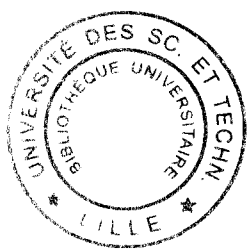
Numéro d'ordre : 3378

Mémoire présenté par

Julien CARTIGNY




pour obtenir le titre de
DOCTEUR EN INFORMATIQUE

# Contributions à la diffusion dans les réseaux ad hoc

Thèse soutenue le 19 décembre 2003, devant la Commission d'Examen :

| | | | |
|---|---|---|---|
| Président | : | Jean-Marc Geib | Professeur, USTL |
| Rapporteurs | : | Ana Cavalli | Professeur, INT, Evry |
| | | Eric Fleury | Professeur, INSA, Lyon |
| | | Ivan Stojmenović | Professeur, University of Ottawa, Canada |
| Directeur de thèse | : | Vincent Cordonnier | Professeur, USTL |
| Co-Directeur de thèse | : | David Simplot-Ryl | Maître de conférences habilité, USTL |
| Examinateurs | : | Piet Demeester | Professeur, Ghent University, Belgique |

UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE
LIFL – UMR 8022 – Cité Scientifique, Bât. M3 — 59655 Villeneuve d'Ascq Cedex

# Remerciements

*Je remercie grandement Jean-Marc Geib d'avoir accepté de présider le jury de cette thèse.*

*Je suis très reconnaissant à Eric Fleury, Ana Cavalli et Ivan Stojmenovic d'avoir accepté de rapporter mes travaux. Je suis très touché du soin avec lequel ils ont lu ce mémoire et je tiens à les remercier d'avoir accepté d'être dans mon jury.*

*Je tiens à exprimer toute ma gratitude à Piet Demeester ; Je suis très sensible à sa présence dans le jury.*

*Un grand merci à Vincent Cordonnier pour avoir accepté de me prendre sous son aile pendant trois ans et quelques mois. Je tiens tout particulièrement à le remercier de sa présence à ce jury, mais aussi pour l'aide qu'il m'a apporté lorsque j'ai rencontré certains problèmes extra-universitaires.*

*Mes remerciements les plus sincères à David Simplot-Ryl pour avoir été un encadrant hors pair, me guidant vers certaines pistes de recherche tout en me laissant une certaine autonomie pour aller explorer des sentiers non balisés.*

*Mes sincères remerciements à l'ensemble de l'équipe RD2P passée et présente pour leur support, leurs aides multiples ou tout simplement pour leur amitié. Je voudrais remercier Michaël Hauspie pour son amitié constante et sa désespérée tentative de me mettre à un sport de combat ; Gilles Grimaud pour sa bonhomie relaxante pour tous les membres de l'équipe ; Caroline Fontaine pour son support et ses leçons de japonais ; Alexandre Courbot pour sa passion partagée avec moi pour le logiciel libre, et François Ingelrest qui prend ma succession en tant que thésard sous la responsabilité de David. Ce travail n'aurait pas été possible sans les autres membres de l'équipe : Damien Deville, Jean-Jacques Vandewalle, Farid Nait, Mamhoud Taifour, Jean Carle, Laurence Caubrière, Christophe Rippert et Gabriel Bizzotto, notre expatrié Brésilien*

*Je voudrais bien sûr remercier les différents relecteurs de ce mémoire pour leurs multiples corrections : David Simplot-Ryl, Jean-Phillipe Vandeborre, Vinca Rivière, mon père Bernard Cartigny, Yann Hodique, Caroline Fontaine, et Michaël Hauspie.*

*Je voudrais aussi remercier tous les membres du Laboratoire d'Informatique de Lille. Je pense tout particulièrement à Marie-Paule Lecouffe, Isabelle Simplot-Ryl, Jean-François Roos, Raphaël Marvie, Eric Wegrzynowski, Léopold Weinberg, et sûrement bien d'autres personnes... Je tiens à présenter toute ma gratitude aux secrétaires du LIFL : Bérangère Dassonville, Annie Dancoisne, Nicole Flinois et Julienne Nzamukosha. Elles ont non seulement résolu quelques problèmes techniques lors de mon premier déplacement à l'étranger mais aussi accepté, malgré cet incident malencontreux, que je refasse d'autres déplacements.*

*Je souhaite à tous mes collègues thésards une bonne continuation et tous mes vœux de réussite. Je pense à Vincent Housseaux, Benjamin Weinberg, Emmanuel Renaux, Ammar Aljer, Ahmad-Chadi Aljundi, Vincent Benony, Arnaud Bailly, Damien Devigne, Michaël Hauspie, Yann Hodique, Alexandre Courbot, François Ingelrest, Mamhoud Taifour, Nicolas Jozefowiez, Sylvain Leblanc, Damien Marchal, Romain Rouvoy, et Marie-Hélène Verrons. Pour d'autres, l'étape de la soutenance est déjà un souvenir, et je leur souhaite bonne chance pour leur future carrière, spécialement pour Amar Abdelkader, Laetitia Jourdan, Violeta Felea, Gaëtan Scotto Di Apollonia, Stéphane Louis Dit Picard et Yann Secq*

*Je voudrais remercier ma famille pour leur support tout au long de mes études : À ma mère Pascale et à mon père Bernard pour m'avoir élevé et donné un certain regard sur ce qui m'entoure ; À Vinca, pour m'avoir donné goût aux études ; À mon frère Olivier, pour m'avoir ouvert à une certaine sensibilité musicale ; À ma demi-sœur Azelyne et mon demi-frère Auxane pour leurs petits yeux ronds pleins de curiosité ; À mes grands-parents Jacques et Monique pour leur soutien ; À l'ensemble des familles Cartigny et Rivière pour les moments de détente passés ensemble. Je n'oublie pas non plus Ayako Iguchi, mon soleil levant, qui m'a apporté un grand support moral lors de la fin de rédaction de ce mémoire. Enfin, j'ai une pensée émue pour Marie-Thérèse Capdeville-Rivière, grand-mère, décédée à la fin de l'année 2002.*

*Je ne peux oublier l'ensemble de mes amis qui m'ont apporté leur soutien ; Guillaume Denry et Cécile Lesgoirres pour leur réconfort, leur gentillesse et leur sofa, qui m'a accueilli certaines nuits lorsque le dernier métro était déjà en train de dormir ; Minoushka, délicieux félin appartenant à ces derniers, qui s'amusait à taquiner mon orteil à des heures incongrues de la nuit, lorsque je tentais de m'endormir sur le sofa ; Mathieu et Laeticia Vermeulen pour leurs petits plats et leurs oreilles attentives lorsque je sombrais dans un pessimisme effrayant ; Mélanie Morin pour son sens de l'humour et les peines partagées lors des affres estudiantines ; Nicolas, Laeticia et Julien pour les différentes soirées ensemble. Enfin, je remercie l'ensemble des membres de MTP (Melting-Pot), du nom d'un babillage électronique qui connecta de nombreux étudiants de la formation informatique de l'université de Lille 1. Je pense tout particulièrement à Nicolas Guillois, Hervé Meunier, Sébastien Wachter, Benjamin Legros, Gregory Bouilliez, Matthieu Cardon, Fabrice Lété, Jean-Paul De Lemos, Marie-Pierre Etienne, Marie Weerts, Yann Le Maner, Cédric Lallain, Christophe Caron, Antoine Bardet, Rémy Obein, Mathieu Durand, Raphael Raimbault, Alban Lecocq, Frederic Dhieux, Francois Bonami, Laurent Niemann, Grégory Guche, Nicolas Trentesaux, Benoit Lefevre, Louis Coilliot, Samuel Ledjmi et Cédric Roux.*

# Table des matières

# Première partie

# Présentation

# Introduction

## Les réseaux ad hoc

Internet est un environnement distribué, c'est-à-dire qu'il ne dépend pas d'une entité centrale. Les liens existants entre les nœuds de ce réseau permettent d'utiliser différents chemins pour arriver à destination. Ainsi, en cas de rupture d'une liaison, un ordinateur peut échanger des informations avec un autre sans nécessairement devoir passer par les mêmes chemins. Cette architecture est l'une des clés du succès d'Internet, car elle donne un système robuste et une forme d'égalité entre participants. D'ailleurs, l'une des applications les plus populaires sur Internet sont tous les programmes appelés communément P2P, (d'égal-à-égal ou *peer-to-peer*) [69] qui permettent à chacun de communiquer et d'échanger des informations sans le recours d'instances dirigeantes pour la recherche d'informations.

Dans les réseaux sans fil, on retrouve de façon élargie cette notion d'universalité : chaque personne à portée radio d'un nœud peut écouter ses communications. Ce système peut donc être considéré comme un système démocratique, permettant à chacun de participer. Mais, à l'opposé d'Internet, une grande majorité des produits radio fonctionne de manière hiérarchique et centralisée. Le système GSM [65, 77] par exemple, oblige chaque téléphone portable a être à portée de communication d'une base reliée au réseau téléphonique. Il existe donc un contrôle, une mécanique sous-jacente structurant l'ensemble des communications.

Pourtant, il est possible d'envisager un réseau sans fil universel où chaque mobile participerait aux communications. Si la couverture du réseau est suffisante (c'est-à-dire qu'il existe assez de nœuds pour un espace donné), chacun peut joindre un autre, soit s'il est à portée radio, soit en utilisant des nœuds situés entre eux-deux pour relayer leurs messages. Ce contexte est connu sous le nom de réseaux ad hoc.

Si l'idée générale d'un réseau ad hoc est triviale, il n'en est pas de même pour la réalisation et le déploiement d'un tel système. Il existe de très nombreux défis à résoudre : trouver le chemin entre deux nœuds ou assurer une bonne stabilité dans les communications entre deux nœuds par exemple. Le problème vient du fait que les nœuds peuvent être mobiles, ce qui entraîne des changements topologiques continuels dans l'état du réseau. De plus, le manque de centralisation d'une telle approche oblige à l'élaboration d'algorithmes localisés.

Un des problèmes étudiés par la communauté des chercheurs sur les réseaux ad hoc est la diffusion d'un message à l'ensemble des nœuds. Cette fonction est nécessaire dans de nombreux cas, notamment lors de la recherche d'une route dans le réseau. Dans ce cas, un message de diffusion est émis par un nœud source et répété par un certain nombre de nœuds pour permettre à l'ensemble du réseau de recevoir le message. Lorsque cette diffusion est réussie, le nœud destinataire de la demande de chemin peut renvoyer un message vers la source, de manière à créer la route les reliant.

## Orientation de notre approche

Notre travail porte sur la réduction du coût de la diffusion dans un réseau ad hoc. Un algorithme de diffusion naïf, appelé inondation, permet de joindre l'ensemble du réseau mais provoque de sérieux problèmes de communication, car chaque nœud se doit de répéter le message de diffusion. De nombreux algorithmes ont été proposés pour pallier ce problème, réduisant le nombre de nœuds réémettant le message de diffusion tout en garantissant une bonne couverture de l'ensemble du réseau. Notre contribution, dans le cadre de la diffusion dans un réseau ad hoc, tourne autour de deux thèmes : la réduction du nombre de réémissions et la diminution de la consommation énergétique. Nos approches se basent sur plusieurs idées originales différant sensiblement des approches existantes :

**Une approche probabiliste :** Une majorité des protocoles existants sont déterministes : ils évaluent la décision de réémission en fonction de règles précises. Au contraire, nous proposons d'utiliser l'approche probabiliste pour évaluer la décision de réémettre ou non. Cette approche prend son sens lorsque l'on considère un ensemble de nœuds : même si la décision d'un nœud peut-être mauvaise, la décision d'un groupe de nœuds se révèle en moyenne satisfaisante, sans la nécessité de communication supplémentaires entre-eux.

**Évaluation des distances sans outils de positionnement :** Certains protocoles utilisent des outils de positionnement (GPS). Mais en l'absence de ceux-ci il est difficile de pouvoir évaluer la distance entre deux nœuds, et les protocoles existants se basent sur l'information topologique du graphe unitaire du réseau ou du voisinage. Nous proposons une méthode pour évaluer une pseudo-distance entre deux nœuds, en se fondant sur le voisinage des deux mobiles.

**L'utilisation des graphes RNG et LMST :** RNG et LMST sont des algorithmes de réduction de graphes diminuant le nombre de liens de manière à connecter uniquement les nœuds proches sans perte de connexité. Nous utilisons ce mécanisme pour diminuer la puissance d'émission d'un nœud et ainsi économiser son énergie tout en maintenant la connexité complète du réseau. Ce procédé est aussi utilisé pour déterminer la décision de réémission dans le cas d'un réseau avec une seule portée d'émission.

**La réduction de portée évaluée de manière locale :** Dans le cadre de la réduction d'energie, une grande majorité des protocoles de diminution de portée se basent sur la connaissance totale de la topologie pour permettre la construction d'arbres recouvrants. Nous proposons, avec l'aide des graphes RNG et LMST, que la prise de décision soit locale à chaque nœud, avec une connaissance limitée au voisinage à deux sauts.

## Organisation du document

L'ensemble de ce document est partagé en trois grandes parties. La première correspond au chapitre 1. Il propose un état de l'art sur les recherches actuelles dans les réseaux ad hoc, sur les différents problèmes rencontrés dans cette environnement, et sur la problématique de la diffusion.

Une deuxième partie propose de s'intéresser à la réduction du nombre de réémissions dans le cas d'une rediffusion. Cette partie est composée dans un premier temps du chapitre 2 qui propose une méthode de diffusion stochastique biaisant les tirages en fonction de la distance séparant la source du nœud. Pour connaître une évaluation de cette mesure, le protocole développé baptisé BRP, utilise une comparaison des voisinages pour en extraire une "pseudo-distance".

Dans la même partie, le chapitre 3 détaille un algorithme qui décide de la réémission à partir d'un sous-ensemble du voisinage. Ces nœuds voisins sont choisis avec l'algorithme de réduction de graphe

RNG, qui permet de choisir des voisins proches et en nombre limité. Le protocole ainsi développé et nommé SSR, n'a alors qu'un petit ensemble de nœuds à surveiller comme base de décision pour la réémission.

La troisième partie s'intéresse à un autre problème dans les réseaux ad hoc : la consommation énergétique. Les nœuds possédant une source d'énergie limitée, il est intéressant de réduire la consommation, surtout de l'interface radio (la plus dépensière). Le chapitre 4 se concentre sur l'idée de réduction de portée, de manière à réduire la consommation énergétique. Pour éviter toute perte de connexité dans le réseau, l'algorithme RBOP utilise les graphes RNG pour limiter la puissance radio aux seuls voisins essentiels.

Toujours dans cette dernière partie, le chapitre 5 propose d'utiliser les idées développées dans le chapitre précédent en les appliquant dans le cas des antennes directionnelles. Nous développons pour cette tâche trois protocoles. Le premier est une version directionnelle de RBOP, baptisé DRBOP ou DLBOP (selon l'algorithme de réduction de graphe utilisé (RNG ou LMST)). Le second OM-DLBOP est plus adapté en cas de grandes densités, en couvrant de nombreux nœuds en un seul envoi. Le troisième, ADLBOP, est un algorithme adaptatif utilisant les deux précédents et choisissant entre l'un ou l'autre en fonction du voisinage, de manière à obtenir la meilleure réduction possible d'énergie.

# Chapitre 1

# État de l'Art

## 1.1 Les réseaux ad hoc

Aujourd'hui, de nombreux systèmes de communication sans fil existent. Ils permettent d'éviter l'obligation pour un usager d'être relié à un ensemble filaire pour accéder aux ressources d'un réseau. De nombreux exemples existent déjà de manière commerciale, comme le GSM [77] (*Global System for Mobile Communication*), un système de téléphonie portable permettant de joindre un correspondant quelle que soit sa position. Mais un tel ensemble est dépendant de l'emplacement des bases (les antennes permettant de relier le monde des ondes hertziennes au réseau filaire) car cette structuration impose certaines restrictions, comme la nécessité d'un déploiement d'infrastructures coûteuses.

On peut imaginer un système plus évolué et décentralisé, utilisant les usagers du réseau comme support de l'ensemble des communications. Dans un emplacement de taille définie (une pièce, un bâtiment, une ville, un pays ou même une planète) se trouve un nombre important d'ordinateurs, éventuellement mobiles. Les entités qui composent ce réseau possèdent un dispositif de communication sans fil leur permettant de communiquer avec les entités situées dans leur voisinage. Chaque nœud peut donc directement joindre ses voisins en utilisant son interface radio. Ils ont aussi la possibilité de contacter n'importe quel autre nœud à l'intérieur du réseau en utilisant les nœuds intermédiaires (situés entre la source et le destinataire). Ces derniers se chargent de relayer les messages (voir figure 1.1) et ainsi offrir un réseau autonome, conçu et supporté par l'ensemble des participants. Ce type d'organisation s'appelle des réseaux ad hoc (*Ad Hoc Networks*). Ce domaine est devenu une nouvelle voie de recherche à part entière, avec la formation d'un groupe de recherche de l'IETF (*Internet Engineering Task Force*) baptisé MANET [94] (*Mobile Ad-hoc Networks*). De nombreuses publications et livres proposent une présentation complète de ce type d'architecture [6, 74, 84, 91].

Mais des problèmes existent, de la couche matérielle jusqu'à la couche application [39]. Par exemple, la possibilité que l'ensemble ou une partie des entités soient mobiles entraîne des variations dans la recherche ou la maintenance d'un chemin entre deux nœuds. On peut aussi citer le fait que chaque entité est autonome et qu'il n'existe pas de système centralisé pour gérer les communications. Cette contrainte oblige alors l'élaboration d'algorithmes totalement distribués, dans le but d'obtenir un comportement global cohérent malgré le caractère plus ou moins indépendant de chaque nœud.

D'autres problématiques se posent : comment distribuer une information à l'ensemble des nœuds (et comment conserver une information cohérente vis-à-vis des évolutions dans le réseau) ? Quelles sont les modifications qu'entraîne ce modèle sur la pile réseau OSI[1] pour apporter une certaine flexi-

[1]Le lecteur pourra trouver une description complète des couches du modèles OSI (*Open System Interconnexion*) de

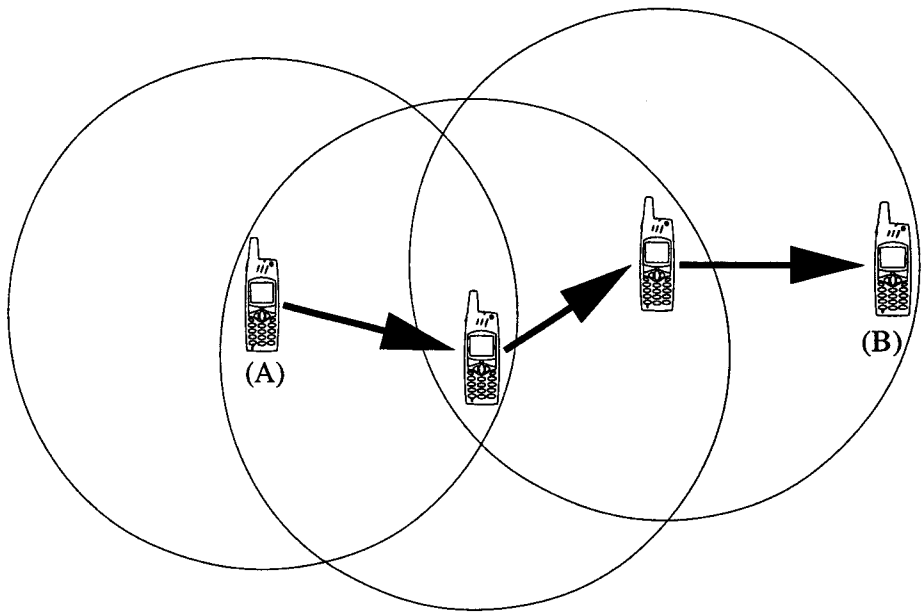



FIG. 1.1 – Un exemple de transmission d'un message entre nœuds dans un réseau ad hoc.

bilité tout en restant compatible avec la plus grande partie possible des protocoles existants ? Il existe aussi des questions sociales et économiques sur l'émergence de réseaux ad hoc en concurrence aux réseaux actuels, qu'ils soient filaires ou dirigés par de grands opérateurs de télécommunications (le téléphone portable par exemple, qui supportera difficilement un réseau ouvert et coopératif de ce type).

### 1.1.1 Définition

Le terme « ad hoc » est une locution d'origine latine qui signifie « qui convient au sujet, à la situation. » On parle donc de réseaux auto-adaptatifs (capables de s'organiser par eux-mêmes). Une autre lecture de la définition peut signifier une propriété d'universalité de ce moyen de communication, comme si ce procédé pouvait satisfaire tous les besoins en terme de communication entre objets mobiles.

La définition la plus concise d'un réseau ad hoc est la suivante : « un réseau ad hoc est un réseau sans fil à contrôle totalement décentralisé. » Par réseau sans fil, on entend que toutes les communications entre objets se font par voie aérienne, une interface radio dans chaque mobile permettant d'émettre et de recevoir. Le terme de contrôle décentralisé indique que l'ensemble des opérations pour la découverte et la maintenance du réseau se fait localement par chaque nœud. Chacun gère ses communications à partir des informations connues sur le réseau et sur l'état interne du nœud, dans le but de faire émerger un comportement cohérent du réseau (*e.g.* des routes correctement établies).

Les réseaux ad hoc peuvent inclure le concept de mobilité [4]. Par mobilité, on désigne le fait que chaque terminal peut se déplacer à l'intérieur du site, seul ou avec un groupe. Ces mouvements entraînent des changements dans les routes construites, ainsi que dans les caches d'information sur la topologie du réseau. Un nœud doit maintenir à jour ces informations et conserver dans un état valide les routes qui commencent, passent ou finissent par lui-même.

---

l'organisme ISO (*International Standard Organisation*) dans [89].

Le concept de mobilité inclut aussi certains états, tels que la déconnexion ou l'impossibilité de joindre le réseau. La topologie des réseaux ad hoc étant volatile, variable et éphémère, chacun des membres peut quitter le groupe de communication sans avertissement. Ainsi, le fait qu'un nœud soit absent du réseau est un état normal, qui ne doit pas gêner les autres participants. Cette caractéristique doit être prise en compte à chaque couche du modèle réseau OSI : le routage doit se faire dans la mesure du possible (*i.e.* le nœud destinataire doit être joignable), de manière transparente, tout en s'adaptant aux déficiences d'une partie du réseau (en trouvant des chemins alternatifs par exemple). Au niveau des couches supérieures (applications), chaque programme doit pouvoir accéder à des informations supplémentaires pour tenir compte de l'aspect changeant et sans garantie du réseau. Par exemple, il peut disposer d'outils lui indiquant la qualité d'un lien entre deux nœuds [40, 41].

### 1.1.2 Applications

Les recherches sur les réseaux ad hoc ont été initiées par le DARPA (*Defense Advanced Research Projects Agency*) avec le développement de *PRN* ou *Packet Radio Networks* [53]. Ce protocole, conçu pour l'armée américaine, permet de déployer une infrastructure de communication entre chaque bataillon, par l'intermédiaire de plusieurs véhicules communiquant ensemble. Il possède des bonnes idées, comme un modèle de couche MAC (*Media Access Control*) avec approbation passive ou la prise en compte de la qualité des liens. Mais ce protocole possède de trop nombreux défauts. D'une part, il prend l'hypothèse que l'ensemble des entités se déplacent lentement (avec peu de changements dans la topologie du réseau). D'autre part, la difficulté de concevoir, dans les années 1970, l'électronique suffisante pour mémoriser les paquets lors d'une réémission impliquait un matériel de taille assez importante et difficile à utiliser.

Le fait que ce soient les militaires qui aient commencé les premières expérimentations sur les réseaux ad hoc n'est pas un hasard. En effet, cette infrastructure est très adaptée aux environnements « hostiles », car ils sont rapidement déployables, et robustes dans les cas de perte de liens. De plus, la possibilité de posséder plusieurs routes renforce la fiabilité de l'ensemble du réseau. Ils sont donc particulièrement intéressants pour un système de communication sur les champs de bataille mais aussi dans d'autres environnements. On peut évoquer les sinistres (tremblements de terre, inondations) où l'ensemble des infrastructures existantes a été détruit. Les unités de secours disposent alors d'un moyen de communication qui n'est pas influencé par les dégâts causés à l'environnement. Ou encore, les survivants peuvent établir un réseau pour aider à leur localisation [103].

Les réseaux ad hoc peuvent aussi être utilisés pour relier plusieurs ordinateurs entre-eux. Ils sont donc adaptés pour la formation de réunions, où la nécessité temporaire d'une infrastructure pour les communications est soutenue par l'ensemble des participants. Il existe aussi des recherches [63] proposant d'utiliser les réseaux ad hoc avec les véhicules routiers. On peut entrevoir de nombreuses applications possibles pour un tel usage : distribution d'information au niveau local (risque d'accidents ou d'encombrements), aide automatique à la conduite (feux d'avertissement), téléphonie entre véhicules, etc...

Avec l'émergence de l'informatique mobile et les possibilités offertes par l'informatique vestimentaire (*Wearable Computing*) [62], chaque usager se voit doté d'ordinateurs qu'il transporte avec lui. Ces appareils peuvent se mettre à communiquer entre eux, ou avec l'environnement. Dans le premier cas, on parle de réseau personnel (*Personal Area Network* ou *PAN*), et la solution ad hoc permet la liaison entre chacun des éléments [9] (avec l'utilisation de Bluetooth [36] par exemple, adapté pour des petits objets et des courtes distances). Dans le deuxième cas, les réseaux ad hoc permettent à chacun de se connecter à l'environnement et d'y participer sans pré-requis particulier. On parle alors

d'informatique omniprésente (*Ubiquitous Computing*) [97] : chaque entité se reconfigure en fonction des communications disponibles, de façon transparente pour l'utilisateur.

Un autre domaine très intéressant pour les réseaux ad hoc concerne les senseurs [29]. Ce sont des équipements possédant des capacités très limitées (mémoire, processeur, bande passante) et de taille réduite. Ces équipements ont de nombreux domaines d'applications : médicales ou militaires par exemple. Ils sont en général utilisés en grande quantité, et les réseaux ad hoc permettent alors la liaison entre tous les objets. On peut citer l'exemple de capteurs météorologiques, de surveillance d'un site, de mesure des constantes d'un être humain ou de contrôle de structures (par exemple, des capteurs coulés dans le béton d'un pont).

Le panel d'applications utilisables pour les réseaux ad hoc est large et varié. Mais de très nombreux défis se posent dans les réseaux ad hoc avant de pouvoir les utiliser de façon intensive. Dans le reste de ce chapitre, nous présentons différents problèmes à certains niveaux de la pile réseau OSI. Dans la section 1.2, la problématique d'accès à la couche MAC (couche 2 du modèle ISO) est étudiée. Dans la section suivante, une présentation des protocoles de routage existants permet au lecteur de se familiariser avec les principaux problèmes de construction de chemin dans un réseau ad hoc. Dans la section 1.4, une étude des différents protocoles d'inondation présente les difficultés d'une telle opération et introduit les éléments nécessaires à la compréhension des chapitres ultérieurs. Enfin, la section 1.5 conlut le chapitre en énumérant d'autres problèmes à résoudre dans les réseaux ad hoc.

## 1.2 L'accès à la couche MAC

Dans un réseau sans fil, deux mobiles peuvent communiquer en émettant des ondes radios. Ils se partagent un médium unique mais ne peuvent émettre en même temps. En effet, deux émissions simultanées sur le même canal entraînent une perte d'information à l'intersection des deux zones de communication (on parle alors de collision). Ce problème est déjà connu dans les réseaux filaires lors du partage d'un bus. Mais dans le cas des réseaux sans fil, il existe des restrictions supplémentaires qui compliquent la situation :

**L'émetteur ne peut entendre une collision qu'il a engendrée** Un mobile ne sait pas quand son émission entre en collision car il ne peut émettre et écouter en même temps. Il ne peut donc savoir si son émission a été reçue par le ou les correspondants. Pour minimiser ou détecter les collisions, le protocole MAC peut disposer d'un mécanisme actif (avec l'écoute du médium pour détecter quand celui-ci est libre) ou passif (attente d'une réponse positive pendant un laps de temps appelé *timeout*).

**Le problème du « terminal caché »** Dans le cas où deux mobiles $A$ et $B$ ne sont pas à portée de communication, et que chacun d'eux communique avec un tiers $C$, il existe une possibilité de collision sur ce dernier. En effet, sans accord préalable $A$ et $B$ n'ont aucun moyen de prendre conscience de l'autre communication en cours. On dit alors que $B$ est caché de $A$ et que $A$ est caché de $B$ (voir figure 1.2). Pour remédier à ce problème, le protocole MAC peut disposer d'un mécanisme pour avertir l'entourage de l'émetteur ET du récepteur de l'existence d'une communication en cours.

**Le problème du « terminal exposé »** Cette difficulté est le pendant du problème du terminal caché. Lors d'une communication radio entre deux mobiles, leurs voisins respectifs ne peuvent émettre car ils risquent de perturber l'échange en cours. Beaucoup de mobiles se retrouvent alors immobilisés. La figure 1.3 représente ce problème : le message du nœud $S$ vers le nœud $D$ fait croire à $A$ qu'il ne peut pas émettre, alors qu'une communication entre $A$ et $B$ ne génerait pas l'autre.

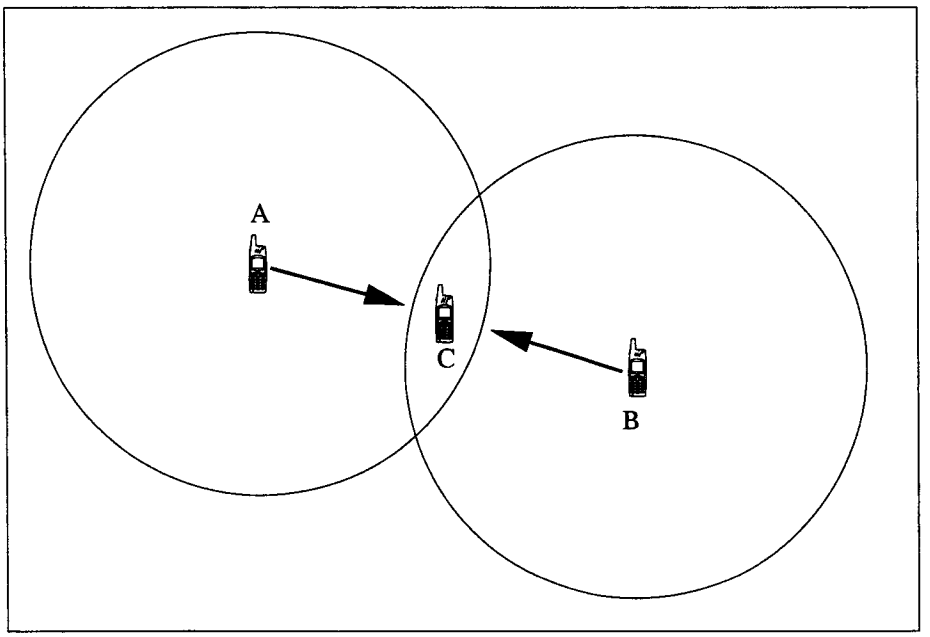



FIG. 1.2 – Problème du terminal caché : Les nœuds $A$ et $B$ n'ont aucun moyen de savoir que leurs communications vers $C$ rentrent en collision.

Il peut être intéressant de posséder un algorithme qui n'impose pas abusivement des restrictions à l'ensemble des voisins à deux sauts. Par exemple, une politique de programmation des envois dans un réseau permettrait de distribuer les échanges plus équitablement (mais ce procédé est en dehors du travail de la couche MAC, car cette idée dépend très fortement des algorithmes des couches supérieures). Une autre solution consiste à varier la portée d'émission des nœuds (voir les chapitres 4 et 5).

De nombreux protocoles ont été développés pour pallier à certains de ses problèmes. Ils peuvent se décomposer en deux grandes familles : ceux conçus dans le cas d'une diffusion (c'est-à-dire pour joindre l'ensemble des voisins), et ceux conçus dans le cas d'une communication point-à-point (c'est-à-dire pour joindre uniquement un nœud voisin).

### 1.2.1 Le cas de la diffusion

Une diffusion est l'opération de transmission d'un message à l'ensemble des voisins. Le terme de voisin regroupe l'ensemble des mobiles à portée radio, c'est-à-dire les nœuds pouvant recevoir le message directement par un message radio. La notion de diffusion est implicite et déjà présente dans les réseaux sans fil : si un mobile émet un message, alors l'ensemble de ses voisins va le recevoir. Mais comme d'autres communications dans le voisinage peuvent perturber le message émis, il est nécessaire de disposer d'un algorithme d'accès et de partage du médium pour empêcher ou, tout au moins, minimiser les collisions possibles.

Le protocole *Aloha* [1] est l'un des premiers protocoles développés pour le partage du médium aérien. Chaque mobile, dont le message est entré en collision avec un autre, attend un certain temps aléatoire avant de réémettre. Cette idée est simple mais donne un rendement très insuffisant (de l'ordre de 18% en cas de forte charge réseau). De plus, les réseaux sans fil n'ont pas la capacité de détecter

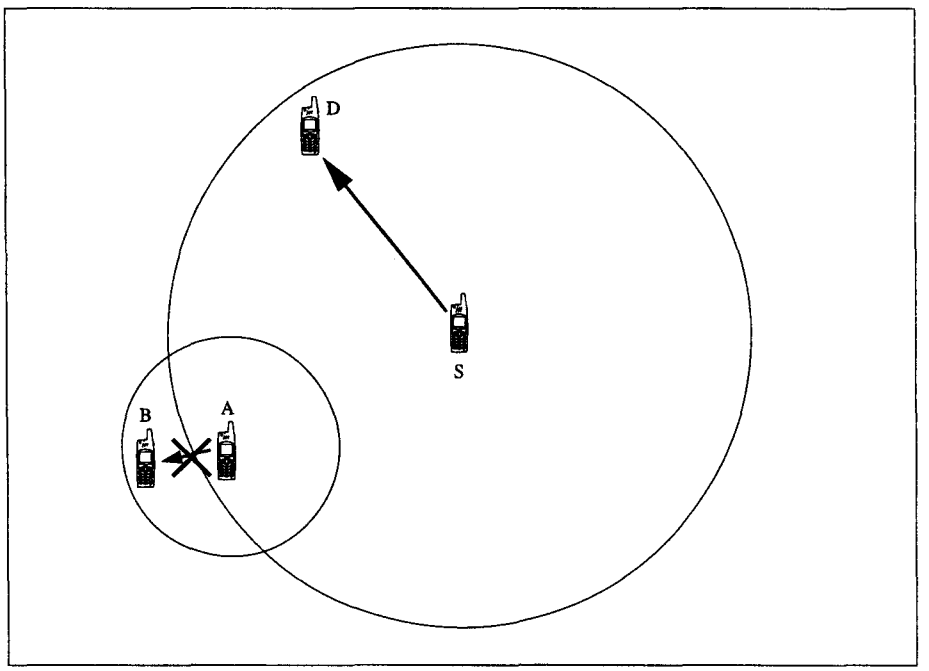



FIG. 1.3 – Exemple du problème de terminal exposé : le nœud $A$ ne peut pas émettre car il entend une communication en cours. Pourtant, si $A$ doit émettre vers $B$, il ne gêne pas celle entre les nœuds $S$ et $D$.

les collisions (un mobile ne peut écouter et émettre en même temps).

Pour rendre fiable ce protocole, il faudrait un message d'approbation de la part de chaque voisin en réponse au message de diffusion. Mais la source se retrouverait alors sous une tempête de messages (avec un grand risque de collisions dans ces réponses). Il est donc nécessaire de se tourner vers des algorithmes plus sensibles aux communications en cours, comme les protocoles à détection de porteuse (*carrier sensing protocols*). L'algorithme CSMA (*Carrier Sensing Multiple Access*) [52] et ses variantes (*persistent CSMA*, *nonpersistent CSMA*, *p-persistent CSMA*) écoutent le canal avant émission. S'il n'y a pas de communication en cours, alors le mobile émet son message (éventuellement après un certain délai). Cette écoute permet de réduire les collisions (de façon limitée) mais ne résout pas le problème du terminal caché.

Une variante de CSMA est utilisée dans le protocole 802.11b [25]. Cette dernière version s'appelle CSMA/CA (*CSMA with Collision Avoidance*) [25] et est utilisée dans le cas d'une diffusion. Le protocole utilise le principe de contention limité pour minimiser les chances de collisions. Un mobile qui désire émettre un message procède comme suit (voir figure 1.4).

1. Il attend pendant un temps incompressible, appelé *DIFS* (*DCF Inter-Frame Spacing*), dans le but de laisser une chance aux autres mobiles d'acquérir l'accès au médium.
2. Il tire un nombre aléatoire, appelé *backoff counter* (compris entre 0 et un temps $\delta$), représentant le nombre d'unités de temps libres à attendre avant l'émission du message.
3. Si la fenêtre de collision est dépassée sans aucune communication autour du nœud, alors il émet son message.

Ce dispositif permet de réduire de façon efficace le nombre de collisions, tout en préservant un bon rendement de l'utilisation en terme de bande passante. Par contre, il n'est pas efficace à 100% (c'est-

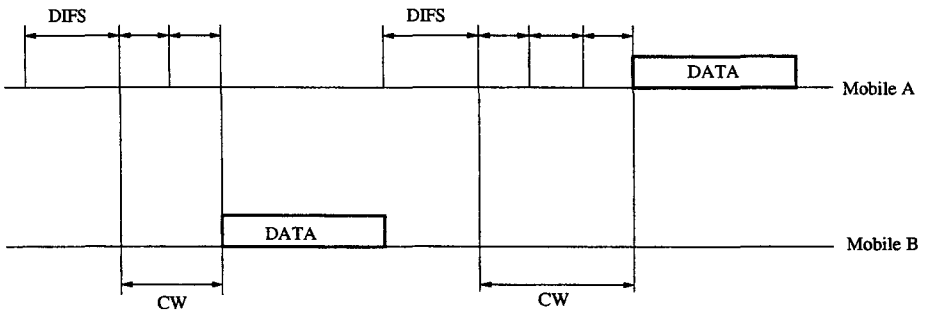



FIG. 1.4 – Chronogramme d'une émission par le protocole CSMA/CA. Le mobile $A$ attend la période DIFS puis décompte les frames pendant sa fenetre de contention. Malheuresement, il est obligé de recommancer par la faute de l'émission $B$. Il peut alors réémettre à la fin de sa deuxième feneètre de contention.

à-dire avec une garantie que tous les voisins reçoivent le message) car des mobiles peuvent quand même émettre en même temps sans s'en rendre compte. Il sera néanmoins utilisé par la suite dans certaines des simulations car c'est le protocole prédominant dans les réseaux sans fil actuellement (il est utilisé dans les interfaces 802.11b, mécanisme le plus populaire en matière de réseaux sans fil).

Signalons une méthode supplémentaire (non présente dans 802.11b) pour améliorer la garantie de réception d'un message de diffusion. L'écoute se déroule après l'émission d'un message. Ainsi, un nœud peut découvrir que son message est entré en collision s'il entend le canal occupé avec un message incomplet (on parle alors de *packet sensing*). Il peut alors éventuellement réémettre son message. Un protocole fondé sur ce modèle, intitulé FAMA (Floor Acquisition Multiple Access) [35] se concentre sur les temps d'attente et d'émission des messages de contrôle, dans le but de garantir des transmissions de données sans aucune collision.

### 1.2.2 Le cas de la communication point-à-point

Dans le cas d'un message point-à-point (à destination d'un seul des voisins), il est plus facile de garantir une communication entre la source et le destinataire. Avec un système d'annonces des deux parties, chaque voisin prend connaissance des transactions qui vont se produire dans son voisinage et peut reprogrammer ses émissions pour éviter une collision. Pour cela, un contact préliminaire, appelé poignée de main (*HandShaking*), est effectué pour l'établissement de la communication. L'émetteur envoie un RTS (*Request To Send*) au récepteur, qui répondra par un CTS (*Clear To Send*). En cas de collision sur un de ces deux messages, le mobile émetteur peut la détecter. En effet, s'il ne reçoit pas la réponse CTS après sa demande RTS, il peut supposer qu'il y a eu collision lors de l'envoi de son message ou durant celui de son correspondant. Il reprogramme alors son envoi, dans un temps déterminé aléatoirement. Outre le fait que l'émetteur et le récepteur s'accordent sur leurs transmissions à venir, les messages RTS et CTS contiennent la durée attendue de la communication, afin de permettre aux voisins de redemander un accès au médium en temps voulu. Ce mécanisme simple est utilisé par le protocole *CSMA/CA* (*CSMA with Collision Avoidance*) dans les interfaces 802.11b lors de communications point-à-point.

Plusieurs protocoles reposent sur le modèle précédent. Le protocole MACA (Multiple Access Collision Avoidance) [50] (et ses variantes MACAW [10], MACA/PR [58] et MACA-BI [87, 88]) propose de se débarrasser de l'écoute nécessaire avant chaque transmission. Les collisions sont évitées par l'écoute passive des RTS/CTS au niveau de chaque mobile. Ce protocole, plus simple et plus

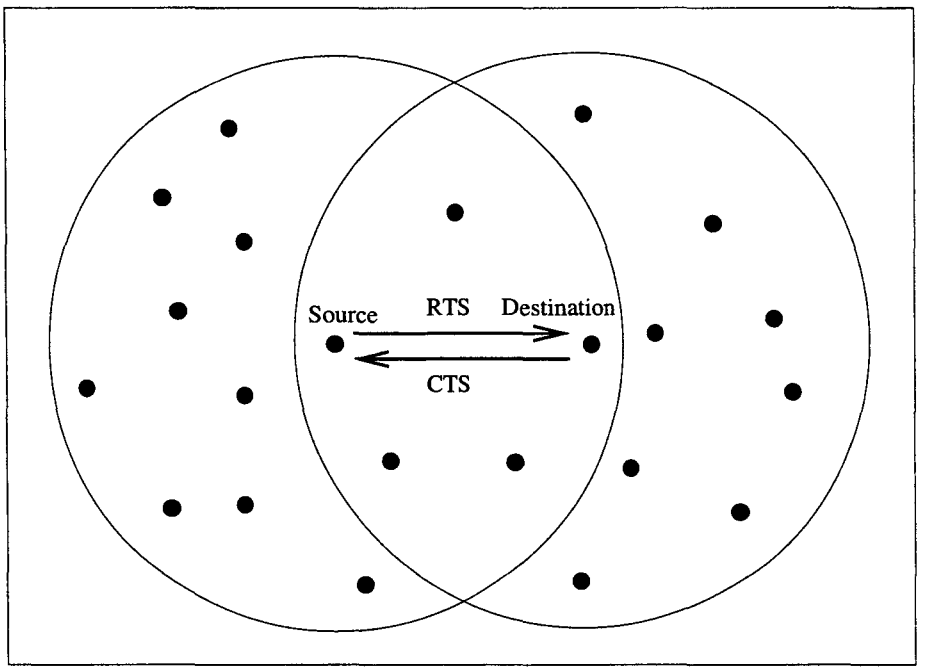



FIG. 1.5 – Ouverture d'une communication avec les messages RTS et CTS.

léger techniquement que CSMA/CA, n'est pas aussi bon que ce dernier. Il possède des performances proches d'ALOHA lors de trafic important avec de nombreux terminaux cachés.

D'autres protocoles existent pour la gestion de la couche MAC. Pour minimiser les problèmes de reprise sur collision, DBTMA (*Dual Busy-Tone Multiple Access*) [37, 27] propose l'idée d'un système de signalisation n'appartenant pas au canal de transmission. Il est plus efficace que les modèles proposés plus haut, mais il est nécessaire de disposer de plusieurs canaux séparés. Certains protocoles abordent le problème de l'économie d'énergie, comme une version hybride de MACA, baptisée PAMAS (*Power Aware Multi-Access Protocol with Signaling for Ad Hoc Networks*) [82]. Ce mécanisme utilise un senseur sur l'antenne pour détecter des communications radios dans le voisinage, et activer le module radio. Ainsi, le dispositif d'émission et de réception est utilisé seulement quand nécessaire ; Il se place en position sommeil le reste du temps pour économiser l'énergie du mobile.

## 1.3 Routage dans les réseaux ad hoc

Le routage (*routing*) est le mécanisme d'ouverture et d'entretien d'une communication entre deux nœuds. L'opération est alors supportée par la source, le destinataire et les relais supportant l'échange. Dans un premier temps, la source doit trouver le chemin jusqu'au destinataire. Elle peut s'appuyer sur une connaissance préalable du chemin ou demander à d'autres entités un chemin partiel ou complet. Si la source utilise une information incomplète, une chaîne de relais peut se créer jusqu'à joindre le destinataire. Ce dernier s'appuie alors sur les informations reçues pour retrouver le chemin vers la source et ainsi construire le chemin.

Dans le cas d'un réseau ad hoc, l'opération de routage se heurte à de nombreuses difficultés car la recherche de routes s'appuie sur des informations dynamiques. Des mécanismes (réguliers ou utilisés seulement lors de la recherche de routes) doivent exister pour obtenir une route valable. En clair, les

nœuds ne peuvent s'appuyer sur une information statique, et doivent obtenir lors de la recherche de route une information la plus « fraîche » possible.

Trouver un chemin n'est qu'une partie du problème, il faut pouvoir assurer la stabilité des communications car la mobilité des nœuds peut entraîner de nombreuses reconfigurations des chemins. Ainsi, durant la communication, l'ensemble des relais d'une communication va changer plus ou moins fréquemment.

De plus, par la nature même des réseaux ad hoc, les déconnexions peuvent être un événement normal (par opposition à un événement anormal, dû à une erreur dans un réseau filaire). En effet, un nœud peut se retrouver sans possibilité de joindre le destinataire, simplement par le fait qu'il ne possède pas de voisins ou que le graphe du réseau joignable n'inclut pas le destinataire. Cette erreur oblige la source et/ou certains relais à temporiser des envois et/ou à informer les applications de la source de cet événement.

Dans les sous-sections suivantes, nous allons présenter les trois familles de protocoles de routage : proactifs, réactifs et hybrides. Pour plus d'informations, le lecteur pourra se reporter à un exposé des problèmes [46] et à différentes analyses des protocoles de routage existants [31, 78, 44].

### 1.3.1 Algorithmes proactifs

Dans ce type d'approche (appelé aussi *table driven*), une maintenance régulière du réseau entre les nœuds permet de faciliter la découverte des routes. Le principe est inspiré du protocole de routage Bellman-Ford [48], utilisé entre autres dans les mises à jour des routeurs sur Internet. Chaque nœud maintient des informations pour chaque autre nœud du réseau, avec une table de routage (indiquant par quel voisin passer pour le destinataire). Pour les changements de topologie, le nœud diffuse les modifications de sa table à une partie du réseau. Il existe plusieurs algorithmes, différentiables par le nombre de tables maintenues par chaque nœud, et par la façon de diffuser les mises à jour lors de modifications de la topologie du réseau.

Le protocole DSDV [71] (*Destination Sequenced Distance Vector*) de Perkins *et al.* conserve dans une table les destinations possibles dans le réseau, avec pour chaque entrée le voisin à joindre, le nombre de sauts et un numéro de séquence. Cette dernière information est un numéro choisi par la source, pour permettre aux autres nœuds de connaître l'information la plus récente. Pour diffuser les informations de sa table, le mobile émet à ses voisins deux types de paquets (dans le but de réduire la consommation du médium aérien) : *full dump* contient l'ensemble de la table et *incremental* contient uniquement les parties de la table ayant changé de valeur.

Murthy *et al.* proposent WRP [66] (*Wireless Routing Protocol*). Le protocole maintient quatre tables : la table de distance (la distance entre le nœud et les différents correspondants), de prochain saut (le voisin à joindre pour contacter un mobile dans le réseau), de coût (la latence entre le nœud et les différents destinataires) et de retransmission de messages (avec les informations de mise à jour). Chaque mobile émet régulièrement un message indiquant les changements dans sa table de routage ; Il diffuse également des demandes de confirmation de présence à ses voisins pour les informer des changements topologiques tout en vérifiant la validité de son voisinage.

Le protocole CSGR [20] (*Cluster Switch Gateway Routing*) proposé par Chiang *et al.* est une architecture reposant sur les groupes (voir la section 1.4.4). Chaque groupe possède un chef qui se charge des communications à l'intérieur de sa « tribu. » La maintenance des informations de routage est située dans chaque chef. Ceux-ci conservent une table de tous les autres chefs accessibles dans le réseau, associés aux nœuds passerelles à utiliser pour les joindre. Cette approche est intéressante lors de la gestion de groupes de nœuds restant ensembles, car il y a peu de changement dans la topologie

locale d'un groupe. Mais si de fréquents changements de groupes interviennent, alors la maintenance devient trop coûteuse.

Le protocole OLSR [22, 23] (*Optimized Link State Routing Protocol*) est un algorithme proactif conçu pour minimiser la taille des messages de contrôle. Chaque nœud calcule régulièrement le sous-ensemble MPR ((*MultiPoint Relaying*) de ses voisins, permettant de joindre l'ensemble des mobiles à deux sauts[2]. Ensuite, un nœud diffuse régulièrement un message TC (*Topology Control*) à l'ensemble du réseau. Ce paquet contient l'ensemble de ses voisins l'ayant choisi pour faire partie de leur MPR. Ainsi, un nœud peut associer le voisin à joindre du réseau au nœud voisin permettant de le joindre. Pour réduire les problèmes de diffusion, chaque nœud réémet le message que s'il appartient à l'ensemble MPR de la source locale.

Un des avantages des protocoles proactifs, sous réserve d'une mise à jour correcte de l'ensemble des tables, est le fait de trouver rapidement le destinataire sans devoir au préalable effectuer une recherche dans le réseau complet (l'information pour router les messages est immédiatement disponible). De plus, les pertes de chemin sont relativement peu fréquentes, car les changements de topologie sont diffusés automatiquement. Enfin, chaque nœud possède des informations sur l'ensemble du réseau, ce qui peut se révéler pratique pour la couche application.

Mais les défauts de ces protocoles se révèlent catastrophiques dans le cas de réseaux ad hoc avec une forte mobilité. Premièrement, il existe un coût constant dans le réseau pour diffuser les informations de routage. Même si certains algorithmes réduisent la quantité d'information, cette occupation d'une partie de la ressource radio réduit la quantité disponible pour les communications entre mobiles. Deuxièmement, ce type de protocole n'est pas adapté pour de grands réseaux. En effet, la quantité d'information à diffuser pour une maintenance cohérente augmente proportionnellement au nombre de nœuds. Finalement, une mobilité importante dans le réseau peut entraîner des risques de perturbations importantes. En effet, la quantité d'information devient trop importante pour le réseau car le nombre de messages est fonction des changements topologiques.

### 1.3.2 Algorithmes réactifs

À l'opposé de l'approche proactive, l'approche réactive (ou *source-initiated on-demand*) découvre le chemin quand nécessaire. Lorsqu'un nœud cherche à joindre un correspondant dans le réseau, il utilise un protocole de diffusion. Une fois atteint, le correspondant peut répondre par un message point-à-point qui informe la source de sa présence et du chemin à suivre pour le joindre. Cette opération, représentée par la figure 1.6, peut être renouvelée à un niveau local pour la maintenance des routes.

Le plus connu des algorithmes réactifs est AODV (*Ad hoc On-demand Distance Vector*) [72, 73] par Perking et Royer. Il apporte plusieurs idées au modèle présenté ci-dessus. D'une part, chaque nœud maintient un numéro de séquence pour permettre une meilleure cohérence lors de la recherche de chemins[3] ; Un mobile qui recherche un chemin va utiliser le dernier numéro de séquence connu, dans le but d'éviter l'utilisation de routes trop anciennes. D'autre part, lors de la découverte de chemins, chaque nœud garde une information sur le message de diffusion, en conservant le nœud prédécesseur.Ainsi, lors de la réponse du destinataire, chaque mobile valide le chemin dont il est un des relais. Cette méthode permet d'avoir une taille de paquet minimale et qui ne dépend pas du nombre de relais franchis.

[2] ce protocole de sélection est détaillé en section 3.2.

[3] Le numéro de séquence est un compteur dans chaque nœud. A chaque envoi de message, un mobile copie dans celui-ci la valeur du compteur, puis incrémente ce dernier.

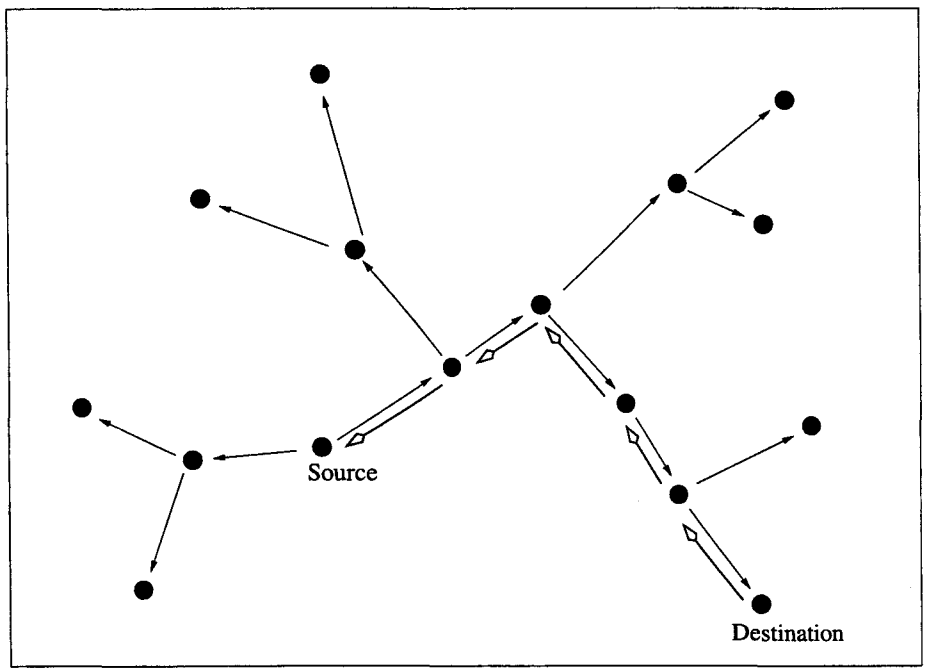



FIG. 1.6 – Diffusion dans le but de chercher une route dans un réseau ad hoc.

Un algorithme très proche d'AODV est DSR [47], proposé par Johnson et Maltz. Les différences les plus notables se situent au niveau du contenu des paquets de création de route et de confirmation de route ; Les deux paquets contiennent la liste des chemins à partir de la source (au lieu de laisser cette information répartie entre les nœuds comme dans AODV). De plus, le protocole gère les liens asymétriques (un nœud $a$ peut joindre un autre nœud $b$, mais $b$ ne peut joindre $a$, par la faute d'une différence de la puissance d'émission entre les deux mobiles).

Une méthode originale, appelée TORA [70] (*Temporally-Ordered Routing Algorithm routing protocol*), maintient un graphe acyclique orienté de l'ensemble du réseau. Chaque nœud choisit de manière localisée le sens de chaque liaison avec ses voisins et modifie ce choix en fonction des changements topologiques. Le principal avantage de cette approche, outre l'absence de boucles dans les routes construites, est que les changements topologiques ne sont transmis qu'à une partie limitée du réseau, un nœud ne retransmettant l'information de changements topologiques que si celle-ci induit des modifications dans le sens des liaisons avec son voisinage.

D'autres protocoles existent, comme par exemple SSR (*Signal Stability Routing*) [28] ou ABR (*Associativity-Based long-lived Routing*) [91]. Très proches d'AODV, ils tiennent compte de la fiabilité des liens, soit en étudiant la puissance du signal en réception (dans le cas de SSR), soit en écoutant les changements topologiques dans le voisinage (dans le cas d'ABR). À partir de ces informations, ils peuvent associer une mesure qualitative à chaque connexion. Ainsi, lors de la construction de la route, un indice de fiabilité est calculé pour chaque route créée, avec une préférence pour les liens ayant un coefficient de stabilité élevé.

Les algorithmes réactifs se révèlent plus adaptés dans le cas de réseaux ad hoc avec une taille importante et/ou une forte mobilité. Le fait qu'ils découvrent la route quand le besoin se fait ressentir permet d'éviter de réserver constamment une partie des communications pour indiquer les changements de topologie. Par contre, le coût de la recherche du chemin peut se révéler très important si la

méthode de diffusion est inefficace (nous étudions le problème de la diffusion dans la section 1.4).

### 1.3.3 Algorithmes hybrides

Certains algorithmes combinent les deux approches précédentes pour essayer de tirer profit de chacune d'elles. On peut citer ZRP (*Zone Routing Protocol*) de Haas [38] qui utilise un protocole réactif au niveau local (*i.e.* avec des voisins situés à une distance inférieure à $k$ sauts et un protocole proactif pour le routage entre groupes (appelés *routing zone*). Pour l'opération de recherche de route, chaque nœud connaît le moyen de joindre les autres dans son groupe. Si le mobile a besoin de contacter un nœud à l'extérieur de cette zone, il utilise le protocole IERP (*Interzone Routing Protocol*) qui envoie une demande de route aux voisins situés à la périphérie du groupe. Ces derniers vérifient alors si le destinataire est dans leur groupe et lui transmettent le message si celui-ci est présent. Dans le cas contraire, l'algorithme est réitéré : chacun de ces nœuds procède à une demande de route vers les nœuds en périphérie de son groupe. Une fois le chemin trouvé, le nœud destinataire renvoie un message point-à-point vers la source. Pour éviter un coût important des méthodes de diffusion entre IERP, certaines optimisations locales à chaque groupe sont proposées dans [38].

L'opération de diffusion est donc une brique majeure de nombreux protocoles de routage. En effet, la diffusion existe naturelement dans les protocoles réactifs, mais aussi dans certains protocoles proactifs (par exemple OLSR) et dans les protocoles hybrides. La diffusion carctérise donc en grande partie les performances du protocole. Dans le cas d'AODV par exemple, il n'y a aucune optimisation de la diffusion, les performances sont donc médiocres et limitées, ce qui réserve ce protocole pour des réseaux de petite taille. Plus généralement, l'utilisation naïve du mécanisme de diffusion se solde par de nombreuses complications, notamment avec les nombreux accès simultanés au médium aérien. Dans la section suivante, nous proposons une analyse du problème de la diffusion, avec une présentation des protocoles de diffusion déjà existants.

## 1.4 Diffusion

La diffusion (ou *broadcast*) est l'opération de transmettre un message à l'ensemble du réseau[4]. Les problèmes de cette opération (*broadcast*) dans un réseau sans fil ont fait l'objet de nombreux travaux avec, comme but premier, la réduction du nombre de réémissions lors de la diffusion d'un message à l'intégralité du réseau. Différentes méthodes sont utilisées, reposant sur une grande variété d'approches : probabilistes, travaux provenant de la théorie des graphes, ou exploitant une caractéristique particulière (comme la qualité des liens par exemple).

### 1.4.1 Caractéristiques

Pour évaluer un algorithme de diffusion, il existe plusieurs caractéristiques.

#### Fiabilité

Une diffusion est dite fiable (*reliable*) lorsqu'elle permet de transmettre l'information à l'ensemble des nœuds joignables. D'un point de vue local, chaque nœud doit alors garantir que l'ensemble de son

[4]En français, le terme diffusion spécifie deux types d'opérations : la transmition d'un message à ses voisins et la transmission d'un message à l'ensemble du réseau. En anglais, on utilise dans le premier cas le mot *narrowcast* et dans le deuxième cas le mot *broadcast*. Pour éviter toute confusion, le terme diffusion utilisé dans la suite de ce document se reporte au deuxième cas.

voisinage est contacté par le message de diffusion. Ainsi, si le réseau est connexe (chaque nœud est joignable), la propriété précédente garantit une couverture totale du réseau. À l'opposé, un protocole de diffusion est dit non-fiable (*unreliable*) lorsque l'algorithme ne garantit pas la diffusion de l'information à l'ensemble des nœuds joignables. Certains algorithmes, comme les protocoles de diffusion probabiliste, rentrent dans cette catégorie, par leur nature stochastique évidente. Une telle propriété peut paraître rédhibitoire mais elle possède certaines caractéristiques intéressantes. Par exemple, certains algorithmes de diffusion peuvent proposer une diffusion partielle de l'information, dans le but d'informer uniquement un sous-ensemble du réseau. Un autre exemple peut concerner le coût élevé de l'accessibilité d'une petite partie difficilement joignable, et dans ce cas, l'algorithme peut se satisfaire de joindre la plus grande partie du réseau pour économiser certaines ressources critiques.

Il est à noter que cette caractérisation est indépendante de la couche MAC. En d'autres termes, la couche MAC est considérée comme idéale ; Aucune transmission n'est perturbée par une autre, et aucun paquet n'est perdu par la suite de collision. Cette précision est importante car, comme la couche MAC fonctionne généralement sur un modèle probabiliste, tout algorithme peut être considéré comme non-fiable lorsqu'il est utilisé dans des conditions réelles.

Dans le cas où l'on considère une couche MAC réelle, si l'algorithme de diffusion utilise un nombre important de retransmissions, alors les probabilités de collision entre deux messages au niveau de la couche MAC s'accroissent de façon significative. Il s'ensuivra qu'un algorithme de diffusion, même fiable, ne pourra joindre l'ensemble du réseau. Le principal dilemme concerne donc l'équilibre à trouver entre la réduction optimale du nombre de paquets lors d'une diffusion (pour minimiser les chances de collisions), et l'augmentation du même nombre de paquets (dans le but de minimiser les risques de perte de connexité du réseau). De plus, comme les collisions ne sont jamais prévisibles, il est intéressant d'avoir un mécanisme de détection de collisions et de récupération.

Nous allons maintenant décrire les différentes propriétés d'un algorithme de diffusion, de manière à caractériser chaque algorithme.

#### Déterminisme

Ce paramètre caractérise le comportement du mobile lors de sa décision de retransmettre à son voisinage le message de diffusion qu'il vient de recevoir. Ainsi, un algorithme de diffusion peut être déterministe ou probabiliste. Dans le premier cas, le mobile prend la décision en fonction de son état et des informations reçues dans le paquet. Le modèle probabiliste, quant à lui, décide d'une probabilité de retransmission (éventuellement à partir de certaines caractéristiques du réseau, et de l'état du mobile).

L'utilisation d'un modèle probabiliste est intéressant pour son comportement en moyenne : même si certaines décisions locales ne donnent pas le meilleur résultat, la réaction de l'ensemble des nœuds permet d'obtenir des résultats acceptables en moyenne (à un niveau global). Cette approche permet de pallier le manque d'information sur le voisinage, en offrant une sélection probabiliste comme hypothèse sur la partie manquante.

#### Information sur le réseau

Chaque mobile déduit, en général, son choix de retransmission à partir d'informations sur la topologie du réseau. Ces indications peuvent être contenues dans le message de diffusion et/ou mémorisées lors des communications précédentes. On peut classer en plusieurs catégories la quantité d'information nécessaire pour chaque algorithme de diffusion.

**Globale** Une connaissance complète du réseau est nécessaire. Mais cela n'implique pas que tous les nœuds aient cette propriété. Cette responsabilité peut être tenue par une seule entité, ou par l'ensemble des nœuds. Dans le premier cas, ce type de configuration est utilisé avec un algorithme centralisé, où un seul nœud contrôle les décisions de retransmission de l'ensemble du réseau. Outre une difficulté inhérente dans le cas d'un réseau avec des nœuds mobiles, ce type de protocole nécessite des communications supplémentaires pour rapatrier la topologie complète vers l'unité de décision, puis diffuser les ordres à l'ensemble du réseau. Dans le deuxième cas, une connaissance complète peut être nécessaire pour chaque nœud. Il faut alors tenir compte du coût, pour chaque nœud, de la connaissance de la topologie complète du réseau (soit le coût pour diffuser une information de $n$ nœuds vers $n$ nœuds).

**Partielle** Une connaissance partielle du réseau est nécessaire ; Un nœud peut connaître une partie de son voisinage, ou plus. On parle de connaissance partielle lorsque la connaissance nécessaire est difficilement identifiable par rapport au voisinage immédiat. Par exemple, dans le cas de la formation de groupes de nœuds (appelés aussi « clusters »), chaque nœud qui appartient à un groupe peut connaître l'intégralité de ses membres, même si il n'est pas en position centrale.

**à N-sauts** Une connaissance du voisinage à $N$ sauts est nécessaire (*i.e.* chaque nœud connaît des informations sur les nœuds joignables avec le même message ayant été relayé au plus $N$ fois). C'est un sous-ensemble de la connaissance partielle du réseau, car on peut le quantifier. Cette connaissance peut être variable : un nœud peut connaître la liste de ses voisins, mais aussi les liens entre ces derniers. Par exemple, si un mobile émet régulièrement un message HELLO avec son identité, alors chaque nœud est en mesure d'avoir une liste des voisins qu'il peut joindre. Si un mobile émet régulièrement un message HELLO avec la liste complète de son voisinage, alors chaque nœud sera en mesure de connaître les voisins à un et deux sauts, les liens entre les nœuds à un saut et les liens entre les mobiles à un saut et les mobiles à deux sauts.

### Le contenu des messages

Pour assurer un bon déroulement de la diffusion, chaque nœud émet des messages concernant des informations sur le réseau, son état interne et/ou sur la diffusion en elle-même. Ce surplus se trouve dans les deux types de paquets utilisés[5] : les messages HELLO et les messages BROADCAST.

Les messages HELLO sont émis régulièrement par chaque nœud pour informer leur voisinage. Ainsi une entité est en mesure de connaître l'ensemble de ses voisins en écoutant les communications. D'autres informations peuvent aussi apparaître dans ces messages. Premièrement, si le mobile possède un dispositif de positionnement (GPS), il peut ajouter sa position au message HELLO dans le but d'en informer son correspondant. Dans ce cas, chaque mobile est en mesure de déduire la topologie complète de son voisinage, (*i.e* les connexions entre chaque voisin à portée). Deuxièmement, un nœud peut ajouter certaines informations sur son état interne, comme le fait d'être relais ou son degré (le nombre de nœuds qu'il peut joindre). Enfin, un mobile peut aussi ajouter la liste de voisins. Ainsi, chaque nœud pourra déduire l'ensemble de la topologie à un saut et tous les nœuds joignables à deux sauts. Il faut signaler que, dans certains cas, il n'est pas nécessaire d'ajouter une information supplémentaire pour informer le correspondant de certains attributs. On peut citer l'exemple des dispositifs de mesure de puissance en réception. Avec un tel mécanisme, un mobile est capable d'évaluer la distance qui le sépare du correspondant qui vient de lui envoyer un message, à partir de la puissance du signal reçu. Mais ces mécanismes sont plus au moins efficaces (voire inopérants) dans certaines conditions (milieux encombrés ou fermés par exemple).

[5] Certains protocoles de diffusion peuvent avoir d'autres types de paquets.

Ces ajouts peuvent se révéler coûteux pour la taille du paquet. D'une part, le message étant émis périodiquement et par tous les mobiles, il est indispensable de minimiser sa taille, afin de réduire les probabilités de collisions (tout en maintenant une quantité d'information exploitable par le protocole de diffusion). D'autre part, la mobilité importante accroît le nombre de messages HELLO, et ainsi les risques de collisions. Il existe un risque d'avoir des difficultés à obtenir un certain niveau de fiabilité si l'algorithme de diffusion s'appuie de façon exagérée sur ces informations. Enfin, en cas de collision de messages HELLO, il est possible que la perte d'information entraîne des erreurs sur la connaissance des caractéristiques et de la topologie des nœuds voisins.

Les messages BROADCAST sont émis lors de l'opération de diffusion. Chacun contient les données à transmettre à l'ensemble des nœuds, mais ils peuvent aussi posséder des informations utilisées par le protocole comme les numéros de séquence, qui permettent d'identifier de manière unique le message de diffusion . Ils peuvent également indiquer des listes de voisins (pour informer le correspondant du voisinage joint par ce message), ou un sous-ensemble de la liste des voisins dans l'émetteur (pour indiquer les voisins qui doivent retransmettre le message).

Encore une fois se pose la problématique de la taille du paquet, mais le contexte d'émission est plus spécifique que celui des messages HELLO. Premièrement, un paquet BROADCAST possède une taille plus élevée, due à la présence des données à diffuser. Les probabilités de collisions sont donc plus importantes. De plus, une diffusion doit se faire dans un temps limité, pour transmettre l'information en un temps raisonnable et pour minimiser l'impact de la mobilité des nœuds sur la diffusion. Le temps écoulé entre la réception d'un paquet et sa réémission doit être le plus court possible. Cet impératif oblige l'ensemble des voisins, qui doivent réémettre le message, à le renvoyer dans un laps de temps très court, augmentant encore les chances de collisions.

Les nombreux problèmes soulevés dans cette dernière partie reflètent le difficile équilibre à mettre en place pour une diffusion complète mais minimisant la surcharge réseau. Pour pouvoir évaluer l'efficacité de chaque algorithme de diffusion, il est nécessaire de posséder des éléments caractérisant l'efficacité de ces protocoles.

### 1.4.2 Préliminaires

Nous allons maintenant définir les principales notations utilisées. Considérons un réseau sans fil multi-saut où tous les nœuds coopèrent dans le but d'assurer des communications entre chacun. Un tel réseau peut être représenté de la manière suivante. Soit un graphe $G = (V, E)$ représentant le réseau sans fil, avec $V$ l'ensemble des nœuds et $E \in V^2$ les arcs donnant les communications directes possibles : $(u, v)$ appartient à $E$ si et seulement si $u$ peut envoyer directement un message à $v$ (on dit alors que $v$ est voisin de $u$). Les couples appartenant à $E$ dépendent de la position des nœuds et de leur portée de communication. Nous prenons l'hypothèse que la portée $R$ de chaque nœud est identique. Soit $d(u, v)$ la distance entre les nœuds $u$ et $v$. L'ensemble $E$ peut-être défini comme suit :

$$E = \{(u, v) \in V^2 | d(u, v) \leq R\}. \tag{1.1}$$

Ce graphe est connu sous le nom de graphe unitaire, avec $R$ comme rayon de transmission. Dans ce graphe, $G = (V, E)$, nous définissons $n = |V|$ comme le nombre de nœuds dans le réseau. Le voisinage $N(u)$ d'un nœud $u$ représente l'ensemble des nœuds voisins de $u$, défini par $\{v|(u, v) \in E\}$. Le degré moyen d'un réseau est la moyenne du nombre de voisins de chaque nœud :

$$deg(G) = \frac{\sum_{i \in V} |N(i)|}{n}. \tag{1.2}$$

### 1.4.3 Évaluer la qualité d'un broadcast

L'efficacité d'un algorithme d'inondation est mesurable avec plusieurs métriques.

**Accessibilité (*Reachibility* ou *RE*) :** le pourcentage de nœuds recevant le message de diffusion par rapport au nombre total de nœuds joignables (c'est-à-dire l'ensemble connexe de nœuds comprenant la source). Si un protocole est parfait, alors il doit être capable de joindre 100% du réseau. Mais certains protocoles peuvent proposer une approche du meilleur effort (*Best Effort*), avec un RE de 90% ou 95% en moyenne.

**Messages de diffusion économisés (*Saved ReBroadcast* ou *SRB*) :** le pourcentage de nœuds joints qui ne réémettent pas le message de diffusion. Plus précisément, $(r-t)/r$ avec $r$ le nombre de nœuds recevant le message et $t$ le nombre de message émis.

**Latence moyenne (*average latency*) :** délai entre l'émission par la source et la dernière réception du message de diffusion.

**Consommation énergétique :** consommation totale du réseau (*i.e.* la somme de l'énergie consommée par tous les nœuds pour la diffusion d'un message). Cette mesure est utilisée dans le cas d'algorithmes de diffusion prévus pour augmenter la durée de vie des batteries de chaque mobile (le problème d'économie d'énergie est abordé dans les chapitres 4 et 5). Dans le cas où les mobiles n'ont qu'une seule portée d'émission, la consommation d'énergie est proportionelle au SRB.

Chacune de ces métriques est utilisée pour l'évaluation des protocoles de diffusion. Ils nous permettront dans les chapitres suivants de quantifier les résultats obtenus dans nos travaux. Pour l'instant, il est nécessaire de présenter les algorithmes de diffusions existants :

### 1.4.4 Études des protocoles existants

#### Inondation

L'algorithme le plus trivial pour diffuser un message est le protocole d'inondation (*blind flooding*). Son fonctionnement est simple : chaque nœud qui reçoit le message d'inondation pour la première fois le réémet pour ses voisins, le mécanisme ne nécessitant qu'une table pour mémoriser les identifiants des messages d'inondation.

Les identifiants des messages d'inondation reposent sur les numéros de séquence (*sequence number*). Chaque mobile possède un compteur interne (initialisé à zéro). Lors de l'envoi d'un message de diffusion, le mobile à l'origine de la diffusion ajoute la valeur du compteur au message puis incrémente celui-ci. Ainsi, chaque nœud est en mesure d'évaluer la «fraîcheur» d'un message de diffusion par rapport à un autre, en comparant leurs numéros de séquence. Cette méthode est déjà utilisée dans les réseaux filaires (dans le protocole de transport TCP par exemple) pour permettre la fragmentation des paquets, le numéro de séquence utilise comme unité le nombre d'octets transmis.

Bien qu'il ne nécessite qu'une table pour mémoriser les identifiants des messages d'inondation, l'algorithme d'inondation est quand même un algorithme coûteux. Malgré sa simplicité, il impose une charge énorme au réseau, car chaque voisin se doit de renvoyer le message. Ce grand nombre de mobiles essayant d'accéder en même temps entraîne une probabilité importante de collisions parmi les rediffusions. Car les messages d'inondation sont envoyés sans accord préalable, en minimisant le temps d'attente dû à l'écoute du médium (pour réduire le temps de latence entre la réception et la réémission). Le défaut est simple, l'algorithme est naïf. Lorsque deux mobiles très proches se décident

à réémettre le même message, une grande partie des voisins de ces deux mobiles vont recevoir exactement la même information. Cette utilisation doublon est pourtant inutile. De plus, tous les voisins vont essayer de réémettre le message, entraînant ainsi des contentions pour l'accès au médium.

Ce problème, dit de la tempête de messages de diffusion (*Broadcast Storm Problem*), a été traité en profondeur par Ni *et al.* [67]. Les auteurs proposent cinq modifications simples de l'algorithme d'inondation pour étudier les effets induits.

**Probabiliste (*Probabilistic Scheme*) :** lorsqu'un mobile reçoit un message pour la première fois, il le réémet avec une probabilité $P$, fixée au départ. Même s'il offre une accessibilité correcte (supérieure à 90%) dans le cas de très forte densité (avec un SRB égal à la valeur $P$), il est néanmoins nettement en position de faiblesse, car chaque nœud possède les mêmes chances de réemettre quelle que soit sa position par rapport au voisin qui lui transmet le message de diffusion, sans tenir compte de la topologie du voisinage.

**Schéma fondé sur le comptage (*Counter-Based Scheme*) :** un mobile ne réémet pas un message s'il l'a déjà entendu plus de $C$ fois. Plus précisément, un mobile attend un certain temps entre la réception et la réémission. Durant cette période, s'il reçoit le nouveau message d'inondation il reprogramme à plus tard sa transmission. Lorsqu'il doit finalement émettre, il regarde s'il a reçu moins de $C$ fois le message d'inondation, auquel cas il émet le message. Dans le cas contraire, il oublie celui-ci. Les auteurs, après expérimentation, recommandent une valeur $C \geq 3$. On obtient dans ce cas une bonne accessibilité mais un SRB trop dépendant de la densité.

**Schéma fondé sur la distance (*Distance-Based Scheme*) :** un mobile ne réémet pas un message s'il le reçoit d'un mobile situé à une distance inférieure à $D$. Comme dans la méthode précédente, il attend un certain temps entre la réception et la réémission, pour laisser une chance à tous les autres voisins d'envoyer leurs messages. Si un de ces messages arrive d'une distance inférieure à $D$ alors il annule son émission. Dans le cas contraire, et au bout du temps d'attente, il réémet le message de diffusion. C'est le protocole le plus mauvais des cinq, offrant un SRB pratiquement nul en cas de forte densité. Le défaut provient du fait que même si un mobile a entendu plusieurs fois le message de diffusion, il peut quand même le réémettre.

**Schéma fondé sur la position (*Location-Based Scheme*) :** un mobile ne réémet pas un message si la couverture supplémentaire par l'envoi de son message est inférieure à un seuil $A$. Encore une fois, un délai d'attente entre la réception et l'émission permet d'optimiser le nombre de voisins qui émet leur message. Ce modèle obtient les meilleurs résultats, avec une excellente économie de messages (de l'ordre de 40% à 60%), une accessibilité proche de 100% et un faible temps de latence. Il est le plus efficace car il utilise l'information la plus précise possible (une information de position).

**Schéma fondé sur les groupes (*Cluster-Based Scheme*) :** cet algorithme se déroule en deux phases. Dans un premier temps, chaque mobile détermine son état dans le réseau. Le mobile qui possède l'ID la moins élevée de son voisinage devient le chef du groupe (*clusterhead*), et ses voisins font alors partie de son groupe (*cluster*). Un mobile capable de joindre des nœuds appartenant à deux groupes distincts devient une passerelle (*gateway*). Lors de la diffusion, seuls le chef de groupe et les passerelles retransmettent le message de diffusion. Le protocole se révèle moyen, offrant une accessibilité très moyenne dans le cas de densité faible. Cette diminution est due à la baisse du nombre de nœuds participant à la propagation du message de diffusion. Un présentation des groupes (appelés aussi clusters ou grappes) est détaillée dans la sous-section suivante.

Plusieurs résultats intéressants peuvent être extraits de cet article. Plus l'information concernant la topologie voisine est précise, plus il est possible d'obtenir un protocole d'inondation efficace (*i.e.* qui

maximise RE et SRB). Les solutions exploitant le maximum d'information sur la topologie (*distance-based*, *location-based* et *cluster-based*) mais aussi sur les communications en cours (*counter-based*) obtiennent les meilleurs résultats. Les auteurs soulignent les relations entre RE et SRB qui montrent la difficulté d'obtenir des résultats parfaits à cause de l'équilibre étroit entre ces deux paramètres. De plus, ils présentent la réaction à la montée en charge des cinq protocoles. Ceux-ci réagissent de la même manière lors d'un nombre élevé de messages d'inondation en cours : l'accessibilité décroît, particulièrement en cas de faible densité. Enfin, il faut noter que ces dispositifs peuvent nécessiter un dispositif de positionnement, qui n'est pas nécessairement disponible.

L'un des schémas proposés se concentre sur la formation de grappes pour mettre en place une hiérarchie dans l'organisation des nœuds. Nous allons étudier dans la section suivante les différentes variantes de cette approche.

**Fondé sur les groupes**

L'idée sous-jacente dans les groupes est celle de hiérarchie parmi les nœuds, en les séparant en plusieurs groupes. Le réseau est alors décomposé en un ensemble de domaines, chacun pouvant contenir une hiérarchie de sous-domaines. Lorsqu'une requête est initiée par un nœud, elle est transmise au chef de groupe, puis peut remonter dans la hiérarchie jusqu'à joindre un chef de niveau supérieur qui pourra la rediriger vers le sous-domaine de destination, pour enfin joindre le ou les correspondants. Une telle organisation est présentée dans la figure 1.7. Au vu de la structuration du réseau, il est logique que certains nœuds aient des statuts spécifiques. Certains sont chargés de maintenir les communications dans le groupe qui leur est affecté, tandis que d'autres se chargent de relayer les messages entre groupes.

Un chef de groupe (*Cluster Head*) est le nœud chargé de diriger les communications du groupe, éventuellement en gérant le partage de la bande passante entre les nœuds du groupe. Il est élu de manière simple, par exemple avec l'algorithme *Lower ID* [57] (qui prend l'identité la plus basse) : chaque nœud émet un message avec son ID puis, lorsque chacun a connaissance de l'ensemble de son voisinage, le mobile avec la plus faible ID du voisinage se proclame chef en diffusant un message à l'ensemble de ses voisins. Une variante de cet algorithme [18] utilise comme critère de sélection le degré de chaque nœud (*i.e* le plus grand nombre de voisins) pour privilégier les nœuds ayant potentiellement sous leur tutelle le plus de voisins (en cas d'égalité, la plus basse ID est privilégiée).

Une passerelle (*Gateway*) est un nœud chargé de faire communiquer les groupes entre-eux. Elle appartient donc à deux groupes différents et doit être capable de joindre les chefs de chacun de ces groupes (soit par communication radio directe, soit en connaissant le chemin jusqu'à eux).

Pour effectuer une diffusion dans cette architecture, la méthode la plus simple proposée dans [68] est de n'autoriser que les chefs de groupe et les passerelles à réémettre le message de diffusion. Cette idée offre un SRB de l'ordre de 50%, mais demande une phase de création des groupes. Plus grave, ce modèle est très sensible à la mobilité et le phénomène d'effet en chaîne [86] provoque un encombrement réseau important dû à la recréation des groupes et la perte des messages d'inondation.

Le modèle de grappes, avec sa structure hiérarchique sous-jacente, se trouve handicapé par la nécessité de reconstruction des groupes lors des changements topologiques. Une idée pour pallier à cet inconvénient est donc la possibilité d'offrir une structure capable de s'adapter aux mouvements dans le réseau. Un ensemble dynamique de construction de sous-graphes, répondant à ce problème, est proposé dans la section suivante.

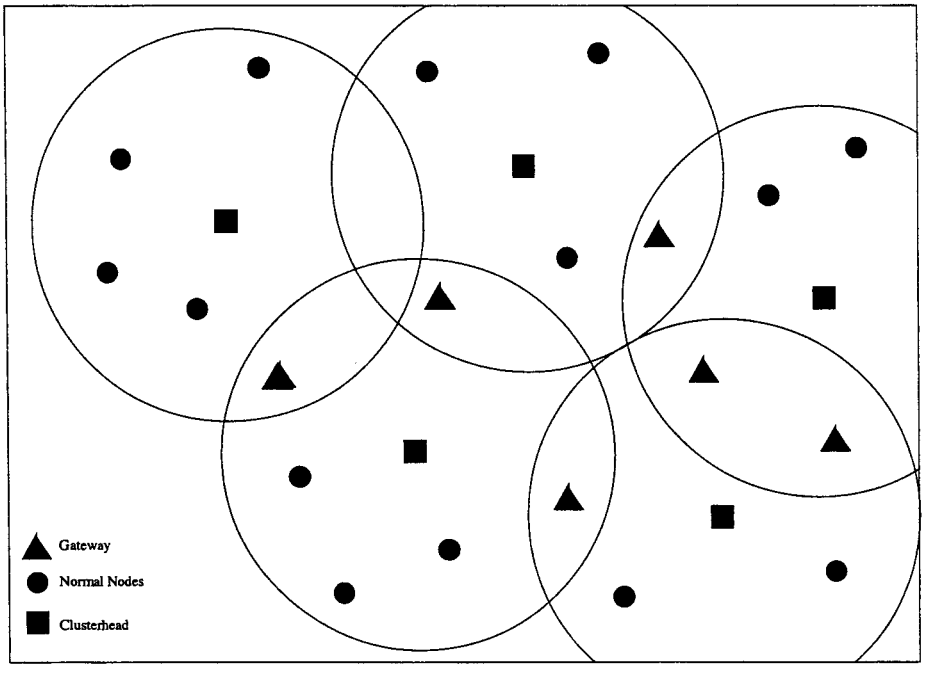



FIG. 1.7 – Exemple d'une formation de groupes.

**L'approche basée sur les ensembles dominants**

Un ensemble dominant (*dominating set*) est une notion de la théorie de graphes. En reprenant les notations développées dans la section 1.4.2, un sous-ensemble $D$ de $V$ est dit dominant si et seulement si tout nœud de $V$ est soit dans $D$ soit voisin d'un nœud de $D$. Plus précisément, l'ensemble $D$ est dominant si et seulement si :

$$\forall i \in V \quad i \in D \wedge (\exists j \in D \quad i \in N(j)) \tag{1.3}$$

Dans un réseau ad hoc, l'ensemble dominant doit être connexe pour assurer une diffusion complète. Un graphe est dit connexe si tous les nœuds sont joignables, c'est-à-dire qu'il existe toujours un chemin constitué d'arcs reliant deux nœuds du graphe. Cette propriété est très importante dans le cas des ensembles dominants, car il garantit que chaque nœud de l'ensemble dominant peut joindre n'importe quel autre dans ce même ensemble. L'algorithme de diffusion est alors très simple : seuls les nœuds de l'ensemble dominant réémettent le message. Chaque nœud de l'ensemble dominant couvre alors l'ensemble de ses voisins, garantissant ainsi une couverture complète du réseau.

Wu et Li proposent dans [100] une méthode simple pour construire un ensemble dominant connexe de manière localisée à partir des informations sur les voisins à deux sauts dans un réseau sans fil. Les auteurs introduisent le concept de nœud intermédiaire : si un nœud $u$ a deux voisins $v$ et $w$ qui ne peuvent se joindre, alors $u$ décide par lui-même qu'il est intermédiaire. Pour déduire cette information, chaque nœud émet régulièrement un message HELLO contenant son identité et la liste de ses voisins.

Deux règles d'élimination sont utilisées par la suite pour réduire l'ensemble dominant constitué de nœuds intermédiaires :

**Règle 1 :** Soient deux nœuds intermédiaires voisins $u$ et $v$. Si chaque voisin de $v$ est aussi un voisin de $u$, et l'identifiant de $u$ est inférieur à l'identifiant de $v$, alors $v$ n'est pas une passerelle

intermédiaire (*inter-gateway*).

**Règle 2 :** Soit trois nœuds passerelles intermédiaires $u$, $v$ et $w$ et voisins mutuels. Si chaque voisin de $v$ est un voisin de $u$ et $w$ et $v$ a le plus bas identifiant des trois, alors $v$ n'est pas une passerelle (*gateway*).

Ces deux règles permettent d'éliminer les nœuds voisins couvrant les mêmes groupes de mobiles. De plus, pour fonctionner de manière décentralisée sans utiliser de messages supplémentaires, l'identifiant permet de prendre la décision du mobile qui se retire, ce qui offre l'avantage de ne pas nécessiter de communication supplémentaire pour que chaque nœud découvre son état. Enfin, le temps de calcul pour évaluer son état est de l'ordre de $0(n^3)$, avec $n$ nombre de voisins.

Stojmenović *et al.* [85] proposent de remplacer la comparaison des identifiants par une comparaison des degrés respectifs de chaque nœud. Cette amélioration permet de privilégier les nœuds possédant le plus de voisins, et donc de minimiser le nombre de passerelles dans le réseau.

Dai et Wu [26] proposent d'offrir une généralisation à k-voisins au lieu de 1 ou 2 voisins (comme spécifiée par les règles 1 et 2). Un noeud $u$ est dit « couvert » par un sous-ensemble $S$ de son voisinage si et seulement si les 3 conditions suivantes sont respectées :

- l'ensemble $S$ est connecté,
- tout voisin de $u$ est le voisin d'au moins un nœud de $S$,
- tous les nœuds de $S$ ont un identifiant supérieur à celui de $u$.

Un nœud appartient à un ensemble dominant si et seulement si il n'existe pas de sous-ensemble qui le couvre complètement.

### Les algorithmes dépendants de la source

Pour permettre à une diffusion d'être efficace, il faut garantir que tous les nœuds à deux sauts de la source reçoivent le message. Si cette règle élémentaire est utilisée par chaque nœud, alors tous les nœuds connexes du réseau pourront être joints. Pour permettre une diminution du nombre de nœuds qui vont réémettre, un sous-ensemble des voisins peut suffire pour joindre l'ensemble des voisins à deux sauts. Lorsque cet ensemble est choisi, un nœud émet son message d'inondation avec la liste des voisins devant réémettre celui-ci. On parle alors de nœud relais (*forwarding nodes*). Le problème est de trouver ce sous-ensemble. Or, c'est un problème NP-complet [56], et il faut utiliser une approche heuristique pour découvrir un ensemble proche de la solution optimale.

Qayyum *et al.* proposent la méthode du relais multi-points (*Multi-Point Relaying method* ou *MPR*) [76]. C'est un protocole évaluant un sous-ensemble du voisinage pour joindre l'ensemble des nœuds à deux sauts. Lors de la diffusion, chaque nœud ajoute à son message la liste de ses voisins qui doivent réémettre le message. Plus précisément, chaque nœud diffuse régulièrement dans ses messages HELLO la liste de ses voisins. Ainsi, chaque nœud possède une connaissance de la topologie réseau à deux sauts. À chaque changement de la topologie locale, chaque nœud calcule un ensemble minimal de voisins pouvant joindre l'ensemble des nœuds à deux sauts. Ce problème étant NP-complet comme le montre les auteurs, une méthode heuristique peut trouver une bonne approximation du sous-ensemble minimal. L'heuristique proposée est simple. Soit l'ensemble $MPR(x)$ contenant le sous-ensemble de relais multi-point du nœud $x$, $N(x)$ l'ensemble des voisins du nœud $x$ et $N^2(x)$ l'ensemble des voisins à deux sauts du nœud $x$.

1. L'heuristique ajoute à $MPR(x)$ les nœuds de $N(x)$ qui sont les seuls voisins de certains nœuds de $N^2(x)$. Il répète cette opération tant qu'il reste des nœuds $i \in N^2(x)$ tel q

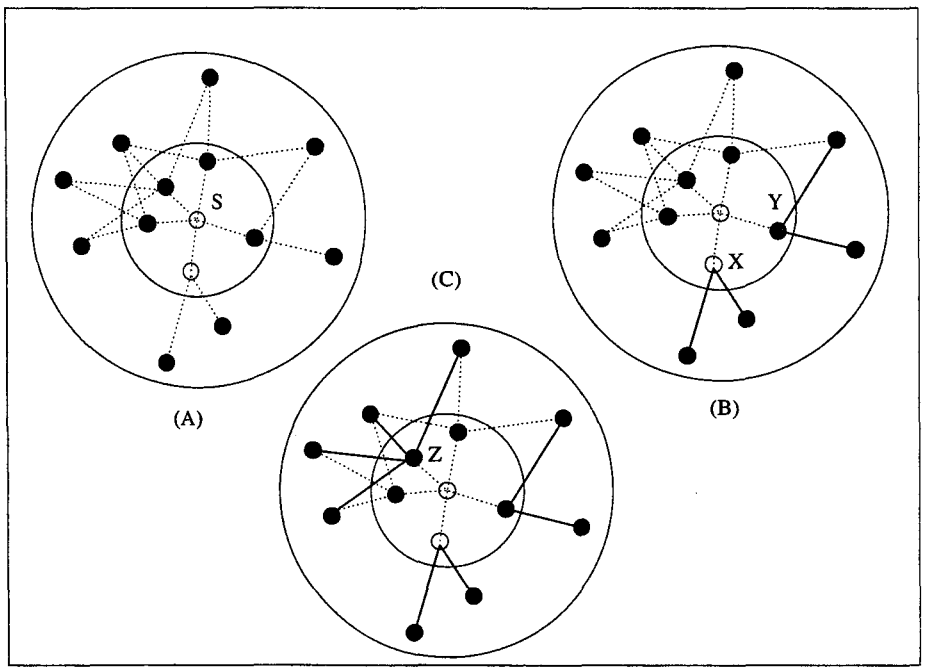



FIG. 1.8 – Exemple de sélection d'un sous-ensemble du voisinage avec MPR.

2. Tant qu'il existe encore des nœuds $i \in N^2(x)$ qui ne sont pas couvert, l'heuristique ajoute à $MPRx)$ un nœud $j \in N(x)$ avec le nombre maximal de voisin non couverts.

Un exemple du fonctionnement de l'algorithme MPR est donné avec la figure 1.8. Dans la situation de départ (A), le nœud source $S$ connaît l'organisation du réseau à deux sauts, c'est-à-dire les connections entre lui-même et ses voisins, les connections entre tous les voisins à un saut, et les connections entre les voisins à un saut et les voisins à deux sauts. Pour la première étape de l'heuristique (B), les nœuds $X$ et $Y$ sont sélectionnés car ce sont les seuls à pouvoir joindre des nœuds isolés à deux sauts. La deuxième étape (C) choisit le nœud $Z$ car c'est le nœud qui possède le plus grand nombre de voisins à deux sauts de $S$, non couverts par l'étape précédente. L'heuristique s'arrête car il ne reste plus de nœuds à deux sauts non couverts.

Lou et Wu [61] présentent deux méthodes se rapprochant du précédent algorithme. La première, baptisée *Total Dominant Pruning* ou TDP, ajoute la liste des voisins à deux sauts dans les messages de diffusion. À la réception de ce message, chaque nœud peut déduire les nœuds qui restent à joindre et ainsi choisir un sous-ensemble des voisins à un saut pour couvrir l'ensemble des nœuds à deux sauts non joints. Cette méthode a le désavantage d'alourdir sensiblement la taille du paquet de diffusion. Pour pallier à cet inconvénient, le second protocole *Partial Dominant Pruning* ou PDP déduit les nœuds à joindre à partir de la liste de voisins de l'émetteur et de sa liste de voisins à deux sauts. La taille du message de diffusion est ainsi réduite mais l'algorithme donne des résultats moins bons que TDP.

### Le mécanisme d'élimination des voisins

Par la nature même de la diffusion, chaque nœud reçoit les messages émis par l'ensemble des mobiles, même si ceux-ci ne lui étaient pas destinés. Il peut donc prendre conscience des informations

que chaque nœud a reçu. Dans le cas d'un message d'inondation, un mobile peut savoir quels sont les mobiles qui ont ou n'ont pas reçu le message.

Pour garantir une accessibilité quasi-parfaite[6], chaque mobile peut ajouter à son message d'inondation sa liste de voisins. Ainsi, chaque nœud, en comparant sa liste de voisinage à celle contenue dans le message d'inondation, peut déduire quels sont les mobiles qui ont déjà reçu le message. Au bout d'un certain temps, lorsque le message d'inondation a été diffusé dans tout le réseau (ou tout au moins, dans l'ensemble du voisinage), chaque nœud regarde la liste de ses voisins. Si au moins un des nœuds n'a pas été contacté par le message d'inondation, il peut réeéettre son message. Un exemple du fonctionnement du mécanisme d'élimination des voisins est présenté dans la figure 1.9.

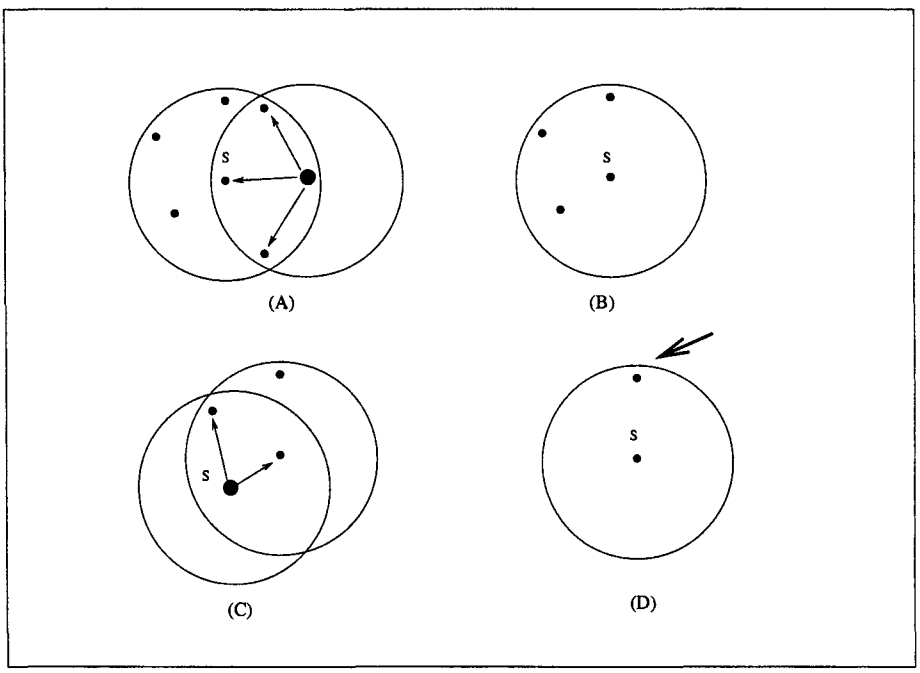



FIG. 1.9 – Exemple du mécanisme d'élimination des voisins : le nœud $S$ écoute les communications dans (A), (B) et (C). Il peut déduire en (D) qu'un nœud n'a pas reçu le message.

Ce procédé n'est pas parfait. Par exemple, si un des voisins $B$ d'un nœud $A$ a été contacté par un mobile éloigné et qu'il ne réémet pas le message d'inondation, alors le mobile $A$ peut croire que ce mobile n'a pas été joint et donc se forcer à réémettre son message d'inondation. Ce surcoût peut dépendre de la densité du réseau et du protocole de diffusion utilisé.

Le problème de diffusion est donc conséquent, et le travail présenté dans cette thèse propose de nouvelles idées, avec l'utilisation d'algorithmes de réduction de graphe ou d'une approche probabiliste. Bien que le travail proposé se concentre sur le problème d'inondation, il est peut-être intéressant de dresser une liste non-exhaustive des différentes problématiques existants dans les réseaux ad hoc.

[6]Une accessibilité parfaite n'est jamais sûre, en raison de la nature non-déterministe de la couche MAC.

## 1.5 Autres défis des réseaux ad hoc

Après avoir présenté les problèmes inhérents au routage, à l'accès à la couche MAC et aux protocoles de diffusion, cette section propose un rapide survol des autres défis, et les travaux actuels qui en découlent, autour des réseaux ad hoc.

**Changement d'échelle :** l'augmentation du nombre de nœuds ou de la taille du réseau peut entraîner des diminutions de performances au niveau des protocoles. Il peut être intéressant de voir le comportement des protocoles dans de tels conditions

**Problème de l'énergie :** chaque entité du réseau consomme de l'énergie, surtout l'émission et la réception des communications. De nombreux travaux s'intéressent à la réduction de la consommation. Une des idées est d'offrir une politique d'alternance des communications entre les nœuds. Une autre idée est de réduire la portée des nœuds, tout en maintenant une connexité complète du réseau.

**Sécurité :** au vu du modèle totalement décentralisé des réseaux ad hoc, la sécurité de cette architecture devient un point très important. Elle peut se situer au niveau des données, où il est nécessaire d'établir un système de chiffrage et/ou d'authentification entre la source et le destinataire. Cette mesure sert alors à éviter que tous les mobiles dans le réseau (qu'ils soient relais du message ou simple mobile entendant les communications dans leur voisinage) puissent espionner ou même modifier les échanges entre ces deux correspondants. De même, le problème d'authentification, bien connu dans le réseau Internet, nécessite la mise en place de serveurs de clés et/ou de certificats de façon totalement décentralisée. Pour plus d'information, on pourra se référer à [102].

**Intergiciels :** une fois mise en place les protocoles de bas niveau (routage, découverte), il existe aussi l'installation de protocoles au niveau applicatif, dans le but d'exploiter les capacités du réseau. Le but est de pouvoir offrir certaines possibilités comme la qualité de service, l'utilisation d'applications distribuées et la distribution de services à l'intérieur du réseau. Ce domaine est étudié dans notre équipe, avec notamment des recherches sur la détection de partition dans un réseau ad hoc [40, 41].

**Connexion à Internet :** concernant la connexion à Internet, un mobile peut éventuellement être relié par plusieurs réseaux ad hoc ou par réseau filaire (lorsque l'utilisateur rentre chez lui et connecte son ordinateur à son modem). La nécessité d'un routage à plus grand grain, c'est-à-dire d'une possibilité de gérer la mobilité sur Internet quel que soit son point d'accès, doit exister. Une solution élégante comme Mobile IP existe, et permet d'attribuer à un mobile une adresse IP permanente quelle que soit sa position dans le réseau des réseaux. Mais son utilisation, de manière transparente dans les réseaux ad hoc, reste néanmoins à étudier.

# Deuxième partie

# Diffusion probabiliste et diffusion indépendante de la source

# Chapitre 2

# Diffusion probabiliste biaisée

Un algorithme de diffusion a deux objectifs : permettre de joindre l'ensemble des nœuds du réseau tout en minimisant le nombre d'émissions nécéssaires pour une telle opération. Ces deux paramètres sont dépendants, et un bon algorithme doit être capable de trouver le bon équilibre entre les deux, en fonction de l'environnement et de l'objectif à atteindre. Dans ce chapitre et le chapitre 3, nous allons proposer deux algorithmes de diffusion qui ont pour but de réduire le nombre de messages nécessaires pour cette opération.

## 2.1 Approches

L'algorithme BRP (*Border Retransmission Probabilistic*) [13, 14] proposé par la suite est fondé sur un certain nombre d'idées innovantes. L'environnement considéré est un ensemble de nœuds mobiles munis d'interfaces radios (idéalement 802.11b) sans système de positionnement. Ce manque d'information sur la position est à la base de deux nouveaux concepts fondamentaux dans BRP. Premièrement l'utilisation d'une approche probabiliste pour permettre un comportement global cohérent en moyenne, cela sans échange supplémentaire entre nœuds. Et deuxièmement, la possibilité d'évaluer une métrique représentant la distance entre deux nœuds sans l'aide d'outil de positionnement.

### 2.1.1 Probabilité

L'utilisation d'un algorithme probabiliste dans les réseaux sans fil semble être une idée impopulaire parmi les algorithmes de routage ou d'inondation. Dans la course à l'optimisation de tels réseaux (nécessaire, en raison de la capacité limitée du médium aérien), le comportement global obtenu lorsque tous les nœuds possèdent un algorithme probabiliste naïf est souvent médiocre, comme le montre certains articles [67, 80]. Une très grande majorité des algorithmes existants utilisent donc plutôt une approche déterministe, et offrent de bons résultats. Pourtant, cette dernière idée possède des défauts particulièrement génants dans certains cas.

Considérons la connaissance de l'environnement comme exemple. Elle peut être précisée à plusieurs niveaux (voir section 1.4.1). Avec les notations définies dans la section 1.4.2, si chaque nœud émet régulièrement un message avec un intervalle $t$, alors un nœud $x$ peut connaître les liens entre lui-même et ses voisins ($(x, i) \subset E, i \in N(x)$), comme le montre le schéma 2.1(A). Cette information possède une validité au plus sur une durée $t$. Si chaque nœud ajoute à ce message la liste de ses voisins, alors $x$ connaît les mêmes informations avec la même durée de validité mais aussi l'identité des nœuds dans le voisinage à deux sauts ($N^2(x)$), les liens qui relient les nœuds à deux sauts

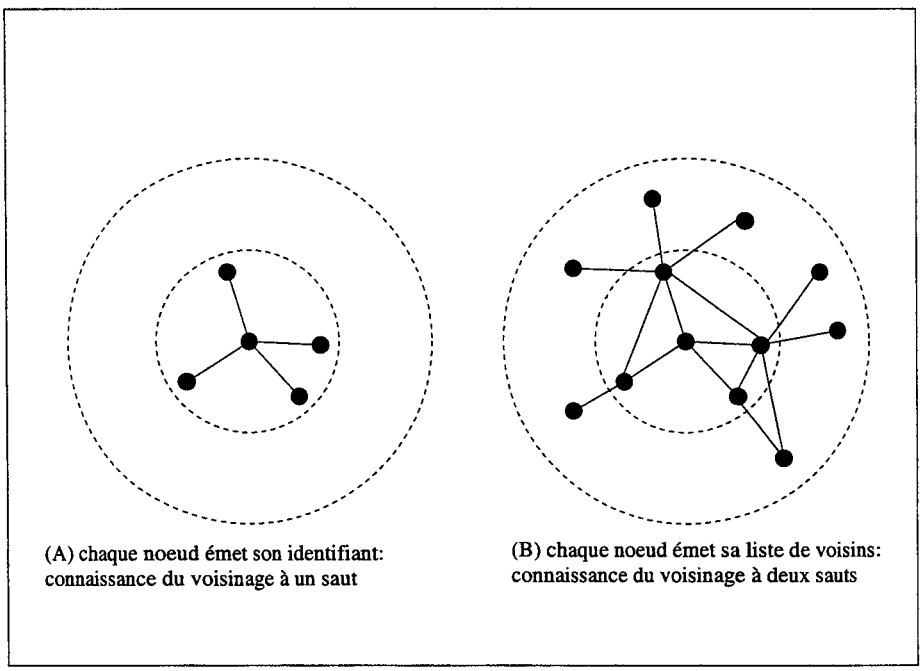



FIG. 2.1 – Connaissance du voisinage à un et deux sauts.

avec les nœuds à un saut ($(i,j) \subset E, i \in N(x), j \in N^2(x)$), et les liens entre les nœuds à un saut ($(i,j) \subset E, i,j \in N(x)$), comme montré dans le schéma 2.1(B). Cette seconde partie est néanmoins valide pour le nœud x au plus sur une durée $2t$. En effet, un nœud qui réémet une information sur son voisinage direct a, au plus, une garantie pour une durée $t$. Mais cette information est rediffusée par tout le voisinage donc elle possède une durée de validité égale au plus à $t + t = 2t$ pour tout nœud ne recevant que ce second message. Cette règle est généralisable à $n$ sauts, avec la validité sur l'information au plus de $n \times t$. L'information sur le voisinage dépend donc d'une part de la durée d'émission entre deux messages HELLO, et d'autre part de l'information topologique du voisinage transportée et prise en compte par chaque nœud. Si la durée de validité maximale est trop importante par rapport aux déplacements de chaque nœud, on peut s'attendre à des problèmes de cohérence.

Un autre défaut concerne la fiabilité des informations transmises. Les données utilisées par le protocole de diffusion sont prises « à la lettre » : chaque information émise par le voisinage est considérée comme valide et aucune supposition n'est faite sur sa véracité. Pourtant, certains messages peuvent entrer en collision avec d'autres, ce qui va donner une information incomplète. De plus, dans le cas particulier des réseaux ad hoc composés d'objets mobiles, les déplacements des nœuds peuvent induire une information erronée : un nœud peut s'appuyer sur un ou plusieurs nœuds pour la rediffusion, sans savoir que ceux-ci ne sont plus à portée de communication, ou sont indisponibles. Cette situation peut se rencontrer dans des réseaux à très forte mobilité, avec des protocoles possédant un long temps d'attente entre chaque message HELLO[1], ou dans le cas où chaque nœud possède une faible portée.

Pour décider s'il doit rediffuser son message, le protocole de diffusion peut donc exploiter une information en partie fausse (soit par le manque d'une partie, soit par l'erreur engendrée sur une partie). Certains protocoles, comme MPR [76] ou les différentes versions de Dominating Set [26, 61, 86], utilisent des procédés qui s'appuient sur une connaissance complète mais non vérifiée du voisinage à

[1] cette caractéristique peut s'apercevoir dans le cas de réseaux avec une bande passante très limitée.

un ou deux sauts. Des erreurs dans les transmissions peuvent alors introduire un dysfonctionnement et donner un algorithme ne recouvrant pas complètement l'ensemble du réseau connecté.

L'approche probabiliste quant à elle présente l'avantage de donner un bon comportement en moyenne[2]. Cette déclaration possède une propriété très intéressante : il n'est pas nécessaire d'avoir de communication spécifique pour obtenir une réduction globale du coût du réseau : une partie des nœuds ne réémettant pas à la suite d'un tirage aléatoire défavorable. Ainsi, même si des erreurs sont présentes dans les messages, la réduction se fait sans l'aide d'interaction entre les nœuds, comme un phénomène de groupe visible à l'échelle globale.

L'algorithme proposé par la suite propose un aspect décentralisé « à l'extrême ». La décision est localisée, fondée sur le voisinage (ce que font d'autres protocoles). Mais cette décision ne privilégie pas une optimisation locale, dans le but de maximiser une rediffusion correcte. Au contraire, la décision est prise de façon à obtenir un comportement correct dans l'ensemble du groupe.

Les résultats obtenus par les méthodes probabilistes déjà proposées [67, 80] possèdent le défaut de ne pas tenir compte des informations topologiques. Il en résulte une efficacité assez faible, car chaque nœud a la même probabilité de réémettre, quelle que soit sa position dans le réseau. Avec le protocole proposé par la suite, la combinaison de l'approche probabiliste et des informations sur le voisinage permet d'augmenter de façon significative l'efficacité de l'approche probabiliste.

### 2.1.2 Mesure de la distance

De nombreux protocoles de diffusion, mais aussi de routage [5, 64], utilisent un outil de positionnement pour pouvoir évaluer les distances entre les nœuds. Cet accessoire peut donner une position relative à une référence globale ou à une référence locale. On peut citer plusieurs exemples de tels systèmes de positionnement :

**GPS** (ou *Global Positionning System*) [49] : système permettant de donner sa position par rapport au repère terrestre. Plusieurs satellites synchronisés envoient régulièrement des messages donnant leur position. Un GPS peut alors calculer les différences entre l'arrivée des messages, et déduire sa position par interpolation. La précision d'un tel mécanisme[3] se situe entre la dizaine de mètres et le mètre (si le GPS est immobile et avec certaines optimisations logicielles et/ou matérielles) ;

**Mesure de puissance :** à la réception d'un signal radio, une interface réseau peut[4] mesurer la puissance reçue. Si le nœud est capable d'associer à cette valeur une mesure de la distance, il peut alors déduire à quelle portée se situe l'émetteur du signal ;

**Différence de phase :** une interface radio possédant deux antennes peut découvrir selon quel angle d'arrivée le signal radio d'un voisin lui est arrivé. Il lui suffit pour cela de calculer la différence de temps entre l'arrivée du signal sur chaque antenne [75].

Cet ensemble d'outils facilite énormément la mise en œuvre des protocoles pour un réseau sans fil. Mais ils sont assujettis à de nombreuses conditions :

[2] par cette phrase, j'entends que, dans le cas où chaque nœud a la même chance de réémettre, la diminution globale du nombre de messages de rediffusion de l'ensemble du réseau sera fonction du pourcentage de réémission.

[3] et le niveau de perturbation introduit par les autorités en charge de la régulation, pour éviter une trop grande précision pour les GPS civils (actuellement, cette erreur engendrée par les satellites est désactivée, mais elle peut être remise en place dans certaines situations).

[4] si le dispositif technique le permet.

**La disponibilité :** pour pouvoir fonctionner, certains de ces mécanismes nécessitent des dispositions particulières. Dans le cas du GPS par exemple, l'entité cherchant à se positionner doit être dans un endroit où elle peut capter l'ensemble des signaux satellites. Son utilisation à l'intérieur d'un bâtiment peut le rendre inopérant ;

**L'encombrement :** chacun de ces mécanismes nécessite l'ajout de nouveaux éléments. Un module GPS nécessite l'utilisation de plusieurs microprocesseurs. Pour sa part, la mesure de puissance demande des moyens d'accès à l'information de puissance reçue. La différence de phase nécessite quant à elle deux antennes, mais aussi les circuits nécessaires à chacune d'elles ;

**L'efficacité :** les conditions particulières d'utilisation de ces procédés introduisent une marge d'erreur qu'il faut évaluer. Le GPS possède plusieurs précisions, selon le statut et la mobilité vis-à-vis du GPS. La mesure de puissance et la différence de phase sont sujets à plusieurs défauts bien connus des systèmes radios : environnement encombré ou multi-chemins dûs aux rebonds des ondes radios.

Le cadre d'utilisation ci-dessus pour l'utilisation d'outils de positionnement, peut se révéler gênant pour certains systèmes, particulièrement dans le cas d'objets mobiles (où la place disponible et les mouvements de l'objet sont des critères pénalisants). Mais sans ces outils, il est plus compliqué d'extraire des informations concernant le statut dans le réseau. Ce manque oblige les algorithmes traditionnels à se baser sur une approche topologique (une connaissance partielle ou complète du voisinage à un ou deux sauts).

À partir des deux considérations développées ci-dessus, nous développons dans l'algorithme BRP une approche probabiliste pour évaluer une métrique représentant la distance qui sépare deux nœuds. Cette métrique est extraite du voisinage des deux nœuds et de la comparaison de leur liste de voisinage. Outre le fait que cette méthode se passe d'outils de positionnement, elle possède l'avantage de n'utiliser que des informations déjà disponibles dans les messages traditionnels utilisés dans le cas de réseaux ad hoc (listes de voisinage dans les messages HELLO et/ou BROADCAST).

Nous allons proposer un nouvel algorithme, baptisé BRP, utilisant une approche probabiliste pour la décision de réémission et une méthode pseudo-statistique pour évaluer la distance avec le nœud source. Dans la section suivante, nous poserons quelques préliminaires. Dans la section 2.2, nous présenterons les travaux existants. Le protocole BRP possède cinq modes, de manière à décomposer l'ensemble des ajouts et pour présenter l'apport de chacun. Le mode 1, présenté dans les travaux existants, est le modèle probabiliste simple. La section 2.3 détaille le mode 2, qui utilise une estimation de la taille du voisinage pour ajuster sa probabilité de réémission. Le mode 3, utilisant l'approche probabiliste et l'estimation du voisinage, est décrit dans la section 2.4. Le mode 4 propose dans la section 2.5 une combinaison du mode 2 et du mode 3 pour offrir une meilleure réactivité à la densité locale. Enfin, le mode 5 est détaillé avec la section 2.6 qui décrit l'hybridation du mode 4 avec un mécanisme d'élimination des voisins. Par la suite, nous détaillerons les résultats expérimentaux dans la section 2.7. Enfin, une conclusion en section 2.8 permettra de présenter les apports de nos travaux.

## 2.2 Travaux existants

L'utilisation d'une fonction probabiliste comme condition de réémission offre certaines particularités intéressantes. Une décision probabiliste à réponse binaire peut offrir localement de mauvais résultats. Mais à l'échelle du réseau, c'est-à-dire d'un point de vue global, la proportion de réponses positives et négatives suit le seuil de probabilité choisi, et ainsi offre un comportement du réseau en

fonction du seuil choisi. L'un des grands intérêts de cette méthode est d'offrir une réponse sans la nécessité de communications supplémentaires : la décision est prise en interne sur la foi d'une fonction probabiliste. Les seuls éléments nécessaires sont la connaissance du seuil et un générateur de nombre aléatoire suffisamment performant pour offrir une distribution aléatoire la plus juste possible (tout au moins suffisante pour offrir une dispersion correcte à l'ensemble des nœuds du voisinage). La décision est donc entièrement locale et il n'est d'ailleurs pas nécessaire à chaque nœud d'émettre régulièrement un message HELLO, car le seuil de probabilité est indépendant de la connaissance topologique locale.

Cette idée est développée dans [67, 80] comme méthode pour réduire le coût d'une diffusion. Un seuil de probabilité fixe $P$ est choisi au départ pour tout le réseau. Chaque nœud recevant un message de diffusion pour la première fois traite les données du message puis tire un nombre aléatoire $x$ entre 0 et 1. Si $x > P$ alors le nœud ne fait rien : il oublie le paquet. Dans le cas contraire ($x < P$), il réémet le message pour ses voisins. Dans notre protocole, ce mode est baptisé mode 1 et nous permet d'avoir une idée du comportement de l'algorithme probabiliste naïf et des performances de nos améliorations proposées par la suite.

Un des problèmes est de pouvoir identifier de manière unique la diffusion, dans le but de posséder un critère de décision pour réémettre ou non. En effet, un nœud ne doit pas réémettre s'il a déjà reçu un message de diffusion provenant de la même « vague » (c'est-à-dire l'ensemble des émissions concernant une diffusion précise). Il peut utiliser comme critère l'identité du nœud émetteur, mais dans ce cas il refusera de faire suivre les messages de diffusion après le premier reçu, même si les suivants font partie d'une autre vague de diffusion. Pour corriger ce défaut, un mécanisme baptisé nombre de séquence (ou *Sequence Number*), hérité des systèmes de numérotation des trames TCP, est présent dans l'ensemble des protocoles de diffusion et de routage dans les réseaux ad hoc. Il consiste à ajouter à chaque message de diffusion un nombre unique. Ainsi, chaque vague de diffusion est identifiable de manière unique à partir du couple composé de l'identifiant de la source d'origine et du nombre de séquence associé. La manière la plus simple pour le comportement du nombre de séquence est de positionner sa valeur à zéro au démarrage, et d'incrémenter la valeur lors de l'envoie de messages de diffusion dont le nœud est l'initiateur. Chaque nœud possède alors une table de diffusion (ou *Broadcast Table*), contenant les couples composés de l'identifiant de la source et du numéro de séquence associé. Chaque fois qu'un nœud reçoit un message de diffusion avec un couple d'identifiants non présent dans la table, il traite le message. Si le couple est déjà présent dans la table, il oublie le message. Signalons que des traitements peuvent être effectués même si le couple d'identifiants est dans la table. De même, il est possible qu'un message de diffusion soit réémis (voir le cas du mécanisme d'élimination des voisins).

Les auteurs montrent l'inefficacité de cette méthode de diffusion probabiliste. Le problème provient du fait que le calcul de la probabilité ne tient pas compte d'autres paramètres que le seuil $P$. Aucune connaissance, même partielle, de la topologie du voisinage ou de l'état des liens ou des mobiles ayant déjà reçu ce message n'est considérée. La répartition des mobiles qui réémettent étant constante, il est nécessaire d'avoir une valeur de $P$ assez grande, au détriment du SRB.

Cette méthode n'est pourtant pas totalement inadaptée. Elle pourrait servir dans le cas de « diffusion partielle ». Par ce terme, on entend la diffusion à une partie du réseau, définit en terme de pourcentage. Cette opération peut être utile dans le cas d'une diffusion limitée pour informer son voisinage proche de sa présence. Elle peut aussi servir à informer de la disponibilité d'un service, en dépassant les frontières de l'information locale des voisins à 1 ou 2 sauts donnée par les messages HELLO. Ce sous-ensemble joignable n'est pas défini explicitement, seule une appréciation de la partie du réseau joignable est disponible.

De plus, cette méthode offre aussi un intérêt non négligeable : comme chaque nœud décide par

lui-même en dehors de critère topologique, alors ce ne sont pas toujours les mêmes nœuds qui réémettent. Cette propriété est importante car elle offre une diversité plus large, et permet de répartir de manière plus efficace le rôle de la diffusion. Dans un contexte de sécurité, cette distribution aléatoire des responsabilités permet de minimiser l'effet d'un ou plusieurs nœuds hostiles. Pour un cadre d'économie d'énergie, l'utilisation équitable en moyenne de chaque nœud permet de mieux répartir la consommation d'énergie.

## 2.3 Prise en compte de la densité (mode 2)

Le mode probabiliste présenté dans la section précédente n'exploite aucune information sur la topologie du réseau, ce protocole étant juste un algorithme probabiliste naïf. L'effet d'une telle restriction se fait sentir sur les performances (voir section 2.7.1), car la probabilité est fixée et ne varie pas en fonction de la configuration du voisinage, des changements dans le réseau et des messages déjà reçus. Pourtant, il est logique de faire varier la probabilité en fonction de la densité, au vu de la courbe 2.10. En effet, la probabilité pour joindre un certain pourcentage de nœuds dépend de la densité moyenne du réseau. Plus exactement, le seuil de probabilité pour contacter une partie des nœuds est inversement proportionnel à la densité globale du réseau. On peut écrire que les courbes correspondent à la formule :

$$f_{mode2} = \frac{k}{n} \tag{2.1}$$

Avec la constante $k$, fonction du pourcentage de nœuds à joindre en moyenne, et $n$ le nombre moyen de voisins. Le nouveau seuil de décision $f_{mode2}$ ainsi choisi peut être utilisé dans l'algorithme probabiliste naïf.

Cette approximation possède plusieurs avantages. Premièrement, elle permet de prendre en compte la densité locale pour affiner la valeur du seuil de probabilité, chaque nœud calculant ce niveau en fonction du pourcentage de nœuds du réseau qu'il cherche à joindre. Cette valeur $k$ peut être choisie par la source de la diffusion ou, en fonction d'un objectif local de diffusion, chaque nœud peut choisir une valeur de $k$ en fonction de ses besoins.

Deuxièmement, elle est facilement calculable, et peut même être implémentée par une méthode matérielle légère ; Le système peut même mémoriser les valeurs de $f_{mode2}$ pour chaque taille de voisinage, dans le but de réduire la puissance machine nécessaire pour une telle opération.

Enfin, elle nécessite peu d'informations. Chaque nœud maintient à jour une table mémorisant les identifiants des nœuds voisins, en fonction des messages HELLO reçus. Lorsqu'il est nécessaire de calculer $f_{mode2}$, $n$ est égal à la taille de cette table.

Il faut néanmoins signaler qu'une surestimation du nombre de voisins est possible. Lorsqu'un voisin quitte la zone de communication d'un nœud, ce dernier va croire qu'il est encore présent[5] et tiendra compte de sa présence lors du calcul de $f_{mode2}$. Il peut donc être nécessaire d'évaluer l'effet de la mobilité avec ce type de protocole, par exemple en surestimant la probabilité obtenue.

L'algorithme proposé est présenté dans la figure 1. Nous étudions les résultats de ce protocole dans la section 2.7.2.

[5] au bout d'un certain temps, le nœud ne recevant plus de messages HELLO de son voisin, il va enlever l'entrée correspondante de la table.

**Algorithme 1** Algorithme du mode 2

```
Protocole receiving()
if The broadcast ID of the message is not in BY_bid then
   Get the Broadcast ID bid from the message
   Create an entry BT_bid in the Broadcast Table
   Generate a random number 0 ≤ x ≤ 1
   if x ≤ (k/n) then
      Broadcast the packet
      Drop the packet
   end if
else
   Drop the packet
end if
```

## 2.4 Evaluation d'une pseudo-distance (mode 3)

Le mode précédent utilise une information numérique obtenue de ses voisins. Mais il n'exploite pas la topologie du voisinage car il ne prend pas compte des liens existants entre chacun. Avec le mode 3, nous proposons une méthode simple pour évaluer cette information et la faire intervenir dans le calcul du seuil de réémission.

Si l'on regarde une nouvelle fois l'article sur le problème de la tempête de diffusion [67] (déjà discuté dans la section 1.4.4), la solution la plus efficace d'après les auteurs est le schéma basé sur la position. Cette méthode donne un des meilleurs résultats en terme de SRB et de RE. Elle fonctionne comme suit ; Chaque fois qu'un mobile reçoit un message d'inondation, il attend un certain temps, pour laisser une chance à son voisinage de diffuser le message. Puis il réémet le message si et seulement si la zone nouvellement jointe par son message est supérieur à un certain seuil. Une autre méthode efficace proposée dans le même article, est le schéma basé sur la distance. Avec cet algorithme, un mobile ne réémet pas si l'un des voisins a réémis le même message, et que ce mobile se trouve à une distance supérieure à un seuil fixé.

Ces deux solutions nécessitent l'ajout d'un système de positionnement (voir section 2.1.2). En effet, dans le cas du schéma fondé sur la position, il est nécessaire de pouvoir évaluer la position des voisins entre-eux, et des distances entre la source et chaque voisin. Dans le cas du schéma basé sur la distance, seule la distance entre les nœuds et leurs voisins est nécessaire.

Si aucun dispositif de positionnement « physique » n'est disponible, alors l'information extractible du voisinage se résume à un graphe unitaire. Ainsi, selon l'information diffusée par chacun, un nœud peut, au maximum, déduire quelles sont les relations binaires entre chacun des nœuds et leur voisinage.

La question est maintenant la suivante : comment construire une information topologique plus fiable sans l'aide d'outil de positionnement ? Il est intéressant de privilégier les nœuds en bordure de la zone de communication, car ce sont ceux qui vont joindre le plus de nœuds supplémentaires. Dans le schéma basé sur la distance, lorsqu'un mobile reçoit un message il le réémet si et seulement si tous les voisins qui ont répété ce message sont à une distance supérieure à un seuil défini. Cette approche donne de bons résultats mais possède plusieurs défauts :

- Si tous les nœuds voisins se trouvent en dessous de la distance seuil, alors aucun d'eux ne va réémetre, même si certains nœuds extérieurs à la zone de communication de l'émetteur sont joignables par les voisins de l'émetteur ;

- Tous les nœuds au dessus de la distance seuil vont réémettre. Si la densité est importante, alors la probabilité de collision devient trop gênante. De plus, si deux voisins sont proches et couvrent les mêmes nœuds, ils vont chacun réémettre alors qu'une émission seule aurait suffit.

Le défaut fondamental se trouve dans le fait que nous sommes dans le cas d'un seuil binaire : aucun nœud ne réémet en dessus du seuil et tous les nœuds réémmettent au dessous du seuil. Il est donc important de chercher une règle plus souple. Nous proposons d'utiliser un gradient dans la décision de retransmission. La solution basée sur la distance a une probabilité de réémission qui est égale à 1 si la distance entre les deux nœuds est supérieure au seuil et 0 dans le cas contraire. Dans notre approche, la probabilité de réémission est linéaire par rapport à la distance entre les deux nœuds. On a une formule du type :

$$p = f(d(src, dst)) \tag{2.2}$$

Il reste le problème de l'évaluation de la distance entre deux nœuds. Il n'existe aucun moyen de positionnement physique, donc les nœuds doivent utiliser une information existant dans les messages de découverte du voisinage. Par observation, nous constatons que plus un mobile est éloigné d'un autre, plus le nombre de voisins communs aux deux nœuds à tendance à croître. Il existe donc un critère permettant d'évaluer la distance entre deux nœuds. Mais il n'est pas sûr : il repose sur l'idée que la densité locale des deux nœuds est uniforme. Malgré l'erreur induite, l'idée d'utiliser le nombre de nœuds communs et non-communs permet d'évaluer une approximation de la distance entre deux nœuds.

Plus précisément, quand deux nœuds $src$ et $dest$ sont mutuellement en contact, l'union de leurs zones de communications ($Z_{src}$ et $Z_{dst}$) peut être partitionnée en trois zones :

- $Z_a = Z_{src} \cap \overline{Z_{dst}}$ : la zone de communication uniquement couverte par le nœud $src$ ;
- $Z_b = \overline{Z_{src}} \cap Z_{dst}$ : la zone de communication uniquement couverte par le nœud $dst$ ;
- $Z_c = Z_{src} \cap Z_{dst}$ : la zone de communication couverte par les nœuds $src$ et $dst$.

Les nœuds ne peuvent pas évaluer l'aire des zones sans outil de positionnement. Mais l'utilisation du nombre de nœuds dans chaque zone permet de caractériser la couverture des zones de communication :

- $N_a$, le nombre de nœuds dans la zone $Z_a$ ;
- $N_b$, le nombre de nœuds dans la zone $Z_b$ ;
- $N_c$, le nombre de nœuds dans la zone $Z_c$.

Nous pouvons maintenant définir le ratio $\mu$ :

$$\mu = \frac{N_b}{N_a + N_c} \tag{2.3}$$

Le ratio $\mu$ est le rapport entre le nombre de mobiles joints par le message de diffusion émis par le nœud $src$ et le nombre potentiel de nouveaux nœuds joints si le nœud $dest$ réémet le message. Le calcul est simple, et ne nécessite que très peu de mémoire et de puissance de calcul. Une comparaison de liste peut se faire en un temps $\theta(n)$ si la liste est triée et $\theta(n^2)$ si la liste n'est pas triée. La place en mémoire est de l'ordre de $\theta(n)$ (avec une constante minime, de l'ordre de 2 ou 3). Cette légèreté au niveau machine le rend très adapté pour des petits objets.

Pour effectuer ce calcul, il est nécessaire que le mobile $dst$ connaisse deux informations : la liste des voisins du mobile $src$ et du mobile $dst$. Il peut connaître ces informations de deux manières :

**Par les messages HELLO :** chaque mobile diffuse régulièrement un message HELLO pour avertir de sa présence. Dans ce cas, un nœud ajoute la liste complète de ses voisins dans chacun de

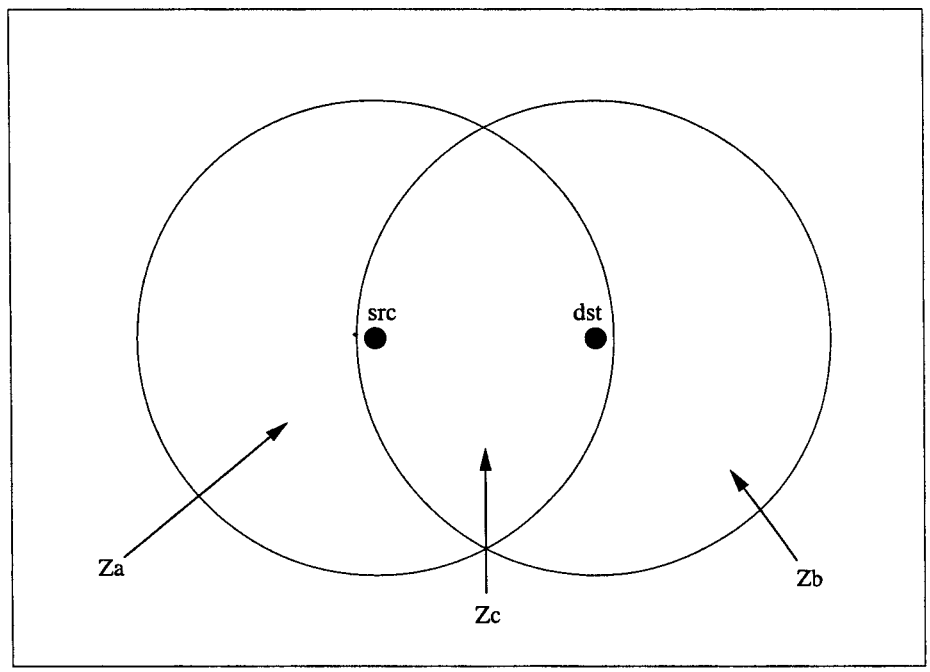



FIG. 2.2 – Séparation en 3 zones de couverture lorsque 2 mobiles sont mutuellement à portée de communication.

ses messages HELLO. Ainsi chacun est en mesure de connaître la topologie à deux sauts. Le message de BROADCAST ne contiendra quant à lui que l'information utile.

**Par les messages BROADCAST :** À chaque fois qu'un nœud émet un message de diffusion BROADCAST, il ajoute la liste complète de son voisinage. Ainsi, chaque nœud voisin est en mesure de connaître le voisinage d'un mobile $src$. Il est néanmoins nécessaire que chaque nœud émette un message HELLO ne contenant que l'identité du nœud. En effet, sans ce message, aucun mobile n'est en mesure de pouvoir connaître son voisinage.

Si la liste de voisins est placée dans les messages HELLO, elle offre une bonne idée de la topologie locale à deux sauts et l'excédent se trouve dans des messages de taille très petites à l'origine. Par contre, le surplus engagé dans chaque paquet HELLO risque d'occuper sensiblement plus de bande passante. En effet, la quantité d'information supplémentaire qui va circuler en un point du réseau est de l'ordre de $0(f_H \times d^2)$ (avec $d$ la densité et $f_H$ la fréquence d'envoi des messages HELLO par un nœud).

Si la liste des voisins est placée dans le message BROADCAST, elle offre l'avantage de réduire la consommation globale de la bande passante : seuls les nœuds qui réémettent le message de diffusion introduisent un surcoût. Si la fréquence des émissions de messages de diffusion est faible, on réduit d'autant le surplus d'information. Dans notre cas, cela fait un surcoût moyen en un point du réseau de l'ordre de $0(f_B \times d \times g(d))$, avec $f_B$ la fréquence d'envoi d'un message de diffusion par un nœud, $d$ la densité et $g(d)$ la diminution de message de diffusion par notre algorithme (intuitivement, elle est fonction de la densité). Le facteur de réduction de la taille du message est de l'ordre de :

$$\frac{f_D \times g(d)}{f_H \times d}.$$

Si l'on considère $f_B$ très petit par rapport à $f_H$, alors il y a une nette diminution du surcoût d'émission engendré si l'on choisit la seconde solution, puisque $g(d)$ est inférieur à $d$ (notre algorithme ne nécessite pas que tous les nœuds réémettent le message de diffusion). Néanmoins, ajouter le surplus d'information dans le paquet BROADCAST possède un désavantage : comme tous les messages BROADCAST sont réémis dans un laps de temps le plus court possible, alors l'augmentation de la taille du paquet entraîne une augmentation des chances de collisions. Bien que ces possibilités soient réduites avec la diminution de rediffusion par l'algorithme, ce risque n'est pas à négliger.

L'utilisation de $\mu$ comme seul critère de décision limite un peu les possibilités de l'algorithme. $\mu$ délivre une information sur la distance entre $src$ et $dst$ qui n'est peut-être pas correcte, avec des variations de densité dans les voisinages de $src$ et $dst$. Cette erreur peut alors entraîner un tirage aléatoire défavorable.

Nous allons offrir plusieurs ajouts à notre protocole, de manière à le rendre plus configurable. Pour cela, nous définissons la constante $A$ pour le seuil minimal de probabilité. Ainsi, nous pouvons garantir à chaque nœud une possibilité de réémission, même si la valeur de $\mu$ est défavorable. De même nous établissons une constante $\alpha$ comme seuil de probabilité maximale pour minimiser l'effet d'un tirage aléatoire trop favorable.

Une autre remarque importante est l'impossibilité d'utiliser $\mu$ directement comme seuil de probabilité. En effet, si deux nœuds sont à la limite de leur portée radio, alors la probabilité de réémettre devrait être égal à 1. Dans notre cas, elle est égale au rapport $Z_b/(Z_a + Z_c)$, lorsque $d(src, dst) = R$. Cette valeur peut être calculée très facilement. Une méthode est proposée dans [67]. Nous allons redémontrer avec une autre technique plus facile que la valeur de cette constante, notée $\sigma$, est égale à 0,601.

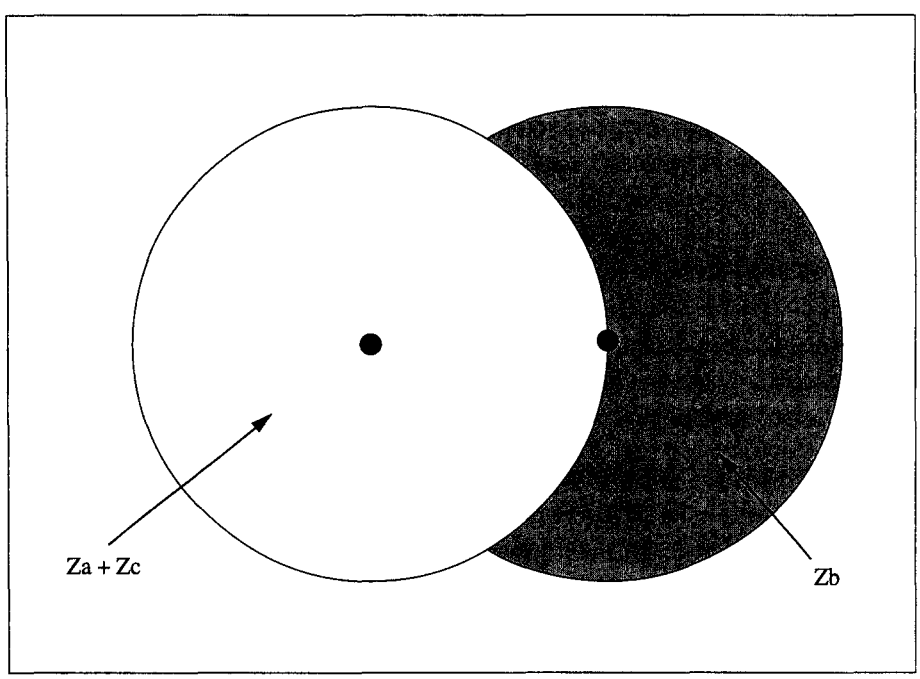



FIG. 2.3 – Configuration pour calculer le rapport $\sigma = \frac{Z_b}{Z_a+Z_c}$

Soit les deux mobiles $a$ et $b$ aux extrémités des zones de communication de chacun (voir Fig 2.3). Soit $Z_a$ l'aire de la zone de communication du nœud $a$ et $Z_b$ l'aire de la zone de communication du

nœud $b$. Nous cherchons à calculer $\sigma = (Z_b - Z_a \wedge Z_b)/(Z_a + Z_a \wedge Z_b)$ quand $d(a,b) = R$. L'aire de $Z_a = Z_b = \pi * R^2$, donc il nous reste à calculer l'aire de $Z_a \wedge Z_b$ (la zone grisée sur le schéma). Pour ça, on cherche à calculer l'aire de la portion de cercle $Z_\beta$ de centre $b$ et de rayon $\beta$, que l'on soustrait à l'aire du triangle $blm$. L'aire $Z_\beta$ est égale à :

$$Z_\beta = \pi \times R^2 \times \frac{\beta}{360}. \tag{2.4}$$

Il nous faut calculer l'angle $\beta$, on peut écrire :

$$\beta/2 = \cos\frac{R/2}{R} = \cos\frac{1}{2} = 60°. \tag{2.5}$$

Soit $\beta = 120°$, on peut maintenant déduire l'aire de la zone $Z_\beta$ :

$$Z_\beta = \frac{120\pi R^2}{360} = \frac{\pi R^2}{3}.$$

Il nous reste à calculer l'aire du triangle $blm$. $Z_{blm}$ peut s'écrire comme suit :

$$Z_{blm} = \frac{1}{2} * d(l,m) * \frac{d(a,b)}{2} = \frac{\sqrt{3} * R^2}{4}$$

L'aire de la zone hachuré est donc égale à :

$$\begin{aligned} Z_c &= 2 * (Z_\beta - Z_{blm}) = 2 * (\frac{\pi * R^2}{3} - \frac{\sqrt{3} * R^2}{4}) \\ &= 2 * \frac{4 * \pi * R^2 - 3 * \sqrt{3} * R^2}{12} \\ &= \frac{4 * \pi - 3 * \sqrt{3}}{6} R^2 \end{aligned}$$

On peut maintenant calculer le coefficient $\mu$ lorsque $d(a,b) = R$ :

$$\begin{aligned} \mu &= \frac{Z_b}{Z_a + Z_c} = \frac{\pi * R^2 - Z_c}{\pi * R^2} \\ &= 1 - R^2 * \frac{4 * \pi - 3 * \sqrt{3}}{6 * \pi * R^2} = 1 - \frac{4 * \pi - 3 * \sqrt{3}}{6 * \pi} \\ &= 1 - \frac{4 * \pi - 3 * \sqrt{3}}{6} = 1 - \frac{4}{6} + \frac{\sqrt{3}}{2 * \pi} \end{aligned}$$

La valeur numérique de $\mu \approx 0,601$ quand $d(a,b) = R$. Nous possédons maintenant la constante nécessaire pour évaluer en moyenne le nombre maximal de nœuds joints par une nouvelle réémission.

L'utilisation d'un gradient linéaire en tant que seuil de décision n'est peut-être pas la meilleure solution. Nous voulons offrir une paramétrisation possible du gradient, de manière à privilégier plus ou moins les nœuds en bordure de la zone de communication. Nous définissons une variable $\sigma$ qui paramètre la courbe. Comme le montre le schéma 2.5, en utilisant la valeur 1, la courbe est linéaire en fonction de $\mu$. Avec un $\sigma > 1$, la courbe prend la forme d'une exponentielle, diminuant la valeur des nœuds les plus proches de la source, de manière à ne privilégier que les nœuds à l'extrémité. Avec

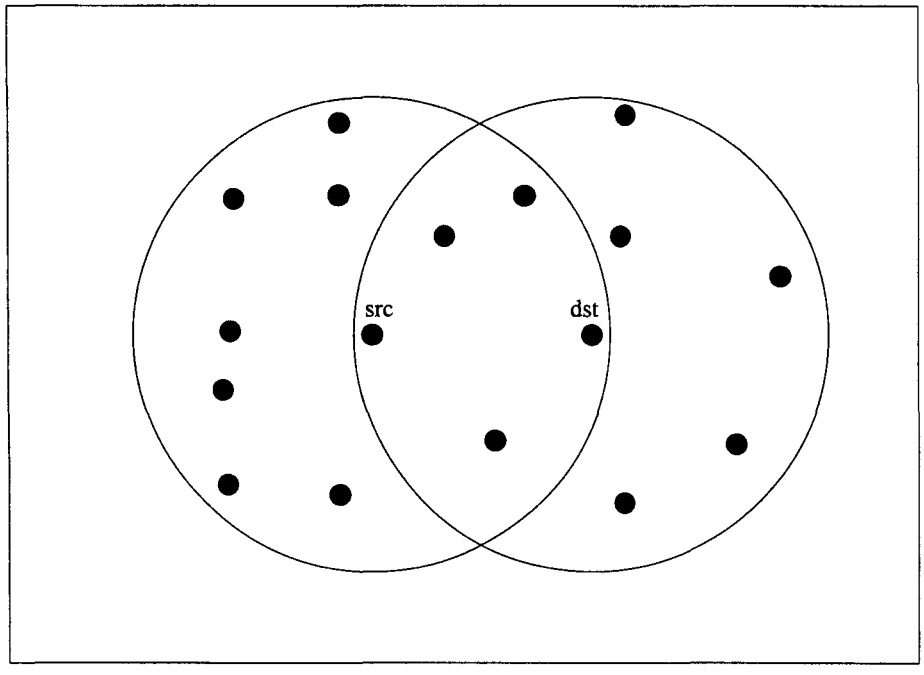



FIG. 2.4 – Exemple de configuration pour l'évaluation de $\mu$.

$\sigma < 1$, la courbe prend la forme d'un logarithme, augmentant pour une grande partie leur chance de réémission.

Ainsi, pour permettre d'offrir une meilleure paramétrisation de $\mu$, nous proposons la formule suivante :

$$f_{mode3} = \frac{A - \alpha}{M^{\sigma}} \mu^{\sigma} + \alpha \tag{2.6}$$

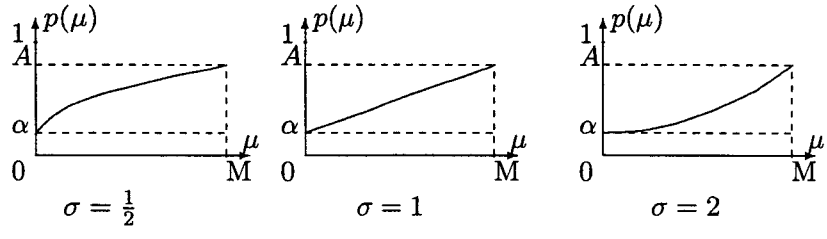



FIG. 2.5 – Exemple de 3 configurations de $\mu$ avec différentes valeurs de $\sigma$.

Cette formule est appliquée pour calculer le seuil de probabilité de réémission de chaque nœud. L'algorithme présenté ici est identique aux 2 précédents modes, sauf au niveau du calcul du seuil :

**Algorithme 2** Algorithme du mode 3

**Protocole receiving()**
**if** The broadcast ID of the message is not in $BY_{bid}$ **then**
  Get the Broadcast ID *bid* from the message
  Create an entry $BT_{bid}$ in the Broadcast Table
  Generate a random number $0 \leq x \leq 1$
  **if** $x \leq f_{mode3}$ **then**
    Broadcast the packet
    Drop the packet
  **end if**
**else**
  Drop the packet
**end if**

## 2.5 Évaluation d'une pseudo-distance avec prise en compte de la densité (mode 4)

Nous avons présenté avec le mode 2 une méthode pour évaluer la meilleure probabilité de réémission pour un algorithme purement probabiliste avec une paramétrisation possible de la couverture attendue. Cette méthode avait le désavantage d'être uniforme, c'est-à-dire qu'elle ne tenait pas compte de l'organisation locale des nœuds entre-eux pour calculer sa probabilité. Le mode 3 propose, quant à lui, une méthode destinée à affûter la probabilité pour privilégier les nœuds en bordure des zones de communication, mais cette solution ne tient pas en compte un élément déterminant. En effet, il se fonde sur des valeurs provenant de la densité locale pour calculer un rapport évaluant la distance. En aucun cas il ne considère l'importance du voisinage, celui-ci ne servant que de comparaison entre les voisinage de la source et du nœud. Le résultat $\mu$ est donc indépendant de la densité locale.

Le problème est montré avec la Figure 2.6. Dans les deux schémas, les probabilités de réémission sont identiques, car la densité est uniforme dans l'ensemble des voisinages. Pourtant, il est clair que dans le second schéma, le même pourcentage de nœuds va réémettre, alors que la densité est plus importante. Cela va entraîner un économie faible en nombre de messages de réémission (sans compter une probabilité plus forte de collisions entre messages).

Nous allons présenter une nouvelle version de l'algorithme combinant le mode 2 et le mode 3. Dans le mode 3 la probabilité maximale de réémission est fixée par un seuil $A$. Cette valeur arbitraire peut être remplacée par la formule utilisée dans le mode 2, qui donne la meilleure probabilité de réémission pour une densité donnée. Lorsque l'on combine les deux approches, on obtient la formule suivante :

$$f_{mode4}(\mu, k) = \frac{\frac{k}{n} - \alpha}{M^{\sigma}} + \alpha$$

Ce nouvel algorithme possède de nombreux avantages. L'ajout de la formule du mode 2 dans le mode 4 ne demande pas de communications supplémentaires car la seule valeur nécessaire (le nombre de voisins du nœud *dst*) est déjà connu du récepteur. De plus, il ne demande pas de ressources supplémentaires importantes : la quantité de mémoire nécessaire est minime et fixe, et le coût en terme de puissance de calcul se résume à une division.

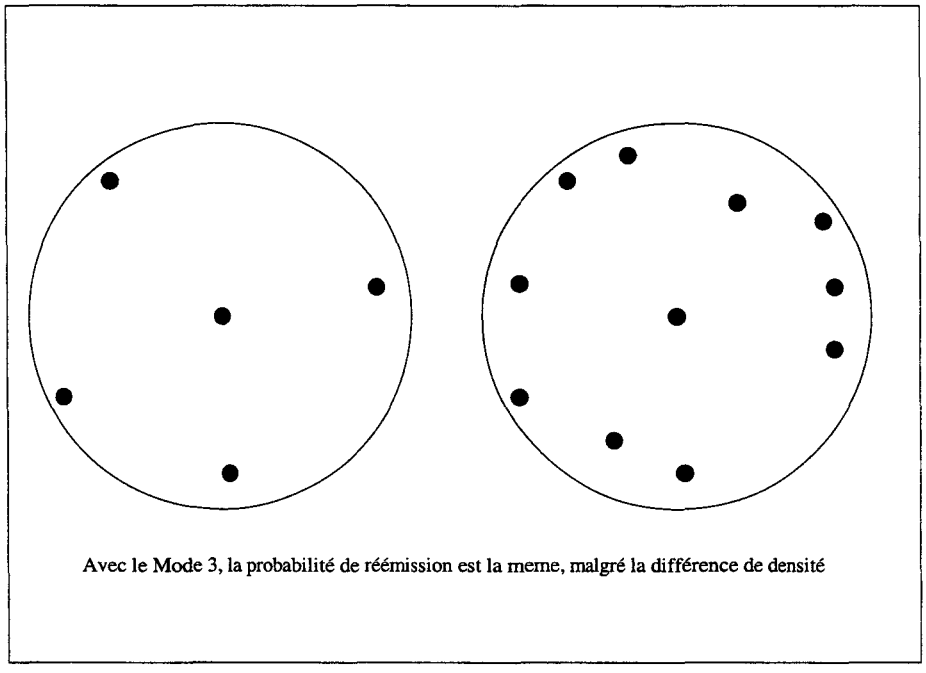



FIG. 2.6 – Pour une densité différente, la probabilité de réémission reste la même pour chaque nœud.

Intuitivement, on peut s'attendre à une augmentation des performances de ce protocole, surtout dans le cas de haute densité. En effet, dans le mode 3 le nombre de nœuds réémettant le message augmente proportionnellement à la densité. Or, il paraît logique que ce nombre de nœuds tende vers une constante, car la taille de la zone de communication reste fixe. Avec cet ajout, l'algorithme contrebalance l'effet en minimisant le nombre de nœuds faisant suivre le message par rapport à la densité.

## 2.6 Ajout d'une mécanisme d'élimination des voisins (mode 5)

Le procédé présenté jusqu'ici présente un problème de taille : il n'est pas fiable. Le taux d'accessibilité n'est jamais parfait (c'est-à-dire proche de 100%). L'approche probabiliste, si elle apporte un comportement en moyenne adapté, ne garantit en aucun cas une couverture parfaite du réseau. Nous allons présenter dans ce dernier mode l'utilisation d'un mécanisme déterministe de manière à assurer une diffusion parfaite.

Un algorithme fiable ou *reliable* garantit de joindre l'ensemble des nœuds connexes, par définition. Soit par exemple la propriété suivante : « Un algorithme de diffusion qui garantit que tous les voisins à deux sauts sont joints par son message est considéré comme fiable ». La démonstration est triviale ; Si un nœud utilise un algorithme qui vérifie cette propriété, alors tous ses voisins permettent de garantir de joindre l'ensemble des voisins à trois sauts. Par réccurence, il est évident que l'ensemble des nœuds connexes sont joints. Si le réseau est connexe, alors l'ensemble du réseau est joint par le message de diffusion.

Des algorithmes fiables par définition existent, comme MPR [76] ou Dominating Set [100]. Mais BRP ne possède pas cette propriété (il est très facile de démontrer ce fait par un simple exemple où aucun mobile voisin ne réémet dû à un mauvais tirage aléatoire). Nous allons présenter maintenant un ajout à notre protocole pour le rendre fiable.

L'idée est la suivante ; Régulièrement, le protocole BRP ajoute aux messages HELLO la liste de voisins du nœud. Ainsi, chaque entité du réseau est capable de connaître la liste de ses voisins à deux sauts. Chaque mobile est à même de connaître les voisins joints par chaque message de diffusion, et peut ainsi déduire si chaque voisin a été contacté. Ce procédé existe déjà sous le nom de mécanisme d'élimination des voisins ou *neighbor elimination scheme*. Il a été présenté dans la section 1.4.4.

L'algorithme permet de déterminer si tous les voisins ont été joints et, si non, quels nœuds n'ont pas été joints par les messages d'inondation. Il se décompose comme suit :

1. Pour chaque message HELLO reçu, le nœud ajoute l'identifiant dans sa table de voisinage. Pour chaque entrée de cette table, si aucun nouveau message HELLO du nœud concerné n'est reçu pendant un certain temps (habituellement, deux à trois fois le temps entre chaque message HELLO), alors le nœud efface l'entrée correspondante ;
2. Lorsque le mobile reçoit un message BROADCAST avec un identifiant qu'il ne connaissait pas, il crée une nouvelle entrée dans la table de broadcast (*broadcast table*). Il associe à cette entrée la liste de ses voisins ;
3. Pour chaque message BROADCAST reçu (y compris le premier avec un nouvel identifiant), il élimine de la liste des voisins associés à l'identifiant du message de BROADCAST tous les nœuds qui sont contenus dans le message BROADCAST ;
4. Un certain temps (*timeout*) après la réception du premier message de BROADCAST, le nœud regarde la liste des voisins attachés à l'identifiant du mobile. Si celle ci est vide, alors chaque voisin a été contacté, sinon la liste des voisins contient les nœuds qui n'ont pas reçu le message de diffusion.

Cette solution permet de s'assurer que l'ensemble des nœuds ont été joints. La démonstration est triviale : si l'algorithme peut garantir que l'ensemble des nœuds à un saut sont joints, alors l'ensemble des mobiles à deux sauts sont joints par les voisins de l'émetteur. Par récursion, l'ensemble des nœuds connexes sont joints.

Par contre, le dispositif d'élimination des voisins n'est pas optimal. Il peut au contraire ajouter un surcoût car il ne garantit pas qu'un nœud soit informé correctement de tous les nœuds joints par les messages de diffusion. Un exemple simple, présente avec le schéma 2.7, est le fait qu'un voisin soit contacté par un nœud en dehors de la zone de communication d'une autre entité. Cette dernière n'a alors pas connaissance que ce nœud a été joints par ce dispositif et, en l'absence d'autres messages de diffusion informant l'entité que son voisin a été joint, devra réémettre son message de diffusion.

Pour gérer le mécanisme d'élimination des voisins, nous proposons deux fonctions. La première appelée *NeighborElimination* (figure 3) est appelée à chaque fois qu'un message de diffusion est reçu. La seconde fonction *CheckElimination* (figure 4), est appelée après un certain temps (*timeout*) pour vérifier s'il est nécessaire de renvoyer un message.

Le principe du mécanisme de l'élimination de voisins doit permettre de couvrir les nœuds restants, mais peut entraîner un surcoût (évoqué plus haut). Le mode 5 fonctionne avec une notion de « double vague ». La première vague est celle de la diffusion basée sur le mode 4. Pour la seconde vague, elle est déclenchée par les nœuds détectant que leur liste de voisins associée au mécanisme d'élimination n'est pas vide. Comme ce dernier dispositif est nécessaire mais peut se révéler coûteux, il faut minimiser son impact de façon à offrir le plus de chances possibles à la diffusion probabiliste du mode 4. Le réglage des différents coefficients est donc crucial pour maximiser les chances d'une « bonne » diffusion, c'est-à-dire qui donne une bonne dispersion des nœuds qui vont réémettre.

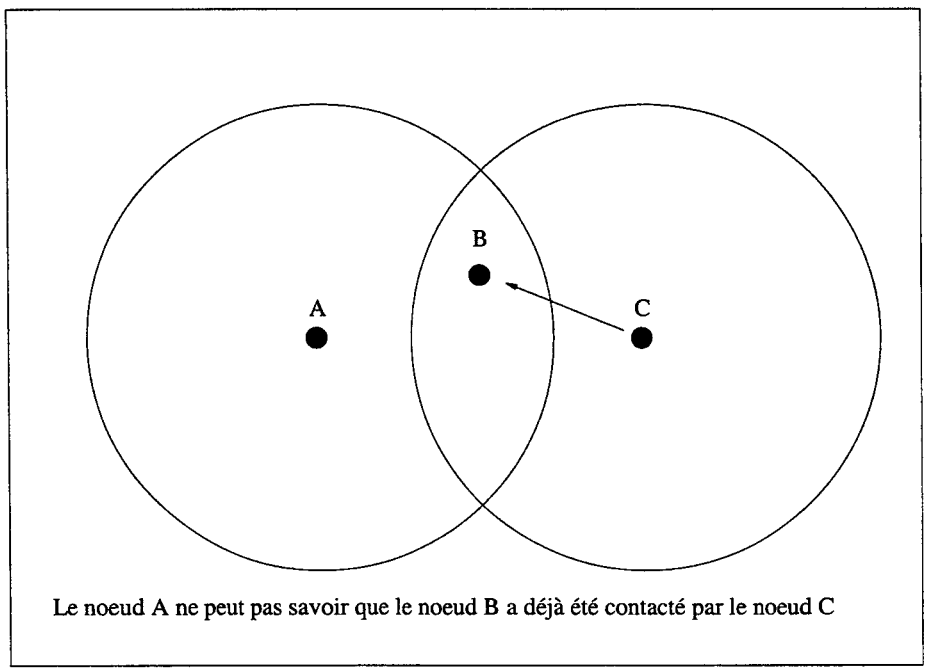



FIG. 2.7 – Défaut du mécanisme d'élimination des voisins

## 2.7 Résultats expérimentaux

Pour expérimenter les 5 modes de notre protocole, nous avons utilisé un simulateur développé dans notre équipe. Ce simulateur travaille par événements discrets et possède une couche MAC simplifiée. Chaque fois qu'un mobile veut émettre un message, il regarde si le canal est libre. Si oui, il attend une période de contention de taille aléatoire puis émet si le canal est libre à la fin. Dans le cas contraire, il attend la fin de la transmission puis rentre en période de contention.

Les paramètres fixés dans notre simulation sont la portée de transmission (100m) et la taille du terrain (400x400). Le nombre de nœuds varie et est égal à 25, 50, 100, 150, 200, 250 ou 300 (équivalent à une densité théorique de 5, 10, 20, 30, 40, 50, et 60 voisins par zone de communication). Dans chacun des cas, le simulateur exécute 1000 diffusions dans le réseau. Les performances observées sont l'accessibilité, le pourcentage de messages de diffusion économisés et la taille moyenne des chemins découverts.

### 2.7.1 Mode 1

Le graphique 2.8 présente une visualisation des résultats de l'accessibilité (RE) en terme de pourcentage du réseau couvert. L'abscisse représente le paramètre $p$ (la probabilité de réémission) et l'ordonnée la couverture correspondante. Chaque courbe représente une densité donnée.

Le mode 1 a déjà été développé dans [67, 80], et nous obtenons des résultats très proches (voir figure 2.9 et figure 2.8). En l'absence de prise en compte du voisinage, la réémission dépend uniquement du tirage aléatoire. Les résultats sont trop mauvais en terme d'accessibilité pour les petites densités et pour des seuils $p$ faibles.

Le pourcentage de messages de diffusion économisés est le complément à un du paramètre $p$, ou plus précisément : $SRB = 1 - p$. Ce résultat est logique, car chaque nœud décide de réémettre en

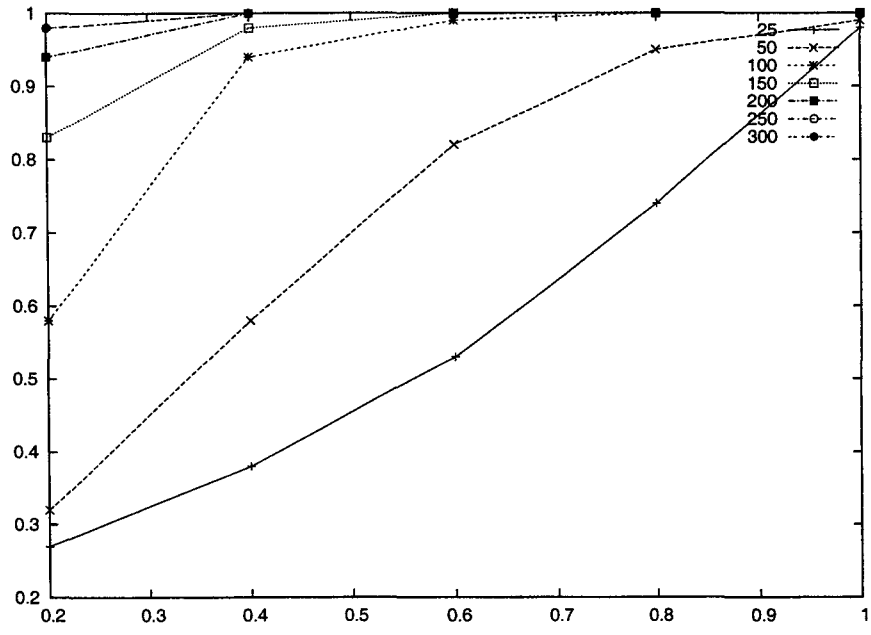



FIG. 2.8 – RE du mode 1 en fonction de la probabilité pour différentes densités

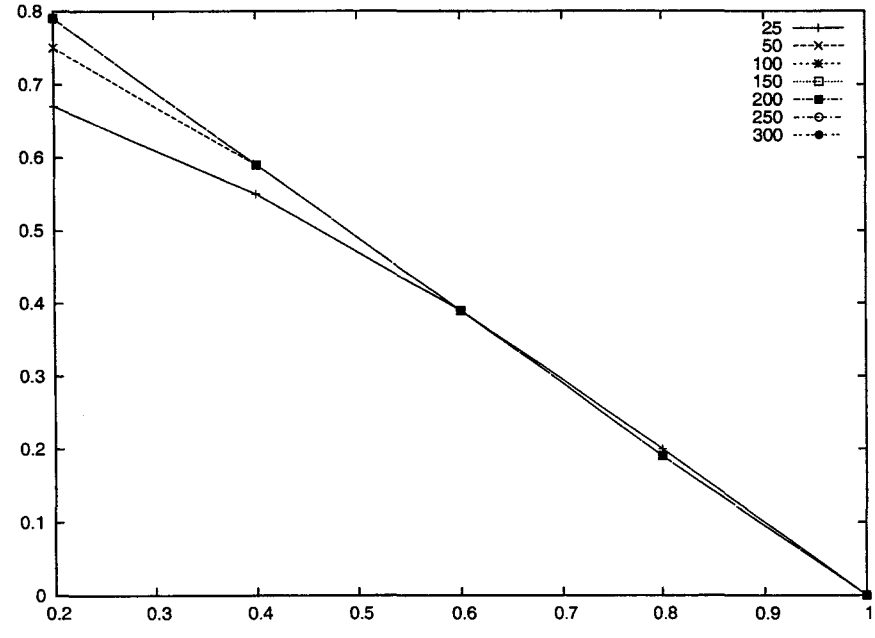



FIG. 2.9 – SRB du mode 1 en fonction de la probabilité pour différentes densités

**Algorithme 3** Algorithme du mode 5 lors de la réception d'un message

```
Protocole neighborElimination()
if message received for the first time then
  Get the Broadcast ID bid from the message
  Create a entry BT_bid in the Broadcast Table
  Create a list L_bid with all the IDs in the neighbor table
end if
for each id included in the message do
  if id is included in L_bid then
    remove id from L_bid
  end if
end for
```

**Algorithme 4** Algorithme du mode 5 lors de la réception d'un message

```
CheckElimination(bid)
if the entry L_bid is not empty then
  create a new BROADCAST message
  set the broadcast identifiant to bid
  send the BROADCAST message
end if
```

fonction d'un tirage aléatoire et du seuil $p$, même si des variations légères existent dans les résultats, surtout dans le cas de densités faibles.

La figure 2.10 présente le pourcentage nécessaire pour joindre 99%, 98%, 95%, 90% et 80% des mobiles lorsque le réseau est connexe. Plusieurs remarques sont à faire. Pour joindre 99% du réseau il est nécessaire d'avoir déjà une densité suffisante, de l'ordre de 11 nœuds par zone de communication avec une probabilité de 1. De plus, l'idée développée pour le mode 2 se trouve confirmée, car chaque courbe possède un comportement proche de $1/n$. Cette propriété est logique, car la surface nouvellement joignable lors d'une réémmission par les voisins est bornée. Donc la probabilité de rediffusion décroît car le nombre de mobiles qui doivent rediffuser le message reste fixe malgré l'augmentation de la densité.

Dans tous les cas, les résultats sont très mauvais. Le pourcentage de messages de diffusion économisés est inversement proportionnel à la probabilité choisie (car chaque nœud ne réémet que par rapport à un seuil de réémission fixe). L'accessibilité dépend du nombre de nœuds qui vont réellement réémettre, et dans notre cas il faut au moins 11 nœuds par zone de communication pour garantir une bonne couverture.

### 2.7.2 Mode 2

Pour le mode 2, on peut apercevoir dans le graphique d'accessibilité (voir figure 2.11) que l'objectif d'une stabilisation du RE quelle que soit la densité est atteint. A l'exception d'une densité de 5 (avec une connexité faible, ce qui est difficile dans le cas d'un algorithme probabiliste qui prend son appui sur un nombre important de voisins pour avoir un comportement global cohérent), l'accessibilité est pratiquement identique, quelle que soit la densité globale du réseau. On obtient globalement une accessibilité proche du parfait pour une valeur de $k$ égale à 11, et cela quelle que soit la densité.

Mais des variations importantes apparaissent pour la quantité de messages de diffusion sauvés

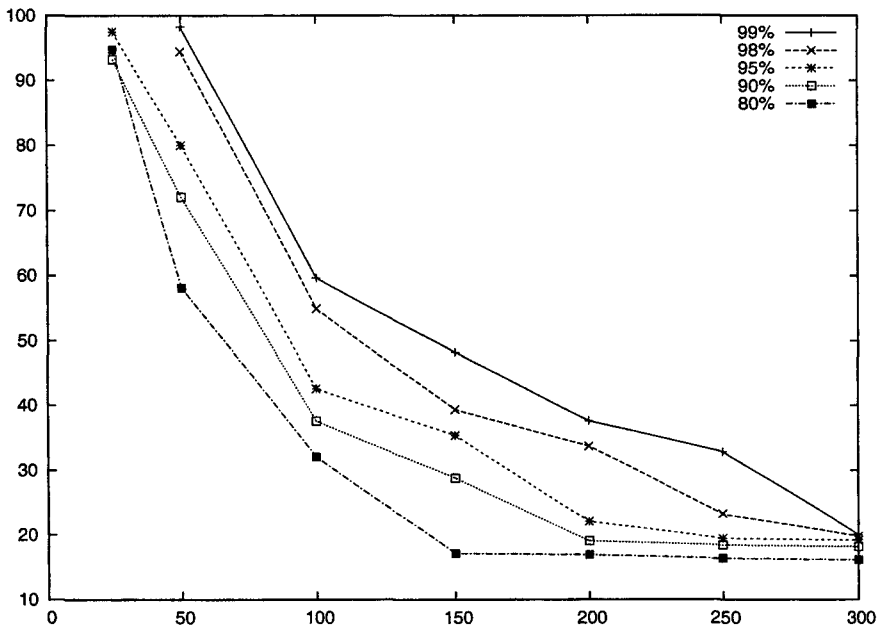



FIG. 2.10 – Probabilité de réémission pour une accessibilité donnée en fonction de différentes densités

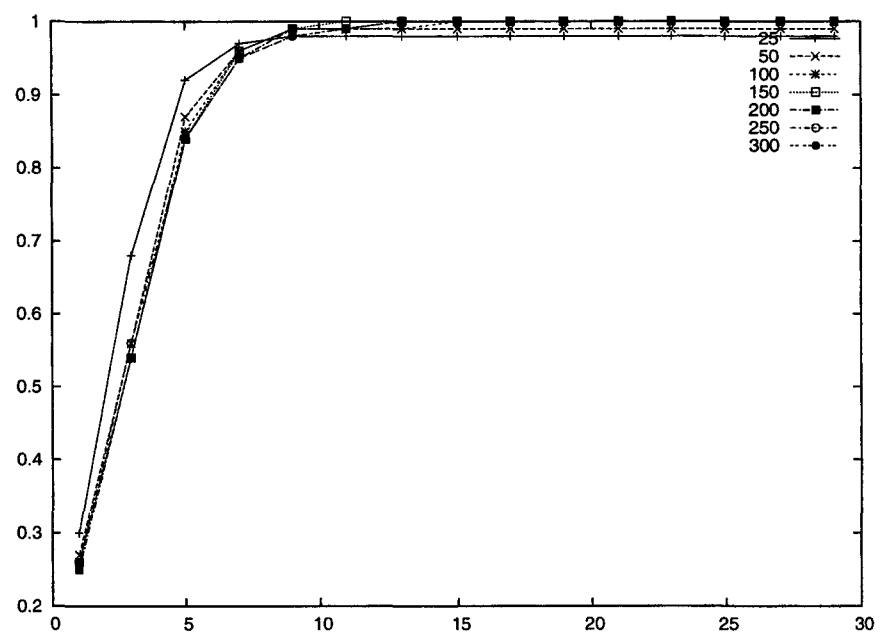



FIG. 2.11 – RE du mode 2 en fonction de la probabilité pour différentes densités

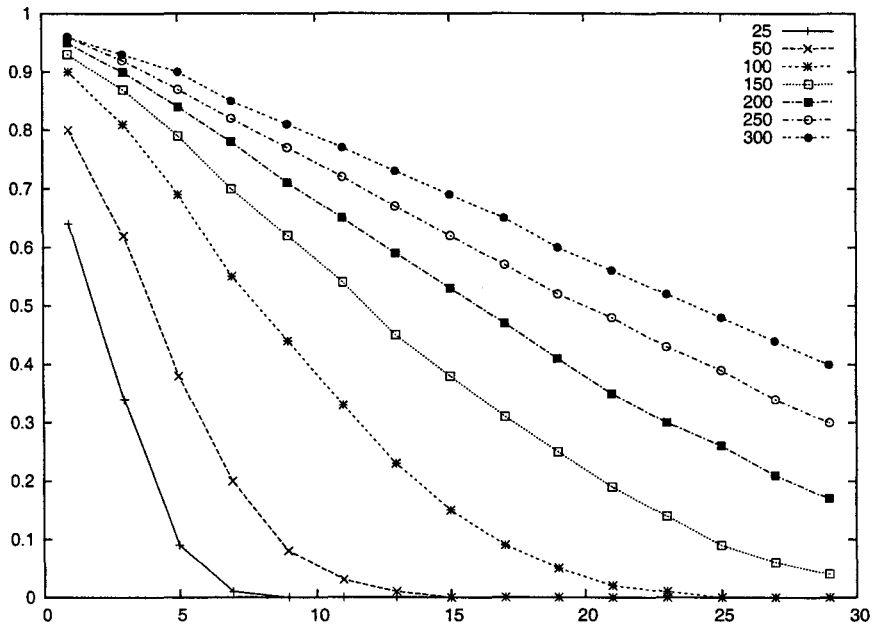



FIG. 2.12 – SRB du mode 2 en fonction de la probabilité pour différentes densités

(voir figure 2.12). Le problème est facilement décelable : les petites densités maximisent le résultat de la fonction $f_{mode2}$, et donc donnent une probabilité de réémission élevée. Cette particularité est très gênante dans le cas de réseaux à faible densité, car le gain obtenu est nul, proche de l'inondation. Par contre, pour de grandes densités (plus de 200 nœuds, soit une densité moyenne de 40 nœuds par zone de communication), les résultats obtenus pour le SRB sont nettement supérieurs à ceux du mode 1. Pour une valeur de $k$ égale à 11, le SRB varie de 65% à 80% du SRB pour ces grandes densités.

Néanmoins, cette idée propose une première approche de l'exploitation de l'information concernant le voisinage. Cette méthode est simple et relativement facile à mettre en oeuvre. Même si elle plus efficace que $f_{mode1}$, elle possède le même défaut : elle ne tient pas compte de la topologie locale, à savoir les liens entre le nœud source et les voisins, et les liens entre voisins.

### 2.7.3 Mode 3

Le graphe 2.13 présente l'accessibilité pour le mode 3. Les performances sont relativement moyennes, l'accessibilité diminue trop rapidement pour être acceptable lorsque le paramètre $\sigma$ augmente. L'accessibilité n'est jamais parfaite pour les faibles densités quelle que soit la valeur $\sigma$ choisie. Dans le cas de grandes densités, l'accessibilité cesse d'être parfaite dès que $\sigma$ devient supérieur à 1.

La figure 2.14 présente le SRB pour le mode 3. Très logiquement, celui-ci est inversement proportionnel au RE. Mais il est très nettement en défaveur du mode 3, surtout comparé au mode 2. Si l'on désire une accessibilité complète, le mode 2 permet d'y arriver avec une valeur $k$ supérieure à 11, alors que le mode 3 n'y arrive même pas avec un $\sigma$ faible. De plus, pour une même accessibilité, le SRB est meilleur pour le mode 2.

L'intérêt d'utiliser les modifications introduites dans le mode 2 à l'intérieur du mode 3 prend donc toute son importance. En effet, la pseudo distance calculée ne tient pas compte de la densité. Il est donc nécessaire d'adapter le seuil de réémission par rapport à la densité locale.

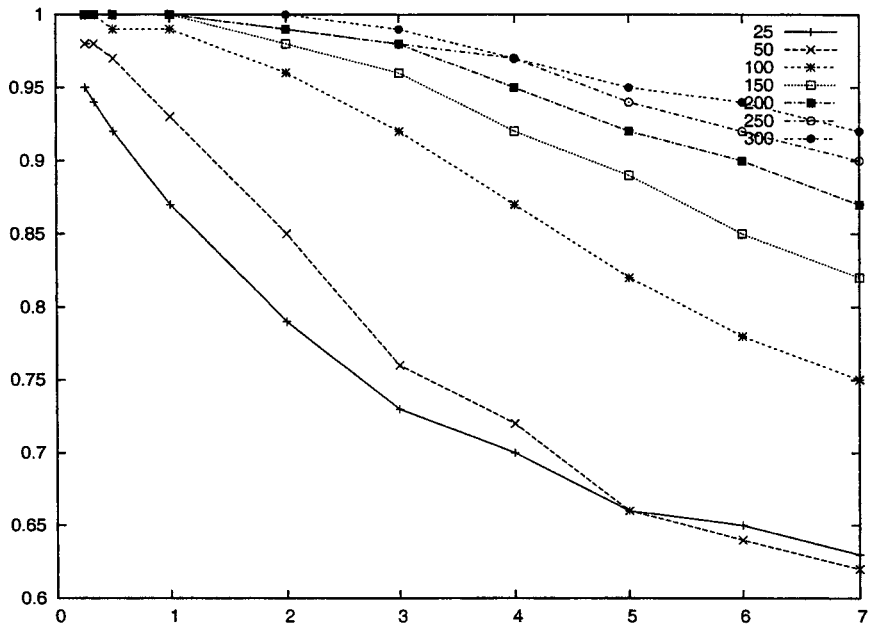



FIG. 2.13 – RE du mode 3 en fonction de la probabilité pour différentes densités

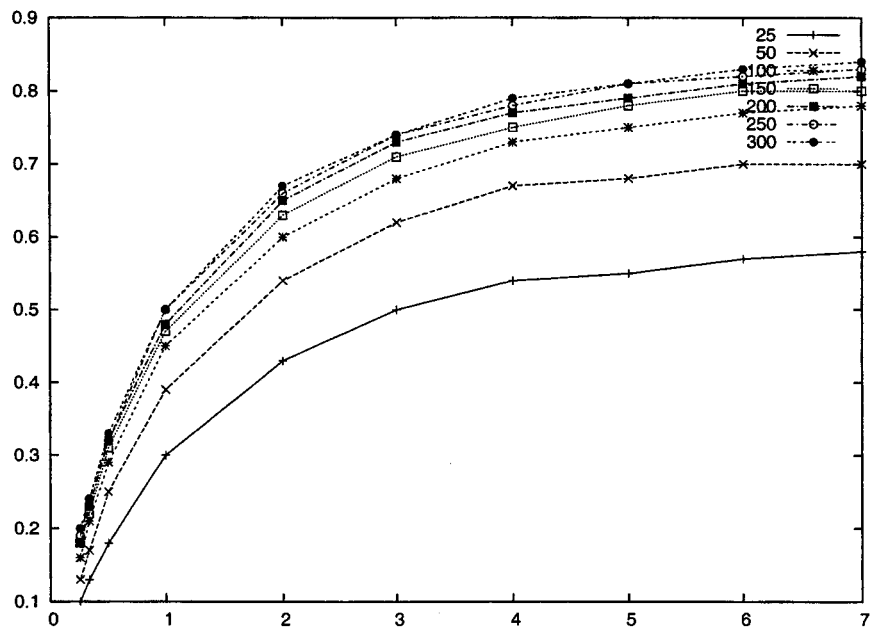



FIG. 2.14 – SRB du mode 3 en fonction de la probabilité pour différentes densités

### 2.7.4 Mode 4

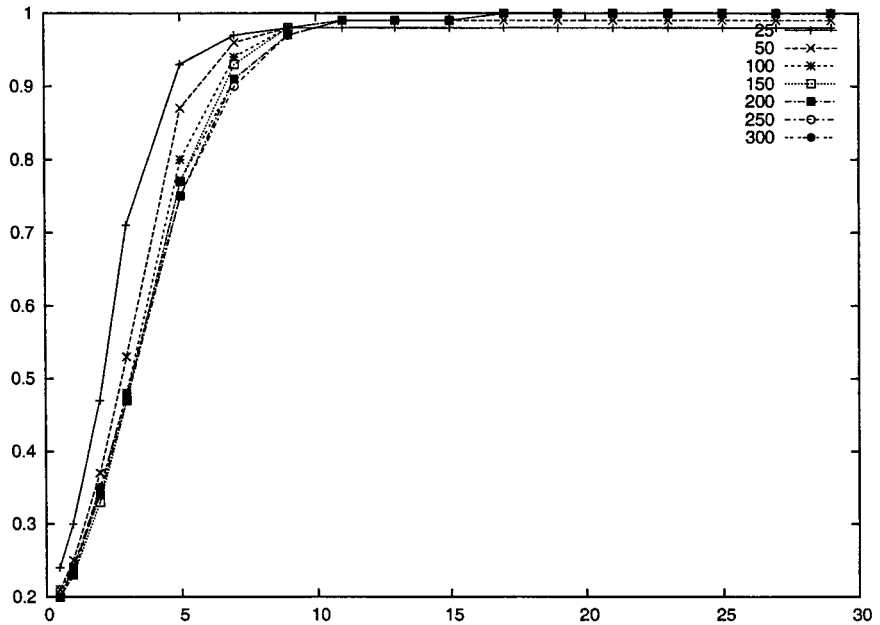



FIG. 2.15 – RE du mode 4 en fonction de la probabilité pour différentes densités, avec $\sigma = 0.5$

Les graphiques 2.15, 2.16, 2.17, 2.18, 2.19 et 2.20 présentent les résultats obtenus avec le mode 4 pour des valeurs de $\sigma$ égales respectivement à 0.5, 1 et 2. Pour chaque graphique, $k$ est évalué pour des valeurs allant de 0.5 à 29.

Cette amélioration permet d'atteindre le RE que n'offrait pas le mode 3. Selon la valeur de $\sigma$, une accessibilité complète est atteignable pour des valeurs de $k$ à partir de 11 (avec un $\sigma$ égal à 0.5), et cela pour tous les modes. Par exemple, pour atteindre 99% des nœuds, on peut utiliser le couple de valeurs $\sigma = 0.5, k = 11$ ou $\sigma = 1, k = 15$ ou $\sigma = 2, k = 27$. Le point à retenir est que, quelle que soit la valeur de $\sigma$ choisie, il faut alors adapter la valeur $k$ en conséquence.

En ce qui concerne le pourcentage de messages de diffusion économisés, on obtient un SRB allant jusqu'à 82% (dans le cas d'une densité de 60 nœuds par zone de communication). On obtient pratiquement les mêmes résultats en terme de SRB par rapport à une accessibilité donnée. Par exemple, dans le cas d'une densité de 60 nœuds par zone de communication, on obtient un SRB de 86% pour $\sigma = 0.5, k = 11$ et $\sigma = 1, k = 15$. On peut remarquer néanmoins un phénomène intéressant : pour une accessibilité donnée, plus le $\sigma$ augmente, plus le SRB décroît (lentement). Mais dans le même temps, le SRB des basses densités devient plus important, surtout pour un $k$ élevé. Par exemple, pour une densité de 20 nœuds par zone de communication et pour une valeur $k$ égale à 30, le SRB avec $\sigma = 1$ est égale à 2% alors qu'avec $\sigma = 2$ il est pratiquement de 50%.

Mais encore une fois, on retrouve la difficile balance entre l'accessibilité et le pourcentage de messages de diffusion économisés. Dès que la valeur de $\sigma$ augmente (3 ou 5), la valeur de RE devient trop mauvaise pour être acceptable. L'approche stochastique démontre son efficacité mais pourrait encore être améliorée. L'utilisation d'un protocole déterministe tel que le mécanisme d'élimination des voisins va permettre de profiter au maximum d'une bonne dispersion de la première vague (celle du mode 4) en comblant les nœuds pauvres des décisions probabilistes de leur voisinage.

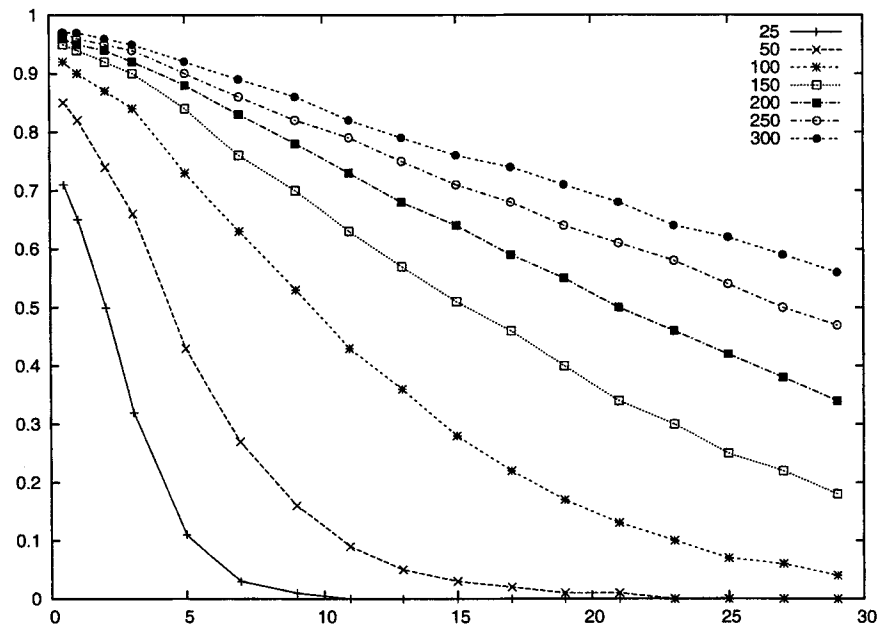



FIG. 2.16 – SRB du mode 4 en fonction de la probabilité pour différentes densités, avec $\sigma = 0.5$

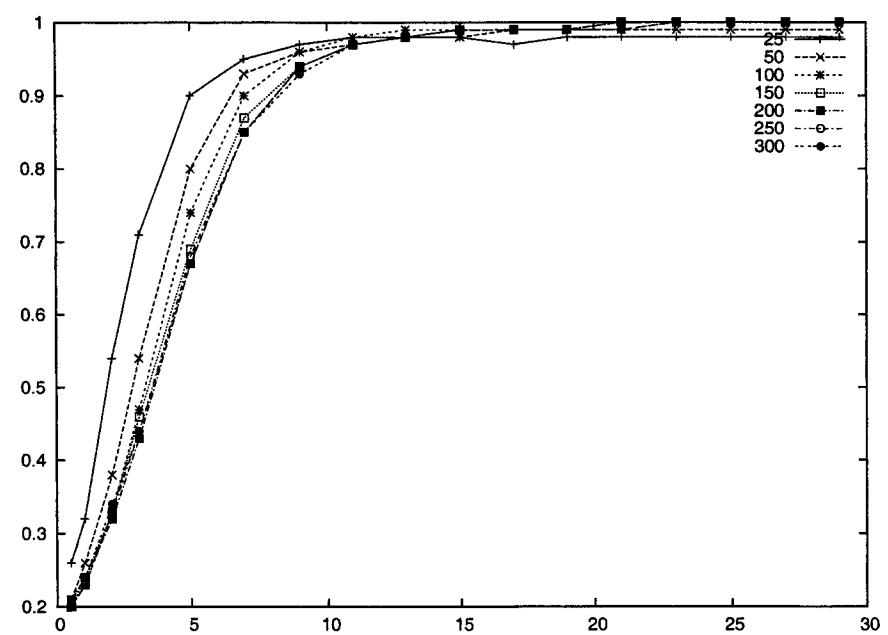



FIG. 2.17 – RE du mode 4 en fonction de la probabilité pour différentes densités, avec $\sigma = 1$

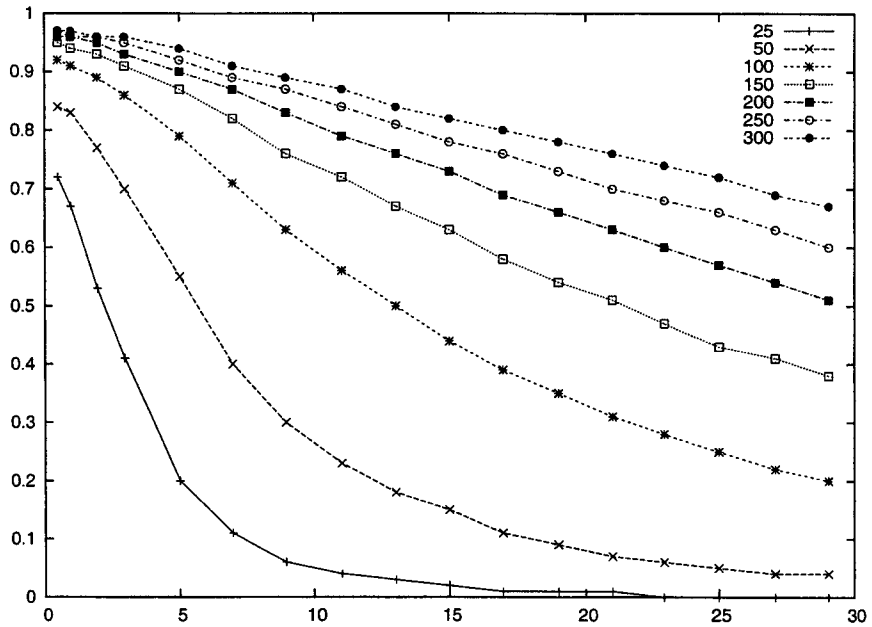



FIG. 2.18 – SRB du mode 4 en fonction de la probabilité pour différentes densités, avec $\sigma = 1$

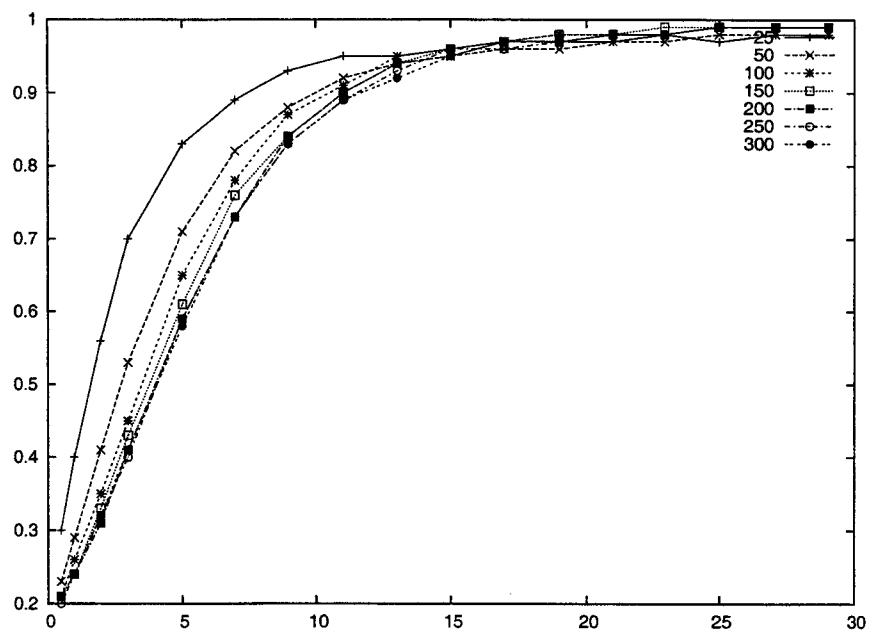



FIG. 2.19 – RE du mode 4 en fonction de la probabilité pour différentes densités, avec $\sigma = 2$

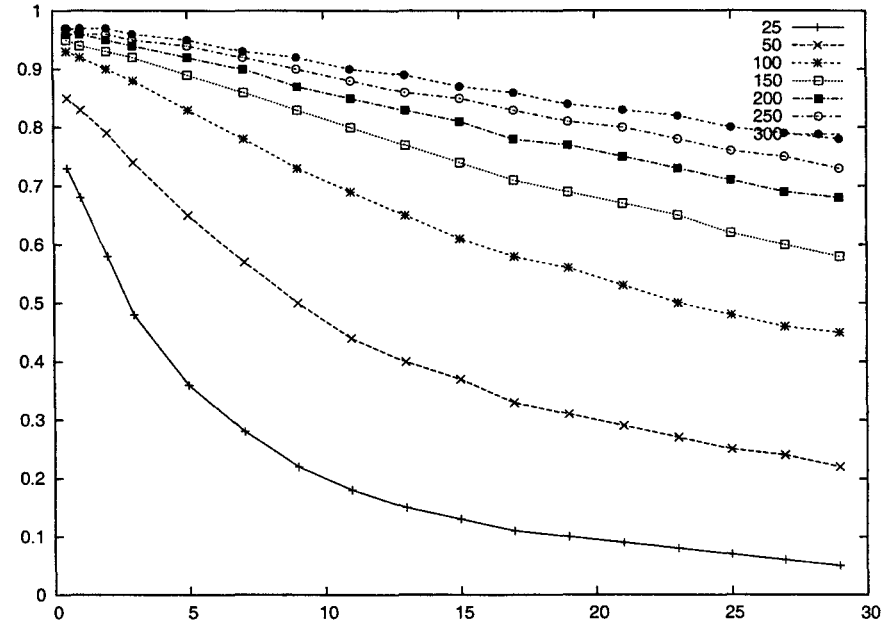



FIG. 2.20 – SRB du mode 4 en fonction de la probabilité pour différentes densités, avec $\sigma = 2$

### 2.7.5 Mode 5

Les graphiques 2.22, 2.21, 2.24, 2.23, 2.26 et 2.25 présentent les résultats obtenus avec le mode 5 pour $\sigma$ égal respectivement à 1, 3 et 5. Pour chaque graphique, la valeur $k$ est évaluée pour des valeurs allant de 0.25 à 29. L'accessibilité (RE) n'est pas présentée car, avec l'aide du mécanisme d'élimination des voisins et du fait que le graphe généré est connexe, chaque membre du réseau reçoit le message de diffusion. Plus exactement, les pertes d'accessibilité proviennent de l'utilisation d'une couche MAC réelle, et la plus basse accessibilité atteinte dans de rares occasions est de 98,75%.

Le pourcentage de messages de diffusion économisés est très bon. Il est très proche du mode 4 (moins de 2% de différence dans le cas de grandes valeurs de $k$), sauf dans le cas de petites valeurs de $k$. En effet, dans ce cas, l'utilisation exagérée du mécanisme d'élimination des voisins réduit le SRB (car l'accessibilité « naturelle » est loin d'être parfaite, comme vu dans le mode 4).

Ces résultats, et surtout le très bon comportement du SRB pour une accessibilité parfaite, sont explicables par plusieurs points importants. Premièrement, le rôle du mécanisme d'élimination des voisins est de réparer les petites erreurs locales dûes à de mauvais tirages. Comme ce rôle est limité, et qu'un mécanisme de *timeout* permet de privilégier les nœuds ayant le plus de chances de joindre les entités isolées, son usage est très léger. Il permet néanmoins de garantir une accessibilité parfaite.

Pour l'utilisation du mécanisme d'élimination des voisins (NES), il existe un équilibre à trouver en fonction du but final d'utilisation du protocole. Si l'on recherche un SRB parfait, il vaut mieux choisir un $k$ faible. En effet, le mécanisme d'élimination favorise alors les nœuds les plus éloignés de la source locale, grâce à une durée *timeout* calculé sur la pseudo-distance. De plus, le mécanisme utilisé de façon intensive permet d'utiliser au maximum l'écoute passive des communications sur le réseau et ainsi maximiser les chances de connaître l'ensemble des nœuds ayant déjà reçu le message. Comme le montrent les graphiques 2.21, 2.23 et 2.25 dans le cas où seul le mécanisme d'élimination est utilisé (c'est-à-dire quand $k = 0$), on obtient les meilleurs SRB.

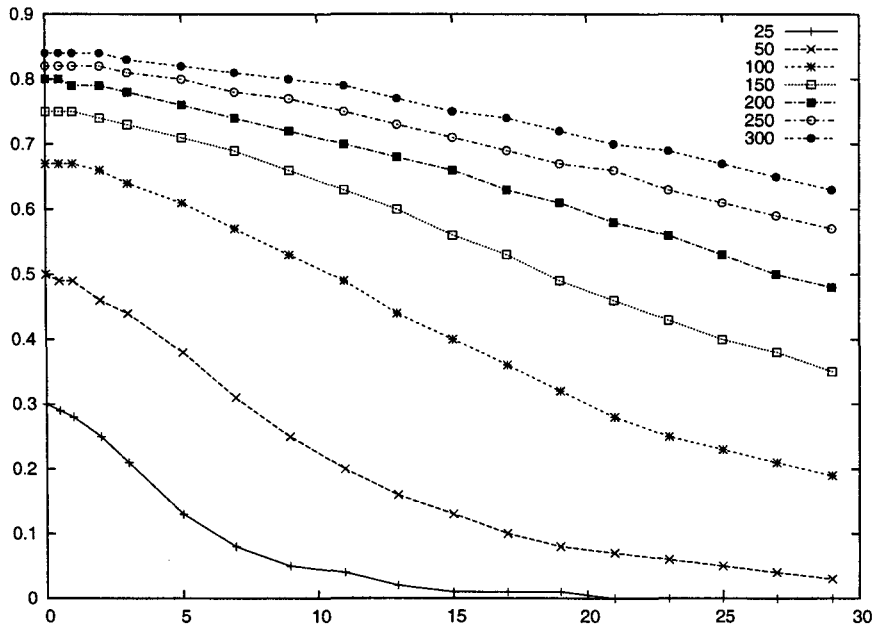



FIG. 2.21 – SRB du mode 5 en fonction de la probabilité pour différentes densités, avec $\sigma = 1$

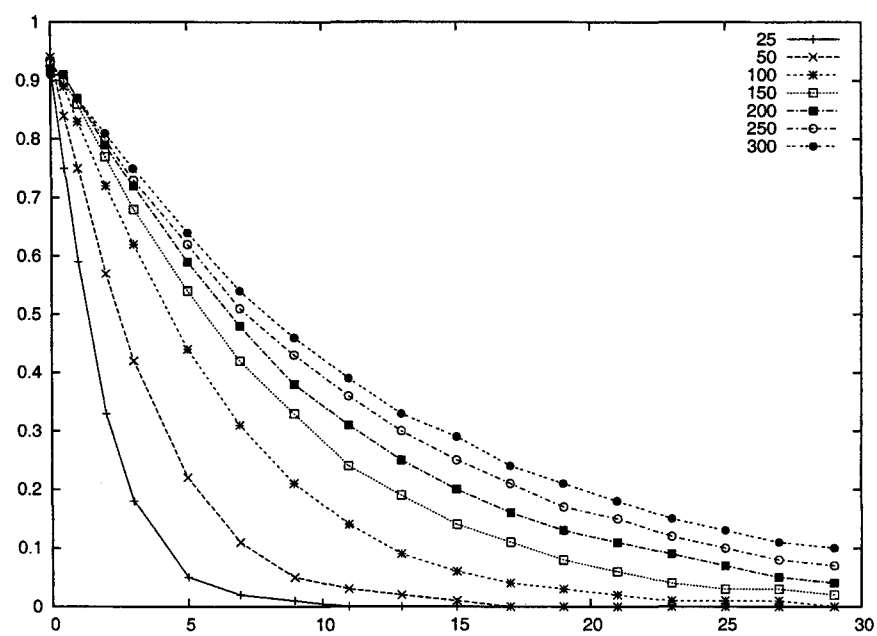



FIG. 2.22 – NES du mode 5 en fonction de la probabilité pour différentes densités, avec $\sigma = 1$

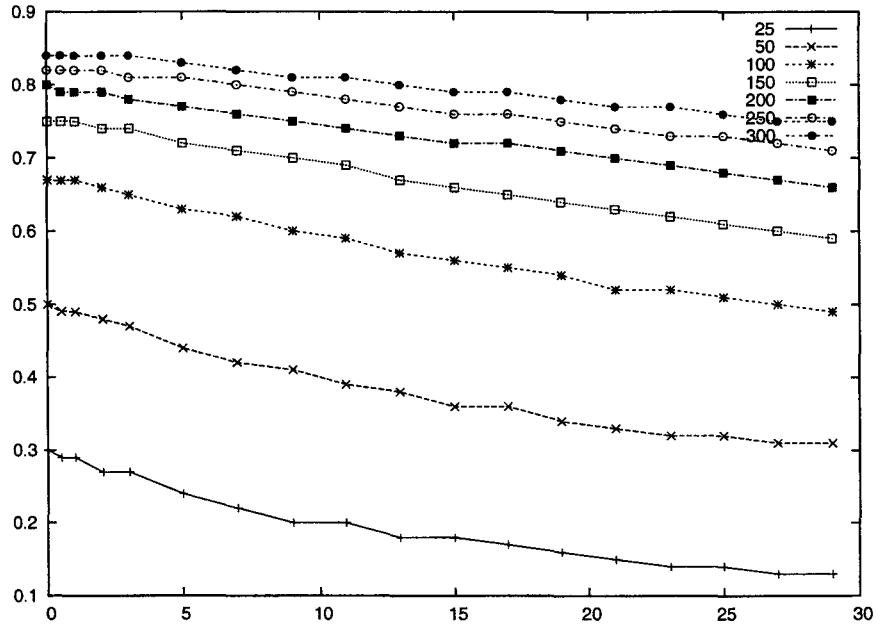



FIG. 2.23 – SRB du mode 5 en fonction de la probabilité pour différentes densités, avec $\sigma = 3$

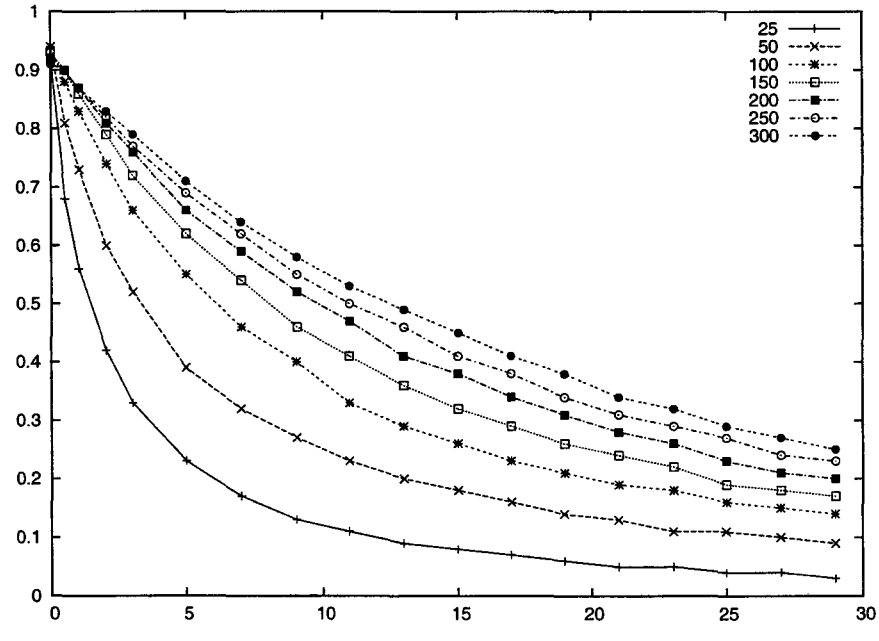



FIG. 2.24 – NES du mode 5 en fonction de la probabilité pour différentes densités, avec $\sigma = 3$

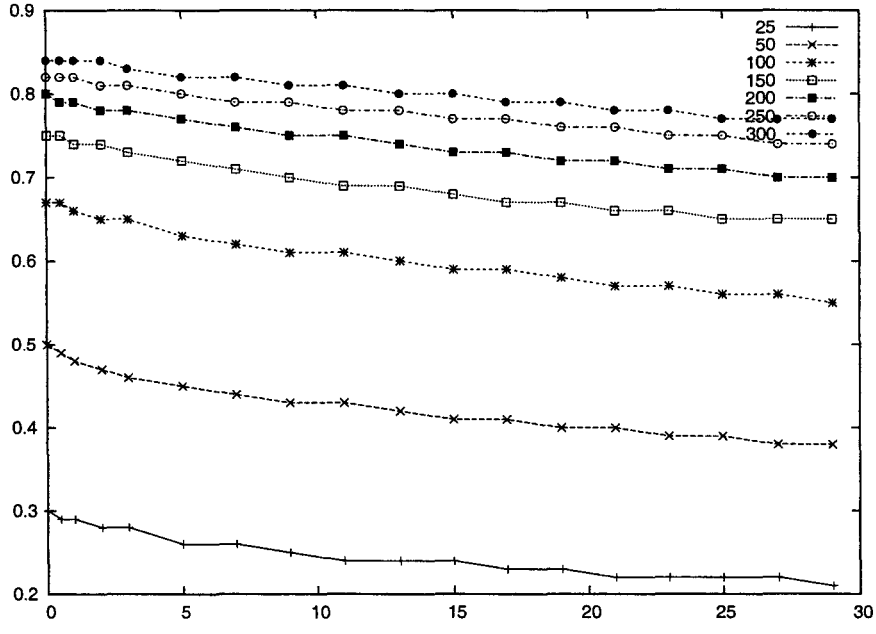



FIG. 2.25 – SRB du mode 5 en fonction de la probabilité pour différentes densités, avec $\sigma = 5$

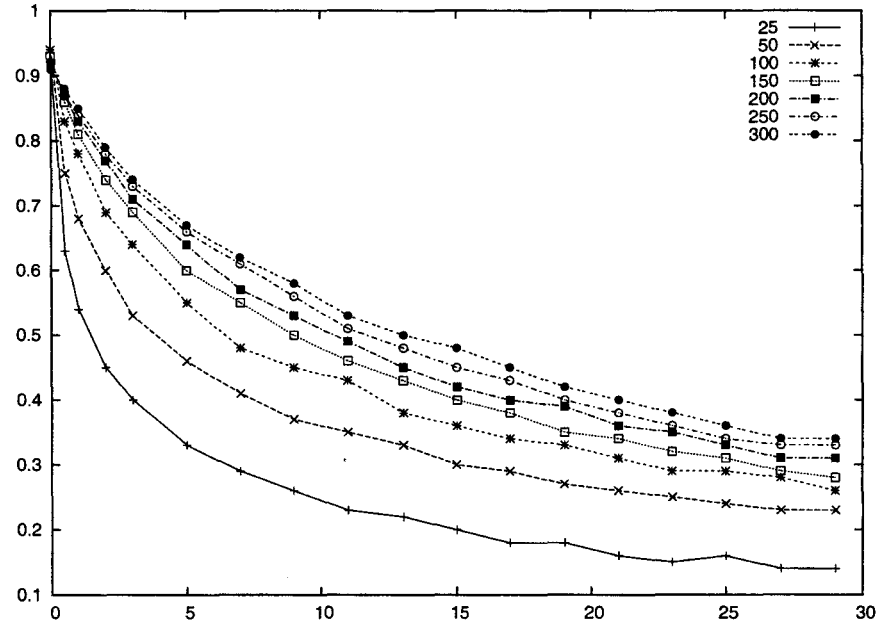



FIG. 2.26 – NES du mode 5 en fonction de la probabilité pour différentes densités, avec $\sigma = 5$

Par contre, cette optimalité introduit un coût dans la durée de la diffusion dans le réseau. Comme chaque mobile attend avant de réémettre, la propagation du message dans le réseau est plus lente. L'algorithme permet, grâce aux paramètres $k$ et $\sigma$ d'économiser l'accès à l'élimination des voisins. Pour des valeurs $\sigma = 1$ et $k = 29$, le mécanisme d'élimination des voisins est utilisé à moins de 10% du nombre total de messages envoyés (voire moins dans le cas de petites densités). Par contre, on obtient une baisse du SRB de l'ordre de 20%.

Il y a donc bien un équilibre, il faut soigneusement séléctionner les valeurs de $\sigma$ et $k$ pour privilégier le temps de propagation ou un SRB optimal.

## 2.8 Conclusion

L'approche probabiliste est resté relativement impopulaire parmi la communauté ad hoc, de peur que la diffusion offre une couverture incomplète. En général, cette opinion était confortée par les faibles performances des versions naïves du protocole probabiliste. Nous avons proposé ici diverses extensions pour permettre de rendre l'approche probabiliste intéressante. Premièrement, la méthode stochastique est utilisée pour permettre la meilleure diffusion possible au voisinage, en tentant de maximiser une bonne distribution des nœuds relais qui diminue le nombre de messages. Deuxièmement, un mécanisme déterministe d'élimination des voisins permet de corriger les erreurs locales, et ainsi assurer une couverture complète du réseau. Le protocole BRP profite des deux approches pour offrir le meilleur d'une bonne répartition des nœuds relais avec l'aide de la notion de pseudo-distance pour privilégier les nœuds en bordure, de l'aléatoire pour posséder un système localisé de prise de décision, et de la garantie de joindre l'ensemble des nœuds avec l'élimination des voisins. Il peut, au vu des résultats, être compétitif à d'autres approches.

Dans ce travail, la mobilité n'a pas été étudiée, mais il serait intéressant de voir quel véritable effet elle provoque sur ce protocole. On peut penser que ce protocole sera robuste, car il tirera parti du fait que la prise de décision est faite en considérant l'information du groupe dans son ensemble, sans s'appuyer sur quelques nœuds susceptibles de manquer à leurs obligations.

Un autre point intéressant, c'est que ce protocole utilise beaucoup de variables, et qu'il est possible que certaines d'entre elles soient superflues. Le comportement de $\sigma$ et $k$ est intéressant, car il est possible que ces valeurs soient fixées, pour réduire la complexité de l'ensemble et offrir un protocole encore plus simplifié.

# Chapitre 3

# Diffusion par relais RNG

Dans le précédent chapitre, nous avons présenté un algorithme probabiliste réduisant le nombre de paquets de diffusion émis tout en maintenant une accessibilité quasi-parfaite. Nous proposons maintenant le protocole RRS [11] réunissant les mêmes conditions, chaque nœud décidant par lui-même s'il a besoin de réémettre ou non. Mais ici, l'approche est différente car le procédé n'est pas probabiliste et s'appuie sur l'utilisation d'un algorithme de réduction de graphe baptisé RNG pour aider à la décision de réémission.

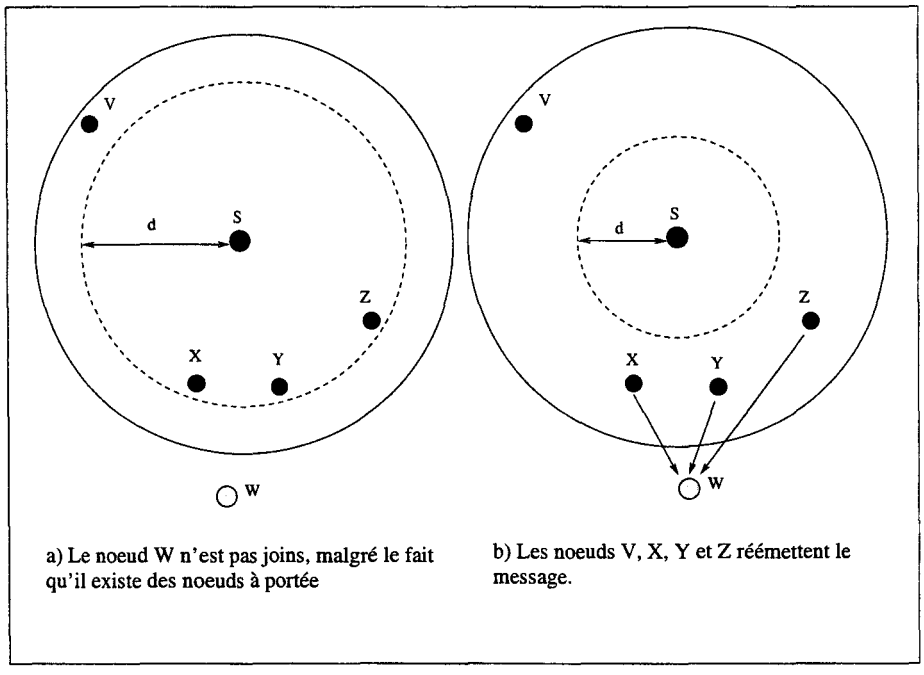
## 3.1 Approches

Avec le protocole que nous développons par la suite, nous nous concentrons sur deux approches. La première est l'utilisation d'une méthode qui évalue la condition de réémission de façon à privilégier les nœuds en bordure de la zone de communication. Utilisée naïvement, en fonction de la distance séparant la source de ses voisins, cette approche est inefficace. Il faut une autre méthode pour la décision de réémission, à partir d'un sous-ensemble de nœuds à joindre. Quant à la deuxième approche, il s'agit celle de l'indépendance de la source, c'est-à-dire de ne pas dépendre du nœud qui a fait parvenir le message lors de la décision de réémission.

### 3.1.1 Privilégier les nœuds en bordure de la zone de communication

Dans le problème de diffusion dans un réseau sans fil, il est plus intéressant de privilégier les nœuds en bordure de la zone de communication pour la réémission. En effet, ils ont le plus de chance de pouvoir joindre de nouveaux nœuds. Cette idée est déjà présente dans [67] qui traite du problème de tempête de messages d'inondation. Les auteurs proposent d'émettre ou non, en se basant sur la distance entre deux nœuds : si cette distance est supérieure à un seuil $d$ alors le nœud réémet. Dans le cas contraire, le nœud ne fait rien. Cette solution n'est pas vraiment bonne, car elle possède deux défauts fondamentaux : le fait que le seuil soit fixe, et l'inefficacité de ce mécanisme en cas de forte densité.

Le premier problème concerne tous les nœuds situés entre le seuil de réémission (c'est-à-dire la distance minimale $d$ entre la source et le nœud pour que ce dernier réémette) et la bordure de la zone de communication. Si l'on considère l'exemple donné dans la Fig. 3.1(b), les nœuds $X$, $Y$ et $Z$ vont réémettre le message reçu de la part du nœud $S$, et le nœud $W$ va recevoir trois fois le même message. De plus, un nœud va réémettre, même s'il n'a pas de voisins à joindre, comme par exemple le nœud $V$. Le deuxième problème, visible sur la Figure 3.1(a), est l'exact opposé. Si le seuil de réémission $d$




a) Le noeud W n'est pas joins, malgré le fait qu'il existe des noeuds à portée

b) Les noeuds V, X, Y et Z réémettent le message.

FIG. 3.1 – Exemples de réémission avec le protocole basé sur la distance.

est trop haut ou si la configuration topologique ne s'y prête pas, aucun nœud ne va réémettre même s'il existe des nœuds à deux sauts joignables. Plus généralement, le fait que la décision soit prise par rapport à un seuil fixé de façon globale, indépendamment de la densité et de la configuration topologique locale, donne un algorithme trop peu adaptatif pour donner de bons résultats.

Un critère supplémentaire est nécessaire. Il doit donner une information caractérisant la nécessité de réémettre ou non. Il pourrait se baser sur une information topologique provenant du voisinage. Ce critère idéal doit pouvoir caractériser les trois règles suivantes :

**Règle 1 :** Un nœud ne doit pas réémettre s'il ne joint pas de nouveaux nœuds.

**Règle 2 :** Si plusieurs nœuds peuvent joindre un ou plusieurs nœuds communs non joints, alors il doit exister une règle minimisant le nombre de nœuds qui doivent réémettre.

**Règle 3 :** Si plusieurs nœuds peuvent joindre un nœud non joints à l'extérieur de la zone de communication, alors il est plus intéressant que ce soit le nœud le plus proche qui réémette. Ce critère apparaît pour plusieurs raisons. Premièrement, si deux nœuds sont proches, alors la communication est meilleure, car elle a moins de chance d'être perturbée par les autres émissions. Deuxièmement, un nœud non joint a de grandes chances de posséder dans son voisinage d'autres nœuds non joints, vu que la communication omnidirectionnelle couvre des ensembles de nœuds. Plus le nœud émetteur est proche de nœuds non joints, plus il a de chance de couvrir d'autres nœuds non joints.

Pour répondre à ces règles, une première idée est d'utiliser le système d'élimination des voisins présenté en section 1.4.4. Il permet alors de répondre aux deux premières conditions : un nœud connaissant son voisinage peut déterminer s'il est nécessaire de réémettre, et comme nous travaillons dans un environnement asynchrone (il n'y a pas d'horloge centrale, l'accès à la couche MAC se fait de façon anarchique), le premier nœud à émettre informe les autres de sa diffusion, et donc de l'inutilité de réémettre. Mais le mécanisme d'élimination des voisins ne permet pas de garantir la troisième

condition. En effet, c'est le premier nœud qui réémet le message qui joint le ou les nœuds à l'extérieur de la zone de communication. Ce défaut entraîne une solution sous-optimale.

Une optimisation possible est de privilégier les nœuds situés à la limite de la zone de communication, en leur donnant un temps plus court avant de réémettre. La formule est simple : soit $t$ la durée maximale du temps d'attente (*timeout*), ce temps est décomposé en deux parties : $t_{fixe}$ représente une durée incompressible d'attente et $t_{alea}$ une durée pendant laquelle les nœuds vont tenter de réémettre. On pose $t = t_{fixe} + t_{alea}$, et la durée d'attente pour un nœud situé à distance $dist$ de l'émetteur est égale à $t_{fixe} + t_{fixe}/dist$. Mais cette approche ne résout pas un autre défaut : celui des nœuds lointains. Si deux nœuds sont à l'extrémité de la zone de communication, et s'ils savent qu'un nœud en dehors de la zone de communication n'a pas été joint, ils vont tous les deux réémettre. Si ces deux nœuds n'ont aucun contact direct entre eux, ils ne peuvent savoir que l'autre a déjà émis.

La nécessité d'avoir un critère supplémentaire de décision est donc indispensable. Il faut que celui-ci permette, de manière décentralisée, d'attribuer à chaque nœud la décision de réémettre en fonction des 3 critères évoqués ci-dessus. La nécessité d'avoir un ordre entre tous les nœuds pouvant réémettre peut être un moyen pour subvenir aux besoins des 3 critères.

### 3.1.2 Le problème d'indépendance de la source

Certains protocoles, comme MPR (voir la section 3.2) ou TBRPF (*Topology Broadcast Based on Reverse-Path Forwarding*) [7], choisissent parmi le voisinage les nœuds qui vont réémettre le message de diffusion. On parle alors de protocole dépendant de la source (ou *source-dependant*). Ces protocoles ajoutent dans leurs messages de diffusion une liste de leurs voisins qui vont réémettre et le voisinage prend ainsi connaissance de la manière de réémettre les messages de diffusion.

Une autre approche est de proposer des protocoles indépendants de la source. Dans ce cas, chaque nœud décide par lui-même s'il doit réémettre ou non. Cette décision doit s'appuyer sur l'état du nœud et les informations qu'il possède du voisinage.

Les avantages de l'indépendance par rapport à la source sont importants dans le cas de certaines difficultés réseaux (comme une forte mobilité et/ou une importante charge) qui peuvent perturber sensiblement les protocoles. En effet, le fait de diffuser la liste des voisins peut entraîner une augmentation sensible de la taille des paquets, offrant plus de chances aux collisions.

De plus, les émissions régulières de l'ensemble des voisins peuvent ne pas suffire à avoir une cohérence locale correcte. Entre deux messages HELLO, le voisinage d'un nœud peut changer de façon importante. Ainsi, un nœud à deux sauts peut se retrouver non couvert car le voisin qui devait lui relayer le message a changé de position. Un protocole dépendant de la source s'appuie sur une connaissance complète des voisins à deux sauts, et prend sa décision sur l'hypothèse qu'aucun voisin n'aura bougé, car il existe une relation forte entre l'émetteur et les ordres qu'il donne à ses voisins. Avec les protocoles indépendants de la source, ce problème est moins important car il s'appuie sur des informations à un saut (il peut connaître des informations à deux sauts, mais une erreur dans cette topologie ne doit pas entraîner pas une incohérence dans la décision de rediffusion).

## 3.2 Protocoles de diffusion par voisins relais

L'un des protocoles les plus populaires concernant le problème d'indépendance de la source est MPR, proposé par Qayyum *et al.*, déjà présenté dans la section 1.4.4. Un des problèmes de MPR, et plus généralement d'autres protocoles, concerne la décision de rediffusion. Chaque nœud décide quel voisin va rediffuser le message. Cette approche possède quelques faiblesses. La nature volatile

et changeante des réseaux ad hoc ne garantit pas que les ordres de rediffusion vont être correctement interprétés. Il est nécessaire d'utiliser une approche offrant une prise de décision par chaque nœud, donc indépendante de la source.

Adjih *et al.* ont présenté dans [2] un algorithme combinant MPR et l'approche *dominating set*. Ce nouveau protocole, baptisé MPR-Dominating set, possède l'avantage de ne pas nécessiter de transmettre une liste de voisins relais dans chaque message de diffusion. À la place, un nœud peut déterminer quels sont ses voisins qui l'ont pris dans son MPR de manière complètement autonome. Pour cela, les auteurs proposent d'utiliser un autre algorithme pour calculer le MPR. Cette heuristique *min-id* sélectionne les nœuds dans l'ordre croissant de leur identifiant. Plus exactement, chaque nœud initialise son ensemble MPR. Puis, tant que tous les voisins à deux sauts ne sont pas couverts, chaque nœud ajoute dans son MPR le voisin non sélectionné possédant l'identifiant le plus petit qui peut joindre les voisins non couverts à deux sauts du nœud.

L'algorithme *min-id* n'est pas optimal (il n'y a pas de borne supérieure à la taille de l'ensemble MPR), mais il possède l'avantage d'avoir une complexité de l'ordre de $\theta(m)$ (avec $m$ taille du voisinage). Le plus intéressant est que chaque nœud peut connaître l'ensemble des voisins qui l'ont choisi comme faisant partie de leur MPR (mais alors la complexité est de l'ordre de $0(m^4)$). L'algorithme de découverte de l'ensemble de sélection MPR (représentant l'ensemble des voisins ayant choisi le nœud comme MPR) est le suivant : Chaque nœud initialise son ensemble de sélection MPR à zéro. Puis, chaque nœud $a$ vérifie pour chaque couple de voisins $(b, c)$ la condition suivante : si le nœud $a$ possède le plus petit identifiant de tous les voisins de $b$ et $c$, alors $b$ et $c$ sont ajoutés à l'ensemble de sélection MPR de $a$.

Comme il est dit plus haut, cet algorithme est loin d'être optimal. Les auteurs proposent de réduire le nombre de nœuds réémetteurs en gardant un réseau connexe. Pour diminuer le nombre de nœuds MPR, l'algorithme suivant est utilisé : chaque nœud décide qu'il fait partie de l'ensemble dominant connecté si et seulement si :

1. Le nœud possède l'identifiant le plus bas de tout le voisinage
2. OU il est le relais multipoint d'un voisin avec le plus petit identifiant du voisinage.

Cette règle minimise le nombre de relais car une sélection au niveau local se réalise en fonction de l'identifiant. Ainsi, les seuls nœuds autorisés à réémettre seront les nœuds avec les plus bas identifiants combinés à leurs voisins MPR. Les auteurs démontrent la validité de leur algorithme à créer un ensemble dominant et présentent des résultats très proches de MPR. De plus, il ne requiert que la connaissance des voisins à deux sauts (les voisins des voisins et l'ensemble MPR). Un exemple de fonctionement de ce protocole est donné avec le schéma 3.2.

Ce protocole est très efficace mais possède un défaut, déjà visible dans les premières versions de Dominating Set : il privilégie les nœuds avec les identifiants les plus bas. Cette contrainte peut poser problème si l'on recherche à économiser l'énergie des nœuds (voir chapitre 4 et 5). Dans le protocole que nous développons par la suite, nous utilisons une autre approche, avec l'aide de l'algorithme de réduction de graphe RNG pour la prise de décision.

Il existe aussi les algorithmes de formation de clusters (voir section 1.4.4). Un nœud connaît son rôle et sait ainsi s'il doit réémettre ou non. Mais la reconstruction des clusters, dans le cas de changements topologiques, les rendent impraticables dans les réseaux ad hoc. Restent les solutions développées dans l'article sur la tempête de message de diffusion [67]. Mais ces solutions sont naïves par rapport aux autres protocoles, et présentent toutes des lacunes importantes (voir section 1.4.4).

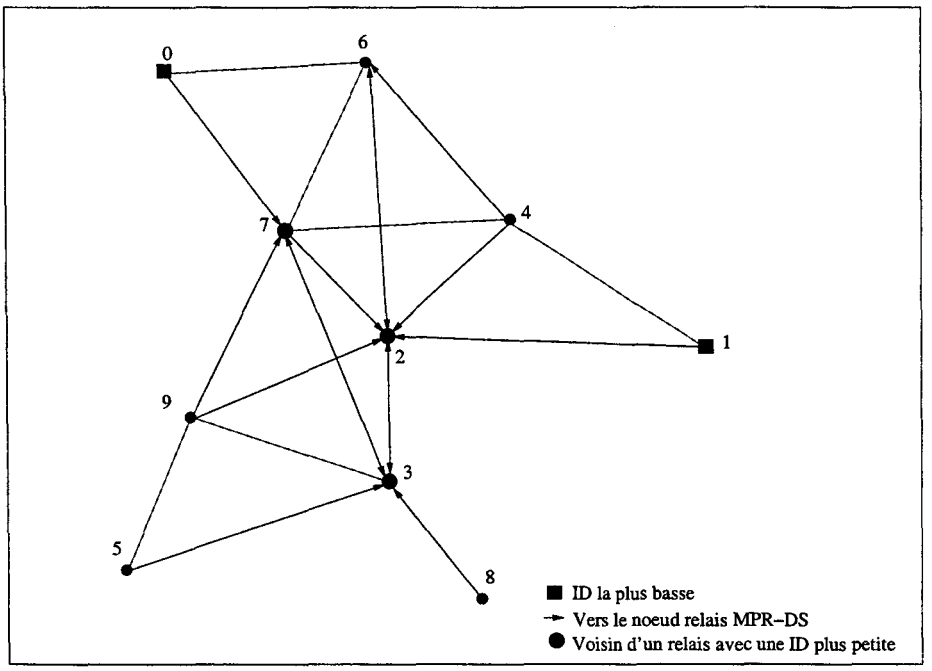



FIG. 3.2 – Exemple de fonctionnement de MPR-Dominating Set.

## 3.3 Relative Neighborhood Graph

Nous allons introduire ici quelques notions sur les graphes RNG (*Relative Neighborhood Graph*). Leurs utilisations dans le cadre de notre protocole sera expliquée dans la section 3.4. Toussaint [92] propose de définir les graphes de voisinage relatif (*Relative Neighborhood Graph* ou *RNG*), première pierre de la famille des graphes de proximité [45]. Cet ensemble s'agrandira par la suite avec les graphes de Gabriel et les $\beta$-squelettes. Le RNG est un fondement de la géométrie informatique, avec des applications dans la géographie, cartographie, biologie, reconnaissance de séquences, etc...

La définition d'un graphe RNG est la suivante. En reprenant les notations développées dans la section 1.4.2, soit $d$ la fonction distance entre deux points. Le graphe $RNG(G)$ contient le sous ensemble $RNG(G) = (V, E_{rng})$ qui répond à la propriété suivante :

$$E_{RNG}(G) = \{(u,v) \in E \mid \nexists w \in E d(u,w) < d(u,v) \wedge d(v,w) < d(u,v).\}$$

Une autre écriture possible est la suivante :

$$E_{RNG}(G) = \{(u,v) \in E \mid \nexists w \in N(u) \cap N(v) d(u,w) < d(u,v) \wedge d(v,w) < d(u,v).\} \quad (3.1)$$

La figure 3.3 présente le cas d'une configuration avec trois nœuds. Le nœud $W$ étant présent, alors le lien $(U,V)$ n'est pas dans le RNG. Les deux liens validés dans le RNG sont alors $(U,W)$ et $(V,W)$.

Un exemple de graphes représentant un réseau sans fil et le graphe RNG associé sont présentés par les figures. 3.4 et 3.5.

Les graphes RNG possèdent quelques propriétés très intéressantes. Toussaint a montré [92] que si le graphe $G$ est connecté alors $RNG(G)$ est lui aussi connecté. Il s'appuie sur le fait que les

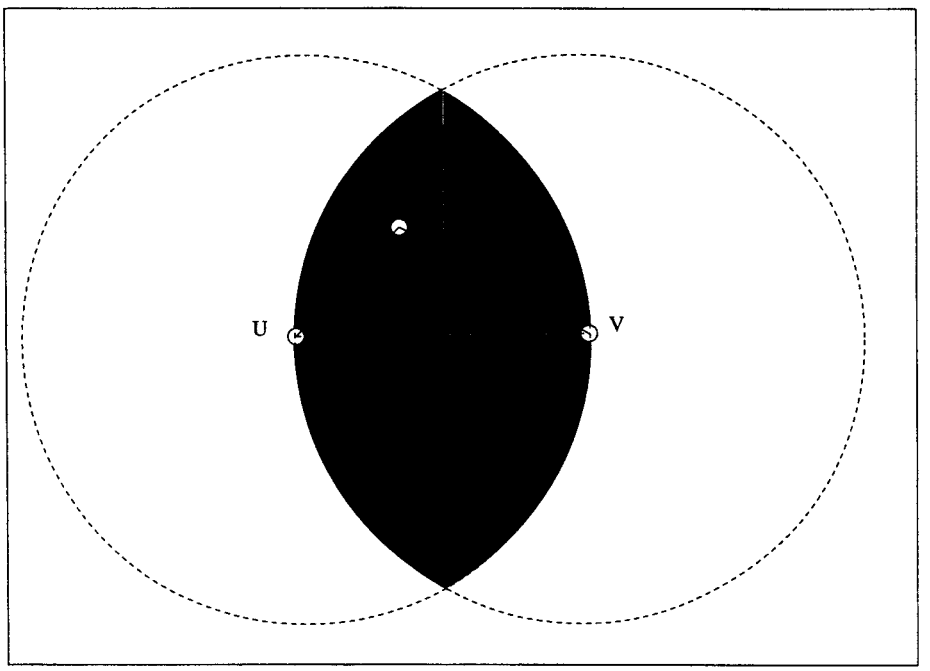



FIG. 3.3 – Configuration simple d'un graphe RNG.

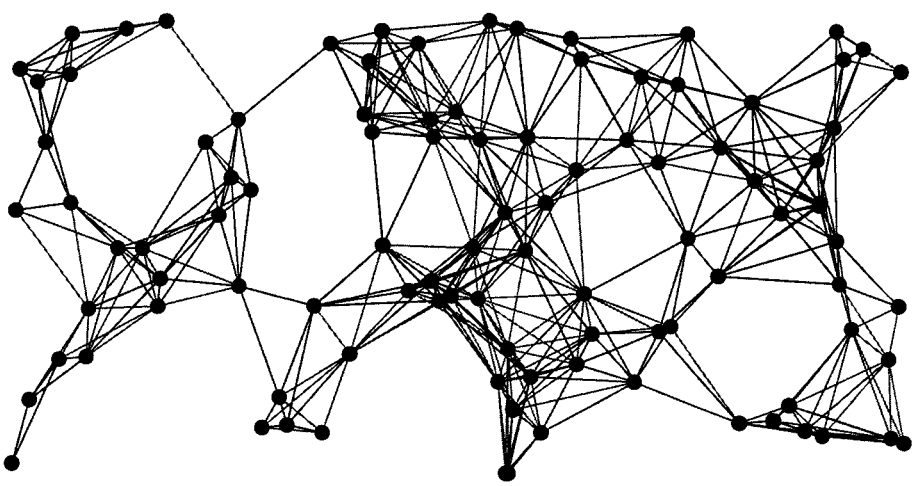


FIG. 3.4 – Le graphe d'un réseau de densité 8.

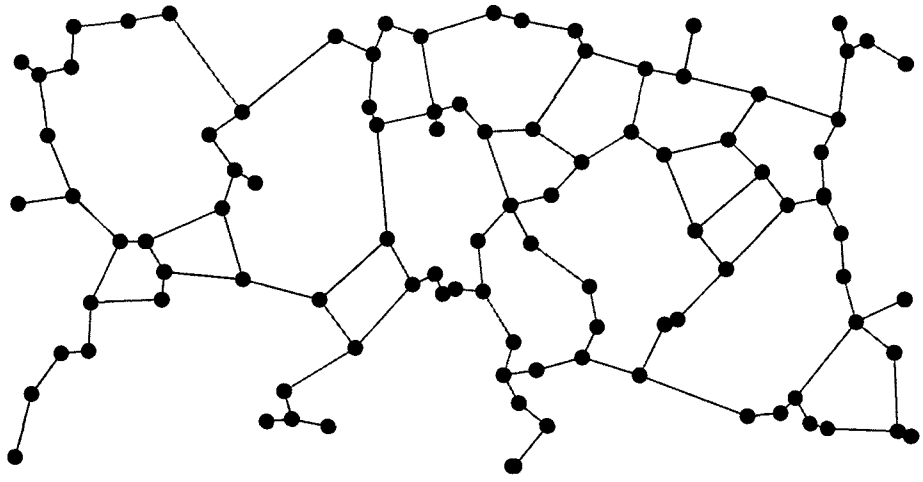


FIG. 3.5 – Le graphe RNG du réseau.

arbres recouvrants minimaux (*Minimum Spanning Tree* ou *MST*) sont inclus dans le graphe $RNG(G)$ (mathématiquement parlant, on a $MST(G) \subset RNG(G)$). De plus, $RNG(G)$ est inclus dans le procédé de triangulation de Delaunay (*Delaunay Triangulations* ou *DT*) ($RNG(G) \subset DT(G)$). Comme $DT(G)$ et $MST(G)$ conserve les propriétés de connexité, alors $RNG(G)$ est connexe si le graphe $G$ est connexe.

Une autre propriété intéressante est la taille du graphe RNG obtenu, en terme de nombre de liens. Il a été démontré que la taille minimale et maximale du graphe RNG sont bornées en deux dimensions [92]. La démonstration est relativement triviale et s'appuie sur le fait que MST est le sous-graphe de RNG et que RNG est le sous-graphe de DT. On peut en déduire que $|MST(G)| \leq |RNG(G)| \leq |DT(G)|$. Soit $n = |V|$ le nombre de nœuds dans le graphe, on peut écrire $n - 1 \leq |RNG(G)| \leq 3n - 6$. Une meilleure estimation de la borne supérieure est même proposée dans [95], avec $3n - 10$, pour $n \geq 8$.

Cette valeur est importante, car elle permet de donner une estimation du nombre moyen de voisins RNG d'un nœud. Si l'on prend la borne supérieure $3n - 6$, chaque voisin a en moyenne $3(n/n) - (6/n) = 3 - (6/n)$. Lorsque $n \rightarrow \infty$ alors le nombre moyen de voisins tend vers 3. Cette propriété indique que si la densité augmente, alors le nombre moyen maximal de voisins est stable. Ce résultat est une borne supérieure théorique. De manière empirique, le nombre moyen de voisins a été évalué à 2,6 nœuds.

Un graphe RNG est un graphe planaire. Par définition, un graphe planaire est un graphe dont il existe une représentation bidimensionnelle sans arrêtes sécantes (voir Fig. 3.5). Une démonstration par l'absurde assez simple existe. Une autre propriété intéressante concerne la fonction de distance. Quelle que soit la fonction de distance utilisée, le graphe reste connexe si cette fonction est monotone.

L'utilisation des graphes RNG dans le cas des réseaux sans fil a déjà fait l'objet de quelques travaux. Le plus notable est celui de Seddigh *et al.* [81] qui proposent de construire un ensemble dominant puis de le réduire avec l'aide du graphe RNG. Des variantes de ce protocole sont également proposées (en inversant le calcul de l'ensemble dominant et la réduction RNG, ou en utilisant le mécanisme d'élimination des voisins).

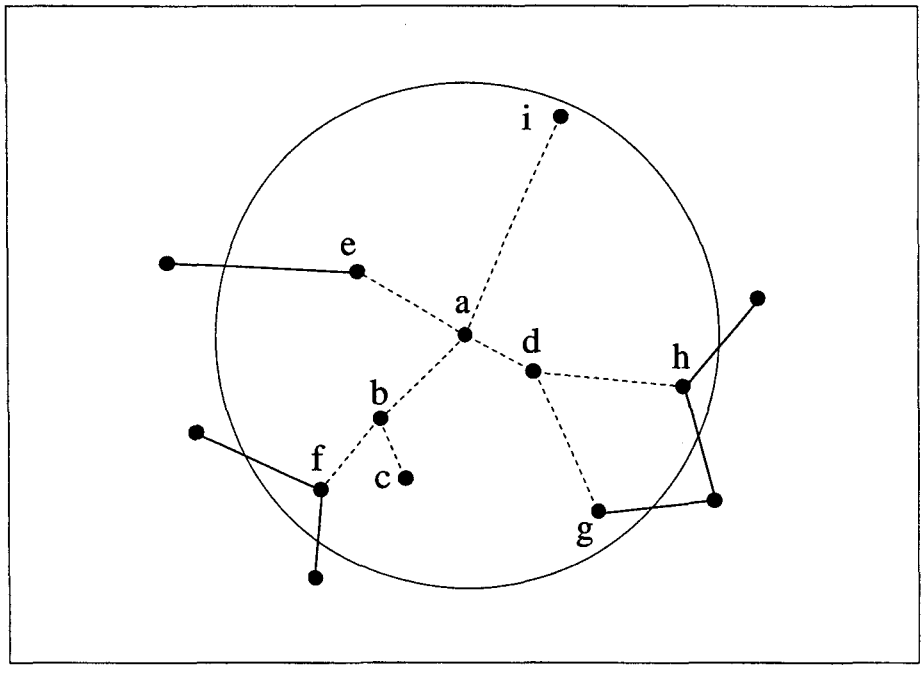



FIG. 3.6 – Exemple d'une diffusion utilisant les voisins RNG.

## 3.4 Algorithme

L'algorithme que nous proposons s'appelle RRS (*RNG Relay Subset*) et fonctionne de la manière suivante. Un nœud qui veut émettre un message de diffusion l'envoie à ses voisins, qui vont prendre la décision de réémettre en s'appuyant sur un critère local de décision. Nous proposons d'utiliser les graphes RNG pour construire un sous-graphe. Un nœud décide de réémettre si un ou plusieurs de ses voisins RNG n'ont pas reçu le message de diffusion. Plus exactement, un nœud $u$ réémet le message provenant d'un nœud $v$ si et seulement si :

$$\exists i \in N_{rng}(u) tq. i \notin N(v).$$

Le schéma 3.6 présente une exemple de fonctionnement. Le nœud $a$ émet le message de diffusion. Les nœuds $b$, $c$, $d$ et $e$ ne vont pas réémettre le message, car leur ensemble RNG est compris dans $N(a)$. Par contre, les nœuds $f$, $g$, $h$ et $i$ vont réémettre le message car ils possèdent chacun un voisin RNG n'appartenant pas au voisinage de $a$.

Le sous-graphe RNG est très intéressant, car il répond aux 3 critères évoqués un peu plus haut :

**Règle 1 :** Un sous-graphe RNG est connexe si le graphe dont il est extrait est connexe. Donc chaque nœud en dehors de la zone de communication est toujours relié, par un ou plusieurs arcs, à un nœud à l'intérieur de cette même zone. Cette propriété garantit qu'il existe toujours au moins un nœud qui a connaissance de la nécessité de réémettre le message à destination d'un de ses voisins RNG.

**Règle 2 :** Une propriété intéressante des graphes RNG est le nombre de voisins. Il a été montré plus haut qu'une borne supérieure du nombre de liens est $3n - 6$ avec $n$ nombre de nœuds. De plus, de manière pragmatique, il a été montré que le nombre moyen est encore plus bas (2,6 voisins RNG par nœud). Chaque nœud à l'extérieur de la zone de communication possède donc un

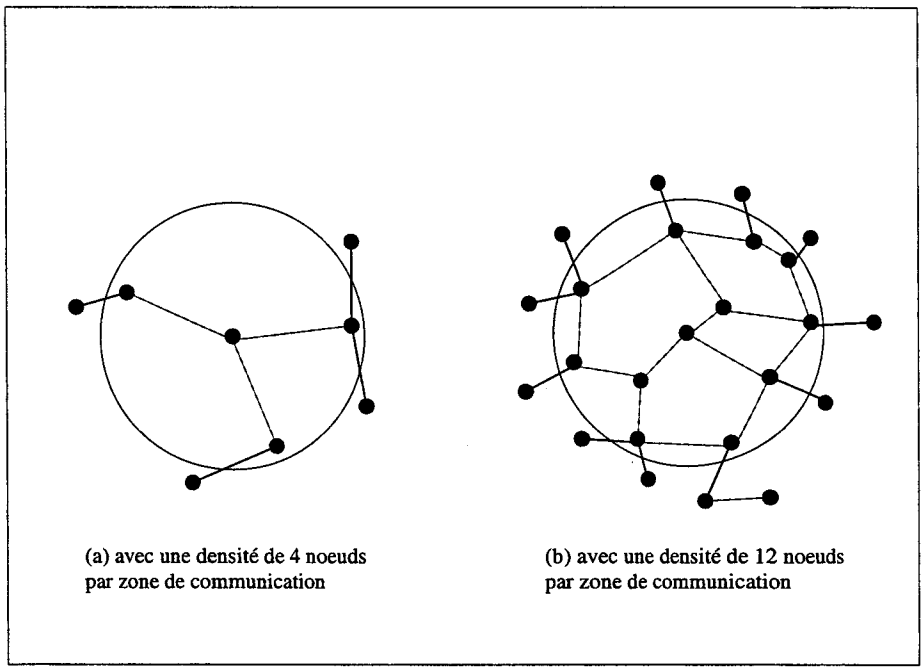



FIG. 3.7 – Deux exemples de graphes RNG avec des densités différentes.

nombre limité de voisins autorisés à réémettre le message de diffusion si ce nœud n'a pas été joint.

**Règle 3 :** Le graphe RNG a la particularité de contenir des voisins très proches de la source. Ce fait trivial provient de la définition même du RNG : « 2 nœuds font mutuellement partie du sous-graphe RNG de l'autre s'il n'existe pas de nœuds plus proches de l'un et de l'autre » (voir la formule 3.1). Ainsi, pour chaque nœud, l'ensemble de ses voisins RNG sont les plus proches pouvant garder dans le même temps la connexité complète du réseau. Grâce à cette propriété, un nœud prend en compte un ensemble réduit de voisins proches. La troisième condition recherchée est présente : privilégier les nœuds les plus proches des nœuds non contactés pour joindre le ou les nœuds à l'extérieur de la zone de communication.

Un défaut persiste dans l'approche RNG proposée. Il existe deux cas où le dispositif va être déficient. Le premier concerne le cas où deux mobiles $u$ et $v$ sont voisins RNG d'un troisième $w$. Si les deux premiers nœuds reçoivent en même temps le message d'inondation alors le nœud $w$ va recevoir le même message plusieurs fois alors qu'une fois aurait suffi. Certes, la réduction du graphe RNG permet de limiter ce nombre de voisins, mais le problème persiste.

Ce défaut n'est rien comparé au problème de la densité. Lors de l'augmentation de la densité, chaque nœud possède toujours le même nombre moyen de voisins RNG. Il y a donc logiquement une diminution importante des distances entre un nœud et ses voisins RNG. Mais dans le même temps, le nombre de nœuds à l'intérieur d'une zone de communication possédant des voisins RNG en dehors de la zone de communication augmente proportionnellement à la densité (alors que le nombre de relais d'un message de diffusion devrait tendre vers une constante, puisque que l'aire joignable par le voisinage à un saut est bornée). Ceci est illustré dans le schéma 3.7 : le second schéma (b) représente une densité triplée par rapport au premier exemple (a). On constate que le nombre de relais dans le deuxième exemple est le triple du premier.

Le but de notre protocole est de minimiser le nombre de paquets émis tout en assurant une couverture complète du réseau avec un mécanisme localisé. Le protocole doit être flexible pour gérer de petites comme de grandes densités. Pour parer aux problèmes soulevés précédemment, nous utilisons un mécanisme d'élimination des voisins. Plus exactement, chaque nœud utilise ce mécanisme seulement sur ses voisins RNG. Cette idée a plusieurs avantages : comme chaque nœud ne s'occupe que de son voisinage RNG, il est moins influencé par la mobilité. En effet, comme les voisins RNG sont très proches, l'information est plus fiable. De plus, comme le nombre de voisins RNG est faible et borné, chaque nœud ne possède que quelques voisins sous sa surveillance.

Chaque nœud qui reçoit un message de diffusion calcule l'ensemble RNG de son voisinage. Ensuite, il regarde si l'un de ses voisins RNG est en dehors de la zone de communication de l'émetteur. Pour cela, l'utilisation de la mesure de puissance n'est pas possible. En effet, si les voisins RNG sont en dehors de la zone de communication, un nœud utilisant ce système ne peut évaluer la distance le séparant de la source. Pour parer à ce problème, les nœuds comparent les listes de leurs voisins. Un nœud source $s$ ajoute à son message de diffusion la liste de son voisinage complet $N(s)$. À la réception du message de diffusion, un nœud $d$ compare la liste du voisinage ajoutée dans le message à sa liste de voisins RNG. Si $i \in N(s)$ et $i \notin N_{rng}(d)$ alors le nœud $d$ réémet le message, puisqu'il existe un voisin RNG non joint par le message de diffusion.

Pour chaque nœud, nous calculons l'ensemble $RRS(u)$, représentant l'ensemble des voisins RNG non contactés par un message de diffusion émis par le nœud $v$ :

$$\forall u \in V \quad RRS(u) = \{v \in N(u) \mid N_{rng}(v)/(N(u) \cup u) \neq \varnothing.\}$$

Un exemple d'une sélection de nœuds relais est donné dans la figure. 3.8. Nous pouvons voir qu'un relais RNG de $a$ est un nœud qui possède un voisin RNG en dehors de la zone de communication du nœud $a$. L'information topologique amenée par l'algorithme RNG assure que tous les nœuds du réseau sont joints. En d'autres termes, un nœud $v$ est un relais de $u$ si et seulement si $v$ est un voisin de $u$ et $v$ a un voisin RNG qui n'est pas couvert par la transmission de $u$. Nous pouvons en déduire l'algorithme localisé de RRS :

1. Un nœud initiant une diffusion envoie son message sans ajouter d'information additionnelle.
2. À la réception du message de diffusion provenant d'un nœud $u$, chaque nœud teste si l'un de ses voisins RNG est en dehors de la zone de réception du précédent message. Il rediffuse dans ce cas le message.

La figure 3.8 présente un exemple de diffusion avec l'algorithme RRS. Les liens pleins représentent les arcs situés de chaque côté d'une zone de communication.

Pour chaque nœud, le minimum d'information nécessaire pour calculer l'ensemble RNG avec un système de positionnement se réduit à l'émission régulière de l'identifiant et de la position de chaque nœud. L'algorithme de RRS est le suivant :

1. Un nœud initiant une diffusion envoie son message.
2. Si un nœud $v$ reçoit un message pour la première fois de la part d'un nœud $u$ ; le nœud génère la liste de ses voisins RNG qui n'ont pas reçus le message, c'est-à-dire $list = N_{rng}/N(u)$. Si la liste est vide, le nœud oublie le message et ignore dans le futur les messages de diffusions avec les mêmes identifiants. Sinon, le nœud prépare une réémission et attend une durée $timeout$.
3. Si un nœud $v$ reçoit un message de diffusion déjà capté de la part d'un nœud $u$, il met à jour sa liste de voisins RNG avec $liste = list - N(u)$. Si la liste est vide, alors le message est oublié, les prochaines réceptions du même message de diffusion sont ignorées et l'émission en attente, déclenchée dans l'étape 2, est annulée.

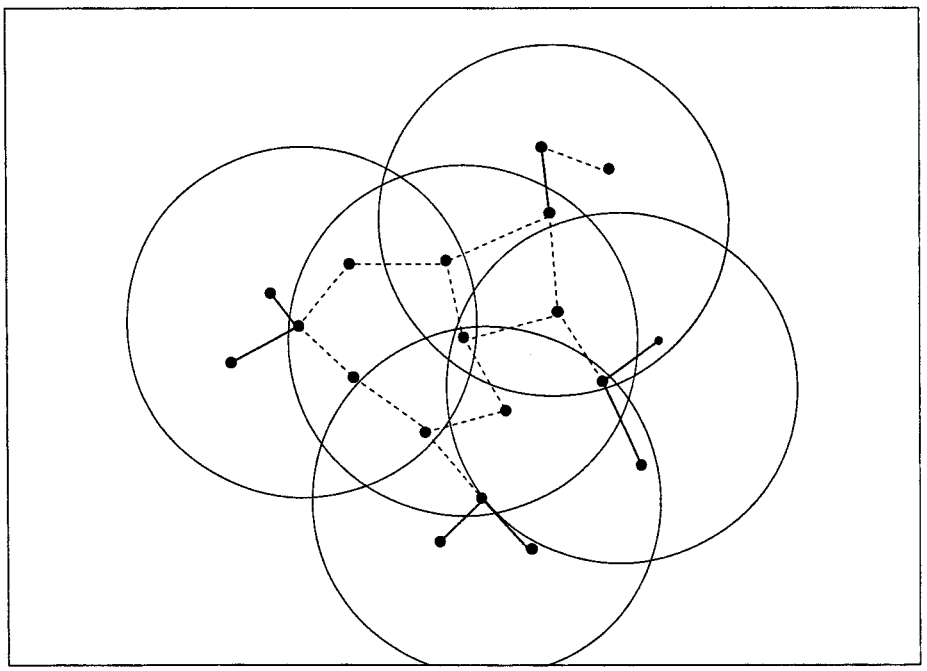


FIG. 3.8 – Un exemple de diffusion avec l'algorithme RRS.

4. Si le délai d'attente initié dans l'étape 2 est fini, alors le message de diffusion est émis, puisque la liste de voisins RNG n'est pas vide.

Pour éviter que tous les nœuds ne réémettent en même temps, le temps entre la réception du message et son éventuel réémission est calculé de manière aléatoire. Pour privilégier les nœuds en bordure lors de la réémission, la valeur aléatoire est biaisée de façon à leur offrir un temps d'attente plus court. La formule suivante est utilisée pour calculer le temps d'attente (*timeout*), avec $u$ le nœud source, $v$ le nœud qui reçoit le message et $max$ une constante qui représente le temps maximum d'attente :

$$timeout = random(\frac{max}{2}) + \frac{max}{2} \times (1 - \frac{d(u,v)}{R}). \tag{3.2}$$

La figure. 3.9 présente la diffusion dans le même réseau que celui présenté dans la figure 3.8, à la différence que le mécanisme d'élimination des voisins est utilisé. On constate qu'un nœud supplémentaire ne réémet pas, car tous ses voisins sont couverts par deux autres émissions.

## 3.5 L'approche $\nu$-voisins

Dans le protocole RRS, il est nécessaire de connaître la distance entre les nœuds de manière à évaluer l'ensemble RNG et de calculer la valeur *timeout*. En utilisant des systèmes de positionnement GPS ou une mesure de puissance à la réception (voir section 2.1.2), un nœud a la possibilité d'évaluer l'information de distance entre ses voisins et lui-même, et les distances entre ses voisins. Si le mobile n'est pas capable d'évaluer les distances réelles, le protocole proposé précédemment est difficilement utilisable.

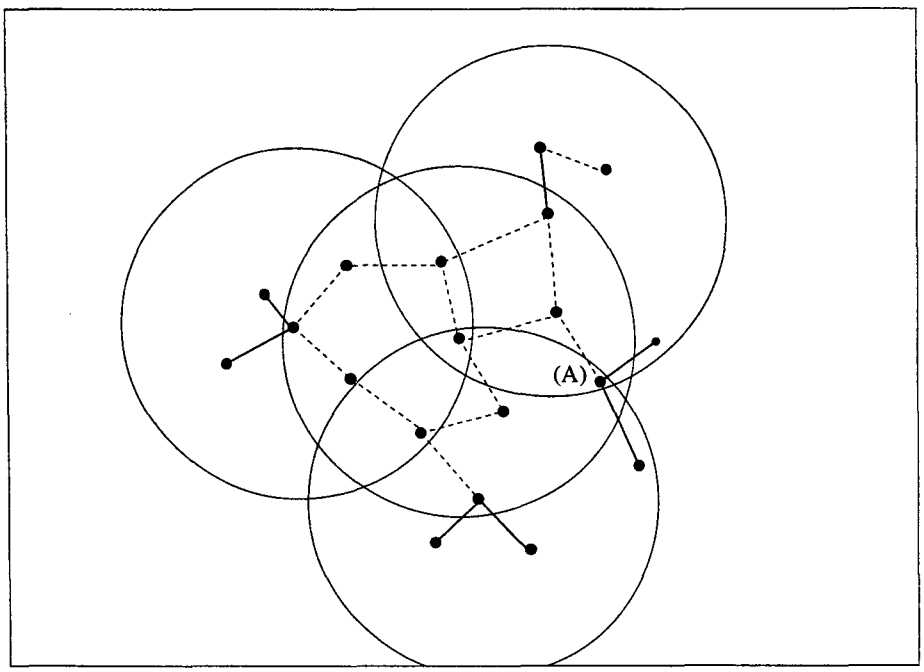



FIG. 3.9 – Un exemple de diffusion avec l'algorithme RRS utilisant le mécanisme d'élimination des voisins RNG, le nœud (A) ne réémet pas car ses voisins sont déjà couverts par d'autres nœuds.

Il est également possible d'utiliser un mécanisme logiciel. La $\mu$-distance proposée dans la section 2.4 est une solution possible pour évaluer une pseudo-distance représentée par les voisins communs et non-communs aux deux nœuds. Mais la formule présentée possède le défaut de ne pas être symétrique : la valeur obtenue par $\mu(u,v)$ et $\mu(v,u)$ peut-être différente car le nombre de voisins non-communs de $u$ et $v$ peut-être différent. Au regard du schéma 3.10, on peut voir que la $\mu$-distance définie par la formule :

$$\mu = \frac{N_b}{N_a + N_c}.$$

donne un résultat différent pour le nœud $a$ et le nœud $b$. Or, il est important d'avoir exactement le même résultat, car la consistance du graphe RNG est invalide dans le cas d'une relation asymétrique. En effet, la formule 3.1, utilisée pour déterminer l'ensemble RNG, spécifie qu'un nœud $v$ n'est pas voisin RNG du nœud $u$ s'il existe un nœud $w$ tel que $d(u,w) < d(u,v)$ et $d(v,w) < d(u,v)$. La même évaluation est effectuée de la part du nœud $v$, qui considère que $u$ n'est pas un voisin RNG s'il existe un nœud $w$ tel que $d(v,w) < d(v,u)$ et $d(u,w) < d(v,u)$. Mais il n'y a aucune garantie que $d(u,v) = d(v,u)$, donc il est possible que la relation RNG entre un nœud et son voisin ne soit pas symétrique.

Pour trouver une solution à ce problème, il est nécessaire que les deux nœuds obtiennent la même pseudo-distance. Si l'on regarde le schéma 3.10, il est nécessaire de tenir compte des nœuds uniquement joignables par chacune des deux parties dans le calcul de la pseudo-distance. Une extension de la formule de $\mu$-distance, appelée $\nu$-distance est proposée comme suit :

$$\nu(u,v) = \frac{|(N(u) \backslash N(v)) \bigcup (N(v) \backslash N(u))|}{|N(u) \bigcup N(v)|}.$$

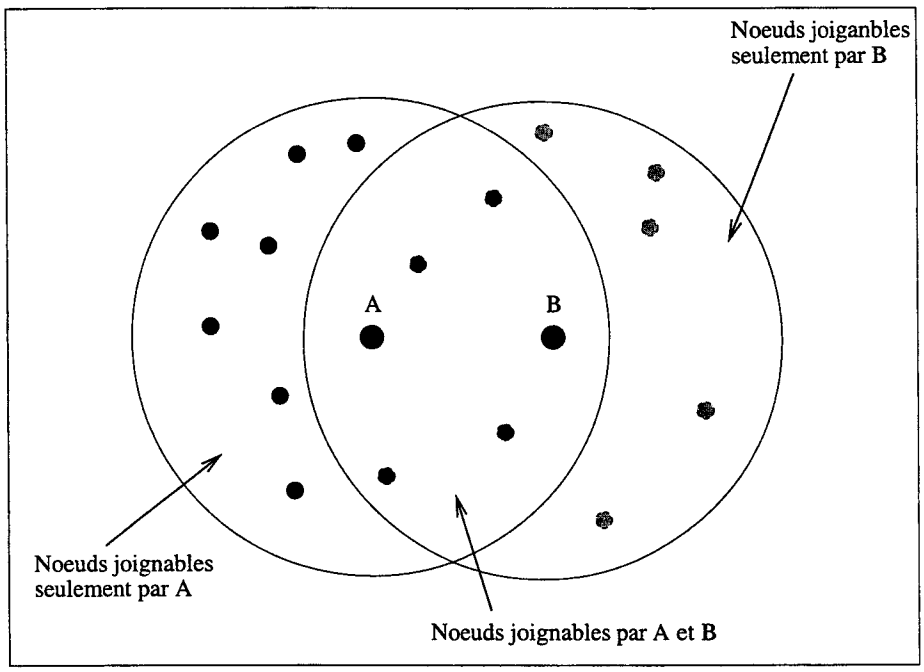



FIG. 3.10 – Évaluation de la fonction $\nu$-distance.

Comme la formule est symétrique, il est logique que la $\nu$-distance donne le même résultat des deux côtés. Chacun des deux nœuds peut calculer l'ensemble de ces paramètres, il leur suffit de connaître la liste de voisins de l'émetteur et sa liste de voisins.

Si l'on regarde un exemple de réseaux avec une évaluation du sous-graphe RNG par la méthode de $\nu$-distance (figure. 3.11), on peut voir que le graphe présente plusieurs aberrations et n'est pas optimal. La figure qui se répète le plus souvent est la présence de liaisons entre trois nœuds. Pourtant, d'après la définition d'un RNG, il est logique de s'attendre à ce qu'un des liens soit retirés. En effet, en distance euclidienne, l'un des arcs serait forcément plus petit que les deux autres[1]. Le problème provient du fait que la fonction $\nu$-distance trouve exactement le même résultat pour l'évaluation des trois arcs : le rapport entre nombre de mobiles uniquement joignable par un nœud sur le nombre de mobiles uniquement joignables par les deux nœuds est à chaque fois identique, la fonction $\nu$-distance étant discrète. Un exemple est présenté avec la figure. 3.11, et l'on peut voir que la fonction $\nu$-distance donne exactement le même résultat.

Un des effets induits par la formation de ces triangles est l'augmentation sensible du nombre de voisins RNG. Un nœud se retrouve avec un nombre plus élevé de voisins RNG à surveiller. Ce problème est présent surtout dans le cas de basses densités, où la chance d'avoir une formation de triangles est plus élevée, car le nombre réduit de voisins entraîne une plus grande probabilité que la $\nu$-distance soit égale pour chacun des trois nœuds. L'inconvénient disparaît avec l'augmentation de la densité, car la distribution est continue.

Mais le plus important reste que le sous-graphe RNG, évalué avec la fonction $\nu$-distance, reste connexe. La démonstration est simple : le graphe d'un arbre recouvrant minimal est toujours connexe, quelle que soit la fonction d'évaluation des distances. Or, un graphe d'arbre recouvrant minimal est

[1] À l'exception du triangle équilatéral, mais ce cas ne se rencontre pratiquement pas avec un dispositif de mesure de la puissance en réception ayant une bonne sensibilité quant au résultat.

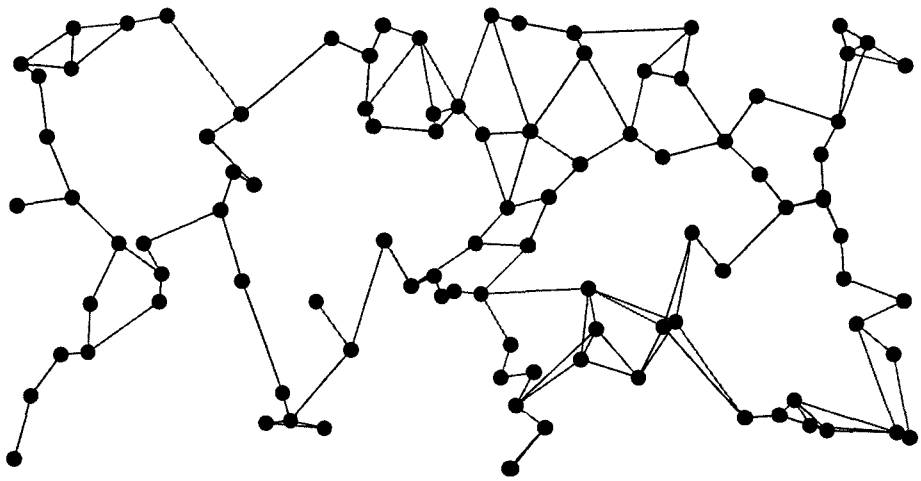


FIG. 3.11 – Le graph RNG évaluée avec $\nu$-distance.

compris dans un graphe RNG. Il est donc logique que le graphe RNG soit connexe, quelle que soit la fonction d'évaluation de la distance.

La formule 3.2 proposée pour le calcul du timeout est utilisée sur la distance séparant les deux nœuds. Il est donc nécessaire de redéfinir cette formule de manière à pouvoir utiliser la fonction $\nu$-distance avec celle-ci. Nous proposons la formule suivante pour le calcul du *timeout* :

$$timeout = random(\frac{max}{2}) + \frac{max}{2} \times (1 - \frac{\nu(u,v)}{R}). \tag{3.3}$$

## 3.6 Évaluation

Nous évaluons notre protocole avec un simulateur à événements discrets. Nous comparons notre protocole RRS au protocole de relais multipoint MPR. Nous utilisons les paramètres suivants de notre simulation. L'évaluation est faite sur la base de 1000 diffusions. L'espace de la simulation est un carré de 400 mètres de côté. Les nœuds ont une position fixe et sont répartis de manière aléatoire. Seuls les graphes connectés sont conservés, de manière à garantir dès le départ une couverture complète du réseau. La portée d'émission de chaque nœud est de 100 mètres. Le nombre de nœuds $n$ est égale à 50, 100, 150, 200, 250 et 300 (ce qui correspond à une densité de 10 à 60 nœuds par zone de communication). Les paramètres observés sont l'accessibilité (RE) et le pourcentage de messages d'émission économisés (SRB), détaillés dans la section 1.4.3.

Au niveau de la couche MAC, nous utilisons celle présente dans la norme IEEE 802.11 (voir section 1.2.1) : le protocole CSMA. Pour RRS, le paramètre $max$ utilisé dans les formules 3.2 et 3.3 est 128 unités, chacune correspondant à la durée DIFS ($32\mu s$) qui représente la durée au niveau MAC pour déterminer si le médium est libre. Ainsi, le délai *timeout* est compris entre 0 et 128 DIFS unités de délai (le délai maximum est donc de $4ms$). La taille du message de diffusion est de 512 bits (en sachant qu'un identifiant requiert au minimum 8 bits). Les messages de diffusion de cette taille sont utilisés par le protocole MPR pour informer les relais de leur rôle à remplir. En accord avec la couche MAC, la transmission d'un message sans relais est de $1.5ms$ pour un débit de 11Mbps.

Les simulations sont effectuées grâce à trois scénarios. Dans le premier, seul un message de diffusion est envoyé à la fois. Dans les deux suivants, le simulateur augmente le trafic réseau en lançant cinq

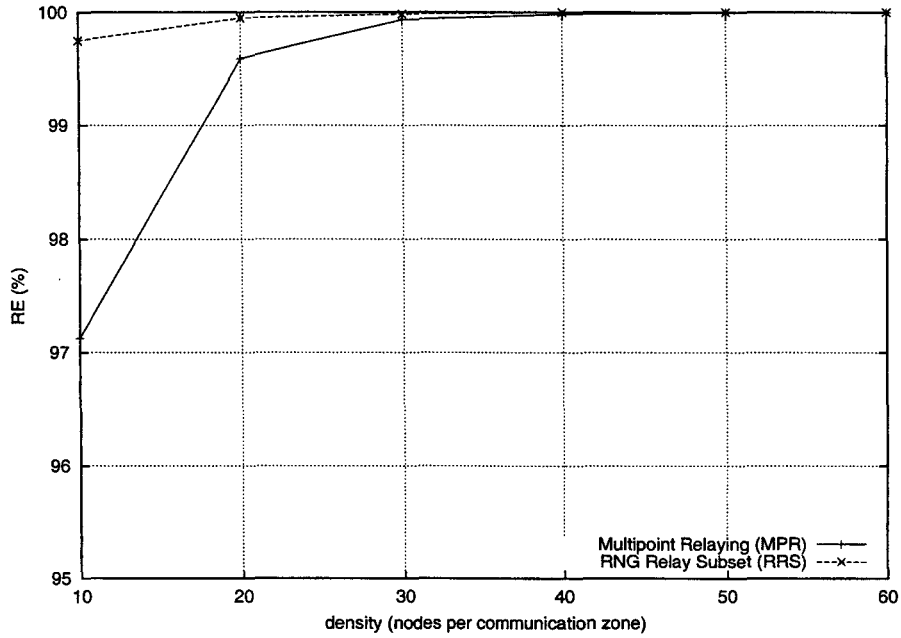



FIG. 3.12 – Accessibilité (RE) dans le cas de la diffusion d'un message.

et dix messages de diffusion à la fois. Les graphiques 3.12, 3.15 et 3.17 montre l'accessibilité pour chacun des trois scénarios. Les graphiques 3.13, 3.16 et 3.18 présentent, quant à eux, le pourcentage de messages de diffusion économisés pour les mêmes trois scénarios.

Dans le cas de la diffusion d'un message à la fois, SSR et MPR sont tous les deux efficaces avec une accessibilité supérieure à 97%. Mais le protocole MPR est plus efficace en ce qui concerne le SRB. Il propose un pourcentage stable de messages de diffusion économisés (de l'ordre de 52%). SSR propose un SRB variant entre 32% en densité faible et 37% en forte densité, ce qui est un désavantage certain par rapport à MPR.

Cette différence s'explique par le nombre moyen de relais. La solution proposée par MPR minimise le nombre de relais avec l'aide d'une heuristique dont le but est de sélectionner un nombre minimal de relais. Le nombre de relais est souvent proche de l'optimum possible, ce qui donne un excellent SRB. La solution SSR a pour but premier de permettre de manière localisée la décision de réémission, sans nécessité d'ajouter des informations dans le message de diffusion. Comme il n'a pas été prévu pour optimiser le nombre de relais, le SRB est moins bon dans ce cas. On peut voir sur le graphique. 3.14 le fait que MPR en possède un nombre moins important que SSR.

Lorsque le trafic réseau augmente (c'est-à-dire quand le nombre de diffusions simultanées augmente sensiblement), la solution SSR prend le pas sur MPR. L'émission en même temps de cinq ou de dix diffusions diminue de manière considérable l'efficacité des deux protocoles. Dans le premier cas, la diffusion de 5 messages fait tomber l'accessibilité de SSR à moins de 50%, voire à moins de 40% pour de basses densités. Dans le cas du SSR, l'accessibilité reste très correcte, elle est supérieure à 90% lorsque la densité dépasse 20 nœuds par zone de communication. Le SRB reste à l'avantage de MPR, mais puisque l'accessibilité est loin d'être parfaite, le SRB n'est calculé que sur les nœuds qui ont reçu le message. De plus, une accessibilité faible n'est pas intéressante dans le cas d'une diffusion.

Un trafic comprenant dix diffusions simultanées donne des performances encore plus faible en

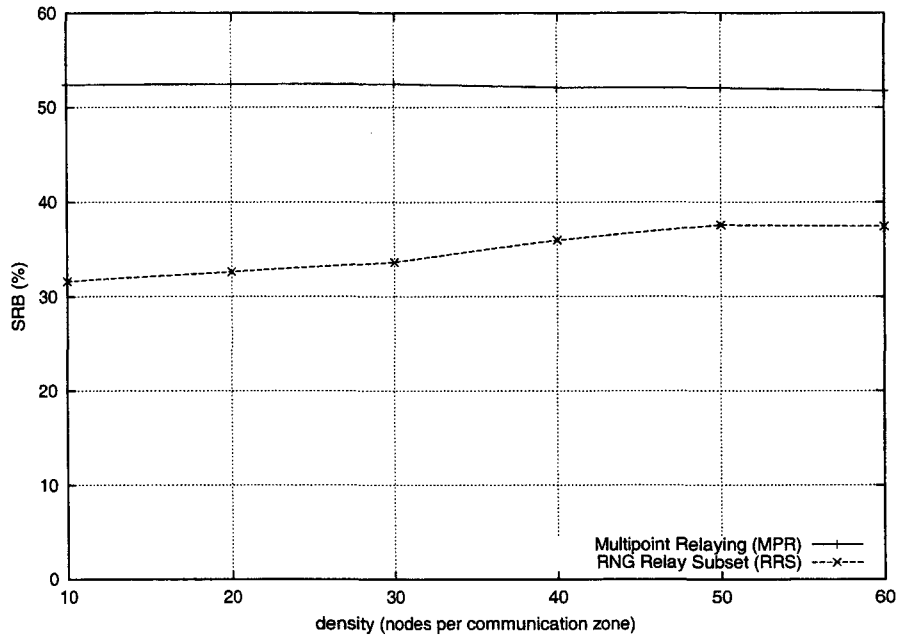



FIG. 3.13 – Pourcentage de messages de diffusion économisés (SRB) dans le cas de la diffusion d'un message.

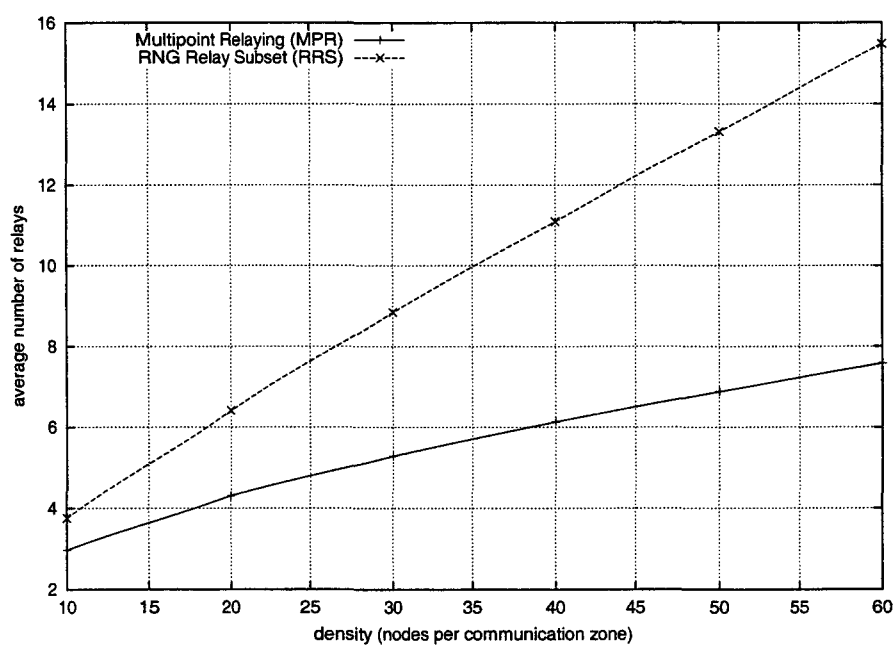



FIG. 3.14 – Nombre moyen de relais pour SSR et MPR en fonction de la densité.

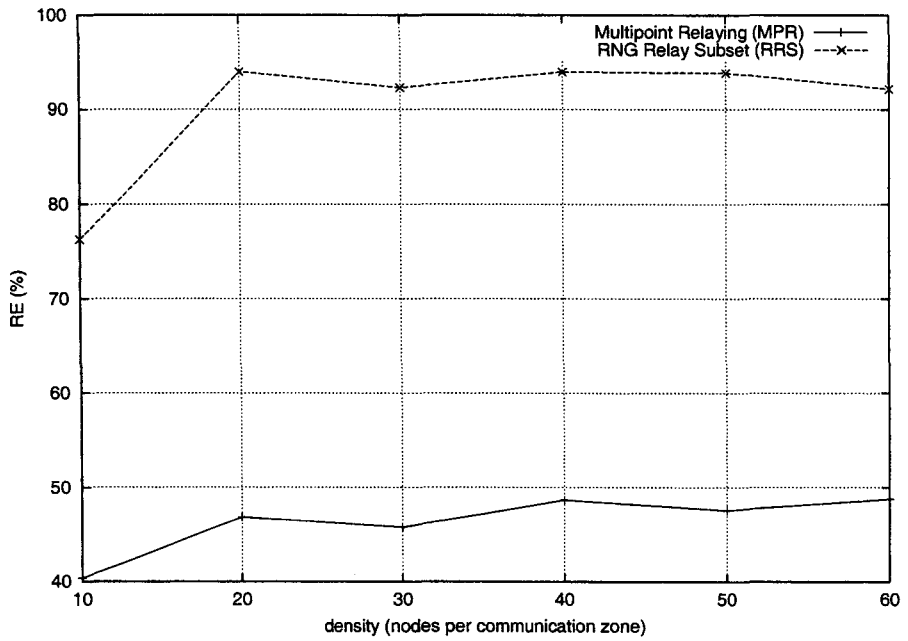



FIG. 3.15 – Accessibilité (RE) dans le cas de la diffusion simultanée de cinq messages.

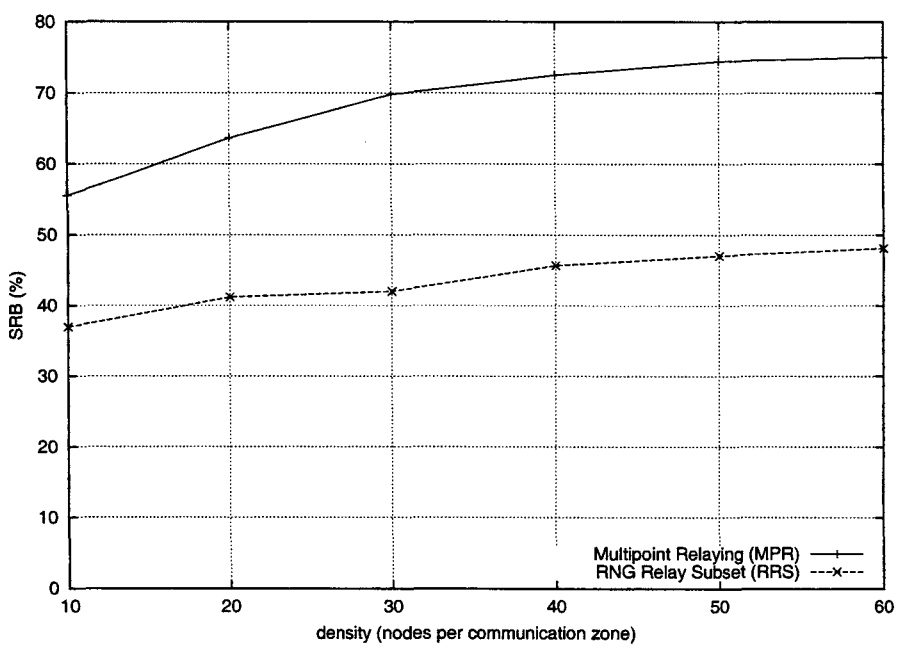



FIG. 3.16 – Pourcentage de messages de diffusion économisés (SRB) dans le cas de la diffusion simultanée de cinq messages.

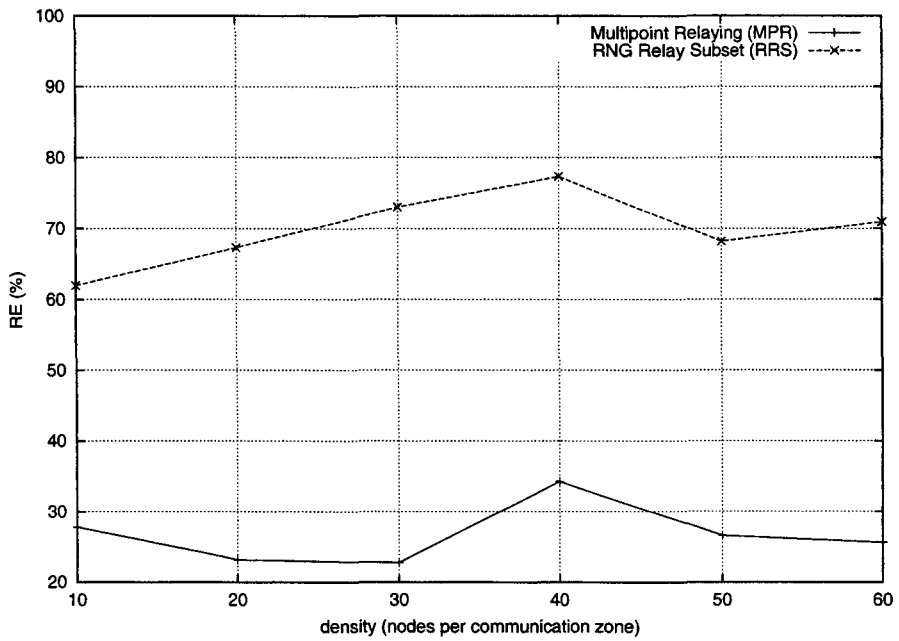



FIG. 3.17 – Accessibilité (RE) dans le cas de la diffusion simultanée de dix messages.

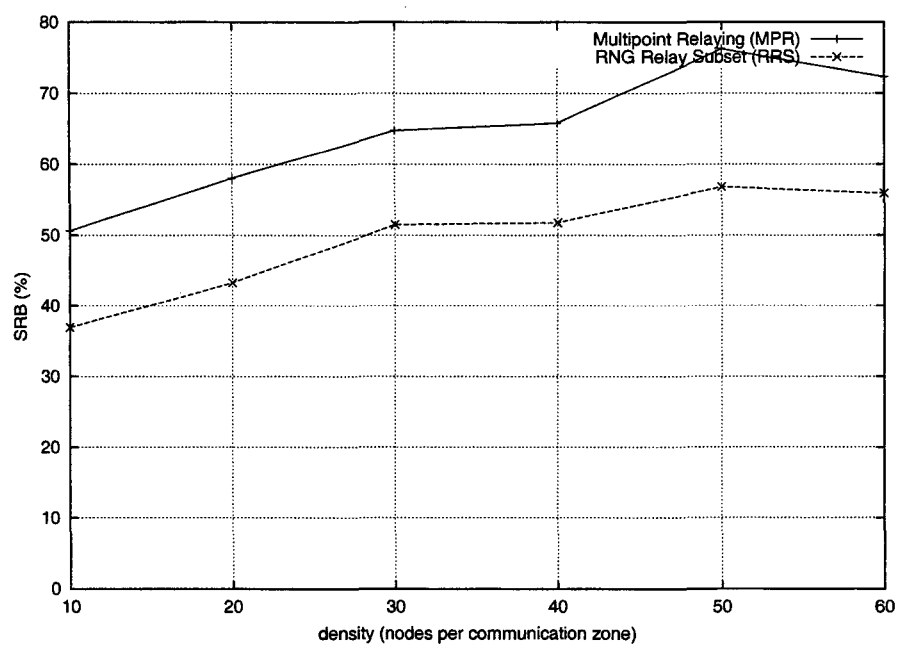



FIG. 3.18 – Pourcentage de messages de diffusion économisés (SRB) dans le cas de la diffusion simultanée de dix messages.

terme d'accessibilité. Le protocole MPR arrive à joindre moins de 30% du réseau[2] tandis que le protocole établit une moyenne de 65% de nœuds joints. Le SRB est encore à l'avantage de MPR, qui réussit à économiser 75% des messages de diffusion dans le cas de hautes densités. SSR se rapproche de MPR en terme de SRB, avec une différence de l'ordre de 13%, mais il reste encore inférieur à ce dernier. Encore une fois, les mêmes critères sont déterminants : une accessibilité moins bonne est défavorable pour une bonne une diffusion, ce qui donne un avantage pour SSR lors de fortes charges.

Pour comprendre ce phénomène, on peut observer de nouveau le graphique 3.14 : le nombre de relais dans le cas de MPR est moins important que SSR. Même si cette propriété rend le protocole SSR moins économique en terme de SRB, il offre l'avantage à ce dernier d'offrir une plus grande stabilité en cas de forte charge. En effet, la présence d'un nombre plus important de relais permet d'être robuste face aux collisions qui sont engendrées. La perte d'un message pour MPR est cruciale, car l'optimisation proposée repose sur l'hypothèse que tous les nœuds relais vont réémettre. Cette contrainte est importante dans le cas d'un trafic réseau important, ce qui entraîne des pertes de connexité conséquentes.

Il est intéressant de voir l'influence de la taille du paquet lors de l'augmentation de la charge réseau. Le protocole MPR nécessite l'ajout dans le message de diffusion de la liste des voisins relais qui vont réémettre le message. Cette surcharge entraîne théoriquement une probabilité de collisions plus importante. Á l'opposé, le protocole SSR détermine de manière localisée la décision de réémission, sans tenir compte du voisin qui a émis le message. Nous simulons l'envoi de messages vides et de messages possédant une surcharge de 512 bits dans la partie données, avec les deux protocoles. Les résultats sont présentés avec le graphique 3.19 en terme d'accessibilité et avec le graphique 3.20 en terme de pourcentage de messages de diffusion économisés.

La taille du paquet, si celui-ci est de taille raisonnable, n'intervient pratiquement pas dans les baisses de performances. Que ce soit en terme d'accessibilité (RE) ou en pourcentage de messages de diffusion économisés (SRB), les résultats entre les messages vides et les messages contenant un supplément de 512 bits sont très proches (une différence minime de l'ordre de 3%). Il est donc clair que, dans le cas d'une bonne fiabilité de la transmission, le paramètre le plus important est bien le nombre de relais et non la taille des messages de diffusion.

Nous avons proposé dans la section 3.5 une alternative à la mesure de puissance. Une fonction $\nu$-distance permet d'évaluer une pseudo-distance entre leur nœuds à partir de leur voisinage. Nous simulons RRS et RRS-$\nu$ dans le cas de la diffusion d'un seul message de diffusion en même temps, avec une taille de paquet vide. Ceci dans le but d'évaluer les différences de performances entre les deux protocoles. Les graphiques 3.21 et 3.22 présentent l'accessibilité et le pourcentage de messages de diffusion économisés pour les deux protocoles en fonction de la densité moyenne du réseau.

L'évaluation de la pseudo-distance se révèle très efficace. Les différences entre SSR et SSR-$\nu$ sont minimes, malgré un nombre plus important de voisins RNG dans le second cas. Ces résultats proches sont explicables par l'utilisation du mécanisme de l'élimination des voisins, qui permet de minimiser l'impact d'un nombre trop important de voisins RNG.

## 3.7 Conclusion

Nous avons proposé un algorithme indépendant de la source garantissant une couverture complète du réseau. L'utilisation combinée des voisins RNG et de la comparaison des voisins permet d'obtenir de bons résultats. Comme les données sur le voisinage concernent entièrement les nœuds à un saut,

[2]avec une pointe à 35% dans le cas d'une densité de 40 nœuds par zone de communication, mais ce n'est qu'un cas particulier dû à une configuration favorable du réseau.

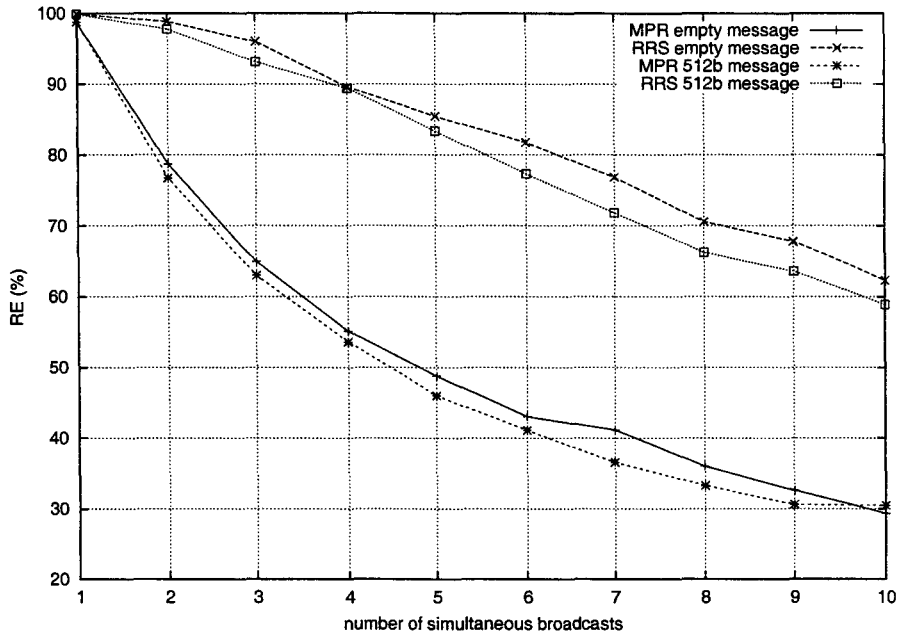



FIG. 3.19 – Accessibilité de MPR et SSR avec un nombre simultané de diffusion variable et une taille de paquet égale à 0 ou 512bits.

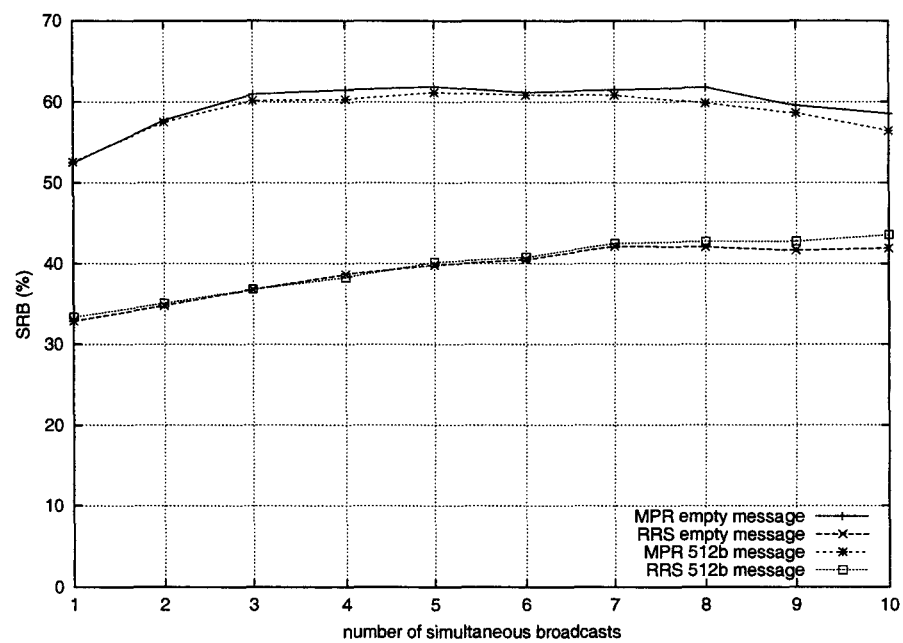



FIG. 3.20 – Pourcentage de messages de diffusion économisés de MPR et SSR avec un nombre simultané de diffusion variable et une taille de paquet égale à 0 ou 512bits.

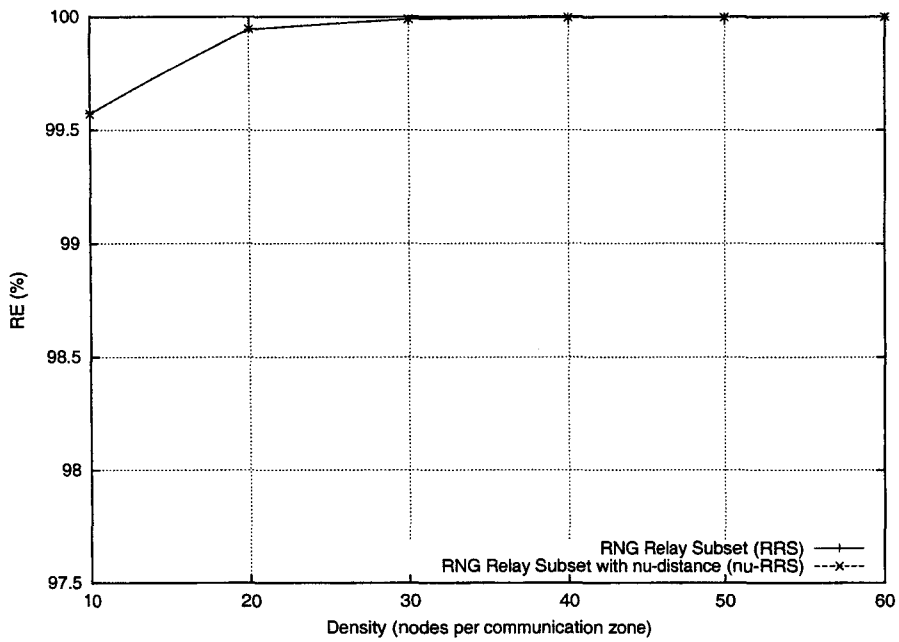



FIG. 3.21 – Accessibilité de SSR et SSR-$\nu$ en fonction de la densité.

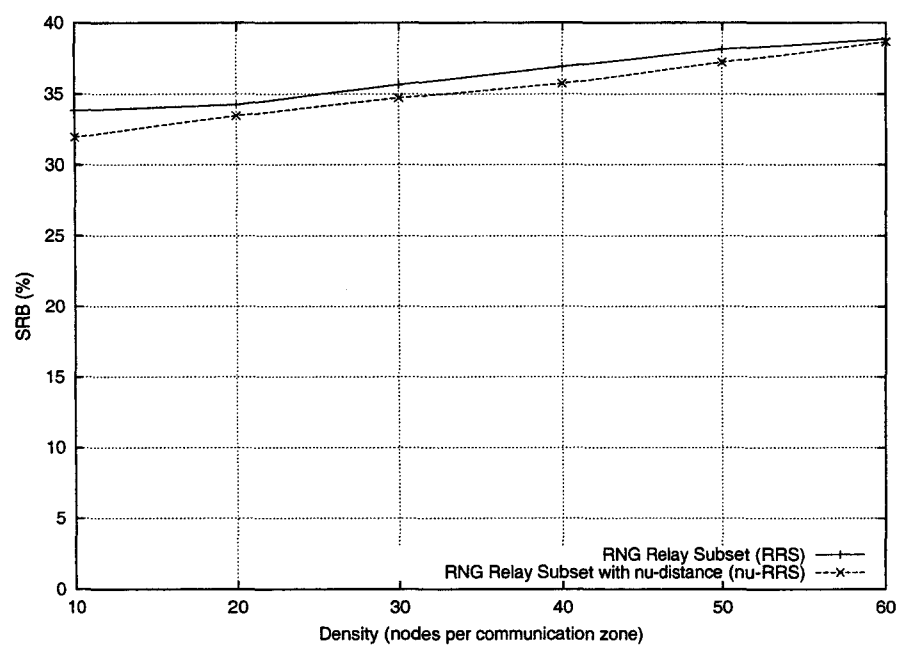



FIG. 3.22 – Pourcentage de message de diffusion économisés de SSR et SSR-$\nu$ en fonction de la densité.

et que les nœuds très proches sont sélectionnés pour la prise de décision, l'algorithme peut gérer une mobilité importante. Cette propriété reste vraie avec l'aide de l'utilisation d'un mécanisme d'élimination des voisins limité aux nœuds RNG voisins. L'algorithme possède une excellente résistance lors d'une montée en charge du réseau importante, grâce à un nombre de relais élevé. L'algorithme peut fonctionner avec l'aide de dispositifs d'acquisition de position, mais peut aussi s'en passer en utilisant l'approche $\nu$-distance, et obtenir des résultats très proches. Cet algorithme offre une nouvelle idée sur la décision prise indépendamment du voisin qui a réémis le message. Signalons pour finir que l'algorithme de réduction de graphe RNG est efficace, mais il existe un autre donnant un nombre moyen de voisins encore plus bas (LMST, décrit dans le chapitre 5). Son utilisation peut offrir de meilleurs résultats pour un même nombre de messages échangés.

# Troisième partie

# Réduction du coût énergétique de la diffusion lors de l'opération de diffusion

# Chapitre 4

# Diffusion avec réduction de portée

Dans les deux premiers chapitres, nous avons proposé et discuté deux protocoles de diffusion pour les réseaux ad hoc. Ils permettent de réduire le nombre de messages nécessaires pour couvrir l'ensemble du réseau, et ainsi minimiser les chances de collision. Cette diminution du nombre d'émissions a un autre intérêt : elle offre une réduction de la quantité d'énergie nécessaire pour l'opération de diffusion. Dans les deux cas, la proportion d'énergie utilisée est fonction du pourcentage de mobiles qui réémettent (SRB). Plus exactement, seuls les mobiles qui réémettent le message utiliseront de l'énergie. Mais attention, de ce point de vue, le phénomène de réduction est global : on s'intéresse à la somme totale d'énergie dépensée sur l'ensemble du réseau. Ainsi, certains nœuds peuvent être utilisés plus que d'autres, et les bonnes performances énergétiques peuvent ne profiter qu'à une partie seulement du réseau.

Selon le modèle d'énergie utilisé, l'énergie dépensée pour l'envoi d'un message par un nœud est de l'ordre de $\theta(d^\alpha)$, avec $d$ la distance d'émission et $\alpha$ une constante ($\alpha \geq 2$). Même si les deux solutions offrent une bonne réduction, il est plus intéressant de réduire la portée de chaque mobile, car la consommation diminue de façon très importante. Mais cette réduction de portée peut entraîner une perte de connectivité avec une partie du voisinage et, dans certains cas, provoquer des scissions dans le réseau. Il est donc nécessaire d'avoir une méthode de diffusion permettant de réduire la portée de chaque mobile sans rompre la couverture totale du réseau.

Dans ce chapitre nous proposons et discutons un algorithme, nommé RBOP [16] (*RNG Broadcast Oriented Protocol*), réduisant la portée d'émission des mobiles dans le but d'économiser l'énergie de chacune des unités. Ce protocole utilise RNG pour calculer un sous-ensemble du voisinage qui contiendra les mobiles à joindre et garantir la connexité du réseau.

## 4.1 Préliminaires

Nous reprenons les notations définies dans la section 1.4.2. Mais ici les nœuds peuvent changer la puissance de leur signal d'émission, ce qui change la distance de communication. La portée d'un nœud $u \in V$ représente la distance maximale entre $u$ et un nœud capable de recevoir la transmission. Elle est définie par $r(u)$ (avec $r(u) \leq R$). Le graphe induit par la fonction $r$ d'assignement des portées est défini par $G_r = (V, E_r)$, avec l'ensemble des arcs $E_r$ donné par :

$$E_r = \{(u, v) \in V^2 \mid d(u, v) \leq r(u)\}.$$

Une fonction d'assignement pour les nœuds dans $V$ est une fonction $r$ de $V$ dans un intervalle

réel $[0, R]$ ($r : V \rightarrow [0, R]$). Dans certains réseaux sans fil, la portée de transmission de chaque nœud a un nombre fini de valeurs possibles, signifiant que $r$ est une fonction dans un sous-ensemble fini de $[0, R]$.

Mais le graphe $G_r$, avec des portées différentes pour chaque nœud, n'est pas toujours bidirectionnel (*i.e.* un noeud $a$ peut joindre $b$ mais l'inverse n'est pas forcément vrai). Il faut donc, pour garantir une couverture complète du réseau, que le graphe $G_r$ soit connexe. On dit qu'un graphe (dirigé) est fortement connexe si, quels que soient les nœuds $u, v \in V$, un chemin existe entre $u$ et $v$. Mais comme nous travaillons sur le problème de diffusion, il suffit qu'une diffusion pour un nœud donné (appelé « source ») permette de joindre l'ensemble des nœuds du réseau. Dans ce cas, une connexité forte n'est pas nécessaire, nous avons seulement besoin d'une connectivité du nœud source vers tous les autres nœuds du réseau.

## 4.2 Travaux existants

L'efficacité d'un algorithme de diffusion (mais aussi de routage), conçu pour économiser la vie des batteries, est conditionnée par les paramètres physiques de consommation énergétique. Dans un premier temps, nous présentons les différents modèles énergétiques pour préciser les conditions et les contraintes de leur utilisation lors de l'émission et de la réception de messages radios. Dans un second temps, nous détaillons les différentes approches utilisées pour résoudre le problème de l'énergie dans le cas de la diffusion.

### 4.2.1 Modèles énergétiques

Un modèle simpliste et largement utilisé pour représenter la consommation de la couche physique est proposé dans [3, 21, 30, 59, 60, 42, 93, 96, 98]. L'énergie utilisée pour une émission est proportionnelle à $\theta(d^\alpha)$, avec $d$ la portée de la transmission et $\alpha$ le facteur représentant la perte en puissance (typiquement, $2 \leq \alpha$). À partir de ce modèle, la meilleure solution consiste à baisser au maximum la portée d'émission de chaque nœud, dans le but de minimiser l'énergie utilisée. Une telle politique présente l'avantage de réduire le risque d'interférence par d'autres nœuds et de minimiser le problème du terminal exposé (voir section 1.2).

Mais ce modèle possède plusieurs défauts. Comme il est montré dans la figure 4.1, avec un paramètre $\alpha$ égal à deux, il est clair que la transmission illustrée dans la sous-figure (d) coûte la même quantité d'énergie que celle des sous-figures (a), (b) et (c) (en utilisant le théorème de Pythagore). Par récurrence , toutes les illustrations ont la même consommation énergétique que le modèle proposé. De plus, ce modèle ne tient pas compte de la taille du paquet ou du coût nécessaire pour le traitement interne dans le mobile (c'est-à-dire le minimum d'énergie requise pour l'envoi d'un message, le traitement du signal et les messages de contrôle de la couche MAC...).

Un autre modèle a été proposé par Feeney *et al.* [32]. Il se concentre sur la taille du paquet et le coût de traitement interne au mobile. Ainsi, l'énergie utilisée est proportionnelle à $m * taille + b$, avec $m$ et $b$ des constantes caractérisant l'interface radio, et $taille$ représentant la taille du paquet. Ce modèle permet logiquement d'affecter un coût pour chaque envoi (à l'aide de la constante $b$) pour simuler l'utilisation de l'interface radio. De plus, il permet de tenir compte de la taille de chaque paquet (avec la variable $taille$ et la constante $m$) pour évaluer l'énergie demandée pour des paquets de taille variable. Mais la constante $m$ étant évaluée pour une seule puissance d'émission, il n'est utilisable que pour une portée unique.

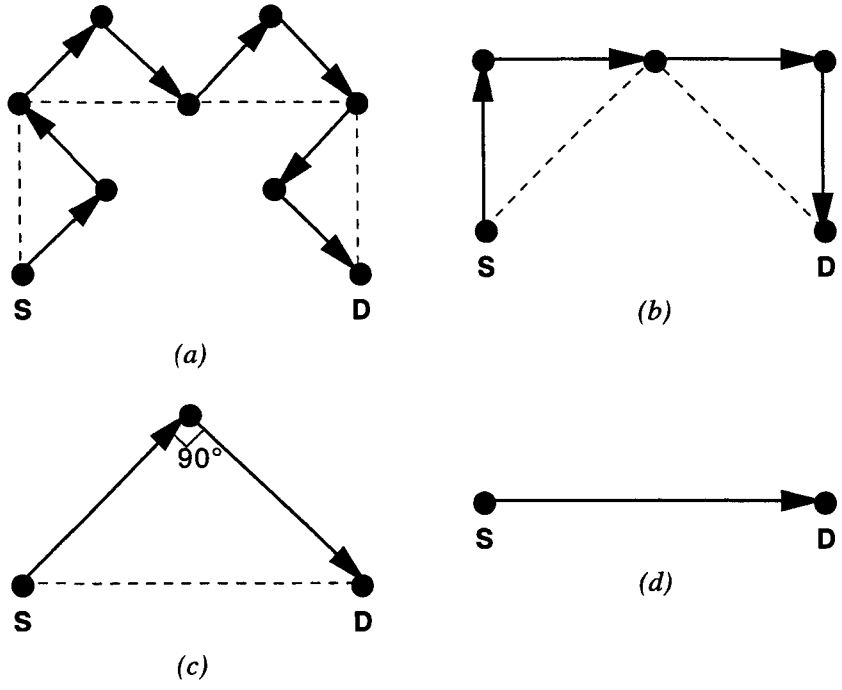



FIG. 4.1 – Exemple de quatre cas où l'énergie dépensée est identique avec $\alpha = 2$

Les deux approches sont valables, mais possèdent chacune une ou plusieurs lacunes. Dans le modèle que nous voulons utiliser, il est nécessaire de conserver le fait que la puissance requise augmente en fonction de la distance, et la présence d'un coût minimal associé chaque envoi. Un modèle énergétique combinant les deux idées précédentes peut se résumer ainsi :

$$E(u) = \begin{cases} r(u)^{\alpha} + c & \text{si } r(u) \neq 0, \\ 0 & \text{sinon.} \end{cases} \tag{4.1}$$

Ce modèle a l'avantage d'être plus flexible. Nous pouvons toujours simuler les cas du premier modèle présenté ci-dessus (par exemple avec les constantes $\alpha = 2$ et $c = 0$). Une autre utilisation est proposée par Rodoplu et Meng [79], avec $\alpha = 4$ et $c = 10^8$. Dans ce cas, une émission à courte portée effectuée par l'ensemble des mobiles n'est pas nécessairement la meilleure. Même si réduire la portée d'émission est intéressant, il est aussi avantageux de ne pas obliger tous les mobiles à réémettre le message. Ainsi, il faut trouver le bon équilibre entre la réduction de portée (qui peut forcer un maximum de nœuds à participer à cette opération) et la minimisation de l'ensemble des mobiles qui réémettent le message (ce qui a pour effet de bord, une tendance à l'augmentation de la portée des nœuds participants). Notons aussi que ce modèle ne tient pas compte de la taille du paquet. En effet, les messages de diffusion sont le plus souvent de taille unique.

Signalons un autre modèle, proposé par Chen *et al.* [19] et inspiré de Feeney [32] dans le cas d'une portée unique. Comparé aux modèles précédents, il prend aussi en compte l'énergie consommée par le récepteur et par les nœuds voisins de l'émetteur. En effet, chaque mobile consomme de l'énergie pour recevoir le message et le traiter (c'est-à-dire déterminer si le message lui est destiné). Ainsi, un nœud concerné par la communication consomme de l'énergie : l'énergie consommée par l'émetteur du message pour l'émission ($E_{send}$), l'énergie consommée par le récepteur pour la réception et le traitement du message ($E_{rec}$), et l'énergie consommée par les mobiles voisins de l'émetteur et du

récepteur pour recevoir le message et reconnaître que celui-ci ne les concerne pas ($E_{discard}$). En plus de ces considérations, les auteurs proposent dans leur modèle de tenir compte de la taille du message et de la dissipation de l'énergie selon la portée d'émission (avec une formule de type $r^{\alpha}$). Même si ce modèle est le plus réaliste, il n'est pas nécessaire dans nos simulations. En effet, ce modèle est plus adéquat dans le cas de transmission point-à-point. Dans le cas de la diffusion, chaque mobile va recevoir le message et le traiter. Ainsi, on peut présumer que $E_{rec}$ et $E_{discard}$ sont identiques, et que la taille de chaque paquet de diffusion est unique. Cette simplification donne alors un modèle très proche du précédent.

### 4.2.2 Réduction d'énergie

L'utilisation d'une interface radio engendre un coût énorme pour la consommation du mobile. Fenney propose plusieurs analyses [32, 34] montrant le surcoût énergétique des interfaces radios et des principaux algorithmes de routage. De même, Chen *et al.* [19] démontrent l'accroissement important de l'énergie requise en fonction de la puissance et de la taille du message. Il est donc logique que de récents travaux s'intéressent à ce problème.

Il existe plusieurs solutions situées à différents niveaux de la pile réseau. Pour la couche réseau, des protocoles de routage conçus spécifiquement peuvent minimiser le coût énergétique des chemins. Dans le cas de la couche de liaison de données, des stratégies de réémission et un mode sommeil peuvent aussi économiser de l'énergie. Enfin, au niveau de la couche physique, plusieurs canaux peuvent partager la bande passante, ou encore le mobile peut réduire la puissance de transmission.

Certains protocoles de routage sont adaptés pour minimiser le coût énergétique. Pour la diffusion dans un réseau ad hoc, Wu *et al.* [101] proposent d'utiliser les algorithmes à ensembles dominants, déjà présentés dans la section 2.2. Les comparaisons d'identifiants sont remplacées par des comparaisons du niveau d'énergie, dans le but d'alterner la consommation entre les nœuds. Ainsi, l'ensemble dominant est construit à partir des nœuds possédant le plus d'énergie, et le renouvellement régulier de l'ensemble permet le partage équitable de la consommation énergétique entre tous les nœuds du réseau.

Une stratégie fondée sur la couche de liaison peut proposer des politiques d'alternance et/ou d'extinction des interfaces radios dans le but de minimiser le nombre de nœuds participants aux communications. Ainsi, Feeney propose dans [33] de basculer les nœuds participants entre le mode sommeil et le mode actif. Par exemple, avec les cartes 802.11b, les interfaces possèdent au moins 3 modes de fonctionnement[1] : *sleeping*, *active* et *listening* . Certaines mesures indiquent que la consommation varie en fonction de l'émission ou de la réception (respectivement 1300mW et 1000mW), et de l'état inoccupé ou en sommeil de l'interface radio (800mW et 130mW). Comme le mode sommeil empêche toute réception ou émission, Feeney propose un mécanisme d'alternance de l'état des interfaces, calculé de manière localisée mais garantissant une couverture complète du réseau. Ce procédé se révèle efficace et se double de la possibilité de gérer la qualité de service en même temps. Signalons que Tian et Georganas [90] présentent un algorithme semblable, fondé sur la possibilité de détecter les nœuds redondants.

Au niveau de la couche physique, la première solution est de partager la bande passante. Cette idée est développée dans PAMAS [82]. Chaque nœud écoute un canal de contrôle avec un mécanisme ne nécessitant que très peu d'énergie. Ce canal est très fin et indique juste la présence ou non d'une communication sur l'autre canal de communication (plus important car transportant les données). S'il détecte une communication dans son voisinage, il réveille son interface radio standard pour qu'elle

[1] Certaines interfaces 802.11b en possèdent plus.

soit en mesure de prendre en compte cette communication. Ce dispositif simple présente le défaut d'avoir un coût important en terme d'ajout de matériel.

Une autre solution, et c'est celle qui nous intéresse, est de varier la portée d'émission dans le but de réduire la consommation d'énergie. En fonction du modèle énergétique utilisé, la réduction est bien plus importante que les solutions proposées précédemment, handicapées par la nécessité d'utiliser une émission à pleine portée. L'ensemble des protocoles de diffusion ajustant la portée des nœuds pour réduire la consommation d'énergie se décomposent en deux grandes familles.

La première famille regroupe les protocoles pour le contrôle de la topologie (ou *Topology Control Oriented Protocols*). Ils ajustent la portée indépendamment de l'utilisation de la diffusion. Plus exactement, tous les nœuds peuvent être source de la diffusion avec la garantie que tous les nœuds du réseau connexe sont joints et que la consommation d'énergie est minimale quelle que soit la source de la diffusion. Pour cela, le critère d'optimisation minimise la somme totale de l'énergie consommée (par rapport à un modèle énergétique donné) par l'ensemble des nœuds lors de la diffusion du message. Ce problème est connu sous le nom de problème d'assignement minimal (ou *Min Assignment Problem*), et a été démontré comme étant NP-dur en deux dimensions par Clementi *et al.* [24].

Kirousis *et al.* proposent dans [51] de trouver de manière centralisée un arbre recouvrant d'énergie minimale (*MST* ou *Minimum-power Spanning Tree*) à partir du graphe du réseau sans fil. La construction de cet arbre MST est possible si nous pouvons déterminer la distance entre les nœuds. Avec cette information, le poids des arcs est calculé avec le modèle énergétique utilisé[2]. L'algorithme est simple : tant que tous les nœuds ne sont pas joints, choisir l'arc le moins coûteux non encore sélectionné et l'ajouter dans l'arbre MST. De plus, pour éviter de choisir deux nœuds faisant partie du même composant connexe, l'algorithme intègre un mécanisme de coloriage des nœuds. Ce protocole possède plusieurs propriétés intéressantes. D'une part, il est connu que le graphe $MST(G) = (V, E_{mst})$ est symétrique (non-dirigé), ce qui permet de ne pas avoir de liens unidirectionels. D'autre part, chaque nœud de $V$ peut-être la racine d'un arbre recouvrant en utilisant $MST(G)$, donc n'importe quel nœud peut être source de la diffusion. Finalement, il est connu que $MST(G)$ est fortement connexe si le graphe $G$ est fortement connexe.

Une fois l'arbre construit, il suffit d'ajuster la portée de chaque nœud pour que chacun couvre uniquement ses voisins dans l'arbre. Pour cela, les auteurs proposent une fonction d'assignement des portées de chaque nœud à partir de MST :

$$\forall u \in V : r(u) = max_{v \in V | (u,v) \in E_{mst}} d(u, v).$$

Pour la suite de ce chapitre, ce protocole sera appelé MTCP (*MST Topology Control Protocol*). Soit $MST^*(G) = G_r$ le graphe avec les portées modifiées en utilisant les arcs du graphe MST. Il est trivial de dire que $MST(G)$ est inclus dans $MST^*(G)$ ($E_r \subseteq E_mst$) et donc que $MST^*(G)$ est fortement connexe. Si l'on reprend le graphe 3.4, on obtient le sous-graphe MST présenté dans la figure 4.2.

La deuxième famille regroupe les protocoles orientés pour la diffusion (ou *Broadcast Oriented Protocols*). Elle a le même objectif (minimiser la somme totale de l'énergie utilisée pour la diffusion d'un message dans le réseau) mais par rapport à un nœud précis comme source de la diffusion. Les contraintes ne sont pas les mêmes que la première famille, car dans ce second cas le sous-graphe induit par l'arbre d'énergie minimale recouvrant n'a pas besoin d'être fortement connexe.

Wieselthier *et al.* ont proposé dans [98] deux heuristiques gloutonnes pour remplir cette tâche de manière centralisée. L'heuristique BLU (*Broadcast Least-Unicast-cost*) applique l'algorithme de

[2] le MST ne dépend pas d'un choix particulier de métrique grâce à sa monotonie.

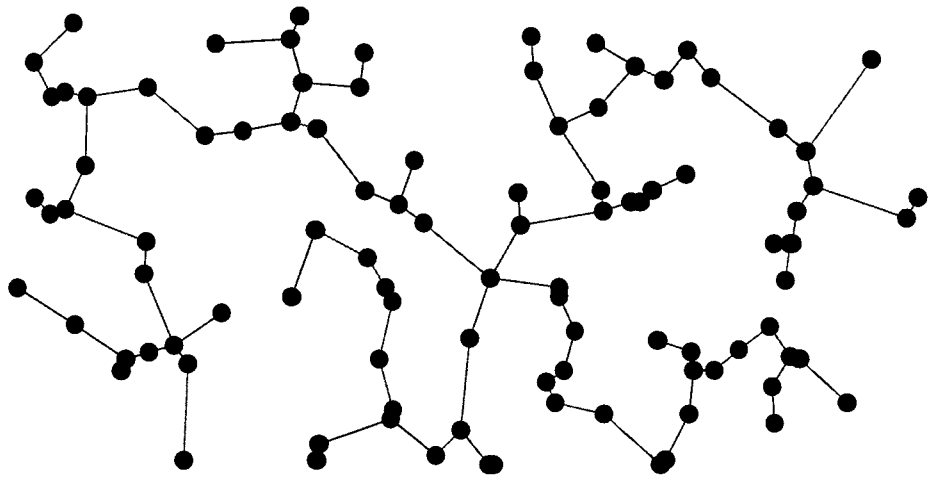


FIG. 4.2 – Exemple de graphe avec l'algorithme MST

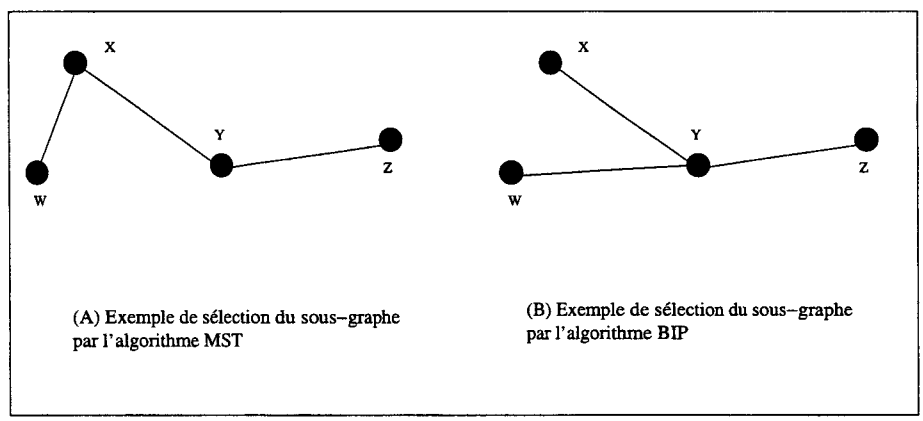



FIG. 4.3 – Exemple de construction des sous-graphes MTCP et BIP

Dïjkstra pour construire un arbre recouvrant d'énergie minimale. Il fusionne les liens les moins coûteux à partir du nœud source vers les autres. Le second heuristique globalisée s'appelle BIP (*Broadcast Incremental Power*). C'est une version modifiée de l'algorithme de Prim, où le critère de sélection est le coût supplémentaire pour couvrir de nouveaux nœuds. Durant la construction de l'arbre BIP, le nœud suivant est sélectionné en fonction de l'énergie additionnelle (soit en augmentant la puissance d'un nœud déjà inclus dans l'arbre, soit en incluant un nœud nouvellement choisi). Ce protocole a l'avantage d'être le plus efficace parmi tous les algorithmes de diffusion avec réduction de portée. Quelques travaux proposent des optimisations du modèle BIP [21, 42, 96] mais l'algorithme est toujours centralisé.

Pour bien comprendre la différence entre l'algorithme MTCP et BIP, nous pouvons observer le schéma 4.3. Dans l'exemple (A), l'arc $(X, W)$ est choisi car il est le moins coûteux dans tout le graphe. Dans l'exemple (B), ce sont les arcs $(X, Y)$ et $(Y, W)$ qui sont choisis car il est moins coûteux, dans le cas de BIP, d'envoyer un message en couvrant $X$ et $W$ que de faire relayer le message pour $W$ par $X$. Cela permet à BIP d'avoir de meilleures performances, car il tire directement partie de la connaissance de la puissance demandée en fonction de la distance.

Une optimisation possible de BIP, baptisée opération de balayage (*Sweep Operation*) est de réduire

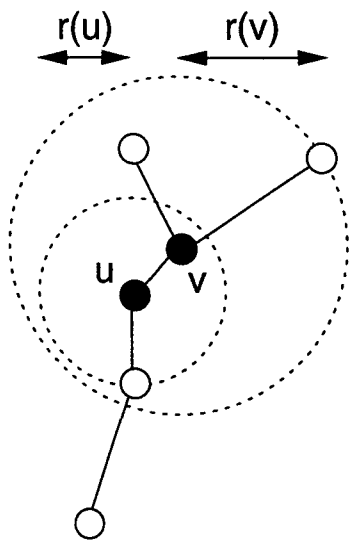



FIG. 4.4 – Réduction de portée pour éliminer une couverture commune

la portée lorsque les voisins MST sont déjà couverts par d'autres nœuds (*i.e.* $\exists v \in N(u)$ tel que $d(u,v) + r(u) \leq r(v)$). Mais ce procédé peut rendre le réseau non connexe, comme illustré par la figure 4.4 : si le nœud $u$ réduit sa portée à zéro alors un message provenant de $s$ ne peut pas joindre $v$.



## 4.3 Approche RBOP

Les algorithmes de réduction de portée, présentés dans la section ci-dessus, sont globalisés : une entité, appartenant ou non au réseau, doit avoir une connaissance complète de la topologie du réseau pour calculer le sous-graphe d'énergie minimale. Sans la présence d'un tel élément dirigeant les opérations, chaque nœud doit avoir une connaissance complète de la topologie du réseau, pour que chacun puisse calculer ce sous-graphe d'énergie minimale.

Avoir la connaissance complète du réseau nécessite certains arrangements. Pour un réseau fixe, le concepteur du réseau peut avoir informé l'entité centrale ou l'ensemble des nœuds de la position de chacun dans le réseau. Mais en général, il est nécessaire d'avoir à disposition des mécanismes pour diffuser et rapatrier cette information dans le ou les entités qui doivent calculer le sous-graphe d'énergie minimale. Une fois ce dernier calculé, il peut être nécessaire de diffuser l'information générée aux nœuds participant à l'opération de diffusion.

Mais ces approches sont peu flexibles et possèdent certaines contraintes. Premièrement, la collecte d'information nécessite de disposer de mécanismes logiciels et/ou matériels. Par exemple, chaque nœud peut diffuser un message à l'ensemble du réseau pour informer de sa présence. Ou encore, chaque nœud envoie un message vers l'entité de contrôle (ce qui nécessite de connaître un moyen de la joindre *à priori*). Deuxièmement, une fois l'arbre construit, il est possible que tous les nœuds participant à l'opération de diffusion ne connaissent pas la décision à prendre. Il est donc nécessaire de leur faire parvenir l'ensemble ou une partie de l'arbre d'énergie minimale afin qu'ils puissent participer à l'opération de diffusion.

L'ensemble de ces pré-requis nécessite des messages supplémentaires (le plus souvent, ce coût est ignoré dans les protocoles de diffusion). Ainsi, la collecte d'information par une entité ou par

l'ensemble des nœuds du réseau peut entraîner un surcoût important en nombre de transmissions, augmentant le coût énergétique de l'ensemble des participants. Ce problème est encore plus important dans le cas de réseaux ad hoc avec des nœuds mobiles. Les changements d'organisation dans la topologie, le départ ou l'arrivée de nœuds induisent l'obligation de constamment renouveler l'information topologique à destination des entités responsables de la diffusion. Cette surcharge peut être répétée régulièrement (avec la mobilité des nœuds, en cas de panne ou d'arrivée de nouveaux participants). Cette obligation est en contradiction avec l'aspect décentralisé des réseaux ad hoc car il peut être trop coûteux, voire impossible de collecter et rediffuser tous les changements dans le réseau. Ce problème devient critique dans le cas de réseaux très importants et/ou à forte mobilité.

Il est donc impératif dans une telle situation de posséder des algorithmes de diffusion distribué, qui ne nécessitent que des informations sur un voisinage proche, et qui soient capables de s'adapter aux changements dans la topologie du réseau.

Nous avons proposé avec RRS (voir chapitre 3) l'utilisation des graphes de voisinage relatif (*RNG*). Ce dernier mécanisme possède de nombreuses propriétés intéressantes (détaillées dans la section 3.3). Premièrement, le sous-graphe $RNG(G)$ d'un graphe $G$ est connexe si le graphe $G$ est connexe. Cette propriété garantit qu'un réseau sans fil construit par le sous-graphe RNG ne perde pas la connexité. Une autre propriété importante indique que les voisins RNG sont les plus proches du nœud. Celle propriété est facile à vérifier à partir de la formule utilisée pour calculer le sous-ensemble RNG. Enfin, une dernière propriété précise que le nombre de voisins RNG est borné et est égal en moyenne à 2,6 nœuds.

Nous proposons d'utiliser uniquement les voisins RNG comme ensemble recevant le message de diffusion. Chaque message émis par un nœud doit uniquement couvrir l'ensemble de ses voisins RNG pour garantir de joindre la totalité du réseau. Plus exactement, la fonction d'assignement des portées ajuste la puissance du mobile dans le but de couvrir l'ensemble des voisins RNG :

$$\exists u \in Vr(u) = max_{v \in V | (u,v) \in E_{rng}} d(u,v).$$

On peut voir un exemple avec le schéma 4.5 de sélection du voisinage RNG. Le graphe induit $G_r$ est nommé $RNG^*(G)$. Il est connu que $MST(G)$ est inclus dans $RNG(G)$ et il est facile de voir que $RNG(G)$ et un sous-ensemble de $RNG^*(G)$. Il est donc garanti que pour un graphe fortement connexe $G$, $RNG^*(G)$ est connexe.

Un des avantages de RNG est de ne pas nécessiter d'information sur la topologie complète du réseau. Chaque nœud doit seulement connaître son voisinage de manière à déterminer quels sont les nœuds qui appartiennent à son voisinage RNG. Si l'objet possède un outil de positionnement de type GPS, alors les messages HELLO suffisent : chaque nœud ajoute son identifiant et sa position géographique dans chacun des messages HELLO. Chaque nœud maintient alors une liste des voisins avec leur position. Un nœud peut déduire de cette liste les informations pour calculer les voisins RNG. Si un nœud ne possède pas d'outils de positionnement global, il doit pouvoir évaluer la distance qui le sépare de chacun de ses voisins, mais aussi les distances entre ses voisins. Quand un nœud reçoit un message, il peut évaluer la distance qui le sépare de l'émetteur en mesurant l'énergie reçue à la réception. Chaque nœud diffuse dans les messages HELLO la liste de ses voisins et la distance les séparant du nœud. Ainsi, chaque nœud possède la topologie complète à deux sauts, les distances séparant tous les nœuds à un saut et les distances le séparant avec son voisinage à un saut. Il peut ainsi déduire le sous-ensemble RNG.

Un point important est que cet algorithme est totalement décentralisé. Il ne nécessite que des informations locales (le voisinage à un saut si le mobile possède un GPS, le voisinage à deux sauts si

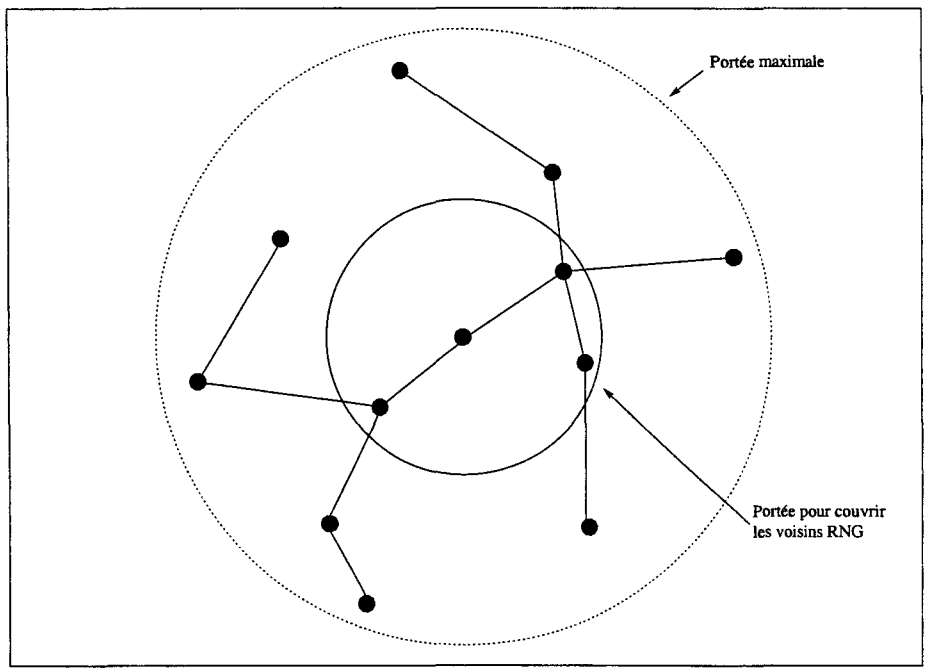



FIG. 4.5 – Exemple de réduction de portée pour couvrir les voisins RNG

chaque nœud peut mesurer la puissance en réception). Par rapport à la majorité des solutions basées sur une connaissance globale de la topologie, cette solution est plus flexible et plus adaptée aux réseaux ad hoc, surtout si ce réseau est composé d'objets mobiles. De plus, l'évaluation du sous-ensemble RNG est faite de façon locale par chacun des nœuds. Le coût de calcul du sous-ensemble RNG est relativement faible, certains algorithmes [45] proposent une complexité de l'ordre de $\theta(n \log n)$.

Le mécanisme décrit précédemment peut encore être amélioré. L'ensemble RNG d'un nœud comporte aussi le nœud qui lui a transmis le message. En effet, la fonction pour déterminer si un noeud fait partie de son RNG est symétrique. Si deux nœuds sont à portée de communication et qu'ils ne possèdent pas de voisins communs, alors chaque nœud est voisin RNG de l'autre.

Le nœud qui doit réémettre son message peut donc ajuster sa portée de façon à ne couvrir que l'ensemble des voisins RNG en excluant la source du message. Cet exemple est visible sur le schéma 4.6. Le nœud $A$ va renvoyer le message aux nœuds $G$ et $F$ en ajustant sa portée car le nœud $S$ est la source du message d'inondation. La fonction d'assignement peut se réécrire comme suit :

$$\exists u \in Vr(u) = max_{v \in V | (u,v) \in E_{rng} - source} d(u, v).$$

Mais un autre apport réduit encore la quantité de voisins RNG à joindre. En suivant la figure. 4.6, le message d'inondation est émis par $S$ à destination de ses trois voisins RNG non encore couverts ($A$, $C$ et $B$). Chacun d'eux reprogramme un envoi pour couvrir leurs voisins RNG sans la source. $F$ va donc émettre un message de manière à joindre $G$. De plus, $C$ va émettre le message de diffusion pour joindre les nœuds $E$ et $D$. La question est la suivante : quel intérêt a le nœud $F$ de réémettre ? En effet, ses deux voisins RNG ont déjà reçu le message de diffusion. Le nœud peut décider de ne pas réémettre car il sait que ses deux voisins RNG ont été couverts : il a entendu les messages de diffusion provenant des nœuds $A$ et $C$. Il peut donc ignorer la réémission.

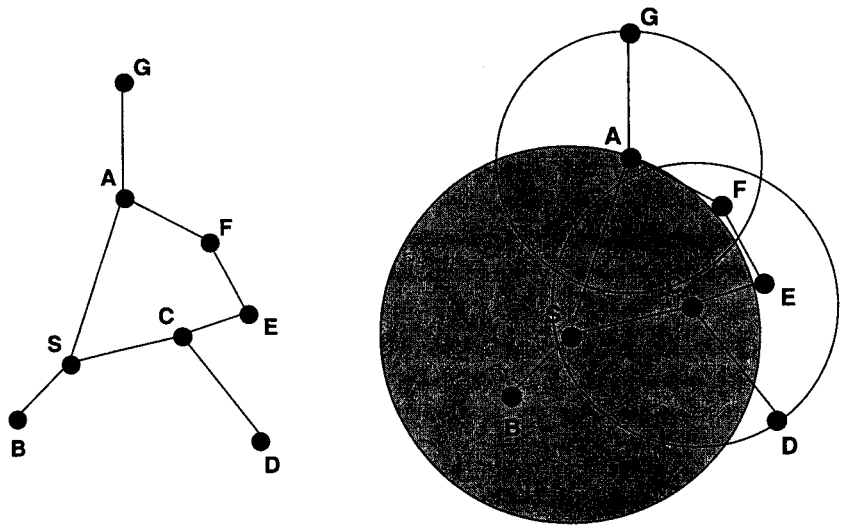



FIG. 4.6 – Diffusion de S avec un mécanisme d'élimination des voisins

On peut extraire de ces observations la règle suivante : un nœud ne réémet un message de diffusion qu'au voisin qui ne lui a pas envoyé auparavant ce même message. Un mécanisme déjà vu auparavant permet de gérer ce type de règle : le mécanisme d'élimination des voisins (voir section 1.4.4). Chaque nœud écoute l'ensemble des messages qu'il reçoit et conserve dans sa table de diffusion l'identifiant de diffusion associé à une liste de l'ensemble des nœuds qui ont déjà émis et reçu ce message. Il peut ainsi déduire, lors de son émission, une nouvelle portée comprenant l'ensemble de ses voisins RNG qui n'ont pas déjà reçu ce message.

## 4.4 Algorithmes

Dans cette section, nous proposons de détailler le fonctionnement de l'algorithme RBOP. Dans la première partie nous présentons le protocole simple, baptisé RTCP. Dans la seconde partie, nous proposons d'aller plus loin en ajoutant le système d'élimination des voisins à ce protocole pour obtenir le protocole RBOP.

### 4.4.1 RNG Topology Control Protocol

Le premier protocole propose de couvrir seulement les nœuds à joindre (c'est-à-dire les voisins RNG). L'algorithme est assez simple :

1. Lorsqu'un nœud initie une diffusion, il adapte sa portée $r$ de façon à ne couvrir que l'ensemble de ses voisins RNG.
2. Lorsqu'un nœud reçoit un message de diffusion qui n'a pas été déjà reçu, il calcule l'ensemble des voisins RNG, ajuste sa portée pour couvrir cet ensemble, et réémet le message de diffusion.
3. Lorsqu'un nœud reçoit un message qu'il a déjà reçu, il ignore le message.

Pour calculer l'ensemble RNG, nous proposons l'algorithme 5.

**Algorithme 5** Algorithme RTCP

```
for chaque voisin a du nœud source do
  drapeau = vrai
  for chaque voisin b (différent de a) du nœud source do
    if distance(a,b) < distance (source,a) then
      if distance(source,b) < distance (source,a) then
        drapeau = faux
      end if
    end if
  end for
  if drapeau then
    marquer le nœud a comme voisin RNG
  end if
end for
```

### 4.4.2 RNG Broadcast Oriented Protocol

Le second algorithme ajoute au précédent protocole le mécanisme d'élimination des voisins. Nous appelons ce nouvel algorithme RBOP (ou *RNG Broadcast Oriented Protocol*). L'algorithme est le suivant :

1. Lorsqu'un nœud initie une diffusion, il adapte sa portée $r$ de façon à ne couvrir que l'ensemble de ses voisins RNG.
2. Lorsqu'un nœud reçoit un message de diffusion qui n'a pas été déjà reçu :
   (a) Si l'émetteur est un voisin RNG : le nœud calcule l'ensemble des voisins RNG (sans inclure l'émetteur). Si cet ensemble est vide alors il ne fait rien. Dans le cas contraire, il ajuste sa portée pour couvrir l'ensemble des voisins RNG à joindre (sauf l'émetteur) et le réémet.
   (b) Si l'émetteur n'est pas un voisin RNG : le nœud associe à l'identifiant $id$ de la diffusion une liste $l_{id}$ de tous ses voisins RNG qui n'ont pas reçu le message. Au bout d'un certain temps, si la liste $l_{id}$ ainsi créée n'est pas vide (les nœuds dans la liste peuvent s'enlever avec la règle 3.3b), le nœud retransmet le message de diffusion en ajustant sa portée pour couvrir l'ensemble des nœuds restants dans la liste $l_{id}$.
3. Lorsqu'un nœud reçoit un message qu'il a déjà reçu :
   (a) Le nœud ignore le message s'il l'a déjà reçu auparavant.
   (b) Le nœud retire les nœuds contenus dans le message de la liste $l_{id}$ associée à l'identifiant $id$ du message de diffusion.
   (c) Le message est ignoré si la liste est vide.
   (d) Sinon, si le message arrive d'un nœud voisin RNG, le nœud renvoie le message de diffusion en réglant sa portée de manière à joindre l'ensemble des voisins dans la liste.

Dans ce nouvel algorithme, nous tenons compte des voisins non-RNG recevant les messages de diffusion. Lorsqu'un nœud reçoit un message provenant d'un voisin n'appartenant pas à son ensemble RNG, il démarre un mécanisme d'attente dans le bût de contrôler si tous ses voisins RNG ont bien été couverts. Ce procédé est intéressant lors de problèmes de risques de coupure de communication de

certains noeuds. Avec ce contrôle des voisins non-RNG, on se prémunit des risques de déficiences du réseau ad hoc.

## 4.5 Résultats expérimentaux

Dans nos simulations, nous comparons quatre protocoles. Les deux premiers sont globalisés : MTCP et BIP, tandis que les deux sont ceux développés dans ce chapitre : RTCP et RBOP. Pour les comparer, nous utilisons le modèle énergétique décrit avec la formule 4.1. Ce modèle est utilisé car il est le plus caractéristique pour évaluer l'efficacité de notre algorithme au niveau de l'économie d'énergie. En effet, il tient compte de la baisse de signal par rapport à la distance, et nous n'avons pas besoin de tenir compte de la taille du paquet, la couche MAC étant idéale.

Nous utilisons deux ensembles de constantes pour le modèle énergétique : $\alpha = 2$, $c = 0$ et $\alpha = 4$, $c = 10^8$. Les paramètres de la simulation sont les suivants. Le nombre de nœuds $n$ est toujours 100 et les nœuds sont immobiles. La portée maximale de chaque nœud est de 250 mètres. Les nœuds sont placés de façon aléatoire de manière à obtenir une densité donnée (de 6 à 30 nœuds par zone de communication), et seuls les graphes totalement connectés sont retenus pour la simulation. La couche MAC est considérée comme idéale. Le délai *timeout* considéré par le mécanisme d'élimination des voisins est fixé à trois fois le temps nécessaire pour envoyer un message. Pour chaque mesure, l'expérimentation porte sur 5000 diffusions.

Avec l'utilisation d'une couche MAC idéale, du fait que le graphe est totalement connecté et par la nature des protocoles, il est certain que tous les nœuds vont recevoir les messages de diffusion. L'accessibilité est toujours égale à 100%. Nous nous intéressons donc seulement à l'énergie dépensée par l'ensemble des nœuds (en accord avec les deux modèles énergétiques utilisés). Pour chaque diffusion, nous calculons la consommation totale par :

$$E_{total} = \sum_{u \in V} E(u),$$

Avec $E(u)$ l'énergie dépensée par chaque nœud, en fonction de la portée choisie. Cette somme de l'énergie totale utilisée $E_{total}$ est comparée avec la somme totale de l'énergie dépensée requise pour faire une diffusion par inondation avec la portée maximale :

$$E_{flooding} = n \times (R^{\alpha} + c).$$

Pour évaluer l'efficacité de chacun des protocoles, nous calculons le ratio d'énergie économisée (*Expended Energy Ratio* ou *EER*) par la formule suivante :

$$EER = \frac{E_{total}}{E_{flooding}} \times 100.$$

Les graphiques 4.7 et 4.8 présentent la comparaison de l'énergie sauvée pour les quatre protocoles et les deux modèles énergétiques. La densité moyenne varie avec la densité théorique (en nœuds par zone de communication) mais n'est pas exactement la même, à cause des effets de bord.

Sur le graphique 4.7, avec les valeurs $\alpha = 2$ et $c = 0$, nous observons que RBOP est très proche des résultats obtenus par MTCP. Ce fait illustre que RBOP obtient des résultats très proches des algorithmes globalisés. Mais il n'atteint pas l'efficacité du meilleur algorithme globalisé : BIP. Ce dernier est meilleur d'environ 30% pour des basses densités et jusqu'à 50% pour des hautes densités.

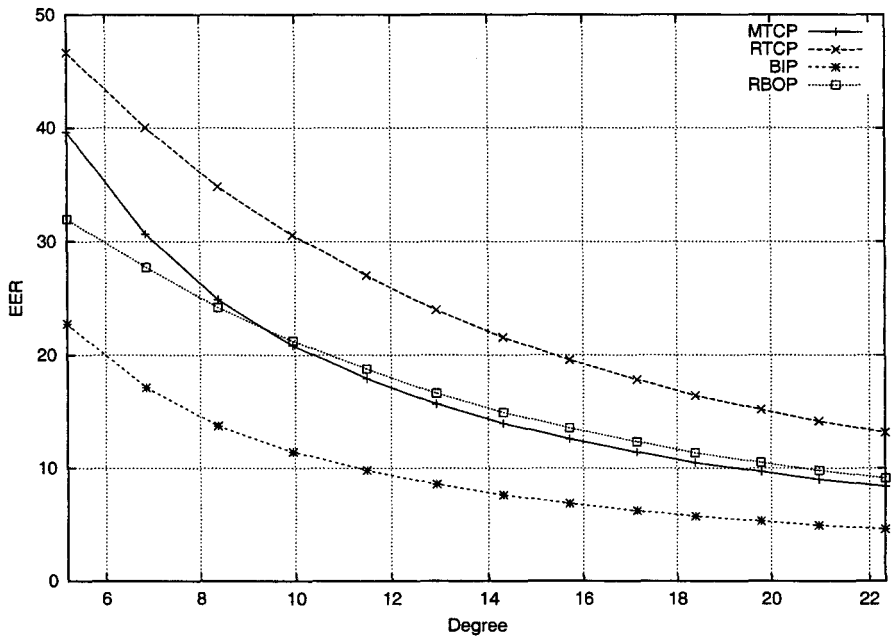



FIG. 4.7 – Comparaison de l'énergie dépensée en fonction de la densité dans le cas où $alpha = 2$

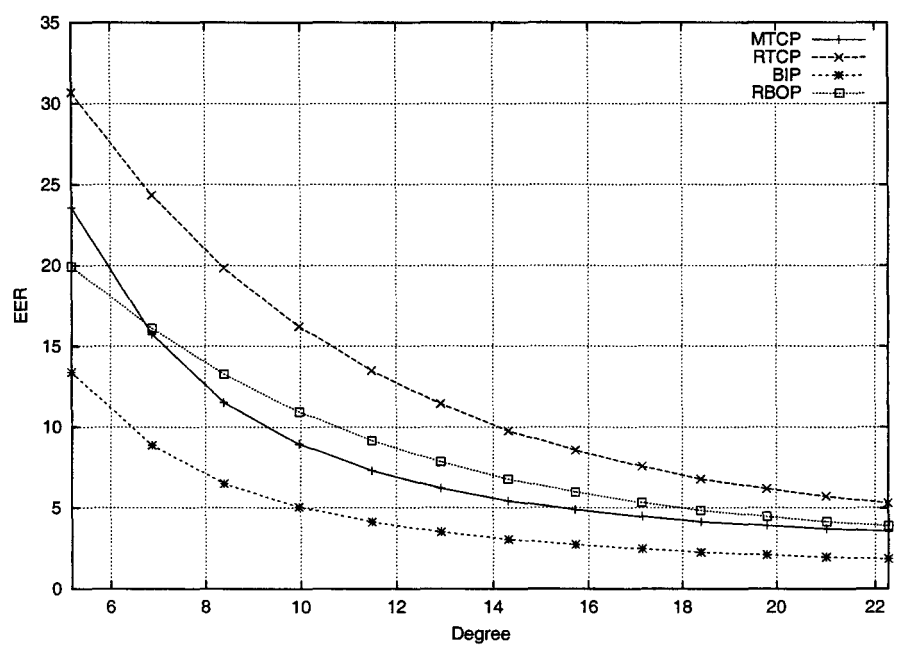



FIG. 4.8 – Comparaison de l'énergie dépensé en fonction de la densité dans le cas où $\alpha = 4$

Mais plusieurs points sont à rappeler. RBOP est un algorithme localisé, au contraire de BIP qui est globalisé. BIP trouve de meilleurs liens grâce à sa connaissance complète du réseau. Mais le coût demandé par les algorithmes globalisés pour rapatrier toutes ces informations dans un nœud central ou pour diffuser la topologie complète à l'intégralité du réseau n'est pas évalué dans nos simulations. Il est prévisible que cette surcharge peut se révéler importante pour ces algorithmes, et peut gommer ainsi les disparités de résultats entre l'approche globalisée et l'approche localisée. De plus, le calcul est plus lourd à exécuter pour les nœuds chargés de l'évaluation du graphe de diffusion, car la complexité est de l'ordre de $\theta(n^2)$, tandis que le calcul distribué du voisinage entre chaque nœud ne requiert que $\theta(m^2)$, avec $m$ nombre de voisins (avec $n >> m$ dans le cas de grandes densités). Enfin, les algorithmes localisés sont plus adaptés dans le cas d'une gestion dans un réseau ad hoc, car la mobilité oblige les algorithmes globalisés à rafraîchir l'ensemble des informations lors d'un changement topologique, tandis que les algorithmes localisés ne nécessitent que les informations sur le voisinage.

La différence entre BIP et RBOP s'accroît quand la densité augmente. En effet, puisque le nombre moyen de degrés dans un graphe RNG est constant (environ 2,6 voisins), la hauteur de l'arbre recouvrant généré par la diffusion avec RBOP est constant (pour des densités suffisamment grandes), et la portée moyenne de retransmission est inversement proportionnelle à la densité. Dans ce cas, il peut être envisageable d'orienter le protocole de façon à recouvrir une plus grande portée que celle nécessaire.

Entre RBOP et RTCP, les différences sont de l'ordre de 33% à l'avantage de RBOP. Le mécanisme d'élimination se révèle donc très utile. Il a été montré de manière expérimentale, que le degré moyen de voisins pour un graphe RNG est de 2,6. Comme le mécanisme d'élimination enlève au moins le voisin source du message de diffusion, cette moyenne tombe à 1,6. C'est donc surtout le fait d'enlever l'initiateur de la diffusion dans le cadre local qui permet de réduire la taille du voisinage RNG, même si le mécanisme intervient aussi dans le cas de la réception d'un message provenant d'un voisin non RNG, ou dans le cas d'une couverture complète du voisinage par l'ensemble des voisins.

Sur le second graphique 4.8, avec $alpha = 4$ et $c = 10^8$, l'écart reste identique entre RBOP et BIP. Par contre, RBOP met plus de temps à converger vers MTCP, du fait du coût au coup initial nécessaire pour envoyer un message. Tous les nœuds provenant de RBOP ont une probabilité plus élevée de réémettre, car ils ne peuvent pas profiter de l'optimisation globale opérée par MTCP, et doivent donc payer le coût de la constante $c$ pour chaque émission, aussi petite soit-elle.

Le point le plus important de ces expérimentations est le suivant : l'énergie économisée est importante par rapport à une diffusion classique en inondation, avec la portée radio au maximum. Avec le premier modèle énergétique ($\alpha = 2$,$c = 0$), le protocole n'utilise que 31% de l'énergie par rapport à une inondation classique dans le cas d'une faible densité. Cette économie devient encore plus importante dans le cas de forte densité (30 nœuds par zone de communication), où RBOP propose une consommation de l'ordre de 9%.

## 4.6 Conclusion

Le protocole RBOP possède de nombreux avantages. Il est localisé et efficace avec des résultats proches de certains modèles centralisés. Il ne nécessite qu'une information locale, ce qui lui permet d'avoir une meilleure adaptabilité dans le cas de réseaux à topologies changeantes.

Mais il est possible d'accroître l'efficacité de ce protocole. Une idée est d'augmenter la portée de chaque nœud au dessus du minimum nécessaire, dans le but de joindre de nouveaux nœuds pour

minimiser encore plus le coût énergétique. La valeur $r(u)$ dans RBOP est actuellement la portée minimale possible qui permet de maintenir une connexité complète dans le processus de diffusion. Une idée serait de trier les voisins non éliminés à partir de leur distance par rapport à $u$, et de considérer le ratio $E(u)/M(u)$, ou $E(u)$ est l'énergie nécessaire pour la transmission et $M(u)$ le nombre de voisins non éliminés qui peut être atteint en transmettant avec une portée $d$. Le ratio optimal peut donner une portée plus importante que la portée minimale pour couvrir le RNG, et ainsi offrir un meilleur rendement énergétique. Il est possible de s'inspirer par des protocoles de réduction, comme MPR ou Dominating Set.

Une idée, développée dans [12], est l'utilisation d'un algorithme de réduction de graphe, baptisé LMST, plus efficace. De plus, le modèle energétique peut-être pris en compte pour optimiser la portée d'émission (la solution n'étant pas nécessairement de minimiser la puissance d'émission) [43]. Les deux papiers cités proposent ces nouvelles fonctionnalités dans le cas d'antennes omnidirectionelles. Nous reprenons une partie de ce raisonnement dans le chapitre suivant, en l'appliquant dans le cas des antennes directionnelles.

# Chapitre 5

# Diffusion par antennes directionnelles

Dans le chapitre 4, nous avons présenté un protocole de diffusion permettant d'économiser l'énergie des batteries d'un objet mobile. Il a l'avantage d'être totalement localisé et de ne pas rompre la connexité du réseau. Il offre d'excellentes performances, avec des résultats proches de certains modèles centralisés. De plus, ce protocole présente l'intérêt d'être compatible avec le matériel existant : certaines cartes 802.11b peuvent évaluer le signal en réception et modifier la portée de leur signal, ce qui répond au pré-requis nécessaire pour faire fonctionner RBOP. De nouvelles recherches proposent d'améliorer la possibilité de changer un signal radio, en concentrant l'onde radio sous la forme d'un fin rayon et dans une direction précise. Les possibilités d'une telle technique sont très attrayantes : minimisation des problèmes d'interférences, des problèmes de collision et possibilité d'informer uniquement une partie du voisinage. Mais la plus importante des propriétés reste la diminution de la consommation énergétique de ce dispositif. Nous proposons dans ce chapitre trois protocoles utilisant les antennes directionnelles. Le premier est l'adaptation du protocole RBOP pour un tel mécanisme, donnant alors le protocole DRBOP [15]. C'est aussi l'utilisation d'un nouvel algorithme de réduction de graphe appelé LMST (ce nouveau protocole est baptisé DLBOP ou *Directional LMST Brodcast Oriented Protocol*) [8]. Le deuxième est un algorithme adaptatif, baptisé OM-DLBOP, utilisant d'une part un algorithme local pour la construction d'un sous-graphe connectant les nœuds proches, et d'autre part l'émission avec un angle élevé et sur une longue portée de manière à diminuer le coût énergétique en couvrant plusieurs voisins en un seul envoi. Ces deux algorithmes sont utilisés par le troisième protocole ADLBOP [17]. Ce dernier est adaptatif et choisit l'un ou l'autre des deux premiers protocoles en fonction du contexte, de manière à réduire au maximum l'énergie dépensée.

## 5.1 Les antennes directionnelles

Les antennes omnidirectionnelles dans les réseaux sans fil émettent dans toutes les directions. Dans un milieu sans obstacle, la couverture radio peut être représentée par un disque, de rayon égal à la portée d'émission. Le fait qu'un nœud puisse diffuser sans restriction autour de lui-même a certains avantages, comme la possibilité d'émettre un seul message pour joindre l'ensemble de ses voisins. Mais des inconvénients majeurs persistent, comme l'accès à la couche MAC, qui oblige la mise en place de protocole de détection d'envois simultanés et éventuellement de protocoles de négociation pour des reprises lors de collisions.

Une nouvelle solution existe, sous la forme d'antennes directionnelles. Elles peuvent concentrer le rayon d'émission dans un cône réduit, sur une distance donnée. Les problèmes d'accès sont alors limités, car deux émissions peuvent exister dans la même zone sans collision (à condition que les

nœuds participant soient distincts). Plus intéressant, l'économie d'énergie induite rend cette solution attractive. Celle-ci est proportionelle à la surface non couverte (la référence étant l'énergie dépensée par une antenne omnidirectionnelle émettant avec la même portée).

Avec les antennes directionnelles, de nouvelles possibilités de communication avec le voisinage sont offertes. Il existe alors plusieurs modèles de communication :

**Un-vers-tous** (*One-to-All*) : les nœuds utilisent des antennes omnidirectionnelles (Voir la figure 5.1(A)). Ils diffusent leurs ondes radio sans aucune restriction. Si l'environnement ne possède pas d'obstacle, tout mobile situé autour du nœud émetteur à une distance inférieure à la portée d'émission peut recevoir les messages du nœud émetteur. C'est une communication universelle, donnant à chaque voisin les mêmes possibilités de recevoir les messages. Le système radio est relativement simple à développer, et ne demande pas de technologie complexe. Il existe néanmoins quelques inconvénients à cette approche (déjà évoqués dans la section 1.2) tels que les problèmes de collisions, de terminal caché et de terminal exposé. De plus, la consommation énergétique dans le cas d'un système radio peut se révéler importante.

**Un-vers-plusieurs** (*One-to-Many*) : les nœuds utilisent des antennes capables de concentrer leurs émissions dans un cône d'angle variable et dans une direction donnée (voir la figure 5.1(B)). Ainsi, un nœud peut choisir de couvrir uniquement un sous-ensemble de son voisinage. La possibilité de diriger les ondes radios permet de réduire les problèmes d'interférence et les risques de collision, de concentrer la puissance radio vers un angle défini[1] et d'introduire la notion de secret (un voisin qui n'est pas inclus dans le cône d'émission ne peut à priori pas entendre les messages[2]).

**Un-vers-un** (*One-to-One*) : les nœuds peuvent émettre un mince filet d'onde radio dans une direction précise (voir la figure 5.1(C)). À la différence du mode précédent, le cône d'envoi des ondes radios est fixe et ne peut être changé. Le dispositif est prévu pour permettre les communications d'un mobile vers un seul autre mobile. Il hérite néanmoins des avantages du mode précédent, et même amplifie leurs capacités. En effet, le rayon (on peut même parler de fil) d'ondes radios est des plus fins possibles[3], donc les problèmes d'interférence et de collision sont très faibles. De plus, le fait de concentrer l'émission dans un cône d'angle réduit permet d'accroître considérablement la portée du nœud émetteur.

Dans le reste de ce mémoire, nous prenons l'hypothèse de la disponibilité d'antennes pouvant contrôler leur puissance et leur angle d'émission (c'est à dire la taille du cône et sa direction).

## 5.2 Préliminaires

Dans la section 4.2.1, nous considérons un modèle extrait de celui de Feeney [32] pour décrire la consommation énergétique avec des antennes omnidirectionnelles. La formule utilise une constante $C$ pour prendre en compte le surcoût dû au traitement du signal, au minimum d'énergie nécessaire pour une réception réussie et à l'utilisation des messages de contrôle MAC. De plus, elle possède une constante $\alpha$ supérieure ou égale à 2, représentant le facteur d'atténuation de l'environnement. Si la distance entre le nœud émetteur $u$ pour joindre $v$ est notée par $d(u, v)$, alors l'énergie consommée

[1] ce qui permet d'accroître la portée radio, car la puissance d'émission est concentrée.

[2] les effets de diffraction et de rebond peuvent jouer et permettre à un nœud non prévu dans le cône de communication de recevoir les messages.

[3] Le cône d'émission doit pouvoir être capté par le nœud récepteur, avec un majorant pour les erreurs d'appréciation de la position de ce dernier.

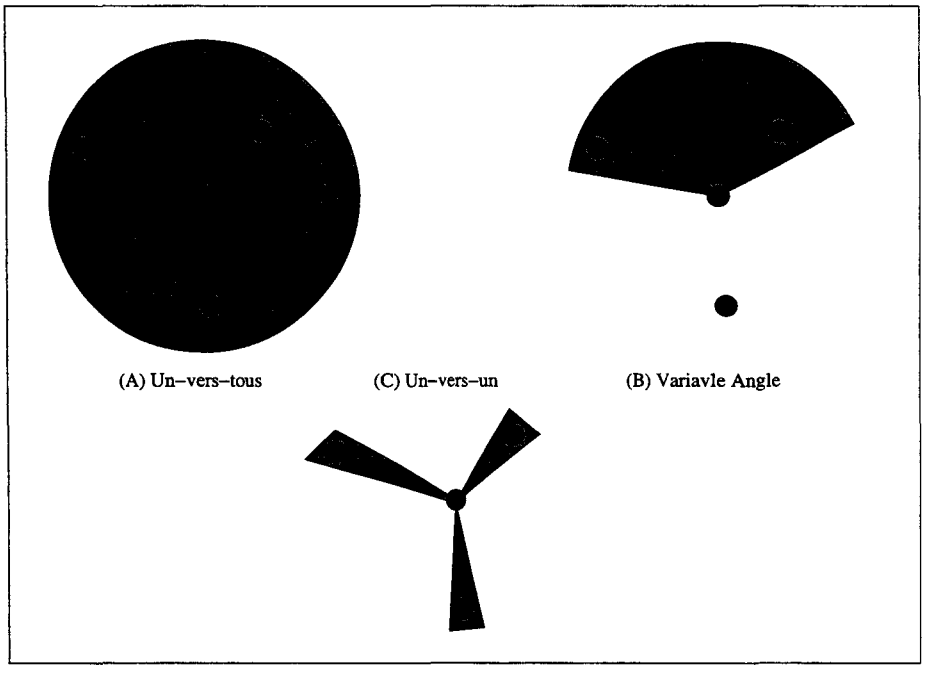



FIG. 5.1 – Les différents modèles de communication

pour envoyer un message d'un nœud $u$ à un nœud $v$ avec une antenne omnidirectionnelle est donnée par la formule suivante :

$$e(u,v) = d(u,v)^{\alpha} + C \tag{5.1}$$

Nous adaptons ce modèle dans le cas des antennes directionnelles. Elles peuvent concentrer l'émission dans un cône de direction, d'angle et de portée choisis par l'émetteur. Nous prenons l'hypothèse que les antennes ont la capacité de concentrer uniformément leur émission en un rayon d'angle $\theta$ (en radians) et nous proposons ce nouveau modèle pour la consommation énergétique :

$$e(u,v) = \theta\frac{d(u,v)^{\alpha} + C_1}{2\pi} + C_2 \tag{5.2}$$

La constante $C_1$ représente le surcoût pour les messages de contrôle MAC, tandis que la constante $C_2$ dénote le coût engendré par le traitement du signal, le minimum d'énergie requis pour garantir une réception correcte et pour orienter le rayon vers une direction précise avec une largeur donnée. Avec le modèle d'angle variable, l'angle du rayon est choisi avec comme limitation physique $\theta_{min} \leq \theta \leq \theta_{max}$. Dans le cas du modèle énergétique un-vers-un, $\theta$ est fixe et considéré comme petit : $\theta = \theta_{min}$. Ce modèle généralise celui utilisé par Wieselthier *et al.* [99]. Nous obtenons d'ailleurs le même modèle en posant $C_1 = C_2 = 0$. Pour associer un coût élevé à chaque transmission, nous proposons l'utilisation des constantes suivantes : $\alpha = 4$, $C_1 = 8.10^7$ et $C_2 = 2.10^7$.

Dans l'opération de diffusion, nous essayons de minimiser l'énergie totale requise par :

$$E = \sum_{u \in V} \sum_{w \in N(u)} E(u,w)$$

Avec :

$$E(u,w) = \begin{cases} e(u,w) & \text{si } u \text{ fait suivre un message à } w, \\ 0 & \text{sinon.} \end{cases}$$

## 5.3 Travaux existants

Nous avons proposé dans le chapitre 3 RBOP, un algorithme localisé de diffusion. Il est fondé sur une méthode de construction de sous-graphe baptisée RNG (détaillée dans la section 3.3). Les principales caractéristiques de RNG sont les suivantes ; Il est entièrement localisé ; Il donne un graphe coplanaire (il n'y a pas de liens qui se croisent si l'on projette la représentation du réseau sur un plan) ; Il conserve la connexité du réseau ; Chaque nœud possède un nombre limité de voisins proches (avec une moyenne expérimentale de 2.6 voisins par nœud) ; Enfin, il ne nécessite que la connaissance des distances entre le nœud et ses voisins, et la distance entre les voisins du nœud.

Li *et al.* [55] ont proposé LMST (*Local Minimum Spanning Tree*), une autre méthode permettant de constituer un sous-graphe pour réduire le nombre de liens. Nous détaillons la méthode de construction du sous-graphe LMST dans la section 5.4.1. Comme RNG, le sous-graphe diminue le degré de chaque nœud, en limitant les liens uniquement entre nœuds proches. Cet algorithme est aussi localisé, et donc utilisable dans les réseaux ad hoc. Plus généralement, LMST possède les mêmes propriétés que RNG à une différence près : le degré moyen du sous-graphe LMST est moins important que celui de RNG. Expérimentalement, le degré est approximativement de 2.04 pour LMST, tandis que celui de RNG est plus élevé (2.6). Cette particularité, comme nous allons le voir par la suite, le rend plus attractif dans un contexte directionnel. Les auteurs ont déjà proposé un protocole omnidirectionel pour le contrôle de topologie utilisant LMST dans [54].

Seuls quelques auteurs s'intéressent à l'utilisation d'antennes directionnelles pour économiser l'énergie dans les réseaux ad hoc. Spyropoulos *et al.* [83] ont proposé un algorithme centralisé pour organiser le réseau dans le but de router le trafic entre les nœuds, en utilisant le moins d'énergie possible. L'algorithme se décompose en quatre phases. Dans un premier temps, la plus courte route est calculée pour chaque couple de nœuds, avec l'hypothèse que chaque nœud possède des antennes omnidirectionnelles. Deux unités différentes de mesure (la quantité d'énergie minimale utilisée par paquet et la durée de vie énergétique du réseau) sont alors calculées dans le but d'évaluer le coût de chaque lien et la consommation énergétique de chaque nœud. Deuxièmement, une matrice contenant le coût de chaque lien est calculée à partir des résultats précédents. Elle définit le taux de trafic généré par unité de temps d'un nœud source vers un nœud destination. Par la suite, une mise à jour de la topologie est réalisée en ne considérant qu'un seul et unique lien par nœud (pour répondre au besoin du modèle de communication *un-vers-un*). Finalement, un système de synchronisation est mis en place pour chaque lien, dans le but de minimiser le temps total nécessaire pour « servir » l'ensemble des liens. Cette dernière étape est effectuée en utilisant des algorithmes de coloriage de graphes. Cet algorithme, destiné à router des messages dans un réseau, peut servir dans le cas de la diffusion. Par contre, il est complètement centralisé et il semble impossible de l'utiliser dans le cas d'un réseau ad hoc avec une forte mobilité.

Nous avons présenté dans la section 4.2.2 deux heuristiques gloutonnes de Wieselthier *et al.* [98] pour permettre une diffusion avec un contrôle globalisé. BLU (*Broadcast Least-Unicast-Cost*) est une heuristique qui détermine un arbre d'énergie minimale à partir d'un nœud source vers tous les autres nœuds. BIP (*Broadcast Incremental Power*) est fondé sur l'algorithme de Prim, il évalue le coût énergétique supplémentaire lors de la couverture de nouveaux nœuds, dans le but de minimiser l'énergie supplémentaire.

Wieselthier *et al.* [99] ont proposé deux extensions du protocole BIP avec des antennes directionnelles dans le cas d'un modèle de communication de type angle variable. Le premier protocole est appelé RB-BIP (*Reduced Beam BIP*). Il réduit l'angle de l'onde radio à sa plus petite valeur possible et utilise le modèle de communication *un-vers-un* pour joindre successivement tous les voisins descendants de l'arbre. Le deuxième protocole s'appelle D-BIP (*Directional BIP*). À chaque étape de la construction de l'arbre, un nœud est sélectionné à partir du coût attendu de la consommation énergétique (à partir de la portée et de l'angle choisis). L'heuristique choisit en fonction de ce critère soit de sélectionner un nouveau nœud dans l'arbre, soit d'augmenter l'angle et/ou la portée d'émission d'un nœud appartenant à l'arbre. Ensuite, chaque nœud doit émettre une et une seule fois vers ses voisins sélectionnés (c'est un modèle de communication *un-vers-plusieurs*). Les auteurs ajoutent des contraintes, comme la limitation de ressource pour minimiser le problème d'affectation de fréquences. Ils proposent aussi l'ajout de limitations d'énergie (réduire l'utilisation des nœuds avec une batterie faible) en augmentant le coût associé à leur usage.

## 5.4 Les protocoles un-vers-un et un-vers-plusieurs

Nous allons maintenant présenter le protocole ADLBOP (*Adaptive Directed LMST Broadcast Oriented Protocol*), un protocole adaptatif et localisé pour la réduction du coût énergétique lors de la diffusion d'un message dans un réseau ad hoc à l'aide d'antennes directionelles. Ce protocole hybride s'appuie sur deux algorithmes. Le premier est un algorithme de diffusion s'appuyant sur une méthode de réduction de graphe. C'est une version directionnelle de l'algorithme RBOP mais pouvant utiliser soit RNG soit LMST, pour donner les protocoles DRBOP (*Directed RNG Broadcast Oriented Protocol*) et DLBOP (*Directed LMST Broadcast Oriented Protocol*). Nous proposons ensuite OM-DLBOP (*One-to-many* ), un protocole de diffusion utilisant des envois proches du modèle omnidirectionnel. Il couvre en une seule fois un nombre important de nœuds pour minimiser la consommation énergétique en cas de grande densité et avec une constante importante associée à chaque envoi.

### 5.4.1 Directed RNG Broadcast Oriented Protocol (DRBOP) et Directed LMST Broadcast Oriented Protocol (DLBOP)

Dans le chapitre 4, nous avons discuté de l'utilisation d'un algorithme de réduction de graphe dans le cas d'une diffusion avec des antennes omnidirectionnelles. L'utilisation de RNG permettait d'obtenir un graphe planaire, de degré réduit avec des liens seulement entre les mobiles proches. Nous proposons d'utiliser le même algorithme dans le cas d'une diffusion avec des antennes directionelles. De plus, nous utilisons l'algorithme de réduction de graphe LMST, qui se révèle plus efficace pour la même opération.

L'algorithme LMST fonctionne comme suit. Chaque nœud $u$ construit le MST de son propre voisinage, *i.e.* $MST(N(u))$. Un arc entre deux nœuds $u, v \in V$ appartient au graphe LMST de $G$ si et seulement si $u$ est un voisin de $v$ dans $MST(N(v))$ et $v$ est un voisin de $u$ dans $MST(N(u))$. Nous écrivons $LMST(G) = (V, E_{lmst})$ le sous-graphe LMST du graphe $G = (V, E)$.

Les deux algorithmes nécessitent exactement le même type d'information : une connaissance globale de la topologie complète du voisinage, c'est-à-dire la liste des nœuds dans le voisinage (le nœud source inclus) et les liens existant entre chaque couple de voisins. Cette connaissance nécessite des outils de positionnement, tels que le GPS ou la mesure de puissance en réception (voir section 2.1.2). Pour collecter ces informations, nous prenons l'hypothèse que chacun des nœuds a une antenne directionnelle mais qu'il peut entendre les communications provenant de chacun de ses voisins et envoyer

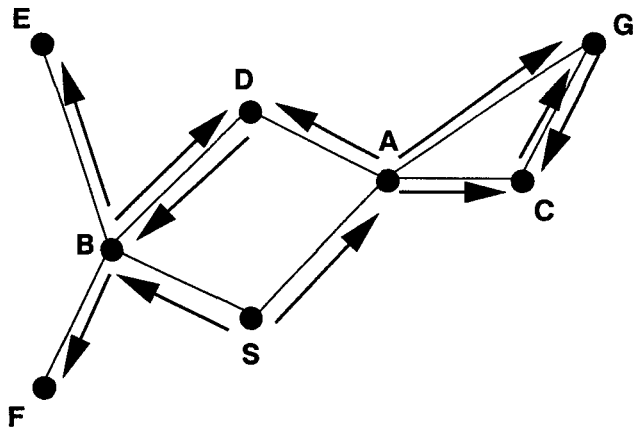



FIG. 5.2 – Transmissions dans le cas d'un algorithme DRBOP pour une diffusion démarrée par le nœud $S$.

un message à chaque voisin avec une communication *un-vers-un*, en dirigeant l'onde radio vers le correspondant.

Nous allons maintenant exposer le fonctionnement de DRBOP et de DLBOP. La méthode de diffusion est la même, seul l'algorithme de réduction de graphe diffère. DRBOP (resp. DLBOP) est inspiré de RBOP, mais la diffusion se fait en utilisant des communications un-vers-un à destination de chacun des voisins RNG (resp. LMST) à joindre. Les antennes directionnelles sont utilisées pour décomposer le message vers chacun des voisins faisant partie de son RNG (resp. LMST). Un nœud recevant un message de la part d'un de ses voisins RNG (resp. LMST) le transmet en diffusant un message à chacun de ses autres voisins RNG (resp. LMST), à l'aide d'un rayon radio d'angle faible (égal à $\theta_{min}$). Cette manière de procéder est intéressante, car le nombre moyen de voisins dans un graphe RNG (resp. LMST) est de 2,6 (resp. 2.04). Ainsi chaque nœud devra transmettre en moyenne un message dans le cas de LMST ou un message et demi dans le cas de RNG.

Considérons un exemple avec le graphe RNG donné en figure. 5.2. Le nœud $S$ veut diffuser un message à l'ensemble du réseau. Il envoie deux messages séparés vers ses voisins RNG $A$ et $B$. Pour ces deux messages, $S$ utilise deux transmissions avec deux portées différentes : $d(S, A)$ et $d(S, B)$. Quand le nœud $A$ reçoit le message provenant de $S$, il le retransmet à l'ensemble de ses voisins RNG, excepté $S$ (la source du message). Ainsi $A$ envoie 3 messages successifs vers $D$, $C$ et $G$. Au même moment $B$ envoie un message vers $D$ et $F$. En accord avec le non déterminisme de la couche MAC, $D$ peut recevoir le message en premier de la part de $A$ ou $B$. Considérons que le message arrive de $A$, $D$ retransmet vers ses voisins RNG excepté $A$, c'est-à-dire $B$. Avec cette règle, $E$ et $F$ ne font pas suivre le message, car leur ensemble de voisins RNG ne contient qu'un élément : le dernier relais, qu'il n'est pas nécessaire de couvrir. Les nœuds $G$ ou $C$ peuvent encore faire une communication vers l'un vers l'autre.

Pour éviter des transmissions non nécessaires (par exemple entre $B$ et $D$ ou entre $C$ et $G$), nous pouvons utiliser le mécanisme d'élimination des voisins. Pour chaque transmission, les nœuds ajoutent dans le message une liste de leurs voisins RNG, pour permettre à chaque nœud de prendre connaissance des voisins déjà couverts. Mais cet ajout ne semble pas donner de meilleurs résultats (moins de 0,01% de gain). Ceci est dû au fait que le mécanisme d'élimination des voisins fonctionne seulement pour trois voisins interconnectés (comme $A$, $C$ et $G$). Mais un tel sous-graphe se trouve très rarement dans les graphes RNG (et encore plus dans un graphe LMST), car la règle de construction du

sous graphe RNG empêche une telle possibilité, et LMST est un sous-graphe de RNG. Le mécanisme d'élimination n'est donc pas utilisé dans DRBOP (ni dans DLBOP, pour la même raison).

Pour la suite de ce mémoire, nous allons nous intéresser uniquement à DLBOP. En effet, ce dernier est plus efficace que DRBOP pour la réduction énergétique associée. Le degré moyen des graphes générés par LMST est d'environ de 2.04, tandis que ceux produits par RNG est de 2.6. Dans le cas où chaque nœud procède à des communications un-vers-un à destination de ses voisins, un nœud qui utilise DLBOP doit émettre en moyenne un message, alors que celui qui utilise DRBOP enverra plus d'un message et demi en moyenne.

La consommation énergétique de DLBOP peut être évaluée en calculant le nombre de messages que chaque nœud doit envoyer en moyenne. Chaque nœud envoie en moyenne 1 message (car il possède 2.04 voisins, dont un qui lui fait parvenir le message de diffusion). Chaque envoi utilise un message un-vers-un d'angle $\beta$ (l'angle minimal pour communiquer) avec une portée égale à la distance moyenne séparant deux voisins LMST $d_{lmst}$. Ainsi, la consommation énergétique totale du réseau peut s'écrire :

$$E_{DLBOP} = n \times e(\beta, d_{lmst}). \tag{5.3}$$

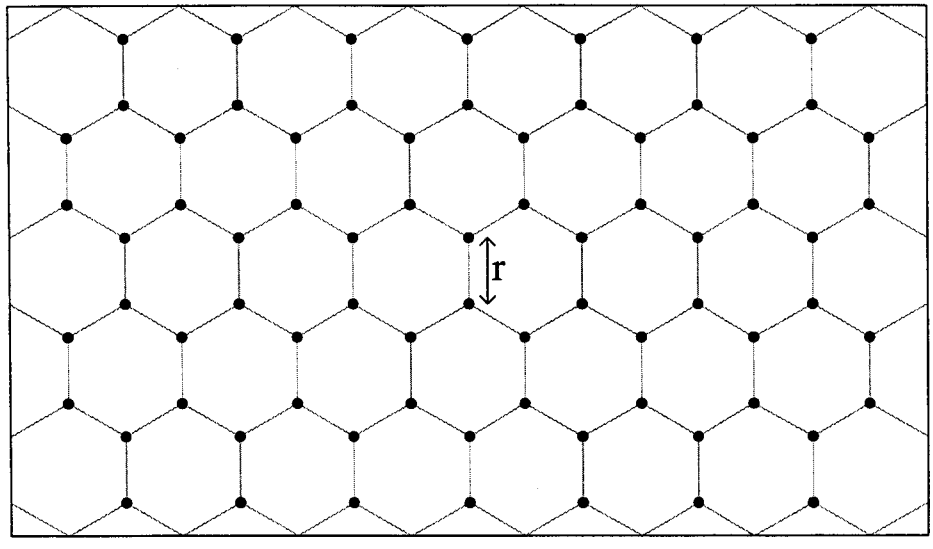



FIG. 5.3 – Modèle du pavage hexagonal

Il est nécessaire d'évaluer $d_{lmst}$ pour avoir une idée de la consommation énergétique de ce modèle. Nous utilisons un pavage hexagonal pour représenter la distribution de $n$ nœuds sur un terrain d'aire $S$. Ce type d'organisation donne une couverture complète du domaine sans recouvrement. Avec cette représentation, présentée avec le schéma 5.3, nous observons que chaque nœud est situé à l'intersection de trois hexagones, et donc que deux nœuds sont nécessaires pour chaque hexagone. La taille d'un côté d'hexagone, qui représente la distance moyenne entre deux voisins LMST, peut alors s'écrire :

$$d_{lmst} = r_{hex} = \sqrt{\frac{4S}{3\sqrt{3}n}}. \tag{5.4}$$

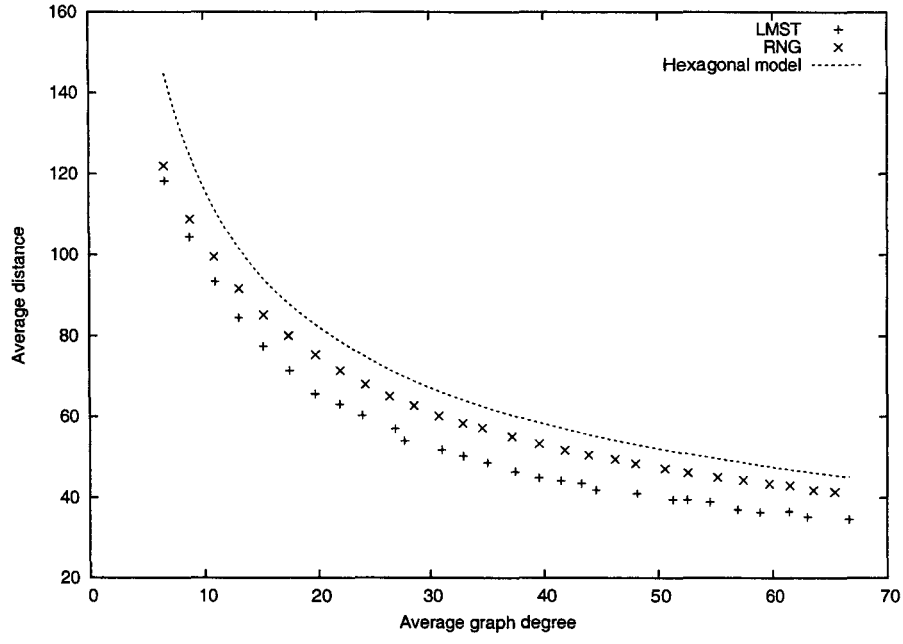



FIG. 5.4 – Distance moyenne entre les voisins RNG, entre les voisins LMST, et entre les voisins du modèle théorique hexagonal.

Cette proposition peut être vérifiée expérimentalement. La figure 5.4 présente le graphique montrant la distance moyenne entre voisin LMST à partir du modèle théorique et du modèle expérimental (avec $S = 2000 \times 2000$m and $R = 250$m). Les deux courbes ont le même comportement, les résultats expérimentaux étant plus bas à cause des effets de bord.

### 5.4.2 One-to-many Directed LMST Broadcast Oriented Protocol (OM-DLBOP)

Les protocoles DRBOP et DLBOP permettent une très bonne réduction de l'énergie consommée, mais possèdent un défaut de taille. Dans le cas où $C_1$ et $C_2$ sont non nuls, la consommation énergétique est encore très importante, particulièrement dans le cas de grandes densités. En effet, chaque nœud va envoyer un ou plusieurs messages, et le coût de $C_1$ et $C_2$ sera important. Dans ce cas, la meilleure solution n'est pas l'envoi de plusieurs messages vers les voisins proches mais de couvrir plusieurs nœuds avec une seule transmission. La variante un-vers-plusieurs de DLBOP, nommée OM-DLBOP, envoie un seul message avec un angle variable au lieu de plusieurs émissions avec un angle $\beta$. Un nœud qui décide de renvoyer le message, utilise alors un simple envoi avec un angle approprié, qui lui permet de couvrir tous les voisins LMST non-couverts et plus. Pour accroître l'économie d'énergie, il peut-être intéressant d'étendre la portée de manière à éviter des retransmissions supplémentaires qui pourraient être coûteuses. Considérons par exemple la diffusion avec un envoi d'angle $\gamma$ ($\gamma \in [\beta, 2\pi]$ où $\beta$ est l'angle minimal) et de portée $R$. Nous cherchons, pour un angle $\gamma$ donné, la portée optimale $R_{opt}(\gamma)$ qui minimise la consommation énergétique totale.

Nous proposons un modèle pour évaluer la consommation de ce type de diffusion. Pour couvrir une aire circulaire autour de lui-même, un nœud doit envoyer $2\pi/\gamma$ messages avec, pour chacun, un coût associé de $e(\gamma, r)$. Supposons que la surface $S$ qui contient tous les nœuds soit idéalement

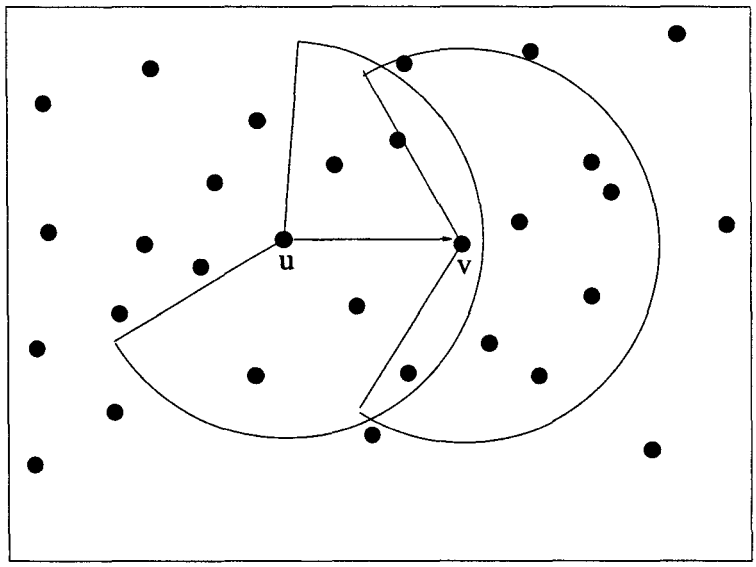



FIG. 5.5 – Une diffusion avec l'algorithme OM-DLBOP

couverte avec un tel procédé, alors la consommation énergétique, notée $E_{area}(r)$, peut s'écrire :

$$\begin{aligned} E_{area}(r) &= \frac{S}{\pi r^2} \times \frac{2\pi}{\gamma} e(\gamma, r) \\ &= \frac{S}{\pi}\left(r^{\alpha-2} + C_1 r^{-2} + \frac{2\pi C_2 r^{-2}}{\gamma}\right). \end{aligned}$$

Le comportement de la fonction $E_{area}(r)$ dépend des constantes $\alpha$, $C_1$ et $C_2$. On peut la dériver par rapport à $r$ pour obtenir son comportement :

$$E_{area}(r)' = r^{-3}\left((\alpha-2)r^{\alpha} - 2C_1 - \frac{4\pi}{\gamma}\right) \tag{5.5}$$

À partir de cette formule, nous obtenons la table 5.1, qui donne le comportement de $E_{area}$. Il est intéressant de voir que le radius optimal ne dépend pas de la densité ou du degré moyen de chaque nœud. Néanmoins, l'analyse proposée n'est valable que pour des réseaux denses, car avec une densité faible, le réseau peut avoir des portions assez grandes de zones vides.

Nous allons présenter maintenant l'algorithme OM-DLBOP. Nous choisissons d'envoyer avec un angle égal à $4\pi/3$, ce qui minimise le recouvrement des zones de communication et donne une bonne couverture du voisinage (comme montré par le schéma 5.5). L'angle est positionné symétriquement par rapport à la droite $(uv)$. Comme l'angle entre deux voisins LMST est au moins de $\pi/6$, l'angle choisi $4\pi/3$ contient l'ensemble des voisins LMST restants de $v$. Les voisins LMST qui ont déjà reçu le même message peuvent être déterminés à partir de la position de la source, la position des voisins, et l'angle et la portée de l'émission de la source. Après avoir utilisé un mécanisme d'élimination réduit aux voisins LMST, un nœud $u$ qui décide de retransmettre calcule l'angle et la portée de son émission comme suit :

- Soit $A$ l'ensemble des voisins non couverts et $B \subseteq A$ l'ensemble des voisins LMST non-couverts.

| | $C_1 = C_2 = 0$ | $C_1 \neq 0 \vee C_2 \neq 0$ |
|---|---|---|
| $\alpha = 2$ | constant<br><br>pas de $R_{opt}(\gamma)$ | monotone<br>décroissant<br>$R_{opt}(\gamma) = R$ |
| $\alpha > 2$ | monotone<br>croissant<br>$R_{opt}(\gamma) = 0$ | minimum à<br>$r = \sqrt[\alpha]{\frac{2C_1 + \frac{4\pi C_2}{\theta}}{\alpha - 2}}$<br>$R_{opt}(\gamma) = min(r, R_{max})$ |

TAB. 5.1 – Comportement de $E_{area}(r)$.

- Le nœud $u$ calcule l'ensemble de nœuds dont la distance est inférieure à $R_{opt}(4\pi/3)$ :

$$A' = \{v \in A \mid d(u,v) \leq R_{opt}(4\pi/3)\}. \tag{5.6}$$

  Le but de $u$ est de joindre l'ensemble des nœuds de $C = A' \cup B$, c'est-à-dire les nœuds à une distance inférieure à $R_{opt}(4\pi/3)$ et les voisins LMST. Si $C_1 = C_2 = 0$, la portée optimale ne peut être évaluée. Dans ce cas, nous considérons que $R_{opt}(4\pi/3) = 0$. Cela implique que $A' = \emptyset$ et que seuls les voisins LMST doivent être couverts.
- Le nœud calcule l'angle $\theta$ nécessaire pour couvrir $C$ et la portée qui permet de joindre tous les nœuds de $C$. Si $\theta < \beta$ alors on fixe $\theta = \beta$. Si $C$ est vide, alors la retransmission est annulée.
- Si $d > R_{opt}(\theta)$ alors le nœud envoie un message d'angle $\theta$ avec une portée $d$. Sinon, le nœud sélectionne la portée associée à l'angle $\theta$ de manière à joindre tous les nœuds de $A$ plus proches que $R_{opt}(\theta)$.

Une évaluation de la consommation énergétique du protocole OM-DLBOP peut être obtenue si nous considérons un envoi avec un angle de $4\pi/3$. Considérons un espace d'aire $S$ avec $N$ nœuds relais. En utilisant l'approximation du pavage hexagonal expliquée plus haut, nous divisions l'espace $S$ en hexagones de côté $R_{opt} = R_{opt}(4\pi/3)$. En posant $N = 2S/A_{hex}$ avec $A_{hex} = 3R_{opt}^2\sqrt{3}/2$, la consommation énergétique s'écrit alors :

$$E_{OM-DLBOP} = N \times e(4\pi/3, R_{opt}) = \frac{8S}{9\sqrt{3}}(R_{opt})^{\alpha-2} + \frac{4S}{3\sqrt{3}}\left(\frac{2}{3}C_1 + C_2\right)R_{opt}^{-2}. \tag{5.7}$$

Si l'on compare le comportement de $E_{OM-DLBOP}$ et de l'approximation théorique offerte par $E_{area}(r)$, on peut voir que les comportements sont les mêmes. Comme vu dans la table 5.1, si $C_1 = C_2 = 0$ et $\alpha = 2$, alors le radius optimal $R_{opt}$ n'a pas d'importance et la consommation énergétique est égale à

$$E_{OM-DLBOP} = \frac{8S}{9\sqrt{3}}.$$

Avec $\alpha = 2$ et $C_1 \neq 0$ ou $C_2 \neq 0$, $E_{OM-DLBOP}$ est minimale quand $R_{opt} = R$, offrant un comportement semblable à $E_{area}(r)$. Dans ce cas, la consommation énergétique est égale à :

$$E_{OM-DLBOP} = \frac{8S}{9\sqrt{3}} + \frac{4S}{3\sqrt{3}}\left(\frac{2}{3}C_1 + C_2\right)R^{-2}.$$

Dans le cas où $\alpha > 2$, le premier cas ($C_1 = C_2 = 0$) indique qu'il vaut mieux minimiser la portée d'émission. La distance minimale entre chaque nœud pouvant être approximer par $d_{lmst}$ (et donc $r_{hex}$), nous pouvons alors écrire :

$$E_{OM-DLBOP} = \frac{8S}{9\sqrt{3}} + 2n\left(\frac{2}{3}C_1 + C_2\right).$$

Avec le deuxième cas ($C_1 \neq 0$ ou $C_2 \neq 0$), il existe un minima (que nous découvrirons par la suite expérimentalement). Nous pouvons écrire que la consommation énergétique dans le cas général est :

$$E_{OM-DLBOP} = \frac{8S}{9\sqrt{3}}R_{opt}^{\alpha-2} + \frac{4S}{3\sqrt{3}}\left(\frac{2}{3}C_1 + C_2\right)R_{opt}^{-2}.$$

### 5.4.3 À la recherche d'un seuil

Les deux approches proposées précédemment sont valides. Les protocoles DRBOP et DLBOP offrent un sous-graphe avec un degré minimal pour chaque nœud, et OM-DLBOP propose de couvrir de larges groupes de nœuds pour réduire le coût associé à chaque envoi. Nous allons maintenant développer une analyse pour savoir quel protocole utiliser en fonction du modèle énergétique utilisé et de la situation. Nous utilisons ici DLBOP au détriment de DRBOP, car nous démontrerons expérimentalement que ce protocole est plus efficace.

Pour les quatre modèles énergétiques, nous étudions quand $E_{OM-DLBOP}$ est plus intéressant que $E_{DLBOP}$. L'inégalité $E_{OM-DLBOP} < E_{DLBOP}$ est résolue en utilisant les formules 5.3 et 5.7 avec les constantes $\alpha$, $C_1$ et $C_2$ correspondant au modèle énergétique.

- Pour $\alpha = 2$, $C_1 = 0$ et $C_2 = 0$, si $E_{OM-DLBOP} < E_{DLBOP}$ alors $4\pi/3 < \beta$. Comme l'angle $\beta$ est généralement petit et inférieure à $4\pi/3$, il est plus intéressant d'utiliser $E_{DLBOP}$ avec ce modèle énergétique, quelle que soit la densité.
- Avec $\alpha = 2$, et $C_1 \neq 0$ ou $C_2 \neq 0$, l'inégalité $E_{OM-DLBOP} < E_{DLBOP}$ est vraie quand :

$$d > \frac{4\pi R^2}{3\sqrt{3}} \times \frac{\frac{1}{R^2}\left(\frac{2}{3}(R^2 + C_1) + C_2\right) - \frac{\beta}{2\pi}}{\frac{\beta}{2\pi}C_1 + C_2},$$

  Où $d$ est la densité en nombre de nœuds par zone de communication. Pour des valeurs de $d$ supérieures, la meilleure solution est d'utiliser l'algorithme OM-DLBOP. Sinon, l'utilisation de DLBOP est recommandée, mais ce cas ne se produit que pour des petites valeurs de $C_1$ et $C_2$.
- Pour $\alpha > 2$, $C_1 = 0$ et $C_2 = 0$, on peut déduire du tableau 5.1 que la meilleure solution est de minimiser la portée. Nous remplaçons alors $R_{opt}$ par $d_{lmst}$ et nous pouvons écrire :

$$n < \sqrt[(\frac{\alpha}{2}-1)]{\frac{\beta}{2\pi}\left(\frac{4S}{3\sqrt{3}}\right)^{\frac{\alpha}{2}}\frac{9\sqrt{3}}{8S}d_{lmst}^{2-\alpha}}$$

  Dès que le nombre de nœuds devient important, il est plus intéressant d'utiliser le mode DLBOP.
- Avec $\alpha > 2$, et $C_1 \neq 0$ ou $C_2 \neq 0$, si l'on considère que $E_{OM-DLBOP}$ est une constante (elle ne dépend pas de $n$ et $\beta$ est fixé à $4\pi/3$), l'inégalité $E_{OM-DLBOP} < E_{DLBOP}$ peut être réduite à :

$$n^{(1-\frac{\alpha}{2})}\frac{\beta}{2\pi}\left(\frac{4S}{3\sqrt{3}}\right)^{(\frac{\alpha}{2})} + n\left(\frac{\beta}{2\pi}C_1 + C_2\right) > E_{OM-DLBOP}.$$

On obtient alors une forme polynomiale qui a au plus deux racines. Nous déterminons les valeurs correspondantes dans la section suivante.

Comme chaque nœud décide indépendamment entre les deux protocoles, il est possible que dans le même réseau, pour la même diffusion, les nœuds puissent faire des choix différents.

### 5.4.4 Adaptive Directed LMST Broadcast Oriented Protocol (ADLBOP)

Nous pouvons maintenant décrire l'algorithme ADLBOP qui utilise les modèles de communication un-vers-un et un-vers-plusieurs. ADLBOP est un protocole de diffusion basé sur DLBOP et OM-DLBOP (que nous avons décrit dans les sections précédentes). Chaque fois qu'un nœud reçoit le message diffusé, il démarre un mécanisme d'élimination limité à ses voisins LMST. À la fin de la période d'attente, le nœud choisit entre le modèle de communication un-vers-un ou un-vers-plusieurs. Pour un nœud $u$, l'algorithme de décision est le suivant :

- Soit $A$ l'ensemble des voisins non couverts et $B \subseteq A$ l'ensemble des voisins LMST non couverts. Nous définissons par $A'$ l'ensemble des nœuds appartenant à $A$ à une distance inférieure de $R_{opt}(4\pi/3)$. Comme précédemment, si $C_1 = C_2 = 0$ alors nous considérons que $R_{opt}(4\pi/3) = 0$. Le but du nœud $u$ est alors de couvrir l'ensemble $C = A' \cup B$. Si l'ensemble $C$ est vide, alors la retransmission est annulée.
- Le choix du modèle de communication est fait à partir d'une comparaison de la consommation énergétique utilisée pour couvrir $C$ :

  **Communication un-vers-un :** pour une diffusion à destination de l'ensemble $C$ avec le modèle de communication *un-vers-un*, chaque nœud retransmet le message vers ses voisins LMST non couverts. En moyenne, chaque nœud a seulement un voisin LMST non-couvert, donc la consommation énergétique avec le modèle *un-vers-un* en utilisant des envois d'angle $\beta$ peut-être évaluée par :

  $$E_{un-vers-un} = |C| \times e(\beta, d_{lmst}).$$

  Le nœud $u$ ignore la distance $d_{lmst}$ qui représente la longueur moyenne des arcs LMST. Il peut seulement l'estimer à partir de la distance le séparant de ses voisins LMST :

  $$d_{lmst}(u) \simeq \frac{1}{|B|}\sum_{v \in B} d(u, v). \tag{5.8}$$

  **Communication un-vers-plusieurs :** Soit $\theta$ l'angle nécessaire pour couvrir $C$ (si $\theta < \beta$ nous considérons que $\theta = \beta$) et $d$ la distance entre le nœud $u$ et le nœud le plus éloigné compris dans $C$. La consommation énergétique d'un simple envoi pour couvrir $C$ est :

  $$E_{un-vers-plusieurs} = e(\theta, d). \tag{5.9}$$

- Si $E_{un-vers-un} < E_{un-vers-plusieurs}$, le nœud $u$ décide d'utiliser le modèle de communication un-vers-un et d'envoyer un message d'angle $\beta$ pour chaque voisin LMST non couverts (les nœuds inclus dans $B$).

- Sinon, le nœud $u$ décide d'utiliser une communication un-vers-plusieurs et procède à un envoi d'angle $\beta$. Si $d < R_{opt}(\theta)$, la portée de l'émission est augmentée de manière à joindre les nœuds de $A$ qui sont plus proches que $R_{opt}(\theta)$.

Ainsi, le protocole ADLBOP est un protocole adaptatif de diffusion où la décision est prise localement pour chaque nœud.

## 5.5 Résultats Expérimentaux

Dans un premier temps, nous étudions l'effet de $R_{opt}$ pour une configuration donnée et les quatre modèles énergétiques décrit ci-dessus. Nous utilisons des réseaux générés aléatoirement de 500 nœuds (nous ne gardons que les graphes connectés), avec une portée maximale de 250 mètres. Les autres paramètres sont la taille de la zone d'évaluation $S = 1000 \times 1000$ (on obtient alors une densité théorique de 78 nœuds par zone de communication) et un angle minimal $\beta = \pi/9$. Nous évaluons chaque instance pour une portée $R_{opt}$ variant de 10m jusqu'à la portée maximale (250m).

Nous calculons les performances des protocoles OM-DLBOP et ADLBOP, car ce sont les seuls à être influencés par les valeurs de $R_{opt}$. Nous ajoutons aux graphiques les résultats les valeurs théoriques de $E_{OM-DLBOP}$ et $E_{DLBOP}$ pour la même configuration, de manière à comparer et justifier la validité de nos modèles théoriques.

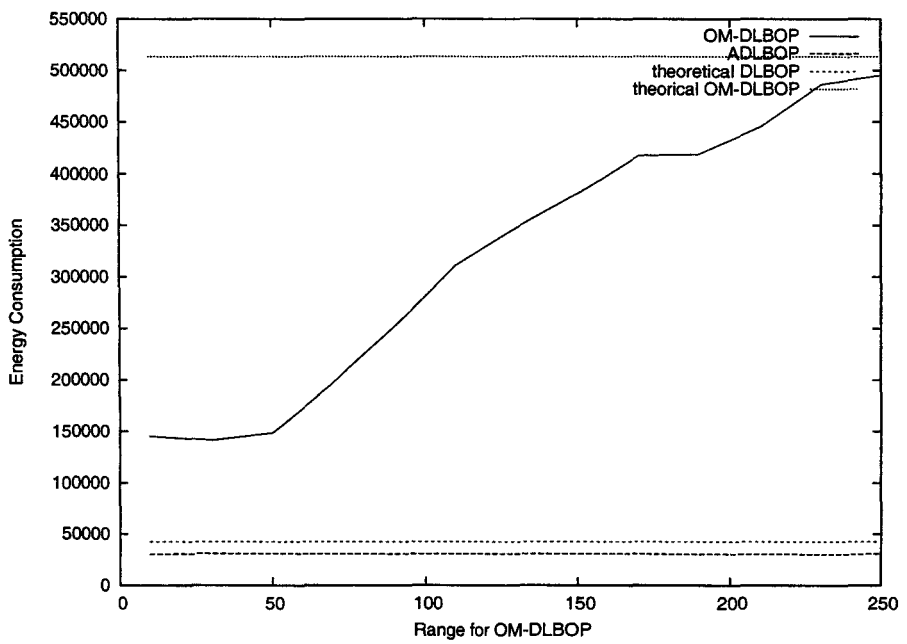



FIG. 5.6 – Évaluation de la portée optimale pour $\alpha = 2, C_1 = C_2 = 0$.

Les graphiques 5.6, 5.7, 5.8 et 5.9 représentent l'impact de $R_{opt}$ sur la consommation énergétique pour les différents protocoles. Concernant le cas où $\alpha = 2$ et $C_1 = C_2 = 0$, malgré les résultats théoriques qui donnent des résultats constants quel que soit $R_{opt}$, on trouve expérimentalement une augmentation de la consommation énergétique pour DLBOP. Ce phénomène est dû aux effets de bord. Dans tous les cas, les résultats présentés valident le choix de l'utilisation de $R_{opt} = 0$ dans le cas des protocoles OM-DLBOP et ADLBOP.

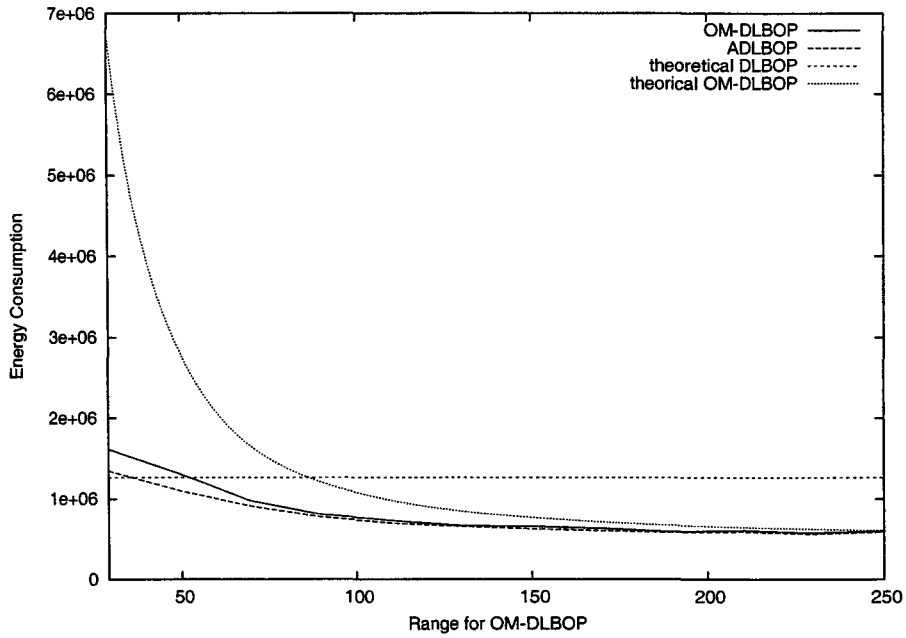



FIG. 5.7 – Évaluation de la portée optimale pour $\alpha = 2, C_1 \neq 0 \vee C_2 \neq 0$.

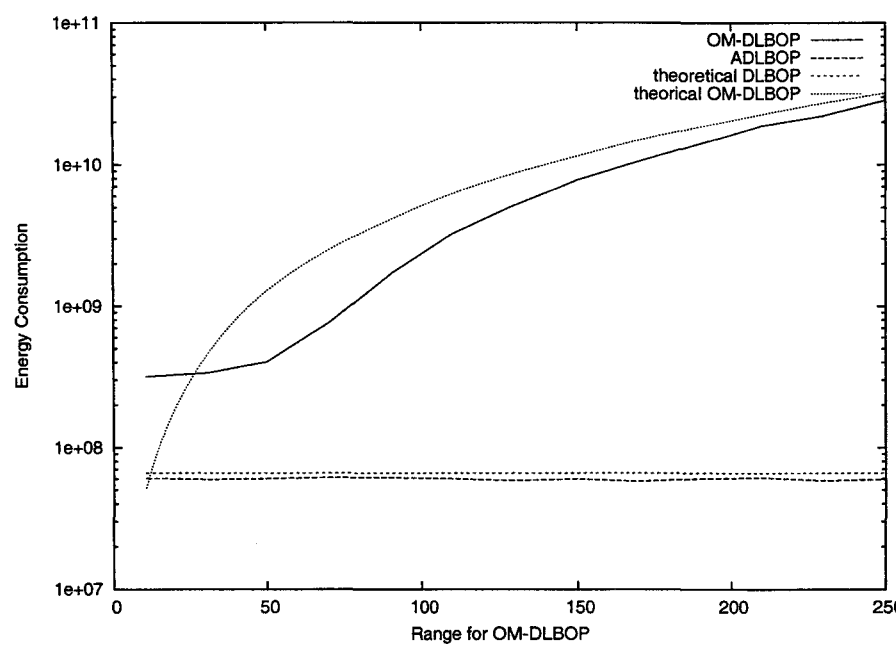



FIG. 5.8 – Évaluation de la portée optimale pour $\alpha > 2, C_1 = C_2 = 0$.

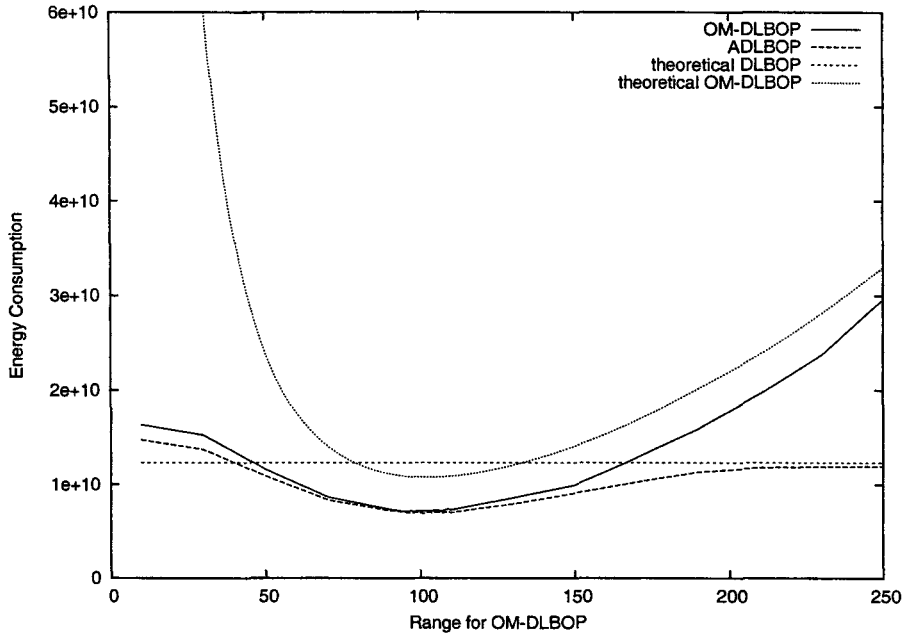



FIG. 5.9 – Évaluation de la portée optimale pour $\alpha > 2, C_1 \neq 0 \vee C_2 \neq 0$.

Dans le cas où $\alpha = 2$, et $C_1 \neq 0$ ou $C_2 \neq 0$ (figure 5.7), nous avons démontré que la meilleure solution est de maximiser $R_{opt}$. Dans ce cas, Les solutions de ADLBOP et DLBOP sont très proches. De plus, les deux courbes suivent le modèle théorique de DLBOP.

Pour le troisième modèle énergétique (figure 5.8), avec $\alpha > 2$ et $C_1 = C_2 = 0$ (présenté avec une échelle logarithmique pour les ordonnées), nous pouvons vérifier une nouvelle fois la validité de notre modèle théorique. Le protocole ADLBOP suit très rapidement la valeur théorique de DLBOP, ce qui prouve le résultat annoncé dans le tableau 5.1 (à savoir que la meilleure valeur de $R_{opt}$ est de réduire la portée à zéro). Plus généralement, si les constantes sont nulles, alors la meilleure solution est de réduire la portée de chaque envoi, et donc d'utiliser le protocole DLBOP. Signalons que, même si le mode ADLBOP donne les meilleures résultats, ce n'est pas forcément valable pour d'autres valeurs de $\beta$, $n$ et $S$, comme montré par les modèles théoriques de DLBOP et OM-DLBOP.

Le dernier modèle énergétique (figure 5.9), avec $\alpha > 2$, et $C_1 \neq 0$ ou $C_2 \neq 0$, présente un minimum lorsque $R_{opt} = 99$, ce qui correspond à l'analyse théorique (la valeur théorique pour la même configuration $R_{opt} = 102,41$). Le protocole ADLBOP réussit à adapter son comportement en fonction de $R_{opt}$ car il utilise OM-DLBOP quand celui ci devient plus intéressant.

Nous allons maintenant présenter les résultats pour les quatre modèles énergétiques. La configuration choisie est la suivante : $S = 1000 \times 1000$ avec $\beta = \pi/36$ ou $\beta = \pi/9$. L'énergie utilisée est présentée de manière normalisée par rapport à la plus basse consommation (qui est égale à 100).

Les graphiques 5.10 et 5.11 présentent les résultats pour le premier modèle énergétique (avec $\alpha = 2$ et $C_1 = C_2 = 0$). Le protocole OM-DLBOP est complètement inefficace, car la consommation augmente dans de grandes proportions, comparativement aux autres algorithmes. C'est le comportement attendu, car les autres protocoles ne sont pas gênés par des constantes non nulles. Le protocole DLBOP est lui très efficace, il donne des résultats proches de DBIP (de 26 à 33% en plus) en étant localisé.

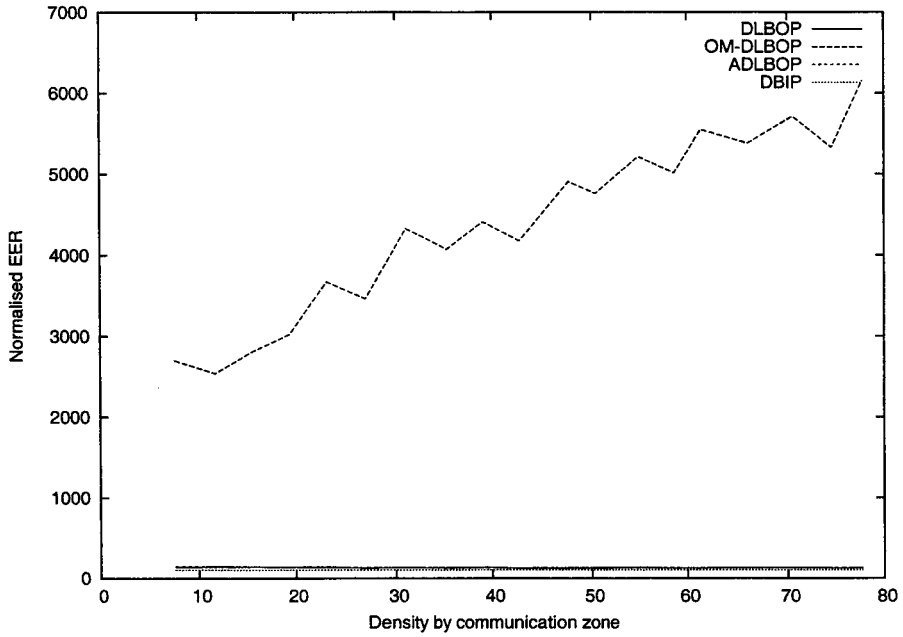



FIG. 5.10 – Consommation énergétique normalisée pour $\alpha = 2$, $C_1 = C_2 = 0$, $S = 1000 \times 1000$ et $\beta = \pi/36$.

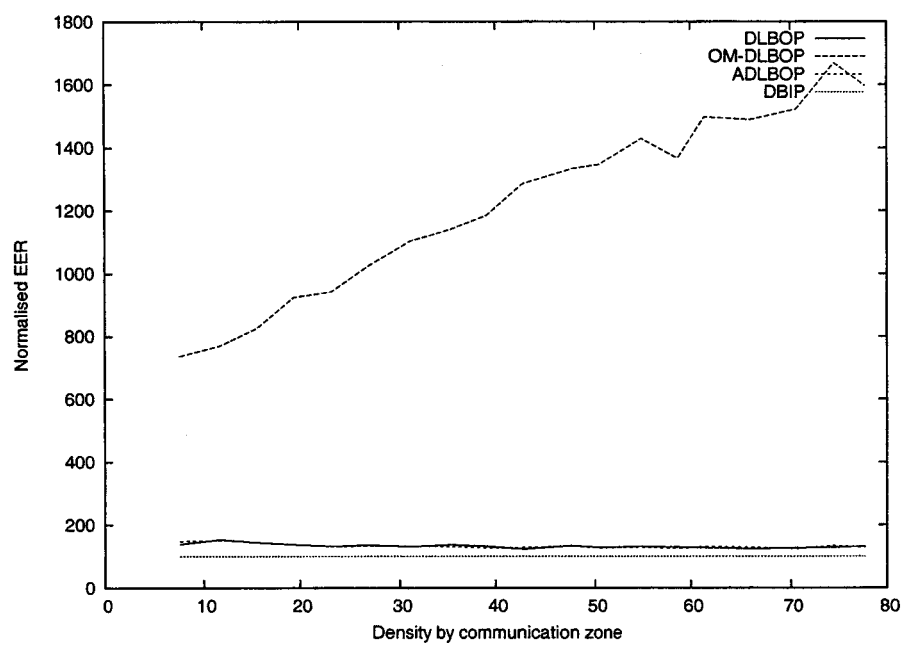



FIG. 5.11 – Consommation énergétique normalisée pour $\alpha = 2$, $C_1 = C_2 = 0$, $S = 1000 \times 1000$ et $\beta = \pi/9$.

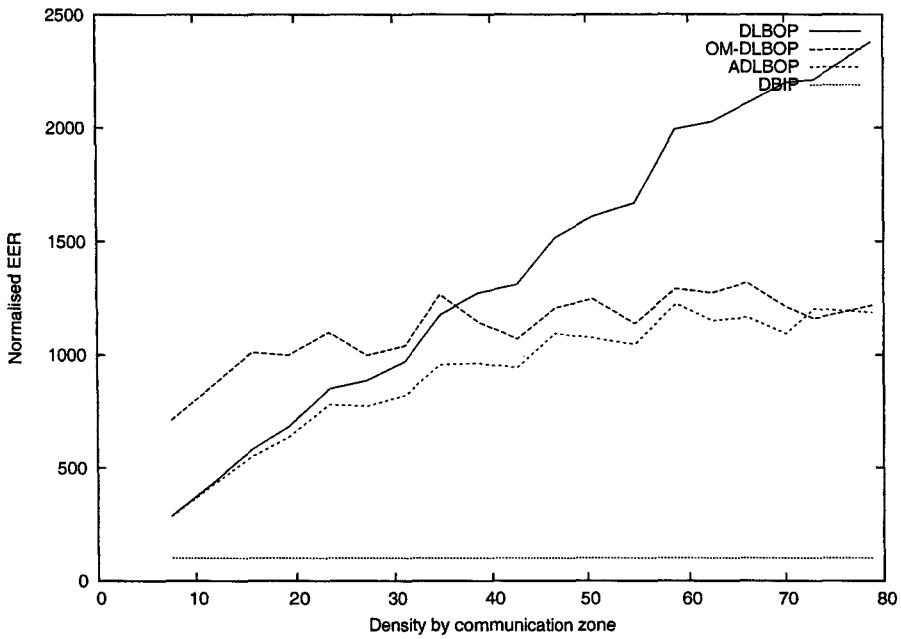



FIG. 5.12 – Consommation énergétique normalisée pour $\alpha = 2$, $C_1 = 8000$, $C_2 = 2000$, $S = 1000 \times 1000$ et $\beta = \pi/36$.

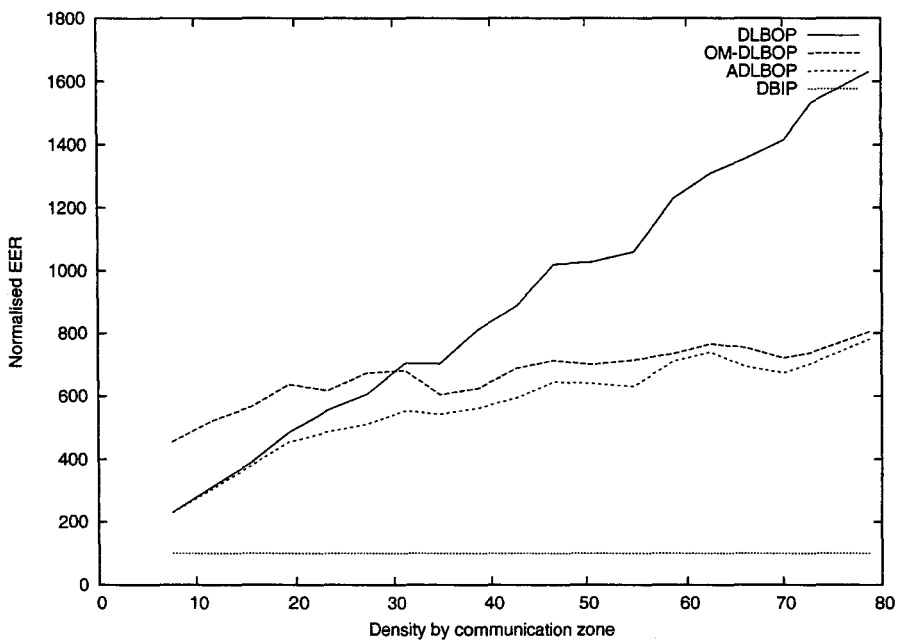



FIG. 5.13 – Consommation énergétique normalisée pour $\alpha = 2$, $C_1 = 8000$, $C_2 = 2000$, $S = 1000 \times 1000$ et $\beta = \pi/9$.

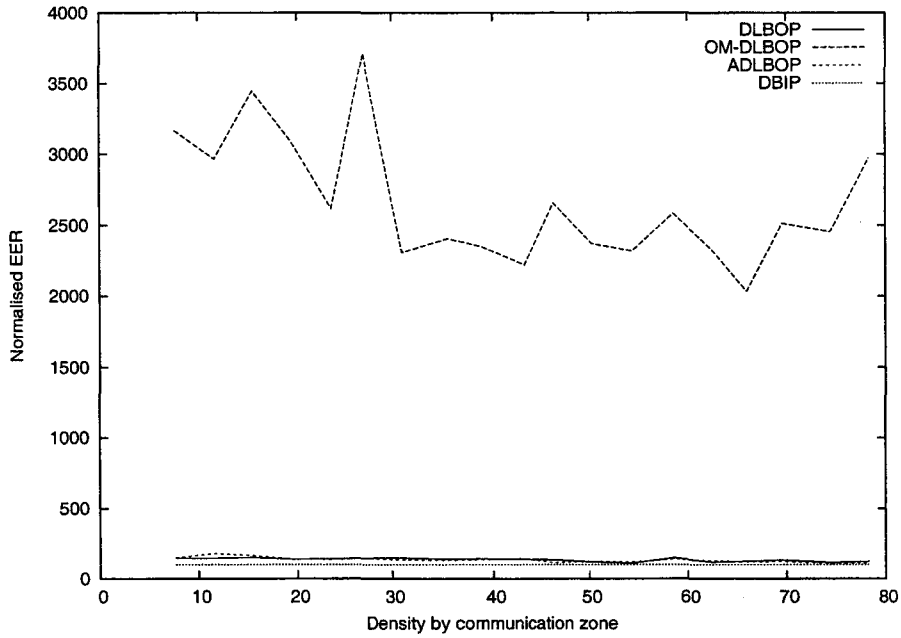



FIG. 5.14 – Consommation énergétique normalisée pour $\alpha = 4$, $C_1 = C_2 = 0$, $S = 1000 \times 1000$ et $\beta = \pi/36$.

Les résultats pour le second modèle énergétique (avec $\alpha = 2$, $C_1 = 8000$ et $C_2 = 2000$) sont présentés avec les figures 5.12 et 5.13. La portée optimale est fixée à la puissance maximale (250m). Ce choix provient de l'analyse résumée dans le tableau 5.1 et des premières expérimentations (voir la figure 5.7). Les graphiques présentent clairement l'intérêt du mode ADLBOP. En effet, quand la densité est inférieure à approximativement 37 nœuds par zone de communication, le modèle de communication *un-vers-un* est préféré. Après ce niveau, le protocole passe à l'utilisation plus accrue du modèle *un-vers-plusieurs*. Ce résultat est confirmé par la théorie, même si l'effet de bord est important et le seuil théorique est plus important (54 nœuds pour $\beta = \pi/9$ et 66 nœuds pour $\beta = \pi/36$).

Pour le troisième modèle énergétique (*i.e.* $\alpha = 4$ et $C_1 = C_2 = 0$), les résultats sont présentés avec les figures 5.14 et 5.15. Les algorithmes ont le même comportement que ceux du premier modèle énergétique : DLBOP est toujours meilleur et OM-DLBOP grandie en même temps que la densité. Plus généralement, avec des constantes nulles, il est plus intéressant d'utiliser la solution DLBOP car OM-DLBOP est inefficace : il n'y a pas de coût constant associé à chaque envoi.

Le dernier modèle énergétique ($\alpha = 4$, $C_1 = 8.10^7$ et $C_2 = 2.10^7$) est présenté avec les figures 5.16 et 5.17. Pour des densités faibles, c'est le protocole DLBOP qui agit. Par la suite, quand la densité augmente (entre 25 et 30 nœuds par zone de communication), le mode OM-DLBOP est utilisé pour améliorer les performances. On peut signaler que le mode ADLBOP utilise efficacement les deux protocoles simultanément, donnant un résultat meilleur que si l'un ou l'autre des protocoles avait été utilisé de manière unique. Ce phénomène peut s'expliquer par une utilisation simultanée de OM-DLBOP pour les voisinages denses et de DLBOP pour des densités plus faibles (par exemple sur les bords).

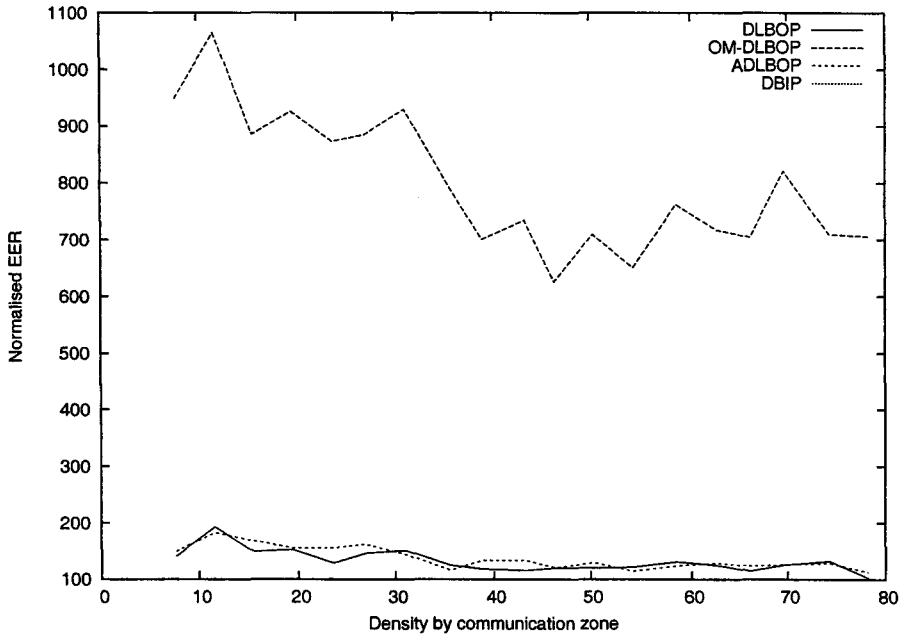



FIG. 5.15 – Consommation énergétique normalisée pour $\alpha = 4$, $C_1 = C_2 = 0$, $S = 1000 \times 1000$ et $\beta = \pi/9$.

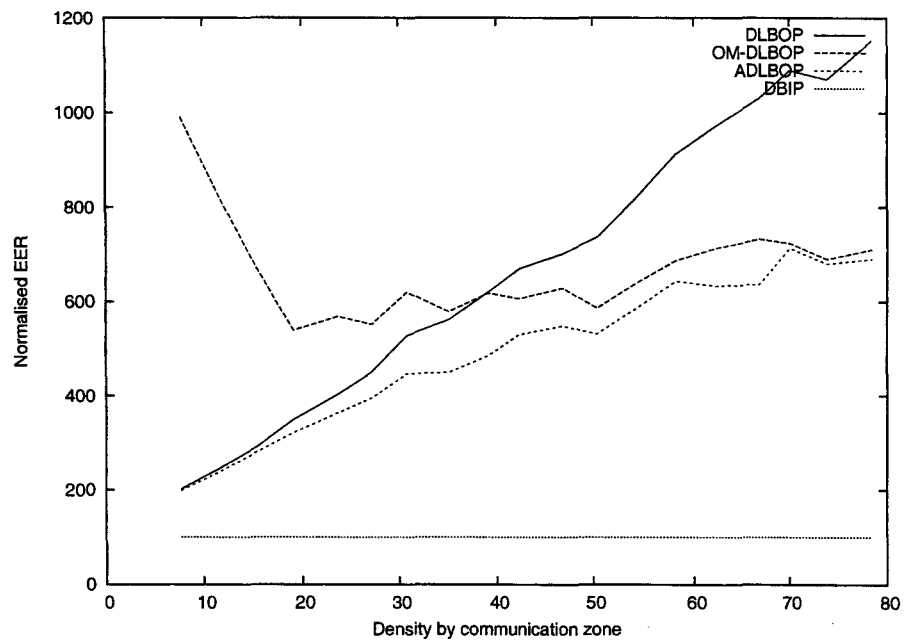



FIG. 5.16 – Consommation énergétique normalisée pour $\alpha = 4$, $C_1 = 8.10^7$, $C_2 = 2.10^7$, $S = 1000 \times 1000$ et $\beta = \pi/36$.

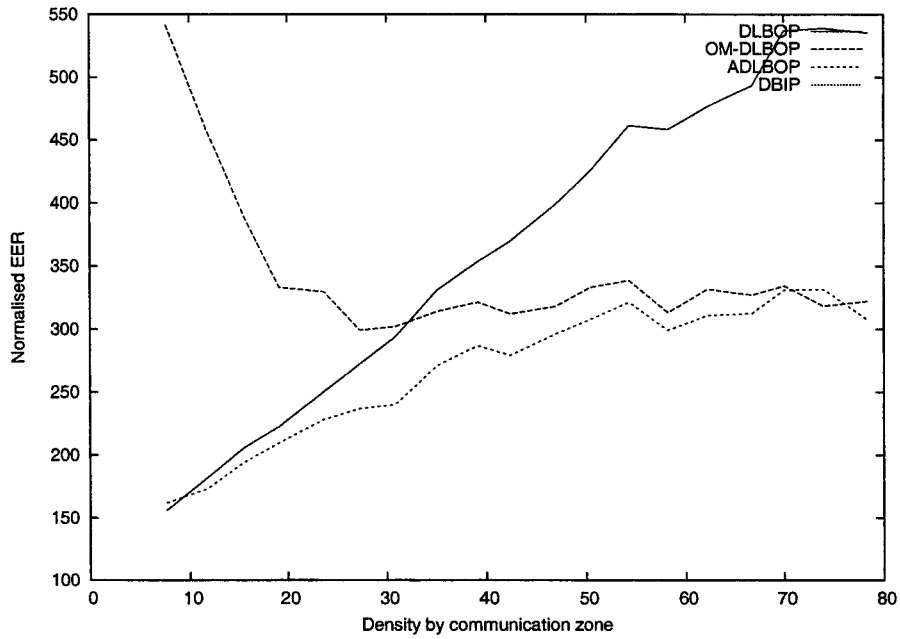



FIG. 5.17 – Consommation énergétique normalisée pour $\alpha = 4$, $C_1 = 8.10^7$, $C_2 = 2.10^7$, $S = 1000 \times 1000$ et $\beta = \pi/9$.

## 5.6 Conclusion

Nous avons proposé dans ce chapitre un nouveau protocole baptisé ADLBOP. Il utilise une combinaison de deux modèles de communication : *un-vers-un* et *un-vers-plusieurs*. Le premier réduit la consommation énergétique en utilisant des émissions d'angle minimal vers les voisins proches. Mais ce protocole souffre d'une très haute consommation en cas de fortes densités, comparé à DBIP. Le second modèle corrige ce problème en utilisant un angle variable de manière à couvrir un nombre important de nœuds, et donc d'offrir une consommation constante, quel que soit le nombre de nœuds. Le protocole ADLBOP est une version hybride sélectionnant l'un ou l'autre en fonction de l'énergie attendue. Nos résultats sont complétés par une étude théorique qui prouve la validité de notre approche, qui montre que les choix localisés de chaque nœud entre les deux modèles sont bons, et que le protocole offre une bonne économie d'énergie.

# Conclusion

Pour les travaux exposés dans ce document, nous proposons des approches originales. Le but étant de se détacher des travaux traditionnels en offrant à chaque fois une nouvelle ouverture aux problèmes rencontrés dans les réseaux ad hoc.

Si l'on prend le cas de l'approche stochastique, celle ci n'était pas utilisée car elle était indépendante de la topologie locale, donnant alors des résultats faibles. Nous avons donc proposé l'utilisation de d'une méthode aléatoire biaisée par l'évaluation de la topologie locale. Pour ce dernier point, nous avons proposé l'utilisation d'une approche statistique pour évaluer une pseudo-distance entre deux nœuds, basée sur l'organisation du voisinage. Ainsi, le protocole privilégie de manière stochastique les voisins à l'extremité de la zone de communication, et permet de garantir une couverture complète du réseau avec l'aide d'un mécanisme d'élimination des voisins.

Dans le cas de l'utilisation de RNG, nous offrons un moyen de construire un graphe coplanaire, ce qui réduit considérablement le problème de la décision de réémission (dans BRP). De plus, les propriétés des graphes RNG ou LMST (distance réduite entre voisins, connexité, nombre moyen de voisins stable...) sont intéressantes dans le cadre des réseaux sans fil. De plus, offrir de réduire l'energie consommée avec des algorithmes localisés est une réelle nouveauté, car elle permet de s'affranchir de la connaissance de l'ensemble du réseau.

## Perspectives

Les différentes approches proposées peuvent, pour certaines, ouvrir des perspectives sur d'autres travaux. L'idée d'utiliser des algorithmes de réduction de graphe semble très intéressante. Il semble difficile de pouvoir obtenir une meilleure réduction que LMST, mais celle-ci est basée sur des informations à un saut. On peut imaginer des nouveaux algorithmes de réduction de graphe utilisant des informations à deux sauts ou plus. Même si cette information est moins fiable, elle peut quand même servir pour améliorer la réduction de portée (comme dans RBOP, DRBOP et DLBOP) ou pour obtenir une meilleure décision de réémission (comme RRS). De plus, l'utilisation de tels algorithmes peut éventuellement servir dans d'autres cas que la diffusion, comme le routage par exemple.

De même, l'utilisation d'une approche stochastique présente certains intérêt, comme démontré par l'algorithme BRP. Certes, l'utilisation naïve ne semble pas donner de bons résultats. Mais combinée à d'autres algorithmes, elle peut offrir une information supplémentaire pour la prise de décision. L'idée d'utiliser des algorithmes probabilistes doit résulter d'un manque d'information dont le relevé serait trop coûteux ou impossible. Elle offre alors un aide qui peut se reveler utile lors d'une prise de décision. En effet, elle permet de séléctionner un sous-ensemble des nœuds de manière totalement autonome, sans coopération ou communications supplémentaires. De plus, elle n'est pas influencée par les changments topologiques.

La notion de pseudo-distance avec les algorithmes BRP et RRS peut être réappliquée à de très

nombreux protocoles. L'avantage est énorme : il n'est plus nécessaire d'avoir des outils de positionnement pour avoir une idée de la distance séparant deux nœuds. Il existe néanmoins des restrictions à cette idée. Premièrement, elle nécessite d'avoir une densité acceptable pour avoir une pseudo-distance valable. De plus, il n'y a pas de relation directe entre la pseudo-distance et la distance réelle. Il est impossible d'avoir une fonction permettant de passer de l'une à l'autre. La pseudo-distance ne peut servir que comme critère, par exemple de comparaison, et ne pourrait servir dans un algorithme comme RBOP, où la pseudo-distance ne peut pas donner la distance pour réémettre le message. Nénamoins, il pourrait être utile de revoir l'ensemble des algorithmes de diffusion et/ou de routage pour voir si ceux-ci pourraient utiliser cette nouvelle notion.

Les deux dernières notions développées peuvent se caractériser par un certain « flou » : une information aléatoire ou donnat un résultat abstrait (la pseudo-distance). Jusqu'ici, le grand intérêt des chercheurs dans la communauté des réseaux ad hoc a toujours été d'avoir les informations les plus précises possibles. Ce pré-requis entraîne certaines nécessités, comme émettre une quantité importante d'information de façon régulière. Pourtant, utiliser une information un peu moins stricte peut offrir certains avantages, comme celui de réduire la masse d'information nécessaire. Une nouvelle voie est donc possible : offrir une information « floue » qui se précise en fonction du contexte, comme le comportement du groupe ou de la distance séparant le noeud cherchant une destination. Cette notion obscure et difficilement matérialisable peut offrir enormémemnt de nouvelles possibilités, et ainsi permettre d'envisager des réseaux ad hoc plus conséquents (plus denses ou plus grands).

# Bibliographie


[1] N. Abramson. The aloha system - another alternative for computer communications. In *Proc. Fall Joint Computer Conference*, pages 281–285, 1970.

[2] C. Adjih, P. Jacquet, and L. Viennot. Computing connected dominating sets with multipoint relays. Technical report, INRIA (Institut National de Recherche en Informatique et en Automatisme, October 2002.

[3] S. Banerjee and A. Misra. Minimum energy paths for reliable communication in multi-hop wireless networks. In *Proc. Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHoc'2002)*, Lausanne, Switzerland, 2002.

[4] N. Bansal and Z. Liu. Capacity, delay and mobility in wireless ad-hoc networks. In *Proc. IEEE INFOCOM 2003*, San Francisco, USA, 2003.

[5] S. Basagni, I. Chlamtac, and V. R. Syrotiuk. Dynamic source routing for ad hoc networks using the global positioning system. In *the IEEE Wireless Communications and Networking Conference 1999 (WCNC'99)*, New Orleans, Louisiana, September 1999.

[6] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, editors. *Ad Hoc Networking*. IEEE Press and John Wiley and Sons, Inc., New York, 2003. To appear.

[7] B. Bellur and R. Ogier. A reliable, efficient topology broadcast protocol for dynamic networks. In *Proc. IEEE INFOCOM '99*, New York, USA, March 1999.

[8] A. Benlarbi-Delaï, D. Simplot, J. Cartigny, and J-C. Cousin. Using 3d indoor microwave phase sensitive stereoscopic location system to reduce energy consumption in wireless ad-hoc networks. In *Proc. Smart Objects Conference (sOc'2003)*, Grenoble, France, 2003.

[9] P. Bhagwat and A. Segall. A routing vector method (rvm) for routing in bluetooth scatternets. In *Mobile Multimedia Communications*, 1999.

[10] V. Bharghavan, A.J. Demers, S. Shenker, and L. Zhang. MACAW : A media access protocol for wireless LAN's. In *Comput. Commun. Rev*, pages 212–225, October 1994.

[11] J. Cartigny, F. Ingelrest, and D. Simplot. Rng relay subset flooding protocols in mobile ad-hoc networks. *International Journal of Foundations of Computer Science*, 14(2) :253–265, 2003.

[12] J. Cartigny, F. Ingelrest, D. Simplot-Ryl, and I. Stojmenović. Localized LMST and RNG based minimum-energy broadcast protocols in ad hoc networks. *Ad Hoc Networks*, 2004. To appear.

[13] J. Cartigny and D. Simplot. Border node retransmission based probalistic broadcast protocols in ad-hoc networks. In *Proc. 36th Annual Hawaii International Conference on System Sciences (HICSS'03)*, Hawaii, USA, 2003.

[14] J. Cartigny and D. Simplot. Border node retransmission based probalistic broadcast protocols in ad-hoc networks. *Telecommunication Systems*, 22(1–4) :189–204, 2003.

[15] J. Cartigny, D. Simplot, and I. Stojmenović. Localized energy efficient broadcast for wireless networks with directional antennas. In *Proc. IFIP Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET'2002)*, Sardegna, Italy, 2002.

[16] J. Cartigny, D. Simplot, and I. Stojmenović. Localized minimum-energy broadcasting in ad-hoc networks. In *Proc. IEEE INFOCOM 2003*, San Fransisco, USA, 2003.

[17] J. Cartigny, D. Simplot-Ryl, and I. Stojmenovic̀. An adaptive localized scheme for energy-efficient broadcasting in ad hoc networks with directional antennas. submitted.

[18] G. Chen, F.G. Nocetti, J.S. Gonzalez, and I. Stojmenović. Connectivity based k-hop clustering in wireless networks. In *Proc. Int. Conf System Science*, Hawaii, January 2002.

[19] Y. Chen, E.G. Sirer, and S.B. Wicker. On selection of optimal transmission power for ad hoc networks. In *Proc. 36th Hawaii International Conference on System Sciences (HICSS'2003)*, Hawaii, January 2003.

[20] C.C. Chiang, H.K. Wu, W. Liu, and M. Gerla. Routing in clustered multihop mobile wireless networks with fading channel. In *Proc. IEEE Singapore International Conference on Networks*, 1997.

[21] T. Chu and I. Nikolaidis. Energy efficient broadcast in mobile ad hoc networks. In *Proc. Ad-Hoc Networks and Wireless (ADHOC-NOW)*, Toronto, Canada, 2002.

[22] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, and L. Viennot. Optimized link state routing protocol. In *Proc. IEEE INMIC*, Pakistan, 2001.

[23] T. Clausen, P. Jacquet, A. Laouitiand P. Minet, P. Muhlethaler, A. Qayyum, and L.Viennot. Optimized link state routing protocol. IETF Internet Draft, http ://www.ietf.org/internet-drafts/draft-ietf-manet-olsr-07.txt, December 2002.

[24] A. Clementi, P. Penna, and R. Silvestri. The power range assignment problem in radio networks on the plane. In H.Reichel and S.Tison, editors, *Proc. 17th Symp. on Theoretical Computer Science (STACS'00)*, volume 1770, pages 651–660, Lille, France, 2000.

[25] IEEE Computer Society LAN MAN Standards Committee. Wireless lan medium access control (mac) and physical layer (phy). IEEE Std. 802.11-1197.

[26] F. Dai and J. Wu. Distributed dominant pruning in ad hoc wireless networks. Technical report, Florida Atlantic University, Feb 2002.

[27] J. Deng and Z. Haas. Dual busy tone multiple access (dbtma) : A new medium access control for packet radio networks. In *Proc. IEEE ICUPC'98*, Florence, Italy, October 1998.

[28] R. Dube, C. Rais, K. Wang, and S. Tripathi. Signal stability based adaptive routing (ssa) for ad hoc mobile networks. *IEEE Personal Communication*, February 1997.

[29] D. Estrin, R. Govindan, J.S. Heidemann, and S. Kumar. Next century challenges : Scalable coordination in sensor networks. In *Mobile Computing and Networking*, pages 263–270, 1999.

[30] O. Eğecioğlu and T.F. Gonzalez. Minimum-energy broadcast in simple graphs with limited node power. In *Proc. IASTED Int. Conf. on Parallel and Distributed Computing and Systems*, pages 334–338, Anaheim, Canada, 2001.

[31] L.M. Feeney. A taxonomy for routing protocols in mobile ad hoc networks. Technical Report T99/07, SICS (Swedish Institute of Computer Science), Sweden, October 1999.

[32] L.M. Feeney. An energy-consumption model for performance analysis of routing protocols for mobile ad hoc networks. *ACM J. of Mobile Networks and Applications*, 3(6) :239–249, 2001.

[33] L.M. Feeney. A qos aware power save protocol for wireless ad hoc networks. In *Proc. Med-Hoc-Net 2002*, Sardegna, Italy, September 2002.

[34] L.M. Feeney and M. Nilson. Investigating the energy consumption of a wireless network interface in an ad hoc networking environment. In *Proc. IEEE INFOCOM 2001*, pages 1548–1557, Anchorage AK, April 2001.

[35] C.L. Fullmer and J.J. Garcia-Luna-Aceves. Floor acquisition multiple access (FAMA) for packet-radio networks. In *SIGCOMM*, pages 262–273, 1995.

[36] J. Haartsen, M. Naghshineh, J. Inouye, O. Joeressen, and W. Allen. Bluetooth : Vision, goals, and architecture. *Mobile Computing and Communications Review*, 2(4) :38–45, October 1998.

[37] Z.J. Haas and J. Deng. Dual busy tone multiple access (dbtma) - performance evaluation. In *VTC'99*, Houston, TX, May 1999.

[38] Z.J. Haas and M.R. Pearlman. The performance of query control schemes for the zone routing protocol. In *ACM SIGCOMM'98*, 1998.

[39] Z.J. Haas and S. Tabrizi. On some challenges and design choices in ad-hoc communications. In *IEEE MILCOM'98*, Bedford, MA, October 1998.

[40] M. Hauspie, J. Carle, and D. Simplot. Partition detection in mobile ad-hoc networks. In *Proc. 2nd IFIP Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET'2003)*, Mahdia, Tunisia, 2003.

[41] M. Hauspie, J. Carle, and D. Simplot. Partition detection in mobile ad-hoc networks using multiple disjoint path set. In *1st International Workshop on Objects models and Multimedia technologies (OMMT)*, Genova, Switzerland, 2003. to appear.

[42] R.J. Marks II, A.K. Das, M. El-Sharkawi, P. Arabshahi, and A. Gray. Minimum power broadcast trees for wireless networks : optimizing using the viability lemma. In *Proc. IEEE Int. Symp. on Circuits and Systems*, Scottsdale, USA, pages 245–248, 2002.

[43] F. Ingelrest, D. Simplot-Ryl, and I. Stojmenocič. Target transmission radius over lmst for energy-efficient broadcast protocol in ad hoc networks. submitted.

[44] A. Jain. Routing protocols for mobile ad-hoc networks. Technical report, Departement of computer science and engineering, Indian institute of Technology, Kanpur, 2000.

[45] J.W. Jaromczyk and G.T. Toussaint. Relative neighborhood graphs and their relatives. In *Proc. IEEE*, volume 80, pages 1502–1517, 1992.

[46] D. Johnson. Routing in ad hoc networks of mobile hosts. In *Workshop on Mobile Computing Systems and Applications*, Santa Cruz, CA, U.S., 1994.

[47] D.B. Johnson, D.A. Maltz, Y. Hu, and J.G. Jetcheva. The dynamic source routing protocol for mobile ad hoc networks. IETF Internet Draft, http ://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-07.txt, February 2002.

[48] L.R. Ford Jr. and D.R. Fulkerson. Improving the routing and addressing of ip. *IEEE Journal Network Magazine*, 7 :10–15, May 1993.

[49] E.D. Kaplan, editor. *Understanding Gps : Principles and Applications*. Artech House Telecommunications Library, 1996.

[50] P. Karn. Maca - a new channel access method for packet radio. In *ARRL/CRRL Amateur Radio 9th Computer Networking Conference*, pages 134–140, 1990.

[51] L.M. Kirousis, E. Kranakis, D. Krizanc, and A. Pelc. Power consumption in packet radio networks. In R.Reischuk and M.Morvan, editors, *Proc. 14th Symposium on Theoretical Computer Science (STACS'97)*, volume 1200 of *Lecture Notes in Computer Science*, pages 363–374, Hansestadt Lübeck, Germany, 1997. Springer-Verlag, Berlin.

[52] L. Kleinrock and F.A. Tobagi. Packet switching in radio channels : carrier sense multiple-access modes and their througput-delay characteristics. *IEEE Trans. Commun.*, 12 :1400–1416, 1075.

[53] B. Leiner, D. Nielson, and F. Tobagi, editors. *Proc. IEEE (Special Issue, Packet Radio Networks)*, volume 25, January 1987.

[54] N. Li and J.C. Hou. BLMST : A scalable, power-efficient broadcast algorithm for wireless sensor networks. Submitted.

[55] N. Li, J.C. Hou, and L. Sha. Design and analysis of an mst-based topology control algorithm. In *Proc. IEEE INFOCOM 2003*, San Francisco, USA, 2003.

[56] H. Lim and C. Kim. Flooding in wireless ad hoc networks. In *Proc. ACM MSWiM Worshop (MOBICOM'2000)*, August 2000.

[57] C.R. Lin and M. Gerla. Adaptive clustering for mobile wireless networks. *IEEE Journal of Selected Areas in Communications*, 15(7) :1265–1275, 1997.

[58] C.R. Lin and M. Gerla. Maca/pr : An asynchronous multimedia multihop wireless network. In *IEEE INFOCOM'97*. IEEE, 1997.

[59] S. Lindsey and C.S. Raghavendra. Energy efficient broadcasting for situation awareness in ad hoc networks. In *Proc. Int. Conf. Parallel Processing (ICPP'01)*, Valencia, Spain, 2001.

[60] E.L. Lloyd, R. Liu, M.V. Marathe, R. Ramanathan, and S.S. Ravi. Algorithmic aspects of topology control problems for ad hoc networks. In *Proc. Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHoc'2002)*, Lausanne, Switzerland, 2002.

[61] W. Lou and J. Wu. On reducing broadcast redundancy in ad hoc wireless networks. *IEEE Transaction on Mobile Computing*, 1(2), apr–jun 2002.

[62] S. Mann. Smart clothing : The shift to wearable computing. *Communications of the ACM*, pages 23–24, August 1996.

[63] R. Morris, J. Jannotti, F. Kaashoek, J. Li, and D.S.J. De Couto. CarNet : A scalable ad hoc wireless network system. In *Proc. 9th ACM SIGOPS European workshop : Beyond the PC : New Challenges for the Operating System*, Kolding, Denmark, September 2000.

[64] R. Morris, J. Jannotti, J. Li, D. Decouto, and F. Kaashoek. Carnet : A scalable ad hoc wireless network system. In *9th ACM SIGOPS European Workshop*, Kolding, Denmark, September 2000.

[65] M. Mouly, M.B. Pautet, and T. Haug. *The GSM System for Mobile Communications*. Telecom Publishing, 1992.

[66] S. Murthy and J.J. Garcia-Luna-Aceves. A routing protocol for packet radio networks. In *Proc. ACM First International Conference on Mobile Computing & Networking (MOBICOM'95)*, November 1995.

[67] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu. The broadcast storm problem in a mobile ad hoc network. In *Proc. MobiCom'99*, pages 151–162, Seattle WA, August 1999.

[68] E. Pagani and G.P. Rossi. Providing reliable and fault tolerant broadcast delivery in mobile ad hoc networks. *Mobile Networks and Applications*, 4 :175–192, 1999.

[69] M. Parameswaran, A. Susarla, and A.B. Whinston. P2P networking : An information sharing alternative. *IEEE Computer*, 34(7), 2001.

[70] V.D. Park and M.S. Corson. A highly adaptive distributed routing algorithm for mobile wireless networks. In *Proc. IEEE INFOCOM '97*, Kobe, Japan, April 1997.

[71] C.E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance vector (DSDV) for mobile computers. *ACM SIGCOMM '94 Computer Communications Review*, 24(4) :234–244, October 1994.

[72] C.E. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In *Proc. Second Annual IEEE Workshop on Mobile Computing Systems and Apllications*, pages 90–100, February 1999.

[73] C.E. Perkins, E.M. Royer, and S.R. Das. Ad hoc on-demand distance vector (AODV) routing. IETF Internet Draft, http ://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-12.txt, November 2002.

[74] C.E. Perlins, editor. *Ad Hoc Networking*. Addison Wesley, 2001.

[75] N. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket location-support system. In *Proc. MOBICOM'2000*, Boston, USA, 2000.

[76] A. Qayyum, L. Viennot, and A. Laouiti. Multipoint relaying for flooding broadcast messages in mobile wireless networks. In *Proc. 35th Annual Hawaii International Conference on System Sciences (HICSS'02)*, Hawaii, 2002.

[77] M. Rahnema. Overview of the gsm system and protocol architecture. *IEEE Communications Magazine*, 31(4) :92–100, apr 1993.

[78] S. Ramanathan and M. Steenstrup. A survey of routing techniques for mobile communications networks. *ACM/Baltzer Mobile Networks and Applications*, 1(2) :89–104, 1996.

[79] V. Rodoplu and T.H. Meng. Minimum energy mobile wireless networks. In *IEEE J. Selected Area in Comm*, volume 17, pages 1333–1344, 1999.

[80] Y. Sasson and D. Cavin abd A. Schiper. Probabilistic broadcast for flooding in wireless mobile ad hoc networks. Technical report, Swiss Federal Institute of Technology (EPFL), 2002.

[81] M. Seddigh, J.S. Gonzalez, and I. Stojmenović. Rng and internal node based broadcasting algorithms for wireless one-to-one networks. *ACM Mobile Computing and Communications Review*, 5(2) :37–44, 1999.

[82] S. Singh and C. Raghavendra. Pamas : Power aware multi-access protocol with signalling for ad hoc networks. In *ACM Computer Communications Review*, 1999.

[83] A. Spyropoulos and C.S. Raghavendra. Energy efficient communications in ad hoc networks using directional antennas. In *Proc. IEEE INFOCOM 2002*, New-York, USA, 2002.

[84] I. Stojmenović, editor. *Handbook of Wireless Networks and Mobile Computing*. John Wiley & Sons, 2002.

[85] I. Stojmenović, M. Seddigh, and J. Zunic. Internal node based broadcasting algorithms in wireless networks. In *Proc. Hawaii Int. Conf. on System Sciences*, January 2001.

[86] I. Stojmenović, M. Seddigh, and J. Zunic. Dominating sets and neighbor elimination based broadcasting algorithms in wireless networks. *IEEE Transactions on Parallel and Distributed Systems*, 13(1) :14–25, January 2002.

[87] F. Talucci and M. Gerla. Maca-bi(maca by invitation). a wireless mac protocol for high speed ad hoc networking. In *IEEE ICUPC'97*. IEEE, 1997.

[88] F. Talucci, M. Gerla, and L. Fratta. Maca-bi(maca by invitation)-a receiver oriented access protocol fot wireless multihop network. In *IEEE PIMRC'97*. IEEE, 1997.

[89] A.S. Tanenbaum. *Computer Networks*. Prentice-Hall, third edition, 1996.

[90] D. Tian and N.D. Georganas. A node scheduling scheme for energy conservation in large wireless sensor networks. *Wireless Communications and Mobile Computing Journal*, May 2002.

[91] C.-K. Toh. *Ad Hoc Mobile Wireless Networks : Protocols and Systems*, chapter 6. Prentice Hall, 2002.

[92] G. Toussaint. The relative neighborhood graph of finite planar set. *Pattern Recognition*, 12(4) :261–268, 1980.

[93] Y.-C. Tseng, Y.-N. Chang, and B.-H. Tzeng. Energy-efficient topology control for wireless ad hoc sensor networks. In *Proc. Int. Conf. Parallel and Distributed Systems (ICPADS 2002)*, Tawain, 2002.

[94] Manet (Mobile Ad-hoc NETwork) group of IETF (Internet Enginering Task Force). URL : http ://tonnant.itd.nrl.navy.mil/manet/manet_home.html.

[95] R.B. Urquhart. Some properties of the planar euclidean relative neighborhood graph. *Pattern Recognition Letters*, pages 317–322, 1983.

[96] P.-J. Wan, G. Calinescu, X.-Y. Li, and O. Frieder. Minimum energy broadcast routing in static ad-hoc wireless networks. *ACM Wireless Networks*, 2002.

[97] M. Weiser. Some computer science issues in ubiquitous computing. *CACM*, 36(7), July 1993.

[98] J.E. Wieselthier, G.D. Nguyen, and A. Ephremides. On the construction of energy-efficient broadcast and multicast trees in wireless networks. In *Proc. IEEE INFOCOM 2000*, pages 585–594, Tel Aviv, Israel, 2000.

[99] J.E. Wieselthier, G.D. Nguyen, and A. Ephremides. Energy-limited wireless networking with directional antennas : the case of session-based multicasting. In *Proc. IEEE INFOCOM 2002*, New-York, USA, 2002.

[100] J. Wu and H. Li. A dominating-set-based routing scheme in ad hoc wireless networks. In *Proc. 3rd Int'l Workshop Discrete Algorithms and Methos for Mobile Computing and Comm (DIALM'99)*, pages 7–14, Seattle, USA, August 1999.

[101] J. Wu, B. Wu, and I. Stojmenović. Power-aware broadcasting and activity scheduling in ad hoc wireless networks using connected dominating sets. In *Proc. IASTED WOC'02*, July 2002.

[102] L. Zhou and Z.J. Haas. Securing ad hoc networks. *IEEE Network Magazine*, 13(6), 1999.

[103] G. Zussman and A. Segall. Energy efficient routing in ad hoc disaster recovery networks. In *Proc. IEEE INFOCOM 2003*, San Francisco, USA, 2003.