ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

COMME EXIGENCE PARTIELLE
À L'OBTENTION DE LA
MAITRISE EN GÉNIE
CONCENTRATION : RÉSEAUX DE TÉLÉCOMMUNICATIONS
M. Ing.

PAR
RHIM, Achour

PRÉVISION DU TEMPS DE VIE DU LIEN POUR AMÉLIORER LA STABILITÉ DE ROUTAGE DANS LES RÉSEAUX AD HOC

MONTRÉAL, LE 9 FÉVRIER 2009

PRÉSENTATION DU JURY

CE MÉMOIRE A ÉTÉ ÉVALUÉ

PAR UN JURY COMPOSÉ DE :

M. Zbigniew Dziong, directeur de mémoire
Département de génie électrique à l'École de technologie supérieure

M. Michel Kadoch, codirecteur de mémoire
Département de génie électrique à l'École de technologie supérieure

M. Mohamed Cheriet, président du jury
Département de génie électrique à l'École de technologie supérieure

IL A FAIT L'OBJET D'UNE SOUTENANCE DEVANT JURY ET PUBLIC

LE 3 FÉVIER 2009

À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

REMERCIEMENTS

Je tiens avant tout à remercier M. Mohamed Cheriet d'avoir accepté de présider le jury. Je souhaite exprimer ma gratitude à mon directeur de recherche, Zbigniew Dziong, pour sa patience et ses conseils ainsi que pour m'avoir donné l'opportunité et la liberté de développer mes idées tout au long de la maîtrise. Je remercie également tout particulièrement Michel Kadoch, le codirecteur de ma maîtrise, pour son temps, sa patience et ses bons conseils.

Un grand merci à tous les membres du LAGRIT, spécialement à Zouheir et Osamah. Leurs éclairages et nos discussions ont été pour moi une constante source de compréhension, de questionnement et d'idées. Une dernière pensée à mes parents, ma famille et surtout à ma femme qui ont été une source continue de soutien et d'encouragement.

PRÉVISION DU TEMPS DE VIE DU LIEN POUR AMÉLIORER LA STABILITÉ DE ROUTAGE DANS LES RÉSEAUX AD HOC

RHIM, Achour

RÉSUMÉ

Les réseaux MANETs (*Mobile Ad hoc NETworks*) ont été le sujet de nombreux travaux de recherche au cours des dernières années. Ces recherches ont couvert plusieurs aspects tels que la qualité de service, les problèmes de routage et le problème d'accès au niveau de la couche MAC, mais bien d'autres ont essayé de résoudre ces problématiques avec une approche plus globale et ceci en diminuant l'importance de l'indépendance des couches pour introduire la collaboration entre les couches (*cross-layer*).

La variation constante de la qualité des liens entre les nœuds, suite au mouvement des nœuds, est un des principaux problèmes dans les MANETs. En effet, de nombreuses approches ont été développées pour prédire la qualité de lien, les modèles de mouvement et aussi le temps de rupture. Nous proposons l'intégration de deux méthodes mathématiques de prédiction de temps de vie de lien en utilisant le *Global Posisioning System* (GPS), la puissance du signal ou les deux systèmes en même temps. Ce qui nous ramène à trois implantations différentes. Le but est de permettre aux nœuds ad hoc de tirer avantage des technologies et outils qui existent sur le marché pour prédire le temps de connectivité restant avec leurs voisins. *Dynamic Source Routing* (DSR) est notre choix du protocole de routage du réseau ad hoc. Par conséquent, nous avons comparé quatre variantes du protocole DSR, notant qu'il est toujours possible d'utiliser les méthodes avec tout autre protocole de routage tout en prenant compte des spécificités de chacun.

Pour tester les propositions, une simulation d'un réseau MANET est de loin meilleure à une étude mathématique ou purement théorique. Pour cette raison le simulateur OPNET a été utilisé pour l'implantation de différentes méthodes de prédiction de temps de vie de lien, a fin de comparer les performances des MANETs avec les différentes variantes du protocole DSR.

À travers des simulations sous OPNET, nous montrons l'avantage des approches implantées par rapport à la version originale du protocole DSR et le paramètre qui permet de maximiser les performances des réseaux MANETs.

Mots-clés : estimation, prédiction, temps de vie de lien, performance, MANET.

PREDICTION OF LINK EXPIRATION TIME TO IMPROVE ROUTING STABILITY IN AD HOC NETWORKS

RHIM, Achour

ABSTRACT

MANETs networks (Mobile Ad hoc Networks) have been the subject of much research in recent years. These researches have covered several aspects such as quality of service, routing problems and medium access problem, but many others have tried to resolve these issues with a more global approach and shall reducing the importance of the independence of layers to introduce collaboration between them (cross-layer).

The link quality variation between nodes consequence of nodes movement, is a major problem in MANETs. Indeed, many approaches have been developed to predict the quality of connection, models of movement and also the breaking time. We propose the integration of two mathematical prediction methods of link life time using the Global Positioning System (GPS), the signal strength or both systems simultaneously. The aim is to enable ad hoc nodes to take advantage of technologies and tools in the market to predict the remaining connectivity time with their neighbors. Dynamic Source Routing (DSR) is our choice of routing protocol for ad hoc network. Therefore, we compared four variants of DSR protocol. We note that still possible to use the same algorithm with any other ad hoc routing protocol.

To test the proposals, a simulation of a MANET network is by far a better than mathematical study or purely theoretically. For this reason the OPNET simulator was used to implement various methods of link life time prediction, in order to compare the performance of MANETs with the different variant of DSR protocol.

Through simulations under OPNET, we show the advantage of our approaches compared to the original version of DSR protocol and the parameter needed to maximize the performance of network.

Keywords: estimation, prediction, link life time, performance, MANET.

TABLE DES MATIÈRES

Page

LISTE DES FIGURES

Page

LISTE DES ABRÉVIATIONS, SIGLES

3G	Réseaux mobiles de troisième Génération
4G	Réseaux mobiles de quatrième Génération
AODV	Ad hoc On-demand Distance Vector
AP	Access Point
BER	Bit Error Rate
BSS	Basic Service Set
CDMA	Code Division Multiple Access
CEDAR	Core Extraction Distributed Ad-hoc Routing
CGSR	Cluster-head Gateway Switch Routing
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CTS	Clear To Send
DCF	Distributed Coordination Function
DSDV	Destination Sequenced Distance-Vector
DSR	Dynamic Source Routing protocol
ESS	Extended Service Set
FDMA	Frequency Division Multiple Access
FHSS	Frequency Hopping Spread Spectrum
FSR	Fisheye State Routing
GPS	Global Positioning System
HSR	Hierarchical State Routing

IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISM	Industrial Scientific Medical
ISO	International Standards Organization
LET	Link Expiration Time
MANET	Mobile Ad-hoc NETwork
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Optimized link state routing
OSI	Open Systems Interconnection reference model
PDA	Personal Digital Assistant
PCF	Point Coordination Function
PLBR	Preferred link-based routing
PRNET	Packet Radio NETwork
QoS	Quality of service
RET	Route Expiration Time
RTS	Request to Send
SNR	Signal to Noise Ratio
TDMA	Time Division Multiple Access
TORA	Temporally Ordered Routing Algorithm
TR	Temps de Réaction
UDP	User Datagram Protocol

UMTS	Universal Mobile Telecommunications System
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WRP	Wireless Routing Protocol
ZRP	Zone Routing Protocol

Par souci de clarté, des termes en anglais ont été utilisés, mis en *caractère italique* dans le texte, pour éviter toute confusion avec la traduction.

INTRODUCTION

De nos jours, l'utilisation des appareils sans fil pour communiquer est de plus en plus ancrée dans les habitudes des gens. Ces appareils sont de plus en plus performants, plus petits, accumulant une multitude de fonctionnalités et ayant une autonomie de plus en plus grande. Ce développement crée des attentes plus grandes vu le potentiel des appareils, ce qui confronte les concepteurs et les gestionnaires des réseaux à de nouveaux défis en terme de gestion des ressources, gestion de la *QoS* (*Quality Of Service*) nécessaire aux applications émergentes, d'interopérabilité de système hétérogène et de dimensionnement.

À partir de ces problématiques, le concept des réseaux ad hoc est né. Comme l'a été Internet à ces débuts, l'utilisation primaire des réseaux ad hoc été seulement envisagé sur des terrains militaires, des sites de catastrophes, des rassemblements à haute densité ou utilisés à grande échelle en réseaux de senseurs (*sensor network*). Il n'y'a aucun doute que les applications futures de ces systèmes autonomes seront largement répondues.

En effet, dans un réseau classique, les équipements peuvent être considérés soit comme des équipements terminaux soit comme des équipements de cœurs du réseau, qui le supportent et sont dédiés à l'acheminement du trafic, par contre un réseau ad hoc est en grande majorité constitué d'équipement de cœur, mais qui sont aussi des terminaux, généralement appelés nœud. Ainsi, la particularité principale d'un réseau ad hoc est l'absence d'infrastructure dédiée à l'acheminement du trafic des usagers, par conséquent un nœud utilise ces paires pour communiquer avec d'autre nœud et peut constituer en même temps un relais pour acheminer le trafic de ces paires.

Dans le cas d'un MANET (*Mobile Ad hoc NETwork*), plusieurs problèmes existent, notamment l'ordonnancement et le routage puisqu'il n'y a pas de point d'accès qui s'occupe de la gestion. Voilà que le mouvement des nœuds ajoute une instabilité des liens entre les paires de nœuds du réseau.

Cette instabilité est une source de variation de la qualité de connexion allant jusqu'à une perte de la connexion. Sachant que les mesures de rétablissement au niveau de routage ne s'opèrent qu'une fois la communication est effectivement rompue, c'est donc nécessaire d'éviter le temps de rétablissement de connexion ce qui a fait que l'idée de prédire le temps de vie de lien est une étape importante pour l'amélioration de performance des réseaux AD HOC. Par la suite l'implantation de la *QoS*, nécessaire de plus en plus pour des applications multimédias, sera plus facile ce qui par la suite, améliore les performances globales des protocoles et algorithmes notamment dans la construction et la maintenance de connexion.

L'apport principal de notre travail est la démonstration, que l'intégration de l'estimation et la prédiction de temps de vie des liens, à travers deux algorithmes qui représentent deux technologies différentes, augmentent la performance des réseaux ad hoc et peut constituer une base pour fournir la qualité de service à des applications en temps réel qui sont les plus exigeants sur les ressources nécessaires à la connexion. Notre implantation peut s'appliquer à d'autres protocoles de routage, plus largement, à tous les protocoles de routage qui utilisent le niveau de puissance reçu et/ou permet la communication des coordonnées aux voisins.
Étant donné que les réseaux ad hoc sont très peu déployés, le principal moyen d'étude de test ou de comparaison de performance est les outils de simulations.
En faite nous nous sommes basées sur les hypothèses, que la variation de puissance de signal entre l'émetteur et le récepteur dépend seulement de la distance entre ces derniers et que tous les émetteurs fonctionnent avec une puissance d'émission constante et ont la même sensibilité de réception.

Nous limitons notre étude aux utilisateurs qui se déplacent avec une vitesse constante sur une surface plate donc sans changement de niveau et non sectorisée (mure, obstacle). Par contre, le déplacement des nœuds utilisés dans nos tests est complètement aléatoire (*Random Waypoint Model*) dans un réseau ad hoc homogène.

Dans le premier chapitre, nous introduisons les réseaux ad hoc, leurs spécificités et les différents concepts proposés dans la littérature. Nous exposerons par la suite, notre problématique et notre méthodologie de recherche. Le troisième chapitre sera consacré à la présentation du protocole de routage DSR sur lequel nous avons effectué nos modifications et tests. Le quatrième chapitre présente les différentes méthodes de prédiction de temps de vie de lien ainsi que notre approche d'implantation. Enfin, le dernier chapitre exposera les détails de différents tests que nous avons effectués et une comparaison de performance entre les réseaux utilisant nos approches et ceux de protocole original. Nous terminerons par une conclusion générale et quelques recommandations.

CHAPITRE 1

LES RÉSEAUX AD-HOC

1.1 Introduction

L'objectif principal des réseaux ad hoc est la communication multi-sauts. Cette idée a trouvé un créateur nommé Darius I, un roi perse qui régnât de 522 à 486. Son innovation consiste à faire passer un message, de sa capitale aux provinces de son empire, en plaçant des hommes sur des hautes structures en guise de relai tout au long du chemin. Cette méthode été 25 fois plus rapide en la comparant au messager de l'époque.

Le PRNET (*Packet Radio NETwork*) a été la première solution multisauts utilisant le concept CSMA[1], pour accéder au canal partagé, suivi par l'arrivée du *Bluetooth* par Ericsson. Les réseaux sans fil ad hoc représentent une innovation à grand succès commercial. Mais le succès d'un déploiement à grande échelle nécessite une solution réaliste pour plusieurs problèmes de ce type de réseau comme le support de la qualité de service, les applications temps réelles, le fonctionnement coopératif, le *load balancing*, le trafic multicast et la sécurité.

Avant de parler plus en profondeur sur les contraintes des Réseaux sans fil ad hoc, il est important de distinguer la différence entre les réseaux cellulaires ou à infrastructure et les Réseaux sans fil ad hoc. Un exemple de chaque architecture de réseau est illustré à la Figure 1.1. Différents points de comparaison de deux types d'architecture sont présentés au Tableau 1.1, où la principale différence entre les deux types est le faite que le réseau cellulaire ou sans fil est un modèle infrastructure (*AP Access Point*) alors que le Réseau sans fil ad hoc se base sur les nœuds du réseau donc sur ses paires pour acheminer l'information.

---

[1] *Carrier Sense Multiple Access*

Les répercutions de cette différence trouve écho sur tous les points de comparaisons en générant plus de complexité et de contraintes aux réseaux ad hoc qui seront discutés dans les sections suivantes.

Malgré les désavantages par rapport aux réseaux à infrastructure, les Réseaux ad hoc suscitent beaucoup d'intérêt dans plusieurs domaines d'applications, vu sa rapidité de déploiement et l'auto configuration qui le caractérise. Nous pouvons citer comme exemple les applications militaires, la collaboration et le calcul distribué, les opérations d'urgences, les réseaux maillés, de sonde et hybride.

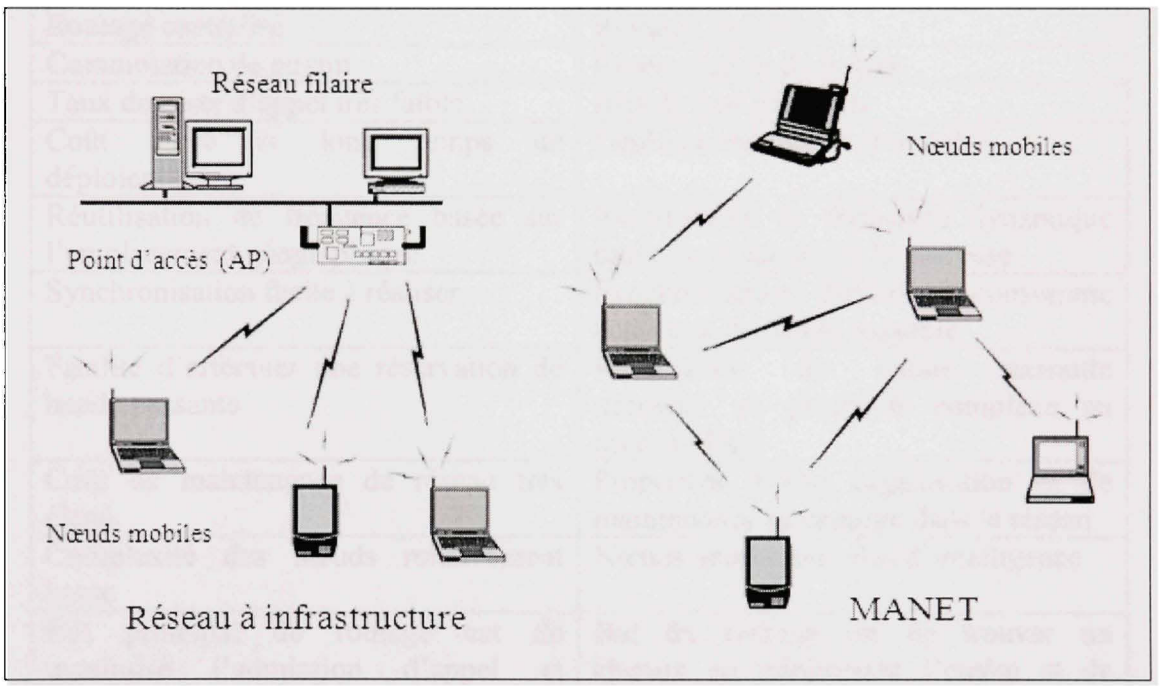


Figure 1.1 Architecture de réseau sans fil à infrastructure et distribué.

Il est à noter que les réseaux ad hoc sont décrits et étudiés par le groupe de travail MANET de l'*Internet Engineering Task Force* (IETF). Une définition formelle de ces réseaux est donnée dans le RFC 2501 (Corson).

Nous aborderons les technologies, protocoles et concepts, que de façon générale, en nous focalisant principalement sur les aspects qui nous intéresse.

Le lecteur pourra se référer aux ouvrages suivants pour compléter toute information complémentaire (AlAgha et al., 2001; Tanenbaum, 2003; Kadoch, 2004; Murthy et al., 2004).

Tableau 1.1

Différence entre les réseaux cellulaires et ad hoc

Réseaux cellulaires	**Réseaux sans fil ad hoc**
Basé sur une infrastructure fixe	Sans infrastructure
Bande passante garantie (pour le trafic voix)	Canal radio partagé (plus adapté pour le trafic de donnée en best effort)
Routage centralisé	Routage distribué
Commutation de circuit	Commutation de paquet
Taux de perte d'appel très faible	Bris de lien fréquents
Coût élevé et long temps de déploiement	Déploiement rapide et rentable
Réutilisation de fréquence basée sur l'emplacement géographique	Réutilisation de fréquence dynamique basée sur l'écoute de la porteuse
Synchronisation facile à réaliser	Synchronisation difficile et consomme beaucoup de bande passante
Facilité d'effectuer une réservation de bande passante	Réservation de bande passante nécessite un protocole complexe au niveau MAC
Coût de maintenance de réseau très élevé	Propriétés d'auto organisation et de maintenance incorporée dans le réseau
Complexité des nœuds relativement basse	Nœuds nécessitent plus d'intelligence
But principal de routage est de maximisé l'admission d'appel et diminuer le rejet	But du routage est de trouver un chemin en minimisant l'entête et de reconfigurer les bris de lien en temps minimum
Largement déployé et actuellement à la 4^{éme} génération de développement.	Plusieurs propositions pour le déploiement commercial existent, mais plus utilisées dans le domaine militaire

1.2 Les réseaux sans fil

Les réseaux sans fil occupent une place très importante dans le domaine de recherche ce qui génère des technologies hétérogènes et diversifiées. Nous survolerons dans cette section les principales technologies de communication sans fil en nous focalisant sur celles qui permettent la communication en mode ad hoc.

La convergence des réseaux cellulaire et sans fil permettra une grande flexibilité et une utilisation très transparente des appareils sans fil.
Les réseaux cellulaires de quatrième génération (4G), sont prévus pour être une convergence entre les réseaux de troisième génération (3G) (CDMA2000 et UMTS) et certaine technologie radio avec pour objectif de fournir un service sans interruption offrant de la qualité de service et proposant un haut débit. Une de ces intégrations est de fournir des capacités de communication ad hoc comme le montre la Figure 1.2. Un grand nombre de publications traite de ce sujet (Gavrilovska, 2005; Meraihi, 2005).

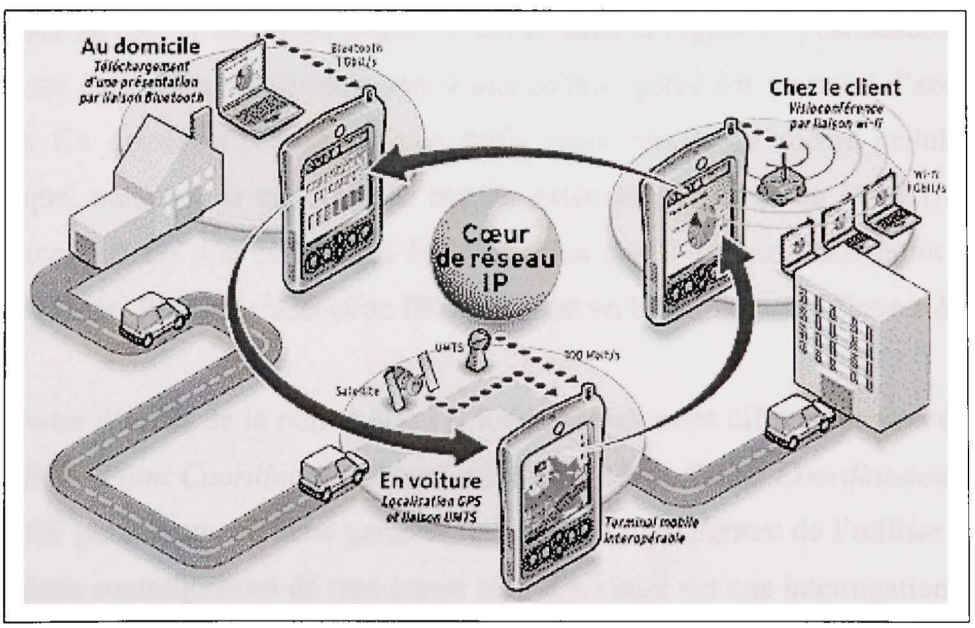


Figure 1.2 Réseau 4G.
Tiré de Xerinay(2004)

Dans le cas de 802.11 et du Bluetooth, l'utilisation de fréquences libres (sans besoin d'autorisation) a été un élément déterminant dans la diffusion des réseaux WLAN et WPAN. Alors que dans la plupart des pays les fréquences dites Industriel-Scientifique-Médical (ISM) dans la bande des 2.4GHz et 5GHz sont, libres, ou en voie de libéralisations.

Les technologies 802.11 permettent la création de WLAN à haut débit et une connexion avec les services des WAN et d'Internet.
Pour des utilisateurs ayant une portée radio plus courte, des technologies telles que Bluetooth, peu gourmandes en énergie, permettent des connexions sans fil et donnent ainsi plus de flexibilité et d'interconnexion entre des équipements personnels (PDA, ordinateurs, cellulaire, imprimante, souris, etc. ...).
Dans les prochaines sections, nous présenterons plus en détail les technologies 802.11 et Bluetooth.

1.2.1 La norme 802.11

L'architecture de base d'un réseau 802.11, illustrée dans la Figure 1.**3**, est basée sur un BSS (*Basic Service Set*), qui peut correspondre à une cellule, gérée par un point d'accès (*Access Point*, AP). Ce dernier s'occupe de tout trafic entre nœuds de même cellule ou entre n'importe quel nœud de la cellule et le monde extérieur. Alors qu'un IBSS (*Independent Basic Service Set*) est une cellule qui fonctionne en mode ad hoc, sans point d'accès ni gestion centralisée. Plusieurs BSS et/ou IBSS forment un ESS (*Extended Service Set*)

Deux méthodes d'accès de la norme 802.11, fondamentalement différentes sont disponibles, les modes PCF (*Point Coordination Function*) et DCF (*Distributed Coordination Function*). Le mode PCF permet une certaine garantie de service ce qui permet de l'utiliser pour servir les applications contraignantes de type temps réel. Il est basé sur une interrogation périodique des nœuds de la cellule par l'AP donc une gestion centralisée de l'accès au médium ce qui permet de prioriser un type d'application par rapport à un autre. Le mode DCF par contre

permet à tous les nœuds d'avoir la même chance d'accéder au canal. Cette chance est calculée aléatoirement par chaque nœud.

Un réseau IEEE 802.11 peut utiliser à la fois les modes DCF et PCF alors que le mode DCF doit être utilisé dans un IBSS. Dans le mode DCF, l'accès au canal est basé sur le protocole CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) dont certains aspects de fonctionnement seront détaillés dans la section 1.3.2.
Une explication détaillée des couches physiques et MAC des différentes technologies 802.11 (802.11a, 802.11b, 802.11g, etc.) est disponible dans la spécification (ANSI/IEEE, 2003) et dans (AlAgha et al., 2001; Tanenbaum, 2003).

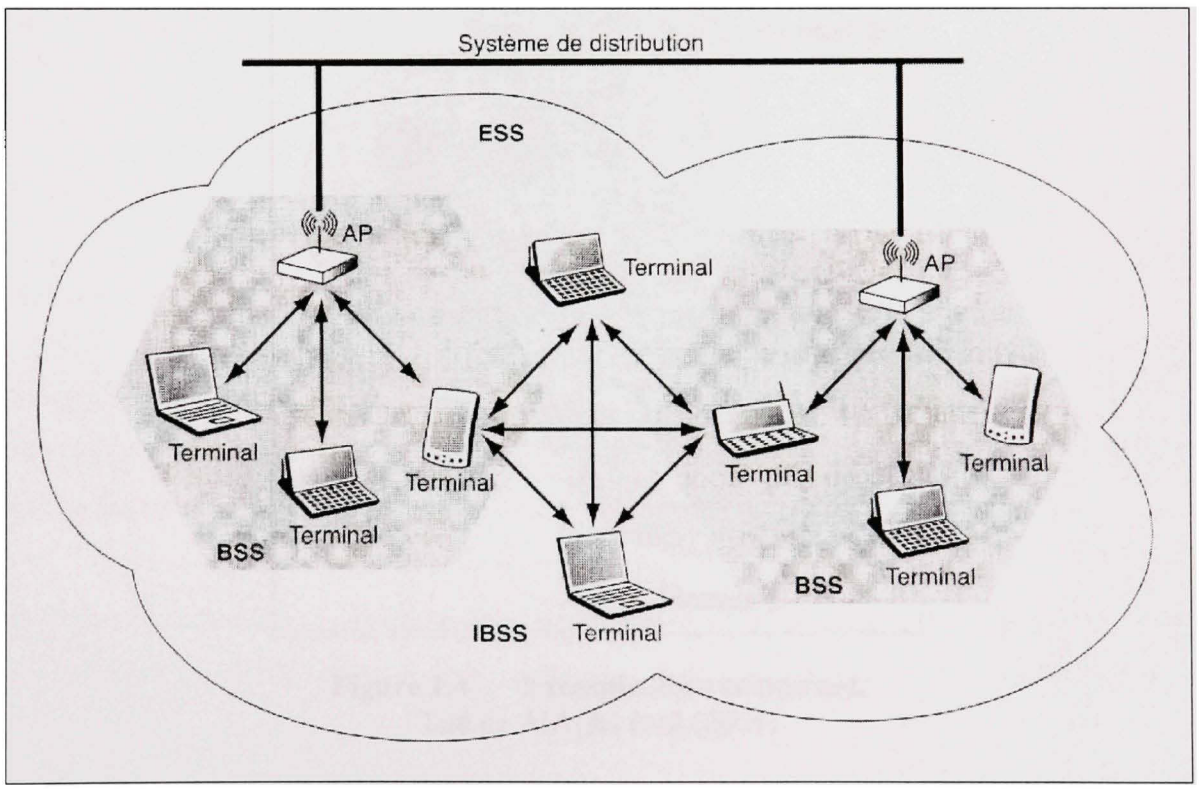


Figure 1.3 Exemple d'un ESS.
Tiré de AlAgha et al (2001)

1.2.2 Le Bluetooth

Le standard Bluetooth a été développé par Ericsson, en 1994, pour permettre la réalisation de réseau personnel de type PAN (*Personal Area Network*).

L'engouement du Bluetooth, conçu pour permettre la communication à faible ou moyen débit entre différents équipements, permit de réunir plusieurs grands joueurs du domaine de télécommunication[2] en un groupe de travail Bluetooth SIG (*Bluetooth Special Internet Group*) pour poursuivre le développement. La première publication du groupe de la spécification de Bluetooth version 1 été disponible en 1999.

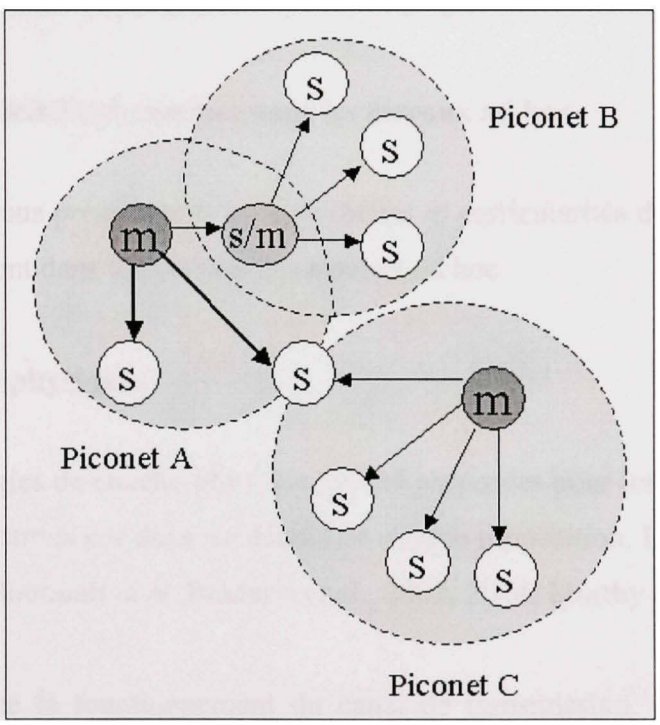


Figure 1.4 Exemple d'un scatternet.
Tiré de AlAgha et al.(2001)

[2] Ericsson, IBM, Intel, Nokia, Toshiba

Les équipements dans les réseaux Bluetooth sont principalement formé d'équipements esclaves (*slave*) et équipements maitres (*master*). Un 'Piconet' est constitué d'un maitre et un maximum de sept esclaves au tour de lui. La communication dans le piconet est gérée par le maitre qui se charge de la répartition des fréquences et des temps de diffusion. Il peut servir aussi de relais pour le trafic entre deux nœuds esclaves qui n'ont pas de lien direct. La Figure 1.4 illustre un regroupement de piconet appelés 'scatternet', dans ce cas un nœud peut appartenir à deux piconets. Par contre, un nœud ne peut pas être un maitre de deux piconets, mais un maitre dans un piconet et un esclave dans le piconet voisin.

Une description plus détaillée est disponible dans (AlAgha et al., 2001; Tanenbaum, 2003).

1.3 Les spécificités des couches dans les réseaux ad hoc

Dans cette section, nous présenterons les spécificités et particularités des couches qui ont un comportement différent dans le contexte des réseaux ad hoc.

1.3.1 La couche physique

Différentes technologies de couche physique ont été proposées pour les réseaux ad hoc. Pour cette raison nous n'entrons pas dans les détails de chaque proposition. Le lecteur peut trouver plus de détail dans (Boulmalf et al.,Bradaric et al., 2003; 2004; Murthy et al., 2004).

La Figure 1.5 illustre le fonctionnement du canal de transmission. Le codage de source correspond à la numérisation et la compression. Le codage de canal compte le codage, le transcodage, le cryptage et le brouillage.

Le canal de propagation est souvent modélisé par le schéma de la Figure 1.6. Le bruit peut être externe ou interne.

Ça peut être des perturbations électromagnétiques, bruit atmosphérique, bruit cosmique, bruits thermiques ou de quantification. Une présentation plus détaillée de ces éléments peut être consultée dans (CNAM). Les distorsions sont principalement dues à des non-linéarités d'amplification, à l'intermodulation entre signaux et cocanal ainsi qu'aux effets de la propagation (atténuations grande et petite échelle). La puissance du signal reçu, le rapport signal sur bruit (*Signal to Noise Ratio*, SNR) et le taux d'erreur binaire (*Bit Error Rate*, BER) sont souvent considérés comme étant de bons indicateurs de la qualité d'une connexion. Le choix de la modulation et le codage du canal ont une influence considérable sur le débit admissible pour un niveau de bruit donné, comme le montre le Tableau 1.2, qui illustre le débit théorique et le taux de codage pour les modulations les plus répandues.

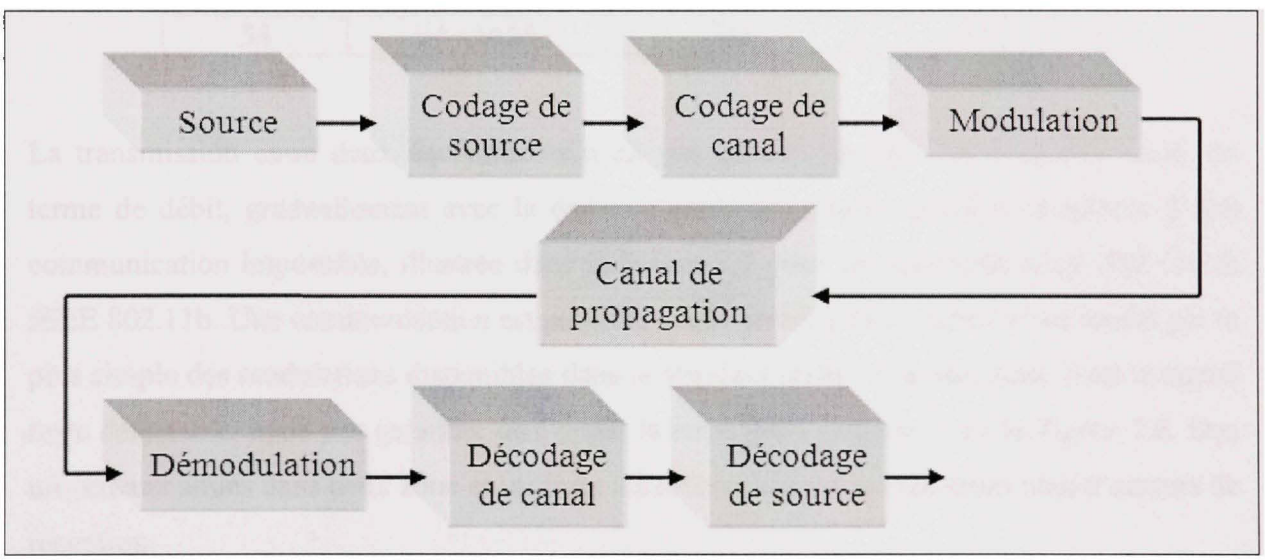


Figure 1.5 Modèle de canal de transmission.

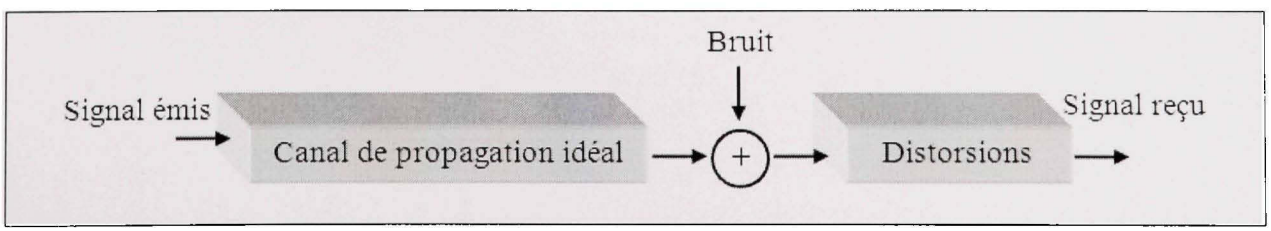


Figure 1.6 Modèle de canal de propagation.

Tableau 1.2
Débit théorique et taux de codage pour
différentes modulations d'un système IEEE 802.11
Tiré de Weiss et al (2003)

Data rate (Mbit/s)	Modulation	Coding rate (R)	Data Bits per Symbol
6	BPSK	1/2	24
9	BPSK	3/4	36
12	QPSK	1/2	48
18	QPSK	3/4	72
24	16-QAM	1/2	96
36	16-QAM	3/4	144
48	64-QAM	2/3	192
54	64-QAM	3/4	216

La transmission entre deux équipements n'est pas binaire (*on/off*). En effet elle varie, en terme de débit, graduellement avec la distance entre une communication excellente à une communication impossible, illustrée dans la Figure 1.**7** pour les standards IEEE 802.11a et IEEE 802.11b. Une communication est possible si elle arrive à être supportée au moins par la plus simple des modulations disponibles dans le standard utilisé. Dépassé cette zone le signal reste détectable, mais pas garantie, on l'appel la zone grise illustrée dans la Figure 1.8. Des utilisateurs situés dans cette zone et utilisant les mêmes canaux entraineront plus d'erreurs de réception.

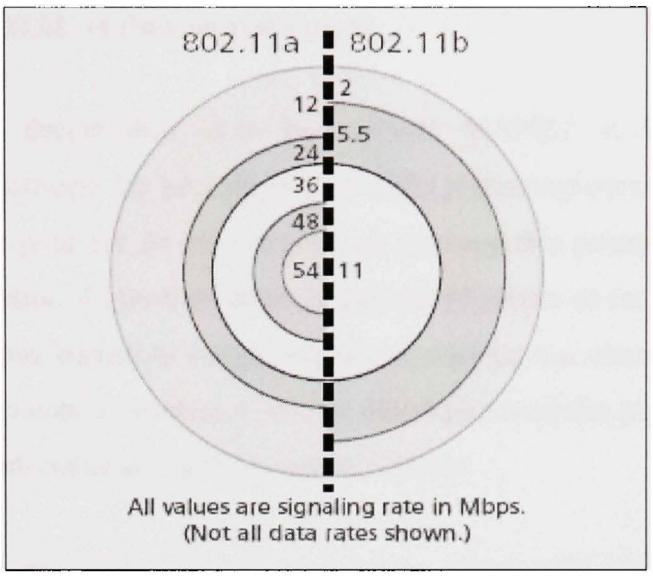


Figure 1.7 Variation du débit avec la distance.
Tiré de Proxim (2003)

Dans notre approche nous ne considérons pas les caractéristiques de la couche physique. Nos méthodes fonctionnent en considérant que l'atténuation du signal n'est l'effet que de la distance entre l'émetteur et le récepteur. Des technologies existent permettant d'estimer le bruit et d'en compenser les effets.

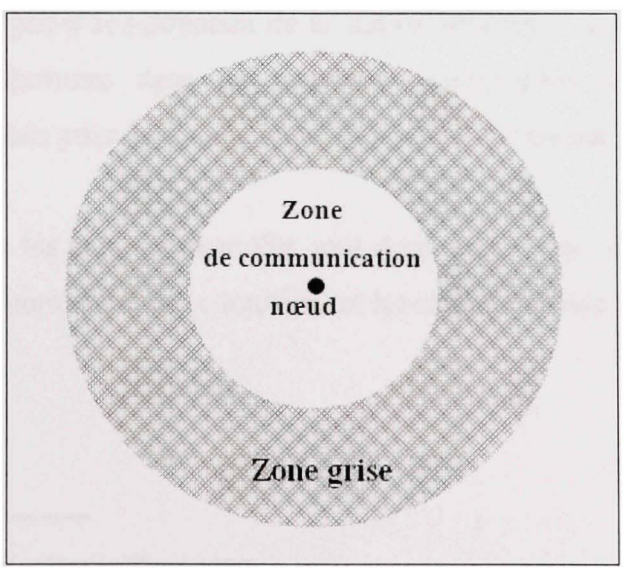


Figure 1.8 Zone de communication et zone grise.

1.3.2 La couche MAC et l'ordonnancement

L'accès au médium décentralisé dans les réseaux MANET et la problématique de l'ordonnancement constituent les plus importants défis technologiques. C'est dans la couche MAC qu'une solution pour ces problématiques est envisageable puisque cette couche est la première qui fait fonction d'interface entre la couche physique et les couches supérieures. Dans cette section, nous survolons les principaux problèmes qui concernent les réseaux ad hoc et présentons les points à considérer lors du développement des protocoles de la couche MAC ainsi que les contraintes auxquelles ils sont exposés.

Dans un réseau sans fil, l'utilisation du mécanisme CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) ne permet pas la détection de collision lors d'une atténuation importante du signal avec la distance. Le mécanisme le plus répondu surtout, avec le 802.11, est l'évitement de collision basé sur le CSMA/CA. Avec ce mécanisme, une station évite les collisions en s'assurant que le canal est libre avant de commencer son émission. Si le canal est libre, la station attend un intervalle de temps aléatoire avant de commencer la transmission. Sur réception d'une communication réussie, un nœud envoie un acquittement.

Si l'émetteur ne reçoit pas d'acquittement de la station réceptrice, il peut conclure qu'il y a eu collision. Nous décrivons dans les prochains paragraphes le fonctionnement des protocoles le plus répondu pour la couche MAC à savoir le protocole MACA[3], MACAW[4] et FAMA[5].

Les stations cachées et les stations exposées sont deux problèmes, respectivement illustrés sur la Figure 1.9 et la Figure 1.10, qui caractérisent les réseaux ad hoc.

---

[3] *Medium Access Collision Avoidance* (Karn, 1990)
[4] *Multiple Access Collision Avoidance protocol for Wireless LANs* (Bharghavan et al., 1994)
[5] *Floor Acquisition Multiple Access* (Garcia-Luna-Aceves et al., 1999)

Dans certains cas et suivant le protocole utilisé, les problèmes des stations cachées et stations exposées peuvent générer des situations de faux blocage ou des situations d'impasse temporaire, respectivement illustrée sur la Figure 1.12 et la Figure 1.13.

Sur la Figure 1.9, la station B est à portée des deux stations, mais, A et C ne peuvent pas se voir, car elles sont hors de portée. Lorsque A émet des données pour la station B, la station C peut très bien essayer de faire la même chose. En effet, lorsqu'elle écoute le support elle n'entend rien, puisque la station est bien hors de sa portée. Ainsi, croyant le support libre, elle va émettre et brouiller la réception de la station B.

Sur la Figure 1.10, C est une station émettrice exposée et D est une station réceptrice exposée. Les transmissions de B à A d'une part et de C à D d'autre part, n'entraîneraient aucune collision. Pour autant, C voyant que B est en transmission va choisir de ne pas émettre vers D. la station C ne peut pas savoir que sa transmission vers D ne générera pas de collision.

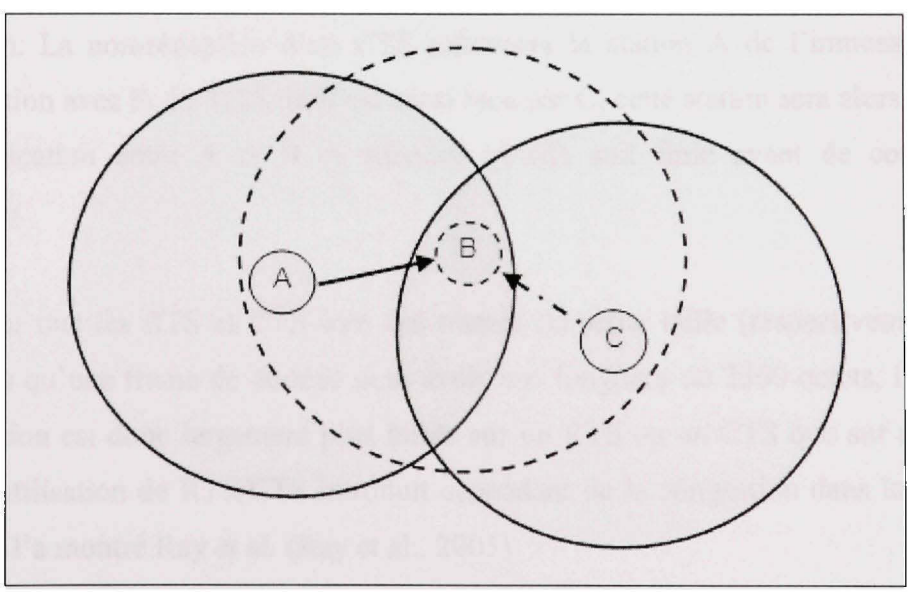


Figure 1.9 Problème des stations cachées.

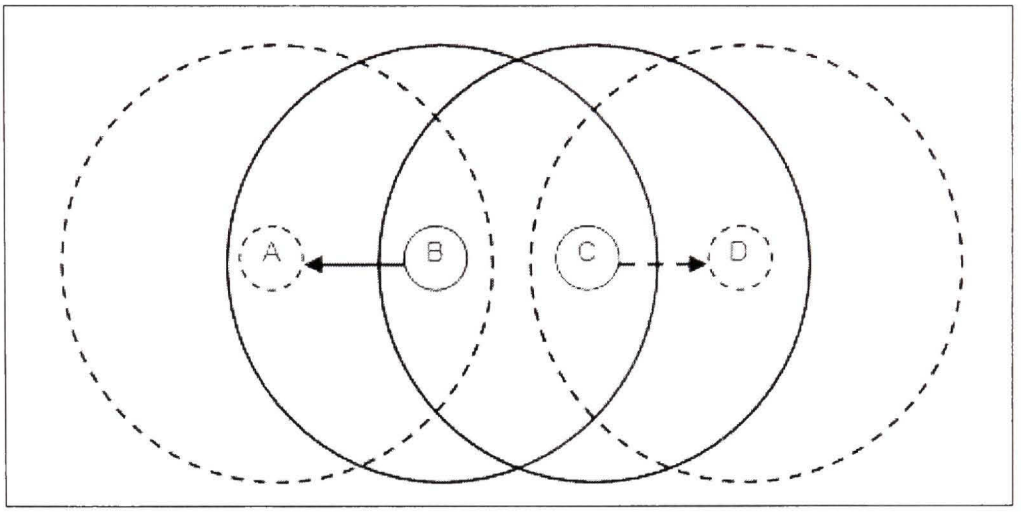


Figure 1.10 Problème des stations exposées.

La méthode la plus répandue pour résoudre le problème des stations cachées, utilisée notamment dans le 802.11, est l'utilisation des RTS/CTS (*Request to Send/Clear To Send*), illustrée sur la Figure 1.11. Dans la configuration présentée, le nœud A envoie un RTS au nœud B lui demandant la permission d'émettre, si aucune transmission n'est en cours dans le voisinage de B, celui-ci répondra par un CTS à A, la réception de l'invitation A commence la transmission. La non-réception d'un CTS informera la station A de l'impossibilité d'une communication avec B. Le CTS de B est aussi reçu par C, cette station sera alors informée de la communication entre A et B et attendra qu'elle soit finie avant de commencer sa transmission.

Il est à noter que les RTS et CTS sont des trames de petite taille (respectivement 20 et 14 octets) alors qu'une trame de donnée peut avoir une longueur de 2300 octets, la probabilité d'une collision est donc largement plus faible sur un RTS ou un CTS que sur un paquet de donnée. L'utilisation de RTS/CTS introduit cependant de la congestion dans les réseaux ad hoc comme l'a montré Ray et al. (Ray et al., 2003).

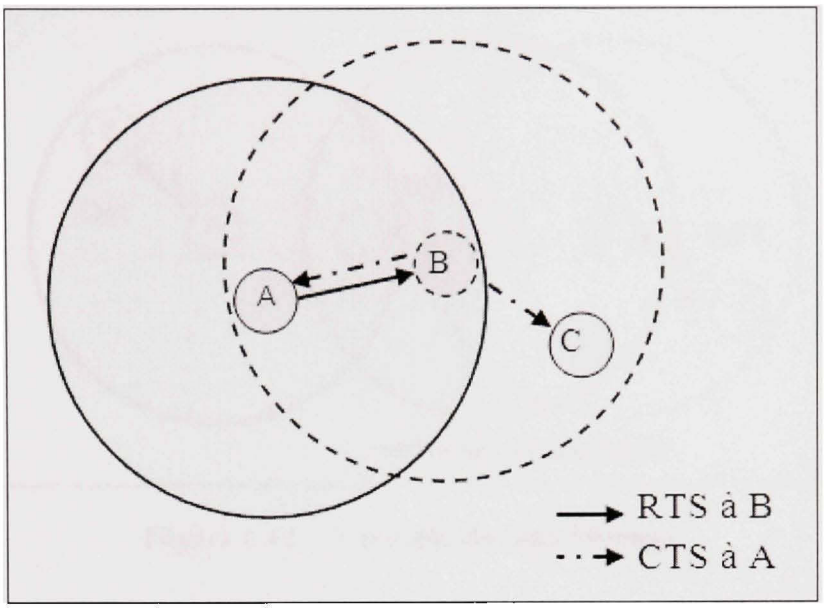


Figure 1.11 Utilisation du RTS/CTS.

La Figure 1.12 illustre une situation de faux blocage. Cette situation est le résultat de l'utilisation de RTS/CTS et du problème des stations cachées (D est caché de E) et de celui des stations exposées (F est émetteur exposé et E est un récepteur exposé de C). La transmission de A à B empêche D de transmettre un CTS à C et l'envoi du RTS de C empêche E d'envoyer un CTS à F puisqu'il ne sait pas si D a envoyé un CTS à C. Cette situation de blocage ne durera pas longtemps, mais entraînera une sous utilisation du réseau et générer une congestion momentanée.

La situation de l'impasse temporaire, qui illustre la Figure 1.13, survient lorsque les stations cachées et les stations exposées entraînent momentanément une boucle de blocage. La transmission (1) empêche E d'envoyer un CTS à D. La transmission (2) empêche G d'envoyer un CTS à F. La transmission (3) empêche C d'envoyer un CTS à B.
La situation se débloquera après avoir engendré un ou plusieurs retards. La probabilité que telles situations surviennent augmente avec le mouvement des nœuds et la densité du réseau.

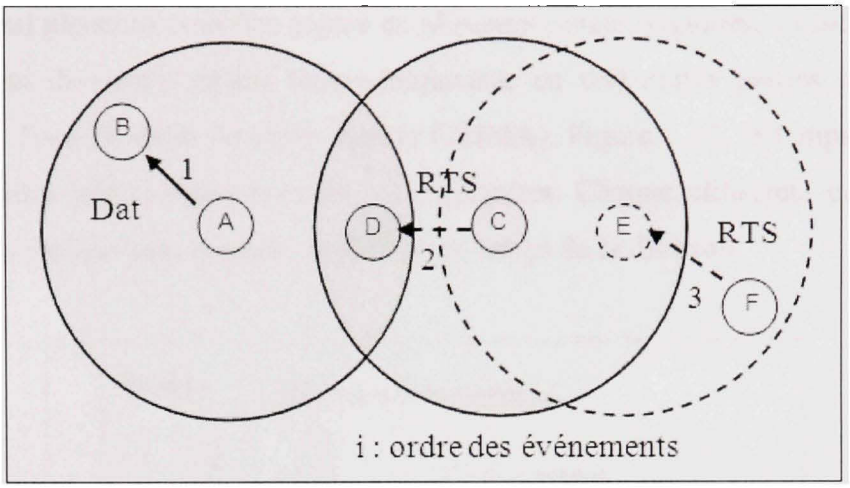


Figure 1.12 Exemple de faux blocage.

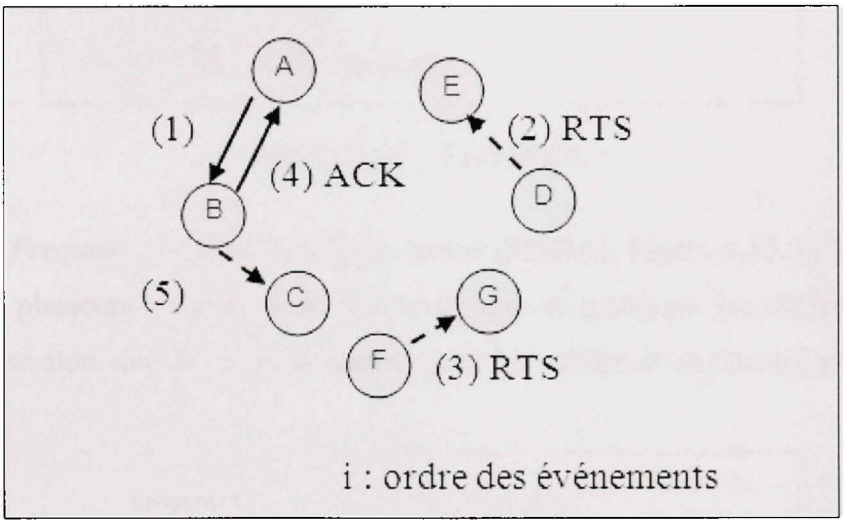


Figure 1.13 Exemple d'impasse temporaire.

Les cas précédents ne sont que des exemples de ces différents types de problèmes, de nombreuses autres situations semblables auraient pu être utilisées pour l'illustration.

Les précédents problèmes concernent le cas d'un seul canal physique disponible pour tous les nœuds. Dans les réseaux sans fil modernes, le canal physique, qui présente la bande passante totale disponible, est séparé en différents canaux logiques, qui sont virtuellement créés en découpant, dans le temps, la bande passante en différentes parties indépendantes.

En effet, le canal physique peut être séparé en plusieurs canaux logiques, à l'aide de plusieurs mécanismes qui divisent l'espace temps-fréquences en différentes parties indépendantes. Dans le mode *Time Division Multiple Access* (TDMA), Figure 1.14, le temps est divisé en unités temporelles (*slots*) réparties entre les utilisateurs. Chaque utilisateur occupe donc la totalité de la bande passante pendant la période de temps de la division.

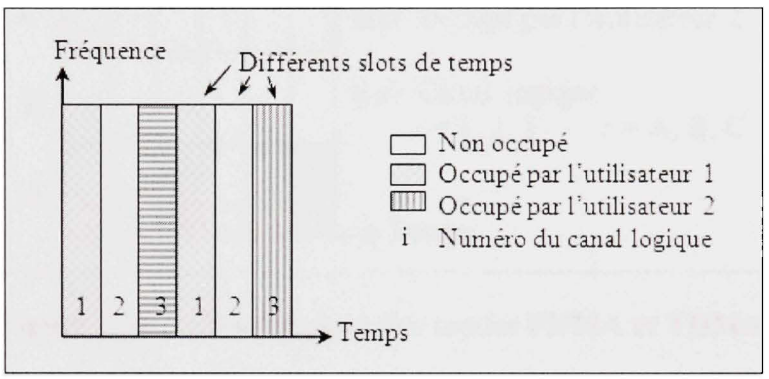


Figure 1.14 Le TDMA.

Dans le mode *Frequency Division Multiple Access* (FDMA), Figure 1.15, la bande passante est divisée en plusieurs intervalles de fréquence que se partagent les utilisateurs. Chaque utilisateur utilise alors une de ces sous bandes durant la totalité de sa transmission.

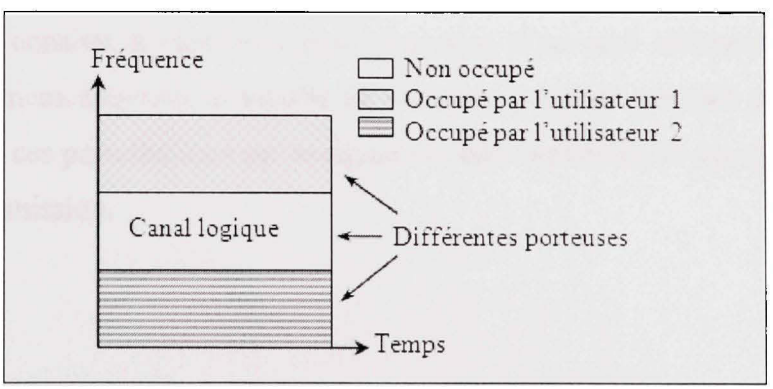


Figure 1.15 Le FDMA.

Sur la Figure 1.16, les modes FDMA et TDMA ont été combinés, ce qui offre une plus grande souplesse d'utilisation. Un *slot* temps-fréquence est alors alloué à chaque utilisateur.

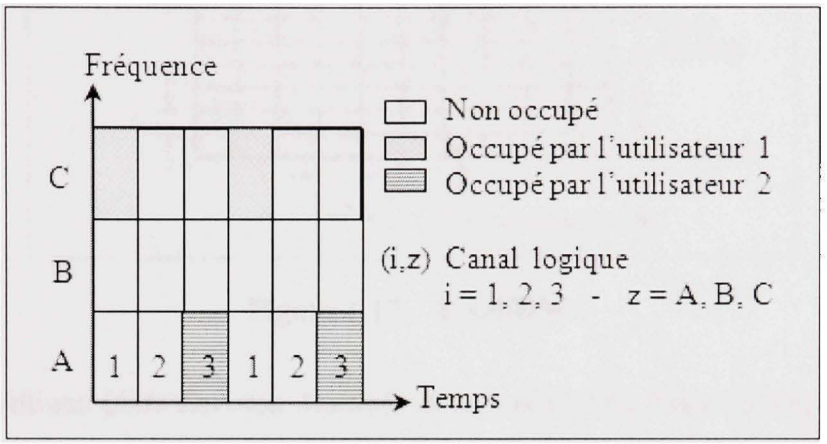


Figure 1.16 Combinaison des modes FDMA et TDMA.

À l'aide de combinaison de méthode, l'optimisation de l'utilisation de la bande passante disponible est presque arrivée à sa limite. Il y a tout de même des problèmes qui surviennent comme les perturbations et interférences qui sont généralement concentrées sur certaines bandes étroites de fréquences. A partir de ce constat, plusieurs approches ont été proposées pour diminuer l'effet des perturbations sur le signal.

Le *Orthogonal Frequency Division Multiplexing* (OFDM), Figure 1.17, est une des propositions qui consiste à répartir une transmission d'un seul utilisateur sur différentes bandes de fréquences couvrant la totalité de la bande passante pendant un certain laps de temps. L'effet de ces perturbations sur le signal est ainsi amoindri, ce qui diminue le nombre d'erreurs de transmission.

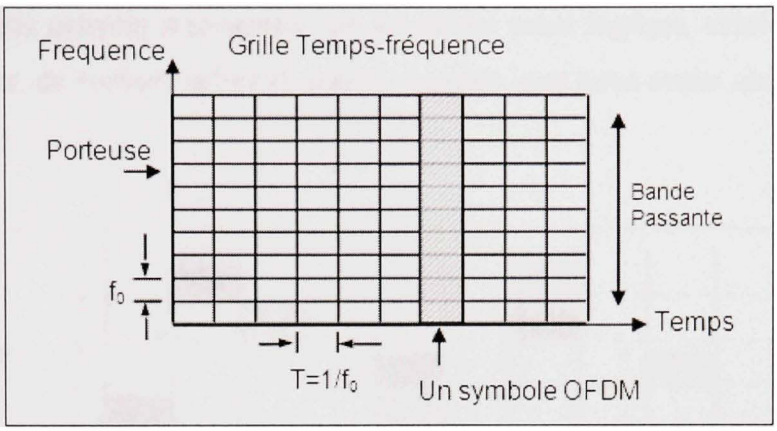


Figure 1.17 L'OFDM.

Dans les propositions *Code Division Multiple Access* (CDMA), Figure 1.18, la transmission du trafic est sur la totalité de la bande passante, mais l'utilisateur encode son trafic avant l'envoi. Si les codes utilisés par les différents utilisateurs sont orthogonaux, les différents trafics ne seront pas affectés par le trafic des autres utilisateurs.

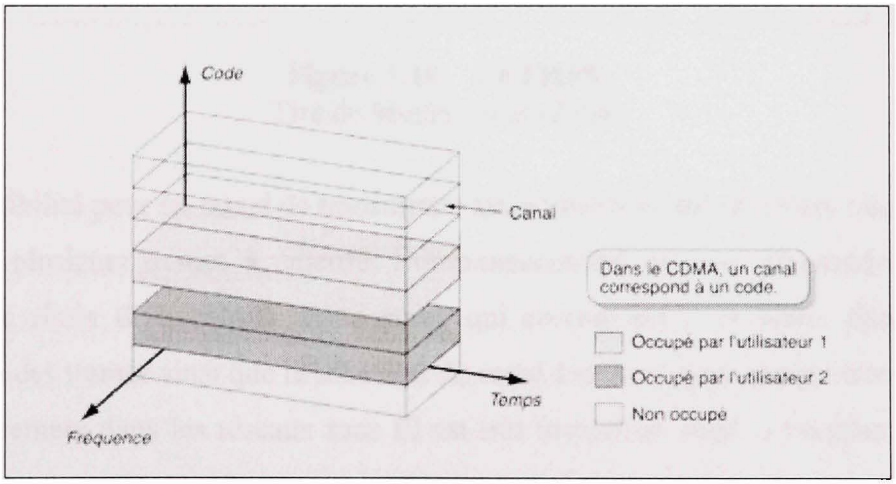


Figure 1.18 Le CDMA.
Tiré de AlAgha et al.(2001)

Le mode *Frequency Hopping Spread Spectrum* (FHSS), Figure 1.19, la transmission entre deux utilisateurs change de bande de fréquence à l'autre suivant une suite pseudo aléatoire connue de l'émetteur et du récepteur.

Si plusieurs nœuds peuvent transmettre sur un même canal logique, celui-ci présentera les mêmes problèmes, de station cachée et station exposée, que nous avons abordés au début de cette section.

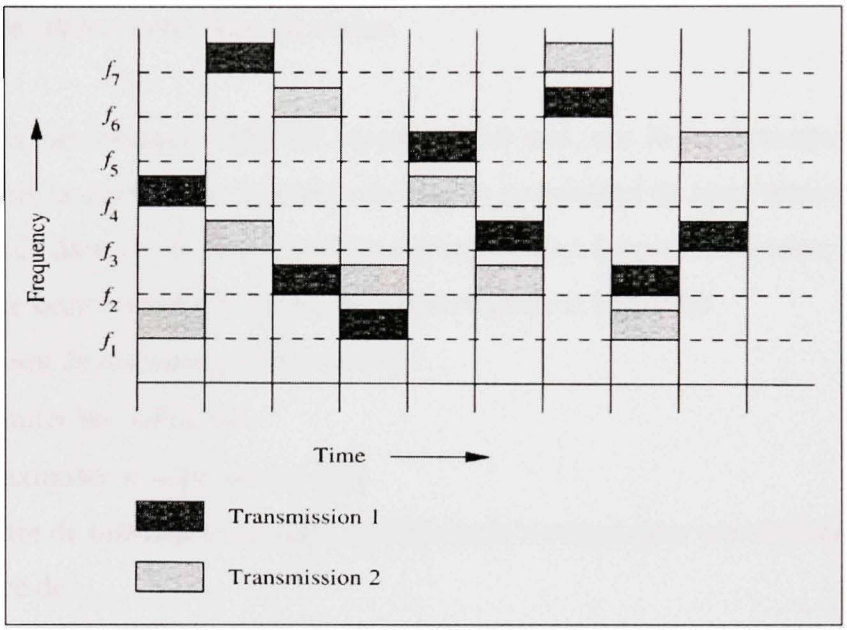


Figure 1.19 Le FHSS.
Tiré de Murthy et al.(2004)

Avec la possibilité pour un nœud de transmettre simultanément sur plusieurs canaux logiques et en ayant plusieurs trames à émettre, l'ordonnancement est une nécessitée. Ce dernier représente le choix d'un couple trame-canal, qui correspond à un choix dans l'ordre de transmission des trames ainsi que la sélection du canal à utiliser pour chaque transmission.
L'ordonnancement dans les réseaux sans fil est très important, mais il est plus important et plus complexe à mettre en place pour les réseaux ad hoc la décentralisation et la variation constante de connectivité entre les nœuds qui caractérise ces types de réseaux.
En ayant tous ces problèmes à résoudre dans les réseaux ad hoc, une approche innovatrice permettant plus de liberté de crée des mécanismes est de mesure.

Cette approche peut résider dans le *Cross Layer* qui permet aux nœuds dans le réseau d'être plus intelligents en ayant les informations de la couche physique au niveau de la couche MAC. Ainsi, une utilisation judicieuse de cette information permettra d'améliorer l'ordonnancement et diminuer les collisions en prenant au niveau de chaque nœud des décisions plus en phase avec l'état du réseau.

La performance des réseaux MANET repose, avant tout, sur la performance de la couche MAC qui permet la distribution équitable de l'accès au médium de transmission.
La couche MAC, dans le cas des MANETs, doit considérer les points suivants :

- Système décentralisé (problème de station cachée et exposée)
- Utilisation de ressources synchronisées:
  - Limiter les collisions.
  - Maximiser le débit sur un lien.
- Permettre de mesurer de la disponibilité des ressources pour une utilisation équitable en terme de :
  - Bande passante.
  - Temps d'accès.
  - Qualité de service.
- Contrôle de la puissance d'émission.
  - Limiter la consommation.
  - Diminuer les interférences inter-nœud.

En tenant compte des considérations générales précédemment citées, des contraintes en découlent pour l'élaboration d'un protocole de la couche MAC. Plusieurs protocoles ont été conçus en essayant de répondre à un nombre maximum d'entre elles. Nous pouvant résumer ces contraintes comme suit :

- Fonctionnement distribué et possibilité de mise à l'échelle.
- Possibilité d'offrir la QoS nécessaire.

- Temps d'accès raisonnable.
- Optimisation de l'utilisation de la Bande passante.
- Trafic de contrôle minimum.
- Impact limité des stations cachées et exposées.
- Mécanismes de contrôle d'énergie.
- Taux de transmission adaptable.
- Mécanisme de synchronisation pour la réservation des canaux logiques.

Une trentaine de protocoles de la couche MAC, pour les réseaux ad hoc, ont été analysé et données dans (Murthy et al., 2004; Wu, 2006).

1.3.3 La couche réseau

Un réseau sans fil ad hoc est constitué de plusieurs nœuds mobiles qui peuvent avoir une connexion sans fil entre eux (direct ou indirect). La topologie d'un tel réseau subit souvent un changement aléatoire et fréquent. Les protocoles de routages permettent de trouver un chemin, en minimisant certaines métriques, pour le transfert des données d'une source à une destination à travers les autres nœuds du réseau. Ces métriques sont collectées à partir de l'état du réseau suivant un algorithme pour permettre aux protocoles de routage de donner une décision optimale de transfert des paquets. Les protocoles de routages du domaine filaire ne peuvent pas être appliqués directement sur les réseaux sans fil ad hoc à cause des différences fondamentales entre les deux types de réseaux (topologie dynamique, absence d'infrastructure centralisée, contrainte énergétique…). Dans les prochaines sections, les contraintes qui interviennent dans la conception d'un protocole de routage seront étalées, par la suite nous détaillerons les différentes classes de protocoles et leurs caractéristiques.

1.3.3.1 Les contraintes du routage pour les réseaux ad hoc

La mobilité dans les réseaux sans fil ad hoc est une vraie contrainte qui affecte les connexions entre les nœuds soit par le déplacement d'un ou plusieurs nœuds intermédiaires soit par le déplacement d'un nœud final. Ce qu'il en résulte plusieurs coupures par transfert. Ce comportement affecte donc le routage par conséquent les caractéristiques des protocoles de routage des MANETs.

Ainsi, tout protocole de routage conçu pour ce type de réseau doit répondre aux exigences suivantes :

- Totalement distribué donc plus tolèrent à la rupture d'un nœud, peut être mis à l'échelle sans une augmentation majeure du trafic de contrôle.
- Supporter le changement fréquent de la topologie causé par la mobilité des nœuds.
- Trouver et maintenir une route doit impliquer un nombre minime de nœuds (diminuer l'inondation de réseau). Un nœud doit avoir accès à une route dans un temps raisonnable.
- Le nombre de collisions doit être maintenu au minimum. Les transmissions doivent être fiables pour réduire la perte de paquet.
- Converger à une route optimale quand la topologie devient stable.
- Utiliser efficacement les rares ressources disponibles comme la bande passante, la puissance de calcul, la mémoire et la vie de la batterie.
- Doit être capable de fournir la QoS si demandée par l'application.

Plusieurs protocoles de routage pour les MANETs ont été élaborés. Sans pour autant répondre à toutes les contraintes citées ci-dessus. Ceci dit que dans certaines configurations de réseau un protocole peut répondre parfaitement aux exigences circonstancielles et donc être fiable.

1.3.3.2 Les classes des protocoles de routages

Une classification des protocoles de routage ad hoc peut être basée sur plusieurs types et critères. Des protocoles peuvent se trouver dans plusieurs classes. Le découpage le plus répondu est fait sur quatre catégories sur la base du mécanisme de routage, l'utilisation d'information temporelle, topologique et l'utilisation de ressource :

- Mécanisme de routage
  - Routage proactif (*proactive* ou *Table driven*) : Ce type de protocole tente de maintenir une table de routage contenant tous les nœuds du réseau au niveau de chaque nœud. Il y a un échange périodique de table dans tout le réseau.
    Un nœud désirant envoyer un paquet vers une destination exécute un algorithme sur la table qu'il détient pour trouver le chemin à coût moindre. Une présentation du fonctionnement et une comparaison des protocoles DSDV (*Destination Sequanced Distance-Vector*), WRP (*Wireless Routing Protocol*) et CGSR (*Cluster-head Gateway Switch Routing*) sont jointes dans l'APPENDICE A.
  - Routage réactif (*reactive* ou *On-demand*) : regroupent les protocoles qui ne permettent pas de maintenir la topologie de tout le réseau. Mais les nœuds obtiennent le chemin quand ils le demandent en établissant une connexion avec leurs voisins. Donc pas d'échange périodique de tables entre les nœuds. Une présentation du fonctionnement et une comparaison des protocoles DSR (*Dynamique Source Routing*), AODV (*Ad hoc On-demand Distance Vector*) et TORA (*Tomporally Ordered Routing Algorithm*) sont jointes dans l'APPENDICE B.
  - Routage Hybrides (*hybrid*) : combine le meilleur des deux catégories précédentes. De sorte qu'il y a recourt à l'échange de table dans un milieu géographiquement restreint, mais pour des destinations au-delà de cette zone l'approche sur demande est utilisée.

Une présentation du fonctionnement et une comparaison des protocoles CEDAR (*Core Extraction Distributed Ad-hoc Routing*) et ZRP (*Zone Routing Protocol*) est jointe dans l'APPENDICE C.

- L'information temporelle
  - Actuelle et/ou passée : comme le statut du lien passé ou le statut d'un lien à un moment donné.
  - Future : aux fins de routage en faisant une approximation sur le temps de vie d'un lien sans fil, temps de vie du nœud, la localisation et la disponibilité de lien.

  Une présentation du fonctionnement et une comparaison des protocoles PLBR (*Preferred link-based routing*) et OLSR (*Optimized link state routing*) est jointe dans l'APPENDICE D.
- La topologie
  - Routage à topologie plate (*flat topology routing*) : pour lequel tous les nœuds sont égaux et un plan d'adressage unique et global est utilisé.
  - Routage à topologie hiérarchique (*hierarchical topology routing*) : Ces types de protocoles instaurent une hiérarchie logique d'adressage qui peut être basée sur l'information géographique ou sur le nombre de sauts.

  Une présentation du fonctionnement et une comparaison des protocoles HSR (*Hierarchical State. Routing*) et FSR (*Fisheye State Routing*) est jointe dans l'APPENDICE E.
- l'utilisation de ressource
  - Routage qui minimise la consommation (*power-aware routing*) : essayent d'allonger la survie du réseau à son maximum.
  - Information géographique (*geographical information assisted routing*) : la décision de routage est prise pour augmenter la performance de routage et réduire l'ajout de l'information dans l'entête (*Overhead*).

On peut remarquer que cette classification n'est pas mutuellement exclusive. Puisqu'un protocole peut appartenir à plusieurs de ces catégories.
Par exemple, le protocole DSR est un protocole réactif qui peut inclure l'information temporelle de statut des liens pour estimer la durée de vie d'un lien.

1.4 Différents concepts des réseaux ad hoc

Dans les sections qui suivent, nous aborderons les architectures de grand intérêt dans le cas des réseaux ad hoc. Ces architectures permettent de donner des caractéristiques supplémentaires aux réseaux ad hoc qui facilitent la gestion et la communication inter nœuds.

1.4.1 La notion de cluster et les backbones

La notion de cluster consiste à répartir les nœuds dans un réseau en plusieurs groupes (appelés *clusters*) et chacun d'entre eux a un nœud privilégié (un *clusterhead*).
Une présentation d'une telle architecture est illustrée sur la Figure 1.20. Un nœud dans un réseau ad hoc constitué par des *clusters* peut être dans l'une des trois états. Un nœud régulier (*clustermember*) attaché à un *clusterhead*. En se trouvant à la jonction de deux *clusters* il sera une passerelle (*clustergateways*). Le troisième état d'un nœud dans un tel type d'architecture est un dominant d'un *cluster* (le *clusterhead*). Ce dernier se charge du fonctionnement du cluster et ayant des fonctions et des façons de se faire élire variante à travers la littérature.

Trois éléments sont importants lorsqu'il est question de *clusters* :

- Le mode d'élection du *clusterhead* qui est effectué par un algorithme d'élection et qui dépend de certaines métriques, tel que le niveau de batterie, la position, la vitesse, le nombre de ses connexions.
- Les responsabilités et le fonctionnement du clusterhead. Les responsabilités de ce nœud très particulier peuvent être très limitées (simple détermination du cluster) ou très étendues (centralisation des informations sur le cluster).

Dans certains cas, le trafic de tout nœud à destination d'un autre cluster que le sien doit transiter par le clusterhead.

- L'éloignement possible, en nombre de sauts, d'un clustermember de son clusterhead. L'étendu d'un cluster dépend du nombre admis de nœuds intermédiaires pouvant relayer le trafic entre un clusterhead et un des ses clustermembers.

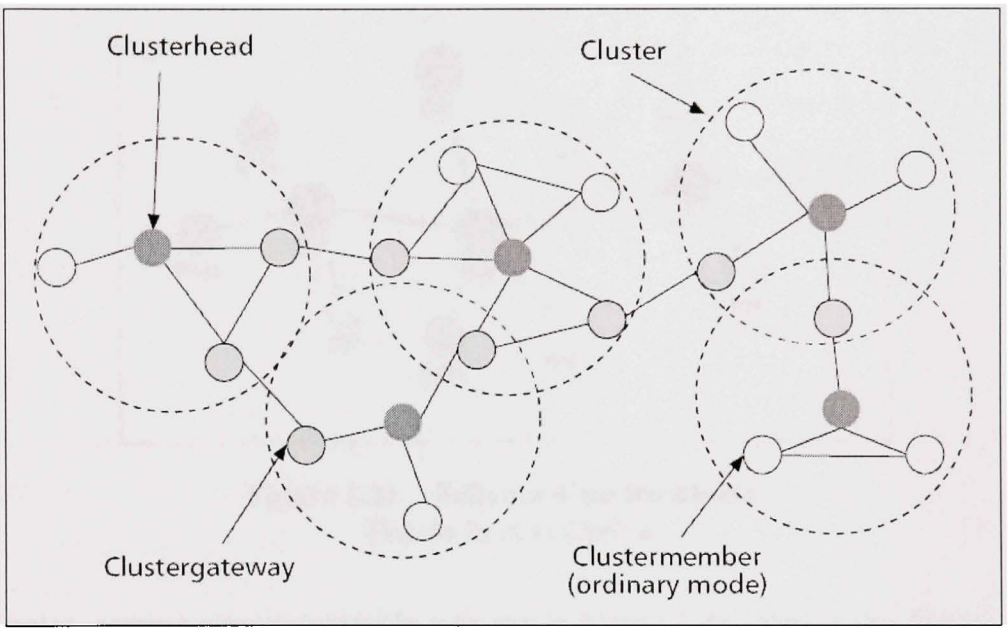


Figure 1.20 Structure d'un cluster.
Tiré de Yu et al.(2005)

La maintenance de l'architecture dans le cas des *clusters* est très importante. C'est à travers la maintenance que le suivie continu des *clusterheads* et leurs élections de nouveau pour un *cluster* ou pour remplacer un autre est fait. Un *clustermembers* peut fréquemment changer de *cluster* suivant sa mobilité et le maintien des connexions entre les voisins.

Dans ce contexte, la possibilité de prédire la qualité des liens entre les nœuds à travers la prédiction de temps de vie des liens peut être un élément qui améliore et simplifie significativement le processus de maintenance.

Un concept emprunté de l'architecture des réseaux filaires est le concept de dorsale (*backbone*). Le mouvement des nœuds et la bande passante pour les sans fil introduisent une complication pour maintenir une dorsale dans un réseau ad hoc.

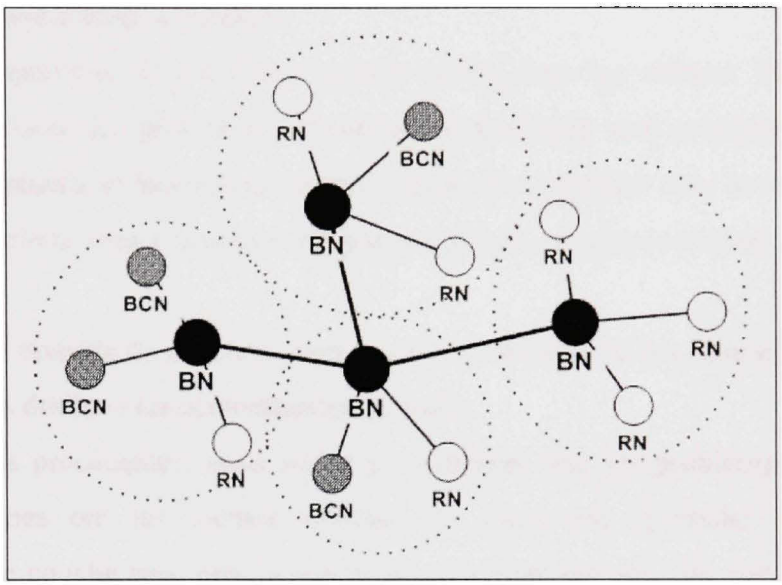


Figure 1.21 Schéma d'un backbone.
Tiré de Ju et al.(2005)

Il est à noter, comme nous pouvons le voir sur la Figure 1.21, que les *backbones* utilisent souvent la notion de *clusters* pour leur construction. Les RN sont des nœuds réguliers (*Regular Nodes*) tandis que les BCN sont des nœuds pouvant appartenir à la dorsale (*Backbone Capable Nodes*). Certains des BCN sont élus pour construire la dorsale, ils sont alors nommés des BN (*Backbone Nodes*). La prédiction de temps de vie de lien présente logiquement les mêmes avantages qu'avec l'utilisation de *cluster*.

1.4.2 Le cross-layer

Le modèle OSI[6] en sept couches, proposé par l'ISO[7], constitue l'architecture de communication classique qui répartit les besoins et services pour l'établissement d'une communication en différentes couches.
Bien que cette approche ait été d'une grande utilité dans les réseaux filaires et sans fil classiques en divisant les problèmes rencontrés en plusieurs sous-problèmes et permettant une évolution graduelle et facilitée des technologies, elle engendre dans le cas des réseaux ad hoc des complications liées à la nature très particulière de ce type de réseaux.

La diminution de nombre de couches, dans le cas des réseaux ad hoc, entraînera la limitation des possibilités et diminue les performances globales.
Dans les sections précédentes, nous avons pu constater que les problèmes rencontrés aux différentes couches ont les mêmes sources. De plus, une approche ou une solution particulière à une couche peut être la source de perturbations pour les couches supérieures. Par conséquent, il apparaît clairement que l'architecture *cross-layer* peut être une grande source d'amélioration des performances.

---

[6] *Open Systems Interconnection reference model*
[7] *International Standards Organization*

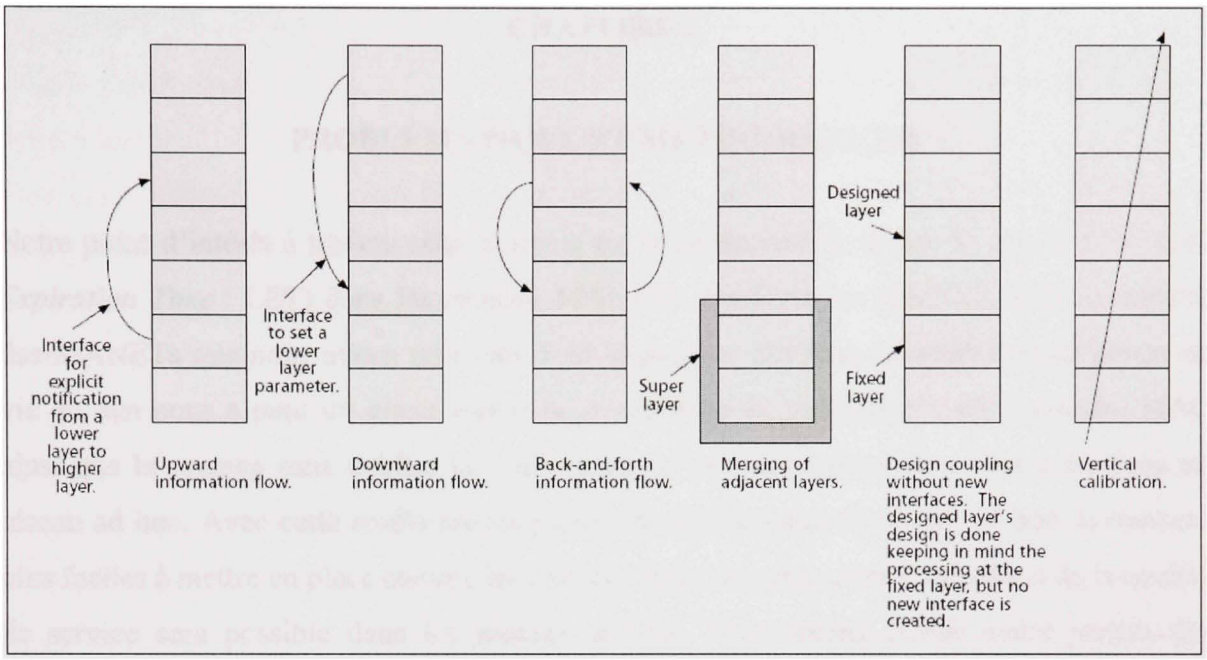


Figure 1.22 Différentes architectures cross-layer.
Tiré de Srivastava et al.(2005)

La Figure 1.22 illustre plusieurs catégories d'utilisation de cross-layer. Srivastava et al. (2005) font une synthèse de l'état de l'art et posent de manière très claire les possibilités, les contraintes et les problèmes que soulèvent les architectures *cross-layer*.

CHAPITRE 2

PROBLÉMATIQUE ET MÉTHODOLOGIE

Notre point d'intérêt à travers cette maîtrise est la prédiction de temps de vie de lien (*Link Expiration Time* : LET) dans les réseaux MANETs. Basé sur les spécificités et contraintes des MANETs que nous avons abordées dans le premier chapitre, la prédiction de temps de vie de lien nous a paru un grand espoir pour améliorer la performance de la couche MAC ainsi que le routage sans oublier la construction et la maintenance de connexions dans un réseau ad hoc. Avec cette amélioration, plusieurs architectures de réseau ad hoc deviennent plus faciles à mettre en place comme les *clusters* et les dorsales ainsi l'utilisation de la qualité de service sera possible dans les réseaux ad hoc. Nous avons étendu notre intérêt des MANETs du cas d'utilisateur se déplaçant à pied jusqu'aux utilisateurs qui peuvent être à bord d'une moto ou une voiture et aussi nous avons considéré que l'environnement de test est fermé et sans obstacle.
Les sites de conférence, les colloques, les situations de réunions importantes de personnes et un groupe de chars d'assaut se déplaçant à toute vitesse en sont de parfaits exemples.

La prise en compte des caractéristiques de la couche physique étant très complexe, nous avons choisi de nous restreindre à la puissance du signal reçu pour mesurer le temps de vie de lien. Contrairement aux différentes autres approches, nous ne voulons considérer aucun a priori sur le mouvement. L'idée est d'effectuer l'estimation et la prédiction de la puissance reçue directement à partir de son historique récent. Enfin, l'estimation et la prédiction se font par un algorithme, nécessitant peu de calcul et d'espace mémoire. Notre système se base sur une approche *cross-layer* dans laquelle des données de la couche physique sont utilisées par la couche MAC pour améliorer les performances de protocole de routage, d'outils des couches supérieures et du réseau plus généralement.
À partir de ces éléments, il est important de considérer les éléments qui influencent la puissance reçue.

Celle-ci est principalement affectée par la variation de la distance due au mouvement des nœuds. Les réseaux ad hoc étant peu déployés, leurs études se font principalement à travers des simulations.
Pour que l'élaboration et le test de notre implantation d'estimation et de prédiction se fassent de façon plus réaliste, nous devions donc utiliser des modèles de mouvement réalistes.

Dans un premier temps, nous avons intégré trois algorithmes d'estimation et prédiction au niveau de la couche MAC et dans un protocole de routage pour les MANETs. La publication de *Qin et al* présente deux algorithmes d'estimation et prédiction. Le premier se base sur les coordonnées des nœuds donc sur GPS (*Global Positioning System*) pour démarrer l'algorithme, alors que le second n'a besoin que de la puissance de signal reçu pour faire l'estimation de temps de vie du lien. Nous avons eu l'intuition d'ajouter un troisième algorithme qui utilise les deux algorithmes précédents pour avoir une estimation et prédiction plus conservative et vérifier si elle sera plus intéressante.

Dans un second temps, il a fallu choisir un modèle de mouvement plus réaliste pour les nœuds dans un réseau ad hoc. Il s'est avéré que le *Random Waypoint* permet de générer des trajectoires totalement aléatoires ce qui été notre but. En ayant des trajectoires de la sorte, nous testons alors notre système de prédiction dans des conditions les plus aléatoires et les plus exigeantes par conséquent les plus réalistes.

Enfin, nous avons testé les trois algorithmes implantés d'estimation et de prédiction sur plusieurs scénarios afin de mesurer des points de performance du réseau et les comparer avec la version originale du protocole.

Rappelons enfin que notre travail consiste à proposer un outil d'estimation et de prédiction du temps de vie de lien qui peut représenter la qualité de lien qui sera utilisable par des protocoles variés au niveau de la couche MAC, du routage, de la construction et la maintenance de *clusters* et de *backbones*. Cependant, nous ne décrirons pas le mécanisme permettant d'appliquer notre méthode à ces différents cas.

Le nombre très important d'approches possibles pour l'intégration de la prédiction dans ces protocoles et les problèmes qui peuvent en découler nous semblent un peu éloigné de nos travaux et sont à eux seuls des sujets de recherches.

CHAPITRE 3

PRÉSENTATION DE DSR

3.1 Introduction

Le protocole *Dynamic Source Routing* (DSR) est un protocole de routage réactif, simple et efficace conçu spécialement pour l'utilisation multi saut dans les réseaux mobiles ad hoc. DSR permet au réseau de s'auto configurer et de s'auto organiser sans la nécessité d'avoir une infrastructure ou une administration du réseau. Les nœuds dans le réseau coopèrent pour transmettre les paquets entre eux, permettant ainsi une communication sur plusieurs sauts entre des nœuds qui ne sont pas directement visibles. Puisque les nœuds dans le réseau peuvent se déplacer, joindre ou quitter le réseau et les transmissions sans fil sujettes à des interférences, toutes les routes sont déterminées et maintenues automatiquement par le protocole DSR. Puisque les nœuds intermédiaires peuvent changer à tout moment, la topologie du réseau peut rapidement changer. DSR a été conçu pour avoir le minimum d'entête possible et de réagir rapidement au changement de topologie dans le réseau. Il permet d'offrir un service réactif pour assurer la livraison de paquet tout en maintenant la connexion avec le changement de la topologie du réseau.
Dans les prochaines sections, nous abordons seulement les mécanismes nécessaires à la compréhension du protocole et que nous avons modifiés à travers notre projet.

3.2 Découverte de route dans DSR

Quand un nœud génère un paquet destiné à une destination donnée, il insère dans l'entête la totalité du chemin (*source route*) que le paquet doit suivre pour arriver à destination. Normalement, la source obtient le chemin vers la destination en cherchant dans son cache (*route cache*) parmi les routes qui sont apprises. Si aucune route vers la destination demandée n'est trouvée dans le cache, le protocole de découverte de route sera initié pour trouver automatiquement une route vers la destination recherchée.

Dans ce cas le nœud qui source est appelé '*initiator*' et le nœud recherché par la découverte de route est appelé '*target*'.

La Figure 3.1 illustre le fonctionnement de la demande de route (*route request*) à travers un réseau composé des nœuds A, B, C, D et E. Le nœud A initie la demande de route et la transmet à ses voisins, qui se trouvent dans sa couverture de transmission. Chaque demande de route est identifiée par la source, la destination et un identifiant unique (2 dans la Figure 3.1) déterminé par la source de la demande. Elle contient un champ qui permet d'enregistrer les adresses des nœuds intermédiaires visités par la copie de la demande de route. Si le nœud qui reçoit la demande est le nœud recherché, il envoie une réponse (*route reply*) vers l'initiateur de la demande en lui donnant une copie du chemin accumulé dans la demande. Quand l'initiateur reçoit la réponse, il insère la route dans son cache pour s'en servir ultérieurement à l'envoi de paquet vers cette destination.

Si un nœud reçoit la même demande de route une deuxième fois, avec le même identifiant, *target* et source, ou sa propre adresse se trouve parmi les adresses déjà enregistrées dans la liste des nœuds visités, le paquet contenant la demande sera rejetée. Sinon le nœud ajoute son adresse dans la liste des nœuds visités et diffuse la demande avec le même identifiant.

Le nœud E dans la Figure 3.1, insère dans son cache la séquence d'adresse inverse des nœuds visités et utilise cette route pour transmettre la réponse de route. Ce mécanisme admet que toutes les routes dans le réseau sont bidirectionnelles.

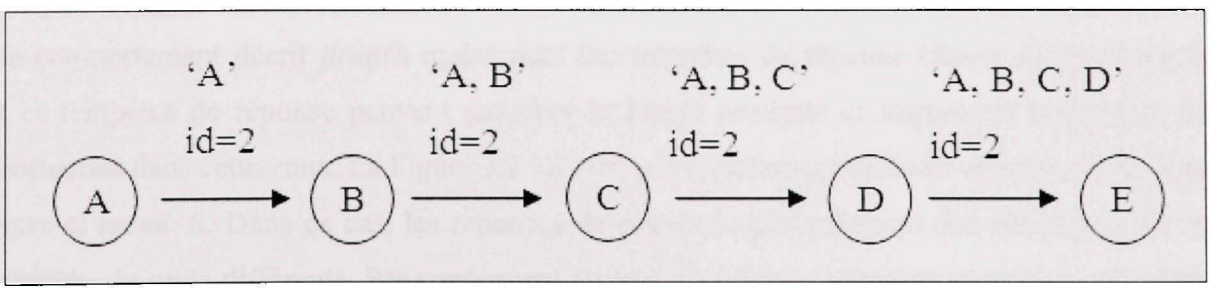


Figure 3.1 Propagation de demande de route dans DSR.

3.2.1 Caching Overheard Routing Information

Le *caching* est le mécanisme qui permet d'apprendre l'état du réseau le plus rapidement possible. Ainsi, chaque nœud dans un réseau ad hoc ajoute les chemins contenus dans les paquets (demande, réponse ou source) qu'il relai prochain saut à son cache pour les utilisés ultérieurement si nécessaire. Si le nœud arrive à capter un paquet sans qu'il soit présent dans la liste des adresses du chemin doit aussi ajouter à son cache qu'il arrive à joindre tout les nœuds cités dans le paquet. Ce mécanisme permet aussi d'éliminer rapidement les liens non fonctionnels à travers l'écoute de l'avertissement de route.

3.2.2 Répondre à la demande de route

Un nœud intermédiaire qui reçoit une demande de route cherche dans son cache un chemin possible pour la destination demandée. S'il trouve un, il concatène le chemin trouvé avec le chemin inscrit dans le paquet et analyse le chemin résultant à la recherche de boucle possible. Si une boucle est trouvée, la demande de route sera diffusée normalement, sinon une réponse de route vers la source est envoyée en suivant le chemin indiqué dans le paquet.

3.2.3 Prévention de réponse de route multiple (*storms*)

La possibilité des nœuds intermédiaires de répondre à la demande de route peut causer avec le comportement décrit jusqu'à maintenant des tempêtes de réponse (*Route Reply Storms*). Ces tempêtes de réponse peuvent gaspiller la bande passante et augmenter le nombre de collisions dans cette zone. La Figure 3.2 montre une situation possible de tempête de réponse vers el nœud A. Dans ce cas, les réponses de route ont généralement des chemins avec un nombre de sauts différents. Par conséquent au lieu d'avoir des réponses quasiment en même temps envoyées par les voisins, augmentant ainsi les risques de collision, un nœud se met en mode écoute pendant une période de temps intégrant dans son calcul le nombre de sauts présent dans le paquet de réponses (équation 3.1). Si dans cette période une route plus courte semble être utilisée, le voisin annule l'envoi de sa réponse.

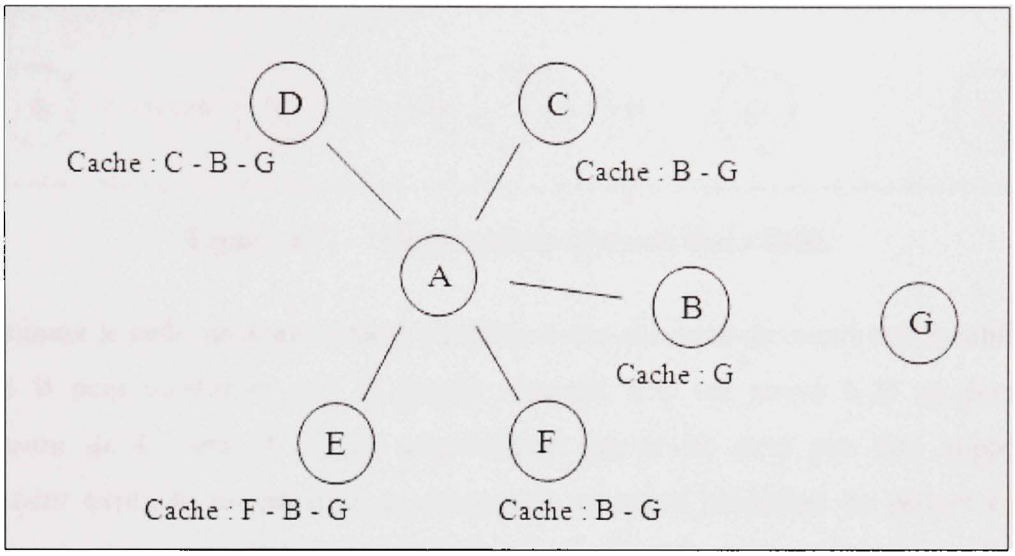


Figure 3.2 cas de tempête de réponse.

$$d = H * (h-1+r) \quad (3.1)$$

(Jonson, et al)

d : délai d'attente avant l'envoi de réponse de route

H : constante (délai de propagation entre voisins)

h : nombre de sauts du chemin de la réponse de route

r : nombre aléatoire ente 0 et 1

3.3 Maintenance de route dans DSR

À partir des spécificités des réseaux MANET, tenir au courant les nœuds des changements typologiques est la tache de la partie maintenance de route dans DSR. Chaque transmetteur est responsable de livrer le paquet au nœud voisin et de confirmer au nœud précédent que son paquet est bel et bien livré. Dans la Figure 3.3, le nœud A envoi un paquet au nœud E, le nœud A est donc responsable du lien A-B, le nœud B est responsable d'assurer la transmission entre B-C et ainsi de suite. Un acquittement peut confirmer que le lien suivant peut transmettre un paquet, au nœud précédent.

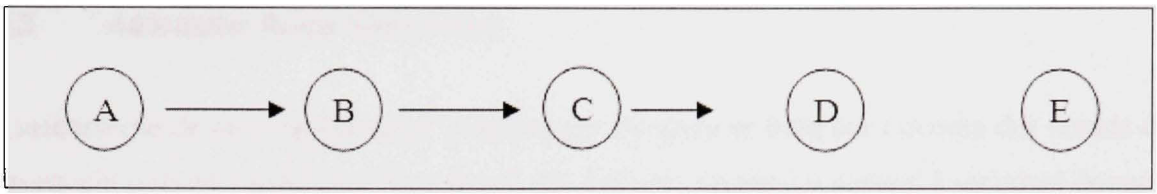


Figure 3.3 Maintenance de route dans DSR.

Pour diminuer le coût, un acquittement passif (*passive acknowledgement*) est possible. Donc, le nœud B peut confirmer que le paquet transmit à C est arrivé à D en écoutant la transmission de C vers D. Si un acquittement passif ne peut pas être supporté, un acquittement explicite est possible en retournant au nœud précédent un paquet contenant l'acquittement du paquet déjà transmis. S'il n'y pas d'acquittement qui provient d'un nœud suivant durant un certain temps, une demande explicite est envoyée un nombre maximum de fois pour rétablir la connexion. Si le nœud ne répond pas après tout ces essais, le nœud considère le lien avec le nœud suivant brisé (*broken*), supprime tout les routes contenant ce lien et envoie une *Route Error* à chaque nœud qui a envoyé un paquet à travers ce lien. Le nœud source en recevant le paquet signifiant l'expiration du lien doit recommencer une demande de route s'il n'a pas d'autre route alternative vers la même destination.

3.3.1 Packet Salvaging

Quand un nœud intermédiaire détecte que le saut prochain demandé par un paquet est interrompu, le nœud doit essayer de sauver le paquet en cherchant dans son cache une route alternative vers la destination du paquet pour réorienté le paquet si aucun chemin n'est trouvé le paquet sera rejeté et un paquet de *Route Error* sera envoyé à la source du paquet l'informant du bris du lien pour qu'elle cherche une autre route. L'envoi de la *Route Error* précède le sauvetage du paquet. Un indicateur est transmis dans le paquet pour signaler que nœuds prochains que le paquet a été sauvé pour éliminer la possibilité d'avoir des paquets qui circulent indéfiniment dans le réseau.

Pour tout autre paquet en attente d'envoi à travers le même lien discontinu, le nœud doit envoyer une *Route Error* à la source du paquet, essayé de sauver le paquet sinon le rejeter.

3.3.2 Automatic Route Shortening

Le mécanisme de raccourcissement automatique de route se base sur l'écoute des nœuds des paquets qui circulent dans le réseau. Si un nœud écoute un paquet destiné à un nœud donné et trouve que son adresse se trouve plus tard dans la séquence des nœuds relais, le nœud doit envoyer un '*Gratuitous Route Reply*' à la source du paquet en lui indiquant un chemin plus cour qui peut être utilisé.

La Figure 3.4 illustre une situation qui nécessite un '*Gratuitous Route Reply*' de la part du nœud D puisqu'il arrive à entendre la transmission du nœud B vers C du paquet provenant du nœud A.

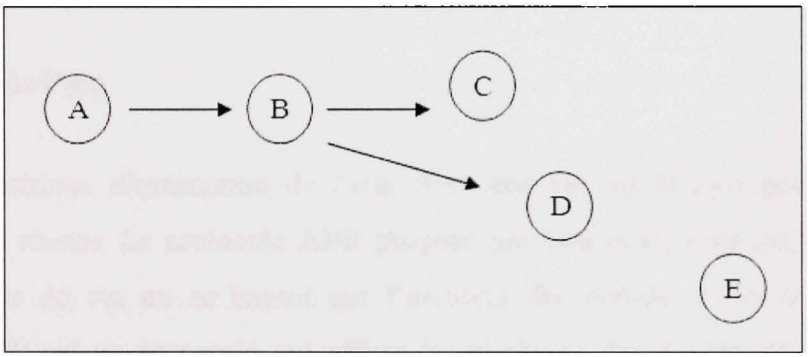


Figure 3.4 Cas d'un Automatic Route Shortening dans DSR.

3.3.3 Diffusion améliorée du message d'erreur de route

En recevant une *Route Error*, la source inclut l'information concernant le lien brisé dans sa prochaine demande de route. De cette façon, tous les nœuds voisins suppriment tous les chemins qui utilisent le lien en question et donne une réponse de route plus fiable.

Pour un complément d'information, Jonson, et al présentent une spécification plus détaillée du protocole DSR.

CHAPITRE 4

PRÉDICTION DE TEMPS DE VIE DE LIEN

Nous présentons dans ce chapitre les principales méthodes utilisées pour la prédiction de temps de vie de lien dans les réseaux ad hoc. Une description plus détaillée des méthodes choisies devancera l'architecture de l'implantation des méthodes dans notre simulateur. Enfin, nous détaillons la façon d'utilisation du temps estimé par chaque méthode. La destination peut déterminer la Route Expiration Time (RET) basée sur la prédiction du lien qui constitue la route. Il informe donc la source lorsque la route est dans un état proche de la rupture pour que celle-ci trouve une route alternative avant.

4.1 État de l'art

Plusieurs propositions d'estimation de l'état des liens ont vu le jour pour augmenter la performance du réseau. Le protocole ABR proposé par Toh et al, favorise les liens avec le plus long temps de vie en se basant sur l'incident des nœuds. *Flow Oriented Routing Protocol* (FORP) est un protocole qui utilise les positions des nœuds en se basant sur le Global Position System (GPS) pour la prédiction de l'état de lien. Goof et al utilisent la puissance de signal reçu pour déterminer la zone critique de la couverture d'un nœud. Il commence des demandes de route plus tôt pour trouver une route alternative avant la rupture du lien. Le ratio utilisé pour déterminer la zone de préemption est constant. Par conséquent, la zone de préemption été la même avec différentes valeurs de vitesse. Il existe principalement deux méthodes pour la prédiction de temps de vie de lien dans les réseaux ad hoc. La première utilise le support de GPS. La seconde se base sur la puissance de signal reçu. Nous avons ajouté une troisième méthode qui bénéficie des deux premiers pour devenir une méthode plus fiable. Ces deux méthodes sont présentées dans la prochaine section.

4.2 Notre outil de simulation

Plusieurs outils de simulation des réseaux sans fil ad hoc s'offrent à nous au moment où nous avons commencé cette recherche. La possibilité d'utiliser un environnement graphique sous le système d'exploitation Windows a tranché entre le simulateur OPNET et NS2 puisque tous les deux offrent les mêmes fonctionnalités.

OPNET Modeler d'OPNET Technologies Inc. est un outil de développement orienté objet et possédant un éditeur graphique qui facilite la compréhension et l'analyse des mécanismes et phénomène. Il incorpore une librairie qui comporte une douzaine de protocoles, technologies et applications incluant WLAN (IEEE 802.11). Ce programme fournie les outils la génération de trafics dans des réseaux ad hoc et permet de créer et de simuler des scénarios de mobilité. Lors du début de notre recherche la dernière version disponible été la version 11.0 PL6.

Le mode DCF du 802.11 a été utilisé pour les réseaux sans fil simulés. Le taux de transfert de la couche MAC est de 2Mb/s avec un rayon de couverture de 250métres. Les paquets en attente d'envoi seront supprimés après 30sec de la file d'envois qui possède une taille infinie.

4.3 Modèle de propagation radio

Dans cet algorithme, un modèle optimiste de transmission radio (*optimistic radio transmission model*) est utilisé. Si un nœud A avec un rayon de couverture R et ayant un voisin B à l'intérieur de ce cercle, B est donc censé recevoir les transmissions de A. Par conséquent, le temps de vie de lien est déterminé pas la distance entre les deux voisins.

D'après OPNET, le modèle de propagation radio est le *Two Ray Ground Reflection Approximation*. À courte distance, la formule d'atténuation en espace libre utilisée est $(1/r^2)$, à longue distance l'approximation est le *Two Ray Ground* $(1/r^4)$. Le point de référence pour utiliser l'une ou l'autre des deux modèles est aux alentours de 85 mètres. Puisque nous nous intéressant aux nœuds qui se déplacent vers l'extérieure de la couverture de transmission l'algorithme se basera sur l'approximation *Two Ray Ground*.

L'équation 4.1 représente l'implantation de *Two Ray Ground* dans OPNET.

$$P = \frac{Pt*Gt*Gr*(ht^2*hr^2)}{d^4} \quad (4.1)$$

Où :

P : puissance du signal reçu
Pt : puissance de transmission
Gt : gain du signal à la transmission
Gr : gain di signal à la réception
ht : la hauteur de l'antenne de transmission
hr : la hauteur de l'antenne de réception
d : la distance entre le transmetteur et le récepteur.

Dans nos simulations, la puissance de transmission est constante, l'environnement de test est plat et les hauteurs des antennes (ht et hr) sont constantes. Par conséquent, l'équation 4.1 peut se simplifier en donnant l'équation 4.2.

$$P = k\frac{Pt}{d^4} \quad (4.3)$$

Où
$k = Pt * Gt * Gr * (ht^2 * hr^2)$

4.4 Descriptions des méthodes choisies

Dans les trois méthodes de prédiction, nous prenons comme hypothèse que le modèle de propagation utilisé est l'espace libre (*free space propagation model*) où la puissance de signal reçu ne dépend que de la distance entre le transmetteur et le récepteur et que la puissance de transmission des nœuds dans le réseau est constante.

4.4.1 GPS

La méthode de prédiction, utilisant le support de GPS, se base sur la détermination des coordonnées des nœuds par la suite un calcul de la direction et vitesse permettra de trouver le temps de vie de lien entre deux nœuds voisins. Considérant deux nœuds voisins (i et j) qui s'éloignent l'un de l'autre avec une direction et vitesse constante.

Ayant la même couverture r. Si les coordonnées des deux nœuds sont connues (x_i, y_i) et (x_j, y_j), avec leurs vitesses constantes v_i et v_j et leurs directions θ_i et θ_j tel que ($0 \leq \theta_i, \theta_j \leq 2\pi$).
Le temps que les deux nœuds vont rester en visibilité directe est donné par l'équation 4.3.

$$D_t = \frac{-(ab+cd)+\sqrt{(a^2+c^2)r^2-(ad-bc)^2}}{a^2+c^2} \tag{4.3}$$

Où

$a = v_i \cos\theta_i - v_j \cos\theta_j$
$b = x_i - x_j$
$c = v_i \cos\theta_i - v_j \cos\theta_j$
$d = y_i - y_j$

Si $v_i = v_j$ et $\theta_i = \theta_j$, D_t sera infini.
Pour avoir une estimation du temps de vie de lien avec la méthode utilisant le GPS, il faut au moins deux échantillons pour calculer les directions des deux nœuds (θ_i, θ_j) ainsi que leurs vitesses (v_i, v_j). Par la suite, il faut pouvoir calculer le temps de vie de lien entre les deux voisins.

4.4.2 Puissance de signal

La prédiction de temps de vie de lien dans cette méthode se base sur la mesure de la puissance de signal reçu. Cette méthode a été proposée par Narendran et al. Elle prend comme hypothèse que la puissance de signal envoyé est constante. Les échantillons de puissance reçue sont mesurés à partir des paquets reçus des voisins. À partir de cette information, le calcul de la variation de puissance est possible. Et puisque la puissance de signal limite (*Signal power threshold*) est fixée, le temps après lequel la puissance sera inférieure à cette limite peut être calculé.

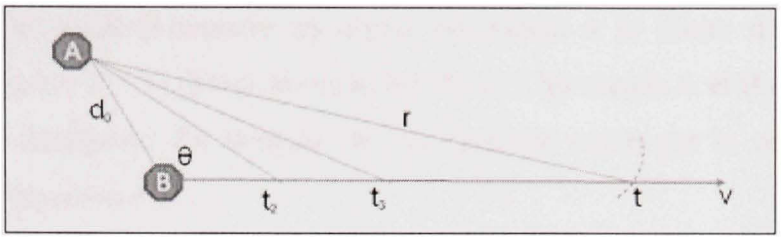


Figure 4.1 Mouvement relatif de deux nœuds mobile.

Le temps de vie de lien est le temps après lequel deux nœuds en visibilité directe ne le seront plus. Puisque la limite de réception de signaux est fixe, si deux nœuds maintiennent leurs vitesses et directions le temps de vie de lien peut être constant. La Figure 4.1 montre un mouvement relatif de deux nœuds mobiles. À T_1 le nœud B reçoit un signal de A, nous supposant qu'a ce moment la distance entre les deux nœuds est d_0 donc la relation de la puissance reçue avec la puissance de transmission, illustrée par l'équation 4.4, ne dépend que de la distance entre les deux nœuds.

$$P_1 = k\frac{P_t}{d_0^4} \tag{4.4}$$

À T_2 le nœud B reçoit un deuxième échantillon de A tel que $t_2 = T_2 - T_1$. L'équation 4.5 représente la puissance reçue.

$$P_2 = k\frac{P_t}{(d_0^2+(vt_2)^2-2d_0vt_2\cos\theta)^2} \tag{4.5}$$

À T_3 le nœud B reçoit un deuxième échantillon de A tel que $t_3 = T_3 - T_2$. L'équation 4.6 représente la puissance reçue. Il n'est pas nécessaire que t_3 soit un multiple de t_2.

$$P_3 = k\frac{P_t}{(d_0^2+(vt_3)^2-2d_0vt_3\cos\theta)^2} \tag{4.6}$$

Au moment T, le nœud B recevra un signal équivalent à la limite de la réception P_s (*threshold*), tel que $t = T - T_1$. Entre les moments T_1 et T les nœuds A et B doivent maintenir leurs vitesses et directions. La formule de la puissance reçue par le nœud B peut être représentée par l'équation 4.7.

$$P_s = k \frac{P_t}{(d_0^2+(vt)^2-2d_0vt\cos\theta)^2} \tag{4.7}$$

De l'équation 4.4, nous pouvons avoir :

$$P_1 d_0^4 = kP_t \tag{4.8}$$

En substituant 4.8 dans les équations 4.5, 4.6 et 4.7 nous obtiendrons :

$$\sqrt{P_2} = \frac{\sqrt{P_1}d_0^2}{d_0^2+(vt_2)^2-2d_0vt_2\cos\theta} \tag{4.9}$$

$$\sqrt{P_3} = \frac{\sqrt{P_1}d_0^2}{d_0^2+(vt_3)^2-2d_0vt_3\cos\theta} \tag{4.10}$$

$$\sqrt{P_s} = \frac{\sqrt{P_1}d_0^2}{d_0^2+(vt)^2-2d_0vt\cos\theta} \tag{4.11}$$

À partir des équations 4.9 et 4.10, la vitesse peut être en relation avec la distance illustrée dans l'équation 4.12.

$$v^2 = \beta d_0^2 \tag{4.12}$$

Où :

$\beta = \frac{(\sqrt{P_1P_2}t_2+\sqrt{P_2P_3}t_3-\sqrt{P_1P_3}t_3-\sqrt{P_2P_3}t_2)}{(t_2t_3^2-t_3t_2^2)\sqrt{P_2P_3}}$ est une constante.

L'équation 4.9 et 4.11 peuvent donner :

$$\sqrt{P_s} = \frac{\sqrt{P_1 P_2} d_0^2 t_2}{(t_2\sqrt{P_2} - t\sqrt{P_2} + t\sqrt{P_1}) d_0^2 + (t_2\sqrt{P_2} t^2 - t_2^2\sqrt{P_2} t) v^2} \tag{4.13}$$

En substituant 4.12 dans 4.13 nous obtenant :

$$\sqrt{P_s} = \frac{\sqrt{P_1 P_2} t_2}{(t_2\sqrt{P_2} - t\sqrt{P_2} + t\sqrt{P_1}) + (t_2\sqrt{P_2} t^2 - t_2^2\sqrt{P_2} t)\beta} \tag{4.14}$$

Donc nous pouvons déduire l'équation 4.15 :

$$at^2 + bt + c = 0 \tag{4.15}$$

Où :

$a = t_2\sqrt{P_2 P_s}\beta$

$b = \sqrt{P_s}\left(\left(\sqrt{P_1} - \sqrt{P_2}\right) - t_2^2\sqrt{P_2}\beta\right)$

$c = t_2\sqrt{P_2 P_s} - t_2\sqrt{P_1 P_2}$

Finalement pour trouver le temps de vie de lien entre deux nœuds voisins il suffit de résoudre l'équation 4.16.

$$t = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{4.16}$$

Puisque t ne peut pas être négative, la solution est :

$$t = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \tag{4.17}$$

L'équation 4.17 est donc notre algorithme de prédiction de temps de vie de lien (LET) qui ne peut fonctionner qu'en recevant au moins trois échantillons du nœud voisin.
Cet algorithme fonctionne pour deux voisins qui s'éloignent l'un de l'autre. Par conséquent, la puissance reçue des deux nœuds doit être de plus en plus faible aux différents moments de la réception de l'échantillonnage suivant la formulation 4.18.

$$P_3 \leq P_2 \leq P_1 \text{ et } T_3 \geq T_2 \geq T_1 \tag{4.18}$$

Si les deux nœuds se déplacent en s'approchant, la prédiction de temps de vie de lien n'est pas possible avec cet algorithme d'autant plus qu'elle n'est pas nécessaire puisque les deux nœuds ne risquent pas d'avoir une rupture de lien en s'approchant l'un de l'autre.
Une autre limitation qui s'impose à l'application de l'algorithme de prédiction est le manque de précision quand la différence de puissance reçue d'un même voisin est inférieure à 1%. Donc les échantillons de puissance reçus, acceptés pour le calcul de temps de vie de lien dans l'algorithme doivent avoir au moins 1% de différence pour donner un temps de vie plus précis.

4.5 Architecture de l'implantation du Cross Layer

Nous avons commencé l'implantation des deux algorithmes de prédiction de temps de vie de lien par la modification des formats de trame et de paquet. Le nouveau format, illustré dans la Figure 4.2, montre les ajouts des paramètres nécessaires au fonctionnement de l'une ou l'autre des méthodes. Dans le cas de la prédiction à l'aide de la puissance de signal l'ajout au niveau du paquet sera suffisant. Alors qu'en utilisant le GPS, il sera nécessaire d'ajouter les coordonnées du transmetteur dans l'entête de la trame.

<table>
<tr><td colspan="2">Entête de la trame</td><td rowspan="2">Entête IP</td><td>Entête DSR</td><td rowspan="2">Donnée</td></tr>
<tr><td>x</td><td>y</td><td>QoS_min</td></tr>
</table>

Figure 4.2 Nouveau format de trame et paquet.

La taille de la variable QoS_min est 14 bits, alors que la taille nécessaire pour enregistrer les coordonnées (x, y) est de 20 bits pour chacun d'entre eux. Ce qui fait un total de 54 bis par paquet pour utiliser la prédiction par GPS ou les deux prédictions en même temps.

La figure 4.3, illustre la nouvelle architecture qui permet une coopération entre la couche MAC et la couche de routage. Cette coopération consiste à calculer le temps de vie de lien pour chaque voisin et de mettre à jour la fiche correspondante. Par la suite la couche routage effectue une lecture de la fiche d'où le paquet provient pour mettre à jour son cache et le QoS_min intégrés dans le paquet s'il y a une nécessité d'émettre le paquet.

La valeur QoS_min qui voyage avec le paquet retient toujours le minimum des temps de vie des liens (LETs) qui constitue la route. Ce qui correspond à la *Route Expiration Time* (RET). À chaque réception d'un échantillon, une mise à jour de toutes les fiches, ayant un *Link Expiration Time* (LET) valide, est faite. Une fiche peut rester avec un LET de zéro un maximum de 30 sec auquel cas elle sera supprimée. Dans les prochaines sections, nous étalons les spécificités de l'implantation de chaque méthode de prédiction.

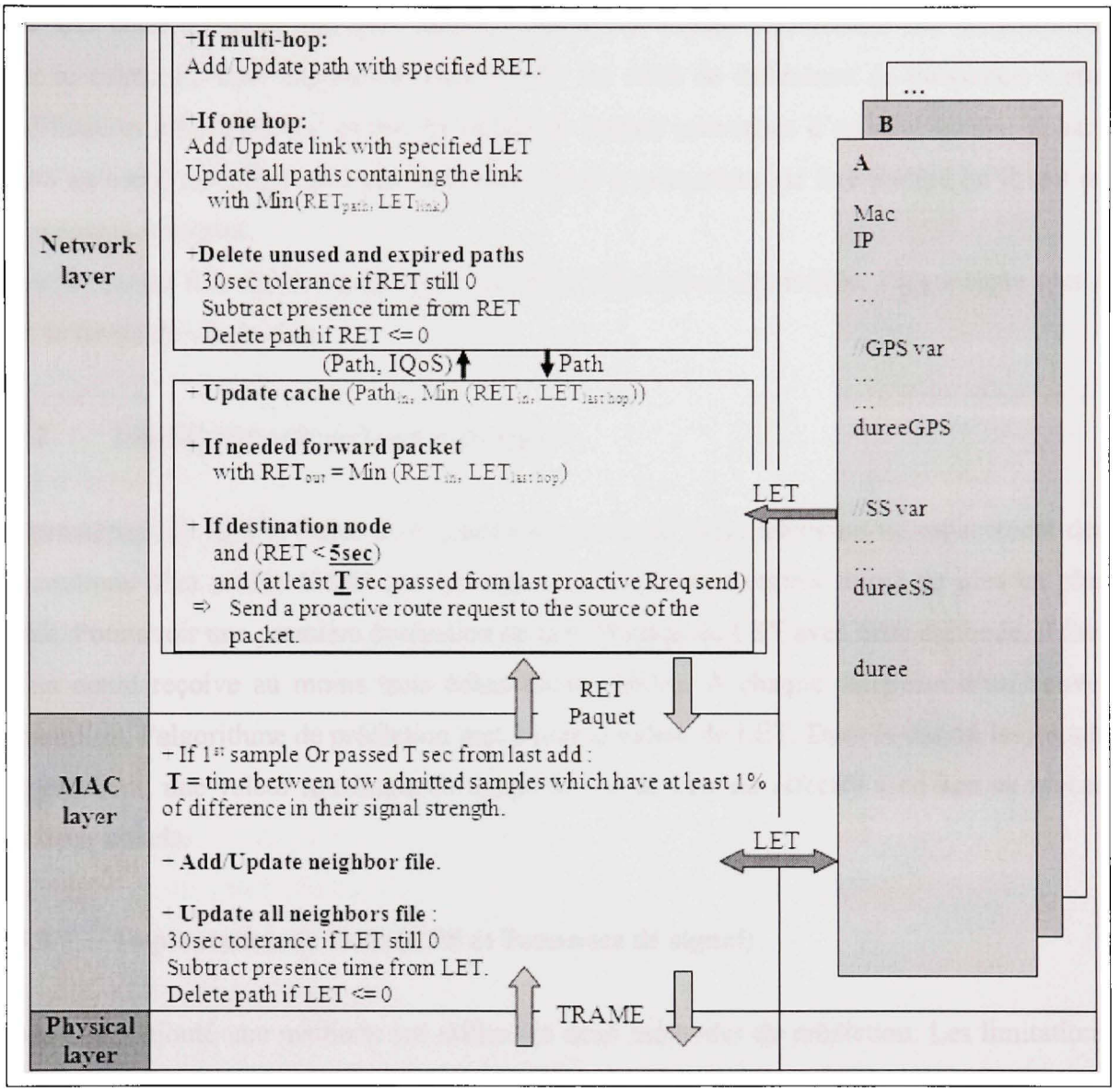


Figure 4.3 Architecture cross-layer pour l'implémentation de temps de vie de lien.

4.5.1 Implantation de GPS

La prédiction de temps de vie de lien par GPS, se base sur la réception d'au moins deux échantillons. Ainsi, un nœud peut calculer l'angle de mouvement et la vitesse de déplacement en ayant les moments de réception de chaque échantillon.

Pour que cette méthode soit plus exacte, nous avons espacé l'admission des échantillons, pour le calcul du *Link Expiration Time* (LET), de ±1% de différence de puissance. Cette modification est nécessaire en cas de rafale de paquet provenant d'un seul voisin, faisant croire au nœud récepteur qu'à certains moments le transmetteur est fixe malgré qu'il soit en mouvement continuel.
Donc à chaque fois qu'un nœud reçoit un autre échantillon admissible, l'algorithme met à jour le temps de vie du lien.

4.5.2 Implantation de puissance de signal

La prédiction du LET à l'aide de la puissance de signal reçu, nécessite un espacement des échantillons d'au moins 1% et que les valeurs de puissance reçues soient de plus en plus faible. Pour avoir une première évaluation de la prédiction du LET avec cette méthode, il faut qu'un nœud reçoive au moins trois échantillons valides. À chaque réception d'un nouvel échantillon, l'algorithme de prédiction met à jour la valeur de LET. Dans le cas où les nœuds s'approchent, une valeur maximale de temps de vie de lien est affectée à ce lien au niveau des deux nœuds.

4.5.3 Implantation de Both (GPS et Puissance de signal)

Nous avons ajouté une méthode qui utilise les deux méthodes de prédiction. Les limitations des deux méthodes précédentes s'appliquent à cette méthode. Nous avons voulu tester une méthode qui se veut conservatrice. Ainsi, si les deux méthodes précédemment présentées donnent une prédiction de temps de vie de lien valide, nous prenons dans cette méthode la valeur minimale. Si une des deux méthodes utilisées ne donne pas encore de valeur de LET valide, nous considérons automatiquement l'autre méthode.

4.5.4 Paramètres supplémentaires du système

Nous essayons de trouver le temps entre chaque échantillon de signal reçu valide du même nœud. Le temps T, illustré dans la Figure 4.3, est utilisé dans la phase de demande proactive pour limiter le nombre de demandes. Ainsi, toutes les réponses seront reçues avec un temps égal ou supérieur à T, ce qui permettra à l'échantillon reçu d'être admis au niveau de la couche MAC pour participer dans le calcul d'un nouveau lien. Donc nous enverrons seulement les demandes qui nous permettent de prendre en considération toutes leurs réponses, sans beaucoup de perte de bande passante. Le temps T est automatiquement ajustable suivant le comportement de chaque nœud (direction, vitesse).

Le deuxième paramètre clé de cette implantation est la valeur de temps de réaction (TR) que nous devons considérer (5sec dans la Figure 4.3). Cette valeur permet de prévenir les déconnexions. Nous avons pris dans toutes nos simulations la valeur 5sec comme valeur logique par défaut quelque soit la vitesse des nœuds dans le réseau. En prenant une valeur de temps pour trouver la zone de préemption celle-ci variera en taille selon la vitesse des nœuds. Si la vitesse est plus grande, la zone de préemption est plus grande, ce qui permet à un nœud sortant de la couverture de trouver un chemin alternatif à temps. Contrairement à Goof *et al* qui utilise un ratio permettant à la zone de préemption de rester fixe quelque soit la vitesse.

4.6 Utilisation de la prédiction

Du moment qu'une prédiction de temps de vie de lien existe et est disponible au niveau des couches supérieures, plusieurs portes permettant l'intégration de la qualité de service dans les réseaux ad hoc s'ouvrent. Nous avons utilisé cette prédiction pour construire le temps de vie d'une route entière, pour maintenir les routes utilisées à jour, pour supprimer plus rapidement les routes désuètes du cache et pour déclencher de demandes proactives.

4.6.1 Prédiction de temps de vie de route

D'après le nouveau format de trame (Figure 4.2), le paquet incorpore un champ qui transporte la qualité de service minimale entre le LET du dernier saut et la valeur transportée par le paquet qui représente le temps de vie de route (RET). À la génération de paquet, cette valeur est initialisée à la valeur maximale. La figure 4.4, illustre notre façon pour garder le temps de vie de lien minimum, parmi tous les liens qui constituent la route, afin de représenter le temps de vie de la route. Le paquet envoyé du nœud S, aura une valeur de qualité de route maximale. Le nœud G, reçoit un paquet contenant le RET de S a H et en estimant le temps de vie de lien H-G, il sera capable de prendre le minimum pour représenté le temps de vie de la route qui débute du nœud S jusqu'au nœud G.

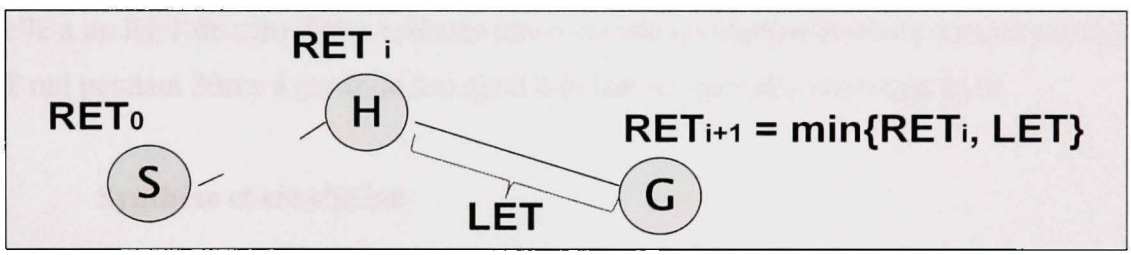


Figure 4.4 Prédiction de temps de vie de route.

4.6.2 Maintenance des routes

La Figure 4.3 illustre la façon dont nous utilisons le RET pour mettre à jour les différentes routes de cache ainsi que les fiches de chaque voisin. Une réception d'un échantillon permet de mettre à jour la fiche du voisin, transmetteur du paquet. Par la suite, nous soustrayons le temps de présence de la prédiction de chaque voisin en mettant à jour le LET de chaque fiche. Quand le paquet arrive à la couche réseau, le nœud met à jour ou ajoute la route de la source jusqu'à lui, avec le minimum entre le RET provenant du paquet et le LET du dernier saut. Par la suite un mécanisme semblable est déclenché pour mettre à jour tous les chemins des nœuds. Chaque fiche correspond à un voisin donc à un lien.

Puisque nous avons mis à jour toutes les fiches au début du processus, il faudra qu'elle atteigne les routes placées dans le cache.
Pour cela nous avons ajouté une fonction qui met à jour toute les chemins qui contiennent les liens avec chaque voisin avec le minimum entre le LET du lien inscrit dans la fiche et le RET inscrit dans le cache.

4.6.3 Suppression des routes désuètes

En ayant le temps de vie de lien et de route et en se basant sur les mécanismes décrits précédemment, un lien sera invalide suivant sa prédiction de temps de vie. Dans la version originale de DSR, une route dans le cache à une validité de 300sec à moins qu'elle déclenche une *Route Error*. Pour ajouter plus de précision au cache, nous éliminons une route dès qu'elle a un RET de zéro. Nous tolérons une nouvelle inscription de route dans le cache avec RET nul pendant 30sec à partir de son ajout à défaut de quoi elle sera supprimée.

4.7 Synthèse et conclusion

Dans ce chapitre, nos approches basées sur une architecture *cross-layer*, a été d'utiliser le (GPS) et /ou la puissance du signal reçu pour calculer le temps de vie de lien et de déduire la qualité future du lien directement de l'historique de la puissance reçue. De fait, nous présentons les spécificités de notre implantation du temps de vie de lien qui permet une prédiction de temps de vie de route, maintient une information à jour au niveau des nœuds du réseau et une élimination des routes désuètes.

En faite ces approches présentent des inconvénients et des limitations dont les plus importants sont :

- La considération des hypothèses simplistes sur le canal de propagation et/ou le mouvement des nœuds.

- Le canal de propagation est considéré sans perturbation (bruit).
- Plusieurs approches utilisent la puissance reçue pour en déduire le mouvement des nœuds. Et par la suite le mouvement des nœuds est prédit et la qualité des liens en est déduite.

CHAPITRE 5

COMPARAISON DE PERFORMANCE

Dans ce chapitre, nous présenterons une comparaison de performance des différentes variantes de notre implantation de DSR, intégrant le support de GPS et/ou la puissance de signal reçu, avec la version originale du même protocole. Pour ce faire, nous avons débuté par la présentation des configurations et résultats de nos tests unitaires qui permettent de valider l'implantation de l'algorithme de prédiction incluant nos modifications, par la suite nous appliquons le nouveau comportement du protocole du routage DSR sur des scénarios plus général et plus réaliste pour constater l'avantage de notre implantation sur le réseau. Dans les prochaines sections, toutes les nouvelles variantes du protocole DSR intégrant l'estimation de temps de vie de route seront indiquées par DSR-RET.

5.1 Choix des paramètres de l'algorithme

Notre implantation présentée dans la section 4.5 du chapitre 4 montre deux nouveaux paramètres qui ont une influence directe sur la performance du réseau. Le premier permet l'envoi de demande de route proactive avec un certain espacement dans le temps. Nous avons initialisé cette variable au temps minimum permit par la version originale de DSR entre deux demandes de route successive par la suite elle sera changée suivant l'arrivé des échantillons aux nœuds. Le deuxième paramètre permet de déterminer la zone de préemption. Un nœud arrivant à cette zone commence l'envoi de demande de route proactive puisque le temps de vie de route utilisé arrive à échéance. Nous avons fixé ce paramètre à 5sec qui semble une valeur proche de la normale. Donc pour une route, ayant un RET de 30sec, qui sert à acheminer l'information entre deux nœuds et arrivant à un RET de 5sec, la source commence à chercher une route alternative pour contrer la déconnexion.

5.2 Test unitaire

Un réseau mobile ad hoc consiste en plusieurs nœuds mobiles qui communiquent entre eux pour joindre une destination donnée plus loin que leur couverture radio (multi saut).
La mobilité dans un réseau introduit un effet de changement de topologie ou de zone. Ce dernier peut augmenter ou diminuer le nombre de sauts pour atteindre la même destination. Dans la version originale de DSR et dans le cas où plusieurs chemins sont disponibles vers la même destination, le changement de zone qui ajoute un chemin plus long que celui en cour d'utilisation ne sera pas effectif tant et aussi longtemps que le chemin en cour d'utilisation ne génère pas de perte ou ne dépasse pas la limite de temps de vie par défaut dans le cache. Avec notre implantation dès qu'une route vers la même destination à un temps de vie de lien (LET) valide, elle se classera dans la liste des routes vers la même destination, selon ce paramètre en premier. Si le LET calculé permet de classer la route dans le première place, celle-ci sera immédiatement utilisée s'il y a un besoin.

Dans cette section nous présenterons des scénarios simples et leur résultat à fin de monter le bon fonctionnement de notre implantation. Nous avons deux principales parties dans cette section. La première est consacrée pour les tests sans changement de zone ou de couverture en ayant une mobilité ou non. La seconde permet de voir le comportement du nouveau protocole avec des changements de zone de couverture qui augmentent ou diminuent le nombre de sauts par rapport à la route précédemment utilisée.

5.2.1 Sans changement de zone

5.2.1.1 Sans mobilité

- Nous avons simulé le scénario, illustré dans la Figure 5.1, pendant 360sec. Le nœud 3 (mobile_node_3) démarre une communication avec le serveur tout au long de la simulation. Les nœuds intermédiaires servent juste de relai.

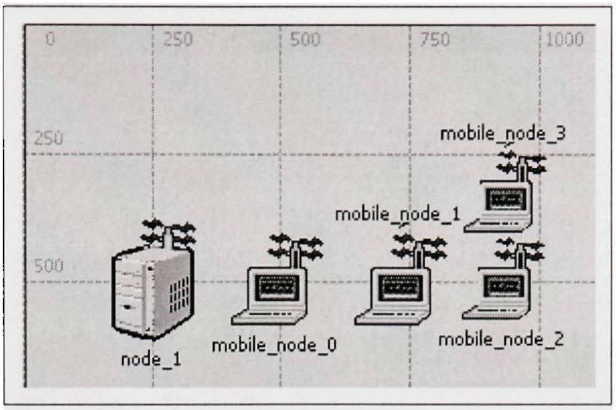


Figure 5.1 Scénario de test unitaire fixe.

Le temps de vie d'une route dans le cache est de 300sec dans la version originale de DSR. Avec notre implantation, une route sans temps de vie de route (RET) valide ne peut rester plus de 30sec dans le cache. Si une route arrive à avoir un RET valide durant les 30 premières secondes, sa suppression sera basée sur sa prédiction (RET). Dès que la route sera expirée, elle sera supprimée du cache diminuant ainsi le risque de perte de paquet à cause de route expiré.

La figure 5.2, montre un point de statistique de plus aux alentours de 5min 30sec pour la version originale de DSR. Ce qui montre qu'il y a eu un ajout de route à ce moment. Mais puisqu'il n'y a pas eu de changement dans la topologie, les routes ajoutées ont été supprimées juste avant puisqu'elles ont atteint les 300sec de présence dans le cache. Avec notre implantation une route est mise à jour à chaque arrivé de paquet valide et la suppression ne se base que sur le temps de vie de la route (RET) par conséquent nous ne supprimons pas de route valide.

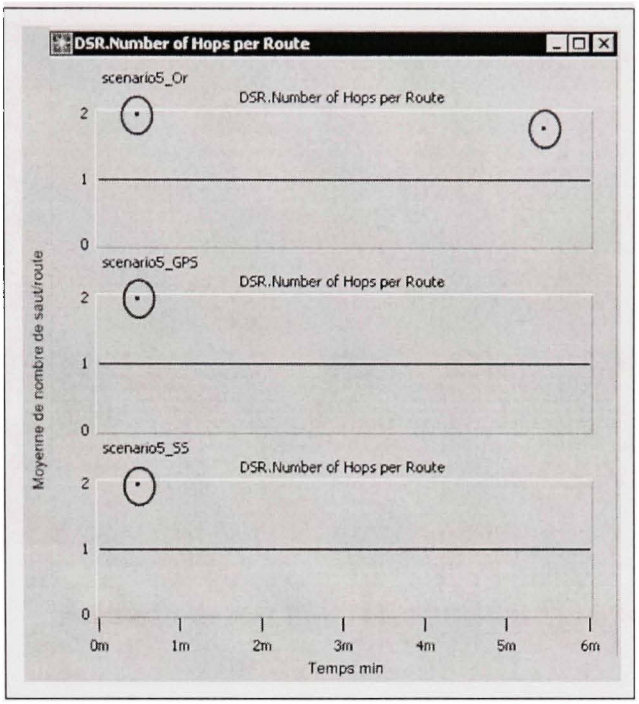


Figure 5.2 Moyenne globale de nombre de saut par route dans le cache.

(nombre de saut de tous les chemins dans le cache sur le nombre de chemins présent dans le cache)

- La figure 5.3 illustre le deuxième scénario que nous avons simulé pour cette section sans mobilité. Nous avons simulé le scénario pendant 300sec. Le nœud 5 (mobile_node_5) démarre une communication avec le serveur tout au long de la simulation. Les nœuds intermédiaires servent juste de relai. Nous avons instauré deux routes vers la destination demandée pas le nœud 5.

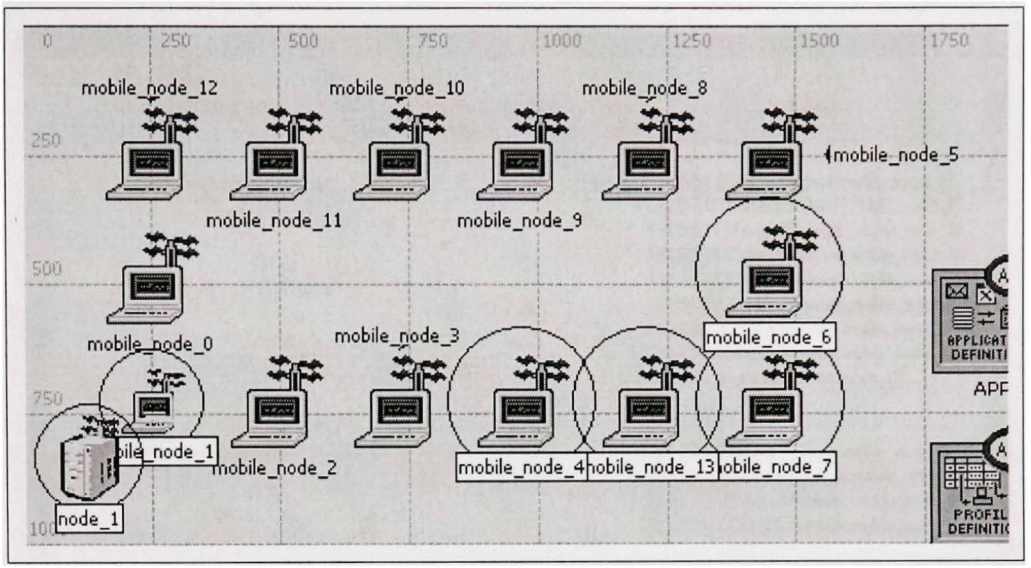
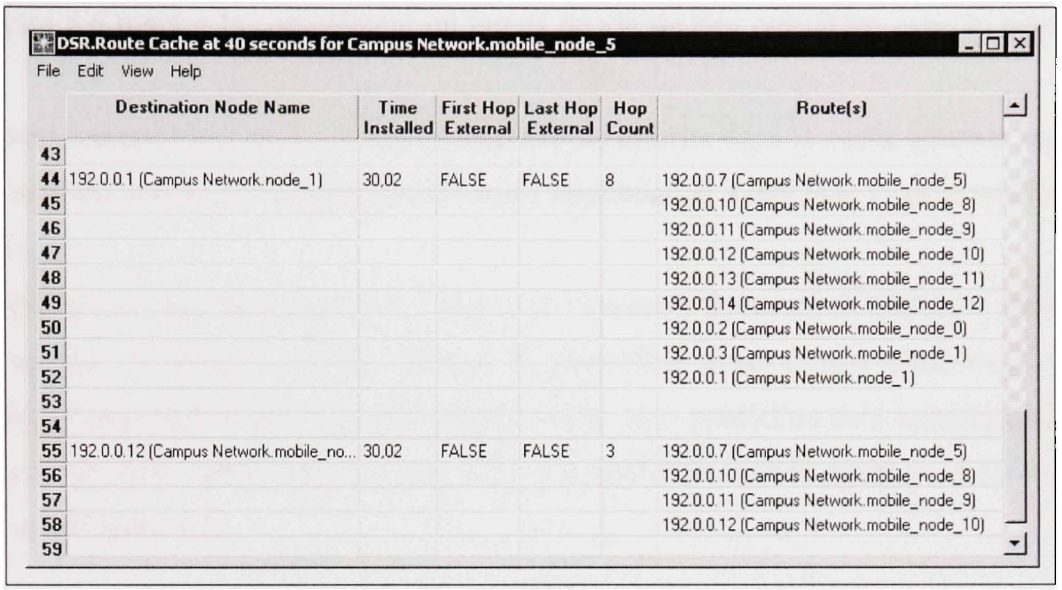


Figure 5.3 Scénario de test fixe : suppression de route invalide.

La demande de route du nœud 5 se propage sur les deux chemins possibles (Figure 5.3) pour atteindre la destination. Dans la version originale de DSR, comme vu dans le CHAPITRE 3, un nœud intermédiaire n'a pas le droit de diffuser une demande de route ayant la même source, destination et identifiant deux fois. Dans ce cas la première demande qui atteint le goulot d'étranglement (nœud 0 ou destination) sera la seule qui déclenchera une réponse de route. La Figure 5.4 montre la table de routage du nœud 5 utilisant le protocole de routage original DSR qui rend disponible une seule route vers la destination. Alors qu'avec notre implantation deux routes sont disponibles vers la destination comme l'illustre la Figure 5.5 qui montre le temps d'inscription de chaque route dans le cache de deux routes vers la même destination.

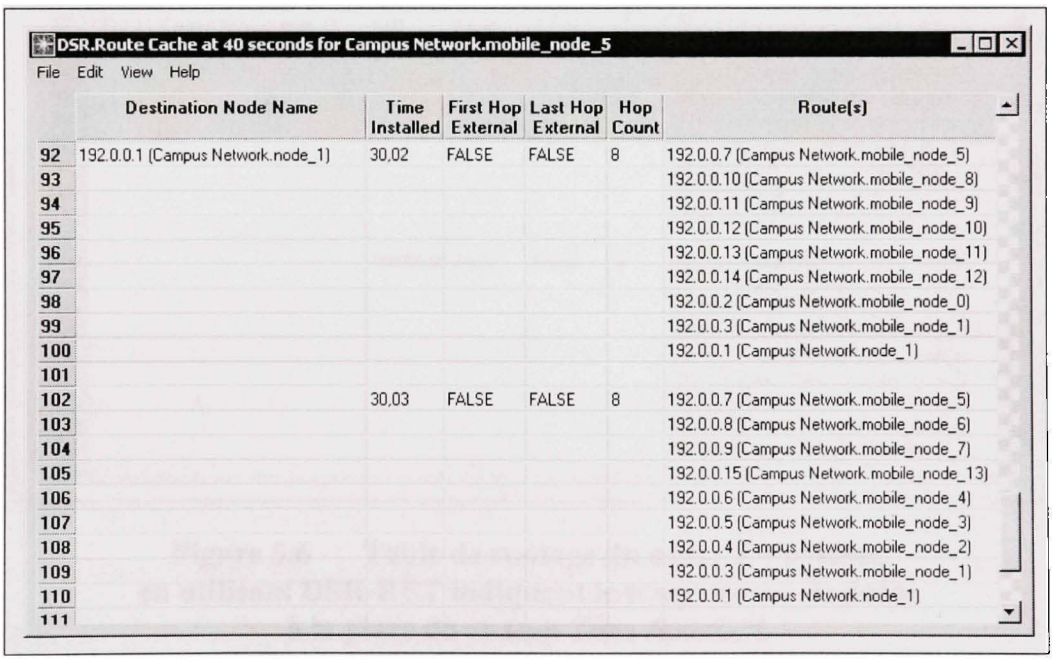


DSR.Route Cache at 40 seconds for Campus Network.mobile_node_5

File Edit View Help

	Destination Node Name	Time Installed	First Hop External	Last Hop External	Hop Count	Route(s)
43						
44	192.0.0.1 (Campus Network.node_1)	30,02	FALSE	FALSE	8	192.0.0.7 (Campus Network.mobile_node_5)
45						192.0.0.10 (Campus Network.mobile_node_8)
46						192.0.0.11 (Campus Network.mobile_node_9)
47						192.0.0.12 (Campus Network.mobile_node_10)
48						192.0.0.13 (Campus Network.mobile_node_11)
49						192.0.0.14 (Campus Network.mobile_node_12)
50						192.0.0.2 (Campus Network.mobile_node_0)
51						192.0.0.3 (Campus Network.mobile_node_1)
52						192.0.0.1 (Campus Network.node_1)
53						
54						
55	192.0.0.12 (Campus Network.mobile_no...	30,02	FALSE	FALSE	3	192.0.0.7 (Campus Network.mobile_node_5)
56						192.0.0.10 (Campus Network.mobile_node_8)
57						192.0.0.11 (Campus Network.mobile_node_9)
58						192.0.0.12 (Campus Network.mobile_node_10)
59						

Figure 5.4 Table de routage du nœud 5 à t=40sec en utilisant la version original de DSR.



DSR.Route Cache at 40 seconds for Campus Network.mobile_node_5

File Edit View Help

	Destination Node Name	Time Installed	First Hop External	Last Hop External	Hop Count	Route(s)
92	192.0.0.1 (Campus Network.node_1)	30,02	FALSE	FALSE	8	192.0.0.7 (Campus Network.mobile_node_5)
93						192.0.0.10 (Campus Network.mobile_node_8)
94						192.0.0.11 (Campus Network.mobile_node_9)
95						192.0.0.12 (Campus Network.mobile_node_10)
96						192.0.0.13 (Campus Network.mobile_node_11)
97						192.0.0.14 (Campus Network.mobile_node_12)
98						192.0.0.2 (Campus Network.mobile_node_0)
99						192.0.0.3 (Campus Network.mobile_node_1)
100						192.0.0.1 (Campus Network.node_1)
101						
102		30,03	FALSE	FALSE	8	192.0.0.7 (Campus Network.mobile_node_5)
103						192.0.0.8 (Campus Network.mobile_node_6)
104						192.0.0.9 (Campus Network.mobile_node_7)
105						192.0.0.15 (Campus Network.mobile_node_13)
106						192.0.0.6 (Campus Network.mobile_node_4)
107						192.0.0.5 (Campus Network.mobile_node_3)
108						192.0.0.4 (Campus Network.mobile_node_2)
109						192.0.0.3 (Campus Network.mobile_node_1)
110						192.0.0.1 (Campus Network.node_1)
111						

Figure 5.5 Table de routage du nœud 5 à t=40sec en utilisant DSR-RET.

La Figure 5.6 montre le complément du temps de vie de lien concaténé avec le nombre de saut.

Nous pouvons constater qu'à t=40 la première route inscrite dans le cache possède un temps de vie de route infini qui correspond dans notre implantation à 999,9sec (valeur maximale du champ).

Alors que sur la seconde route n'ont transigé qu'une seule demande et une seule réponse de route ce qui ne permet pas de calculer la prédiction avec si peu d'échantillons; par conséquent, la présence de cette route dans le cache sans prédiction sera tolérée pendant un maximum de 30sec pour pouvoir construire une prédiction valide après ce délai elle sera supprimée (Figure 5.7).

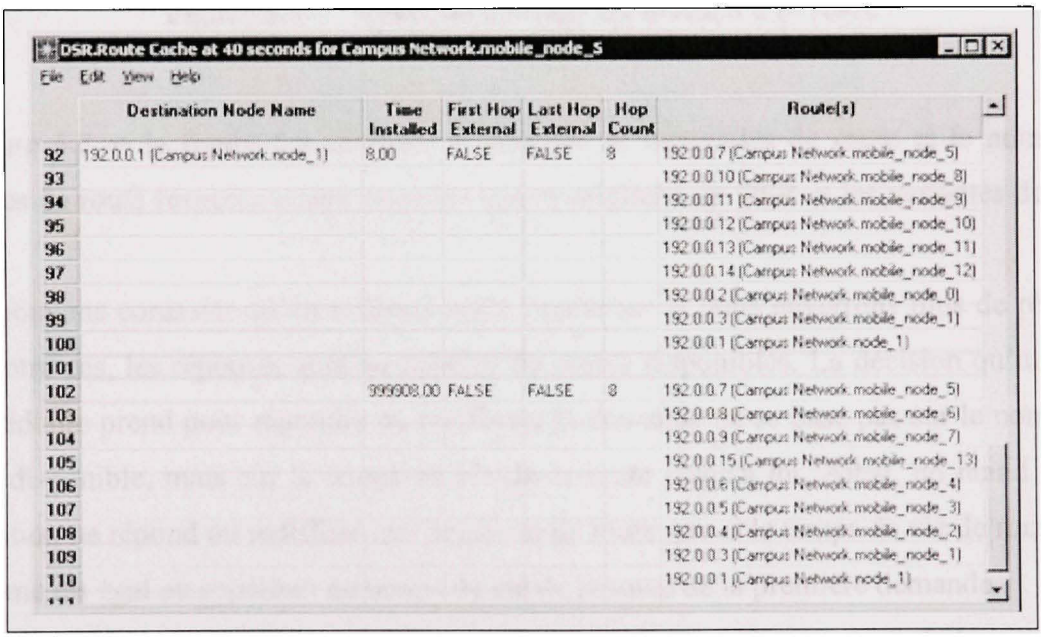
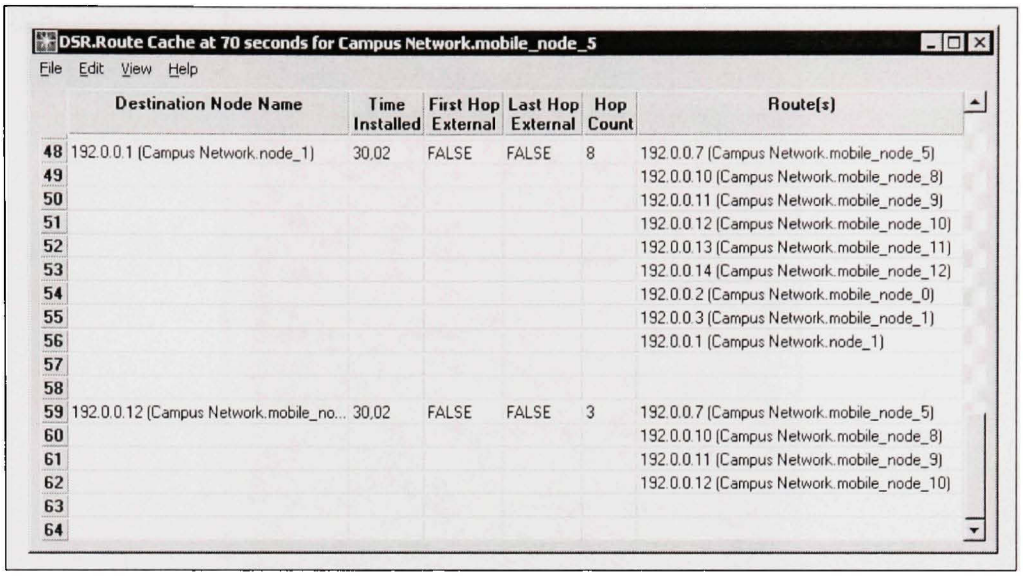


Figure 5.6 Table de routage du nœud 5 à t=40sec en utilisant DSR-RET indiquant le temps de vie de route à la place du champ *Time Installed*.



	Destination Node Name	Time Installed	First Hop External	Last Hop External	Hop Count	Route(s)
48	192.0.0.1 (Campus Network.node_1)	30,02	FALSE	FALSE	8	192.0.0.7 (Campus Network.mobile_node_5)
49						192.0.0.10 (Campus Network.mobile_node_8)
50						192.0.0.11 (Campus Network.mobile_node_9)
51						192.0.0.12 (Campus Network.mobile_node_10)
52						192.0.0.13 (Campus Network.mobile_node_11)
53						192.0.0.14 (Campus Network.mobile_node_12)
54						192.0.0.2 (Campus Network.mobile_node_0)
55						192.0.0.3 (Campus Network.mobile_node_1)
56						192.0.0.1 (Campus Network.node_1)
57						
58						
59	192.0.0.12 (Campus Network.mobile_no...	30,02	FALSE	FALSE	3	192.0.0.7 (Campus Network.mobile_node_5)
60						192.0.0.10 (Campus Network.mobile_node_8)
61						192.0.0.11 (Campus Network.mobile_node_9)
62						192.0.0.12 (Campus Network.mobile_node_10)
63						
64						

Figure 5.7 Table de routage du nœud 5 à t=70sec en utilisant DSR-RET.

La figure 5.8 et la figure 5.9 illustrent le nombre de demandes de route et le nombre de réponses de route respectivement pour la version originale de DSR et les variantes de DSR-RET.

Nous pouvons constater qu'en utilisant notre implantation nous enverrons plus de réponses dans notre cas, les réponses sont au nombre de routes disponibles. La décision qu'un nœud intermédiaire prend pour répondre ou rediffuser la demande ne se base pas sur le nombre de routes disponible, mais sur le temps de vie de la route jusqu'à lui. Ainsi, un nœud ou une destination ne répond ou rediffuse une demande de route que si le temps de vie de route de la deuxième est égal ou supérieur au temps de vie de la route de la première demande.

En intégrant ce comportement nous prenons avantage de l'inondation qui se fait avec chaque envoi de demande de route en permettant au nœud intermédiaire de répondre plus qu'une fois à la demande de route et nous diminuant l'effet négatif de la tempête de réponse de route (*Route Reply Storms*) en utilisant la prédiction de temps de vie pour répondre seulement au meilleur cas.

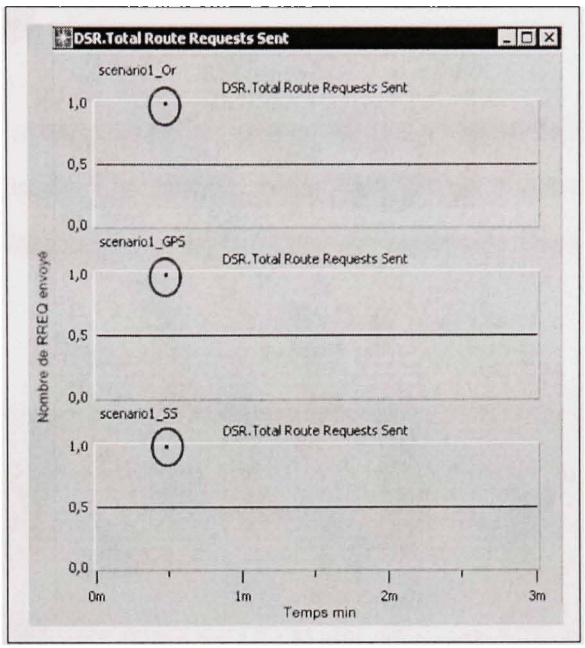


Figure 5.8 Nombre de demande de route envoyé pour les différentes variantes du protocole.

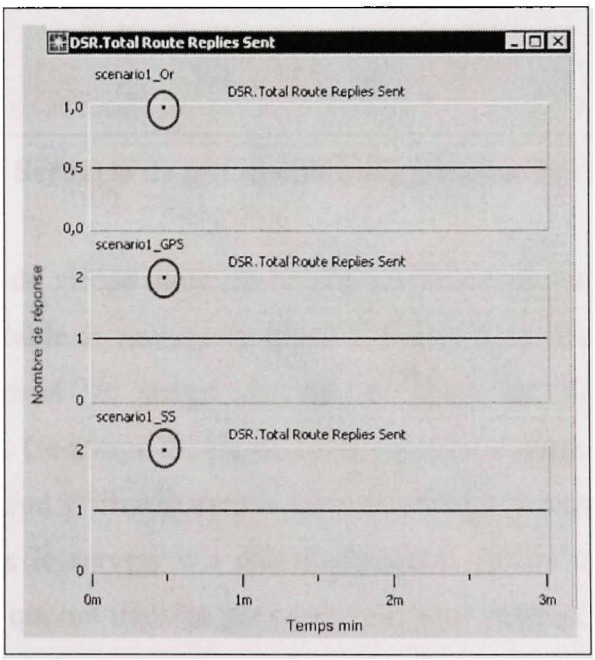


Figure 5.9 Nombre de réponse de route envoyé pour les différentes variantes du protocole.

5.2.1.2 Avec mobilité

Dans cette section nous avons simulé un réseau ad hoc (Figure 5.10) ayant seulement deux nœuds mobiles (mobile_node_9 et mobile_node_4). Chacun d'entre eux se trouve dans une route distincte vers la destination, avec la direction présentée dans la figure et une vitesse constante de 2m/s.

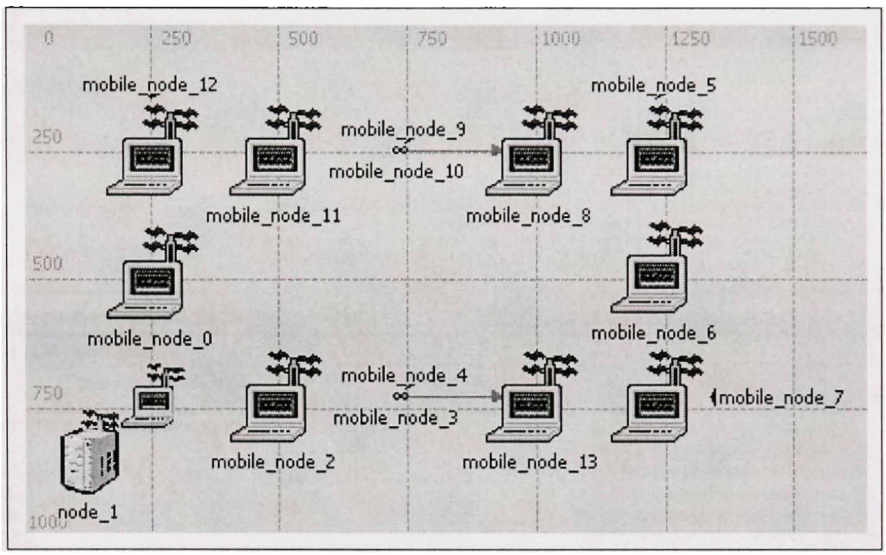


Figure 5.10 Scénario de test mobile : suppression de route invalide.

La prédiction de temps de vie de route est la pire prédiction de temps de vie des liens qui constituent la route. La table de routage du nœud 5, Figure 5.11, montre que la route vers le serveur à un complément de temps de vie de route de 9224 donc un RET de 77,5sec = 999,9 – 922,4. Ce temps de vie de route représente aussi le temps de vie du lien entre le nœud 10 et le nœud 9, illustré dans la table de routage du nœud 9 (Figure 5.12).

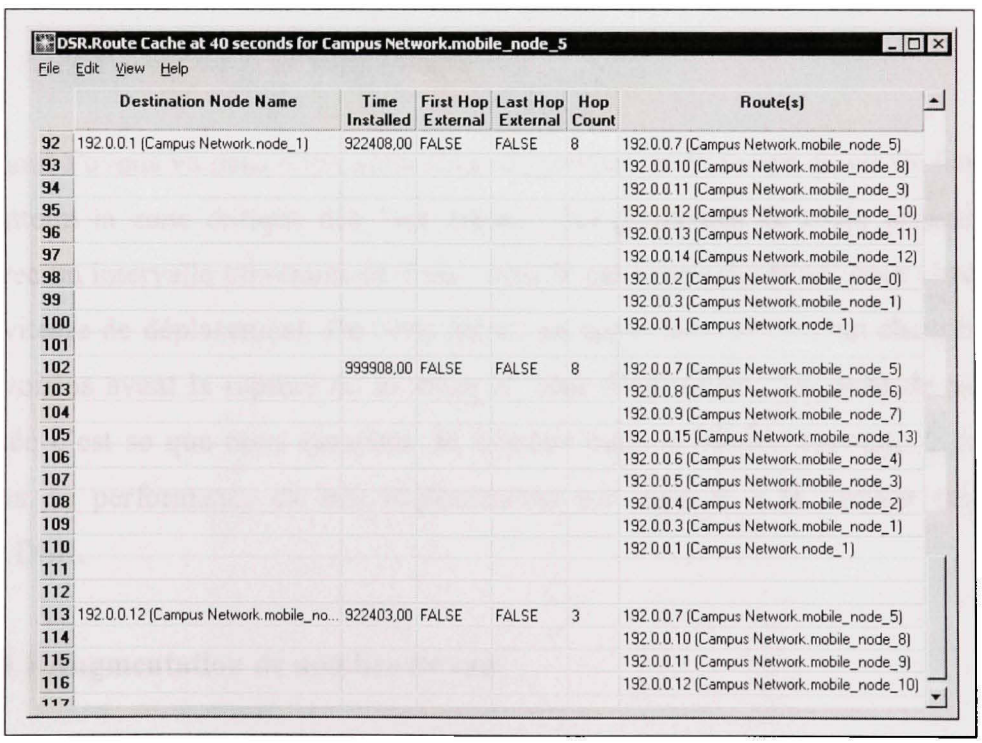
La deuxième route vers le serveur n'a pas d'estimation puisqu'il n'y a pas eu assez de paquets, d'échantillons, qui ont transigé par ce chemin pour pouvoir calculer la prédiction de temps de vie toute au long de la route. Cette route sera donc supprimée après 30sec de survie dans le cache du nœud 5.

La table de routage du nœud 9, Figure 5.12, nous permet de constater deux différentes valeurs de temps de vie de lien.

Ces valeurs dépendent du déplacement du nœud 9 entre les nœuds 8 et 10. Ainsi, quand le nœud 9 s'approche du nœud 8 le temps de vie de ce lien (9 - 8) sera plus long qu'en s'éloignant du nœud 10. Le détail de calcul pour extraire le temps de vie de lien est présenté ci-dessous.

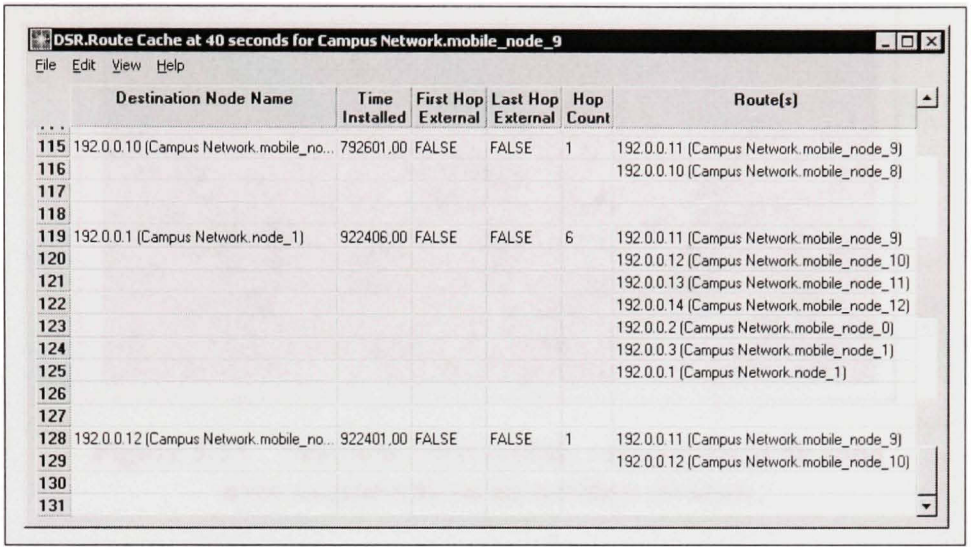
Le temps de vie du lien entre le nœud 9 et 8 : 999,9 – 792.6 = 207,3 sec dans le cas de GPS mais dans le cas d'utilisation de puissance de signal ça sera 999,9 sec puisque l'approche ne permet pas de calculer une prédiction avec cet algorithme.

Le temps de vie du lien entre le nœud 9 et 10 : 999,9 – 922,4 = 77,5 sec avec les deux algorithmes.



	Destination Node Name	Time Installed	First Hop External	Last Hop External	Hop Count	Route(s)
92	192.0.0.1 (Campus Network.node_1)	922408,00	FALSE	FALSE	8	192.0.0.7 (Campus Network.mobile_node_5)
93						192.0.0.10 (Campus Network.mobile_node_8)
94						192.0.0.11 (Campus Network.mobile_node_9)
95						192.0.0.12 (Campus Network.mobile_node_10)
96						192.0.0.13 (Campus Network.mobile_node_11)
97						192.0.0.14 (Campus Network.mobile_node_12)
98						192.0.0.2 (Campus Network.mobile_node_0)
99						192.0.0.3 (Campus Network.mobile_node_1)
100						192.0.0.1 (Campus Network.node_1)
101						
102		999908,00	FALSE	FALSE	8	192.0.0.7 (Campus Network.mobile_node_5)
103						192.0.0.8 (Campus Network.mobile_node_6)
104						192.0.0.9 (Campus Network.mobile_node_7)
105						192.0.0.15 (Campus Network.mobile_node_13)
106						192.0.0.6 (Campus Network.mobile_node_4)
107						192.0.0.5 (Campus Network.mobile_node_3)
108						192.0.0.4 (Campus Network.mobile_node_2)
109						192.0.0.3 (Campus Network.mobile_node_1)
110						192.0.0.1 (Campus Network.node_1)
111						
112						
113	192.0.0.12 (Campus Network.mobile_no...	922403,00	FALSE	FALSE	3	192.0.0.7 (Campus Network.mobile_node_5)
114						192.0.0.10 (Campus Network.mobile_node_8)
115						192.0.0.11 (Campus Network.mobile_node_9)
116						192.0.0.12 (Campus Network.mobile_node_10)

Figure 5.11 Table de routage du nœud 5 à t=40sec en utilisant DSR-RET.



DSR.Route Cache at 40 seconds for Campus Network.mobile_node_9

File Edit View Help

	Destination Node Name	Time Installed	First Hop External	Last Hop External	Hop Count	Route(s)
...						
115	192.0.0.10 (Campus Network.mobile_no...	792601,00	FALSE	FALSE	1	192.0.0.11 (Campus Network.mobile_node_9)
116						192.0.0.10 (Campus Network.mobile_node_8)
117						
118						
119	192.0.0.1 (Campus Network.node_1)	922406,00	FALSE	FALSE	6	192.0.0.11 (Campus Network.mobile_node_9)
120						192.0.0.12 (Campus Network.mobile_node_10)
121						192.0.0.13 (Campus Network.mobile_node_11)
122						192.0.0.14 (Campus Network.mobile_node_12)
123						192.0.0.2 (Campus Network.mobile_node_0)
124						192.0.0.3 (Campus Network.mobile_node_1)
125						192.0.0.1 (Campus Network.node_1)
126						
127						
128	192.0.0.12 (Campus Network.mobile_no...	922401,00	FALSE	FALSE	1	192.0.0.11 (Campus Network.mobile_node_9)
129						192.0.0.12 (Campus Network.mobile_node_10)
130						
131						

Figure 5.12 Table de routage du nœud 9 à t=40sec en utilisant DSR-RET.

5.2.2 Avec changement de zone (*handover*)

Comme nous l'avons vu dans notre algorithme de prédiction de temps de vie de lien, dés que le RET atteint la zone critique des 5sec restant, des demandes de route proactive seront émises avec un intervalle minimum de T sec, calculé par la couche MAC pour chaque voisin selon sa vitesse de déplacement. De cette façon, un nœud peut trouver un chemin à travers d'autres voisins avant la rupture de la route en cour d'utilisation. La perte de paquet sera donc évitée c'est se que nous essayons de montrer dans la section suivante avec d'autres indicateurs de performance de nos implantations par rapport à la version originale du protocole DSR.

5.2.2.1 Augmentation de nombre de saut

Dans le scénario de la Figure 5.13, le nœud 3 (mobile_node_3) se déplace avec une vitesse constante de 3m/s en commençant de la zone de couverture du nœud voisin vers la zone d'un autre voisin avec la direction illustrée. Nous voulons voir la réaction des différentes variantes du protocole dans ce cas.

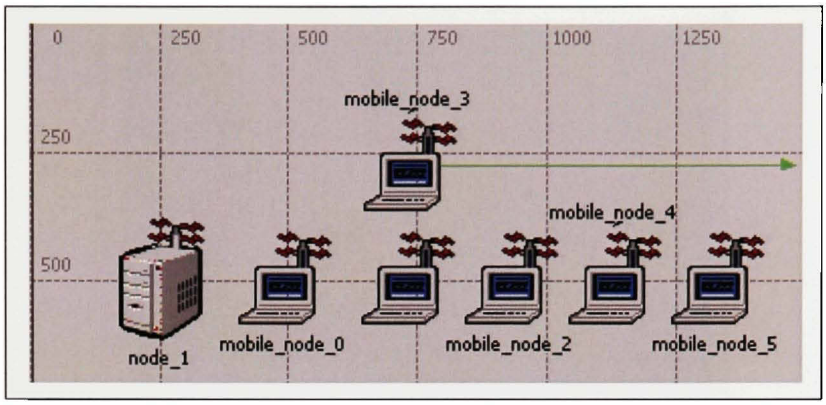


Figure 5.13 Scénario DSR mobile : changement de zone avec augmentation de nombre de saut.

Au moment du changement de zone nous remarquons une explosion du trafic de routage envoyé et reçu avec la version originale de DSR illustré dans la Figure 5.14 et la Figure 5.15 respectivement. Alors qu'avec DSR-RET le trafic de routage n'a pas été influencé par aucun changement de zone (*handover*).

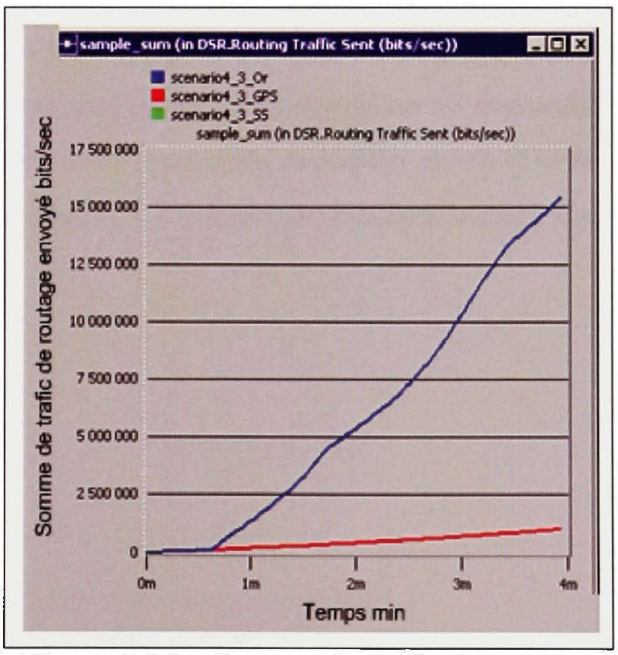


Figure 5.14 Somme de trafic de routage envoyé dans le réseau.

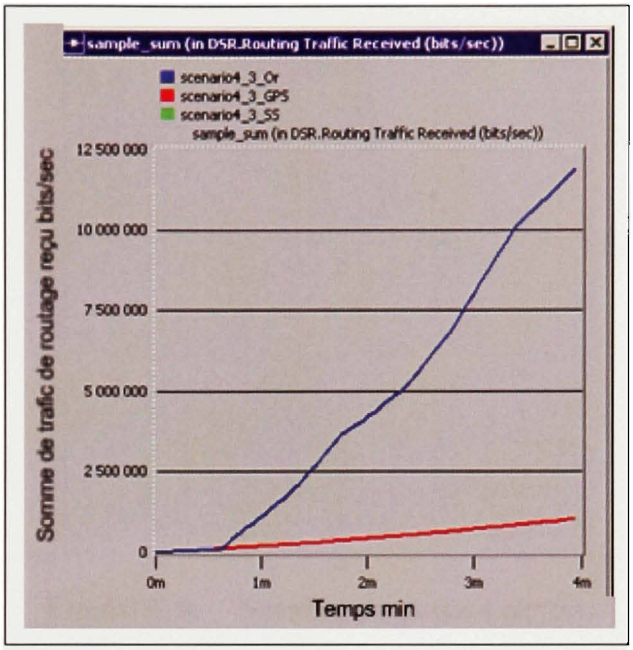


Figure 5.15 Somme de trafic de routage reçu dans le réseau.

Une perte de paquet a été constatée pour la version originale de DSR (Figure 5.16) alors qu'il n'y a pas eu de perte dans les versions modifiées. Nous constatons que la version originale de DSR à réussi de sauvé des paquets en les envoyant sur de nouvelles routes. Ce nombre peut être déduit de la différence entre le nombre de paquets perdu et le nombre d'erreurs de routes envoyées par les nœuds (Figure 5.17) à chaque fois que la route inscrite dans le paquet n.est plus valide.

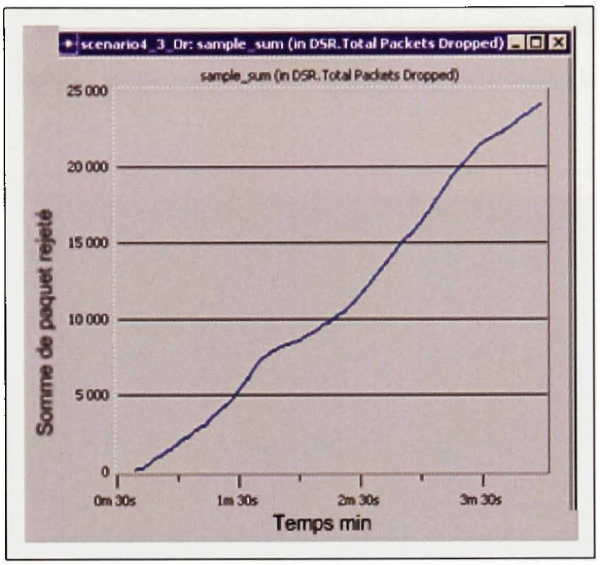


Figure 5.16 Nombre de paquet perdu.

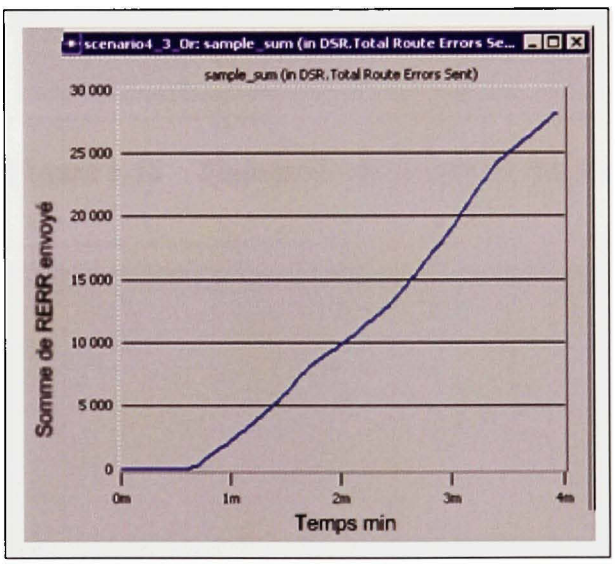


Figure 5.17 Nombre de notification de route erreur.

La Figure 5.18 et la Figure 5.19 illustrent une augmentation quasi linéaire des nombres de demandes de routes et de réponses de route respectivement à partir du premier changement de zone en utilisant la version originale de DSR alors que les variantes de DSR-RET n'ont quasiment pas consommé de bande passante pour cette fin.

Nous remarquons que les variantes basées sur notre implantation réagissent plus rapidement en ayant des réponses de routes plus rapidement que la version originale du protocole.

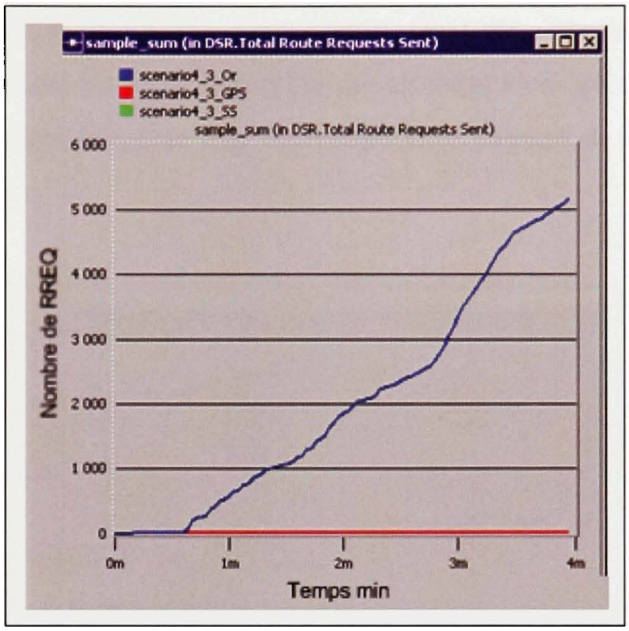


Figure 5.18 Somme de demande de route.

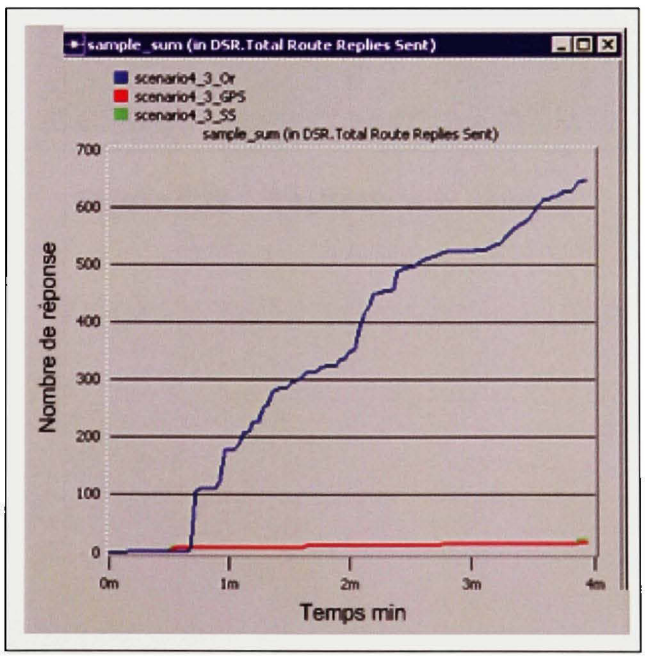


Figure 5.19 Somme de réponse de route.

Le trafic de voix envoyé dans le réseau pour les différentes variantes de DSR est illustré dans la Figure 5.20.

La Figure 5.21 montre qu'à chaque changement de zone, les paquets de voix reçues diminuent et arrivent même à s'annuler pendant un moment alors qu'avec notre implantation le protocole DSR maintient le même taux de réception de paquets de voix même au moment de changement de zone.

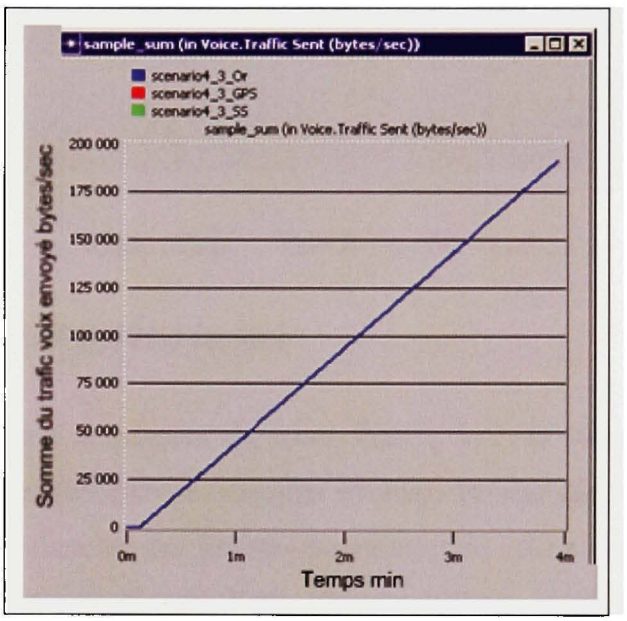


Figure 5.20 Trafic de voix envoyé.

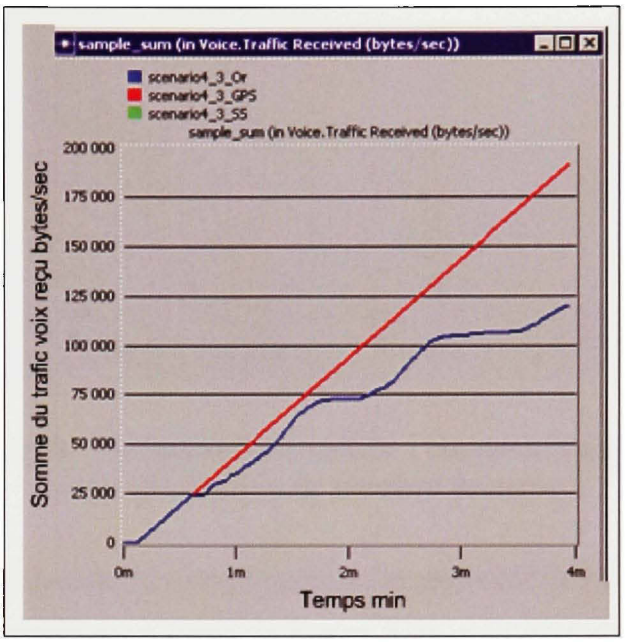


Figure 5.21 Trafic de voix reçu.

5.2.2.2 Diminution de nombre de saut

Dans le cas de diminution de nombre de sauts, Figure 5.22, la version DSR-RET est plus rapide à prendre en considération le nouveau chemin. Puisqu'une fonction au niveau du cache a été ajoutée pour chercher des liaisons possibles d'un voisin nouvellement connu avec d'autres destinations sans avoir besoin d'attendre une réponse gratuite (proactive) venant de ce nœud et sans même avoir besoin de faire d'autre demande de route.

Dans ce scénario, Figure 5.22, le nœud 3 (mobile_node_3) se déplace avec une vitesse de 3m/s permettant la diminution de nombre de sauts en changeant de zone.

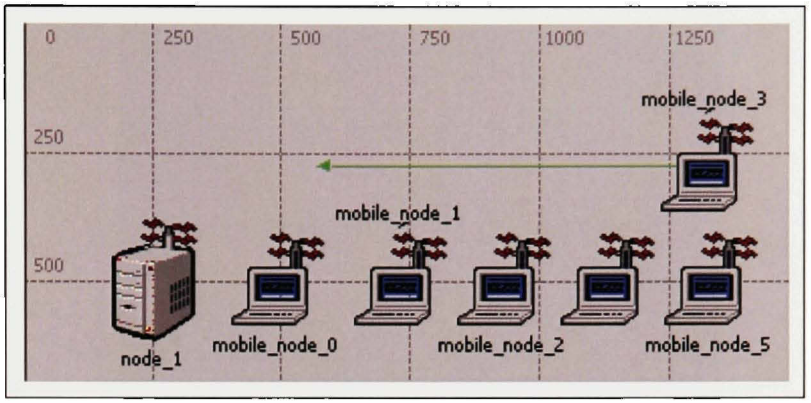


Figure 5.22 Scénario DSR mobile : changement de zone avec diminution de nombre de saut.

Comme nous l'avons vu dans la section précédente, le protocole original n'arrive pas à suivre la vitesse de changement de zone. Ainsi la Figure 5.23 et la Figure 5.24 respectivement le trafic de routage envoyé et reçu dans le réseau, permet de constater une augmentation phénoménale du trafic de routage en utilisant la version originale de DSR alors que les variantes de notre implantation montrent une augmentation normale.

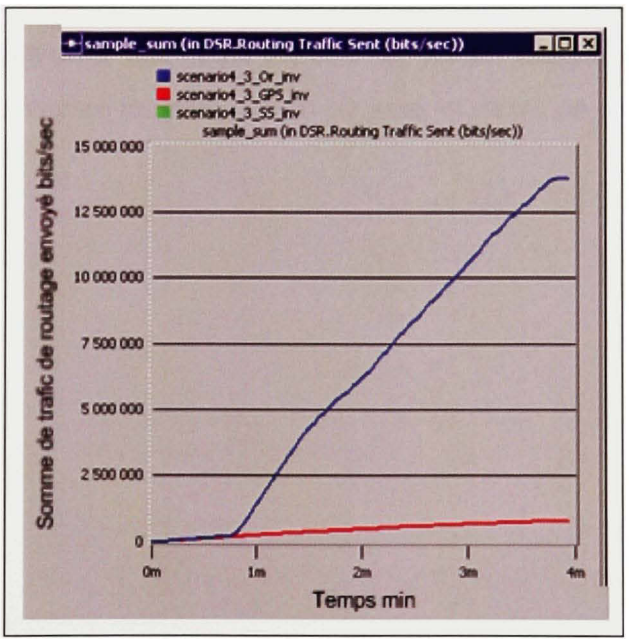


Figure 5.23 Somme du trafic de routage envoyé.

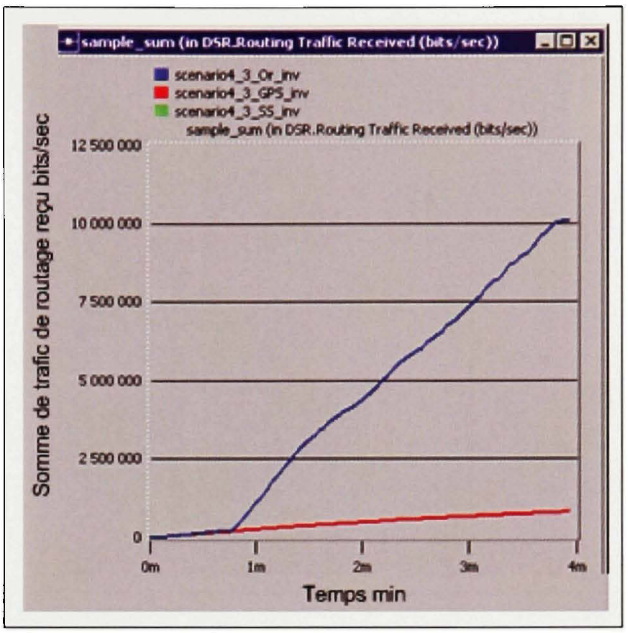


Figure 5.24 Trafic de routage reçu.

Le nombre de demandes de routes et de réponses des variantes de DSR sont illustrées respectivement à la Figure 5.25 et la Figure 5.26.

Nous pouvons constater que les variantes de notre implantation n'ont envoyé qu'une seule demande ce qui correspond à une seule réponse de route. Alors que la version originale n'arrive pas à suivre la vitesse de changement de zone et envoi de plus en plus de demande de route.

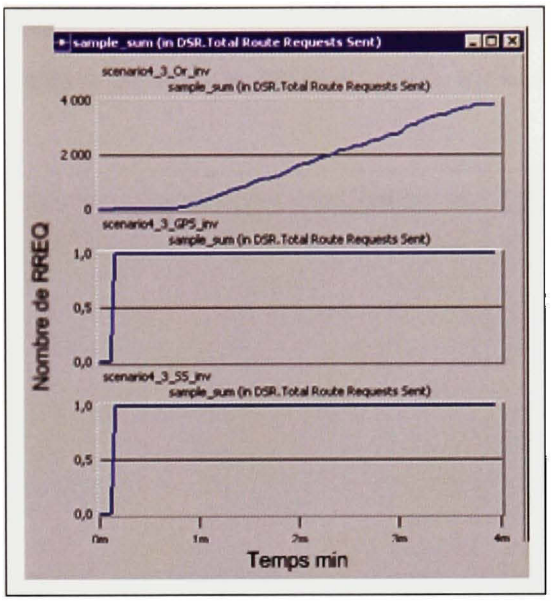


Figure 5.25 Nombre de demande de route des différentes variantes de DSR.

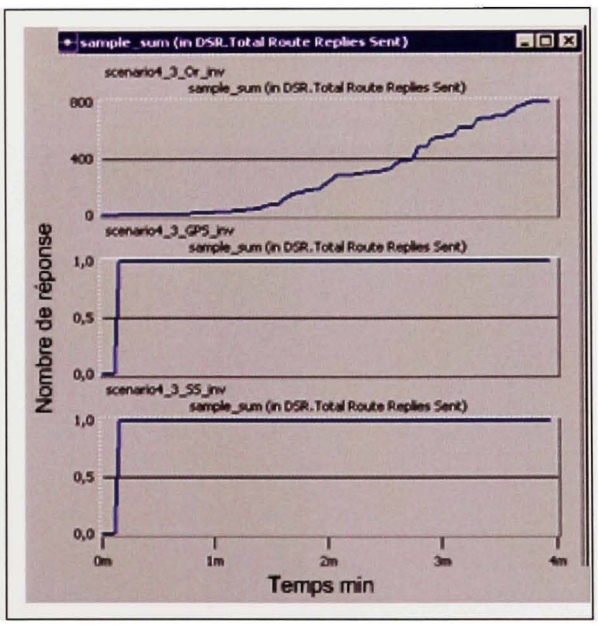


Figure 5.26 Nombre de réponse de route des différentes variantes de DSR.

La Figure 5.27 et la Figure 5.28 illustrent respectivement le trafic voix envoyé et reçu dans le réseau pour les différentes variantes de DSR.

La Figure 5.28 illustre le constat de l'avantage de l'implantation du temps de vie de lien dans le protocole DSR puisque ca nous permet de recevoir tout le trafic envoyé sans aucune perte.

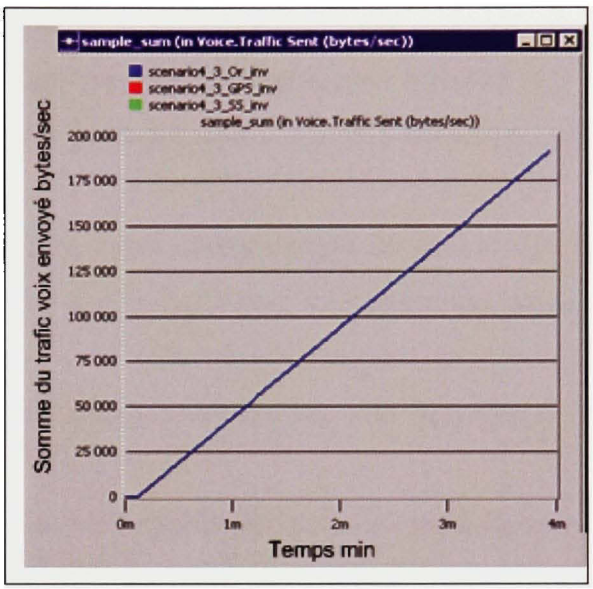


Figure 5.27 Trafic de voix envoyé.

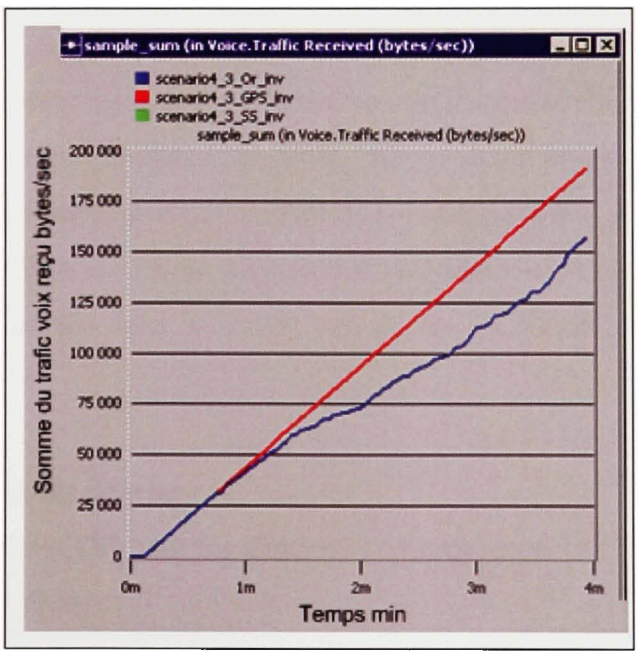


Figure 5.28 Trafic de voix reçu.

5.3 Test de production

Dans le but de montrer que notre modèle implémenté dans le protocole DSR augmente la performance de ce dernier, nous avons effectué une série de tests qui incluent plusieurs nœuds mobiles et fixes et qui sollicitent le réseau pour effectuer une communication à travers un serveur ou une passerelle de sortie, afin d'arriver à simuler un environnement plus proche de la réalité.

Dans notre scénario de base, nous avons intégré 20 nœuds (15 nœuds fixes et 5 nœuds mobiles) et un serveur fixe, Figure 5.29 avec une couverture du terrain de 1400m x 300m. Dans la première itération du test, nous utilisons un seul nœud mobile, Figure 5.30.

Les nœuds mobiles utilisent une application voix avec le codec G.729 pour communiquer à travers le serveur.

Un nœud qui a le droit d'utiliser l'application voix débute la communication à partir de 12sec jusqu'à la fin de la simulation. Le début de communication de chaque nœud qui suit est espacé de 2 secondes. La durée de chaque simulation est 4 minutes.

Les trajectoires des nœuds mobiles ont été créées par le modèle aléatoire d'OPNET (*Random Waypoint model*) en variant la vitesse sans temps de pause.

Nous avons essayé à travers les tests de cette section de comparer les performances du réseau en utilisant les différentes variantes de DSR. Ainsi, nous avons sollicité le réseau en augmentant la charge en augmentant le nombre de sources possibles passant progressivement de la Figure 5.30 à la Figure 5.29, en augmentant le nombre de nœuds dans le réseau et en variant la vitesse des nœuds dans le réseau tout en les conservant constantes au cours du même scénario.

Spécifications des scénarios de tests

- Temps de réaction (TR) pour les demandes de route proactive : 5 secondes
- 20 nœuds + 1 serveur
- Maximum 5appels voix
- Étendu de la zone de test : 1400m x 300m

- Le modèle de mobilité est *Random Waypoint* sans temps de pause
- Le codec de voix utilisé est G729
- Le déclenchement d'appel est à partir de 12 secondes jusqu'à la fin de la simulation espacé de 2 secondes pour le début des appels suivants
- Variation de la charge : de 1 à 5 sources
- Variation de la densité : de 21 à 31 nœuds
- Variation de la vitesse : de 3,6 à 36km/h

Spécifications des nœuds ad hoc utilisés

- Rayon de couverture radio de 250métres
- Puissance de transmission constante de 0,005W
- Couche MAC basée sur le 802.11 en mode DCF
- Taux de transfert de la couche MAC est de 2Mbps

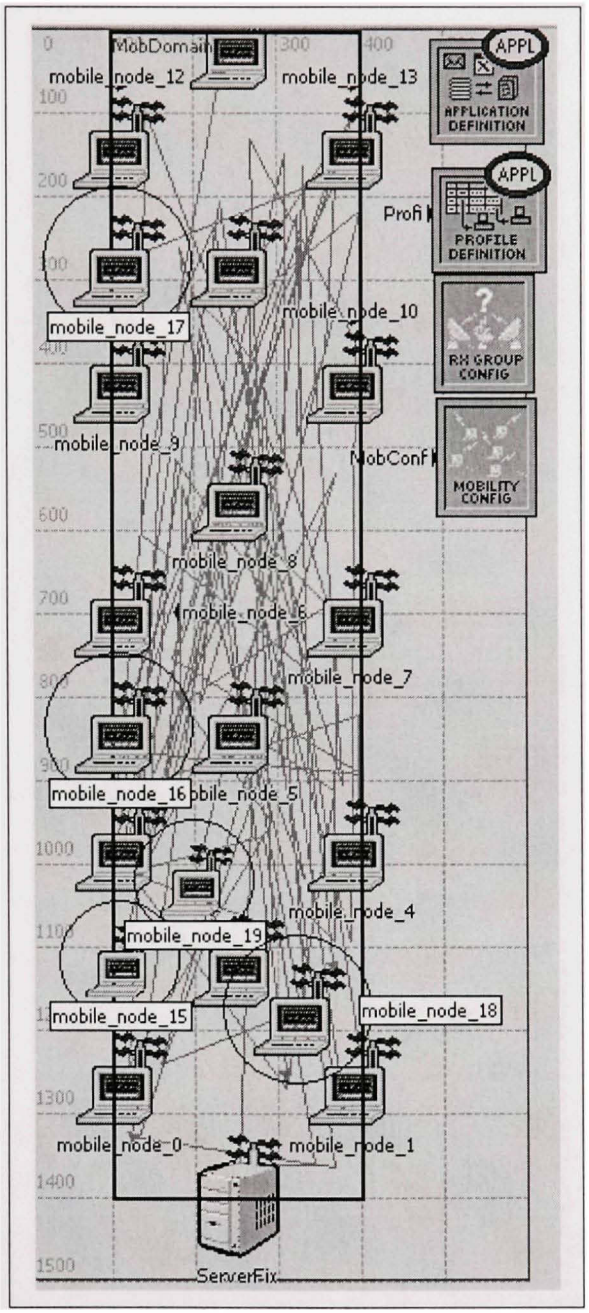


Figure 5.29 Scénario de test pour mesurer la performance de DSR avec 5 sources mobiles.

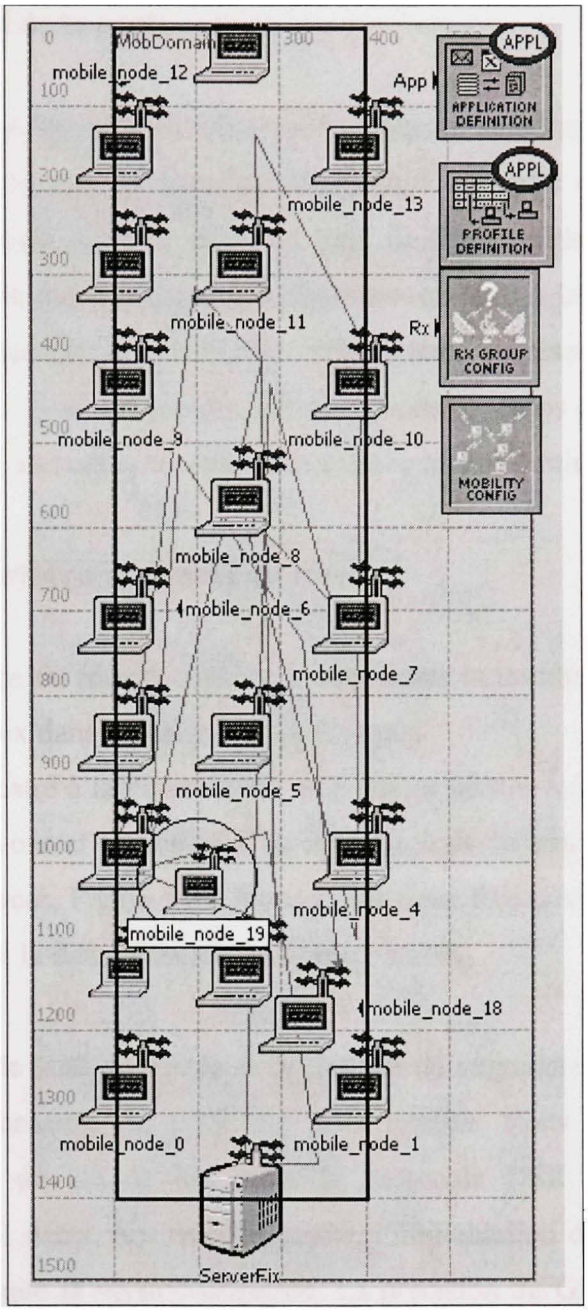


Figure 5.30 Scénario de test pour mesurer la performance de DSR avec une source mobile.

5.3.1 Paramètre clé de la performance

Dans notre étude, nous avons considéré le taux de livraison de donnée comme paramètre clé de performance du réseau qui est constitué du rapport du trafic reçu divisé par le trafic envoyé dans tout le réseau. Ainsi en ayant un taux de livraison de donnée plus proche de maximum (1) le plus part des autres paramètres seront affectés à la hausse. Prenant comme exemple le cas d'une application voix (UDP) utilisée dans un réseau ad hoc. Si le taux de livraison de donnée est à 1 ou très proche de cette valeur, le temps de livraison pourrait être aussi performant pour ne pas entrainer des rejets et donc ne pas diminuer le taux de livraison.

5.3.2 Effet de la variation de charge du réseau

La variation de la charge du réseau consiste à augmenter le nombre de nœuds mobiles qui utilisent l'application voix dans le réseau de 1 à 5 nœuds.
À partir du scénario, illustré à la Figure 5.30, nous avons permis a de plus en plus de nœuds d'utiliser l'application voix et se déplacer en même temps au cours de la simulation pour arrivé à l'ajout de 5 sources, Figure 5.29. Nous avons donc fixé la vitesse de déplacement de tous les nœuds à 2 m/s et la densité du réseau à rester stable.

La Figure 5.31 illustre le taux de livraison de donnée en augmentant le nombre de sources pour les différentes variantes de DSR qui sont testées. Nous pouvons constater que l'intégration de temps de vie de lien dans le protocole DSR permet d'augmenter la performance de celui-ci. Ainsi, nos trois variantes d'implantation donnent un meilleur taux de livraison de donnée que la version originale. La précision du GPS lui offre un avantage avec une et deux sources; par la suite la méthode de puissance de signal prend l'avantage avec trois et quatre sources à cause de l'interférence croissante avec l'augmentation de sources.

La variante utilisant les deux méthodes de prédiction n'est pas aussi stable que nous croyons puisque les deux méthodes utilisées ne donnent pas une prédiction de temps de vie en même temps et le fait de prendre toujours le minimum des deux prédictions augmente le nombre de demandes de route ce qui gaspille la bande passante.

Le temps de réaction pour la zone de préemption à une grande influence, en effet en utilisant un temps de réaction de 5,5 sec avec 2 sources les deux résultats des deux méthodes de prédiction seront optimaux.

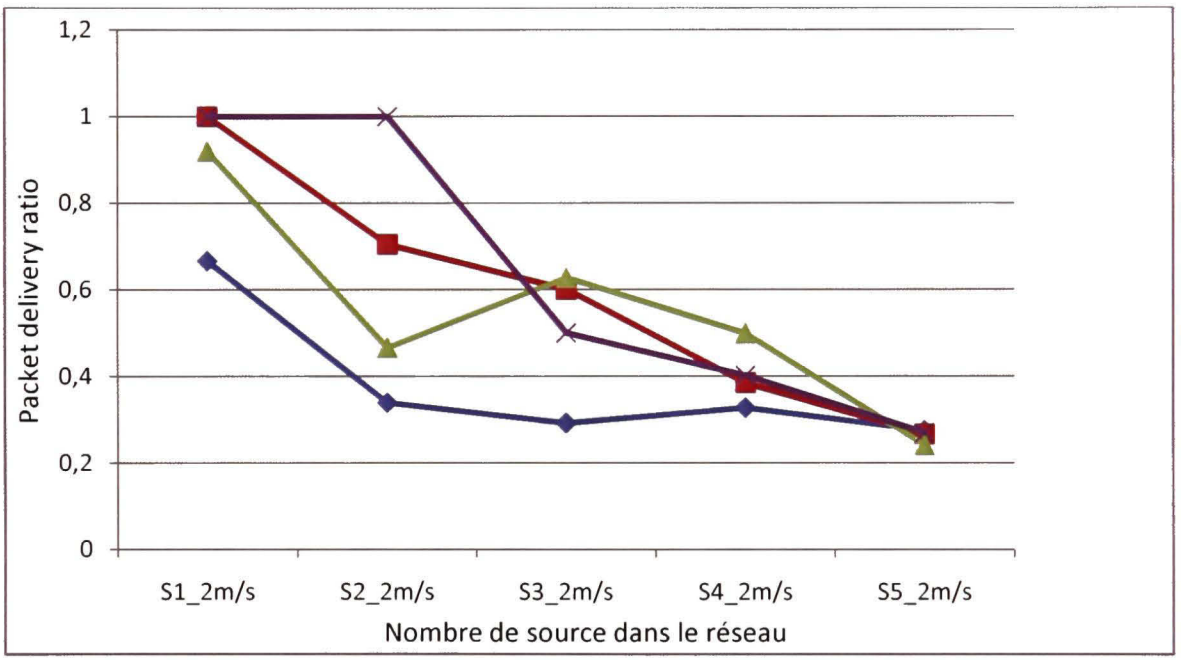


Figure 5.31 Taux de livraison de donnée avec l'augmentation de la charge du réseau.

5.3.3 Effet de la variation de la densité du réseau

La variation de la densité de réseau consiste à augmenter le nombre des nœuds fixes et mobiles dans la même surface de test qui est de 1400m x 300m.

À partir du scénario, illustré à la Figure 5.30, nous avons ajouté des nœuds dans le réseau jusqu'à concurrence de 10. Nous avons donc fixé la vitesse à 2 et 3m/s et le nombre de sources à 1.

Une performance optimale est illustrée à la Figure 5.32, à travers le taux de livraison de donnée avec l'augmentation de nombre de nœud dans le réseau, de nos variantes d'implémentation par rapport à la version originale de DSR. Il semble que la valeur de 5sec de la zone de préemption et la vitesse à 2m/s permet d'atteindre une performance et efficacité élevée.

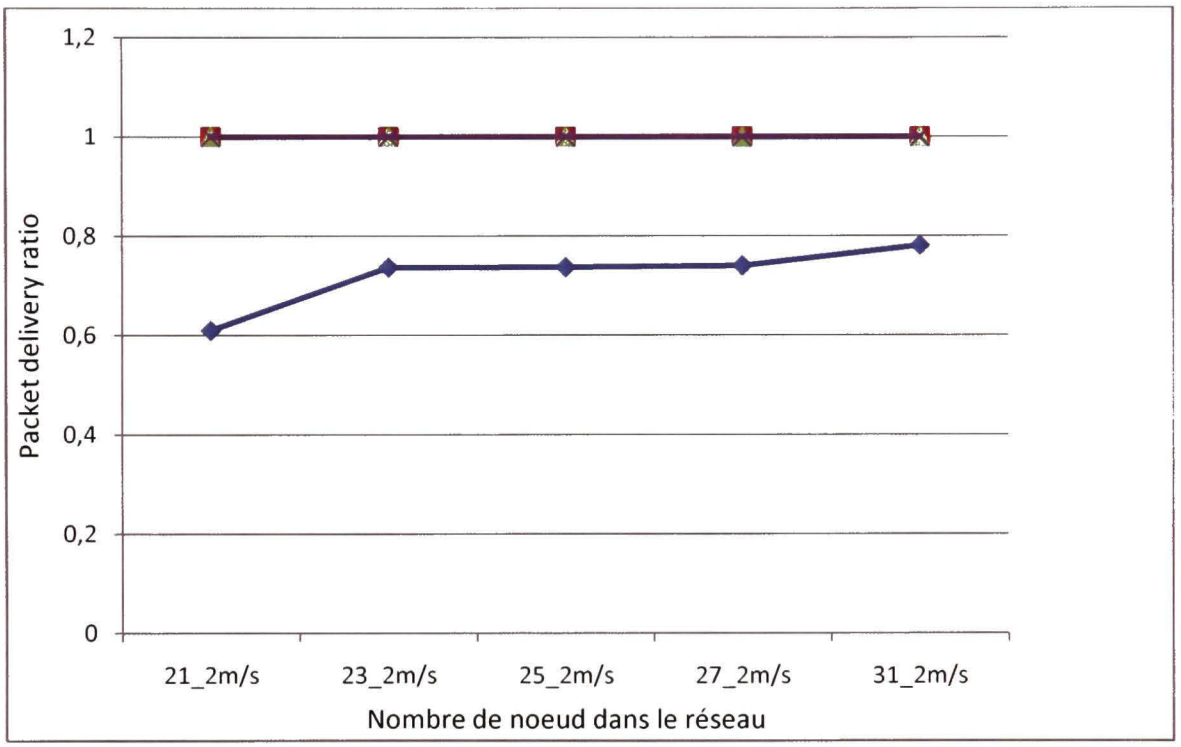


Figure 5.32 Taux de livraison de donnée avec l'augmentation de la densité du réseau à 2m/s.

Nous avons repris les mêmes tests précédents, mais avec une vitesse de 3m/s cette fois-ci. La Figure 5.33 présente les résultats de nos tests. Nous constatons encore que nos variantes d'implantation donnent une meilleure performance que la version originale du protocole. Ainsi, la majorité des points se trouve dans la partie supérieure à 90%. Nous remarquons qu'à partir de 25 nœuds dans le réseau la performance de celui-ci s'améliore.

La dégradation de performance peut être corrigée par un bon calibrage du temps de réaction pour la zone de préemption ainsi avec 23 nœuds et en considérant un temps de réaction de 7,9sec nous pouvons avoir une performance optimale pour nos différentes variantes.

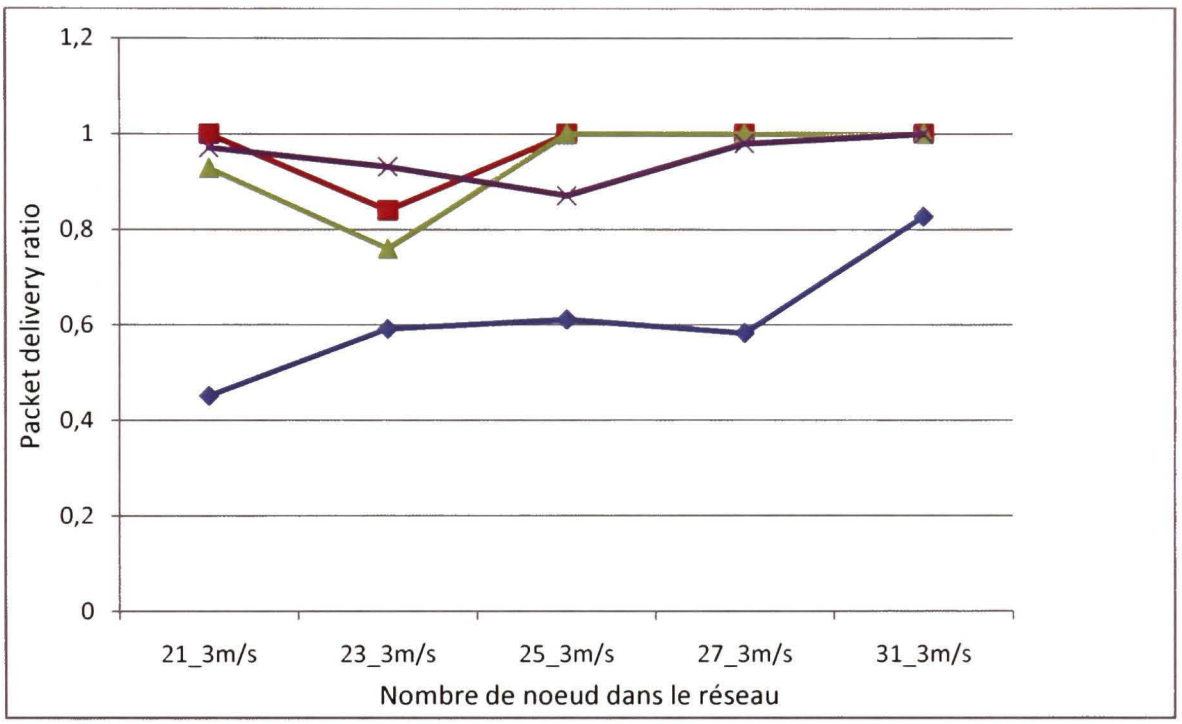


Figure 5.33 Taux de livraison de donnée avec l'augmentation de la densité du réseau à 3m/s.

5.3.4 Effet de la variation de la vitesse des nœuds

Pour mesurer l'effet de la variation de la vitesse de déplacement dans les réseaux ad hoc, nous avons augmenté la vitesse de 1m/s à 10m/s correspondant à 3,6k/h et 36km/h.

Commençant par le scénario, illustré à la Figure 5.30, nous avons augmenté la vitesse du nœud mobile tout en gardant la densité (21 nœuds) et le nombre de source (1 source) constants.

En analysant la Figure 5.34, nous constatons que nos différentes variantes permettent au réseau de donner une meilleure performance que le protocole DSR original. En effet la méthode basée sur le GPS ne semble pas affectée par la vitesse des nœuds et permet de donner une performance optimale avec toutes les valeurs de vitesse testées.

Alors que la méthode de prédiction basée sur la puissance de signal enregistre quelque perturbation à cause de la lenteur de l'évaluation de la prédiction et le calibrage du temps de réaction pour la zone de préemption qui permet de corriger cette lacune.

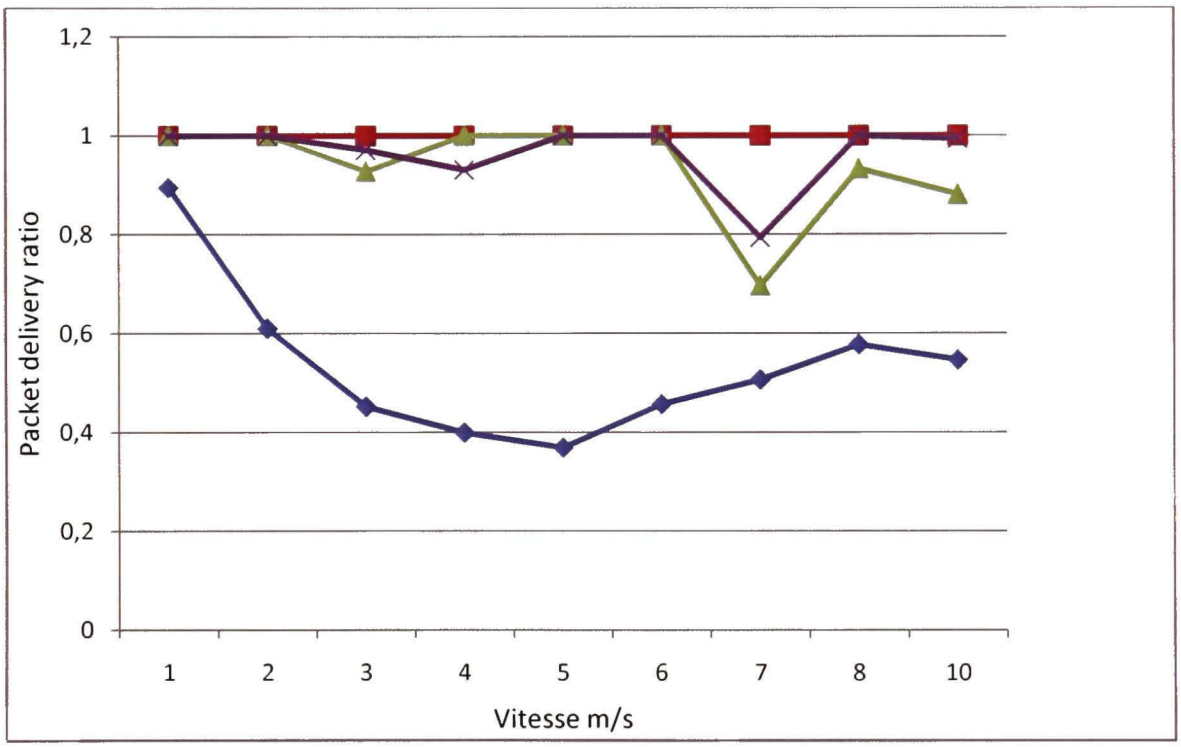


Figure 5.34 Taux de livraison de donnée avec l'augmentation de la vitesse.

Nous présentons dans la Figure 5.35 les valeurs de TR optimaux (défini dans 4.5.4) pour différentes valeurs de vitesse et avec une source et 21 nœuds dans le réseau. Ces paramètres permettent d'utiliser les demandes de route proactives au minimum diminuant ainsi le trafic de routage. La figure 5.36 montre les performances du réseau en appliquant les temps de réaction optimaux à leur vitesse correspondante.

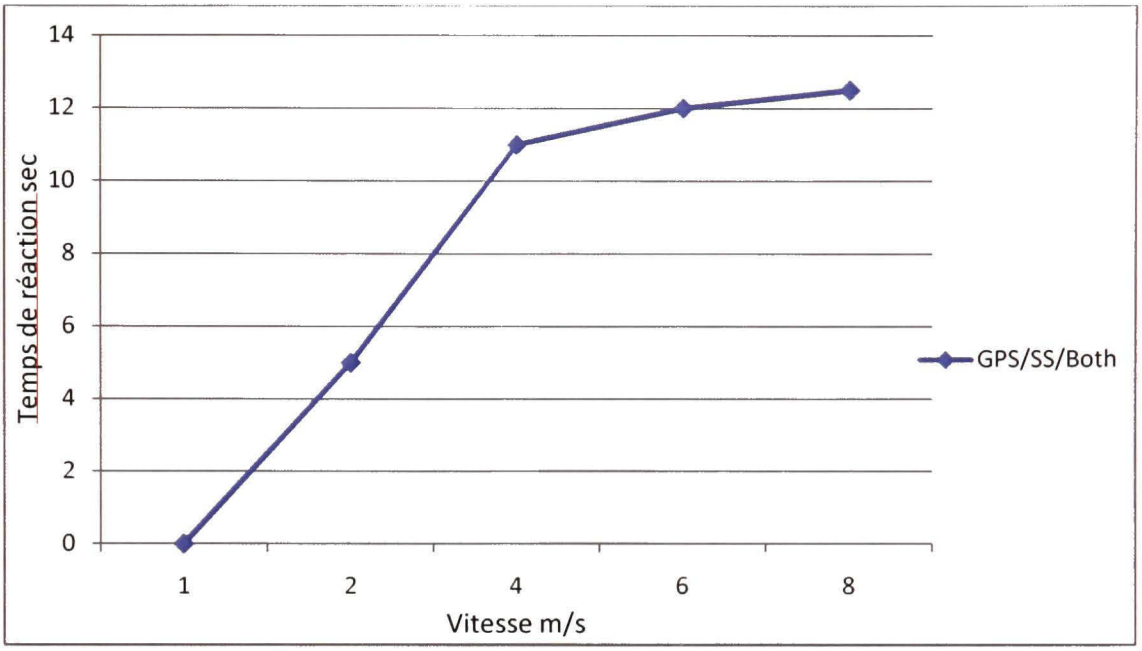


Figure 5.35 Temps de réaction optimum pour 1 source et 21 nœuds dans le réseau.

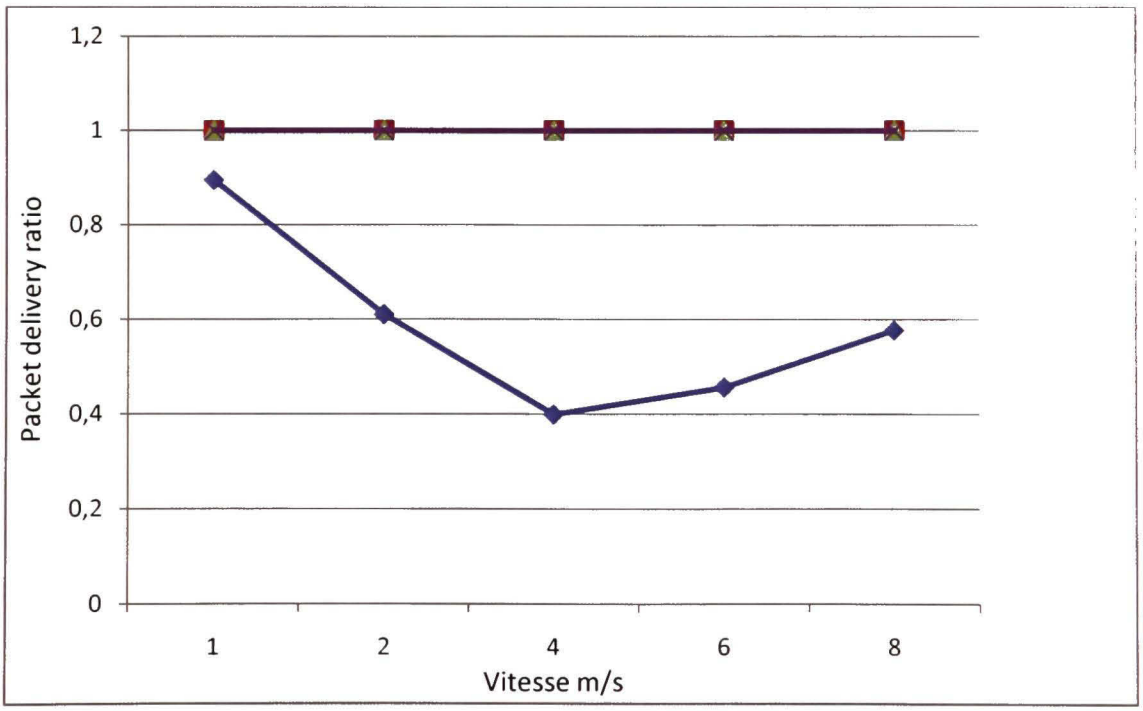


Figure 5.36 Taux de livraison de données avec différentes vitesses et les temps de réaction optimisés correspondant pour les différentes variantes de DSR.

Voyant un exemple d'utilisation du temps de réaction optimal avec la méthode de prédiction de temps de vie de lien qui utilise la puissance de signal et avec une vitesse de déplacement de 8m/s.

Les trois variantes que nous allons comparer sont les suivants :

- DSR originale
- DSR intégrant la prédiction de LET avec un temps de réaction de 5 sec
- DSR intégrant la prédiction de LET avec un temps de réaction de 11 sec

En analysant la figure 5.37, nous remarquons que les trois variantes envoient la même quantité de données dans le réseau. Alors que la figure 5.38 montre que seule la version utilisant un temps de réaction de 11sec arrive à recevoir toutes les données transmises.

La figure 5.39 montre que même si nous arrivons à une bonne performance, il peut y avoir du gaspillage de la bande passante. En effet la méthode de prédiction de LET avec un temps de réaction de 5 sec émet plus de trafic de routage que la version originale de DSR qui a un taux de livraison de donnée plus faible.

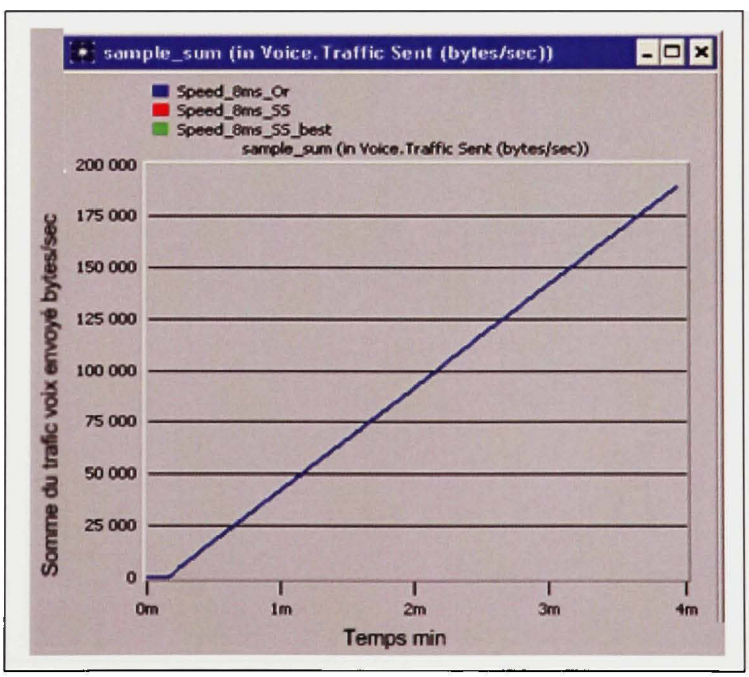


Figure 5.37 Somme de trafic de voix envoyé pour trois variantes de DSR.

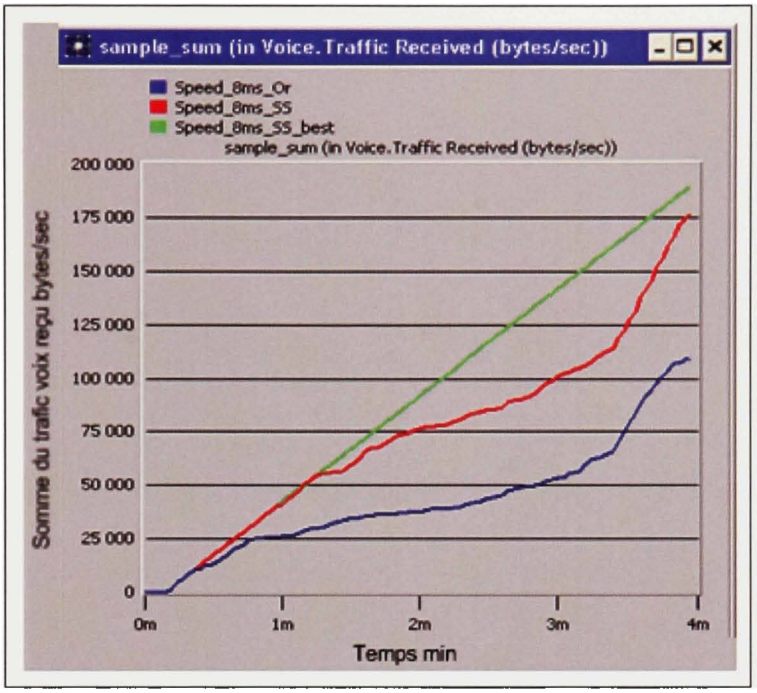


Figure 5.38 Somme de trafic de voix reçu pour trois variantes de DSR.

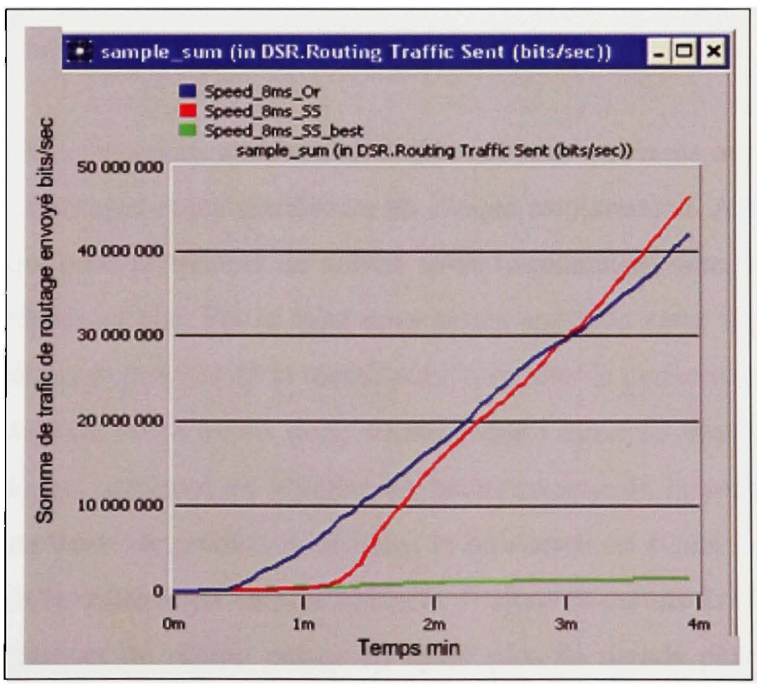


Figure 5.39 Somme de trafic de routage envoyé pour trois variantes de DSR.

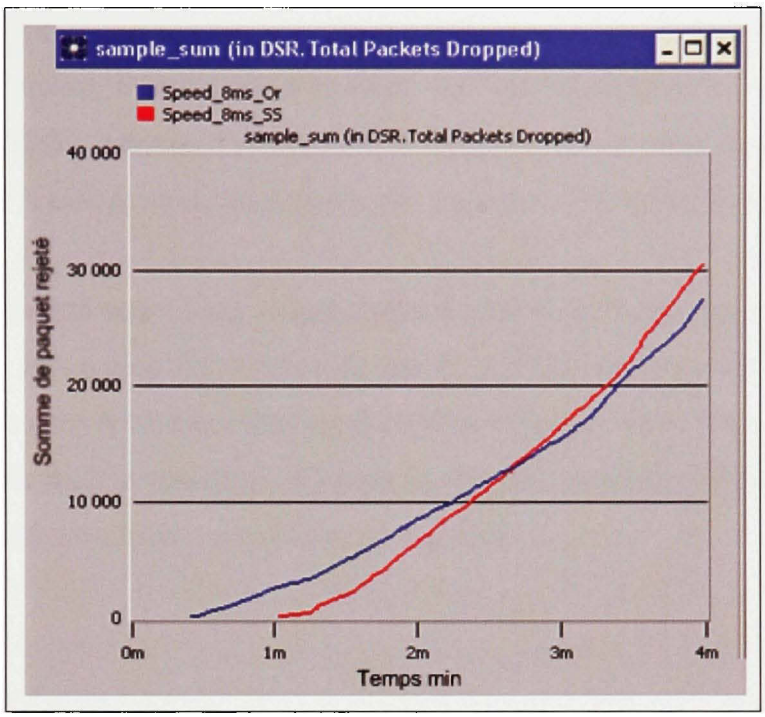


Figure 5.40 Somme de paquet perdu pour deux variantes de DSR.

5.4 Synthèse et conclusion

Nous avons présenté à travers ce chapitre les différents tests que nous avons effectués pour pouvoir cerner les avantages et inconvenances de chaque implantation. Ainsi, nous avons vu les tests unitaires qui nous permettent de valider notre implantation dans la majorité des cas possible dans un réseau ad hoc. Par la suite nous avons appliqué notre implantation sur des scénarios plus généraux et proches de la réalité pour comparer la performance du réseau avec différentes implantations. Nous avons donc constaté que l'ajout de sources peut engendrer plus d'interférences qui affectent en premier les performances de la prédiction utilisant le GPS alors que la méthode de prédiction utilisant la puissance de signal arrive à contourner cette interférence en la considérant comme obstacle. L'ajout de nœuds dans le réseau un effet plus ou moins perturbant du réseau puisqu'en ayant plus de nœuds plus de problèmes de stations cachées et exposées seront présent dans le réseau donc plus de contention en plus du problème de calibrage du temps de réaction pour la zone de préemption.

Enfin, nous avons vu la performance du réseau en augmentant la vitesse pour les différentes variantes d'implantation. Et nous avons constaté que la performance du réseau, en utilisant nos variantes de DSR, permet d'augmenter sa performance et surtout, en choisissant le meilleur temps de réaction, un nœud peut trouver une route alternative avant la rupture de la route courante.

À travers les différents tests, nous avons constaté que le calibrage du temps de réaction nécessite la prise en compte du nombre de nœuds voisins, des vitesses des nœuds et du nombre de sources dans le réseau. Ainsi en ayant plus de nœuds voisins qui sont susceptibles de prendre la parole dans le voisinage, le temps de réaction risque de grandir et le sera plus si un nœud intermédiaire ou final a une vitesse plus grande.

CONCLUSION

Beaucoup d'études faites dans le domaine des réseaux ad hoc se focalisent sur la possibilité d'intégration de la qualité de service dans un réseau complètement décentralisé, pour répondre a ce besoin des propositions de nouvelles architectures ont été faites, parmi elles on peut citer l'utilisation des clusters et des dorsales sans oublier la coopération entre les couches (cross layer).

Cependant, en général ces approches sont inapplicables pour tout environnement à cause de la variation de la qualité des liens entre les nœuds dans ce type de réseau, due d'une part aux mouvements des nœuds et d'autre part aux changements de l'environnement qui les entoure. En faite la variation de la qualité de liens et les ruptures fréquentes causent des problèmes au niveau de la couche MAC, ajoute de la complexité à la conception du protocole du routage, de la construction et maintenance de clusters et dorsales. Rappelons que l'approche classique ne permet pas de devancer la rupture des liens; ainsi, l'application d'une nouvelle approche basée sur la prédiction de temps de vie de lien sera un bon apport pour les différents protocoles des différentes couches. En appliquant cette approche, les performances des réseaux ad hoc seront certainement meilleures.

Plusieurs approches de prédiction de temps de vie de lien ont été élaborées. Dans notre recherche nous avons choisi deux méthodes de prédiction. La première consiste à tirer avantage de la dernière technologie sur le marché, le GPS. Alors que la deuxième méthode n'utilise pas de nouvelles composantes permettant ainsi aux anciens appareils de bénéficier de prédiction de temps de vie de lien.

Notre travail consiste à l'intégration de temps de vie de lien dans le protocole de routage DSR et la modification de la couche MAC en se basant sur les deux méthodes de prédiction citée précédemment, afin d'instaurer la collaboration entre ces couches ce qui entraine l'augmentation de la performance du protocole de routage et la performance du réseau.

Dans le but d'avoir une méthode plus stable et conservatrice, nous avons élaboré une troisième méthode qui consiste à jumeler les deux méthodes précédemment citées.
Nous avons étendu notre cas d'étude aux utilisateurs plus rapides, dans une zone non sectorisée de plus notre approche se veut sans apriori sur le mouvement des nœuds. Enfin, nous considérons seulement le cas où les nœuds sont identiques et interchangeables (même caractéristique physique, rayon de couverture radio) du point de vue du réseau.

À la suite d'une batterie de tests effectués dans le dernier chapitre, nous avons constaté une nette amélioration de la performance du réseau qui se manifeste dans la supériorité du taux de livraison des données de nos différentes variantes du protocole DSR par rapport à la version originale. Ce qui appuie l'idée que l'intégration de temps de vie de lien dans les protocoles de routage permet d'augmenter la performance de celui-ci.

D'après nos différents points de comparaison entre les différentes variantes de DSR, nous avons constaté que la prédiction avec GPS souffre plus de l'interférence lorsque la densité du réseau et le nombre de sources sont élevés. Alors que la prédiction avec la puissance de signal permet de contourner la zone d'interférence en la considérant comme une zone accidentée ainsi cette dernière devance la performance de la méthode avec GPS dans les mêmes conditions.

Enfin, malgré l'augmentation substantielle de la performance du réseau avec l'intégration de temps de vie de lien, nous ne pouvons garantir ou s'approcher des performances optimales sans un bon calibrage du temps de réaction qui permet de déterminer la zone de préemption. Nous avons fixé le temps de réaction dans nos tests, mais une nouvelle recherche pourra effectuer ce travail en trouvant une méthode qui permet de le dynamiser en tenant compte de la densité du voisinage, le nombre de sources dans le réseau et les vitesses des nœuds qui participent à l'acheminement de l'information.

APPENDICE A

PROTOCOLE DE ROUTAGE BASÉ SUR L'ÉCHANGE DE TABLE

Les protocoles de routage dans cette section constituent une extension des protocoles de routage dans les réseaux filaires. Ces protocoles proactifs maintiennent l'information de la topologie complète du réseau dans une table au niveau de chaque nœud. Ces tables sont mises à jour périodiquement par un mécanisme d'échange d'information.

Destination Sequanced Distance-Vector (DSDV) utilise l'algorithme de Bellman Ford pour calculer le chemin le plus court à partir d'un nœud jusqu'à tout les autres et le premier nœud sur ce chemin. Chaque nouvelle table de mise à jour possède un numéro de séquence supérieur à l'ancien, si ce n'est pas le cas, la table sera ignorée. Si un lien est brisé, son numéro de séquence devient impair indiquant une valeur infinie et sera envoyé par le premier nœud qui découvre la rupture. Si le nouveau numéro de séquence est égal à l'ancien, la valeur de la distance la plus courte sera conservée. Le principal avantage de ce protocole de routage est l'application de numéro de séquence ce qui montre qu'un protocole de routage filaire peut être adéquat pour les réseaux sans fil ad hoc. Par contre, l'utilisation fréquente des mises à jour dans tout le réseau consomme beaucoup trop de bande passante ce qui diminue énormément la performance.
Le nombre excessif des messages de contrôle est proportionnel au nombre de nœud dans le réseau ce qui va à l'encontre de la mise à l'échelle. En plus, un nœud qui veut atteindre une destination doit attendre son annonce à ses voisins immédiats.
Wireless Routing Protocol (WRP) diffère par rapport à DSDV par la maintenance des tables et la procédure de mise à jour. Les différentes tables utilisées sont : Table de distance, Table de routage, Table de cout de lien et une liste de message retransmis. À l'aide de ces tables WRP arrive rapidement à une convergence en impliquant peu de mises à jour.
Mais la complexité de maintenance de plusieurs tables demande plus de mémoire et plus de puissance de calcul au nœud dans les réseaux sans fil ad hoc. Il est à noter que dans un milieu à haute mobilité le nombre de paquets de contrôle est le même que dans le protocole DSDV, ce qui diminue les chances de mise à l'échelle.

Cluster-head Gateway Switch Routing (CGSR) est une autre variante de DSDV, tous les nœuds maintiennent une table contenant le *clusterhead* de chaque nœud dans le réseau.
L'algorithme least cluster change (LCC) est employé pour désigner les *clustershead* dynamiquement en se basant sur l'ID minimum ou la connectivité la plus grande des nœuds. Pour lier les *clustershead*, il faut avoir des passerelles qui servent à acheminer les paquets d'un *clusterhead* à un autre. Le *clusterhead* donne aux nœuds, qui se trouvent sous sa couverture, l'accès au canal par le mécanisme de jeton. Le routage avec le CGSR est hiérarchique, il peut donc permettre une meilleure utilisation de la bande passante.
Les chemins utilisés sont souvent longs est instable dans un milieu mobile ce qui implique un changement de *clusterhead* fréquent.

La consommation des ressources au niveau d'un *clusterhead* est haute puisqu'il doit servir tout les nœuds qui sont liés à lui, ce qui augmente la fréquence de changement de *clusterhead*.

On peut remarquer que dans les protocoles de routage proactif, la fréquence d'échange de tables et la zone de l'échange constituent les principaux problèmes qui limitent la mise à l'échelle, l'énergie et la bande passante pour les données utiles.

De l'autre coté la disponibilité de toute la topologie du réseau au niveau de chaque nœud permet de transmettre un paquet vers n'importe quelle destination dans le réseau à travers le plus court chemin immédiatement après recevoir le paquet de la couche supérieure. Il reste à voir si un nœud a besoin de connaitre tous les chemins vers les autres nœuds du réseau.

Tableau A.1

Tableau récapitulatif de protocoles proactifs.

	DSDV	WRP	CGSR
Implantation	Simple	Complexe, plusieurs tables impliquées	Complexe, il faut élire les *clustershead* et les *gateway*. (LCC)
Ressources les plus utilisées	Bande passante du au grand nombre de mises à jour	Bande passante, mémoire et puissance de calcul.	Énergie au niveau des *clustershead*. Ces derniers servent tous les nœuds qui sont au tour d'eux.
Chemin	Un seul, le plus court	Un seul, le plus court	Un seul, mais pas forcement le plus court, il faut passer par le *clusterhead*.
Table de routage	Contient tout les nœuds du réseau et l'interface de sortie pour atteindre chacun.	4 tables : T. de distance, T. de routage, T. de cout de lien et une liste de message retransmis.	Contient le *clusterhead* de chaque nœud dans le réseau.
Maintenance	Périodique au niveau du réseau en entier.	Périodique au niveau du réseau en entier.	Périodique au niveau du *clusterhead* seulement.
Opportunité de mise à l'échelle	Très faible, plus le réseau est grand plus les paquets et les tables le sont.	Très faible	Faible, les tables de routage sont proportionnelles au nombre de nœuds.
Support de la QoS	Non, pas de champ ou mécanisme prévu.	Non	Non, pas de choix disponible au niveau du chemin, à part le nombre de sauts.

APPENDICE B

PROTOCOLE DE ROUTAGE SUR DEMANDE

Contrairement aux protocoles de routage basé sur l'échange de table, les protocoles de routage sur demande n'exécutent la recherche de route que lorsqu'un nœud a besoin d'un chemin pour communiquer avec une destination donnée dans le réseau.

Dynamique Source Routing (DSR) est conçue pour minimiser le nombre de messages de contrôle. Il n'utilise pas les messages de présence (*Hello*) ce qui laisse plus de ressource pour les paquets de données (bande passante, énergie).
Si un nœud à besoin de chemin vers une destination, il cherche dans sa table de routage, s'il y en a pas, il envoie une demande de route (*Route Request*) en diffusion à ses voisins et chacun d'eux retransmet la requête jusqu'à arrivé à la destination. Un nœud ne doit pas retransmettre sa propre demande en se servant de l'ID pour décider. Ainsi, la redondance des paquets de contrôle sera diminuée et le spectre radio sera plus libre pour des émissions plus importantes. Un nœud intermédiaire qui connait un chemin vers la destination peut envoyer une réponse (*Route Reply*) à la demande à la place de la destination. Le mécanisme de maintenance ne répare pas le bris de lien au niveau local ce qui augmente les paquets de contrôle et des fausses routes peuvent être utilisées au moment de la reconstruction par conséquent une perte de paquet plus grande. Le temps nécessaire pour obtenir une route avec un routage réactif est plus long que le temps obtenu avec le routage proactif. La performance de DSR est bonne dans un environnement statique et avec une faible mobilité, mais se dégrade rapidement en augmentant la mobilité. La performance se dégrade également en augmentant le nombre de nœuds dans le réseau puisque les paquets contiendront un nombre plus long de nœuds intermédiaires.

Ad hoc On-demand Distance Vector (AODV) diffère de DSR dans la façon de router les paquets de données. Alors que DSR inclut tous les nœuds du chemin dans le paquet, AODV met juste l'adresse du prochain saut. Le nœud intermédiaire change l'adresse du prochain saut en regardant dans sa table le chemin vers la destination. Chaque nœud qui diffuse une demande de route enregistre l'identificateur de diffusion et l'adresse du dernier diffuseur, puis il attend une réponse de route qui porte le même identificateur pour garder la route sinon il l'efface. Si un nœud intermédiaire possède une route vers la destination demandée et le numéro de séquence de la destination au niveau du nœud est supérieur ou égal au numéro de séquence dans le paquet, il a donc la permission d'envoyer une réponse à la source. Parmi les désavantages d'AODV est qu'une route d'un nœud intermédiaire peut avoir un identificateur supérieur à celui du paquet et ne pas être une route valide.
Les réponses multiples à une même demande de route augmentent le nombre de paquets de contrôle dans le réseau. Aussi les paquets envoyés périodiquement pour maintenir la route peuvent consommer inutilement la bande passante disponible.
Tomporally Ordered Routing Algorithm (TORA), on trouve le concept de niveau par rapport à la destination de sorte qu'une source construit un arbre à l'établissement de route vers une

destination. En sachant combien de nœuds les séparent de la destination, les mises à jour seront limitées à cette zone d'arbre. Chaque nœud peut avoir plusieurs routes vers une même destination. Un nœud intermédiaire peut répondre à une demande de route (*Query*) par un Update si la route est active et son temporisateur n'est pas expiré. En ayant un graphe directionnel acyclique (DAG) pour chaque destination, les paquets de contrôle de reconfiguration sont limités à une petite zone, ce qui diminue *l'overhead*. Il reste qu'au moment de l'établissement de route tout le réseau est inondé.

Les protocoles réactifs présentent une bonne base de routage dans les réseaux sans fil ad hoc. Puisqu'ils diminuent énormément le nombre de paquets de contrôle par rapport au protocole proactif. L'inconvénient dans les protocoles réactifs est la fraicheur de la route qui peut induire une grande perte. L'idée de mettre seulement le prochain saut dans le paquet dans le cas d'AODV permet de diminuer l'overhead, mais la façon de gestion de route peut être améliorée si les nœuds intermédiaires gardent toutes les routes qui aboutissent à la même destination. De cette façon, il peut envoyer les paquets à travers plusieurs routes. Ce qui peut décongestionner la zone du chemin.

Tableau B.1

Tableau récapitulatif de protocoles réactifs.

	DSR	AODV	TORA
Implantation	Moyenne, les nœuds doivent tenir compte de chaque paquet qui passe en vérifiant son type.	Moyenne, les nœuds doivent tenir compte de chaque paquet qui passe en vérifiant son type.	Complexe, la maintenance d'un arbre vers la même destination et sans boucle.
Ressources les plus utilisées	Énergie et bande passante dans les parties du réseau à haute concentration.	Bande passante, s'il y a absence de trafic des messages Hello sont transmis.	Bande passante, s'il y a absence de trafic des messages Hello sont transmis.
Chemin	Possibilité d'avoir plusieurs chemins vers la même destination.	Possibilité d'avoir plusieurs chemins vers la même destination.	Plusieurs chemins sont retournés à la source.
Table de routage	Contient les chemins vers les destinations demandés ou écoutés.	Contient le premier nœud sur le chemin de chaque destination.	Contient les différents chemins de l'arbre vers chaque destination.
Maintenance	Sur demande et avec le trafic	Périodique s'il n'y a pas de trafic.	Message de contrôle périodique pour maintenir l'arbre.
Opportunité de mise à l'échelle	Faible, limité par la taille du paquet qui augmente à chaque passage par un nœud intermédiaire.	Moyenne, le paquet contient seulement l'adresse du prochain saut vers une destination donnée.	Moyenne, un changement de topologie dans une partie de l'arbre n'affecte pas la connexion si on peut réorienter le trafic vers un autre chemin de l'arbre sans faire une autre demande de route.
Support de la QoS	Non mais peut être intégré si plusieurs routes retournées à la source.	Non mais peut être intégré si plusieurs routes retournées à la source.	Non mais peut être intégré puisque plusieurs routes retournées à la source.

APPENDICE C

PROTOCOLE DE ROUTAGE HYBRIDE

Les protocoles de routage hybride combinent les deux types de routage réactif et proactif en essayant de garder les meilleurs mécanismes des deux.

Core Extraction Distributed Ad-hoc Routing (CEDAR) est basé sur la formation de groupe dominant qui est choisi dynamiquement par le nombre de nœuds qui entour chaque nœud cœur (Core nodes).
La sélection des nœuds cœur représente la phase d'extraction de cœur. L'établissement de route est constitué de deux parties. La première est de trouver les différents chemins entre le nœud cœur de la source et celui de la destination. La deuxième partie est pour trouver la QoS voulue en termes de bande passante et longueur de chemin. En cas de bris, c'est le nœud cœur destination qui se charge d'informer le nœud cœur source qui par la suite fait une demande de route pour trouver un chemin alternatif s'il n'en a pas. Parmi les désavantages de CEDAR est la haute consommation d'énergie au niveau des nœuds cœur et le mouvement de ces derniers affecte énormément la performance du réseau. On peut remarquer que CEDAR constitue un mixe de cluster head (CGSR) et DSR qui sont deux protocoles proactif et réactif respectivement.

Zone Routing Protocol (ZRP) intègre les meilleures caractéristiques des deux types de protocole de routage. L'utilisation du routage proactif se limite au niveau de la zone de chaque nœud qui se limite à deux sauts. Ainsi, tous les nœuds au tour du nœud avec une limite de deux sauts se reconnaissent. Chaque nœud fait la même chose avec ces voisins. Pour lier deux zones qui ne se croisent pas, le routage réactif est utilisé. Si un nœud veut atteindre un nœud d'une autre zone, il envoie une diffusion aux nœuds de bordure, si ces derniers n'ont pas de réponses ils retransmettent la diffusion en intégrant leur adresse pour une éventuelle réponse. Si un bris de lien est détecté, il sera traité localement par le routage proactif à deux sauts.
Avec cette méthode les paquets de contrôle sont minimisés par rapport à la procédure de maintenance dans le routage sur demande et par rapport à l'inondation faite dans le routage proactif.
Le principal problème dans les deux protocoles de routages présentés ci-dessus est la mise à l'échelle.
Puisque dans CEDAR les nœuds cœurs sont trop sollicités par rapport aux autres nœuds alors que dans ZRP l'initialisation du réseau peut saturer la bande passante par conséquent bloquer tout le trafic. Il reste que l'idée de ZRP de la recherche de route est bonne puisqu'on ne faisant la diffusion qu'aux nœuds de bordure on diminue le nombre de paquets de contrôle.

Tableau C.1

Tableau récapitulatif de protocoles hybrides.

	CEDAR	ZRP
Implantation	Peu complexe, DSR sur CGSR ou vice versa.	Complexe, gestion de deux types de routage avec différents politiques
Ressources les plus utilisées	Énergie au niveau des nœuds cœurs et bande passante au niveau de dorsale.	Bande passante dans la zone proactive.
Chemin	Possibilité de plusieurs chemins entre deux nœuds cœurs.	Possibilité d'avoir plusieurs chemins.
Table de routage	Contient les chemins appris ou demandés.	Contient les chemins pour atteindre les voisins, leurs voisins et les chemins demandés vers des nœuds hors zone.
Maintenance	Sur demande et avec le trafic	Proactive dans un rayon de deux sauts et réactif dans le reste du réseau.
Opportunité de mise à l'échelle	Moyenne, hiérarchisation avec le concept de cluster et un trafic sur demande avec les mécanismes de DSR.	Plus que moyenne, un bris de lien est traité localement par le protocole proactif.
Support de la QoS	Oui, plusieurs routes disponibles avant l'envoi.	Non mais peut être intégré si plusieurs chemins disponibles.

APPENDICE D

PROTOCOLE DE ROUTAGE AVEC MÉCANISME D'EFFICACITÉ DE FLUX

Dans plusieurs protocoles de routage sur demande une route est obtenue après l'inondation du réseau par la demande de route. Cette inondation génère un grand nombre de redondances de paquet de contrôle, gaspillage de bande passante, augmentation du nombre de collisions et des rafales de diffusion au moment de changement de topologie fréquente. Le protocole *Preferred link-based routing* (PLBR) et *Optimized link state routing* (OLSR) utilise une inondation efficace pour trouver une route vers une destination donnée.

Preferred Link-Based Routing (PLBR) utilise une approche où seulement les liens fort ou stable peuvent être considérés pour retransmettre une demande de route. Deux algorithmes ont été présentés par *Sisodia* et al pour trouver le sous-ensemble de voisin en se basant sur le lien ou les caractéristiques des nœuds. Ce sous-ensemble s'appel *preferred list* (PL).
Il est introduit dans le paquet de demande de route de sorte que seulement les nœuds présents dans la liste ont le droit de diffuser la demande. Ainsi, on diminue le nombre de diffusions par conséquent le nombre de paquets de contrôle. Chaque nœud maintient aussi une liste des voisins de ses voisins dans une table périodiquement échangée.
La première phase dans PLBR est la phase d'établissement de route qui démarre en recevant un paquet de la couche supérieure destiné à un nœud inconnu. Si la table des voisins de voisin contient la destination, le paquet sera directement envoyé sinon une diffusion de demande de route est faite. Chaque demande de route contient l'adresse de la source et la destination, un numéro de séquence, la liste des nœuds traversés (TP), liste de préférence (PL), TTL et un drapeau *NoDelay*. Chaque nœud change la liste de préférence par sa propre liste, mais en gardant la même taille de la liste. Si la destination est dans la table des voisins de voisin, un unicast direct est transmis.

Si la liste de préférence d'un nœud est vide, le paquet est rejeté et marqué comme envoyé, le drapeau de *NoDelay* donne le choix de la procédure de sélection de route à la destination. Si le drapeau est marqué, seulement la première demande qui arrive à destination est considérée et le reste des requêtes qui arrivent plus tard avec le même numéro de séquence sont rejetées. Sinon une période d'attente est déclenchée à l'arrivée de la première demande et les chemins collectés pendant ce temps sont traités par un algorithme qui peut calculer la stabilité, le délai ou le plus court chemin. En ayant le poids de chaque lien dans le paquet reçu, on prend le poids minimum qui représentera le poids du chemin en totalité. Si deux nœuds ont le même poids, on prend celui qui a le plus court chemin.

Les deux algorithmes qui permettent de trouver les liens de préférence se basent sur la concentration de nœud donc le nombre de voisins ou le lien le plus stable en se basant sur la force de signal reçu.

Le mécanisme d'inondation efficace employé dans ce protocole minimise le problème de rafale d'inondation vu dans les protocoles réactifs. Ce qui donne à PLBR un degré plus haut de mise à l'échelle comparé aux autres protocoles réactifs.
La réduction de paquet de contrôle soulage le réseau en augmentant la bande passante disponible et en diminuant le nombre de collisions.

Optimized Link Stat Routing (OLSR) est un protocole de routage proactif qui utilise un mécanisme d'inondation efficace à travers le *multipoint relaying*. Chaque nœud essaye de trouver les relais multipoints en suivant deux critères, le premier est que chaque lien entre le nœud et son nœud relai soit bidirectionnel, le deuxième critère que les nœuds choisis comme relai peut atteindre deux sauts à partir du nœud d'origine de sorte que si ce dernier diffuse un message de contrôle les voisins de ses voisins peuvent recevoir le message à travers les nœuds relais comme présenté dans la figure D.1. Avec cette méthode tous les messages de contrôle transiteront seulement à travers les nœuds relais.
En même temps ces messages sont transmis aux nœuds qui ne sont pas des nœuds relai ce qui leur permet de calculer leur propre chemin vers les autres nœuds du réseau. L'avantage d'OLSR est l'originalité et l'ingéniosité du mécanisme de nœuds relais. La sélection de ces derniers est faire de sorte que les messages de contrôle de topologie qui transit d'un point relai à un autre informe les nœuds qui n'appartiennent pas à ce groupe de point relai. Ce mécanisme d'efficacité de flux diminue grandement le nombre de paquets de contrôle échangé dans le réseau ce qui donne plus de chance de mise à l'échelle.

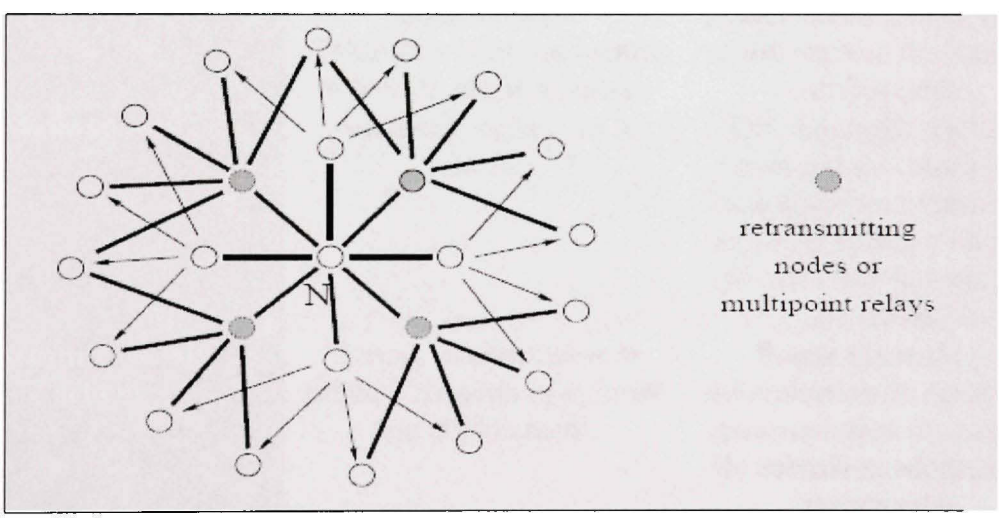


Figure D.1 : Relai multipoints.
Tiré de Murthy et al (2004)

Tableau D.1

Tableau récapitulatif de protocoles à mécanisme d'efficacité de flux.

	PLBR	OLSR
Implantation	Complexe, pour trouver la liste de lien prioriser pour le trafic.	Complexe, gestion de plusieurs table comme le la table de voisin et table de multipoint. la signalisation pour ces derniers et les messages de control de topologie.
Ressources les plus utilisées	Bande passante au niveau de des nœuds indiqués dans la liste de préférence.	Bande passante entre les nœuds multipoints.
Chemin	Un seul retourner après un temps d'attente ou non.	Un seul chemin calculé pour chaque destination à partir de la table de routage contenant tout les nœuds du réseau.
Table de routage	Contient les chemins appris ou demandés. Table de voisin des voisins et liste de lien référencier.	Contient un chemin pour chaque nœud dans le réseau et son numéro de séquence correspondant.
Maintenance	Sur demande et avec le trafic	Des messages appelés : message de control de topologie sont transmise entre les nœuds relai pour mettre à jour la topologie du réseau.
Opportunité de mise à l'échelle	Bonne, minimisation de rafale d'inondation et limité son déploiement.	Bonne puisqu'il y a minimisation de nombre de retransmission de message de control en adoptant les nœuds relai.
Support de la QoS	Oui, la destination peut retourner le chemin avec les critères demandés.	Non mais peut être intégré si plusieurs chemins disponible.

APPENDICE E

PROTOCOLE DE ROUTAGE HIÉRARCHIQUE

Le routage hiérarchique a plusieurs avantages, le plus important est la réduction de la taille des tables de routages par conséquent une meilleure adaptation pour la mise à l'échelle.

Le protocole HSR (*Hierarchical State. Routing*) combine les notions de groupes dynamiques et niveaux hiérarchiques avec une gestion efficace de localisation. Dans le HSR, l'image de la topologie du réseau est sauvegardée sous forme hiérarchique.
Le réseau est partitionné en un ensemble de groupes : dans un groupe, un nœud doit être élu pour représenter le reste des membres. Les représentants des groupes dans un niveau l, deviennent des membres dans le niveau l + 1. Ces nouveaux membres s'organisent en un ensemble de groupes de la même manière du niveau bas, et ainsi de suite pour le reste des niveaux.
La figure E.1 illustre l'application du mécanisme de partitionnement hiérarchique.

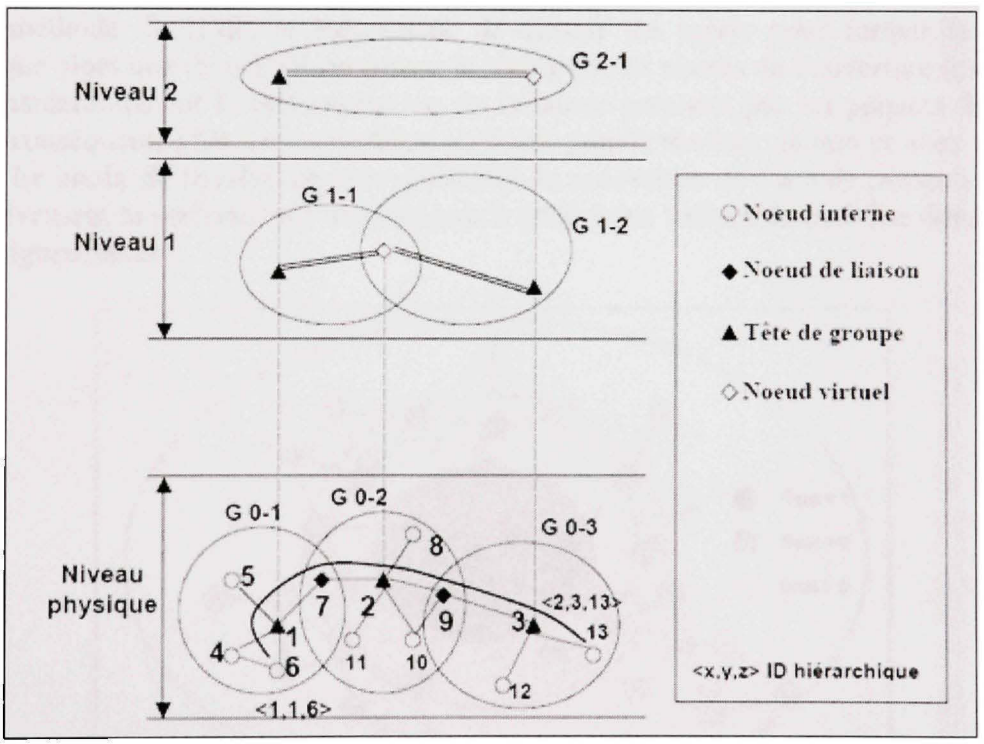


Figure E.1 Partitionnement de réseau en groupes.
Tiré de Murthy et al (2004)

L'adresse hiérarchique suffit pour délivrer les paquets de données à une destination, indépendamment de la localisation de la source et cela en utilisant la table HSR. La table HSR contient les adresses hiérarchiques des nœuds voisins et des nœuds demandés. Exemple : l'acheminement des données entre le nœud 6 et le nœud 3 (Figure E.1).

Fisheye State Routing (FSR) est basé sur l'utilisation de la technique "œil de poisson" (*fisheye*), proposée par Kleinrock et Stevens, qui l'ont utilisé dans le but de réduire le volume d'information nécessaire pour représenter les données graphiques.
Dans la pratique, l'œil d'un poisson capture avec précision, les points proches du point focal. La précision diminue quand la distance séparant le point vu et le point focal augmente.
Dans le contexte du routage, l'approche du "*fisheye*" matérialise pour un nœud le maintien des données concernant la précision de la distance et la qualité du chemin d'un voisin direct avec une diminution progressive du détail et de précision quand la distance augmente. La diminution de fréquence est assurée en changeant les fréquences de mise à jour et cela en utilisant des périodes d'échanges différentes pour les différentes distances entrées de la table de routage. Les entrées qui correspondent aux nœuds les plus proches sont envoyées aux voisins avec une fréquence élevée (donc avec une période d'échange relativement petite).

Dans la méthode de HSR, le mécanisme de cluster est repris pour former la structure hiérarchique alors que dans FSR on trouve la technique de niveau de couverture multiple qui réduit considérablement la consommation de la bande passante par les paquets de mises à jour. Par conséquent, FSR est performant pour des grands réseaux ad hoc et avec une haute mobilité. Le choix de nombre de saut qui défini la couverture de l'œil de poisson influence significativement la performance de protocole à différentes valeurs de mobilité donc il faut le choisir soigneusement.

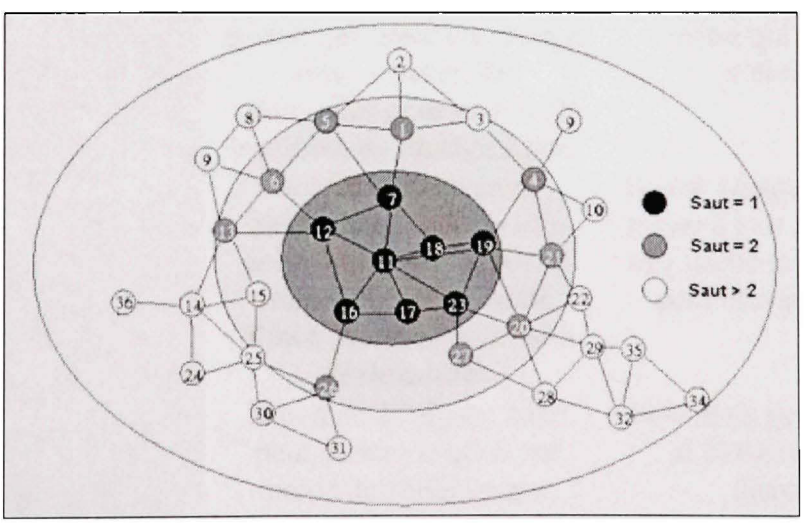


Figure E.2 Topologie du réseau en appliquant la technique 'œil de poisson'.
Tiré de Murthy et al (2004)

Tableau E.1

Tableau récapitulatif de protocoles hiérarchique.

	HSR	FSR
Implantation	Complexe, pour trouver les clusters head et la gestion de niveau d'hiérarchie.	Complexe, gestion de plusieurs niveaux de réseau avec différent fréquence de mise à jour.
Ressources les plus utilisées	Bande passante au niveau de des nœuds sous la juridiction du même cluster head.	Bande passante au tour du point focal et mémoire pour la table de routage si densité forte du réseau.
Chemin	Peut avoir plusieurs chemins mais pas forcement le plus court (il faut suivre la dorsale).	Possibilité d'avoir plusieurs chemins.
Table de routage	Contient les chemins hiérarchiques vers les destinations demandées et les chemins directs vers les voisins immédiats ou sous la juridiction du même cluster head.	Contient les chemins pour atteindre les voisins au niveau du point focal et les chemins vers les nœuds de chaque niveau diminue en fiabilité en s'éloignant du centre.
Maintenance	Il y a un échange périodique entre les clusters head à travers les passerelles pour maintenir les tables de routage à jour.	Échange plus fréquent au centre qui diminue en s'éloignant.
Opportunité de mise à l'échelle	Bonne, le concept de hiérarchie réduit la taille des paquets de control et minimisation de rafale d'inondation et limité son déploiement.	Bonne puisque l'étendu des mises à jour périodique est très limité même si la table peut être assez grande.
Support de la QoS	Non mais le cluster head peut donner le choix au nœud de choisir entre plusieurs dorsales.	Non mais peut être intégré si plusieurs chemins disponible.

BIBLIOGRAPHIE

AlAgha K., Pujolle G., et al. (2001). Réseaux de mobiles & réseaux sans fil. Eyrolles.

ANSI/IEEE (2003). Information technlogy - telecommunications and information exchange between systems - lacal and metropolitan area networks - specifis requirements - part 11:Wireless lan medium access control (mac) and physical layer (phy) specifications, ANSI/IEEE. ANSI/IEEE Std 802.11, 1999 Edition (R2003).

Bharghavan V., Demers A., et al. (1994). «Macaw: A media access protocol for wireless lan's». Proceedings of the conference on Communications architectures, protocols and applications.

Boulmalf M., Sohb A., et al. (2004). «Physical layer performance of 802.11g wlan». Applied Telecommunication Symposium.

Bradaric I., Dattani R., et al. (2003). «Analysis of physical layer performance of ieee 802.11a in an ad-hoc network environment».

CNAM. Cours b11: Transmission des telecommunications - partie2. http://www.cnam.fr/elau/polycop/images/B11_Caract%E9risation.pdf.

Corson S. Rfc 2501, mobile ad hoc networking (manet) : Routing protocol performance issues and evaluation considérations».

Garcia-Luna-Aceves J.J. et Fullmer C.L. (1999).«Floor acquisition multiple access (fama) in single-channel wireless networks». Mobile Networks and Applications.

Gavrilovska L.M. (2005).«Ad hoc networking towards 4g: Challenges and qos solutions». IEEE.

Goff et N. B. Abu-Ghazaleh (2001), «Preemptive Routing in Ad Hoc Networks», Proc. of the Seventh Annual International Conference on Mobile Computing and Networking, Rome,Italy, 43-52.

Johnson et al. (2003) The Dynamic Source Routing Protocol, section: 3.3.3. http://tools.ietf.org/html/draft-ietf-manet-dsr-08

Ju H. et Rubin I. (2005). «Performance analysis of mobile backbone topology synthesis algorithm for wireless ad hoc networks».

Kadoch M. (2004). Protocoles et réseaux locaux : Accés à internet. Press ETS.

Karn P. (1990). «Maca - a new channel access method for packet radio». ARRL/CRRL Amateur Radio 9th computer Networking Conference.

Meraihi R. (2005). Gestion de la qualité de service et controle de topologie dans les réseaux ad hocParis, Ecole Nationale Supérieure des Telecommunications.

Murthy C.S.R. et Manoj B.S. (2004). Ad hoc wireless networks. Prentice Hall Communications Engineering and Emerging Technologies Series.

Murthy et al (2004), Ad Hoc wireless networks: Architectures and Protocols, Prentice Hall

Narendran, P. Agrawal et D. K. Anvekar (1994), Minimizing Cellular Handover Failures without Channel Utilization Loss. Proceedings of IEEE Global Communications Conference, 3, 1679-1685.

NS2 manual, http://www.isi.edu/nsnam/ns/doc/index.html.

OPNET v11.0 PCL6, http://www.opnet.com.

Proxim. (2003). 802.11a white paper by proxim wireless networks. http://www.proxim.com/learn/library/whitepapers/80211a.pdf.

Qin L. et Kunz T. (2002) «Increasing packet delivery ratio in DSR by link prediction», IEEE Computer Society.

Ray S., Carruthers J.B., et al. (2003). «Rts/cts-induced congestion in ad hoc wireless lans». WCNC.

RMHD, Xerinay Aziz, FERON Nicolas (2004), Les réseaux GSM, 3G, UMTS, 4G, GPRS.

Srivastava V. et Motani M. (2005).«Cross-layer design: A survey and the road ahead». Communications Magazine, IEEE, 43(12),112-119.

Tanenbaum A. (2003). Computer networks, fourth edition. Prentice Hall.

Toh et al. (1997) «Associativity-Based Routing for Ad-Hoc Networks», Wireless Personal Communications Journal, Special Issue on Mobile Networking and Computing Systems, 4(2), 103-139.

Weiss E., Kurowski K., et al. (2003). «Avoiding route breakage in ad hoc networks using link prediction».

Wu M. (2006). A survey of mac protocols in ad hoc networks. http://www.utdallas.edu/~mxw013200/MAC_ADHOC.html.

Yu J.Y. et Chong P.H.J. (2005).«A survey of clustering schemes for mobile ad hoc networks». Communications Surveys & Tutorials, IEEE, 7(1),32-48.