Université de Montréal

Protocoles de routage pour les réseaux ad hoc

par
Redouane Hamza

Département d'informatique et de recherche opérationnelle

Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures

en vue de l'obtention du grade de Maître ès sciences (M.Sc.)

en informatique

Novembre 2004

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

Protocoles de routage pour les réseaux ad hoc

présenté par :

Redouane Hamza

a été évalué par un jury composé des personnes suivantes :

Abdelhakim Hafid
président-rapporteur

Brigitte Jaumard
directrice de recherche

Michel Barbeau
membre du jury

Mémoire accepté le 21 décembre 2004

Résumé

Les réseaux ad hoc (souvent appelés MANET pour Mobile Ad hoc NETworks) consistent en des hôtes sans fil qui communiquent entre eux en l'absence d'infrastructures fixes de communication. Ils sont utilisés dans les cas de catastrophes qui endommagent les infrastructures de communications, pour des conférences et sur les champs de batailles (applications militaires), et reçoivent actuellement une attention significative.

Un des grands défis dans la conception de ces réseaux à l'état actuel est le développement de protocoles de routage qui sont capables de trouver des routes d'une façon efficace entre les nœuds communicants. Les protocoles de routage doivent être en mesure de s'adapter avec les changements imprévisibles de topologie. Nous présentons ici deux nouveaux protocoles de routage pour ces réseaux.

Nous proposons un premier protocole qui considère seulement une diffusion partielle. Nous examinons plusieurs définitions possibles pour la liste des meilleurs candidats parmi les hôtes, pour permettre à la diffusion partielle d'avoir un taux de succès le plus proche possible de la diffusion pure, tout en utilisant moins de ressources dans le réseau.

Le deuxième protocole traite le cas où des hôtes sans fil, fixes et connus de tous les autres hôtes sont présents dans le réseau ad hoc. Nous étudions comment définir un protocole de routage qui permette d'exploiter ces hôtes fixes.

Mots clés : réseaux ad hoc, réseaux mobiles, MANET, protocoles de routage.

Abstract

Mobile ad hoc networks (often referred to as MANET) consist of wireless hosts that communicate with each other in the absence of a fixed infrastructure. They are used in disaster relief, conference and battlefield environments, and are currently receiving a significant attention.

A central challenge in the design of MANET is the development of routing protocols that can efficiently find routes between two communicating nodes. The routing protocol must be able to keep up with the high degree of mobility that often changes the network topology drastically and unpredictably. We will present two new protocols for these networks.

We propose a first protocol that considers only a partial flooding. We examine some possible definitions for a list of best candidates from a list of nodes that allows the partial flooding to have a success rate as close as possible to a pure flooding strategy, but requiring much less resources in the ad hoc network.

The second protocol deals with the case of presence of fixed nodes in the ad hoc network. We study how we can define a routing protocol that allows the exploitation of these fixed hosts.

Keywords: Ad hoc networks, Mobile networks, MANET, routing protocol

Table des matières

Liste des figures

Liste des tableaux

Liste des sigles et abréviations

ACK	Acknowledgment
ADRP	AD hoc Routing Protocol
ADRPH	AD hoc Routing Protocol Hop by hop
AODV	Ad hoc On demand Distance Vector
ASNRP	Ad hoc with Static Nodes Routing Protocol
CTS	Clear To Send
DSR	Dynamic Source Routing
FTP	File Transfer Protocol
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LLC	Link Layer Control
MAC	Medium Access Layer
MANET	Mobile Ad hoc NETworks
OSI	Open Systems Interconnect
RSVP	Resource ReSerVation Protocol
RTS	Request To Send
TCP	Transport Control Protocol
TTL	Time To Live

Remerciements

Je tiens tout d'abord à remercier Dr Brigitte Jaumard, directrice de cette thèse, pour sa disponibilité, ses conseils et son soutient tout au long de ce travail.

Je tiens à remercier ma famille pour m'avoir encouragé à retourner aux études.

Je remercie également, tous mes collègues du lab ORC, du DIRO et du CRT, où j'ai effectué cette maîtrise.

Chapitre 1

Introduction

Les réseaux sans fil sont en pleine expansion et ont suscité beaucoup d'intérêt ces dernières années. La téléphonie cellulaire a atteint un très grand niveau d'utilisation, avec un besoin de mobilité qui a encouragé la recherche et le développement de la technologie sans fil dans deux directions : les réseaux cellulaires avec infrastructure de communication et les réseaux ad hoc qui sont des réseaux sans fil, mobiles et sans infrastructure fixe de communication.

1.1. Réseaux sans fil avec infrastructure

Ces réseaux sont constitués de plusieurs stations de base fixes, appelées aussi points d'accès, reliées entre elles par des connexions filaires formant une épine dorsale par laquelle transitent toutes les communications.

L'exemple typique de ces réseaux est la téléphonie mobile tel qu'illustrée sur la figure 1.1, chaque station de base sert une zone divisée en plusieurs cellules (d'où l'appellation téléphonie cellulaire). Les communications des mobiles se trouvant dans cette zone avec d'autres mobiles qui peuvent eux-mêmes se trouver ou pas dans cette

zone, passent par la station de base qui sert cette zone et qui les acheminera à travers l'épine dorsale vers d'autres stations de base.

Dans ces réseaux, quand un nœud se déplace et sort du champ d'une station de base, il se retrouve affecté à la station de base qui dessert la zone où il s'est déplacé.

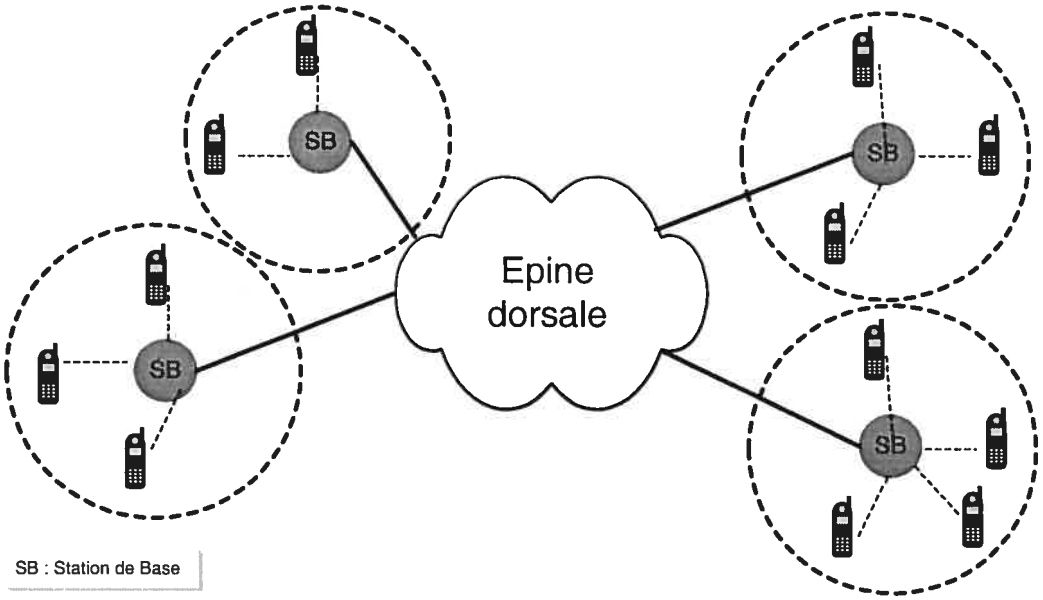


Figure 1.1 : réseau sans fil avec infrastructure (téléphonie mobile).

1.2. Réseaux sans fil sans infrastructure

En l'absence d'infrastructure fixe de communication, les nœuds ne sont plus liés à aucun point d'accès. Avec l'absence d'épine dorsale la communication entre les nœuds ne peut se faire qu'à travers d'autres nœuds, chaque nœud du réseau se comporte comme hôte et routeur en même temps, ces réseaux sont appelés réseaux ad hoc. Ils sont aussi appelés réseaux multi-saut qui vient du fait que la communication passe par un ou plusieurs nœuds pour atteindre son destinataire et aussi par

opposition aux réseaux sans fil avec infrastructure qui sont des réseaux à un seul saut (du nœud mobile à la station de base).

L'absence d'infrastructure fixe de communication rend le déploiement des réseaux ad hoc très facile, c'est un des premiers avantages de ces réseaux.

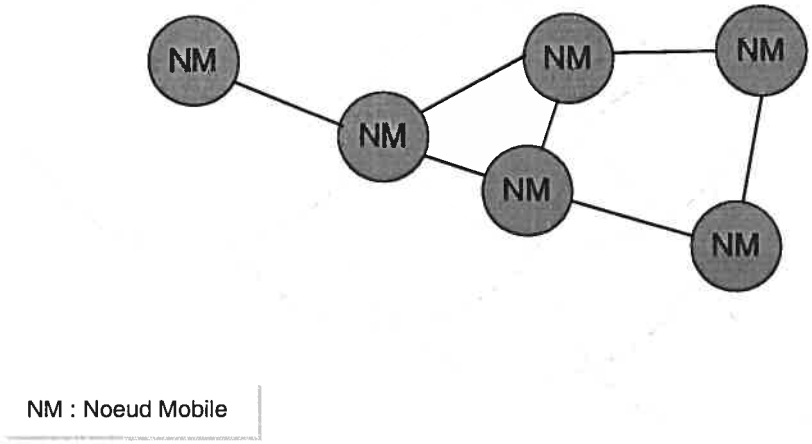


Figure 1.2 : réseau sans fil sans infrastructure (réseau ad hoc).

Comme il apparaît dans la figure 1.2, les réseaux ad hoc sont formés par des nœuds mobiles, où les liens se forment selon que deux nœuds se trouvent à la portée d'émission l'un de l'autre. Les cercles en pointillés sur la figure représentent les portées d'émission des nœuds.

Un réseau ad hoc est représenté par un graphe G(N,U) où N est l'ensemble des nœuds et U l'ensemble des liens sans fil entre les nœuds qui communiquent directement. Les nœuds qui communiquent directement sont appelés des nœuds adjacents (ou voisins).

Le graphe peut être orienté ou non, selon que les portées de transmissions sont les mêmes pour tous les nœuds (non orienté) ou diffèrent d'un nœud à un autre (orienté)[1].

Sauf mention, le graphe est considéré comme non orienté, ainsi les communications sont considérées comme étant bidirectionnelles.

Dans la suite de ce document, un nœud sans fil sera indifféremment appelé nœud ou station sans fil, ou encore station.

1.3. Caractéristiques des réseaux ad hoc

Dans les réseaux ad hoc les nœuds sont mobiles et sont donc alimentés par des batteries d'énergie de capacité limitée, toutes les opérations qu'effectuent ces nœuds consomment de l'énergie (déplacement, envoi, réception, ...), il faudrait prendre en considération cela à tous les niveaux de conception afin de maintenir le réseau en activité le plus de temps possible.

Le champ d'émission est quant à lui limité par la puissance des émetteurs qui équipent ces nœuds. Un nœud communique directement avec les nœuds qui sont dans son champ d'émission, les communications avec les autres nœuds situés plus loin passeront par les premiers voisins.

La topologie des réseaux ad hoc est dynamique, les liens entre les nœuds se font et se défont suivant le déplacement des nœuds.

Les réseaux ad hoc sont des réseaux sans fil, on retrouve donc toutes les caractéristiques des transmissions sans fil. Les bandes passantes sont de capacité inférieure à celle des transmissions filaires. De plus, la bande passante disponible est toujours inférieure à la bande passante effective due aux interférences et à d'autres

[1] Certaines couches MAC emploient des mécanismes qui exigent des nœuds une communication bidirectionnelle, ce qui forcerait le graphe à être non orienté même si les portées sont différentes.

conditions qui influencent les transmissions sans fil tel que les problèmes de la station cachée et de la station exposée qui seront présentés au chapitre 2.

Du côté de la sécurité, les réseaux ad hoc sont plus sensibles aux menaces physiques que les réseaux filaires fixes. Les possibilités accrues d'attaques par écoute passive, par usurpation d'identité et par déni de service doivent être étudiées avec attention.

1.4. Applications des réseaux ad hoc

Les réseaux ad hoc ont été développés en premier par la défense américaine au début des années 70, leurs premières applications étaient militaires, le but était de les utiliser là où les infrastructures de communication n'existaient pas ou étaient détruites, tels que les champs de bataille.

Dans les applications civiles, ces réseaux sont d'une grande utilité dans les opérations de secours où les infrastructures de communication sont endommagées par les catastrophes naturelles (tremblements de terre, ...).

D'autres applications sont envisageables pour les réseaux ad hoc tel que les réseaux spontanés (conférence, business, ...).

Pour l'usage personnel ou ce qu'on appelle réseau personnel, les réseaux ad hoc permettent de connecter plusieurs équipements tels l'ordinateur de bureau, l'ordinateur portable et l'ordinateur de poche. Ceci permet le transfert d'informations entre différents équipements sans aucun branchement filaire.

Pour plus de détails sur l'historique des réseaux ad hoc ainsi que leurs éventuels applications, le lecteur peut se référer à [17] et [18].

1.5. Le projet de maîtrise et ses contributions

Le présent mémoire apporte deux nouveaux protocoles de routage pour les réseaux ad hoc. Le premier protocole est classé dans la catégorie des protocoles de routage géographiques. Dans la littérature, ces protocoles définissent la problématique de routage comme suit : étant donné la position du nœud source, les positions de ses voisins et la position de la destination, il faudrait trouver une route entre la source et la destination en exploitant ces informations pour minimiser l'utilisation des ressources du réseau. Le protocole que nous proposons est, à notre connaissance, le premier qui pose la problématique sans avoir d'information sur la position de la destination, qui se trouve être le plus grand inconvénient des protocoles géographiques. Dans ce protocole, chaque nœud choisit, parmi ses voisins, ceux qui auront à acheminer la requête de route, ce choix se fait selon la position des voisins.

Le deuxième protocole est conçu pour des réseaux ad hoc particuliers où des nœuds fixes sont présents dans le réseau et sont connus des autres nœuds : le protocole proposé exploite les nœuds fixes dans le routage. Des routes entre les nœuds fixes sont maintenues d'une façon proactive et seront utilisées pour l'acheminement du trafic dans le réseau.

1.6. Plan du mémoire

Le reste de ce document se compose des chapitres suivants :

Le chapitre 2 expose la couche MAC des réseaux ad hoc en mettant l'accent sur la norme 802.11 des réseaux locaux sans fil.

Le chapitre 3 traite des travaux réalisés sur le routage dans les réseaux ad hoc, ces travaux sont classés selon les techniques de routage utilisées. Une revue de la littérature des travaux sur la qualité de service dans les réseaux ad hoc est aussi présentée dans ce chapitre.

L'essentiel de ce document se trouve dans les chapitres 4 et 5. Le chapitre 4 présente en détail les protocoles de routage réalisés : définition de la problématique de routage, notre objectif, les motivations dans nos choix pour définir les méthodes de routage, ainsi que les détails conceptuels de ces protocoles.

Le chapitre 5 présente les résultats des tests réalisés sur un simulateur en les comparant à d'autres protocoles de routage existants.

Enfin, le chapitre 6 conclut ce mémoire en résumant ses contributions ainsi que leurs possibles extensions.

Chapitre 2

La couche liaison de données dans les réseaux ad hoc

2.1. Introduction

Dans le modèle de référence OSI [9] qui définit l'architecture en couche d'un réseau, la couche liaison de données a pour tâche principale de transmettre les données à la couche physique en procédant au contrôle des erreurs et à la régulation du flux avant de fournir des données fiables à la couche réseau.

Les réseaux sans fil sont des réseaux à diffusion, c'est-à-dire que le canal de transmission est partagé entre plusieurs nœuds du réseau. Contrairement à une liaison point à point où il suffit de séparer physiquement l'émission de la réception pour ne pas avoir à gérer le canal de transmission, les réseaux à diffusion nécessitent une gestion de l'accès au canal partagé, pour assurer que les nœuds du réseau n'émettent pas en même temps ce qui provoquerait des collisions, et assurer aussi une certaine équité entre les nœuds pour l'accès au canal.

Pour cela, la couche liaison de données est dotée d'une sous-couche de contrôle d'accès au canal, appelée communément sous-couche MAC pour «*Medium Access Control*». La sous-couche MAC est constituée d'un ensemble de procédures et mécanismes qui permettent de gérer efficacement l'accès au canal. Pour des questions d'efficacité et/ou de faisabilité, les procédures implémentées dans la sous-couche MAC dépendent des caractéristiques physiques du canal de transmission, ce qui rend les sous-couches MAC différentes les unes des autres suivant le canal de transmission utilisé. Une autre sous-couche de la couche liaison de donnée, appelée protocole de contrôle de liaison logique ou LLC pour «*Logical Link Control*», se charge entre autres de rendre les différences entre les sous-couches MAC transparentes aux couches supérieures du réseau.

Ce chapitre est consacré aux sous-couches MAC dans les réseaux ad hoc, et traite aussi des caractéristiques de transmissions sans fil ainsi que les problèmes qui leurs sont liés. Par abus de langage, la sous-couche MAC est souvent appelée couche MAC.

2.2. Problèmes dans les transmissions sans fil

Outre la limitation de la bande passante effective, le canal partagé entre les nœuds et les interférences sur ce canal engendrent des problèmes de transmission dans les réseaux sans fil. Deux problèmes importants et connus dans les réseaux sans fil, qui sont le problème de la station cachée et le problème de la station exposée, seront détaillés ici.

2.2.1. Le problème de la station cachée

Une station est cachée à une autre lorsqu'elle se trouve hors de portée de sa zone de transmission. Le problème de la station cachée survient lorsque les deux

stations, essayent d'envoyer en même temps vers la même station, ce qui résulte en une collision au niveau de la station destinataire des deux transmissions.

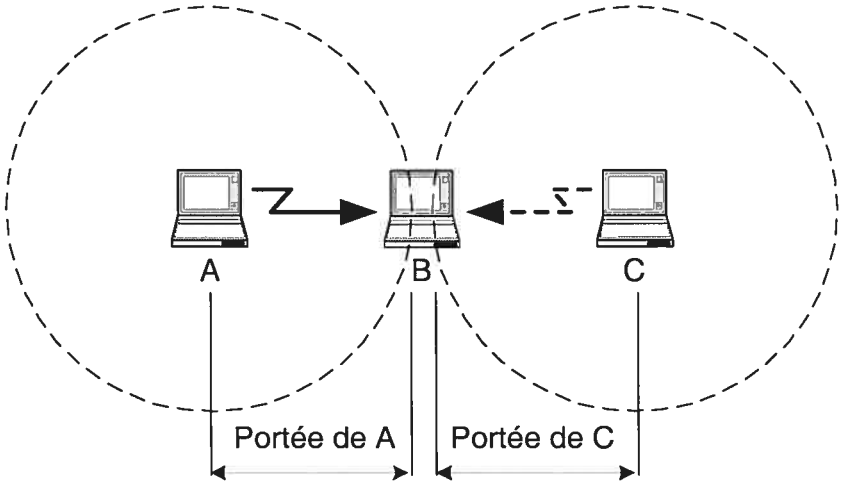


Figure 2.1 : le problème de la station cachée.

Dans la figure 2.1, la station C n'entend pas les transmissions de A qui émet vers B, C croit donc que le canal est libre et transmet vers B, cette transmission va entrer en interférence avec la transmission de A vers B et provoquer des erreurs de données au niveau de B.

Le fait qu'aucune des deux stations émettrices ne sache que l'autre est sur le point d'émettre est la principale cause qui conduit à la collision, une façon de remédier à ce problème et de mettre en place une procédure informative qui permet à la station qui désire émettre d'informer les autres de son intention, et ne commence vraiment à émettre que lorsqu'elle reçoit une réponse de la station destinataire l'informant qu'elle aussi est prête à recevoir. Nous verrons plus tard comment cette procédure est implémentée et nous verrons aussi quelles sont ses limites.

2.2.2. Le problème de la station exposée

Une station est exposée à une autre lorsqu'elle se trouve dans sa portée d'émission. Ce problème survient lorsqu'une station se trouve exposée à la station émettrice, et en même temps, elle se trouve hors de portée de la station destination. La position de la station exposée la pénalise et l'empêche d'émettre quelle que soit la destination à laquelle elle veut transmettre.

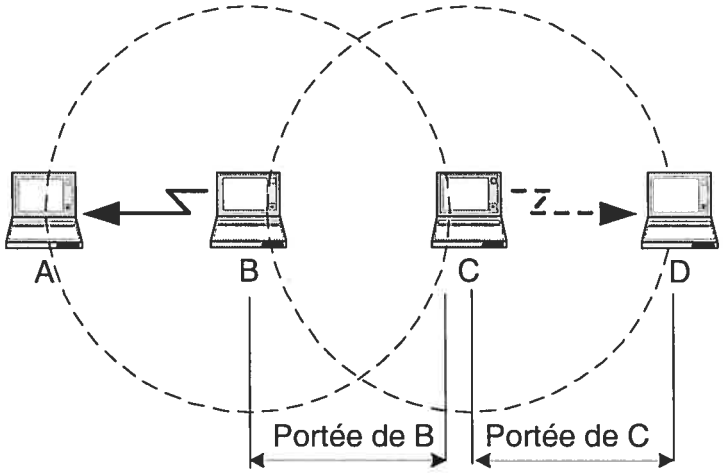


Figure 2.2 : le problème de la station exposée

Dans la figure 2.2, la station C entend B et sait que B est en train de transmettre, C conclut que le canal est occupé et ne va donc pas transmettre à D, alors qu'on réalité si C transmet vers D ceci ne créera d'interférence que dans la région entre C et B mais pas d'interférence au niveau de D, autrement dit les données envoyées par C à D ne seront pas altérées par l'exposition de C à B.

Le problème de la station exposée peut être réduit si des antennes directionnelles sont utilisées. Dans la figure 2.2, si B était équipée de ce genre d'antenne, sa transmission vers A n'aurait pas empêché C d'envoyer vers D.

2.3. Protocoles MAC pour les réseaux sans fil

2.3.1. Le protocole MACA

Le protocole MACA [10] «*Multiple Access with Collision Avoidance*» a été conçu pour les réseaux de radio amateur à paquets afin de minimiser les problèmes de la station cachée et celui de la station exposée. Ce protocole est inspiré par la méthode de détection de la porteuse avec évitement de collision CSMA/CA «*Carrier Sense Multiple Access with Collision Avoidance*», mais n'utilise pas de détection de la porteuse d'où le nom MA/CA ou MACA. Il propose le protocole RTS/CTS pour minimiser le problème de la station cachée.

Le protocole RTS/CTS

Quand une station veut émettre, elle envoie un petit paquet de demande d'envoi RTS «*request to send*» à la destination. Cette dernière répond à ce paquet par une autorisation d'envoi CTS «*clear to send*».

Le fonctionnement de cette méthode est décrit dans la figure 2.3 :

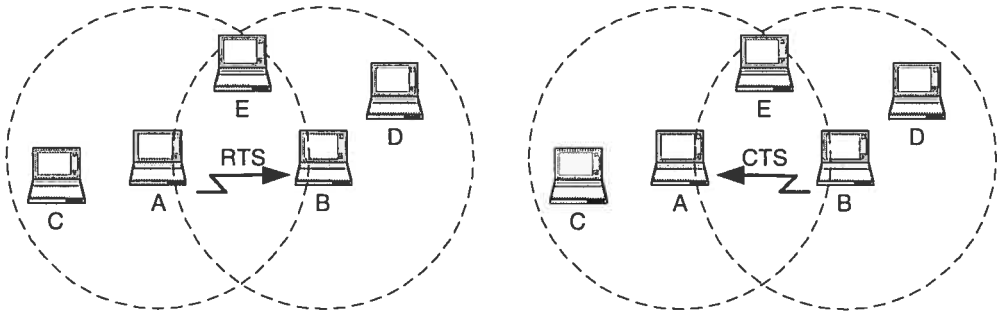


Figure 2.3 : le protocole RTS/CTS.

Quand la station A veut émettre des données vers B comme indiqué sur la figure 2.3, elle lui envoie un paquet RTS qui contient la taille du paquet de données qui va être envoyé. Quand la station B reçoit le paquet RTS, elle répond avec un paquet CTS qui contient l'information de la taille des données qui vont être reçues, cette information est obtenue de la trame RTS. Toutes les stations se trouvant dans la portée de transmission de B vont recevoir la trame CTS et sauront que B va recevoir un paquet d'une taille donnée. Ces stations vont devoir retarder toute transmission jusqu'à ce que B finisse de recevoir.

Le protocole RTS/CTS minimise le problème de la station cachée mais ne l'élimine pas complètement. L'exemple du réseau ad hoc multi-saut de la figure 2.4 illustre bien cela. En effet, au moment où B répond par CTS au RTS reçu de A, la station D, qui est hors de portée de B, envoie un RTS à C, ce qui provoque une collision au niveau de C. Il en résulte que C ne reçoit ni le RTS de D, ni le CTS de B. La station D n'ayant pas reçu de CTS de C retransmet sa requête RTS. La station A qui a reçu le CTS de B, commence sa transmission en même temps que l'envoi de CTS par C vers D. Les envois de C et A vont provoquer une collision au niveau de B, ce qui engendre cette fois une perte de données.

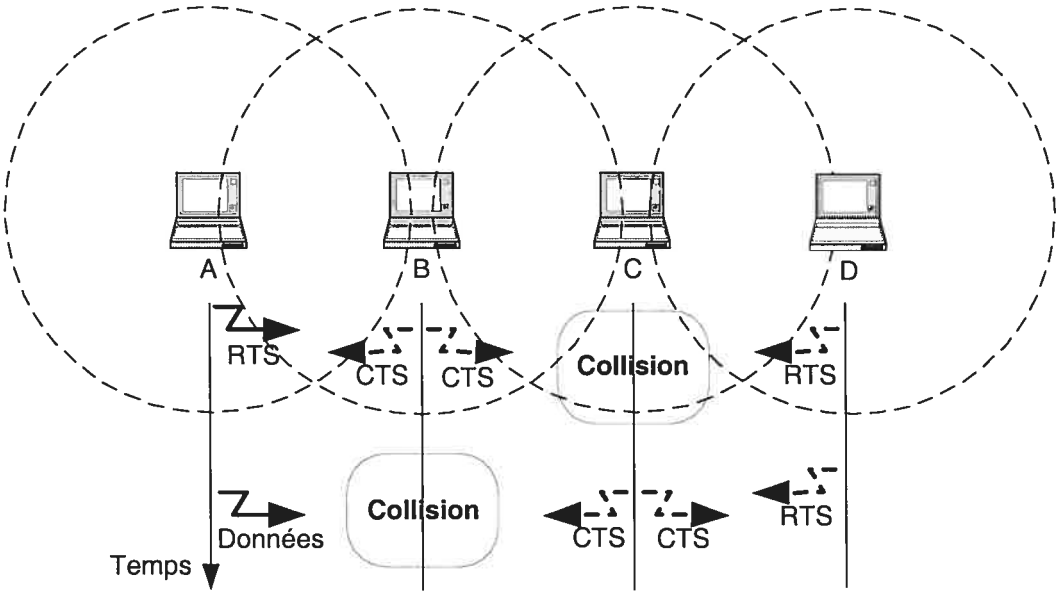


Figure 2.4 : les limites de la solution RTS/CTS pour le problème de la station cachée.

D'autres protocoles ont été inspirés de MACA, tel que le protocole MACAW et MACA-BI.

Le protocole MACAW [11] «*MACA for Wireless*» est une optimisation du protocole MACA. En plus de RTS/CTS, MACAW prévoit l'envoi d'accusé de réception pour chaque paquet de données reçu, afin d'éviter que les trames perdues ne soient détectées qu'au niveau de la couche transport du réseau. La détection de la porteuse est aussi utilisée dans ce protocole.

Le protocole MACA-BI [12] élimine la requête RTS et ne garde que CTS par rapport à MACA, ce qui veut dire que c'est au destinataire d'inviter l'envoyeur pour l'émission.

2.4. Le protocole 802.11 : un protocole pour les réseaux locaux sans fil

Le comité de normalisation des réseaux Locaux 802 de IEEE a défini le protocole 802.11 [13] comme standard pour les réseaux locaux sans fil. Ce protocole couvre la sous-couche MAC et la couche physique de ces réseaux.

Le protocole 802.11 a deux modes de fonctionnement, le mode avec infrastructure et le mode sans infrastructure. Dans le mode avec infrastructure, les communications passent par une station de base qu'on appelle souvent point d'accès. Chaque station de base contrôle un certain nombre de stations sans fil qui sont dans sa portée de transmission et est en mesure de se charger de certaines fonctions telles que la synchronisation. Les stations de base peuvent être connectées entre elles par des liens filaires et peuvent aussi être connectées à un réseau filaire comme Ethernet. Dans le mode de fonctionnement sans infrastructure, appelé aussi mode ad hoc, les stations sans fil communiquent directement entre elles sans passer par un point d'accès.

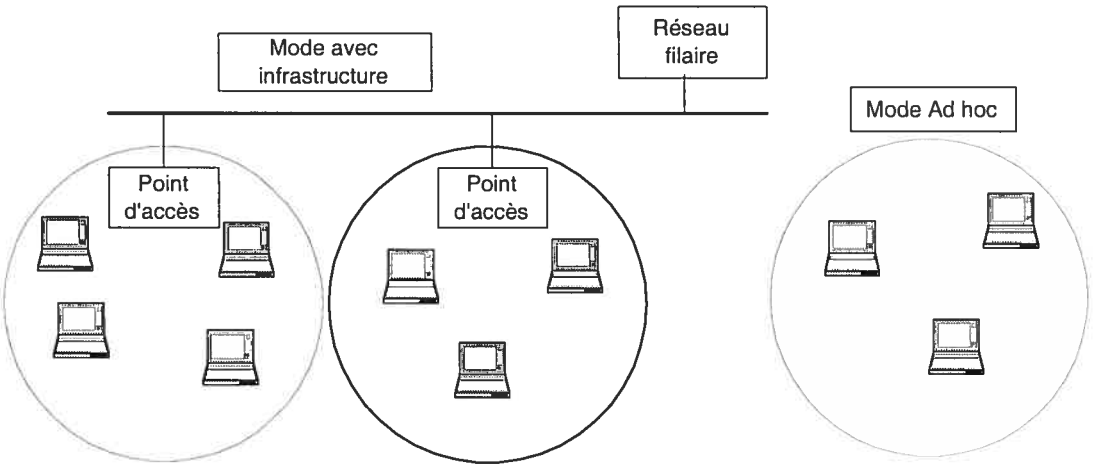


Figure 2.5 : les réseaux locaux sans fil 802.11.

2.4.1. La couche physique du protocole 802.11

Dans la première version du protocole 802.11, trois technologies de transmission sans fil ont été définies pour la couche physique : les ondes infrarouges, l'étalement de spectre par saut de fréquences et l'étalement de spectre par séquence directe. Ces technologies fonctionnent à des débits de 1 et 2 Mbps.

<table>
<tr><td colspan="6">Sous-couche LLC</td><td rowspan="2">Couche liaison de données</td></tr>
<tr><td colspan="6">802.11 MAC</td></tr>
<tr><td>802.11 infrarouge</td><td>802.11 FHSS</td><td>802.11 DSSS</td><td>802.11a OFDM</td><td>802.11b HR-DSSS</td><td>802.11g OFDM</td><td>Couche physique</td></tr>
</table>

Figure 2.6 : les couches physiques du protocole 802.11

Ondes infra rouges (IR)

La couche physique infra rouge pour les réseaux locaux sans fil 802.11 utilise une transmission diffusée et non un signal lumineux direct, elle opère sur des longueurs d'ondes variant entre 850 nm et 950 nm, et a une portée de transmission qui peut atteindre un rayon de 20 mètres. Deux débits sont permis, 1 Mbps et 2 Mbps. A 1Mbps un schéma d'encodage de 16 bits (un seul bit à 1) est utilisé pour coder une information de 4 bits. A 2 Mbps un schéma d'encodage de 4 bits (un seul bit à 1) est utilisé pour coder une information de 2 bits. Les rayons infra rouges peuvent être submergés par les rayons du soleil et ne peuvent pas franchir les murs, par conséquent cette technologie ne peut pas être utilisée à l'extérieur.

Étalement de spectre par saut de fréquences (FHSS)

L'étalement de spectre par saut de fréquences ou FHSS pour «*Frequency Hopping Spread Spectrum*», utilise un codage gaussien de décalage de fréquence pour transmettre des données à 1 ou 2 Mbps dans la bande de fréquence 2.4 Ghz [14]. Ce codage produit un signal analogique à partir du signal digital. Une séquence de nombres pseudo aléatoires est utilisée comme index dans une table de fréquence contenant 79 canaux de 1Mhz dans la bande de fréquence 2.4 Ghz. A chaque intervalle de temps déterminé, une fréquence est choisie dans la table et est modulée par le signal analogique. La répétition de cette opération produit un signal par saut de fréquence. Deux niveaux de codage gaussien de décalage de fréquences sont utilisés pour un débit de 1Mbps et 4 niveaux pour un débit de 2Mbps.

Étalement de spectre par séquence directe (DSSS)

L'étalement de spectre par séquence directe ou DSSS pour «*Direct Sequence Spread Spectrum*», opère dans la bande passante 2.4 Ghz qui est divisée en 11 sous canaux. Chaque bit est transmit comme une séquence de 11 fragments en utilisant la séquence de Barker [13]. Elle utilise une modulation par saut de phase binaire pour transmettre à un débit de 1 Mbps et une modulation par saut de phase quadratique pour transmettre à un débit de 2Mbps.

Les débits limités laissaient les réseaux locaux sans fil très loin derrière les réseaux filaires. Pour remédier à cela, le comité 802 a dû revoir les spécifications physiques pour la norme 802.11. Le résultat a été la définition de nouvelles normes découlant de la première et offrant des débits plus élevés, elles portent les noms 802.11a, 802.11b et 802.11g.

La norme 802.11a

La norme 802.11a [14] opère sur la bande passante de fréquence 5GHz et peut offrir un débit de 54Mbps. Elle utilise la technologie de multiplexage orthogonal en répartition de fréquence ou OFDM pour «*Orthogonal Frequency Division Multiplexing*». OFDM divise le spectre disponible en plusieurs porteuses, chacune d'elle est modulée en utilisant la modulation par saut de phase pour des débits allant jusqu'à 18Mbps et en utilisant la modulation de l'amplitude en quadrature de phase pour de plus grands débits. L'utilisation de plusieurs bandes étroites rend OFDM plus robuste aux interférences inter bandes et permet aussi l'utilisation de bandes non adjacentes.

La norme 802.11b

La norme 802.11b [14] opère sur la bande de fréquence 2.4GHz, elle utilise la technologie DSSR à haut débit ou HR-DSSR pour «*High Rate DSSR*». Elle est entièrement compatible avec les spécifications initiales du protocole 802.11, mais elle est incompatible avec la norme 802.11a. Pour atteindre des débits supérieurs à la norme initiale et allant jusqu'à 11Mbps, la norme 802.11b utilise une modulation par code complémentaire à 8 bits.

La norme 802.11g

La norme 802.11g [14] opère sur la bande de fréquence 2.4GHz et utilise la technologie OFDM ce qui lui permet d'atteindre un débit de 54Mbps. La norme 802.11g utilise une modulation par code complémentaire et est entièrement compatible avec la norme 802.11b.

2.4.2. La sous-couche mac du protocole 802.11

Deux modes de fonctionnement sont définis dans la sous-couche MAC du protocole 802.11, le mode appelé fonction de coordination distribuée (FCD) et le mode appelé fonction de coordination par point (d'accès) (FCP). Le premier mode doit exister dans toute implémentation de la norme 802.11, et comme son nom l'indique, ne fait appel à aucun contrôle centralisé. Le deuxième mode est optionnel et requiert la présence d'un point d'accès.

L'architecture de la sous-couche MAC est décrite dans la figure 2.7 où le mode FCP est fourni à travers les services du mode FCD.

Le terme conflit dans la figure 2.7 désigne le conflit d'accès au canal.

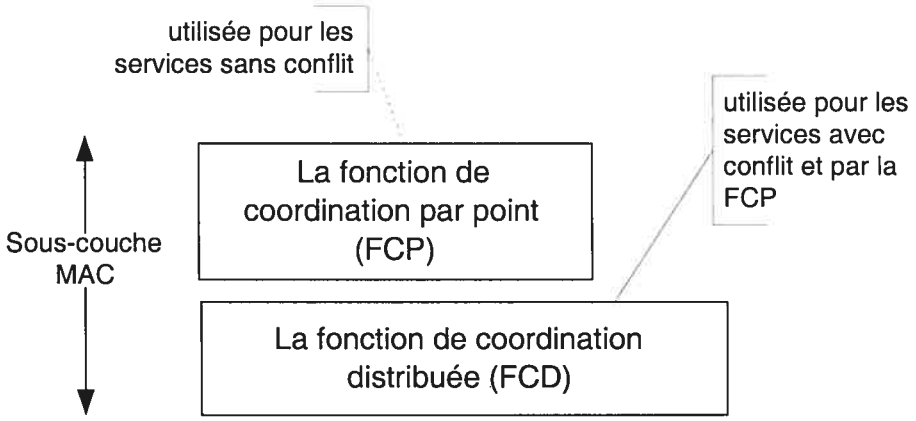


Figure 2.7 : architecture de la sous-couche MAC du protocole 802.11 [13].

La fonction de coordination distribuée (FCD)

La fonction de coordination distribuée est le mécanisme fondamental d'accès au canal dans le protocole 802.11, la base de ce mécanisme correspond au protocole CSMA/CA. Le protocole 802.11 définit des durées ou espaces de temps entre les trames. Quand une station veut émettre, elle doit écouter le canal. Si le canal est libre pendant l'intervalle de temps défini, elle commence à émettre. Si le canal est occupé

ou devient occupé pendant la durée de temps, la station diffère la transmission. Une fois le canal redevenu libre, la station attend pendant un temps aléatoire déterminé par l'algorithme stochastique d'attente, puis tente à nouveau de transmettre.

L'algorithme stochastique d'attente utilise un temps d'attente exponentiel, c'est-à-dire que si après l'attente le canal se trouve toujours occupé, l'intervalle de temps dans lequel l'algorithme puise ses valeurs se verra augmenté d'une façon exponentielle.

Une collision peut se produire si deux stations commencent à émettre en même temps, les collisions doivent être identifiées afin que les retransmissions se fassent par la couche MAC et non pas par les couches supérieures. Les protocoles filaires tel que Ethernet règlent ce problème en utilisant le protocole CSMA avec détection de collisions CSMA/CD. La détection des collisions n'est pas implémentée dans les protocoles sans fil pour deux raisons majeures :

- on ne peut pas assurer que toutes les stations s'écoutent entre elles (cas de la station cachée), alors que ceci est l'hypothèse de base de la détection de collision;
- la détection de collision requiert des émetteurs full duplex, alors que les émetteurs radio communiquent en semi duplex, c'est-à-dire qu'ils ne peuvent envoyer et recevoir en même temps.

Pour parer au problème de collision, le protocole 802.11 utilise le mécanisme d'évitement de collisions avec accusé de réception.

Pour expliquer le fonctionnement du protocole, prenons l'exemple de la figure 2.3 et examinons ce qui se passe. La station A qui veut envoyer des données à B, commence par envoyer une trame RTS. Lorsque B reçoit la demande, elle répond par une trame CTS pour que A puisse commencer à envoyer les données. A la réception de la trame CTS la station A envoie une trame de donnée et attend l'acquittement (ACK). Lorsque B aura reçu la trame complète, elle répondra par une trame ACK ce qui met fin à la transmission. Si le temps d'attente de l'acquittement de A expire avant la

réception de la trame ACK envoyée par B, A considère que la trame n'a pas été reçue et doit la retransmettre.

Les autres stations du réseau qui ont reçu, soit la trame RTS, soit la trame CTS, activent l'indicateur d'écoute virtuelle de la porteuse appelé vecteur d'allocation de réseau ou NAV pour «*Network Allocation Vector*» pendant la durée de transmission (indiquée dans les trames RTS et CTS). Le NAV est un indicateur virtuel de canal occupé comme illustré dans la figure 2.8.

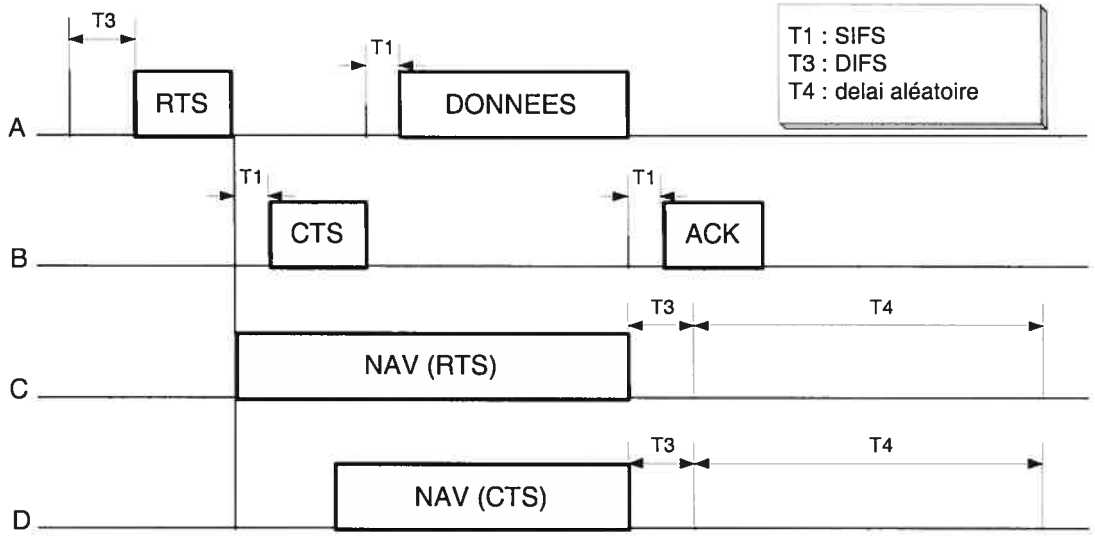


Figure 2.8 : détection virtuelle de la porteuse

2.4.3. Fragmentation et défragmentation

Les transmissions sans fil se caractérisent par un taux d'erreur élevé, et la probabilité d'erreur augmente avec la taille des paquets. Pour résoudre se problème, le protocole 802.11 autorise la fragmentation de trames en portions plus petites, qui sont acquittées individuellement suivant le protocole de type «envoyer et attendre». Ceci permet, en cas d'erreur, de ne renvoyer que les fragments erronés.

2.4.4. Espace de temps entre les trames

Dans la figure 2.8 les trames sont espacées par des intervalles de temps qui diffèrent selon le type de trame. Le protocole 802.11 définit quatre types d'intervalle de temps appelés espace de temps entre les trames, qui sont utilisés pour établir des priorités entre les trames. Ils sont ici présentés par ordre de durée croissante.

- SIFS : Intervalle court inter trame ou SIFS pour «*Short InterFrame Spacing*». C'est le plus petit intervalle de temps possible et il donne la plus grande priorité. Il est utilisé pour les trames telles que CTS et ACK.
- PIFS : Intervalle inter trame FCP ou PIFS pour «*Point InterFrame Spacing*». Il est utilisé par le point d'accès pour prendre possession du canal avant les stations.
- DIFS : Intervalle inter trame FCD ou DIFS pour «*Distibuted InterFrame Spacing*». Utilisé par les stations désirant commencer une transmission.
- EIFS : Intervalle inter trame étendu ou EIFS pour «*Extended InterFrame Spacing*». Utilisé par les stations recevant un paquet qu'elles n'arrivent pas à interpréter.

2.4.5. La fonction de coordination par point (FCP)

Le mode FCP est une méthode d'accès optionnelle implémenté par-dessus le mode FCD. Il n'est utilisé que dans le mode avec infrastructure, par conséquent il ne concerne pas les réseaux ad hoc.

Dans ce mode, c'est le point d'accès qui va inviter les stations à émettre en les interrogeant, et comme c'est la station de base qui régule les transmissions, les collisions ne peuvent pas avoir lieu.

2.5. Le protocole 802.11 et les réseaux ad hoc multi saut

Le protocole 802.11 prévoit de fonctionner en mode ad hoc. Selon la définition donnée par le groupe de travail 802.11 [13], un réseau ad hoc est composé de stations à portée d'émissions les unes des autres. Mais qu'en est-il des réseaux ad hoc multi saut ? Autrement dit le cas qui nous intéresse dans ce travail.

Le protocole 802.11 est implémenté dans tous les simulateurs de réseaux, parfois c'est le seul disponible; il est utilisé dans quasiment tous les travaux sur les réseaux ad hoc (routage, transport, applications ...), sauf, bien sûr, dans les travaux qui ont pour objectif de concevoir des protocoles pour la sous-couche MAC. Le protocole 802.11 est aussi utilisé dans les plates-formes de tests, en effet, les cartes réseaux sans fil les plus disponibles sur le marché sont du type 802.11, quoique qu'il existe des cartes Bluetooth [3] aussi, mais le protocole Bluetooth est conçu pour fonctionner sur des distances très courtes.

Néanmoins, l'utilisation du protocole 802.11 a été remise en question dans certains travaux [19] [20]. En effet, Xu et Saadawi [19] ont montré que des problèmes rencontrés avec le protocole TCP sur les réseaux ad hoc multi-saut tel que le problème de stabilité, le problème d'impartialité dans l'occupation de canal entre deux ou plusieurs session TCP, ou encore l'impossibilité de coexistence simultanée de session TCP résident en fait au niveau du protocole 802.11. Des modifications du protocole 802.11 pour l'adapter aux réseaux ad hoc multi-saut ont été proposées comme dans [21].

Cependant beaucoup de temps pourrait s'écouler avant qu'un protocole pour la sous-couche MAC plus adapté pour les réseaux ad hoc multi-saut fasse l'unanimité et apparaisse sur le marché. En attendant, le protocole 802.11 reste une très bonne alternative et les améliorations des débits enregistrés dans les dernières versions laissent présager que ce protocole primera encore pour quelques années dans le domaine des ordinateurs sans fil.

Chapitre 3

État de l'art - routage et qualité de service dans les réseaux ad hoc

Après un aperçu du fonctionnement de la couche liaison de données des réseaux ad hoc, nous allons monter d'un niveau dans l'architecture des réseaux pour voir ce qui a été fait au niveau de la couche réseau, plus particulièrement les protocoles de routage dans les réseaux ad hoc qui sont le thème de ce mémoire de maîtrise.

Nous verrons aussi les travaux réalisés relativement à la qualité de service et ceci à différents niveaux d'implémentation.

3.1. Routage dans les réseaux ad hoc

La recherche sur le routage dans les réseaux sans fil date du début des années 70 quand le DARPA «*U.S. Defense Advanced Research Projects Agency*» a commencé le projet PRNET «*Packet Radio Network*» [22] et son successeur SURAN «*Survivable Adaptive Networks*» [23] . Le protocole de routage de PRNET utilise une forme de routage à vecteurs de distance, où chaque nœud diffuse un paquet de mise à

jour de route toutes les 7.5 secondes. L'entête de chaque paquet contient les adresses des nœuds source et destination, le nombre de sauts effectués depuis la source et le nombre de sauts restants pour atteindre la destination (basé sur la table de routage de la source), les nœuds recevant ce paquet mettent à jour leur table de routage sur la base des informations contenues dans l'entête de ce paquet.

Plusieurs protocoles de routage ont été conçus pour les réseaux ad hoc, ils se classifient selon le type de routage utilisé (proactif, réactif, ...). Le groupe MANET «*Mobile Ad hoc NETworking*» [1] de IETF «*Internet Engineering Task Force*» [2] a pour premier objectif de standardiser un ou plusieurs protocoles de routage IP pour les réseaux ad hoc [24].

3.2. Protocoles de routage proactif

Dans un protocole de routage proactif, chaque nœud maintient une table de routage qui contient les informations sur tous les autres nœuds du réseau. Ceci s'accomplit par des échanges d'information entre les nœuds à intervalles de temps régulier ou dès qu'il y a un changement dans une des tables de routage.

Selon les informations de routage échangées et les méthodes de calcul des routes utilisées, on distingue deux grandes familles de routage, les routages à vecteurs de distance et les routages à état de liens.

Dans un routage à vecteurs de distance, chaque nœud diffuse périodiquement sa table de routage à ses voisins, la table contient les adresses des nœuds destination du réseau et la distance en nombre de sauts pour atteindre chacun d'eux. Un nœud met sa table de routage à jour s'il trouve une route plus courte que celle qu'il a dans sa table, ou si le nœud par lequel il passe pour atteindre une destination donnée change la distance vers cette destination, ou encore s'il trouve un nœud inconnu (c'est-à-dire, qui n'existe pas dans sa table).

Dans un routage à état de liens, chaque nœud vérifie l'état des liaisons avec ces voisins (peut aussi calculer le coût de ces liens), et diffuse un paquet contenant ces informations à tout le réseau. Ces diffusions permettent à chaque nœud d'avoir une connaissance complète de la topologie du réseau. Pour calculer les routes, l'algorithme du plus court chemin de Dijkstra (voir [15] pour une référence générale sur les algorithmes de chemin et [16] pour leur utilisation dans les réseaux de communication) est utilisé.

Le routage proactif est le plus utilisé dans les réseaux filaires où les liens entre les nœuds sont très stables, avec des pannes peu fréquentes sur les liaisons et où les routeurs ne tombent pas trop souvent en panne.

Ce n'est pas le cas dans les réseaux mobiles, où le déplacement d'un nœud peut rompre un ou plusieurs liens, ce qui induit des changements dans les tables de routage. Si un protocole de routage proactif est utilisé, la densité d'échanges d'information de routage devient très grande et diminue la performance du réseau dans l'acheminement de données.

Cependant, dans certains contextes, l'utilisation d'un protocole de routage non proactif peut engendrer des temps d'attente supplémentaires de recherche de route inacceptables. Dans un tel cas, si la bande passante et les ressources du réseau le permettent, un routage proactif optimisé peut être utilisé. Ceci explique les raisons qui ont poussé le groupe MANET à retenir deux protocoles proactifs à état de liens dans le but de les standardiser, et qui sont TBRPF [25] et OLSR [26].

Un des premiers protocoles proposés pour les réseaux ad hoc était aussi proactif, il a pour nom DSDV «*Destination Sequenced Distance Vector routing*».

3.2.1. Le protocole de routage DSDV

DSDV [27] est un protocole à vecteurs de distance basé sur l'algorithme distribué de Bellman-Ford avec quelques améliorations.

Chaque nœud maintient une table de routage qui contient une entrée pour chacun des autres nœuds du réseau, cette entrée contient les informations suivantes :

- identifiant du nœud ;
- le nombre de sauts pour atteindre ce nœud ;
- un numéro de séquence attribué par le nœud destination, ce numéro permet de reconnaître la dernière mise à jour de route et préserve ainsi le réseau du bouclage.

Les mises à jour dans DSDV sont transmises périodiquement à travers deux types de paquets.

Mise à jour complète

Elle correspond à un envoi de toutes les informations de la table de routage et nécessite plusieurs paquets pour l'envoi.

Mise à jour incrémentale

Occasionnellement, un paquet contenant les changements depuis la dernière mise à jour complète est envoyé, cette opération ne nécessite qu'un seul paquet. Une table additionnelle est maintenue par chaque nœud pour la sauvegarde des mises à jour incrémentales.

3.2.2. Le protocole de routage TBRPF

TBRPF [28] «*Topology Broadcast Protocol for Dynamic Networks*» est un protocole de routage proactif à état de liens. Chaque nœud calcule un arbre ayant comme racine la destination (un arbre est calculé pour chaque destination atteignable du réseau), le calcul de l'arbre se fait par l'algorithme de Dijkstra en se basant sur la table de topologie et la table des voisins.

Chaque nœud maintient à son niveau les informations suivantes :

- la table de topologie qui contient tous les arcs du réseau, chaque arc a un coût et un numéro séquentiel de mise à jour ;
- la table des voisins ;
- et pour chaque destination du réseau, le nœud maintient l'information nœud père (dans l'arbre qui a comme racine cette destination) et les nœuds fils.

Le nœud père est calculé par l'algorithme de Dijkstra en se basant sur la table de topologie et la table des voisins. Un message est envoyé au père pour l'informer de ce choix, ce message sert aussi à construire la liste des fils.

L'arbre est construit à partir des feuilles vers la racine, par contre, la mise à jour se fait à partir de la racine par envoi des tables de topologie. TBRPF utilise une mise à jour périodique et différentielle, où chaque nœud diffuse sa table pour ses fils seulement, ce qui réduirait le trafic par rapport à la diffusion pure.

TBRPF utilise aussi des messages d'information entre voisins pour mettre à jour l'état des liens entre voisins.

3.2.3. Le protocole de routage OLSR

OLSR [29] «*Optimized Link State Protocol*» est un protocole de routage proactif à état de liens. OLSR est vu comme une optimisation des protocoles à état de liens, le trafic des paquets de contrôle est réduit par la sélection des nœuds qui en feront la diffusion. Chaque nœud sélectionne parmi ses voisins immédiats (un seul saut) un ensemble de nœuds qu'il appelle relais multipoints, à qui revient la tache de diffusion. L'ensemble des relais multipoints est calculé de manière à ce que l'ensemble des nœuds à un saut qu'il contient permet d'atteindre tous les nœuds se trouvant à deux sauts. Chaque nœud doit diffuser, à intervalle de temps régulier, un message d'information à ses voisins immédiats. Ce message contient la liste de tous

les voisins du nœud et sa liste des relais multipoints. La diffusion des messages d'information permet la mise à jour de la table de voisins, dans laquelle il y a une entrée pour chaque voisin immédiat ainsi que pour les voisins de ce dernier (nœuds à deux sauts qu'il permet d'atteindre). Les messages d'informations permettent aussi de mettre à jour la table des sélecteurs: dans cette table, chaque nœud met la liste des nœuds qu'ils l'ont sélectionné comme relais multipoints. La table des sélecteurs est diffusée dans tout le réseau à travers les relais multipoints pour minimiser le trafic.

Chaque nœud maintient aussi une table de topologie construite à partir des tables de sélecteurs reçus. Chaque entrée de la table de topologie contient l'adresse du nœud (dernier nœud avant la destination) et sa table de sélecteurs (destinations potentielles), qui seront considérés comme des paires (dernier nœud, destination). La table de routage est construite à partir de la table de topologie en recherchant les paires connectées dans l'ordre descendant. Pour trouver la route vers la destination D, il faut trouver la paire (X, D), puis la paire (Y,X) jusqu'à ce qu'un voisin du nœud source soit trouvé.

3.3. Protocoles de routage réactif

Au lieu de maintenir des tables de routage en tout temps, le routage réactif crée les routes à la demande du nœud émetteur. Quand un nœud a besoin de connaître une route vers une destination donnée, une procédure de découverte de route est lancée. Une fois que la route est déterminée, elle sera maintenue par une procédure de maintenance de route. L'instabilité des liens dans les réseaux ad hoc due aux déplacements des nœuds rend le routage réactif plus adapté à ces réseaux par rapport au routage proactif.

En effet, il est plus raisonnable d'établir des routes à la demande que de maintenir des échanges d'information sur les routes entre les nœuds avec des informations qui

changent très fréquemment. Le groupe MANET a ainsi retenu deux protocoles de routage réactif qui sont DSR [30] et AODV [31].

3.3.1. Le protocole de routage DSR

DSR «*Dynamic Source Routing*» [32] est un protocole réactif basé sur le routage par la source, c'est-à-dire que la source des données détermine le chemin complet par lequel les données vont transiter et le transmet avec les données. Dans chaque paquet transmis, il y a un champ qui contient la séquence de nœuds à suivre pour atteindre la destination.

Ce protocole consiste en deux procédures, une procédure de découverte de route et une procédure de maintenance de route.

Procédure de découverte de route

Le nœud initiateur de la procédure de découverte de route, diffuse un paquet de requête de route. Si la requête aboutit à la destination, le nœud initiateur reçoit un paquet réponse de route qui contient la séquence de nœuds par laquelle le premier paquet de requête de route a atteint la destination. La requête de route contient le champ enregistrement de route dans lequel s'enregistre l'adresse de tous les nœuds visités par le paquet voir la figure 3.1 pour une illustration.

La réponse de route retransmet donc cette séquence de route, voir la figure 3.2 pour une illustration.

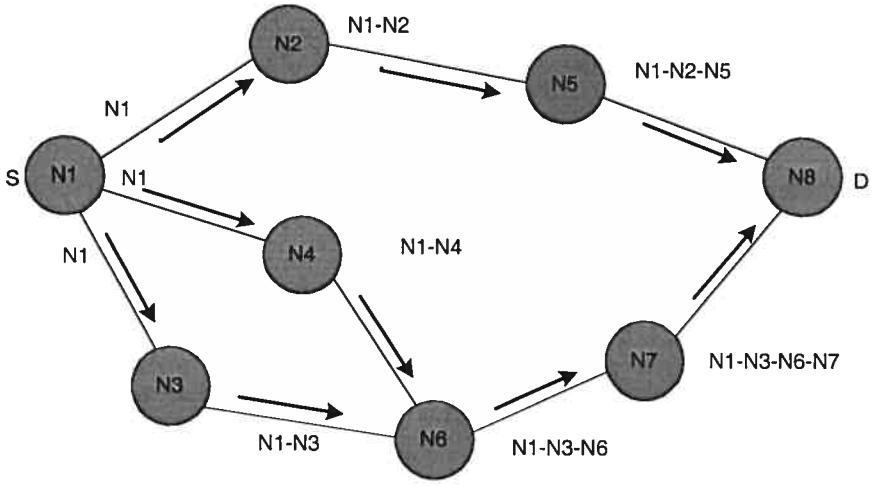


Figure 3.1 : construction de la route source de la requête de route dans DSR.

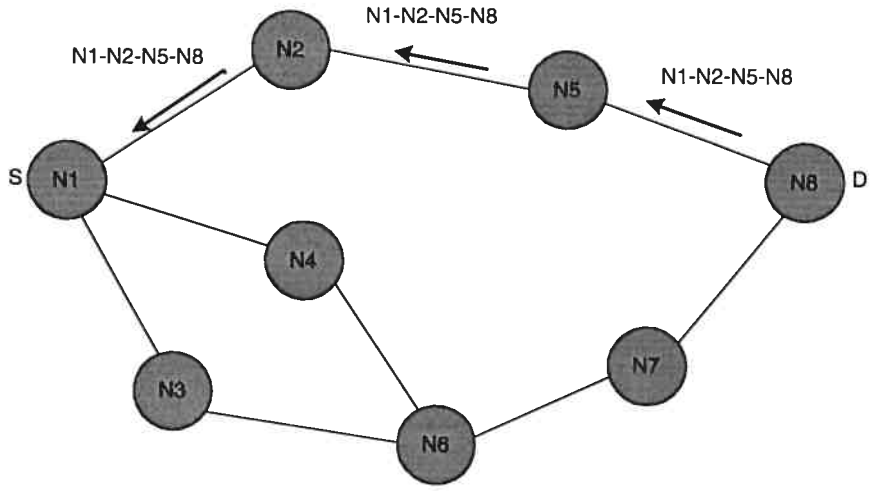


Figure 3.2 : propagation de la réponse de route dans DSR.

La réponse de route que nous venons de décrire s'applique dans le cas ou les liens sont symétriques. Dans le cas ou le réseau supporte des liens asymétriques, le nœud destination doit à son tour initier une requête de route vers le nœud source lorsqu'il reçoit la requête de route.

DSR utilise une procédure de maintenance de route pour s'assurer de la validité des chemins utilisés. Quand un nœud détecte que le nœud qui le suit dans la route source

n'est plus atteignable, il envoie un paquet erreur de route vers le nœud source pour l'informer que la route n'est plus valide et qu'il doit initier une autre requête de route s'il n'a pas d'autres routes disponibles dans son cache de routes.

3.3.2. Le protocole de routage AODV

AODV «*Ad hoc On-Demand Distance Vector*» [33] a été conçu comme une amélioration de DSDV. Il s'agit d'un protocole de routage réactif, qui utilise le routage saut par saut : chaque nœud qui reçoit un paquet a pour charge de déterminer à qui l'envoyer en consultant sa table de routage.

Comme dans DSR, le nœud source diffuse une requête de route (RREQ) pour obtenir un chemin vers une destination donnée. Cette requête est diffusée dans le cas où le nœud source n'a pas de route vers la destination ou que la durée de vie de la route a expiré.

Chaque requête de route est identifiée par un numéro de requête qui, avec l'adresse du nœud source, identifie d'une façon unique la requête dans le réseau.

Pendant la propagation de la requête de route, les nœuds intermédiaires enregistrent dans leurs tables de routage l'adresse du nœud qui leur a envoyé la requête dans l'entrée correspondant au nœud source afin d'établir un chemin inverse pour cette requête, voir la figure 3.3 pour une illustration.

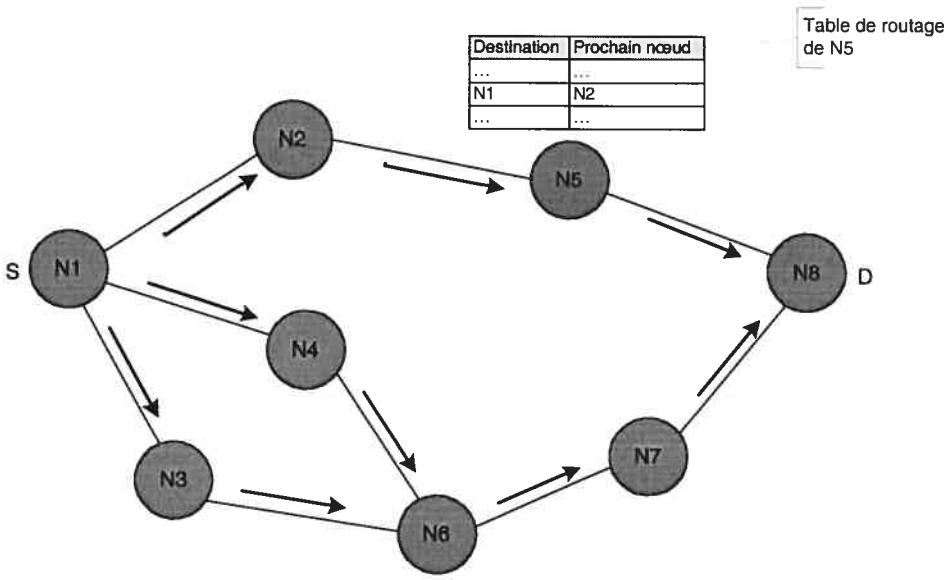


Figure 3.3 : propagation du paquet RREQ dans AODV.

Une fois la requête arrivée au nœud destination, ce dernier répond par un paquet réponse de route (RREP). Pendant la propagation du paquet RREP les nœuds intermédiaires mettent à jour l'entrée correspondant au nœud destination dans leurs tables de routage, voir la figure 3.4.

Compte tenu du fait que les nœuds mettent à jour leurs tables de routages en établissant des chemins inverses, AODV ne fonctionne que sur les réseaux ayant des liens symétriques.

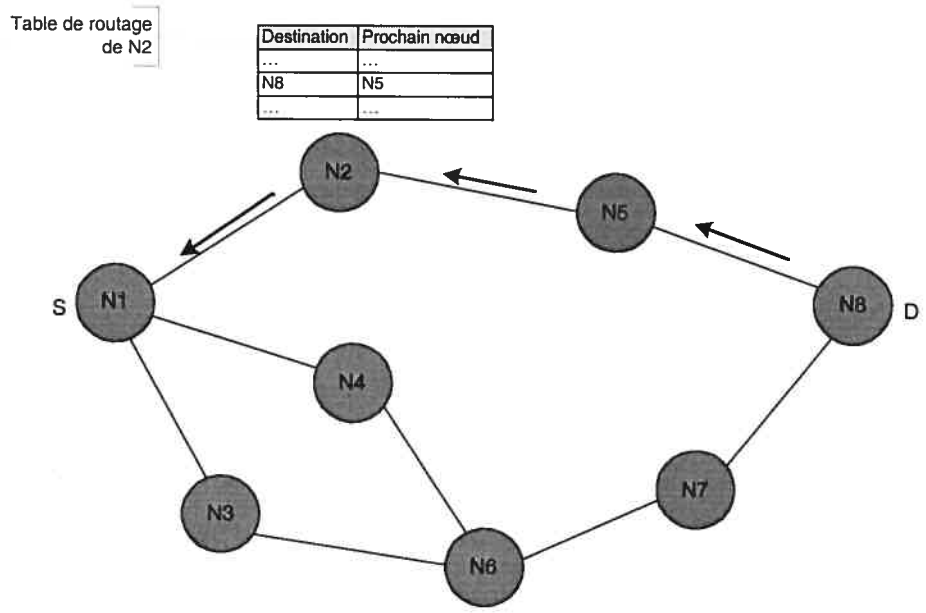


Figure 3.4 : propagation du paquet RREP dans AODV.

Plusieurs autres protocoles de routage réactif ont été proposés pour les réseaux ad hoc, le lecteur intéressé peut se référer à [34].

3.4. Les protocoles de routage hybride

Les protocoles de routage hybride se présentent comme une alternative entre le routage proactif et le routage réactif. D'un coté, ils limitent le routage proactif dans des régions, et d'un autre coté, ils réduisent la diffusion de la requête de route du routage réactif à certains nœuds du réseau.

3.4.1. Le protocole ZRP

ZRP [35] «*Zone Routing Protocol*» est un protocole de routage hybride (proactif/réactif). Le routage réactif se limite à la zone déterminée par le nombre de sauts ρ, ainsi si $\rho = 2$, pour chaque nœud, le routage proactif sera limité aux voisins se trouvant à deux sauts de lui au plus. Dans ses spécifications, ZRP [35] utilise

DSDV avec de petites modifications comme protocole de routage proactif, mais n'importe quel autre protocole proactif pourrait être utilisé.

Pour le routage interzone, ZRP emploie un protocole réactif. Si le nœud source ne trouve pas la destination dans sa zone, il envoie une requête de route aux nœuds de bord de sa zone. Par exemple, si $\rho = 2$, les nœuds de bord de la zone sont ceux qui se trouvent à deux sauts de la source, les nœuds se trouvant à un saut de la source, sont dans la zone, mais ne sont pas des nœuds de bord. Chaque nœud qui reçoit la requête, vérifie si la destination se trouve dans sa zone. Si c'est le cas, il envoie une réponse de route au nœud source. Sinon, il envoie la requête aux nœuds de bord de sa zone à lui qui exécuterons la même procédure.

3.5. Protocoles de routage géographique

Les protocoles de routage réactif font de la diffusion pure pour les requêtes de route, faute d'information sur le réseau. L'inconvénient majeur de la diffusion pure est l'augmentation du trafic dans le réseau : si le réseau a une taille de quelques centaines voir de milliers de nœuds, la diffusion risque de provoquer une congestion dans le réseau.

Les protocoles de routage géographique, appelés aussi protocoles de routage basés sur les positions, utilisent les informations sur les positions des nœuds pour éviter de faire de la diffusion pure et ainsi réduire le nombre de nœuds participants à la découverte de route et par la même occasion réduire le taux de congestion du réseau.

Dans un protocole de routage géographique, un nœud qui veut obtenir une route vers un autre nœud, doit connaître sa position, celle de ses voisins immédiats et celle du nœud destination. Ces informations vont permettre de sélectionner qui, parmi les nœuds voisins, seront choisis pour acheminer la requête de route vers la destination.

Le fait que les protocoles géographiques réduisent le nombre de nœuds participants à la découverte de route et réduisent ainsi la congestion du réseau, les rend plus adaptés aux réseaux ad hoc de grande taille.

Les positions des nœuds peuvent être obtenues par le système GPS si les nœuds sont équipés de récepteurs GPS. Dans le cas où les nœuds ne sont pas équipés de récepteurs GPS, des méthodes géométriques pour obtenir les positions (relatives) des nœuds ont été proposées, voir par exemple [36]. Ces méthodes sont beaucoup moins précises que le système GPS.

3.5.1. Le protocole de routage LAR

LAR «*Location Aided Routing*» [37] se propose comme une amélioration des protocoles de routage qui utilisent la diffusion pour la découverte de route. Cette amélioration est obtenue en utilisant les positions des nœuds. Le nœud source calcule la zone dans laquelle la destination est prévue se trouver en se basant sur sa dernière position, soit un cercle centré en D, la dernière position de la destination connue par la source. La zone de diffusion est déterminée par le rectangle qui comprend le nœud source et le cercle centré en D, voir la figure 3.5.

La source envoie la requête de route vers les nœuds voisins qui sont dans la zone de diffusion seulement et qui sont plus proches de la destination que lui. Chaque nœud intermédiaire fait la même chose jusqu'à ce que la requête atteigne la destination.

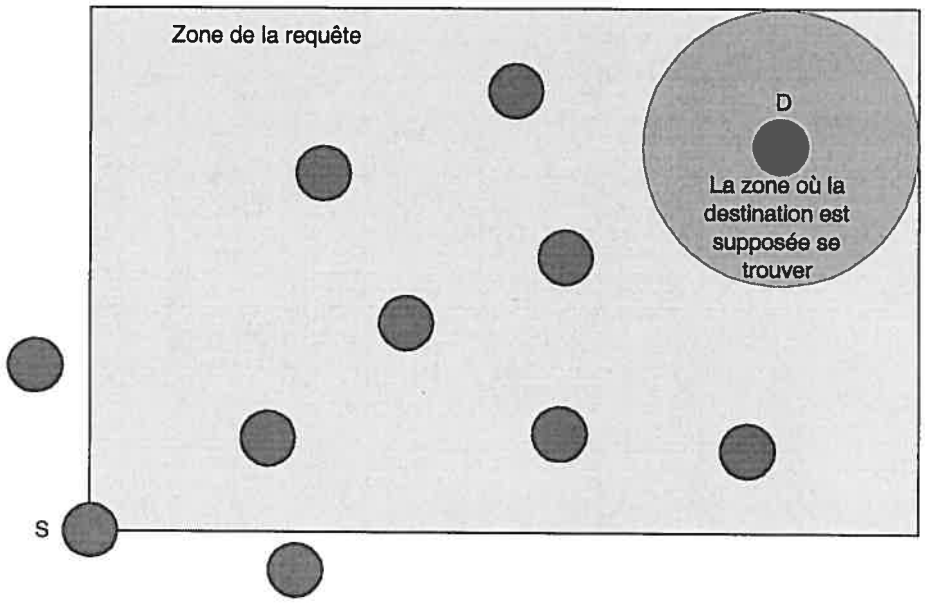


Figure 3.5 : la zone de diffusion dans LAR.

L'absence d'infrastructure fixe ou de station fixe pour récupérer les positions des nœuds dans les réseaux ad hoc, pose le problème de mise à jour des positions. En effet, en utilisant le système GPS (ou une autre méthode) le nœud ne peut connaître que sa propre position. Le problème de trouver la position du nœud destination se révèle être aussi complexe que le problème de routage lui-même [39]. Plusieurs méthodes ont été proposées, ces méthodes vont de la diffusion simple de position à l'élection de serveurs de position suivant leur degré (nombre de voisins) et leur position [40].

Les méthodes de découverte de route utilisées par les protocoles de routage géographiques peuvent, dans certain cas, échouer à trouver un chemin vers la destination. Une procédure de recouvrement qui assure la livraison du paquet de découverte de route est utilisée pour remédier à ce problème. Dans le cas de LAR, la diffusion pure est utilisée comme procédure de recouvrement. Si un nœud ne reçoit pas de réponse de route après un temps déterminé, il diffuse une requête de route qui se propagera dans tout le réseau.

Un grand nombre de protocoles pour les réseaux ad hoc font partie de la famille des protocoles de routage géographique, pour plus d'informations sur ces protocoles, voir [38] et [40].

3.6. Protocoles de routage hiérarchique

Les réseaux de grande taille tel que le réseau Internet ou les réseaux téléphoniques ont une structure hiérarchique, ceci permet de prévoir les extensions futures, et facilite la gestion de ces réseaux.

Des protocoles de routage hiérarchique ont été proposés pour les réseaux ad hoc afin de leur imposer une topologie hiérarchique. Le réseau est décomposé en plusieurs groupes, chaque groupe a un nœud responsable du groupe et communique avec les autres groupes à travers un nœud passerelle, voir la figure 3.6 [41].

La formation des groupes se fait généralement suivant les positions géographiques des nœuds. Le choix du responsable du groupe peut se faire sur le degré des nœuds, comme il peut se faire sur l'ordre d'arrivée dans le groupe. Pour tenir compte du déplacement des nœuds, il y a toujours une procédure d'élection et une procédure de révocation du responsable du groupe.

Chaque nœud dans un groupe doit pouvoir communiquer directement avec le responsable. Si un nœud veut communiquer avec un autre se trouvant sur un autre groupe, la communication passera d'abord par le responsable puis par la passerelle pour aller vers d'autres groupes jusqu'à ce que le groupe où se trouve le nœud destinataire soit atteint.

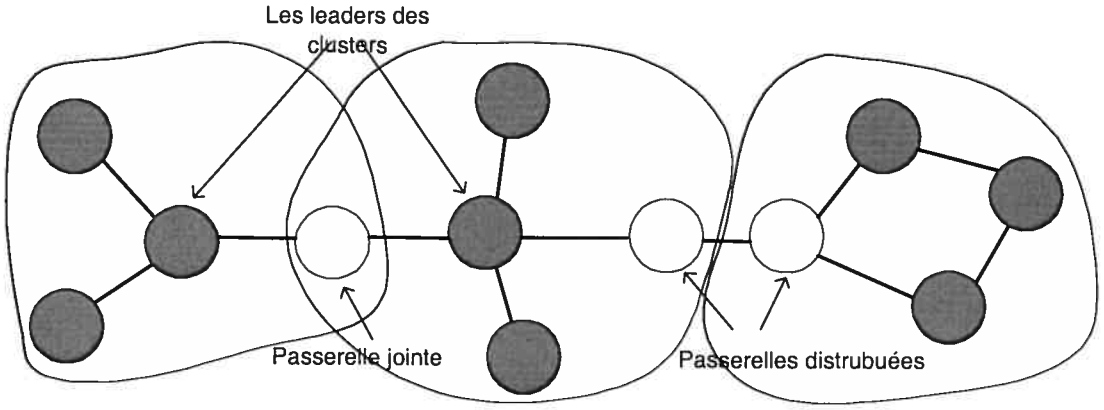


Figure 3.6 : communication entre groupes dans un protocole de routage hiérarchique.

3.7. Autres protocoles de routage pour les réseaux ad hoc

D'autres protocoles de routage se basent sur d'autres caractéristiques des réseaux ad hoc pour déterminer une métrique sur laquelle les choix de route s'effectuent. La consommation d'énergie est une caractéristique importante dans les réseaux ad hoc. Aussi, plusieurs protocoles la prennent en considération dans le but de maintenir le plus longtemps possible le réseau en marche. En effet, un nœud qui consomme la totalité de son énergie n'est plus en mesure de communiquer et est donc coupé du réseau.

Dans [42], l'algorithme de routage utilise une fonction $f(A)$ qui évalue la réticence du nœud A à envoyer le paquet, et choisit le chemin qui minimise la somme des $f(A)$ des nœuds du chemin. Cet algorithme s'intéresse aux nœuds à énergie critique, la fonction f est égale a $1/g(A)$ où $g(A)$ est la durée d'énergie restante pour le nœud A, (la fonction g est définie sur l'intervalle [0,1]), ce qui fait que la réticence augmente quand l'énergie diminue.

3.8. Qualité de service pour les réseaux ad hoc

La qualité de service dans un réseau est définie par l'ensemble des mécanismes mis en œuvre pour satisfaire les contraintes (besoin en ressources) pour le transfert d'un flux d'une source à une destination.

Beaucoup de travaux ont été menés sur la qualité de service dans les réseaux filaires, et plusieurs modèles ont été proposés et implémentés sur des routeurs. Cependant ils ne sont pas directement applicables aux réseaux ad hoc à cause des caractéristiques de ces derniers. En effet, pour qu'un réseau puisse supporter la qualité de service, les informations telle que la bande passante ou le délai doivent être gérables. Cependant il est très difficile de collecter et de gérer les informations sur l'état des liens dans les réseaux ad hoc à cause du changement fréquent de l'état des liaisons sans fil, les ressources limitées et la mobilité.

Dans les réseaux ad hoc la qualité de service a été étudiée à différents niveaux de l'architecture des réseaux : la qualité de service au niveau MAC, protocole de routage avec qualité de service, protocole de signalisation, pour la réservation et la libération des ressources, et enfin un modèle de qualité de service, c'est-à-dire une architecture qui définit les services qui peuvent être fournis et les mécanismes utilisés afin de les offrir. Nous allons présenter ces niveaux et nous citerons un travail comme exemple de la qualité de service à chacun des niveaux.

3.8.1. Modèles de qualité de service pour Internet

IETF a proposé deux modèles de qualité de service pour Internet, IntServ/RSVP [43] et DiffServ [44].

IntServ/ RSVP est un modèle de qualité de service qui utilise la granularité par flot, l'état du flot est gardé sur tous les routeurs (qui intègrent IntServ). Le flot est une session d'une application entre deux nœuds terminaux.

IntServ est implémenté avec quatre composantes. Le protocole de signalisation RSVP, le contrôle d'admission, le classificateur et enfin l'ordonnanceur de paquets.

IntServ requiert un volume de traitement important, ce qui engendre des problèmes de consommation dans le cas des réseaux mobiles. De plus, la signalisation de type RSVP n'est pas adaptée à ce type de réseaux car trop volumineuse par rapport à la bande passante limitée des réseaux sans fil.

DiffServ a été proposé pour remédier à la difficulté d'implanter et de déployer IntServ/RSVP dans Internet. DiffServ est basé sur la granularité de service par classe et fournit un nombre limité de classes d'agrégation. Ce sont les routeurs placés aux extrémités du réseau (les routeurs de bord) qui contrôlent le trafic en classifiant et en marquant les paquets, les autres routeurs acheminent les paquets en se basant sur le marquage effectué sur les paquets par les routeurs des extrémités.

Le modèle DiffServ semble plus adapté aux réseaux ad hoc. Cependant, il a été conçu pour des réseaux possédant une bande passante importante et dont la topologie est relativement statique.

3.8.2. FQMM : un modèle de qualité de service pour les réseaux ad hoc

FQMM [45], pour «*Flexible Qualité of service Model for Mobile ad hoc networks*», est un modèle de qualité de service conçu spécialement pour les réseaux ad hoc, qui essaie de tirer avantage de la granularité de services par flot dans IntServ et la différentiation de services dans DiffServ en se situant entre les deux, tout en prenant en considération les caractéristiques des réseaux ad hoc.

Comme pour DiffServ trois types de nœuds sont définis : les nœuds d'entrée (source), les nœuds intermédiaires et les nœuds de sortie (destination). La classification et le marquage des paquets sont à la charge des nœuds d'entrée.

FQMM requiert un protocole de routage capable de trouver des routes satisfaisant certaines contraintes (délai, bande passante).

3.8.3. Protocoles de signalisation

Les protocoles de signalisation fournissent un moyen de propager les informations de contrôle dans le réseau, la signalisation en qualité de service est utilisée pour réserver et libérer les ressources. On distingue deux types de signalisation, les signaux intra bande, où le contrôle d'information est inclus dans le paquet, et les signaux hors bande, où un paquet de contrôle explicite est utilisé.

Insigna

Insigna [46] est un protocole de signalisation intra bande conçu pour la qualité de service dans les réseaux ad hoc et permet de réserver la bande passante.

Insigna utilise une granularité par flot et offre une qualité de service aux applications capables d'adapter leurs comportements en fonction de la bande passante disponible. Deux niveaux de qualité de service peuvent être spécifiés, le niveau de base qui permet de spécifier la bande passante minimale et le niveau amélioré qui permet de spécifier le débit optimal dans le cas où les ressources seraient disponibles.

Les informations transmises par Insigna sont incluses dans chaque paquet de données dans l'entête IP, ce champ est rempli par le nœud source et pourra être modifié tout au long du chemin. Insigna n'est pas lié à un protocole de routage particulier.

3.8.4. Routage avec qualité de service

Les protocoles de routage avec qualité de service cherchent à trouver des routes satisfaisant certaines contraintes. Par exemple, on s'intéressera à des routes disposant

d'une certaine bande passante ou des routes assurant que les paquets seront livrés dans un certain délai.

Plusieurs études ont été faites sur le routage avec qualité de service et quelques protocoles ont été proposés, voir les références récentes pour plus de détails [47][48][49][50][51][52][53][54][55].

Ticket Based Probing

L'obtention des routes par diffusion pure inonde le réseau et la recherche de route devient très coûteuse. Le but du protocole Ticket Based Probing [48] est de limiter le coût de recherche de route et de fournir des garanties sur la qualité de service.

Un nœud qui veut établir une route avec des contraintes de qualité de service, associe à sa demande de route un certain nombre d'étiquettes, chaque étiquette correspond à un chemin de recherche, ce qui fait que le nombre de chemins de recherche est limité par le nombre d'étiquettes qui est lui même choisi selon le flux de données à transmettre.

Dans [49], les auteurs ont proposé un protocole de routage multi-chemin avec qualité de service lui aussi basé sur la distribution d'étiquettes.

3.8.5. Qualité de service au niveau de la couche MAC

Les protocoles de la couche MAC assurent le partage de la bande passante, ils ont la responsabilité d'éviter les collisions et de résoudre les problèmes liés aux transmissions radio.

Qualité de service au niveau du protocole IEEE 802.11

Comme nous l'avons vu dans le chapitre 2, chaque nœud doit s'assurer que le canal est libre depuis un temps DIFS avant de commencer à émettre. Un temps aléatoire est ajouté au DIFS pour éviter que deux nœuds émettent en même temps et entrent en collision, ce délai aléatoire est compris entre deux valeurs Cwmin et CWmax.

Dans [56] les auteurs ont proposé de doter le protocole 802.11 d'un mécanisme de priorité entre les trames, en affectant aux trames les plus prioritaires des délais proches de CWmin et aux trames les moins prioritaires des délais proches de Cwmax.

Chapitre 4

Deux nouveaux protocoles de routage pour les réseaux ad hoc

4.1. Un nouveau protocole de routage pour les réseaux ad hoc mobiles

Les protocoles de routage réactifs tel que DSR et AODV utilisent la diffusion pure pour leurs requêtes de routes. Cette méthode peut rapidement devenir coûteuse en ressources dans les réseaux ad hoc. Le fait que la quasi-totalité des nœuds du réseau reçoivent la requête de route peut mener à une surcharge de trafic, et ceci nuit aux performances du réseau (taux de paquets reçus, délai,...).

Les protocoles de routage géographique réduisent la diffusion des requêtes de route à un certain nombre de nœuds. Ceci est rendu possible par la connaissance des positions des nœuds voisins et celle de la destination ce qui aide à orienter la requête par une sélection des nœuds qui sont en charge d'acheminer un paquet vers sa destination.

Ces protocoles ont néanmoins besoin d'une procédure de mise à jour des positions des nœuds pour qu'ils puissent fonctionner. Comme cité dans la section 3.5, cette procédure peut être aussi coûteuse que la recherche de route. En effet, pour connaître la position d'une destination (qui n'est pas un voisin immédiat) une stratégie de mise à jour et de diffusion des positions doit être mise en œuvre. Les stratégies qui ont été mises en œuvre dans des implémentations de protocoles de routage géographique pour les réseaux ad hoc varient selon les caractéristiques des réseaux. La méthode la plus simple à mettre en œuvre, mais aussi la plus coûteuse en trafic, est la diffusion pure des positions. D'autres implémentations utilisent un serveur de position où chaque nœud envoie sa position et récupère celles des autres nœuds. Cette méthode se trouve être bonne si le serveur est fixe mais le devient beaucoup moins si le serveur est mobile, parce qu'il faut connaître la position du serveur et une route valide vers lui. Enfin, on trouve aussi la diffusion hiérarchique quand le réseau est divisé en groupes et qu'un serveur de position est désigné dans chaque groupe.

Dans notre travail, nous proposons un protocole de routage pour les réseaux ad hoc qui emploie une solution intermédiaire entre la diffusion pure et le routage géographique comme présenté ci-dessus.

Ce protocole utilise une requête de route sélective mais sans s'encombrer d'une procédure de mise à jour des positions. L'objectif est d'avoir un taux de réussite de découverte de route le plus proche possible de la diffusion pure, pour ainsi minimiser l'utilisation d'une procédure de recouvrement qui se trouve être nécessaire dans toute requête de route n'assurant pas la livraison dans la totalité des cas.

Notre objectif avec ce protocole est réduire la charge du trafic dans le réseau et d'en améliorer ainsi les performances.

Dans le protocole de routage que nous proposons chaque nœud a besoin de connaître les positions de ses voisins immédiats seulement. Ceci peut être réalisé avec une procédure d'envoi de messages entre voisins à des intervalles de temps réguliers. Ce

protocole de routage porte le nom ADRP pour «*ADhoc Routing Protocol*», et sera ainsi appelé dans toute la suite de ce document. ADRP utilise le routage à la source comme DSR, il y a alors une certaine similarité dans le fonctionnement des deux protocoles.

Quand un paquet de données arrive de la couche application à la couche réseau pour une destination donnée, ADRP cherche une route vers cette destination dans sa table de routage. Si une route existe, la liste des adresses représentant cette route est ajoutée au complet dans le paquet, ce dernier est envoyé directement au premier nœud de la liste. Les nœuds intermédiaires qui reçoivent la requête l'acheminent suivant la route qui se trouve dans le paquet lui-même (routage par la source). Un indicateur est utilisé pour déterminer quel est le prochain nœud dans la liste à qui sera acheminé le paquet. Le dernier nœud de la liste livre le paquet directement à la destination.

4.1.1. La découverte de route

Si aucune route n'existe dans la table de routage pour la destination, ADRP doit envoyer une requête de route, le paquet de données à transmettre est alors mis dans une mémoire tampon jusqu'à ce que la réponse de route arrive.

Afin d'optimiser l'utilisation des ressources du réseau, le nœud source sélectionne, parmi ses voisins immédiats, ceux qui seront chargés de diffuser la requête de route. Les informations sur les voisins, position et azimut, sont sauvegardées dans la table de voisins, qui est mise à jour chaque fois qu'un nœud reçoit un message d'information de l'un de ses voisins.

Pour le nœud source, le choix des voisins se fait selon leurs positions. On considère le cercle centré à la position du nœud source et qui englobe tous ses voisins immédiats. Ce cercle est divisé en quarts pour déterminer le quart qui contient le plus de voisins.

Le premier voisin est choisi dans le quart le plus peuplé, comme le nœud le plus proche de l'axe médian du quart, voir la figure 4.1 pour une illustration.

Les deux autres nœuds choisis sont les plus proches des axes se trouvant à 120 degrés à gauche et à droite du premier nœud choisi.

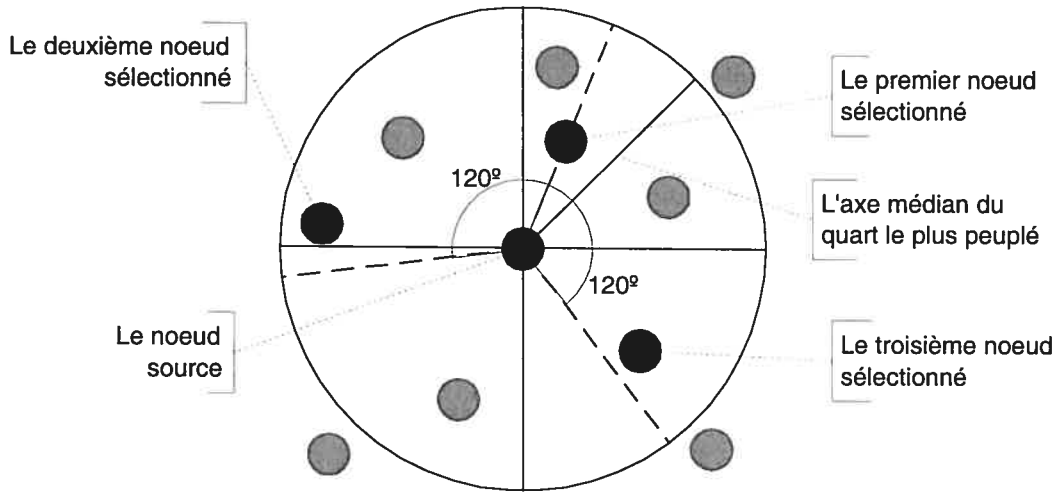


Figure 4.1 : la sélection des nœuds par le nœud source dans la requête de route de ADRP.

Le choix de trois voisins les plus équidistants possibles permet une meilleure couverture autour du nœud source, et permet aussi d'avoir les mêmes chances dans toutes les directions du réseau par rapport à la position du nœud source. Ces explications ont été confirmées par les résultats de calcul obtenus, voir la section 5.1 du chapitre 5.

Le choix de sélectionner trois voisins est un choix expérimental et non théorique, nous avons expérimenté la méthode sur des réseaux de différentes tailles. Nous avons cherché à obtenir un compromis entre le taux de réussite, qui doit être très proche de la diffusion pure, et le nombre de paquets échangés suite à cette requête de route, qui doit être inférieur à celui de la diffusion pure. Nous avons trouvé les résultats obtenus assez satisfaisants pour que la méthode soit implémentée dans un protocole de routage. Les expérimentations et les résultats se trouvent dans la section 5.1 du chapitre 5.

La densité du réseau est un facteur important. Elle peut être mesurée par l'azimut moyen des nœuds. Dans un réseau à faible densité, l'azimut moyen est entre 3 et 4. Dans un réseau à forte densité l'azimut moyen peut facilement dépasser 7. Plus le réseau est dense, plus il est intéressant de faire une sélection des voisins pour l'acheminent des requêtes de route afin de réduire la congestion du réseau. Pour en avoir une idée, prenons l'exemple de la figure 4.1. Quand les nœuds sélectionnés par le nœud source envoient la requête, le nœud source va recevoir trois fois sa propre requête. Dans le cas de la diffusion pure, le nœud source aurait reçu sa requête autant de fois que le nombre de voisins qu'il a, sept fois dans cet exemple.

Les nœuds intermédiaires qui reçoivent la requête de route doivent eux aussi choisir parmi leurs voisins qui leurs succéderont dans l'acheminement de la requête de route. Ce choix diffère de celui fait par le nœud source. Dans le cas des nœuds intermédiaires le choix se fait dans le demi-cercle se trouvant dans la direction du vecteur déterminé par le nœud courant et son prédécesseur. L'objectif est de ne pas retourner en direction du nœud précédent, voir la figure 4.2.

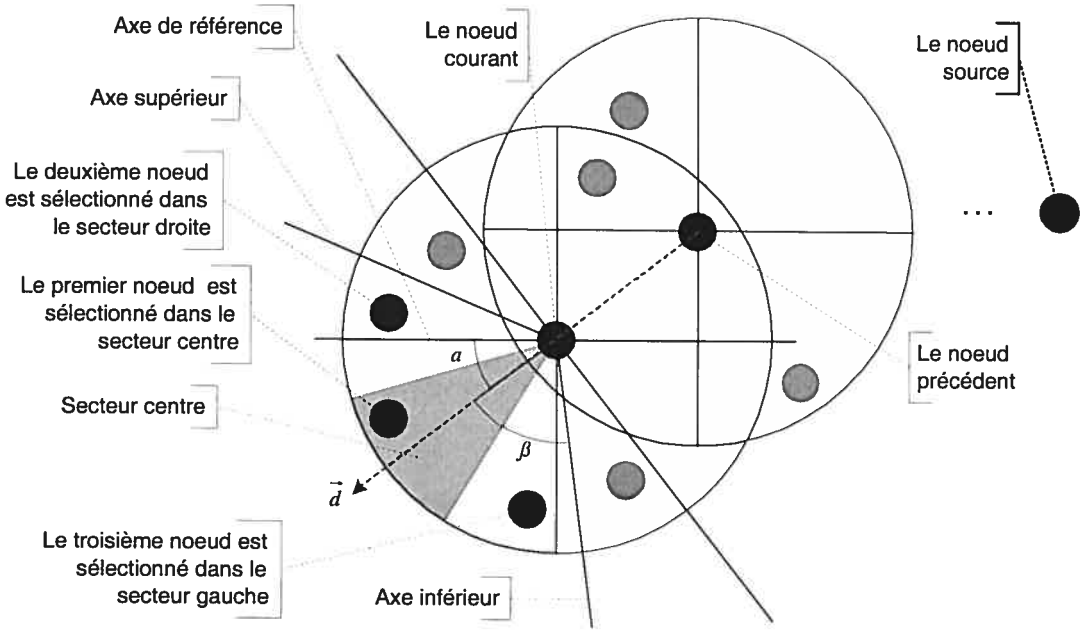


Figure 4.2 : la sélection des nœuds par les nœuds intermédiaires dans la requête de route de ADRP.

Considérons l'illustration de la figure 4.2, et supposons que l'axe de référence est l'axe horizontal qui passe par le nœud courant, et que l'orientation des angles est dans le sens antihoraire. Le choix se fait dans le secteur délimité par les deux axes supérieur et inférieur qui ont pour valeur respectivement $Max\{\alpha+\beta, \alpha-\beta\}$ et $Min\{\alpha+\beta, \alpha-\beta\}$,

où

α est l'angle formé par l'axe de référence et le vecteur reliant le nœud précédent et le nœud courant (direction $\vec{d}$),

l'angle β prend ses valeurs dans l'ensemble $\{\pi/6, \pi/3, \pi/2\}$.

Le secteur, défini par les axes inférieur et supérieur, est divisé en trois sous secteurs égaux. Un nœud est choisi, s'il existe un, dans chacun de ces sous secteurs. Le choix se fait selon l'azimut, c'est le nœud qui a le plus grand azimut qui est choisi dans chaque sous secteur.

Si aucun voisin ne se trouve dans le sous secteur du centre, β est augmenté de $\pi/6$ pour élargir le champ de sélection. Si, malgré cela, aucun voisin ne satisfait les critères de sélection, seulement deux nœuds sont sélectionnés dans tout l'intervalle entre les axes supérieur et inférieur.

Dans le cas où aucun voisin ne serait trouvé avec la valeur maximale de β, la procédure s'arrête pour ce nœud, mais bien sûr elle continue pour les autres nœuds sélectionnés auparavant.

Une question que l'on peut se poser ici: pourquoi ne pas orienter le choix du secteur de sélection par le nœud source? C'est-à-dire, pourquoi ne pas utiliser le vecteur formé par le nœud source et le nœud courant plutôt que le vecteur formé par le nœud précédent et le nœud courant? La réponse à cette question est que les expérimentations ont montré que le fait d'orienter la requête par le nœud source nuirait à l'efficacité de la découverte de route en réduisant son taux de réussite. Les résultats de ces expérimentations sont présentés dans la section 5.1 du chapitre 5.

Dans un souci d'avoir des routes les plus disjointes possible, parce qu'il est plus intéressant pour la maintenance de route d'avoir des routes disjointes, un marquage des chemins est employé dans la requête de route. C'est aux nœuds sélectionnés par le nœud source que revient la tâche du marquage, le premier nœud marque le chemin à un, le deuxième nœud marque le chemin à deux et le troisième nœud marque le chemin à trois. Par la suite, les autres nœuds intermédiaires trouveront le marquage déjà effectué et s'en serviront pour la construction de chemins disjoints dans la mesure du possible. Dans notre cas, nous nous restreignons aux chemins complètement disjoints ou à arcs disjoints. Notons qu'un nœud peut recevoir plusieurs fois le même paquet de requête de route. Dans les protocoles où les chemins ne sont pas numérotés, une requête, identifiée par son numéro et l'adresse de la source, n'est traitée qu'une seule fois par un nœud, les requêtes reçues plus d'une fois sont ignorées. Par contre, si les chemins sont numérotés, considérons un nœud qui vient de recevoir la requête R avec le même identifiant et la même adresse source qu'une requête R' reçue auparavant par ce même nœud. Si R a un numéro de chemin différent de R', le nœud peut envoyer la requête R à condition qu'il sélectionne des nœuds voisins différents de ceux qu'il a sélectionnés pour R'. Ceci permet d'obtenir des chemins à arcs disjoints.

Quand un nœud reçoit une requête de route avec la destination comme nœud voisin, il la sélectionne toute seule.

Si aucune réponse à la requête de route ne parvient au nœud source après un certain temps, le nœud source renvoie la requête de nouveau en augmentant le temps d'attente avant un autre renvoi. Le temps est augmenté pour permettre aux requêtes d'atteindre la destination dans le cas des grands réseaux où les temps d'attente sont plus grands.

Format du paquet requête de route

- Numéro du chemin : un indicateur de chemin, dans le cas où il est possible d'avoir des chemins disjoints.
- Numéro de la requête : un numéro unique qui avec l'adresse de l'envoyeur de la requête désigne de façon unique une requête dans le réseau.
- Adresse de la destination : adresse du nœud destination
- Adresse du nœud sélectionné [1..3] : adresses des nœuds sélectionnés.
- Adresse [1..n] : les adresses des nœuds dans la route source.

4.1.2. La réponse de route

Quand le nœud destination reçoit la requête de route, il répond par un paquet de réponse de route, la liste des adresses contenues dans la requête de route est insérée dans la réponse de route et sera suivie dans l'acheminement de la réponse.

Il se peut que plusieurs requêtes de route atteignent la destination. Pour éviter qu'il ait autant de réponses de route que de requêtes arrivées, les numéros de chemins serviront à contrôler les réponses de route. Le numéro du chemin de la requête R_0 qui arrive en premier à la destination est considéré comme le chemin le plus court, et il ne sera pas répondu aux autres requêtes ayant le même numéro de chemin, vu qu'ils ont un arc en commun avec le plus court chemin. Pour les requêtes ayant l'un des deux autres numéros de chemins, il ne leurs sera répondu que lorsque la route est plus disjointe de R_0 que les précédentes. Considérons une requête R avec un numéro de chemin différent de celui de R_0. Il lui sera répondu seulement si elle est plus disjointe de R_0, en terme de nœuds, que la requête $R`$ qui est arrivée auparavant avec le même numéro de chemin que $R$. Soit si R a moins de nœuds en commun avec $R_0$ que $R`$.

Réponse de route par les nœuds intermédiaires

Il est possible dans ADRP de permettre aux nœuds intermédiaires qui acheminent la requête de route d'envoyer une réponse de route au nœud source s'ils ont une route valide dans leurs tables de routage vers la destination, ce qui réduirait la propagation des requêtes de route dans le réseau. Mais si une telle possibilité était admise, les chemins disjoints ne pourraient plus être respectés comme l'illustre la figure 4.3. Par défaut, dans ADRP, les nœuds intermédiaires répondent aux requêtes de route s'ils ont une route valide vers la destination.

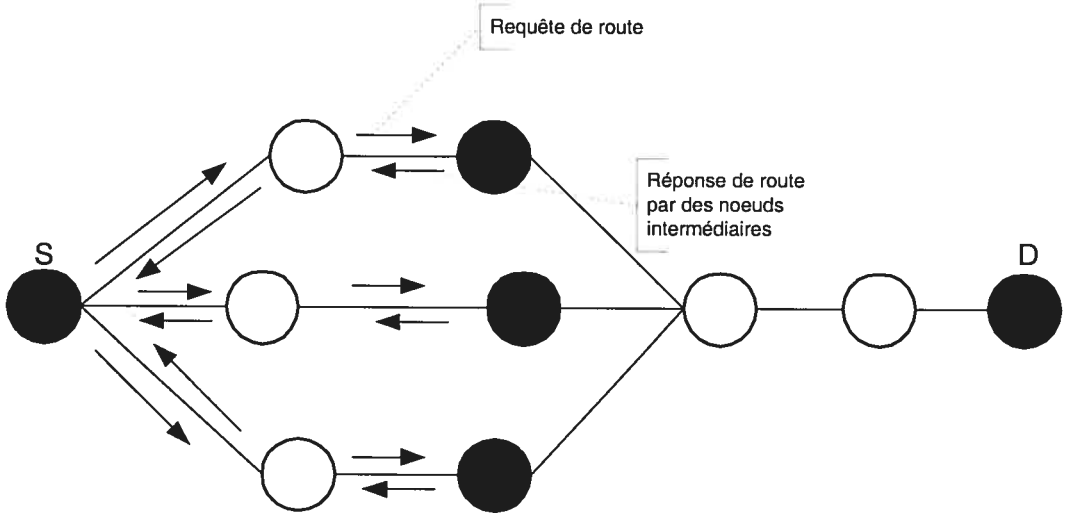


Figure 4.3 : chemins disjoints et réponse de route par les nœuds intermédiaires.

Raccourcissement des routes

Il est aussi possible aux nœuds intermédiaires de procéder au raccourcissement des routes dans les réponses de route de ADRP. Un nœud intermédiaire qui reçoit une réponse de route, vérifie dans la portion de route restant à parcourir, s'il a un voisin parmi les nœuds constituants cette portion de route. Si c'est le cas, il supprime tous les nœuds qui se trouvent entre lui et ce voisin dans la portion de route. Ceci évitera de parcourir des nœuds inutilement. A noter que la vérification se fait dans le sens inverse du parcours dans le but de supprimer le maximum de nœuds possible. Par

défaut dans ADRP, les nœuds intermédiaires procèdent au raccourcissement de routes.

Le format du paquet de réponse de route

- Numéro du chemin : le numéro de chemin suivant l'ordre dans lequel il est reçu par la destination.
- Numéro du nœud : la position, dans la liste des adresses, du prochain nœud qui acheminera la réponse de route.
- Adresse [1..n] : la liste des adresses copiées directement de la requête de route.

4.1.3. La maintenance

Pour s'assurer que le protocole de routage livre le paquet de données à la destination, une procédure de maintenance est appliquée entre chaque paire de nœuds adjacents sur une route. Le paquet de données est alors envoyé avec un accusé de réception. Si le nœud ne reçoit pas de réponse à l'accusé de réception après un certain temps, le paquet est considéré comme perdu et est renvoyé de nouveau. Si, après un certain nombre de tentatives, aucune réponse à l'accusé de réception n'est obtenue, le lien entre les deux nœuds adjacents est considéré comme rompu et la route devient non valide. Dans ce cas là, un paquet d'erreur de route doit être envoyé au nœud source du paquet de données pour lui indiquer que la route qu'il a choisie n'est plus valide. La maintenance de route est illustrée dans la figure 4.4.

Format du paquet route source et demande d'accusé de réception

- adresse [1..n] : la liste des adresses formant la route source.
- Le nombre de sauts restants pour atteindre la destination.

- Demande d'accusé de réception : numéro séquentiel qui permet, avec l'adresse du nœud source, d'identifier d'une façon unique un accusé de réception.

Format de la réponse à l'accusé de réception

- Réponse d'accusé de réception : C'est le numéro de la demande d'accusé de réception.

4.1.4. L'erreur de route

L'erreur de route est envoyée à destination du nœud qui a envoyé le paquet de données pour lui indiquer que la route qu'il a mise dans le paquet n'est plus valide. L'erreur de route est envoyée par le nœud qui n'a pas reçu d'accusé de réception du nœud qui le suit dans la route source. Ces deux nœuds sont alors considérés comme une paire d'adresses non valides dans une route. Tous les nœuds qui reçoivent l'erreur de route doivent supprimer de leur table de routage toute route qui contient la paire fautive (Adresse du nœud expéditeur de l'erreur de route, Adresse du nœud non atteignable).

Le format du paquet erreur de route

- Adresse du nœud expéditeur : le nœud qui a détecté la rupture de route.
- Adresse du nœud destinataire : le nœud qui a envoyé le paquet de données.
- Adresse du nœud non atteignable : le nœud avec lequel la route est coupée.

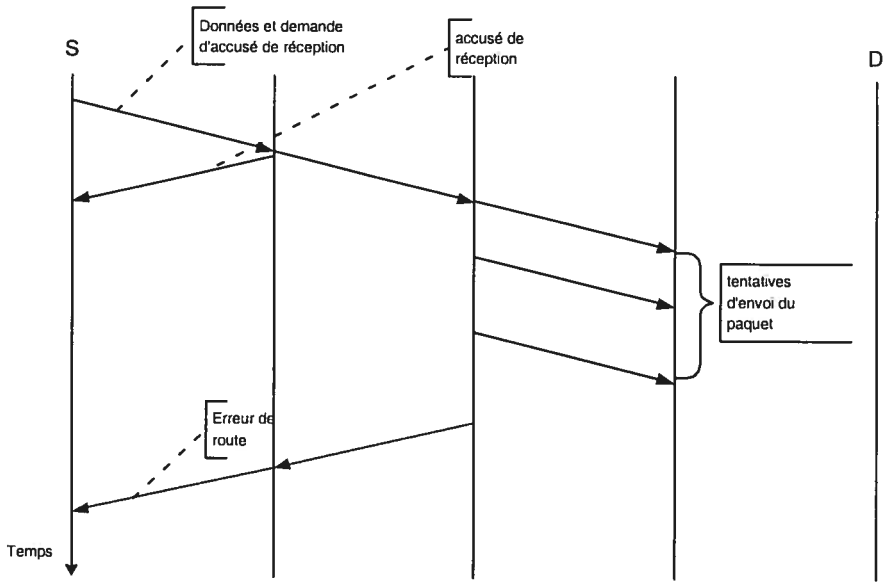


Figure 4.4 : synoptique temporelle de la maintenance de route dans ADRP.

4.1.5. Les messages d'information entre voisins

Les messages d'information entre voisins sont envoyés à intervalles de temps régulier pour mettre à jour les informations de la table des voisins, les informations transmises sont le degré et la position en coordonnées X et Y du nœud expéditeur. Ces informations ne sont pas rediffusées par les nœuds qui les reçoivent.

Les nœuds obtiennent leurs positions dans la forme que délivre les récepteurs GPS, c'est-à-dire le triplet (latitude, longitude, altitude), ces coordonnées sont converties en coordonnées X et Y sur la surface de la terre.

4.1.6. La procédure de recouvrement

La méthode utilisée pour l'envoi de la requête de route ne garantit pas la livraison à 100%. Quand une telle méthode est utilisée, une procédure de recouvrement doit être implémentée et doit être déclenchée dans le cas où la requête de route se solderait par

un échec. La procédure de recouvrement implémentée dans ce protocole est la diffusion pure.

4.2. ADRPH une variante saut par saut de ADRP

ADRP est un protocole qui utilise le routage à la source, la route est toujours incluse dans les paquets. Avec ADRP on veut montrer que la requête de route sélective améliore les performances des réseaux ad hoc par rapport à la diffusion pure. Pour cela il faut comparer ADRP avec un protocole qui utilise la diffusion pure.

Cependant, en consultant les travaux comparatifs des protocoles de routage pour les réseaux ad hoc, il se trouve que les protocoles de routage saut par saut ont de meilleures performances que les protocoles de routage à la source, voir pour cela la comparaison entre AODV et DSR [59]. Nous concluons que nous ne pouvons pas tirer des jugements sur l'apport de la requête de route sélective aux performances d'un protocole en faisant des comparaisons sur des protocoles utilisant des techniques de routage différentes. C'est-à-dire que, si on implémente la requête de route sélective dans un protocole de routage à la source, et on le compare à un protocole de routage saut par saut, et qu'il ne démontre pas de meilleures performances, on ne peut pas conclure que la requête de route sélective n'apporte rien de plus au protocole. Inversement, si on implémente la requête de route sélective sur un protocole de routage saut par saut et on le compare à un protocole de routage à la source, on ne peut pas dire que c'est la requête de route sélective qui est à l'origine de la performance du protocole.

Pour ces raisons, et pour un jugement plus objectif de la requête de route sélective que nous avons conçu, nous avons décidé d'implémenter une version saut par saut de ADRP, soit le protocole ADRPH.

ADRPH («*ADRP Hop-by-Hop*») est un protocole de routage saut par saut qui utilise les mêmes techniques de routage que AODV. Dans ADRPH les nœuds n'enregistrent pas leurs adresses dans les requêtes de route. Quand un nœud reçoit une requête de route, il sait qui est le nœud source et le dernier nœud qui lui a envoyé la requête. Ce qui lui permet d'établir un chemin inverse vers le nœud source. Ceci va servir pour acheminer la réponse de route si elle passe par ce nœud. Voir la section 3.3.2 du chapitre 3 pour AODV.

Pour la requête de route, ADRPH utilise la requête de route sélective comme décrite dans ADRP. Pour rendre cela possible, ADRPH utilise aussi les messages d'informations entre voisins comme ADRP.

4.3. Protocole de routage pour les réseaux ad hoc en présence de nœuds fixes

Il est possible d'avoir des réseaux ad hoc incluant des nœuds sans fil avec une position fixe et qui jouent un rôle important. C'est le cas, par exemple, lorsque des bases sont stationnées temporairement avec des stations mobiles qui se déplacent autour de ces bases.

Dans cette partie, nous considérons les réseaux ad hoc avec des nœuds sans fil fixe et sans liens directs entre eux, en présence de nœuds mobiles autour d'eux.

Ce problème peut être vu comme un cas particulier d'un réseau ad hoc hiérarchisé, où les nœuds fixes sont les nœuds responsables de groupes et les communications entre les nœuds mobiles passent par les nœuds fixes, et les communications entre les nœuds fixes passent par les nœuds mobiles.

Cependant, nous proposons un protocole de routage qui utilise une approche différente des méthodes hiérarchiques pour exploiter la présence de nœuds fixes dans le réseau.

Dans cette approche, les nœuds mobiles vont utiliser les nœuds fixes pour diffuser la requête de route dans le réseau. Pour que cela soit possible, les nœuds fixes doivent réaliser certaines procédures qui seront détaillées dans ce qui suit.

Ce protocole porte le nom ASNRP pour «*Ad hoc with Static Nodes Routing Protocol*», et il sera appelé ainsi dans toute la suite de ce document.

4.3.1. Description du réseau

Le réseau est constitué de nœuds fixes et de nœuds mobiles, il n'y a bien sûr aucun lien filaire entre les nœuds.

Le protocole de routage que nous allons décrire ici, utilise les informations sur les nœuds fixes pour limiter la diffusion des requêtes de route dans le réseau, les positions des nœuds fixes doivent être connues par tous les nœuds du réseau. En plus, les nœuds fixes doivent maintenir des routes entre eux d'une façon bien déterminée qui sera expliquée dans la phase d'initialisation.

4.3.2. Phase initialisation

Une phase d'initialisation s'impose dans ce protocole, pour rendre disponible les positions des nœuds fixes à tout le réseau et établir les liens entre les nœuds fixes.

Diffusion des positions

La diffusion des positions est la première étape dans ASNRP. Chaque nœud fixe doit diffuser un paquet contenant ses coordonnées dans le même format que la diffusion des informations entre voisins dans ADRP. Les nœuds, mobiles et fixes, qui reçoivent ce paquet pour la première fois doivent le diffuser à leur tour et doivent l'ignorer dans le cas contraire.

Construction de l'arbre minimal

Les nœuds fixes doivent maintenir des routes entre eux qui serviront par la suite dans l'acheminement du trafic. Nous avons jugé que l'utilisation d'un graphe complet serait trop coûteuse vu le nombre de routes qu'il y aurait à maintenir. Nous avons alors conçu le protocole ASNRP avec un arbre de poids minimal [57] comme structure pour maintenir des liens entre les nœuds fixes, pour réduire le nombre de routes à maintenir. L'arbre est minimal au sens des distances euclidiennes entre les nœuds fixes et non pas en nombre de sauts. L'étape de construction de l'arbre minimal n'est effectuée que par les nœuds fixes, elle s'exécute un certain temps après la diffusion des positions. La construction de l'arbre commence par le nœud fixe le plus à gauche du réseau qui est le premier à être mis dans l'ensemble constituant l'arbre et devient par conséquent la racine de l'arbre. Ce choix est arbitraire, comme pour les méthodes de construction de l'arbre minimal, où le premier nœud est choisi arbitrairement. Ce qui compte dans notre cas, c'est que tous les nœuds fixes fassent le même choix. Le deuxième nœud choisi, est le plus proche de la racine en distance euclidienne, et est mis à son tour dans l'arbre. Le nœud racine doit maintenir une route vers ce nœud. Les nœuds suivants sont choisis l'un après l'autre le plus proche en distance euclidienne d'un des nœuds de l'arbre. Le nœud qui est déjà dans l'arbre et qui se trouve être le plus proche du nœud qui vient d'être choisi, est considéré comme le père du nouveau nœud, et c'est toujours le père qui doit maintenir une route vers ses fils.

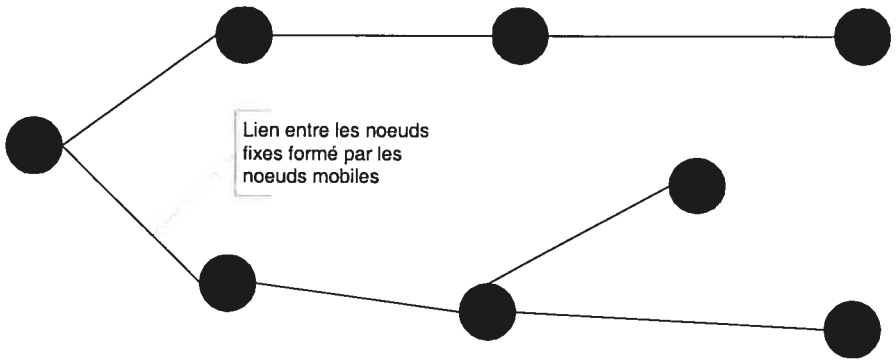


Figure 4.5 : arbre de coût minimal des nœuds fixes.

4.3.3. Maintenance des routes entre les nœuds fixes

Après la fin de la construction de l'arbre de poids minimum sur les nœuds fixes, la procédure de maintenance de route est lancée. Elle commence d'abord par la découverte de route entre les nœuds fixes à travers les nœuds mobiles. Les routes construites entre les nœuds fixes ne doivent pas contenir d'autres nœuds fixes, pour éviter d'avoir des arcs en plus dans l'arbre. La procédure de découverte de route utilisée ici est la même procédure qu'utilise le protocole ADRP.

Une fois les routes trouvées, il faut les maintenir. La procédure de maintenance consiste en l'envoi d'un accusé de réception de route et d'attente de la réponse à l'accusé de réception. Les envois d'accusés de réception se font à intervalles de temps réguliers. Si après un certain temps, aucune réponse à l'accusé de réception ne parvient, la procédure est réitérée un certain nombre de fois, avec, à chaque fois, un intervalle de temps d'attente plus grand. Si à la fin, la réponse à l'accusé de réception n'est pas reçue, la route est considérée comme rompue et une nouvelle requête de route doit être envoyée.

Procédure de recouvrement pour l'arbre minimal

L'arbre minimal est construit suivant les distances euclidiennes entre les nœuds fixes. Mais cela ne garantit pas que des routes existent effectivement entre deux

nœuds fixes à travers des nœuds mobiles, pour cette raison une procédure de recouvrement est mise en œuvre. Si un nœud père P_1 n'a aucune réponse de route de son fils P_2, après un certain nombre de tentatives de découverte de route sans succès, P_1 considère alors qu'il n'y a aucune route qui passe seulement par des nœuds mobiles, le reliant à P_2. Dans ce cas là, c'est le père de P_1 qui prendra la relève et maintiendra par la suite une route vers son nouveau fils P_2. Pour que cela se fasse, P_1 envoie un paquet spécial de recouvrement de l'arbre à tout le réseau pour indiquer ce changement. Si c'est le nœud racine de l'arbre qui n'arrive plus à trouver une route vers un de ses fils, et puisqu'il n'a pas de père, il doit choisir un nœud parmi ses autres fils pour lui léguer la tache de maintenir la route.

Cette façon de reconstruire l'arbre, permet de préserver la structure d'arbre. Cette reconstruction minimise aussi les changements dans l'arbre, une seule route est supprimée et est remplacée par une autre. Mais cela ne garantit pas que l'arbre reste minimal en termes de distance euclidienne. Nous avons préféré cette façon de reconstruire l'arbre que de relancer la procédure de construction de l'arbre minimal. Parce que la reconstruction de l'arbre minimal pourrait mener à beaucoup de changements en termes de routes à établir entre les paires (père, fils) de nœuds fixes dans le nouvel arbre minimal obtenu.

Format du paquet de reconstruction de l'arbre

- Identifiant de la reconstruction : numéro séquentiel qui permet d'identifier le paquet de reconstruction de l'arbre.
- Adresse du nœud déconnecté : l'adresse du fils avec qui le père (nœud envoyeur de ce paquet) n'arrive plus à établir de route.
- Adresse du nouveau père : l'adresse du nœud qui va devenir le père du nœud déconnecté.

4.3.4. La découverte de route entre deux nœuds quelconques

Quand un paquet de données arrive à la couche réseau en provenance de la couche application, et qu'aucune route n'existe vers le destinataire, une procédure de découverte de route est lancée. Sans perte de généralité, nous considérons les sources et destinations de données comme étant des nœuds mobiles. Le cas où l'un des deux est un nœud fixe, est un cas inclus dans le cas que nous considérons ici, comme nous l'expliquerons à la fin de cette section.

Pour pouvoir exploiter la présence des nœuds fixes et les routes qu'ils maintiennent entre eux, la découverte de route est constituée de trois types de requêtes de route. Le premier type de requête de route est envoyé par le nœud source, le deuxième type de requêtes est envoyé par les nœuds fixes aux nœuds mobiles et le troisième type de requêtes est envoyé d'un nœud fixe à d'autres nœuds fixes.

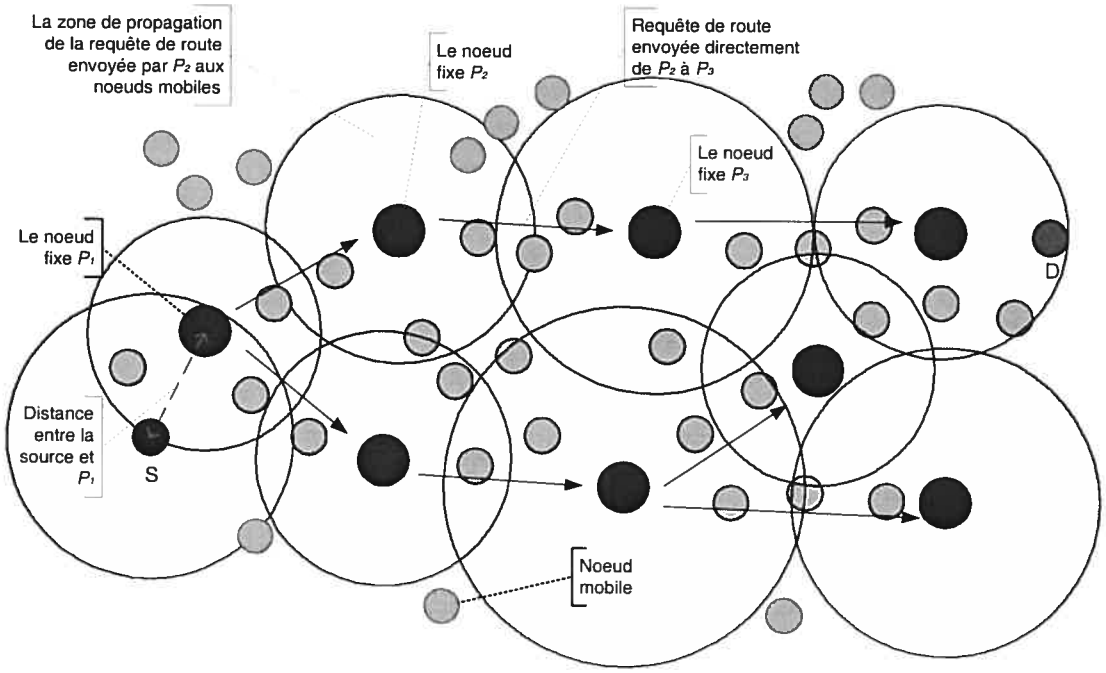


Figure 4.6 : propagation de la requête de route dans ASNRP.

Requête de route envoyée par le nœud source

Cette requête est envoyée par le nœud mobile source, elle est destinée aux nœuds mobiles les plus proches et au nœud fixe le plus proche P_1, le nœud fixe P_1 aura pour rôle de diffuser les deux autres types de requêtes. Pour éviter que cette requête ne se propage dans tout le réseau, elle sera limitée à un certain nombre de sauts, calculé en fonction de la distance séparant la source de P_1. Le nombre de sauts a comme borne inférieure la valeur :

$$Borne\ inf = Valeur\ entière\ (Distance/\ portée\ des\ transmetteurs),$$

où *Distance* est la distance euclidienne entre la source et P_1. Pour limiter le nombre de sauts, nous avons majoré la distance réelle entre les deux nœuds par le demi cercle qui a pour diamètre *Distance*. Le nombre de sauts, représenté par le champ *TTL* du paquet IP [58], dans cette requête est alors égal à :

$$TTL = valeur\ entière\ (Distance \times \pi / portée\ des\ transmetteurs)+1.$$

La propagation de cette requête est représentée par le cercle centré au nœud source S et qui couvre le nœud fixe P_1 dans la figure 4.6. Si la destination se trouve à un nombre de sauts inférieur ou égal à *TTL*, elle sera atteinte par cette requête et répondra par une réponse de route. Dans le cas contraire, c'est P_1 qui poursuivra la tâche de diffuser la requête dans le réseau, et c'est cela l'intérêt de la construction de l'arbre minimal. P_1 construit deux requêtes à partir de celle qu'il a reçu. La première est envoyée directement, puisque les routes sont connues, à chacun des nœuds fixes auxquels il est relié dans l'arbre, son père et ses fils. La deuxième requête est envoyée aux nœuds mobiles qui se trouvent près de lui. Cette dernière requête est envoyée avec un nombre de sauts limité pour restreindre sa propagation aux alentours de P_1.

Enfin, tous les nœuds fixes qui reçoivent la requête envoyée par P_1 répètent les mêmes opérations que lui, c'est-à-dire, qu'ils envoient deux types de requêtes, une pour les nœuds fixes qui leurs sont directement reliés dans l'arbre et l'autre pour les nœuds mobiles proches d'eux.

Format de la requête de route envoyée par le nœud source

La requête de route envoyée par le nœud source utilise la diffusion sélective comme dans ADRP. Nous décrivons ci-dessous le format de cette requête.

- Numéro du chemin : un indicateur de chemin, dans le cas où il est possible d'avoir des chemins disjoints.
- Numéro de la requête : un numéro unique qui, avec l'adresse de l'envoyeur de la requête, désigne de façon unique une requête dans le réseau.
- Adresse de la destination : adresse du nœud destination.
- Adresse du nœud fixe le plus proche : l'adresse du nœud fixe le plus proche en distance euclidienne.
- Adresse du nœud sélectionné [1..3] : adresses des nœuds sélectionnés.
- Adresse [1..n] : les adresses des nœuds dans la route source.

Requête de route envoyée d'un nœud fixe aux nœuds mobiles

Pour construire sa requête, le nœud fixe P_i récupère les informations à partir de la requête qu'il a reçue, ou bien du nœud source, s'il s'agit du nœud fixe P_l désigné par le nœud source, ou bien d'un nœud fixe P_j qui a fait la diffusion.

Le nombre de sauts dans cette requête est limité en majorant la distance entre P_i et P_i', le plus lointain nœud fixe qui est directement relié à P_i dans l'arbre. Cette distance, représentée par *Distance*, est majorée par le demi-cercle ayant pour diamètre la mi-distance euclidienne entre P_i et P_i'. Le nombre de sauts, représenté par le champ *TTL* de IP, est alors égal à :

$$TTL = valeur\ entière\ (Distance/2 \times \pi / portée\ des\ transmetteurs) + 1.$$

La propagation de cette requête est représentée par les cercles autour des nœuds fixes dans la figure 4.6.

Format de la requête de route envoyée d'un nœud fixe aux nœuds mobiles

La requête de route envoyée d'un nœud fixe aux nœuds mobiles utilise la diffusion sélective comme dans ADRP. Nous décrivons ci-dessous le format de cette requête.

- Numéro du chemin : un indicateur de chemin, dans le cas où il est possible d'avoir des chemins disjoints.
- Numéro de la requête : un numéro unique qui avec l'adresse de l'envoyeur de la requête désigne de façon unique une requête dans le réseau.
- Adresse de la destination : adresse du nœud destination.
- Adresse de la source : adresse du nœud source mobile qui a généré la requête de route.
- Adresse du nœud sélectionné [1..3] : adresses des nœuds sélectionnés.
- Adresse [1..n] : les adresses des nœuds dans la route source copiés de la requête reçue.

Requête de route envoyée d'un nœud fixe à d'autres nœuds fixes

Le nœud fixe P construit cette requête de route de la même façon que la requête qu'il a envoyé aux nœuds mobiles, c'est-à-dire, avec les informations de la requête reçue. Pour chaque nœud fixe P' qui lui est directement relié, P ajoute la route le reliant à P' dans la requête de route. La requête est envoyée directement en utilisant la route reliant P à P'.

Format de la requête de route envoyée d'un nœud fixe à d'autres nœuds fixes

- Numéro de la requête : un numéro unique qui avec l'adresse de l'envoyeur de la requête désigne de façon unique une requête dans le réseau.
- Adresse de la destination : adresse du nœud destination.
- Adresse de la source : adresse du nœud source mobile qui a généré la requête de route.
- Adresse du nœud sélectionné [1..3] : adresses des nœuds sélectionnés.
- Adresse [1..n] : les adresses des nœuds dans la route source copiés de la requête reçue, plus les adresses reliant les deux nœuds fixes P et P'.

Dans le cas où la source est un nœud fixe, la découverte de route sera composée des requêtes envoyées des nœuds fixes aux nœuds mobiles et des requêtes envoyées des nœuds fixes aux nœuds fixes. En d'autres termes, la requête envoyée par le nœud source pour atteindre le plus proche nœud fixe n'est pas nécessaire, vu que le nœud source est lui-même un nœud fixe. Dans le cas où la destination est un nœud fixe, la découverte de route sera composée de la requête envoyée par le nœud source et des requêtes envoyées par les nœuds fixes aux nœuds fixes. C'est-à-dire, que les requêtes de route envoyées par les nœuds fixes aux nœuds mobiles qui sont proches d'eux ne sont pas nécessaires, vu que la destination est un nœud fixe.

4.3.5. La réponse de route

La réponse de route est envoyée de la même façon que le fait le protocole ADRP, c'est-à-dire, en copiant la route reçue dans la requête de route. La réponse de route va parcourir le chemin inverse de la requête de route pour atteindre le nœud source.

4.3.6. Maintenance de route

La maintenance de route est appliquée au paquet de données de la même façon que pour le protocole ADRP. Entre chaque paire de nœuds adjacents un accusé de réception est envoyé avec le paquet de données, et une réponse à cet accusé est attendue, autrement le paquet est considéré comme perdu.

4.3.7. Erreur de route

L'erreur de route ne diffère en rien de celle existante dans ADRP. Le nœud ayant détecté la rupture de route, envoie une erreur de route pour informer la source qui a envoyé les données. Comme pour ADRP, l'erreur de route engendre la suppression des routes ayant la paire (nœud expéditeur de l'erreur de route, nœud non joignable) dans les tables de routage de tous les nœuds qui la reçoivent.

4.3.8. Procédure de recouvrement

Le protocole ASNRP utilise une diffusion sélective comme ADRP, ce qui nécessiterait une procédure de recouvrement. Quelle que soit la raison pour laquelle la requête de route échoue à atteindre la destination, le recouvrement se fait par l'envoi d'une requête de route qui utilise la diffusion pure, ce qui veut dire que dans le cas ou la procédure de recouvrement est lancée, il ne sera fait aucun usage particulier des nœuds fixes et ces derniers seront considérés comme des nœuds quelconques du réseau.

Chapitre 5

Simulations et résultats

La simulation est une étape essentielle dans le processus de conception des protocoles réseaux. En effet, tester un protocole sur un simulateur de réseau est un moyen très économique pour mesurer ses performances et donner une idée précise des performances à attendre sur une plate forme réelle.

En ce qui concerne les réseaux ad hoc, et on consultant les articles et le forum du groupe de travail MANET de IETF, trois simulateurs sont le plus cités, NS-2, Opnet et GloMoSim.

NS-2 [4] pour «*Network Simulator 2*» est un simulateur à événements discrets, développé par un groupe d'universités et d'organismes. Il est libre d'utilisation pour la recherche scientifique. NS-2 offre un cadre de simulation pour les réseaux filaires et sans fil. Le fait qu'il soit un logiciel libre, NS-2 est très utilisé chez la communauté universitaire.

Opnet Modeler [5] est un produit commercial de la société Opnet. Développé à l'origine au MIT [6], il a été introduit en 1987 comme le premier simulateur commercial de réseaux, il est très utilisé dans le domaine de l'industrie.

GloMoSim a été développé par l'université UCLA [7] et a été conçu spécialement pour les réseaux mobiles. Ce simulateur supporte les réseaux filaires bien que la version disponible ne contient aucun protocole standard au niveau MAC, et seulement du routage statique. Il existe une version commerciale de GloMoSim qui porte le nom de QualNet [8].

Les études comparatives sur les simulateurs pour les réseaux ad hoc sont peu nombreuses, en effet, un seul article traite de ce sujet [60]. Il serait très difficile de tirer des conclusions de cette étude qui compare les simulateurs tout en sachant que l'implémentation de la couche mac 802.11 diffère d'un simulateur à un autre. Il aurait été plus intéressant d'avoir une étude qui compare les simulateurs par rapport à une plate forme réelle de tests, et de voir non pas celui qui donne les meilleurs performances mais celui qui se rapproche le plus de la réalité, comme il a été fait pour les réseaux filaires [61].

Ceci dit, notre choix s'est porté sur Opnet Modeler pour les raisons suivantes :

- la société Opnet offre des licences gratuites, renouvelables plusieurs fois, aux universités, pour la recherche académique et comme outils pour l'enseignement;
- Opnet Modeler offre une interface utilisateur très conviviale;
- enfin, Opnet a un groupe de travail spécialisé dans les réseaux ad hoc et disponibles pour répondre au questions relatives à ces réseaux.

Avant d'entamer la simulation avec Opnet Modeler, nous avons testé les requêtes de route proposées dans ce mémoire sur un simulateur de requêtes que nous avons nous même développé. Nous allons présenter ce simulateur ainsi que les résultats que nous avons obtenu.

5.1. Le simulateur de requêtes de route REQSIM

REQSIM a été conçu sous Visual C++ version 6.0. Il permet une seule requête à la fois sur des graphes représentant des réseaux ad hoc de taille variable. La disposition des nœuds ainsi que les nœuds source et destination sont déterminés aléatoirement.

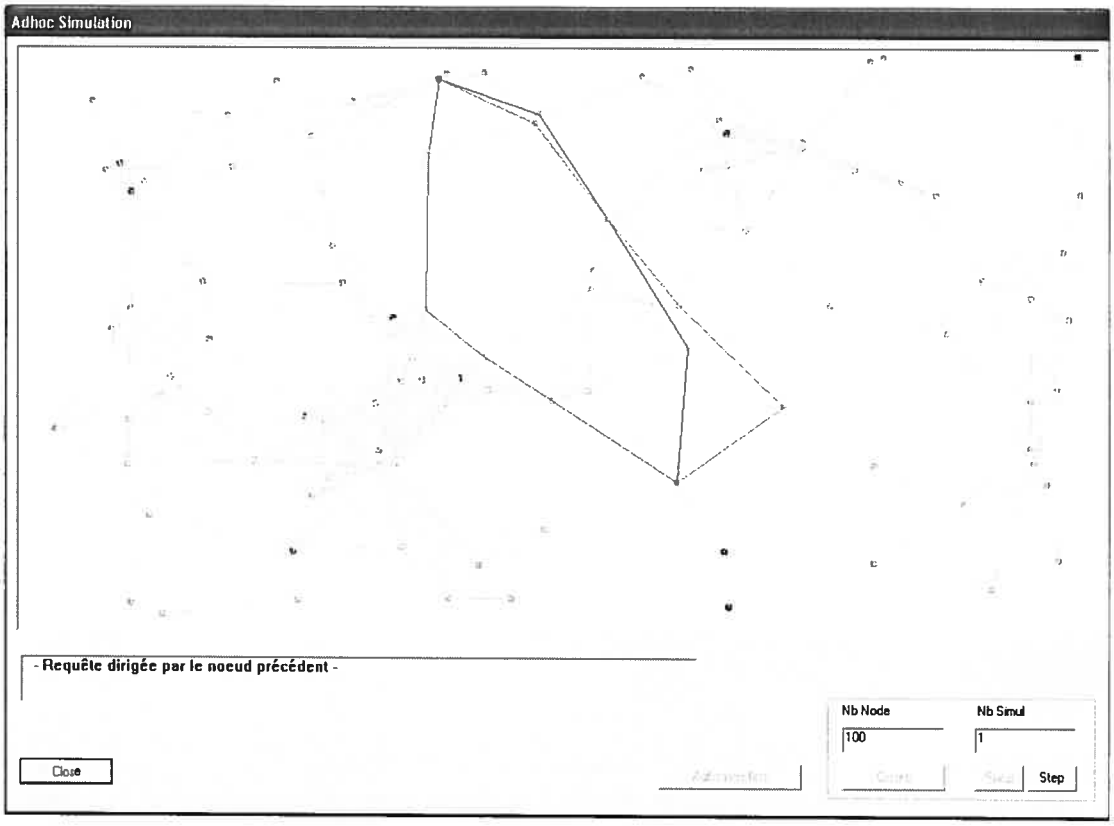


Figure 5.1 : l'interface du simulateur REQSIM.

La figure 5.1 montre l'interface du simulateur qui permet de visualiser la topologie du réseau ainsi que les routes obtenues. L'utilisation de ce simulateur permet d'avoir une estimation du taux de réussite de la requête de route sélective par rapport à la diffusion ainsi que le nombre de paquets reçus suivant les différentes tailles de réseau et différents degrés moyens (la moyenne des degrés des nœuds du réseau). Le fait d'isoler la requête de route de tout autre trafic dans le réseau permet d'évaluer son efficacité indépendamment de tout autre paramètre lié aux réseaux ad hoc.

Pour déterminer combien de voisins il faudrait sélectionner pour acheminer la requête de route, et comment contrôler la propagation de la requête de route, c'est-à-dire, comment la requête de route sera orientée pour minimiser le trafic qu'elle engendre dans le réseau. Nous avons fait plusieurs simulations, le tableau 5.1 et le tableau 5.2 montrent les résultats les plus pertinents.

Pour déterminer le nombre de voisins à sélectionner, nous avons fait des simulations sur des réseaux de tailles variables. Pour chaque simulation, trois types de requêtes sont générés. Dans la première requête, chaque nœud sélectionne deux voisins pour l'acheminement de la requête, dans la deuxième requête, chaque nœud sélectionne trois voisins et enfin, la dernière requête est envoyée en utilisant la diffusion pure. Les résultats sont illustrés dans le tableau 5.1. Chaque ligne de ce tableau représente la moyenne de 50 simulations, la première et la deuxième colonne représentent respectivement la taille et le degré moyen du réseau. Les trois colonnes suivantes représentent le type de requête de route utilisé, et qui sont respectivement, sélection de deux voisins, sélection de trois voisins et enfin la diffusion pure. Chacune des trois dernières colonnes est divisée en trois sous colonnes représentants dans l'ordre le taux de succès de la requête de route, le taux de nœuds participant à la requête et le nombre de paquets échangé dans le réseau. Les résultats obtenus montrent que le choix de trois voisins donne des taux de succès plus proches de la diffusion pure avec moins de trafic dans le réseau.

réseau		choix de deux voisins			choix de trois voisins			diffusion		
taille	degré	succès (%)	participation (%)	paquets reçus	succès (%)	participation (%)	paquets reçus	succès (%)	participation (%)	paquets reçus
20	3.9	0.58	0.34	6.2	0.64	0.34	7.8	0.68	0.42	21.4
30	6.0	0.86	0.40	12.2	0.92	0.42	16.1	0.94	0.58	52.9
35	7.1	0.90	0.42	18.6	0.98	0.45	29.6	1.00	0.60	125.7
50	10.1	0.94	0.51	27.0	1.00	0.59	54.9	1.00	0.73	252.1
60	6.0	0.68	0.42	31.2	0.80	0.48	48.7	0.86	0.65	185.9
70	6.9	0.74	0.52	48.3	0.88	0.61	78.5	0.92	0.78	313.3
80	7.9	0.88	0.59	63.0	0.94	0.67	117.6	0.96	0.84	415.6
90	8.9	0.82	0.64	87.7	0.92	0.72	148.0	1.00	0.88	566.2
100	10.0	0.88	0.63	98.6	0.92	0.76	197.1	1.00	0.92	787.1
120	11.9	0.98	0.62	147.3	1.00	0.72	305.8	1.00	0.87	1070.9
135	13.5	0.98	0.75	144.6	0.98	0.84	310.8	0.98	0.93	1340.9
150	15.2	0.96	0.68	199.8	1.00	0.79	460.2	1.00	0.87	1729.8

Tableau 5.1 : résultats des simulations pour déterminer le nombre de voisins à sélectionner.

Comme indiqué dans la section 4.1.1 du chapitre 4, la sélection des voisins par les nœuds intermédiaires se fait suivant l'orientation du vecteur formé par le nœud précédent et le nœud courant. Pour arriver à ce choix, nous avons fait les expérimentations sur différentes tailles de réseau. Pour chaque simulation, trois types de requêtes sont générés. Dans la première requête, l'orientation se fait par le nœud source, dans la deuxième requête, l'orientation se fait par le nœud précédent et enfin, la dernière requête est envoyée en utilisant la diffusion pure. Les résultats sont illustrés dans le tableau 5.2, où les trois dernières colonnes représentent respectivement, la requête orientée par le nœud source, la requête orientée par le nœud précédent et la diffusion pure. Chaque ligne du tableau représente la moyenne de 50 simulations. Quand on vient à comparer les deux premières requêtes par rapport à la diffusion pure on trouve que la requête orientée par le nœud précédent donne un taux de réussite très proche de la diffusion pure, avec moins de trafic dans le réseau. Ce qui a fait porter notre choix sur cette façon d'orienter la requête de route.

Ces expérimentations nous ont permis de conclure que le fait de sélectionner trois voisins et d'orienter la requête par le nœud précédent, donne un taux de succès très proche de la diffusion pure. Ce qui justifié les choix que nous avons fait dans la section 4.1.1 du chapitre 4.

réseau		noeud source			noeud précédent			diffusion		
taille	degré	succès (%)	participation (%)	paquets reçus	succès (%)	participation (%)	paquets reçus	succès (%)	participation (%)	paquets reçus
20	3.8	0.68	0.33	7.7	0.70	0.35	8.3	0.74	0.43	21.8
30	5.8	0.76	0.41	17.2	0.84	0.48	22.4	0.90	0.62	77.7
35	6.7	0.92	0.35	17.4	0.98	0.43	25.5	0.98	0.57	91.2
50	9.7	0.94	0.44	38.4	1.00	0.58	60.7	1.00	0.76	270.9
60	5.8	0.65	0.37	30.6	0.87	0.54	52.6	0.96	0.79	216.7
70	6.7	0.82	0.48	51.2	0.93	0.66	88.9	1.00	0.86	328.0
80	7.8	0.80	0.43	55.6	0.89	0.66	112.5	0.93	0.85	433.4
90	8.9	0.91	0.43	67.3	0.98	0.61	127.2	1.00	0.77	497.8
100	9.9	0.93	0.48	89.3	1.00	0.72	201.2	1.00	0.84	676.4
120	11.8	0.93	0.54	131.7	1.00	0.82	312.4	1.00	0.91	1070.5
135	13.3	0.93	0.51	136.6	1.00	0.80	351.5	1.00	0.91	1390.0
150	14.9	0.92	0.54	174.8	1.00	0.79	417.5	1.00	0.89	1694.2

Tableau 5.2 : résultats des simulations pour déterminer comment orienter la requête de route.

5.2. Opnet Modeler

Opnet Modeler offre une interface de développement en C/C++ avec une bibliothèque de fonctions pour l'interfaçage avec le simulateur, tel que la gestion des paquets, des processus...etc. En plus de l'interface de simulation, Opnet Modeler offre un ensemble de modèles qui représentent la majorité des protocoles réseaux existants sur Internet, le code source de ces protocoles est accessible pour toute modification et adaptation. Opnet modeler offre aussi des ensembles d'objets représentant des équipements de réseau (commutateur, routeur, ...) de la plupart des manufacturiers (Cisco, Nortel,...) ce qui permet de modéliser des réseaux et de faire des simulations de trafic sans avoir à écrire du code.

Les résultats de la simulation peuvent être directement récupérés dans des graphiques ce qui facilite leurs interprétations.

En ce qui concerne les réseaux ad hoc, Les protocoles de routage AODV et DSR sont disponibles dans Opnet. Au niveau MAC, c'est le protocole 802.11 qui est implémenté.

5.3. Implémentation de protocoles

Les modules dans Opnet Modeler (protocoles, Applications, ...) sont implémentés comme des processus qui sont modélisés par des automates d'états finis. Les processus sont créés durant la simulation, à l'instar du processus racine qui est créé par le noyau du simulateur, les autres processus sont créés par d'autres processus, et chaque processus père peut invoquer ses processus fils durant la simulation, la communication inter processus se fait donc par invocation.

Le processus Manet est implémenté dans Opnet pour servir d'interface avec le processus IP, tous les protocoles de routage pour les réseaux ad hoc sont implémentés comme des processus fils du processus Manet.

5.4. Implémentation du protocole ADRP

ADRP se présente à l'utilisateur comme le montre la figure 5.2 les principaux paramètres sont détaillés dans le tableau 5.3.

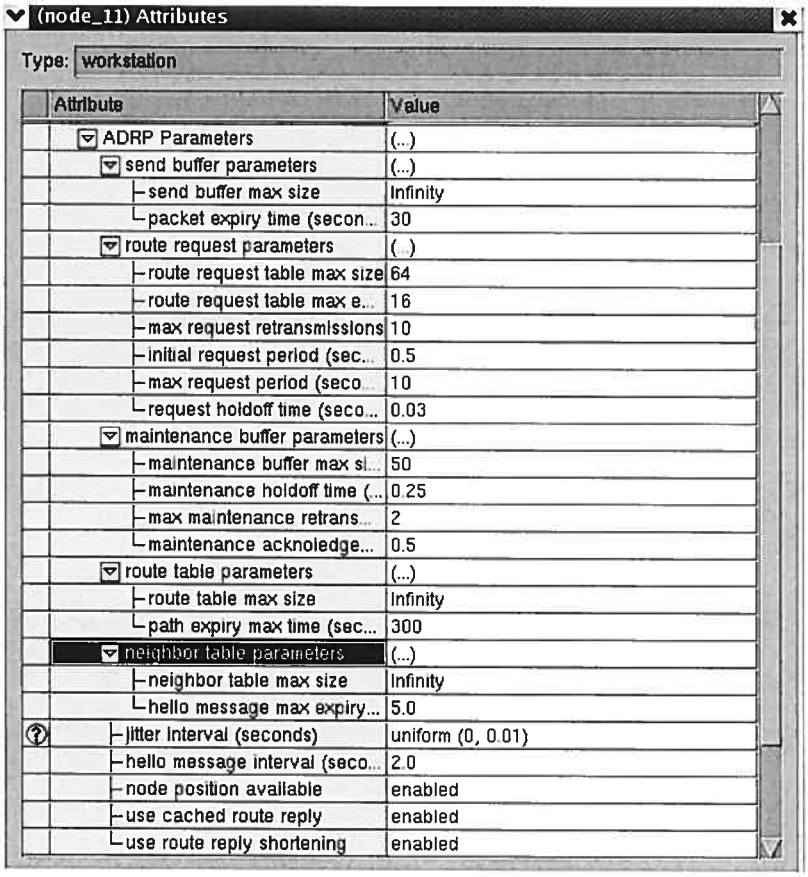


Figure 5.2 : l'interface utilisateur du protocole ADRP.

Paramètres	Détails
Send buffer parameters	Les paramètres de la mémoire tampon où sont stockés les paquets de données en attente d'une route valide.
Route request parameters	Les paramètres de la table où sont stockées les requêtes de route générées ou reçues par ce noeud.
Maintenance buffer parameters	Les paramètres de la mémoire tampon où sont stockés les paquets en attente de la réponse à l'accusé de réception.
Route table parameters	Les paramètres de la table des routes.
Neighbor table parameters	Les paramètres de la table des voisins
Hello message interval	L'intervalle de temps pour l'envoi des messages d'information entre voisins.
Node position available	Indique si les positions sont disponibles ou pas. Par défaut les positions sont disponibles.
Use cached route reply	Indique si les nœuds intermédiaires peuvent envoyer une réponse de route. Par défaut l'option est active.

Tableau 5.3 : les principaux paramètres du protocole ADRP.

A noter que les paramètres «*Send buffer parameters*», «*Route request parameters*», «*Maintenance buffer parameters*» et «*Route table paramètres*» sont ceux du protocole DSR et nous les avons utilisé comme tels.

5.4.1. Le processus ADRP

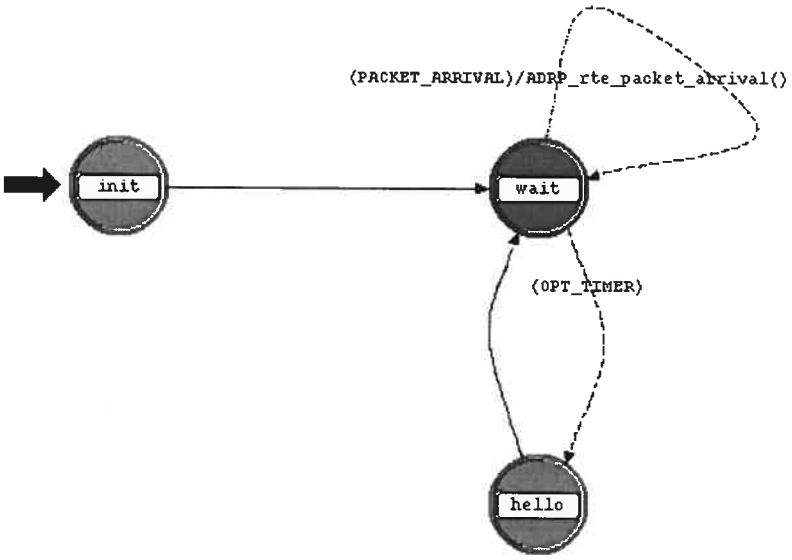


Figure 5.3 : le processus ADRP.

Le processus ADRP est composé de trois états, le premier état est l'étape d'initiation du processus, qui comprend la création des tables et la lecture des différents paramètres du protocole. Le deuxième état est l'état où le processus se met en mode d'attente d'un événement (arrivée d'un paquet, expiration d'une minuterie,...). Une fois l'événement exécuté, le processus revient à cet état et se remet en mode d'attente. Le troisième état est l'état dans lequel le processus transite à intervalles de temps réguliers pour exécuter la procédure d'envoi de messages d'information aux voisins. Une fois la procédure exécutée le processus revient à l'état d'attente.

5.4.2. Le format du paquet ADRP

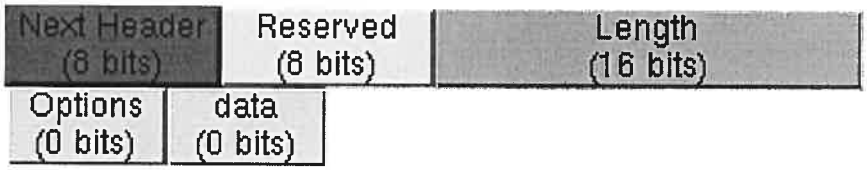


Figure 5.4 : format du paquet ADRP.

Comme le montre la figure 5.4, le paquet ADRP contient le champ entête suivante pour pointer vers le prochain protocole qui suit ADRP dans le datagramme IP, le champ option quant à lui est utilisé pour insérer les options d'ADRP et peut contenir les options suivantes :

- option requête de route;
- option réponse de route;
- option erreur de route;
- option message d'information;
- option route source et demande d'accusé de réception;
- option réponse d'accusé de réception.

Les formats de ces options ont été détaillés dans le chapitre 4.

5.4.3. Le traitement du trafic de ADRP

Le fonctionnement du protocole ADRP a été décrit en détail dans le chapitre 4. Nous décrivons ici le traitement du trafic et son acheminement entre les processus dans Opnet Modeler. Ce que nous décrivons ici pour ADRP est valable pour tout protocole Ad hoc implémenté dans Opnet, à quelques différences près pour AODV et ADRPH.

Arrivée d'un paquet de données de la couche application

Le processus de routage IP achemine le paquet de données vers le processus Manet si le protocole ADRP est spécifié comme protocole de routage. Le processus Manet envoie le paquet au processus ADRP qui ajoutera un paquet ADRP avec l'option route source dans le datagramme IP et l'enverra à la couche MAC.

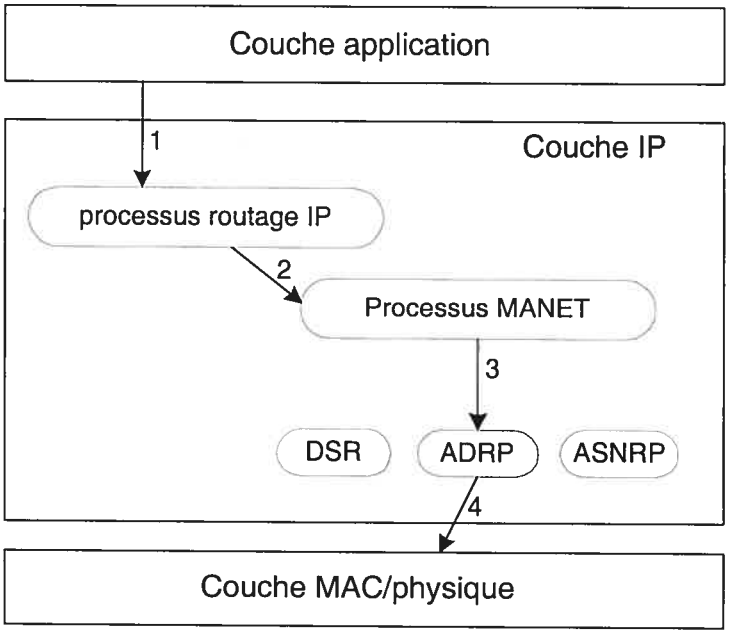


Figure 5.5 : trafic de données provenant des couches supérieures.

Arrivée d'un paquet de données de la couche MAC

Quand le paquet de données provenant de la couche MAC est envoyé au processus ADRP, ce dernier vérifie si le paquet est destiné à ce nœud. Si c'est le cas, le paquet ADRP est supprimé du datagramme IP et le reste du paquet est envoyé à la couche application. Dans le cas contraire, le paquet est envoyé à la couche MAC pour être acheminé vers le prochain nœud dans la route source.

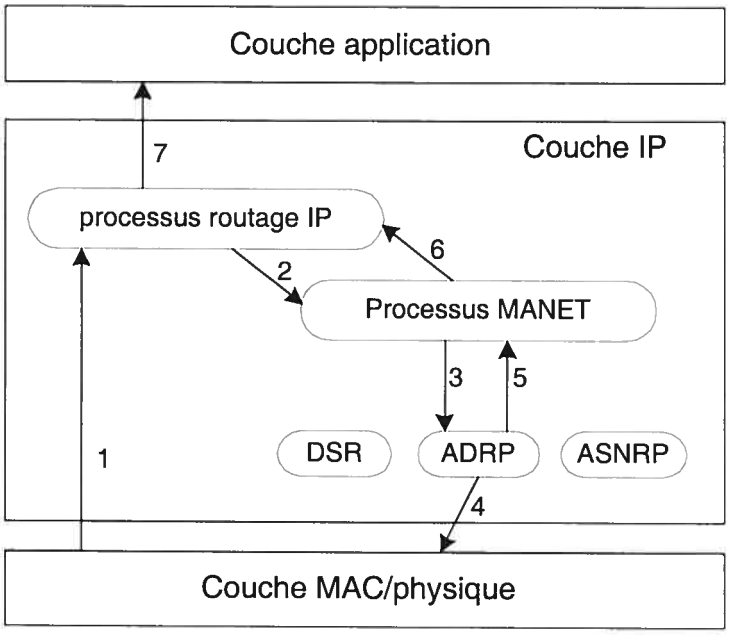


Figure 5.6 : trafic de données provenant des couches inférieures.

Paquet de signalisation du protocole de routage

Les paquets de signalisation de routage sont générés par le protocole de routage et ne vont pas au-dessus de la couche réseau. Les paquets de requête de route, réponse de route, erreur de route et accusé de réception en font partie.

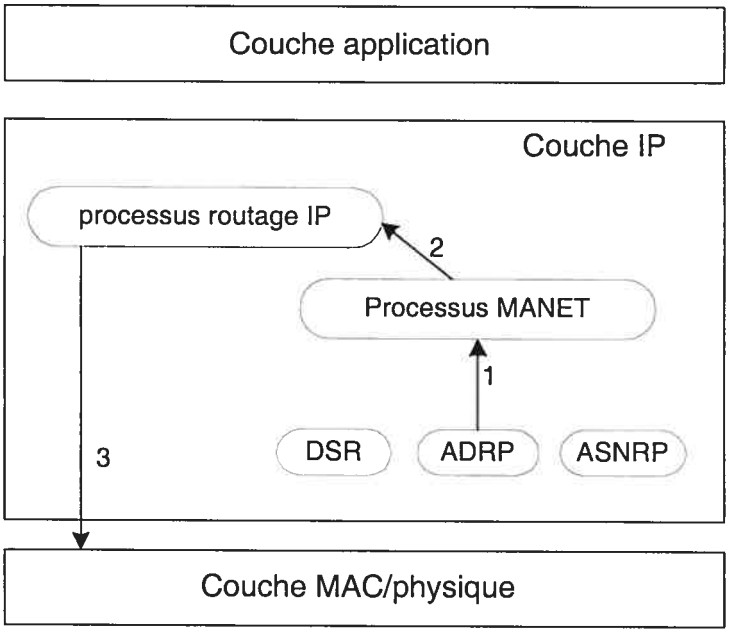


Figure 5.7 : trafic de routage provenant du protocole de routage.

Paquet de signalisation de la couche mac

De même, les paquets de signalisation provenant de la couche MAC et contenant l'option ADRP sont acheminés vers le processus ADRP. Le paquet est traité selon l'option qu'il contient (requête de route, réponse de route, ...). Ou bien il sera acheminé vers la couche MAC, cas d'une requête de route ou réponse de route, ou bien il sera détruit, cas d'un message d'information entre voisins.

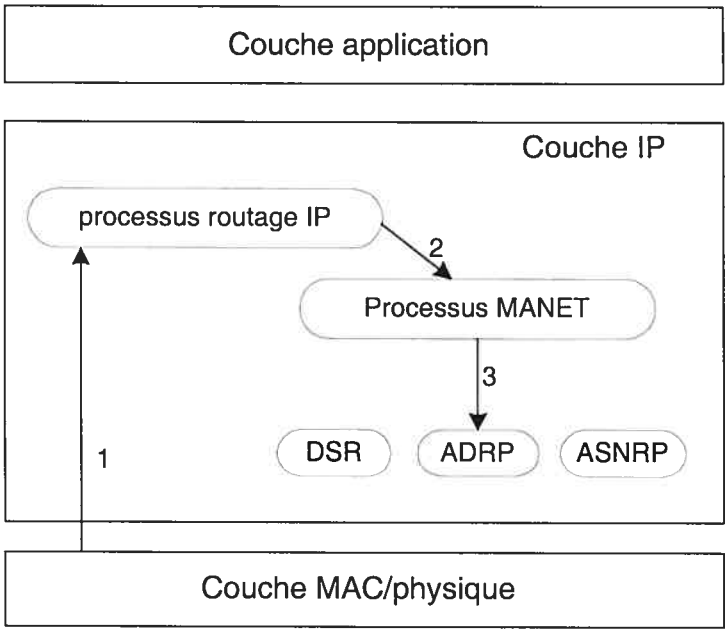


Figure 5.8 : trafic de routage provenant des couches inférieures.

5.5. Implémentation de ADRPH

Pour des raisons de simplification, le protocole ADRPH, la version saut par saut de ADRP, a été implémenté directement sur le code de AODV, en ajoutant la requête de route sélective et les messages d'information entre voisins. Comme AODV, ADRPH utilise la table de routage commune de IP. Quand un paquet arrive de la couche application, le module IP vérifie si une route existe dans la table de routage commune. Si c'est le cas, le paquet est directement envoyé à la couche MAC sans qu'il passe par ADRPH. Ce qui veut dire qu'il n y aura aucune trace, au niveau de ADRPH, des paquets de données pour lesquelles une route existe dans la table de routage commune. Mise à part la découverte de route et les messages d'information entre voisins, ADRPH a les mêmes spécifications techniques que AODV, les spécifications de AODV sont décrites dans [31].

ADRPH se présente à l'utilisateur comme le montre la figure 5.9. Le tableau 5.4 donne une description des principaux paramètres.

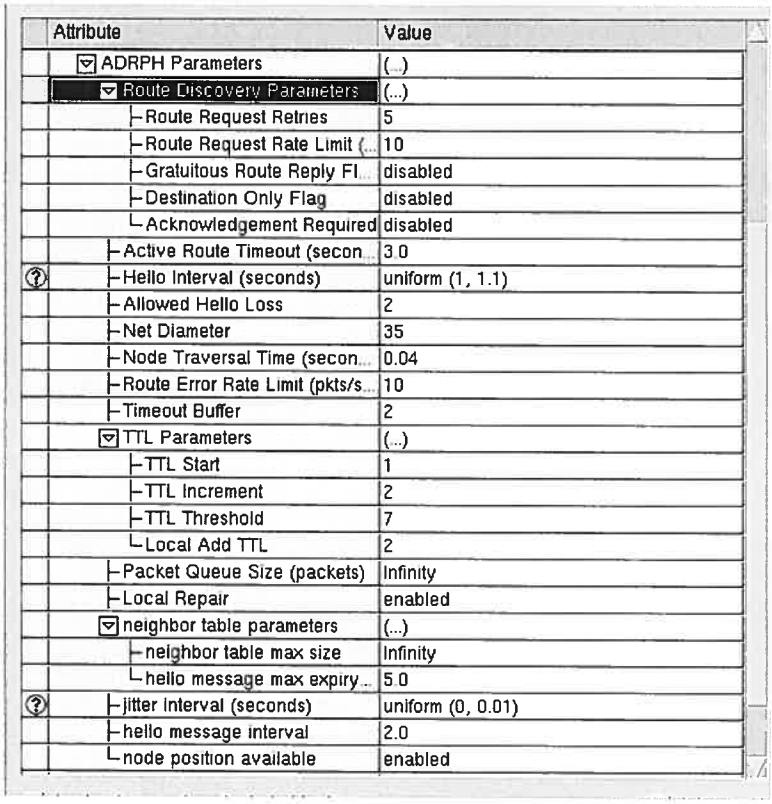


Figure 5.9 : l'interface utilisateur du protocole ADRPH.

Paramètres	Détails
Route Discovery Parameters	Les paramètres de la découverte de route
Net Diameter	La valeur maximale de nombre de sauts dans le réseau
TTL Parameters	les valeurs que peut prendre TTL pour la découverte de route. Si TTL atteint la valeur TTL threshold sans que la reponse de route arrive, alors il prend la valeur Net Diameter.
Neighbor table parameters	Les paramètres de la table des voisins

Tableau 5.4 : les principaux paramètres du protocole ADRPH.

5.6. Implémentation du protocole ASNRP

ASNRP se présente à l'utilisateur de la même façon que ADRP, excepté pour les paramètres des nœuds fixes, comme le montre la figure 5.10. Les paramètres spécifiques à ASNRP sont expliqués dans le tableau 5.5.

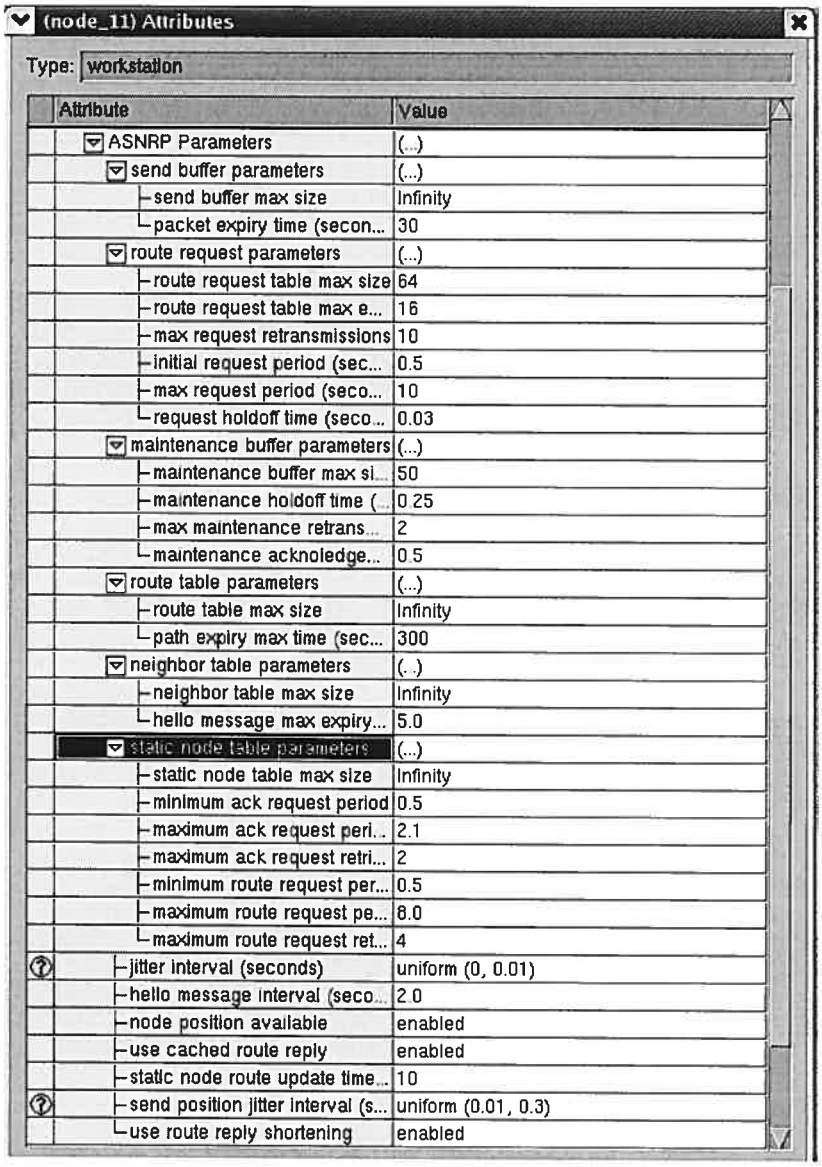


Figure 5.10 : l'interface utilisateur du protocole ASNRP.

Paramètres	Détails
Static node table parameters	Les paramètres de la table des nœuds fixes.
Static node route update timer	L'intervalle de temps pour la mise à jour des routes entre les nœuds fixes
Send position jitter interval	Parce qu'il est primordial que les positions des nœuds fixes atteignent tous les nœuds du réseau. Les nœuds fixes ajoutent un temps d'attente supplémentaire, pris sur cet intervalle, pour l'envoi de leurs positions. Ce qui d'éviterait que les envoient des positions se fassent au même instant.

Tableau 5.5 : les paramètres spécifiques du protocole ASNRP.

5.6.1. Le processus ASNRP

Outre les états que contient le processus ADRP, le processus ASNRP contient l'état d'initialisation des nœuds fixes qui se fait avant que le processus entre en mode d'attente.

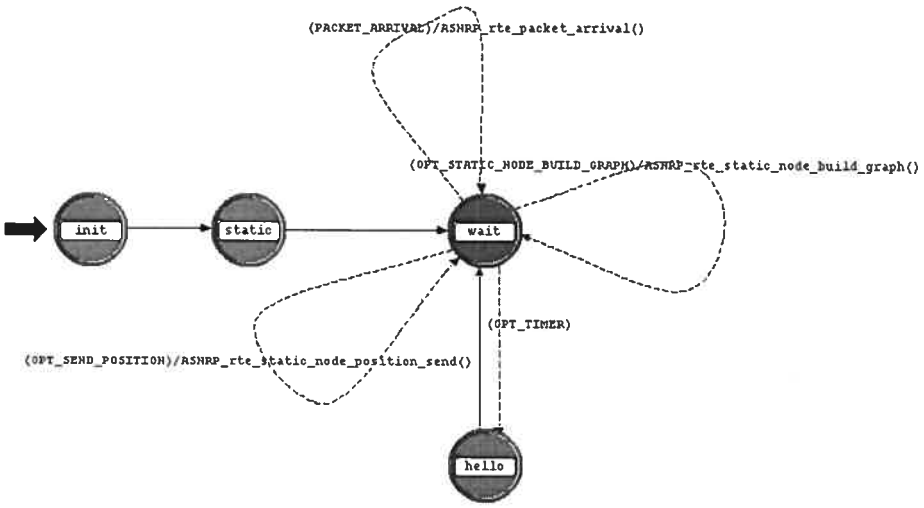


Figure 5.11 : le processus ASNRP.

5.6.2. Le format du paquet ASNRP

Le paquet ASNRP a le même format que le paquet ADRP représenté dans la figure 5.4. ASNRP utilise des options de paquets supplémentaires réservées aux nœuds fixes et qui sont :

- l'option envoi des positions des nœuds fixes;
- l'option accusé de réception pour la maintenance de routes entre les nœuds fixes;
- l'option réponse d'accusé de réception pour la maintenance de routes entre les nœuds fixes;
- l'option requête de route d'un nœud source;

- l'option requête de route d'un nœud fixe à un autre nœud fixe;
- l'option requête de route d'un nœud fixe aux nœuds mobiles;
- l'option de reconstruction de l'arbre.

Chacune de ces options a été décrite dans la section 4.3 du chapitre 4.

5.6.3. Le fonctionnement de ASNRP

En ce qui concerne le fonctionnement de ASNRP du point de vue trafic, le protocole réagit de la même façon que ADRP, les paquets suivent les mêmes acheminements schématisés dans les figures 5.5 à 5.8.

5.7. Simulations et comparaisons

Pour évaluer les protocoles que nous avons conçus, nous les avons testés sur plusieurs scénarios, et nous avons comparé leurs performances avec d'autres protocoles.

Le protocole ADRP a été comparé au protocole DSR, étant donné que les deux protocoles utilise le routage à la source. ADRPH a été comparé à AODV puisque ce sont deux protocoles saut par saut. Quant au protocole ASNRP, vu qu'on ne trouve pas un autre protocole utilisant les nœuds fixes qui soit implémenté sur Opnet, nous l'avons comparé à ADRP pour essayer de montrer quel est l'apport de l'utilisation des nœuds fixes dans le routage.

Sauf mention contraire, les paramètres que nous allons décrire ici, sont les paramètres utilisés par défaut dans les simulations effectuées.

Les nœuds ont un débit de 2 mbps et la portée des transmetteurs est de 250 m.

Le trafic utilisé est un trafic à débit constant, il est généré par le module Manet de Opnet, c'est-à-dire, qu'il ne va pas passer au-delà de la couche réseau, et n'utilise donc aucun protocole de transport. Les caractéristiques de ce trafic sont les suivantes :

- début du trafic à 100s;
- le trafic s'arrête à la fin de la simulation;
- l'intervalle de temps entre les paquets de données est de 1s;
- la taille des paquets de données est de 1024bits;
- la destination est déterminée aléatoirement.

La mobilité utilisée, est une mobilité aléatoire [62]. Le nœud choisit un point aléatoirement dans le réseau, se déplace jusqu'à ce point, fait un temps de pause en ce point, puis recommence en choisissant un autre point du réseau. Les paramètres suivants sont utilisés pour cette mobilité :

- la vitesse est prise dans l'intervalle d'entiers [0, 10] m/s;
- le temps de pause est de100s;
- la mobilité commence 10s après le début de la simulation;
- la mobilité se termine à la fin de la simulation.

5.7.1. Les métriques de comparaison

Cinq métriques de performance, que nous avons jugé les plus importantes, ont été évaluées pour comparer les protocoles :

- **le taux de paquets reçus** : c'est le ratio des paquets reçus par rapport aux paquets envoyés par les sources de trafic.

- **le délai de bout en bout** : c'est le délai, en secondes, calculé par le nœud destinataire du paquet. Il inclut tout le temps passé par le paquet dans le réseau depuis sa génération.
- **les données abandonnées au niveau MAC** : calculées en bit par seconde, c'est l'ensemble des données qui ont été abandonnées au niveau MAC, soit parce que l'envoyeur n'arrivait pas à recevoir d'accusé de réception, soit parce que les tampons mémoires étaient pleins.
- **le délai au niveau MAC** : représente le délai, en secondes, d'envoi entre deux nœuds adjacents. Ce délai est calculé depuis que le paquet arrive à la couche MAC en provenance des couches supérieures, au niveau du nœud envoyeur, jusqu'à ce qu'il soit livré aux couches supérieures, au niveau du nœud récepteur.
- **le taux de trafic de routage** : représente le nombre de paquets de routage envoyés par rapport au nombre total de paquets envoyés.

5.7.2. Comparaison de ADRP vs DSR

Nous avons testé le protocole ADRP sur plusieurs scénarios pour nous assuré de son bon fonctionnement et de son efficacité, et pour mesurer ses performances nous l'avons comparé au protocole DSR. Le protocole ADRP a été testé avec ses paramètres par défaut, comme illustré sur la figure 5.2. Quant à DSR, l'option sauvetage de paquet, qui n'existe pas dans ADRP, a été désactivée. Cette option est utilisée par DSR pour tenter de sauver un paquet de données, pour lequel il n'a pas reçu d'accusé de réception, cas d'une rupture de route par exemple. Au lieu de rejeter le paquet, le nœud regarde si dans sa table de route, il existe une route valide vers la destination. Il remplace la portion de route invalide dans le paquet de données par la nouvelle route, et essaye de renvoyer le paquet. Nous avons testé DSR avec cette option, et nous avons constaté qu'elle détériore nettement les performances du

protocole, et nos constatations concordent avec les discussions de [63] sur DSR. De même, la réponse de route par les nœuds intermédiaires est activée pour les deux protocoles. Nous avons fait quelques tests sans cette option, mais les résultats ont montré une détérioration des performances du réseau avec une congestion très rapide, et ceci pour les deux protocoles.

Pour ce mémoire, nous avons choisi cinq scénarios pour la comparaison des deux protocoles.

Scénario 1

Dans le scénario 1, le réseau est constitué de 100 nœuds fixes et un serveur FTP, fixe aussi. Le trafic utilisé ici, n'est pas le trafic que nous avons défini comme trafic par défaut, mais du trafic FTP que s'échangent les nœuds et le serveur. Voici les caractéristiques du scénario :

- la superficie : 2000×2000m;
- la durée de la simulation : 1h;
- le nombre de simulations effectuées : 5;
- le nombre de source de données : 100.

Le trafic FTP a les caractéristiques suivantes :

- le temps inter requêtes : 20s;
- la taille des fichiers de données : 1000 octets;
- la destination des requêtes : le serveur FTP.

Scénario 2

Dans le scénario 2, le réseau est constitué de 25 nœuds mobiles, se déplaçant selon des trajectoires définies au lieu de la mobilité aléatoire. Chaque trajectoire est

formée d'un ou de plusieurs segments de droite. Pour chaque segment, on peut spécifier soit la vitesse, soit le temps que mettra le nœud pour le parcourir. Pour ce scénario, nous avons utilisé deux trajectoires. Dans la première trajectoire, le nœud se déplace à gauche puis vers le nord. Dans la deuxième trajectoire, le nœud se déplace à droite puis vers le sud. Chaque trajectoire à une longueur de près de 400m, et les nœuds la traversent en un peu moins de 20mn. Et on ne peut associer plus d'une trajectoire à un nœud. Il s'agit donc, d'une mobilité restreinte et lente.

Ce scénario a les caractéristiques suivantes :

- la superficie : 1000×1000m;
- la durée de la simulation : 20mn;
- le nombre de simulations effectuées : 5;
- le nombre de sources de données : 25;
- le trafic est celui défini par défaut.

Scénario 3

Dans le scénario 3, le réseau est formé de 50 nœuds mobiles et a les caractéristiques suivantes :

- la superficie : 1500×800m;
- la durée de la simulation : 1h;
- le nombre de simulations effectuées : 5;
- le nombre de sources de données : 25;
- le trafic est celui défini par défaut;
- la mobilité est celle définie par défaut.

Scénario 4

Dans le scénario 4, le réseau est formé de 100 nœuds mobiles et a les caractéristiques suivantes :

- la superficie : 2200×600m;
- la durée de la simulation : 1h;
- le nombre de simulations effectuées : 5;
- le nombre de sources de données : 50;
- le trafic est celui défini par défaut;
- la mobilité est celle définie par défaut;

Scénario 5

Dans le scénario 5, le réseau est formé de 100 nœuds aussi, mais la mobilité et la taille des paquets sont plus grands. Voici les caractéristiques de ce réseau :

- la superficie : 2200×600m;
- la durée de la simulation : 1h;
- le nombre de simulations effectuées : 5;
- le nombre de sources de données : 50.
- le trafic est celui défini par défaut sauf pour la taille des paquets qui est de : 4096 bits (ou 512 octets).

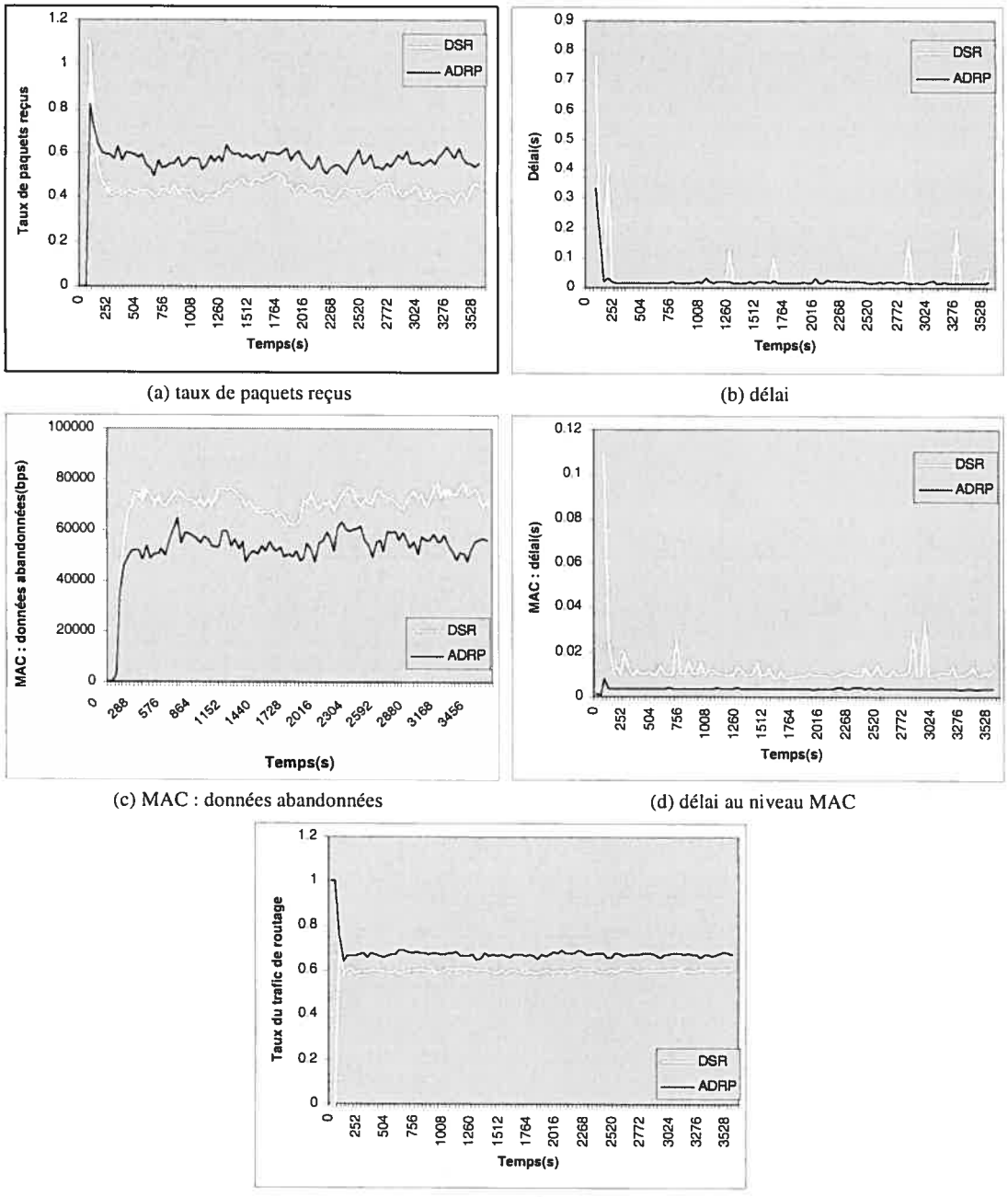
La mobilité est celle définie par défaut avec les modifications suivantes :

- la vitesse est prise sur l'intervalle d'entiers [0, 20] m/s;
- le temps de pause est pris sur l'intervalle d'entiers [20, 100] s;

Résultats des expérimentations

Les résultats obtenus sont affichés sous la forme de graphes qui regroupent les cinq scénarios que nous venons de décrire. Chaque point dans les graphes représente la moyenne des simulations d'un scénario. Mais avant de présenter ces résultats, nous allons monter ce qui se passe au niveau d'un scénario, et nous avons choisi à titre d'exemple le scénario 4.

Comme l'illustre la figure 5.12, les deux protocoles montrent une stabilité en ce qui concerne le taux de paquets reçus, voir le graphe (a), mais ce taux est nettement supérieur pour ADRP par rapport à DSR. A certains moments, DSR affiche des délais de livraison meilleurs que ceux de ADRP, voir le graphe (b). Ceci s'explique par le fait que DSR dispose de plus de routes dans ses tables que ADRP : la diffusion pure permet aux nœuds de recueillir plus de routes que la diffusion sélective de ADRP. Il y a cependant le désavantage que ces routes deviennent rapidement invalides à cause de la mobilité. Les graphes (c) et (d) montrent ce qui se passe au niveau MAC. La taille des données abandonnées et le délai au niveau MAC sont plus grands pour DSR, ce qui veut dire que le réseau est plus chargé dans le cas de DSR. Le nombre élevé de données abandonnées au niveau MAC pour DSR explique bien pourquoi ce protocole a un taux de paquets reçus plus faible que ADRP. Le graphe (e) montre que DSR génère moins de trafic de routage que ADRP. Ce taux est à prendre avec réserve dans la conception d'un protocole de routage, parce qu'il ne reflète pas réellement la charge du trafic dans le réseau. En effet, selon le type de trafic de routage, le trafic au niveau MAC peut varier. Les paquets qui sont envoyés en diffusion comme les requêtes de route et les messages d'informations entre voisins, ne nécessitent pas d'accusé de réception au niveau MAC. Par contre, les paquets qui sont envoyés directement comme les réponses de route et les erreurs de route, nécessitent des accusés de réception au niveau MAC, et risquent d'être renvoyés dans le cas où l'accusé de réception ne parviendrait pas. C'est ce qui contribue à générer plus de trafic au niveau MAC.



(a) taux de paquets reçus

(b) délai

(c) MAC : données abandonnées

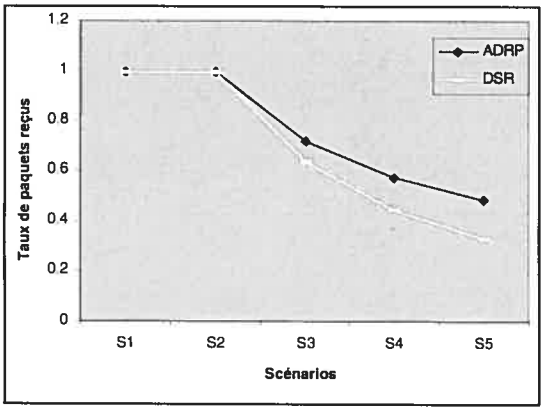
(d) délai au niveau MAC

(e) taux de trafic de routage

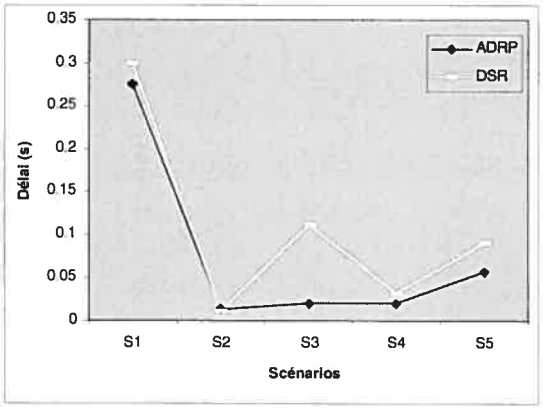
Figure 5.12 : résultats des simulations de ADRP et DSR dans le scénario 4.

La figure 5.13 représente les graphes où sont regroupés les cinq scénarios représentés par les symboles S1 à S5. Le graphe (a), montre que plus la mobilité augmente, plus

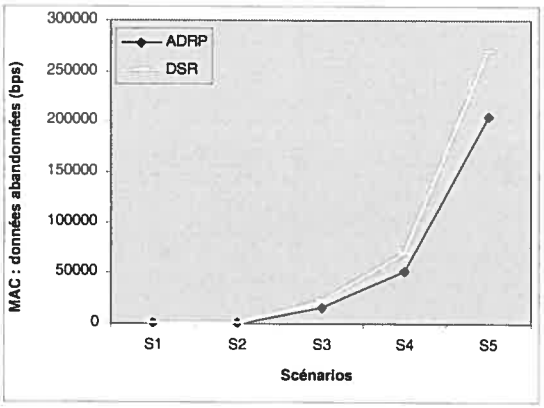
le taux de paquets reçus diminue. Pour les réseaux sans mobilité ou avec une mobilité restreinte, c'est la quasi-totalité des paquets qui sont reçus. Mais dès que la mobilité augmente, le taux de paquets reçus diminue, et l'écart entre les deux protocoles augmente en faveur de ADRP. Dans le graphe (b), le délai élevé pour le scénario 1 est expliqué par le fait qu'il y a un seul serveur FTP qui répond à toutes les requêtes. Les graphes (c) et (d) reflètent bien le trafic qui circule dans le réseau. En effet, plus la mobilité augmente avec le nombre de source de données, plus les routes se brisent, ce qui provoque la génération de requêtes de route. Le scénario 5, où la mobilité et le trafic sont très grands, la taille des données abandonnées et les délais au niveau MAC augmentent rapidement, ce qui explique le très faible taux de paquets reçus dans ce scénario. Encore une fois, le graphe (e) du taux de trafic de routage, qui a aussi été utilisé comme métrique dans [59] et [62], ne reflète pas ce qui se passe réellement dans le réseau, ce graphe montre que DSR génère toujours moins de trafic de routage que ADRP, mais cela ne se traduit pas au niveau du taux de paquets reçus.



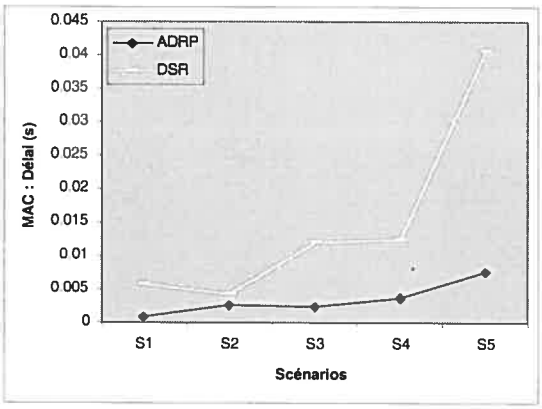
(a) taux de paquets reçus



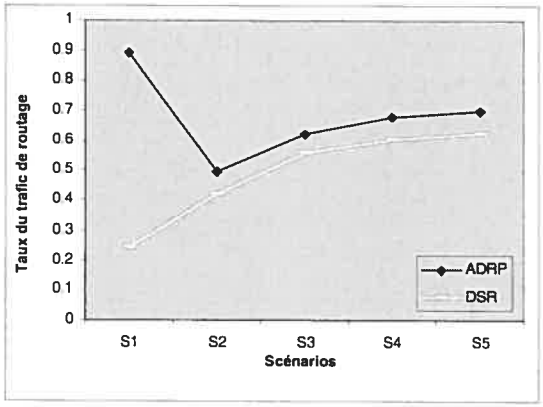
(b) délai



(c) MAC : données abandonnées



(d) délai au niveau MAC



(e) taux de trafic de routage

Figure 5.13 : résultats de la comparaison de ADRP vs DSR sur les 5 scénarios.

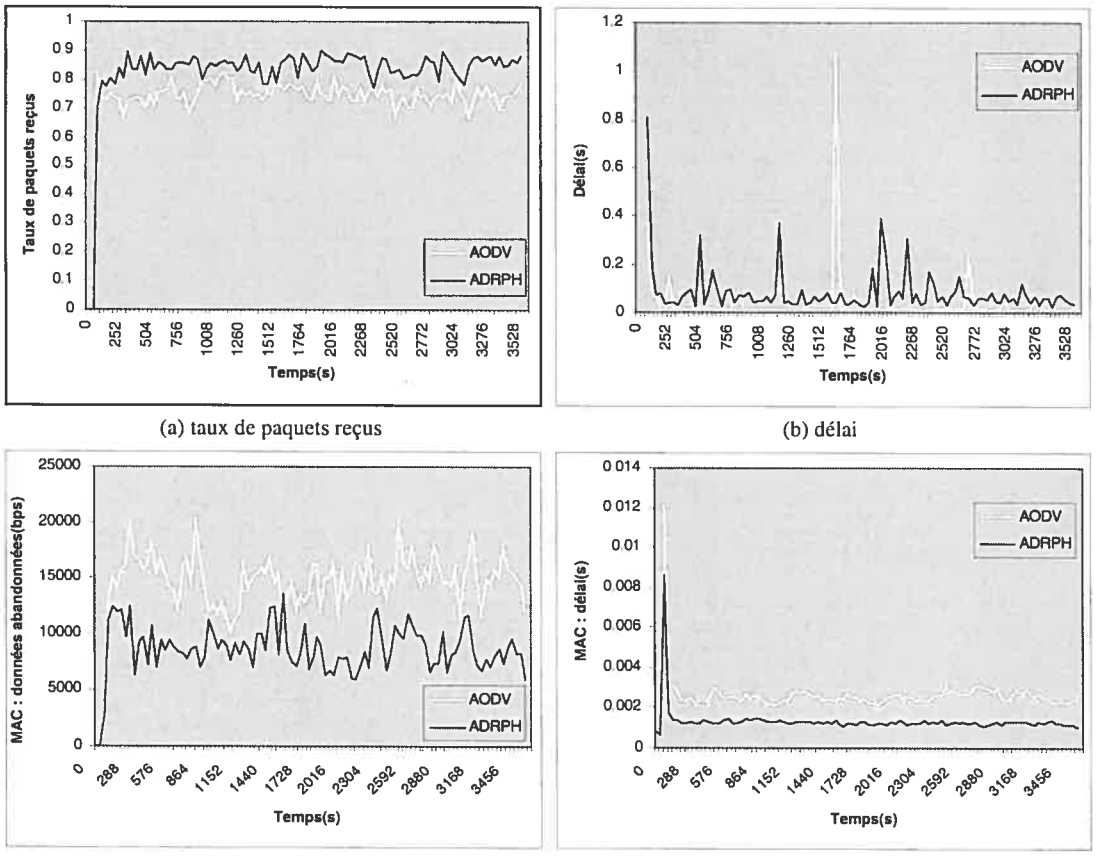
5.7.3. Comparaison de ADRPH vs AODV

Sachant que les protocoles de routage saut par saut ont de meilleures performances que les protocoles de routage à la source, nous avons comparé ADRPH et AODV sur les scénarios où il y a le plus de trafic et de mobilité dans le réseau, c'est-à-dire, les scénarios 4 et 5 de la section précédente. D'une simulation à une autre du scénario 5, nous avons fait varier le nombre de sources de données de 20 à 60 sources. Les deux protocoles ont été utilisés avec leurs paramètres par défaut, voir la figure 5.9 pour les paramètres de ADRPH.

Résultats des expérimentations

Les résultats des deux scénarios sont présentés dans la figure 5.14 et la figure 5.15. Les graphes du taux de paquets reçus, figure 5.14 (a) et figure 5.15 (a), montrent que ADRPH a un meilleur taux que AODV, ce taux est expliqué par les graphes (c) et (d) des deux figures 5.14 et 5.15. Les données abandonnées au niveau MAC et le délai au niveau MAC reflètent réellement ce qui se passe dans le réseau et montrent clairement que ADRPH génère moins de trafic que AODV. Les graphes (b) des deux figures 5.14 et 5.15, montrent que AODV a de meilleurs délais que ADRPH. Comme il a été dit pour DSR, la diffusion pure permet d'avoir plus de routes disponibles dans les tables. Cependant, cela se fait au détriment du taux de paquets reçus. Le taux de trafic de routage n'est pas pris en compte dans ces deux protocoles, parce qu'ils ne gardent pas trace du trafic total à leur niveau, comme il a été expliqué dans la section 5.5 de ce chapitre.

Le scénario 4 donne une idée claire de la supériorité des protocoles de routage saut par saut par rapport aux protocoles de routage à la source. En effet, les taux de paquets reçus de ADRPH et AODV, graphe (a) de la figure 5.14, sont nettement supérieurs aux taux de paquets reçus par ADRP et DSR, graphe (a) de la figure 5.12.



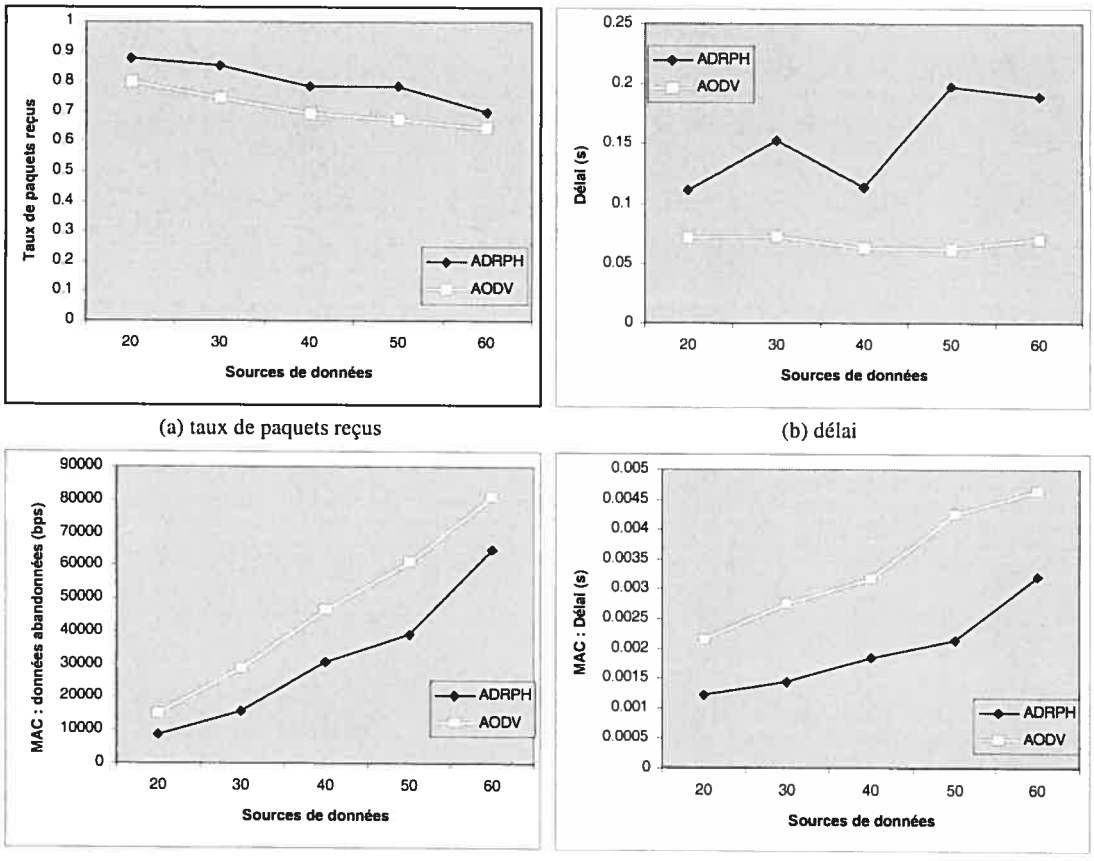
(a) taux de paquets reçus

(b) délai

(c) MAC : données abandonnées

(d) délai au niveau MAC

Figure 5.14 : résultats des simulations du scénario 4 pour ADRPH et AODV.



(a) taux de paquets reçus

(b) délai

(c) MAC : données abandonnées

(d) délai au niveau MAC

Figure 5.15 résultats des simulations du scénario 5 pour ADRPH et AODV.

A partir des résultats de comparaison de ADRP vs DSR et de ADRPH vs AODV, nous pouvons conclure que les protocoles de routage pour les réseaux ad hoc mobiles qui utilisent la requête de route sélective sont plus performants que ceux qui utilisent la diffusion pure pour leurs requêtes de route.

5.7.4. Comparaison de ASNRP vs ADRP

ASNRP est un protocole qui utilise le routage à la source, et exploite la présence de nœuds fixes dans le réseau. Pour évaluer ASNRP, nous avons utilisé un seul scénario où nous faisons varier le nombre de nœuds fixes après chaque série de

simulation. Pour montrer l'apport de l'utilisation des nœuds fixes dans le routage, nous avons comparé ASNRP à ADRP, qui lui ne fait aucun usage particulier des nœuds fixes. D'après les résultats de la comparaison de ADRP et DSR, nous avons jugé inutile de faire la comparaison de ASNRP et DSR pour chaque série de simulation. Nous avons fait la comparaison des trois protocoles, ASNRP, ADRP et DSR, sur une seule série, et pour le reste, la comparaison se fait entre ASNRP et ADRP.

Scénario 1

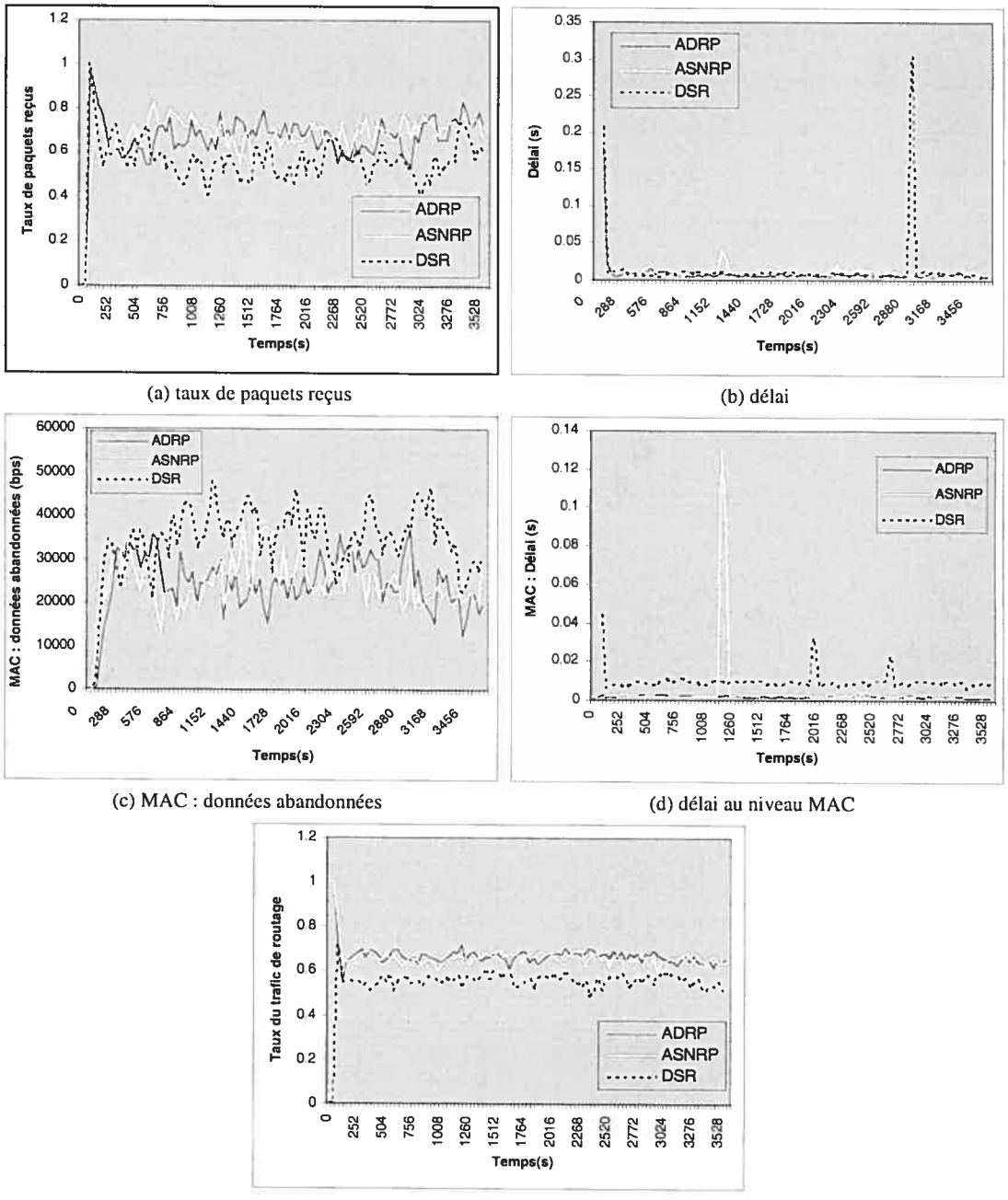
Dans le scénario1, le réseau est composé de 80 nœuds mobiles, et il a les caractéristiques suivantes

- la superficie : 1600×500m;
- la durée de la simulation : 1h;
- le nombre de simulations effectuées par série : 5;
- le nombre de source de données (tous des nœuds mobiles): 32;
- le nombre de nœuds fixes dans le réseau est augmenté après chaque série de simulation, et est pris de l'ensemble {5, 7, 9, 10, 12};
- le débit des nœuds fixes est : 11Mbps;
- le trafic est celui défini par défaut;
- la mobilité est celle définie par défaut.

Résultats des simulations

DSR a été évalué avec ASNRP et ADRP dans le réseau avec 7 nœuds fixes, les résultats de cette série de simulation sont dans la figure 5.16. Les graphes montrent

clairement que ASNRP et ADRP ont de meilleures performances que DSR, et montrent aussi que les performances de ASNRP et ADRP sont très proches.



(a) taux de paquets reçus

(b) délai

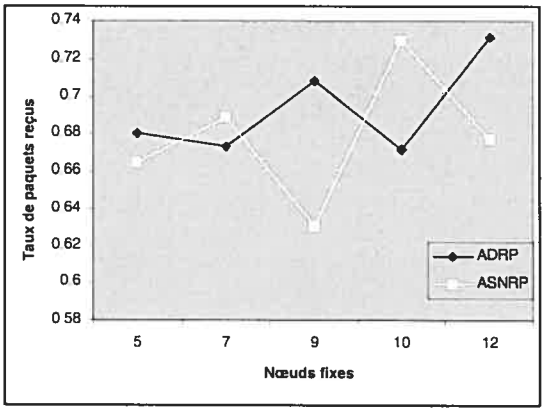
(c) MAC : données abandonnées

(d) délai au niveau MAC

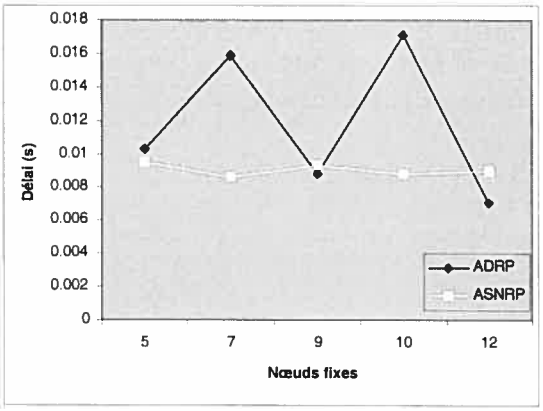
(e) taux de trafic de routage

Figure 5.16 : comparaison de ASNRP, ADRP et DSR sur un réseau avec sept nœuds fixes.

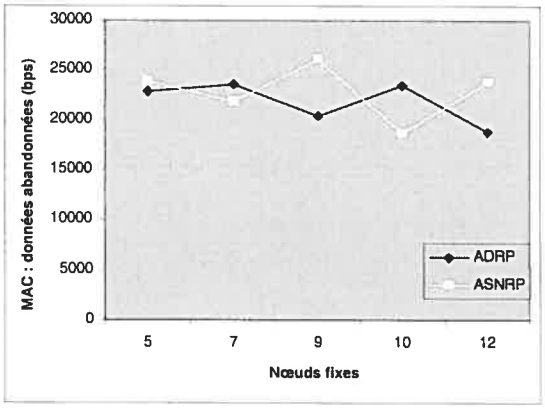
Les résultats de la comparaison de ASNRP et ADRP sont regroupés dans la figure 5.17. L'apport de l'utilisation des nœuds fixes dans le routage dépend de leurs nombres et de leurs dispositions dans le réseau. La stabilité des routes entre les nœuds fixes dépend de la présence des nœuds mobiles autour des nœuds fixes. Pour ce scénario constitué de 80 nœuds mobiles et 32 sources de données, le cas où dix nœuds sources ont été utilisés dans le réseau, a donné les meilleures performances pour ASNRP par rapport à ADRP, sur la base de l'écart dans le taux de paquets reçus. Par contre, le cas où neuf nœuds fixes ont été utilisés, a donné la plus mauvaise performance de ASNRP par rapport ADRP, toujours sur la base de l'écart dans le taux de paquets reçus.



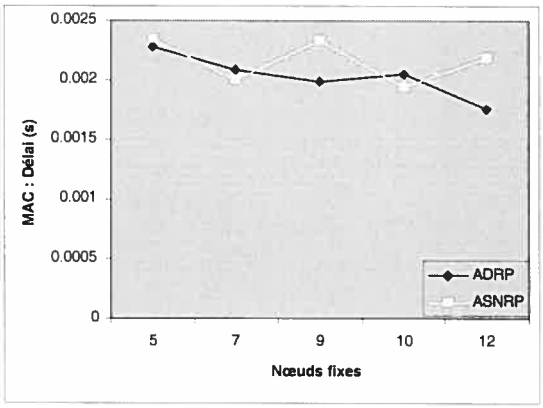
(a) taux de paquets reçus



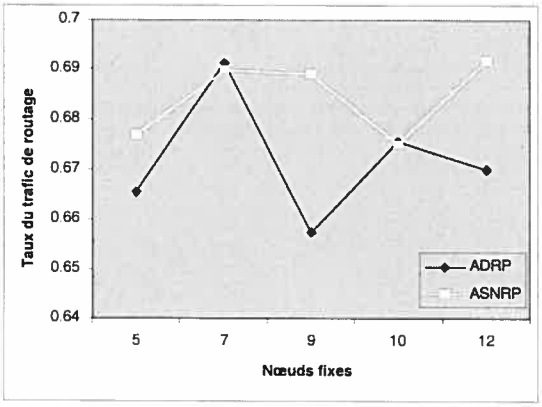
(b) délai



(c) MAC : données abandonnées



(d) délai au niveau MAC



(e) taux de trafic de routage

Figure 5.17 : résultats des simulations de ASNRP et ADRP.

Chapitre 6

Conclusion

Dans ce mémoire, nous avons traité des problèmes de routage dans les réseaux ad hoc. Nous avons proposé deux protocoles de routage pour ces réseaux et que nous avons présenté au chapitre 4.

Le premier protocole a été conçu pour les réseaux ad hoc mobiles. Il a pour nom ADRP, c'est un protocole de routage géographique, réactif et qui utilise le routage à la source. ADRP se distingue des protocoles géographiques par le fait qu'il n'a besoin que des positions de ses voisins immédiats, et pas de celle de la destination. Il se distingue aussi des protocoles réactifs purs, par le fait qu'il utilise une requête de route sélective, en choisissant parmi ses voisins les meilleurs candidats pour l'acheminement des requêtes de route. Une variante saut par saut de ce protocole, et qui a pour nom ADRPH, a été proposée et présentée au même chapitre.

ADRP et ADRPH ont été évalués sur le simulateur Opnet Modeler et ont été comparés respectivement à DSR et AODV, deux protocoles utilisant la diffusion pure pour les requêtes de route.

Les résultats obtenus montrent que les protocoles ADRP et ADRPH ont des performances nettement meilleurs que DSR et AODV, ce qui nous permet de dire

que les requêtes de routes sélectives sont préférables à la diffusion pure, et nos conclusions vont à dire que ce type de requête sera d'un apport non négligeable pour l'avenir du routage dans les réseaux ad hoc.

Le deuxième protocole que nous avons proposé, est un protocole de routage pour les réseaux ad hoc en présence de nœuds fixes, et il a pour nom ASNRP. Dans ce protocole nous tentons d'exploiter les nœuds fixes dans l'acheminement des requêtes de route, ceci en construisant un arbre minimal, où les nœuds sont formés par les nœuds fixes et les arcs par les nœuds mobiles.

Nous avons évalué et comparé ce protocole à ADRP, et les résultats obtenus montrent que la performance du protocole dépend du nombre de nœuds fixes, qui lui dépend non seulement de la disposition de ces nœuds, mais dépend aussi du nombre de nœuds mobiles et du nombre de sources de données dans le réseau.

Travaux futurs

Le protocole ADRP et sa variante ADRPH ont montré de très bonnes performances, il serait très intéressant comme futures perspectives de les évaluer dans un contexte de qualité de service surtout dans des applications qui nécessitent de la bande passante vu que ces protocoles réduisent considérablement la charge du trafic dans le réseau.

Il serait aussi intéressant d'envisager une version multi distribution de ce protocole, qui est d'une grande utilité dans le cas où on veut envoyer les mêmes données à un groupe de nœuds au lieu d'un seul (cas de la vidéo par exemple).

Dans le protocole ASNRP, la construction d'un arbre minimal certes diminue le nombre de routes à maintenir entre les nœuds fixes par rapport à un graphe complet, mais les routes à travers l'arbre peuvent être plus grandes. Il serait intéressant de tester le protocole avec d'autres structures de graphes, où il y aurait une plus grande

connexion que dans un arbre mais bien sûr toujours moins que dans un graphe complet.

Bibliographie

[1] IETF MANET Working Group. http://www.ietf.org/html.charters/manet-charter.html

[2] IETF web site. http://www.ietf.org

[3] Bluetooth web site. http://www.bluetooth.com

[4] K. Fall, K. Varadhan, Eds. The ns Manual. http://www-mash.cs.berkeley.edu/ns/, December 2003.

[5] Opnet web site. http://www.opnet.com

[6] Massachusetts Institute of Technology web site. http://www.mit.edu

[7] GloMoSim web site. http://pcl.cs.ucla.edu/projects/glomosim

[8] Qualnet web site. http://www.qualnet.com

[9] J. Day, H.Zimmermann. The OSI Reference Model. Proceedings of the IEEE, 71(12) :1334-1340, December 1983.

[10] P. Karn. MACA : A New Channel Access Method for Packet Radio. ARRL/CRRL Amateur Radio 9th Computer Networking Conference, London, Ontario, Canada, September 1990.

[11] V. Bharghavan. MACAW: A media access protocol for wireless LAN's. In proceedings of SIGCOMM'94, London, 1994.

[12] F. Talucci, M. Gerla, L. Fratta. MACA-BI (MACA by invitation): A receiver-oriented access protocol for wireless multiple networks. In PIMRC '97, septembre 1997.

[13] IEEE Computer Society, IEEE Std 802.11 - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999 Edition.

[14] P. Nicopolitidis [et al.]. Wireless networks, Chichester, England; Hoboken, NJ:J. Wiley, 2003.

[15] M. Gondran, M. Minoux. Graphes et algorithmes. 2eme edition, Paris, Eyrolles, 1985.

[16] A. Tanenbaum, Réseaux, 4eme edition, Prentice Hall, 2003.

[17] C.K. Toh. Ad hoc mobile wireless networks : protocols and systems. Upper Saddle River, NJ : Prentice Hall, 2002.

[18] C.E. Perkins. Ad Hoc Networking. Addison-Wesley, 2001.

[19] S. Xu, T. Saadawi. Revealing the problems with 802.11 medium access control protocol in multi-hop wireless ad hoc networks. Computer Networks, 38(4) :531-548, March 2002.

[20] K. Sundaresan, H-Y. Hsieh, R. Sivakumar. IEEE 802.11 over multi-hop wireless networks: problems and new perspectives. Elsevier, Ad Hoc Networks, 2(2) :109-132, April 2004.

[21] G. Holland, N. Vaidya, P. Bahl. A rate-adaptive MAC protocol for multi-Hop wireless networks. Proceedings of the 7th annual international conference on Mobile computing and networking, 236-251, July 2001.

[22] J. Jubin, J.D. Tornow. The DARPA packet radio network protocols. Proceedings of the IEEE, 75(1) :21-32, January 1987.

[23] G.S. Lauer. Packet-radio routing. In Routing in Communications Networks, edited by Martha E. SteenStrup, chapter 11, 55-76. Prentice-Hall, Englewood Cliffs, New Jersey, 1995.

[24] S. Corson, J. Macker. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. Internet Request For Comments RFC 2501, IETF, January 1999.

[25] R.G. Ogier [et al]. Topology dissemination based on reverse-path forwarding (TBRPF). Internet Request For Comments RFC 3684, IETF, February 2004.

[26] P. Jacquet [et al]. Optimized link state routing protocol. Internet Request For Comments RFC 3626, IETF, October 2003.

[27] C.E. Perkins, P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In Proceedings of the SIGCOMM 94 Conference on Communications Architectures, Protocols and Applications, 234-244, August 1994.

[28] B. Bellur, R.G. Ogier. A reliable, efficient topology broadcast protocol for dynamic networks. In Proceedings IEEE INFOCOM, Volume (1) :178-186, March 1999.

[29] P. Jacquet [et al]. Optimized link state routing protocol for ad hoc networks. In Proceedings IEEE INMIC,62-68, December 2001.

[30] D.B. Johnson [et al]. The dynamic source routing protocol for mobile ad hoc networks. IETF Internet draft (work in progress), Internet Engineering Task Force, July 2004. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt

[31] C.E. Perkins, E.M. Royer, and S.R. Das. Ad hoc on-demand distance vector (AODV) routing. Internet Request For Comments RFC 3684, IETF, July 2003.

[32] D. Johnson, D.A. Maltz, Dynamic source routing in ad hoc wireless networks. In Mobile Computing, Ch. 5 (T. Imielinski and H. Korth, eds.), Kluwer, 1996.

[33] C.E. Perkins and E.M. Royer. Ad Hoc On-demand Distance Vector Routing. Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., Feb. 1999, pp. 90-100.

[34] E.M. Royer, C-K. Toh. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications, 6(2) :46-55, April 1999.

[35] Z.J. Haas. A New Routing Protocol for the Reconfigurable Wireless Networks. ICUPC'97, San Diego, CA, October 1997.

[36] S. Capkun, M. Hamdi, and J. Hubaux. Gps-free Positioning in Mobile Ad Hoc Networks. Proc. Hawaii Int'l. Conf. System Sciences, January 2001.

[37] Y-B. Ko, N.H. Vaidya. Location-aided routing (LAR). in mobile ad hoc networks. In ACM/IEEE Int. Conf. on Mobile Computing and Networking (MobiCom'98), 66-75, October 1998.

[38] S. Giordano, I. Stojmenovic. Position based routing algorithms for ad hoc networks: A taxonomy. in Ad Hoc Wireless Networking, X. Cheng, X. Huang and D.Z. Du (eds.), Kluwer,103-136, 2004.

[39] I. Stojmenovic. Location updates for efficient routing in ad hoc wireless networks. In Handbook of Wireless Networks and Mobile Computing, Wiley, 451-471, 2002.

[40] M. Mauve, A. Widmer, H. Hartenstein. A survey on position-based routing in mobile ad hoc networks. Network, IEEE, 15(6) :30-39, Nov-Dec 2001.

[41] W.H. Liao, Y.C. Tseng, J.P. Sheu. GRID: A fully location-aware routing protocols for mobile ad hoc networks. Proc. IEEE HICSS, Telecommunication Systems, January 2000.

[42] S. Singh, M. Woo, C.S. Raghavendra. Power-aware routing in mobile ad hoc networks. Proc. MOBICOM, 181-190, 1998.

[43] R. Braden, D. Clark, S. Shenker. Integrated services in the internet architecture: an overview. Internet Request For Comments RFC 1633, IETF, June 1994.

[44] S. Blake [et al]. An architecture for differentiated services. Internet Request For Comments RFC 2475, IETF, December 1998.

[45] H. Xiao [et al]. A flexible quality of service model for mobile ad hoc networks. In IEEE Vehicular Technology Conference, 445-449, Tokyo, Japan, Mai 2000.

[46] S.B. Lee [et al]. INSIGNIA : An ip-based quality of service framework for mobile ad hoc network. Journal of Parallel and Distributed Computing (Academic Press), Special issue on Wireless and Mobile Computing and Communications, 60(4) :374-406, 2000.

[47] Z.Wang, J.Crowcroft, QoS Routing for supporting resource reservation, JSAC, September 1996.

[48] S. Chen, K. Nahrstedt. Distributed quality-of-service routing in ad hoc networks. IEEE Journal on Selected Areas in Communications, special issue on Wireless Ad Hoc Networks, 17(8) :1488-1505, august 1999.

[49] W.H. Liao, S.L. Wang, J.P. Sheu, A Multi-Path QoS Routing Protocol in a Wireless Mobile Ad Hoc Network. Kluwer Academie Publishers, NH, 2002, Telecommunication Systems 19(3): 329-347, 2002.

[50] C. Zhu, M.S. Corson. QoS routing for mobile ad hoc networks. In Proceedings of The 21st Annual Joint conference of the IEEE Computer and Communications Societies, INFOCOM 2002, Vol.2 :958-967, June 2002.

[51] Y. Ge, T. Kunz, L. Lamont. Quality of service routing in ad-hoc networks using OLSR. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 300-308, January 2003.

[52] S.H. Shah, K. Nahrstedt. Predictive location-based QoS routing in mobile ad hoc networks. IEEE International Conference on Communications, Vol.2:1022-1027, May 2002.

[53] H. Liu, Y. Li. A location based QoS routing protocol for ad hoc networks. In Proceedings of 17th International Conference on Advanced Information Networking and Applications, 830-833, March 2003.

[54] Y. Hwang, P. Varshney. An adaptive QoS routing protocol with dispersity for ad-hoc networks. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 302-311, January 2003.

[55] I. Gerasimov, R. Simon. Performance analysis for ad hoc QoS routing protocols. In Proceedings of the International Mobility and Wireless Access Workshop MobiWac 2002, 87-94. October 2002.

[56] A.Veres [et al]. Supporting Service Differentiation in Wireless Packet Networks Using Distributed Control, IEEE Journal of Selected Areas in Communications, October 2001.

[57] R.C. Prim. Shortest connection networks and some generalizations. The Bell System Technical Journal, vol.36: 1389-1401, 1957.

[58] DARPA Internet Program. Internet Protocol. Internet Request For Comments RFC 791, IETF, September 1981.

[59] S.R. Das [et al]. Performance Comparison of Two On-demand Routing Protocols for Ad hoc Networks. IEEE Personal Communications Magazine special issue on Ad hoc Networking,16-28, February 2001.

[60] D. Cavin, Y. Sasson, A. Schiper. On the Accuracy of MANET Simulators. In Proceedings of the second ACM international workshop on Principles of mobile computing, 38 - 43, 2002.

[61] G.F. Lucio [et al]. OPNET Modeler and Ns-2: Comparing the Accuracy of Network Simulators for Packet-Level Analysis using a Network Testbed. In the WSEAS Transactions on Computers, 3(2) :700-707, July 2003.

[62] J. Broch [et al]. A Performance Comparison of Multihop Wireless Ad Hoc Network Routing Protocols. In Proceedings of IEEE/ACM MOBICOM 98, 85-97, October 1998.

[63] G. Holland, N. Vaidya. Analysis of TCP performance over mobile ad hoc networks. In Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking (MOBICOM), 219-230, August 1999.