RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
Université El Hadj Lakhdar de Batna
Faculté des Sciences de L'ingénieur
Département D'informatique

Mémoire pour L'obtention du Diplôme du Magistère en Informatique

OPTION : INFORMATIQUE INDUSTRIELLE

THEME

Prise en Compte de la QoS par les Protocoles de Routage dans les Réseaux Mobiles Ad Hoc

Présenté par : ***M. Boulkamh Chouaib***

Sous la Direction de : ***Dr. Bilami Azeddine***

Devant le jury composé de:

Dr. Belattar Brahim M.C Université de Batna (Président de jury)
Dr. Chaoui Alloua M.C Université de Constantine (Examinateur)
Dr. Kezzar Okba M.C Université de Biskra (Examinateur)
Dr. Bilami Azeddine M.C Université de Batna (Rapporteur)

N° d'ordre :……
Série :……

Année 2007-2008.

Remerciement

Je suis profondément reconnaissant à monsieur Bilami Azeddine, Maître de conférence à l'université de Batna, pour m'avoir proposé ce sujet, m'avoir aiguillé dans ma recherche, ainsi que pour ses conseils et ses critiques.

Je tiens à remercier Dr. Belattar Brahim de m'avoir honoré en présidant le jury. Merci également à Messieurs Dr. Chaoui Alloua et Dr. Kezzar Okba pour l'honneur qu'il me font en participant à ce jury.

Je tiens aussi à exprimer toute ma gratitude envers mes parents, mes frères Fateh et Hichem et mes sœurs dont l'aide et l'encouragement m'ont permis de continuer mes études.

Merci aussi à messieurs Sedrati Maamar et Maamri Ramdane, pour leur aide et leurs conseils.

Je terminerais en remerciant tous les amis et les collègues qui ont aidé à l'accomplissement de ce travail.

Résumé

Les réseaux ad hoc sont des réseaux mobiles et sans fil capables de fonctionner sans infrastructure. Ils s'adaptent dynamiquement à leur environnement et à leur topologie.

Les réseaux mobiles ad hoc étant généralement multi-saut. Par conséquent, un protocole de routage est nécessaire. Plusieurs protocoles de routage ont été développés et standardisés par l'IETF pour ce type de réseaux. Ces protocoles calculent les routes en minimisant le nombre de sauts entre la source et la destination.

Avec l'émergence des services multimédias dans les réseaux mobiles, des travaux pour l'introduction de la qualité de service dans les réseaux ad hoc ont été proposés. Les études existantes sont souvent basées sur des hypothèses limitées et inadaptées aux propriétés des réseaux ad hoc. En effet, les réseaux mobiles ad hoc (MANET) posent des problèmes spécifiques ayant une influence importante sur les solutions à mettre en place pour assurer la QoS. Les principaux problèmes sont : la mobilités des nœuds et l'incertitude des liens.

La QoS peut être fournie à différents niveaux, mais notre étude se concentrera sur les solutions implémentées dans des protocoles de routage des réseaux Ad Hoc.

Les algorithmes de routage dans les réseaux mobiles Ad Hoc n'ont pas été développés initialement pour tenir compte de contraintes temps réel et sont de ce fait non adaptés aux applications qui nécessitent le support de la QoS (Quality of Service). Ce travail traite d'un protocole qui met en œuvre des solutions pour la garantie d'une QoS dans les réseaux mobiles Ad Hoc. Des simulations sous Network Simulator ns2 ont été conduites pour étudier le comportement de notre protocole, et le comparer avec le protocole AODV, en se focalisant sur le trafic de contrôle, le taux des paquets perdus/reçus et le délai de bout en bout (latence).

Mots-clés : Réseaux mobiles Ad hoc, métriques de qualité de service, routage avec qualité de service, équilibrage de la charge de réseau.

Abstract

Mobile ad hoc networks are able to work without infrastructure. They are dynamically adaptable to their environment and their topology.

Mobile Ad hoc networks are generally multi-hop. Consequently, a routing protocol is necessary. Several routing protocols were developed and standardized by the IETF for this kind of networks. These protocols calculate the routes by minimizing the number of hops between the source and the destination.

With the emergence of multimedia services in the mobile networks, several works to introduce the quality of service into mobile ad hoc networks were proposed. The existing studies are insufficient and unsuited to the properties of ad hoc networks. In fact, these networks introduce new problems and have to be addressed in order to provide an efficient quality of service solution. The principal problems are: mobility of the nodes and the nature of the wireless medium.

QoS can be provided at various levels, but our study will concentrate on the solutions implemented in routing protocols in ad hoc networks.

The routing protocols in Mobile Ad hoc NETworks (MANET) were not developed initially to be considered in real time constraints and are not adapted to the applications that require the support of QoS (Quality of Service). In this work we aim to develop a routing protocol which implements solutions for the guarantee of QoS in mobile ad hoc networks. A number of simulations under the Network Simulator NS2 were led to study the behaviour of our protocol, and to compare it with the AODV routing protocol, we set our interest on the traffic of control, the packet delivery ratio (PDR) and the end to end delay.

Key words: mobile Ad hoc networks, performance metrics, QoS routing, network load balancing.

Table des matières

3. La Qualité de Service Dans les Réseaux Mobiles Ad Hoc

4. Le Protocole HCAR

5. Simulations et Résultats

6. Conclusion et perspectives.

Références.

Introduction Générale

Le progrès technologique, en particulier, l'avènement de la microélectronique et la miniaturisation des circuits imprimés et des puces ont permis la fusion du terminal et de l'interface de communication radio en une seule entité, ce qui a permis le développement des moyens de communications mobiles tels que les téléphones cellulaires, les assistants personnels et les ordinateurs portables.

Le développement important des réseaux sans fil, aussi bien à l'intérieur des entreprises, pour remplacer des réseaux filaires traditionnels, qu'au niveau des lieux publics, ainsi que le grand succès connu par la téléphonie mobile, ont montré l'intérêt commercial des moyens de transmissions sans fil et laisse à penser que l'utilisateur va devenir de plus en plus mobile. Dans ce contexte, des travaux de recherches ont débuté afin d'obtenir des solutions de communication sans fil de plus en plus performantes.

En 1999, l'IEEE a standardisé le protocole d'accès au medium radio 802.11 [1] visant à assurer la communication entre ordinateurs personnels utilisant le medium radio. Aujourd'hui, le protocole IEEE 802.11 a subi plusieurs évolutions et est devenu un standard. Cependant, l'utilisation des stations de base pour la communication entre terminaux ne pouvait résister longtemps au désir de s'affranchir de toute contrainte, les travaux des recherches militaires sur les packet radio networks (PRNet) ont réussi de se passer de ces stations de bases formant ainsi des réseaux mobiles totalement dynamiques et spontanés. Il s'agit des réseaux Ad Hoc.

Un réseau mobile ad hoc est une collection d'entités mobiles, interconnectées par une technologie sans fil formant un réseau temporaire sans l'aide d'aucune infrastructure préexistante ou administration centralisée. Dans de tels environnements, les hôtes mobiles sont obligés de se comporter comme des routeurs afin de maintenir les informations de routage du réseau.

Nul doute que, cette nouvelle technologie constitue un domaine de recherche actif et ouvre de nombreuses perspectives, cela est du essentiellement à la diversité des applications potentielles, ainsi qu'au contraintes introduites par ces réseaux, entre autre : la mobilité des nœuds, le changement dynamique de la topologie, la bande passante limitée, des sources d'énergie autonomes, etc. Ces contraintes font que les solutions retenues pour les réseaux classiques ne sont pas applicables directement aux réseaux mobiles ad hoc.

Comme pour les réseaux filaires, le besoin de transmettre différents types de média sur les réseaux Ad hoc est important et même nécessaire. Ce type d'applications, telles que la téléphonie, la vidéo à la demande ou la conférence multimédia, exigent un transfert de données complexe et l'en voit apparaître un réel besoin de garantie sur la qualité de service offert, par exemple, garantir une borne sur le délai de transmission des paquets peut être profitable aux applications de téléphonie, garantir un débit peut être nécessaire pour les applications de vidéo à la demande. Cependant, au regard des spécificités des réseaux Ad hoc, la garantie d'une qualité de service pour certains types d'applications est une tâche très complexe.

Le terme « Qualité de Service« désigne la capacité du réseau à fournir un service, transfert de données par exemple. Cette notion est vaste et influence tous les protocoles utilisés dans les différentes couches OSI. Dans le cadre de notre travail, nous nous sommes intéressés au

problème de routage avec qualité de service pour les réseaux Ad hoc, car ce point soulève beaucoup de problèmes auxquels il n'existe pas encore de solutions satisfaisantes.

Ce mémoire est structuré en cinq chapitres :

Dans le premier chapitre, nous avons présenté les différents concepts liés aux réseaux sans fil et environnements mobiles.

Le deuxième chapitre est consacré aux réseaux mobiles Ad hoc, en mettant la lumière sur ses caractéristiques et ses spécificités, et nous présentons à ce niveau une classification des différentes approches pour le routage dans ce type de réseaux.

La notion de la qualité de service et ses solutions dans les réseaux filaires, ainsi que les travaux développés pour la garantie de la qualité de service dans les réseaux Ad hoc, sont illustrés dans le troisième chapitre.

Dans le quatrième chapitre, nous proposons un protocole de routage avec qualité de service pour les réseaux ad hoc, que nous appelons **HCAR**, nous présentons d'abord son principe de fonctionnement, ensuite nous spécifions les messages de contrôle utilisés pour l'établissement et le maintien des routes, ainsi que le mécanisme adopté pour la gestion des nœuds éloignés.

Dans le chapitre cinq, nous présentons l'outil de simulation Network Simulator 2 (NS2), ainsi que les langages et outils graphiques utilisés pour l'interprétation et l'analyse des résultats de simulation. Après avoir présenté le modèle de simulation, et de trafic utilisé, une étude comparative entre notre protocole de routage et le protocole AODV est donnée.

Finalement, nous terminerons par une conclusion générale, avec quelques perspectives définissant les travaux futurs que nous comptons mener et qui vont dans le sens de l'amélioration de la QoS dans les réseaux ad hoc.

.

Chapire01 :
Réseaux sans fil et Environnements mobiles

Le rôle essentiel des réseaux et le développement rapide d'Internet témoignent des avantages réels du partage des données et des ressources. Pour conserver leur souplesse, les entreprises ont besoin de solutions innovantes, pour lesquelles la mobilité est un facteur clé [2].

Le concept de mobilité est lié à la notion de réseaux sans-fil qui procure une liberté et un gain de productivité réels. Les technologies sans-fil permettent d'élargir les possibilités de la mobilité en offrant un nombre plus important de services aux utilisateurs en fonction de leurs activités (marketing, commerciale, direction,…) [3].

Un réseau sans fil est un système de transmission des données conçu pour assurer une liaison indépendante de l'emplacement des périphériques informatiques qui composent le réseau et utilisant les ondes radio plutôt qu'une infrastructure câblée. A cette fin, des bornes sont installées pour délimiter une zone de couverture; les utilisateurs peuvent en profiter à condition de disposer d'un adaptateur pour émettre et recevoir sur ce réseau. Cet adaptateur peut prendre la forme d'un boîtier, d'une carte PCI ou encore, pour les ordinateurs portables, d'une carte au format PCMCIA.

Un réseau sans fil offre toutes les fonctions d'un réseau câblé, sans les contraintes liées au branchement des câbles. Autrement dit, La mise en place d'un réseau sans fil offre aux utilisateurs l'accès aux données partagées sans avoir à chercher de prise pour se brancher. Cette mobilité accrue permet d'accéder à l'information indépendamment des facteurs temps et lieu.

Les réseaux sans fil connaissent aujourd'hui un grand succès grâce à leur grande flexibilité, leur souplesse d'utilisation, en outre, leur déploiement est facile et rapide (pas de câble), ils permettent, en particulier, la mise en réseau des sites dont le câblage serait trop onéreux à réaliser dans leur totalité, voire même impossible.

Ce chapitre a pour objectif de présenter la technologie de communication sans fil; pour cela nous détaillons quelques principales notions nécessaires à la compréhension de ces systèmes, on s'intéresse plus particulièrement aux couches : liaison de données et physique utilisées dans le modèle OSI. Nous introduisons, également, L'environnement mobile, et les principaux concepts liés à ce nouvel environnement.

1 Les Réseaux sans Fil :

Un réseau sans fils (*en anglais wireless network*) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fils, un utilisateur à la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu. Le développement constant de ces réseaux sans fil a amené la création de nouvelles normes afin de mieux interconnecter les machines.

1.1.1 Historique

Les progrès considérables établis au XXe siècle ont été le facteur essentiel dans le développement des télécommunications et tout cela ne serait rien sans le concours providentiel de certains hommes qui ont révolutionné le domaine des télécommunications sans fil.

En 1873, James Maxwell, à Londres, publie son traité d'électricité de magnétisme: raisonnement qui établit que des perturbations électromagnétiques de fréquences diverses, non perceptibles par nos sens, rayonnent dans l'espace.

Plus tard, en 1887, Heinrich HERTZ à Karlsruhe, vérifiera par l'expérience des théories de Maxwell : une étincelle électrique jaillit entre deux boules de cuivre, et à quelques mètres, simultanément, une étincelle minuscule prend naissance sur des armatures en forme de boucles. Il est ainsi prouvé que les oscillations électromagnétiques sont induites à distance, c'est la naissance des ondes Hertziennes. Désormais, il est possible de déclencher une action mécanique importante à distance, à travers les murs, sans lien matériel.

Dans les années 1900, le jeune Guglielmo MARCONI, qui va devenir le grand promoteur et industriel de la TELEGRAPHIE SANS FIL, commence ses expériences près de BOLOGNE. Lui aussi a l'idée de transmettre SANS FIL des messages MORSE. Il pressent que les ondes Hertziennes peuvent se propager A GRANDE DISTANCE. Muni de capitaux importants, il augmente progressivement la puissance des appareils émetteurs de HERTZ et la sensibilité des dispositifs récepteurs de BRANLY.

Fin 1895, il fait inscrire des signaux MORSE à 24OO mètres puis en Décembre 1901, installé à TERRE-NEUVE, il perçoit des signaux émis depuis la côte Est de l'ANGLETERRE : 3400 Km. Le succès de cette expérience est confirmé en 1903 par la réception d'un message télégraphique complet.

C'est après la libération que débute la révolution technique qui a vu successivement les télécommunications s'automatiser, " s'électroniser " et se numériser.

C'est en 1938 que commence l'aventure de l'ordinateur moderne. L'allemand Konrad Zuse conçoit le premier calculateur universel binaire commandé par programme. Cette machine appelée Z1 était composée d'une unité mémoire et d'une unité arithmétique. Deux ans plus tard, en 1940, la guerre fait naître l'ordinateur électronique. En 1941, le Z3 comprenait un calculateur universel contrôlé par programme, un lecteur de bande perforée et une console pour l'opérateur.

En 1949, le Z4, plus puissant avec une mémoire de 512 mots de 32 bits, sera le premier ordinateur vendu par Konrad Zuse. Au même moment, de l'autre côté de l'Atlantique, Howard HAiken conçoit un calculateur électromagnétique à registres, le " HAVARD MARK 1 ", composé de 765 299 éléments. Il pesait 5 tonnes et avait besoin de plusieurs tonnes de glace par jour pour le refroidir.

C'est bien plus tard, aux Etats-Unis que commence l'aventure d'Internet dans les années 1960. La peur d'une guerre nucléaire incite à cette époque les responsables de l'armée américaine, au sein du Pentagone, à inventer un système de communication qui serait toujours en état de fonctionnement : Internet était né. Près de 10 ans plus tard, Internet quitte le domaine militaire pour celui de l'Université. Les calculateurs de quatre universités américaines sont connectés entre eux. Mais il faut attendre 1990 et la mise en service par le CERN (Centre Européen de la Recherche Nucléaire) du WWW (World Wide Web) pour que les ordinateurs du monde entier puissent communiquer entre eux grâce à ce langage. De nos jours, au vu du

nombre de personnes désirant s'abonner à Internet, ce dernier doit se servir de tous les moyens de communication mis à sa disposition, par conséquent les ondes hertziennes.
C'est ainsi que de nouveaux modes de communication sont apparus afin de relier différents sites au réseau Internet. L'autre besoin se faisant sentir est bien évidemment l'aspect mobilité, en effet, il est beaucoup plus aisé de se déplacer avec des équipements sans fil.

De nos jours, la technologie permet d'envoyer de plus en plus d'informations de plus en plus vite. Nous avons donc vu tout naturellement apparaître les communications numériques via les ondes hertziennes.

[9]

1.1.2 Catégories de réseaux sans fil

Plusieurs gammes de produits sont actuellement commercialisées, mais la normalisation pourrait encore modifier les choses. Les groupes de travail qui se chargent de cette normalisation proviennent de l'IEEE aux États-Unis et de l'ETSI en Europe. La figure suivante décrit les différentes catégories de réseaux sans fil suivant leur étendue (appelé zone de couverture).

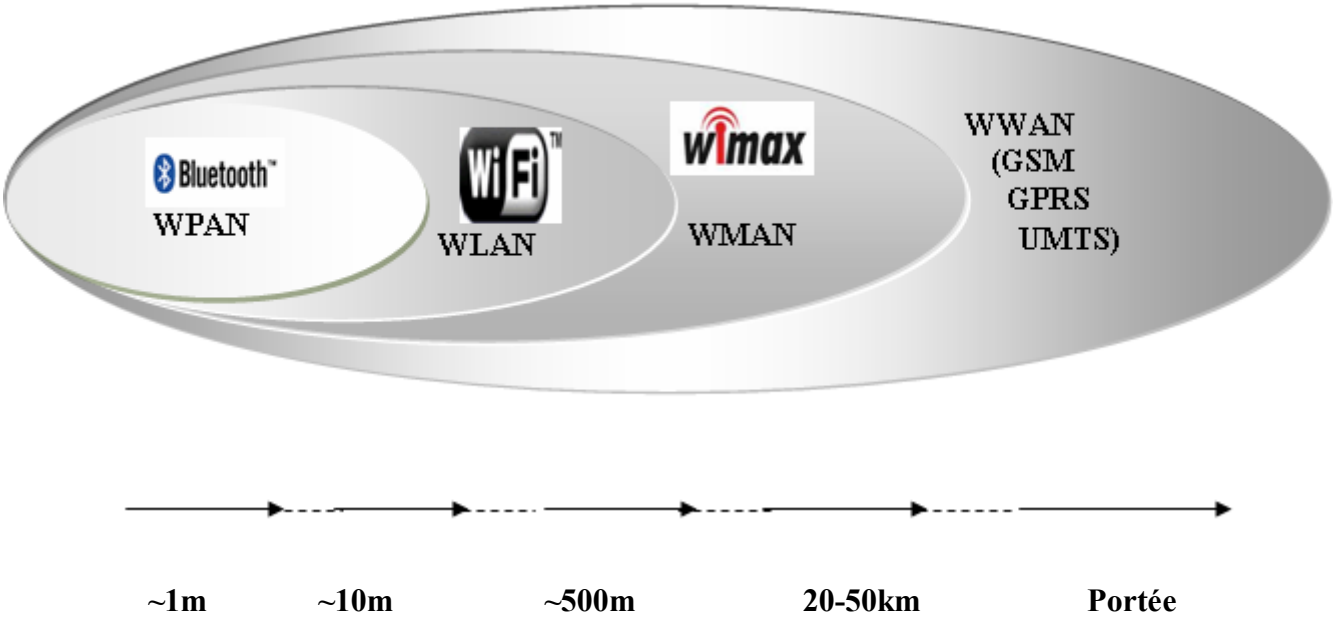


Figure1 : Type des réseaux sans fils.

- **Réseaux personnels sans fils (WPAN)**

Le réseau personnel sans fils (appelé également réseau individuel sans fils ou réseau domotique sans fils et noté WPAN pour *Wireless Personal Area Network*) concerne les réseaux sans fils d'une faible portée : de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison

filaire ou bien à permettre la liaison sans fils entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN : **Bluetooth**, **HomeRF, ZigBee, infrarouges**.

- **Réseaux locaux sans fils (WLAN)**

Le réseau local sans fils (WLAN pour *Wireless Local Area Network*) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes : **WiFi, hiperLAN2, DECT**.

- **Réseaux métropolitains sans fils (WMAN)**

Le réseau métropolitain sans fils (WMAN pour *Wireless Metropolitan Area Network*) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication. **WiMAX** étant certainement le plus prometteur dans ce domaine.

- **Réseaux étendus sans fils (WWAN)**

Le réseau étendu sans fils (WWAN pour *Wireless Wide Area Network*) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fils les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fils. Les principales technologies sont les suivantes : **GSM, GPRS, UMTS.**

[5]

1.1.3 La Technologie Wi-Fi

Les spécifications WLAN les plus importantes ont été développées par le groupe 802.11 de l'IEEE (Institute of Electrical and Electronics Engineers). C'est en 1997 que ce groupe a donné naissance au standard IEEE 802.11 qui est utilisé pour définir les réseaux locaux hertziens. [6]

L'élaboration du premier standard Wi-Fi (IEEE 802.11) en 1997 et son développement rapide ont accéléré l'engouement dans le déploiement de tels réseaux. Il a d'abord été conçu pour fournir des accès à « haut débit » pour des utilisateurs nomades dans les entreprises, puis dans des lieux de passage à large public (« hotspots ») tels que des gares, des aéroports, des centres d'affaires, des hôtels,… Il a ainsi permis de mettre à portée de tout un vrai système de communication sans fil pour la mise en place des réseaux informatiques « hertziens ». Le projet CitySpace de Irisnet propose même depuis la fin 2003 un accès complet et gratuit à Internet aux citoyens bruxellois circulant sur la petite ceinture.

Le Wi-Fi, pour Wireless Fidelity, est une technologie standard d'accès sans fil à des réseaux locaux (WLAN). Le principe consiste à établir des liaisons radio rapides entre des terminaux et des bornes reliées aux réseaux Haut Débit. Grâce à ces bornes Wi-Fi, l'utilisateur se connecte à Internet ou au système d'informations de son entreprise et accède à de nombreuses

applications reposant sur le transfert de données. Cette technologie a donc une réelle complémentarité avec les réseaux ADSL (Asymetric Digital Subscriber Line), les réseaux d'entreprise ou encore les réseaux mobiles comme GPRS/UMTS (Global Packet Radio Service / Universal Mobile Telecommunications System).

Ce standard a été développé pour favoriser l'interopérabilité du matériel entre les différents fabricants ainsi que pour permettre des évolutions futures compatibles. Ainsi, les consommateurs peuvent mélanger des équipements de différents fabricants afin de satisfaire leurs besoins.

[7]

1.1.3.1 L'architecture Wi-Fi

Comme tous les standards IEEE 802, la norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- La couche physique (notée parfois PHY), proposant trois types de codage de l'information, et
- La couche liaison de données, constituée de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC) (voire la Figure2). [7]

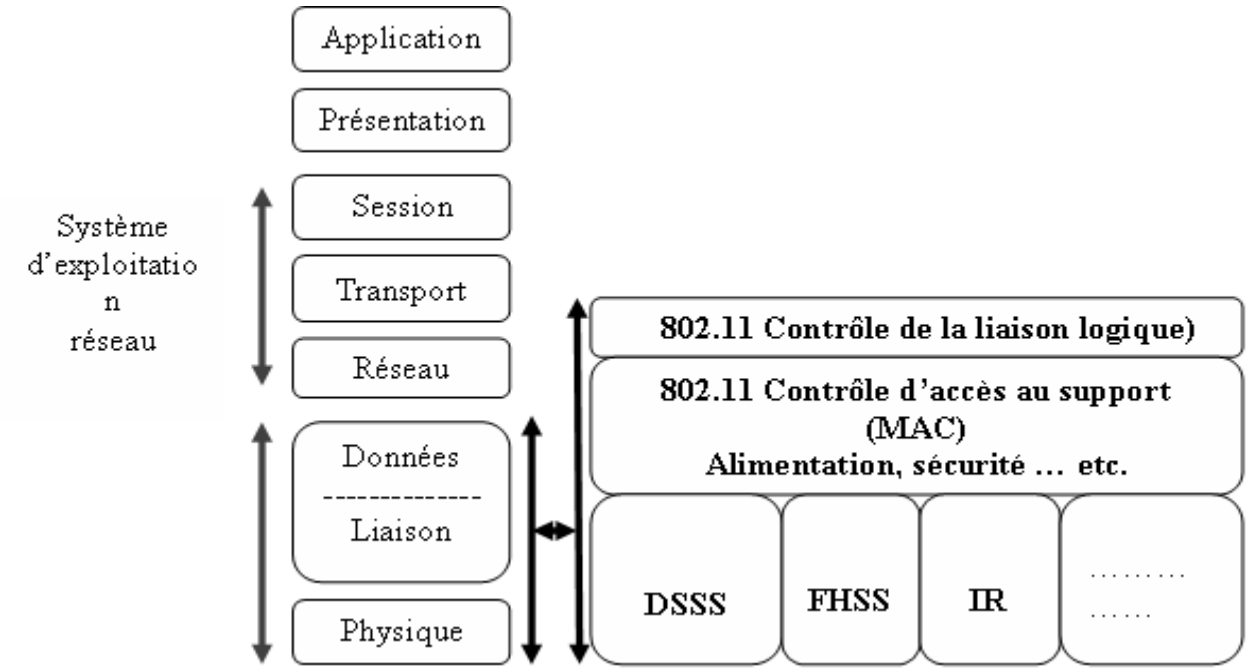


Figure2 : couche 1 et 2 de 802.11 du modèle OSI.

a) La couche physique

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données.

Les trois couches physiques définies à l'origine par 802.11 incluaient deux techniques radio à étalement de spectre et une spécification d'infrarouge diffus. Les techniques d'étalement de spectre, en plus de satisfaire aux conditions réglementaires, améliorent la fiabilité, accélèrent le débit et permettent à de nombreux produits non concernés de se partager le spectre avec un minimum d'interférences.

Trois couches physiques étaient définies dans la norme initiale 802.11 :

- **DSSS** (Direct Sequence Spread Spectrum) : étalement de spectre à séquence directe, Technique opérant dans la bande des 2,4GHz à des débits de 1 et 2 Mbits/sec, elle divise la bande des 2,4 GHz en 13 ou 14 canaux de 22 MHz. Ces canaux fournissent un signal très bruité, car les canaux adjacents ont des bandes passantes qui se recouvrent partiellement et peuvent donc se perturber mutuellement.

- **FHSS** (Frequency-Hopping Spread Spectrum) : étalement de spectre par saut de fréquence, Le nombre de canaux disponibles est plus grand que dans le DSSS. En effet, la bande passante est divisée en un minimum de 75 canaux d'une largeur de 1MHz, la transmission se faisant en utilisant une combinaison de canaux connue de toutes les stations de la cellule.

- **Infrarouge (IR)** : mêmes débits que pour les autres couches mais utilisant des longueurs d'onde différentes.

Une nouvelle couche physique a été ajoutée par la suite, c'est la couche OFDM. Le principe de l'OFDM consiste à diviser le signal que l'on veut transmettre sur différentes ondes porteuses, comme si l'on combinait ce signal sur un grand nombre d'émetteurs indépendants, fonctionnant à des fréquences différentes. Pour que les fréquences des porteuses soient les plus proches possibles et ainsi maximiser la quantité d'information transmise sur une plage de fréquences donnée, l'OFDM utilise des porteuses orthogonales entre elles. Les signaux des différentes porteuses se chevauchent mais, grâce à l'orthogonalité, n'interfèrent pas entre eux.

[5], [6], [7]

b) La couche liaison de données

La couche liaison de données définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations.

La couche liaison de données de la norme 802.11 est composée de deux sous-couches:

- La couche de contrôle de la liaison logique LLC,

- La couche de contrôle d'accès au support MAC.

Le standard 802.11 utilise la LLC 802.2 et l'adressage sur 48 bits, tout comme les autres LAN 802, simplifiant ainsi le pontage entre les réseaux sans fil et câblés. Le 802.11 MAC est très proche de 802.3 dans sa conception : En effet, il est conçu pour supporter de multiples utilisateurs sur un support partagé en faisant détecter le support par l'expéditeur avant d'y accéder.

b.1 L'accès au médium

Dans 802.11 deux fonctions de base existent pour l'accès au medium. Le DCF (Distributed Coordination Function) qui s'appuie sur le protocole CSMA/CA (Carrier Sense Multiple Acces with Collision Avoidance), et le PCF (Point Coordination Function).

Le DCF est responsable des services asynchrones, alors que PCF a été développé pour les services à contraintes temporelles. Le PCF est utilisé pendant la contention-free period (CFP) période de non contention, alors que DCF utilise la contention period (CP).Une CFP et une CP forme une super trame. Les super trames sont séparées par des trames périodiques de gestion appelées Beacon ou balise.

Le 802.11 utilise trois intervalles de temps différents, nommés interframe spaces (espaces inter trames) pour contrôler l'accès au médium, c.à.d pour donner aux stations dans des cas bien spécifiques une plus ou moins importante priorité:

- Short Interframe Space (SIFS),
- PCF Interframe Space (PIFS),
- DCF Interframe Space (DIFS).

SIFS est le plus court intervalle. Il est utilisé pour les accusés de réception ACK, les trames CTS (Clear to Send) et les différents fragments du paquet d' information MPDU, ainsi que pour la réponse d'une station au AP dans le mode Polling (mode vote) dans PCF. SIFS représente la plus haute priorité et assure qu'une station est capable de finir la séquence de transmission de trame avant qu'une autre station puisse accéder au médium.

PIFS est plus long que SIFS. Après l'expiration de cet intervalle, n'importe quelle trame du mode PCF peut être transmise.

DIFS est plus long que PIFS. Après l'expiration de cet intervalle, n'importe quelle trame du mode DCF peut être transmise, de façon asynchrone selon le mécanisme du backoff de la CSMA/CA. Donc DIFS a la plus faible priorité.

b.1.1 Le protocole CSMA/CA

Cette méthode d'accès consiste en une écoute du canal de transmission avant l'envoi. Si le canal est libre, l'envoi est immédiat. Autrement, le noeud attend un temps aléatoire avant de

transmettre (back-off value). La probabilité que deux nœuds choisissent le même back-off étant faible, le risque de collision l'est aussi. Ceci étant, il n'y a pas de mécanisme de détection des collisions. En effet, les WLAN sont généralement munis d'une seule antenne et les noeuds ne sont donc pas capables d'écouter pendant qu'ils envoient. Un système de confirmation (ACK) est donc mis en place entre le récepteur et l'émetteur pour confirmer la réception d'un paquet.

b.1.2 DCF: Distributed Coordination Function

Dans DCF les stations utilisent le mode de contention pour accéder au canal. Pour cela elles utilisent le "carrier sense multiple access with collision avoidance" (CSMA/CA) pour que plusieurs stations puissent accéder le médium en utilisant la méthode de détection de porteuse à accès multiples et évitement de collision. DCF ne fonctionne que durant la période CP. Chaque station, après que le médium devient libre, attend une durée fixe DIFS suivie d'une durée aléatoire appelée backoff time, avant de commencer à émettre, si le canal est toujours libre.

Effectivement la durée backoff time est donnée par la formule :

Backoff time = Random(0, CW) x SlotTime,

Où Random(0, CW) est une valeur aléatoire entière uniformément distribuée sur [0, CW] avec CW (Contention Window) la fenêtre de contention vérifiant CWmin <= CW <= CWmax=1023 .

Initialement on a CW= CWmin = 15 dans 802.11. SlotTime est une durée fixe (9µs dans 802.11a)

Si le médium devient occupé avant l'expiration de la durée du backoff, la station attend de nouveau la libération du médium puis attend DIFS et le reste du backoff précédent avant d'émettre de nouveau.

Au cas où deux stations émettent en même temps, ce qui entraîne une collision détectée par la non- réception d'un ACK la nouvelle fenêtre de contention CW est augmentée pour réduire la probabilité de collision, et devient :

CWnew = 2*CWold + 1 (15, 31, 63, 127, 255, 511, 1023).

b.1.3 PCF: Point Coordination Function

Le PCF peut être uniquement utilisé dans les réseaux à infrastructure, car il nécessite la présence d'un AP (access point). Le PC (Point Coordinator) normalement installé sur l'AP, contrôle l'accès au médium par la méthode du Polling. Il faut noter que PCF est optionnel, et peut donc être implémenté avec DCF.

Le PC après un temps PIFS pendant lequel le canal est libre envoie la balise " Beacon " qui marque le début de la super trame, divisée en deux parties: la CFP et la CP. Initialement la

durée maximale de la CFP CFPMaxDuration, ainsi que sa fréquence sont données; mais cette dernière n'est pas respectée la plupart du temps car le beacon peut être retardé, à cause d'une longue transmission d'une trame à la fin de la CP. Ce problème ne permet pas d'avoir une séquence rigoureusement périodique de la balise. Comme PCF a été développée au dessus de DCF toutes les stations doivent activer leur NAV (Network Allocation Vector) au début de la CFP à la valeur CFPMaxDuration pour bloquer toute transmission parasite (contention) pendant la durée CFP, car aucune station n'a le droit d'émettre que si on le lui demande pendant la CFP.

Pendant la durée du CFP le PC attend une durée SIFS après le beacon avant d'envoyer une trame de données ou le CF-Poll ou faire du piggybacking (une trame de données qui contient aussi un message de polling). Le PC va séquentiellement faire du polling, pendant la durée CFP, pour toutes les stations déjà enregistrées dans sa liste. La station concernée va répondre au PC ou à une autre station dans le réseau par des trames de données ou un ACK séparés par SIFS. Si une station ne répond pas, le PC passe à la suivante après PIFS. Si le PC ou les stations n'ont plus de trames à transmettre, la CFP se termine par l'envoi de la trame CF-end par le PC. Toutes les stations vont alors remettre a zéro leur NAV, et la CP va débuter, et on repasse alors au mode DCF. Il faut noter qu'aucune station n'a le droit d'émettre que si on le lui demande pendant la CFP.

Si le PCF est utilisé pour les applications à contraintes temporelles, le PC doit établir une liste de polling. Chaque station doit être votée au moins une fois par CFP. Les stations peuvent demander une place dans la liste de polling avec des trames de gestion d'associations. Le PC peut avoir un modèle de priorité pour les différentes stations.

b.1.4 RTS/CTS et le problème de la station caché

Un problème crucial pendant la CP est celui de la station cachée. Celui-ci a lieu lorsqu'une station ne peut pas entendre toutes les communications entre deux stations car l'une des deux est éloignée d'elle, et considère alors que le medium est libre. Une collision va avoir lieu si cette station va essayer d'émettre. Pour résoudre ce problème on a dû ajouter deux paquets de contrôle à la DCF: RTS (Request To Send) demande d'émission, et CTS (Clear to Send) permission d'émission. Lorsqu'une station a accès au médium elle commence à émettre un RTS (après la libération du canal pendant au moins DIFS) reçoit un CTS (Clear to Send) transmet sa trame (ou ses fragments) et reçoit l'ACK (ou les ACK).La durée qui sépare ces messages est SIFS (Short IFS), avec SIFS< DIFS pour ne pas interrompre la transmission par une autre station. Le RTS contient un champ de durée qui donne la durée totale du CTS, des données, et ACK ainsi que les SIFS. Toutes les stations réceptrices vont mettre leur NAV à cette valeur, spécifiant alors la durée d'occupation du canal. Un champ de durée existe aussi dans CTS comprenant la durée totale des données, ACK et SIFS. De cette manière les stations qui reçoivent RTS ou CTS mettent leurs NAV à la valeur correspondante, ce qui résout le problème des stations cachées. Comme la collision ne peut avoir lieu que seulement avec RTS, ce mécanisme fournit une excellente protection contre les collisions pour les grandes trames. Le désavantage majeur est l'overhead de RTS/CTS avec une perte de bande passante et un délai plus important.

b.1.5 Propriétés supplémentaires des couches MAC et LLC

La couche MAC de 802.11 offre deux autres caractéristiques de robustesse à savoir les sommes de contrôle CRC et la fragmentation des paquets.

Une somme de contrôle est calculée pour chaque paquet et rattachée à celui-ci afin d'assurer que les données n'ont pas été corrompues durant leur transfert. Cette technique diffère d'Ethernet où les protocoles de niveau supérieur tels que TCP gèrent le contrôle d'erreur.

La fragmentation des paquets permet de casser les gros paquets en unités de plus petite taille, ce qui s'avère particulièrement utile dans les environnements très congestionnés ou lorsque les interférences posent problème, puisque les gros paquets courent plus de risque d'être corrompus. Cette technique limite le risque de devoir retransmettre un paquet et améliore ainsi globalement les performances du réseau sans fil. La couche MAC est responsable de la reconstitution des fragments reçus, le traitement étant ainsi transparent pour les protocoles de niveau supérieur.

La couche LLC de 802.11 gère aussi la gestion d'énergie. Deux modes de gestion d'alimentation sont prévus :

- Le **CAM** (Continuous Aware Mode) : l'appareil, toujours allumé, consomme de l'énergie en permanence.

- Le **PSPM** (Power Save Polling Mode) : l'appareil est mis en veille. L'AP met alors en file d'attente les données qui lui sont destinées.

[6], [7], [8]

1.2 Les environnements mobiles

Un environnement mobile est un système composé de sites mobiles et qui permet à ses utilisateurs d'accéder à l'information indépendamment de leurs positions géographiques [4].

Les réseaux mobiles ou sans fil, peuvent être classés en deux classes : les réseaux avec infrastructure et les réseaux sans infrastructure.

1 Architecture avec une infrastructure

Dans le mode infrastructure, le modèle de système est composé de deux ensembles d'entités distinctes :

- les "sites fixes" d'un réseau de communication filaire classique (wired network),
- les "sites mobiles" (wireless network).

Chaque unité mobile (notée UM) se connecte à une station de base (point d'accès) via une liaison sans fil. L'ensemble formé par la station de base et les unités mobiles situés dans sa zone de couverture est appelé ensemble de services de base (en anglais *Basic Service Set*, noté BSS) et constitue une cellule (voir Figure3).

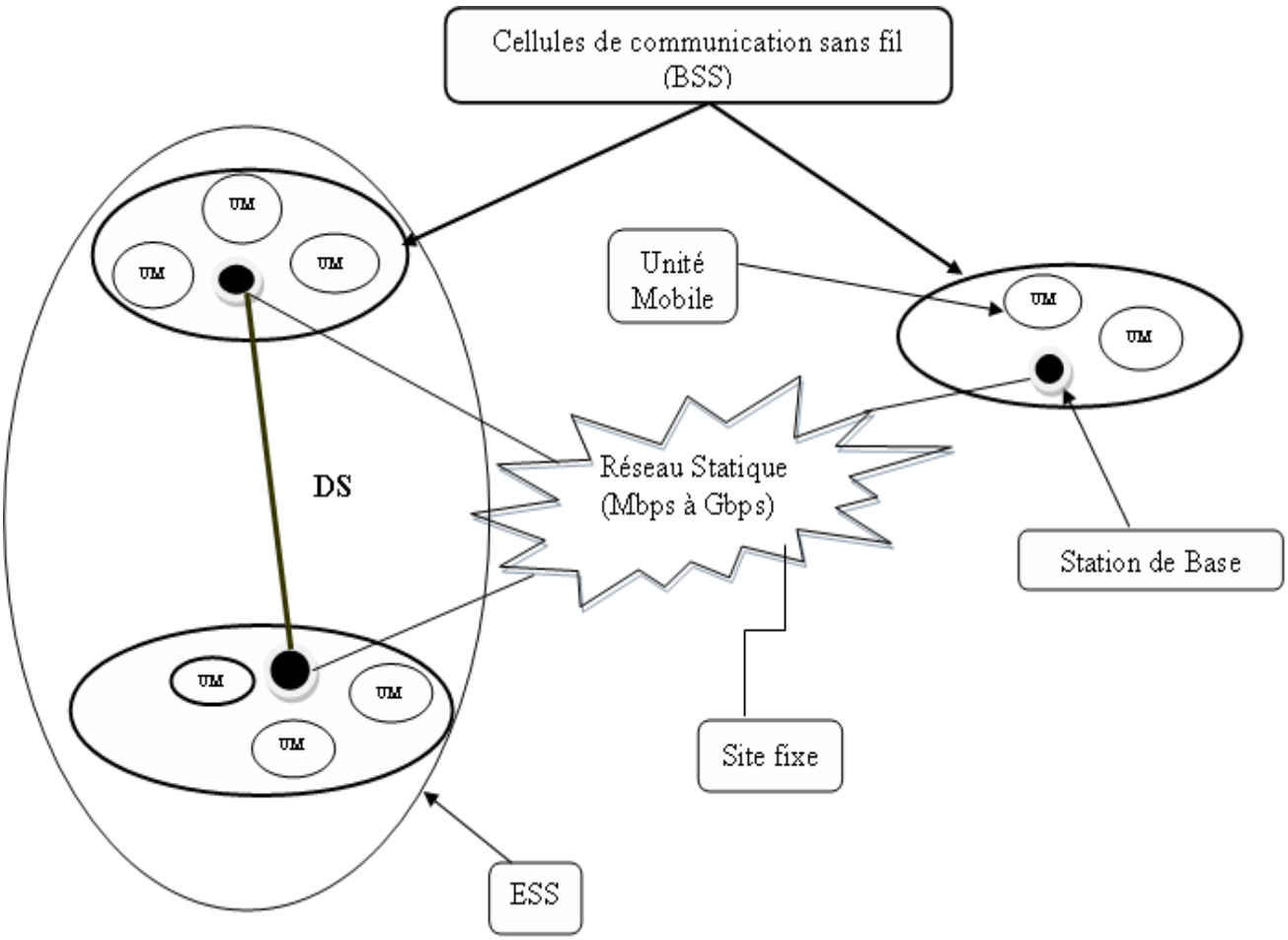


Figure3 : Le modèle des réseaux mobiles avec infrastructure.

Chaque BSS est identifié par un BSSID, un identifiant de 6 octets (48 bits). Dans le mode infrastructure, le BSSID correspond à l'adresse MAC du point d'accès. Il est possible de relier plusieurs points d'accès entre eux (ou plus exactement plusieurs BSS) par une liaison appelée système de distribution (notée DS pour *Distribution System*) afin de constituer un ensemble de services étendu (*Extended Service Set* ou ESS). Le système de distribution (DS) peut être aussi bien un réseau filaire, qu'un câble entre deux points d'accès ou bien même un réseau sans fil, Un ESS est repéré par un ESSID (*Service Set Identifier*), c'est-à-dire un identifiant de

32 caractères de long (au format ASCII) servant de nom pour le réseau. L'ESSID, souvent abrégé en SSID, représente le nom du réseau et représente en quelque sort un premier niveau de sécurité dans la mesure où la connaissance du SSID est nécessaire pour qu'une station se connecte au réseau étendu.

2 Architecture sans infrastructure (le mode Ad Hoc)

Le modèle de réseau sans infrastructure préexistante ne comporte pas l'entité "site fixe", tous les sites du réseau sont mobiles et se communiquent d'une manière directe en utilisant leurs interfaces de communication sans fil (voir figure 4).

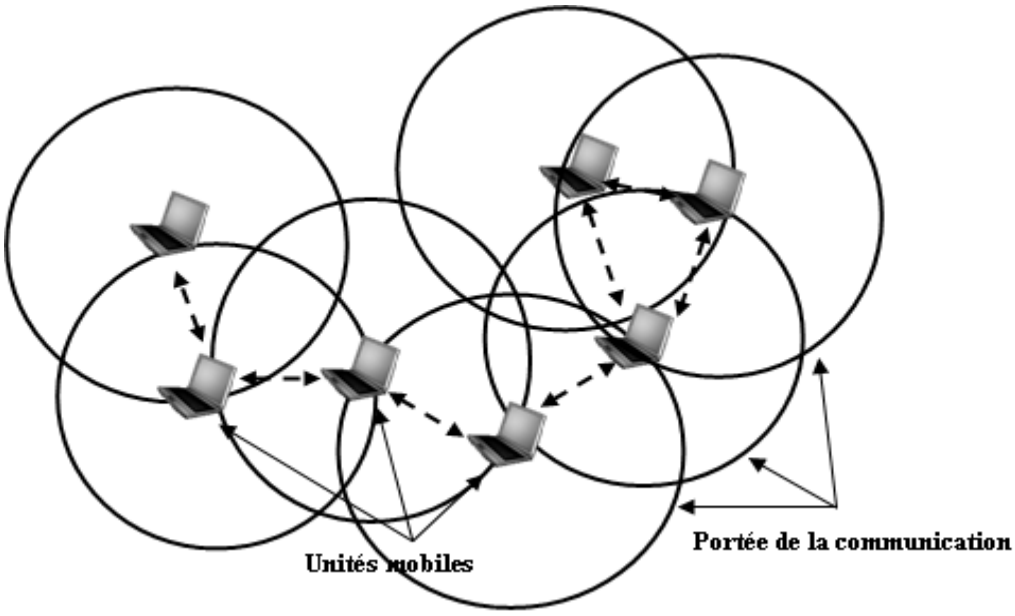


Figure4: Le modèle des réseaux mobiles sans infrastructure.

En mode ad hoc, les machines sans fil clientes se connectent les unes aux autres afin de constituer un réseau point à point (*peer to peer* en anglais), c'est à dire un réseau dans lequel chaque machine joue en même temps de rôle de client et le rôle de point d'accès. L'ensemble formé par les différentes stations est appelé ensemble de services de base indépendants (en anglais *independant basic service* set, abrégé en IBSS). Un IBSS est ainsi un réseau sans fil constitué au minimum de deux stations et n'utilisant pas de point d'accès. L'IBSS constitue donc un réseau éphémère permettant à des personnes situées dans une même salle d'échanger des données. Il est identifié par un SSID, comme l'est un ESS en mode infrastructure. Dans

un réseau ad hoc, la portée du BSS indépendant est déterminée par la portée de chaque station. Cela signifie que si deux des stations du réseaux sont hors de portée l'une de l'autre, elles ne pourront pas communiquer, même si elles "voient" d'autres stations. En effet, contrairement au mode infrastructure, le mode ad hoc ne propose pas de système de distribution capable de transmettre les trames d'une station à une autre.

[5]

2 La communication cellulaire

La configuration standard d'un système de communication cellulaire est un maillage (grid) de cellules hexagonales (figure 5). Initialement, une région peut être couverte uniquement par une seule cellule. Quand la compétition devient importante pour l'allocation des canaux, la cellule est généralement divisée en sept cellules plus petites, dont le rayon est égal à un tiers du rayon de la cellule de départ. Cette subdivision peut être répétée et l'on parle alors de systèmes micro cellulaires. Les cellules adjacentes dans le maillage doivent utiliser des fréquences différentes, contrairement à celles qui sont situées sur les côtés opposés du maillage et qui peuvent utiliser la même fréquence sans risque d'interférence.

[4]

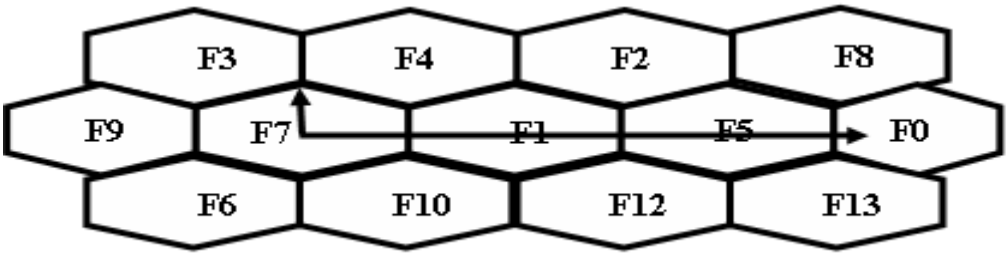


Figure 5: Le principe de réutilisation de fréquence.

Lorsqu'un utilisateur nomade passe d'une cellule à une autre lors de son déplacement, l'adaptateur réseau sans fil de sa machine est capable de changer de point d'accès selon la qualité de réception des signaux provenant des différents points d'accès. Les points d'accès communiquent entre eux grâce au système de distribution afin d'échanger des informations sur les stations et permettre le cas échéant de transmettre les données des stations mobiles. Cette caractéristique permettant aux stations de "passer de façon transparente" d'un point d'accès à un autre est appelé itinérance (en anglais ***roaming***).

1.4 L'utilisation des ondes radio dans la communication sans fil

La transmission radio utilisée dans la communication sans fil des unités mobiles, est basée sur le principe que l'accélération d'un électron crée un champ électromagnétique qui à son tour accélère d'autres électrons et ainsi de suite. Il est alors possible de provoquer le déplacement électromagnétique. Plus le nombre d'électrons déplacés est important, plus le signal est fort et plus sera grande sa portée, avec une vitesse proche de celle de la lumière.

Un déplacement coordonné d'électrons peut alors servir pour le transfert d'information et constitue la base de la communication sans fil. L'approche standard de la transmission radio est le déplacement des électrons à une fréquence donnée. Des techniques de modulation et de multiplexage permettent d'adapter les signaux transmis à la bande passante du support de communication et de rentabiliser son utilisation.

[4]

1.5 Problématiques techniques des réseaux sans fil

Comme nous l'avons vu, la technologie des réseaux sans fil apporte des gains considérables en terme d'infrastructures, puisque l'on n'a plus besoin de fils pour relier les différents sites. De plus, le simple fait que chaque machine ne soit plus reliée aux autres par un fil permet la mobilité dans l'espace de celle-ci. En effet, cette mobilité et ce gain en infrastructure ne sont malheureusement pas sans conséquence : on se heurte à des problèmes physiques liés à l'utilisation même du media radio. La propagation électromagnétique (obstacles multi trajets) et le fait que le signal soit accessible à tous, sont deux phénomènes fortement gênants pour la sécurité des données transmises.

Les principaux obstacles rencontrés sur le terrain peuvent être résumés ainsi :

1.5.1 La sécurité

La sécurité est le premier souci de ceux qui déploient les réseaux locaux sans fil. Le comité de 802.11 a apporté une solution en élaborant un processus appelé WEP (Wired Equivalent Privacy). Le principal, pour les utilisateurs, est d'être sûr qu'un intrus ne pourra pas :

- Accéder aux ressources du réseau en utilisant le même équipement sans fil,
- Capturer le trafic du réseau sans fil (écoute clandestine).

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

L'écoute clandestine est bloquée par l'utilisation de l'algorithme WEP qui est un générateur de nombres pseudo aléatoires initialisé par une clef secrète partagée. Le générateur de nombres pseudo aléatoires ressort une séquence de clefs de bits pseudo aléatoires, égales en longueur au paquet le plus large possible, qui, combiné avec des paquets entrants ou sortants produit le paquet transmis par la voie des airs.

L'algorithme WEP est un simple algorithme basé sur l'algorithme RC4 de RSA, qui a les propriétés suivantes :

- Raisonnablement fort : l'attaque par force brute de cet algorithme est difficile du fait que chaque trame est envoyée avec un vecteur d'initialisation qui relance le générateur de nombres pseudo aléatoires.

- Auto synchronisé : l'algorithme se resynchronise pour chaque message. Ceci est nécessaire pour travailler en mode non connecté, où les paquets peuvent être perdus, comme dans tout réseau local.

Cependant, des informaticiens américains ont découvert une brèche dans la sécurité des systèmes de communication sans fil, notamment ceux utilisés par Apple et sa solution AirPort. Selon le groupe d'informaticiens qui a révélé l'affaire, des pirates pourraient exploiter cette faille pour épier ou modifier les données transmises par cette voie.

Au cœur du problème : le mode de codage utilisé dans ce type de transmission par ondes radio (norme dite 802.11). "Nous avons découvert un certain nombre de failles dans l'algorithme Wep, qui entachent sérieusement les prétentions de sécurité de ce système", expliquent dans leur communiqué les chercheurs de l'université de Berkeley (Californie) dirigés par le professeur David Wagner, qui s'est déjà distingué par ses travaux sur le chiffrement des téléphones portables.

Le Wep est notamment utilisé par Apple et son système Airport : il assure une communication sans fil entre plusieurs portables iBooks et le réseau téléphonique pour se connecter au net à distance. Tout récemment Toshiba en a proposé une version pour PC. Il est normalement censé offrir un haut niveau de sécurité, puisqu'il sert notamment à créer des réseaux d'entreprise, où la confidentialité est incontournable.

Selon les chercheurs californiens, c'est toute la crédibilité du système qui est remise en cause. Pour atteindre un réseau situé à plus d'1 km, il suffit d'une antenne et de matériel électronique un peu sophistiqué. Leurs expérimentations auraient montré la possibilité d'intercepter les transmissions, et de se livrer à de l'espionnage domestique ou industriel. Une antenne et du matériel électronique un peu sophistiqué, placés à plus d'un kilomètre du réseau visé, peuvent suffire. Pire, les données peuvent également être altérées et renvoyées après modification sans que le système ne s'en aperçoive. Et cela peut fonctionner avec des messages texte. Enfin, selon les chercheurs, des pirates pourraient facilement réaliser un système de capture des mots de passe exploitant la vulnérabilité du Wep.

Les clefs WEP à 40 bits sont cassables en environ 15 minutes de l'avis général. D'où le développement de technologies alternatives, le plus souvent propriétaires, comme celle de Funk Software pour 802.11b, ou d'Enterasys avec sa génération de clefs rapide ("Rapid Re-Keying") basée sur 802.1x, actuellement en cours d'homologation aux Etats-Unis. Avec cette technologie, il est possible de générer de nouvelles clefs de cryptage, 40 ou 128 bits, toutes les 60 secondes, ce qui réduit considérablement les possibilités de craquer les codes.

D'autres solutions de cryptage sont en cours d'élaboration, comme le WPA (WiFi Protective Acces), présenté fin octobre 2002 par la WFA (Wireless Fidelity Alliance), mais c'est une technologie qui est encore en phase de test. De plus, comme les appareils utilisant les WEP et ceux utilisant le WPA ne sont pas compatibles entre eux, il se pose le problème de faire évoluer les réseaux existants vers cette nouvelle norme.

Un autre aspect du problème est que le WPA est une solution d'attente avant la finalisation dans environ un an d'une véritable norme de sécurité, le 802.11i, appelé "Robust Security Network", actuellement en cours d'élaboration par l'IEEE.

[10]

1.5.2 Les interférences

Les réseaux sans fil utilisent des gammes de fréquences très communes et déjà utilisées par de nombreux appareils (fours à micro-ondes, téléphones sans fil DECT …). Les interférences entre les équipements du réseau et ces appareils ne peuvent donc pas être ignorées. De plus, ces gammes de fréquences ont le plus souvent été réservées dans le passé à des applications militaires sensibles. [11]

1.5.3 Les sources de perturbation pour une communication sans fil

1. Affaiblissement

La puissance d'un signal décroît avec la distance. Pour un média sans guide physique, l'atténuation est fonction de la distance et des conditions atmosphériques. Cet affaiblissement est plus important aux hautes fréquences ce qui entraîne des distorsions plus importantes.

2. Le bruit

Pendant le trajet, le signal est altéré par des signaux perturbateurs, provenant par exemple d'autres antennes. Ce sont ces signaux qui sont appelés bruit. Ce bruit peut être réparti en plusieurs catégories :

- **Le bruit thermique** : provoqué par l'agitation des électrons, il est présent dans tous les équipements électroniques.
- **Le bruit d'inter modulation** : résultant du partage d'un média par des signaux de fréquences différentes.
- **La diaphonie** : il s'agit d'un couplage perturbateur de trajets de signaux voisins. L'exemple classique, que tout un chacun a déjà expérimenté lors d'une communication téléphonique, est de percevoir une autre conversation.
- **Le bruit impulsif** : bruit changeant, apparaissant sous forme de pics irréguliers et dont les causes sont diverses. Il peut provenir de défauts internes à l'antenne ou de perturbations extérieures comme la foudre.

3. Absorption atmosphérique

La vapeur d'eau et l'oxygène sont deux éléments intervenant fortement dans l'affaiblissement d'un signal, en absorbant une partie de celui-ci.

4. Propagation multi trajet

Rappelons les trois effets de propagation qui entrent en ligne de compte lors d'une transmission :

- **La réflexion** : survient lorsqu'une onde rencontre une surface qui est plus grande que sa longueur d'onde.

- **La diffraction** : se produit quand l'onde frappe le coin d'un obstacle plus grand que sa longueur d'onde. Des ondes se propagent alors dans différentes directions à partir de ce coin.

- **La dispersion** : a lieu quand la taille de l'objet est de l'ordre de la longueur d'onde du signal. Celui-ci est alors dispersé en plusieurs signaux plus faibles.

Dans la plupart des cas, on trouve une multitude d'obstacles entre l'émetteur et le récepteur. Le signal peut donc être réfléchi un grand nombre de fois et plusieurs copies du signal original peuvent exister. Le récepteur capte alors un signal qui est la résultante du signal principal et de tous les signaux réfléchis qui sont captés par son antenne. Le signal peut être renforcé ou atténué (voir même annulé) par ces différentes composantes et les effets de la propagation multi trajet ont donc une importance considérable sur les transmissions sans fils.

En plus des perturbations dont nous venons de discuter, il y a un autre problème qui surgit dans un environnement mobile, c'est le phénomène d'évanouissement (fading). Ce terme désigne la variation dans le temps de la puissance du signal reçu, due à des changements dans le support ou dans le chemin de transmission emprunté.

[6]

1.6 Conclusion

Communiquer sans contrainte au cours d'un déplacement ou d'un voyage d'affaires et accéder au système de prises de commande, de gestion de stock, surfer sur l' internet à partir d'un ordinateur portable, d'un mobile ou d'un PDA (Personal Digital Assistant) dans un aéroport avec des vitesses de transfert proches ou supérieures aux raccordements fixes de type ADSL ; tout ceci est désormais devenu réalité. [12]

Cette révolution annoncée pour l'accès à l'information en réponse aux nouveaux besoins de mobilité est aujourd'hui possible grâce aux nouvelles technologies dites "wireless" ou sans fil. Ces technologies de réseaux sans-fil ont depuis leurs débuts fortement évolué, et continuent encore aujourd'hui de changer constamment : fréquences, types de bornes et de cartes de connexion, protocoles de sécurisation et d'authentification, etc.

Ce chapitre a été consacré à l'utilisation de la technologie de communication sans fil et le concept des environnements mobiles. Nous avons donné les notions de base nécessaires à la

compréhension de la communication utilisée dans le nouvel environnement, à savoir : l'utilisation des ondes radio, les techniques de transmission de données (étalement de spectre), les techniques d'accès au médium, etc. Le but de ce chapitre a été de donner un aperçu général sur cette technologie qui ne cesse pas de croître. Dans le chapitre suivant on va entamer le concept de réseaux mobiles Ad hoc.

Chapire02 :
Les Réseaux Mobiles Ad hoc

2.1 Les réseaux sans fil Ad hoc

Les réseaux sans fil les plus couramment déployés aujourd'hui s'appuient sur des infrastructures fixes : sites accueillant des stations de base dans le cas des réseaux cellulaires ou câbles pour les infrastructures filaires. La connectivité entre les différents éléments du réseau y est organisée et centralisée.

Les réseaux ad hoc sont des réseaux sans fil formés par des personnes ou des appareils, appelés nœuds, qui communiquent entre eux sans passer par une autre infrastructure et sans que ces communications nécessitent une administration centrale. Les appareils en question peuvent être aussi variés que des ordinateurs, des PDA, des téléphones mobiles, etc. Chaque nœud du réseau est équipé d'une interface radio, qui peut être différente d'un nœud à l'autre : Bluetooth™, Wifi, UWB, … et reste libre d'intégrer ou de quitter le réseau. A condition qu'il y ait suffisamment de nœuds dans une zone, le réseau s'adapte spontanément, pour répondre à un besoin, d'où la terminologie ad hoc (en latin : *pour cela*) et se configure de façon complètement autonome et dynamique en fonction des possibilités de connexions existantes. Même si l'exemple peut paraître simpliste, échanger des données entre plusieurs PC connectés par une liaison infrarouge consiste à créer un réseau ad hoc fixe. Lorsque les nœuds des réseaux ad hoc sont mobiles, on parle de MANET (Mobile Ad hoc NETwork). [13]

Ce chapitre se concentre sur ces MANET. Après avoir décrit les réseaux ad hoc et leurs principales caractéristiques, ainsi que leurs domaines d'application, nous présenterons le problème de routage dans les réseaux Ad Hoc, ainsi que les principes des protocoles de routages Ad hoc les plus connus.

2.1.1 Le concept

Le concept des réseaux mobiles ad hoc tente d'étendre les notions de la mobilité à toutes les composantes de l'environnement. Ici, contrairement aux réseaux basés sur la communication cellulaire, aucune administration centralisée n'est disponible, ce sont les nœuds mobiles eux mêmes qui forment, d'une manière ad hoc, une infrastructure du réseau. Aucune supposition ou limitation n'est faite sur la taille du réseau ad hoc, le réseau peut contenir des centaines ou des milliers d'unités mobiles. [14]

2.1.2 Modélisation

Un réseau mobile Ad Hoc, appelé généralement MANET (*Mobile Ad hoc NETwork*), consiste en une grande population, relativement dense, d'unités mobiles qui se déplacent dans un territoire quelconque. Le seul moyen de communication est l'utilisation « des ondes radio » qui se propagent entre les différents nœuds mobiles, sans l'aide d'une infrastructure préexistante ou administration centralisée. Un réseau ad hoc peut être modéliser par un graphe Gt = (Vt, Et) où Vt représente l'ensemble des nœuds (i.e. les unités ou les hôtes mobiles) du réseau et Et modélise l'ensemble des connections qui existent entre ces nœuds (figure6). Si e = (u, v) appartient à Et, cela veut dire que les nœuds u et v sont en mesure de communiquer directement à l'instant t.

La figure 6 représente un réseau Ad hoc de 7 unités mobiles sous forme d'un graphe:

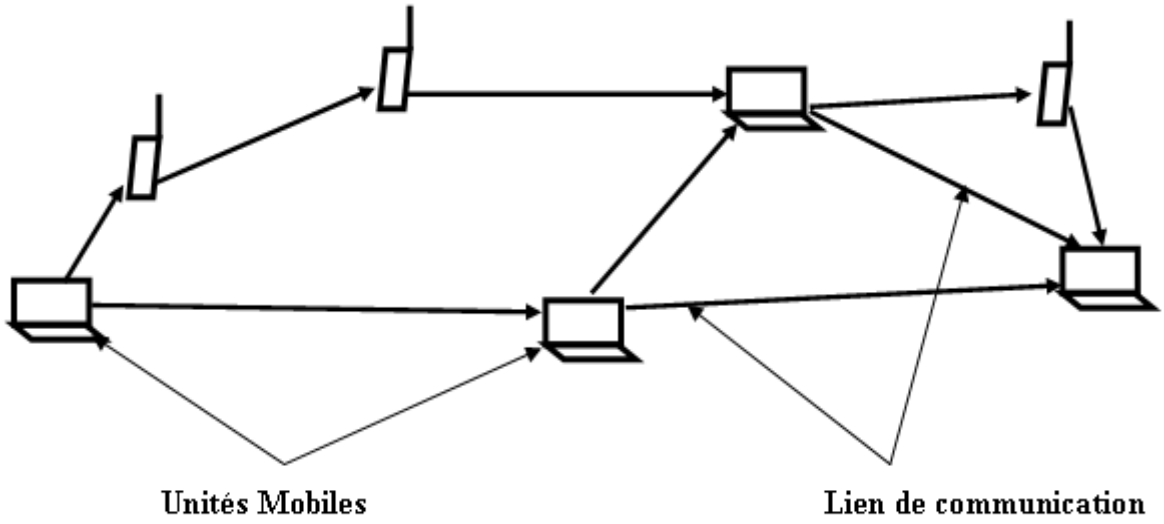


Figure 6: La modélisation d'un réseau ad hoc.

La topologie du réseau peut changer à tout moment (voir la figure 7). Elle est donc dynamique et imprévisible ce qui fait que la déconnexion des unités soit très fréquente.

[14]

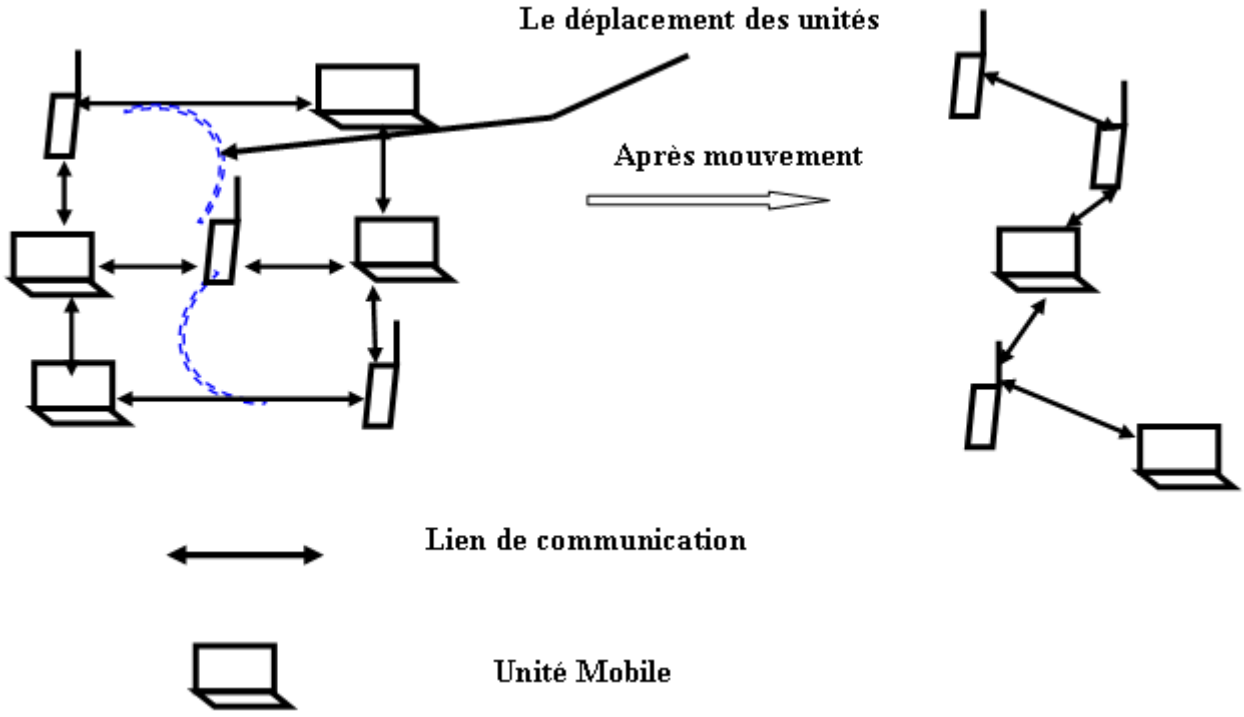


Figure 7 : le changement de la topologie des réseaux ad hoc.

2.1.3 Applications

La particularité du réseau Ad hoc est qu'il n'a besoin d'aucune installation fixe, ceci lui permettant d'être rapide et facile à déployer. Les applications tactiques comme les opérations de secours, militaires ou d'explorations trouvent en Ad Hoc, le réseau idéal. La technologie Ad Hoc intéresse également la recherche, des applications civiles sont apparues. On distingue :

- **Les services d'urgence :** opération de recherche et de secours des personnes, tremblement de terre, feux, inondation, dans le but de remplacer l'infrastructure filaire.

- **Le travail collaboratif et les communications dans des entreprises ou bâtiments :** dans le cadre d'une réunion ou d'une conférence par exemple.

- **Home network :** partage d'applications et communications des équipements mobiles.

- **Applications commerciales :** pour un paiement électronique distant (taxi) ou pour l'accès mobile à l'Internet, où service de guide en fonction de la position de l'utilisateur.

- **Réseaux de senseurs :** pour des applications environnementales (climat, activité de la terre, suivi des mouvements des animaux, . . . etc.) ou domestiques (contrôle des équipements à distance).

- **Réseaux en mouvement :** informatique embarquée et véhicules communicants.

- **Réseaux Mesh :** c'est une technologie émergente qui permet d'étendre la portée d'un réseau ou de le densifier.

[15]

2.1.4 Caractéristiques

Les réseaux mobiles ad hoc sont caractérisés par ce qui suit :

Une topologie dynamique:
Les unités mobiles du réseau, se déplacent d'une façon libre et arbitraire. Par conséquent la topologie du réseau peut changer, à des instants imprévisibles, d'une manière rapide et aléatoire. Les liens de la topologie peuvent être unis ou bidirectionnels.

Une bande passante limitée:
Un des caractéristiques primordiales des réseaux basés sur la communication sans fil est l'utilisation d'un médium de communication partagé. Ce partage fait que la bande passante réservée à un hôte soit modeste.

Des contraintes d'énergie :
Les hôtes mobiles sont alimentés par des sources d'énergie autonomes comme les batteries ou les autres sources consommables. Le paramètre d'énergie doit être pris en considération dans tout contrôle fait par le système.

Une sécurité physique limitée :
Les réseaux mobiles ad hoc sont plus touchés par le paramètre de sécurité, que les réseaux filaires classiques. Cela se justifie par les contraintes et limitations physiques qui font que le contrôle des données transférées doit être minimisé.

L'absence d'infrastructure :
Les réseaux ad hoc se distinguent des autres réseaux mobiles par la propriété d'absence d'infrastructures préexistante et de tout genre d'administration centralisée. Les hôtes mobiles sont responsables d'établir et de maintenir la connectivité du réseau d'une manière continue.

[6]

2.1.5 Avantages des réseaux Ad hoc

Parmi les avantages de ces réseaux, citons :

- La rapidité de mise en place,
- Un coût faible,
- L'indépendance, technique et commerciale, vis à vis de points d'accès,
- La robustesse du par une conception évolutive et dynamique et adaptée intrinsèquement à la mobilité. [13]

2 Le problème de routage dans les réseaux ad hoc

1 Définition

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

Par exemple si on suppose que les coûts des liens sont identiques, le chemin indiqué dans la figure suivante est le chemin optimal reliant la station source et la station destination. Une bonne stratégie de routage utilise ce chemin dans le transfert des données entres les deux stations.

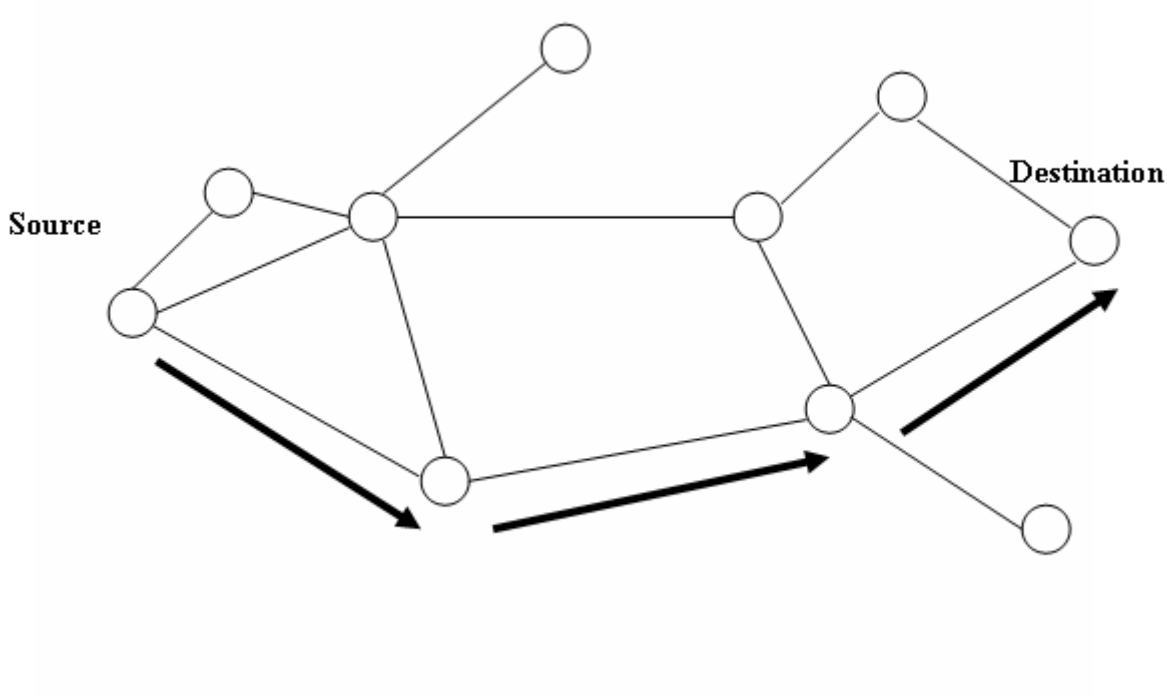


Figure8 : Schéma de routage entre une source et une destination.
[14]

2.2.2 La difficulté du routage dans les réseaux ad hoc

Dans le but d'assurer la connectivité du réseau, malgré l'absence d'infrastructure fixe et la mobilité des stations, chaque nœud est susceptible d'être mis à contribution pour participer au routage et pour retransmettre les paquets d'un nœud qui n'est pas en mesure d'atteindre sa destination ; tout nœud joue ainsi le rôle de station et de routeur.

Le fait que la taille d'un réseau ad hoc peut être énorme, souligne que la gestion de routage de l'environnement doit être complètement différente des approches utilisées dans le routage classique. Le problème qui se pose dans le contexte des réseaux ad hoc est l'adaptation de la méthode d'acheminement utilisée avec le grand nombre d'unités existant dans un environnement caractérisé par de modestes capacités de calcul et de sauvegarde.

Dans la pratique, il est impossible qu'un hôte puisse garder les informations de routage concernant tous les autres nœuds, dans le cas où le réseau serait volumineux. Le problème ne se pose pas dans le cas de réseaux de petites tailles, car l'inondation (la diffusion pure) faite dans ces réseaux n'est pas coûteuse ; par contre dans un réseau volumineux, le manque de données de routage concernant les destinations peut impliquer une diffusion énorme dans le réseau, et cela si on considère seulement la phase de découverte de routes. Le trafic causé par la diffusion, dans ce cas, est rajouté au trafic déjà existant dans le réseau ce qui peut dégrader considérablement les performances de transmission du système caractérisé principalement par une faible bande passante. Dans le cas où le nœud destination se trouve dans la portée de communication du nœud source le routage devient évident et aucun protocole de routage n'est initié. Malheureusement, ce cas est généralement rare dans les réseaux ad hoc. Une station source peut avoir besoin de transférer des données à une autre

station (nœud intermédiaire) qui ne se trouve pas dans sa portée de communication ce qui nécessite un protocole de routage approprié.

Dans la pratique, le problème de routage est plus compliqué à cause de la non uniformité de la transmission sans fil et de la possibilité du déplacement imprévisible de tous les nœuds concernés par le routage.

[15]

2.2.3 La conception des stratégies de routage

L'étude et la mise en œuvre d'algorithmes de routage pour assurer la connexion des réseaux ad hoc au sens classique du terme (tout sommet peut atteindre tout autre), est un problème complexe. L'environnement est dynamique et évolue donc au cours du temps, la topologie du réseau peut changer fréquemment. Il semble donc important que toute conception de protocole de routage doive étudier les problèmes suivants :

1- La minimisation de la charge du réseau : l'optimisation des ressources du réseau renferme deux autres sous problèmes qui sont l'évitement des boucles de routage, et l'empêchement de la concentration du trafic autour de certains nœuds ou liens.

2- Offrir un support pour pouvoir effectuer des communications multi-points fiables : le fait que les chemins utilisés pour router les paquets de données puissent évoluer, ne doit pas avoir d'incident sur le bon acheminement des données. L'élimination d'un lien, pour cause de panne ou pour cause de mobilité devrait, idéalement, augmenter le moins possible les temps de latence.

3- Assurer un routage optimal : la stratégie de routage doit créer des chemins optimaux et pouvoir prendre en compte différentes métriques de coûts (bande passante, nombre de liens, ressources du réseau, délais de bout en bout,…etc.). Si la construction des chemins optimaux est un problème dur, la maintenance de tels chemins peut devenir encore plus complexe, la stratégie de routage doit assurer une maintenance efficace de routes avec le moindre coût possible.

4- Le temps de latence : la qualité des temps de latence et de chemins doit augmenter dans le cas où la connectivité du réseau augmente.

[4]

2.2.4 L'évaluation des protocoles de routage

Les protocoles de routage doivent être évalués afin de mesurer les performances de la stratégie utilisée et de tester sa fiabilité. L'utilisation d'un réseau ad hoc réel dans une évaluation est difficile et coûteuse, en outre de telles évaluations ne donnent pas généralement des résultats significatifs. Le réseau réel n'offre pas la souplesse de varier les différents paramètres de l'environnement et pose en plus le problème d'extraction de résultats; c'est pour cela la majorité des travaux d'évaluation de performances utilisent le principe de simulation vu les avantages qu'il offre. En effet, la simulation permet de tester les

protocoles sous une variété de conditions. Le simulateur, qui constitue une plate-forme construite avec un certain langage (Maisie/PARSEC par exemple), permet de varier les différents facteurs de l'environnement tel que le nombre d'unités mobiles, l'ensemble des unités en mouvement, les vitesses des mouvements, le territoire du réseau et la distribution des unités dans ce territoire. Initialement, chaque unité est placée aléatoirement dans l'espace de simulation. Une unité reste dans sa position courante pendant une certaine durée (pause time), par la suite elle choisit une nouvelle vitesse et une nouvelle localisation vers laquelle elle se déplace. Chaque unité répète ce même comportement jusqu'à la fin de la simulation.

Les paramètres mesurés dans une évaluation dépendent de la stratégie de routage appliquée (par exemple dans le cas où on veut comparer deux versions d'un même protocole), mais généralement tout simulateur doit être en mesure d'évaluer :

- le contrôle utilisé dans le mécanisme de mise à jour de routage,
- les délais moyens du transfert des paquets et
- le nombre moyen de nœuds traversés par les paquets de données.

[14]

2.2.5 Gestion et transfert de l'information

2.2.5.1 La notion de "Multihoping"

Les stratégies de routage utilisées dans les réseaux Ad hoc sont caractérisées par le fait de pouvoir acheminer les paquets de données sans l'aide des stations de base utilisées dans la communication cellulaire (*Base Station, Mobile Station*).

Dans le modèle cellulaire, la communication entre deux nœuds est faite en utilisant les stations de base (*Base Station*), par conséquent aucune unité mobile n'est utilisée comme routeur intermédiaire, le modèle cellulaire est dit alors "S*ingle Hop*" (i.e. le nombre de routeurs mobiles intermédiaires est nul). La contrepartie de ce modèle est le modèle de communication sans infrastructure. Dans ce modèle plusieurs nœuds peuvent participer au routage c'est pour cela que l'environnement des réseaux Ad hoc est dit "*Multihop*" (i.e. le nombre de stations mobiles qui peuvent être utilisées comme routeurs intermédiaires peut dépasser un).

2.2.5.2 L'inondation

L'inondation ou la diffusion pure (*Broadcast*), consiste à faire propager un paquet (de données ou de contrôle) dans le réseau entier. Un nœud qui initie l'inondation envoie le paquet à tous ses voisins directs. De même, si un nœud quelconque du réseau reçoit le paquet, il le rediffuse à tous ses voisins.

Ce comportement se répète jusqu'à ce que le paquet atteigne tous les nœuds du réseau (Figure 9). Notons que les nœuds peuvent être amenés à appliquer, durant l'inondation, certains traitements de contrôle, dans le but d'éviter certains problèmes, tels que le bouclage et la duplication des messages.

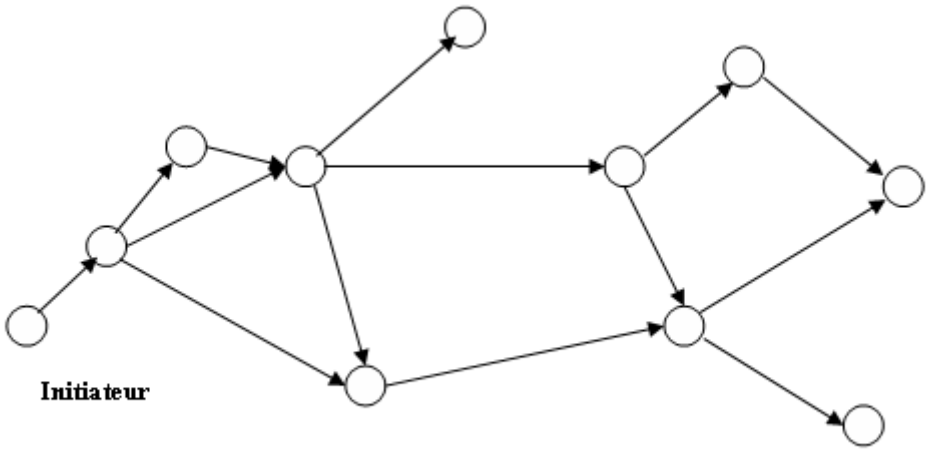


Figure 9 : Le mécanisme d'inondation (Broadcast).

Le mécanisme d'inondation est utilisé généralement dans la première phase du routage, plus exactement dans la procédure de découverte des routes, et cela dans le cas où le nœud source ne connaît pas la localisation exacte de la destination. Un paquet de requête de route est inondé par la source afin qu'il atteigne la station destination. Il faut noter que l'inondation est très coûteuse surtout dans le cas ou le réseau est volumineux (latence, surcharge des messages…etc.), c'est pour cela que les protocoles de routage essaient de minimiser au maximum la propagation des paquets inondés en rajoutant d'autres paramètres de diffusion.

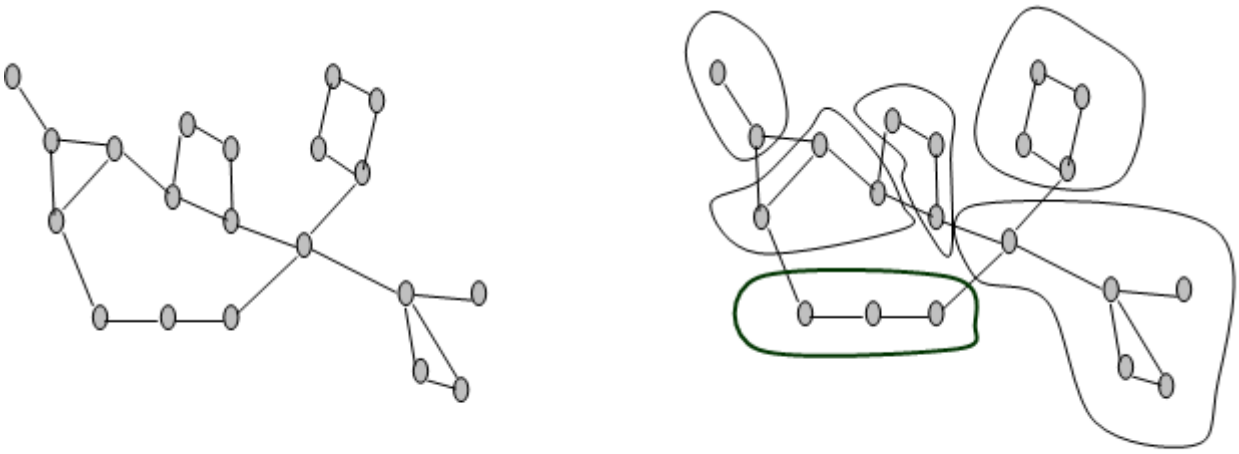
[14]

2.2.5.3 Le concept de groupe

Dans la communication de groupes, les messages sont transmis à des entités abstraites ou groupes, les émetteurs n'ont pas besoin de connaître les membres du groupe destinataire. La communication de groupe a fait déjà l'objet de nombreux travaux, principalement dans le cadre des projets ISIS, TRANSIS et HORUS. La gestion des membres d'un groupe dynamique permet à un élément de se joindre à un groupe, de quitter ce groupe, se déplacer ailleurs puis rejoindre le même groupe. C'est en ce sens que la communication de groupe assure une indépendance de la localisation; ce qui la rend parfaitement adaptée à des topologies de réseaux reconfigurables, telles que les architectures avec sites mobiles. [4]

Le concept de groupe de communication dans un environnement mobile a été utilisé dans [16] pour améliorer les performances du protocole de diffusion sélective, et dans [17] pour adapter les canaux de communication de l'environnement ISIS à des sites mobiles. Dans le contexte de routage dans les réseaux ad hoc, certains protocoles utilisent des stratégies d'acheminement basées sur les groupes. Le concept de groupe facilite les tâches de la gestion du routage (telles que les transmissions des paquets, l'allocation de la bande passante, la réutilisation spatiale,…etc.) et cela en décomposant le réseau en un ensemble de groupes connectés mais indépendants du point de vu contrôle.

Lin et Gerla proposent un algorithme de décomposition en groupes pour les réseaux mobiles sans fil. L'algorithme partitionne le réseau en un ensemble de groupes de telle sorte que tout nœud du réseau peut atteindre n'importe quel autre nœud en utilisant, au plus, un seul nœud intermédiaire (figure 10).



(a) La topologie du système. (b) Le partitionnement en groupes

Figure 10 : La décomposition du réseau en groupes.

[4]

La section suivante s'attache à présenter une description des protocoles de routage pour les réseaux mobiles Ad hoc.

2.3 Les protocoles de routage ad hoc

Comme nous avons déjà vu, les réseaux ad hoc se caractérisent par une absence d'infrastructure et de gestion centralisée. Dans ce type de réseaux, chaque élément peut bien évidemment émettre et recevoir des messages, mais assure également un rôle de relais de l'information afin que les messages circulent dans le réseau de proche en proche. Chaque noeud du réseau doit donc posséder des capacités de routage, c'est le routage dit ad hoc. Grâce à ce routage, la portée radio d'un noeud peut être virtuellement étendue en utilisant ses voisins comme relais de l'information.

La problématique du routage de l'information dans ce type de réseau est complexe. En effet, les réseaux ad hoc sont souvent peu stables :

- les noeuds peuvent être mobiles ;
- les noeuds peuvent entrer et sortir du réseau à tout moment, soit parce qu'ils s'éteignent, soit parce qu'ils sortent de la portée radio de noeuds du réseau ;

- les ressources des noeuds sont souvent limitées (capacité de calcul, énergie...) car ce sont des équipements embarqués légers et mobiles ;
- le médium radio est peu fiable en termes de perte d'information et de sécurité ;
- les liens radio peuvent être asymétriques, l'information passe dans un sens mais pas dans l'autre (à cause des irrégularités des ondes électromagnétiques).

Il existe différentes méthodes pour résoudre cette problématique qui correspondent à autant de protocoles de routage différents. Classiquement, trois grandes familles de protocoles peuvent être distinguées : les proactifs, les réactifs et les hybrides. Les protocoles proactifs ou "Table Driven" se comportent comme les protocoles de routage des réseaux filaires : les routes pour atteindre les noeuds du réseau sont maintenues en permanence et stockées dans des tables de routage au niveau des noeuds. Les protocoles réactifs ou "On Demand", quant à eux, ne calculent pas de routage avant qu'il n'y ait une demande par un noeud pour une transmission. Les routes sont donc uniquement cherchées à la demande. Les protocoles hybrides mélangent les techniques des deux précédents.

Avec l'apparition de systèmes de positionnement bas coût, une quatrième catégorie peut être ajoutée aux trois précédentes : elle est basée sur la position des noeuds du réseau, ce sont les protocoles géographiques.

[18]

Dans les paragraphes suivants, une présentation non exhaustive des protocoles représentatifs de ces différentes familles est réalisée au travers de leurs principales caractéristiques.

2.3.1 Les protocoles proactifs

Les protocoles de routage proactifs tentent de maintenir à jour dans chaque noeud les informations de routage concernant tous les autres noeuds du réseau. Il nécessite ainsi que chaque noeud maintienne une ou plusieurs tables pour stocker les informations de routage qui grandissent avec la taille du réseau. Ils répondent aux changement de topologies du réseau en propageant à chaque voisin les mises à jours des routes afin que chacun puisse maintenir une vue consistante du réseau.

Cette politique de routage est proche de celle des réseaux filaires actuel basé sur des méthodes de vecteur de distance ou d'état de lien où chaque noeud maintient une vision globale de la topologie. Cette famille convient donc bien aux applications interactives mettant en scène chaque noeud du réseau.

Les différences entre les protocoles membres de cette famille se situent au niveau du nombre de table nécessaire pour stocker l'information et la manière dont ils propagent les changements de topologie.

Malheureusement ces protocoles atteignent rapidement leurs limites avec l'accroissement du nombre de noeuds et de leur mobilité. Les changements de topologies sont fréquents. Le réseau sera ainsi constamment inondé par les paquets de contrôle qui ne se propagent pas assez vite pour que chaque noeud soit informé à temps des changements. Il en résulte des incohérences dans les tables, un problème de convergence du réseau et une bande passante réduite par la surcharge des paquets de mise à jour.

Cette famille de protocole est ainsi limitée à des réseaux de petites taille, avec une faible mobilité et où chaque noeud à besoin d'être en permanence connecté avec les autres membres du réseau.

[19]

2.3.1.1 Le protocole DSDV (Destination Sequenced Distance Vector)

L'algorithme de routage de Perkins appelé "Vecteur de Distance à Destination Dynamique Séquencée" ou DSDV (Dynamic Destination Sequenced Distance Vector) a été conçu spécialement pour les réseaux mobiles. Il est basé sur l'idée classique de l'algorithme distribué de Bellman-Ford (DBF : Distributed Bellman-Ford) en rajoutant quelques améliorations. Chaque station mobile maintient une table de routage qui contient :

- Toutes les destinations possibles.
- Le nombre de nœud (ou de sauts) nécessaire pour atteindre la destination.
- Le numéro de séquences (SN : sequence number) qui correspond à un nœud destination.

Pour chaque nœud *i*, le numéro de séquence (NS) de la destination *j*, est associé à chaque entrée de distance $D^{i}_{jk,}$ pour chaque voisin *k*. Le NS est utilisé pour faire la distinction entre les anciennes et les nouvelles routes, ce qui évite la formation des boucles de routage.

Afin de maintenir la consistance des tables de routage dans une topologie qui varie rapidement, chaque nœud du réseau transmet périodiquement sa table de routage à ses voisins directs. Le nœud peut aussi transmettre sa table de routage si le contenu de cette dernière subit des changements significatifs par rapport au dernier contenu envoyé. La mise à jour dépend donc de deux paramètres : Le temps, c'est à dire la période de transmission, et Les événements *(ou* les déclencheurs*)*, exemple : apparition d'un nœud, détection d'un nouveau voisin…etc. La mise à jour doit permettre à une unité mobile de pouvoir localiser, dans la plupart des cas, une autre unité du réseau.

La mise à jour de la table de routage peut se faire de deux façons :

- Une mise à jour complète.
- Une mise à jour incrémentale.

Dans la mise à jour complète, la station transmet la totalité de la table de routage aux voisins ce qui nécessite l'envoi de plusieurs paquets de données ; alors que dans une mise à jour incrémentale, juste les entrées qui ont subit un changement par rapport à la dernière mise à jour, sont envoyées ce qui réduit le nombre de paquets transmis. La façon de faire la mise à jour des tables de routage est liée à la stabilité du réseau. Dans le cas où le réseau serait relativement stable, la mise à jour incrémentale est utilisée pour réduire le trafic de la communication, la mise à jour complète n'est pas fréquente dans ce genre de situation. Dans le cas opposé, où le réseau subit des changements rapides, le nombre de paquets incrémentaux envoyés augmente, ce qui fait que la mise à jour complète est fréquente.

Un paquet de mise à jour contient :

1- Le nouveau numéro de séquence incrémenté, du nœud émetteur.

Et pour chaque nouvelle route :

2- L'adresse de la destination.

3- Le nombre de nœuds (ou de sauts) séparant le nœud de la destination.
4- Le numéro de séquence (des données reçues de la destination) 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 (i.e. la route la plus récente), est la route utilisée. Si deux routes ont le même numéro de séquence, alors la route qui possède la meilleure métrique, est celle qui sera utilisée. La métrique utilisée dans le calcul des plus courts chemins est, tout simplement, le nombre de nœuds existant dans le chemin. Les valeurs des métriques des routes, choisies après réception des données de routage, sont incrémentées. 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 de routage. 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, i.e. une valeur plus grande que la valeur maximale permise par la métrique.

Le DSDV élimine les deux problèmes de boucle de routage "routing loop", et celui du "counting to infinity". Cependant, dans ce protocole, 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. On trouve ce même problème dans l'algorithme DUAL - utilisé dans des protocoles Internet tel que EIGRP- et dans les algorithmes similaires basés sur la synchronisation explicite. En outre, le DSDV utilise une mise à jour périodique et basée sur les événements, ce qui cause un contrôle excessif dans la communication.

[4]

2.3.2 Les protocoles de routage réactifs

Les protocoles de routage proactifs essaient de maintenir les meilleurs chemins existants vers toutes les destinations possibles (qui peuvent représenter l'ensemble de tous les nœuds du réseau) au niveau de chaque nœuds du réseau. Les routes sont sauvegardées mêmes si elles ne sont pas utilisées. La sauvegarde permanente des chemins de routage, est assurée par un échange continu des messages de mise à jour des chemins, ce qui induit un contrôle excessif surtout dans le cas des réseaux de grande taille.

Les protocoles de routages réactifs (à la demande) créent et maintiennent les routes selon les besoins. Lorsqu'un noeud à besoin d'une route, une procédure de découverte globale est lancée. Cette procédure s'achève par la découverte de la route ou lorsque toutes les permutations de routes possibles ont été examinées. La route trouvée est maintenue par une

procédure de maintenance de routes jusqu'à ce que la destination soit inaccessible à partir du nœud source ou que le nœud source n'aura plus besoin de cette route.

La majorité des approches utilisées lors de la découverte des routes sont basées sur le mécanisme d'apprentissage en arrière (*backward learning).* Le noeud source, qui est à la recherche d'un chemin vers la destination, diffuse par inondation une requête dans le réseau. Lors de la réception de la requête, les noeuds intermédiaires essaient de faire apprendre le chemin au noeud source, et de sauvegarder la route dans la table envoyée. Une fois la destination atteinte, elle peut envoyer une réponse en utilisant le chemin inverse, un chemin full duplex est alors établit entre le noeud source et le noeud destination. Le travail peut être réduit, dans le cas où un noeud de transit posséderait déjà un chemin vers la destination. Une fois que le chemin est calculé, il doit être sauvegardé et mis à jour au niveau de la source, tant qu'il est en cours d'utilisation. Une autre technique pour tracer les chemins demandés, est la technique appelée "routage source". Dans cette dernière tous les paquets de données diffusent leur information de cheminement en tant que leur en-tête, donc la décision de cheminement est prise dès au départ ce qui permet d'éviter des boucles ; cependant pour des topologies fortement mobiles c'est inefficace, puisque le protocole devient imprécis en raison de l'invalidation d'itinéraire pendant la transmission de paquet.

La recherche des chemins dans le routage à la demande entraîne une lenteur qui peut dégrader les performances des applications interactives. Des exemples de protocoles de routage réactifs sont : AODV et DSR (Dynamic Source Routing Protocol).

[20]

2.3.2.1 Le protocole DSR (Dynamic Source Routing Protocol)

DSR est un protocole de routage qui est basé sur le concept de routage par la source. Chaque noeud maintient en cache l'adresse source des routes découvertes. Chaque entrée dans la cache est continuellement mise à jour lorsque de nouveaux chemins sont découverts. Le protocole consiste essentiellement en deux phases :

1. la découverte d'une route, et

2. la maintenance d'une route.

Lorsqu'un noeud désire envoyer un paquet à un destinataire, il consulte préalablement sa cache pour déterminer s'il connaît déjà une route vers la destination. Si c'est le cas, et que le timer de la route n'a pas expiré, alors il utilisera cette route pour envoyer le paquet. Dans le cas inverse, ce noeud initiera le processus de découverte de route par diffusion d'un message RREQ (Route REQuest). Ce message contient l'adresse du destinataire, l'adresse de la source et un identifiant de diffusion. Chaque noeud recevant le paquet vérifie s'il possède une route pour ce même destinataire. Si ce n'est pas le cas, il rajoutera sa propre adresse à la liste des noeuds traversés, qui est contenue dans le paquet, et transmettra à son tour le paquet. Un noeud ne retransmettra le paquet que si son adresse n'est pas déjà contenue dans la liste où s'il ne possède pas en cache un couple <adresse source, id diffusion>. Ces deux cas reflètent respectivement la formation d'une boucle dans la route construite et un duplicata du paquet reçu.

Un paquet RREP (Route REPly) est généré lorsque le RREQ atteint la destination ou un noeud possédant une route vers cette destination. Dans les deux cas, la liste des noeuds à traverser pour atteindre la destination est incorporée dans le RREP qui est renvoyé à la source du RREQ. Le chemin suivit par ce paquet est le chemin inverse de celui contenu dans le RREQ. La maintenance de la route est accomplie par l'utilisation de paquets RERR (Route Error) renvoyé vers la source lorsqu'un noeud de la route n'est plus accessible. Ce noeud sera alors supprimer des listes des chemins le traversant et la source pourra alors relancer un processus de découverte afin de découvrir un chemin alternatif.

Le protocole DSR ne nécessite donc pas d'information de routage mise à jour pour les noeuds intermédiaires, le chemin à suivre étant contenu dans le paquet. Le routage par la source le prémuni de formation de boucle et permet un contrôle de la diffusion. En contre partie, la taille des paquets envoyés sur le réseau grandit avec le nombre de noeuds à traverser. DSR convient donc mieux pour des réseaux de petite taille. Aucune métrique de routage n'est définie dans ce protocole, le chemin formé le plus rapidement sera le chemin préféré pour la transmission des paquets. Il s'agira donc du chemin le plus rapide et le moins congestionné à cet instant.

[19]

2.3.2.2 Le protocole AODV

Le protocole AODV (Ad hoc On-Demand Distance Vector Routing Protocol), est un protocole de routage réactif conçu par Charles E. Perkins et Elizabeth M. Royer. Il peut être considéré comme une combinaison des deux protocoles DSDV et DSR, car il détient de DSR ses mécanismes de découverte et de maintenance de routes "Route Discovery" et "Route Maintenance" ; et de DSDV, son routage par sauts "hop by hop", ses numéros de séquences ainsi que la diffusion des mises a jour des tables de routage. Il est basé sur le principe de routage à vecteur distance.

Au vu de ses caractéristiques, ce protocole est devenu très connu et a fait l'objet d'un grand nombre de recherches. Il est tout à fait adapté aux réseaux mobiles ad hoc de part sa prise en charge de la mobilité des nœuds dans le réseau. Ce protocole permet à des nœuds mobiles d'obtenir des routes rapidement pour les nouvelles destinations sans maintenir des routes pour lesquelles il n'existe pas de communication active, ainsi l'établissement d'une route se fait uniquement en cas de besoin, Si un nœud source veut envoyer des paquets de données vers un nœud destination, il doit établir et maintenir une route vers ce nœud destination durant le temps qu'il en fait usage.

[21]

- **Table de routage et paquets de contrôle**

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 nouvelles ou autrement dit les plus fraîches (fresh routes).

L'AODV utilise une requête de route dans le but de créer un chemin vers une certaine destination. 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 :

- L'adresse de la destination,
- Le nœud suivant,
- La distance en nombre de nœud (i.e. le nombre de nœud nécessaire pour atteindre la destination).

- Le numéro de séquence destination qui garantit qu'aucune boucle ne peut se former.
- Liste des voisins actifs (origine ou relais d'au moins un paquet pour la destination pendant un temps donné).
- Le temps d'expiration de l'entrée de la table (temps au bout duquel l'entrée est invalidée).
- Un tampon de requête afin qu'une seule réponse soit envoyée par requête.

A chaque utilisation d'une entrée, son temps d'expiration est remis à jour (temps courant + active route time).

Si une nouvelle route est nécessaire, ou qu'une route disparaît, la mise à jour de ces tables s'effectue par l'échange de trois types de messages entre les nœuds :

- **RREQ** Route Request, un message de demande de route,
- **RREP** Route Reply, un message de réponse à un RREQ et
- **RERR** Route Error, un message qui signale la perte d'une route.

- ## Fonctionnalité

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. Cela peut arriver si la destination n'est pas connue au préalable, ou si le chemin existant vers la destination a expiré sa durée de vie ou il est devenu défaillant (i.e. la métrique qui lui est associée est infinie). Le champ numéro de séquence destination du paquet RREQ, contient la dernière valeur connue du numéro de séquence, 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. 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 de manière unicast (cela veut dire qu'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 (temps d'expiration, numéro de séquence et prochain saut).

Afin de limiter le coût dans le réseau, AODV propose d'étendre la recherche progressivement. Initialement, la requête est diffusée à un nombre de sauts limité. Si la source ne reçoit aucune réponse après un délai d'attente déterminé, elle retransmet un autre message de recherche en augmentant le nombre maximum de sauts. En cas de non réponse, cette procédure est répétée un nombre maximum de fois avant de déclarer que cette destination est injoignable.

A chaque nouvelle diffusion, le champ Broadcast ID du paquet RREQ est incrémenté pour identifier une requête de route particulière associée à une adresse source. Si la requête RREQ est rediffusée un certain nombre de fois (RREQ_RETRIES) sans la réception de réponse, un message d'erreur est délivré à l'application.
La destination renvoie un message RREP, ce message peut donc être acheminé vers la source. Chaque nœud traversé incrémentera le nombre de sauts. Et ajoutera une entrée à sa table pour la destination.

Une réponse adéquate peut aussi être donnée par un nœud situé entre la source et la destination. Dans ce cas l'obtention de routes bidirectionnelles est néanmoins possible grâce au drapeau "Gratuitous RREP". Le nœud intermédiaire enverra alors en plus un RREP vers la destination. Les nœuds entre le nœud intermédiaire et la destination ajouteront donc à leur table une entrée vers la source du RREQ. Cette disposition permettra à la destination d'envoyer directement des paquets à la source sans devoir procéder à la recherche d'une route. C'est utile lors de l'établissement de communications TCP pour l'envoi du premier ACK.

- **Maintenance des routes**

Afin de maintenir des routes consistantes, une transmission périodique du message « HELLO » (qui est un RREP avec un TTL de 1) est effectuée. Si trois messages « HELLO » ne sont pas reçus consécutivement à partir d'un nœud voisin, le lien en question est considéré défaillant. Les défaillances des liens sont, généralement, dues à la mobilité du réseau ad hoc. Les mouvements des nœuds qui ne participent pas dans le chemin actif, n'affectent pas la consistance des données de routage. Quand un lien, reliant un nœud *p* avec le nœud qui le suit dans le chemin de routage, devient défaillant, le nœud *p* diffuse un paquet UNSOLICITED RREP, avec une valeur de numéro de séquence égale à l'ancienne valeur du paquet RREP incrémentée d'une, et une valeur infinie de la distance. Le paquet UNSOLICITED RREP est diffusé aux voisins actifs, jusqu'à ce qu'il arrive à la source. Une fois le paquet est reçu, la source peut initier le processus de la découverte de routes.

L'AODV maintient les adresses des voisins à travers lesquels les paquets destinés à un certain nœud arrivent. Un voisin est considéré actif, pour une destination donnée, s'il délivre au moins un paquet de données sans dépasser une certaine période (appelée active timeout period*)*. Une entrée de la table du routage est active, si elle est utilisée par un voisin actif. Le chemin reliant la source et la destination en passant par les entrées actives des tables de routage, est dit un chemin actif. Dans le cas de défaillances de liens, toutes les entrées des tables de routage participantes dans le chemin actif et qui sont concernées par la défaillance

sont supprimées. Cela est accompli par la diffusion d'un message d'erreur entre les nœuds actifs.

Le protocole de routage AODV, n'assure pas l'utilisation du meilleur chemin existant entre la source et la destination. Cependant, des évaluations de performances récentes ont montré qu'il n'y a pas de grandes différences (en terme d'optimisation) entre les chemins utilisés par le protocole AODV et celles utilisées par les protocoles basés sur les algorithmes de recherche des plus courts chemins. En plus de cela, le protocole AODV ne présente pas de boucle de routage, et évite le problème « comptage à l'infini » de Bellman-Ford, ce qui offre une convergence rapide quand la topologie du réseau ad hoc change. En effet :

Dans AODV, chaque nœud maintient une table qui contient une entrée pour chaque destination accessible. Pour éviter le problème du comptage à l'infini de BellmanFord. On a recours à l'utilisation de numéros de séquences dans les tables de routage en plus de la distance.

Chaque nœud possède un numéro de séquence. Il est le seul habilité à l'incrémenter. Ce numéro personnel ne peut être incrémenté que dans deux situations :

- Avant d'entreprendre un processus de recherche de route par l'envoi d'un paquet RREQ, le nœud incrémente son numéro.

- Avant de répondre à un message RREQ par un message RREP, le numéro de séquence doit être remplacé par la valeur maximale entre son numéro de séquence actuel et celui contenu dans le message RREQ.

Ce numéro accompagne son adresse dans les messages de contrôle et permet aux autres de distinguer les messages importants des messages redondants. Une mise à jour de la table de routage ne s'effectue que si les conditions suivantes sont observées :

- Le numéro de séquence du paquet de contrôle est strictement supérieur au numéro de séquence présent dans la table.

- Les numéros de séquence (de la table et du paquet) sont égaux mais, la distance en nombre de sauts du paquet plus 1 est inférieure à la distance actuelle dans la table de routage.

- Le numéro de séquence pour cette destination est inconnu.

Cette façon de procéder garantit la création de route sans boucles.

- ## Gestion de la connectivité locale

Lorsqu'un nœud reçoit un paquet en Broadcast, il met à jour ses informations de connectivité locale pour s'assurer qu'elles incluent ce voisin. Si aucun paquet n'est émis aux voisins actifs pendant le dernier hello_interval, un nœud va envoyer un hello (RREP non sollicité) contenant :

- son identité,
- son numéro de séquence (non modifié pour les hello),

- time to live de 1 pour ne pas être retransmis,
- liste des nœuds pour lesquels il a reçu un hello.

[15]

2.3.3 Les protocoles de routage hybrides

En plus des protocoles de routage proactifs et réactifs, il existe une famille de protocole de routage qui est une combinaison des deux précédents et est dite 'hybrides' par exemple ZRP (the Zone Routing Protocol) et CBRP (Cluster Based Routing Protocol).

Ils utilisent un protocole proactif, pour apprendre le proche voisinage par exemple voisinage à deux sauts ou trois sauts. Ainsi ils disposent des routes immédiatement dans le voisinage. Au delà de cette zone prédéfinie, le protocole hybride fait appel aux techniques des protocoles réactifs pour chercher des routes. Avec ce découpage, le réseau est partagé en plusieurs zones, et la recherche de route en mode réactif peut être améliorée. A la réception d'une requête de recherche réactive, un nœuds peut indiquer immédiatement si la destination est dans le voisinage ou non, et par conséquent savoir s'il faut aiguiller la dite requête vers les autres zones sans déranger le reste de sa zone. Ce type de protocole s'adapte bien aux grands réseaux, cependant, il cumule aussi les inconvénients des protocoles réactifs : messages de contrôle périodiques, plus le coût d'ouverture d'une nouvelle route.

[20]

2.3.3.1 Le protocole ZRP

Le protocole ZRP (Zone Routing Protocol) utilise en fait deux protocoles de routage, un proactif et un réactif. Une taille de zone en nombre de sauts est définie, par exemple, comme sur la Figure 11. Les noeuds présents dans la zone A à 2 sauts sont gérés suivant un protocole proactif : le protocole IARP (IntrAzone Routing Protocol). Les paquets de contrôle possèdent une durée de vie en nombre de sauts ; lorsqu'un noeud reçoit un paquet de contrôle, il actualise sa table de routage et il retransmet le paquet en décrémentant la durée de vie du paquet. Lorsque la durée de vie du paquet de contrôle est nulle, la bordure de zone est atteinte et le paquet n'est plus retransmis. Les noeuds hors de la zone A sont atteints grâce à un protocole réactif : le protocole IERP (IntErzone Routing Protocol). Un troisième protocole gère les transitions entre les deux précédents : le protocole BRP (Border Resolution Protocol).

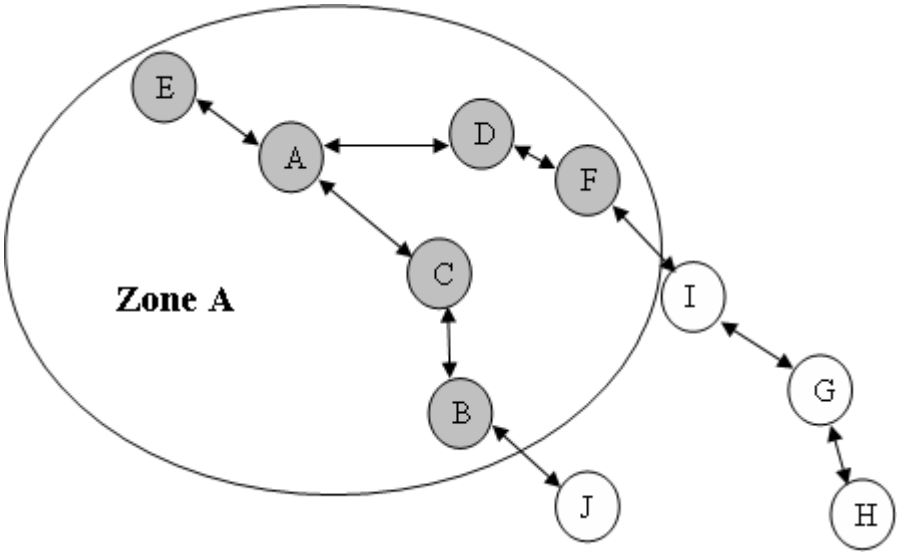


Figure 11 : Le principe des zones dans le protocole ZRP.

Le fait de considérer différentes zones dans le réseau est très intéressant, car un nœud peut ainsi adapter son comportement en fonction de la distance qui le sépare de ses voisins. Un noeud a plus d'interactions avec ses voisins proches qu'avec ceux plus éloignés. En revanche, dans le cas de ZRP, la mise en oeuvre au niveau du noeud est plus complexe que pour les autres protocoles : un noeud exécute en fait trois protocoles de routage et cela peut être préjudiciable à ses ressources CPU et mémoire.
[18]

4 Conclusion

L'étude effectuée sur les réseaux mobiles ad hoc nous a permis de connaître leurs différentes caractéristiques (absence d'infrastructure, topologie dynamique, bandes passantes limitées, sécurité physique limitée, contraintes d'énergie, …etc.), et ainsi constater que leur apparition a, certes, facilité la mise en œuvre d'applications mobiles et ne supportant pas d'infrastructure préexistante (opération de recherche et de secours des personnes,…), mais en revanche, a laissé émerger un bon nombre de problèmes dont celui du routage.

Dans l'étude des protocoles de routage, on a commencé par présenter les trois classes de protocoles de routage : Proactifs, Réactifs et hybrides, on a donné les politiques et les méthodes d'acheminement sur lesquelles ils reposent, ainsi que quelques exemples de protocoles pour chacune des trois classes, à savoir : DSDV, DSR, AODV, ZRP. D'autres protocoles existent évidemment, mais, dans le cas de notre travail, on se contente de ceux-là, car le plus important pour nous est le routage avec qualité de service et non pas le routage au mieux (best effort).

Chapire03 :
La qualité de Service dans les Réseaux Mobiles Ad hoc

Le terme Qualité de Service ou QoS déferle sur les réseaux. C'est aujourd'hui le sujet le plus confus dans ce domaine, comportant de multiples définitions pour répondre à de multiples objectifs. Il est donc difficile d'en donner une définition rigoureuse et satisfaisante. Dans [22], Ferguson pose un certain nombre de questions sur l'expression Qualité de Service. Elle est composée de deux mots qui sont eux mêmes mal définis et très ambigus, Le terme qualité est utilisé pour décrire un processus de livraison de données d'une manière fiable ou meilleure que la normale. La notion de service quand à elle peut recouvrir des niveaux d'abstraction plus ou moins élevés. Il est important de distinguer la notion de Qualité de Service de celle de classes de services différentiés qui se réfère à la capacité de différentier les types de trafics ou de services afin que les utilisateurs puissent traiter une ou plusieurs classes de trafic de manière différente des autres.

En fait, l'origine de l'expression qualité de service est relativement ancienne dans les réseaux et est emprunté au réseau postal. On retrouve des définitions de QoS dans X25, dans le modèle OSI, dans la spécification de la couche transport. Dans ce contexte, la qualité de service défini exactement quels paramètres parmi un ensemble de paramètres sont significatifs pour un contrat de service particulier.

Le sujet de ce chapitre se situe au cœur du concept de la qualité de service, nous commençons par définir la notion de la QoS, ainsi que les différents critères de performance que doit avoir le réseau pour satisfaire les besoins de l'utilisateur. Ensuite, nous décrivons quelques mécanismes et approches permettant d'implémenter la Qualité de Service dans les réseaux IP sous forme de services différenciés, ainsi que l'architecture "Integrated Services" développée par l'IETF. Enfin, un état de l'art de travaux de recherche traitant la qualité de service dans le contexte particulier des réseaux ad hoc sera présenté.

3.1 La qualité de service

3.1.1 Définition

Dans les réseaux de télécommunication, l'objectif de la qualité de service est d'atteindre un meilleur comportement de la communication, pour que le contenu de cette dernière soit correctement acheminé, et les ressources du réseau sont utilisées d'une façon optimale.

La qualité de service QoS peut être définie comme le degré de satisfaction d'un utilisateur des services fournis par un système de communication. La QoS est définie dans [23] comme la capacité d'un élément du réseau (ex : routeur, nœud ou une application) de fournir un niveau de garantie pour un acheminement des données.

Le RFC 2386 [24] caractérise la QoS comme un ensemble de besoins à assurer par le réseau pour le transport d'un trafic d'une source à une destination.

3.1.2 Critères de la qualité de service

La QoS au niveau d'un réseau se décline en quatre paramètres : le délai, la gigue, le débit (la bande passante) et la perte.

Le délai de bout en bout : c'est le temps mis pour transférer un paquet entre deux noeuds ,

La gigue : c'est la variation de l'intervalle de temps entre deux paquets durant leur acheminement entre la source et la destination,

La bande passante : c'est le volume total d'informations qui peut absorber un lien entre deux noeuds sans créer de file d'attente ,

La perte de paquets : c'est le nombre de paquets perdu par rapport au nombre de paquets émis.

En fonction des applications considérées, le paramètre à prendre en compte varie : par exemple, pour la vidéo, les paramètres importants sont la bande passante, la gigue et le délai, pour un échange de fichiers, il vaut mieux limiter la perte de paquets. La figure suivante illustre les besoins en délai et débit des applications.

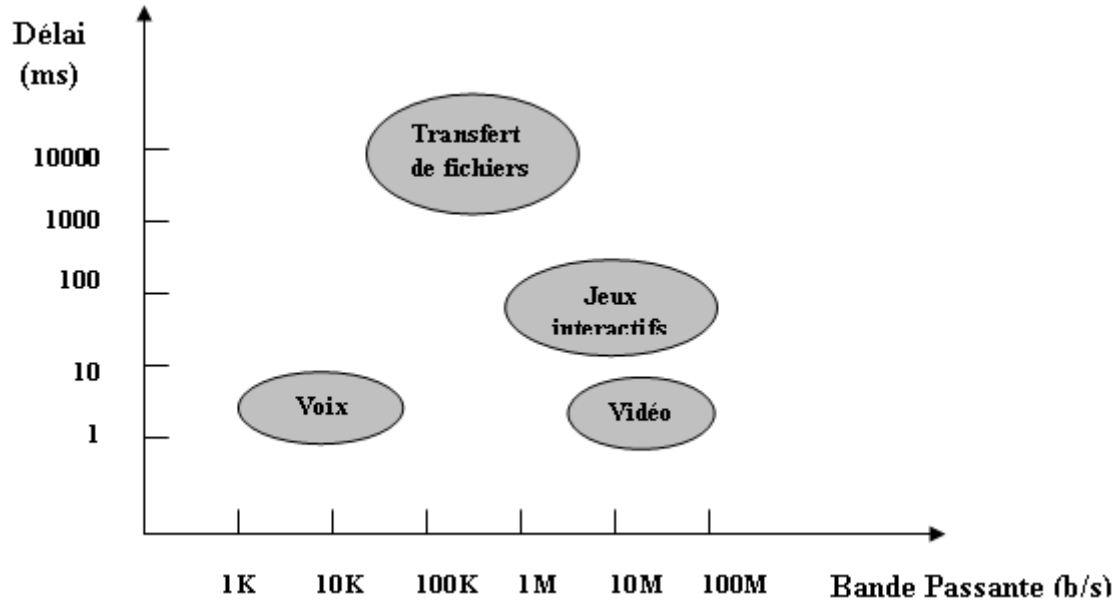


Figure12 : Besoin en délai et bande passante des applications.

[18]

3.2 La qualité de service sur IP

À ses débuts, Internet avait pour seul objectif de transmettre les paquets à leur destination. Conçu pour le transport asynchrone des données, IP (Internet Protocol) n'a pas été prévu pour les applications en temps réel comme la téléphonie ou la vidéo, très contraignantes. Les paquets sont tous traités de la même façon sans aucune différenciation. Ainsi, un flux temps réel (comme le streaming vidéo) et la messagerie sont traités avec le même service: "Best Effort". Ils sont stockés dans la file d'attente selon le principe FIFO (First In First Out). C'est pourquoi le temps de transmission peut être long et surtout il n'est pas constant d'où l'apparition de Gigue, phénomène auquel la transmission multimédia et en particulier la transmission audio est très sensible.

Le besoin en équipements de plus en plus fiables, d'un bout à l'autre du réseau, est donc devenu incontournable. Cependant, les défauts rencontrés sur les réseaux (perte de paquets, congestion) ne peuvent pas être surmontés sans une rénovation profonde de l'architecture.

Afin de garantir cette qualité de service, trois protocoles se sont imposés : Intserv (Integrated Service, protocole inclus dans RSVP, Ressource Reservation Protocol), Diffserv (Differentiated Services) et MPLS (MultiProtocol Label Switching). Leur standardisation est effectuée par l'IETF (Internet Engineering Task Force).

3.2.1 Historique

Ce paragraphe présente un court Historique de la QoS :

1976 : recherches préliminaires sur Arpanet
Le 'Department of Defense américain' décide de migrer le réseau Arpanet, ancêtre d'Internet, vers TCP/IP, et teste les premiers mécanismes de qualité de service sur le réseau.

1995 : création du protocole RSVP
Développement et mise au point de RSVP (dont Intserv fait partie), projet conduit par Xerox PARC, le MIT ainsi que l'Information Sciences Institute et le Computer Science Department, deux entités de l'université de Californie.

1997 : Diffserv comble les lacunes de l'architecture IP
Le groupe de travail Diffserv au sein de l'IETF revisite l'entête du paquet IPv4 et réutilise le champ dédié à la qualification des flux transportés.

1998 : MPLS rénove l'approche de la QoS
Poussés par Cisco, les équipementiers et opérateurs se rallient au sein de l'IETF pour standardiser la procédure de routage MPLS. À ce sujet, de nombreux travaux sont encore en cours.

[25]

Nous allons maintenant présenter le fonctionnement de la mise en œuvre de QoS sur les réseaux IP. Avant de présenter les modèles standard Intserv et Diffserv, nous indiquons d'abord quelques approches permettant d'implémenter des classes de services différenciées, a savoir : la classification des paquets, les mécanismes mis en oeuvre pour la gestion des files d'attente ainsi que ceux qui permettent de contrôler le volume du trafic entrant et prévenir les situations de congestion.

3.2.2 Implémentation des services différenciés

3.2.2.1 Classification des paquets

Afin de pouvoir appliquer une politique de QoS spécifique à un flux de données il est nécessaire de pouvoir marquer les paquets transitant étant donné que différents flux peuvent circuler sur un même lien. Un paquet est donc, en fonction de l'adresse de destination présente, de son en-tête et de son marquage, placé dans une des files d'attente du routeur.

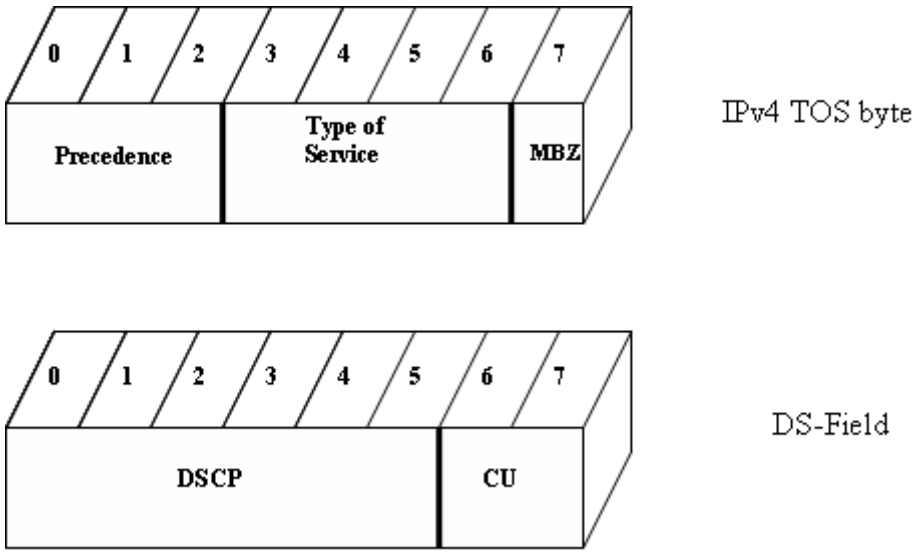


Figure 13: Structure du champ TOS d'IPv4 et signification dans DiffServ.

Valeur du champ TOS	Signification
0000	Normal
0001	Minimiser le coût
0010	Maximiser la fiabilité
0100	Maximiser le débit
1000	Minimiser le délai

Table1 : Utilisation du champ TOS.

Les paquets IPv4 possèdent dans leur en-tête 8 bits destinés à gérer la QoS. La RFC 1349 [26] nous précise la composition de l'octet TOS comme le montre la figure 13 :

- le champ *Precedence* codé sur 3 bits permet de décrire 8 niveaux de priorité ;
- le champ *Type of Service* codé sur 4 bits permet de spécifier des propriétés de délai, débit, fiabilité et coût comme spécifié dans le tableau 1 ;
- le champ *Must Be Zero* (MBZ) qui est fixé à 0 (non utilisé).

Dans un modèle DiffServ, la RFC 2474 a renommé l'octet TOS en Diffserv et sa composition est la suivante :

- le champ *DSCP* (Differentiated Service Code Point) codé sur 6 bits permet de décrire 64 niveaux de priorité,
- le champ *CU* (Currently Unused) codé sur 2 bits qui reste inutilisé.

Grâce à la spécification de cet octet, il est possible de classer un paquet IP en fonction :

- de son protocole de transport (TCP ou UDP),
- de sa source et de sa destination (adresse IP et port),

- et de son octet TOS ou DSCP.

[27], [28]

3.2.2.2 Gestion des files d'attente

La file d'attente est un composant central dans l'architecture des routeurs (figure 14). La stratégie de gestion des diverses files d'attente sur un routeur joue un rôle essentiel dans la différenciation des services, à travers le choix de l'algorithme qui place les paquets dans la queue de sortie, et le choix de la taille maximale de la queue.

Plusieurs algorithmes ont été développés:

- **First In First Out (FIFO)**

C'est la méthode standard de gestion de trafic entre une interface d'entrée et une interface de sortie. Les paquets sont placés dans la file de sortie dans l'ordre dans lequel ils sont reçus. Compte tenu des optimisations logicielles effectuées depuis le début, cette technologie peut-être considérée comme la plus rapide du point de vue de la transmission en paquets par seconde alors que des techniques plus élaborées risquent de dégrader ces performances.

Dans un environnement réseau avec capacité suffisante, cette technique est efficace, le délai de mise en file d'attente des paquets étant alors insignifiant par rapport au temps de transmission de bout en bout. En revanche, en situation de rafales, la file d'attente déborde et les paquets suivants sont jetés. Des stratégies de mise en file d'attente différenciée peuvent limiter la dégradation du service, en permettant à certains trafics d'être traités.

- **Priority Queuing (PQ)**

C'est la forme primitive de différenciation des services. Un trafic particulier peut être identifié et réordonné dans la file de sortie suivant un critère fourni par l'utilisateur dans la file de sortie. La granularité de la classification est flexible : par protocoles ou par services au sein d'un protocole. Mais en contrepartie, cela induit une dégradation des performances. De plus, lorsque le trafic classé prioritaire est anormalement élevé, le trafic normal peut-être rejeté par manque de buffers. Enfin, il est difficile de calculer précisément la gigue induite dans le chemin de bout en bout dans les techniques non-FIFO, le trafic pouvant rester dans la queue pour une période indéterminée.

- **Class-Based Queuing (CBQ)**

Ce mécanisme, utilisé pour éviter qu'une seule classe de trafic ne monopolise les ressources, définit plusieurs files de sortie avec une priorité et un total de trafic autorisé. Le trafic est extrait de chaque queue suivant une rotation.

Le principe de ce mécanisme est que l'absence de ressources est pire qu'une réduction des ressources. Il convient à des liens bas débit, car il induit un surcroît de traitement et une réorganisation des files pouvant dégrader les performances du routeur à haut débit.

- **Weighted Fair Queing (WFQ)**

Cet algorithme donne un traitement prioritaire aux flux de faible volume et permet aux flux de volume important d'utiliser la place qui reste. Pour cela, il trie et regroupe les paquets par flux, puis met ceux-ci en file d'attente suivant le volume de trafic dans chaque flux.

L'implémentation de la politique de caractérisation du flux est dépendante du constructeur, elle peut utiliser les bits IP Precedence dans le champ TOS de l'en-tête du paquet pour trier les paquets. Dans ce cas, le traitement rapide par le matériel peut ne pas affecter les performances. Mais le contrôle du mécanisme de tri, dépendant du constructeur, est figé et peu satisfaisant.

[28]

3.2.2.3 Lissage du trafic

En alternative ou en complément à ces techniques de gestion des files d'attente autres que FIFO, d'autres techniques sont utilisées, telles que "Trafic shaping" qui permet de contrôler le volume de trafic entrant dans le réseau ainsi que le débit avec lequel il est transmis.

Les deux techniques principales de Lissage du trafic sont:

- **Leaky Bucket**

Le trafic entrant dans la file (le seau) est régulé pour sortir à débit constant sur le réseau. La taille du seau et le débit en sortie sont configurables par l'utilisateur. La taille étant déterminante en ce qui concerne les pertes de paquets (lorsque le seau est plein le trafic entrant peut être jeté).

Le *leaky bucket* est composé d'un compteur t, d'un seuil C et d'un taux de vidage, le *leaky rate* : µ. Chaque fois qu'un paquet arrive dans le seau, le compteur est incrémenté et ce même compteur est décrémenté par le *leaky rate*. Si un paquet arrive au moment ou $t=C$, alors celui-ci est jeté.

- **Token Bucket**

Le trafic ne traverse pas directement le seau mais est transmis sur la base de jetons présents dans le seau. Un jeton correspond à un nombre de bits donné, le taux d'arrivée des jetons (µ) correspond au débit moyen, et la profondeur (C) du seau à la taille de la rafale.

Ce mécanisme permet à un trafic en rafale d'être transmis tant qu'il y a des jetons dans la file d'attente, ceux-ci ayant pu être accumulés en situation de réseau peu chargé.

3.2.2.4 Prévention de la congestion

On constate qu'une fois la congestion atteinte, on peut essayer de mettre en place des techniques de gestion de cette congestion plus ou moins efficaces, mais dans l'absolu, il vaudra toujours mieux éviter d'en arriver là, car :

- Les paquets TCP rejetés devront être réémis ce qui surchargera à nouveau les buffers,

- L'entrée en phase de démarrage d'une session TCP est lent (mécanisme du Slow Start).

Parmi les méthodes de prévention de la congestion, nous citons :

- **Random Early Detection (RED)**

Cette méthode a pour vocation la détection de la congestion avant que cette dernière ne se produise. Pour se faire, on va :

- à partir d'un premier seuil_mini, on rejettera quelques paquets avec une probabilité p, ce qui indique à la source qu'elle doit réduire son débit,

- au-delà d'un certain seuil_maxi > seuil_mini, on rejettera les paquets.

Ce système permet au RED de maintenir une taille de file d'attente raisonnable, et de garantir ainsi des délais de transit faibles.

La probabilité p est déterminée par la part du flot global représenté par le flux d'une source particulière : plus une source émet vers une file, et plus elle risque de voir ses paquets être rejeté en cas de charge de la file.

- **Weighted Random Early Detection (WRED)**

Même technique que la précédente mais qui permet de déterminer quel trafic on jette grâce à la prise en compte du champ IP Precedence par les routeurs et cela afin d'éviter la monopolisation des ressources par certaines classes de trafic. Cette pondération gérée via ce champ permet au réseau de demander aux flux de trafic moins prioritaires de s'adapter au profit du trafic plus prioritaire.

[29]

Dans le paragraphe suivant, nous allons présenter l'architecture d'un routeur supportant la QoS.

3.2.3 Architecture d'un routeur supportant la QoS

La figure 14 présente l'architecture d'un routeur gérant la QoS. On peut remarquer qu'en plus de router les paquets vers la bonne interface de sortie (fonction de routage), ce type de routeur comporte un système de files d'attente sur chaque interface de sortie et un Ordonnanceur permettant de choisir les paquets qui seront envoyés. C'est grâce au marquage des paquets présenté ci-dessus que les paquets sont placés dans les files d'attente logicielles pour finalement être placés dans une file matérielle après l'ordonnancement.

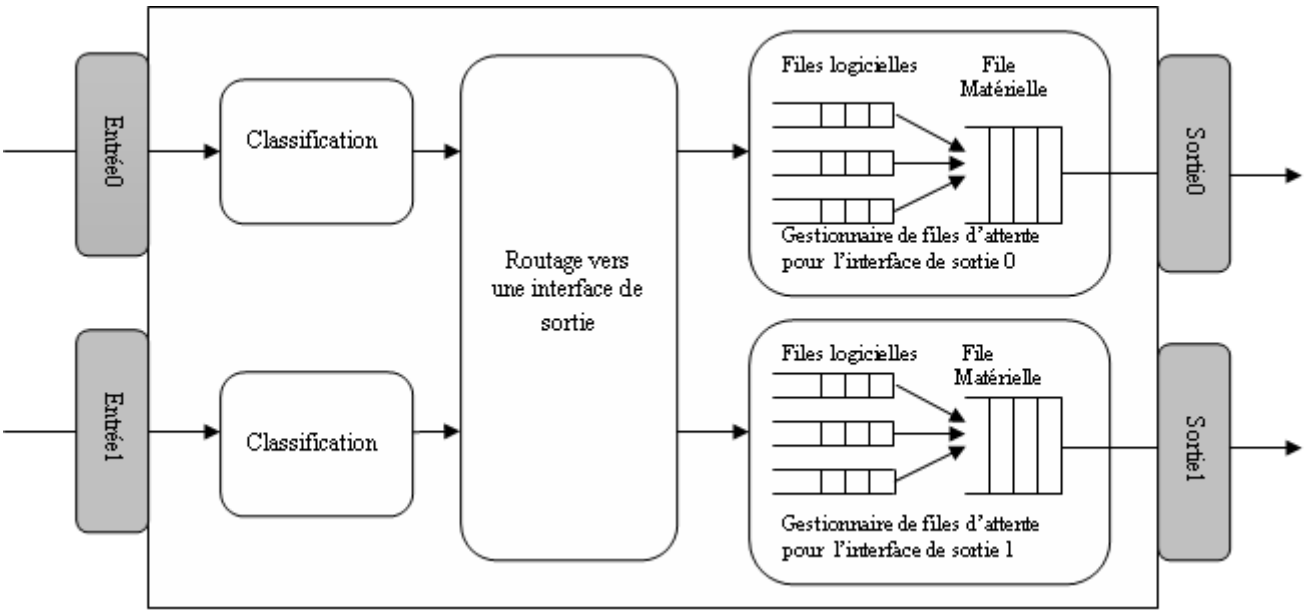


Figure14 : Architecture d'un routeur supportant la QoS

[27]

3.2.4 Modèles IntServ et DiffServ

Afin d'avoir une gestion de la QoS de bout en bout il faut que tous les routeurs du réseaux soient paramétrés de la même façon. Dans un soucis de standardisation, deux approches ont vu le jour : Intserv et DiffServ.

3.2.4.1 Le modèle Intserv/RSVP

Le modèle IntServ définit une architecture capable de prendre en charge la QoS sans toucher au protocole IP. IntServ utilise pour cela un protocole spécifique de signalisation appelé RSVP (Resource ReSerVation Protocol), Quand une source produit un flux de données, elle peut également émettre des messages de signalisation RSVP, décrivant les caractéristiques de celui-ci. Cette signalisation ayant la même destination que le flux (il peut aussi s'agir d'une adresse de multicast), traversera les mêmes routeurs intermédiaires qui y ajouteront leurs caractéristiques, principalement leur temps de traversée. Les flux restent traités par les routeurs en *Best-Effort*. Le destinataire recevant les messages de signalisation, en plus des données du flux, peut décider d'améliorer la qualité de celui-ci en envoyant un message de réservation vers la source pour demander aux routeurs d'améliorer le traitement du flux. Mais le routage dans l'Internet n'est pas symétrique, il faut donc que les routeurs se souviennent pour chaque flux quel était le précédent routeur. Un contexte doit être établi dans chaque routeur pour chaque flux signalé par la source. A la réception d'un message de réservation, un contrôle d'admission est fait par le routeur pour déterminer si l'ajout d'un nouveau flux ne perturbera pas ceux pour qui une réservation a déjà été faite.

Le groupe de travail IntServ a actuellement défini deux types de services lors de la réservation :

- Le service garanti est basé sur les résultats du Network Calculus qui permet de trouver une borne maximale pour le temps de transmission d'un paquet et la taille maximale des mémoires tampons nécessaires dans les équipements pour éviter les pertes de paquets. Le destinataire en fixant le débit minimal que doit offrir le réseau à ce flux influe sur le temps maximal de transmission des paquets. Ainsi, pour réduire les temps de traversée, il est possible de réserver à un débit nettement supérieur à celui de la source.

- Le service contrôlé a une définition relativement vague : un service contrôlé offre un service proche de l'Internet peu chargé. Ce type de service a un intérêt si l'on considère que des outils de téléconférence comme vat pour la vidéo ou vic pour l'audio offrent une bonne qualité quand le réseau est peu utilisé, mais la qualité se dégrade très vite si le réseau est saturé.

1 Caractéristiques du protocole RSVP

- RSVP est avant tout un protocole de signalisation qui permet de réserver dynamiquement la bande passante, et de garantir un délai, ce qui le rend particulièrement efficace pour des applications comme la VoIP.

- RSVP rend obligatoire la demande de QoS par le récepteur plutôt que par l'émetteur, ce qui permet d'éviter que certaines applications émettrices monopolisent des ressources inutilement, au détriment de la performance globale du réseau. Le fait que le récepteur décide des ressources dont il a besoin permet aussi une facturation différenciée par récepteur.

- Les équipements d'interconnexions (routeurs), sur le chemin du flux des données, répondent aux requêtes RSVP, établissent et maintiennent les connexions. Les routeurs communiquent via RSVP pour initialiser et gérer la QoS réservée aux sessions.

- RSVP travaille au dessus de IP (IPv4 ou IPv6) et occupe la place d'un protocole de transport dans la pile des protocoles mais ne transporte pas de données utilisateurs comme ICMP ou IGMP. Dans les cas où le système ne permet pas l'utilisation de services réseau directement, RSVP est encapsulé dans des paquets UDP.

- RSVP passe de façon transparente les routeurs non RSVP.

- RSVP n'est pas un protocole de routage. Il est sensé travailler avec les protocoles de routage unicast et multicast comme RIP, OSPF, RPM,...

- RSVP fait des réservations de ressources pour les applications unicast et multicast et s'adapte dynamiquement aux évolutions (participants, changements de routes) Il demande des ressources dans une seule direction et traite l'émetteur et le récepteur de manière différente.

- Il est utilisé par un "host" pour le compte d'une application, pour demander une QoS au réseau (bande passante garantie, ...)

- Il est utilisé par les routeurs pour le contrôle de la QoS et l'établissement et maintient du service demandé.

- Les routeurs réservent les ressources en mémorisant des informations d'état (SOFT STATE). Quand un chemin n'est plus utilisé, il est nécessaire de libérer ces ressources. De même si le chemin est modifié, les tables d'états doivent pouvoir être tenues à jour, ce qui engendre des échanges périodiques entre routeurs.

2 Limitations du protocole RSVP

RSVP oblige à maintenir des informations d'état à chaque nœud du chemin liant l'émetteur au récepteur. Lorsque le nombre d'usagers augmente (scalability), le nombre d'états devient conséquent, et le trafic est d'autant plus saturé que les rafraîchissements entre routeurs deviennent importants et créent de l'overhead. Cela nuit aux performances du système dans son ensemble. C'est pourquoi RSVP est plus adapté à des réseaux de petite taille comme les LAN.

[29], [30]

3.2.4.2 Le modèle Diffserv

La différenciation de services consiste dans une situation de congestion à reporter les pertes de paquets sur certaines classes de trafic, pour en protéger d'autres. Il n'y a donc pas de garantie sur les flux car il n'y a pas de contrôle d'admission dynamique permettant d'éviter une congestion. Le contrôle d'admission est fait a priori par la définition d'un contrat pour chaque classe de trafic et par le dimensionnement des ressources pour pouvoir garantir ce contrat.

Les paquets DiffServ sont marqués à l'entrée du réseau et les routeurs décident en fonction de cette étiquette de la file d'attente dans laquelle les paquets vont être placés. Cette architecture convient à des réseaux pour lesquels il n'est pas raisonnable d'envisager une signalisation flux par flux. Elle ne considère donc que des agrégats de flux pour lesquels une signalisation avec réservation de ressources peut-être envisagée. En fait un routeur de cœur ne conserve pas d'état pour un flux ou un agrégat donné, mais traite tous les paquets d'une classe donnée de la même manière. Les données sont identifiées grâce à un marquage dans le champ ToS (Type of Service, champ spécifique réservé dans l'en-tête IP de 8 bits), qui fixe les priorités.

La différenciation de services présente les avantages suivants :

- La signalisation est faite dans chaque paquet en attribuant une signification différente aux bits du champ type de service. Il n'est plus besoin de garder dans le routeur un contexte liant le flux de signalisation au flux de données. Cela permet aussi une agrégation naturelle des flux, ainsi pour un opérateur, les paquets qui sont marqués pour une certaine classe peuvent appartenir à plusieurs sources.

- La complexité du traitement est concentrée dans les routeurs aux frontières du réseau. Ils effectuent les opérations « complexes » de contrôle de la validité du contrat pour les différentes classes de trafic. Dans le cœur du réseau, le traitement est plus simple, ce qui autorise un relayage rapide des données.

- La tarification du service est plus simple, il suffit de définir les paramètres de contrôles de classes de service.

Au contraire du modèle Intserv qui traite indépendamment chaque flot, le modèle Diffserv sépare le trafic par classes. Nous avons donc affaire à une granularité moins fine mais qui devient en revanche plus « scalable ». En effet, la granularité du flot implique la réaction en chaîne suivante : plus il y a d'utilisateurs dans le réseau, plus il y a de flots, plus il y a de variables de classification et d'ordonnancement dans les routeurs à maintenir, ce qui a pour conséquence une charge importante au niveau des routeurs qui deviennent alors de moins en moins performants.

Les routeurs DiffServ traitent les paquets en fonction de la classe codée dans l'entête IP (champ DS) selon un comportement spécifique : le PHB (Per Hop Behaviour). Chaque ensemble de paquets défini par une classe reçoit alors un même traitement et chaque classe est codée par un DSCP (DiffServ Code Point). Un PHB est défini par les priorités qu'il a sur les ressources par rapport à d'autres PHB.

En aucun cas, les routeurs ne traiteront différemment des paquets de même PHB et de sources différentes. L'avantage de Diffserv est qu'il n'y a plus nécessité de maintenir un état des sources et des destinations dans les routeurs, d'où une meilleure extensibilité.

Diffserv définit quatre PHB ou classes de service :

- Best Effort (priorité basse) : PHB par défaut et dont le DSCP vaut 000000,

- Assured Forwarding (AF) (RFC 2597) : regroupant plusieurs PHB garantissant un acheminement de paquets IP avec une haute probabilité sans tenir compte des délais, cette famille de PHB est scindée en 4 classes garantissant de fournir une bande passante et un délai minimum, chaque classe comprenant 3 niveaux de priorité (*Drop Precedence*),

- Expedited Forwarding (EF) ou Premium Service (RFC 2598) : correspondant à la priorité maximale et a pour but de garantir une bande passante avec des taux de perte, de délai et de gigue faible en réalisant le transfert de flux à fortes contraintes temporelles comme la téléphonie sur IP par exemple,

- Default Forwarding (DF), utilisé uniquement pour les flux Internet qui ne nécessitent pas un trafic en temps réel.

Cette notion de PHB permet de construire une variété de services différenciés. Les PHB sont mis en oeuvre par les constructeurs dans les routeurs en utilisant des mécanismes de gestion de files d'attente (Custom Queuing, Weighted Fair Queuing, ...) et de régulation de flux.

L'architecture des services différenciés proposée dans le [RFC2475] contient deux types d'éléments fonctionnels :

- Les **éléments de bordures** (edge functions) : ils sont responsables de la classification des paquets et du conditionnement du trafic. En bordure du réseau, c'est à dire à l'arrivée du premier élément actif capable de traiter le champs DS (*DS-capable*), les

paquets arrivant ont dans leur champ TOS (pour IPv4) ou Traffic Class Octet (pour IPv6), une certaine valeur DS. La marque qu'un paquet reçoit identifie la classe de trafic auquel il appartient. Après son marquage, le paquet est envoyé dans le réseau ou jeté.

- Les **éléments du cœur du réseau** (core functions) : ils sont responsables de l'envoi uniquement. Quand un paquet, marqué de son champ DS, arrive sur un routeur *DS-capable*, celui-ci est envoyé au prochain nœud selon ce que l'on appelle son *Per Hop Behaviour* (PHB) associé à la classe du paquet. Le PHB influence la façon dont les buffers du routeur et les liens sont partagés parmi les différentes classes de trafic. en aucun cas ils ne traiteront différemment des paquets de sources différentes.

Dans l'architecture Diffserv, le traitement différencié des paquets s'appuie sur 3 opérations fondamentales :

- la classification des flux en classes de services,
- l'introduction de priorités au sein des classes (*Scheduling*),
- et la gestion du trafic dans une classe donnée (*Queue management*).

[31]

3.2.5 Complémentarité de IntServ et de DiffServ

IntServ et Diffserv peuvent être utilisés d'une manière complémentaire afin de bénéficier des possibilités de IntServ sur des réseaux à large échelle. L'idée, présentée dans [32] est d'avoir des routeurs IntServ en bordure du réseau et des routeurs DiffServ au cœur. Il faudra dans ce cas que les requêtes RSVP soient traduites pour modifier le champ DSCP des paquets. [27]

3.3 Réseaux Ad hoc et qualité de service

La problématique de QoS a été largement étudiée dans le cas des réseaux filaires. Dans ce type de réseaux, des équipements tels que les routeurs peuvent assurer le contrôle de la QoS en différenciant les paquets (certains sont prioritaires) ou en adaptant les routes suivies par les données en fonction des besoins à satisfaire. Mais, dans le cas des réseaux sans fil ad hoc, la problématique est complètement différente. En effet, il n'existe aucun élément du réseau pouvant s'occuper de la QoS. Cette fonction doit donc être distribuée. De plus, les conditions de transmission dans le réseau sont en constante évolution : mobilité des noeuds, médium radio peu fiable, changement brusque de la capacité d'échange des liens...etc. Les ressources du réseau sont également plus limitées que celles des réseaux filaires, notamment pour la bande passante, il n'est donc pas possible de satisfaire les mêmes besoins que pour les applications de réseaux filaires.

Dans le cas de réseaux ad hoc, la qualité de service nécessaire pour certaines applications est fortement dépendante de la qualité du réseau (y a-t-il des mobiles dans un environnement suffisamment proche pour permettre une communication de bonne qualité). Il faut donc une autre approche de la qualité de service.

Les recherches concernant la qualité de service dans les réseaux ad-hoc sont souvent classées en quatre grandes catégories : les modèles de qualité de service définissent des architectures globales dans lesquelles des garanties peuvent être fournies, les protocoles d'accès au médium cherchent à ajouter des fonctionnalités aux couches basses du modèle OSI afin de pouvoir offrir des garanties, les protocoles de routage avec qualité de service recherchent les routes ayant suffisamment de ressources disponibles pour satisfaire une requête, les protocoles de signalisation cherchent à offrir des mécanismes de réservation de ressources indépendants du protocole de routage sous jacent.

Ces travaux sont souvent inspirés des solutions déjà proposées dans les réseaux fixes, tout en essayant de tenir compte de l'environnement ad hoc.

Des contraintes liées aux réseaux sans fil ad hoc sont aussi traitées dans d'autres travaux, en particulier:

- L'adaptation de puissance d'émission : maximise la puissance d'émission pour les trafics prioritaires,
- Le partage de charge : distribution de la charge entre les différents nœuds du réseau,
- L'économie de batterie : vise à trouver la plus courte route en minimisant l'énergie consommée.

Ces mécanismes de qualité de service permettent de gérer au mieux les ressources du réseau (bande passante, mémoire, batterie … etc.), dans le but de satisfaire les différents besoins de QoS des applications.

Le but de cette section est de dresser un état de l'art de ce domaine afin de déterminer les problèmes qui subsistent.

3.3.1 Modèle de qualité de service pour les réseaux ad hoc

Les modèles de qualité de service IntServ/RSVP et DiffServ ont été proposés par l'IETF pour fournir des garanties aux besoins des services temps réel dans les réseaux filaires. D'un coté, l'application du modèle IntServ dans les MANETs s'avère inadaptée à l'environnement ad hoc. Ceci est justifié du fait que les capacités des nœuds mobiles sont trop variables et limitées pour supporter un traitement complexe et gérer les réservations ainsi que les états des communications en cours. De plus, une réservation dans les réseaux filaires est différente de celle d'un réseau mobile sans fil, car les liens sont partagés, limités, et susceptibles à des variations spatio-temporelles. D'un autre coté, le modèle DiffServ semble le mieux adapté aux réseaux mobiles. Pour résoudre le problème de passage à l'échelle, ce modèle utilise une granularité par classe, où aucune signalisation pour la réservation de ressources n'est utilisée. Cependant, dans ce modèle le cœur du réseau est supposé bien dimensionné, et un administrateur de domaine est nécessaire. Ces deux contraintes restent difficiles à satisfaire.

- **Flexible Quality of service Model for MANETs (FQMM)**

Le modèle FQMM repose sur une architecture réseau plate (non hiérarchique), constituée d'une cinquantaine de nœuds mobiles, formant un domaine DiffServ. Il combine les

propriétés des modèles filaires IntServ et DiffServ, en offrant une méthode d'approvisionnement hybride : par flux, pour les trafics prioritaires, et par classe pour les autres trafics. Dans le réseau, les nœuds peuvent avoir des rôles différents suivant les trafics existants : nœud d'entrée du trafic, intermédiaire ou de sortie. Les nœuds d'entrée permettent de marquer et classifier les paquets, qui seront ensuite relayés par les nœuds intermédiaires suivant leurs PHB (Per Hop Behavior), jusqu'à arriver au nœud destinataire. Ce modèle repose essentiellement sur la couche IP, où les fonctionnalités sont séparées en deux grands plans, le plan relayage de données et le plan contrôle et gestion. Les techniques d'ordonnancement et de gestion de mémoires tampons sont étudiées dans la section précédente. Dans ce modèle, le protocole de routage est supposé fournir des routes ayant suffisamment de ressources.

L'avantage d'une telle approche est la possibilité d'interfacer le réseau avec l'Internet, vu les mécanismes de qualité de services offerts qui sont proches des protocoles filaires. Cependant, plusieurs mécanismes ainsi que l'interaction avec la couche MAC restent à définir pour s'adapter aux conditions variables du réseau ad hoc.

- **Service differentiation in wireless ad hoc networks (SWAN)**

SWAN est un modèle réseau basé sur des algorithmes de contrôle distribués dans le but d'assurer une différenciation de services dans les réseaux ad hoc. Il offre la priorité (au niveau paquet) aux trafics temps réel en contrôlant la quantité de trafics best effort acceptée par nœud. Pour accepter un nouveau trafic temps réel, le contrôle d'admission sonde la bande passante minimale disponible sur la route (valide et obtenu par un protocole de routage). Une décision à la source est alors prise suivant la bande passante obtenue. Pour maintenir la qualité de service des trafics déjà acceptés, le débit des trafics best effort est régulé en utilisant les mesures de délais au niveau MAC comme paramètre. Un classificateur et un shaper permettent de différencier les deux types de trafic. En cas de congestion, les bits ECN (Explicit Congestion Notification) de l'entête des paquets IP sont positionnés pour permettre à la source de re-initier le contrôle d'admission. Si la route ne dispose pas d'assez de bande passante, le trafic est supprimé. Ainsi, SWAN permet de fournir une QoS logiciel (soft QoS).

Un flux prioritaire admis n'est pas sûr d'avoir des garanties pour l'entière durée de la communication, et peut à tout moment être violé par d'autres demandes de trafics. Un mécanisme de contrôle de débit des flux best effort n'est pas à lui seul suffisant pour offrir des garanties aux applications temps réel. En outre, dans cette approche, le protocole de routage ainsi que la couche d'accès au médium sont de type best effort.

- **Modèle iMAQ**

Le modèle iMAQ fournit le support des transmissions des données multimédia dans un MANET. Le modèle inclut une couche ad hoc de routage et une couche de service logiciel (Middleware). Dans chaque nœud, ces deux couches partagent les informations et communiquent afin de fournir les garanties de QoS aux trafics multimédia. Le protocole de routage est basé sur la prédiction de la position des nœuds (predictive location-based) et orienté QoS. La couche Middleware communique également avec la couche application et la couche réseau et essaye de prévoir le partitionnement du réseau. Pour fournir une meilleure

accessibilité aux données, il réplique les données entre les différents groupes du réseau avant d'effectuer le partitionnement.

[33]

3.3.2 Les protocoles d'accès au medium

Les spécificités du médium radio rendent l'utilisation d'un protocole d'accès au médium efficace primordiale. Le rôle du protocole d'accès au médium est multiple. Il est en charge d'éviter les collisions, d'assurer le partage de la bande passante et de résoudre certains problèmes spécifiques aux transmissions hertziennes (stations cachées ou exposées). Cependant, beaucoup de protocoles de routage avec qualité de service pour les réseaux ad-hoc pourraient tirer parti de protocoles de niveau 2 capables de gérer une certaine qualité de service.

- **Différenciation de services pour 802.11**

Dans [34], les auteurs proposent de doter le protocole IEEE 802.11 d'un mécanisme de priorités entre les trames afin de concevoir des mécanismes de différenciation de services efficaces. Pour ce faire, les auteurs proposent d'adapter certains paramètres de la fonction de coordination distribuée (DCF) du protocole selon la priorité des paquets.

La fonction de coordination distribuée repose sur la détection de porteuse (CSMA). Avant d'émettre sur le médium, tout nœud doit s'assurer que le canal radio est libre depuis un certain temps (DIFS – *DCF Inter Frame Spacing*), afin de privilégier certains paquets de signalisation dont la transmission peut s'effectuer dès que le médium a été libre durant un temps SIFS (*Short Inter Frame Spacing*) plus court que le DIFS.

On ajoute au DIFS, constant, un délai supplémentaire aléatoire permettant d'éviter que deux mobiles ne commencent à émettre au même moment. Dans ce cas, si une collision survient, le processus est réinitialisé et le délai aléatoire supplémentaire est allongé.

Un certain nombre de ces paramètres peuvent être adaptés dynamiquement afin d'offrir un mécanisme de priorités au protocole 802.11 :

- Lorsqu'une collision survient, les délais avant retransmission sont allongés aléatoirement. Il est possible d'incrémenter ces délais différemment selon le niveau de priorité.

- Il est possible d'utiliser différentes valeurs du délai de silence avant une transmission (DIFS) selon le niveau de priorité de la transmission.

- Enfin, il est possible de limiter la longueur des trames selon le niveau de priorité, les trames peu prioritaires occupant le canal moins longtemps.

Les trois principes ont été testés sur des flots UDP et TCP. De ces trois méthodes, la deuxième, consistant à jouer sur le délai DIFS, semble la plus stable et la plus performante.

- **MACA / PR**

Le protocole MACA/PR (Multiple Access Collision Avoidance with Piggyback Reservation) propose de différencier la politique d'accès au médium selon la nature des flux. Les paquets des flux non privilégiés sont traités de façon standard.

Pour les flux temps réel, une unique demande d'autorisation à transmettre (échange RTS-CTS) est effectuée en début de flux. Tous les paquets suivants sont transmis directement et doivent être acquittés par le récepteur. Dès qu'un paquet n'est pas acquitté, une nouvelle demande d'autorisation est émise. Afin de traiter les réservations de bande passante, l'émetteur inclut des informations dans chaque paquet sur l'ordonnancement du paquet suivant. Tous les voisins du nœud récepteur, en écoutant l'acquittement d'un paquet de données possèdent des informations sur la date d'arrivée du prochain paquet et peuvent différer leurs transmissions. Ce mécanisme permet de résoudre le problème des stations cachées sans avoir recours à des paquets de signalisation particuliers.

[35]

3.3.3 Routage avec qualité de service

Le routage avec QoS est un élément clé pour réaliser une architecture de QoS pour les MANETs. Il est important de définir les objectifs visés par le routage avec QoS. Le routage au mieux (sans QoS) consiste en général à trouver le plus court chemin en terme de distance ou de délais entre une source et une destination. Dans le cas du routage avec QoS, l'objectif n'est pas seulement de trouver le meilleur chemin selon un critère précis, mais de trouver un chemin "admissible"satisfaisant certaines contraintes. Plusieurs paramètres peuvent être utilisés tels que le délai, la bande passante, la disponibilité en terme de QoS ou encore le coût de transmission.

On voit apparaître donc des spécificités où les routes doivent être calculées par flux et non par destination. En effet, un flux peut avoir des besoins de QoS alors qu'un autre flux entre ces mêmes nœuds en aura d'autres. Le routage avec QoS est très difficile dans les MANETs car il engendre un overhead important. En effet, les nœuds doivent mettre en place un mécanisme permettant de stocker et mettre à jour les états de liens dans un environnement mobile. Cette mobilité rencontrée rend le maintient de l'état précis des liens très difficile et très coûteux. De plus, la mobilité ou le manque d'énergie peuvent causer des ruptures dans les chemins établis, le protocole doit donc être capable de réagir très vite à ce genre d'événement en recalculant des routes valides. Par conséquent, la complexité de la recherche de routes optimales dépend des types de contraintes. L'idée est donc de trouver un équilibre entre le gain apporté par le routage QoS et l'importance de l'overhead.

Le contrôle d'admission, l'équilibrage de la charge du réseau ainsi que la recherche de routes répondant aux critères des applications sont en général les tâches incombant à un protocole de routage avec qualité de service.

[15], [36]

- **Routage avec QoS sur DSDV (DSDV+)**

DSDV (Dynamic Destination Sequenced Distance-Vector) ou vecteur de distance à destination dynamique séquencée est un protocole de routage proactif implémenté avec la qualité de service afin de résoudre les problèmes liés aux stations cachées. En effet, Lors d'une demande de réservation, DSDV évalue la quantité de bande passante disponible sur la route principale. Tout en évaluant le nombre d'unités TDMA (Division du temps en unités) appelées slots, disponible sur chaque lien tout au long de la route.

Il est nécessaire de ne pas utiliser les mêmes unités pour les transmissions entre deux liens adjacents. Dès que le destinataire reçoit la demande de route, il renvoie à l'émetteur une confirmation indiquant la politique d'allocation des unités choisie sur la route empruntée, la réservation de ressources se fait parallèlement à cette réponse.

Pour pallier aux problèmes liés à la mobilité, une route secondaire non optimale en terme de nombre de sauts est maintenue. Bien que ce protocole évalue bien la bande passante disponible sur un chemin et offre le calcul de la probabilité de rejet des appels lors des simulations, il est incapable de résoudre les problèmes d'interférences, en particulier lorsque deux nœuds utilisant les mêmes unités TDMA se rapprochent et arrivent à portée d'émission l'un de l'autre.

- **Ticket Based Probing (TBR)**

Ticket-Based QoS Routing est un protocole de routage qui permet de réduire la quantité des messages de routage diffusée pour la découverte de la route, car la recherche de routes par inondation peut être très coûteuse. Ce protocole de routage QoS a été conçu pour des réseaux à faible mobilité pour éviter de réel problème (scénario de type salle de conférence). La durée de vie des routes doit être grande devant le temps nécessaire à l'établissement ou à la restauration d'une route. Le protocole utilise une technique de réparation locale des routes.

Le but de Ticket Based Probing est de limiter ce surcoût et de fournir des garanties de qualité de service. La découverte de route est limitée, car l'émetteur va associer une demande de route à un certain nombre de tickets logiques qui va limiter la diffusion des requêtes. Chaque message de découverte (ou d'observation) de route doit avoir au moins un ticket. Quand un message arrive à un noeud, il peut être divisé en plusieurs messages d'observation, qui sont relayés vers les prochains sauts. Chaque message 'fils' contiendra un sous ensemble des tickets de son message 'père'. Evidemment, un message ayant un seul ticket ne peut être divisé. Lors de l'arrivée d'un message de découverte de route à la destination, le chemin saut par saut est connu et les informations de délai ou de bande passante peuvent être utilisées pour effectuer la réservation de ressources pour la route répondant aux besoins de QoS. Par conséquent, chaque noeud aura la connaissance des caractéristiques des liens vers ses voisins immédiats grâce à la transmission périodique de paquets de signalisation. Il peut donc ainsi sélectionner efficacement les voisins à qui transmettre les demandes de route. Plus un flux de données aura de contraintes, plus on associera de tickets à la demande correspondante, le nombre de tickets généré est fonction de la précision des informations d'états disponibles à la source et les besoins de QoS de la communication.

Deux problèmes sont étudiés:

- Etablir des routes, les plus proches de l'optimal possible, de moindre coût avec des contraintes de délai (NP complet).

- Etablir des routes de moindre coût avec des contraintes de débit (solvable en temps polynômial).

Afin d'augmenter la probabilité de trouver une route, deux types de tickets sont utilisés:

- Des tickets jaunes : Pour permettre de rechercher des chemins respectant la contrainte imposée.
- Des tickets verts : Pour permettre d'obtenir des solutions à faible coût.

Malgré le fait que les noeuds ne connaissent que leur voisinage immédiat, Ticket Based Probing est efficace car il permet de trouver des routes avec une probabilité proche de celle des algorithmes basés sur l'inondation du réseau et meilleure que des algorithmes recherchant un plus court chemin. Il permet en outre de trouver des routes de plus faible coût que ces deux types d'algorithmes.

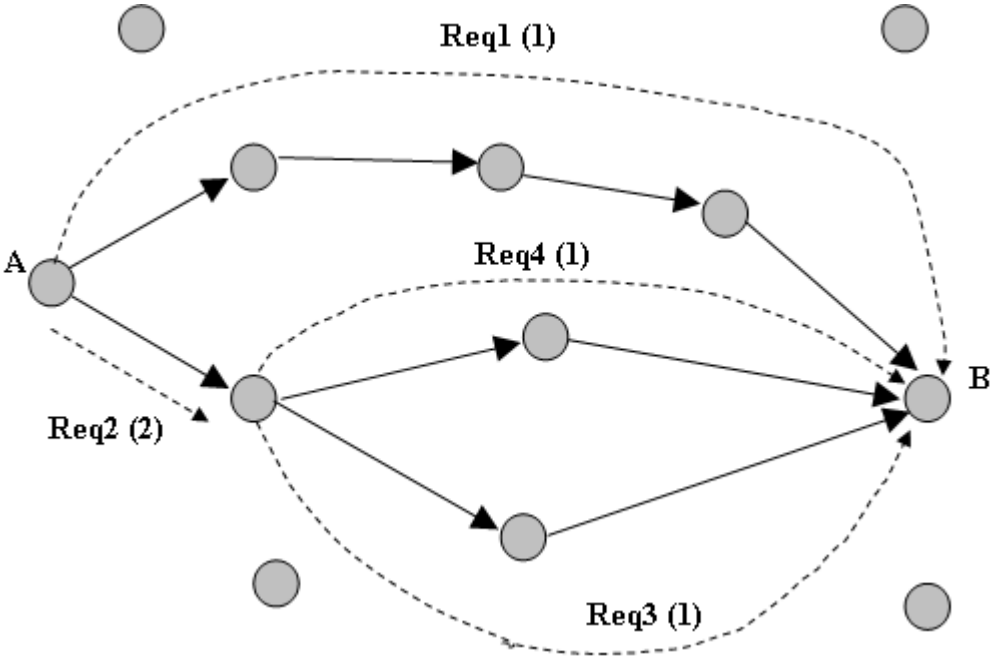


Figure15: Principe de Ticket Based Probing.

[36]

- **CEDAR (Core-Extraction Distributed Ad hoc Routing Algorithm)**

Dans les protocoles de routage avec qualité de service, le but est de trouver une route satisfaisant des critères de QoS, souvent de bande passante ou de délai. Le problème majeur réside dans le surcoût engendré, car les informations d'état des routes maintenues dans le réseau et les échanges d'informations consomment plus de bande passante, dans un système où cette dernière est limitée. Un autre problème est la difficulté d'avoir une information d'état précise (cohérente) de la route, vu la nature dynamique des réseaux ad hoc.

CEDAR est un protocole de routage réactif avec qualité de service basé sur une élection dynamique d'un cœur de réseau stable. Des informations sur les liens stables disposant d'une grande bande passante sont propagées entre les nœuds du cœur.

Utilisé dans des réseaux de petite taille, il est basé sur trois composantes essentielles :

– Extraction d'un cœur du réseau : un ensemble de nœud est dynamiquement choisi pour calculer les routes et maintenir l'état des liens du réseau. L'avantage d'une telle approche est qu'avec un ensemble réduit de nœuds les échanges d'information d'état et de route seront minimisés, évitant ainsi plus de messages circulant dans le réseau. En outre, lors d'un changement de route, seuls les nœuds du cœur serviront au calcul.

– Propagation d'état de lien : le routage avec qualité de service est réalisé grâce à la propagation des informations sur les liens stables avec une grande bande passante.

– Calcul de route : celui-ci est basé sur la découverte et l'établissement d'un plus court chemin vers la destination satisfaisant la bande passante demandée. Des routes de 'secours' sont utilisées lors de la reconstruction de la route principale, quand cette dernière est perdue. La reconstruction peut être locale (à l'endroit de la cassure), ou à l'initiative de la source.

Au lieu de calculer une route avec un minimum de saut, l'objectif principal de CEDAR est de trouver un chemin stable pour garantir plus de bande passante. La figure suivante décrit le principe du protocole CEDAR.

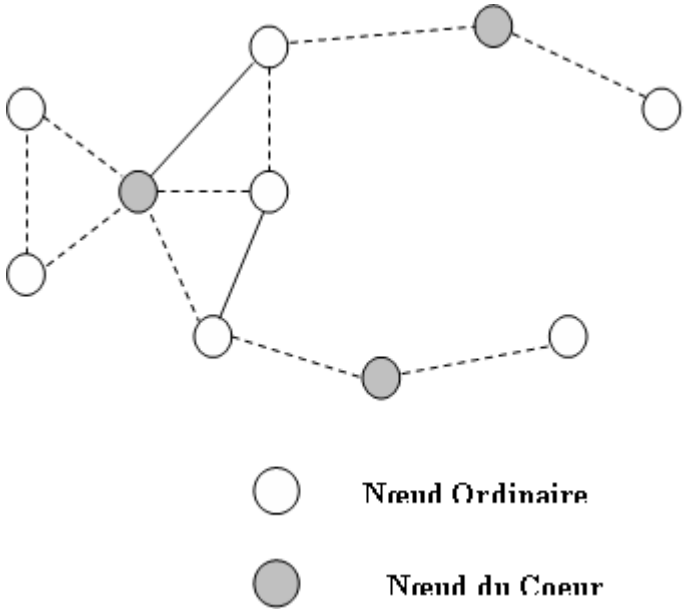


Figure16: principe du protocole CEDAR.

[36], [37]

- **QOLSR**

QOLSR est un protocole de routage proactif basé sur le protocole OLSR. Ce dernier propose d'avoir des messages de contrôle réduit et de minimiser l'inondation du trafic de contrôle. Pour réduire cette inondation, on utilise le concept des Relais Multipoints (MPR), un nœud

donné sélectionne ses MPRs parmi ses voisin à un saut (envoie de message HELLO) dont le lien est symétrique, de manière à couvrir tous les voisins se trouvant à 2 sauts. Pour offrir la QoS, QOLSR ajoute des extensions aux messages de contrôle durant la découverte des voisins. Il est pertinent d'intégrer des paramètres tels que le délai, la bande passante, le coût du lien, la perte de paquet. Les messages de contrôle TC (diffusés par les MPRs pour annoncer l'ensemble des nœuds qu'il peut atteindre) intègrent des informations de métrique additive. Une route avec un délai minimum peut être trouvé en utilisant l'algorithme Dijkstra, si on veut inclure la métrique de bande passante, alors s'il n'existe plus d'une route avec la Bande Passante maximale, la route avec le délai minimale sera choisie.

- **BRuiT**

Le principe de BRuIT est d'essayer d'apporter la QoS dans les réseaux Ad Hoc en limitant l'impact des interférences sur les communications entre les noeuds. Ce n'est pas un protocole de routage à proprement parler mais plutôt un protocole de réservation de bande passante s'appuyant sur un protocole de routage réactif basique. Son fonctionnement s'appuie sur deux phases (en soft state):

1- D'abord une phase de "découverte des voisins" qui leur permet de s'échanger leur état de charge respectif (e.g. la valeur totale de leur bande passante déjà réservée). Cette phase permet à chaque noeud de disposer de l'état de charge de son environnement radio.

2- Ensuite vient la phase de réservation de ressources qui est effectuée par l'ouverture d'une route sur laquelle les ressources nécessaires au flux seront réservées. Au niveau de chaque noeud, le contrôle d'admission va se faire en fonction de la bande passante disponible et de la charge du medium radio.

[38]

- **AODV avec qualité de service**

AODV se base sur un algorithme « à la demande » cela veut dire qu'il ne construit des routes entres noeuds que lorsqu'ils sont demandés par des noeuds sources. L'ajout dans les paquets de contrôle d'un champ 'route response' RREP associé au paramètre délai ou au paramètre bande passante, À la réception d'un message 'route request' RREQ ajouté également. Du fait que les informations suivantes sont ajoutées dans la table de routage: bande passante minimale, délai maximum, et la liste des sources qui ont demandé des garanties de délai ou de bande passante. Chaque mobile vérifie s'il est en mesure d'honorer le service demandé, avant de retransmettre le message. Si un nœud détecte que la QoS demandée n'est pas satisfaite alors il envoie un message à la source ayant initiée cette demande de QoS, pour l'informer.

Une métrique appelée BWER (Bandwidth Efficicency Ratio) est utilisée pour l'estimation de la bande passante résiduelle au niveau de chaque noeud. C'est la ration entre le nombre de paquets transmis et reçus. A un saut, ce protocole utilise les messages Hello pour collecter les informations de bande passante des mobiles dans son voisinage. La bande passante résiduelle d'un mobile est égale au minimum de la bande passante résiduelle estimée par ce mobile et de celle des mobiles dans son voisinage à un saut.

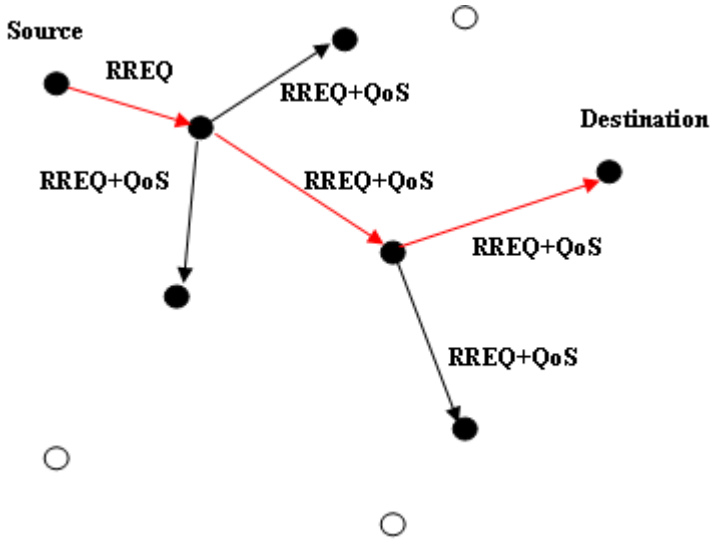


Figure17 : AODV route request.

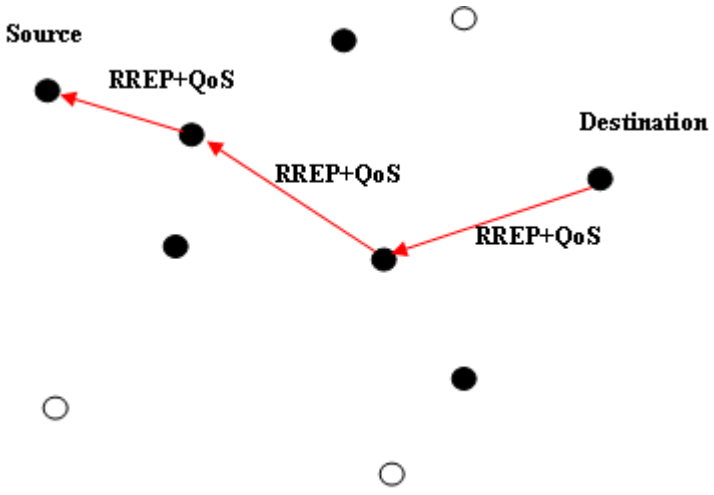


Figure18 : AODV route response.

[36]

3.3.4 Les protocoles de signalisation

Le but des protocoles de signalisation est de fournir un moyen de propagation des informations de contrôle à travers un réseau. Les informations transmises peuvent être de différentes natures. Il peut s'agir d'informations topologiques, de demandes de recherche de routes satisfaisant certaines contraintes ou encore de rapports sur l'état du réseau et la disponibilité des ressources. De ce fait, la conception d'un protocole de signalisation consistera à définir les données et la manière de les échanger pour la réalisation d'une tâche particulière.

- **INSIGNIA**

INSIGNIA fut le premier système de signalisation *in-band* permettant la QoS pour les MANET en 1998. Comme c'est un protocole qui repose sur la signalisation in-band, les messages de contrôle sont alors encapsulés comme une option dans les paquets de données IP, ce qui permet de réduire l'overhead généré par les messages de signalisation, et ce afin d'éviter de surcharger le réseau ; Contrairement à une signalisation out-band. INSIGNIA supporte deux types de services (temps réel et best effort). Il offre des algorithmes de réservation, restauration et d'adaptation rapides pour répondre aux changements de topologie du réseau et aux dégradations des liens.

INSIGNIA offre des garanties sur la base d'une granularité par flot aux applications adaptatives capables de modifier leur comportement en fonction de la quantité de bande passante qui leur est allouée. Ainsi, chaque application spécifie deux niveaux de qualités de service :

- Le niveau de base (TR: Temps Réel) : Permet de spécifier la bande passante minimale nécessaire au trafic c'est le niveau dégradé.

- Le niveau amélioré (BE : Best Effort) : Permet de spécifier le débit optimal à atteindre lorsque les ressources sont disponibles.

Description de l'algorithme de réservation de ressources:

La demande de réservation est effectuée lors de l'envoi du premier paquet de données avec le champ INSIGNIA Option (20 bits). Le bit Reservation Mode indiquant si ce paquet est en cours de réservation (REQ) ou s'il a déjà réservé des ressources (RES). Dans le cas REQ, le paquet est envoyé au module INSIGNIA qui va se charger de la suite du traitement. Le module INSIGNIA va alors définir si des ressources peuvent être allouées à ce paquet ou non. Si les ressources peuvent être allouées, le champ Service Type est mis à RT, sinon, il est descendu à BE. Dans les deux cas le paquet sera transmis au prochain nœud et la demande de réservation sera rafraîchie. Arrivé à la destination, le paquet contient donc soit la valeur RT soit la valeur BE La quantité de bande passante demandée par le paquet se trouve dans le champ Bandwidth Request, qui indique un minimum et un maximum pour cette valeur. En se basant sur cette information, le module INSIGNIA peut déterminer la quantité de bande passante à attribuer. Enfin le bit Bandwidth Indicator est un drapeau utilisé par le récepteur pour savoir si la demande de bande passante maximale a été satisfaite.

Le destinataire informe donc la source de l'état de la route en envoyant des rapports de QoS

(QoS Reporting), qui contiennent des statistiques sur la latence, le taux de perte et le débit, afin que la source puisse réguler son débit d'émission.

Lorsque le débit d'un flux ne peut plus être assuré, la destination est chargée d'avertir la source afin qu'elle prenne les mesures adéquates. Lorsqu'un flux transite à débit réduit dans le réseau, la disponibilité de nouvelles ressources est signalée à la destination qui, encore une fois, avertit la source explicitement. Ce qui permettra de réagir rapidement aux changements de topologie.

Il faut noter que dans certaines situations, des nœuds peuvent être des goulots d'étranglement pour diverses raisons. Cela signifie que tous les flux qu'ils vont transmettre vont être dégradés.

Il est important de rappeler que INSIGNIA est seulement un protocole de signalisation. On doit l'associer à un protocole de routage tel que AODV ou DSR qui va détecter les changements de topologie et mettre à jour les tables de routage. On a aussi besoin d'un module de contrôle de disponibilité des ressources ainsi que d'un mécanisme de contrôle d'admission qui va allouer les ressources. Les simulations montrent que ce mode de réservation est très rapide.

INSIGNIA possède néanmoins quelques lacunes :

- Un problème de passage à l'échelle. En effet, INSIGNIA suit le modèle Intserv et le problème du maintient de l'état des flux dans chaque nœud ne peut pas être évité.

- La gestion de la bande passante n'est pas très optimale car la réservation effectuée avant un goulot d'étranglement est perdue. Meme si ce gaspillage ne dure que pendant un temps limité, car la source va rapidement être informée du problème.

- INSIGNIA ne propose que deux classes de service: RT ou BE, une granularité plus fine pourrait permettre plus de flexibilité pour les applications.

- **Dynamic Qos / dRSVP**

Dans les protocoles usuels, les applications demandent une quantité précise de bande passante. Très souvent, le même niveau de service est conservé durant toute la transmission. Les auteurs de Dynamic QoS remettent en cause cet aspect statique de la réservation de bande passante. Lors de la demande de réservation, les applications ne spécifient pas une valeur précise mais un intervalle de valeurs. La borne inférieure représente le débit nécessaire au fonctionnement de l'application et la borne supérieure le débit maximal qui pourra être attaint.

Lors de la confirmation de réservation, le réseau indique à l'émetteur la quantité de bande passante qui lui a été effectivement allouée. D'autre part, on considère souvent qu'un lien a une capacité fixe mais sur le canal qu'est l'air, cette capacité est variable. Dans Dynamic QoS, la quantité de bande passante réservée par les applications peut être modifiée en cours de transmission, soit à l'initiative du réseau dans le cas où les ressources deviennent rares ou se libèrent, soit à l'initiative de l'application émettrice elle-même afin de libérer des ressources dans le réseau. Si cette approche est originale et peut permettre de diminuer la

probabilité de rejet des demandes de réservation, elle nécessite un accord entre les différents émetteurs s'il n'y a pas d'administration centralisée. Elle pourrait être très efficace dans des réseaux avec points d'accès.

[36]

3.4 Conclusion

La qualité de service est un aspect important de la communication dans les réseaux. Ce chapitre tente de faire le point sur cette notion, Après avoir regroupé quelques définitions relatives à la Qualité de Service, nous avons présenté les critères ou indicateurs généralement retenus pour caractériser les performances d'un réseau et assurer un service de bonne qualité. Ensuite, nous avons décrit quelques mécanismes et approches permettant d'implémenter la Qualité de Service dans les réseaux IP et on a terminé avec les travaux de QoS dans le contexte particulier des réseaux ad hoc.

Notre proposition d'un protocole de routage avec qualité de service est exposée dans le chapitre suivant.

Chapire04 :
Le Protocole HCAR (Hybrid with Congestion Avoidance Routing protocol)

Les réseaux mobiles ad hoc définissent une nouvelle approche pour la mise en œuvre des réseaux de communication. Ce nouveau paradigme est basé sur la capacité des terminaux à communiquer directement entre eux de proche en proche en traversant plusieurs sauts par le biais de liens sans fil, et par conséquent sans nécessité d'infrastructure réseau fixe pré-établie.

Ce nouvel environnement mobile offre beaucoup d'avantages par rapport à l'environnement habituel. Cependant de nouveaux problèmes peuvent apparaître, causés par les nouvelles caractéristiques du système : absence d'entité de contrôle, partage de ressources, hétérogénéité des noeuds, …etc. Ces spécifications compliquent d'avantage le déploiement de fonctionnalités avancées comme le routage, la qualité de service, la sécurité, … Afin de répondre aux besoins des applications/utilisateurs dans un réseau ad hoc, l'usage de solutions adaptées aux spécifications évoquées est indispensable.

Le problème de routage est loin d'être évident dans les réseaux mobiles et particulièrement dans les réseaux ad hoc. C'est ce sur quoi portent les travaux du groupe de travail MANET (Mobile Ad-hoc NETwork) de l'IETF.

Par ailleurs, les applications visées étant de plus en plus variées, beaucoup d'entre elles sont confrontées à des contraintes temporelles de bout-en-bout (ex. délai, gigue). Cependant, Les protocoles de routage dans les réseaux mobiles Ad Hoc n'ont pas été développés initialement pour tenir compte de contraintes temporelles et sont de ce fait inadaptés aux applications qui nécessitent le support de la Qualité de Service.

L'étude et la mise en œuvre des protocoles de routage intégrant de la qualité de service pour les MANET constituent une problématique d'actualité. Ce chapitre traite une solution qui permet de développer un protocole de routage pour garantir de la qualité de service dans les réseaux mobiles Ad Hoc, il s'agit du protocole HCAR : Hybrid with Congestion Avoidance Routing protocol.

Dans ce qui suit, nous présentons le principe de fonctionnement de notre protocole pour voir dans quelles mesures il répond à la problématique de la QoS dans les réseaux Ad Hoc.

4.1 Le protocole de routage proposé

Dans notre protocole que nous appelons HCAR (Hybrid with Congestion Avoidance Routing protocol), nous avons opté sur une prise en charge de la QoS à travers un contrôle de la congestion. En effet, notre solution passe par le contrôle de la congestion. Car, en l'absence de congestion, chaque flot de données peut utiliser le niveau de bande passante qu'il souhaite, aucun paquet ne sera perdu. Le délai est alors minimal et la gigue est nulle. Nous tendons à travers ce protocole HCAR de fournir une stratégie de routage, qui permet à la fois de prévenir la congestion, d'équilibrer la charge du réseau et de contrôler la consommation d'énergie.

Ce protocole est inspiré essentiellement du protocole AODV, qui est l'un des principaux protocoles au sein du groupe de recherche MANET, et qui a fait l'objet d'un grand nombre de recherches dû à toutes ses caractéristiques.

Comme nous avons indiqué dans le chapitre 2, les protocoles de routage proactifs essayent de maintenir les meilleurs chemins existants vers toutes les destinations possibles (qui peuvent

représenter l'ensemble de tous les nœuds du réseau) au niveau de chaque nœud du réseau. Les routes sont sauvegardées mêmes si elles ne sont pas utilisées. La sauvegarde permanente des chemins de routage, est assurée par un échange continu des messages de mise à jour des chemins, ce qui induit un contrôle excessif surtout dans le cas des réseaux de grande taille. Par contre, Les protocoles de routage réactifs, créent et maintiennent les routes selon les besoins. Lorsque le réseau a besoin d'une route, une procédure de découverte globale de routes est lancée, et cela dans le but d'obtenir une information. Le routage à la demande induit une lenteur à cause de la recherche des chemins, ce qui peut dégrader les performances des applications interactives (exemple les applications des bases de données distribuées). En outre, il est impossible de connaître au préalable la qualité du chemin (en termes de bande passante, délais,… etc.). Une telle connaissance est importante dans les applications multimédias.

Dans notre protocole de routage, nous avons adopté une solution intermédiaire, dans la mesure où l'établissement d'une route se fait uniquement en cas de besoin (l'aspect réactif), mais une fois une route est établie entre une source et une destination, cette route reste valide (tant qu'il n'y a pas une mobilité ou un lien brisé d'un nœud intermédiaire) même s'il n'y a plus une communication entre la source et la destination. S'il y a une mobilité, on n'invalide que la partie de route affectée par cette mobilité (si la mobilité affecte tout le chemin alors on invalide la route sans le maintenir). En outre, chaque nœud maintient dynamiquement une liste de ses voisins, et une liste de destinations qu'il peut atteindre directement par chacun de ses voisins (l'aspect proactif).

Le protocole HCAR a pour objectifs de :

- Diminuer le nombre de messages de signalisation ;
- Optimiser le temps de découverte de la route ;
- Introduire une métrique plus appropriée que la distance (nombre de sauts) ;
- Faire face aux changements fréquents de la topologie due à la mobilité des nœuds ;

4.2 Fonctionnalités de HCAR

Comme nous avons déjà indiqué, le protocole HCAR intègre également la prise en charge de la qualité de service, par l'équilibrage de la charge du réseau, la prévention de la congestion, et la rationalisation de la consommation d'énergie.

Lorsque un nœud A veut communiquer avec un nœud B, le nœud A vérifie, tout d'abord que le nœud B n'est pas dans la table des destinations éloignées ELG_DST. Si tel est le cas, le nœud A se met en attente jusqu'à le rapprochement du nœud B. Sinon, le nœud A cherche dans sa table de routage s'il existe une route valide ou active pour la destination qu'il souhaite atteindre, s'il n'en existe aucune, il cherche la destination dans son voisinage (chaque nœud connaît ses voisins à deux sauts). Si B n'est pas dans le voisinage de A, alors A génère un message de demande de construction de route vers la destination B. Ce message contient deux champs particuliers ACTIVE_COUNT et ROUTE_COUNT qui représentent, respectivement, le nombre de noeuds qui participent à au moins une autre route active et la somme des nombres de routes actives dans chaque nœud constituant un chemin, ils servent à calculer la charge moyenne des nœuds d'un chemin, AVR_LOAD (AVR_LOAD= ROUTE_COUNT/ ACTIVE_COUNT). A la réception du message de demande de route chaque nœud mettre à jour ces champs, puis achemine le message à ses voisins, jusqu'à ce

que celle-ci atteigne B (ou un nœud intermédiaire qui contient un chemin valide vers B). Celui-ci envoie alors une réponse, qui confirme à tous les nœuds intermédiaires, et à A, que la route est bien valide. Lorsque le nœud A reçoit plusieurs réponses de route, il choisit celle avec la valeur de la charge moyenne des noeuds la plus petite (c.à.d le chemin le moins chargé), et non plus la route avec un minimum de sauts entre la source et la destination.

Cette nouvelle métrique (AVR_LOAD : Average Load) permet de limiter la surcharge de certains nœuds du réseau par l'équilibrage de la charge du réseau, ce qui permet d'éviter la congestion. Elle permet également d'assurer une meilleure distribution de l'énergie dissipée sur le réseau. En effet, l'utilisation massive d'un même chemin peut amener certains noeuds à leur extinction prématurée.

Comme le fait AODV, HCAR maintient les chemins d'une façon distribuée en gardant une table de routage au niveau de chaque noeud de transit appartenant au chemin cherché. Une entrée de la table de routage contient essentiellement :

- L'adresse de la destination,
- Le noeud suivant,
- Le nombre de noeuds qui participent à au moins une autre route active,
- la somme des nombres de routes actives dans chaque nœud constituant le chemin,
- la moyenne de charge des nœuds du chemin,
- Le numéro de séquence de destination.

4.3 Paquets de contrôle

Pour mettre en œuvre le comportement décrit ci-dessus, le protocole HCAR utilise principalement quatre types de messages de signalisation :

- **Hello**

Ces messages sont émis régulièrement (diffusé chaque 1s) par chaque nœud, à l'intention de ses voisins à deux saut (le paramètre Time To Live 'TTL' = 2), pour leur signaler sa présence. Ils servent essentiellement à vérifier et maintenir la connectivité. En effet, l'émission régulière de ces informations permet de rendre compte de l'évolution du réseau, due à l'apparition ou à la disparition de routes, ou à la mobilité des nœuds. Ils contiennent l'adresse IP de l'émetteur de message, son numéro de séquence et le nombre de routes actives auxquelles participe ce nœud. Chaque nœud écoute les paquets transmis par ses voisins, si pendant un laps de temps, un nœud ne reçoit rien de la part d'un ou de plusieurs des ses voisins, il considère que le lien est défaillant et envoie un message d'erreur pour invalider la route (dans le cas ou ce voisin est un nœud participant à une route active ou valide).

Ces messages sont utilisés également pour détecter le rapprochement des nœuds éloignés. En effet, lors de la détection d'un nouveau voisin, on lui inscrit dans la table des voisins, puis on vérifie, sur la table des destinations éloignées si ce nœud était éloigné ou non.

@source	Num. seq.Source	ROUTE_COUNT

Figure 19 : format d'un message HELLO.

NB : le protocole HCAR utilise les numéros de séquences, comme dans le protocole AODV, pour éviter les problèmes classiques de boucle de routage et de comptage à l'infini.

- **RREQ (Route Request)**

Une demande de route par un nœud consiste à émettre sur une adresse de type broadcast (IP_BROADCAST) un message RREQ. Avant de l'envoyer, le nœud origine (source) sauvegarde l'identifiant du message et l'adresse IP de façon à ne pas traiter le message dans le cas ou un voisin le lui renverrait. Une fois la demande de route est effectuée, le nœud demandeur se met en attente de réponse.

La figure suivante représente le format général d'un message de demande de route :

@source	Num. seq. Source	Broadcast id	@destination	Num. seq. Destination	ACTIVE_COUNT
ROUTE_COUNT					
AVR_LOAD					

Figure 20 : format d'un message RREQ.

La recherche d'une route est réalisée par la diffusion des messages RREQ au travers du réseau, cette diffusion engendre une quantité importante de message de contrôle, ce qui peut être très coûteuse.

Pour minimiser les messages de contrôle sur le réseau et limiter ainsi la consommation des ressources limitées du réseau ad hoc (bande passante, énergie…etc.), le protocole HCAR effectue une recherche de route progressive (recherche dichotomique). Pour ce faire, le protocole HCAR divise le réseau en deux zones (NETWORK_DIAMETER / 2), la recherche d'une route est effectuée tout d'abord sur la première zone qui est divisée à son tour en trois zones.

L'émetteur va donc limiter la diffusion du RREQ sur la zone A (Figure 21), si la destination est dans cette zone alors le processus de découverte d'une route est terminé avec succès, sinon l'émetteur élargit la recherche sur la zone B, s'il ne reçoit pas une réponse (RREP) de la part de la destination, il continu la recherche de route avec un nombre plus grand de saut,

pour atteindre la zone C (TTL= NETWORK_DIAMETER / 2). Si aucune réponse ne revient au nœud source après une certaine durée d'attente, alors le nœud source diffuse le message de demande de route sur tout le réseaux (TTL= NETWORK_DIAMETER) et se met en attente de réponse.

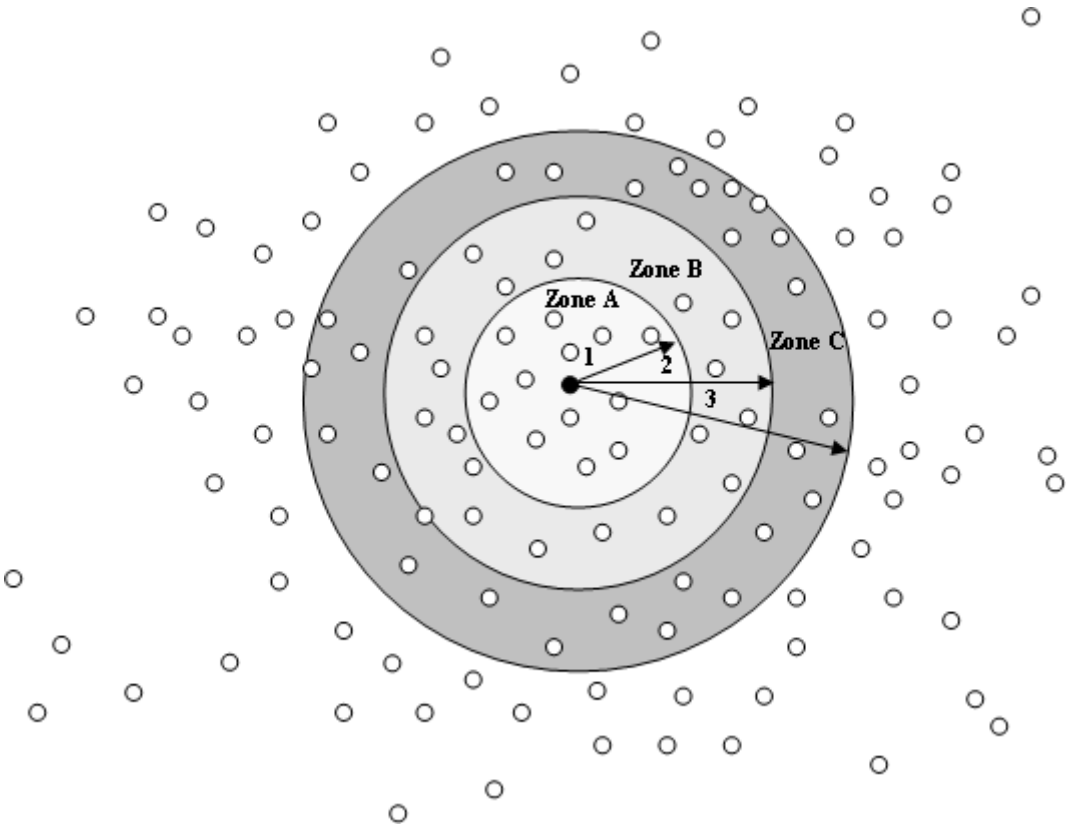


Figure 21 : recherche dichotomique dans le protocole HCAR.

- **RREP (Route Reply)**

Lorsqu'un nœud reçoit un message de demande de route RREQ, il met à jour sa table de routage, et notamment sa liste des précurseurs pour la route demandée, et le champ qui représente le nombre de nœud participant à d'autres routes actives, ensuite il génère un message de réponse RREP si :

- Il est lui-même le destinataire du message de demande de route RREQ,
- Il possède dans sa table de routage une route valide pour la destination,
- La destination demandée est dans le voisinage (à deux saut) du ce nœud.

Le format général d'un RREP est représenté par la figure ci-dessous.

@source	@destination	Num. seq. Destination	ACTIVE_COUNT	ROUTE_COUNT
AVR_LOAD				

Figure 22 : format d'un message RREP.

- **RERR (Route Error)**

Ces messages sont générés lorsqu'un nœud détecte qu'une route est brisée. Par exemple, si un nœud n'a pas reçu de message Hello de l'un de ses voisins pendant un certain temps, il doit considérer que ce voisin a disparu, rechercher quelles entrées de sa table de routage utilisent ce voisin, marquer ces entrées comme correspondant à des routes détruites, avertir les sources de ces routes. En règle générale, un nœud envoi un message d'erreur si :

- Il a détecté un lien brisé pour le saut suivant sur une route valide dans sa table de routage,
- Il a reçu un paquet destiné à un nœud pour lequel il n'existe pas de route active dans sa table de routage,
- Il a reçu un message RERR de la part d'un voisin pour une ou plusieurs routes actives.

La figure suivante illustre le principe de fonctionnement du protocole HCAR.

Un nœud qui participe à x routes actives.

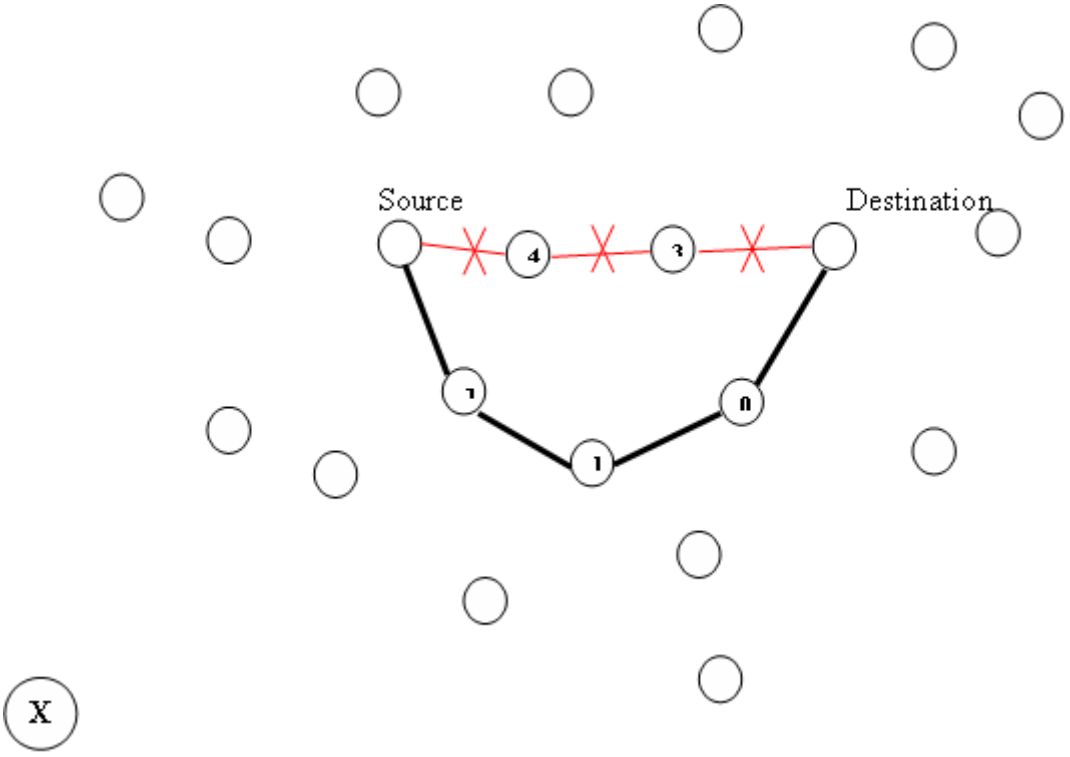


Figure 23 : principe du protocole HCAR.

Si nous utilisons le protocole de routage AODV, alors le chemin établi entre la source et la destination est celui désigné par la couleur rouge, le chemin avec un minimum de sauts entre la source et la destination, qu'il n'est pas le cas avec l'utilisation du protocole de routage HCAR. En effet, ce dernier privilège des routes avec les nœuds moins chargés. Par conséquent, le chemin emprunté est celui désigné par la couleur noir.

4.4 Mécanisme de gestion des nœuds éloignés

Les protocoles de routages présentés dans les chapitres précédents, best effort ou avec qualité de service, n'adoptent pas un mécanisme de gestion des nœuds éloignés. Cependant un tel mécanisme est important et à une influence directe sur la qualité de service dans les MANET.

4.4.1 Motivation

Soit le réseau mobile ad hoc suivant, constitué de 8 nœuds mobiles.

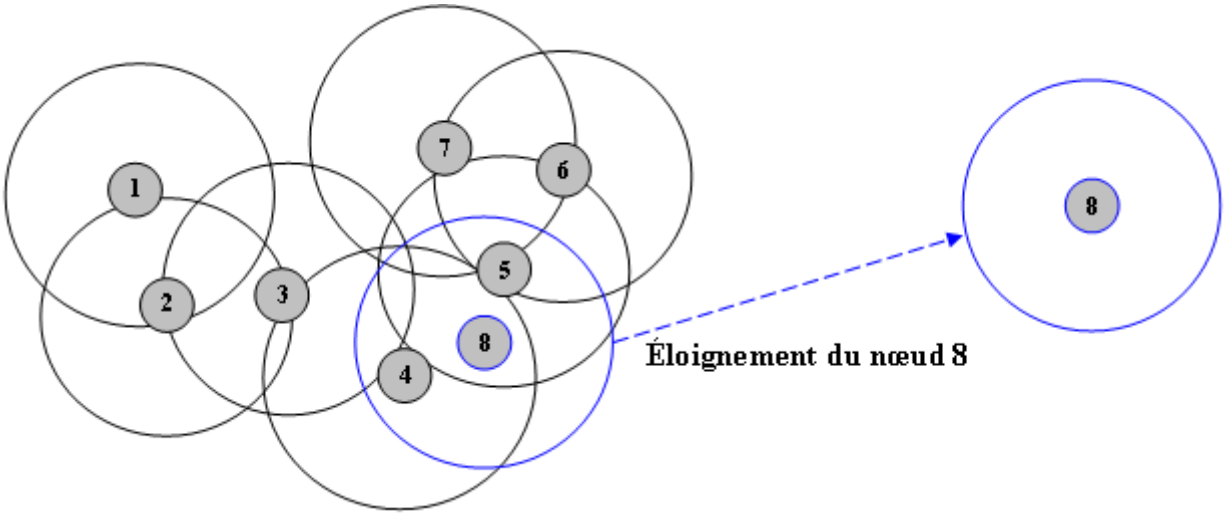


Figure 24 : exemple d'un nœud éloigné.

Pour mettre en exergue l'importance de mécanisme de gestion des nœuds éloignés, on va étudier le comportement du protocole AODV face à l'éloignement des nœuds.

Afin d'établir une route entre une source et une destination, le protocole AODV diffuse la requête de demande de route (RREQ) et attendra une période RREP_WAIT_TIMEOUT, si une réponse est reçue alors l'opération de découverte de route est terminée, sinon il rediffuse le RREQ et attend une période plus grand, si aucune réponse n'est reçu il continuer la rediffusion du RREQ jusqu'à un nombre maximum de tentatives RREQ_RRTRIES (03 tentatives), si après RREQ_RETRIES tentatives d'établissement de route, il n'y a aucune réponse alors le processus est abandonné et un message d'erreur est signalé à l'application.

Après une certaine période d'attente (10 sec), l'application demande la route et par conséquent l'opération de découverte de route est initiée, la non découverte de route est due généralement à l'éloignement des nœuds.

Si le nœud 1, par exemple, veut communiquer avec le nœud 8, alors une route est établie entre ces deux nœuds. Cependant, si durant la communication le nœud 8 effectue une mobilité et sorte de la portée des autres nœuds, alors le nœud source tente de chercher une nouvelle route.

Le nœud source échoue de trouver une nouvelle route après RREQ_RETRIES tentative, et attend une durée de 10 sec avant que le processus de découverte de route soit initié.

Problèmes

- Si d'autres nœuds tentent de communiquer avec le nœud 8, ils vont générer, inutilement, une grande masse des messages de contrôles qui dégrade considérablement les performances du réseau.

- Supposons que le nœud 8 se rapproche durant la période d'attente du nœud source (par exemple après 2 sec d'attente), le nœud source ne détecte pas le rapprochement du nœud éloigné. Par conséquent, l'établissement d'une nouvelle route se fait uniquement après l'expiration de la durée d'attente, ce qui augmente la durée de découverte d'une route (figure 25). Pour remédier à ce problème, nous avons modifié le code source du protocole AODV de telle sorte que ce dernier ne fasse aucun test sur le nombre de tentatives de diffusion de RREQ. Une version modifiée d 'AODV, appelée AODV-MC est ainsi définie (figure 26) [21]. Cependant, si le nœud éloigné ne se rapproche pas durant la période d'attente, alors le protocole AODV-MC continue de générer, inutilement, des messages de demande de route (RREQ).

D' où la nécessité d'un mécanisme de gestion des nœuds éloignés.

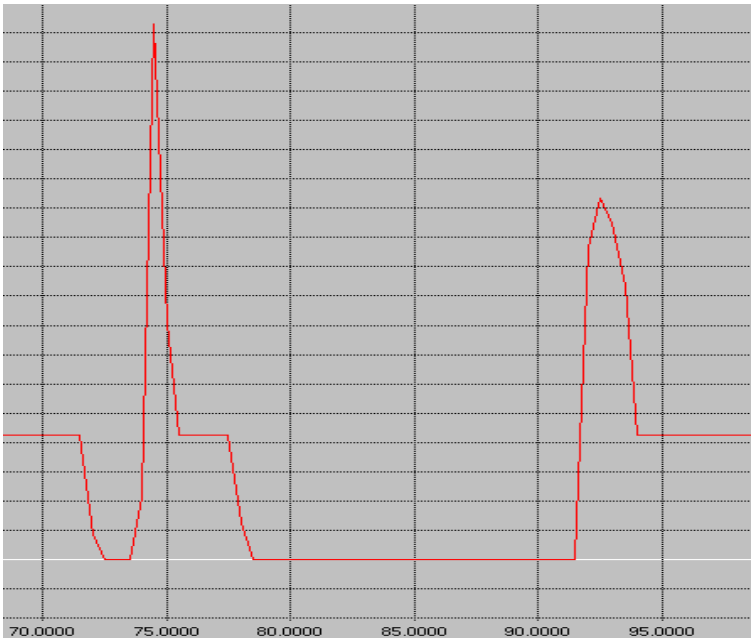
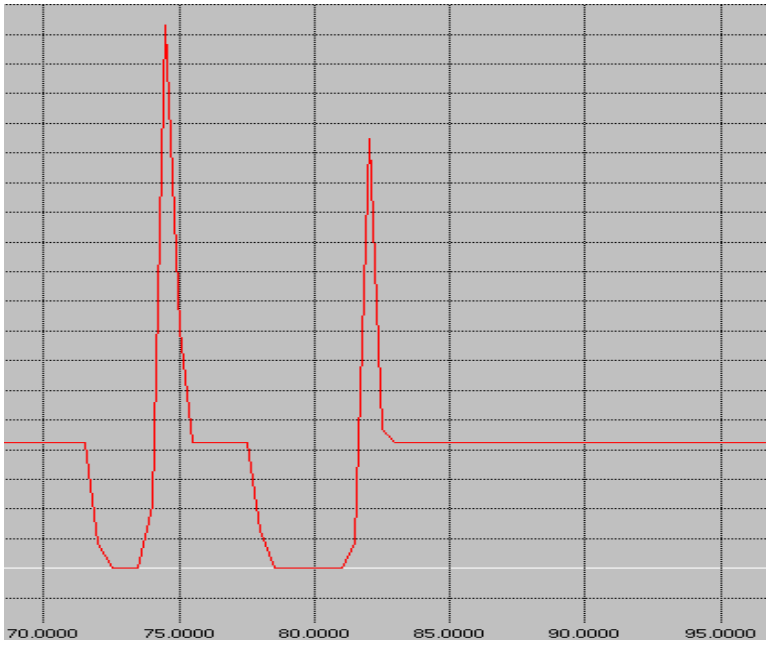


Figure 25: débit des paquets reçus avec AODV.



Figue 26: débit des paquets reçus avec AODV-MC.

Pour mettre en œuvre un tel mécanisme de gestion des destinations éloignées, nous avons défini une table des destinations éloignées au niveau du chaque agent de routage (dans la classe HCAR.h), la structure de cette table est comme suite :

```
Class ELG_DST {
        Friend class HCAR;
        Public:
        ELG_DST (nsaddr_t i){ dst=I;}
        Protected:
        LIST_ENTRY (ELG_DST) link;
        nsaddr_t dst;           // la destination éloignée.
};

LIST_HEAD (hcar_edst, ELG_DST);   // l'entête de la table.

hcar_edst edsthead; // la liste de destinations éloignées.
```

Pour la gestion de la table des destinations éloignées, nous avons implémenté trois fonctions :

```
Void  dst_insert (nsaddr_t dst) ;   // insérer la destination éloignée dans la table.
Void  dst_delete (nsaddr_t dst) ;  // supprimer la destination éloignée de la table.
Bool dst_lookup (nsaddr_t dst) ;  // vérifier si la destination 'dst' est dans la table.
```

En plus de cette table, le protocole HCAR utilise trois types de message de contrôle pour la gestion de destinations éloignées: URDST (Unreachable Destination), WNTD (Wanted), DAPR (Destination Approched). Pour chaque type de message, nous avons défini deux fonctions : send_URDST(), recv_URDST(), send_WNTD(), recv_WNTD(), send_DAPR(), recv_DAPR().

- **URDST (Unreachable Destination)**

Ce message est diffusé par le nœud demandeur de la route après un échec d'établissement d'une route entre la source et la destination au bout d'une seule tentative (une tentative avec TTL=NETWOK_DIAMETER). Ce message sert, d'une part, à ajouter la destination éloignée dans la table de destinations éloignées (ELG_DST), d'autre part, il joue le rôle d'une requête de route, pour traiter le cas où la destination se rapproche au moment de la propagation de ce message.

- **WNTD (Wanted)**

Envoyé par les voisins de destination éloignée, lorsque cette dernière se rapproche. En effet, lorsque un nœud reçoit un message HELLO, il vérifie si l'émetteur est un nouveau voisin. S'il est le cas, il l'inscrit dans sa table de voisins (HCAR_Neighbor), puis consulte sa table de destinations éloignées, ELG_DST, pour déterminer si ce nouveau voisin était éloigné ou non. S'il était éloigné, on lui envoi un message WNTD, pour leur indiquer qu'il est recherché par d'autres noeuds.

- **DAPR (Destination Approched)**

Ce message est diffusé par le nœud destination suite à la réception de message WNTD,

```
Void recv_WNTD(Packet *p){
        Nsaddr_t dst=index;
        Send_DAPR(dst);
}
```

Il contient l'adresse IP de cette destination et permet principalement de:

- Enlever cette destination de la table des destinations éloignées,
- Donner l'autorisation aux nœuds demandeurs de cette destination pour lancer le processus de découverte de route.

4.5 Conclusion

Le routage est nécessaire pour rendre les réseaux ad hoc fonctionnels, mais on peut aussi penser de rajouter d'autres services à la couche réseau pour améliorer la performance de MANET et permettre une meilleure exploitation des ressources limitées. Il peut en effet être souhaitable de faire communiquer deux nœuds entre eux de sorte que le flux de données échangées entre ces nœuds possède certaines propriétés, telles qu'une perte de données bornée, un délai entre émission et réception que l'on maîtrise . . . etc. En outre, certain type d'applications exigent certaine QoS, par exemple, pour les applications temps réel, comme la voix et la vidéo, le délai de bout en bout d'un paquet doit être limité, autrement le paquet est inutile.

Le routage étant un domaine où la Qualité de Service est peu intégrée et faisant également l'objet de travaux. Cependant, les solutions actuelles ne sont pas encore pleinement satisfaisantes et un travail très important reste donc à faire dans ce domaine.
Dans ce chapitre, nous avons proposé une solution au problème de routage avec QoS basée sur l'équilibrage de la charge du trafic circulant sur le réseau Ad hoc, ce qui a permis d'éviter la congestion et de contrôler la consommation d'énergie.

Après avoir détaillé le principe de fonctionnement de notre protocole, il convient de procéder à une étude comparative avec le protocole AODV pour en dégager quelques concepts de la QoS dans les réseaux Ad hoc. Une évaluation comparative des performances de ces protocoles en fonction de la densité du réseau (nombre des noeuds) et du mobilité est fournie dans le chapitre suivant.

Chapire05 :
Simulations et résultats

Pour tester un protocole de routage on a recours souvent à la simulation. En effet, il serait très coûteux voire impossible de mettre en place un réseau à des fins de tests pour certains critères.
Dans ce chapitre on présente une étude comparative des protocoles AODV et HCAR au moyen du simulateur NS2. Nous commençons tout d'abord par présenter l'outil de simulation NS2 et son architecture. Plusieurs modèles de propagation radio et des modèles de mobilité supportés par NS sont ensuite listés. Nous décrivons par la suite la structure des Nœuds Mobiles sous NS2 avant d'illustrer le processus d'installation, configuration, utilisation et modification de NS2. Par la suite, on donnera les formats des fichiers de trace générée par NS2, en plus de la Visualisation des résultats sous NS2. Puis on passe à la description de Scénario de la simulation d'un réseau mobile. Des simulations aussi sont faites montrent une comparaison en tant que : délai de découverte d'une route, la quantité du trafic de contrôle générée et le taux de paquets reçus (PDR).

5.1 Le simulateur NS2

5.1.1 Introduction

NS-2 est un outil logiciel de simulation libre à code source ouvert et à évènements discrets permettant l'étude, la conception et la gestion des protocoles pour les réseaux informatiques. Il a été développé à partir de méthodes de conception orientées objets dans le projet VINT associant plusieurs centres de recherche comme AT&T research institute à Berckeley (ACIRI), Xerox PARC et Sun Microsystems. NS-2 contient des librairies pour la génération des fonctions (topologie, trafic, routage, MAC, LLC,…) et des outils graphiques pour faciliter l'interprétation (Xgraph) et la visualisation (network animator NAM) des résultats.

Le simulateur NS-2 dans sa version actuelle est particulièrement bien adapté aux réseaux à commutation de paquets et à la réalisation de simulations de réseaux de petite taille. Il contient les fonctionnalités nécessaires pour l'étude des méthodes d'accès au médium, des algorithmes de routage point à point ou multipoint, des protocoles de transport, de session, de réservation de ressources, des protocoles d'application comme *HTTP* (*HyperText Transfer Protocol*). Cependant, il ne contient pas toutes les fonctionnalités nécessaires de la couche physique telles que les modèles de propagation (seuls les modèles de propagation dans l'air sont prévus, mais pas le modèle de propagation aquatique) et les supports de transmission (seuls les liens filaires et les liens radio sont prévus). Le Tableau ci-dessous donne les principaux composants disponibles pour chaque couche et par catégorie disponible dans NS-2. L'ensemble de ces capacités utilisées conjointement ont permis l'étude des différents mécanismes au niveau de différentes couches de l'architecture réseau et font de NS-2 un standard reconnu par la communauté scientifique pour échanger les résultats et scripts de simulation entre les chercheurs.

Application	Web, Ftp, Telnet, générateur de trafic (CBR,….)
Couche Transport	TCP, UDP, RTP, SRM
Couche Réseau	Routage Statique et dynamique unicast et multicast (vecteur de distance, DSR, AODV)
Couche liaison de Données	CSMA/CD, CSMA/CA, Liaisons point à point, MAC 802.11,…
Couche Physique	Médium Filaire, Sans Fil et Satellite (Trafic, topologie du réseau, mobilité, model de propagation).
Gestion de la file d'attente	RED, DropTail, Token bucket, etc
Discipline de service	CBQ, SFQ, DRR, Fair queueing

NS2 est écrit en C++ et utilise le langage OTCL (Object Tools Command Language) dérivé de TCL. A travers OTCL, l'utilisateur décrit les conditions de la simulation : la topologie du réseau, les caractéristiques des liens physiques, les protocoles utilisés, les communications qui ont lieu. La simulation doit d'abord être saisie sous forme de fichier que NS va utiliser pour produire un fichier contenant les résultats. Mais l'utilisation de l'Otcl permet aussi à l'utilisateur de créer ses propres procédures (par exemples il souhaite enregistrer dans un fichier l'évolution d'une variable caractéristique du réseau au cours du temps).

[39], [42]

5.1.2 Architecture et Implémentation

L'architecture réseau de NS2 est fortement basée sur le modèle des couches OSI, il s'agit de la décomposition de la pile réseau en couches.

Au plus bas niveau de ns2, il y a six classes qui définissent l'ensemble de la structure du Programme et fournissent les méthodes élémentaires, il s'agit des classes TCL**,** TclObject, TclClass, TclCommand, EmbeddedTcl, InstVar. Elles définissent entre autres les méthodes utilisées par C++ pour accèder à l'interpréteur, la hiérarchie, les principales commandes de haut niveau et les Méthodes d'accés aux variables C++ et Otcl. La simulation est configurée, contrôlée et gérée à l'aide des interfaces fournies par la classe OTclSimulator, cette classe fournit des procédures pour créer et gérer la topologie, initialiser le format des paquets et choisir le planificateur d'évènements, elle stocke intérieurement des références à chaque élément de la topologie, un script donc devra toujours commencer par l'instanciation d'une variable de cette classe. L'utilisateur crée ensuite la topologie à travers OTcl en utilisant les classes Node et Link, composants essentiels de la topologie. Ces éléments sont décrits dans la sous section suivante.

5.1.2.1 Composants de la topologie

La topologie NS2 est essentiellement composée de nœuds et de liens :

- **Les Noeuds**

La définition des nœuds se fait dans un premier temps à travers l'instance de Simulator puis à travers l'instance de la classe Node, la fonction d'un nœud est de recevoir des paquets, les examiner et les mapper à ses interfaces sortantes appropriées. Cette classes est composée d'un classificateur et de méthodes pour configurer un nœud, les méthodes proposées sont des fonctions de contrôle, de gestion d'adresse et de port, de gestion d'agents et de repérage des voisins, le classificateur est la partie du nœud qui traite chaque segment des paquets reçus, il en existe donc plusieurs, chacun étant spécifique au champs examiné.

- **Les liens**

Les liens constituent la deuxième partie de la topologie, les liens entre les nœuds sont définit dans la classe Link et SimpleLink plus précisément lorsqu'il s'agit de relier deux nœuds. Plusieurs types de liassions sont supportés, comme le point à point, le broadcast ou les liaisons sans fil pour la mobilité.

- **La gestion des files d'attente**

La gestion des files d'attente et la simulation des délais sur les liens sont implémentés dans les classes Queue et LinkDelay respectivement. Les files d'attente actuellement disponible dans NS sont:

- FIFO ;
- RED buffer management ;
- CBQ (priorité et circulaire) ; …….etc.

Pour simuler un quelconque délai dans la réception ou l'émission d'un paquet, la file d'attente correspondante est simplement bloquée.

- **Les agents**

L'agent est un autre composant d'un nœud. Il modélise les constructeurs et les consommateurs de paquets IP. La classe agent fournit des méthodes utiles au développement de la couche transport et à d'autres protocoles du plan de signalisation ou de gestion. Cette classe est à la fois dans l'interpréteur et dans le simulateur. C'est la classe de base pour définir des nouveaux protocoles dans NS. Elle fournit l'adresse locale et de destination, les fonctions pour générer les paquets, l'interface à la classe application. Actuellement NS comporte de nombreux agents citons: UDP, protocoles de routage, différentes versions de TCP, RTP, …etc.

[40], [41]

5.1.3 Les différents modèles de propagation radio sous NS2

NS2 permet également de choisir parmi les modèles de propagation suivants, qui influeront en particulier sur la manière dont seront atténués les signaux en fonction de la distance :

- **Le modèle de propagation en espace libre (Free space model)**

Ce modèle considère le cas idéal où il y a un seul chemin de propagation entre l'émetteur et le récepteur et qu'il est en vue directe. L'équation suivante permet de calculer la puissance du signal reçu en environnement libre à une distance d de l'émetteur.

$$\Pr(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L}$$

Où Pt est la puissance d'émission, Gt et Gr les gains respectifs des antennes de l'émetteur et du récepteur. L (avec L >= 1) est la perte du système, et λ est la longueur d'onde. Ce modèle de propagation représente les zones de communication comme un cercle autour de l'émetteur. Si un récepteur est dans ce cercle il reçoit tous les paquets, s'il est en dehors il n'en reçoit aucun.

- **Le modèle de propagation utilisant deux rayons (Two-ray ground reflection model):**

En environnement réel, il est en fait peu probable que le seul chemin de propagation soit le chemin direct. Le modèle two-ray ground considère donc à la fois le chemin direct et une réflexion sur le sol. Ce modèle donne des résultats plus justes que le modèle de propagation en espace libre quand la distance est assez grande. La puissance reçue à une distance d est calculée de la manière suivante :

$$\Pr(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L}$$

Où ht et hr sont les hauteurs des antennes de transmission et de réception. Afin que NS soit cohérent avec le modèle de propagation en espace libre, L a été ajouté à l'équation.
Cette équation présente une décroissance de la puissance reçue en fonction de la distance plus rapide que l'équation précédente. Cependant, pour des distances courtes, le modèle à deux rayons ne donne pas de bons résultats. Le modèle de propagation en espace libre est donc utilisé à la place de celui-ci quand d est suffisamment petit.

- **Le modèle Shadowing**

Les modèles de propagation en espace libre ou utilisant deux rayons calculent de manière déterministe la puissance reçue en fonction de la distance. Ils représentent tous deux la zone de communication comme un cercle idéal. Dans la réalité, la puissance reçue à une certaine distance varie de manière aléatoire, à cause des effets de propagation par des chemins multiples. En fait, les deux modèles précédents calculent la puissance moyenne reçue à une distance d.
Le modèle "shadowing" est composé de deux parties. La première est le modèle d'atténuation en fonction de la distance, qui calcule la puissance moyenne reçue à une distance d, notée Pr

(d). Il utilise une distance courte comme référence, notée d0. Pr (d) est calculé relativement à Pr (d0) de la manière suivante :

$$\frac{P_r(d_0)}{P_r(d)} = \left(\frac{d}{d_0}\right)^{\beta}$$

β est appelé l'exposant d'atténuation en fonction de la distance, et est généralement déterminé de façon empirique par des mesures en environnement réel. Les grandes valeurs de β correspondent à une obstruction plus forte et donc à une décroissance plus rapide de la puissance reçue en fonction de la distance.
Le shadowing model étend le cercle idéal de communication à un modèle statistique plus riche ; les nœuds ne peuvent communiquer qu'avec une certaine probabilité lorsqu'ils sont vers la limite de portée.

5.1.4 Les modèles de mobilité sous NS2

Puisque les réseaux ad hoc (MANET) sont souvent analysés par des simulations, leurs résultats d'exécution dépendent légèrement des paramètres de réseau de simulation. Ainsi, l'évaluation d'un protocole de routage ad hoc dépend de choisir soigneusement un modèle de mobilité pour illustrer les mouvements réalistes des utilisateurs.
Les modèles de mobilité d'entité représentent les nœuds mobiles dont les mouvements sont indépendant l'un de l'autre. D'autre part, les modèles de mobilité de groupe représentent les nœuds mobiles dont les mouvements dépendent l'un de l'autre et ils tendent à être plus réalistes dans les applications impliquant la communication de groupe.

- **Le modèle de mobilité random waypoint (RWP)**

Dans ce modèle la mobilité des nœuds est typiquement aléatoire et tous les nœuds sont distribués uniformément dans l'espace de simulation. En effet il consiste en :
• Le placement d'un certain nombre de mobiles dans une zone carrée de laquelle ils ne peuvent sortir.
• L'affectation d'une position, d'une vitesse et d'une destination initiale à chaque mobile.
• Le déroulement proprement dit de la simulation, où à chaque fois que les mobiles atteignent leur destination dans le carré, ils repartent vers une autre destination choisie aléatoirement après un éventuel temps de pause.
Du fait de la simplicité de ce modèle, il n'est pas toujours adapté pour décrire des comportements de mobilité complexes.

- **Le modèle Random Walk**

Ce modèle est développé pour imiter un mouvement imprévisible. Un nœud mobile dans ce modèle se déplace de son endroit courant à un nouvel endroit en choisissant aléatoirement une direction et une vitesse suivant lesquelles il se déplace. La nouvelles vitesse et direction toutes les deux sont choisies dans des gammes prédéfinies, [speedmin, speedmax] et [0, 2π] respectivement. Un nœud mobile atteignant la frontière de simulation, rebonds avec l'angle déterminé par la direction entrante et puis continue le long du nouveau chemin.

- **Modèle aléatoire de direction (random direction model)**

Il vient comme une modification sur le modèle de RWP. Dans RWP, la probabilité d'un nœud mobile de choisir une nouvelle destination située au centre du la zone de simulation ou une destination qui nécessite un déplacement par le centre est haute. Ce modèle essaye d'alléger ce comportement, fournissant un nombre constant de voisins dans toute la simulation. Les nœuds mobiles choisissent une direction aléatoire suivant laquelle ils se déplacent en tant que modèle de mobilité de random walk, où ils se déplacent vers la frontière de la simulation dans cette direction. Une fois que la frontière est atteinte, le nœud mobile fait une pause pendant le temps indiqué, choisit une autre direction angulaire entre (0 et 180) continue alors le processus.

[15]

5.1.5 Les Noeuds Mobiles sous NS2

Dans un premier temps, la mobilité a été introduite dans NS-2 par les chercheurs de l'université Cartegie Mellon de Pittsburgh (CMU) dans la volonté de simuler des réseaux ad hoc.

L'apport de la mobilité passe par l'ajout d'un nouveau type de nœuds définis dans la classe *MobileNode*, qui ne sont pas connectés entre eux. Les caractéristiques de la mobilité telles que le mouvement des nœuds, les mises à jour de localisation ou les limites de la topologie sont implémentées en C++. Par contre, les composants réseaux comme le nœud mobile lui-même (classificateur, couche liaison…) sont implémentés en OTcl.

Comme l'objectif était de simuler des réseaux entièrement mobiles, il a fallu mettre en place des protocoles de routage. Actuellement, il y a quatre protocoles de routage mis en œuvre dans NS-2 : DSDV, DSR, TORA, AODV.

Lorsqu'un nœud mobile est crée dans une simulation, le simulateur crée un objet *MobileNode*, un agent de routage et la pile réseau. Ensuite ces composants sont interconnectés et la pile est connectée au canal. Ces composants sont illustrés dans la figure 27.

Une caractéristique forte des nœuds mobiles est bien sûr de pouvoir se déplacer. NS-2 a été conçu pour exécuter des déplacements en 3D, mais actuellement la troisième dimension n'est pas utilisée (Z=0). Il existe deux mécanismes pour l'utilisateur pour donner du mouvement aux nœuds mobiles :

- Indiquer le point d'origine, la destination et la vitesse explicitement pour chaque nœud mobile. Les mises à jour sont déclenchées chaque fois que l'on exige la position du nœud mobile à un moment donné. Cette solution est plutôt faite pour des petites simulations.

- Générer des mouvements aléatoires : à l'appel d'une procédure, le nœud mobile démarre à partir d'une position aléatoire et exécute des déplacements. Le nœud mobile exécute des mises à jour de routage pour changer de destination et de vitesse.

Indépendamment des méthodes utilisées pour générer les mouvements des nœuds mobiles, il faut définir une topographie ; L'espace est considéré comme étant une grille dont il faut donner les frontières (valeurs de x abscisse et y ordonnée).

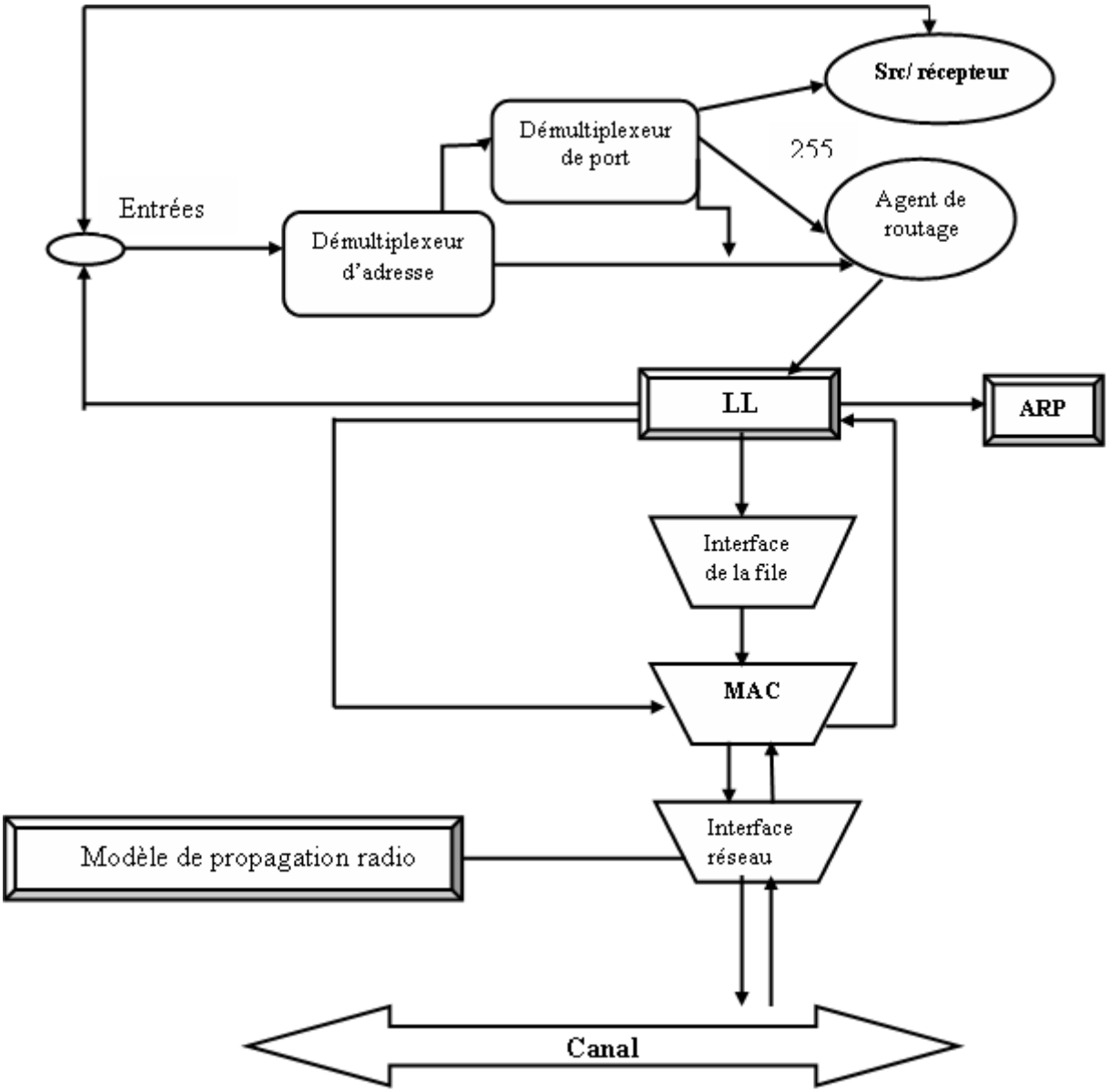


Figure 27: schémas d'un nœud mobile sous ns.

Voyons à présent plus en détail les composants réseaux d'un nœud mobile :

- Un classifieur de l'adresse a utilisé pour donner des paquets au classifieur de port ou à un agent de routage. la cible par défaut du classifieur de l'adresse est souvent l'agent de routage, tenir en compte d'expédition du paquet.

- Un classifieur de port, utilisé pour donner des paquets aux agents attachés au nœud mobile.
- Un agent de routage pour la gestion de la table et l'expédition (l'avancement) des paquets. L'agent de routage devrait mettre le champ next-hop du paquet pour indiquer leur next-hop (prochain) destination.
- Une couche de liaison (Link layer) pour convertir les adresses réseau aux adresses matérielles (avec l'aide du module ARP) et préparer des paquets pour être mis sur un canal sans fil.
- Un module ARP qui résout les adresses réseau aux adresses matérielles (MAC).
- Une file d'interface, utilisée pour stocker les paquets qui devraient être envoyés à l'extérieur.
- Une couche MAC pour la gestion d'accès au canal sans fil.
- Une interface réseau qui envoie et reçoit des paquets sur le canal sans fil.
- Un modèle de la propagation radio (radio propagation) qui détermine la fréquence du signal reçu, et d'où, si un paquet peut être reçu par une interface réseau ou pas.
- Un canal sans fil (Wireless Channel) sur lequel les paquets sont distribués [43]

5.1.6 Installation, configuration, utilisation et modification de NS2

5.1.6.1 Installation et configuration de NS2

L'outil NS2, si on respecte le concept de linux, est installé dans /user/local/ns, on peut l'installer dans notre répertoire spécifique (comme /home ou /root...) , normalement, il n y a aucune variable d'environnement à positionner, néanmoins, si le besoin s'en fait sentir, on peut rajouter /usr/local/ns/bin dans notre PATH pour utiliser les exécutables (ns, nam et éventuellement xgraph), généralement NS2 est fournit sous forme d'un code source, les sources se présentent sous deux formes : l'une dite tout en un « allinone » qui contient le code NS2 et d'autres composants utilisés (comme Otcl, NAM, xgraph ….), soit par morceaux, c'est-à-dire qu'on peut choisir uniquement les composants dont a besoin. Le package comprend aussi des exemples de script ainsi que des modèles de mouvement pour les nœuds mobiles ou de génération de trafic. On note qu'il y a des versions de linux qui ne supporte pas certaine version de NS2 (exemple ns2.27 sous fedora 5), La procédure d'installation de NS-2 « allinone » (exemple ns2.31 sous Debian GNU/linux) se fait comme suit :

1- tar xzvf ns-allinone-2.31.tar.gz

2- cd ns-allinone-2.31

3- . /install

Ensuite les PATH:

> export LD_LIBRARY_PATH=$usr/local/bin/ns-allinone-2.31/otcl-1.9:$usr/local/bin/ns-

allinone-2.31/lib:$LD_LIBRARY_PATH
> export TCL_LIBRARY=$usr/local/bin/ns-allinone-2.31/tcl8.4.5/library:$TCL_LIBRARY
> export PATH=$usr/local/bin/ns-allinone-2.31/bin:$PATH.

4- cd ns-2.31

5- . /validate

5.1.6.2 Utilisation de NS2

NS-2 permet à l'utilisateur de définir un réseau et de simuler des communications entre les nœuds de ce réseau, NS2 utilise le langage otcl (une extension objet du langage tcl) dérivé de TCL, à travers ce langage, l'utilisateur décrit les conditions de la simulation : la topologie du réseau, les caractéristiques des liens physique, les protocoles utilisés, les communications qui ont lieu.

L'utilisateur peut écrire son script dans n'importe quel éditeur de texte, le plus simple est d'utiliser la commande vi comme suit :

Vi <NomdeFichier>.tcl : le fichier doit être enregistré avec une extension **tcl**.

Ce fichier est ensuite passé au simulateur proprement dit, celui-ci se nomme ns, et pour exécuter le script, l'utilisateur doit taper l'instruction suivante :

. /ns <NomdeFichier>.tcl

Après l'exécution de cette instruction, le réseau est simulé, ce qui produits des traces et des statistiques. Ensuite, il peut utiliser des outils périphériques permettent l'animation du réseau (comme l'outil nam) ou la conversion vers d'autres outils (comme gnuplot et tracegraph pour dessiner des courbes).

5.1.6.3 Ajout d'éléments et modification de NS2

Comme nous l'avons indiqué précédemment, NS-*2* est un simulateur dont le code source est libre et par conséquent extensible (possibilité de modifier la source et de la recompiler). Pour modifier le comportement d'objets existants ou rajouter des nouveaux objets, il est donc nécessaire de modifier le code source *C++* qui réalise l'implantation de l'objet en question ou d'étendre les fonctionnalités de l'interpréteur *OTCL* (fichier *API OTCL* dans *NS-2* : *ns-lib.tcl*).

Le tutorial NS-2 de Marc Greis [40] donne la méthodologie avec un exemple d'ajout de nouveaux protocoles à NS-2. La méthode utilisée pour ajouter des fonctionnalités à NS-2 dépend du niveau protocolaire du protocole à implémenter. Lorsque le protocole est de

niveau IP ou au-dessus, il est codé sous forme d'un agent (classe dérivée de la classe agent). Si le nouveau protocole est de niveau inférieur à IP, il doit être codé comme une classe dérivée de la classe racine (la classe *NsObjec*t). D'une manière plus générale, ajouter un nouveau élément à *NS-2* nous conduit aux étapes suivantes:

- définir les nouveaux fichiers d'entête (*fichier.h*) pour la déclaration de la structure de données,
- déclarer la classe du protocole,
- définir la liaison entre le code source *C++* et le code *OTCL,*
- modifier le fichier *makefile* par l'ajout du ficher rajouté à la liste des fichiers de *NS-2,*
- Recompiler. [42]

5.1.7 Le format des traces sans fil dans NS2

Le format des traces sans fil diffère de celui des environnements filaires, la figure 28 représente un exemple de ces nouvelles traces.

```
r 1.016685301 _0_ MAC  --- 0 ACK 38 [0 0 0 0]
s 1.017095301 _0_ MAC  --- 0 RTS 44 [139e 1 0 0]
r 1.017447318 _1_ MAC  --- 0 RTS 44 [139e 1 0 0]
s 1.017457318 _1_ MAC  --- 0 CTS 38 [1264 0 0 0]
s 1.017684885 _0_ AGT  --- 9 cbr 1000 [0 0 0 0] ------- [0:0 1:0 32 0] [5] 0 0
r 1.017684885 _0_ RTR  --- 9 cbr 1000 [0 0 0 0] ------- [0:0 1:0 32 0] [5] 0 0
s 1.017684885 _0_ RTR  --- 9 cbr 1020 [0 0 0 0] ------- [0:0 1:0 30 1] [5] 0 0
r 1.017761334 _0_ MAC  --- 0 CTS 38 [1264 0 0 0]
```

Figure28 : Exemple de fichier de trace de NS2 d'un réseau mobile.

Le tableau suivant présente la signification des différents champs de ce fichier de trace.

Colonne	Signification
1	L' évènement : S (Send), R(receive),D(drop) et F(Forward)
2	Temps de l'évènement
3	Concerne le nœud
4	Nom de trace
5	Raison
6	Identificateur de l'évènement
7	Type de paquet
8	Longueur de paquet
9	Temps d'émission de données
10	Adresse MAC de destination

11	Adresse MAC de source
12	Type (ARP, IP)
13	Adresse IP de source
14	Numéro de port de source
15	Adresse IP de destination
16	Numéro de port de destination
17	Valeur de TTL (TIME TO LIFE)
18	Adresse de nœud suivant
19	Numéro de séquence

Pour être exploitables, ces informations doivent être traitées par un filtre qui analyse chaque ligne du fichier pour donner des informations interprétables. NS2 ne propose pas ce filtre et on a choisi l'outil de filtrage GAWK [44]. Les graphes sont obtenus en utilisant l'Excel, ainsi on a utilisé l'outil gnuplot [45] pour produire des courbes concernant le délai de découverte d'une route ainsi que le taux des paquets reçus dans le réseau simulé.

5.1.8 Visualisation des résultats sous NS2

5.1.8.1 Utilitaire NAM

Pour visualiser, animer et interpréter les données fournies à travers les fichiers trace et donner un compte-rendu graphique NS2 emploie l'outil d'animation NAM (Network AniMator), basé sur le langage TCL/TK, NAM permet également de donner une représentation graphique du réseau décrit dans le fichier de simulation TCL tout en animant les liens entre les nœuds du réseau, le modèle théorique du NAM a été non seulement créé pour lire un large ensemble de donnés d'animation, mais aussi suffisamment extensible pour être utilisé quelque soit le type de réseau simulé (fixe ou mobile ou mixte), ce qui permet de visualiser tout type de simulation possible. Généralement les scénarios simulés génèrent des fichiers avec l'extension .nam, la visualisation de ces scénarios avec NAM se fait à l'aide de la commande :

./nam <FichierNAM>.nam ou l'exécution de cette commande à travers le script par l'ajout de l'instruction :

```
Proc finish {} {

        ……

        exec   ./nam <FichierNAM>.nam  & exit
}
```

5.1.8.2 Outil graphique xgraph

Xgraph est un autre utilitaire utilisé par NS2 et qui permet lui aussi de fournir un compte-rendu graphique, mais cette fois-ci sous forme de courbes statistiques, les formats de données acceptés en entrée sont de type deux dimensions (x et y). Les valeurs dans chaque ligne séparées par des espaces ou des colonnes, et les données peuvent être à deux ou à plusieurs colonnes.

5.2 Modèle de Simulation

Afin d'étudier et d'analyser le fonctionnement et le comportement de notre protocole de routage dans un réseau ad hoc, nous avons utilisé le simulateur Network Simulator (NS2) version 2.31 installée sur Debian GNU/ Linux.

Le tableau ci-dessous illustre le contexte de notre simulation :

Paramètre	Valeur
Temps de simulation	40s
Protocole	AODV,HCAR
Taille du paquet de données	512 octets
Topographie de simulation	1000mx1000m
Taille du buffer (file) des nœuds	50 paquets
Vitesse d'émission	5 paquets/s

Un exemple de disposition visualisé par l'outil d'animation utilisé dans NS (Network Animation Manager) est donné dans la figure 29.

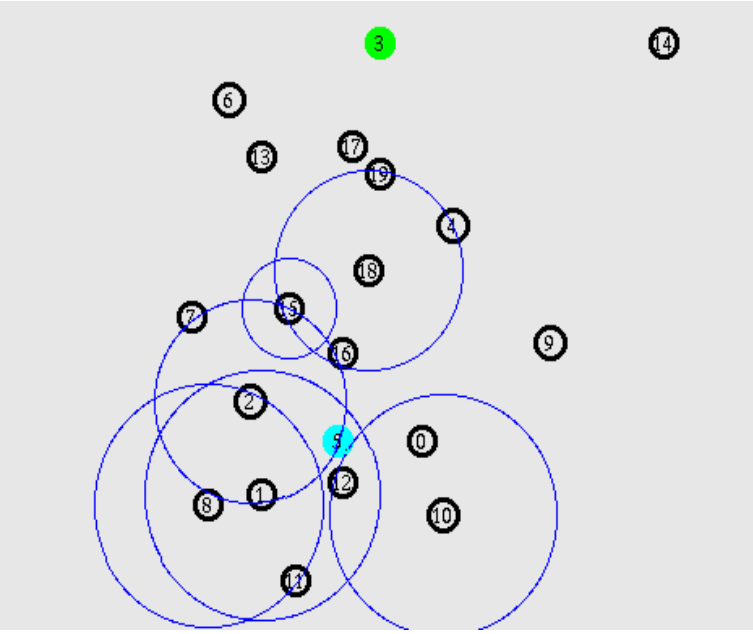


Figure 29 : Disposition des noeuds, exemple de scénario avec 20 nœuds.

Les paramètres standard pour le medium et la propagation radio sont utilisés. Le protocole IEEE 802.11, est utilisé comme protocole d'accès au medium. Le type de gestion de la file

ou queue en chaque nœud est « Drop Tail ». Dans ce type de gestion de files, les paquets venant de différents flots sont traités comme étant de même ordre de priorité (selon le principe FIFO), c'est-à-dire, une fois que le file se vide, le routeur peut accepter des paquets, si le tampon est plein, le dernier paquet qui arrive est supprimé. Le nombre maximum des paquets dans le tampon d'émission de chaque routeur est de 50 paquets.

5.2.1 Modèle de Trafic

Nous avons utilisé des applications qui sont des sources de trafic de type CBR (Constant Bit Rate) et qui émettent des paquets à intervalles réguliers. Ces sources de trafic modélisent la couche application sur des agents de transport UDP. L'utilisation de ce protocole permet d'éviter d'avoir à gérer le contrôle de flux qui amènerait à une analyse plus complexe des résultats. La source émet des paquets de taille 512 octets avec un débit de 5 paquets par seconde.

5.3 Comparaison HCAR et AODV

Après avoir détailler le principe de fonctionnement de notre protocole, nous avons procédé à une étude comparative avec le protocole AODV, en s'intéressant à quelques métriques ayant un rapport avec la QoS dans les réseaux Ad hoc. Pour cela, des simulations de ces deux protocoles ont été faites sur le même modèle de simulation (mêmes valeurs des paramètres et même modèle de trafic).

5.3.1 Métriques

Il est important de fixer les critères que l'on va prendre en considération pour garantir une QoS. Dans notre travail, nous nous sommes intéressés essentiellement au délai de découverte de route (qui influe directement sur le délai de bout en bout), la quantité du trafic de contrôle généré (qui influe sur la consommation des ressources limitées du réseau ad hoc) et le taux de paquets reçus ((PDR: Packet Dropped Ratio), ce qui influe sur la fiabilité des liaisons).

5.3.2 Analyse et discussion des résultats

Les figures 30 et 31 représentent respectivement, le temps de découverte d'une route entre deux nœuds (nœuds 5 et 3 dans notre cas), dans les deux protocoles AODV et HCAR, en fonction de la taille du réseau estimée en nombre de nœuds, et de la mobilité des nœuds.

Notons que dans notre étude, la mobilité de nœuds est mesurée par la fréquence de changement d'emplacement des nœuds, ainsi que par la vitesse de déplacement. Nous considérons deux types de scénarios que nous qualifions avec mobilité et avec moins de mobilité. Pour changer l'emplacement d'un nœud, nous utilisons la commande TCL : $mobilenode_ setdest <x> <y> <velocity>, par exemple :

$ns at 0.0 "$n (0) setdest 100.0 100.0 3000.0"

D'après les résultats de simulation obtenus, on constate que la durée de découverte d'une route dans le protocole HCAR, est plus courte que celle du protocole AODV. En effet,

AODV est un protocole réactif, l'établissement d'une route se fait uniquement à la demande. Dans le protocole HCAR, l'établissement d'une route se fait aussi à la demande, mais une fois une route est établie, elle reste valide tant qu'il n y a pas une mobilité ou un lien brisé. S'il y a une mobilité, on n'invalide que la partie de route affectée par cette mobilité (si la mobilité affecte tout le chemin alors on invalide la route sans le maintenir). En outre, dans le protocole HCAR, chaque nœud connaît ses voisins à deux sauts, de ce fait, lorsque un nœud source (nœud 5 dans notre exemple), veut communiquer avec un nœud destination (ici nœud 3), il reçoit une réponse de route rapidement. Cela est justifié par le fait qu'il y avait des communications actives vers ce même nœud destination, lorsque ces communications deviennent inactives, les routes utilisées restent valides tant qu'il n'y a pas une mobilité du nœud. Ce qui n'est pas le cas dans le protocole AODV où la validité de ces routes expire après un certain temps d'inactivité (10 s).

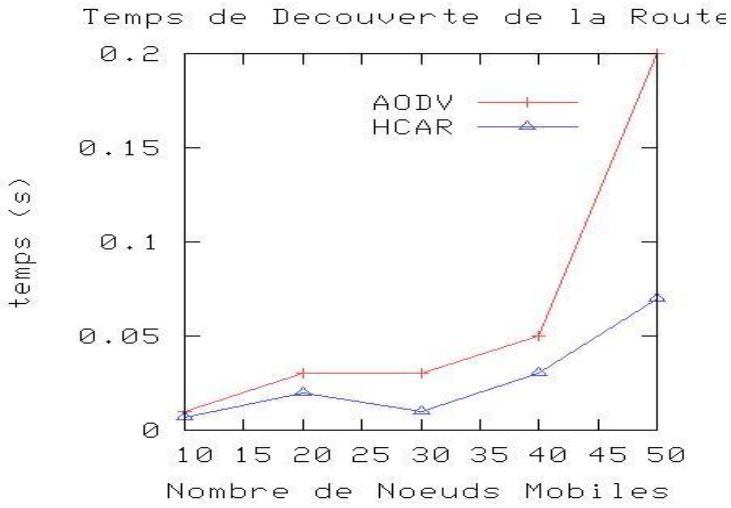


Figure30 : Temps de découverte d'une route (dans un contexte avec moins de mobilité).

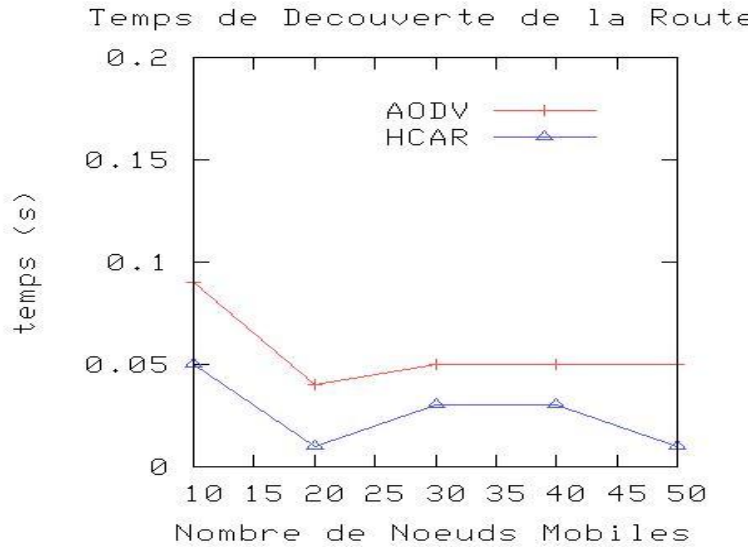


Figure 31 : Temps de découverte d'une route (dans un contexte avec mobilité).

Les graphes ci-dessous, illustrent la quantité du trafic de contrôle généré par le protocole AODV et HCAR dans un réseau ad hoc constitué de 50 nœuds mobiles en fonction de la mobilité des nœuds.

Dans un MANET avec moins de mobilité, la charge de contrôle générée par le protocole AODV est supérieure à celle générée par le protocole HCAR. En effet, dans le protocole HCAR, lorsqu'un nœud reçoit une requête, alors si ce nœud contient une route valide pour la destination demandée, il envoie une réponse en unicast, plutôt que de diffuser (en broadcast) la requête. Ce qui permet de diminuer le trafic de contrôle.

Par contre, dans un MANET avec mobilité, le protocole HCAR génère une quantité du trafic de contrôle supérieure à celle générée par le protocole AODV. Cela est dû essentiellement à la mobilité, qui entraîne une invalidation des routes valides et par conséquent, la génération d'un trafic de contrôle supplémentaire.

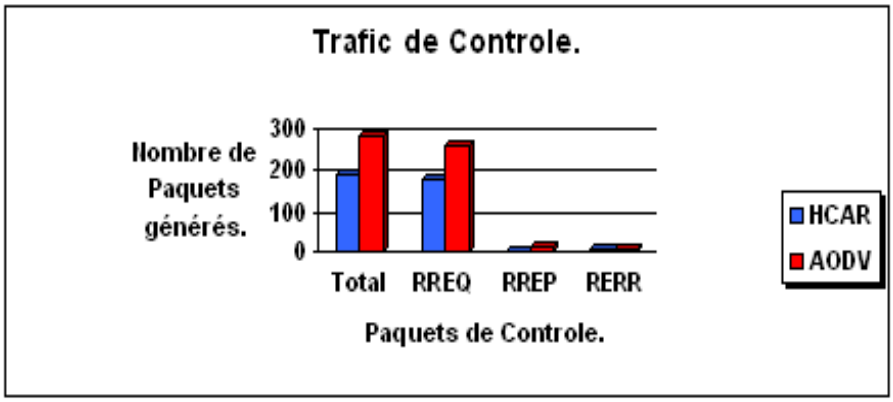


Figure 32 : Trafic de contrôle généré (dans un contexte avec moins de mobilité).

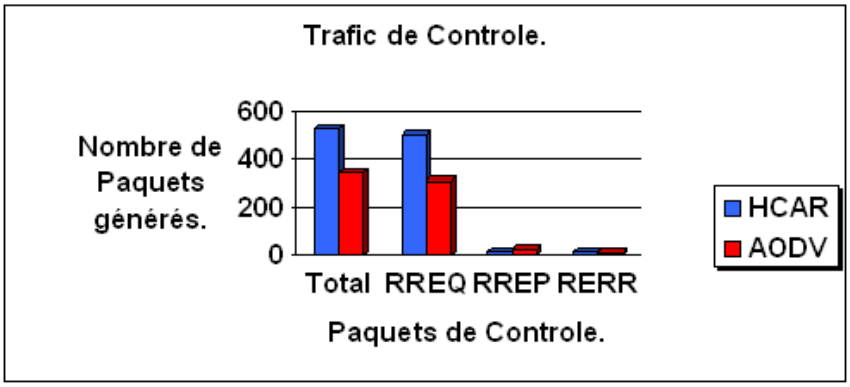


Figure 33 : Trafic de contrôle généré (dans un contexte avec mobilité).

Les courbes 34 et 35 illustrent le taux des paquets reçus dans les deux protocoles. Sur l'intervalle 0 à 5 sec, ces deux courbes sont presque identiques, après cet intervalle le débit des paquets reçus commence à diminuer jusqu'à ce qu'il atteint une valeur minimale, cela est dû à une perturbation du réseau causée par l'éloignement des nœuds. Dans le protocole HCAR, après une courte durée (5sec) le débit commence à augmenter de nouveau, cela signifie qu'une nouvelle route est établie (la destination est rapprochée), ce qui n'est pas le

cas dans le protocole AODV où le débit n'augmente qu'après une durée relativement longue(>12sec). Ce résultat est justifié par le fait que dans le protocole AODV et après qu'une route est brisée (à cause l'éloignement de destination), le nœud source tente de chercher une nouvelle route, si le nœud échoue après RREQ_RETRIES tentative (ici 3), il attend une durée (10s) avant que le processus de découverte de route soit initié. Par contre dans le protocole HCAR, lorsque la destination est éloignée le noeud demandeur se met en attente jusqu'à le rapprochement de cette destination (dans notre cas, à l'instant 10s). Pour la gestion de destinations éloignées le protocole HCAR utilise trois types de message, URDST, WNTD et DAPR.

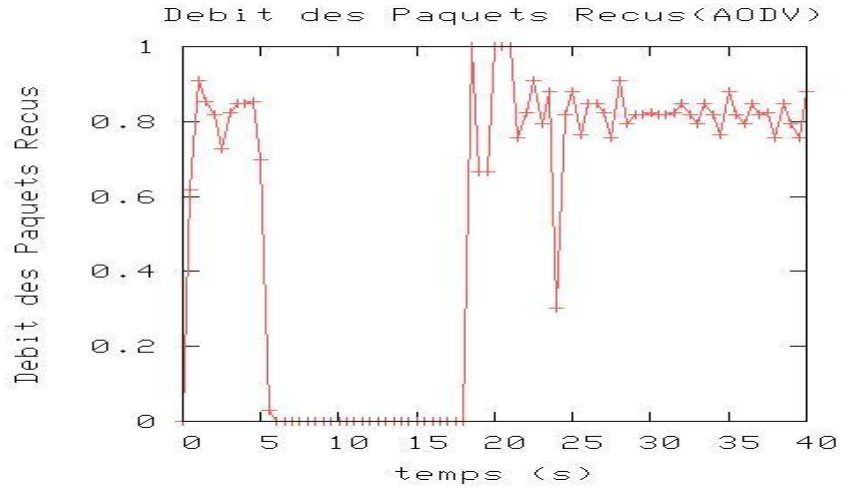


Figure 34 : Taux de paquets reçus (protocole AODV).

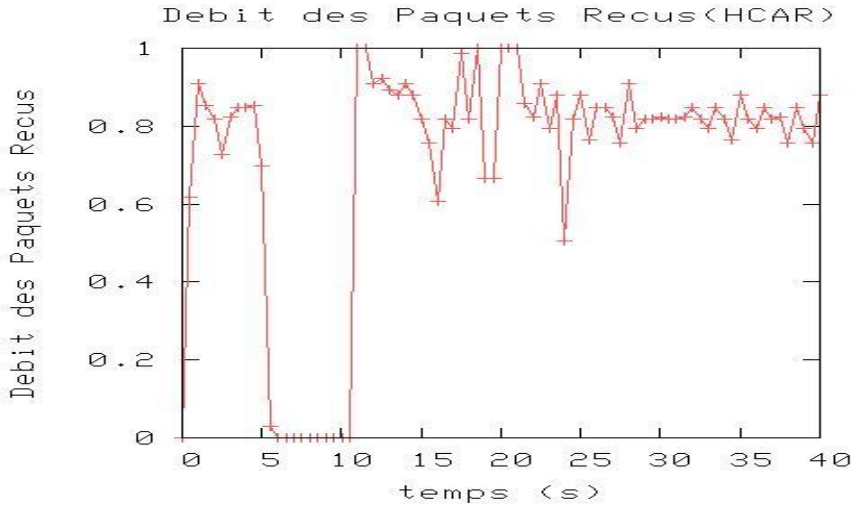


Figure 35 : Taux de paquets reçus (protocole HCAR).

5.4 Conclusion

Les MANETs ne sont qu'à leurs débuts. Le routage simple pose déjà des problèmes en pratique. De nombreux obstacles restent difficiles à franchir, c'est pourquoi les simulations de MANETs dépassent très rarement les quelques centaines de nœuds. L'introduction de la QoS dans ces réseaux est une tâche particulièrement difficile car la mobilité des nœuds rend la maintenance très coûteuse et ne permet pas de garantir des paramètres de QoS, on ne peut

que les approximer. Les nombreux algorithmes imaginés dans ce domaine témoignent de l'intérêt suscité par ce problème dans la communauté scientifique mais aussi du fait qu'aucun ne parvient à réellement s'imposer.

Dans ce chapitre nous avons présenté une comparaison entre notre protocole et le protocole AODV, Les résultats de simulation montrent que, pour différents scénarios, les performances de la solution retenue sont appréciables comparées à celles obtenues par un protocole de routage classique sans garantie de la QoS (AODV).

Conclusion et perspectives

Depuis la fin du 20e siècle, le monde a de plus en plus besoin de la mobilité, de l'accès et du partage de l'information. Cette mobilité se matérialise par la miniaturisation des périphériques et leur autonomie électrique (assistant personnel digital, appareil photo numérique, téléphone portable…). Cependant, au début de leur création, ces différents appareils ne pouvaient communiquer entre eux ou se connecter à des réseaux informatiques. Il a donc été rapidement implémenté dans ces appareils les technologies des réseaux sans-fil.

Le domaine des réseaux sans fil connaît aujourd'hui un grand succès, et présente de plus en plus une grande flexibilité d'emploi. Ils permettent la mise en réseau des sites dont le câblage serait trop onéreux à réaliser dans leur totalité, voire même impossible.

Les réseaux informatiques basés sur la communication sans fil sont classés en deux catégories, les réseaux avec infrastructure fixe préexistante, et les réseaux sans infrastructure. Dans la première catégorie, le modèle de la communication utilisé est généralement le modèle de la communication cellulaire. Dans ce modèle les unités mobiles sont couvertes par un ensemble de stations de base reliées par un réseau filaire, et qui assurent la connectivité du système. La deuxième catégorie essaie d'étendre les notions de la mobilité à toutes les composantes de l'environnement, toutes les unités du réseau se déplacent librement et aucune administration centralisée n'est disponible. Les réseaux de cette catégorie sont appelés : les réseaux ad hoc.

Un réseau Ad Hoc est une collection de périphériques équipés d'une technologie de transmission sans fil et dotés de protocoles permettant la mise en réseaux de ceux-ci. La particularité de ce type de réseau est que chaque noeud peut communiquer avec n'importe quel autre noeud du réseau. En effet, si un noeud A veut communiquer avec un noeud B qui n'est pas dans sa portée, alors il passera par une série de noeuds intermédiaires qui joueront le rôle de relais entre la source et la destination. Il est dès lors possible de créer un réseau par la simple présence de terminaux équipés de cartes d'interfaces adéquates. Ces réseaux mobiles et dynamiques peuvent être utilisés pour étendre la portée de stations de base, offrant ainsi un accès à l'Internet sur une zone géographique étendue à moindre coût. Ils peuvent être déployés rapidement et être utilisés par exemple dans des situations d'urgence.

Les caractéristiques particulières du médium radio, telle que la portée de communication limitée ou le mode de partage du canal radio ainsi que la mobilité des terminaux rendent souvent les mécanismes et protocoles issus du monde filaire peu performants. À l'heure actuelle, de nombreux travaux ont été effectués afin de concevoir des protocoles de routage adaptés à ces réseaux. Le groupe de travail MANET de l'IETF est en passe de standardiser une ou plusieurs solutions de routage. De nombreuses problématiques restent cependant ouvertes telles que la sécurité, le multicast ou encore la qualité de service. Ces différents sujets ont fait couler beaucoup d'encre durant ces dernières années. Toutes les solutions issues du monde filaire ont été réexaminées et adaptées mais peu de propositions réellement adaptées aux spécificités de ces réseaux ont vu le jour.

Dernièrement, avec l'émergence des services multimédia temps réel, et les champs variés des applications des réseaux ad hoc, la qualité de service dans les réseaux ad hoc est devenu un thème de recherche qui a suscité beaucoup d'intérêts.

La qualité de service est importante dans les MANET, car elle peut en améliorer le rendement et permettre à l'information essentielle de circuler malgré des conditions difficiles.

Cependant, il est très difficile de garantir une quelconque qualité de service à une application temps réel dans un réseau ad hoc, car il faut prendre en considération les spécificités de ces réseaux.

Le routage étant un domaine où la Qualité de Service est peu intégrée et faisant également l'objet de travaux. Dans ce travail, nous avons proposé un protocole de routage pour garantir la qualité de service dans les réseaux mobiles Ad Hoc. Nous avons illustré tout d'abord le principe de fonctionnement de notre protocole pour voir dans quelles mesures il réponde à la problématique de la QoS dans les réseaux Ad Hoc. Puis nous avons présenté une comparaison de notre protocole de routage avec le protocole AODV, en conduisant des simulations sous Network Simulator ns2, ce qui nous a permis de dégager les principales caractéristiques de notre protocole.

Ce travail toujours en cours, constitue une base pour nos futurs travaux de recherche. Voici les extensions qui nous semblent importantes :

- rendre le protocole capable d'isoler les flots pour leur fournir la QoS requise (mécanisme de contrôle d'admission), par exemple, rechercher une route disposant d'une certaine quantité de bande passante pour un trafic vidéo, garantir une borne sur le délai de transmission des paquets pour les applications de téléphonie…etc.

- étendre les fonctionnalités du protocole HCAR, pour qu'il soit adapté aux réseaux à grande échelle, en utilisant les techniques de hiérarchisation ou de 'clustring'.

Références

[1] C.Chaudet, I.Lassous, « Routage QoS et réseaux ad-hoc : de l'état de lien à l'état de nœud », Rapport de recherche n° 4700, Janvier 2003. INRIA, France.

[2] « Réseaux sans fil et mobilité », Dimension Data 2007-2008, URL: http://www.dimensiondata.com/fr/Solutions/IntegrationDeReseaux/R%C3%A9seauxSansFilEtMobilit%C3%A9.htm.

[3] « Réseaux sans fil», NTT Communications, NTT Europe LTD. Paris Branch, URL: http://www.ntt.fr/sol-int-mob_1.php.

[4] N.Badache, T.Lemlouma, « Le routage dans les réseaux mobiles ad hoc«, Mini projet, Septembre 2000. Université Houari Boumediene, Algérie.

[5] D.G.Frédéric, « WIFI l'essentiel qu'il faut savoir…«, Extraits de sources diverses récoltées en 2003.

[6] Van der Meerschen Jerome, "Hybridation entre les modes ad-hoc et infrastructure dans les réseaux de type Wi-Fi", Mémoire de fin d'études, Année 2006, Université Libre de Bruxelles.

[7] Michel Duchateau, «Analyse et simulation du déploiement d'un réseau sans fil à l'ULB «, Mémoire de fin d'études, Année 2005, Université Libre de Bruxelles.

[8] Rabih MOAWAD, « QoS dans les WPAN, WLAN et WMAN «, MEMOIRE DE DEA RESEAUX ET TELECOMMUNICATIONS, Decembre 2004, UNIVERSITE SAINT JOSEPH.

[9] David CARSENAT, « CONTRIBUTION A L'ETUDE DE RESEAUX DE COMMUNICATION SANS FIL. APPLICATION AU LMDS. «, Thèse N° 30-2003, pour obtenir le grade de docteur de l'université de LIMOGES, le 15 octobre 2003.

[10] « Les réseaux sans fil », URL : http://igm.univ-mlv.fr/~dr/XPOSE2002/Sansfils/index.php?rubrique=Sécurité.

[11] « Mobilité, et réseaux sans fil », par Cisco Systems, Dossier de presse Avril 2003.

[12] « Les Réseaux sans Fil : La révolution annoncée pour l'accès à l'information et les solutions de mobilité », Dossier préparé par Christian Sinephro, Phrywave: Mobile Data Services.

[13] Anne Gégout, «Les réseaux ad hoc«, Fiche Savoir, mars 2005, Réf.: sav0132 Version 1.

[14] Abdelhamid Zabdi, « DZ-MAODV : NOUVEAU PROTOCOLE DE ROUTAGE MULTICAST POUR LES RÉSEAUX ADHOC MOBILES BASÉ SUR LES ZONES DENSES «, mémoire présenté à l'université du Québec à Trois-Rivières, Avril 2006.

[15] Mariam Dawoud, « Analyse du protocole AODV «, DEA d'Informatique**,** Université Paul Sabatier, Année 2005/2006.
[16] Acharya A. and Badrinath B. R. "Delivering multicast messages in networks ith mobile hosts", In Proceeding of the 13th Intl, On Distr, Computing Systems, Pittsburg, pp 292-299, May 1993.

[17] Cho K. and Birman K. P. "A group communication approach for mobile computing. Mobile channel: an ISIS tool for mobile services". Workshop on Mobile Computing Systems and Applications, Santa Cruz, CA, U.S., 8-9 December 1994.

[18] Jean-Pierre CHANET, « Algorithme de routage coopératif à qualité de service pour des réseaux ad hoc agri- environnementaux «, Thèse pour obtenir le grade de DOCTEUR D'université Blaise Pascal - Clermont II, 20 avril 2007.

[19] David Elorrieta, « Protocoles de routage pour l'interconnexion des réseaux Ad- Hoc et UMTS «, mémoire de fin d'étude, Année 2006-2007, Université Libre de Bruxelles.

[20] Bécaye DIOUM, » Effets de la mobilité sur les protocoles de routage dans les réseaux ad hoc », Université MOULOUD MAMMERI de TIZI OUZOU, Algérie.

[21] Chouaib BOULKAMH, Mohamed Nadjib OUNES, Khaled LAGGOUN, Maamar SEDRATI, Azeddine BILAMI, « Impact de la Charge de Contrôle de Routage Sur la QdS dans un Réseau Ad hoc. «, the International Conference on Computer Integrated Manufacturing CIP'2007, November, 03-04, 2007 Setif, Algeria.

[22] Paul Ferguson and Geoff Huston, "Quality of Service, Delivering QoS on the Internet and in Corporate Networks*"*, Wiley Computer Publishing, New-York, January 1998.

[23] QoS Forum. QoS protocols and architectures. White paper of QoS Forum, July 1999. http ://www.qosforum.com

[24] E. Crawley, R. Nair, B. Rajagopalan, H. Sandick, "A Framework for QoS-based Routing in the Internet", IETF RFC2386

[25] Christophe Benoit, Rauch Jérome, Morgado Gonçalves Nuno, "La qualité de service dans l'Internet, IntServ et RSVP", ESIAL 3A – TRS

[26] P. Almquist. RFC 1349:" Type of service in the Internet Protocol suite", Technical report, July 1992, Status: PROPOSED STANDARD.

[27] Emmanuel JEANVOINE, « Qualité de service dans les réseaux actifs «, Mémoire de D.E.A présenté à l'université de Franche-Comté, juin 2004.

[28]Claudine Chassagne*,* »Qualité de Service dans l'Internet », UREC/CNRS**,** Août 1998**,** *URL :* http://www.urec.fr/metrologie/qos.html

[29] Jean Sébastien NATCHIA KOUAO, Abdelkader BENLAHCEN, "QoS IP: MODELES INTSERV / DIFFSERV", Telecom Lille 1.

[30] Laurent Toutain, Jean Marie Bonnin, *Octavio* Medina, «La qualité de service dans l'Internet «, ENST Bretagne - Campus de Rennes, France.

[31] Sylvain FRANCOIS, Anne-Lise RENARD, Jérémy ROVARIS, «Etude du service DiffServ «, ESIAL 2002-2003.

[32] Y. Bernet. RFC 2998, "A framework for integrated services operation over diffserv networks", Technical report, November 2000.

[33] Rabah MERAIHI, «Gestion de la qualité de service et contrôle de topologie dans les réseaux ad hoc «, Thèse présentée pour obtenir le grade de docteur de l'Ecole nationale supérieure des télécommunications, TELECOM PARIS.

[34] I. Aad and C. Castelluccia,"Differentiation mechanisms for IEEE 802.11", In *to appear in IEEE Infocom 2001*, april 2001.

[35] Claude Chaudet, « Qualité de service et réseaux ad-hoc – un état de l'art », Ecole Normale Supérieure de Lyon, Unité Mixte de Recherche CNRS-INRIA-ENS LYON no 5668, Research Report No 2001-46, November 2001.

[36]O.Bamouh, H.Lalaoui, «Les principaux modéles de QOS dans les réseaux Ad Hoc «, url : http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2007 /Bamouh-Lalaoui/solutio.html.

[37] Rabah Meraihi, Gwendal Le Grand, Samir Tohmé, Michel, Riguidel, « Gestion multicouches de la qualité de service dans un réseau ad hoc à cœur stable «,Département Informatique et Réseaux École Nationale Supérieure des Télécommunications, paris.

[38] Dorland Adrien, Gautier Loic, Kovalenko Alexis, Nallamoutou Hervé and Ribeiro Alexandre, « Analyse des techniques de routage avec QoS dans les réseaux ad hoc », Université Pierre et Marie Curie - Paris VI.

[39] P. Anelli & E. Horlait, » NS-2: Principes de conception et d'utilisation », Version1.3

[40] Tutorial de NS disponible sur :
http://titan.cs.uni-bonn.de/~greis/ns/
http://titan.cs.uni-bonn.de/~greis/ns/nstutorial.tar.gz

[41] Kevin Fll Kannan, «The ns manual«, URL: http://www.isi.edu/nsnam/ns/ns-documentation

[42] Ahcene BOUZOUALEGH, « étude et proposition d'un réseau local acoustique aquatique«, Thèse de doctorat de l'université de toulouse II, juillet 2006.

[43] Nicolas Montavont, « LA MOBILITE DANS LES RESEAUX IP », Rapport de D.E.A.Informatique, Université Louis Pasteur de Strasbourg.

[44] Arnold D. Robbins, « GAWK: Effective AWK Programming «, A User's Guide for GNU Awk Edition 3 June, 2004.

[45] Thomas Williams & Colin Kelley, »gnuplot An Interactive Plotting Program », manual of gnuplot, 26 August 2007, url: http://sourceforge.net/projects/gnuplot.