1 INTRODUCTION

De nos jours, différentes technologies d'accès aux réseaux sans-fil coexistent. A quelques exceptions près, elles permettent à un terminal de se déplacer tout en gardant une connectivité avec un réseau de cœur (réseau d'interconnexion). Plusieurs points d'attachements sont répartis dans le réseau, et assurent la connectivité des terminaux mobiles. Une caractéristique primordiale d'une technologie d'accès est la distance maximale (la portée) entre un point d'attachement et un terminal mobile, à partir duquel la réception des informations devient précaire. La zone délimitée par cette portée est appelée cellule de bas niveau. La figure 3.1 présente un terminal mobile connecté à un point d'attachement **A** relié à un réseau filaire. La portée du point d'attachement est symbolisée par la cellule **A**. Tant que le terminal mobile est situé au centre de la cellule **A**, la qualité de réception de la communication sans-fil est optimale. Plus le terminal mobile se rapprochera du bord de la cellule, plus la qualité de réception se dégradera. En dehors de la cellule **A**, le terminal mobile ne peut plus communiquer avec le point d'attachement **A**, et le terminal perd sa connectivité. Le déplacement du terminal mobile entraîne la déconnexion du terminal mobile avec le point d'attachement **A**, et la connexion avec le point **B**. Ce phénomène est le *Handover (HO)*. Les technologies d'accès sans-fil étant incompatibles, ce type de *Handover* de bas niveau ne permet pas au terminal mobile d'effectuer un mouvement entre cellules hétérogènes (technologies d'accès distinctes). Le délai *D* de déconnexion au réseau est susceptible de provoquer des pertes de paquets, et d'influencer sur les délais de transmission des autres paquets. Durant cette période, aucun paquet ne peut être transmis vers ou depuis le terminal mobile.

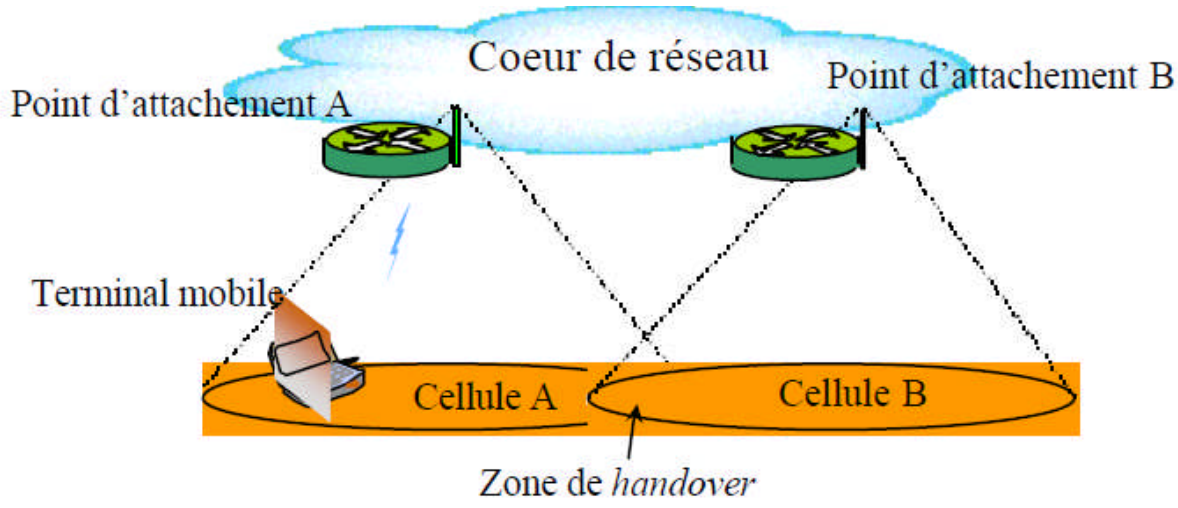

Figure 3.1 : Interaction entre un terminal mobile et le cœur de réseau

2 Handover en général

La structure cellulaire, si elle offre le principal avantage de pouvoir desservir des densités d'abonnés importantes, a pour principale inconvénient de devoir assurer les transferts des communications entre cellules. Le mécanisme assurant cette fonction est appelé transfert automatique intercellulaire ou Handover et se produit uniquement en cours de communication(en état de veille du terminal, aucun Handover n'est exécuté).

Il y a plusieurs raisons pour lesquelles des Handover doivent être exécutés. D'une façon générale les Handovers sont nécessaires quand le raccordement n'est plus satisfaisant.

Dans cette situation, un Handover est initialisé avec certaines règles. Les raisons les plus communes pour qu'un HO soit exécuté sont en raison de manque de qualité de signal ou niveau du trafic pour une station de base. [9].

2.1 Définition du Handover

Le Handover (HO) ou le transfert intercellulaire est l'ensemble des fonctions et des opérations mises en œuvre entre une ou plusieurs stations de service et une station mobile, pour permettre à cette dernière de changer son point d'attachement au réseau Internet (changement de cellule) et de bénéficier des services d'une autre cellule au lieu de l'ancienne. La station mobile aura la possibilité de continuer sa communication en cours avec un minimum d'interruption [10] sachant que les deux cellules impliquées sont gérées soit par le même réseau (Handover horizontal) soit par des différents réseaux (Handover vertical).

3 Les raisons pour exécuter le Handover

3.1 Qualité de signal

Le Handover est déclenché dans le cas où les signaux émis par une station de base voisine sont reçus avec un niveau de puissance supérieure a celle signaux issus de la station de base courante. Cette méthode présente ainsi l'inconvénient d'entrainer un nombre de handovers trop importants dans le cas où la station de base courante a une puissance insuffisante et que celle-ci peut donc encore desservir le mobile. [9].

3.2 Le trafic de Handover

Lors du dimensionnement du réseau, le taux de trafic est estimé dans chaque cellule. Il faut donc prendre en compte les appels (regroupés sous le terme de trafic <<trafic de frais>>) dans la cellule et également les appels qui en en sorte ou qui y rentrent après handover (regroupés sous le terme de <<trafic de handover>>). Le trafic de handover négligeable dans le système de première génération devient important dans les systèmes de deuxième génération et sera encore plus important dans la troisième génération.

4 Handover dans le réseau WIFI

4.1 Gestion de mobilité

La spécification 802.11 traite la mobilité de façon simple par rapport à un autre réseau (UMTS par exemple). Il n'y a pas de distinction entre gestion de localisation et gestion de handover.

4.2 Gestion de localisation

La gestion de localisation dans 802.11 diffère fortement de la gestion de localisation UMTS (par exemple).

Quand une station est associée à un AP de BSS ou ESS, le DS connait la position de la station dans le Basic Service Set (BSS) ou l'Extended Service Set (ESS). Pour que la station demeure dans le BSS/ ESS, la station doit capable de transmettre et recevoir des trames de AP.

4.3 Gestion de handover

802.11 gère le handover en termes de transition. Il existe 3 types de transitions différentes : Aucune transition, transition BSS, transition ESS.

- **Aucune transition** : tant que la station reste dans l'AP service area, elle n'effectue aucune transition.

- **Transition BSS** : si une station, initialement située dans le BSS d'un AP1 est associée à cet AP1, sort de ce BSS pour entrer dans le BSS de l'AP2 de l'ESS.

La station utilise alors le service réassociation pour s'associer avec l'AP2 qui commence alors à envoyer des trames vers la station. La transition BSS demande une communication entre les APs via le protocole IAPP. En effet, lors de réassociation, AP2 doit signaler à AP1 que la station lui est a présent associée.

Dans ce type de transition, les BSS des APs doivent se supposer en partie pour assurer la mobilité des stations. [9].

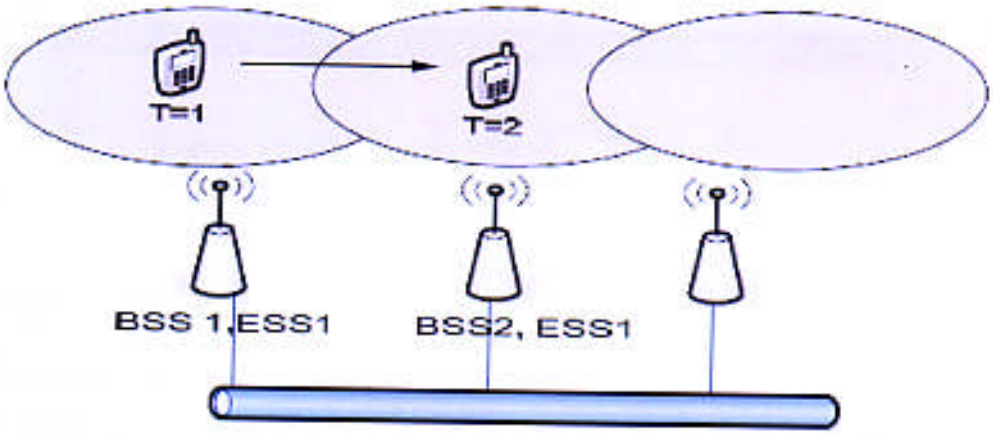

Figure **3.2 : Transition BSS [9]**

- **Transition ESS** : une transition ESS correspond au mouvement d'une station d'un ESS1 vers un ESS2 distinct. 802.11 supporte ce type de transition dans le sens où la station peut s'associer à

un AP de l'ESS2 en quittant l'ESS1 mais aucune garantie n'est faite quand maintien de la connexion. Dans la pratique, la connexion est supposée se couper. Ceci signifie que les connexions de couche réseau et les couches supérieures sont rompues. Afin de conserver les connexions de couche réseau, le recours à des protocoles de mobilité est requis.

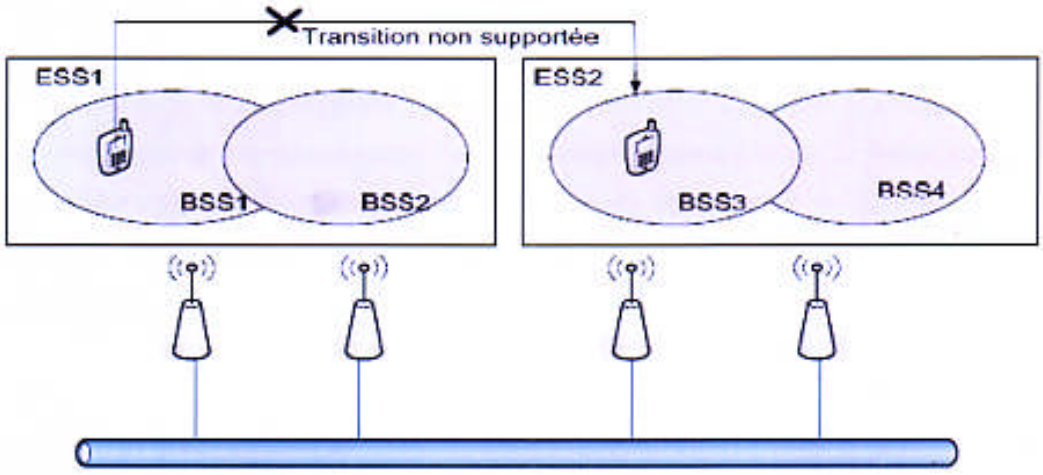

Figure 3.3 : Transition ESS [9]

5 L'utilisation de handover

Le handover a pour principales fonctions de permettre :

- aux utilisateurs de se déplacer pendant un appel.
- d'équilibrer la charge du trafic entre cellules.
- le maintien d'une qualité acceptable pour l'usager en cas d'interférences.
- d'optimiser l'utilisation des ressources radio,

5.1 Il existe trois cas où un handover est nécessaire

• **Rescue Handover** : la station mobile quitte la zone couverte par une cellule vers une autre. C'est la qualité de transmission qui détermine la nécessité du handover, qualité indiquée par le taux d'erreur, l'intensité du signal reçu, le niveau d'interférences et le délai de propagation.

• **Confinment handover** : la station mobile subirait moins d'interférences si elle changeait de cellule (les interférences sont dues en partie aux autres stations mobiles dans la cellule). La station mobile écoute en permanence d'autres cellules pour mesurer la qualité d'une connexion à ces dernières. De plus, chaque station mobile est synchronisée avec plusieurs BTS pour être prête en cas de handover.

• **Traffic Handover** : le nombre de stations mobiles est trop important pour la cellule, et des cellules voisines peuvent accueillir de nouvelles stations mobiles. Cette décision nécessite de connaître la charge des autres BTS. Le handover tient compte de la direction du mouvement.

6 Types de handover

Il existe plusieurs types, parmi ces types on a :

6.1 Hard handover

Le mécanisme du Hard Handover est appliqué généralement dans le cas d'une mobilité relativement lente ou moyenne. Durant le Handover, ce mécanisme oblige la station mobile à interrompre la connexion avec l'ancienne station de base avant d'établir la connexion avec la nouvelle station de base (mécanisme Break-Before-Make).[11].

Ce type de Handover est utilisé dans les systèmes cellulaires, ou chaque cellule à une bande de fréquences différentes. Quand l'utilisateur entre dans une nouvelle cellule, il entraine la démolition de la connexion existante avant qu'une nouvelle connexion utilisant une autre fréquence soit établie dans la cellule visitée, l'algorithme de ce type de handover est assez simple ; la station mobile effectue un Handover lorsque la puissance du signal d'une cellule voisine dépasse la puissance du signal de la cellule actuelle à un seuil donné.

Le problème majeur du hard Handover c'est la coupure de communication causé par la non disponibilité des ressources. Ce problème peut être résolu par l'introduction d'un critère de priorité concernant l'allocation des ressources. Dans une cellule donnée, la demande des ressources pour Handover est prioritaire par rapport aux nouvelles demandes. Cette idée mène à une mauvaise efficacité spectrale puisque, pour une cellule donnée, on aura des ressources non utilisées lorsqu'il n'y a pas de demandes de Handover vers cette cellule ce qui implique un blocage pour les nouvelles demandes.

Ce mécanisme est bénéfique du point de vue de l'allocation des ressources, mais en cas d'échange du trafic temps-réel de volume important, ou dans le cas du déplacement du mobile avec une vitesse importante, ce mécanisme provoque une interruption de service au cours du Handover, ce qui n'est pas bon pour le trafic temps-réel. [11].

Le Handover du GSM est un Hard Handover car le circuit est complètement relâché avant qu'un nouveau soit établit. Aussi le réseau WIMAX utilise ce type de Handover.

Figure 3.4 : Hard handover

6.2 Soft handover

Le mobile se trouve dans la zone de la couverture commune à deux stations de base. Le mobile et la station de base utilise simultanément deux canaux radios, deux signaux sont donc reçus par le mobile. Notons que de point de vue du mobile, il existe très peu de différence entre un soft handover et softer handover. Le soft-Handover est réalisable, si le mobile est capable de communiquer simultanément avec plusieurs routeurs d'accès (mécanisme make-before-Break) soit le mobile dispose de plusieurs interfaces sans-fil (homogène ou hétérogène), soit la

technologie d'accès permet la connexion du mobile vers plusieurs routeurs d'accès (802.11 en mode ad-hoc, ou WCDMA) [12].

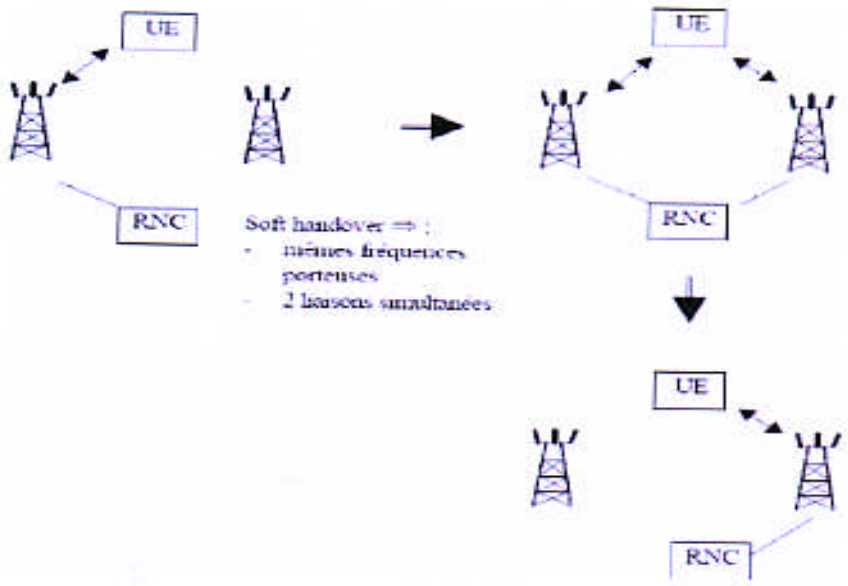

Figure 3.5 : Soft handover

7 Les différentes phases d'exécution de handover

7.1 Qualité de signal

Si le rapport de signal/bruit diminue au-dessous d'un certain niveau c'est-à-dire la diminution de la qualité de signal qui est indiqué par le système, le HO sera exécutée.

7.2 Qualité de service appliquée dans le handover

Quand un utilisateur se déplace loin de son AP dans les réseaux WiFi, la puissance de signal reçue se dégrade et que son AP ne peut plus répondre à sa demande en termes du débit supporté et du taux de la perte paquet. Il doit passer de son AP courant à un nouveau AP, avec laquelle il a une meilleure réception du signal. Cependant, même si cet utilisateur a choisi de se connecter à un nouveau AP, ce dernier ne peut pas répondre de façon certaine à sa demande s'il ya déjà des charges importantes sur cet AP. Ces charges de l'AP sont constituées par les différents utilisateurs qui n'ont pas le même niveau de priorité de service dans les réseaux, de même pour les différents types d'applications qui n'ont pas la même demande qualitative. Chaque application a une demande qualitative particulière, par exemple, l'application VOIP n'a besoin qu'une bande passante faible, tolère un certain niveau de perte de paquet, mais elle a des contraintes très fortes sur le délai et l'application FTP demande plus de bande mais elle tolère un

certain niveau du délai. Par conséquent, la Qualité de service (en anglais Quality of Service – QoS) doit être appliquée dans les réseaux pour mieux servir aux utilisateurs selon leurs priorités, leurs demandes qualitatives et équilibrer les différentes besoins des utilisateurs. La QoS est définie comme l'effet général de la performance du service qui détermine le degré de satisfaction d'un utilisateur du système par l'Union Internationale des Télécommunications [ITU94].

8 Les différentes phases du Handover

8.1 Phase de découverte

La notion de découverte est importante car elle pose de nombreuses difficultés. La procédure du Handover suppose un grand nombre de mesures pour qu'un mobile puisse découvrir son environnement et les points d'accès auxquels il peut potentiellement s'attacher.
Ces mesures sont :

- la puissance du signal reçu (qui est un indicateur de qualité).
- le taux d'erreur binaire.
- la distance entre le mobile et le point d'attachement.

Dans la phase du Handover vertical, ce dernier doit être utilisé en conjonction avec les mesures (signal reçu, taux d'erreur,..). Les éléments sont les suivants :

- Type de service : On peut avoir différents types de service qui demande des qualités de service différentes.
- Le coût : il s'agit d'un élément très important pour l'utilisateur, car les opérateurs vont utiliser des stratégies de taxation qui vont déterminer son choix.
- Paramètres réseau : les paramètres de réseau comme le trafic, la bande passante disponible.
- Performance du système : On peut inclure ici des paramètres de canal comme la BER, l'interférence. La batterie peut avoir aussi une influence dans le handover.

8.2 Phase de décision

Lorsque des paramètres mesurés sur l'accès courant franchissent certains seuils (puissance de signal, taux de perte), le mécanisme de HO est déclenché.

La phase de décision qui vient une fois que le mobile a déjà acquis son environnement et qui consiste à choisir parmi la liste des AR disponibles le prochain AR auquel il va s'attacher. Ce choix peut être fait par le mobile ou par une entité dans le réseau. La seconde approche est

souvent utilisée pour préparer l'attachement avant que le changement de AR ne soit commencé afin de réduire le temps d'interruption.

En fonction du niveau de la pile réseau auquel on se place, les informations utilisées pour prendre la décision ne sont pas de même nature. De plus en plus d'approches cherchent à

S'affranchir de la séparation stricte en couche dont on n'est plus très sûr qu'elle soit bien adaptée à la gestion de la mobilité. Elle limite, en effet, le cheminement des données utiles au déclenchement du Handover puis à la sélection du prochain AR, surtout en environnement hétérogène ou chaque niveau liaison ne dispose que des informations relatives à sa technologie d'accès et ne voit pas les AR des autres technologies présentes dans la zone.

8.3 Phase d'exécution du Handover

La phase d'exécution comprend l'attachement au nouvel AR, c'est-à-dire l'ensemble des actions que le mobile doit entreprendre pour être capable de communiquer à travers le nouvel AR. Une fois l'attachement effectué, il est nécessaire de faire la publicité de la nouvelle localisation pour permettre aux nouveaux correspondants de joindre le mobile en fonction d'une identité qu'ils connaissent. Il s'agit donc d'avertir le réseau et/ou les correspondants courants ou potentiels de la nouvelle position du mobile. Il faut ensuite diriger le trafic vers la nouvelle position. Dans le cas de la mobilité IP les deux dernières actions sont combinées lors des mises à

jour d'association qui informe l'agent mère (ou Home Agent) ou les correspondants pour qu'ils envoient leur trafic vers la nouvelle position.

9 Communications vertes (green communications) :

9.1 Définition

Green Communications offre une toute nouvelle technologie pour les réseaux qui permet de réaliser des connexions afin de garantir une bonne qualité de service tout en économisant l'énergie.

Green Communications fournit des équipements de réseau contenant des ressources virtuelles qui sont capables, aussi bien dans un réseau filaire que sans fil, pour mettre en place des réseaux performants qui consomment le moins possible d'énergie et de ressources. Les réseaux peuvent être de type Mesh, ad hoc ou filaire en utilisant la technologie Start & Stop de Green Communications. En outre, le routage et la virtualisation offrent des fonctions plus efficaces concernant la qualité de service et la consommation d'énergie.

Green Communications peut donc créer des réseaux à la demande pour optimiser les performances tout en diminuant les ressources utilisées [14].

9.2 Green Communications introduit la qualité de service dans les réseaux sans fil « low cost »

Les solutions mesh existantes sont principalement basées sur des points d'accès Wi-Fi et souffrent de la fluctuation du signal, des déconnexions fréquentes et des interférences. Un canal Wi-Fi est soumis à des nombreuses perturbations réduisant ses performances et sa robustesse.

Green Communications introduit la qualité du service dans les réseaux maillés où les liens Wi-Fi sont estimés avec précision. L'estimation est diffusée aux routeurs du réseau afin de sélectionner en permanence les chemins pour le transfert de données. La solution proposée met fin aux déconnexions possibles et maintient une communication stable et robuste et élimine aussi toute émission radio inutile pour diminuer la propagation des ondes parasites.

9.3 Les avantages de Green communications

9.3.1 Economie d'énergie

- Qualité de service dans les réseaux sans fil « low cost ».

- Réduction des interférences et d'ondes parasites.
- Absence de signalisation supplémentaire.
- Virtualisation associée à des systèmes autonomes.

9.3.2 Marchés

- Connectivité dans des zones pauvres en énergie.
- Connectivité bas coût.
- Connexion en terrain hostile et en terrain dynamique (jeu, rassemblements …).

10 Handover dans le wifi mesh

Il existe plusieurs types de handover dans le réseau mesh, parmi eux [15] :

1- Intra-système HO: se produit dans un seul système. Cela peut être divisée en intra-fréquence HO et Inter-fréquence HO. L'Intra-fréquence se produit entre les cellules appartenant à un même support réseau maillé sans fil, tandis que l'inter-fréquence se produit entre des cellules fonctionnant sur différents supports de réseau maillé sans fil.

2- Inter-système HO: a lieu entre les cellules appartenant à deux différentes technologies d'accès radio (RAT) ou différents modes d'accès radio (RAM).

3- Hard HO: une catégorie de procédure en HO où toutes les anciennes liaisons radio d'un mobile sont libérés avant que les nouvelles liaisons radio sont établies.

4- Soft HO : est une technique qui permet au mobile de se déplacer d'un routeur d'accès à un autre routeur d'accès sans déconnexion. Ainsi le mobile a toujours une connectivité de bonne qualité avec le réseau de cœur.

11 Conditions d'exécution de Handover

- Un nœud mobile fonctionne et passer d'une zone de couverture d'un AP vers un autre AP.
- Un nœud mobile qui se trouve dans l'intersection de deux couvertures provoque l'augmentation de taux d'erreur => qualité de transfert.
- Le trafic est important, donc on a besoin d'un handover pour établir une connexion avec un nouveau AP.

12 Objectif de Handover

- ✓ garantir la continuité des services sans fil.
- ✓ Garder la QoS nécessaire.
- ✓ Minimiser le niveau d'interférence de l'ensemble du système en gardant le mobile attaché avec l'AP le plus fort.
- ✓ Itinérance entre différents réseaux.
- ✓ Distribution de charges sur les zones de points chauds (équilibrage de charge).

13 Soft Handover :

Cette partie détaille le fonctionnement de soft handover qui a de bons avantages. Cependant il a aussi des inconvénients de la complexité et de la consommation des ressources supplémentaires.

13.1 Le principe de soft handover :

Durant le soft handover, le mobile étant en communication avec une seule station de base, il utilise simultanément deux canaux radio. Dans le sens descendant, deux codes d'étalement sont activés pour que le mobile distingue les signaux issus des deux secteurs. Dans le sens

montant, les signaux émis par le mobile sont reçus par les deux secteurs de la station de base et dirigés vers le même récepteur. Ils sont donc combinés au niveau de la station de base.

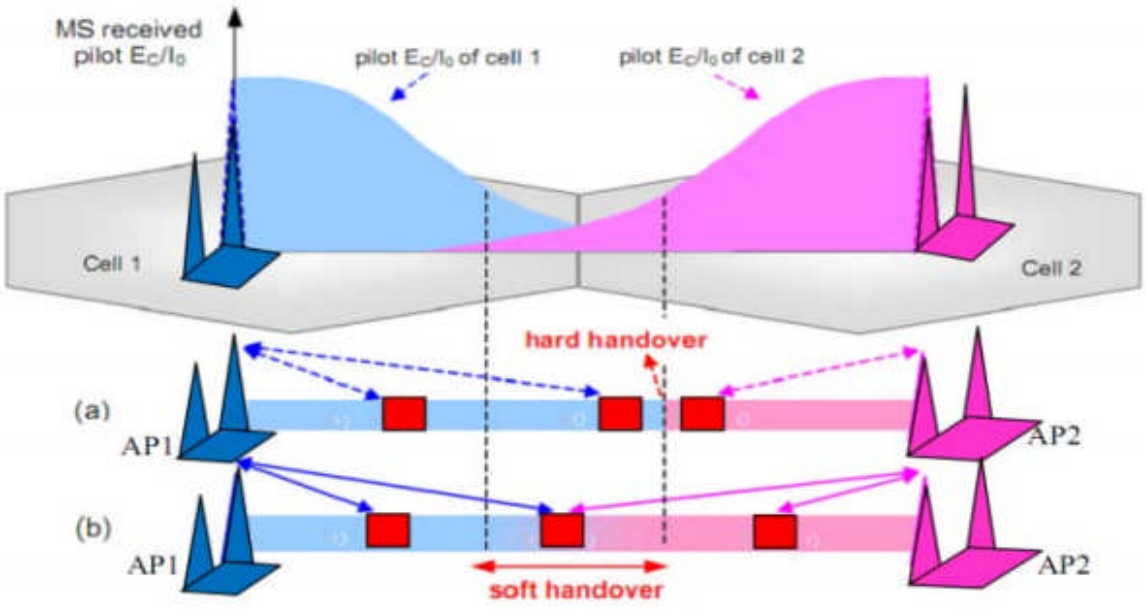

Figure 3.6 : comparaison entre soft et hard handover

Cette figure montre le processus de base entre hard handover et soft handover, il s'agit d'un nœud mobile qui passe d'un AP1 à AP2. Pendant la mobilité, le nœud mobile mesure continument la puissance du signal pilotée reçue de l'AP à proximité.

13.2 Algorithme de soft handover

Comme il est illustré sur la figure 3.7, le soft handover peut être divisé en trois phases: évaluation, décision et exécution [16],

- Dans la phase de mesure, l'information est nécessaire pour prendre la décision de handover.

- Dans la phase de décision, les résultats de mesure sont comparés à des seuils prédéfinis pour prendre la décision du handover ou non.

- Dans la phase d'exécution, le processus de transfert est achevé et les paramètres relatifs sont modifiés, en fonction des différents types de handover. La performance du soft handover est étroitement liée à l'algorithme**.**

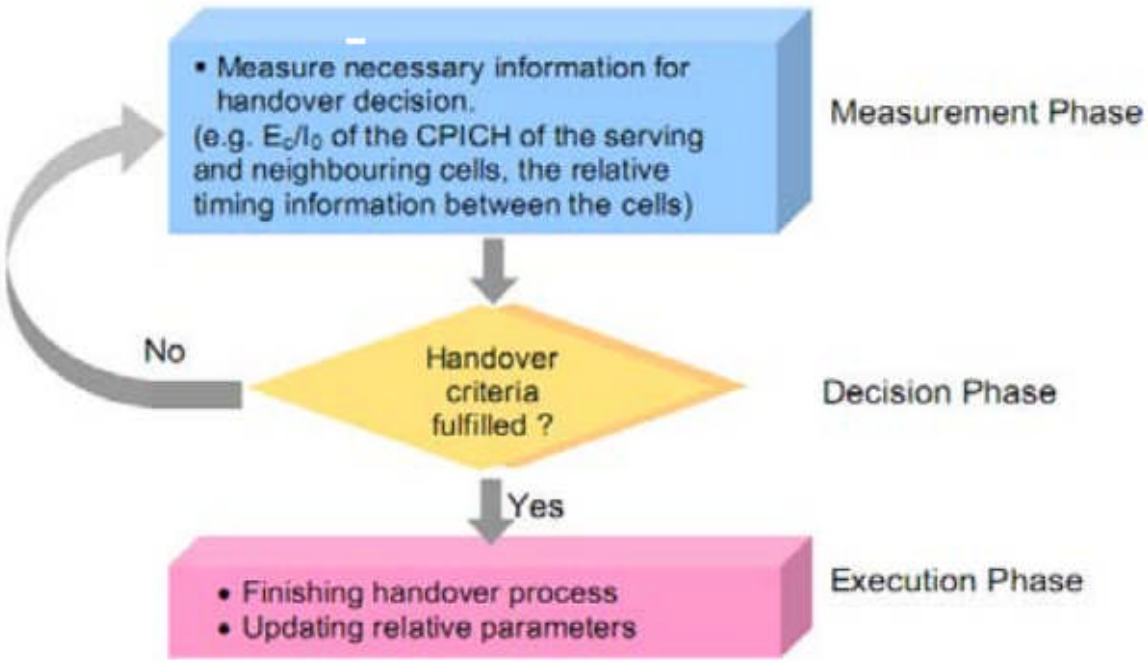

Figure 3.7 : la procédure de soft handover

14 Conclusion

Dans ce chapitre, dans un premier temps, Le Handover est le processus qui permet, à un terminal mobile, d'effectuer le passage entre deux points d'attachement à un réseau. Ce changement de point d'attachement implique une déconnexion momentanée du terminal mobile, et des perturbations des communications en cours. Ainsi, pour disposer d'une communication de qualité avec un terminal mobile, le Handover doit introduire dans plusieurs réseaux (mesh, ad hoc). Plusieurs techniques de Handover ont été proposées. a fin que la performance de handover seras efficace.

1. Introduction

Le simulateur de réseau NS (Network Simulator) est un simulateur à événements discrets développé par l'université de Californie. Il permet la simulation d'un grand nombre de réseaux locaux et/ou étendus, filaires ou sans fil.

En 1998, l'université de Carnegie Mellon a ajouté une extension sans fil connue sous le nom de Monarch. Il permet au simulateur de simuler des nœuds mobiles connectés par des interfaces réseau sans fil. Le simulateur permet de réaliser des simulations de transferts de données sur un réseau, de mesurer des débits, des taux de perte et des latences.

Dans ce chapitre, on va décrire ce simulateur et on va examiner un scénario de simulation dans le réseau wifi mesh 802.11s après et avant l'excusions du handover

2. Définition

NS est un outil logiciel de simulation de réseaux informatiques développé lors d'un projet de la **DARPA**. Il est devenu aujourd'hui un standard de référence en ce domaine. C'est un logiciel dans le domaine public disponible su l'Internet. Son utilisation est gratuite. Le logiciel est exécutable tant sous Unix que sous Windows. Le Simulateur se compose d'une interface de programmation en **tcl** et d'un noyau écrit en **C++** dans lequel la plupart des protocoles réseaux ont été implémentés.

- **Traffic**: WEB, CBR, FTP, etc.
- **Couche Transport :** TCP, UDP
- **Couche Réseaux :** routage dans les réseaux ad hoc (AODV, DSR, DSDV, TORA), routage dans les réseaux filaire (Link state, Distance Vector).
- **Couche MAC :** CSMA, CDMA, liens satellite, etc.

Le simulateur peut être vu sous deux aspects :

- La spécification des protocoles et la création des classes de base, principalement codée En **C++.**
- La spécification et la configuration des scénarios, codée en **Otcl.**

Interface utilisateur **(Contrôle)** Langage Otcl
Cœur du simulateur **(Données)** Langage C++

3. Organisation du simulateur

NS-2 est un interpréteur de commandes OTcl qui comporte un ordonnanceur d'événements et une bibliothèque des composants réseaux. L'utilisation de NS-2 se fait en trois temps comme montre la figure suivante :

Fichier .tcl ns Fichier.tcl -network animator(NAM)

-fichier trace

FIGURE 4.1 : Flot de simulation avec NS-2.

1) L'utilisateur écrit un script Otcl pour définir la topologie du réseau, pour instancier les différents modules du réseau et pour décrire des scénarios de trafic.

2) NS-2 interprète le script et exécute la simulation. Les résultats sont stockés dans des fichiers en fonction des commandes du simulateur utilisé.

3) Une fois la simulation terminée, les résultats peuvent être analysés directement avec l'outil de visualisation NAM et un fichier de trace.

3.1) Network Animator

Il permet de visualiser le déroulement d'une simulation en affichant la topologie du réseau et le déplacement des paquets.

3.2) Fichier trace

L'exécution d'un Fichier.tcl donne un fichier trace contient un événement (d'émission, de réception ou de suppression), le temps simulé auquel chaque événement est arrivé, le type et la taille du paquet.

4. Architecture du réseau

NS-2 permet de construire des réseaux fonctionnant sur le principe de la commutation de paquets. Le paquet est l'élément d'information qui circule sur un réseau. Il comporte un en- tête avec les paramètres spécifiques au protocole utilisé. Il contient également un espace qui modélise les données échangées entre les composants du réseau.

Pour définir un réseau, il faut assembler les différents composants suivants :

- **Nœuds** : endroits où est généré le trafic, ou noeuds de routage.
- **Liens** de communication entre les réseaux.
- **Agents** de communication, représentant les protocoles de niveau transport (TCP, UDP); ces agents sont attachés aux noeuds et connectés l'un à l'autre, ce qui représente un échange de données (connexion TCP, flux UDP).
- **Applications** qui génèrent le trafic de données selon certaines lois, et se servent des agents de transport.

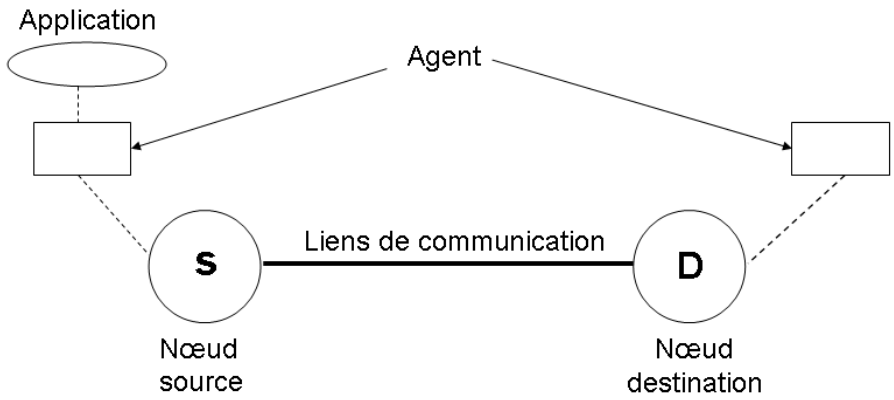

FIGURE 4.2 : Composants d'un modèle de réseaux en NS.

5. Création d'un scénario

Pour décrire un réseau et son trafic, il faut définir dans l'ordre :

1. la topologie du réseau : les noeuds et les liaisons.
2. la couche transport (UDP, TCP, ...) entre des pairs de nœuds.
3. la couche application qui va fournir les données.
4. des temporisateurs précisant les instants auxquels les transferts vont démarrer.

6. Les modules nécessaires pour la simulation

Le Neighbor Discovery (ND), le module Media Independent Handover (MIH) et le module de gestion de mobilité (MIPv6) sont les éléments clés utilisés dans le code de simulation.

6.1. Module de découverte voisin

Le module ND est utilisé pour fournir la détection de mouvement de la couche3. Dans le réseau, la BS envoie périodiquement des messages RAs (Router Advertisement) pour informer les MNs au sujet du préfixe de réseau. L'agent de ND situé dans le MN reçoit ces RAs et détermine si le message contient un nouveau préfixe et informe le directeur d'interface. Un temporisateur est associé au préfixe. Quand le préfixe est expiré, un avis est envoyé au directeur d'interface. L'implémentation supporte également RS (Router Solicitation) pour permettre à un MN de découvrir une nouvelle BS après un Handover.

6.2. Media Independent Handover (MIH IEEE 802.21)

La réalisation de handover entre des réseaux d'accès hétérogènes de manière transparente du point de vue de l'utilisateur mobile (sans couture ni détérioration) nécessite la prise en compte de certaines notions telles que la continuité de service, la qualité de service, la découverte et la sélection du réseau **[17] [18]**.

Le groupe de travail IEEE 802.21 a pour cela créé une architecture de base qui définit une fonction MIHF « Media Independent Handover Function » qui va aider les systèmes mobiles à effectuer un handover sans couture entre des réseaux d'accès hétérogènes tels que IEEE 802.3 (réseau local filaire), IEEE 802.11x (réseau local sans fil), IEEE 802.16e (réseau WiMAX mobile), GPRS et UMTS (réseau mobile 3G).

6.2.1. Présentation du standard IEEE802.21

Le standard IEEE 802.21 **[17]** consiste en l'élaboration d'une architecture qui permet la continuité de service de manière transparente lorsque le terminal mobile (MN) passe entre deux réseaux hétérogènes au niveau liaison de données.

Un ensemble de fonctions permettant l'optimisation du Handover est défini dans la pile protocolaire de gestion de mobilité MME (Mobility Management Entity) des éléments du réseau et il y a une création d'une nouvelle entité appelée MIHF (Media Independent Handover Function). Cela fonctionne sur la couche 3 et peut communiquer entre les interfaces locales et à distance. Les interfaces à distance peuvent être entrées en contact par l'intermédiaire d'un autre MIHF. Ceci est illustré sur la figure ci-dessous.

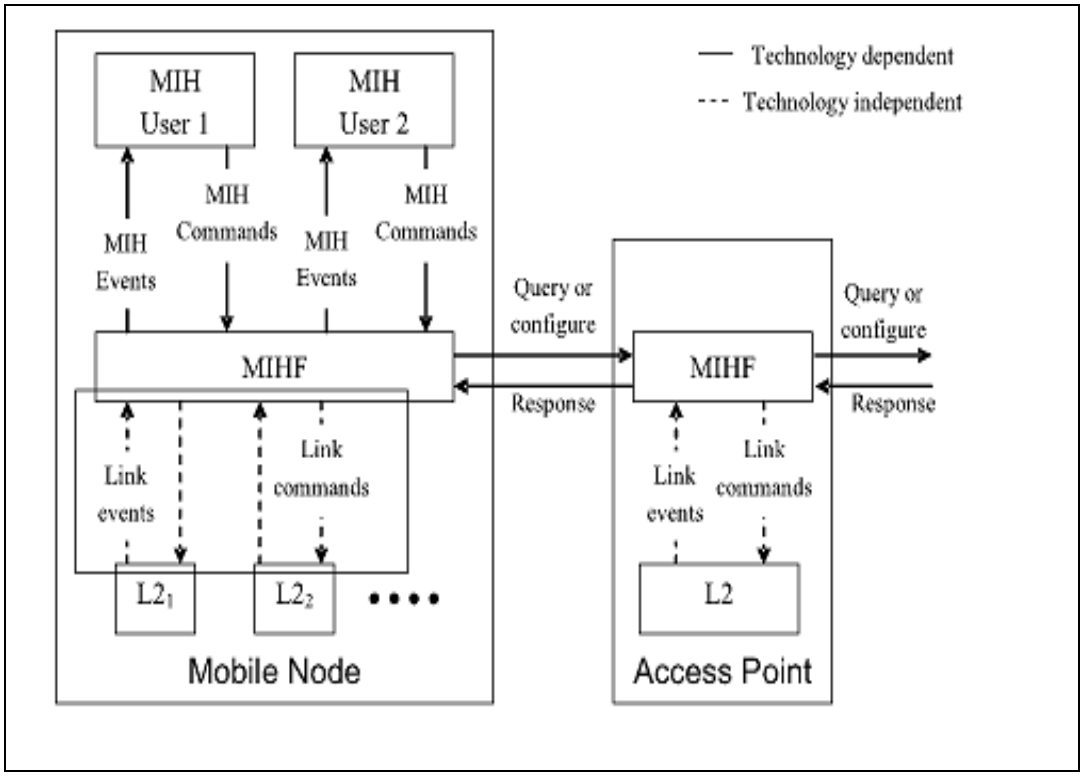

Figure 4.3 : Vue d'ensemble de conception de MIH [19].

6.3. La gestion de mobilité MIPv6

Le MIPv6 décrit un moyen de gérer la mobilité de terminaux IPv6. Cette mobilité permet qu'un terminal IPv6 soit toujours joignable quelle que soit sa localisation dans l'Internet et que ses connexions en cours restent actives malgré ses déplacements.

La figure ci-dessous comportant plusieurs acteurs :

- Le terminal mobile (MN) : est le terminal IPv6 pouvant se déplacer ;
- L'agent mère (Home Agent, HA) : est un équipement de réseau qui gère la mobilité à la manière d'un HLR dans les réseaux cellulaires ;
- Terminal correspondant (Correspondent Node, CN) : est un terminal IPv6 avec qui MN a ou aura une connexion active ;

On distingue deux types de réseaux sur lesquels MN peut venir se connecter :

Réseau mère : est le réseau d'origine de MN, ou il est adressable par son adresse mère (HA : Home adress).

Réseau visité : est le réseau où se déplace MN. Lors de son arrivée dans ce type de réseau, MN récupère grâce au mécanisme d'auto-configuration d'IPv6 **[20]** une adresse IPv6 topologiquement correcte appelée adresse temporaire (Care-of Address).

Le principe de base de Mobile IPv6 est que MN est toujours adressable par son adresse mère, qu'il soit sur son réseau mère ou sur un réseau visité.

Dans le cas où MN est dans son réseau mère, le routage des paquets s'effectue de manière standard, en se basant sur les tables des routeurs. MN n'est ni plus ni moins qu'un terminal IPv6 "fixe".

Dans le cas où MN effectue un mouvement pour aller sur un réseau visité ❶, celui-ci récupère une adresse temporaire sur ce réseau ; c'est-à-dire appartenant au préfixe utilisé sur ce lien du réseau. Il enregistre sa nouvelle position auprès de l'agent mère ❷, grâce à un message appelé Binding Update (BU) comportant à la fois son adresse mère et son adresse temporaire, et attend une confirmation de sa part ❸ sous la forme d'un message appelé Binding Acknowledgment (BA). L'agent mère joue alors le rôle de proxy et intercepte tous les paquets à destination de l'adresse mère pour les orienter vers la nouvelle position de MN - c'est-à dire son adresse temporaire « primaire ».

MN signale sa nouvelle position ❹ aux correspondants avec lesquels il était en communication, toujours grâce aux messages BU et BA, afin d'optimiser les communications (les communications ne seront plus envoyées à l'adresse mère puis orientées par l'agent mère vers l'adresse temporaire "primaire", mais directement envoyées du correspondant vers le mobile).

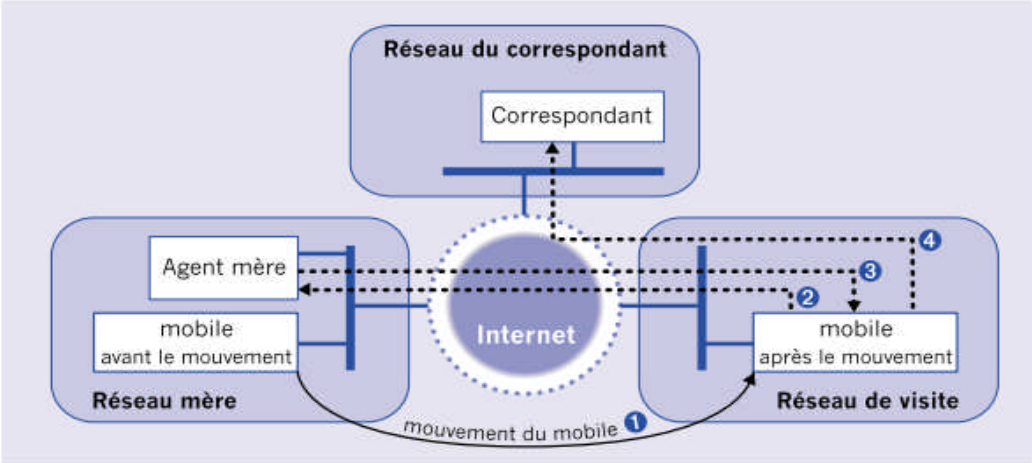

Figure 4.4 : Mécanisme de base de mobilité IPv6.

La figure 4.5 montre le déroulement de la connexion optimisée. Si un autre correspondant CN veut communiquer avec MN, il envoie son premier paquet à l'adresse mère de MN ❶, où le HA joue son rôle de proxy et transfère le paquet vers le MN ❷. Voyant arriver un paquet transféré, ce dernier peut choisir de signaler au correspondant sa position actuelle ❸, permettant ainsi une communication directe entre CN et MN ❹.

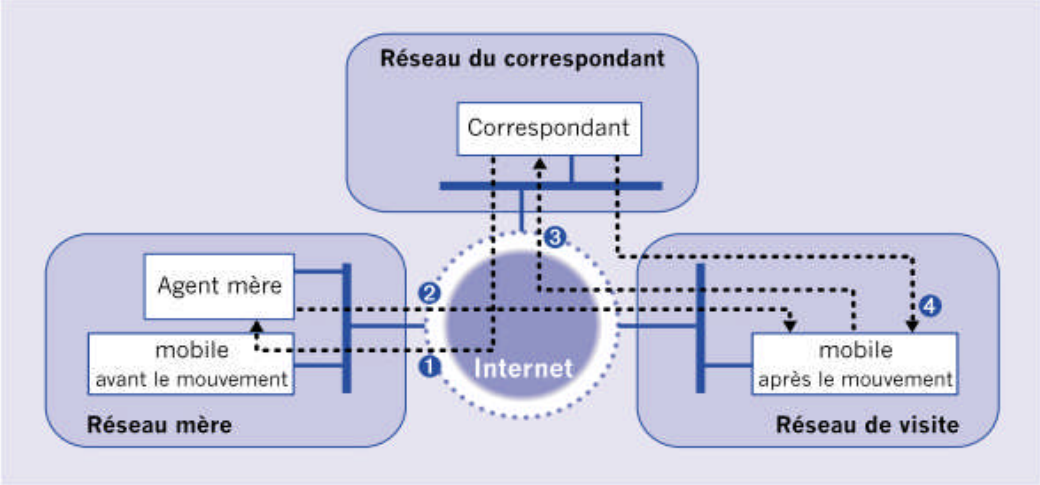

Figure 4.5 : Optimisation du routage entre le correspondant et le mobile.

7. Description du travail

7.1. Travail réalisé

Notre travail consiste à :

- créer et simuler un scénario de handover dans wifi mesh
- Evaluer les performances de ce scénario.

Nous présenterons alors le scénario de script à simuler. Ensuite nous définirons les paramètres nécessaires du réseau.

7.2. But de travail

Le but de ce travail est d'exploiter les traces de cette simulation afin d'en extraire des mesures sur les performances du réseau.

7.3. Scénario de simulation

Dans cette partie nous considérons une topologie simple comprenant un nœud multi-interface supportant les deux technologies WiFi. Le nœud mobile (MN) établit une connexion avec le CN (Correspenent Node).

Supposant que le MN emploie au début l'interface WiFi, on commute le trafic à autre interface WiFi quand il devient disponible.

La figure suivante contient les éléments essentiels de notre scénario :

- Router 0 (CN)
- Router1 (passerelle)
- Point d'accés WiFi2 (AP2 802.11)
- Point d'accès WiFi1 (AP 802.11)
- Nœud mobile (MN1)
- Nœud mobile(MN2)

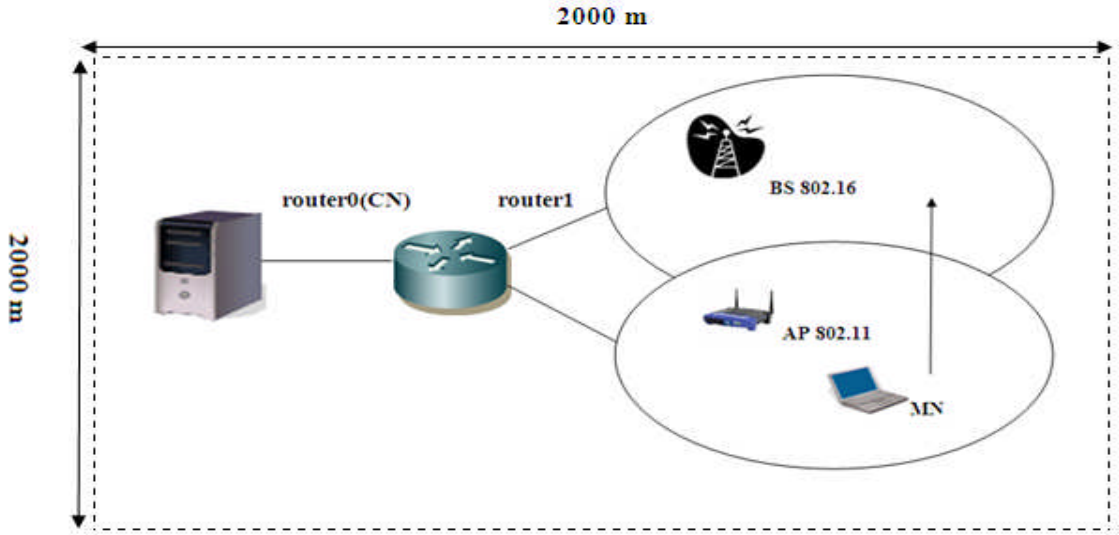

Figure 4.6 : Topologie du scénario (500m x 500m).

8. Paramétrage et configuration du réseau

Avant de pouvoir utiliser le simulateur, la topologie du réseau et le besoin de chaque nœud doivent être décrits dans un fichier TCL qui sera ensuite lu par le simulateur. Les paramètres et les configurations définis au niveau de ce fichier sont les suivants :

8.1. Paramètres de simulation

Paramètres	Signification
Trafic_start	=5s : le début de trafic
Trafic_stop	=70 s: la fin de trafic
Simulation_stop	=70s : la fin de simulation
Seed	RNG (Random Number Generator) fixé à 1 pour tous les scénarios simulés

Tableau 4.1 : Les paramètres de simulation.

8.2. Paramètres du réseau WiFi

paramètres	Signification
Channel/WirelessChannel	type de canal : sans fils
Propagation/TwoRayGround	modèle de propagation radio : 802.11
Phy/WirelessPhy	type d'interface du réseau : 802.11
Mac/802_11	type de couche MAC 802.11

Tableau 4.2 : Les paramètres du réseau WiFi

a) Configuration du point d'accès

paramètres	Signification
WiFi Coverage	potée de la station de base fixée à 20 m de rayon
Pt_	=0.025w : puissance du signal transmis de la station de base
freq_	=2412 e+6 : fréquence de 2.4GHz
RXThresh_	=6.12277e-09w: seuil de réception de puissance
CSThresh_	= [expr 0.9*[6.1227e-09]] w:seuil de détection de porteuse

Tableau 4.3 : Les paramètres du point d'accès WiFi.

9. Cadres des simulations

Les simulations ont été effectuées par le moyen du simulateur NS2 déjà décrit précédemment. Nous avons travaillé avec la version 2.29 sous Windows.

Nous rappelons que le simulateur NS2 comprend deux parties :

- Une partie cœur du réseau en langage C++ qui définit les protocoles et tous les modules nécessaires pour le support des mécanismes de handover.
- Une partie pour la description de la topologie du réseau et du scénario de trafic en langage tcl.

Au cours de ce travail, nous avons intervenu au niveau des deux parties.

9.1 La programmation TCL

Le travail se déroule en trois phases : pré-simulation, simulation et post-simulation.

9.1.1 Pré-simulation

Cette première phase consiste à paramétrer et configurer notre réseau.

9.1.2 Simulation

Cette phase consiste dans l'exécution du programme principal Fichier.tcl. A partir des fichiers définis dans la phase de pré-simulation, le simulateur enregistre le déroulement du scénario dans un fichier trace nommé trace.tr.

A la fin de la simulation, nous obtenons un fichier trace complet. Il s'agit d'un fichier de données structurées qui renferme tous les évènements survenus pendant la simulation.

Le fichier trace sera par la suite filtré pour en extraire l'information à interpréter.

9.1.3 Post-simulation

On a simulé un réseau mesh qui utilise le protocole de routage AODV (réactive).
Notre scénario décompose de deux partie, la 1 ére parties on suppose on n'a pas le handover et 2 éme en fait appelle aux handover.
La dernière étape consiste à tracer les courbes qui illustrent les résultats de nos simulations. Nous avons utilisé pour le traçage des courbes le logiciel Matlab.

Le diagramme ci-dessous récapitule les différentes phases du travail de simulation.

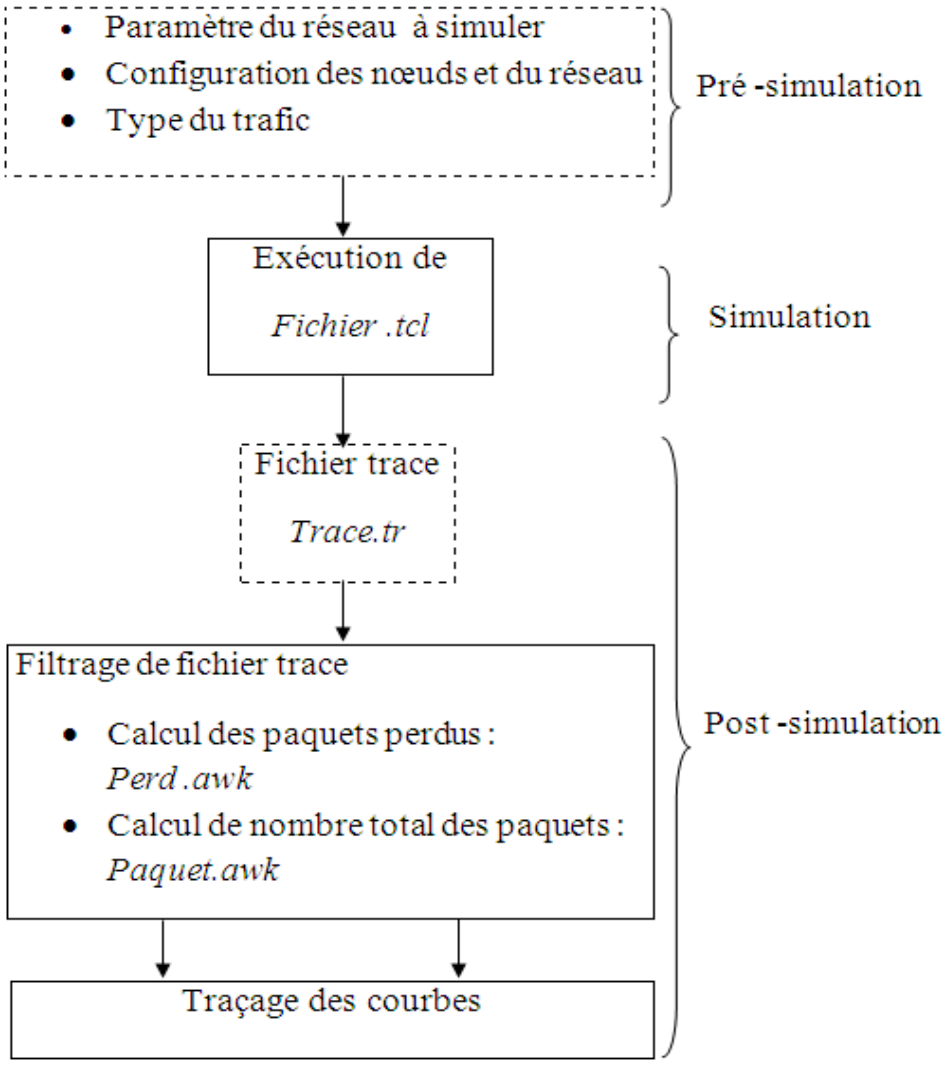

Figure 4 .7 : Diagramme de fonctionnement de tcl

10. Simulation et évaluation des performances du handover WiFi mesh

10.1. Introduction

Cette partie contient les résultats des scénarios simulés et les analyses pour dépeindre l'influence de la métrique utilisée dans l'exécution avant et après de handover dans le réseau mesh :

Finalement, nous comparerons les performances obtenues.

10.2 Performance du handoff

1. La qualité de service au niveau applicatif est affectée par la perte de paquet pendant le handoff7.Le délai (Delay) : il correspond au temps que met un paquet pour traverser le réseau d'un point d'entrée à un point de sortie. débit **:** il désigne le nombre de bits transmis par seconde Un nœud de l'Internet quelconque transmet un flot de paquets périodiquement au nœud mobile. Avant qu'un handoff ne soit effectué, les paquets sont acheminés le long de l'ancienne route. Dans la simulation, on suppose que le Correspondent Node (CN) connaisse d'avance lequel des paquets du flot sera le dernier pour atteindre le nœud mobile à son ancienne localisation. On suppose que le CN marque ce paquet. En recevant le paquet marqué, le nœud mobile exécute un handoff et transmet immédiatement un paquet de mise à jour à travers la nouvelle station de base. Les paquets acheminés par le CN après le paquet marqué sont envoyés à l'ancienne station de base avant l'arrivée du paquet de mise à jour, enfin ils sont perdus. Cet intervalle de temps est égal à la somme du temps pris par le paquet marqué pour atteindre le nœud mobile et le temps pris pour le paquet de mise à jour pour atteindre le CN. La perte de paquet dû au handoff est donc liée au temps d'aller-retour entre l'ancienne et la nouvelle localisation et le CN.

PARAM2TRE DE SIMULATION

10.3. Taux des paquets perdus sans handover

La figure 4.8 montre l'évolution du taux des paquets perdus en fonction du temps de la simulation.

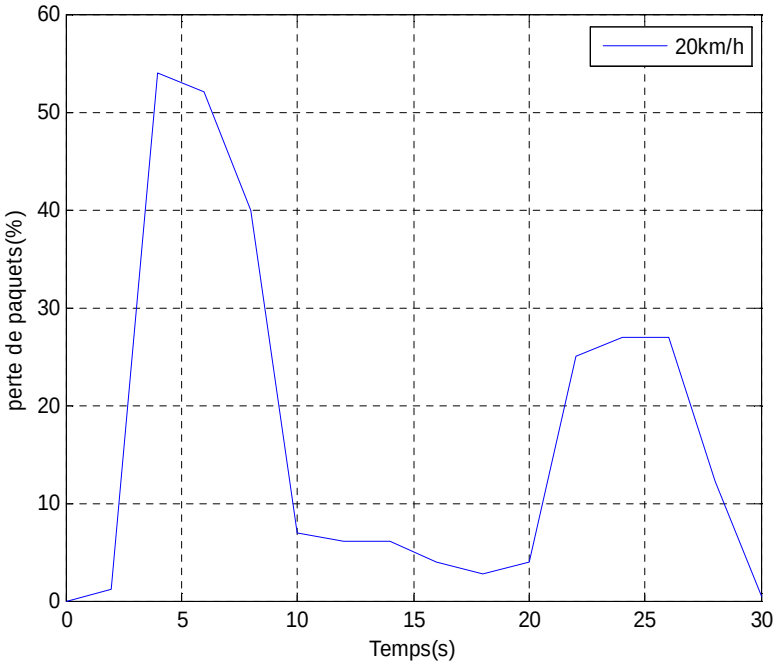

Figure 4.8: Evolution du Taux des pertes de paquets avant Handover.

D'après cette figure nous déduisons que :

- Pour un faible temps de simulation le nombre des paquets perdus est très élevé.
- Lorsqu'on augmente le temps de simulation le nombre des paquets perdus diminue ; cela signifie que lorsque le MN se déplace d'un réseau mère (WiFi) vers un autre réseau (WiFi), il communique d'abord avec son point d'accès puis il va a cheminer vers un autre point d'accès d'un autre réseau.
- si on examine les fichiers traces générés, on trouve que la destruction des paquets est due au temps d'établissement d'une nouvelle localisation où le mobile ne reçoit plus des paquets de l'ancienne station de base

10.4 Délai sans handover

La figure 4.9 montre l'évolution de Délai en fonction du temps de la simulation.

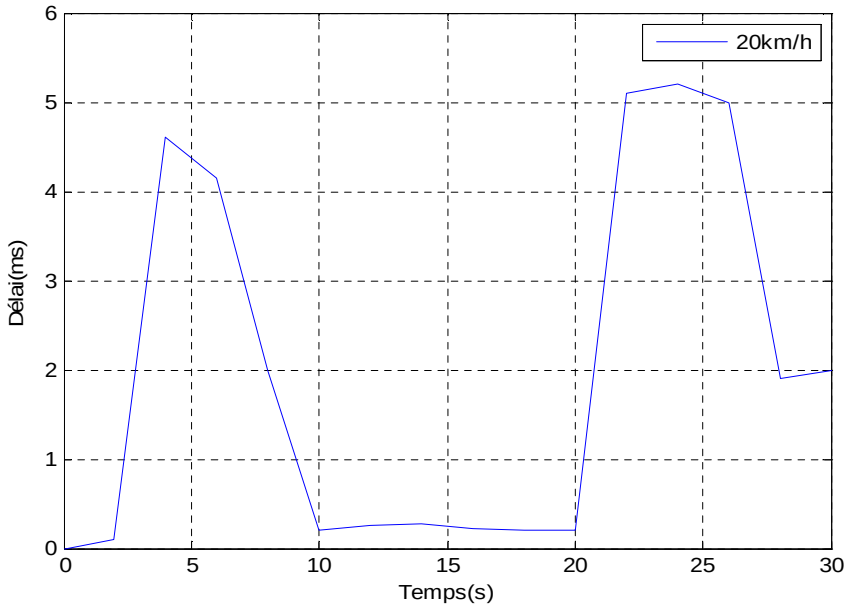

Figure 4.9 : Evolution de délai de avant Handover.

En remarque au début de simulation un délai important mais à t=10(s) le délai seras constante grâce a la perte de paquet perdue a t=20 (s) le délai augmente

10.5 Débit sans handover

La figure 4.10 montre l'évolution de Débit en fonction du temps de la simulation.

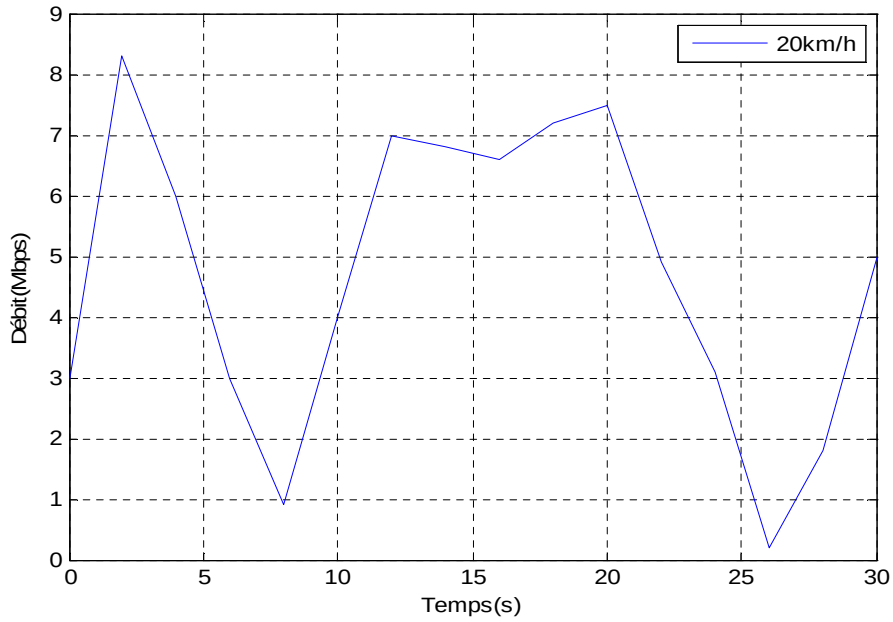

Figure 4.10 : Evolution le débit avant Handover.

10.6 Taux des paquets perdus avec Handover

La figure ci-dessous montre l'évolution du taux des paquets perdus en fonction du temps de la simulation.

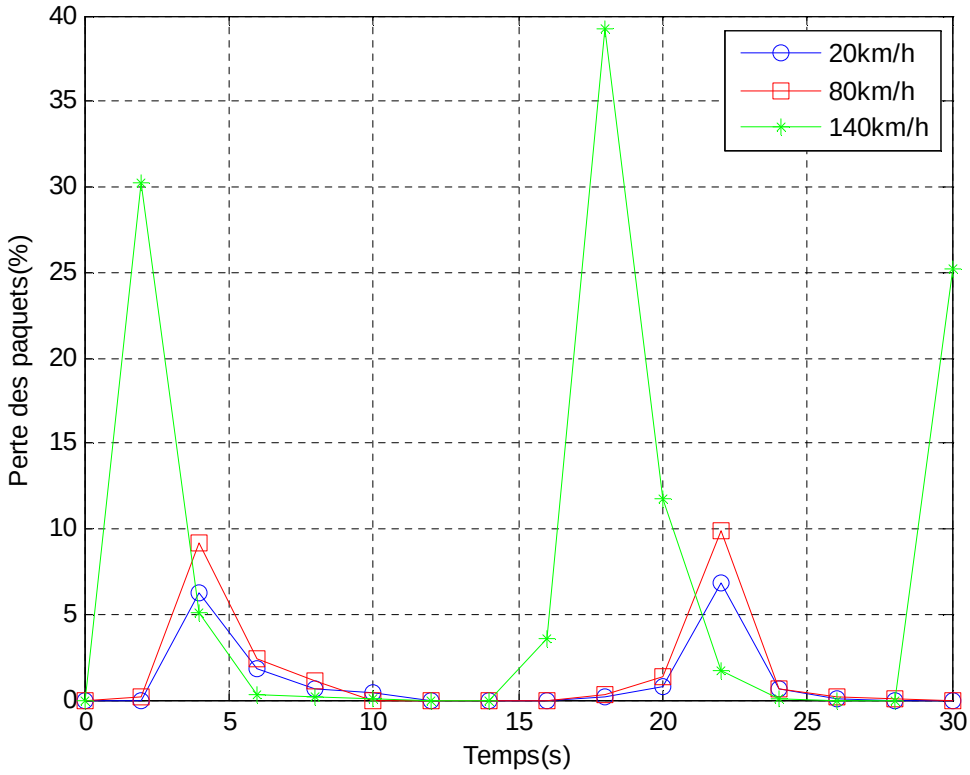

Figure 4.11 : Evolution du Taux des paquets perdus avec Handover .

L'évolution des paquets perdus est quasiment identique à celle obtenue dans le premier scénario. Sauf que pendant le handover le nombre des paquets perdus est minimum lorsqu'on visualise le fichier d'animation (NAM) à ce moment.

Pour des vitesses élevées les performances du Handover chutent considérablement.

Le nombre des paquets détruits augmente avec la vitesse et avec l'exécution du handover.

10.7 Délai avec handover

La figure suivante illustre le délai en fonction de temps de simulation a différents vitesse.

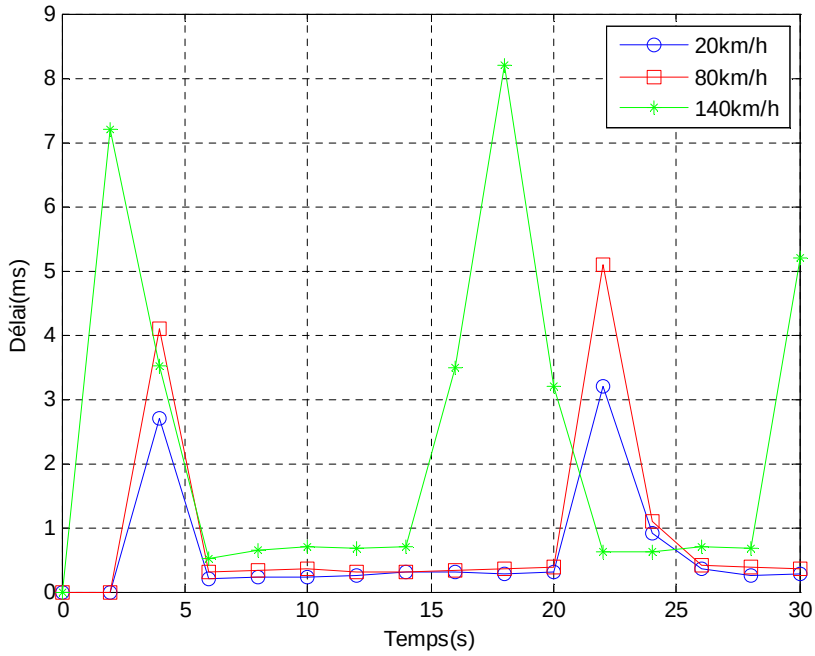

Figure 4.12 : Evolution du Délai avec Handover .

Avec une faible vitesse le délai au moment de Handover est plus important .Par contre lorsque

On augmente la vitesse le délai est inconsidérable à l'exécution du Handover.

10.8 Débit avec handover

La figure suivante illustre le débit en fonction de temps de simulation a différents vitesse.

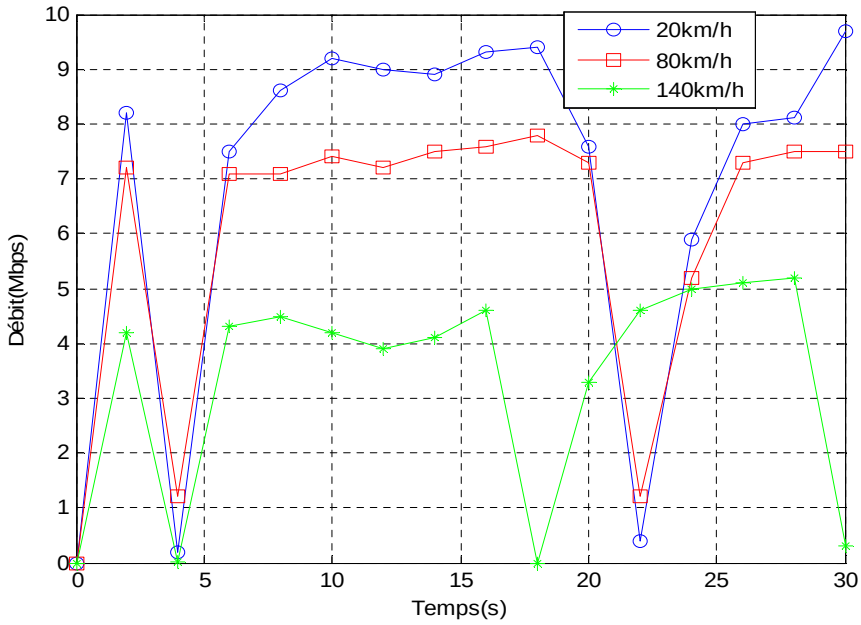

Figure 4.13 : Evolution du Débit avec Handover

D'après cette figure nous déduisons que : au moment de Handover avec vitesse faible on a un débit très élévés

11 L'étude comparative

Dans cette partie, on va faire la comparaison entre les deux cas en fonction de temps de simulation et la vitesse de déplacement de MN.

Pour les différents temps de simulation, le nombre des paquets perdus pendant l'exécution de handover est plus important par rapport au celle de est ça signifier que lorsque le MN déplace d'un réseau local (WiFi) vers un autre (WiFi), le nombre des paquets perdus est petit au moment de handover.le Délai important avec un débit élevé.

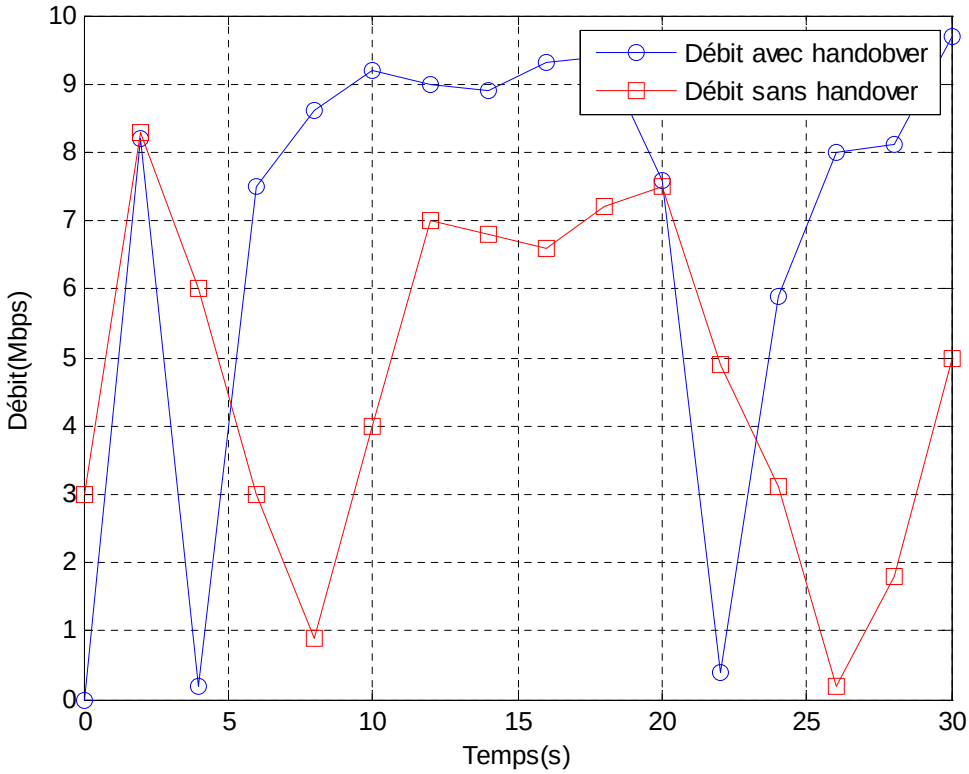

Figure 4.14 : **Comparaison de Débit avant et après le handover**

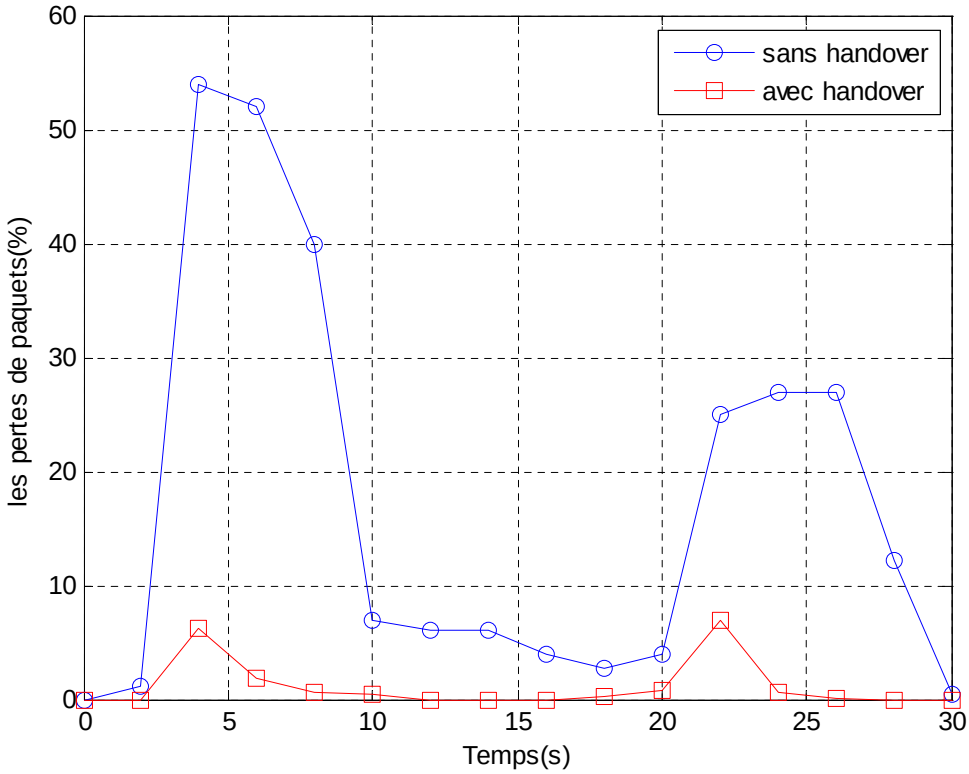

Figure 4.15 : **Comparaison des pertes de paquets avant et après le handover**

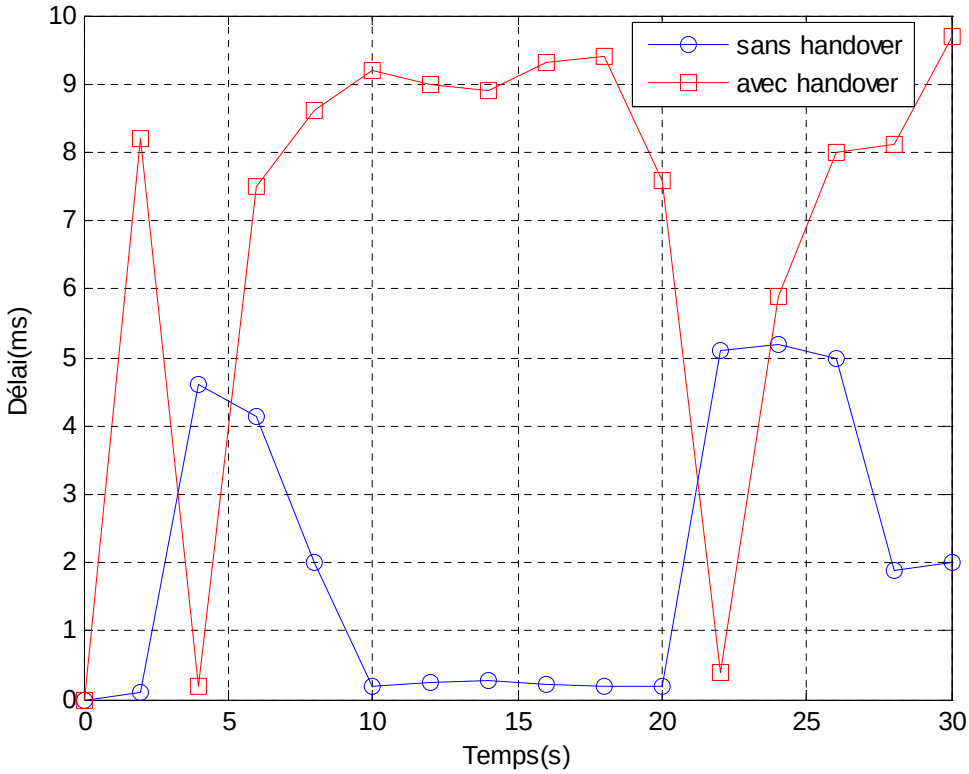

Figure 4.16 : **Comparaison le Délai avant et après le handover**

D'après ces figures nous déduisons que :

Au lancement de Handover dans un WiFi mesh on obtient une bonne performance de qualité service tel que (débit, Délai, Perte de paquet) avec une vitesse important a fin d'éviter la coupure.

12. Conclusion

Pour un bon handover dans wifi mesh il faut toujours respecte le principe de communication active avec moins de pertes de paquets

1 Introduction

Le 802.11s est une évolution des réseaux 802.11 qui facilite la formation d'un réseau maillé entre des points d'accès 802.11, dans un objectif d'étendre la couverture du réseau WLAN. Un réseau maillé est un réseau multi-sauts basé sur une infrastructure contrairement à un réseau Ad-hoc (MANET pour Mobile Ad hoc Network) qui ne nécessite aucune infrastructure, il offre naturellement un accès sans fil, avec un coût attractif et avec des débits élevés.

Le groupe IEEE 802.11s a été créé en Janvier 2004 pour offrir les fonctionnalités du maillage aux architectures et protocoles de la famille IEEE 802.11. Plus Spécifiquement, pour définir les amendements nécessaires au niveau des couches MAC et physique pour la création d'un système de distribution sans fil à base de la technologie IEEE 802.11.

Dans les réseaux WLAN non maillés, les stations (STAs) doivent s'associer à un point d'accès (AP) afin d'accéder au réseau, et ces STAs dépendent de ce point d'accès avec lequel ils se sont associés pour communiquer. Dans un réseau maillé les APs peuvent communiquer entre eux directement sans l'intermédiaire d'un réseau externe [2].

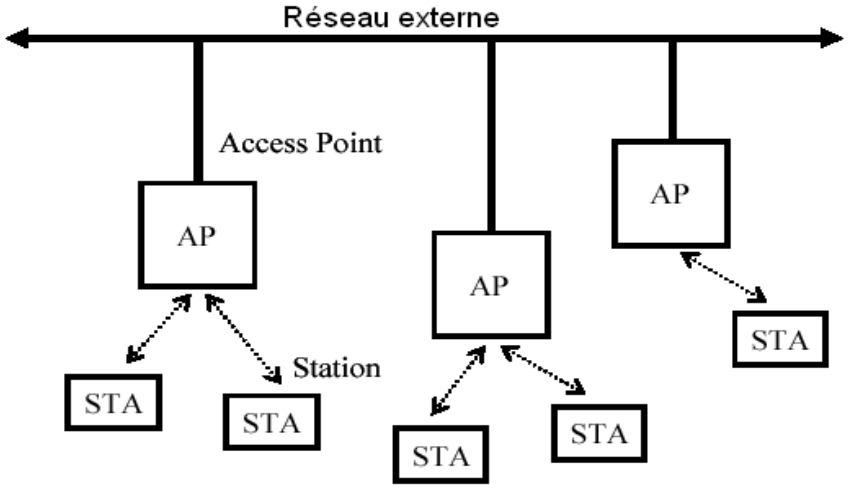

FIGURE 1.1 *:* Communications dans un réseau WLAN maillé

2 Le réseau Mesh

2.1 Définition de WMN

Le mot clé pour ce type de réseau est « maillé » (Mesh). Un réseau maillé est tout simplement un réseau où chaque nœud peut communiquer, directement ou non, avec n'importe Quel nœud, et où la perte d'un lien ne compromet pas complètement la connectivité. Un réseau maillé peut être défini comme un réseau qui, pour un nœud donné, fournit au minimum deux chemins différents vers n'importe quel autre nœud du réseau. Les données circulent alors de nœud à nœud (hop by hop) jusqu''à atteindre le nœud de destination. Un réseau sans fils maillé WMN est un cas particulier de réseau maillé où pour une transmission entre deux nœuds, les autres nœuds fonctionnent comme des routeurs et effectuent les fonctions de relaya gé via des liens sans fil.

Après le succès qu'ont connu les réseaux 802.11 avec infrastructure et les réseaux ad-hoc au cours des dernières années, les WMN se présentent comme une nouvelle architecture réseau qui permet de combler les faiblesses et les limites de ses prédécesseurs en améliorant les services tout en minimisant les coûts. Les WMN permettent alors de fournir une connectivité à large bandes avec un déploiement facile et à faible coût.

Les WMN permettent d'offrir une connectivité aux utilisateurs en tout temps et en tout lieu grâce à un dorsal réseau (back haul) constitué de routeurs sans fils qui ont pour fonction de relayer le trafic jusqu'à une passerelle qui est connectée d'une manière filaire aux réseaux extérieurs et essentiellement Internet et vice versa. Au contraire des réseaux cellulaires et les WLAN, les WMN fournissent alors à travers cette topologie maillée aux clients mobiles une infrastructure décentralisée qui constitue comme on le verra plus tard l'un des avantages des WMN, à savoir la résistance aux pannes.

Le caractère multi-sauts des WMN permet d'augmenter la couverture du réseau.

	802.11a(WIFI 5)	802.11b(WIFI)	802.11g
Débit	54Mbit/s	11Mbit /s	20Mbit/s
Fréquence	5GHZ	2.4GHZ	2.4GHZ
Portée	40m	100m	100m
Principale	Permet d'obtenir un haut débit, il est incompatible avec 802 .11b	C'est la norme la plus répondue actuellement	Plus répondue dans le commerce actuellement, Assure la compatibilité avec le standard 802.11b

TABLEAU 1.1 : Les différents types du 802.11

2.1.1 Les autres normes de WIFI

Référence	Description
802.11c	Modification de la norme 802 .11 au niveau interne.
802.11e	Ce standard ajoute un supplément de QoS (qualité de service) pour les applications données, voix, vidéo.
802.11f	Elle achève le point de l'interopérabilité entre les différents standards.
802.11h	Ce standard est développé pour mieux gérer la consommation d'énergie des mobiles, selon leurs locations (indoor or outdoor).
802.11X et 802.11i	Ces deux standards assurent la sécurité des réseaux WLAN utilisant la norme IEEE802 .11.

TABLEAU 1.2 : Les références du 802.11

2.2 Les composantes de WMN

Avant d'avoir l'architecture de WMN, il est essentiel d'identifier les différentes composantes de ces réseaux .Notons que plusieurs dénominations sont présentes dans la littérature ; on a choisi celle proposée par IEEE802.11s :

- MP (Mesh Point) : ils forment la dorsale du réseau. Ce sont des routeurs sans fils qui ont la capacité de router et relayer le trafic d'un MP à un autre jusqu'à la passerelle. Les MP sont généralement fixes et n'ont pas de contraintes de consommation d'énergie.
- MAP (Mesh Access Point) : c'est un MP qui joue parallèlement le rôle d'un point d'accès. Il fournit l'accès au réseau pour les stations ou les clients mobiles.
- MPP (Mesh Portal Point) : un MP qui joue aussi un rôle de passerelle vers d'autres types de réseaux comme Wimax. Il est généralement connecté au réseau filaire afin de fournir aux clients une connectivité Internet en tout temps et en tout lieu.
- STA (Station) : il s'agit du client ou l'utilisateur. Les STAs ne participent ni au routage ni aux services Mesh. Ils sont mobiles et ils communiquent entre eux à travers leurs stations de base. Les STAs peuvent être un ordinateur portable.

2.3 Les architectures de WMN

Un WMN peut avoir l'une des trois architectures suivantes, le choix de l'une ou de l'autre dépend du but d'utilisation. Il est à noter que la dénomination varie dans la littérature.

2.3.1 WMN avec infrastructure ou hiérarchique

Ce type d'architecture est caractérisé par plusieurs niveaux. Les clients constituent le niveau plus bas. Ce sont l'origine du trafic et ils ne participent pas au routage ou à l'acheminement (relais). Les MPs forment la dorsale et ont pour fonction le relai du trafic.

Le troisième niveau est constitué des passerelles MPP qui permettent l'accès à l'Internet ou bien l'intégration des WMN avec les réseaux sans fils existants. Cette architecture qui est nommée aussi WMN fixe permet d'étendre la couverture réseau pour les clients. Les MP peuvent être installés a l'extérieur, dans les rues, dans les lieus publics, …etc. tout comme ils peuvent être installés à l'intérieur des entreprises, par exemple, et ainsi le client qui est mobile peut toujours avoir une connectivité. Cette architecture est la plus utilisée et elle est illustrée par la figure 1.2.

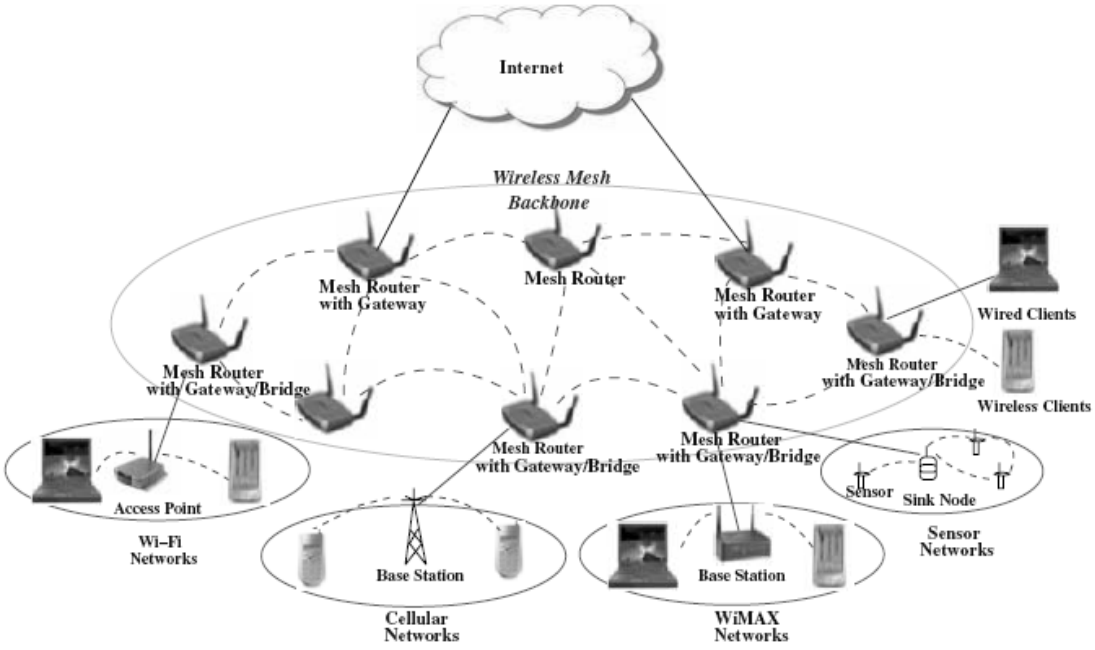

FIGURE 1.2 : WMN hiérarchique

2.3.2 WMN plats ou mobiles

Ce type d'architecture est nommé aussi WMN ad-hoc car elle est très similaire aux réseaux ad-hoc. Tous les équipements sont sur le même niveau et ils peuvent être à la fois des clients et des routeurs. Ce type d'architecture fournit un réseau point à point entre les clients (AKyildiz, Wang, 2005). Les WMN utilisent les MAP et les MPP qui sont nécessaires dans le cas où il y a un besoin de joindre des réseaux externes comme l'Internet.

Ce type d'architecture est idéal pour les applications distribuées. La topologie du réseau change fréquemment en raison de la mobilité des équipements. Ce qui exige une mise à jour fréquente des tables de routage et résulte en une charge importante. Cette architecture est utilisée pour plusieurs cas d'usage comme par exemple pour les services de sécurité publique, les applications de transport etc.… (Bing 2008). La figure 1.3 illustre ce type d'architecture

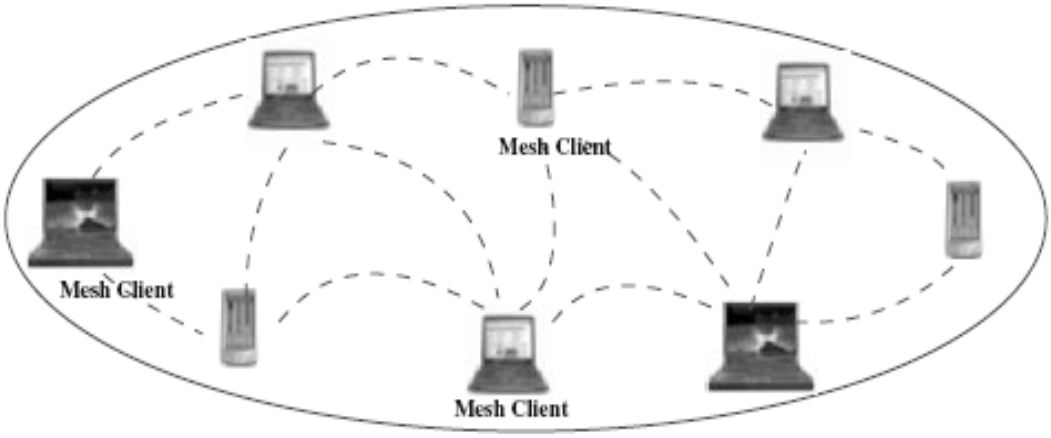

FIGURE 1.3 : WMN plats

2.3.2.1 Le mode Ad-hoc

Le mode ad hoc (généralement baptisé point à point) représente simplement un ensemble de stations sans fil 802.11 qui communiquent entre elles sans avoir recours à un point d'accès ou une connexion à un réseau filaire à travers le système de distribution. Chaque station peut établir une communication avec n'importe quelle autre station dans la cellule que l'on appelle cellule IBSS (Independent Basic Service Set). Ces réseaux ont été étudiés au début des années 1970 à des fins militaires sous le nom de réseau en mode paquet.

Comme dans le mode infrastructure, un réseau ad hoc est généralement identifié par une identification de réseau SSID.

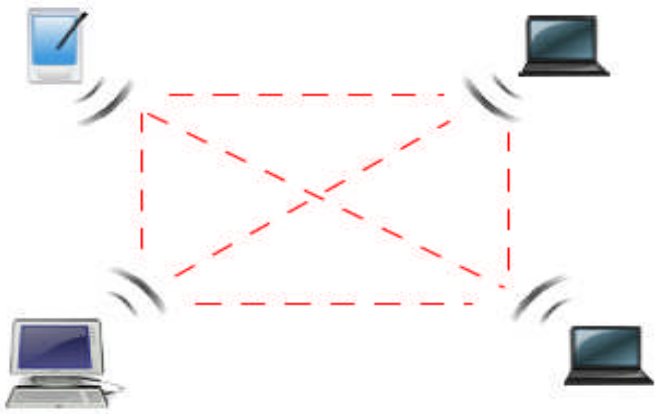

FIGURE 1.4 : Fonctionnement en mode ad hoc

2.3.3 WMN hybride

Cette architecture est une combinaison entre les deux architectures précédentes. Les clients peuvent communiquer directement entre eux et ils sont munis des fonctions de routage pour passer le trafic d'un client à un autre, et utilise l'infrastructure pour avoir une connectivité aux réseaux externes (donc Internet). Cette architecture devient de plus en plus importante pour le développement de WMN (AKyilidz, Wang et Wang, 2005). La figure 1.5 illustre cette architecture.

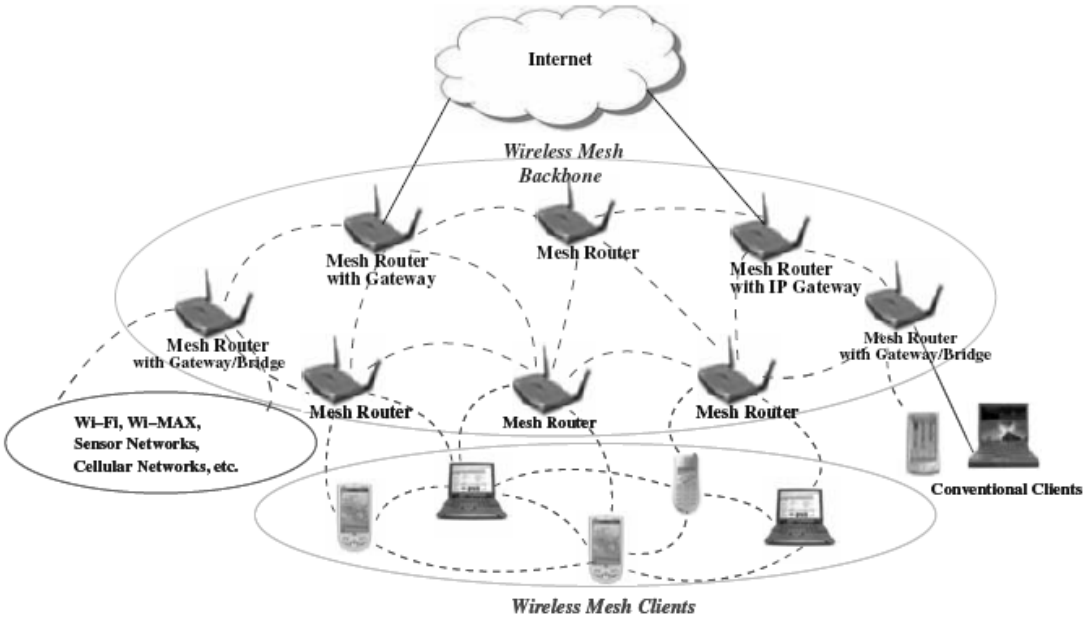

FIGURE 1.5 : WMN hybride

2.4 Caractéristiques

Les caractéristiques du réseau maillé sont expliquées dans ce qui suit :

a- Un réseau à multi-sauts: Une incitation à développer les réseaux maillés est d'étendre la zone de couverture des réseaux sans fil actuels sans compromettre la capacité du canal. Un autre objectif majeur des réseaux maillés est de fournir une connectivité directe entre les utilisateurs. Pour répondre à ces exigences, les multi-sauts sont indispensables, ce qui facilite un débit plus élevé sans sacrifier la gamme radio, réduire les interférences entre les nœuds et la réutilisation des fréquences les plus efficaces [3].

b- **Support des réseaux Ad-hoc :** est de la capacité d'auto-formation, d'auto-guérison et d'auto-organisation: Les réseaux Ad-hoc améliorent les performances du réseau, la facilité du déploiement et de la configuration, la tolérance aux pannes, et la connectivité. Grâce à ces caractéristiques, Les réseaux maillés ont une faible exigence de placement initial, et le réseau peut se développer graduellement selon les besoins [3].

c- **La mobilité dépend des types de nœud** : les routeurs maillés ont généralement une mobilité minimale, tandis que les clients peuvent être des nœuds fixes ou mobiles [3].

d- **Plusieurs types d'accès au réseau:** Dans les réseaux maillés, l'accès simultané aux communications Peer-to-Peer (P2P) et à l'Internet au sein des réseaux maillés sont prises en charge. En outre, l'intégration des réseaux maillés avec d'autres réseaux sans fil fournit des services supplémentaires aux utilisateurs finals de ces réseaux [3].

e- **La dépendance en vue la consommation d'énergie:** En général, les routeurs maillés ne disposent pas des contraintes strictes sur la consommation d'énergie puisqu'ils sont généralement alimentés en énergie. Toutefois, les clients maillés peuvent exiger des protocoles efficaces en économie d'énergie [3].

f- **Compatibilité et interopérabilité avec les réseaux sans fil existants :** Le réseau maillé est construit sur la base des technologies IEEE 802.11, et doit être compatible avec les normes IEEE 802.11. Les réseaux maillés ont aussi besoin d'être interopérables avec d'autres réseaux sans fil comme le WiMAX, ZigBee et des réseaux cellulaires. Sur la base de leurs caractéristiques, les réseaux maillés sont généralement considérés comme un type de réseau Ad-hoc en raison de l'absence d'infrastructure filaire qui existe dans la téléphonie cellulaire ou WiFi à travers le déploiement des réseaux de stations de base ou points d'accès. Bien que les techniques Ad-hoc de réseau soient tenus par les réseaux maillés, les capacités supplémentaires nécessitent des algorithmes plus sophistiqués et des principes de conception pour la réalisation de ce type de réseau. Plus précisément, au lieu d'être un type de mise en réseau Ad-hoc, les réseaux maillés visent à diversifier les capacités des réseaux Ad-hoc. Par Conséquent, les réseaux Ad-hoc peuvent effectivement être considérés comme un sous-ensemble des réseaux maillés [3].

g- **Intégration:** Les réseaux en maillage supportent les utilisateurs qui utilisent les mêmes technologies radio comme un routeur maillé. Ceci est accompli grâce à une fonction de routage disponible dans ces routeurs. Les réseaux maillés permettent également l'intégration des différents réseaux existants, tels que WiFi, Internet, réseaux cellulaires et de capteurs par le biais des fonctionnalités de la passerelle. Les réseaux sans fil intégrés par le biais des réseaux maillés ressemblent à la dorsale d'Internet.

h- Mobilité: La topologie et la connectivité du réseau dépendent de la circulation des usagers. Cela impose des défis supplémentaires pour les protocoles de routage ainsi que la configuration et le déploiement du réseau. Comme les routeurs maillés fournissent l'infrastructure dans les réseaux maillés, la couverture du réseau peut être conçue facilement tout en supportant la mobilité des utilisateurs [3].

i- Compatibilité: les réseaux maillés contiennent de nombreuses différences par rapport aux réseaux Ad-hoc. Toutefois, comme indiqué plus haut, les réseaux Ad-hoc peuvent être considérés comme un sous-ensemble des réseaux maillés. Plus précisément, les techniques existantes développées pour les réseaux Ad-hoc sont déjà applicables dans les WMNs [3].

2.5 Applications de WMN

A l'origine, la technologie des réseaux maillés mobiles, ou Mesh, a été mise au point par les militaires pour déployer rapidement des réseaux de radiocommunication sur les champs de bataille. En dix ans, grâce aux recherches de l'agence de recherche militaire américaine et de l'INRIA (institut de recherche en informatique et automatique) en France, ces réseaux sont devenus des réseaux de haut débit et ont fait leurs preuves, notamment en Iraq.

Depuis peu, les applications civiles se multiplient tels que la domotique, les systèmes embarqués, les systèmes de surveillances, les systèmes de santé, le multimédia, etc. [4], [5].

2.5.1 Réseau Domestique (Broadband Home Networking)

les réseaux domestiques classiques (qui utilisent la technologie IEEE 802.11) soufrent d'un problème de coût de déplacement des points d'accès filaires , d'où il faut faire une étude préalable de localisation des points d'accès pour assurer une couverture idéale dans tous les coins de la maison, et éviter par conséquence le déplacement des points d'accès. Cette étude ne résoudre pas le problème définitivement, lorsque il y a des changements dans la structure de la maison (travaux de construction), ceci peut engendrer des points morts (non couverts) et dans ce cas le déplacement des points d'accès est inévitable. La solution Mesh est capable de résoudre ce problème par l'utilisation des points d'accès sans fil à moindre coût avec une facilité de déplacement et ajustement.

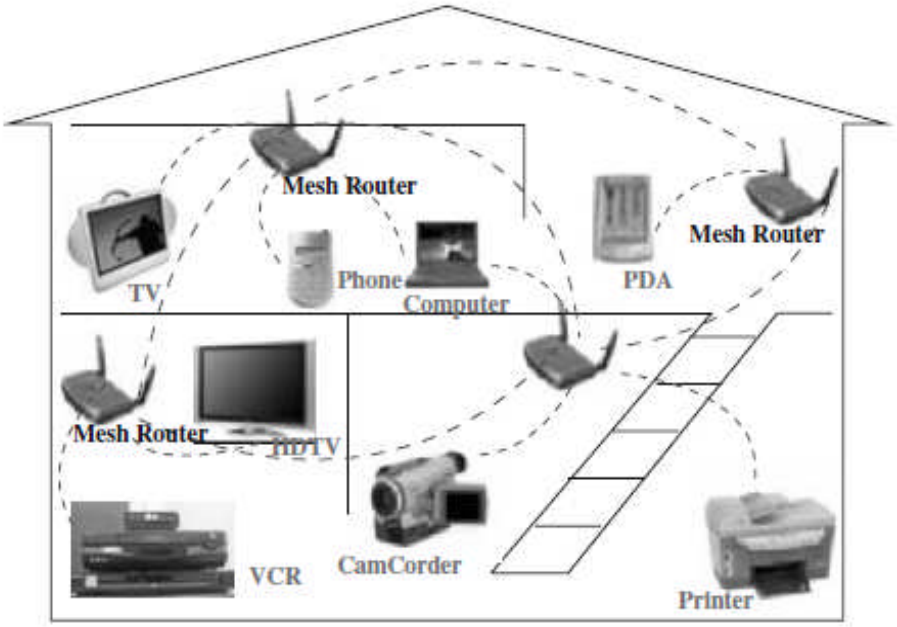

Figure 1.6 : Les réseaux maillés pour la maison numérique

2.5.2 Réseau de communauté et de Voisinage (community and Neighborhood Networking)

Actuellement, la communication entre maisons se fait par l'intermédiaire du réseau internet.

L'avantage de cette architecture est la couverture étendue du réseau. Par contre, elle possède des inconvénients :

- N'importe quelle communication entre deux utilisateurs passe obligatoirement par internet.
- La nécessite d'une passerelle pour chaque maison.

La solution Mesh peut faire face à ces problèmes par l'installation des mesh routeurs pour chaque maison, ainsi que doter quelques maisons par des passerelles pour permettre l'accès aux autres réseaux. Dans ce cas, les communications sont assurées par le backbone, ainsi que l'accès aux autres réseaux se fait seulement lorsqu'il y a besoin par n'importe quel utilisateur, et pas forcement possédant une passerelle.

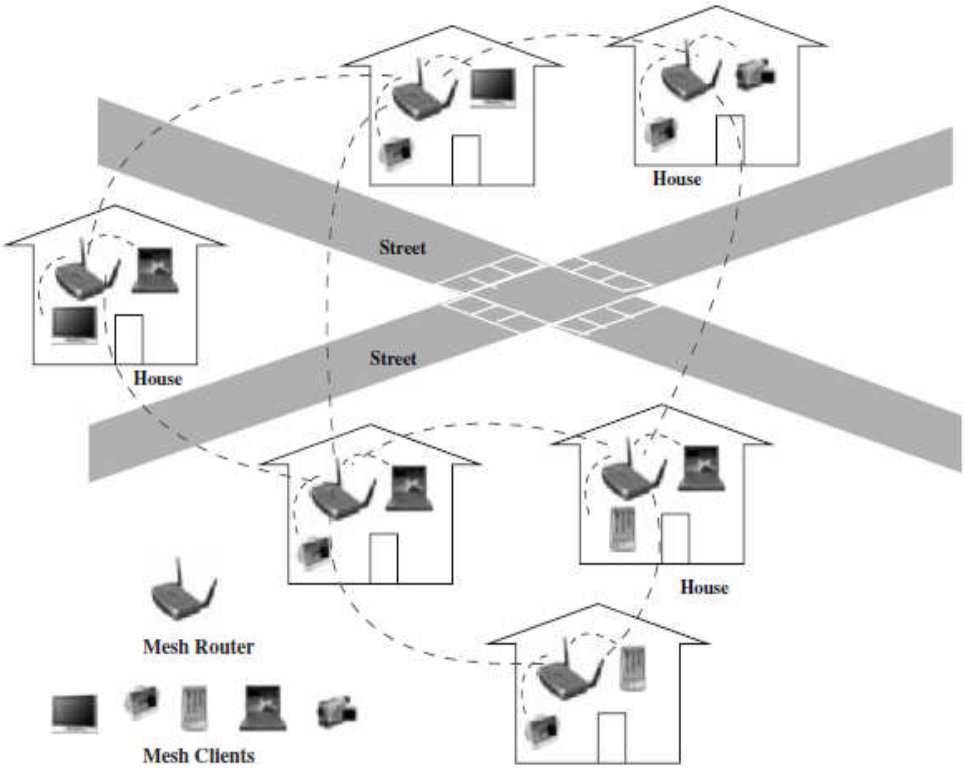

Figure 1.7: Les réseaux maillés pour les réseaux de voisinage

2.5.3 Réseaux d'entreprises

Cela peut être un petit réseau dans un bureau ou un réseau de taille moyenne pour l'ensemble des bureaux dans tout le bâtiment, ou d'un réseau à grande échelle entre les bureaux dans plusieurs bâtiments. Actuellement le standard IEEE 802.11 est largement utilisé dans les différents bureaux. Cependant, ces réseaux sans fil sont encore isolés. Les connexions entre eux doivent être atteintes grâce à des connexions Ethernet câblées, qui est la principale raison du coût élevé des réseaux d'entreprise. En outre, l'ajout des modems d'accès ne font qu'accroître les capacités locales, mais elles n'améliorent pas la robustesse aux pannes de liens, la congestion du réseau et d'autres problèmes du réseau d'entreprise.

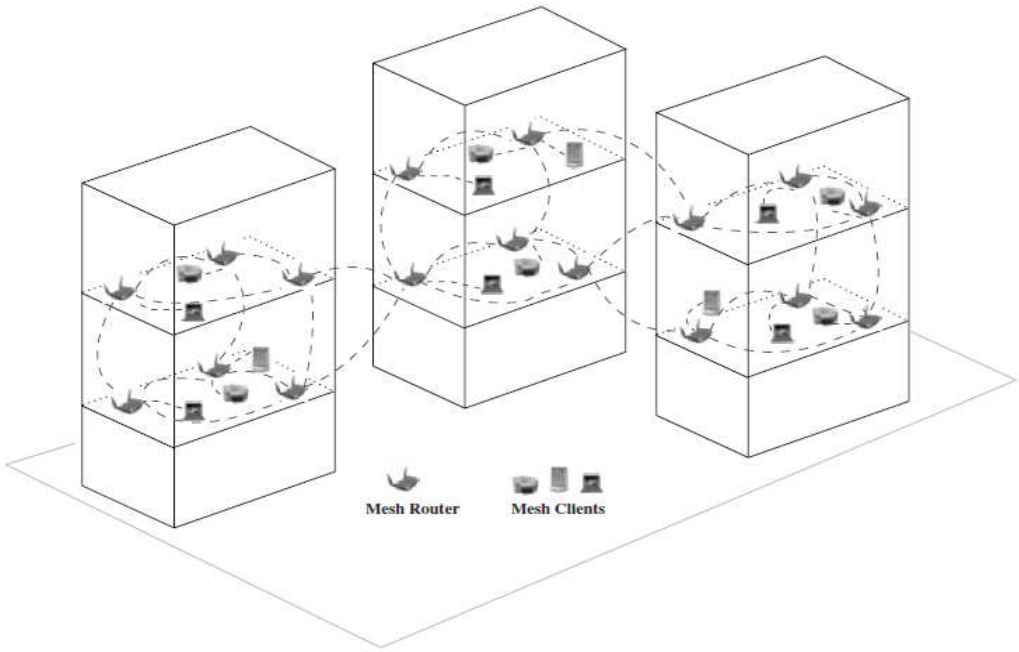

Figure 1.8 : Les réseaux maillés pour les entreprises

Si les points d'accès sont remplacés par des routeurs Mesh, comme le montre la figure 1.8, le coté filaire peut être éliminé. Plusieurs modems d'accès peuvent être partagé par tous les nœuds du réseau, et donc d'améliorer l'utilisation des ressources et la robustesse des réseaux d'entreprise. Les WMNs peuvent se développer facilement une fois que la taille de l'entreprise devienne importante [3].

2.5.4 Réseaux métropolitain (WMAN)

Les réseaux maillés dans une région métropolitaine ont plusieurs avantages. Le taux de transmission de la couche physique d'un nœud dans les réseaux maillés est beaucoup plus élevé que dans les systèmes cellulaires. Par exemple, un port IEEE 802.11g peut transmettre un débit de 54 Mbps. De plus, la communication entre les nœuds du maillage ne repose pas sur un réseau fédérateur câblé. Par rapport aux réseaux câblés, par exemple, le câble ou les réseaux optiques, Le réseau maillé est une alternative économique aux réseaux à large bande, en particulier dans les régions sous-développées. Le WMAN couvre une zone potentiellement beaucoup plus grande qu'une maison, entreprise, bâtiment ou les réseaux communautaires, comme le montre la figure 1.9. Ainsi, l'exigence sur l'évolutivité du réseau WMN est beaucoup plus élevée que par d'autres applications [3].

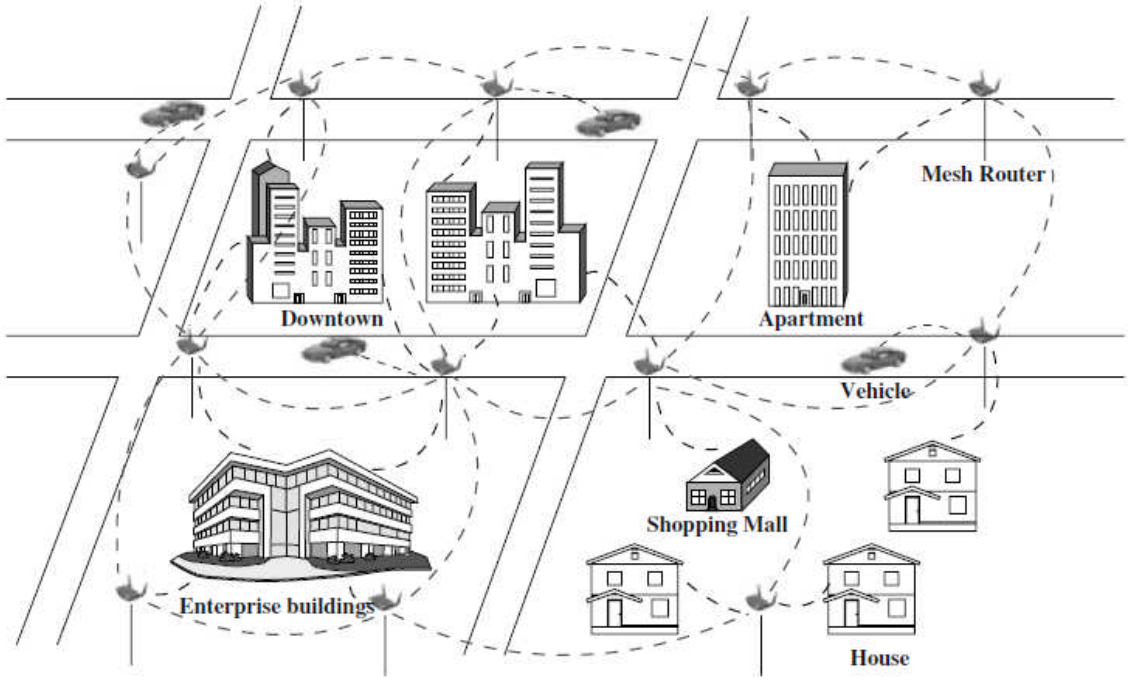

Figure 1.9 : Les réseaux maillés metropolitan

2.5.5 Systèmes médicaux et de santé

Dans un hôpital ou un centre médical, des données de surveillance et de diagnostic doivent être traités et transmis d'une pièce à l'autre. La transmission des données est généralement à large bande, car les images médicales à haute résolution et diverses informations de suivi périodique peuvent facilement produire un volume constant et important de données. Les réseaux filaires traditionnels ne peuvent fournir un accès réseau limité à certains dispositifs médicaux fixes. Des réseaux WiFi doivent se fonder sur l'existence de connexions Ethernet, ce qui peut causer le coût élevé et la complexité du système. Cependant, ces problèmes n’existent pas dans les réseaux.

2.5.6 Sécurité et systèmes de surveillance

Comme la sécurité est en passe de devenir un sujet de préoccupation très élevé, les systèmes de surveillance et de sécurité sont devenus une nécessité pour les bâtiments d'entreprise, les centres commerciaux, les Bans, etc. Afin de déployer ces systèmes dans des endroits comme nécessaire, les réseaux maillés sont une solution beaucoup plus fiable pour connecter tous les périphériques. Les images fixes et les vidéos sont les trafics majeurs circulant dans le réseau, ces applications exigent la capacité du réseau beaucoup plus élevé que d'autres applications [3].
En plus de ces applications, les réseaux maillés peuvent également être appliqués à des applications spontanées (urgences / catastrophes). Par exemple, les réseaux sans fil pour une équipe d'intervention d'urgence et les pompiers n'ont pas une connaissance en avance du lieu où le réseau doit être déployé. En plaçant simplement les routeurs maillés sans fil dans des endroits souhaités, un WMN peut être rapidement mis en place. Pour un groupe de personnes détenant des dispositifs avec une capacité de mise en réseau sans fil, par exemple, les ordinateurs portables et des PDA, les communications P2P n'importe quand n'importe où est une solution efficace pour le partage de l'information. Les réseaux maillés sont en mesure de répondre à cette demande. Ces applications montrent que ce type de réseau a un sur-ensemble des réseaux Ad-hoc, et donc, peut accomplir toutes les fonctions offertes par les réseaux Ad-hoc.

3 Conclusion

Dans ce chapitre, nous avons présenté la technologie mesh qui permet aux équipements sans fil de se connecter de proche en proche, d'une façon dynamique et \ ou statique et instantanée, sans hiérarchie centrale, formant ainsi une structure maillée. Par la suite, nous avons détaillé les caractéristiques et les applications de la technologie mesh et nous avons parcouru les travaux de normalisation des réseaux mesh.

1 Introduction

Les réseaux locaux conventionnels ont néanmoins quelques limitations, notamment, le besoin d'une infrastructure filaire (généralement Ethernet) reliant chaque point d'accès (AP). En effet, l'extension de leur couverture devient couteuse et peu pratique. Les réseaux maillés sans fil ont dernièrement été proposé afin de répondre à cette limitation. Libre de toute exigence d'infrastructure, les routeurs peuvent être ajoutés suivant la situation et la demande, offrent une excellente flexibilité. Le réseau peut ainsi se prolonger sur plusieurs Kilomètres, et offrir un accès sans fil à Internet.

Ces réseaux maillés sans fil définissent des nouveaux protocoles et métriques de routage pour tenir compte des nouvelles exigences autre que la consommation d'énergie et la mobilité.

Ces nouvelles exigences sont principalement l'augmentation de la capacité des nœuds et des chemins.

2 Couche physique

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données. Chaque couche physique (couche physique d'IEEE 802.11et amendements 802.11b, 802.11a, 802.11g) est divisée en deux sous-couches :

La couche PLCP (Physical Layer Convergence Protocol) et le couche PMD (Physical Medium Dependent). La couche PMD définit les caractéristiques de la couche physique employée à savoir les techniques de transmissions utilisées (FHSS, DSSS ou OFDM). La couche PLCP permet la liaison entre la couche PMD et la couche MAC et à pour principal rôle la gestion des trames (encapsulation, décapsulation, etc.). Elle permet aussi d'envoyer à la couche MAC des rapports d'erreur ou encore de lui signifier si le support est libre ou non.

2.1 FHSS

Le FHSS est un système à saut de fréquence ou la totalité disponible est divisée en 79 canaux de 1 MHz. Les transmissions se font sur l'ensemble des canaux selon une séquence de sauts prédéfinie, définissant ainsi le facteur d'étalement : le système passe d'un canal à un autre toute les 300 ms selon cette séquence. L'avantage de cette technique est que toute personne écoutant la bande et ne connaissant pas la séquence de sauts ne pourra intercepter les données. D'autre part, étant donné que le système saute d'un canal à un autre, le FHSS possède une immunité contre des interférences locales. Son seul défaut réside dans la fiable largeur de bande par canal qui ne lui permettant pas d'atteindre des vitesses de transmission élevées.

2.1.1 La structure de la trame en FHSS

Une trame au niveau physique est composée de trois parties. Elle débute par un préambule, suivi d'un entête et se termine par la partie données (figure 2.1).

Préambule		En-tête			
Synchro 80 bits	SFD 16 bits	PLW 11bits	PSF 5 bits	CRC En-tête 16 bits	Trame MAC

FIGURE 2.1 : La structure de la trame 802.11 au niveau physique, FHSS

Avec l'étalement de spectre par saut de fréquence, ou FHSS (Frequency Hopping Spread Spectrum), le signal est transmis en diffusion générale (broadcast) en une suite apparemment aléatoire de fréquences radio, passant ou sautant d'une fréquence à une autre à des intervalles fixes. Pour récupérer le message transmis, le récepteur passe lui aussi d'une fréquence à une autre en synchronisation avec l'émetteur. Une écoute clandestine ne permet de récupérer que des signaux inintelligibles et les tentatives de brouillage sur une fréquence donnée ne touchent que quelques bits.

Le FHSS, dont le champ d'applications s'est désormais élargi, utilise ainsi un signal à bande étroite qui "saute" sans arrêt d'une fréquence à l'autre, suivant un algorithme spécifique connu de l'émetteur et du récepteur. Ensuite, tout dépend du système standard ou propriétaire que l'on utilise : la bande de fréquence utilisée, le nombre de canaux dans lequel le signal peut sauter ou encore le temps de séjour du signal dans chaque canal, sont spécifiques au système utilisé [6].

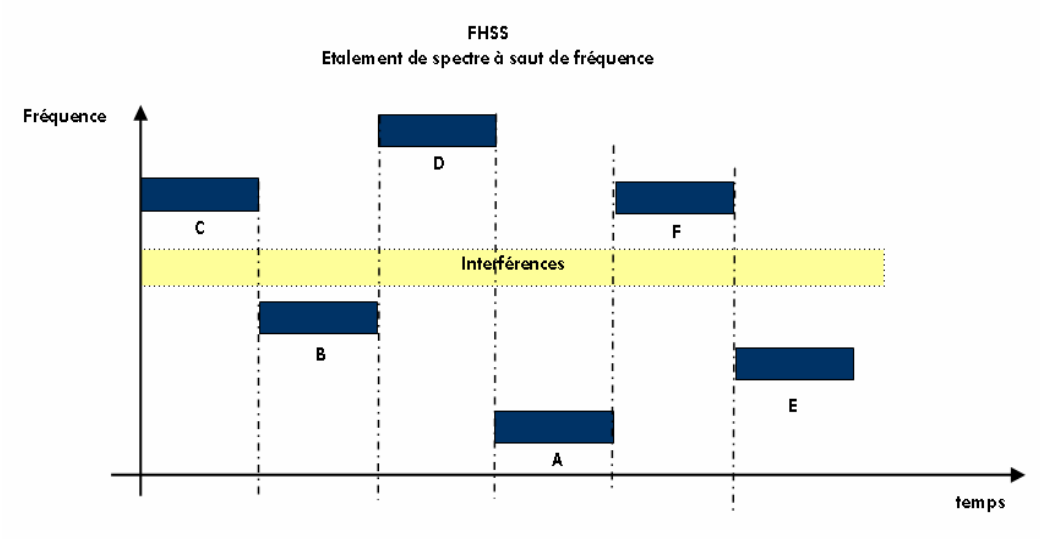

FIGURE 2.2 : Etalment de spectre à saut de fréquence

Ce type de modulation presente les avantages suivant :

- La densité spectrale du signal transmis est fiable car le signal à large bande.
- L'étalement améliore la sécurité en gardant bien sûr le code d'étalement secret.
- Le signal étalé est moins sensible face à des signaux à bande étroite.
- La tolérance vis-à-vis du multi-trajet est obtenue en choisissant des codes qui ont des facteurs d'auto corrélation très fiables.

2.1.2 La technique DSSS

Le DSSS utilise, quant à lui, comme facteur d'étalement une technique de chipping. Au lieu de découper la bande en canaux de 1MHz, la bande est découpée en quatorze canaux de 20 MHz mais un seul des canaux sera utilisé pour les transmissions. La technique de chipping consiste à envoyer un ensemble de bits (le chip) correspondant à un bit de données. L'étalement se fait donc au niveau de la quantité d'information envoyée. IEEE 802.11 définit le code de Barker sur 11 bits comme technique de chipping tandis que 802.11b et 802.11g utilise le CCK (8 bits).

L'avantage de cette technique couplée à différentes techniques de modulation est de proposer des immunisés contre les interférences locales étant donné qu'un seul canal de 20 MHz est utilisé.

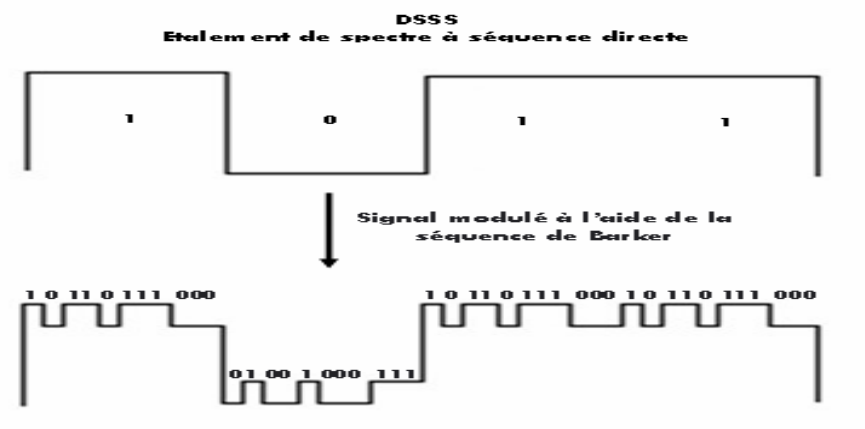

FIGURE 2.3: Technique de chipping

2.1.2.1 La structure de la trame en DSSS

Une trame au niveau physique est composée, comme pour la technique précédente, de trois parties : un préambule, puis un entête et enfin la partie données (figure 2.4).

Préambule		En-tête				
Synchro 128 bits	SFD 16 bits	Signal 8 bits	Service 8 bits	Longueur 16 bits	CRC En-tête 16 bits	Trame MAC

FIGURE 2.4 :

La composition de la trame 802.11 au niveau physique pour le DSSS

2.1.2.2 Les avantages de DSSS

- Utilisation de messages de négociation pour s'assurer que le récepteur peut comprendre les paquets émis.
- Si la qualité du signal se dégrade : *décalage dynamique de débit.*
- Systèmes de redondance par étalement peu sensible aux interférences et aux erreurs de transmission.
- Bonne efficacité spectrale → Possibilité d'obtenir des débits élevés.
- Possibilité d'améliorer les performances par allongement du vecteur d'étalement.

2.1.3 La technique OFDM

OFDM est une technique de transmission largement utilisée dans les transmissions satellitaires telles que DAB (Digital Auto Broadcast) ou DVB (Digital Vidéo Broadcast) ou dans l'ADSL (Asymétrique Digital Subscriber Line). Cette technique devient de plus en plus présente dans la standardisation des réseaux locaux sans fil. Ainsi ; on la trouve dans les amendements 802.11a et 802.11g dans hyper LAN mais aussi dans des standards pour réseaux locaux personnels sans fil ou certains standards pour réseaux mobiles.

Comme pour le DSSS, la bande disponible est divisée en canaux de 20 MHz et sa transmission se fait que sur un canal. Chaque canal est divisé en 52 sous-canaux ayant pour largeur 300Khz. 48 sous-canaux sont utilisés pour la transmission des données tandis que les quatre autres sont chargés de la correction d'erreur ou FEC (Forward Error Correction). A chaque sous-canal est appliquée une technique de modulation définissant ainsi un canal à très bas débit. L'avantage d'OFDM vient de la formation d'un canal très haut débit de ces sous-canaux à très fiable débit, permettant ainsi d'atteindre des vitesses de transmission jusqu'à 54 Mbit/s pour 802.11a ou 802.11s. L'avantage d'OFDM est le mécanisme de correction d'erreur sur l'interface physique, évitant ainsi la gestion des retransmissions au niveau de la couche MAC.

3 La couche liaison

La couche liaison de données est composée de deux sous-couches :

- La sous-couche de contrôle de liaison logique (LLC : Ligical Link Control)
- La sous-couche de contrôle d'accès au support (MAC : Medium Access Control)

3.1 Sous couche LLC

La sous-couche LLC 802.11est totalement identique à la sous-couche LLC 802.2. Son but est de permettre aux protocoles réseaux de niveau 3 (par exemple IP) de reposer sur une couche unique (la couche LLC) quel que soit le protocole sous-jacent utilisé, dont le Wifi, l'Ethernet ou le Token Ring, par exemple. Tous les paquets de données WiFi transportent donc un paquet LLC. Il est possible d'avoir en même temps, sur même réseau trois protocoles de niveau 3 [6].

3.1.1 Sous-couche MAC

3.1.1.1 Principe

- Les terminaux écoutent la porteuse avant d'émettre.
- Si la porteuse est libre, le terminal émet; si non, il se met en attente.

La couche MAC 802.11 intègre beaucoup de fonctionnalités que l'on ne trouve pas dans la version 802.3.

Particularité du standard : Définition de 2 méthodes d'accès fondamentalement différentes au niveau de la couche MAC

- **DCF:** Distributed Coordination Function
- **PCF**: Point Coordination Function

3.1.1.2 Méthodes d'accès aux supports

- **DCF** : Distributed Coordination Function

Assez similaire au réseau traditionnel supportant le Best Effort.

- Conçue pour prendre en charge le transport de données asynchrones.
- Tous les utilisateurs qui veulent transmettre ont une chance égale d'accéder au support.

- **PCF :** Point Coordination Function

- Interrogation à tour de rôle des terminaux (polling).
- Contrôle par le point d'accès.
- Conçue pour la transmission de données sensibles.
- Gestion du délai, application de type de temps réel : Voix, Vidéo.

Le **DCF** est basé sur le CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), Ethernet : CSMA/CD (Collision Detection)

- CSMA/CD ne peut pas être utilisé dans les environnements sans fil

• Pour détecter une collision, une station doit être capable d'écouter et de transmettre en même temps

• Dans les systèmes radio, la transmission couvre la capacité de la station à entendre la collision. Si une collision se produit, la station continue à transmettre la trame complète : perte de performance du réseau. Le principe de la technique CSMA/CA se présente dans les actions suivantes :

- ✓ L'utilisation d'acquittements positifs
- ✓ Les temporisateurs IFS
- ✓ L'écoute du support
- ✓ L'algorithme de Back off

Évite les collisions en utilisant des trames d'acquittement .ACK envoyés par la station destination pour confirmer que les données sont reçues de manière intacte→ contrôler les collisions.

Accès au support contrôlé par l'utilisation d'espace inter-trame ou IFS (Inter-Frame Spacing) :

- Intervalle de temps entre la transmission de 2 trames
- Intervalles IFS = périodes d'inactivité sur le support de transmission.

3.1.1.3 Ecoute de support

- La station voulant émettre écoute le support.

- Si aucune activité n'est détectée pendant un DIFS; transmission immédiate des données
- Si le support est occupé, la station écoute jusqu'à ce qu'il soit libre.

- Quand le support est disponible, la station retarde sa transmission en utilisant l'algorithme de back off avant de transmettre.

- Si les données ont été reçues de manière intacte (vérification du CRC de la trame), la station de destination attend pendant un SIFS et émet un ACK.

- Si l'ACK n'est pas détecté par la source ou si les données ne sont pas reçues correctement, on suppose qu'une collision s'est produite et la trame est retransmise.

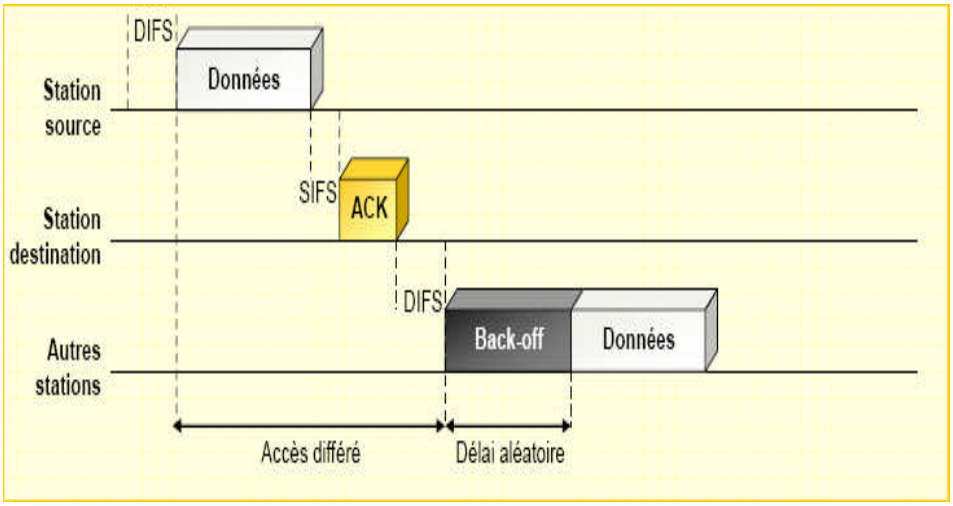

Figure 2.5 : Accès au support CSMA/CA

3.1.1.4 Algorithme de Back off

➧ Permet de résoudre le problème de l'accès au support lorsque plusieurs stations veulent transmettre des données en même temps.

➧ Temps découpé en tranches (Time slots) : Le Time slot de 802.11 est un peu plus petit que la durée de transmission minimale d'une trame ; utilisé pour définir les intervalles IFS.

➧ Initialement, une station calcule la valeur d'un temporisateur = Timer back off, compris entre 0 et 7. Lorsque le support est libre, les stations décrémentent leur temporisateur jusqu'à ce que le support soit occupé ou que le temporisateur atteigne la valeur 0.

- Si le temporisateur n'a pas atteint la valeur 0 et que le support est de nouveau occupé, la station bloque le temporisateur.

- Dès que le temporisateur atteint 0, la station transmet sa trame.

- Si 2 ou plusieurs stations atteignent la valeur 0 au même instant, une collision se produit et chaque station doit régénérer un nouveau temporisateur, compris entre 0 et 15.

➧ Pour chaque tentative de retransmission, le temporisateur croît de la façon suivante : [2 ^2+1* randf()] * time slot .

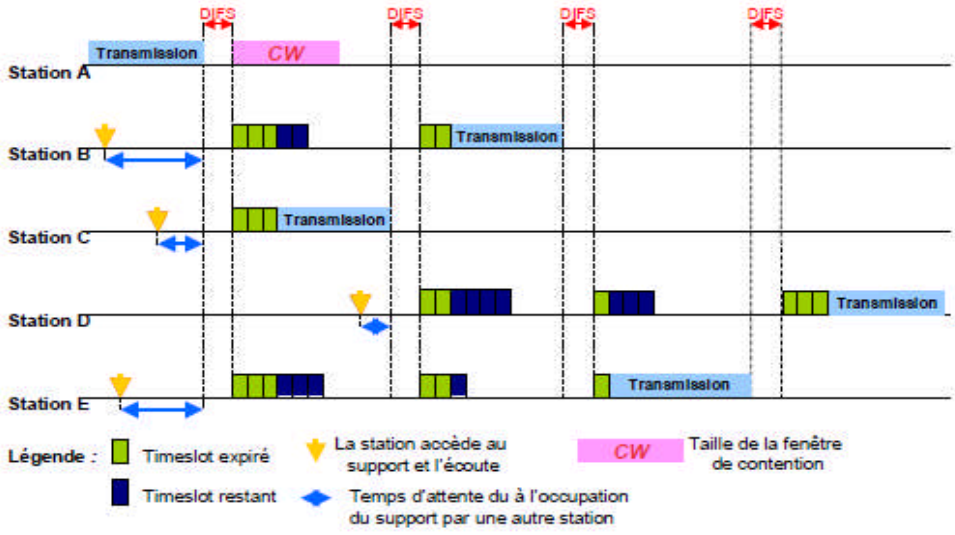

FIGURE 2.6 : Algorithme de Back off

3.1.1.5 Mécanisme de réservation

Envoi de trames RTS/CTS (Request To Send/Clear To Send) entre une station source et une station destination avant tout envoi de données.

- La station qui veut émettre envoie un RTS

➧ Toutes les stations du BSS entendent le RTS, lisent le champ de durée du RTS et mettent à jour leur NAV.

- La station destination répond après un SIFS, en envoyant un CTS.

- Les autres stations lisent le champ de durée du CTS et mettent de nouveau à jour leur NAV

- Après réception du CTS par la source, celle-ci est assurée que le support est stable et réservé pour la transmission de données.

➧ Le NAV est calculé par rapport à l'information située dans le champ de durée de vie ou TTL contenu dans les trames envoyée. Le NAV permet de retarder toutes les transmissions.

Transmission des données et réception de l'ACK sans collision.

➧ Les trames RTS / CTS réservent le support pour la transmission d'une station.

Le mécanisme est habituellement utilisé pour envoyer de grosses trames pour lesquelles une retransmission serait trop coûteuse en termes de bande passante.

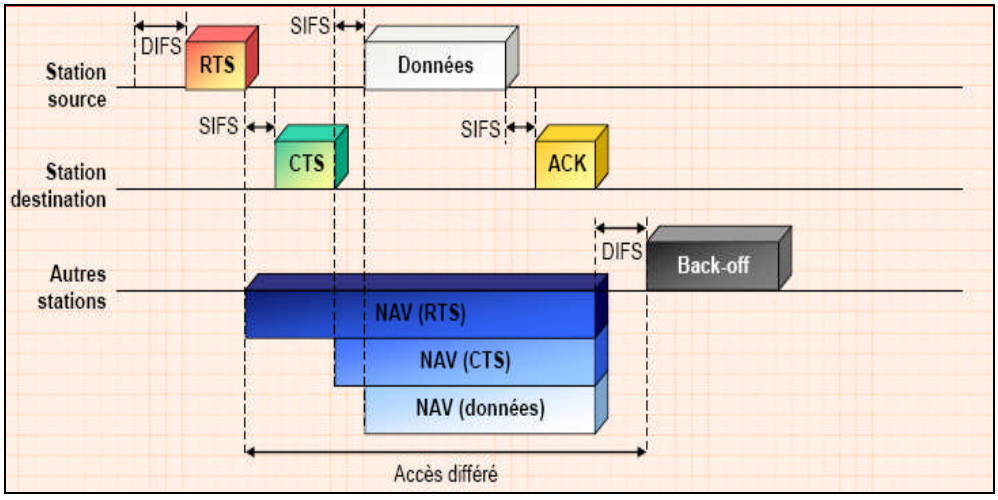

Figure 2.7 : Réservation du support avec les trames RTC/CTS

4 La couche réseaux

4.1 Routage

Le routage est une méthode d'acheminement des informations à la bonne destination à travers un réseau de connexion donné. Le problème du routage est posé pour un réseau dont les arcs, les nœuds et les capacités sur les arcs sont fixés, et il est nécessaire de déterminer un acheminement optimal et de qualité des paquets de données (de message, de produit….. etc.) à travers les réseaux au sens d'un certain critère de performance. Le but et de trouver l'investissement de moindre coût en capacités nominales et de réserves qui assure le routage du trafic nominal et garantit sa suivre en cas de n'importe quelle panne d'arc ou de nœud.

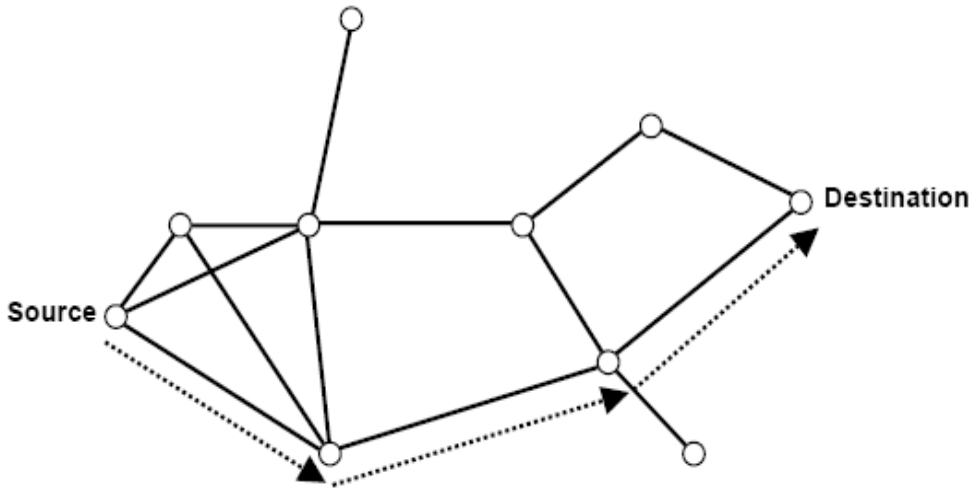

FIGURE 2.8 : Exemple de routage

La performance des WMNs repose énormément sur le routage. L'algorithme de routage doit prendre en compte l'extensibilité, le découvert rapide des routes et des pannes. Il doit aussi supporter la mobilité et assurer la flexibilité et la QoS. Les nœuds dans les WMNs ont une mobilité réduite et n'ont pas de contrainte de consommation d'énergie. Plusieurs types de protocoles sont proposés et utilisés pour résoudre le problème de routage dans les WMNs. il existe deux types de base de protocoles : les protocoles réactifs et les protocoles proactifs.

Les protocoles réactifs ne vont chercher à calculer une route que sur la demande d'une application. Ils réduisent ainsi le trafic de contrôle mais augmentent le délai nécessaire pour obtenir la route vers sa destination. Parmi ces protocoles, on cite :

4.1.1 Le protocole HWMP

Le protocole HWMP (Hybride Wireless Mesh Protocol) [1, 2, 27, 28] est un protocole de routage dévloppé pour les réseaux maillées. Il combine les deux approches proactive à base d'arbre et réactive. HWMP utilise un ensemble de primitives et de traitements acquis du protocole AODV (Ad-hoc On Demande Distance Vector) [17, 18]. L'extension de AODV pour les réseaux mesh est adaptée pour faire l'adressage au niveau de la couche 2 (couche liaison) et l'utilisation d'une métrique radio. AODV est le protocole de base pour la version reactive .

Cependant, des primitives sont utilisées pour installer un arbre à vecteur de distance pour un routage vers la racine. Le rôle de la racine qui permet la formation d'une topologie en arbre est une option configurable d'un MP.HWMP qui supporte deux modes opératoires en fonction de la configuration.

- **Mode réactif** : dans ce mode, les nœuds créent et maintiennent les routes selon le besoin. Lorsque un nœud à besoin d'une route qui n'exsite pas dans sa table de routage, une procédure de découverte globale de route est lancée.

- **Mode proactif** : dans ce mode, lorsqu'un nœud du réseau souhaite communiquer avec un autre nœud, il peut localement intérroger la table de routage dont il dispose. Le routage peut ainsi ètre effectué de proche en proche, à l'image du routage IP. Le mode proactif définit deux sous modes à base d'arbre :

  - Proactive Path REQuest (Proactive PREQ)
  - Proactive Route ANNouncement (Proactive RANN)

4.1.2 Le protocole DSDV

DSDV (Destination Séquence Distance Vector) : Ce protocole est considéré comme un protocole proactif, il est basé sur l'idée classique de l'algorithme distribué de Bellman-Ford (DBF : Distrubted Bellman Ford :algorithme qui calcule le meilleur chemin pour accéder d'une source à une destination) en rajoutant quelques améliorations.

Chaque station mobile maintient une table de routage qui contient :

- Toutes les destinations qui sont possibles.
- Le nombre de nœuds (ou de sauts) nécessaire pour atteindre la destination.
- Le numéro de séquence (N.S) qui correspond à un nœud destination.

- Le N.S est utilisé pour faire la distinction entre les anciennes et les nouvelles routes, ce qui évite la formation des boucles de routage.

La mise à jour dépend de deux paramètres : Le temps (c'est-à-dire la période de la transmission) et les événements.

Un paquet de mise à jour contient :

- Le nouveau numéro de séquence incrémenté du nœud émetteur.
- Pour chaque nouvelle route :

- l'adresse de la destination.
- Le nombre de sauts (hop count) séparant le nœud de la destination.
- Le numéro de séquence tel qu'il a été estampillé par la destination.

Les données de routage reçues par une unité mobile sont comparées avec les données déjà disponibles. La route étiquetée par la plus grande valeur du numéro de séquence (la route la plus récente) est la route utilisée. Si deux routes ont le méme numéro de séquence alors la route qui posséde la meilleure métrique (hop count) est celle qui sera utilisée. Les modifications faites sur les données de routage locales sont immédiatement diffusées à l'ensemble courant des voisins. Les routes reçues par une diffusion seront aussi envoyées quand le récepteur procédera à l'envoi de ses paquets. Le récepteur doit incrémenter les métriques des routes reçues avant l'envoi car le récepteur représente un nœud en plus qui participe dans l'acheminement des messages vers la destination. Un lien rompu est matérialisé par une valeur infinie de sa métrique, une valeur plus grande que la valeur maximale permise par la métrique. A titre d'exemple, la figure 2.9 montre la représentation d'un réseau Ad hoc.

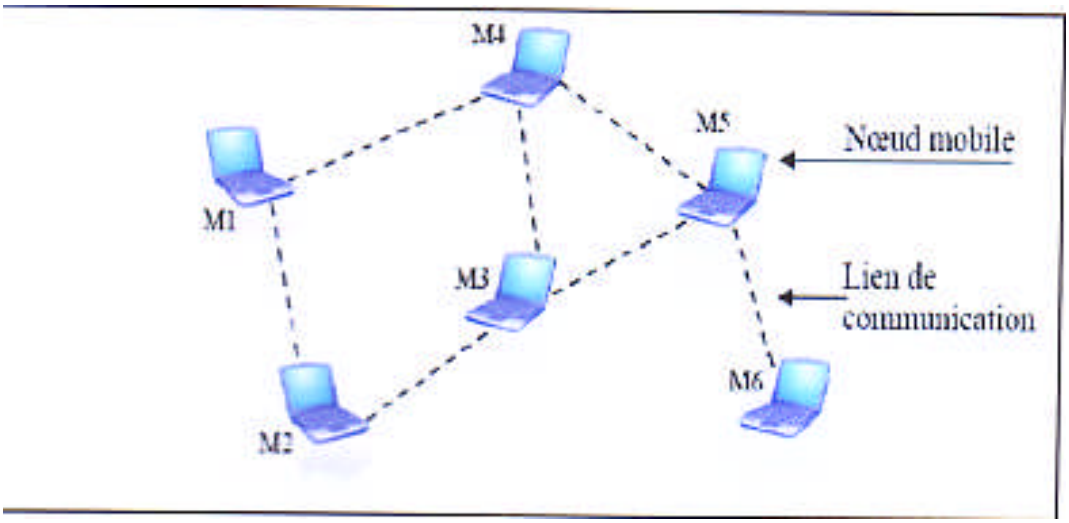

FIGURE 2.9 : Un réseau ad hoc

Si on utilise le protocole de routage DSDV, la table de routage correspondante au nœud M1 représentée dans le tableau ci-dessous ressemblera à la suivante :

Destination	Nombre de sauts	Prochaine saut	Numéro de séquence
M1	0	M1	NS1
M2	1	M2	NS2
M3	2	M2	NS3
M4	1	M4	NS4
M5	2	M4	NS5
M6	3	M4	NS6

TABLEAU 2.1 : Table de routage du nœud M1

Le DSDV élimine deux problémes : le probléme de boucle de routage ‘’routing loop’’ et celui du comptage à l’infini ‘’counting to infinity’’. Cependant, on décèle les problèmes suivants :

- Une unité mobile doit attendre jusqu’à ce qu’elle reçoive la prochaine mise à jour initiée par la destination afin de mettre à jour l’entrée associée à cette destination dans la table de distance, ce qui fait que le DSDV est lent.
- Le DSDV utilise une mise à jour périodique ce qui cause un contrôle excessif.

4.1.3 Le protocole AODV

Le protocole AODV ‘’Routage avec Vecteur de Distance à la Demande’’ (AODV :Ad hoc On demand Distance Vector), représente essentiellement une amélioration de l’algorithme DSDV. Le protocole AODV, réduit le nombre de diffusions de messages, et cela en créant des routes en cas de besoin, contrairement au DSDV, qui maintient la totalité des routes. L’AODV est basé sur l’utilisation des deux mécanismes ‘’Découverte de route’’ et ‘’Maintenance de route’’ (utilisés par le DSR), en plus du routage nœud-par-nœud, le principe des numéros de séquence et l’échange périodique du DSDV.

L’AODV utilise les principes des numéros de séquence à fin de maintenir la consistance des informations de routage. A cause de la mobilité des nœuds dans les réseaux ad hoc, les routes changent fréquemment ce qui fait que les routes maintenues par certains nœuds, deviennent invalides. Les numéros de séquence permettent d’utiliser les routes les plus récentes ou autrement dit les plus fraiches (fresh routes).

De la même manière que dans le DSR, l’AODV utilise une requête de route dans le but de créer un chemin vers une certaine distination. Cependant, l’AODV maintient les chemins d’une façon distribuée en gardant une table de routage, au niveau de chaque nœud de transit appartenant au chemin cherché. Une entrée de la table de routage contient essentiellement :

1- L’adresse de la destination.

2- Le nœud suivant.

3- La distance en nombre de nœud (i.e le nombre de nœuds nécessaires pour atteindre la destination).

4- Le numéro de séquence destination.

5- Le temps d’expiration de l’entrée de la table.

Quand un nœud de transit (intermédiaire) envoie le paquet de la requête à un voisin, il sauvegarde aussi l'identificateur du nœud à partir duquel la première copie de la requête est reçue. Cette information est utilisée pour construire le chemin inverse, qui sera traversé par le paquet réponse de route (cela veut dire que l'AODV supporte seulement les liens symétriques).

Puisque le paquet réponse de route va être envoyé à la source, les nœuds appartenant au chemin de retour vont modifier leurs tables de routage suivant le chemin contenu dans le paquet de réponse.

Un nœud diffuse une requête de route (RREQ :Route REQuest), dans le cas où il aurait besoin de connaître une route vers une certaine destination et qu'une telle route n'est pas disponible comme dans la figure 2.10. Cela peut arriver si la destination a expirée sa durée de vie ou elle est devenue défaillante (i.e la métrique qui lui est associée est infinie).

Le champ numéro de séquence est associé au nœud destination. Cette valeur est recopiée de la table de routage.

Si le numéro de séquence n'est pas connu, la valeur nulle sera prise par défaut. Le numéro de séquence source du paquet RREQ contient la valeur du numéro de séquence du nœud source. Comme nous avons déjà dit, après la diffusion du RREQ, la source attend le paquet réponse de route (RREP :Route REPly). Si ce dernier n'est pas reçu durant une certaine période (appelée RREP_WAIT_TIME), la source peut rediffuser une nouvelle requête RREQ. A chaque nouvelle diffusion, le champ Broadcast ID du paquet RREQ est incrémenté. Si la requête RREQ est rediffusée un certain nombre de fois (RREQ_RETRIES) sans l'obtention de réponse, un message d'erreur est délivré à l'application [7].

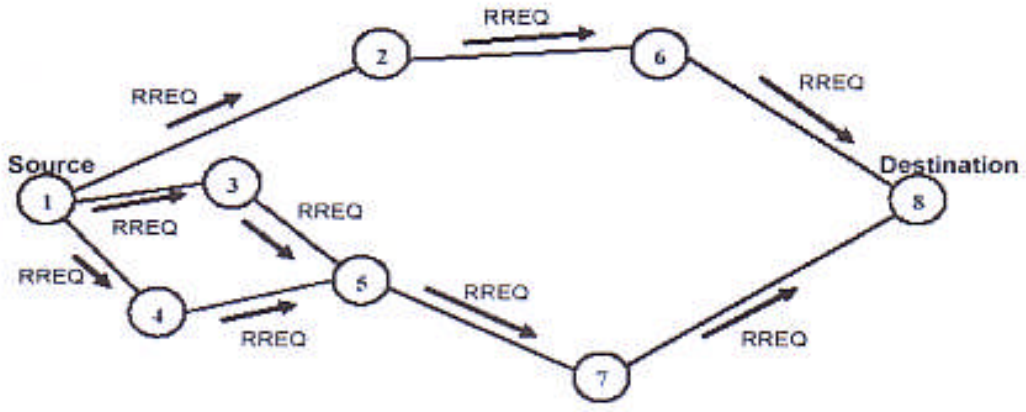

FIGURE 2.10 : La requête RREQ

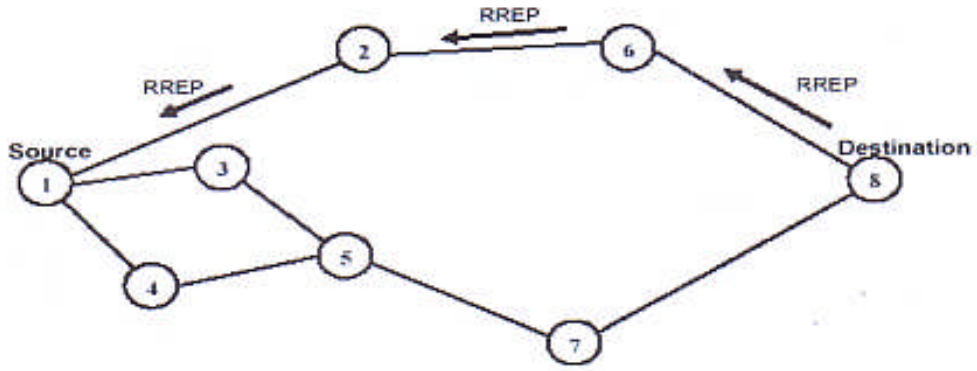

FIGURE 2.11 : La requête RREP

4.1.4 Le protocole DSR

Le DSR (Dynamic Source Routing) est un protocole semblable au protocole AODV, il utilise une technique appelée « Source Routing » dans laquelle l'émetteur (la source) indique la route complète par le quel un paquet doit passer pour atteindre sa destination, cette route est insérée dans l'entête du paquet. Les nœuds intermédiaires entre le nœud source et le nœud destination n'ont pas besoin de maintenir à jour les informations sur la route traversée puisque la route complète est insérée dans l'entête du paquet.

Si un nœud dans DSR veut communiquer avec une destination à laquelle il ne possède pas de route, il inonde le réseau avec un paquet de requête (RREQ) similaire a celui de AODV. Chaque nœud qui reçoit la requête et qui ne possède pas de route à la destination demandée insère son adresse dans le paquet RREQ et le diffuse à ses voisins.

La réponse à la requête (RREP) est retournée par la destination ou par un autre nœud qui possède une route à la destination.

Les routes dans AODV sont construites en traversant la route inverse vers la source (de la destination à la source). Dans le DSR, les routes sont construites quand la requête traverse le réseau vers la destination (de la source à la destination).

Si un nœud reçoit un paquet de données, et le lien à utiliser pour retransmettre ce paquet est coupé (coupure de route), le nœud envoie un message d'erreur de route (RERR) semblable à celui de AODV au nœud source ; le nœud source va lancer une autre requête de découverte de route pour atteindre la destination.

Le protocole DSR comme le protocole AODV utilise l'inondation pour découvrir les routes ce qui génère un trafic de contrôle énorme quand le réseau est très utilisé. La taille des paquets de données dans le DSR devient très grande quand le nombre de nœuds dans le réseau est grand, puisque les paquets doivent porter les adresses de chaque nœud dans la route traversée . Le DSR a aussi un délai avant de commencer la transmission des paquets provoqués par la procédure de découverte de route [7].

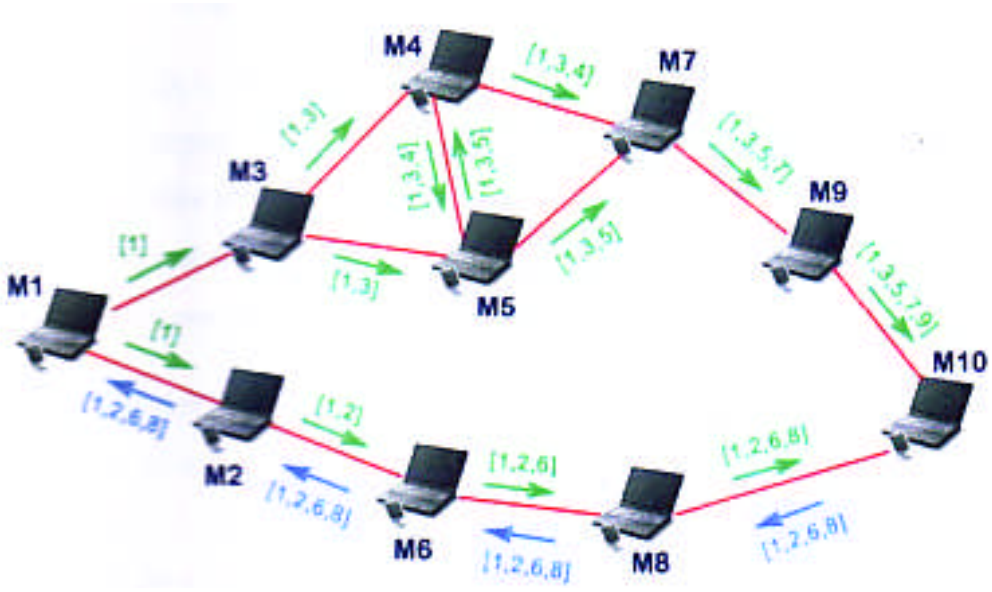

FIGURE 2.12 : Le principe de decouverte de route par DSR [8]

4.1.5 Le protocole OLSR :

Le OLSR (Optimized Link State Routing) est un protocole de routage proactif non uniforme dédié aux réseaux ad hoc, inspiré de l'algorithme état des liens classiques, développé dans le cadre du projet Hipercom de l'institut national de la recherche en informatique et algorithmique (INRIA) et proposé en tant que RFC (Request For Comment). Il a comme objectif de fournir des routes de plus court chemin en termes de nombre de sauts. Le OLSR utilise les multipoints relais (MPR) pour retransmettre les messages diffusés au cours d'une inondation dans le but de réduire le nombre de messages envoyés, ce qui réduit par conséquence les frais ; tel que, lorsqu'un nœud MPR reçoit un message de diffusion, il traite et rediffuse le message. Par contre un nœud non MPR traite seulement le message. Par ailleurs, le OLSR utilise le concept d'interface, tel qu'un

nœud peut possèder plusieurs instances d'écoute, ce qui lui donne le comportement de plusieurs nœuds virtuels. C'est un protocole qui fonctionne mieux dans les réseaux denses et larges.

4.1.6 Tableaux de comparaison

Nous décrivons dans les deux tableaux suivants les différentes classes de protocoles de routage pour les réseaux ad hoc ainsi que les protocoles de routage présentés dans ce chapitre :

Classes	Caractéristique	Avantages	Inconvenient
Proactif	- Calculer les routes à l'avance.	- Transmission immédiate des données.	- Utiliser beaucoup de paquets de contrôles. - Consomation de la bande passante.
Réactif	- Calculer les routes à la demande.	- Utiliser moins de paquets de contrôles. - Economisation de la bande passante	- Délai initial avant de commencer la transmission des données.
Hybride	- Combinaison des deux approches précédentes.	- Bénéficier des avantages des deux approches précédentes	- Cumuler les inconvénients des deux approches précédentes

TABLEAU2.2 : Les classes des protocoles de routage pour les réseaux ad hoc

Protocoles	Classe	Avantages	Inconvénients
DSDV	Proactif	- fournit à tout moment des routes valables vers toutes les destinations du réseau.	- L'inondation des paquets de mis à jour cause une charge de contrôles importante au réseau.
AODV	Réactif	- découvre les routes à la demande en inondant le réseau avec un paquet de requête.	- Délai initial avant de commencer la transmission des données.
DSR	Réactif	- découvre les routes à la demande en inondant le réseau avec un paquets de requête. - Les paquets de données peuvent être redirigés pendant leurs transmissions.	- Délai initial avant de commencer la transmission des données. - La taille des paquets de données très grande quand le nombre de nœud dans le réseau est grand.
OLSR	Proactif non uniforme	- fournir des routes de plus court chemin	- rediffuse les messages qui va diminuer la capacité d'energie
HWMP	Prpactif et réactif	- découvre la route selon le besoin	- introduit la table de routage

TABLEAU 2.3 : les avantages et les inconvénients des protocoles

5 Conclusion

Dans ce chapitre, nous avons focalisé sur le principe de fonctionnement de WMN et surtout sur le routage et nous sommes intéressés aux spécificités du routage dans le cadre de réseau WLAN mesh par rapport aux autres types de réseaux sans fil en détaillant la métrique de routage et les mécanismes de découverte des routes.

Ensuite, nous avons présenté une comparaison détaillée des protocoles de routage IEEE 802.11s dans un réseau mesh.