSSID** Basic Service Set IDentification. 28, 36, 52

**CBF** Contention Based Forwarding. 64, 87, 88, 149

**CBR** Constant Bit Rate. 107, 116–122, 124, 125, 150

**CCK** Complementary Code Keying. 23, 25

**CCMP** Counter Cipher Mode with Block Chaining Message Authentication Code Protocol. 24

**CDF** Cumulative Distributed Function. 2, 125

**CDMA** Code Division Multiplexing Access. 14, 147

**CETX** Cooperative ETX. 95, 126

**CGSR** Clusterhead Gateway Switch Routing. 64

**CN** Community Network. 19

**CoAP** Constrained Application Protocol. 61

**CORE** Constrained RESTful Environments. 60, 61

**CRS** Candidate Relay Set. 85

**CSMA** Carrier Sense Multiple Access. 17

**CSMA/CA** Carrier Sense Multiple Access with Collision Avoidance. 4, 17, 29, 31, 36, 127

**CTS** Clear-To-Send. 29, 30, 35, 51, 80, 82, 87, 104, 148

**CW** Contention Window. 97, 110, 114, 115

**DAO** Destination Advertisement Option. 70

**DARPA** Defense Advanced Research Projects Agency. 57

**DCF** Distributed Coordination Function. 30–33, 37, 50, 52

**DIFS** DCF Inter-Frame Spacing. 29–33

**DIO** Destination Information Object. 69, 70

**DIS** Destination Information Sollicitation. 69

**DODAG** Destination Oriented Directed Acyclic Graph. 69, 70, 148

**DSN** Deep Space Network. 62

**DSR** Dynamic Source Routing. 57, 74

**DSSS** Direct-Sequence Spread Spectrum. 22, 25

**DTN** Delay Tolerant Network. 61–63, 98, 148

**EDCA** Enhanced Distributed Channel Access. 33

**EDCF** Enhanced Distributed Coordination Function. 30, 31

**EIFS** Extended Inter-Frame Spacing. 29, 30

**ESS** Extended Service Set. 28, 37, 96

**ESSID** Extended Service Set IDentification. 19

**ETP** Expected Throughput. 78, 79

**ETT** Expected Transmission Time. 78

**ETX** Expected Transmission Count. 68, 77, 78, 85, 86, 88, 95

**EWMA** Exponential Weighted Moving Average. 48, 77

**ExOR** Extremely Opportunistic Routing. 86, 123

**FAI** Fournisseur d'accès à Internet. 2, 18, 19

**FBR** Forwarding By Retransmission. 65, 82, 88, 93–97, 99–101, 103, 107–112, 114–120, 122, 123, 125–127, 149

**FDMA** Frequency Division Multiplexing Access. 14, 147

**FHSS** Frequency Hop Spread Spectrum. 22

**FO** Forward Order. 87

**FOA** Forward Order Acknowledgement. 87

**GPS** Global Positionning System. 81

**GSM** Global System for Mobile Communication. 8, 10, 14

**HD** High Definition. 24

**HSR** Hierarchical State Routing. 64

**HTS** Helper-To-Send. 80

**HTTP** Hypertext Transfer Protocol. 61

**HWMP** Hybrid Wireless Mesh Protocol. 73–75, 149

**IARP** Intra-zone Routing Protocol. 73

**iAWARE** Interference Aware. 78

**IBSS** Independant Basic Service Set. 26, 96

**ICMPv6** Internet Control Message Protocol version 6. 68

**IERP** Inter-zone Routing Protocol. 74

**IETF** internet Engineering Task Force. 57, 60, 66, 68, 70, 72, 73

**IFS** Inter-Frame Spacing. 29, 30

**IP** Internet Protocol. 13, 52, 57, 58, 60–62, 68, 132, 133, 137

**IPN** InterPlanetary Networking. 61, 62

**IPv4** Internet Protocol version 4. 60, 96

**IPv6** Internet Protocol version 6. 60, 61, 68, 96

**ISM** Industrial, Scientifique et Médicale. 25

**ITS** Intelligent Transport Service. 58, 59, 63

**JPL** Jet Propulsion Laboratory. 61

**LANMAR** LANdMark Ad hoc Routing. 64

**M2M** Machine to Machine. 59

**MAC** Medium Access Control. 13, 24, 39, 54, 68, 80, 82, 99, 103, 104, 133, 137

**MANET** Mobile Ad hoc NETwork. 57, 59, 61, 63

**MANETs** Mobile Ad hoc NETworks. 57–59, 62, 63, 76

**MAP** Mesh Access Point. 74, 76

**mETX** Modified ETX. 77

**MIMO** Multiple Input, Multiple Output. 23

**MP** Mesh Point. 74–76

**MPP** Mesh Portal Point. 75

**MPR** Multi-Point Relay. 67, 68

**NAV** Network Allocation Vector. 35, 51, 103

**NDP** Neighbor Discovery Protocol. 73

**NS-2** Network Simulator version 2. 38, 53, 93, 103, 108

**OAR** Opportunistic Auto Rate. 50, 51, 148

**OFDM** Orthogonal Frequency Division Multiplexing. 23, 41, 53, 151

**OGM** OriGinator Message. 68

**OLPC** One Laptop Per Child. 74

**OLSR** Optimized Link State Routing. 57, 64, 66–68, 73

**OMR** Opportunistic Multi-Path Reliable Routing Protocol. 89

**OSI** Open Systems Interconnection. 13, 137

**PCF** Point Coordination Function. 30

**PDA** Personal Digital Assistant. 57

**PER** Packet Error Rate. 39–41, 44, 45, 47, 103, 107, 109, 111–113, 115–117, 120, 128, 148–150

**PF** Potential Forwarder. 96

**PHY** PHYsical Layer. 24

**PIFS** PCF Inter-Frame Spacing. 29, 30

**PLCP** Physical Layer Convergence Protocol. 39, 40

**PREP** Path Reply. 75, 76

**PREQ** Path Request. 75, 76

**PSK** Pre Shared Key. 24

**QAM-16** Quadratic Amplitude Modulation (16 symbols). 41, 43, 148

**QAM-64** Quadratic Amplitude Modulation (64 symbols). 41, 43, 148

**QoS** Quality of Service. 30

**QPSK** Quadratic Phase-Shift Keying. 41, 42, 148

**RADIUS** Remote Access Dial In User Service. 24

**RANN** Root Annoucement. 76

**RBF** RSSI Based Forwarding. 64, 65, 82

**RERR** Route Error. 71–73

**RFC** Request For Comment. 60, 62, 68, 70, 72, 73

**ROLL** Routing Over Low power and Lossy links. 60, 68

**RPL** IPv6 Routing Protocol for Low-Power and Lossy Networks. 60, 61, 66, 68–70, 148

**RREP** Route Reply. 71, 72, 148

**RREQ** Route Request. 71, 72, 148

**RSSI** Radio Signal Strength Indicator. 25, 47, 52, 82, 94, 95, 104, 105, 107, 125

**RTS** Request-To-Sent. 29, 30, 35, 51, 80, 82, 87, 104, 139, 148

**RxC** Reception Coordination. 103, 104

**SDF** Selection diversity forwarding. 86, 87, 123, 149

**SHF** Super High Frequency. 9

**SIF** State-free Implicit Forwarding. 64, 81, 82, 149

**SIFS** Short Inter-Frame Spacing. 29, 30, 38, 98, 125, 130, 131

**SINR** Signal to Interference plus Noise Ratio. 39, 40, 44–46, 48, 49, 78, 148

**SIP** Session Initiation Protocol. 58

**SNR** Signal Noise Ratio. 10, 107

**SSID** Service Set IDentification. 1, 2, 27, 28, 36, 133

**STA** STAtion. 74

**SURAN** SURvivable rAdio Network. 57

**TCL** Tool Command Language. 38, 103

**TCP** Transmission Control Protocol. 3, 13, 53, 61

**TDMA** Time Division Multiplexing Access. 13–15, 147

**TORA** TORA. 57

**TTL** Time To Live. 73

**TxC** Transmission Coordination. 104

**UDP** User Datagram Protocol. 52, 68, 132, 134

**UHF** Ultra High Frequency. 9, 10, 62

**UMTS** Universal Mobile Telecommunications System. 10, 13, 14

**V2I** Vehicule-to-Infrastructure. 58

**V2R** Véhicule-to-Roadside. 58

**V2V** Vehicule-to-Vehicule. 58

**VANETs** Vehicular Ad hoc NETwork. 58, 59

**VLF** Very Low Frequency. 9

**VT** Village Telco. 57

**WCETT** Weighted Cumulativ ETT. 78

**WEP** Wireless Encryption Protection. 24

**WHAN** Wireless Home Ad hoc Network. 60

**WiFi** Wireless Fidelity. 8, 10, 18, 19, 22, 24, 25, 27, 28, 31, 47, 55, 132, 147

**WPA** Wireless Protected Access. 24

**WPA1** Wireless Protected Access. 24

**WPA2** Wireless Protected Access. 24

**WPS** Wireless Protected Setup. 29

**ZRP** Zone Routing Protocol. 73, 74

# Liste des figures

# Liste des tableaux

# Bibliographie


[AAM13] P. Gronerth A. Achtzehn, L. Simic and P. Mahonen. Survey of ieee 802.11 wifi deployments for deriving the spatial structure of opportunistic networks. In *Proceeding 24th Annual Conference on Personal Indoor and Mobile Radio Communications*, pages 1–4, 2013.

[ABB+04] Daniel Aguayo, John Bicket, Sanjit Biswas, Glenn Judd, and Robert Morris. Link-level measurements from an 802.11 b mesh network. *ACM SIGCOMM Computer Communication Review*, 34(4) :121–132, 2004.

[Abr70] Norman Abramson. The aloha system : another alternative for computer communications. In *Proceedings of the November 17-19, 1970, fall joint computer conference*, pages 281–285. ACM, 1970.

[AGS11] Michael Adeyeye and Paul Gardner-Stephen. The village telco project : a reliable and practical wireless mesh telephony infrastructure. *EURASIP Journal on Wireless Communications and Networking*, 2011(1) :1–11, 2011.

[All06] ZigBee Alliance. Zigbee specification. *Document 053474r06, Version*, 1, 2006.

[ALRS09a] Azlan Awang, Xavier Lagrange, and David Ros Sanchez. A Cross-Layer Medium Access Control and Routing Protocol for Wireless Sensor Networks. In *10èmes Journées Doctorales en Informatique et Réseaux, 2-4 février, Belfort, France*, 2009.

[ALRS09b] Azlan Awang, Xavier Lagrange, and David Ros Sanchez. RSSI-based forwarding for multihop wireless sensor networks . *Lecture notes in computer science*, 5733 :138 – 147, august 2009.

[AWW05] Ian F Akyildiz, Xudong Wang, and Weilin Wang. Wireless mesh networks : a survey. *Computer networks*, 47(4) :445–487, 2005.

[Bah06] Michael Bahr. Proposed routing for ieee 802.11 s wlan mesh networks. In *Proceedings of the 2nd annual international workshop on Wireless internet*, page 5. ACM, 2006.

[Bah07] Michael Bahr. Update on the hybrid wireless mesh protocol of ieee 802.11 s. In *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference on*, pages 1–6. IEEE, 2007.

[BCD+02] Scott Burleigh, Vinton Cerf, Robert Durst, Kevin Fall, Adrian Hooke, Keith Scott, and Howard Weiss. The interplanetary internet : a communications infrastructure for mars exploration. In *IAF abstracts, 34th COSPAR Scientific Assembly*, volume 1, page 700, 2002.

[BCJP07] Chiara Boldrini, Marco Conti, Jacopo Jacopini, and Andrea Passarella. Hibop : a history based routing protocol for opportunistic networks. In *World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium on a*, pages 1–12. IEEE, 2007.

[BCL+09] Paramvir Bahl, Ranveer Chandra, Patrick PC Lee, Vishal Misra, Jitendra Padhye, Dan Rubenstein, and Yan Yu. Opportunistic use of client repeaters to improve performance of wlans. *IEEE/ACM Transactions on Networking (TON)*, 17(4) :1160–1171, 2009.

[Bey90] David A Beyer. Accomplishments of the darpa suran program. In *Military Communications Conference, 1990. MILCOM'90, Conference Record, A New Era. 1990 IEEE*, pages 855–862. IEEE, 1990.

[BM05] S. Biswas and R. Morris. Exor : opportunistic multi-hop routing for wireless networks. In *ACM SIGCOMM Computer Communication Review*, volume 35, pages 133–144. ACM, 2005.

[BMJ+98] Josh Broch, David A Maltz, David B Johnson, Yih-Chun Hu, and Jorjeta Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, pages 85–97. ACM, 1998.

[C+07] Car 2 Car Communication Consortium et al. Car 2 car communication consortium manifesto. *Braunschweig, November*, 2007.

[CA12] Llorenç Cerdà-Alabern. On the topology characterization of guifi. net. In *Wireless and Mobile Computing, Networking and Communications (Wi-*

*Mob), 2012 IEEE 8th International Conference on*, pages 389–396. IEEE, 2012.

[CABM05] DouglasS.J.De Couto, Daniel Aguayo, John Bicket, and Robert Morris. a high-throughput path metric for multi-hop wireless routing. *Wireless Networks*, 11 :419–434, 2005.

[CBE03] Alberto Cerpa, Naim Busek, and Deborah Estrin. Scale : A tool for simple connectivity assessment in lossy environments. 2003.

[CBH+07] V Cerf, S Burleigh, A Hooke, L Torgerson, R Durst, K Scott, K Fall, and H Weiss. Rfc 4838, delay-tolerant networking architecture. *IRTF DTN Research Group*, 2(4) :6, 2007.

[CDV05] Dazhi Chen, Jing Deng, and Pramod K Varshney. A state-free data delivery protocol for multihop wireless sensor networks. In *Wireless Communications and Networking Conference, 2005 IEEE*, volume 3, pages 1818–1823. IEEE, 2005.

[Cha02] Benjamin A Chambers. *The grid roofnet : a rooftop ad hoc wireless network*. PhD thesis, Massachusetts Institute of Technology, 2002.

[CJA+03] Thomas Clausen, Philippe Jacquet, Cédric Adjih, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Amir Qayyum, Laurent Viennot, et al. Optimized link state routing protocol (olsr). 2003.

[CJS+10] Jung Il Choi, Mayank Jain, Kannan Srinivasan, Phil Levis, and Sachin Katti. Achieving single channel, full duplex wireless communication. In *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, pages 1–12. ACM, 2010.

[CLM11] German Castignani, Lucien Loiseau, and Nicolas Montavont. An evaluation of IEEE 802.11 community networks deployments. In IEEE, editor, *ICOIN 2011 : International Conference on Information Networking*, pages 498 – 503, 2011.

[CSEJ+07] Q. Chen, F. Schmidt-Eisenlohr, D. Jiang, M. Torrent-Moreno, L. Delgrossi, and H. Hartenstein. Overhaul of ieee 802.11 modeling and simulation in ns-2. In *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*, pages 159–168. ACM, 2007.

[CWLG97] Ching-Chuan Chiang, Hsiao-Kuang Wu, Winston Liu, and Mario Gerla. Routing in clustered multihop, mobile wireless networks with fading channel. In *proceedings of IEEE SICON*, volume 97, pages 197–211, 1997.

[Dar05] Paul Darbee. Insteon : The details. *Smarthome Technology*, pages 1–64, 2005.

[DBRP03] Samir R Das, Elizabeth M Belding-Royer, and Charles E Perkins. Ad hoc on-demand distance vector (aodv) routing. 2003.

[DCACM03] Douglas SJ De Couto, Daniel Aguayo, Benjamin A Chambers, and Robert Morris. Performance of multihop wireless networks : Shortest path is not enough. *ACM SIGCOMM Computer Communication Review*, 33(1) :83–88, 2003.

[DH07] Elizabeth M Daly and Mads Haahr. Social network analysis for routing in disconnected delay-tolerant manets. In *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*, pages 32–40. ACM, 2007.

[DLC07] Junzhao Du, Hui Liu, and Ping Chen. Omr : An opportunistic multipath reliable routing protocol in wireless sensor networks. In *Parallel Processing Workshops, 2007. ICPPW 2007. International Conference on*, pages 74–74. IEEE, 2007.

[DPZ04] Richard Draves, Jitendra Padhye, and Brian Zill. Routing in multi-radio, multi-hop wireless mesh networks. In *Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 114–128. ACM, 2004.

[Eas07] D Eastlake. Modified 802.11 tgs par and 5c. *IEEE*, 802 :11–07, 2007.

[ECM+08] Pedro Miguel Esposito, M Campista, Igor M Moraes, LHMK Costa, OCMB Duarte, and Marcelo G Rubinstein. Implementing the expected transmission time metric for olsr wireless mesh networks. In *Wireless Days, 2008. WD'08. 1st IFIP*, pages 1–5. IEEE, 2008.

[Fal03] Kevin Fall. A delay-tolerant network architecture for challenged internets. In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 27–34. ACM, 2003.

[FHM03] Kevin Fall, Wei Hong, and Samuel Madden. Custody transfer for reliable delivery in delay tolerant networks. *IRB-TR-03-030, July*, 2003.

[FWK+03] Holger Füßler, Jörg Widmer, Michael Käsemann, Martin Mauve, and Hannes Hartenstein. Contention-based forwarding for mobile ad hoc networks. *Ad Hoc Networks*, 1(4) :351–369, 2003.

[Gal06] Mikhail T Galeev. Catching the z-wave. *Embedded Systems Design*, 19(10) :28, 2006.

[HF04] Melissa Ho and Kevin Fall. Poster : Delay tolerant networking for sensor networks. In *Proc. of IEEE Conference on Sensor and Ad Hoc Communications and Networks*, 2004.

[HHSW10] D. Halperin, W. Hu, A. Sheth, and D. Wetherall. Predictable 802.11 packet delivery from wireless channel measurements. In *ACM SIGCOMM Computer Communication Review*, volume 40, pages 159–170. ACM, 2010.

[HKL+07] Tuomo Hyyryläinen, Teemu Kärkkäinen, Cheng Luo, Valdas Jaspertas, Jouni Karvo, and Jörg Ott. Opportunistic email distribution and access in challenged heterogeneous environments. In *Proceedings of the second ACM workshop on Challenged networks*, pages 97–100. ACM, 2007.

[HPS01] Zygmunt J Haas, Marc R Pearlman, and Prince Samar. The interzone routing protocol (ierp) for ad hoc networks. *draft-ietf-manetzone-ierp-01. txt, IETF MANET Working Group*, 2001.

[HPS02a] Zygmunt J Haas, Marc R Pearlman, and Prince Samar. Intrazone routing protocol (iarp). `http://tools.ietf.org/html/draft-ietf-manet-zone-iarp-02`, 2002.

[HPS02b] Zygmunt J Haas, Marc R Pearlman, and Prince Samar. The zone routing protocol (zrp) for ad hoc networks. 2002.

[HRBSD03] Martin Heusse, Franck Rousseau, Gilles Berger-Sabbatel, and Andrzej Duda. Performance anomaly of 802.11 b. In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 2, pages 836–843. IEEE, 2003.

[HRGD05] Martin Heusse, Franck Rousseau, Romaric Guillier, and Andrzej Duda. Idle sense : an optimal access method for high throughput and

fairness in rate diverse wireless lans. In *ACM SIGCOMM Computer Communication Review*, volume 35, pages 121–132. ACM, 2005.

[HT11] J Hui and P Thubert. Rfc 6282 compression format for ipv6 datagrams over ieee 802.15. 4-based networks. *Sep-2011.[Online]. Available : http ://www. ietf. org/rfc/rfc6282. txt*, 2011.

[IET12] IETF. Rpl : Ipv6 routing protocol for low-power and lossy networks. 2012.

[JL07] Kipp Jones and Ling Liu. What where wi : An analysis of millions of wi-fi access points. In *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on*, pages 1–4. IEEE, 2007.

[JMB+01] David B Johnson, David A Maltz, Josh Broch, et al. Dsr : The dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad hoc networking*, 5 :139–172, 2001.

[JMS+07] D Johnson, K Matthee, D Sokoya, L Mboweni, A Makan, and H Kotze. Building a rural wireless mesh network : A do-it-yourself guide to planning and building a freifunk based mesh network. *Meraka Institutue*, 2007.

[KB06] Can Emre Koksal and Hari Balakrishnan. Quality-aware routing metrics for time-varying wireless mesh networks. *IEEE JSAC*, 24 :1984–1994, 2006.

[Lar01] Peter Larsson. Selection diversity forwarding in a multihop packet radio network with fading channel and capture. *ACM SIGMOBILE Mobile Computing and Communications Review*, 5(4) :47–54, 2001.

[LTN+07] Pei Liu, Zhifeng Tao, Sathya Narayanan, Thanasis Korakis, and Shivendra S Panwar. Coopmac : A cooperative mac for wireless lans. *Selected Areas in Communications, IEEE Journal on*, 25(2) :340–354, 2007.

[MDK10] David Murray, Michael Dixon, and Terry Koziniec. An experimental comparison of routing protocols in multi hop ad hoc networks. In *Telecommunication Networks and Applications Conference (ATNAC), 2010 Australasian*, pages 159–164. IEEE, 2010.

[Mil03] LE Miller. Validation of 802.11 a/uwb coexistence simulation. *national institute of standards and technology (NIST), WCTG white paper*, 2003.

[MLD07] Vivek P Mhatre, Henrik Lundgren, and Christophe Diot. Mac-aware routing in wireless mesh networks. In *Wireless on Demand Network Systems and Services, 2007. WONS'07. Fourth Annual Conference on*, pages 46–49. IEEE, 2007.

[NALW08] Axel Neumann, Corinna Aichele, Marek Lindner, and Simon Wunderlich. Better approach to mobile ad-hoc networking (batman). *IETF draft, October*, 2008.

[NZJ13] NZJRS. Osm gps map. http://nzjrs.github.com/osm-gps-map/, 2013. [Online ; accessed 05-October-2013].

[PC97] Vincent Park and M Scott Corson. Temporally-ordered routing algorithm (tora) version 1 functional specification. Technical report, Internet-Draft, draft-ietf-manet-tora-spec-00. txt, 1997.

[PGH00] Guangyu Pei, Mario Gerla, and Xiaoyan Hong. Lanmar : landmark routing for large scale wireless ad hoc networks with group mobility. In *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*, pages 11–18. IEEE Press, 2000.

[PGHC99] Guangyu Pei, Mario Gerla, Xiaoyan Hong, and C-C Chiang. A wireless hierarchical routing protocol with group mobility. In *Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE*, pages 1538–1542. IEEE, 1999.

[Ph.07] Derek Smithies Ph.D. minstrel algorithm specification for linux wireless driver. Website, 2007. http://linuxwireless.org/en/developers/Documentation/mac80211/RateControl/minstrel/#EWMA.

[SAZ07] Lifeng Sang, Anish Arora, and Hongwei Zhang. On exploiting asymmetric wireless links via one-way estimation. In *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*, pages 11–21. ACM, 2007.

[SB07] Keith L Scott and Scott Burleigh. Bundle protocol specification. 2007.

[SBM06] Anand Prabhu Subramanian, Milind M Buddhikot, and Scott Miller. Interference aware routing in multi-radio wireless mesh networks. In *Wireless Mesh Networks, 2006. WiMesh 2006. 2nd IEEE Workshop on*, pages 55–63. IEEE, 2006.

[SKSK05] Bahareh Sadeghi, Vikram Kanodia, Ashutosh Sabharwal, and Edward Knightly. Oar : an opportunistic auto-rate media access protocol for ad hoc networks. *Wireless Networks*, 11(1-2) :39–53, 2005.

[VdM77] E Van der Meulen. A survey of multi-way channels in information theory : 1961-1976. *Information Theory, IEEE Transactions on*, 23(1) :1–37, 1977.

[wav01] wavenis. Wavenis technology. http://www.coronis.com/en/specifications.html, 2001. [Online ; accessed 06-September-2013].

[WIG13] WIGLE. Wireless geographic logging engine : Making maps of wireless networks since 2001. http://wigle.net, 2013. [Online ; accessed 05-October-2013].

[Win12] Tim Winter. Rpl : Ipv6 routing protocol for low-power and lossy networks. 2012.

[WMRD11] Thomas Watteyne, Antonella Molinaro, Maria Grazia Richichi, and Mischa Dohler. From manet to ietf roll standardization : A paradigm shift in wsn routing protocols. *Communications Surveys & Tutorials, IEEE*, 13(4) :688–707, 2011.